

BlackBerry Business Cloud Services



Administration Guide

Contents

1	About BlackBerry Business Cloud Services	8
	BlackBerry Business Cloud Services feature overview	8
	BlackBerry solution comparison chart	9
2	Connecting to Blackberry Business Cloud Services	15
	System requirements: Browser for BlackBerry Business Cloud Services	15
	Enabling the BlackBerry Business Cloud Services in Microsoft Office 365	16
	Enable the BlackBerry Business Cloud Services and register your organization as a tenant	16
	Log in to the BlackBerry Administration Service	17
	There is a problem with this website's security certificate	18
	This connection is untrusted	19
3	Configuring user accounts	20
	Creating groups	20
	Create a group to manage similar user accounts	20
	Add user accounts to a group	20
	Adding user accounts to the BlackBerry Business Cloud Services	21
	Add a user account	21
	Importing a list of user accounts to the BlackBerry Business Cloud Services	22
	Export a list of user accounts	24
4	Activating BlackBerry devices	26
	Activate a device using the BlackBerry Administration Service	26
	Activating a device over the wireless network	27
	Activation passwords	27
	Send an activation password to a user	28
	Send an activation password to multiple users	28
	Activating devices using the BlackBerry Web Desktop Manager	29
5	Using IT policies to manage security	30
	Using IT policy rules to manage security	30
	Preconfigured IT policies	31
	Default values for preconfigured IT policies	31
	Creating IT policies	33
	Create an IT policy	33
	Create an IT policy based on an existing IT policy	33
	Change the value for an IT policy rule	34
	Assign an IT policy to a group	34
	Assign an IT policy to a user account	34

	Resolving IT policy conflicts	35
	How conflicting IT policies are resolved	35
	Rank IT policies	36
	Preview how the BlackBerry Business Cloud Services resolves IT policy conflicts	37
	View the resolved IT policy rules that are assigned to a user account	37
	Sending an IT policy over the wireless network	38
	Resend an IT policy to a device manually	38
	Export all IT policy data to a data file	38
	Delete an IT policy	39
6	Setting up cloud messaging services	40
	Creating email message filters	40
	Create an email message filter	40
	Turn on an email message filter that applies to a specific user account	41
	Copying existing email message filters to user accounts	42
	Export email message filters for a user account	42
	Import email message filters for a user account	42
	Mapping contact-information fields for synchronization and contact lookups	43
	Map a contact list field to a contact list field on a device	43
	Map a contact list field from an email account to a contact list field on a device	44
7	Configuring the BlackBerry Web Desktop Manager	45
	Installing the client components of the BlackBerry Web Desktop Manager on users' computers	45
	Allow users to activate devices using the BlackBerry Web Desktop Manager	45
	Allow users to perform self service tasks using the BlackBerry Web Desktop Manager	46
	Allow users to back up and restore data using the BlackBerry Web Desktop Manager	46
	Configure the domains for backing up data using the BlackBerry Web Desktop Manager	47
8	Installing applications on devices	48
	Installing applications using the BlackBerry Desktop Software	48
	Make an application available for download from the BlackBerry Desktop Software	49
	Installing applications using a web browser on devices	49
	Make an application available on a web server	49
	Install an application using a web browser on the device	50
9	Creating and configuring Wi-Fi profiles and VPN profiles	51
	Creating and configuring Wi-Fi profiles	51
	Prerequisites: Creating Wi-Fi profiles and VPN profiles	51
	Create a Wi-Fi profile	52
	Create a Wi-Fi profile based on an existing Wi-Fi profile	52
	Configure a Wi-Fi profile	53
	Assign a Wi-Fi profile to a group	53
	Assign a Wi-Fi profile to a user account	54
	Delete a Wi-Fi profile	54

	Creating and configuring VPN profiles	54
	Create a VPN profile	55
	Create a VPN profile based on an existing VPN profile	55
	Configure a VPN profile	55
	Assign a VPN profile to a group	56
	Assign a VPN profile to a user account	56
	Associate a VPN profile with a Wi-Fi profile	57
	Delete a VPN profile	57
	Importing profile information from a .csv file	58
	Best practices: Creating a .csv file that contains profile information that you want to import	58
	Create a .csv file that contains profile information that you want to import	58
	Import profile information from a .csv file	60
10	Configuring encryption and authentication methods for Wi-Fi enabled devices	62
	Configuring WEP encryption	62
	Configure WEP keys for devices using a Wi-Fi profile	62
	Configuring PSK encryption	63
	Configure PSK encryption data for devices using a Wi-Fi profile	63
	Configuring LEAP authentication	64
	Configure LEAP authentication data for devices using a Wi-Fi profile	64
	Configuring PEAP authentication	65
	Configure PEAP authentication data for devices using a Wi-Fi profile	65
	Prerequisites: Distributing a certificate using the BlackBerry Desktop Software	66
	Distribute a certificate using the BlackBerry Desktop Software	67
	Configure PEAP configuration settings in the Wi-Fi profile on a device	68
	Configuring EAP-TLS authentication	69
	Configure EAP-TLS authentication data for devices using a Wi-Fi profile	69
	Configure EAP-TLS configuration settings in the Wi-Fi profile on a device	70
	Configuring EAP-TTLS authentication	71
	Configure EAP-TTLS authentication data for BlackBerry devices using a Wi-Fi profile	71
	Configure EAP-TTLS configuration settings in the Wi-Fi profile on a device	72
	Configuring EAP-FAST authentication	73
	Configure EAP-FAST authentication	73
	Send EAP-FAST authentication data to a device using a Wi-Fi profile	74
	Configure EAP-FAST configuration settings in the Wi-Fi profile on devices	75
11	Configuring software tokens for devices	76
	Prerequisites: Configuring devices for RSA authentication	76
	Configure devices for RSA authentication	77
	Configure RSA authentication over a Wi-Fi network using a software token	77
	Configure RSA authentication over a VPN network using a software token	78
	Assign software tokens to a user account	79

12	Protecting and redistributing devices	80
	Using IT administration commands to protect a lost or stolen device	80
	Protect a lost or stolen device by locking it	81
	Protect a lost or stolen device by deleting all data	81
	Protect a lost device that a user might recover	82
	Preparing a device for redistribution to a new user	83
	Delete user data and assign a device to a new user	83
	Delete user data and device data and assign a device to a new user	84
13	Managing groups and user accounts	85
	Managing groups	85
	Using default groups to manage user accounts	85
	Remove a user account from a group	85
	Change the properties of a group	86
	Rename a group	86
	Delete a group	86
	Managing user accounts	87
	Move a user account to a different group	87
	Delete a user account from the BlackBerry Business Cloud Services	87
	Update a user account manually	88
	Resend service books to a BlackBerry device	88
14	Managing organizer data synchronization	89
	Managing the wireless backup and recovery of organizer data	89
	Turn off the wireless backup of organizer data for a user account	89
	Delete a user's organizer data from the BlackBerry Business Cloud Services	90
	Delete organizer data for members of a user group from the BlackBerry Business Cloud Services	90
	Changing how organizer data synchronizes	90
	Turn off organizer data synchronization for a user account	91
	Change the direction of organizer data synchronization for a user account	91
	Change how the BlackBerry Administration Service resolves conflicts for a specific user account during organizer data synchronization	92
	Synchronizing contact pictures	93
	Turn off synchronization of contact pictures for a user account	93
	Synchronizing calendars	94
	Start corrective calendar synchronization manually for a user account	94
15	Managing your organization's cloud messaging services	95
	Managing message forwarding	95
	Forward email messages to a device when filter rules do not apply	95
	Do not deliver email messages to a BlackBerry device when no filter rules apply	96
	Forward email messages from inbox subfolders to a BlackBerry device	96
	Turn off email message forwarding to a user account	97

	Turn off email message forwarding to user accounts in a group	97
	Turn off synchronization for email messages that are sent from a BlackBerry device	98
	Managing the incoming message queue	98
	Delete email messages for user accounts from the incoming message queue	98
	Viewing email messages that contain HTML and rich content	99
	View whether a user turned on support for email messages that contain HTML and rich content for a BlackBerry device	99
	Synchronizing folders on a BlackBerry device	100
	Control which personal contact subfolders a user can synchronize with a BlackBerry device	100
	Control which personal email folders a user can synchronize with a BlackBerry device	100
	Managing signatures and disclaimers in email messages	101
	Add a signature to email messages that a user sends from a BlackBerry device	101
	Add a disclaimer to email messages that a user sends from a device	102
	How the BlackBerry Business Cloud Services manages attachments	102
	Attachment file formats that are supported	103
16	Managing the delivery of IT policies to devices	104
	Managing the distribution settings for a specific job	104
	Change how a job sends IT policies to devices	104
	Specify the start time and priority for a job	105
	View the status of a job	106
	View the status of a task	106
	Stopping a job that is running	107
	Stop a job that is running	107
17	Glossary	108
18	Provide feedback	111
19	Legal notice	112

About BlackBerry Business Cloud Services

1

The BlackBerry Business Cloud Services is designed to be a secure link between your organization's cloud messaging services and BlackBerry devices. The BlackBerry Business Cloud Services can provide mobile access to the email accounts and organizer data that are part of your organization's resources.

The BlackBerry Business Cloud Services supports AES encryption to help protect wireless data that is transmitted between the BlackBerry Business Cloud Services and devices.

BlackBerry Business Cloud Services feature overview

Feature	Description
Single login	<ul style="list-style-type: none">Log in to the BlackBerry Business Cloud Services using the same credentials that you use to access Microsoft Office 365
Powerful and familiar administration	<ul style="list-style-type: none">Look and feel similar to the BlackBerry Administration Service for the BlackBerry Enterprise ServerManage individual user accounts, groups, and your entire organization from the BlackBerry Business Cloud Services administration console. You can also activate BlackBerry devices and send wireless commands.
Wireless activation	<ul style="list-style-type: none">Activate devices over the wireless network and associate them with the BlackBerry Business Cloud Services
Support for personal devices	<ul style="list-style-type: none">For BlackBerry device users that have both personal and work data on a device, the BlackBerry Business Cloud Services offers BlackBerry Balance technology. BlackBerry Balance technology offers the ability to delete only

Feature	Description
	work data from the device (for example, you might want to delete work data if a user leaves the organization). You can use this feature on devices that are running BlackBerry 6 or later.
Instant messaging	<ul style="list-style-type: none"> Supports BlackBerry Messenger and consumer instant messaging applications available from the BlackBerry App World storefront
Data protection	<ul style="list-style-type: none"> Uses AES encryption to protect data that is in transit between the BlackBerry Business Cloud Services and devices Protects the connection between the BlackBerry Business Cloud Services and the BlackBerry Administration Service using HTTPS Provides IT policies and IT administration commands to control the behavior of the device
Web-based self-service	<ul style="list-style-type: none"> Allows users to switch devices, back up and restore data on devices, set their own activation passwords, or send wireless commands to lock or delete the data on devices
User features	<ul style="list-style-type: none"> Supports all of the messaging features that users expect with BlackBerry devices, including wireless email reconciliation, email filters, email forwarding, signatures, out-of-office reply, contact lookup and updates, attachment viewing and downloading, personal distribution lists, personal folders and subfolders, follow-up flags, calendar event forwarding, availability viewing in meeting invitations, and so on

BlackBerry solution comparison chart

Messaging features

Feature	BlackBerry Enterprise Server	BlackBerry Enterprise Server Express	BlackBerry Internet Service	BlackBerry Business Cloud Services
Supported messaging environments	Microsoft Exchange, Lotus	Microsoft Exchange and Lotus Domino	IMAP and POP (for example, Google Mail,	Microsoft Office 365

Feature	BlackBerry Enterprise Server	BlackBerry Enterprise Server Express	BlackBerry Internet Service	BlackBerry Business Cloud Services
	Domino, and Novell GroupWise		Yahoo! Mail, Microsoft Outlook Web Access)	
Wireless email messaging	√	√	√	√
Email reconciliation	√	√	√	√
Contact lookup	√	√	√	√
Sent message reconciliation	√	√	√	√
Reconciliation of permanently deleted messages (hard delete)	√	√	√ Some messaging environments	√
Email messages with HTML and rich content	√	√	√	√
Remote email message lookup	√	√	√ Google Mail only	√
Email message filters	Global filters and user filters	Global filters and user filters	User filters	User filters
Separate inboxes for work and personal accounts	√	√	√	√
Synchronization of published public contact folders	√	√	√ With limitations	
Synchronization of personal contact folders	√	√		√
Synchronization of personal mail folders	√	√		√
Synchronization of organizer data (memos and tasks)	√	√		√

Calendar features

Feature	BlackBerry Enterprise Server	BlackBerry Enterprise Server Express	BlackBerry Internet Service	BlackBerry Business Cloud Services
Calendar synchronization	√	√	Google Mail only	√
Ability to check the availability of meeting participants	√	√	√	√
Ability to forward calendar entries	√	√	√	√
Calendar attachments	√	√		√

Enterprise instant messaging features

Feature	BlackBerry Enterprise Server	BlackBerry Enterprise Server Express	BlackBerry Internet Service	BlackBerry Business Cloud Services
Supported enterprise instant messaging environments	IBM Lotus Sametime, Microsoft Office Communications Server, Microsoft Lync Server, and Novell GroupWise Messenger	None	None	None

Console support features

Feature	BlackBerry Enterprise Server	BlackBerry Enterprise Server Express	BlackBerry Internet Service	BlackBerry Business Cloud Services
Administration console	√	√	√ With limitations	√
Administrative roles	√	√ With limitations	√	Limited to Microsoft Office 365 administrative roles
Self-service console	√	√	√	√
Languages	English, Brazilian Portuguese, French, German,	English, Brazilian Portuguese, French, German, Italian,	For a list of supported languages, visit www.blackberry.com/	English, Brazilian Portuguese, French, German, Italian,

Feature	BlackBerry Enterprise Server	BlackBerry Enterprise Server Express	BlackBerry Internet Service	BlackBerry Business Cloud Services
	Italian, Japanese, and Spanish	Japanese, and Spanish	support to read article KB12859.	Japanese, and Spanish

Activation features

Feature	BlackBerry Enterprise Server	BlackBerry Enterprise Server Express	BlackBerry Internet Service	BlackBerry Business Cloud Services
Supported activation methods	<ul style="list-style-type: none"> BlackBerry Administration Service Over the wireless network BlackBerry Desktop Software BlackBerry Web Desktop Manager Over your organization's Wi-Fi network 	<ul style="list-style-type: none"> BlackBerry Administration Service Over the wireless network (requires app or specific data plan) BlackBerry Desktop Software BlackBerry Web Desktop Manager Over your organization's Wi-Fi network 	—	<ul style="list-style-type: none"> BlackBerry Administration Service Over the wireless network BlackBerry Web Desktop Manager

Security features

Feature	BlackBerry Enterprise Server	BlackBerry Enterprise Server Express	BlackBerry Internet Service	BlackBerry Business Cloud Services
Transport layer encryption	√ (AES and Triple DES)	√ (AES and Triple DES)		√ (AES)
Enhanced encryption	√ (S/MIME and PGP)	√ (S/MIME and PGP)	√ (SSL)	
BlackBerry Balance technology	√	√		√
IT administration commands	Supports:	Supports:	Supports:	Supports:

Feature	BlackBerry Enterprise Server	BlackBerry Enterprise Server Express	BlackBerry Internet Service	BlackBerry Business Cloud Services
	<ul style="list-style-type: none"> Specify new device password and lock device Delete only work data and remove device Delete all device data and remove device 	<ul style="list-style-type: none"> Specify new device password and lock device Delete only work data and remove device Delete all device data and remove device 	<ul style="list-style-type: none"> Specify new device password and lock device Delete all device data and remove device 	<ul style="list-style-type: none"> Specify new device password and lock device Delete only work data and remove device Delete all device data and remove device
IT policy rules	All	Subset		Subset
Two-factor authentication	√	√		

Application and browsing features

Feature	BlackBerry Enterprise Server	BlackBerry Enterprise Server Express	BlackBerry Internet Service	BlackBerry Business Cloud Services
Web browsing	√	√	√	√
Intranet browsing	√	√		
Methods for installing applications	Supports: <ul style="list-style-type: none"> Over the wireless network BlackBerry Administration Service BlackBerry Desktop Software BlackBerry Web Desktop Manager Standalone application loader tool 	Supports: <ul style="list-style-type: none"> Over the wireless network BlackBerry Administration Service BlackBerry Desktop Software BlackBerry Web Desktop Manager Standalone application loader tool 	Supports: <ul style="list-style-type: none"> BlackBerry Desktop Software Web browser on BlackBerry devices BlackBerry App World 	Supports: <ul style="list-style-type: none"> BlackBerry Desktop Software Web browser on BlackBerry devices BlackBerry App World

Feature	BlackBerry Enterprise Server	BlackBerry Enterprise Server Express	BlackBerry Internet Service	BlackBerry Business Cloud Services
	<ul style="list-style-type: none"> • Web browser on BlackBerry devices • BlackBerry App World 	<ul style="list-style-type: none"> • Web browser on BlackBerry devices • BlackBerry App World 		
Ability to push applications to devices	√	√		
Application control policies	√	√		
Methods for updating BlackBerry Device Software	Supports: <ul style="list-style-type: none"> • Over the wireless network • BlackBerry Administration Service • BlackBerry Desktop Software • BlackBerry Web Desktop Manager • Standalone application loader tool • BlackBerry Desktop Software update sites 	Supports: <ul style="list-style-type: none"> • Over the wireless network • BlackBerry Administration Service • BlackBerry Desktop Software • BlackBerry Web Desktop Manager • Standalone application loader tool • BlackBerry Desktop Software update sites 	Supports: <ul style="list-style-type: none"> • Over the wireless network • BlackBerry Desktop Software 	Supports: <ul style="list-style-type: none"> • Over the wireless network • BlackBerry Desktop Software

Connecting to Blackberry Business Cloud Services

2

System requirements: Browser for BlackBerry Business Cloud Services

Item	Requirement
Browser	<ul style="list-style-type: none">• Windows Internet Explorer 8.0• Mozilla Firefox 3.6• Safari 4 for Mac• Google Chrome 4
Browser settings for Windows Internet Explorer	<p>To support browser access, configure the following settings:</p> <ul style="list-style-type: none">• Language preferences configured to display encoded web pages• Microsoft hotfix 955839 installed on the users' computers to make sure the correct time zones are displayed• The following settings turned on to support Microsoft ActiveX:<ul style="list-style-type: none">• 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• Support for JavaScript• Cookies turned on

Item	Requirement
Browser settings for Firefox, Safari, and Google Chrome	<ul style="list-style-type: none"> • Support for TLS or SSL • The SSL certificate installed to permit trusted connections to the BlackBerry Administration Service • If using Windows Vista, the BlackBerry Administration Service web address added as a trusted web site and Enable protected mode cleared <p>To support browser access, configure the following settings:</p> <ul style="list-style-type: none"> • Support for JavaScript • Cookies turned on • Support for TLS or SSL • To permit trusted connections to the BlackBerry Administration Service, the SSL certificate installed

Enabling the BlackBerry Business Cloud Services in Microsoft Office 365

You must be a Microsoft Office 365 global administrator with a tenant organization or a Microsoft Partner providing administration services to enable the BlackBerry Business Cloud Services in and register as a tenant with the BlackBerry Business Cloud Services.

Enable the BlackBerry Business Cloud Services and register your organization as a tenant

You must be a Microsoft Office 365 global administrator to complete this task. You only need to complete this task one time for your organization.

1. Log in to Microsoft Office 365.
2. On the **Resources** menu, click **Setting up email on mobile phones**.
3. Click **Enable BlackBerry Business Cloud Services**.
4. Read the associated services information.

5. Authorize access by selecting the **Yes, I have read and understand the associated services information** check box and click **OK**.
6. After approximately 15 minutes, in the **Authorized Services** section, click **Manage**. Microsoft Office 365 redirects you to the BlackBerry Business Cloud Services console.
7. In the BlackBerry Business Cloud Services console, click **Sign up now**.
8. Select a language.
9. Read the license agreement and select the **I Agree** check box.
10. Click **Continue**.
11. Read the additional terms and select the **I Agree** check box.
12. Click **Login to BlackBerry Administration Service**. The BlackBerry Business Cloud Services redirects you to the BlackBerry Administration Service console.

Log in to the BlackBerry Administration Service

Before you begin:

- Microsoft Office 365 global administrator enabled the BlackBerry Business Cloud Services and registered your organization as a tenant.
- The browser must permit Microsoft ActiveX controls to manage a BlackBerry device that is connected to your computer.

1. Log in to .
2. In the **Authorized Services** section, click **Manage**.
You are redirected to the BlackBerry Administration Service. You are also logged into BlackBerry Web Desktop Manager.

After you finish:

- If you use Windows Internet Explorer and the browser displays an error when you try to access BlackBerry Administration Service, see [There is a problem with this website's security certificate](#).
- If you use Mozilla Firefox and the browser displays an error when you try to access BlackBerry Administration Service, see [This connection is untrusted](#).

There is a problem with this website's security certificate

Possible cause

The browser displays this error message when you try to navigate to the BlackBerry Administration Service using Windows Internet Explorer 8 or later.

Possible solution

Add the web address for the BlackBerry Administration Service to the list of trusted web sites in Windows Internet Explorer, and install the certificate for the BlackBerry Administration Service in the certificate store of your computer.

1. In Windows Internet Explorer, navigate to the BlackBerry Administration Service console.
2. Click **Continue to this website (not recommended)**.
3. On the **Tools** menu, click **Internet Options**.
4. On the **Security** tab, click **Local Intranet**.
5. Click **Sites**.
6. Click **Add** to add the console to the list of trusted websites.
7. Click **Close**.
8. Click **OK**.
9. In the browser window, on the toolbar, click **Certificate Error**.
10. Click **View certificates**.
11. Click **Install certificate**. The Certificate Import Wizard opens.
 - a In the **Certificate Store** dialog box, click **Place all certificates in the following store**.
 - b Click **Browse**.
 - c Click **Trusted Root Certification Authorities**.
 - d Click **OK**.
12. Close and reopen the browser.

This connection is untrusted

Possible cause

The browser displays this error message when you try to navigate to the BlackBerry Administration Service using Mozilla Firefox 3.6.

Possible solution

Install the certificate for the BlackBerry Administration Service in the certificate store of your computer.

1. In Firefox, navigate to the BlackBerry Administration Service console.
2. Click **I Understand the Risks**.
3. Click **Add Exception**.
4. Click **Confirm Security Exception**.
5. Close and reopen the browser.

Configuring user accounts

3

Creating groups

You can create groups and assign user accounts to groups based on custom criteria, such as user location, organizational group, or BlackBerry device model.

Create a group to manage similar user accounts

You can reduce the time that you spend managing user accounts by adding similar user accounts to a group, and assigning shared properties, such as IT policies, to the group. Properties that you assign to a group are assigned to all user accounts in the group.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Create a group**.
3. In the **Group information** section, type a name and description for the group.
4. Click **Save**.

After you finish:

- Add properties to the group.
- Add user accounts to the group.

Related information

[Add user accounts to a group](#), 20

[Managing groups](#), 85

Add user accounts to a group

You can add user accounts to a group to assign the properties of the group to user accounts automatically.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.

2. Click **Manage users**.
3. Search for the user accounts.
4. Select the user accounts.
5. In the **Add to user configuration** list, click **Add group**.
6. In the **Available groups** list, click the group that you want to add the user accounts to.
7. Click **Add**.
8. Click **Save**.

Adding user accounts to the BlackBerry Business Cloud Services

Add a user account

You can add a user account to the BlackBerry Business Cloud Services, assign a BlackBerry device to a user account, and activate the device. The user account must exist in Microsoft Office 365.

Before you begin: If required, create a group so that you can manage user accounts that are similar.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Create a user**.
3. Type the search criteria in the appropriate fields to search for a user account (for example, a partial name or email address). Click **Search**.
4. Select the check box beside the display name for the user account.
5. Click **Continue**.
6. If groups exist in the **Available groups** list, click at least one group that you want to add the user account to.
7. Click **Add**.
8. To select an activation option, perform one of the following actions:

Option	Step
Specify an activation password for the user account.	<ol style="list-style-type: none"> 1. Click Create a user with activation password. 2. In the Set activation password, section, type and confirm an activation password.

Option	Step
	<ol style="list-style-type: none"> In the Password expiration (hours) field, type the amount of time, in hours, that you want to elapse before the activation password expires. Click Create user.
Generate an activation password for the user account automatically.	Click Create a user with generated activation password .
Activate the user account without using an activation password.	Click Create a user without activation password .

After you finish:

After you create new user accounts, Microsoft Office 365 must give BlackBerry Business Cloud Services access to the users' email accounts. You need to wait approximately 20 minutes after adding user accounts before users can activate their devices.

Related information

[Managing user accounts, 87](#)

[Activating BlackBerry devices, 26](#)

Importing a list of user accounts to the BlackBerry Business Cloud Services

You can add multiple user accounts to BlackBerry Business Cloud Services by importing a .csv file that contains a list of user accounts and the required information to activate the user accounts on BlackBerry Business Cloud Services. The maximum number of user accounts in the .csv file is 100.

The .csv file can include the following information:

- User accounts that you want to add
- Names of the groups you want to add the user accounts to
- Activation passwords that you want to assign to the user accounts

The BlackBerry Administration Service processes actions in the order that they appear in the .csv file. If the BlackBerry Administration Service encounters an error that is specific to an action during the import process (for example, an action is incorrectly formatted in the .csv file), the BlackBerry Administration Service continues to process the remaining actions that are listed in the file and displays an error message for the action that the BlackBerry Administration Service could not process.

Fields in a .csv file that contain user account information

The BlackBerry Administration Service uses a .csv file to add user account information to the BlackBerry Business Cloud Services. The following table lists the fields in the .csv file that might be populated when you import user account information.

Field	Description
Email Address	The field is required and specifies the email address for the user account.
Group Names	This field specifies the names of groups that you want to add the user account to.
Activation Password Operation	<p>This field specifies whether an activation password is required to activate the user account and whether that password should be specified by the administrator or the BlackBerry Administration Service. The activation password value specified in this field can either be "specify", "none", or "generate" in lower case only. The activation password operation must be the same on each line in the .csv file.</p> <p>If the field is set to "specify", the activation password and the expiry time (in hours) are optional fields in the .csv file. If the activation password and the expiry time values are not included in the .csv file, you are prompted to specify these values the after uploading the .csv file. If you specify the activation password and the expiry time for the user accounts, the values must be provided on every line of the csv file.</p> <p>If the field is set to "generate", the password is automatically generated by the BlackBerry Administration Service and the final two fields of each .csv line must be empty. The activation password expires if the user does not activate the BlackBerry device on the BlackBerry Business Cloud Services before the password timeout elapses. The default value is 48 hours.</p> <p>If the field is set to "none", the user account is created without an activation password and the final two fields of each .csv line must be empty.</p> <p>To activate a device on the BlackBerry Business Cloud Services over the wireless network, an activation password is required.</p>
Activation Password	This field specifies the activation password for the user account if an activation password is required.
Activation Password Expiry	This field specifies the amount of time, in hours, that can elapse before the activation password expires if an activation password is required.

Field	Description
	The activation password will expire if the user does not activate the device on the BlackBerry Business Cloud Services before a default value of 48 hours elapses.

Example: Importing user accounts to the BlackBerry Business Cloud Services

```
"Email Address", "Group Names", "Activation Password
Operation", "Activation Password", "Activation Password Expiry"

"wbarichak@example.com", "Admins", "specify", "asdf", "24"
"jbuac@example.com", "Admins", "specify", "asdf", "24"
```

Create multiple user accounts by importing the user accounts from a .csv file

You can import a list of user accounts from a .csv file and add them to BlackBerry Business Cloud Services. The user accounts must exist in Microsoft Office 365.

Before you begin: Prepare a .csv file of user accounts that you want to import into BlackBerry Business Cloud Services. If you want to import more than 100 user accounts, create multiple .csv files of less than 100 user accounts in each file.

1. In BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Create a user**.
3. Click **Import new users**.
4. In the **Import users from a list** section, click **Browse**.
5. Navigate to the .csv file that contains the user accounts that you want to import.
6. Click **Continue**.
7. Perform the appropriate actions for the user accounts.

After you finish:

After you create new user accounts, Microsoft Office 365 must give BlackBerry Business Cloud Services access to the users' email accounts. You need to wait approximately 20 minutes after adding user accounts before users can activate their devices.

Export a list of user accounts

You can export a list of user accounts from the BlackBerry Business Cloud Services to a .csv file. The .csv file contains information about the user accounts, such as the user ID, display name, PIN and email address.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Select the check boxes beside the display names of the appropriate user accounts.
4. In the **Export users** list, click **Export selected users**.
5. Click **Download file**.
6. Save the .csv file.

Activating BlackBerry devices

4

To assign BlackBerry devices to user accounts and activate the devices, you can use any of the following methods:

Method	Description
BlackBerry Administration Service	You can activate devices before you distribute them to users by connecting the devices to a computer and logging in to the BlackBerry Administration Service.
Over the wireless network	New users and users that are receiving replacement devices can activate the devices without requiring a physical connection to your organization's network. Devices that are associated with the BlackBerry Internet Service cannot be activated over the wireless network.
BlackBerry Web Desktop Manager	New users and users that are receiving replacement devices can activate the devices by connecting the devices to a computer that hosts the BlackBerry Web Desktop Manager.

Activate a device using the BlackBerry Administration Service

Before you begin:

- For activation to complete, you need wireless connectivity or Wi-Fi connectivity to the BlackBerry Infrastructure.
- If necessary, prepare a BlackBerry device so that you can distribute it to a user.

1. Connect the device to a computer that can access the BlackBerry Administration Service.
2. On the **Devices** menu, expand **Attached devices**.
3. Click **Manage current device**.
4. Click **Assign current device**.
5. Search for a user account.
6. In the search results, click the display name for a user account.
7. Click **Associate user**.

8. Click **Assign current device**.

Related information

[Protecting and redistributing devices](#), 80

Activating a device over the wireless network

To activate a BlackBerry device over the wireless network, you assign an activation password to a user account. The user receives the activation password in an email message and associates the device with the email account by typing the password on the device.

The wireless activation process activates devices on the BlackBerry Business Cloud Services over the wireless network. Neither you nor the users are required to connect the devices to a computer to complete the activation process.

You can use the wireless activation process to activate a large number of devices over the wireless network. When users want to activate devices on the BlackBerry Business Cloud Services over the wireless network, they must notify you. You can use the BlackBerry Administration Service to configure activation passwords and distribute the passwords to the users.

The wireless activation process can begin automatically or when users open the activation application on the devices and type an activation password and email address. When the activation process completes, users can send email messages from and receive email messages on their devices.

When you initiate the wireless activation process, the BlackBerry Business Cloud Services sends an email message with an `etp.dat` attachment from the `blackberry.net` domain to the cloud messaging services. To make sure that the email message is not blocked or changed, add the `blackberry.net` domain to the whitelist in your organization's cloud messaging services.

Activation passwords

The BlackBerry Business Cloud Services activates a BlackBerry device over the wireless network using the wireless activation authentication protocol and an activation password that is specific to the user account that is associated with the device.

Item	Description
character support	Activation passwords can include any type of character.
security	Wireless activation is designed so that short activation passwords do not compromise the security of the protocol. You must distribute the activation password to the authenticated user securely. If the user receives the activation password, but does not activate the device on the BlackBerry Business Cloud Services, a potentially malicious user who can

Item	Description
	<p>access the activation password can connect another device to the BlackBerry Business Cloud Services and assume the identity of the intended user.</p> <p>When a user activates a device on the BlackBerry Business Cloud Services, the activation password becomes inactive and a potentially malicious user cannot reuse it to activate another device.</p> <p>If a user receives an activation password, you cannot generate a new activation password for the user until the activation password expires. An activation password expires after 48 hours by default. You can configure an activation to password expire earlier than the default value of 48 hours.</p>
password validity	<p>An activation password is no longer valid if any of the following events occur:</p> <ul style="list-style-type: none"> • the user does not activate the device on the BlackBerry Business Cloud Services before the password expires • the user types the activation password incorrectly five consecutive times • the BlackBerry Business Cloud Services activates a device using the activation password

Send an activation password to a user

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. In the **Device activation** list, click **Specify an activation password**.
6. In the **Activation password** field and **Confirm password** field, type an activation password. The password should not contain special characters. Some BlackBerry devices do not support special characters and do not unlock when a user types a password that contains special characters.
7. In the **Password expiration (hours)** field, type the amount of time that can elapse before the activation password expires.
8. Click **Specify an activation password**.

Send an activation password to multiple users

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.

3. Search for one or more user accounts.
4. Select the check boxes beside the display names for the appropriate user accounts.
5. In the **Device activation** list, click **Specify an activation password**.
6. In the **Activation password** field and **Confirm password** field, type an activation password. The password should not contain special characters. Some BlackBerry devices do not support special characters and do not unlock when a user types a password that contains special characters.
7. In the **Password expiration (hours)** field, type the amount of time, in hours, that can elapse before the activation password expires.
8. Click **Specify an activation password**.

Activating devices using the BlackBerry Web Desktop Manager

Users can activate BlackBerry devices by connecting the devices to computers using a USB cable and logging in to the BlackBerry Web Desktop Manager. For activation to complete, devices need a wireless connection or Wi-Fi connection to the BlackBerry Infrastructure.

During the activation process, the BlackBerry Web Desktop Manager prompts users to associate the devices with their email accounts and generate encryption keys. When users complete the activation process, the BlackBerry Business Cloud Services synchronizes email messages and organizer data to devices. For more information, see the *BlackBerry Web Desktop Manager for BlackBerry Business Cloud Services User Guide*, or the hosted help files at <http://docs.blackberry.com/HLP/BBCS/WDT/1.0/en>.

Using IT policies to manage security

5

You can use IT policies to control and manage BlackBerry devices in your organization's environment. An IT policy consists of multiple IT policy rules that manage the security and behavior of the BlackBerry Business Cloud Services. For example, you can use IT policy rules to manage the following device behaviors and security features:

- Use of a password or pass phrase
- Protection of user data on the device
- Control of device resources, such as the camera
- Control personal devices using BlackBerry Balance

The BlackBerry Business Cloud Services includes preconfigured IT policies that you can use. The Default IT policy includes IT policy rules that are configured to indicate the default behavior of the device.

After a user activates a device, the BlackBerry Business Cloud Services automatically sends the IT policy that you assigned to the user account or group to the device. By default, if you do not assign an IT policy to the user account or group, the BlackBerry Business Cloud Services sends the Default IT policy. If you delete an IT policy that you assigned to the user account or group, the BlackBerry Business Cloud Services automatically re-assigns the Default IT policy to the user account and resends the Default IT policy to the device.

For more information, see the *BlackBerry Business Cloud Services Policy Reference Guide*.

Using IT policy rules to manage security

You can use IT policy rules to customize and control the actions that users can perform.

To use an IT policy rule on a BlackBerry device, you must verify that the BlackBerry Device Software version supports the IT policy rule. For example, you cannot use the Enable Separation of Work Content IT policy rule to control whether a device distinguishes between work data and personal data if the BlackBerry Device Software version does not support the IT policy rule. For information about the BlackBerry Device Software version that is required for a specific IT policy rule, see the *BlackBerry Business Cloud Services Policy Reference Guide*.

The BlackBerry Administration Service groups the IT policy rules by common properties or by application. Most IT policy rules are designed so that you can assign them to multiple user accounts and groups.

Preconfigured IT policies

The BlackBerry Business Cloud Services includes the following preconfigured IT policies that you can use to meet the requirements of your organization.

Preconfigured IT policy	Description
Default	This policy includes all the standard IT policy rules that are set in the BlackBerry Business Cloud Services.
Basic Password Security	This policy requires a basic password that users can use to unlock their BlackBerry devices. Users must change the passwords regularly. The IT policy includes a password timeout that locks devices.

Default values for preconfigured IT policies

You can configure additional IT policy rules in the preconfigured IT policies or change any of the following values:

IT policy rule	Default IT policy	Basic Password Security IT Policy
Device-Only Items		
Enable Long-Term Timeout	—	—
Maximum Security Timeout	—	30 minutes
Maximum Password Age	—	60 days
Minimum Password Length	—	—
Password Pattern Checks	No restriction	No restriction
Password Required	No	Yes
User Can Change Timeout	Yes	Yes
User Can Disable Password	Yes	No
Password policy group		
Forbidden Passwords	—	—
Maximum Password History	—	—

IT policy rule	Default IT policy	Basic Password Security IT Policy
Periodic Challenge Time	—	—
Set Maximum Password Attempts	—	—
Set Password Timeout	—	—
Suppress Password Echo	—	—
Personal devices policy group		
Enable Separation of Work Content	—	—
Disable Forwarding of Work Content Using Personal Channels	—	—
Require Work Resources for Conducting Work Activities	—	—
Work Domains	—	—
Security policy group		
Content Protection Strength	—	—
Disable External Memory	No	—
External File System Encryption level	Not required	—
Required Password Pattern	No	—
BlackBerry App World policy group		
Enable Wireless Service Provider Billing	—	—
Camera policy group		
Disable Photo Camera	—	—
Disable Video Camera	—	—
PIM Synchronization policy group		
Disable All Wireless Synchronization	—	—
Wired Software Updates policy group		
Allow Web-Based Software Loading	—	—

Creating IT policies

Create an IT policy

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Create an IT policy**.
3. Type a name and description for the IT policy.
4. Click **Save**.
5. To configure the IT policy, perform the following actions:
 - a. In the **IT policy information** section, click the IT policy.
 - b. Click **Edit IT policy**.
 - c. On a tab for an IT policy group, configure values for the IT policy rules.
 - d. Click **Save All**.

After you finish: For more information, see the *BlackBerry Business Cloud Services Policy Reference Guide*.

Create an IT policy based on an existing IT policy

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the list of IT policies, click the IT policy that you want to copy.
4. Click **Copy IT policy**.
5. Type a name and description for the new IT policy.
6. Click **Save**.
7. To change the IT policy settings, perform the following actions:
 - a. In the **IT policy information** section, click the IT policy.
 - b. Click **Edit IT policy**.
 - c. On a tab for an IT policy group, change the appropriate values for the IT policy rules.
 - d. Click **Save all**.

After you finish: For more information, see the *BlackBerry Business Cloud Services Policy Reference Guide*.

Related information

[Preconfigured IT policies, 31](#)

Change the value for an IT policy rule

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the **IT policy information** section, click the IT policy.
4. Click **Edit IT policy**.
5. On a tab for an IT policy group, change the appropriate values for the IT policy rules.
6. Click **Save all**.

Assign an IT policy to a group

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. In the **Manage groups** section, click the group that you want to assign an IT policy to.
4. On the **Policies** tab, click **Edit group**.
5. In the drop-down list, click an IT policy.
6. Click **Save all**.

Related information

[Resolving IT policy conflicts, 35](#)

[Create a group to manage similar user accounts, 20](#)

Assign an IT policy to a user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.

2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name of the user account.
5. On the **Policies** tab, click **Edit user**.
6. In the drop-down list, click an IT policy.
7. Click **Save all**.

Related information

[Resolving IT policy conflicts](#), 35

[Add a user account](#), 21

Resolving IT policy conflicts

You can assign IT policies directly to a user account or to a group. If you do not assign an IT policy to a user account or a group that the user is a member of, the BlackBerry Business Cloud Services applies the Default IT policy to the user account. If you assign an IT policy to a group that a user account is a member of, the BlackBerry Business Cloud Services applies the group IT policy to the user account. If you assign an IT policy to the user account directly, the BlackBerry Business Cloud Services applies this IT policy to the user account instead of the group IT policy or Default IT policy.

If a user account is a member of multiple groups that have different IT policies, the BlackBerry Business Cloud Services applies all of the group IT policies to the user account, resulting in a combined IT policy that has a unique ID. The BlackBerry Business Cloud Services resolves conflicting IT policy rules using the ranking of the available IT policies that you specified using the BlackBerry Administration Service. If an IT policy rule is different in the multiple IT policies, the BlackBerry Business Cloud Services applies the rule setting from the IT policy that you ranked the highest.

How conflicting IT policies are resolved

The BlackBerry Business Cloud Services can apply multiple IT policies to a user account if the user account is a member of multiple groups that are assigned different IT policies. The BlackBerry Administration Service uses predefined rules to apply an IT policy to a user account.

The BlackBerry Administration Service might have to resolve conflicting IT policies if you perform any of the following actions:

- Add an IT policy to or remove an IT policy from a user account or group
- Change an IT policy
- Change the ranking of IT policies
- Delete an IT policy

Scenario	Rule
<p>You add a new user account to the BlackBerry Business Cloud Services. You do not assign an IT policy directly to the user account and you do not add the user account to a group.</p>	<p>The Default IT policy is assigned to the user account.</p>
<p>You assign an IT policy to a user account and different IT policies to the groups that the user account belongs to.</p>	<p>The IT policy that you assign to a user account takes precedence over the IT policies that you assign to the groups that the user belongs to.</p>
<p>A user account belongs to multiple groups. You assign different IT policies to the groups but you do not assign an IT policy to the user account.</p>	<p>If you assign different IT policies to the groups that the user account belongs to, the BlackBerry Business Cloud Services resolves the IT policy rule settings in the multiple IT policies and assigns a combined IT policy that has a unique ID to the user account. The BlackBerry Business Cloud Services resolves conflicting settings for IT policy rules by applying the rule setting from the IT policy that you ranked the highest in the BlackBerry Administration Service.</p> <p>For example, you configure the Disable Photo Camera IT policy rule to Yes in IT policy A and to No in IT policy B. If you rank IT policy A higher than IT policy B, the Yes setting is applied for this rule.</p>
<p>A user account belongs to two groups. You assign the first group IT policy A, which has the Disable Photo Camera IT policy rule as blank (which means that it uses the default value of No). You assign the second group IT policy B, which has the Disable Photo Camera IT policy rule set to Yes. You ranked IT policy A higher than IT policy B in the BlackBerry Administration Service.</p>	<p>When the BlackBerry Business Cloud Services resolves conflicting rule settings, any rule settings that have been explicitly configured to a value take precedence over IT policy rule settings that are blank (these rules revert to the default value).</p> <p>For example, in this scenario, the Disable Photo Camera IT policy rule setting from IT policy B, Yes, is applied to the user account even though IT policy A is ranked higher than IT policy B, because the Disable Photo Camera IT policy rule is blank in IT policy A. If the Disable Photo Camera IT policy rule was configured to No in IT policy A, the No value would be applied to the user account.</p>

Rank IT policies

You must rank the IT policies that you create so that the BlackBerry Business Cloud Services can resolve IT policy conflicts when a user account is a member of multiple groups that have different IT policies.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. Click **Set priority of IT policies**.
4. To move the IT policies higher or lower in the list, click the **up arrow** icon or **down arrow** icon.
5. Click **Save**.

Preview how the BlackBerry Business Cloud Services resolves IT policy conflicts

You can preview how the BlackBerry Business Cloud Services resolves conflicting settings for IT policy rules for multiple IT policies that you select. You can use this feature to determine which IT policies have conflicting IT policy rules and how the BlackBerry Business Cloud Services resolves the conflicting rules. The preview displays the conflicting IT policy rules and the resolved settings for each rule. If an IT policy rule is not conflicting in the multiple IT policies that you selected, the preview does not display the policy rule in the results.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. Click **Preview resolved IT policies**.
4. Select two or more IT policies.
5. Click **Preview**.

View the resolved IT policy rules that are assigned to a user account

If a user account belongs to multiple groups and you assign a different IT policy to each group, the BlackBerry Business Cloud Services resolves the conflicting IT policy rule settings. You can view the resolved settings for each rule in the BlackBerry Administration Service. If an IT policy rule is not conflicting in the multiple IT policies that were applied to the user account, the resolved IT policy does not display the IT policy rule.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for a user account.
5. On the **Policies** tab, in the **Resolved IT Policy name** section, click the name of the IT policy.

Sending an IT policy over the wireless network

BlackBerry Business Cloud Services sends changes to an IT policy to a BlackBerry device over the wireless network automatically. The BlackBerry Business Cloud Services resends an IT policy to the device within a short period of time after you update the IT policy using the BlackBerry Administration Service. You can also resend an IT policy to a specific device manually. When the device receives an updated IT policy or a new IT policy, the device applies the configuration changes in near real-time.

Related information

[Resolving IT policy conflicts, 35](#)

[Using IT policy rules to manage security, 30](#)

[Using IT policies to manage security, 30](#)

[Preconfigured IT policies, 31](#)

Resend an IT policy to a device manually

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. On the **Policies** tab, in the **Resolved IT policy name** section, click the name of the policy.
6. Click **Resend IT policy to a device**.

Export all IT policy data to a data file

If you export all IT policy data to a data file, you must create an encryption password for the data file that you can use to protect the data file.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.

3. Click **Export IT policy list**.
4. In the **File encryption password** field and **Confirm file encryption password** field, type a password so that the BlackBerry Enterprise Server can encrypt the IT policy data file.
5. Click **Export**.
6. Click **Download file**.
7. Click **Save**.
8. Browse to a location on a local or network drive where you want to save the data file.
9. Click **Save**.
10. Click **Close**.

Delete an IT policy

You can only delete policies that you or another administrator created. The preconfigured IT policies cannot be deleted.

If you delete an IT policy, the BlackBerry Administration Service identifies the users or groups that used the IT policy and determines what IT policy to apply to the users or groups instead. For example, when an IT policy is assigned to a user account and the user account is not a member of a group, if you delete the IT policy, the BlackBerry Administration Service applies the default IT policy to the user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy**.
2. Click **Manage IT policies**.
3. In the list of IT policies, click an IT policy.
4. Click **Delete IT policy**.
5. Click **Yes – Delete the IT policy**.

Setting up cloud messaging services

6

Creating email message filters

You can create email message filters to define which email messages the BlackBerry Business Cloud Services forwards to a BlackBerry device. When users receive email messages in the incoming message queue, the BlackBerry Business Cloud Services applies email message filters to determine how to direct the messages: forward, forward with priority, or do not forward to the devices.

Email message filters that you create and apply to a user account override the email message filters that the user creates on the device or using the BlackBerry Web Desktop Manager. You can specify the order that the BlackBerry Business Cloud Services applies the email message filters in.

Create an email message filter

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Email** tab, in the **Email message filter name** field, type a name for the email message filter.
8. In the **Email message filter rules** section, configure the options for the email message filter. Use semicolons (;) to separate multiple items that you specify.

If you specify multiple users in the **From** field or **Sent to** field, or multiple subject terms in the **Subject** field, the message filter is applied to email messages that contain any of the users or terms that you specify. All of the users or terms that you specify do not have to be satisfied for the message filter to be applied.

9. Perform one of the following tasks:

- To create an email message filter that does not deliver email messages that match the filter criteria to BlackBerry devices, select **Do not forward email messages to the device**.
 - To create an email message filter that forwards email messages that match the filter criteria to devices, select **Forward email messages to the device**.
10. Click the **Add** icon.
 11. To move the email message filter higher or lower in the list, click the **Up** or **Down** icons. The BlackBerry Business Cloud Services applies email message filters in the order that they are listed in. Organize the email message filters from the least restrictive to the most restrictive.
 12. Click **Continue to user information edit**.
 13. Click **Save all**.

Turn on an email message filter that applies to a specific user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Email** tab, click the **Edit** icon beside the email message filter that you want to turn on.
8. In the **Enabled** drop-down list, click **Yes**.
9. Click **Continue to user information edit**.
10. Click **Save all**.
The BlackBerry Administration Service applies email message filters in the order that they are listed.

Copying existing email message filters to user accounts

You can copy the existing email message filters for a user account and apply them to other user accounts so that you can easily apply the same set of filters to multiple user accounts. To create a copy of existing email message filters, you must export the existing email message filters for a user account as an .xml file. You can then import the .xml file to other user accounts.

Export email message filters for a user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. In the **Messaging configuration** section, click **Default configuration**.
6. On the **Email** tab, click **Export email message filters**.
7. Click **Download file**.
8. Save the .xml file.

Import email message filters for a user account

Before you begin: Export email message filters for a user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for the user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Email** tab, at the bottom of the screen, click **Import email filters**.

8. In the **Import email message filters** section, click **Browse**. Navigate to the .xml file that contains the email message filters that you want to import.
9. Click **Import email message filters**.
10. Click **Continue to user information edit**.
11. Click **Save all**.

Mapping contact-information fields for synchronization and contact lookups

You can map contact-information fields from email accounts to the contact list fields on BlackBerry devices. The information in the fields in the email account synchronizes to the fields on the device.

You can map up to four fields that users define in the contact information in their email accounts to their devices. When users request a remote contact lookup, the fields that you configure display on devices.

Map a contact list field to a contact list field on a device

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Mappings for organizer data synchronization** tab, in the **Mappings for organizer data synchronization** section, select the **Turned on** option.
8. In the appropriate drop-down lists, select the fields on the device that you want to map the information to.
9. Click **Continue to user information edit**.
10. Click **Save all**.

Map a contact list field from an email account to a contact list field on a device

You can map up to four contact list fields that users define in their email account to a BlackBerry device.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Mappings for organizer data synchronization** tab, in the **Mappings for organizer data synchronization** section, select the **Turned on** option.
8. In the **Other mappings** section, in each **User defined string** drop-down list, select the contact field that you want to map to the device.
9. Click **Continue to user information edit**.
10. Click **Save all**.

Configuring the BlackBerry Web Desktop Manager

7

You can configure the BlackBerry Web Desktop Manager to permit users to perform certain self service tasks such as creating a password for wireless activation, locking a lost or stolen BlackBerry device, deleting data from a device, or backing up device data.

For more information about the BlackBerry Web Desktop Manager, see the *BlackBerry Web Desktop Manager User Guide*.

Installing the client components of the BlackBerry Web Desktop Manager on users' computers

By default, when BlackBerry device users open the BlackBerry Web Desktop Manager for the first time, the browser prompts them to accept a client authentication certificate and install the required RIMWebComponents.cab file. The RIMWebComponents.cab file provides the BlackBerry Device Manager and USB drivers that users require to use the BlackBerry Web Desktop Manager. To install these RIMWebComponents.cab file, users must log in to their computers as a local administrator.

Allow users to activate devices using the BlackBerry Web Desktop Manager

You can specify whether users can use the BlackBerry Web Desktop Manager to activate BlackBerry devices using a wired connection to a computer.

1. In the BlackBerry Administration Service, in the **Tenant administration** menu, expand **Organization**.
2. Click **My organization**.

3. Click the **BlackBerry Web Desktop Manager information** tab.
4. Click **Edit organization** and perform one of the following actions:
 - To allow users to activate or re-activate devices, change **Allow user wireline activation** to **Activate Any PIN**.
 - To permit users to activate new devices only, change **Allow user wireline activation** to **Activate Unused PIN only**.
 - To prevent users from activating devices, change **Allow user wireline activation** to **No**.
5. Click **Save all**.

Allow users to perform self service tasks using the BlackBerry Web Desktop Manager

You can allow users to perform all of the following self service tasks using the BlackBerry Web Desktop Manager:

- specify an enterprise activation password for a BlackBerry device
 - specify a new device password and lock a device
 - delete all device data and deactivate a device
 - switch services and data from their current device to a new device
1. In the BlackBerry Administration Service, on the **Tenant administration** menu, expand **Organization**.
 2. Click **My organization**.
 3. Click the **BlackBerry Web Desktop Manager information** tab.
 4. Click **Edit organization**.
 5. Change **Allow users to perform self service tasks** to **Yes**.
 6. Click **Save all**.

Allow users to back up and restore data using the BlackBerry Web Desktop Manager

You can specify whether users can back up and restore data on BlackBerry devices using the BlackBerry Web Desktop Manager.

1. In the BlackBerry Administration Service, in the **Tenant administration** menu, expand **Organization**.
2. Click **My organization**.
3. Click the **BlackBerry Web Desktop Manager information** tab.
4. Click **Edit organization**.
5. Change **Allow users to back up and restore data** to **Yes**.
6. Click **Save all**.

Configure the domains for backing up data using the BlackBerry Web Desktop Manager

You can specify the domains that users' computers are located in so that you can limit which users can back up data on their BlackBerry devices using the BlackBerry Web Desktop Manager.

1. In the BlackBerry Administration Service, in the **Tenant administration** menu, expand **Organization**.
2. Click **My organization**.
3. Click the **BlackBerry Web Desktop Manager information** tab.
4. Click **Edit organization**.
5. In the **Device backup domains** field, type a domain that permits the user to back up data.
6. Click the **Add** icon.
7. Repeat steps 5 and 6 for each domain that you want to add.
8. Click **Save all**.

Installing applications on devices

8

You can provide applications for users to install on BlackBerry devices. You can use the following methods to provide applications to users:

Method	Description
Using the BlackBerry Desktop Software	You can install an application on a device by instructing the user to use the application loader tool that is part of the BlackBerry Desktop Software. An automated application installer installs the application files on the computer. The user uses the BlackBerry Desktop Manager to navigate to the application files and install the application on a device that the user connects to the computer.
Using the web browser on devices	You can install an application on a device by installing the files for the application on a web server and instructing the user to browse to the appropriate web address using a web browser on the device. Users can download the application from the web server using the web browser. This method does not require the user to connect the device to the computer.

Installing applications using the BlackBerry Desktop Software

You can use the automated installer for a BlackBerry Java Application to install the application files (such as the .alx identifier file and the application's .cod files) on computers. You can then instruct users to use the BlackBerry Desktop Software to install the BlackBerry Java Application on BlackBerry devices. Users must connect the devices to their computers to install the application.

If users do not have the BlackBerry Desktop Software 4.0 or later installed on the computers, they can download it from www.blackberry.com/support/downloads.

Make an application available for download from the BlackBerry Desktop Software

To allow users to install an application on BlackBerry devices using the BlackBerry Desktop Software, you must first make the application available to the BlackBerry Desktop Software.

1. Obtain the application installer for the application from the application developer, vendor, or wireless service provider. The application installer is usually an .exe file.
2. Run the application installer on the user's computer to install the .alx identifier file and .cod file in an installation folder. You can also run the application installer to install the .alx identifier file and .cod file in a shared network folder that users can access from their computers.

After you finish:

When the application is available, users can install it on their devices. For more information about installing an application using the BlackBerry Desktop Software, visit www.blackberry.com/go/docs to find the required version of the *BlackBerry Desktop Software User Guide*.

Installing applications using a web browser on devices

You can install applications on BlackBerry devices over the wireless network. This method does not require users to connect the devices to their computers.

You can add the required files for the application to a web server, and instruct users to navigate to the web address for the web server using a browser on the devices. The files that the user requires are a .jad file and the application .cod files or .jar files. Users can use the BlackBerry Browser or the wireless service provider's WAP Browser to download the files. When users access the web address, they can click a download option to install the application on their devices.

Make an application available on a web server

Before you begin:

Verify that the following MIME types are configured on the web server so that users can download and install applications on BlackBerry devices:

- .cod files: application/vnd.rim.cod
- .jad files: text/vnd.sun.j2me.app-descriptor

- .jar files (optional): application/java-archive

Obtain the .jad files and .cod files or .jar files for the application from the application developer, vendor, or wireless service provider.

1. Create a web page that you can use to install the application on devices.
2. Copy the .jad files and .cod files or .jar files to the web server that hosts the web page.
3. Send an email message to users to provide them with the web address for the web page that you created.

Install an application using a web browser on the device

Send the following instructions for installing an application to users.

1. Open a web browser on the BlackBerry device.
2. Navigate to the web address that your administrator provided you with.
3. Click **Download**.

Creating and configuring Wi-Fi profiles and VPN profiles

9

Creating and configuring Wi-Fi profiles

You can use Wi-Fi configuration settings and optional VPN configuration settings to manage BlackBerry devices that can operate on both mobile and Wi-Fi networks.

You can manage the configuration settings for user accounts that are associated with the BlackBerry Business Cloud Services by creating Wi-Fi profiles. You can create and assign one or more Wi-Fi profiles to a user account or to a group using a process that is similar to the process you use to create an IT policy and assign it to a user account.

Prerequisites: Creating Wi-Fi profiles and VPN profiles

Before you create Wi-Fi and VPN profiles, you must appropriately install, configure, and secure your organization's Wi-Fi network.

If your organization's environment requires a VPN concentrator, you must also configure a VPN concentrator for VPN access security using IPsec VPN.

To configure firewall settings, perform the following actions:

- If your organization use a proxy firewall, configure the proxy server so that it is transparent to users.
- Verify that the IP addresses for the BlackBerry Business Cloud Services that are relevant to your organization's environment are permitted addresses.
- Verify that the Wi-Fi network can connect to the BlackBerry Business Cloud Services.
- Verify that you add the IP address of the BlackBerry Business Cloud Services to the DNS server.

To configure access to the DHCP server and DNS server, you must perform the following actions:

- If necessary, configure your organization's enterprise Wi-Fi network to access the DHCP server.
- If you do not use static IP addresses, use the DNS lookup tool on a Wi-Fi enabled BlackBerry device to verify that the device can access the DHCP server.
- Use the DNS lookup tool on a Wi-Fi enabled device to verify that the device can access one or more DNS servers.

To configure user accounts in your organization's environment, perform the following actions:

- Create authentication credentials for the user accounts.
- If your organization uses EAP-TLS, EAP-TTLS, or PEAP authentication methods, permit the BlackBerry Business Cloud Services to access to the PKI infrastructure and certificates.

To permit or restrict access to a specific enterprise Wi-Fi network, do one of the following:

- Add the MAC addresses of every permitted device on a specific enterprise Wi-Fi network to an allowed list for the controller for each access point.
- Add the MAC addresses of every device that is not permitted on a specific enterprise Wi-Fi network to a restricted list for the controller for each access point.

Create a Wi-Fi profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Create Wi-Fi profile**.
3. In the **Name** field, type a name for the Wi-Fi profile.
4. Click **Save**.

After you finish: Configure the Wi-Fi profile.

Create a Wi-Fi profile based on an existing Wi-Fi profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to copy.
4. Click **Copy profile**.
5. Type a name for the new Wi-Fi profile.
6. Click **Save**.

After you finish: Configure the Wi-Fi profile.

Configure a Wi-Fi profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click a Wi-Fi profile.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, change the values for the configuration settings.
6. Click **Save All**.

After you finish:

- If the Wi-Fi network includes a captive portal, verify that you change the WLAN Enable Authentication Page option to True to permit users to access the captive portal using the WLAN Login browser on their BlackBerry devices.
- To update the device information immediately, resend the IT policy to the device.

For information about the Wi-Fi configuration settings, see the *BlackBerry Business Cloud Services Policy Reference Guide*.

Assign a Wi-Fi profile to a group

You can assign one or more Wi-Fi profiles to a group.

Before you begin: Create and configure a Wi-Fi profile.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. In the **Manage groups** section, click the group that you want to assign a Wi-Fi profile to.
4. On the **Wi-Fi profiles** tab, click **Edit group**.
5. In the **Available Wi-Fi profiles** list, click the profile that you want to assign to the group and click **Add**. Repeat for any additional profiles that you want to assign to the group.
6. Click **Save all**.

When you assign a Wi-Fi profile to a group that has at least one user account assigned to it, the BlackBerry Administration Service creates jobs to deliver the resulting objects to BlackBerry devices.

Assign a Wi-Fi profile to a user account

You can assign more than one Wi-Fi profile to a user account.

Before you begin: Create and configure a Wi-Fi profile.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for one or more user accounts.
4. Click the name of the user account that you want to assign a Wi-Fi profile to.
5. Click **Edit user**.
6. On the **Wi-Fi profiles** tab, in the **Wi-Fi profile name** section, in the drop-down list, click the Wi-Fi profile.
7. If required, in the **Wi-Fi user specific settings** section, specify the login information for the Wi-Fi profile.
8. Click the **Add** icon.
9. Click **Save all**.

When you assign a Wi-Fi profile to a user account, the BlackBerry Administration Service creates a job to deliver the resulting object to the BlackBerry device.

Delete a Wi-Fi profile

Before you begin: Verify that the Wi-Fi profile is not assigned to a user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of a Wi-Fi profile.
4. Click **Delete profile**.
5. Click **Yes - Delete the profile**.

Creating and configuring VPN profiles

Wi-Fi enabled BlackBerry devices have built-in VPN clients that supports several types of VPN concentrators.

To create a VPN profile, you configure the VPN configuration settings, such as the IP address of the VPN concentrator, user names and passwords, and cryptographic methods that the BlackBerry Business Cloud Services uses, on a device or in the BlackBerry Administration Service using a VPN profile or IT policy. You can assign one or more VPN profiles to a user account or to a group. If a user account has a VPN profile, you can associate the VPN profile with the Wi-Fi profile for the user account.

Depending on your organization's security policy, you can save a user name and password to a device to prevent the device from prompting the user for the login information the first time, or each time the device connects to the enterprise Wi-Fi network.

Create a VPN profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Create VPN profile**.
3. In the **Name** field, type a name for the VPN profile.
4. Click **Save**.

After you finish: Configure the VPN profile.

Create a VPN profile based on an existing VPN profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage VPN profiles**.
3. Click the name of the VPN profile that you want to copy.
4. Click **Copy profile**.
5. Type a name for the new VPN profile.
6. Click **Save**.

After you finish: Configure the VPN profile.

Configure a VPN profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage VPN profiles**.

3. Click the name of the VPN profile.
4. Click **Edit profile**.
5. On the **VPN profile settings** tab, change the values for the configuration settings.
6. Click **Save All**.

After you finish:

- For information about VPN configuration settings, see the *BlackBerry Business Cloud Services Policy Reference Guide*.
- To update BlackBerry device information immediately, resend the IT policy to the device.

Assign a VPN profile to a group

You can assign one or more VPN profiles to a group.

Before you begin: Create and configure a VPN profile.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. In the **Manage groups** section, click the group that you want to assign a VPN profile to.
4. On the **VPN profiles** tab, click **Edit group**.
5. In the **Available VPN profiles** list, click the profile that you want to assign to the group and click **Add**. Repeat for any additional profiles that you want to assign to the group.
6. Click **Save**.

When you assign a VPN profile to a group that has at least one user account assigned to it, the BlackBerry Administration Service creates jobs to deliver the resulting objects to BlackBerry devices.

Assign a VPN profile to a user account

You can assign one or more VPN profiles to a user account.

Before you begin: Create and configure a VPN profile.

1. In the BlackBerry Administration Service, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. Click the display name for the user account.
5. Click **Edit user**.
6. On the **VPN profiles** tab, in the **VPN profile name** section, in the drop-down list, click the appropriate VPN profile.

7. If required, in the **VPN user specific settings** section, specify the login information that you want to associate with the VPN profile.
8. Click the **Add** icon.
9. Click **Save All**.

When you assign a VPN profile to a user account, the BlackBerry Administration Service creates a job to deliver the resulting object to the BlackBerry device.

Associate a VPN profile with a Wi-Fi profile

To permit a BlackBerry device to connect to a Wi-Fi network using a VPN session, you must associate a VPN profile with a Wi-Fi profile that you assigned to the user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, in the **Wi-Fi associations** section, in the **Associated VPN Profile** drop-down list, click the VPN profile that you want to associate with the Wi-Fi profile.
6. Click **Save All**.

After you finish: To update the BlackBerry device information immediately, resend the IT policy to the device.

Delete a VPN profile

Before you begin: Verify that the VPN profile is not assigned to a user account or associated with a Wi-Fi profile.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage VPN profiles**.
3. Click the name of a VPN profile.
4. Click **Delete profile**.
5. Click **Yes - Delete the profile**.

Importing profile information from a .csv file

You can update the Wi-Fi profiles and VPN profiles that you want to assign to user accounts and the user names and passwords for the profiles by importing a .csv file using the BlackBerry Administration Service. When you import profile information from a file, you can configure the profile information for multiple user accounts at the same time.

The .csv file must contain the following information:

- user accounts that you want to update
- names of profiles that you want to change
- whether you want to add, remove, or change the profiles

Best practices: Creating a .csv file that contains profile information that you want to import

Consider the following guidelines:

- Specify only one action that you want the BlackBerry Business Cloud Services to perform in each row of the file.
- To assign more than one action to a user account, create multiple rows for the user account.
- If you are using a text editor to create the .csv file, include a comma (,) after the value that appears in each field in each row. If a field does not contain a value, include only a comma in the field.
- If you are using a text editor to create the .csv file, include a character return at the end of each row.
- If you are using a text editor to create the .csv file, use quotation marks (" ") if the value for a field contains a space (for example, "Westlee Barichak").
- Add no more than 2000 actions to a file.
- Assign a maximum of 64 profiles to BlackBerry devices.

Create a .csv file that contains profile information that you want to import

Before you begin: Using the BlackBerry Administration Service, create profiles and specify the configuration settings for the profiles.

1. Using the BlackBerry Administration Service, export user information for the user accounts that you want to update profile information for to a .csv file.

2. In any application that permits you to update .csv files, add the following fields to the .csv file that you exported in step 1:
 - Attribute Name
 - Attribute Type
 - Action
 - User Name
 - Password
3. Configure the fields for each user account in the file.
4. Save the changes.

Example: Adding profile information to user accounts

```
"User Id","Display Name","PIN","Email Address","Logon Name","Attribute
Name","Attribute Type","Action","User Name","Password"
"16","Westlee
Barichak","","wbarichak@example.com",,"wifi_1","WLAN","ADD","test
user","test password"
"17","Jovanka Buac","","jbuac@example.com",,"vpn_1","VPN","ADD"
"8","Sherisse Da
Silva","2072C4B7","sdasilva@example.com",,"wifi_1","WLAN","ADD","wlan_u
ser","wlan_pass"
"8","Sherisse Da
Silva","2072C4B7","sdasilva@example.com",,"vpn_1","VPN","ADD"
```

Example: Changing profile information that you assigned to user accounts

```
"User Id","Display Name","PIN","Email Address","Logon Name","Attribute
Name","Attribute Type","Action","User Name","Password"
"16","Westlee
Barichak","","wbarichak@rim.com",,"wlan_1","WLAN","UPDATE","update_user
name","update_password"
"8","Sherisse Da
Silva","2072C4B7","sdasilva@.rim.com",,"wifi_1","WLAN","UPDATE","update
_username","update_password"
```

Example: Removing profile information from user accounts

```
"User Id","Display Name","PIN","Email Address","Logon Name","Attribute
Name","Attribute Type","Action","User Name","Password"
"8","Lou
Sicoli","2072C4B7","lsicoli@example.com",,"wlan_1","WLAN","DELETE"
"9","Sarah
Symonds","2072C4B7","ssymonds@example.com",,"vpn_1","VPN","DELETE"
"16","Westlee
Barichak","","wbarichak@example.com",,"wlan_1","WLAN","DELETE"
```

```
"16", "Westlee
Barichak", "", "wbarichak@example.com", , "vpn_1", "VPN", "DELETE"
```

Fields in the .csv file that contains profile information

The following table describes the fields that you can configure in a .csv file. The BlackBerry Administration Service uses the fields in the .csv file to update profile information that you assigned to user accounts.

Field	Description
User Id	This field specifies the user identifier that the BlackBerry Business Cloud Services creates for each user account. You must specify a value in this field.
Display Name	This field specifies the user name for the user account.
PIN	This field specifies the BlackBerry device PIN.
Logon Name	This field specifies the name that the user can use to log in to the BlackBerry Administration Service or BlackBerry Web Desktop Manager.
Attribute Name	This field specifies the name of the Wi-Fi profile or VPN profile. You must specify a value in this field.
Attribute Type	This field specifies whether the profile is a Wi-Fi profile or VPN profile. You must specify either WLAN or VPN as the value in this field.
Action	This field specifies whether you want to add, remove, or update the profile. You must specify ADD, DELETE, or UPDATE as the value in this field.
User Name	This field specifies the user name that the device can use to access the enterprise Wi-Fi network or VPN, if a user name is required.
Password	This field specifies the password that the device can use to access the enterprise Wi-Fi network or VPN, if a password is required. You can include quotation marks (" ") in the password.

Import profile information from a .csv file

The BlackBerry Administration Service processes actions in the order that they appear in the .csv file. If two actions that you listed in the file contradict each other, the action that appears closer to the end of the file is the action that the BlackBerry Administration Service processes. If the BlackBerry Administration Service notices an error that is specific to an action during the import process (for example, you formatted an action incorrectly in the .csv file), the BlackBerry Administration Service continues to process the remaining actions in the file and displays an error message for the action that the BlackBerry Administration Service could not process.

1. In the BlackBerry Administration Service, expand **User > Manage users**.
2. In the **Search for users** section, click **Update Wi-Fi Information for users from a list**.
3. Click **Browse**.
4. Navigate to the .csv file that you want to import.
5. Click **Open**.
6. Click **Save**.

Configuring encryption and authentication methods for Wi-Fi enabled devices

10

For information about the encryption and authentication methods for Wi-Fi connections, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Business Cloud Services Security Technical Overview*.

Configuring WEP encryption

WEP encryption uses wireless clients and matching encryption keys that are located at wireless access points to secure wireless communication.

To configure WEP encryption, you must distribute the WEP keys in the Wi-Fi profiles that you assign to user accounts. The BlackBerry Business Cloud Services sends the WEP key information when users activate Wi-Fi enabled BlackBerry devices.

The WEP keys on devices must match the WEP keys that are located at the access points.

You can configure four WEP keys and a default key ID. The WEP key numbering on devices does not match the WEP key numbering in the configuration settings of the Wi-Fi profile for the enterprise Wi-Fi network. For example, WEP key 1 on the device is WEP key 0 in the configuration settings, and WEP key 2 on the device is WEP key 1 in the configuration settings. You type or copy the WEP keys for the access points as a string of hexadecimal digits.

BlackBerry devices do not support a WEP passphrase.

Configure WEP keys for devices using a Wi-Fi profile

Before you begin: Obtain the WEP keys for the wireless access point. For more information, see the documentation for the access point.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to change.

4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, configure the values for the following configuration settings:
 - Wi-Fi WEP Key 1
 - Wi-Fi WEP Key 2
 - Wi-Fi WEP Key 3
 - Wi-Fi WEP Key 4
6. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Business Cloud Services Policy Reference Guide*.
- Assign the Wi-Fi profile to the user accounts.
- Resend the IT policy that you assign to the user accounts to Wi-Fi enabled BlackBerry devices.

Related information

[Creating and configuring Wi-Fi profiles, 51](#)

Configuring PSK encryption

The IEEE 802.1X™ standard specifies PSK encryption as an access control method for enterprise Wi-Fi networks. You can use PSK encryption in small office and home environments where it is not feasible to configure server-based authentication.

To configure PSK encryption, you must distribute a passphrase to Wi-Fi enabled BlackBerry devices that matches the key or passphrase for the wireless access points. You must distribute the passphrase using the Wi-Fi profiles that you assign to user accounts. The BlackBerry Business Cloud Services sends the passphrase when users activate the BlackBerry devices.

Configure PSK encryption data for devices using a Wi-Fi profile

Before you begin: Obtain the passphrase for the wireless access point. For more information, see the documentation for the access point.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.

3. Click the name of the Wi-Fi profile that you want to change.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, in the **Wi-Fi Preshared Key** field, type the passphrase.
6. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Business Cloud Services Policy Reference Guide*.
- Assign the Wi-Fi profile to the user accounts.
- Resend the IT policy that you assign to the user accounts to Wi-Fi enabled BlackBerry devices.

Related information

[Creating and configuring Wi-Fi profiles, 51](#)

Configuring LEAP authentication

LEAP authentication is a proprietary authentication method that was developed by Cisco Systems. LEAP authentication provides one-side, server-based authentication between an enterprise Wi-Fi network and Wi-Fi enabled BlackBerry devices and provides per-client dynamic generation of WEP keys and automatic WEP key updates during a session.

BlackBerry devices support LEAP authentication that uses a user name and password. You must distribute the user name and password using a Wi-Fi profile that you assign to user accounts. Devices use a one-way function to encrypt passwords before they send the passwords to the authentication server.

Configure LEAP authentication data for devices using a Wi-Fi profile

Before you begin:

- Using the wireless access point, configure the LEAP settings to accept SSID association requests from users that have the credentials that you specify or to identify the authentication server that the Wi-Fi enabled BlackBerry devices use to verify user credentials. For more information, see the documentation for your organization's access points.
 - Configure strong password policies if Wi-Fi network authentication uses LEAP authentication.
1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
 2. Click **Manage Wi-Fi profiles**.
 3. Click the name of the Wi-Fi profile that you want to change.

4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, perform the following actions:
 - In the **Wi-Fi User Name** field, type the user name for LEAP authentication.
 - In the **Wi-Fi User Password** field, type the password for LEAP authentication.
6. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Business Cloud Services Policy Reference Guide*.
- Assign the Wi-Fi profile to the user accounts.
- Resend the IT policy that you assign to the user accounts to devices.

Related information

[Creating and configuring Wi-Fi profiles, 51](#)

Configuring PEAP authentication

If your organization implements PEAP authentication, Wi-Fi enabled BlackBerry devices must authenticate to an authentication server before they can connect to the enterprise Wi-Fi network.

PEAP authentication requires that BlackBerry devices trust the authentication server certificate. To trust the authentication server certificate, devices must trust the certification authority that issued the certificate. A certification authority that the devices and the authentication server trust mutually must generate the certificate for the authentication server.

Each device stores a list of explicitly trusted certification authority certificates. Devices that use PEAP authentication require the root certificate for the certification authority that issued the certificate.

To distribute the root certificate to devices, you can use the certificate synchronization tool in the BlackBerry Desktop Software. You must configure a Wi-Fi profile to provide the user name and password for authentication.

Configure PEAP authentication data for devices using a Wi-Fi profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to configure.

4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, perform the following actions:
 - In the **Wi-Fi User Name** field, type the user name for PEAP authentication.
 - In the **Wi-Fi User Password** field, type the password for PEAP authentication.
6. If necessary, on the **Wi-Fi profile settings** tab, configure the following configuration settings:
 - Wi-Fi Link Security
 - Wi-Fi Hard Token Required
 - Wi-Fi Server Subject
 - Wi-Fi Server SAN
 - Wi-Fi Disable Server Certificate Validation
7. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Business Cloud Services Policy Reference Guide*.
- Resend the IT policy that you assign to the user accounts to BlackBerry devices.
- Distribute the certificates.

Related information

[Creating and configuring Wi-Fi profiles, 51](#)

Prerequisites: Distributing a certificate using the BlackBerry Desktop Software

- Using a public or private certification authority, obtain or generate a digital certificate for the authentication server. The root.der certificate file is stored in the location where the certificate was created. For example, the authentication server stores a self-signed certificate locally.
- Configure each wireless access point as a client of the authentication server. You must use the same authentication version on clients and servers. For more information, see the documentation for the access points.
- Use the certificate management features of Microsoft Active Directory to download the root certificate from the certification authority server to the computer.

Distribute a certificate using the BlackBerry Desktop Software

If a BlackBerry device requires the root certificate for the certification authority, a client certificate, or both, you can distribute the certificates using the BlackBerry Desktop Software. The device can add the certificates to the list of explicitly trusted certification authority certificates or the list of client certificates.

1. On the user's computer, right-click the certificate. Click **Install certificate**.
2. Click **Next**.
3. Click **Place all certificates in the following store**.
4. Click **Browse**.
5. Perform one of the following actions:
 - If you are distributing a root certificate, click **Trusted Root Certification Authorities**.
 - If you are distributing a client certificate, click **Personal**
6. Click **OK**.
7. Click **Finish**.
8. In the **Security Warning** dialog box, click **Yes**.
9. Connect the device to the BlackBerry Desktop Software.
10. In the BlackBerry Desktop Software, select the **Certificate Synch** tool.
11. Type a password that you can use as the keystore password.
12. Perform one of the following actions:
 - If you are distributing a root certificate, on the **Root Certificates** tab, select the certificate that you add to the certificate list on the device.
 - If you are distributing a client certificate, on the **Personal** tab, select the certificate that you want to add to the certificate list on the device.

Users cannot find the certificate synchronization tool in the BlackBerry Desktop Software

Possible cause

The certificate synchronization tool was not installed when the user installed the BlackBerry Desktop Software.

Possible solution

Instruct the user to re-install the BlackBerry Desktop Software using the custom installation option. During the custom installation process, the user can install the certificate synchronization tool.

Configure PEAP configuration settings in the Wi-Fi profile on a device

If you do not configure the PEAP configuration settings using the BlackBerry Administration Service, instruct users to configure the settings in the Wi-Fi profile on the BlackBerry device.

1. On the device, in the device options, click **Wi-Fi Connections**.
2. Click the Wi-Fi profile that you want to configure.
3. Click **Edit**.
4. In the **Security Type** list, select **PEAP**.
5. Type the user name and password for the messaging server.
6. In the **CA certificate** list, click the certificate for the authentication server.
7. Select the **Inner link security type**.
8. If your organization does not use EAP-MS-CHAPv2, if necessary, in the **Token** list, select the token type.
9. If necessary, in the **Server subject** field, type the server name in the server certificate, in URL format (for example, server1.domain.com or server1.domain.net). If you leave the field blank, the device skips over it during server authentication.
10. If necessary, in the **Server SAN** field, type the alternative name for the server, in URL format (for example, server1.domain.com or server1.domain.net). If you leave the field blank, the device skips over it during server authentication.
11. If your organization uses dynamic IP addresses, verify that the **Automatically obtain IP address and DNS** option is selected.
12. Verify that the **Allow inter-access point handover** option is selected.
13. If necessary, select the **Prompt before connection** check box. If you do not select the check box, the device connects to an available wireless access point automatically.
14. If necessary, select the **Notify on authentication failure** check box.
15. If necessary, select the VPN profile.

Configuring EAP-TLS authentication

If your organization implements EAP-TLS authentication, Wi-Fi enabled BlackBerry devices must authenticate to an authentication server so that they can connect to the enterprise Wi-Fi network.

EAP-TLS authentication requires that devices trust the authentication server certificate and use a client-side certificate as the supplicant credentials. To trust the authentication server certificate, devices must trust the certificate authority that issued the certificate. A certificate authority that the devices and the authentication server trust mutually must generate the certificate for the authentication server and the certificate for each device.

Devices that use EAP-TLS authentication require a client certificate and the root certificate for the certificate authority server that created the certificate for the authentication server. You can obtain and install both certificates using the same distribution method.

To distribute the certificates to devices, you can use the certificate synchronization tool in the BlackBerry Desktop Software, or you can enroll the certificate over the wireless network. You must configure a Wi-Fi profile to provide the user name and password for authentication.

Configure EAP-TLS authentication data for devices using a Wi-Fi profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to change.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, perform the following actions:
 - In the **Wi-Fi User Name** field, type the user name for EAP-TLS authentication.
 - In the **Wi-Fi User Password** field, type the password for EAP-TLS authentication.
6. If required, configure the following configuration settings:
 - Wi-Fi Link Security
 - Wi-Fi Hard Token Required
 - Wi-Fi Server Subject
 - Wi-Fi Server SAN

- Wi-Fi Disable Server Certificate Validation

7. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Business Cloud Services Policy Reference Guide*.
- Resend the IT policy that you assign to the user accounts to Wi-Fi enabled BlackBerry devices.
- Distribute the certificates.

Related information

[Creating and configuring Wi-Fi profiles, 51](#)

[Prerequisites: Distributing a certificate using the BlackBerry Desktop Software, 66](#)

Configure EAP-TLS configuration settings in the Wi-Fi profile on a device

If you do not configure the EAP-TLS configuration settings using the BlackBerry Administration Service, instruct the users to configure the settings in the Wi-Fi profile on the Wi-Fi enabled BlackBerry device.

1. On the device, in the device options, click **Wi-Fi Connections**.
2. Click the Wi-Fi profile that you want to change.
3. Click **Edit**.
4. If a warning about a VPN profile appears, click **OK**. EAP-TLS does not require a VPN profile.
5. In the **Security Type** list, select **EAP-TLS**.
6. Type the user name and password for the messaging server.
7. In the **CA certificate** list, click the root certificate for the certification authority that created the authentication server certificate.
8. In the **Client certificate** list, click the user certificate.
9. If necessary, in the **Server subject** field, type the server name in the server certificate, in URL format (for example, server1.domain.com or server1.domain.net). If you leave the field blank, the device skips over it during server authentication.
10. If necessary, in the **Server SAN** field, type the alternative name for the server, in URL format (for example, server1.domain.com or server1.domain.net). If you leave the field blank, the device skips over it during server authentication.
11. If your organization uses dynamic IP addresses, verify that the **Automatically obtain IP address and DNS** option is selected.
12. Verify that the **Allow inter-access point handover** option is selected.

13. If necessary, select the **Prompt before connection** check box. If you do not select the check box, the device connects to an available wireless access point automatically.
14. If necessary, select the **Notify on authentication failure** check box.

Configuring EAP-TTLS authentication

If your organization implements EAP-TTLS authentication, Wi-Fi enabled BlackBerry devices must authenticate to an authentication server so that they can connect to the enterprise Wi-Fi network.

EAP-TTLS authentication requires that devices trust the authentication server certificate. To trust the authentication server certificate, devices must trust the certification authority that issued the certificate. A certification authority that the devices and the authentication server trust mutually must generate the authentication server certificate.

Each device stores a list of explicitly trusted certification authority certificates. Devices that use EAP-TTLS authentication require the root certificate for the certification authority that created the authentication server certificate.

To distribute the root certificate to devices, you can use the certificate synchronization tool in BlackBerry Desktop Software or you can enroll the certificate over the wireless network.

Configure EAP-TTLS authentication data for BlackBerry devices using a Wi-Fi profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to change.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, perform the following actions:
 - In the **Wi-Fi User Name** field, type the user name for EAP-TTLS authentication.
 - In the **Wi-Fi User Password** field, type the password for EAP-TTLS authentication.
6. If required, configure the following configuration settings:
 - Wi-Fi Link Security
 - Wi-Fi Hard Token Required
 - Wi-Fi Server Subject
 - Wi-Fi Server SAN

- Wi-Fi Disable Server Certificate Validation

7. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Business Cloud Services Policy Reference Guide*.
- Resend the IT policy that you assign to the user accounts to Wi-Fi enabled BlackBerry devices.
- Distribute the certificates.

Related information

[Creating and configuring Wi-Fi profiles, 51](#)

[Prerequisites: Distributing a certificate using the BlackBerry Desktop Software, 66](#)

Configure EAP-TTLS configuration settings in the Wi-Fi profile on a device

If you do not configure the EAP-TTLS configuration settings using the BlackBerry Administration Service, instruct a user to configure the settings in the Wi-Fi profile on the Wi-Fi enabled BlackBerry device.

1. On the device, in the device options, click **Wi-Fi Connections**.
2. Click the Wi-Fi profile that you want to change.
3. Click **Edit**.
4. In the **Security Type** list, select **EAP-TTLS**.
5. Type the user name and password for the messaging server.
6. In the **CA certificate** list, click the root certificate for the certification authority that created the authentication server certificate.
7. In the **Inner link security type** list, select **EAP-MS-CHAPv2**.
8. If necessary, in the **Server subject** field, type the server name in the server certificate, in URL format (for example, server1.domain.com or server1.domain.net). If you leave the field blank, the device skips over it during server authentication.
9. If necessary, in the **Server SAN** field, type the alternative name for the server, in URL format (for example, server1.domain.com or server1.domain.net). If you leave the field blank, the device skips over it during server authentication.
10. If your organization use dynamic IP addresses, verify that the **Automatically obtain IP address and DNS** option is selected.
11. Verify that the **Allow inter-access point handover** option is selected.
12. If necessary, select the **Prompt before connection** check box. If you do not select the check box, the device connects to an available wireless access point automatically.

13. Verify that the **Allow inter-access point handover** option is selected.
14. If necessary, select the **Notify on authentication failure check box**.

Configuring EAP-FAST authentication

EAP-FAST is an authentication method that was developed by Cisco Systems. Similar to PEAP authentication, EAP-FAST authentication encrypts EAP transactions within a TLS tunnel. Although PEAP uses a server-side digital certificate to configure the TLS tunnel, EAP-FAST uses a .pac file.

The .pac file that the BlackBerry devices and the authentication server share contains secret keys that are unique to the BlackBerry devices. The EAP-FAST master key on the authentication server generates the .pac file. EAP-FAST uses the .pac file to open the TLS tunnel and authenticates the user credentials through the TLS tunnel.

Configure EAP-FAST authentication

1. Distribute the .pac file to the wireless client over a network connection that is designed to be secure using automatic PAC provisioning.
2. Configure each wireless access point to connect to the access control server and a DHCP server.
3. Verify that the DHCP server can provide the following information to the wireless client:
 - IP address or network
 - default gateway
 - IP address of the DNS server
4. Configure the access control server.

After you finish:

- For information about the automatic provisioning process, see the documentation for your organization's authentication server.
- For information about configuring wireless access points, see the documentation for the access points.
- For information about configuring the access control server, see the documentation for the access control server.

Related information

[Creating and configuring Wi-Fi profiles](#), 51

[Prerequisites: Distributing a certificate using the BlackBerry Desktop Software](#), 66

Send EAP-FAST authentication data to a device using a Wi-Fi profile

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to configure.
4. Click **Edit profile**.
5. In the **Wi-Fi profile settings** tab, perform the following actions:
 - In the **Wi-Fi User Name** field, type the user name for PEAP authentication.
 - In the **Wi-Fi User Password** field, type the password for PEAP authentication.
6. If required, configure the following configuration settings:
 - Wi-Fi Link Security
 - Wi-Fi Inner Authentication Mode
 - Wi-Fi Hard Token Required
 - Wi-Fi Server Subject
 - Wi-Fi Server SAN
 - Wi-Fi EAP-FAST Provisioning method
 - Wi-Fi Disable Server Certificate Validation
7. Click **Save All**.

After you finish:

- For more information about configuration settings, see the *BlackBerry Business Cloud Services Policy Reference Guide*.
- Resend the IT policy that you assign to the user accounts to BlackBerry devices.
- Distribute the certificates.

Configure EAP-FAST configuration settings in the Wi-Fi profile on devices

If you do not configure the EAP-FAST configuration settings using the BlackBerry Administration Service, instruct users to configure the settings in the Wi-Fi profile on the Wi-Fi enabled BlackBerry device.

1. On the device, in the device options, click **Wi-Fi Connections**.
2. Click the Wi-Fi profile that you want to change.
3. Click **Edit**.
4. In the **Security Type** list, select **EAP-FAST**.
5. Type the user name and password for the messaging server.
6. In the **Inner link security** list, click the security type.
7. If necessary, in the **Token** list, select the token type.
8. If your organization uses dynamic IP addresses, verify that the **Automatically obtain IP address and DNS** option is selected.
9. If necessary, select the **Prompt before connection** check box. If you do not select the check box, the device connects to an available wireless access point automatically.
10. If necessary, select the **Notify on authentication failure** check box.

Configuring software tokens for devices

11

The BlackBerry Business Cloud Services is designed to work with the RSA Authentication Manager to provide software token support for use with layer 2 and layer 3 Wi-Fi authentication on Wi-Fi enabled BlackBerry devices.

When you configure a software token for users, devices use the passcode to authenticate the users to the Wi-Fi network and VPNs automatically using the PEAPv1, EAP-GTC, and EAP-TTLS or EAP-GTC authentication methods.

You can configure multiple software tokens for each user. For example, you can configure one software token that a user can use with Wi-Fi authentication and a second software token that a user can use with VPN authentication. When users try to open a Wi-Fi or VPN connection that requires two-factor authentication on the devices, the devices prompt the users to type the software token PIN and submit the current tokencode for the connection type to create the passcode for two-factor authentication.

For more information about how the BlackBerry Business Cloud Services supports software tokens, see the *BlackBerry Business Cloud Services Security Technical Overview*.

Prerequisites: Configuring devices for RSA authentication

To perform tasks in the RSA Authentication Manager, see the RSA Authentication Manager documentation, and the documentation for the RSA SecurID token.

- In the RSA Authentication Manager, configure the following policies for the PINs of the software tokens in your organization's environment:
 - whether a PIN is required for authentication
 - whether a PIN is defined by the user or generated by the RSA Authentication Manager
 - whether a PIN is alphanumeric or numeric only
 - whether a PIN has a fixed length or a variable length, with a minimum of four characters and a maximum of eight characters

- Import the token seed file (also known as the *.sdtid file) that contains the UID for each software token into the RSA Authentication Manager Database.
- In the RSA Authentication Manager Database, create a user record for each software token holder.
- In the RSA Authentication Manager Administration application, configure the following parameters for the software token seed file:
 - serial number
 - cryptographic algorithm
 - user account that you can assign the software token to
 - password to protect the software token seed file
- Communicate the password to the user.

Configure devices for RSA authentication

Software tokens use the UID and current time to authenticate the Wi-Fi enabled BlackBerry devices to the RSA Authentication Manager. To permit devices to authenticate to the RSA Authentication Manager, users must synchronize the time and date on the devices with the time and date on the computer that hosts the RSA Authentication Manager, even though the RSA Authentication Manager is designed to accommodate time differences of up to three minutes.

Instruct users to synchronize the date, time, and time zone settings on their devices with the RSA Authentication Manager by adjusting the time on the device using the Date/Time option.

After you finish:

- Assign the Wi-Fi profile to the user accounts.
- Resend the IT policy to the devices.

Configure RSA authentication over a Wi-Fi network using a software token

You must add the serial number of the software token that the Wi-Fi enabled BlackBerry devices can use to a Wi-Fi profile so that RSA authentication can occur over Wi-Fi connections.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.

2. Click **Manage Wi-Fi profiles**.
3. Click the name of the Wi-Fi profile that you want to change.
4. Click **Edit profile**.
5. On the **Wi-Fi profile settings** tab, in the **Wi-Fi Token Serial Number** field, type the serial number of the software token.
6. Click **Save All**.

After you finish:

- Assign the Wi-Fi profile to the user accounts.
- Resend the IT policy that you assign to the user accounts to BlackBerry devices.

Configure RSA authentication over a VPN network using a software token

You must add the serial number of the software token that the Wi-Fi enabled BlackBerry device can use to a VPN profile so that RSA authentication can occur over VPN connections.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Policy > Wi-Fi configuration**.
2. Click **Manage VPN profiles**.
3. Click the name of the VPN profile that you want to change.
4. Click **Edit profile**.
5. On the **VPN profile settings** tab, in the **VPN Token Serial Number** field, type the serial number of the software token.
6. Click **Save All**.

After you finish:

- Assign the VPN profile to the user accounts.
- Resend the IT policy that you assign to the user accounts to BlackBerry devices.

Assign software tokens to a user account

You must assign the software tokens that users can use to authenticate their BlackBerry devices to a Wi-Fi network or VPN network to the user accounts. Depending on the number of software token records that are available to you, you can assign up to three software tokens to each user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. Click the display name for the user account.
5. Click **Edit user**.
6. On the **Software tokens** tab, type the serial number of the software token.
7. To import the software token seed file for the user account, perform the following actions:
 - a. Click **Browse**.
 - b. Navigate to the software token seed file for the user account.
 - c. Click **Open**.
8. If you configured a password in the RSA Authentication Manager so that you can encrypt the .sdtid file, type and confirm the password.
9. In the **Timeout (minutes)** field, type the length of time, in minutes, that the Wi-Fi enabled device takes to cache the PIN.
10. Click the **Add** icon.
11. Click **Save all**.

Protecting and redistributing devices

12

Using IT administration commands to protect a lost or stolen device

The BlackBerry Business Cloud Services includes IT administration commands that you can send over the wireless network to protect sensitive data on a BlackBerry device. You can use the commands to lock the device, permanently delete work data, permanently delete user information and application data, or return the device settings to the default values.

IT administration command	Description
Specify new device password and lock device	<p>This command creates a new password and locks a device over the wireless network. You can communicate the new password to the user verbally when the user locates the device. When the user unlocks the device, the device prompts the user to accept or reject the new password.</p>
Delete only the organization data and remove device	<p>This command permanently deletes all work data that the device stores and removes the device from the BlackBerry Business Cloud Services. All personal data remains on the device.</p> <p>You can send this command to a personal device when a user no longer works at your organization and you want to delete work data from the device.</p> <p>You can also specify whether you want to delete or disable a user account from the BlackBerry Business Cloud Services after the device deletes all work data.</p> <p>This command is only available for devices that support BlackBerry Balance.</p>
Delete all device data and remove device	<p>This command permanently deletes all user information and application data that the device stores. You can configure the following options when you use this command:</p> <ul style="list-style-type: none"> Require the device to return to its factory default settings when it receives this command

IT administration command	Description
	<ul style="list-style-type: none">• Specify a delay, in hours, that must occur before the device starts to delete all the user information and application data• Specify whether the user can stop the device from permanently deleting data if the device is recovered during the delay period <p>You can send this command to a device that you want to distribute to another user in your organization, or to a device that is lost and that the user might not recover.</p> <p>You can also specify whether you want to delete or disable a user account from the BlackBerry Business Cloud Services after the device deletes all user information and application data.</p>

Protect a lost or stolen device by locking it

If a user misplaces a BlackBerry device or if a device is stolen, you can protect the data on the device by changing the password and locking the device so that it cannot be used.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the PIN for the user account.
5. In the **Device activation** section, click **Specify new device password and lock device**.
6. Type and confirm an activation password.
7. Click **Specify new device password and lock device**.

Protect a lost or stolen device by deleting all data

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the PIN for the user account.
5. In the **Device activation** list, click **Delete all device data and remove device**.
6. Click **Yes - Delete all device data and remove device**.
7. Optionally, in the **Removing users and devices** section, in the **Actions** drop-down list, perform one of the following actions:

- To delete a user account from the BlackBerry Business Cloud Services but retain the BlackBerry Business Cloud Services information in the user's email account, click **Delete the user**.
- To delete a user account from the BlackBerry Business Cloud Services and remove the BlackBerry Business Cloud Services information from the user's email account, click **Delete the user and remove BlackBerry information from the user's messaging system**.
- To disable a user account from the BlackBerry Business Cloud Services but retain the BlackBerry Business Cloud Services information in the user's email account, click **Disable as BlackBerry user**.
- To disable a user account from the BlackBerry Business Cloud Services and remove the BlackBerry Business Cloud Services information from the user's email account, click **Disable the user and remove BlackBerry information from the user's messaging system**.

After you finish:

- Verify that the BlackBerry device received the command.
- Contact your organization's wireless service provider to turn off the service for a device after you send the IT administration command that deletes all of the device data and deactivates the device.

Protect a lost device that a user might recover

If a BlackBerry device is lost but the user might recover it, you can protect the information on the device by scheduling it to start deleting all user information and application data and to become unavailable after a period of time that you specify. You can also specify whether the user can cancel the scheduled command if the user recovers the device before the data is deleted.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the PIN for the user account.
5. In the **Device activation** section, click **Delete all device data and remove device**.
6. In the **Erase Data Settings** section, perform the following actions:
 - In the **Erase Data Delay (hours)** field, type the number of hours that must elapse before the device starts deleting user information and application data.
 - In the **Allow User Override** drop-down list, click **Yes** to permit the user to cancel the scheduled command on the device if the user recovers it.
7. Optionally, in the **Removing users and devices** section, in the **Actions** drop-down list, perform one of the following actions:

- To delete a user account from the BlackBerry Business Cloud Services but retain the BlackBerry Business Cloud Services information in the user's email account, click **Delete the user**.
 - To delete a user account from the BlackBerry Business Cloud Services and remove the BlackBerry Business Cloud Services information from the user's email account, click **Delete the user and remove BlackBerry information from the user's messaging system**.
 - To disable a user account from the BlackBerry Business Cloud Services but retain the BlackBerry Business Cloud Services information in the user's email account, click **Disable as BlackBerry user**.
 - To disable a user account from the BlackBerry Business Cloud Services and remove the BlackBerry Business Cloud Services information from the user's email account, click **Disable the user and remove BlackBerry information from the user's messaging system**.
8. Click **Yes - Delete all device data and remove device**.

Preparing a device for redistribution to a new user

You can prepare a BlackBerry device for redistribution to a new user by performing one of the following actions:

- Use the security options on the device to permanently delete all user data
- Connect the device to the BlackBerry Administration Service and delete all user data from the device permanently
- Connect the device to the BlackBerry Administration Service and delete all user and device data from the device permanently

For more information about using the security options on the device to permanently delete all user data, see the user guide for the device.

After the user receives the device, you must activate it.

Related information

[Activating BlackBerry devices](#), 26

Delete user data and assign a device to a new user

1. Connect the BlackBerry device to the computer that you used to log in to the BlackBerry Administration Service.
2. If you receive a prompt, type the device password.
3. In the BlackBerry Administration Service, on the **Devices** menu, click **Attached devices > Manage current device**.
4. Click **Remove user data from current device**.

5. Click **Yes – Remove user data**.
6. Click **Assign current device**.
7. Search for the user account that you want to assign the device to.
8. Select the user name.
9. Click **Associate user**.
After you assign the user account to the device, the activation process begins automatically.
10. On the **Devices** menu, click **Attached devices > Device software**.
11. Install the applications that the user requires on the device.

Delete user data and device data and assign a device to a new user

If you perform this task, you are deleting user data and device data permanently. You must reinstall the BlackBerry Device Software before you assign the BlackBerry device to a new user.

1. Connect the device to the computer that you used to log in to the BlackBerry Administration Service.
2. If you receive a prompt, type the device password.
3. In the BlackBerry Administration Service, on the **Devices** menu, click **Attached devices > Manage current device**.
4. Click **Delete all device data and remove device**.
5. Click **Yes – Delete all device data and remove device**.
6. Reinstall the BlackBerry Device Software using the BlackBerry Administration Service, BlackBerry Desktop Manager, or BlackBerry Web Desktop Manager.
7. Activate the device.

Related information

[Activating BlackBerry devices](#), 26

Managing groups and user accounts

13

Managing groups

You can reduce the time that you spend managing user accounts by creating groups of similar user accounts and assigning IT policies, to the group. Properties that you assign to a group are assigned to all user accounts in the group.

You can assign properties to user accounts at the individual level or group level. The properties at the individual level override the properties at the group level.

After you add a user account to a group, you can override the properties that you configured for the account at the group level by changing the properties at the user account level.

If you remove a user account from a group, the account name remains in the global users list but it does not appear in the group list.

Using default groups to manage user accounts

The BlackBerry Business Cloud Services includes preconfigured default groups that you can use in your organization's environment instead of creating groups.

Default group	Description of the default group
Default	This group assigns the Default IT policy to group members.
Password required	This group assigns members the Password Required IT policy to group members.

Remove a user account from a group

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.

2. Click **Manage groups**.
3. Click the group name.
4. In the **Manage users in group membership** list, click **Remove users from group membership**.
5. Search for a user account.
6. Select the check boxes beside the display names for the user accounts that you want to remove.
7. Click **Remove from group membership**.

Change the properties of a group

After you create a group, specify the properties that you want to apply to all user accounts that are in the group. You can copy the properties from one group to another. When you add user accounts to a group, the group properties are applied to the new accounts automatically.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. Click the group name.
4. Click **Edit group**.
5. Switch between the appropriate tabs and make the appropriate changes.
6. Click **Save all**.

Rename a group

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.
3. Click the group name.
4. Click **Edit group**.
5. In the **Group information** section, in the **Name** field, type a new name for the group.
6. Click **Save all**.

Delete a group

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **Group**.
2. Click **Manage groups**.

3. Click the group name.
4. Click **Delete group**.
5. Click **Yes - Delete the group**.

Managing user accounts

You can move user accounts from one group to another and you can delete user accounts from the BlackBerry Business Cloud Services.

If you change a user's display name in their email account, the BlackBerry Business Cloud Services should update the user account within 15 minutes of when the change occurs. If you move a hidden email account that does not appear in the contact list, you must update the user account that is associated with the BlackBerry Business Cloud Services manually. You can reload the user account information to display the most up-to-date information on the screen.

When you delete a user account, all of the user account information is deleted from the BlackBerry Business Cloud Services.

Move a user account to a different group

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. On the **Groups** tab, in the **Current groups** list, click the group that you want to remove the user from.
7. Click **Remove**.
8. In the **Available groups** list, click the group that you want to move the user account to.
9. Click **Add**.
10. Click **Save all**.

Delete a user account from the BlackBerry Business Cloud Services

If you delete a user account, you also delete all user account information from the BlackBerry Business Cloud Services.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Disable as BlackBerry user**.
6. Click **Yes - Disable as BlackBerry user**.
7. Click **Back to search**.
8. In the **Search users > User criteria** section, type the display name for the user account.
9. Click the display name for the user account.
10. In the **Status** list, click **Yes - Delete user**.

Update a user account manually

You can reload user account information to display the latest information on the screen without searching for a user account again.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. In the **Status** list, click **Reload user**.

Resend service books to a BlackBerry device

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the BlackBerry device PIN.
5. In the **Communications** list, click **Resend service books to a device**.

Managing organizer data synchronization

14

Managing the wireless backup and recovery of organizer data

The wireless backup feature backs up user account settings and data from BlackBerry devices to the BlackBerry Business Cloud Services automatically. You can use the wireless backup feature to synchronize organizer data to devices without affecting the performance of Microsoft Office 365. You can also use the wireless backup feature to restore data from the BlackBerry Business Cloud Services to the device. By default, wireless backup is turned on when you activate BlackBerry devices.

Turn off the wireless backup of organizer data for a user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Organizer data synchronization** tab, in the **General** section, in the **Automatic wireless backup turned on** drop-down list, click **No**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Delete a user's organizer data from the BlackBerry Business Cloud Services

If the BlackBerry Business Cloud Services writes a user's organizer data from a BlackBerry device to the BlackBerry Business Cloud Services incorrectly, the organizer data on the BlackBerry Business Cloud Services might become corrupt. In this case, you can delete the organizer data from the BlackBerry Business Cloud Services.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for one or more user accounts.
4. Select the check boxes beside the display names of the appropriate user accounts.
5. In the **Organizer data synchronization** list, click **Clear backed up data for organizer data synchronization**.

Delete organizer data for members of a user group from the BlackBerry Business Cloud Services

If the BlackBerry Business Cloud Services is not writing organizer data for members of a user group from their BlackBerry devices to the BlackBerry Business Cloud Services correctly, the organizer data in the BlackBerry Business Cloud Services might be corrupted. You can delete the organizer data from the BlackBerry Business Cloud Services. This action forces the devices to synchronize the current organizer data with the BlackBerry Business Cloud Services over the wireless network.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Click **View more criteria**.
4. In the **Group criteria** section, in the **Specific group** drop-down list, click the appropriate group.
5. Click **Search**.
6. Select all users.
7. In the **Organizer data synchronization** list, click **Clear backed up data for organizer data synchronization**.

Changing how organizer data synchronizes

Turn off organizer data synchronization for a user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Organizer data synchronization** tab, in the **General** section, perform one of the following actions:
 - To prevent the synchronization of organizer data, in the **General** section, in the **Wireless synchronization turned on** drop-down list, click **No**.
 - To prevent the synchronization of specific types of organizer data, in the **General** section, in the **Wireless synchronization turned on** drop-down list, click **Yes**. In the **Synchronization turned on** drop-down list, click **No** for each type of organizer data that you do not want to synchronize.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Change the direction of organizer data synchronization for a user account

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name of the user account.
5. Click **Edit user**.
6. In the **Message configuration** section, click **Default configuration**.
7. On the **Organizer data synchronization** tab, for each type of organizer data, in the **Synchronization type** drop-down list, perform one of the following actions:

- To synchronize data from the BlackBerry Business Cloud Services to a BlackBerry device only, click **Server to Device**.
 - To synchronize data from the device to the BlackBerry Business Cloud Services only, click **Device to Server**.
 - To synchronize data from the device to the BlackBerry Business Cloud Services and from the BlackBerry Business Cloud Services to the device, click **Bidirectional**.
8. Click **Continue to user information edit**.
 9. Click **Save all**.

Change how the BlackBerry Administration Service resolves conflicts for a specific user account during organizer data synchronization

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Organizer data synchronization** tab, for each type of organizer data, in the **Conflict resolution** drop-down list, perform one of the following actions:
 - To specify that the BlackBerry Business Cloud Services data overrides the BlackBerry device data, click **Server Wins**.
 - To specify that the device data overrides the BlackBerry Business Cloud Services data, click **Device Wins**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Synchronizing contact pictures

By default, the BlackBerry Business Cloud Services synchronizes pictures that users add to contact list entries between the BlackBerry device and their email account. A user can add, delete, and change pictures in the email account or on the device.

If a picture is larger than 32 KB, the BlackBerry Business Cloud Services cannot synchronize the contact picture with a device from the email account.

Turn off synchronization of contact pictures for a user account

Before you begin: Verify that you turned on the mappings for organizer data synchronization for a specific user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the display name for the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Mappings for organizer data synchronization** tab, in the **Additional mappings** section, in the **Picture** drop-down list, click **None**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Synchronizing calendars

Start corrective calendar synchronization manually for a user account

By default, the BlackBerry Business Cloud Services synchronizes the calendar on each BlackBerry device user's computer with the calendar on each BlackBerry device at a regular interval. You can use the BlackBerry Administration Service to start corrective calendar synchronization manually for a user account.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the PIN for the user account.
5. In the **Communications** list, click **Synchronize calendar**.

Managing your organization's cloud messaging services

15

Managing message forwarding

You can define the message forwarding settings for user accounts and groups that are associated with the BlackBerry Business Cloud Services. The settings control how the BlackBerry Business Cloud Services forwards email messages to BlackBerry devices. By default, email message forwarding is turned on when you add a user account to the BlackBerry Business Cloud Services.

Users can configure message forwarding settings on their devices, or by using the BlackBerry Web Desktop Manager. The settings that you define override the settings that users define.

Forward email messages to a device when filter rules do not apply

You can configure the BlackBerry Business Cloud Services to deliver email messages to a user's BlackBerry device when email filters do not apply.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of a user account.
5. In the **Messaging configuration** section, click **Default configuration**.
6. Click **Edit user**.
7. On the **Email** tab, in the **Email message filter rules** section, click **Forward email messages to the device**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Do not deliver email messages to a BlackBerry device when no filter rules apply

You can configure the BlackBerry Business Cloud Services to prevent the delivery of email messages to a BlackBerry device when email message filters do not apply to the email messages.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of a user account.
5. In the **Messaging configuration** section, click **Default configuration**.
6. Click **Edit user**.
7. On the **Email** tab, in the **Email message filter rules** section, click **Do not forward email messages to the device**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Forward email messages from inbox subfolders to a BlackBerry device

You can specify which email subfolders the BlackBerry Business Cloud Services can forward email messages from. By default, the BlackBerry Business Cloud Services forwards messages from the inbox only.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Email** tab, in the **Redirection settings** section, select the folders that you want the BlackBerry Business Cloud Services to forward email messages from.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Turn off email message forwarding to a user account

You can temporarily stop the BlackBerry Business Cloud Services from forwarding email messages to a BlackBerry device (for example, if a user is out of a wireless coverage area and does not want to receive email messages during that time). When you turn off message forwarding for a user account, the user can send email messages from the device, but cannot receive email messages.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. Click **Edit user**.
5. In the **Messaging configuration** section, click **Default configuration**.
6. In the **Email services settings** section, in the **Redirect to BlackBerry device** drop-down list, click **No**.
7. Click **Continue to user information edit**.
8. Click **Save all**.

After you finish: The user can turn on message forwarding on the device manually.

Turn off email message forwarding to user accounts in a group

You can temporarily stop the BlackBerry Business Cloud Services from forwarding email messages to user accounts that belong to a user group (for example, if the members of the user group are out of a wireless coverage area and do not want to receive email messages during that time). When you turn off message forwarding for user accounts, users can send email messages from their BlackBerry devices, but cannot receive email messages.

Users can turn on email message forwarding on the device manually.

1. In the BlackBerry Administration Service, on the **BlackBerry Solution management** menu, expand **User**.
2. Click **Manage users**.
3. Click **View more criteria**.
4. In the **Group criteria** section, in the **Specific group** drop-down list, click the group you want to turn off message forwarding for.
5. Click **Search**.
6. Select all users.
7. In the **Device services** list, click **Turn off redirection for selected devices**.

Turn off synchronization for email messages that are sent from a BlackBerry device

If you do not want the Sent Items folder on a BlackBerry device to receive a copy of email messages that a user sends from the device, you can turn off synchronization for email messages that the user sends from the device.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Services** tab, in the **Email services settings** section, in the **Save copy in sent folder** drop-down list, click **No**.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Managing the incoming message queue

The incoming message queue stores email messages from the cloud messaging services until the BlackBerry Business Cloud Services processes the email messages and sends them to BlackBerry devices.

Delete email messages for user accounts from the incoming message queue

You can delete email messages for one or more user accounts from the incoming message queue. This permits you to manage the size of the queue and to manage user accounts that have a high number of pending email messages.

When you delete pending email messages from the incoming message queue, the BlackBerry Business Cloud Services does not send the email messages to the user's BlackBerry device but the messages are not deleted from the user's Inbox.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.

3. Search for one or more user accounts.
4. Select the user accounts that you want to delete incoming messages for.
5. In the **Pending data packets** list, click **Purge pending data packets for selected devices**.

If wireless calendar synchronization for a user account is turned on, the BlackBerry Business Cloud Services deletes pending meeting invitations or updates from the incoming message queue and sends them at a later time. The BlackBerry Business Cloud Services does not delete IT policies and IT administration commands from the incoming message queue.

Viewing email messages that contain HTML and rich content

The BlackBerry Business Cloud Services supports email messages that contain HTML and rich content.

View whether a user turned on support for email messages that contain HTML and rich content for a BlackBerry device

You can view whether a user turned on support for email messages with HTML and rich content and whether a user can download images to a BlackBerry device automatically. A user can choose whether to turn off support on the device.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for the user account that you assigned the device to.
4. In the search results, click the user name.
5. In the **Messaging configuration** section, click **Default configuration**.
6. In the **Email Services Settings** section, check if **Rich content turned on** and **Automatic downloading of inline images turned on** are configured to **Yes**.

Synchronizing folders on a BlackBerry device

Control which personal contact subfolders a user can synchronize with a BlackBerry device

By default, a user can synchronize all of the personal contact subfolders on the cloud messaging services with the contact lists on a BlackBerry device. To help manage network resources, you can select the personal contact subfolders that a user can synchronize.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. Click the display name for the user account.
5. Click **Edit User**.
6. In the **Messaging configuration** section, click **Device configuration**.
7. On the **Email** tab, in the **Private contact folders** section, select the private contact subfolders that you want to permit the user to synchronize with the contact lists on the device.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Control which personal email folders a user can synchronize with a BlackBerry device

To help manage network resources, you can select the personal email folders that a user can synchronize with a BlackBerry device.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for the user account.

4. In the search results, click the display name for a user account.
5. Click **Edit User**.
6. In the **Messaging configuration** section, click **Device configuration**.
7. On the **Email** tab, in the **Redirection settings** section, select the folders that you want to permit the user to synchronize with the device.
8. Click **Continue to user information edit**.
9. Click **Save all**.

After you finish: To permit the user to select which folders that the user can synchronize, instruct the user to select folders using the BlackBerry Web Desktop Manager.

Managing signatures and disclaimers in email messages

Add a signature to email messages that a user sends from a BlackBerry device

To enforce a signature format policy in your organization, you can add a standard signature to the email messages that users send from their BlackBerry devices.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Email** tab, in the **Mail options** section, in the **Auto signature** field, type the signature that you want to appear in the email messages that the user sends from the device.
8. Click **Continue to user information edit**.
9. Click **Save all**.

Add a disclaimer to email messages that a user sends from a device

You can add a disclaimer to all email messages that a user sends. A user cannot change the disclaimer that you define.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for the user account.
4. In the search results, click the name of the user account.
5. Click **Edit user**.
6. In the **Messaging configuration** section, click **Default configuration**.
7. On the **Email** tab, in the **Mail options** section, perform one of the following actions:
 - To add a disclaimer before the body of the message, in the **Prepended disclaimer text** field, type the disclaimer.
 - To add a disclaimer after the user signature, in the **Appended disclaimer text** field, type the disclaimer.
8. Click **Continue to user information edit**.
9. Click **Save all**.

How the BlackBerry Business Cloud Services manages attachments

The BlackBerry Business Cloud Services receives message attachments from supported BlackBerry devices and reconciles the attachments with the cloud messaging services.

The BlackBerry Business Cloud Services limits the file size of attachments that it can receive from a device to a maximum of 3 MB. If the BlackBerry Business Cloud Services receives more than one attachment at a time, it limits the total file size of all of the attachments to a maximum of 5 MB.

Users can download attachments in any format to their devices. Users can open and make changes to file formats using an appropriate third-party application on their devices. Users might be able to open specific file formats using the media application on the devices.

Attachment file formats that are supported

Format	Extension
Adobe Acrobat	.pdf
ASCII text	.txt
Audio	.amr, .mp3, .wav, .wma
Corel WordPerfect 7 to 10	.wpd
HTML	.htm, .html
Images	.bmp, .gif, .jpeg, .jpg, .png, .ppm, .tif, .tiff, .wmf
Microsoft Excel 97 to 2003, 2007, 2010, and XP	.xls, .xlsx
Microsoft PowerPoint 97 to 2003, 2007, 2010, and XP	.pps, .ppsx, .ppt, .pptx
Microsoft Word 97 to 2003, 2007, 2010, and XP	.doc, .dot, .dotx, .docx
OpenOffice.org 1.1	.odp, .ods, .odt, .ott
RTF	.rtf
ZIP archives	.zip

Managing the delivery of IT policies to devices

16

Managing the distribution settings for a specific job

When you assign or change an IT policy, the BlackBerry Administration Service creates jobs to deliver the resulting settings to BlackBerry devices. Before the BlackBerry Administration Service delivers a specific job, you can change the delivery schedule of the job, priority of the job, and how the job delivers IT policies to devices.

If you do not change the schedule, priority, or distribution settings for a job, the job uses the default schedule and distribution settings.

Change how a job sends IT policies to devices

You can change how the BlackBerry Administration Service sends IT policy settings and changes that are part of a specific job to BlackBerry devices. You can change a job's distribution settings for IT policies only if the job is not running. If you change the distribution settings for a job, your organization's environment might experience an effect on performance.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Manage deployment jobs**.
3. Search for the job that you want to change.
4. In the search results, click the ID of the job that you want to change.
5. Click **Edit job**.
6. On the **IT Policy Distribution** tab, perform any of the following tasks:

Task	Steps
Change the default recurrence day for sending IT policy changes.	1. Click the Edit icon for the default recurrence day.

Task	Steps
	<ol style="list-style-type: none"> 2. In the Scheduled deployment day(s) drop-down list, click the appropriate recurrence option. If necessary, select the appropriate days of the week. 3. In the Start time drop-down list, click the appropriate option. If necessary, change the start time and end time. 4. Click the Update icon. <p>By default, the recurrence day is Every day and the start time is All day.</p>
Add a new recurrence day for sending IT policy changes.	<p>If you want to add more than one recurrence day for sending IT policy changes, the schedules for the separate recurrence days cannot overlap.</p> <ol style="list-style-type: none"> 1. In the Scheduled deployment day(s) drop-down list, click the appropriate recurrence option. If necessary, select the appropriate days of the week. 2. In the Start time drop-down list, click the appropriate option. If necessary, change the start time and end time. 3. Click the Add icon.
<ol style="list-style-type: none"> 7. To turn on throttling for all IT policy tasks in the job, in the Default throttling enablement for all IT policy tasks in each job in a time window section, select Enabled to reduce load on system. 8. If necessary, in the Default throttling for all IT policy tasks in each job in a time window section, in the Maximum number of simultaneous tasks per BlackBerry Administration Service instance field, type the maximum number of IT policy tasks in the job that you want the BlackBerry Business Cloud Services to process at the same time. The default value is 25. 9. If necessary, in the Total number of tasks per time window per BlackBerry Administration Service instance field, type the total number of IT policy tasks in the job that you want the BlackBerry Business Cloud Services to process during each processing interval. The default value is 150. 10. Click Save all. 	

Specify the start time and priority for a job

If a job has not started running, you can specify when you want the job to start. If you do not specify the start time for a job, the job starts according to the distribution settings that you configured in the BlackBerry Administration Service. You can also change the priority of a job. By default, all jobs have a medium priority. If you change the priority of a job to low, the BlackBerry Business Cloud Services processes it after the jobs with a medium or high priority. The BlackBerry Business Cloud Services processes jobs with a high priority before it processes jobs with a medium or low priority.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.

2. Click **Manage deployment jobs**.
3. Search for the job that you want to change.
4. In the search results, click the ID of the job that you want to change.
5. Click **Edit job**.
6. In the **Priority** drop-down list, click the appropriate priority for the job.
7. In the **Job Schedule** section, in the **Effective Date** field, select the start date for the job.
8. Click **Save all**.

View the status of a job

After you assign an IT policy to user accounts or change an existing IT policy, a job sends the IT policy changes to BlackBerry devices. You can view the status of a job to determine if it is ready to run, currently running, completed, or completed with task failures.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Manage deployment jobs**.
3. Search for a job.
4. In the search results, in the **Status** column, view the status of the job.
5. To view more information about a job or to change a job, click the ID of the job.

Related information

[Stopping a job that is running](#), 107

View the status of a task

Each deployment job consists of multiple tasks. Each task delivers a specific object or setting that performs an action on the BlackBerry device, such as applying updated IT policy settings.

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Manage deployment job tasks**.
3. Search for a task.
4. In the search results, in the **Status** column, view the status of the task.
5. To view more information about a task, click **More**.

Stopping a job that is running

After you assign an IT policy to user accounts or change an existing IT policy, a job sends the IT policy changes to BlackBerry devices. If you want to make changes to a job that is running, you can stop a job.

When you stop a job, the BlackBerry Business Cloud Services does not process the remaining tasks in the job, and the BlackBerry Administration Service changes the scheduled start time for the job to the following day. The job returns to a ready to run status. You can make changes to the start time, priority, and distribution settings of the job. If you do not change the start time for the job, the BlackBerry Business Cloud Services delivers the job on the following day using the default job schedule settings. When the job starts again, the BlackBerry Business Cloud Services processes the remaining tasks in the job.

If you want to delete a job, change the start date of the job to a date that exceeds the job failure period that you configured in the job schedule settings. The default job failure period is 30 days.

Stop a job that is running

1. In the BlackBerry Administration Service, on the **Devices** menu, expand **Deployment jobs**.
2. Click **Manage deployment jobs**.
3. Search for the job that you want to stop.
4. In the search results, click the ID of the job that you want to stop.
You can only stop jobs with a Running status.
5. Click **Stop Current Execution**.
6. Click **Yes - Stop Current Execution**.

Related information

[View the status of a job, 106](#)

[Managing the distribution settings for a specific job, 104](#)

Glossary

17

AES	Advanced Encryption Standard
API	application programming interface
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	A Domain Name System (DNS) is an Internet database that translates domain names that are meaningful and recognizable by people into the numeric IP addresses that the Internet uses.
EAP-FAST	Extensible Authentication Protocol Flexible Authentication via Secure Tunneling
EAP-GTC	Extensible Authentication Protocol Generic Token Card
EAP-TLS	Extensible Authentication Protocol Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol Tunneled Transport Layer Security
EAP	Extensible Authentication Protocol
ETP	Email Transfer Protocol
GPO	Group Policy Object
GPS	Global Positioning System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IP address	An Internet Protocol (IP) address is an identification number that each computer or mobile device uses when it sends or receives information over a network, such as the Internet. This identification number identifies the specific computer or mobile device on the network.
IPsec	Internet Protocol Security
IT administration command	An IT administration command is a command that you can send over the wireless network to protect sensitive information on a BlackBerry device or delete all BlackBerry device data.
IT policy	An IT policy consists of various IT policy rules that control the security features and behavior of BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager.

IT policy rule	An IT policy rule permits you to customize and control the actions that BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager can perform.
LEAP	Lightweight Extensible Authentication Protocol
MAC	message authentication code
messaging server	A messaging server sends and processes messages and provides collaboration services, such as updating and communicating calendar and address book information.
MIME	Multipurpose Internet Mail Extensions
PAC	proxy auto-configuration
PEAP	Protected Extensible Authentication Protocol
PIN	personal identification number
PKI	Public Key Infrastructure
PSK	pre-shared key
RTF	Rich Text Format
SAN	subject alternative name
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service
SQL	Structured Query Language
SSID	service set identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of communication protocols that is used to transmit data over networks, such as the Internet.
TLS	Transport Layer Security
Triple DES	Triple Data Encryption Standard
UID	unique identifier
USB	Universal Serial Bus
VPN	virtual private network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WLAN	wireless local area network

XML

Extensible Markup Language

Provide feedback

18

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

Legal notice

19

©2012 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated. Alt-N Technologies is a trademark of Alt-N Technologies, Ltd. AOL is a trademark of AOL LLC. 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. Corel and WordPerfect are trademarks of Corel Corporation. Google Mail is a trademark of Google Inc. IEEE and 802.1X are trademarks of the Institute of Electrical and Electronics Engineers, Inc. IBM, Domino, Lotus, and Sametime are trademarks of International Business Machines Corporation. Microsoft, Active Directory, ActiveX, Excel, Internet Explorer, Outlook, Lync, MSN, PowerPoint, Windows, Windows Vista, and Windows XP are trademarks of Microsoft Corporation. Firefox is a trademark of Mozilla Foundation. Novell and GroupWise are trademarks of Novell, Inc. PGP is a trademark of PGP Corporation. Java and JavaScript RSA and RSA SecurID are trademarks of RSA Security. Wi-Fi is a trademark of the Wi-Fi Alliance. Yahoo! is a trademark of Yahoo! Inc. 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 Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM 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 web sites (collectively the "Third Party Products and Services"). RIM 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 RIM 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, MERCHANTABILITY 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 RIM 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 RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM 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 RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM 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 RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM 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 RIM OR ANY AFFILIATES OF RIM 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 RIM'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 RIM'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 RIM and RIM 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 RIM.

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

This product contains a modified version of HTML Tidy. Copyright © 1998-2003 World Wide Web Consortium (Massachusetts Institute of Technology, European Research Consortium for Informatics and Mathematics, Keio University). All Rights Reserved.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada