BlackBerry UEM

Profiles, variables, and email templates

Administration

12.13

Contents

Using profiles, variables, and email templates

Profiles, variables, and email templates help you to manage user accounts and communicate with users efficiently.

Profiles are an efficient way for your organization to configure multiple devices. They allow you to store all the settings for a specific configuration in one place and quickly deliver the settings to the appropriate devices.

Variables represent standard account attributes (for example, username) and other predefined attributes (for example, server address used for device activation). You can use variables in profiles, compliance notifications, activation emails, and event notifications.

Email templates allow you to customize and personalize email messages that BlackBerry UEM sends to users and administrators.

Profiles

A profile contains configuration information for devices and each profile type supports a particular configuration, such as certificates, work connection settings, or settings that enforce certain standards for devices. You can specify settings for BlackBerry 10, iOS, macOS, Android, and Windows devices in the same profile and then distribute the configuration information to devices by assigning the profile to user accounts, user groups, or device groups.

Assigning profiles

You can assign profiles to user accounts, user groups, and device groups. Some profile types may use ranking to determine which profile is sent to a device.

- Ranked profile type: You can assign one profile to a user and one profile to each group they belong to, and BlackBerry UEM sends only one of the assigned profiles to the user's device.
- Non-ranked profile type: You can assign multiple profiles to a user and multiple profiles to each group they belong to, and BlackBerry UEM sends all the assigned profiles to the user's device.

Note: You cannot assign an activation profile to a device group.

For a complete list of profiles, see the Profiles reference.

For information on how to assign profiles, see Assign a profile or IT policy to a user account or Assign a profile or IT policy to a user group

How BlackBerry UEM chooses which profiles to assign

For ranked profile types, BlackBerry UEM sends only one profile of each type to a device and uses predefined rules to determine which profile to assign to a user and the devices that the user activates.

Assigned to	Rules
User account (view Summary tab)	1. A profile assigned directly to a user account takes precedence over a profile of the same type assigned indirectly by user group. 2. If a user is a member of multiple user groups that have different profiles of the same type, BlackBerry UEM assigns the profile with the highest ranking. 3. If applicable, the preconfigured Default profile is assigned if no profile is assigned to a user account directly or through user group membership. **Note:** BlackBerry UEM includes a Default activation profile, Default compliance profile, Default enterprise connectivity profile, and Default Enterprise Management Agent profile with preconfigured settings for each device type.

Assigned to	Rules
Device (view device tab)	By default, a device inherits the profile that BlackBerry UEM assigns to the user who activates the device. If a device belongs to a device group, the following rules apply: 1. A profile assigned to a device group takes precedence over the profile of the same type that BlackBerry UEM assigns to a user account. 2. If a device is a member of multiple device groups that have different profiles of the same type, BlackBerry UEM assigns the profile with the highest ranking.

BlackBerry UEM might have to resolve conflicting profiles when you perform any of the following actions:

- Assign a profile to a user account, user group, or device group
- Remove a profile from a user account, user group, or device group
- Change the profile ranking
- Delete a profile
- Change user group membership (user accounts and nested groups)
- Change device attributes
- Change device group membership
- Delete a user group or device group

Copy a profile

You can copy existing profiles to quickly create similar profiles for different groups in your organization.

1. On the menu bar, click **Policies and profiles**.
2. Click a profile type.
3. Click the name of the profile that you want to copy.
4. Click .
5. Type a name and description for the new profile.
6. Make changes on the appropriate tab for each device type.
7. Click **Save**.

After you finish: If necessary, rank profiles.

View a profile

You can view the following information about a profile:

- Settings common to all device types and specific to each device type
- List and number of user accounts that the profile is assigned to (directly and indirectly)
- List and number of user groups that the profile is assigned to (directly)

1. On the menu bar, click **Policies and profiles**.
2. Expand a profile type.
3. Click the name of the profile that you want to view.

Change profile settings

If you update an activation profile, the new profile settings apply only to additional devices that a user activates. Activated devices do not use the new profile settings until the user reactivates them.

1. On the menu bar, click **Policies and profiles**.
2. Click a profile type.
3. Click the name of the profile that you want to change.
4. Click ✎.
5. Make changes to any common settings.
6. Make changes on the appropriate tab for each device type.
7. Click **Save**.

After you finish: If necessary, rank profiles.

Remove a profile from user accounts or user groups

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

Note: The Default activation profile, Default compliance profile, Default enterprise connectivity profile, and Default Enterprise Management Agent profile can only be removed from a user account if you assigned them directly to the user.

1. On the menu bar, click **Policies and profiles**.
2. Select a profile type.
3. Click the name of the profile that you want to remove from user accounts or user groups.
4. Perform one of the following tasks:

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

Delete a profile

When you delete a profile, BlackBerry UEM removes the profile from the users and devices that it is assigned to. To delete a profile that is associated with other profiles, you must first remove all existing associations. For

example, before you can delete a proxy profile that is associated with a VPN profile and a Wi-Fi profile, you must change the associated proxy profile value in both the VPN profile and the Wi-Fi profile.

Note: You cannot delete the Default activation profile, Default compliance profile, Default enterprise connectivity profile, or Default Enterprise Management Agent profile.

1. On the menu bar, click **Policies and profiles**.
2. Click a profile type.
3. Select the check boxes for the IT policies you want to delete.
4. Click 🗑.
5. Click **Delete**.

Rank profiles

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

- A user is a member of multiple user groups that have different profiles of the same type.
- A device is a member of multiple device groups that have different profiles of the same type.

1. On the menu bar, click **Policies and profiles**.
2. Select a profile type.
3. Click ⬇⬆.
4. Use the arrows to move profiles up or down the ranking.
5. Click **Save**.

Profiles reference

The following table lists all BlackBerry UEM profiles:

Profile name	Description	Supported device types	Ranked or not ranked[1]	Configure
Policy				
Activation	Specifies the device activation settings for users, such as the activation type and the number and types of devices.	All devices	Ranked	Create an activation profile
BlackBerry Dynamics	Allows devices to access BlackBerry Dynamics apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect.	iOS macOS Android Windows	Ranked	Create a BlackBerry Dynamics profile

Profile name	Description	Supported device types	Ranked or not ranked[1]	Configure
App lock mode	Specify a single app to run on devices.	Supervised iOS device Samsung Knox devices activated with MDM Windows 10 Education and Windows 10 Enterprise devices	Ranked	Create an app lock mode profile
Enterprise Management Agent	Specifies when devices connect to BlackBerry UEM for app or configuration updates when a push notification is not available.	iOS Android Windows BlackBerry 10	Ranked	Create an Enterprise Management Agent profile
Compliance				
Compliance	Defines the device conditions that are not acceptable in your organization and sets enforcement actions.	All devices	Ranked	Create a compliance profile
Compliance (BlackBerry Dynamics)	This is a read-only profile that displays the compliance settings that were imported from Good Controlinto an on-premises BlackBerry UEM.	iOS macOS Android Windows	N/A	Managing BlackBerry Dynamics compliance profiles
Device SR requirements	Defines the software release versions that devices must have installed.	Android BlackBerry 10	Ranked	Create a device SR requirements profile
Email, calendar, and contacts				
Email	Specifies how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler.	All devices	Ranked	Create an email profile

Profile name	Description	Supported device types	Ranked or not ranked[1]	Configure
IMAP/POP3 email	Specifies how devices connect to an IMAP or POP3 mail server, and how to synchronize email messages.	iOS Android macOS Windows	Not ranked	Create an IMAP/POP3 email profile
Gatekeeping	Specifies the Microsoft Exchange servers to use for automatic gatekeeping.	All devices	Ranked	Create a gatekeeping profile
CalDAV	Specifies the server settings that devices can use to synchronize calendar information.	iOS macOS	Not ranked	Create a CalDAV profile
CardDAV	Specifies the server settings that devices can use to synchronize contact information.	iOS macOS	Not ranked	Create a CardDAV profile
Networks and connections				
Wi-Fi	Specifies how devices connect to a work Wi-Fi network.	All devices	Not ranked	Create a Wi-Fi profile
VPN	Specifies how devices connect to a work VPN.	All devices	Not ranked	Create a VPN profile
Proxy	Specifies how devices use a proxy server to access web services on the Internet or a work network.	iOS macOS Android BlackBerry 10	Ranked	Create a proxy profile

Profile name	Description	Supported device types	Ranked or not ranked[1]	Configure
Enterprise connectivity	Specifies how devices can connect to your organization's resources using enterprise connectivity. Enterprise connectivity is always enabled for BlackBerry 10 devices. For iOS, Android Enterprise, Samsung Knox Workspace, and BlackBerry 10 devices, the enterprise connectivity profile specifies whether devices can use BlackBerry Secure Connect Plus.	iOS Android BlackBerry 10	Ranked	Enable BlackBerry Secure Connect Plus Managing enterprise connectivity for BlackBerry 10 devices
BlackBerry Dynamics connectivity	Defines the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when using BlackBerry Dynamics apps.	iOS macOS Android Windows	Ranked	Create a BlackBerry Dynamics connectivity profile
BlackBerry 2FA	Enables two-factor authentication for users and specifies the configuration of the preauthentication and self-rescue features.	iOS Android BlackBerry 10	Ranked	Create a BlackBerry 2FA profile
Network usage	Allows you to control whether work apps on iOS devices can use the mobile network or data roaming.	iOS	Ranked	Create a network usage profile
Web content filter	Limits the websites that a user can view on supervised iOS devices.	Supervised iOS device	Not ranked	Create a web content filter profile
Single sign-on	Specifies how devices authenticate with secure domains automatically after users type their username and password for the first time.	iOS BlackBerry 10	Ranked	Create a single sign-on profile

Profile name	Description	Supported device types	Ranked or not ranked[1]	Configure
Managed domains	Configures iOS devices to notify users about sending email outside of trusted domains and restricts the apps that can view documents downloaded from internal domains.	iOS	Not ranked	Create a managed domains profile
AirPrint	Allows you to add printers to users' AirPrint printer lists.	iOS	Not ranked	Create an AirPrint profile
AirPlay	Allows you to add devices to users' AirPlay device lists.	iOS	Not ranked	Create an AirPlay profile
Access Point Name	Allows you to specify APNs for devices to use to connect to carriers.	Android	Not ranked	Create an Access Point Name profile
Single sign-on extension	Allows devices running iOS (or iPadOS) 13 and later to authenticate using single sign-on.	iOS	Not ranked	Create a single sign-on extension profile
Protection				
Windows Informat Protection	Specifies the Windows Information Protection setting in Windows 10.	Windows 10	Ranked	Create a Windows information protection profile
Microsoft Intune app protection	Allows you to manage apps protected by Microsoft Intune.	iOS Android	Not ranked	Create a Microsoft Intune app protection profile
Location service	Allows you to request the location of devices and view the approximate locations on a map.	iOS Android Windows	Ranked	Create a location service profile
Do not disturb	Allows you to block BlackBerry Work for Android and BlackBerry Work for iOS notifications during off-work days and hours that you define.	iOS Android	Ranked	Create a Do not disturb profile
Custom				

Profile name	Description	Supported device types	Ranked or not ranked[1]	Configure
Device	Allows you to configure the information that displays on devices.	iOS Android BlackBerry 10 Windows	Ranked	Create a device profile
Custom payload	Specifies custom configuration information using payload code for devices.	iOS	Not ranked	Create a custom payload profile
Per-app notification	Allows you to configure the notification settings for system apps and apps that you manage using BlackBerry UEM.	Supervised iOS devices running	Ranked	Create a per-app notification profile
Certificates				
CA certificate	Specifies a CA certificate that devices can use to establish trust with a work network or server.	All devices	Not ranked	Create a CA certificate profile
Shared certificate	Specifies a client certificate that devices can use to authenticate users with a work network or server.	iOS macOS Android	Not ranked	Create a shared certificate profile
User credential	Specifies the CA connection that devices use to obtain a client certificate that is used to authenticate with a work network or server.	iOS macOS Android BlackBerry 10	Not ranked	Create a user credential profile
SCEP	Specifies the SCEP server that devices use to obtain a client certificate that is used to authenticate with a work network or server.	All devices	Not ranked	Create a SCEP profile
Certificate retrieval	Specifies how devices retrieve certificates from LDAP servers.	BlackBerry 10	Ranked	Create a certificate retrieval profile
OCSP	Specifies the OCSP responders that BlackBerry 10 devices can use to check the status of certificates.	BlackBerry 10	Ranked	Create an OCSP profile

Profile name	Description	Supported device types	Ranked or not ranked[1]	Configure
CRL	Specifies the CRL configurations that BlackBerry UEM can use to check the status of certificates.	BlackBerry devices powered by Android BlackBerry 10	Ranked	Create a CRL profile
Certificate mapping profile	Specifies which client certificates apps must use	Android	Ranked	Create a certificate mapping profile

[1]For definitions of ranked or non-ranked profiles, see Assigning profiles.

Profiles reference - iOS devices

The following table lists all BlackBerry UEM profiles supported on iOS devices:

Profile name	Description	Configure
Policy		
Activation	Specifies the device activation settings for users, such as the activation type and the number and types of devices.	Create an activation profile
BlackBerry Dynamics	Allows devices to access BlackBerry Dynamics apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect.	Create a BlackBerry Dynamics profile
App lock mode	Specify a single app to run on devices. Supervised iOS devices only.	Create an app lock mode profile
Enterprise Management Agent	Specifies when devices connect to BlackBerry UEM for app or configuration updates when a push notification is not available.	Create an Enterprise Management Agent profile
Compliance		
Compliance	Defines the device conditions that are not acceptable in your organization and sets enforcement actions.	Create a compliance profile
Compliance (BlackBerry Dynamics)	This is a read-only profile that displays the compliance settings that were imported from Good Controlinto an on-premises BlackBerry UEM.	Managing BlackBerry Dynamics compliance profiles
Email, calendar, and contacts		

Profile name	Description	Configure
Email	Specifies how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler.	Create an email profile
IMAP/POP3 email	Specifies how devices connect to an IMAP or POP3 mail server, and how to synchronize email messages.	Create an IMAP/POP3 email profile
Gatekeeping	Specifies the Microsoft Exchange servers to use for automatic gatekeeping.	Create a gatekeeping profile
CalDAV	Specifies the server settings that devices can use to synchronize calendar information.	Create a CalDAV profile
CardDAV	Specifies the server settings that devices can use to synchronize contact information.	Create a CardDAV profile
Networks and connections		
Wi-Fi	Specifies how devices connect to a work Wi-Fi network.	Create a Wi-Fi profile
VPN	Specifies how devices connect to a work VPN.	Create a VPN profile
Proxy	Specifies how devices use a proxy server to access web services on the Internet or a work network.	Create a proxy profile
Enterprise connectivity	Specifies how devices can connect to your organization's resources using enterprise connectivity. For iOS devices, the enterprise connectivity profile specifies whether devices can use BlackBerry Secure Connect Plus.	Enable BlackBerry Secure Connect Plus
BlackBerry Dynamics connectivity	Defines the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when using BlackBerry Dynamics apps.	Create a BlackBerry Dynamics connectivity profile
BlackBerry 2FA	Enables two-factor authentication for users and specifies the configuration of the preauthentication and self-rescue features.	Create a BlackBerry 2FA profile
Network usage	Allows you to control whether work apps on iOS devices can use the mobile network or data roaming.	Create a network usage profile

Profile name	Description	Configure
Web content filter	Limits the websites that a user can view on supervised iOS devices. Supervised iOS devices only.	Create a web content filter profile
Single sign-on	Specifies how devices authenticate with secure domains automatically after users type their username and password for the first time.	Create a single sign-on profile
Single sign-on extension	Allows devices running iOS (or iPadOS) 13 or later to authenticate using single sign-on.	Create a single sign-on extension profile
Managed domains	Configures iOS devices to notify users about sending email outside of trusted domains and restricts the apps that can view documents downloaded from internal domains.	Create a managed domains profile
AirPrint	Allows you to add printers to users' AirPrint printer lists.	Create an AirPrint profile
AirPlay	Allows you to add devices to users' AirPlay device lists.	Create an AirPlay profile
Protection		
Microsoft Intune app protection	Allows you to manage apps protected by Microsoft Intune.	Create a Microsoft Intune app protection profile
Location service	Allows you to request the location of devices and view the approximate locations on a map.	Create a location service profile
Do not disturb	Allows you to block BlackBerry Work for iOS notifications during off-work days and hours that you define.	Create a Do not disturb profile
Custom		
Device	Allows you to configure the information that displays on devices.	Create a device profile
Custom payload	Specifies custom configuration information using payload code for devices.	Create a custom payload profile
Per-app notification	Allows you to configure the notification settings for system apps and apps that you manage using BlackBerry UEM. Supervised iOS devices only.	Create a per-app notification profile
Certificates		

Profile name	Description	Configure
CA certificate	Specifies a CA certificate that devices can use to establish trust with a work network or server.	Create a CA certificate profile
Shared certificate	Specifies a client certificate that devices can use to authenticate users with a work network or server.	Create a shared certificate profile
User credential	Specifies the CA connection that devices use to obtain a client certificate that is used to authenticate with a work network or server.	Create a user credential profile
SCEP	Specifies the SCEP server that devices use to obtain a client certificate that is used to authenticate with a work network or server.	Create a SCEP profile

Profiles reference - macOS devices

The following table lists all BlackBerry UEM profiles on macOS devices:

Profile name	Description	Configure
Policy		
Activation	Specifies the device activation settings for users, such as the activation type and the number and types of devices.	Create an activation profile
BlackBerry Dynamics	Allows devices to access BlackBerry Dynamics apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect.	Create a BlackBerry Dynamics profile
Compliance		
Compliance	Defines the device conditions that are not acceptable in your organization and sets enforcement actions.	Create a compliance profile
Compliance (BlackBerry Dynamics)	This is a read-only profile that displays the compliance settings that were imported from Good Controlinto an on-premises BlackBerry UEM.	Managing BlackBerry Dynamics compliance profiles
Email, calendar, and contacts		
Email	Specifies how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler.	Create an email profile

Profile name	Description	Configure
IMAP/POP3 email	Specifies how devices connect to an IMAP or POP3 mail server, and how to synchronize email messages.	Create an IMAP/POP3 email profile
Gatekeeping	Specifies the Microsoft Exchange servers to use for automatic gatekeeping.	Create a gatekeeping profile
CalDAV	Specifies the server settings that devices can use to synchronize calendar information.	Create a CalDAV profile
CardDAV	Specifies the server settings that devices can use to synchronize contact information.	Create a CardDAV profile
Networks and connections		
Wi-Fi	Specifies how devices connect to a work Wi-Fi network.	Create a Wi-Fi profile
VPN	Specifies how devices connect to a work VPN.	Create a VPN profile
Proxy	Specifies how devices use a proxy server to access web services on the Internet or a work network.	Create a proxy profile
BlackBerry Dynamics connectivity	Defines the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when using BlackBerry Dynamics apps.	Create a BlackBerry Dynamics connectivity profile
Certificates		
CA certificate	Specifies a CA certificate that devices can use to establish trust with a work network or server.	Create a CA certificate profile
Shared certificate	Specifies a client certificate that devices can use to authenticate users with a work network or server.	Create a shared certificate profile
User credential	Specifies the CA connection that devices use to obtain a client certificate that is used to authenticate with a work network or server.	Create a user credential profile
SCEP	Specifies the SCEP server that devices use to obtain a client certficate that is used to authenticate with a work network or server.	Create a SCEP profile

Profiles reference - Android devices

The following table lists all BlackBerry UEM profiles supported on Android devices:

Profile name	Description	Configure
Policy		
Activation	Specifies the device activation settings for users, such as the activation type and the number and types of devices.	Create an activation profile
BlackBerry Dynamics	Allows devices to access BlackBerry Dynamics apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect.	Create a BlackBerry Dynamics profile
App lock mode	Specify a single app to run on devices. Samsung Knox devices activated with MDM only	Create an app lock mode profile
Enterprise Management Agent	Specifies when devices connect to BlackBerry UEM for app or configuration updates when a push notification is not available.	Create an Enterprise Management Agent profile
Compliance		
Compliance	Defines the device conditions that are not acceptable in your organization and sets enforcement actions.	Create a compliance profile
Compliance (BlackBerry Dynamics)	This is a read-only profile that displays the compliance settings that were imported from Good Controlinto an on-premises BlackBerry UEM.	Managing BlackBerry Dynamics compliance profiles
Device SR requirements	Defines the software release versions that devices must have installed and specifies an update period for apps that are running in the foreground.	Create a device SR requirements profile
Email, calendar, and contacts		
Email	Specifies how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler.	Create an email profile
IMAP/POP3 email	Specifies how devices connect to an IMAP or POP3 mail server, and how to synchronize email messages.	Create an IMAP/POP3 email profile
Gatekeeping	Specifies the Microsoft Exchange servers to use for automatic gatekeeping.	Create a gatekeeping profile
Networks and connections		

Profile name	Description	Configure
Wi-Fi	Specifies how devices connect to a work Wi-Fi network.	Create a Wi-Fi profile
VPN	Specifies how devices connect to a work VPN.	Create a VPN profile
Proxy	Specifies how devices use a proxy server to access web services on the Internet or a work network.	Create a proxy profile
Enterprise connectivity	Specifies how devices can connect to your organization's resources using enterprise connectivity. For Android Enterprise and Samsung Knox Workspace devices, the enterprise connectivity profile specifies whether devices can use BlackBerry Secure Connect Plus.	Enable BlackBerry Secure Connect Plus
BlackBerry Dynamics connectivity	Defines the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when using BlackBerry Dynamics apps.	Create a BlackBerry Dynamics connectivity profile
BlackBerry 2FA	Enables two-factor authentication for users and specifies the configuration of the preauthentication and self-rescue features.	Create a BlackBerry 2FA profile
Access Point Name profile	Allows you to specify APNs for devices to use to connect to carriers.	Create an Access Point Name profile
Protection		
Microsoft Intune app protection	Allows you to manage apps protected by Microsoft Intune.	Create a Microsoft Intune app protection profile
Location service	Allows you to request the location of devices and view the approximate locations on a map.	Create a location service profile
Do not disturb	Allows you to block BlackBerry Work for Android notifications during off-work days and hours that you define.	Create a Do not disturb profile
Custom		
Device	Allows you to configure the information that displays on devices.	Create a device profile
Certificates		
CA certificate	Specifies a CA certificate that devices can use to establish trust with a work network or server.	Create a CA certificate profile

Profile name	Description	Configure
Shared certificate	Specifies a client certificate that devices can use to authenticate users with a work network or server.	Create a shared certificate profile
User credential	Specifies the CA connection that devices use to obtain a client certificate that is used to authenticate with a work network or server.	Create a user credential profile
SCEP	Specifies the SCEP server that devices use to obtain a client certificate that is used to authenticate with a work network or server.	Create a SCEP profile
CRL	Specifies the CRL configurations that BlackBerry UEM can use to check the status of certificates. BlackBerry devices powered by Android only	Create a CRL profile
Certificate mapping profile	Specifies which client certificates apps must use	Create a certificate mapping profile

Profiles reference - Windows 10 devices

The following table lists all BlackBerry UEM profiles supported on Windows 10 devices:

Profile name	Description	Configure
Policy		
Activation	Specifies the device activation settings for users, such as the activation type and the number and types of devices.	Create an activation profile
BlackBerry Dynamics	Allows devices to access BlackBerry Dynamics apps such as BlackBerry Work, BlackBerry Access, and BlackBerry Connect.	Create a BlackBerry Dynamics profile
App lock mode	Specify a single app to run on devices. Supported by Windows 10 Education and Windows 10 Enterprise devices only.	Create an app lock mode profile
Enterprise Management Agent	Specifies when devices connect to BlackBerry UEM for app or configuration updates when a push notification is not available.	Create an Enterprise Management Agent profile
Compliance		

Profile name	Description	Configure
Compliance	Defines the device conditions that are not acceptable in your organization and sets enforcement actions. BlackBerry UEM includes a Default compliance profile.	Create a compliance profile
Compliance (BlackBerry Dynamics)	This is a read-only profile that displays the compliance settings that were imported from Good Controlinto an on-premises BlackBerry UEM.	Managing BlackBerry Dynamics compliance profiles
Email, calendar, and contacts		
Email	Specifies how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler.	Create an email profile
IMAP/POP3 email	Specifies how devices connect to an IMAP or POP3 mail server, and how to synchronize email messages.	Create an IMAP/POP3 email profile
Gatekeeping	Specifies the Microsoft Exchange servers to use for automatic gatekeeping.	Create a gatekeeping profile
Networks and connections		
Wi-Fi	Specifies how devices connect to a work Wi-Fi network.	Create a Wi-Fi profile
VPN	Specifies how devices connect to a work VPN.	Create a VPN profile
BlackBerry Dynamics connectivity	Defines the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when using BlackBerry Dynamics apps.	Create a BlackBerry Dynamicsconnectivity profile
Protection		
Windows Information Protection	Specifies the Windows Information Protection setting in Windows 10.	Create a Windows Information Protection profile
Location service	Allows you to request the location of devices and view the approximate locations on a map.	Create a location service profile
Custom		
Device	Allows you to configure the information that displays on devices.	Create a device profile
Certificates		

Profile name	Description	Configure
CA certificate	Specifies a CA certificate that devices can use to establish trust with a work network or server.	Create a CA certificate profile
SCEP	Specifies the SCEP server that devices use to obtain a client certificate that is used to authenticate with a work network or server.	Create a SCEP profile

Profiles reference - BlackBerry 10 devices

The following table lists all BlackBerry UEM profiles supported on BlackBerry 10 devices:

Profile name	Description	Configure
Policy		
Activation	Specifies the device activation settings for users, such as the activation type and the number and types of devices.	Create an activation profile
Enterprise Management Agent	Specifies when devices connect to BlackBerry UEM for app or configuration updates when a push notification is not available.	Create an Enterprise Management Agent profile
Compliance		
Compliance	Defines the device conditions that are not acceptable in your organization and sets enforcement actions.	Create a compliance profile
Device SR requirements	Defines the software release versions that BlackBerry 10 devices must have installed.	Create a device SR requirements profile
Email, calendar, and contacts		
Email	Specifies how devices connect to a work mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler.	Create an email profile
Gatekeeping	Specifies the Microsoft Exchange servers to use for automatic gatekeeping.	Create a gatekeeping profile
Networks and connections		
Wi-Fi	Specifies how devices connect to a work Wi-Fi network.	Create a Wi-Fi profile
VPN	Specifies how devices connect to a work VPN.	Create a VPN profile

Profile name	Description	Configure
Proxy	Specifies how devices use a proxy server to access web services on the Internet or a work network.	Create a proxy profile
Enterprise connectivity	Specifies how devices can connect to your organization's resources using enterprise connectivity. Enterprise connectivity is always enabled for BlackBerry 10 devices. The enterprise connectivity profile also specifies whether devices can use BlackBerry Secure Connect Plus.	Managing enterprise connectivity for BlackBerry 10 devices Enable BlackBerry Secure Connect Plus
BlackBerry 2FA	Enables two-factor authentication for users and specifies the configuration of the preauthentication and self-rescue features.	Create a BlackBerry 2FA profile
Single sign-on	Specifies how devices authenticate with secure domains automatically after users type their username and password for the first time.	Create a single sign-on profile
Custom		
Device	Allows you to configure the information that displays on devices.	Create a device profile
Certificates		
CA certificate	Specifies a CA certificate that devices can use to establish trust with a work network or server.	Create a CA certificate profile
User credential	Specifies the CA connection that devices use to obtain a client certificate that is used to authenticate with a work network or server.	Create a user credential profile
SCEP	Specifies the SCEP server that devices use to obtain a client certficate that is used to authenticate with a work network or server.	Create a SCEP profile
Certificate retrieval	Specifies how devices retrieve certificates from LDAP servers.	Create a certificate retrieval profile
OCSP	Specifies the OCSP responders that BlackBerry 10 devices can use to check the status of certificates.	Create an OCSP profile
CRL	Specifies the CRL configurations that BlackBerry UEM can use to check the status of certificates.	Create a CRL profile

Variables

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

You can use variables in profiles,compliance notifications, activation emails, and event notifications. Use variables to reference values instead of specifying the actual values. When the profile, compliance notification, activation email, or event notification is sent to devices, the variables are replaced with the values that they represent.

Note: IT policies and BlackBerry Dynamics app configurations do not support variables.

Using variables in profiles

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

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

In compliance profiles, you can use variables to customize the compliance notifications that BlackBerry UEM sends to users.

Default variables

The following default variables are available in BlackBerry UEM:

Variable name	Description	Primary use
%AccessKeyExpiry%	Date and time that an access key expires	Activation email messages
%AccessKeys%	Access keys that are automatically generated and used to activate BlackBerry Dynamics apps	Activation email messages
%ActivationPassword%	Activation password that is automatically generated or that you set for a user	Activation email messages
%ActivationPasswordExpiry%	Date and time that an activation password expires	Activation email messages
%ActivationQRCode%	QR Code for device activation	Activation email messages
%ActivationURL%	Web address of the server that receives activation requests	Activation email messages

Variable name	Description	Primary use
%ActivationUserName%	Username for activation requests Equivalent to %UserEmailAddress% (if available for a user) or SRP ID\%UserName%	Activation email messages
%AdminPortalURL%	Web address of BlackBerry UEM management console	Administrator access email messages (not customizable)
%AllEventVariables%	A list of events (as configured in an event notification) that occurred in BlackBerry UEM	Event notifications
%ClientlessActivationURL%	Web address of the server that receives activation requests from devices that are running Windows 10	Activation email messages
%CommonName%	Common Name (CN) attribute extracted from the distinguished name	App configurations
%ComplianceApplicationList%	List of apps that violate compliance rules (non-assigned apps are installed and required apps are not installed)	Compliance notifications
%ComplianceEnforcementAction%	Enforcement action that BlackBerry UEM performs if a device is non-compliant	Compliance notifications
%ComplianceEnforcementActionWitl %	Enforcement action that BlackBerry UEM performs if a device is non-compliant, including a description of the enforcement action	Compliance notifications
%ComplianceRuleViolated%	Compliance rule that a device violated	Compliance notifications
%DeviceIMEI%	International Mobile Equipment Identity number of a device	Profiles
%DeviceModel%	Model number of a device	Compliance notifications
%EmailAddressDomain%	Domain of an email address	App configurations
%EmailAddressLocalPart%	Local part of an email address (for example, "username" in username@example.com)	App configurations
%ExchangeAlloweddeviceId%	Gatekeeping device ID	App configurations
%ICCIdentifier%	Integrated Circuit Card Identifier	App configurations
%IMSIdentity%	International Mobile Subscriber Identity	App configurations

Variable name	Description	Primary use
%IOSUDIdentifier%	iOS Unique Device Identifier	App configurations
%MEIdentifier%	Mobile Equipment Identifier	App configurations
%OrganizationUnit%	Organizational Unit (OU) attribute extracted from the distinguished name	App configurations
%PhoneNumber%	Phone number of a device	App configurations
%RsaRootCaCertUrl%	Web address of the RSA root CA certificate	Activation email messages
%SamAccountName%	Username used to support earlier versions of Windows	App configurations
%SerialNumber%	Serial number of a device	Subject setting in SCEP profiles
%SSLCertName%	Common Name of the secure communication certificate	Activation email messages
%SSLCertSHA%	Fingerprint of the secure communication certificate	Activation email messages
%UserDisplayName%	Display name of a user	Activation email messages, profiles
%UserDisplayName_RDNValue%	Display name of a user with special characters escaped according to the LDAP DN specification	Subject setting in SCEP profiles
%UserDistinguishedName%	Directory user's distinguished name with special characters escaped according to the LDAP DN specification For a local user, equivalent to %UserName_RDNValue%	Subject setting in SCEP profiles
%UserDomain%	Microsoft Active Directory domain that a directory user belongs to	Profiles
%UserDomain_RDNValue%	Microsoft Active Directory domain that a directory user belongs to with special characters escaped according to the LDAP DN specification	Subject setting in SCEP profiles
%UserEmailAddress%	Email address of a user	Activation email messages, profiles

Variable name	Description	Primary use
%UserEmailAddress_RDNValue%	Email address of a user with special characters escaped according to the LDAP DN specification	Subject setting in SCEP profiles
%UserFirstName%	First name of a user	App configurations
%UserLastName%	Last name of a user	App configurations
%UserLocale%	Locale of a user (for example, en-US)	App configurations
%UserName%	Username of a user	Activation email messages, profiles
%UserName_RDNValue%	Username of a user with special characters escaped according to the LDAP DN specification	Subject setting in SCEP profiles
%UserPrincipalName%	Directory user's principal name For a local user, equivalent to %UserEmailAddress%	Profiles
%UserPrincipalName_RDNValue%	Directory user's principal name with special characters escaped according to the LDAP DN specification For a local user, equivalent to %UserEmailAddress_RDNValue%	Subject setting in SCEP profiles
%UserSelfServicePortalURL%	Web address of BlackBerry UEM Self-Service	Activation email messages
%WIFIMacAddress%	Wi-Fi MAC address	App configurations

If you configure high availability for the management consoles in the BlackBerry UEM domain in an on-premises environment, it is a best practice to update the %AdminPortalURL% and %UserSelfServicePortalURL% variables. For more information, see the Planning content.

Custom variables

You use labels to define the attributes and passwords that custom variables represent. For example, you can specify "VPN password" as the label for the %custom_pswd1% variable. When you create or update a user account, labels are used as field names and you specify the appropriate values for the custom variables that your organization uses. All user accounts support custom variables, including administrator user accounts.

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

The following custom variables are available in BlackBerry UEM:

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

Define custom variables

You must define custom variables before you can use them. Only custom variables that have a label are displayed when you create or update a user account.

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

Using custom variables

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

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

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

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

Email templates

Using email templates allows you to customize and personalize email messages that are sent to users for any of the following reasons:

- Device activation - send emails to users with instructions for activating their device and send separate emails containing their activation passwords
- Compliance - send email notifications to users when their device is out of compliance
- BlackBerry Dynamics apps activation - send emails to users containing access keys
- Event notifications - send emails to notify administrators about particular events in BlackBerry UEM

You can personalize email messages by using variables in the email templates for items like the user's name, email address, or activation password. Using the HTML editor, you can customize the appearance of emails by using different fonts, colors, and images. You can create multiple templates to use for different device types or activation types. You can edit the default email templates or create new ones.

When you add a user to BlackBerry UEM, create a compliance profile, or generate passwords, you can select the email template to use. BlackBerry UEM sends the personalized email message to the user based on the template that you select.

Default email templates

BlackBerry UEM includes some default email templates. Depending on your BlackBerry UEM configuration, you will see some or all of the following default email templates in Settings > General settings > Templates:

Type	Default email template	Description
Device activation	Default activation email	This template contains the instructions that a user needs to activate their device. You can choose to send two separate emails to the user: one containing the activation instructions and a second that contains only the activation password. If you don't select a different template, BlackBerry UEM uses this template when it sends an activation email to a user. You can edit this template, but you can't delete it.
Default managed Google account credentials	Default managed Google account credentials	This template is used in environments that have a managed Google domain. It provides the user's Google account password. Users automatically receive this email if they are assigned an Android Enterprise activation type. You can edit this template, but you can't delete it. You should also send the Default activation email template to provide users with the instructions to activate their devices in BlackBerry UEM.

Type	Default email template	Description
Default Android Enterprise activation code	Default Android work profile activation code	This template is used in environments that have a managed Google domain. It provides a Google activation code. You can edit this template, but you can't delete it. You should also send the Default activation email template to provide users with the instructions to activate their devices in BlackBerry UEM.
Apple DEP device activation	Apple DEP activation email	This template contains the instructions that a user needs to activate an Apple DEP device. You can choose to send two separate email messages to the user: one containing the activation instructions and a second that contains only the activation password. You can edit or delete this template.
BlackBerry Dynamics access key	BlackBerry Dynamics access key email	This template contains the instructions that a user needs to activate a BlackBerry Dynamics app using an access key. You can edit or delete this template.
Default Work space only (Android Enterprise) activation email	Default Work space only (Android work profiles) activation	This template is used in environments that do not have a managed Google domain and that use Android Enterprise. This template contains the instructions that a user needs to activate their device. You can choose to send two separate emails to the user: one containing the activation instructions and a second that contains only the activation password. You can edit or delete this template.
Compliance violation	Default compliance email	This template contains information about a user's device compliance. You can associate this template with a compliance profile. You can edit this template, but you can't delete it.
Event notification	BlackBerry UEM event notification email	This template contains information for administrators about an event that has occurred in BlackBerry UEM. You can associate this template with an event notification. You can edit this template, but you can't delete it.
Device activated notification	Device activated notification email	This template contains information about the device that a user activated. A device activated notification email is sent when the user activates their device using the BlackBerry UEM Client. A BlackBerry Dynamics device activated notification email is sent when the user activates a BlackBerry Dynamics app on their device. You can edit this template, but you can't delete it.

Type	Default email template	Description
Self-service login notification	Self-service login notification email	This template contains information about the user that logged into the BlackBerry UEM Self-Service portal (for example, the IP address and the date and time). You can edit this template, but you can't delete it.

Edit an email template

1. On the menu bar, click **Settings > General settings**.
2. Click **Templates**.
3. Click the template that you want to edit.
4. Edit the **Name**, **Subject**, or **Message** fields.
5. When you have completed your changes, click **Save**.

Suggested template text

The suggested text is used in the default email templates. If you edit the default email templates and later want to use the default text, you can copy and paste it from here. If the default text is updated between releases of BlackBerry UEM, you can see the updated text here. For a list of variables that you can use in email templates, see Default variables.

Name	Suggested text
Android work profile activation code	**Subject: An Android work profile activation code has been created for you** %UserDisplayName%, To activate an Android device with a work profile only, your administrator has created an Android work profile activation code for you. You will receive your BlackBerry UEM activation password in a separate email message. Your Android work profile activation code: %GoogleActivationCode% Your Android work profile activation code will expire on %ActivationPasswordExpiry%. If you have any questions, contact your administrator.

Name	Suggested text
Default managed Google acc credentials	**Subject: A Google account has been created for you** %UserDisplayName%, To enable the work profile on your device, your administrator has created a Google account for you. You will need your Google account password when you activate the work profile. The Google account password displayed here is not the password that you use when you activate your device on BlackBerry UEM. You will receive your BlackBerry UEM activation password in a separate email message, or you can set your BlackBerry UEM activation password in BlackBerry UEM Self-Service. You will need the following information when you activate the work profile: • Your work email address: %UserEmailAddress% • Your Google account password: %Password% You can manage your Google Account at https://myaccount.google.com. If you change the password for your Google Account, the password included in this email will no longer apply, and you must use the new password instead. Please keep this information for your records. If you have any questions, contact your administrator.
Apple DEP device activation email First email	**Subject: Activating your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled your iOS device for BlackBerry UEM. To activate your device you need the following information: • Your work email address: %UserEmailAddress% • Your device activation password: Your activation password will be delivered in a separate email. You can manage your own device with BlackBerry UEM Self-Service at %UserSelfServicePortalURL%. To log in, use the following username: • BlackBerry UEM Self-Service username: %UserName% Your BlackBerry UEM Self-Service password may have been delivered in a separate email. If you have not received it, contact your administrator. Please keep this information for your records. If you have any questions, contact your administrator.

Name	Suggested text
Apple DEP device activation email Second email	**Subject: Password to activate your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled your mobile device for BlackBerry UEM. To activate your device you need the following information: Your device activation password: %ActivationPassword% Your password will expire on %ActivationPasswordExpiry%. Please follow the instructions in the "Activating your device on BlackBerry UEM" email to activate your iOS device on BlackBerry UEM. If you have any questions, contact your administrator. Welcome to BlackBerry UEM!
BlackBerry Dynamics access key email	**Subject: An access key for a BlackBerry Dynamics app has been created for you** %UserDisplayName%, Your administrator has created an access key for a BlackBerry Dynamics app. This email contains the access key and instructions to set up the app. If you have been given permission to use more than one app, you will receive more than one email. Each email has an access key that can be used to set up an app. You can use any of your access keys to set up any app, but you can only use each access key once. Before you begin, make sure you have mobile data or Wi-Fi coverage. 1. Open the BlackBerry Dynamics app. 2. When you are prompted, enter the following information. • Email address: %UserEmailAddress% • Access key: %AccessKeys% Your access key will expire on %AccessKeyExpiry%. 3. You may be prompted to create a password. You will need to enter this password when you open the app. If you have any questions, contact your administrator.

Name	Suggested text
Default activation email First email	**Subject: Activating your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled your mobile device for BlackBerry UEM. To activate your device you need some or all of the following information: • Your work email address: %UserEmailAddress% • Server name: %ActivationURL% • Activation username: %ActivationUserName% • Your device activation password: Your activation password will be delivered in a separate email. You can watch a video on how to activate your device here: https://docs.blackberry.com/en/endpoint-management/blackberry-uem-activation-videos For Android devices: If you are using an Android device, you must install the BlackBerry UEM Client from Google Play. For iOS devices: If you are using an iOS device, you must install the BlackBerry UEM Client from the App Store. For iOS devices, open Safari and go to workspace://apps to install apps that your administrator has assigned to you. If available, you can also tap Work Apps on your device. For macOS devices: If you are using a macOS device, you must activate your device using BlackBerry UEM Self-Service. For devices running Windows 10 or later: You will need the following information to activate your device: • Server name: %ClientlessActivationURL% • Certificate server URL: %RsaRootCaCertUrl% • You must install the RSA certificate. Type the Certificate server URL in the address bar of the browser on your device. Follow the instructions and install the certificate into the Trusted Root Certification Authorities folder. • On your device, go to Settings > Accounts > Access work or school and tap Enroll only in device management. To manage your devices You can manage your own device with BlackBerry UEM Self-Service at %UserSelfServicePortalURL%. To log in, use the following username: BlackBerry UEM Self-Service username: %UserName% Your BlackBerry UEM Self-Service password may have been delivered in a separate email. Welcome to BlackBerry UEM!

Name	Suggested text
Default activation email Second email	**Subject: Password to activate your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled your mobile device for BlackBerry UEM. To activate your device you need the following information: • Your device activation password: %ActivationPassword% • Your password will expire on %ActivationPasswordExpiry% Please follow the instructions in the "Activating your device on BlackBerry UEM" email to activate your BlackBerry 10, iOS, Android, or Windows device on BlackBerry UEM. If you have any questions, contact your administrator. Welcome to BlackBerry UEM!
Default compliance email	**Subject: Notification of noncompliant device** Your device is not compliant with your organization's policies. If this condition persists your administrator might limit access to the organization's data from your device, delete the organization's data on your device, or delete all content and settings from your device.

Name	Suggested text
Default Work space only (Android work profiles) activation email First email	**Subject: Activating your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled your Android device (6.0 and later) for BlackBerry UEM. To activate your device, you need the following information: • Activation username: %ActivationUserName% • Your device activation password: Your activation password will be delivered in a separate email. To activate your device, perform the following actions: 1. If you do not see the device setup Welcome screen, reset your device to the factory default settings. 2. During the device setup, in the Add your account screen enter afw#blackberry. Wait while the device updates some important system applications and downloads the UEM Client. 3. In the BlackBerry UEM Client, follow the instructions on the screen to activate your device. You can manage your own device with BlackBerry UEM Self-Service at %UserSelfServicePortalURL%. To log in, use the following username: BlackBerry UEM Self-Service username: %UserName% Your BlackBerry UEM Self-Service password may have been delivered in a separate email. If you have not received it, contact your administrator. Please keep this information for your records. If you have any questions, contact your administrator. Welcome to BlackBerry UEM!
Default Work space only (Android work profiles) activation email Second email	**Subject: Password to activate your device on BlackBerry UEM** %UserDisplayName%, Your administrator has enabled your Android device for BlackBerry UEM. To activate your device you need the following information: • Your device activation password: %ActivationPassword% • Your password will expire on %ActivationPasswordExpiry% Please follow the instructions in the "Activating your device on BlackBerry UEM" email to activate your device on BlackBerry UEM. If you have any questions, contact your administrator. Welcome toBlackBerry UEM!
BlackBerry UEM event notification email	**Subject: BlackBerry UEM event notification** The following event occurred: %AllEventVariables%

Name	Suggested text
Device activated notification	**Subject: Device activated on BlackBerry UEM** %UserDisplayName%, Your device has been activated on BlackBerry UEM. Device information Model: %DeviceModel% Serial Number: %SerialNumber% IMEI: %DeviceIMEI% If you did not activate this device, contact your administrator. **Subject: BlackBerry Dynamics device activated on BlackBerry UEM** %UserDisplayName%, Your BlackBerry Dynamics device has been activated on BlackBerry UEM. If you did not activate this device, contact your administrator.
Self-service login notification	**Subject: Self-service login notification** %UserDisplayName%, You have logged in to BlackBerry UEM Self-Service. IP address: %IPAddress% Time: %Timestamp% If you did not log in, contact your administrator.

Create an activation email template

1. On the menu bar, click **Settings > General settings**.
2. Click **Templates**.
3. Click ✛. Select **Device activation**.
4. In the **Name** field, type a name to identify this template.
5. In the **Subject** field, edit the text to customize the subject line of the first activation email.
6. In the **Message** field, type the body text of the activation email.
   - Use the HTML editor to select the font format and to insert images (for example, a corporate logo).
   - Insert variables in the text to personalize the message (for example, you can use the variable %UserDisplayName% to insert the recipient's name). For a list of available variables, see Default variables.
   - To see sample text, click **Suggested text**.
7. If you want users to activate their device using a QR Code instead of an activation password, select the **Append a QR code to email message for iOS and Android device activation** check box.
8. To send the activation password or QR Code separately from the activation instructions, select **Send two separate activation emails - first for complete instructions, second for password**. If you decide to send only one activation email, make sure that you include the activation password, the activation password variable, or the QR Code in the first email.

9. In the **Subject** field, type a subject line for the second activation email.
10. Customize the body text of the second activation email template and include the activation password, the activation password variable, or select the **Append a QR code to email message** check box.
11. Click **Save**.

For more information on device activation, see Activating devices.

Create a template for compliance email notifications

You can create multiple email templates, customize them to apply to specific device types or groups of users, and assign an appropriate template to each user account. When a user's device does not comply with a compliance profile, BlackBerry UEM can send a personalized email message based on the assigned template. BlackBerry UEM includes a default compliance violation email template that can be edited, but not deleted. If you don't assign a different template to a user account, BlackBerry UEM uses the default template.

1. On the menu bar, click **Settings > General settings**.
2. Click **Templates**.
3. Click ╈. Select **Compliance violation**.
4. In the **Name** field, type a name to identify this template.
5. In the **Subject** field, type a subject for the email message.
6. In the **Message** field, type the body text of the compliance email message. Use the HTML editor to select the font format and to insert images, for example a corporate logo. Insert variables in the text to personalize the message, for example you can use the variable %UserDisplayName% to insert the recipient's name. For a list of available variables, see Default variables.
7. Click **Save**.

Create an event notification email template

You can create event notification email templates to associate with event notifications.

1. On the menu bar, click **Settings > General settings**.
2. Click **Templates**.
3. Click ╈ and select **Event notification**.
4. In the **Name** field, type a name to identify this template.
5. In the **Subject** field, complete one of the following tasks:
   - Clear the **Append event type to the email subject** check box and type a subject.
   - Leave the **Append event type to the email subject** check box selected, and type additional text in the subject field.
   - Leave the **Append event type to the email subject** check box selected.
6. In the **Message** field, type the body text of the event notification email.
   - Use the HTML editor to select the font format and to insert images (for example, your organization's logo).
   - To see sample text, click **Suggested text**.
7. Click **Save**.

For more information on event notifications, see Creating event notifications.

Legal notice

©2020 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. 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 on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

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

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

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

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

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

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

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

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

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada