Security Note

BlackBerry 10 Devices

Published: 2016-12-22
SWD-20161212134708655

Contents

Document revision history

1

Date	Description
22 December 2016	Updated BES12 product names to BlackBerry UEM product names throughout the document.
4 October 2016	Updated the Data wipe topic to provide additional details about what happens when a work data wipe occurs.

Introduction

BlackBerry 10 devices provide extensive security features, including the following:

Feature	Description
BlackBerry manufacturing security model	BlackBerry's end-to-end manufacturing model ensures device hardware integrity and that only genuine BlackBerry devices connect to the BlackBerry Infrastructure.
BlackBerry 10 OS protection	The OS is tamper-resistant, resilient, and secure, and includes many security features that protect data, apps, and resources on devices.
Protection of data at rest	Data at rest on devices is protected using security features such as encryption, passwords, and data wiping.
Protection of data in transit	Data in transit is protected using security features such as VPN encryption, certificates, and secure email.
Cryptography	Devices support various types of cryptographic algorithms, codes, protocols, and APIs.
App testing and approval for the BlackBerry World storefront	All apps are tested to make sure that they don't interfere with the core functionality of devices before they're approved by BlackBerry and made available in the BlackBerry World storefront. BlackBerry can remove any apps from BlackBerry World that are identified as potentially malicious or don't follow the BlackBerry World Vendor Agreement.

Secure device management

BlackBerry 10 devices support the following BlackBerry UEM enterprise management options:

Activation type	Description
Work and personal - Corporate	This activation type creates a BlackBerry Balance device. This activation type provides control of work data on devices, while making sure that there's privacy for personal data. When a device is activated, a separate work space is created on the device and the user must create a password to access the work space. Work data is protected using encryption and password authentication. You can control the work space on the device using IT administration commands and IT policy rules, but you can't control any aspects of the personal space on the device.
Work and personal - Regulated	This activation type creates a regulated BlackBerry Balance device. This activation type provides control of both work and personal data. When a device is activated, a separate work space is created on the device and the user must create a password to access the work space. Work data is protected using encryption and password authentication. You can control both the work space and the personal space on the device using IT administration commands and IT policy rules.
Work space only	This activation type creates a work space only device. This activation type provides full control of devices and doesn't provide a separate space for personal data. When a device is activated, the personal space is removed, a work space is installed, and the user must create a password to access the device. Work data is protected using encryption and password authentication. You can control the device using IT administration commands and IT policy rules.

Securing BlackBerry Balance devices

You can activate BlackBerry 10 devices using the "Work and personal - Corporate" activation type to provide users with BlackBerry Balance devices. These devices have a personal space and a work space and you have control of only the work space. Your organization can use BlackBerry Balance technology to permit users to use devices for both work and personal use. For example, your organization might want to permit users to activate their personal devices on BlackBerry UEM or permit users to use devices that your organization provides for personal use.

BlackBerry UEM security features and BlackBerry Balance can control how devices protect your organization's content and resources (data, apps, and network connections) and allow devices to treat work apps and data differently from personal apps and data. These features and options have the following benefits:

- Permit your organization to control access to work apps and data on devices
- Help prevent your organization's data from being compromised
- Provide a unified experience for users when they access personal data and work data within some core apps
- Permit you to manage and monitor apps that your organization wants to make available as work apps
- Permit you to delete your organization's apps and data from personal devices when users are no longer a part of your organization
- Permit you to control network connections for work and personal apps

Securing regulated BlackBerry Balance devices

You can activate BlackBerry 10 devices using the "Work and personal - Regulated" activation type to provide users with regulated BlackBerry Balance devices. These devices have a personal space and a work space and you have control of both spaces. Your organization can use BlackBerry Balance technology to permit users to use devices for both work and personal use and still give your organization control over device features.

BlackBerry UEM security features and regulated BlackBerry Balance can control how devices protect your organization's content and resources (data, apps, and network connections) and allow devices to treat your organization's data and apps differently from personal data and apps.

Regulated BlackBerry Balance devices treat work and personal data in the same way as BlackBerry Balance devices. Everything you can do to manage BlackBerry Balance devices, including using IT policy rules, you can do with regulated BlackBerry Balance devices. However, regulated BlackBerry Balance devices also give you additional management options, including:

- Disable device features, even when users are in the personal space
- Prevent users from having personal accounts on the device
- Block communication paths for phone calls, SMS, and BBM
- Block communication paths such as Wi-Fi, Bluetooth, and NFC
- Use advanced data at rest protection for work space data

Users with regulated BlackBerry Balance devices should be aware that your organization can audit personal data on their devices. When a device is activated using the "Work and personal - Regulated" activation type, the user is presented with a general disclaimer stating that the device is managed by your organization and the user must accept the disclaimer for activation to continue. You can configure an additional notice that outlines the terms and conditions that users must follow to comply with your organization's security requirements. For regulated BlackBerry Balance devices that are running BlackBerry 10 OS version 10.3.1 and later, you can specify in the IT policy whether a device displays the organization notice each time a user restarts the device.

Securing work space only devices

You can activate BlackBerry 10 devices using the "Work space only" activation type to provide users with work space only devices. These devices have only one space, which is considered a work space and is secure. All data and apps on these devices are classified as work resources. You can activate work space only devices if users will use devices almost exclusively for work purposes or if you have particularly sensitive positions in your organization that require full management of devices.

With this activation option, you have full control over devices and you can:

- Approve all apps and services on devices
- Disable device features such as the camera or GPS
- Block communication paths such as Wi-Fi or Bluetooth
- Control what apps users can download
- Prevent access to personal email messaging services
- Use advanced data at rest protection for work space data

Password protection on work space only devices isn't optional. To secure work data on these devices, users must set a device password during activation.

Users with work space only devices should be aware that your organization can audit all data on their devices, even if they're using their devices for personal use. When a device is activated using the "Work space only" activation type, the user is presented with a general disclaimer stating that the device is completely managed by your organization and the user must accept the disclaimer for activation to continue. You can configure an additional notice that outlines the terms and conditions that users must follow to comply with your organization's security requirements. For work space only devices that are running BlackBerry 10 OS version 10.3.1 and later, you can specify in the IT policy whether a device displays the organization notice each time a user restarts the device.

If a device has a personal space or a work space before you activate it, it's wiped during the activation process and any data, apps, or network connections that the device used before activation are removed.

Controlling access to content

BlackBerry Balance and regulated BlackBerry Balance devices control what users can do with work and personal content as follows:

- Devices don't permit users to move files from the personal space to the work space or from the work space to the personal space.
- Devices don't permit users to cut, copy, or paste text from work space apps to personal space apps. Devices do permit users to cut, copy, or paste text from personal space apps to work space apps. Devices store data that users copy from work space apps in the work space only and data that users copy from personal space apps in the personal space only.

- Apps that are available in the work and personal spaces in a unified view can attach personal files to the work portion of the app. For example, users can attach personal files to work email messages. Devices use read-only versions of these files and don't transfer or copy those files from the personal file system to the work file system.

By default, work apps can access shared files that are located in the personal space if a user permits it. When a user installs a work app, the device displays a message that provides the user with the option to allow or deny the app’s request to access shared files or content. If you want to prevent work apps from accessing shared personal files, make sure the "Allow work apps to access shared files or content in the personal space" IT policy rule isn't selected. This will prevent work apps from accessing shared files or content that is located in the personal space, regardless of the user settings on the device. It will also prevent users from attaching personal files to messages that they send from a work account and from sharing personal files or content with work apps using the "Share" option.

By default, all apps in the personal space can access required data for work contacts. Users can also use the "Copy to" and "Save to" options for work contacts in the Contacts app.

You can change IT policy rule settings to:

- Prevent all personal apps from accessing data for work contacts at all times by setting the "Allow personal apps to access work contacts" IT policy rule to None
- Allow only the following personal apps developed by BlackBerry to access data for work contacts by setting the "Allow personal apps to access work contacts" IT policy rule to "Only BlackBerry apps": Phone, BBM (including BBM Video and BBM Voice), Text Messages, Smart Tags, and visual voice mail.
- Prevent users from sharing work screens with other BBM Video chat participants during a BBM Video chat. If you don't allow users to share work screens during a BBM Video chat, the device locks the work space when a user shares the screen during a BBM Video chat and the user can't unlock the work space until the screen sharing part of the BBM Video chat is complete.

Controlling device features

BlackBerry 10 devices support an extensive list of IT policy rules that control device features. Depending on the activation type, you can enable or disable a wide range of device features, such as the media card, camera, roaming, and location services.

Controlling software updates

By default, users can update their device software by downloading BlackBerry 10 OS updates over the wireless network. Users can download all software updates that BlackBerry or a service provider makes available. On regulated BlackBerry Balance and work space only devices, you can use an IT policy rule to limit users to downloading only security-related software updates over the wireless network that BlackBerry or the wireless service provider makes available, or prevent users from downloading any software updates over the wireless network.

Controlling device log synchronization with BlackBerry UEM

By default, regulated BlackBerry Balance and work space only devices don't synchronize log files for BBM, Phone, SMS, MMS, PIN, and BBM Video chat features with BlackBerry UEM. If you need to log one or more of these communication paths, you can use IT policy rules to configure devices to generate log files.

When you log these communication paths for regulated BlackBerry Balance devices, log files contain both work and personal data.

Controlling connections from devices

By default, regulated BlackBerry Balance devices and work space only devices can make various connections. You can use IT policy rules to control connections such as Bluetooth and Wi-Fi. If you disallow any of these connections on regulated BlackBerry Balance devices, they're disallowed for both the personal and work spaces.

Using Bluetooth wireless technology, users can open wireless connections between a BlackBerry Balance or regulated BlackBerry Balance device and other Bluetooth enabled devices. Users must request a pairing with another Bluetooth device and use a passkey to complete the pairing. Devices prompt users each time another Bluetooth enabled device tries to connect to their devices.

By default, regulated BlackBerry Balance and work space only devices can make Bluetooth connections. You can use IT policy rules to control Bluetooth connections and control some of the criteria that a device must use when it pairs with another device.

By default, users can transfer files, contacts, and messages from the work space on devices to Bluetooth enabled devices that they have successfully paired with. You can use IT policy rules to prevent users from transferring work data, such as files, contacts, and messages, to other Bluetooth enabled devices. You can also prevent users with regulated BlackBerry Balance devices from making any Bluetooth connections.

Data that BlackBerry Balance and regulated BlackBerry Balance devices receive from other devices using NFC is generally classified as personal data. However, if a work app supports a specific NFC tag format that is unique to the work app, any data that a device receives with that NFC tag is classified as work data.

By default, devices can use NFC to send work data to other NFC-enabled devices. You can use an IT policy rule to allow or prevent users from sharing work data in a file format (for example, pictures or documents) using NFC. Regardless of how IT policy rules are set, devices can use NFC to send certain MIME or URI data types, such as web addresses and phone numbers to other NFC-enabled devices. You can also use an IT policy rule to prevent users from sending work data to another NFC-enabled device using NFC. You can also prevent users with regulated BlackBerry Balance devices from making any NFC connections.

Ensuring device compliance

The BlackBerry 10 OS performs checks on the integrity of the kernel and the file system. If the BlackBerry 10 OS detects a problem, it alerts BlackBerry UEM. You can specify integrity alert settings in the compliance profile to control the actions that BlackBerry UEM would take if one of the integrity checks fails.

Possible actions include quarantining the device from access to work resources, notifying the user by email or device notification, wiping work data, and wiping the entire device.

Hardware root of trust

4

BlackBerry ensures the integrity of device hardware and makes sure that counterfeit devices can't connect to the BlackBerry Infrastructure and use BlackBerry services.

From the beginning of the product lifecycle, BlackBerry integrates security into every major component of the product design of devices. BlackBerry has enhanced its end-to-end manufacturing model to securely connect the supply chain, BlackBerry manufacturing partners, the BlackBerry Infrastructure, and BlackBerry devices, which allows BlackBerry to build trusted devices anywhere in the world.

The BlackBerry manufacturing security model prevents counterfeit devices from impersonating authentic devices and makes sure that only genuine BlackBerry devices can connect to the BlackBerry Infrastructure. The BlackBerry Infrastructure uses device authentication to cryptographically prove the identity of the device that attempts to register with it. The BlackBerry manufacturing systems use the device’s hardware-based ECC 521-bit key pair to track, verify, and provision each device as it goes through the manufacturing process. Only devices that complete the verification and provisioning processes can register with the BlackBerry Infrastructure.

The BlackBerry 10 OS

The BlackBerry 10 OS is the microkernel operating system of the BlackBerry 10 device. Microkernel operating systems implement the minimum amount of software in the kernel and run other processes in the user space that is outside of the kernel.

Microkernel operating systems are designed to contain less code in the kernel than other operating systems. The reduced amount of code helps the kernel to avoid the vulnerabilities that are associated with complex code and to make verification easier. Verification is the process of evaluating a system for programming errors. Many of the processes that run in the kernel in a conventional operating system run in the user space of the OS.

The OS is tamper-resistant. The kernel performs an integrity test when the OS starts and if the integrity test detects damage to the kernel, the device doesn't start.

The OS is resilient. The kernel isolates a process in its user space if it stops responding and restarts the process without negatively affecting other processes. In addition, the kernel uses adaptive partitioning to prevent apps from interfering with or reading the memory used by another app.

The OS is secure. The kernel validates requests for resources and an authorization manager controls how apps access the capabilities of the device, such as access to the camera, contacts, and device identifying information.

The file system

The BlackBerry 10 device file system runs outside of the kernel and keeps work data secure and separate from personal data. The file system is divided into the following areas:

- Base file system
- Work file system
- Personal file system (on devices with a personal space)

The base file system is read-only and contains system files. Because the base file system is read-only, the OS can check the integrity of the base file system and mitigate any damage done by an attacker who changed the file system.

The work file system contains work apps and data. The device encrypts the files stored in the work space.

On devices with a personal space, the personal file system contains personal apps and data. Apps that a user installed on the device from the BlackBerry World storefront are located in the personal file system. The device can encrypt the files stored in the personal file system.

Sandboxing

The BlackBerry 10 OS uses a security mechanism called sandboxing to separate and restrict the capabilities and permissions of apps that run on the device. Each app process runs in its own sandbox, which is a virtual container that consists of the memory and the part of the file system that the app process has access to at a specific time.

Each sandbox is associated with both the app and the space that it's used in. For example, an app can have one sandbox in the personal space and another sandbox in the work space; each sandbox is isolated from the other one.

The OS evaluates the requests that an app’s process makes for memory outside of its sandbox. If a process tries to access memory outside of its sandbox without approval from the OS, the OS ends the process, reclaims all of the memory that the process is using, and restarts the process without negatively affecting other processes.

When the OS is installed, it assigns a unique group ID to each app. Two apps can't share the same group ID, and the OS doesn't reuse group IDs after apps are removed. An app’s group ID remains the same when the app is upgraded.

By default, each app stores its data in its own sandbox. The OS prevents apps from accessing file system locations that aren't associated with the app’s group ID.

An app can also store and access data in a shared directory, which is a sandbox that is available to any app that has access to it. When an app that wants to store or access files in the shared directory starts for the first time, the app prompts the user to allow access.

Device resources

The BlackBerry 10 OS manages the device's resources so that an app can't take resources from another app. The OS uses adaptive partitioning to reallocate unused resources to apps during typical operating conditions and enhance the availability of the resources to specific apps during peak operating conditions.

App permissions

The authorization manager is the part of the BlackBerry 10 OS that evaluates requests from apps to access the capabilities of the device. Capabilities include taking a photograph and recording audio. The OS invokes the authorization manager when an app starts to set the permissions for the capabilities that the app uses. When an app starts, it might prompt the user to allow access to a capability. The authorization manager can store a permission that the user grants and apply the permission the next time that the app starts.

Verifying software

Verifying the boot loader code

The BlackBerry 10 device uses an authentication method that verifies that the boot loader code is permitted to run on the device. The manufacturing process installs the boot loader into the flash memory of the device and a public signing key into the processor of the device. The BlackBerry signing authority system uses a private key to sign the boot loader code. The device stores information that it can use to verify the digital signature of the boot loader code.

When a user turns on a device, the processor runs internal ROM code that reads the boot loader from flash memory and verifies the digital signature of the boot loader code using the stored public key. If the verification process completes, the boot loader is permitted to run on the device. If the verification process can't complete, the device stops running.

Verifying the OS and file system

If the boot loader code is permitted to run on a BlackBerry 10 device, the boot loader code verifies the BlackBerry 10 OS. The OS is digitally signed using EC 521 with a series of private keys. The boot loader code uses the corresponding public keys to verify that the digital signature is correct. If it's correct, the boot loader code runs the OS.

Before the OS mounts the read-only base file system, it runs a validation program that generates a SHA-256 hash of the base file system content, including all metadata. The program compares the SHA-256 hash to a SHA-256 hash that is stored outside the base file system. This stored hash is digitally signed using EC 521 with a series of private keys. If the hashes match, the validation program uses the corresponding public keys to verify the signature and the integrity of the stored hash.

Verifying apps and software upgrades

Once the base file system is validated, the BlackBerry 10 OS verifies existing apps by reading an app's XML file and verifying the assets of the app against the cryptographically signed hashes contained in the XML manifest.

Each software upgrade and app for the BlackBerry 10 device is packaged in the BlackBerry Archive (BAR) format. This format includes SHA-2 hashes of each archived file, and an ECC signature that covers the list of hashes. When a user installs a software upgrade or app, the installation program verifies that the hashes and the digital signature are correct.

The digital signatures for a BAR file also indicate the author of the software upgrade or app. The user can then decide whether to install the software based on its author.

Because the device can verify the integrity of a BAR file, the device can download BAR files over an HTTP connection, which makes the download process faster than over a more secure connection.

Preventing memory corruption

BlackBerry 10 devices prevent exploitation of memory corruption in a number of different ways, including the security mechanisms listed in the following table:

Security mechanism	Description
Non-executable stack and heap	The stack and heap areas of memory are marked as non-executable. This means that a process can't execute machine code in these areas of the memory, which makes it more difficult for an attacker to exploit potential buffer overflows.
Stack cookies	Stack cookies are a form of buffer overflow protection that helps prevent attackers from executing arbitrary code.
Robust heap implementations	The heap implementation includes a defense mechanism against the deliberate corruption of the heap area of memory. The mechanism is designed to detect or mitigate the overwriting of in-band heap data structures so that a program can fail in a secure manner. The mechanism helps prevent attackers from executing arbitrary code via heap corruption.
Address space layout randomization (ASLR)	By default, the memory positions of all areas of a program are randomly arranged in the address space of a process. This mechanism makes it more difficult for an attacker to perform an attack that involves predicting target addresses to execute arbitrary code.
Compiler-level source fortification	The compiler GCC uses the FORTIFY_SOURCE option to replace non-secure code constructs where possible. For example, it might replace an unbounded memory copy with its bounded equivalent.
Guard pages	If a process attempts to access a memory page, the guard page raises a one-time exception and causes the process to fail. These guard pages are placed strategically between memory used for different purposes, such as the standard program heap and the object heap. This mechanism helps prevent an attacker from causing a heap buffer overflow and changing the behavior of a process or executing arbitrary code with the permissions of the compromised process.

Data at rest

6

BlackBerry 10 devices support various methods to keep data private and secure while it's stored on the device.

Encryption

Encryption is used to protect data that's stored on BlackBerry 10 devices. Only the contents of files are encrypted; the files themselves and directory names aren't encrypted.

Type of data	Description
Work space data	If your devices are managed by BlackBerry UEM, they have a work space. Devices encrypt all data stored in the work space. Work space encryption isn't optional.
Personal space data	Devices with a personal space can protect personal data by encrypting the files stored in the personal space. Personal space encryption is optional. Users can turn on personal data encryption using device settings. If your devices are managed by BlackBerry UEM, an administrator can use BlackBerry UEM to turn on personal space encryption on a device.
Media card data	Devices can protect media card data by encrypting the files stored on media cards. Media card encryption is optional. Users can turn on media card encryption using device settings. The media card is disabled if another device encrypted the data on it. If your devices are managed by BlackBerry UEM: • An administrator can turn on media card encryption • By default, devices with a personal space allow users to store only personal data on media cards and that data is stored in an unencrypted format. • On work space only devices, because users can store work data on media cards in an unencrypted format by default, it's highly recommended to use media card encryption. • By default, work space only devices allow users to save data to media cards, and that data is stored in an unencrypted format. • On regulated BlackBerry Balance and work space only devices, media card encryption is only allowed if an IT policy rule is selected.

How devices protect work data

Work space encryption for BlackBerry 10 devices encrypts data stored in the work file system using XTS-AES-256. Since work space only devices only have a work space, they encrypt all data using XTS-AES-256.

A device randomly generates an encryption key to encrypt the contents of a file. The file encryption keys are protected by a hierarchical system of encryption keys as follows:

- The device encrypts the file encryption key with the work domain key and stores the encrypted file encryption key as a metadata attribute of the file.
- The work domain key is a randomly generated key that's stored in the file system metadata and is encrypted using the work master key.
- The work master key is also randomly generated. The work master key is stored in NVRAM on the device and is encrypted with the system master key.
- The system master key is stored in the replay protected memory block on the device.
- The replay protected memory block is encrypted with a key that's embedded in the processor when the processor is manufactured.

The file encryption keys, the work domain key, the work master key, and the system master key are generated using the BlackBerry OS Cryptographic Kernel, which received FIPS 140-2 certification for the BlackBerry 10 OS.

How devices protect personal data

Personal space encryption for BlackBerry 10 devices encrypts files stored in the personal file system using XTS-AES-256. A device randomly generates an encryption key to encrypt the contents of a file. The file encryption keys are protected by a hierarchical system of encryption keys, as follows:

- The device encrypts the file encryption key with the personal domain key and stores the encrypted file encryption key as a metadata attribute of the file.
- The personal domain key is a randomly generated key that's stored in the file system metadata and is encrypted using the personal master key.
- The personal master key is also randomly generated. The personal master key is stored in NVRAM on the device and is encrypted with the system master key.
- The system master key is stored in the replay protected memory block on the device.
- The replay protected memory block is encrypted with a key that's embedded in the processor when the processor is manufactured.

The file encryption keys, the personal domain key, the personal master key, and the system master key are generated using the BlackBerry OS Cryptographic Kernel, which received FIPS 140-2 certification for the BlackBerry 10 OS.

How devices protect media card data

Media card encryption for BlackBerry 10 devices encrypts files stored on the media card. A device randomly generates an encryption key to encrypt the contents of files on the media card. The encryption key is protected as follows:

- The device concatenates the personal domain key and a randomly generated key and hashes them to generate a media card key. If the device is a work space only device or if personal space data encryption has not been turned on, the device first generates a personal domain key.
- The device encrypts the file encryption key with the media card key and stores the encrypted file encryption key as a metadata attribute of the file.
- A hash of the media card key is stored in the replay protected memory block on the device to allow for the media card key to be verified.
- The replay protected memory block is encrypted with a key that is embedded in the processor when the processor is manufactured.

The media card encryption key is generated using the BlackBerry OS Cryptographic Kernel, which received FIPS 140-2 certification for the BlackBerry 10 OS.

Advanced data at rest protection for BlackBerry 10 devices

Advanced data at rest protection is a data at rest encryption model that you can use to protect work space data on locked regulated BlackBerry Balance and work space only devices running BlackBerry 10 OS version 10.3.1 and later. It helps to secure sensitive data by restricting access to certain files in the device's work space when the work space is locked. When the work space is locked, only apps that have been specifically developed to support advanced data at rest protection are allowed to continue to run in the work space, and they're restricted to accessing only certain parts of the work space file system.

In addition to restricting access to sensitive data when the work space is locked, advanced data at rest protection also encrypts data that the device receives when the work space is locked. Both the data that's stored in the work space on devices and work data that locked devices receive are encrypted. The domain keys for encrypting work space files are also encrypted. The files are encrypted using keys that are tied to information that's not stored on the device, such as a user's work space password or smart card.

Advanced data at rest protection provides different domains to store the following classifications of data:

Domain name	Description
Lock	This domain stores sensitive data. The data in this domain is encrypted and can only be accessed while the work space is unlocked. The domain key can only be decrypted after the user unlocks the work space.
Operational	This domain stores sensitive data that must be available when the work space is locked or unlocked. After the device starts for the first time or restarts, the data isn't available until the user unlocks the work space. The data is then available until the device is turned off or

Domain name	Description
	restarts. The domain key can be decrypted only after the user unlocks the work space for the first time after the device starts up.
Startup	This domain stores data that must be encrypted but must be available during device startup without requiring the user to unlock the work space first. Any data that's required for device startup or must be available before the user unlocks the work space must be stored in this domain. The domain key can be retrieved and decrypted without requiring the user to unlock the work space first.

When the "Advanced data at rest protection timeout" IT policy rule is set to a value greater than 0, the data in the lock domain can be accessed normally until advanced data at rest protection is turned on.

You can use advanced data at rest protection on regulated BlackBerry Balance and work space only devices. On regulated BlackBerry Balance devices, advanced data at rest protection doesn't affect personal apps. They continue to run and can access the device’s personal file system normally.

Managing advanced data at rest protection

You can use an IT policy rule to turn on advanced data at rest protection on devices. Users can’t turn advanced data at rest protection on or off on their devices.

You might not want advanced data at rest protection to be activated as soon as the work space locks and would prefer that there be a delay between the work space locking and advanced data at rest protection being activated. If so, you can use an IT policy rule to set a delay of up to 24 hours. When advanced data at rest protection isn't activated, the data in the lock domain can be accessed normally.

You can require that two-factor authentication be used to protect the encryption keys for advanced data at rest protection using an IT policy rule. Two-factor authentication protects the encryption keys for advanced data at rest protection with both a private key that’s stored on a smart card and the work space password.

You can choose where Wi-Fi and VPN profiles are stored in the work space on devices that use advanced data at rest protection. Using the "Data security level” profile setting in Wi-Fi and VPN profiles, you can choose to make Wi-Fi and VPN profiles always available, available after authentication, or available only when the work space is unlocked. If you choose to make the profile always available, it’s stored in the startup domain and is available when the work space is locked. If you choose to make the profile available after authentication, it’s stored in the operational domain and is available after the work space is unlocked once until the device restarts. If you choose to make the profile available only when the work space is unlocked, it’s stored in the lock domain and can be used for Wi-Fi or VPN connections only when the work space is unlocked.

Passwords

Passwords protect access to your users' information and your organization's information stored on BlackBerry 10 devices. Users with BlackBerry Balance devices can have both device and work space passwords, and any users who employ personal data encryption must have a device password. The following password-related security features protect information stored on devices:

Item	Description
Secure password generation and storage	Devices securely generate and store device and work space passwords.
Software tools require authentication	Software programs or tools, such as BlackBerry Link, can't access a password-protected device without the device owner allowing access by typing in their device password. This prevents tools from bypassing the device security.
Incorrect password attempts	If the device is password-protected, a user has a limited number of attempts to enter the correct password before the device performs a data wipe. The maximum number of password attempts is determined by device settings or BlackBerry UEM (if the device is managed by BlackBerry UEM).

If your devices are managed by BlackBerry UEM, an administrator can enforce password protection and control password requirements, such as complexity and length, to ensure that a device meets the requirements of your organization. BlackBerry UEM also provides management options for a lost device, including the ability to lock it remotely. An administrator can do this, for example, if a device is lost or if a user forgets their password.

Passwords for BlackBerry 10 devices

BlackBerry 10 devices use the same password rules for the device and the workspace. Passwords are not optional on work space only devices. Users must set a password and, because there is only a work space on these devices, password enforcement and options apply to the entire device.

For BlackBerry Balance and regulated BlackBerry Balance devices, the “Password required for work space” IT policy rule specifies whether the work space must have a password. When this rule is selected, the Work Password (in the “BlackBerry Balance” settings on the device) is used as the work space password.

When the “Password required for work space” IT policy rule is selected, you can also require that users set a full device password using the “Require full device password” rule. If you do this, for devices running BlackBerry 10 OS version 10.3.1 or later, you can then use the “Define work space and device password behavior” IT policy rule to specify whether the work space password and device password need to be the same or different, or you can allow the user to choose. If you allow users to choose, a user can use their work space password as their device password using device settings. If the work space and device passwords are the same, the work space password is used as the password for the entire device and the IT policy rules in the “Password” rule group apply to the password for the entire device. When a user unlocks the device, the work space is unlocked at the same time. Users can choose to lock the work space manually when they’re using the personal space on devices.

If you don’t require users to have a work space password, you won’t be able to require a full device password, define work space and device password behavior, or enforce additional password requirements on devices.

Users can configure device password settings using device settings. If a user turns on personal data encryption using device settings, the user must set a device password. Devices permit users to make password settings more restrictive, but never less restrictive, than the password rules that you specify. If the "Minimum password complexity" IT policy rule is set to "No restriction", users can turn on a simple password option to set a numeric work space or device password instead of an alphanumeric password.

Changing BlackBerry 10 device passwords

You can use BlackBerry UEM to send the "Specify device password, lock, and set message" IT administration command to a device to change the device password.

This command has different results on devices, depending on their passwords and settings. The following table lists the results the command has on devices given certain conditions:

Conditions	Results
The device has a work space password, but doesn't have a full device password.	• The command creates a full device password. • The work space password isn't affected. • The entire device locks and the new password is the device password.
The device has a work space password and a full device password, but the passwords aren't linked by you or the user.	• The command changes the full device password. • The work space password isn't affected. • The entire device locks and the new password is the device password.
The device has a work space password, and you enforce the work space password as the full device password.	• The command changes the work space password. • The command changes the full device password. • The entire device locks, both passwords are synchronized, and the new password is the password for the entire device.
The device has a work space password, and the user sets the work space password as the full device password.	• The command changes the full device password. • The work space password isn't affected. • The entire device locks and the new password is the device password. • The passwords are unlinked.

You can also use the "Specify device password, lock, and set message" IT administration command to set a message that appears on a device's home screen. For example, it can display contact information that can be used to return the device to its owner.

If BlackBerry UEM can't connect to a device because the device is off or not connected to a network, the command is sent after the device connects to a network. The new password can be communicated to the user verbally when they locate the device. When the user unlocks the device, the device prompts the user to accept or reject the new password.

Changing BlackBerry 10 work space passwords

You can use BlackBerry UEM to send the “Specify work space password and lock” IT administration command to a device to change the work space password.

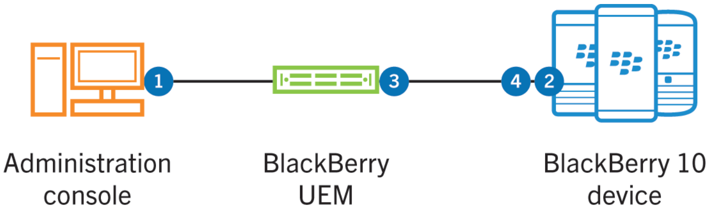
Work space only devices have a device password only. Although you can send this command to work space only devices, it achieves the same result as sending the “Specify device password, lock, and set message” IT administration command.

When you send the “Specify work space password and lock” IT administration command to BlackBerry Balance or regulated BlackBerry Balance devices, this command has different results on devices, depending on their passwords and settings. The following table lists the results the command has on devices given certain conditions:

Conditions	Results
The device doesn't have a work space password or a full device password.	• The command creates a work space password. • The work space locks and the new password is the work space password. • The device continues not to have a full device password.
The device has a work space password but doesn't have a full device password.	• The command changes the work space password. • The work space locks and the new password is the work space password. • The device continues not to have a full device password.
The device has a work space password and a full device password, but the passwords aren't linked by you or the user.	• The command changes the work space password. • The work space locks and the new password is the work space password. • The full device password isn't affected.
The device has a work space password, and you enforce the work space password as the full device password.	• The command changes the work space password. • The command changes the full device password. • The entire device locks, both passwords are synchronized, and the new password is the password for the entire device.
The device has a work space password, and the user sets the work space password as the full device password.	• The command changes the work space password. • The work space locks and the new password is the work space password. • The full device password isn't affected. • The passwords are unlinked.

If BlackBerry UEM can't connect to a device because the device is off or not connected to a network, the command is sent after the device connects to a network. The new password can be communicated to the user verbally when they locate the device. When the user unlocks the device, the device prompts the user to accept or reject the new password.

Data flow: When you change the work space password on a BlackBerry Balance or regulated BlackBerry Balance device



1. You send the "Specify work space password and lock" IT administration command to the device.
2. The device sends the encrypted intermediate key to BlackBerry UEM.
3. BlackBerry UEM uses the private key that is associated with the device to decrypt the intermediate key and sends the intermediate key back to the device.

   BlackBerry UEM stores a unique private key for each activated device.

4. The device performs the following actions:

   - Uses the intermediate key to rederive the work master key and decrypts the work domain key
   - Computes a SHA-512 hash of the new password and a random 64-bit salt and stores it on the device
   - Generates a new intermediate key
   - Uses the new intermediate key to generate a new work master key and uses it to encrypt the work domain key
   - Encrypts the new intermediate key using the public key that BlackBerry UEM associates with the device and stores the encrypted key on the device

   Because only BlackBerry UEM has the corresponding private key, only BlackBerry UEM can decrypt the encrypted intermediate key. The intermediate key is never persistently stored on the device in unencrypted form.

   The work space password is reset.

Data flow: When a user changes the work space password on a BlackBerry Balance or regulated BlackBerry Balance device

1. In the BlackBerry Balance settings on the device, the user types the current password and the new password.
2. The device authenticates the user by computing a SHA-512 hash of the current password and a stored 64-bit salt and compares the result with the stored hash of the current password.

   If the two hashes match, the work space unlocks and the password reset continues.

3. The device performs the following actions:

   - Computes a SHA-512 hash of the new password and a random 64-bit salt and stores it on the device

- Derives the current intermediate key
- Uses the current intermediate key to derive the current work master key and decrypts the work domain key
- Derives a new intermediate key
- Uses the new intermediate key to derive a new work master key that it uses to encrypt the work domain key
- Encrypts the new intermediate key using the public key that the BlackBerry UEM Core associates with the device and stores the encrypted key on the device

Because only the BlackBerry UEM Core has the corresponding unique private key for each device that is activated on the BlackBerry UEM Core, only the BlackBerry UEM Core can decrypt the encrypted intermediate key. The intermediate key isn't persistently stored on the device in unencrypted form.

The work space password is reset.

Controlling the security timeout

You can use the "Security timeout" IT policy rule to require that a BlackBerry 10 device lock the work space or the entire device after a certain period of inactivity as follows:

Device type	Description
• BlackBerry Balance • Regulated BlackBerry Balance	• On devices that have different work space and device passwords, the "Security timeout" IT policy rule controls the security timeout of the work space. • On devices that have a work space password that applies to the full device, the "Security timeout" IT policy rule controls the security timeout for the entire device.
Work space only	On work space only devices, because there is only a work space on these devices, the "Security timeout" IT policy rule controls the security timeout for the entire device.

Work apps (including apps that display work data and personal data in a unified view) follow the security timeout for the work space, and if there is no user activity in the work space within the time specified, the work space locks automatically even if the user is using personal apps (not including apps that display work and personal data in a unified view) at the time.

Certain apps, such as apps that display navigation information, slideshows, and videos, can extend the security timeout. By default, these apps can reset the security timer to prevent the device from locking after the specified period of user inactivity. If you want to prevent apps from doing this, make sure that the "Allow app security timer reset" IT policy rule isn't selected.

Data wipe

To protect your organization's data and user information on BlackBerry 10 devices, a user can delete their work data or all data on their device, including data on the media card.

If your devices are managed by BlackBerry UEM, an administrator can control when a device must wipe its data. For example, BlackBerry UEM allows you to require that a device automatically deletes device data, work data, or the work space after a specific time or under specific conditions.

Devices perform a full device wipe or work data wipe as follows:

- If the device is password-protected and the user types the device password incorrectly more times than device settings or BlackBerry UEM allow, the device deletes all user information and app data, and returns the device to factory defaults.
- If the work space is password-protected and the user types the work space password incorrectly more times than device settings or BlackBerry UEM allow, the device deletes all work space information and the work space is removed from the device.
- A user wipes the work data or all data on their device using device settings.
- A user uses BlackBerry Protect to delete all device data.

When a device wipe occurs, all data on the device is permanently deleted, including email accounts, downloaded apps, media files, documents, browser bookmarks, and settings. The BlackBerry 10 OS overwrites the device memory with zeros, and performs a secure TRIM operation on a section of device memory. The secure TRIM operation causes the flash memory chip to delete all of its memory.

When a work data wipe occurs, all work data on the device is permanently deleted. To perform the data wipe, the file system erases the domain key associated with each encryption domain in the work space. Erasing (zeroizing) the domain key of each encryption domain renders all data within the encryption domain cryptographically destroyed and marks the blocks that store each file as unused. All unused blocks in the work space are then block erased, which zeroizes them.

Wiping BlackBerry 10 devices

BlackBerry 10 devices delete all data in the device memory when any of the following events occur:

Event	Device type	Description
You send the “Delete all device data” IT administration command to a device.	• BlackBerry Balance • Regulated BlackBerry Balance • Work space only	You can use BlackBerry UEM to delete all data from devices using the "Delete all device data" IT administration command. You can send this command, for example, to a device to redistribute a previously used device to another user in your organization, or to a device that is lost and unlikely to be recovered. This command deletes all user information and app data that the device stores, including information in the work space, and information on the media card. It returns the device to factory defaults, and removes the device from BlackBerry UEM. After you submit this command, an option to remove the device from BlackBerry UEM is displayed. If the device can no

Event	Device type	Description
		longer connect to BlackBerry UEM, you can remove the device from BlackBerry UEM. If the device connects to BlackBerry UEM after you removed it, only the work data is removed from the device, including the work space, if applicable.
You send the “Delete only work data” IT administration command to a device.	Work space only	You can send the "Delete only work data" IT administration command to a work space only device to delete all data on it. Because these devices only have a work space, you can use either the "Delete all device data" or "Delete only work data" IT administration commands to wipe these devices. If BlackBerry UEM can’t connect to the device because it's off or not connected to a network, BlackBerry UEM sends the command after the device connects to a network.
More time elapses without the device connecting to your organization's network than the "Wipe the device without network connectivity" IT policy rule allows.	• Regulated BlackBerry Balance • Work space only	The device deletes all user information and app data that the device stores, including information in the work space, and returns the device to factory defaults. You can use this rule to make the device delete all data if it can't receive updates or commands.
A device sends an Integrity Alert to BlackBerry UEM and the Enforcement action is set to "Delete all device data".	• Regulated BlackBerry Balance • Work space only	If the BlackBerry 10 OS detects a problem with the integrity of a device, it alerts BlackBerry UEM. If an Integrity Alert occurs and the Enforcement action is set to "Delete all device data", the full device is wiped.
A device sends an Integrity Alert to BlackBerry UEM and the Enforcement action is set to "Delete only work data".	Work space only	If the BlackBerry 10 OS detects a problem with the integrity of a device, it alerts BlackBerry UEM. Because these devices only have a work space, if an Integrity Alert occurs and the Enforcement action is set to "Delete only work data," the full device is wiped.
A user types the device password incorrectly more times than the "Maximum password attempts" IT policy rule allows.	• BlackBerry Balance • Regulated BlackBerry Balance • Work space only	The device deletes all user information and app data that the device stores, including information in the work space, and returns the device to factory defaults. On BlackBerry Balance and regulated BlackBerry Balance devices, when a device has one password for the entire device, if a user types the device password incorrectly more times than the "Maximum password attempts" IT policy rule allows, the device is wiped.

Event	Device type	Description
		On work space only devices, if a user types the device password incorrectly more times than the "Maximum password attempts" IT policy rule allows, the full device is wiped.
A user uses the "Security Wipe" option on the device.	• BlackBerry Balance • Regulated BlackBerry Balance • Work space only	A user can delete all data on devices using the "Security Wipe" option in the "Security and Privacy" settings on the device.
A user uses BlackBerry Protect to delete all device data.	• BlackBerry Balance • Regulated BlackBerry Balance • Work space only	A user can also use BlackBerry Protect to wipe a device. Users can use BlackBerry Protect only if the "Allow BlackBerry Protect" IT policy rule is selected.

BlackBerry 10 devices delete all data from the work and personal spaces when a full device wipe occurs.

Work data wiped from BlackBerry 10 devices

When only the work data is wiped from a BlackBerry Balance or regulated BlackBerry Balance device, all personal data remains on the device. The following table lists examples of data that is removed when devices delete all data from the work space:

Item	Description
Work email messages	• Email messages that are sent to the user’s work email account and email messages that the user sends from the work email account • Draft email messages that the user creates using their work email account
Attachments	• Attachments that are sent to the user’s work email account and attachments that the user sends from the work email account • Attachments that the user saves to the work space
Calendar entries	Calendar entries that the user creates using their work calendar
Contacts	Contacts that BlackBerry UEM synchronizes with the user’s work email account

Item	Description
BlackBerry Remember	All tasks and memos that BlackBerry UEM synchronizes with the user's work email account
Browser	All work browser data
Files	Files that the user accessed and downloaded from your organization's network
IT policy	IT policy that is associated with your organization
Device transport key	References to the device transport key, which prevents the device from communicating with BlackBerry UEM
Work apps	Work apps that a user downloaded and installed on a device
Work app data	Work data that is associated with work apps on the device
Work Wi-Fi profiles	Work Wi-Fi profiles on the device
Work VPN profiles	Work VPN profiles on the device

App security

There are two main types of apps that BlackBerry 10 devices can run, depending on the BlackBerry UEM activation type. Personal apps are available in the personal space of BlackBerry Balance and regulated BlackBerry Balance devices. A work app can be either an internal app that an administrator sends to the device or a public app available from the public BlackBerry World storefront that an administrator has added to the allowed list. Work apps are available in the work space on devices.

Some apps can be useful for both personal and work purposes (for example, an IM app). In this situation, the user can install one instance of the app in the personal space using the public BlackBerry World, and an administrator can allow a separate instance of the app in the work space using BlackBerry World for Work. The instances are controlled independently, and changes to one instance have no effect on the other instance. For example, an administrator can restrict a personal IM app from adding work contacts, but the work IM app won't have that restriction.

To make sure that your organization maintains control of the work apps, an administrator needs to approve them before users can add them to the work space. An administrator can control what data apps can access and how they run. BlackBerry 10 devices use sandboxing, permissions, and allowed lists to protect both apps and data from attacks.

App vetting

You need to know how apps collect data, how they use and store it, and who can access it. Our app vetting processes and privacy notices play a key role in protecting your organization's data and user information, and securing users' identities.

To vet apps, we use BlackBerry Guardian, a program that combines automated and manual analysis with Trend Micro Mobile App Reputation Service. BlackBerry Guardian continuously monitors apps submitted to BlackBerry World to help protect devices from malware and privacy issues.

BlackBerry Guardian checks for apps that don't adequately inform users how they access and use personal data. Personal data can include highly sensitive information such as account details, unique device information, geolocation data, and user-generated content.

When BlackBerry Guardian identifies a suspicious app, we investigate and take whatever action is needed to protect you. We can deny the app or remove it from BlackBerry World and issue a privacy notice.

In BlackBerry 10 OS version 10.3.0 and later, BlackBerry Guardian automatically checks all Android apps that users install from sources other than BlackBerry World or the Amazon Appstore. If a suspicious app is detected, the user can choose to proceed or cancel the installation.

How BlackBerry Balance devices classify apps and data

BlackBerry Balance devices and regulated BlackBerry Balance devices can distinguish between data that's for work use and data that's for personal use. Devices classify data as work or personal data based on the source of the data, and these classifications determine how data is stored, protected, and handled on devices. Work data is any data that's managed by apps in the work space and personal data is any data that's managed by apps in the personal space. For example, if data comes from a work account, it's stored in the work space on the device, and if data comes from a personal account, it's stored in the personal space on the device. After devices classify data as work data or personal data, personal data can't be reclassified as work data and work data can't be reclassified as personal data.

All data and apps on work space only devices are classified as work resources, even when users use the devices for personal tasks, such as visiting personal web pages or receiving personal email messages.

The following table describes each app classification for devices with a personal space and lists examples of apps that belong to each app classification:

Description	Apps
Apps that are available only in the work space and display only work data	• BlackBerry World for Work • Any apps that users download from BlackBerry World for Work
Apps that are available only in the personal space and that display only personal data	• BBM, BBM Video, SMS text messaging, and visual voice mail (with access to work contacts except if prevented by the "Allow personal apps to access work contacts" IT policy rule) • BlackBerry World • Consumer Instant Messaging Apps

Description	Apps
	• Any apps that users download from BlackBerry World (including BlackBerry Runtime for Android apps)
Apps that are available in both the work and personal spaces and display work and personal data in a unified view These apps classify the data that they use as either work or personal data based on the source of the data and manage each type of data within the space that it belongs to. These apps manage work data within the restrictions of the work file system, policies, permissions, and rules to ensure that the data is secured inside the work space and no data is available to users when the work space is locked. These apps are strictly controlled and limited to core apps that are developed by BlackBerry only.	• BlackBerry Remember • BlackBerry Hub • Calendar • Contacts
Apps that have one instance in the work space and a separate instance in the personal space These app instances operate independently in both the work and personal spaces on devices. For example, the Documents To Go app that is located in the work space can manage only files that are located in the work space and the BlackBerry 10 OS prevents this app from interacting with files that are located in the personal space. Each instance of these apps is kept separate from the other, and each app operates under the rules and restrictions that apply to the space it's installed in. For example, the File Manager app displays only work files when a user opens the app in the work space and displays only personal files when the user opens the app in the personal space.	• Adobe Reader • Browser • Documents To Go • File Manager • Help • Pictures

Installing personal apps on devices

On BlackBerry Balance and regulated BlackBerry Balance devices, users can install apps in the personal space from various sources such as BlackBerry World, the Amazon Appstore, email attachments, downloads through the browser, media cards, and using development mode (if development mode isn't restricted).

On regulated BlackBerry Balance devices, you can use an IT policy rule to prevent users from installing apps in the personal space from sources other than BlackBerry World or using development mode. However, if development mode is also restricted in the IT policy, users can't install personal apps using development mode either.

BlackBerry Balance and regulated BlackBerry Balance devices classify all Android apps as personal apps and as such, they can be installed only in the personal space on devices. You can't deploy or approve Android apps for installation in the work space. Android apps can access only personal data that is located in the personal space.

Managing work apps on devices

You can use BlackBerry UEM to manage and monitor apps that your organization wants to make available as work apps on BlackBerry 10 devices.

Work apps are added to the work space on devices and work apps can only access work data and interact with other work apps. Devices can have the same app installed separately in the work space and the personal space. Each instance of the app is kept separate from the other and each operates under the rules and restrictions that apply to the space that it's installed in. The apps can be configured, upgraded, or removed independently, and changes to one instance have no effect on the other instance. For example, an instant messaging app installed in the personal space might be restricted from adding work contacts, while the same instant messaging app installed in the work space doesn't have that restriction.

Note: The work space doesn't support BlackBerry Runtime for Android apps.

BlackBerry World for Work

The BlackBerry World for Work app is installed in the work space on BlackBerry 10 devices during activation.

BlackBerry World for Work contains a Company Apps tab and a Public Apps tab that lists optional apps. The Company Apps tab provides a list of optional apps that are hosted by your organization and deployed using BlackBerry UEM. The Public Apps tab provides a list of apps from the public BlackBerry World app that you specified as optional apps for the work space.

If any of the apps that you specify as optional apps don't meet specific criteria for devices (for example, service provider, country, or device version), the apps don't appear in BlackBerry World for Work on those devices. If you specify an Android app from the public BlackBerry World as an optional app, it doesn't appear in BlackBerry World for Work on devices.

Preventing users from installing apps using development tools

App developers can use development tools to test apps that they're developing by installing the apps on BlackBerry 10 devices using a USB or Wi-Fi connection. You can use IT policy rules to prevent users from using development tools to install apps on devices or to only the work space on devices.

When development mode isn't permitted on devices:

- Users can install apps in the work space only from the BlackBerry World for Work storefront.
- On BlackBerry Balance and regulated BlackBerry Balance devices, users can install apps in the personal space from all available sources (such as BlackBerry World and downloading apps through the browser), except using development mode.

Managing how apps open links in the work and personal spaces on devices

In general, work apps can open only other work apps and personal apps can open only other personal apps on BlackBerry Balance and regulated BlackBerry Balance devices. For example, if a user clicks a link in a personal email message, the browser in the personal space opens. In a few cases, work apps open apps that are classified as personal apps, such as Phone, BBM, or SMS. In these cases, devices have restrictions in place to protect against data leakage and to make sure that only the minimum amount of data required to initiate the personal apps is passed between the work and personal apps.

By default, users can use the browser in the personal space to open links in both personal and work email messages. Links in work email messages open in the browser in the personal space and devices display a message that provides users with the option to open the link in the browser in the work space instead. You can use an IT policy rule to require links in work email messages to always open in the browser in the work space.

Making preinstalled apps unavailable on devices

You can use IT policy rules to make some preinstalled apps, such as BBM and apps installed by wireless service providers, unavailable on work space only devices and in the personal and work spaces on regulated BlackBerry Balance devices. You can also prevent users from creating accounts for services such as Facebook and Twitter on the device.

Controlling how apps on devices connect to networks

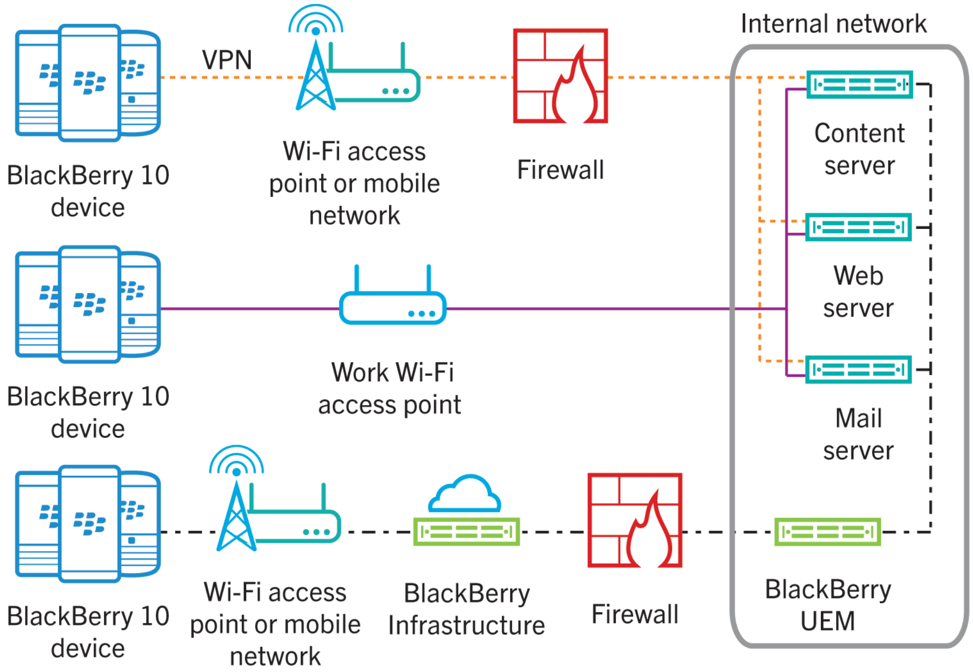
You can use IT policy rules to control how work apps and personal apps connect to networks. On BlackBerry Balance and regulated BlackBerry Balance devices, work data traffic and personal data traffic are routed independently. Because work space only devices are entirely controlled by your organization, all apps and data on these devices are considered work apps and work data.

Controlling how work apps connect to work networks

You can use IT policy rules to control the type of connections that work apps on BlackBerry 10 devices use to connect to your organization’s network. Work apps can access your organization’s network using a number of communication methods. These connections are prioritized, and work apps usually use the default route.

The "Force network access control for work apps" IT policy rule controls what connections are available to work apps. If the "Force network access control for work apps" IT policy rule isn't selected, work apps attempt to connect to your organization's network using the following communication methods, in order:

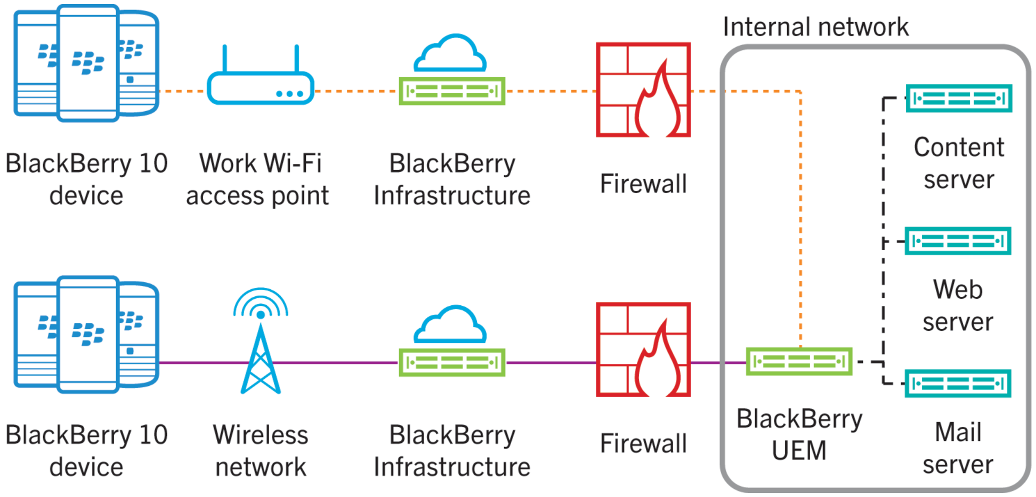
1. Work VPN profiles over a Wi-Fi network
2. Work VPN profiles over a mobile network
3. Work Wi-Fi profiles
4. BlackBerry Infrastructure over a Wi-Fi network
5. BlackBerry Infrastructure over a mobile network



By default, work apps can use Wi-Fi profiles, VPN profiles, or BlackBerry UEM to connect to your organization's network. If you want to control or filter all work traffic on devices, you can select the "Force network access control for work apps" IT policy rule. When you select this rule, you disable Wi-Fi and VPN connections for work apps and limit connectivity exclusively to BlackBerry UEM (using the BlackBerry MDS Connection Service and the BlackBerry Infrastructure).

If the "Force network access control for work apps" IT policy rule is selected, work apps attempt to connect to your organization's network using the following communication methods, in order:

1. BlackBerry Infrastructure over a Wi-Fi network
2. BlackBerry Infrastructure over a mobile network



Preventing personal apps from connecting to work networks

By default, personal apps on BlackBerry Balance and regulated BlackBerry Balance devices can use your organization’s VPN or Wi-Fi network to connect to the Internet.

You can prevent all apps in the personal space from using your organization’s networks to connect to the Internet using an IT policy rule. If you prevent personal apps from using your organization's networks to connect to the Internet and if a personal network isn't available, personal apps that need access to the Internet might not work.

BBM Video is classified as a personal app on BlackBerry Balance and regulated BlackBerry Balance devices. If you allow personal apps to use your organization's networks to connect to the Internet, you can prevent BBM Video from using your organization’s networks for incoming and outgoing video chats using an IT policy rule.

Allowing work apps to connect to personal networks

By default, work apps on BlackBerry Balance and regulated BlackBerry Balance devices can’t use personal networks to connect to the Internet. You can allow work apps, including organizer apps, to make connections using personal networks when a work Wi-Fi or work VPN connection isn’t available using an IT policy rule.

Most apps on work space only devices send all data through your organization's network. The following apps and features on work space only devices don't route data traffic through your organization's network and can send data through any personal Wi-Fi connection or over the mobile network:

- Software updates
- BBM, including BBM Voice and BBM Video
- Hotspot Browser
- Mobile payment communication with a payment service
- Initial setup of personal email accounts (personal email messages go through your organization's network)

Smart cards

Smart cards can be used with BlackBerry 10 devices to:

- Allow users to authenticate with their smart cards and log in (this is called two-factor authentication)
- Import the certificates that are required for S/MIME encryption
- Allow app developers to develop their own secure solutions using the BlackBerry 10 platform
- Import the certificates that are required to authenticate with secure websites

BlackBerry 10 supports the integrated microSD smart card reader on devices, supports external smart card readers, and includes native smart card drivers for PIV and CAC standardized smart cards.

To use a microSD smart card, a user must insert the smart card into the device and configure the smart card settings on the device. Smart card settings include options such as LED notifications when the smart card on a device is accessed. For more information about configuring a device to support a microSD smart card, see the user guide for the device and the user guide for the microSD smart card. To configure a device to support an external smart card reader, see the user guide for the external smart card reader.

To permit apps on the device to access the microSD smart card, a developer can use the Smart Card API in the BlackBerry 10 Native SDK.

If your devices are managed by BlackBerry UEM, an administrator can control how certain devices can use smart cards. For example, BlackBerry UEM allows an administrator to:

- Specify whether two-factor authentication is required, allowed, or disallowed
- Specify whether users also must enter the work space password to unlock the work space, or if they need only the smart card and smart card password to unlock the work space
- Specify whether two-factor authentication can be used to unlock the work space, the device, or both
- Specify whether a device can cache the smart card password in the device RAM
- Specify whether a device or the work space on a device locks when a user removes the smart card from a supported smart card reader or disconnects a supported smart card reader from the device

Unbinding the current smart card from a device

The binding between a user's current smart card and a BlackBerry 10 device is deleted when:

- An administrator or a user wipes the device. During this process, the device deletes the smart card binding information from device memory. When the process completes, a user can authenticate with the device using a new smart card. An administrator can wipe the device by sending an IT administration command to the device.
- An administrator or a user turns off two-factor authentication. During this process, the device turns off two-factor authentication with the installed smart card and deletes the smart card binding information from the device.

Authenticating a user using a smart card

When an administrator or a user turns on two-factor authentication on a BlackBerry 10 device, the user is required to authenticate with the device using a smart card. Users must prove their identities by demonstrating two factors:

- What they have (the smart card)
- What they know (the smart card password)

When a user or an administrator turns on two-factor authentication on the device, the following events occur:

1. The device prompts the user to:
    - Type the device password if the user or an administrator configured the device to require two-factor authentication for the full device.
    - Type the work space password if the user or an administrator configured the device to require two-factor authentication for the work space.

If the user hasn’t configured a device password or a work space password, two-factor authentication can’t be configured. The device activation type and IT policy rule settings determine which smart card settings are available on a device for two-factor authentication.

2. The device prompts the user to type the smart card password to turn on two-factor authentication with the installed smart card.

BlackBerry Link

BlackBerry 10 device users can use BlackBerry Link on a computer to:

- Synchronize music, pictures, videos, contacts, calendar appointments, and documents between devices and computers over USB or Wi-Fi connections
- Import contacts and calendar appointments from Microsoft Outlook to a device
- Back up and restore apps and data
- Update or reinstall device software
- Transfer supported settings and data to a new device
- Manage multiple devices that use the same or a different BlackBerry ID
- Allow remote file access, so that their devices can access files stored in user-selected folders on their computers

BlackBerry Link and devices offer data and connection protection during backup, restore, remote media, and remote file access operations.

If your devices are managed by BlackBerry UEM, BlackBerry Balance devices and regulated BlackBerry Balance devices can back up and restore the work space and personal space. Work space only devices can back up the work space (because they have only one space). An administrator can prevent users from backing up and restoring apps and data on devices.

Authentication between devices and BlackBerry Link

When BlackBerry 10 device users open BlackBerry Link for the first time, they can log in using their BlackBerry ID login information to authenticate the connection between their devices and BlackBerry Link.

BlackBerry Link uses the BlackBerry Infrastructure to establish a trusted pairing with a device using a TLS tunnel. BlackBerry Link and the device share keys that are based on the user’s BlackBerry ID. The certificates are encrypted using secp521r1. When the certificate exchange is complete, BlackBerry Link and the device establish a mutually authenticated TLS connection.

During the initial authentication, if the device has a password, BlackBerry Link has to log in to the device using login.cgi. A token is then granted which allows for token-based authentication for subsequent logins.

Data protection between BlackBerry Link and devices

The communication channel between BlackBerry Link and a BlackBerry 10 device uses DTLS 1.0 and TLS 1.1 and is encrypted using AES-256. ECDH and ECDSA are used to establish the secure channel.

The communication channel uses DTLS 1.0 for UDP connections and TLS 1.1 for TCP connections. BlackBerry Link and devices support the TLS_ECDH_ECDSA_AES_256_SHA cipher suite when establishing a TLS connection.

Backup and restore

BlackBerry 10 device users can back up and restore apps and data on devices using BlackBerry Link. Users can restore the backed up data to devices after the device software is updated or if issues occur that require users to restore the information. Users can restore the data to the same device or transfer it to another device. The data is encrypted and stored on the users' computers. An administrator can generate the required encryption keys in BlackBerry UEM and BlackBerry UEM delivers the keys to devices.

BlackBerry Balance devices and regulated BlackBerry Balance devices can back up and restore the work space and personal space. Work space only devices can back up the work space (because they have only one space). An administrator can use BlackBerry UEM to prevent users from backing up and restoring apps and data on devices.

Backup protection

When a BlackBerry 10 device user backs up apps and data, the device encrypts the apps and data and then authenticates the backup file and header information before it sends the file to BlackBerry Link. BlackBerry Link then stores the file on the user's computer.

The device uses AES in CTR mode with a 256-bit key to encrypt and decrypt backup files and HMAC-SHA-256 to verify the integrity and authenticity of the backup files. Personal and work spaces are encrypted with different encryption keys.

To encrypt backup files for the personal space, the device uses a secret associated with the user's BlackBerry ID account to generate the encryption key and HMAC key. The secret isn't accessible to the user and is never stored as part of the device backup file. The encryption key is stored on the device in an encrypted format.

To encrypt backup files for the work space, the devices uses a secret associated with the user's account associated with BlackBerry Link to generate the encryption key and HMAC key. The secret isn't accessible to the user and is never stored as part of the device backup file. The encryption key is stored in the device keystore in the work file system, which is encrypted.

The device uses the secret and a random salt to generate a 256-bit symmetric encryption key and a 256-bit authentication key. The device uses the encryption key to encrypt and decrypt the backup file and the authentication key to verify the integrity and authenticity of the backup file.

Restore protection

When a BlackBerry 10 device user restores backed up apps and data to a device, the device verifies the authenticity and integrity of the backup file before it decrypts and restores it.

To restore an encrypted backup file to the personal space on a new device during a device switch, the new device must use the same BlackBerry ID as the old device.

To restore an encrypted backup file to the work space on a new device during a device switch, the work space on the new device must be activated using the same user from your organization's user directory.

Remote media and file access architecture

Remote media and file access over Wi-Fi connections on BlackBerry 10 devices is exposed through a WebDAV interface that is implemented using the following extension modules on top of the Nginx HTTP and proxy server:

- Media Sync module
- Nginx module
- WebDAV module

Remote access to files and media is restricted to the personal space on BlackBerry Balance and regulated BlackBerry Balance devices.

Data in transit

7

BlackBerry 10 devices support various methods to keep data private and secure while it's in transit to and from devices.

Data sent between devices and your organization's resources is protected using various methods depending on the path that the data takes. Data sent between your organization's mail, web, and content servers and devices can travel directly over a work VPN or work Wi-Fi network or, depending on the device activation type and the options you choose, through BlackBerry UEM and the BlackBerry Infrastructure.

When BlackBerry UEM sends device management data such as IT policies, profiles, or IT administration commands and required apps from your organization's network to devices, it always sends the data through the BlackBerry Infrastructure, even when the device is connected to a work Wi-Fi network or work VPN.

Regardless of the type of data and the path it takes, the data is encrypted and travels over mutually authenticated connections. The data can't be decrypted by the BlackBerry Infrastructure or at any other point in transit.

Protecting data in transit over the BlackBerry Infrastructure

Data sent between devices and your resources passes through the BlackBerry Infrastructure in the following circumstances:

- BlackBerry UEM sends internal apps and all device management data, such as IT policies, profiles, and IT administration commands, to devices through the BlackBerry Infrastructure, even when the device is connected to a work VPN or work Wi-Fi network.
- Data sent between a device and your organization's mail, web, and content servers travels through BlackBerry UEM and the BlackBerry Infrastructure only when the device isn't connected to a work VPN or work Wi-Fi network.

Protecting device management data sent between BlackBerry UEM and devices

When BlackBerry UEM sends device management data such as IT policies, profiles, IT administration commands, and internal apps from your organization's network to devices, it always sends the data through the BlackBerry Infrastructure, even when the device is connected to a work Wi-Fi network or work VPN.

During the activation process, a mutually authenticated TLS connection is established between BlackBerry UEM and BlackBerry 10 devices. When BlackBerry UEM needs to send configuration information to a device, BlackBerry UEM and the device use the TLS connection to protect the data.

How BlackBerry UEM authenticates with the BlackBerry Infrastructure

To protect data in transit between BlackBerry UEM and the BlackBerry Infrastructure, BlackBerry UEM and the BlackBerry Infrastructure must authenticate with each other before they can transfer data. BlackBerry UEM and the BlackBerry Infrastructure use different authentication methods, depending on the connection options you choose and the type of data being sent:

- When BlackBerry UEM sends device management data to a BlackBerry 10 device, BlackBerry UEM and the BlackBerry Infrastructure establish a mutually authenticated TLS connection that uses AES-256 to protect the data in transit.
- When BlackBerry UEM sends work data from your organization's mail, web, and content servers to BlackBerry 10 devices through the BlackBerry Infrastructure using enterprise connectivity, BlackBerry UEM uses SRP to authenticate with and connect to the BlackBerry Infrastructure.
- When BlackBerry UEM sends work data from your organization's mail, web, and content servers to BlackBerry 10 devices using BlackBerry Secure Connect Plus, BlackBerry UEM uses SRP to authenticate with the BlackBerry Infrastructure and then establishes a secure IP tunnel using DTLS between BlackBerry UEM and the device.

After BlackBerry UEM and the BlackBerry Infrastructure open an SRP connection, BlackBerry UEM establishes a persistent TCP/IP connection over TCP port 3101 that it can use to send data to the BlackBerry Infrastructure.

SRP is a proprietary point-to-point protocol that runs over TCP/IP. BlackBerry UEM uses SRP to contact the BlackBerry Infrastructure and open a connection. When BlackBerry UEM and the BlackBerry Infrastructure open a connection, they can perform the following actions:

- Authenticate with each other
- Exchange configuration information
- Send and receive data

Data flow: Authenticating BlackBerry UEM with the BlackBerry Infrastructure when sending device management data

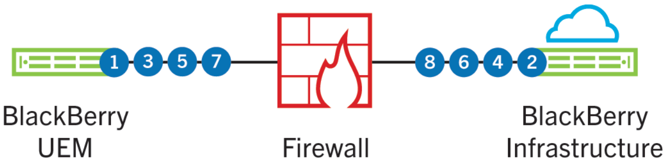
1. BlackBerry UEM connects to the BlackBerry Infrastructure and initiates a TLS connection.
2. The BlackBerry Infrastructure sends an authentication certificate to BlackBerry UEM.
3. BlackBerry UEM performs the following actions:

- Verifies that the authentication certificate is signed by a trusted CA
- Verifies the name of the server in the BlackBerry Infrastructure to establish the TLS connection
- Sends a data packet that contains its unique SRP ID and SRP authentication key to the BlackBerry Infrastructure to claim the SRP ID

4. The BlackBerry Infrastructure verifies the SRP ID and SRP authentication key sent by BlackBerry UEM and performs one of the following actions:

    - If the credentials are valid, sends a confirmation to BlackBerry UEM to complete the authentication process and configure an authenticated SRP connection
    - If the credentials aren't valid, stops the authentication process and closes the SRP connection

Data flow: Authenticating BlackBerry UEM with the BlackBerry Infrastructure when sending work data to devices



1. BlackBerry UEM connects to the BlackBerry Infrastructure and initiates a TLS connection.
2. The BlackBerry Infrastructure sends an authentication certificate to BlackBerry UEM.
3. BlackBerry UEM performs the following actions:

    - Verifies that the authentication certificate is signed by a trusted CA
    - Verifies the name of the server in the BlackBerry Infrastructure to establish the TLS connection
    - Sends a data packet that contains its unique SRP ID and SRP authentication key to the BlackBerry Infrastructure to claim the SRP ID

4. The BlackBerry Infrastructure sends a random challenge string to BlackBerry UEM.
5. BlackBerry UEM sends a challenge string to the BlackBerry Infrastructure.
6. The BlackBerry Infrastructure hashes the challenge string it received from BlackBerry UEM with the SRP authentication key using HMAC with the SHA-1 algorithm. The BlackBerry Infrastructure sends the resulting 20-byte value to BlackBerry UEM as a challenge response.
7. BlackBerry UEM hashes the challenge string it received from the BlackBerry Infrastructure with the SRP authentication key, and sends the result as a challenge response to the BlackBerry Infrastructure.
8. The BlackBerry Infrastructure performs one of the following actions:

    - Accepts the challenge response and sends a confirmation to BlackBerry UEM to complete the authentication process and configure an authenticated SRP connection

- Rejects the challenge response

If the BlackBerry Infrastructure rejects the challenge response, the authentication process isn't successful. The BlackBerry Infrastructure and BlackBerry UEM close the SRP connection.

If BlackBerry UEM uses the same SRP authentication key and SRP ID to connect to (and then disconnect from) the BlackBerry Infrastructure five times in one minute, the BlackBerry Infrastructure deactivates the SRP ID to help prevent an attacker from using the SRP ID to create conditions for a DoS attack.

How devices connect to the BlackBerry Infrastructure

Devices and the BlackBerry Infrastructure send all data to each other over a TLS connection. The TLS connection encrypts the data that devices and the BlackBerry Infrastructure send between each other.

If an attacker tries to impersonate the BlackBerry Infrastructure, devices prevent the connection. Devices verify whether the public key of the TLS certificate for the BlackBerry Infrastructure matches the private key of the root certificate that's installed on devices during the activation process. If a user accepts a certificate that isn't valid, the connection can't open unless the device can also authenticate with a valid BlackBerry UEM instance.

In a BlackBerry Infrastructure connection, a device connects to your organization’s resources through any wireless access point, the BlackBerry Infrastructure, your organization's firewall, and BlackBerry UEM. Wi-Fi encryption is only used if the wireless access point is set up to use it.

Data flow: Opening a TLS connection between the BlackBerry Infrastructure and a device

1. A device sends a request to the BlackBerry Infrastructure to open a TLS connection.
2. The BlackBerry Infrastructure sends its TLS certificate to the device.
3. The device verifies the TLS certificate using a root certificate preloaded on the device during the manufacturing or activation process.
4. The device opens the TLS connection.

How devices connect to your resources

BlackBerry 10 devices with enterprise connectivity enabled can connect to your organization’s resources such as mail servers, web servers, and content servers, using several communication methods. By default, devices try to connect to your organization’s resources using the following communication methods, in order:

1. Work VPN profiles that you configure (iOS devices only)
2. Work Wi-Fi profiles that you configure
3. The BlackBerry Infrastructure and BlackBerry UEM
4. Personal VPN or Wi-Fi settings that a user configures on the device

Protecting work data in transit between devices and your resources

Before BlackBerry UEM or a BlackBerry 10 device sends data between the device and your organization's mail, web, and content servers over the BlackBerry Infrastructure, they compress the data, encrypt the data using message keys, and encrypt the message keys using the device transport key. When BlackBerry UEM or a device receives the data, they decrypt the message keys using the device transport key, decrypt the data, and then decompress the data. This process is known as BlackBerry transport layer encryption.

Data in transit between devices and your organization's servers that is sent over the TCP/IP connection between BlackBerry UEM and the BlackBerry Infrastructure is secure because no intermediate point between BlackBerry UEM and the device decrypts and encrypts the data again.

No data traffic sent from devices through the BlackBerry Infrastructure can reach your organization's resources unless BlackBerry UEM can decrypt the data using a valid device transport key.

BlackBerry UEM and devices use AES-256 in CBC mode as the symmetric algorithm for BlackBerry transport layer encryption.

Device transport keys

The device transport key encrypts the message keys that protect data in transit between your organization's resources and BlackBerry 10 devices sent through BlackBerry UEM and the BlackBerry Infrastructure. BlackBerry UEM and a device generate the device transport key when a user activates the device.

Only BlackBerry UEM and the device know the value of the device transport key. They reject a data packet if they don't recognize the format of the data packet or don't recognize the device transport key that protects the data packet.

Devices store device transport keys in a keystore database in flash memory. The keystore database prevents an attacker from copying the device transport keys to a computer by trying to back up the device transport keys. An attacker can't extract key data from flash memory.

Generating the device transport key for a device

When a user activates a BlackBerry 10 device, the device sends a CSR to BlackBerry UEM. BlackBerry UEM uses the CSR to create a client certificate, signs the client certificate with its enterprise management root certificate, and sends the client certificate and the enterprise management root certificate to the device. To protect the connection between the device and BlackBerry UEM during the certificate exchange, the device and BlackBerry UEM create a short-lived symmetric key using the activation password and EC-SPEKE.

When the certificate exchange is complete, the device and BlackBerry UEM establish a mutually authenticated TLS connection using the client certificate and the server certificate. The device verifies the server certificate using the enterprise management root certificate.

To generate the device transport key, the device and BlackBerry UEM use the authenticated long-term public keys that are associated with the client certificate and with the server certificate for BlackBerry UEM, and ECMQV. The ECMQV protocol is used over the mutually authenticated TLS connection. The elliptic curve used in ECMQV is the NIST-recommended 521-bit curve.

BlackBerry UEM and the device don't send the device transport key over the wireless network when they generate the device transport key or when they exchange data.

Message keys

Message keys protect the integrity of data sent between your organization's resources and BlackBerry 10 devices through BlackBerry UEM and the BlackBerry Infrastructure.

BlackBerry UEM and a BlackBerry 10 device generate one or more message keys for all data channeled through BlackBerry UEM and the BlackBerry Infrastructure. If the data exceeds 2 KB and consists of several data packets, BlackBerry UEM and the device generate a unique message key for each data packet.

Each message key consists of random data that makes it difficult for a third party to decrypt, re-create, or duplicate the message key.

BlackBerry UEM and the device don't store the message keys in persistent storage. They free the memory that is associated with the message keys after BlackBerry UEM or the device uses the message keys to decrypt the data.

The device uses bits retrieved from the randomization source on the device to generate a pseudorandom high entropy message key.

Data flow: Generating a message key on a device

A BlackBerry 10 device uses the DRBG function to generate a message key.

To generate a message key, the device performs the following actions:

1. Retrieves random data from multiple sources to generate the seed using a technique that the device derives from the initialization function of the ARC4 encryption algorithm
2. Uses the random data to reorder the contents of a 256-byte state array
3. Adds the 256-byte state array into the ARC4 encryption algorithm to further randomize the 256-byte state array
4. Draws 521 bytes from the ARC4 state array

   The device draws an additional 9 bytes for the 256-byte state array, for a total of 521 bytes (512 + 9 = 521) to make sure that the pointers before and after the call aren't in the same place, and in case the first few bytes of the ARC4 state array aren't random.

5. Uses SHA-512 to hash the 521-byte value to 64 bytes
6. Uses the 64-byte value to seed the DRBG function

The device stores a copy of the seed in a file. When the device restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.

7. Uses the DRBG function to generate 256 pseudorandom bits for use with AES encryption
8. Uses the pseudorandom bits to create the message key

For more information about the DRBG function, see *NIST Special Publication 800-90*.

Data flow: Generating a message key in BlackBerry UEM

BlackBerry UEM uses the DSA PRNG function to generate a message key.

To generate a message key, BlackBerry UEM performs the following actions:

1. Retrieves random data from multiple sources for the seed, using a technique that BlackBerry UEM derives from the initialization function of the ARC4 encryption algorithm
2. Uses the random data to reorder the contents of a 256-byte state array

   BlackBerry UEM requests 512 bits of randomness from the Microsoft Cryptographic API to increase the randomness of the data.

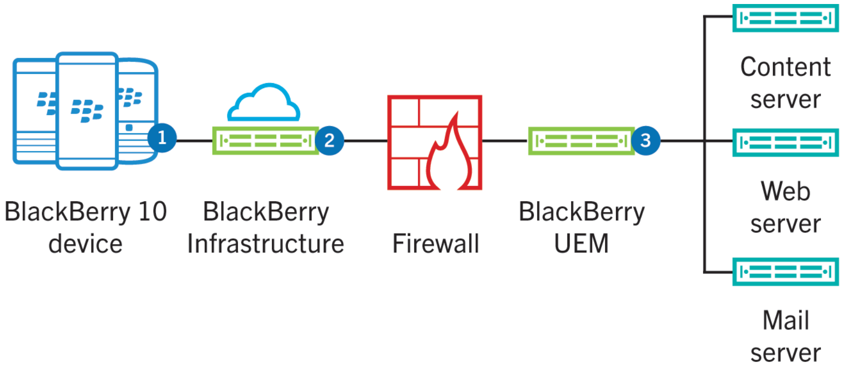
3. Adds the 256-byte state array into the ARC4 algorithm to further randomize the 256-byte state array
4. Draws 521 bytes from the 256-byte state array

   BlackBerry UEM draws an additional 9 bytes for the 256-byte state array, for a total of 521 bytes (512 + 9 = 521) to make sure that the pointers before and after the generation process aren't in the same place, and in case the first few bytes of the 256-byte state array aren't random.

5. Uses SHA-512 to hash the 521-byte value to 64 bytes
6. Uses the 64-byte value to seed the DSA PRNG function
7. Uses the DSA PRNG function to generate 256 pseudorandom bits for use with AES encryption
8. Uses the pseudorandom bits with AES encryption to generate the message key

For more information about the DSA PRNG function, see *Federal Information Processing Standard - FIPS PUB 186-2*.

Data flow: Sending data from devices to your servers through the BlackBerry Infrastructure



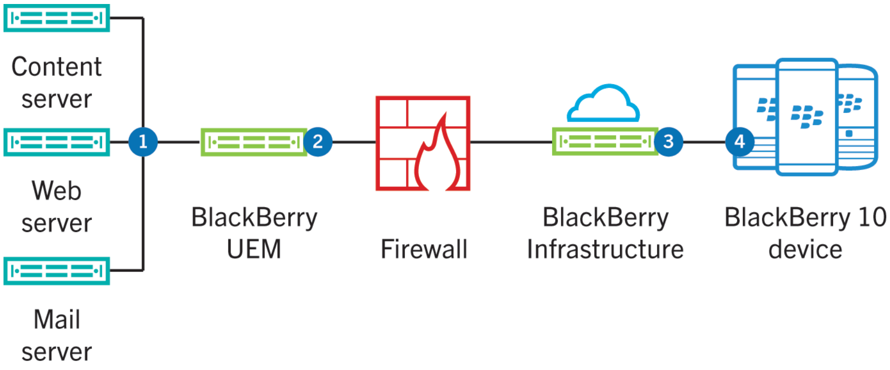
1. The BlackBerry 10 device performs the following actions:

   a. Compresses the data
   b. Encrypts the data using message keys
   c. Encrypts the message keys using the device transport key
   d. Sends the data to the BlackBerry Infrastructure over a TLS connection

2. The BlackBerry Infrastructure sends the data to BlackBerry UEM over a persistent TCP/IP connection.
3. BlackBerry UEM performs the following actions:

   a. Decrypts the message keys using the device transport key
   b. Decrypts the data using message keys
   c. Decompresses the data
   d. Sends the data to the destination server inside your firewall

Data flow: Sending data from your servers to devices through the BlackBerry Infrastructure



1. A mail, web, or content server inside your firewall sends the data to BlackBerry UEM.
2. BlackBerry UEM performs the following actions:

   a Compresses the data
   b Encrypts the data using message keys
   c Encrypts the message keys using the device transport key
   d Sends the data to the BlackBerry Infrastructure over a persistent TCP/IP connection

3. The BlackBerry Infrastructure sends the data to the BlackBerry 10 device over a TLS connection.
4. The BlackBerry 10 device performs the following actions:

   a Decrypts the message keys using the device transport key
   b Decrypts the data using message keys
   c Decompresses the data

Restricting cipher suites on devices

BlackBerry UEM allows you to restrict which cipher suites from the SSL library that BlackBerry 10 devices support. You can do this if you want to remove support for a cipher suite that has a security vulnerability and your organization's resources don't require that cipher suite for communication.

In most deployments, the default SSL configuration values are acceptable. Pushing out a custom SSL configuration to your user's devices can have a severe impact on the systems that your user's devices need to connect to. If you plan to push out a custom SSL configuration to devices, you should test it on a few devices first.

NIAP Common Criteria functionality on devices

NIAP is a United States government initiative to meet information technology security requirements.

BlackBerry UEM and BlackBerry 10 devices (BlackBerry 10 OS version 10.3.3 and later) support NIAP Common Criteria functionality. When the “Enable NIAP Common Criteria functionality” IT policy rule is selected, regulated BlackBerry Balance and work space only devices negotiate all TLS connections according to the Suite B Profile defined in RFC 6460 and support the following cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

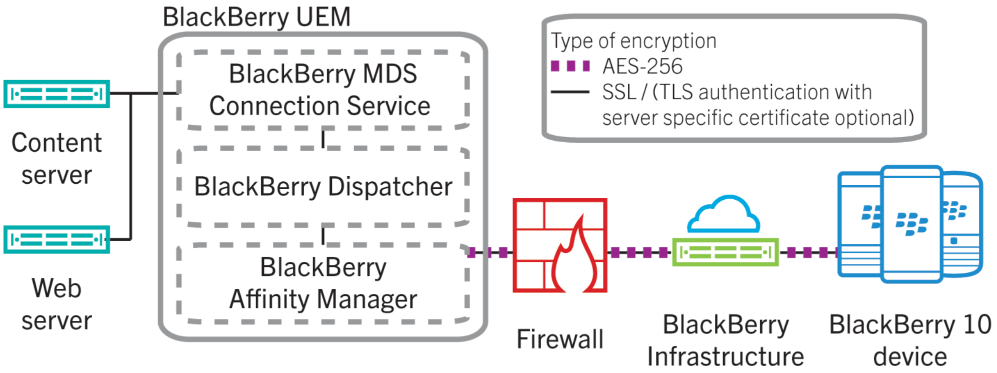
Securing the communication between apps on devices and your organization's network

BlackBerry 10 devices permit work apps and personal apps (on devices with a personal space) to use any available Wi-Fi profile or VPN profile to connect to your organization's network. If you configure Wi-Fi profiles or VPN profiles using BlackBerry UEM, you permit personal apps to access your organization's network.

If the security requirements of your organization don't permit personal apps to access your organization's network, you can restrict connection options. You can use the "Allow personal apps to use work networks" IT policy rule to prevent personal apps from using your organization's network to connect to the Internet using your work Wi-Fi network or work VPN connection.

You can also limit the communication methods that devices can use to connect to your organization's network through BlackBerry UEM by limiting connectivity options to the BlackBerry MDS Connection Service and the BlackBerry Infrastructure. Personal apps can't use the BlackBerry MDS Connection Service and the BlackBerry Infrastructure to connect to your organization’s network.

Securing data pushed to apps on devices


BlackBerry UEM
BlackBerry MDS Connection Service
BlackBerry Dispatcher
BlackBerry Affinity Manager
Content server
Web server
Type of encryption
AES-256
SSL / (TLS authentication with server specific certificate optional)
Firewall
BlackBerry Infrastructure
BlackBerry 10 device

The BlackBerry MDS Connection Service connects push applications hosted on your organization's application servers or web servers to apps on BlackBerry 10 devices. The BlackBerry MDS Connection Service sends push requests, received from push applications, through the BlackBerry Infrastructure to apps on BlackBerry 10 devices.

You can permit only specific push applications to push data to BlackBerry 10 devices and you can turn on authentication to prevent the BlackBerry MDS Connection Service from sending data from unauthorized push applications.

To protect the connection between push applications and the BlackBerry MDS Connection Service, you can use TLS. Push applications can use the self-signed certificate that is generated when you configure the BlackBerry MDS Connection Service keystore, or you can add a signed certificate from a trusted public CA to the keystore.

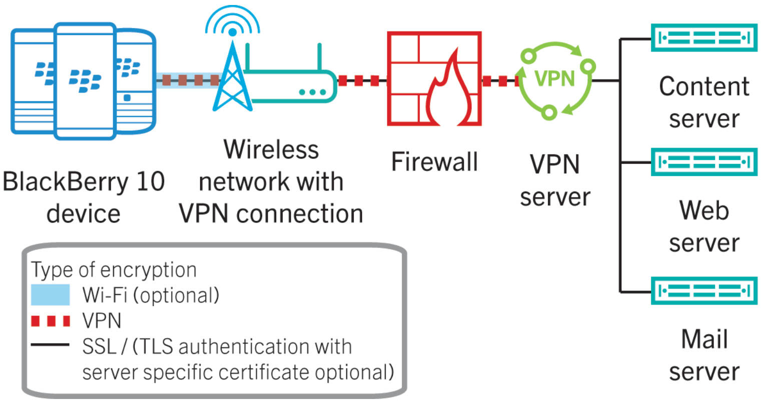
Connecting to a VPN

BlackBerry 10 devices support a number of VPN solutions to provide secure connectivity to your organization's network from the outside. A VPN solution consists of a VPN client on a device and a VPN concentrator. The device can use the VPN client to authenticate with the VPN concentrator, which acts as the gateway to your organization's network.

Each device includes a built-in VPN client that supports several VPN concentrators. Depending on the VPN solution, a client app may need to be installed on the device. The VPN client on the device supports the use of strong encryption to authenticate itself with the VPN concentrator. It creates an encrypted tunnel between the device and the VPN concentrator that the device and your organization's network can use to communicate.

If your devices are managed by BlackBerry UEM, an administrator can configure devices to authenticate with a VPN to access your organization's network.

VPN encryption



In a VPN connection, devices connect to your organization's resources through any wireless access point or a mobile network, your organization's firewall, and your organization's VPN server. Wi-Fi encryption is used if the wireless access point is set up to use it.

The device can use either password or certificate-based authentication to connect.

Connecting to Wi-Fi

BlackBerry 10 devices can connect to work Wi-Fi networks that use the IEEE 802.11 standard. The IEEE 802.11i standard uses the IEEE 802.1X standard for authentication and key management to protect work Wi-Fi networks. The IEEE 802.11i standard specifies that organizations must use the PSK protocol or the IEEE 802.1X standard as the access control method for Wi-Fi networks.

If your devices are managed by BlackBerry UEM, an administrator can use Wi-Fi profiles to send Wi-Fi configuration information, including security settings and any required certificates to devices.

Layer 2 security methods

BlackBerry 10 devices can use security methods for layer 2 (also known as the IEEE 802.11 link layer) so that a wireless access point can authenticate the device to allow the device and the wireless access point to encrypt the data that they send to each other. BlackBerry 10 devices support the following layer 2 security methods:

- WEP encryption (64-bit and 128-bit)
- IEEE 802.1X standard and EAP authentication using PEAP, EAP-TLS, EAP-TTLS, and EAP-FAST
- TKIP and AES-CCMP encryption for WPA-Personal, WPA2-Personal, WPA-Enterprise, and WPA2-Enterprise

To support layer 2 security methods, BlackBerry 10 devices have a built-in IEEE 802.1X supplicant.

If a work Wi-Fi network uses EAP authentication, you can permit and deny device access to the work Wi-Fi network by updating your organization's central authentication server. You're not required to update the configuration of each access point.

For more information about IEEE 802.11 and IEEE 802.1X, see www.ieee.org/portal/site. For more information about EAP authentication, see RFC 3748.

IEEE 802.1X standard

The IEEE 802.1X standard defines a generic authentication framework that a device and a work Wi-Fi network can use for authentication. The EAP framework is specified in RFC 3748.

BlackBerry 10 devices support EAP authentication methods that meet the requirements of RFC 4017 to authenticate the device to the work Wi-Fi network. Some EAP authentication methods (for example, EAP-TLS, EAP-TTLS, EAP-FAST, or PEAP) use credentials to provide mutual authentication between the device and the work Wi-Fi network.

BlackBerry 10 devices are compatible with the WPA-Enterprise and WPA2-Enterprise specifications.

Data flow: Authenticating a BlackBerry 10 device with a work Wi-Fi network using the IEEE 802.1X standard

If you configured a wireless access point to use the IEEE 802.1X standard, the access point permits communication using EAP authentication only. This data flow assumes that a BlackBerry 10 device is configured to use an EAP authentication method to communicate with the access point.

1. The BlackBerry 10 device associates itself with the access point that you configured to use the IEEE 802.1X standard. The device sends its credentials (typically a username and password) to the access point.
2. The access point sends the credentials to the authentication server.
3. The authentication server performs the following actions:
   a Authenticates the device on behalf of the access point
   b Instructs the access point to permit access to the work Wi-Fi network
   c Sends Wi-Fi credentials to the device to permit it to authenticate with the access point
4. The access point and device use EAPoL-Key messages to generate encryption keys (for example, WEP, TKIP, or AES-CCMP, depending on the EAP authentication method that the device uses).

   When the device sends EAPoL messages, the device uses the encryption and integrity requirements that the EAP authentication method specifies. When the device sends EAPoL-Key messages, the device uses the ARC4 algorithm or AES algorithm to provide integrity and encryption.

After the access point and device generate the encryption key, the device can access the work Wi-Fi network.

EAP authentication methods that devices support

BlackBerry 10 devices support several EAP authentication methods.

PEAP authentication

PEAP authentication permits devices to authenticate with an authentication server and access a work Wi-Fi network. PEAP authentication uses TLS to create an encrypted tunnel between a device and the authentication server. It uses the TLS tunnel to send the authentication credentials of the device to the authentication server.

Devices support PEAPv0 and PEAPv1 for PEAP authentication. Devices also support EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols during PEAP authentication so that devices can exchange credentials with the work Wi-Fi network.

To configure PEAP authentication, you must send a CA certificate that corresponds to the authentication server certificate to devices and enroll client certificates, if required. You can use SCEP to enroll client certificates on devices.

EAP-TLS authentication

EAP-TLS authentication uses a PKI to permit a device to authenticate with an authentication server and access a work Wi-Fi network. EAP-TLS authentication uses TLS to create an encrypted tunnel between the device and the authentication server. EAP-TLS authentication uses the TLS encrypted tunnel and a client certificate to send the credentials of the device to the authentication server.

Devices support EAP-TLS authentication when the authentication server and the client use certificates that meet specific requirements.

To configure EAP-TLS authentication, you must send a CA certificate that corresponds to the authentication server certificate to devices and enroll client certificates. You can use SCEP to enroll certificates on devices.

For more information about EAP-TLS authentication, see RFC 2716.

EAP-TTLS authentication

EAP-TTLS authentication extends EAP-TLS authentication to permit a device and an authentication server to mutually authenticate. When the authentication server uses its certificate to authenticate with the device and open a protected connection to the device, the authentication server uses an authentication protocol over the protected connection to authenticate with the device.

Devices support EAP-MS-CHAPv2, MS-CHAPv2, and PAP as second-phase protocols during EAP-TTLS authentication so that devices can exchange credentials with the work Wi-Fi network.

To configure EAP-TTLS authentication, you must send a CA certificate that corresponds to the authentication server certificate to devices.

EAP-FAST authentication

EAP-FAST authentication uses PAC to open a TLS connection to a device and verify the supplicant credentials of the device over the TLS connection.

Devices support EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols during EAP-FAST authentication so that devices can exchange authentication credentials with work Wi-Fi networks. Devices support the use of automatic PAC provisioning with EAP-FAST authentication only.

For more information about EAP-FAST authentication, see RFC 4851.

Supported EAP authentication methods when using CCKM

BlackBerry 10 devices support the use of CCKM with all supported EAP authentication methods to improve roaming between wireless access points. Devices don't support the use of CCKM with the CKIP encryption algorithm or the AES-CCMP encryption algorithm.

Using certificates with PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication

If your organization uses PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication to protect the wireless access points for a work Wi-Fi network, a device must authenticate mutually with an access point using an authentication server. To generate the certificates that the device and authentication server use to authenticate with each other, you require a CA.

For PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication to be successful, the device must trust the certificate of the authentication server. The device doesn't trust the certificate of the authentication server automatically. Each device stores a list CA certificates that it explicitly trusts. To trust the certificate of the authentication server, the device must store the CA certificate for the certificate of the authentication server.

If your devices are managed by BlackBerry UEM, an administrator can send CA certificates to every device and can use SCEP to enroll client certificates on devices.

Protecting work data in transit using BlackBerry Secure Connect Plus

BlackBerry Secure Connect Plus is a BlackBerry UEM component that provides a secure IP tunnel between apps and your organization’s network.

All work space apps use the secure tunnel. This tunnel gives users access to work resources behind your organization’s firewall while ensuring the security of data using standard protocols and end-to-end encryption.

BlackBerry Secure Connect Plus and a supported device establish a secure IP tunnel when a connection to your work Wi-Fi network or VPN isn't available.

Devices communicate with BlackBerry UEM through the BlackBerry Infrastructure to establish the secure tunnel. As long as the tunnel is open, apps can access network resources. When the tunnel is no longer required (for example, the user is in range of the work Wi-Fi network), BlackBerry Secure Connect Plus terminates it.

BlackBerry Secure Connect Plus offers the following advantages:

- The IP traffic that is sent between devices and BlackBerry UEM is encrypted end-to-end using AES-256, ensuring the security of work data.
- BlackBerry Secure Connect Plus provides a secure, reliable connection to work resources when a device user can't access the work Wi-Fi network or VPN.

- BlackBerry Secure Connect Plus is installed behind your organization’s firewall, so data travels through a trusted zone that follows your organization’s security standards.

After BlackBerry UEM and the device determine that a secure IP tunnel is the best available method to connect work space apps to your organization’s network, the device and BlackBerry UEM negotiate the tunnel parameters through the BlackBerry Infrastructure. The established tunnel is authenticated and encrypted end-to-end with DTLS. It supports standard IPv4 protocols (TCP and UDP). BlackBerry Secure Connect Plus encrypts and decrypts traffic using FIPS-140 certified BlackBerry libraries with cipher suites for RSA and ECC keys.

Protecting communication with devices using certificates

A certificate is a digital document that binds the identity and public key of a certificate subject. Each certificate has a corresponding private key that is stored separately. A CA signs the certificate to verify that it can be trusted. Many certificates used for different purposes can be stored on BlackBerry 10 devices.

Devices can use certificates to:

- Authenticate using SSL/TLS when they connect to web pages that use HTTPS
- Authenticate with a work mail server
- Authenticate with a work Wi-Fi network and, for devices that support it, VPN
- Encrypt and sign email messages using S/MIME protection

A user can import certificates into the device’s certificate store. The certificates can be imported from various locations, including a computer, an email, or a smart card.

Certificates can be provided to a device in several ways. An administrator might need to distribute certificates to a device if the device uses certificate-based authentication to connect to a network or server in your organization, or if your organization uses S/MIME. BlackBerry UEM gives you several options to send certificates to devices.

Providing client certificates to devices

Many certificates used for different purposes can be stored on a device. You can provide client certificates to devices in several ways.

How the certificate is added	Description
During device activation	BlackBerry UEM sends certificates to devices during the activation process. Devices use these certificates to establish secure connections between the device and BlackBerry UEM.

How the certificate is added	Description
SCEP profiles	You can create SCEP profiles that devices use to connect to, and obtain client certificates from, your organization's CA using a SCEP service. Devices can use these certificates for certificate-based authentication from the browser and to connect to your work Wi-Fi network, work VPN, and work mail server.
User credential profiles	If your organization uses Entrust or OpenTrust software products to issue and manage certificates, you can create user credential profiles that devices use to get client certificates from your organization's CA. Devices use these certificates for certificate-based authentication from the browser, and to connect to your work Wi-Fi network, work VPN, and work mail server.
User import	Users can import client certificates into the device's certificate store using device settings. Certificates intended for use by the work browser or for sending S/MIME-protected messages from the work email account can be imported from the file system on the device or from a network location that's accessible from the work space.
Smart cards	Users can import S/MIME and SSL certificates to their devices from a smart card.

Enrolling client certificates to devices using SCEP

SCEP is an IETF protocol that simplifies the process of enrolling certificates to a large number of devices without any administrator input or approval required to issue each certificate. Devices can connect to, and obtain client certificates from, your organization's CA using a SCEP service. You can use SCEP to enroll client certificates to devices so that the devices can use certificate-based authentication in the browser and to connect to a work Wi-Fi network, work VPN, or work mail server.

Certificate enrollment starts after a device receives a SCEP profile that's assigned to the user or associated with an assigned Wi-Fi, VPN, or email profile. Devices can receive a SCEP profile from BlackBerry UEM during the activation process, when you change a SCEP profile, or when you change another profile that has an associated SCEP profile. After the certificate enrollment completes, the client certificate and its certificate chain and private key are stored in the work keystore on the device.

If you use a Microsoft CA, the CA must support challenge passwords. The CA uses challenge passwords to verify that the device is authorized to submit a certificate request. If the CA has implemented NDES, you can use dynamic challenge passwords. You specify the static challenge password or the settings to obtain a dynamically generated challenge password from the SCEP service in the SCEP profile. On BlackBerry 10 devices, to help protect the password, it's not sent to the devices. On other devices, the password is sent to the devices to allow the devices to make the certificate request. If you use a static challenge password, all SCEP requests from devices use the same challenge password.

The certificate enrollment process doesn't delete existing certificates from devices or notify the CA that previously enrolled certificates are no longer in use. If a SCEP profile is removed from BlackBerry UEM, the corresponding certificates aren't removed from the assigned users' devices.

To read the SCEP Internet Draft, visit www.ietf.org.

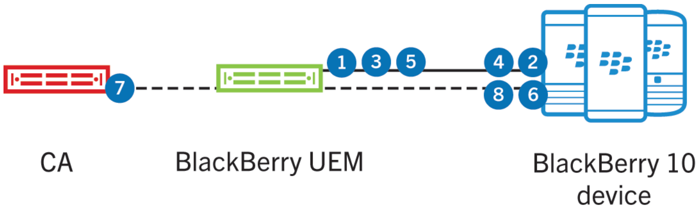
Managing certificates that a device enrolls using SCEP

After a device enrolls a certificate using SCEP, the SCEP component monitors the expiry date of the certificate. When the expiry date of a certificate approaches, the SCEP component starts the enrollment process for a new certificate. You can use a SCEP profile setting to configure how many days before a certificate expires that automatic renewal occurs.

The certificate enrollment process can also start again if you change any of the SCEP profile settings that specify the CA, connection, or the encryption keys. For example, this applies to the URL, SCEP challenge type, Key algorithm, and Key size profile settings.

The certificate enrollment process doesn't delete existing certificates from devices or notify the CA that previously enrolled certificates are no longer in use. If a SCEP profile is removed from BlackBerry UEM, the corresponding certificates aren't removed from the assigned users' devices.

Data flow: Enrolling a client certificate to a BlackBerry 10 device using SCEP



1. BlackBerry UEM sends a SCEP profile that is assigned to the user or associated with an assigned Wi-Fi, VPN, or email profile to the device.
2. The device performs the following actions:
   a Generates a key pair using the key algorithm and strength that is specified in the SCEP profile
   b Generates a PKCS#10 CSR containing all required attributes for the request, except for the challenge password
   c Sends the SCEP profile name, PKCS#10 CSR, and hash type to BlackBerry UEM
3. BlackBerry UEM performs the following actions:
   a Verifies that the subject distinguished name, subject alternative names, and email address that are contained in the request match the user account information in the BlackBerry UEM database
   b Adds the challenge password to the PKCS#10 CSR
   c Hashes the PKCS#10 CSR
   d Sends the PKCS#10 CSR hash to the device
4. The device computes the signature on the PKCS#10 CSR hash, and sends the SCEP profile name, original PKCS#10 CSR, signature request, computed signature response, CA certificate (to encrypt the SCEP request), hash type, and encryption type to BlackBerry UEM.
5. BlackBerry UEM performs the following actions:

   a Verifies the CA certificate that it receives
   b Verifies that the subject distinguished name, subject alternative names, and email address that are contained in the request match the user account information in the BlackBerry UEM database
   c Adds the challenge password to the PKCS#10 CSR
   d Adds the computed signature response to the PKCS#10 CSR
   e Encrypts the PKCS#10 CSR using PKCS#7 enveloped data format and the CA public key
   f Sends the PKCS#7 enveloped data to the device

6. The device completes the SCEP request by signing the PKCS#7 enveloped data using PKCS#7 signed data format and sends the SCEP request through BlackBerry UEM to the CA.
7. The CA issues the certificate and sends it through BlackBerry UEM to the device.
8. The Enterprise Management Agent on the device adds the certificate and corresponding private key to the keystore on the device and, if the SCEP profile is associated with an assigned Wi-Fi, VPN, or email profile, makes the certificate available for the specified connection.

Sending CA certificates to devices

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

When the certificates for the CAs that issued your organization's network and server certificates are stored on devices, the devices can trust your networks and servers when making secure connections. When the CA certificates for the CAs that issued your organization's S/MIME certificates are stored on devices, the devices can trust the sender's certificate when an S/MIME-protected email message is received.

You can use CA certificate profiles to send CA certificates to devices.

Protecting email messages

Devices support using Exchange ActiveSync to synchronize email messages, calendar entries, contacts, and other organizer data with your organization’s mail server. BlackBerry 10 devices also support IBM Notes Traveler. BlackBerry UEM can allow devices that aren't connected to your organization's internal network or don't have a VPN connection to synchronize with the mail server without requiring you to make connections to the mail server available from outside the firewall.

BlackBerry UEM allows devices to synchronize securely with the mail server over the BlackBerry Infrastructure using the same encryption methods that it uses for all other work data. When BlackBerry UEM provides the connection between your mail server and devices, BlackBerry UEM IT policies take precedence over any policies set for the devices on the mail server.

If your organization uses SCEP to enroll certificates to devices, you can associate a SCEP profile with an email profile to require certificate-based authentication to help protect connections between devices and the mail server.

Controlling which devices can use Exchange ActiveSync

You can configure Microsoft Exchange to block devices from using Exchange ActiveSync unless the devices are explicitly added to an allowed list. Devices that aren't on the allowed list can't access work email and organizer data. In BlackBerry UEM, you can set up Microsoft Exchange gatekeeping to control which devices are automatically added to the allowed list on your Microsoft Exchange Server.

If you use Microsoft Exchange gatekeeping, when a user who is assigned an email profile activates a device, the device is automatically added to the allowed list in Microsoft Exchange. A device is automatically removed from the allowed list if you remove the email profile from the user account, if the device violates the settings in the assigned compliance profile, or if the device is deactivated.

Extending email security

Secure email adds another level of security to email messages. Secure email services, such as S/MIME, allow users to digitally sign or encrypt email messages that they send or receive from their devices:

- Digital signatures help recipients verify the authenticity and integrity of messages that users send. When a user digitally signs a message with their private key, recipients use the sender's public key to verify that the message is from the sender and that the message hasn't changed.
- Encryption helps to keep messages confidential. When a user encrypts a message, the device uses the recipient's public key to encrypt the message. The recipient uses their private key to decrypt the message.

BlackBerry 10 devices support the following secure email services: S/MIME, PGP, and IBM Notes email encryption.

S/MIME

Users can use S/MIME to sign, encrypt, or sign and encrypt messages that they send using a work email account that supports S/MIME-protected messages on BlackBerry 10 devices.

Keys and certificates in the PEM (.pem, .cer), DER (.der, .cer), and PFX (.pfx, .p12) file formats and file name extensions are supported. S/MIME private keys stored on smart cards are also supported.

Users must store a certificate for each recipient that they want to send an encrypted email message to on their device. Users must store their private keys on their devices or a smart card, otherwise the devices can't read S/MIME-encrypted messages.

Users can configure S/MIME preferences, including choosing certificates and encoding methods, in the device settings. Users can also configure the S/MIME settings on the device to send either clear-signed messages that any email application can open, or opaque-signed messages that only email applications that support encryption can open. Devices support attachments in S/MIME-protected email messages; users can view, send, and forward attachments in S/MIME-protected email messages.

If your devices are managed by BlackBerry UEM, you can control S/MIME options on devices. For example, BlackBerry UEM allows you to specify whether devices can send S/MIME-protected email messages.

S/MIME certificates and private keys

Devices can use public key cryptography with S/MIME certificates and S/MIME private keys to encrypt and decrypt email messages.

Item	Description
S/MIME public key	When a user sends an email message from a device, the device uses the S/MIME public key of the recipient to encrypt the message. When a user receives a signed email message on a device, the device uses the S/MIME public key of the sender to verify the message signature.
S/MIME private key	When a user sends a signed email message from a device, the device hashes the message using SHA-1 or SHA-2. The device then uses the S/MIME private key of the user to digitally sign the message hash. When a user receives an encrypted email message on a device, the device uses the private key of the user to decrypt the message. The private key is stored on the device.

S/MIME encryption algorithms

When you or a user turns on S/MIME encryption on BlackBerry 10 devices, the value of the "Encryption algorithms" setting specifies that a device can use any of the following encryption algorithms to encrypt messages: AES-256, AES-192, AES-128, RC2, and Triple DES. You can change the value of the "Encryption algorithms" setting to use a subset of the encryption algorithms if your organization's security policies require it.

When a user receives an S/MIME-protected message, the device stores the encryption algorithms that the sender's email application supports. When the user sends an encrypted message to a recipient that the device has stored encryption algorithm information for, the device uses an algorithm that is supported by the recipient. By default, if the device can't determine the encryption algorithms that the recipient's email application can support, the device encrypts the email message using Triple DES.

Data flow: Sending an email message from a BlackBerry 10 device using S/MIME encryption

1. A user sends an email message from a BlackBerry 10 device using S/MIME encryption. The device performs the following actions:

   a Checks the device keystore for the S/MIME certificate of the recipient

   b If the device keystore doesn't include the S/MIME certificate of the recipient, the device retrieves the S/MIME certificate of the recipient from the LDAP server and verifies the certificate status

   c Encrypts the email message with the S/MIME certificate of the recipient

   d If the device is connected to the BlackBerry Infrastructure, uses BlackBerry transport layer encryption to encrypt the S/MIME-encrypted message

   e Sends the encrypted message to BlackBerry UEM

2. If the device is connected to the BlackBerry Infrastructure, BlackBerry UEM decrypts the BlackBerry transport layer encryption.
3. BlackBerry UEM sends the S/MIME-encrypted message to the mail server.
4. The mail server sends the S/MIME-encrypted message to the recipient.
5. The recipient decrypts the S/MIME-encrypted message using their S/MIME private key.

Using S/MIME with a smart card

BlackBerry 10 devices support using S/MIME protection with a smart card and include tools to import certificates onto devices. To use S/MIME protection with a smart card, a user needs to bind the device with the smart card.

After the user binds the device with the smart card, the user can see the list of S/MIME certificates that are stored on the smart card and choose which ones to import into the certificate store on the device. The private keys remain on the smart card. To sign messages or decrypt them, the device must be bound to the smart card.

PGP

Users can use PGP to sign, encrypt, or sign and encrypt messages that they send using a work email account that supports PGP protected messages on devices that are running BlackBerry 10 OS version 10.3.1 or later.

BlackBerry UEM supports the OpenPGP format on devices. For more information about the OpenPGP format, see RFC 4880.

Keys and certificates in the PEM (.pem, .cer) and ASC (.asc, .cer) file formats and file name extensions are supported.

Users can configure PGP preferences, including choosing PGP keys and encoding methods, in the device settings. Devices support attachments in PGP protected email messages. Users can view, send, and forward attachments in PGP protected email messages.

If users don't have their PGP private keys on their devices, the devices can't read PGP protected email messages.

If your devices are managed by BlackBerry UEM, you can control PGP options on devices. For example, BlackBerry UEM allows you to specify whether devices can send PGP protected email messages.

PGP public and private keys

BlackBerry 10 devices use public key cryptography with PGP public keys and private keys to send and receive PGP protected email messages.

Key	Description
PGP public key	When a user sends an email message from a device, the device uses the PGP public key of the recipient to encrypt the message. When a user receives a signed email message on a device, the device uses the PGP public key of the sender to verify the message signature.

Key	Description
	The PGP public key is designed so that recipients and senders can distribute and access the key without compromising it. The PGP public key is usually stored on your organization’s Symantec Encryption Management Server.
PGP private key	When a user sends a signed email message from a device, the device uses the PGP private key of the user to digitally sign the email message. When a user receives an encrypted email message on a device, the device uses the PGP private key of the user to decrypt the message. The private key is stored on the device.

PGP encryption algorithms

When you or a user turns on PGP encryption on BlackBerry 10 devices, the devices can use any of the following algorithms to encrypt email messages: AES-256, AES-192, AES-128, Triple DES-168, and CAST-128.

The PGP public key of the recipient indicates which encryption algorithms the recipient's email application supports. The device is designed to use the strongest encryption algorithm available. By default, if the PGP public key of the recipient doesn't include a list of encryption algorithms, the device encrypts the email message using one of the algorithms in the following order of priority: AES-256, AES-192, AES-128, Triple DES-168, and CAST-128.

Data flow: Sending an email message from a BlackBerry 10 device using PGP encryption

1. A user sends an email message from a BlackBerry 10 device using PGP encryption. The device performs the following actions:
   a. The device checks the device keystore for the PGP public key of the recipient.
   b. If the device keystore doesn't include the PGP public key of the recipient, the device retrieves the PGP public key of the recipient from the Symantec Encryption Management Server.
   c. The device encrypts the email message using the PGP public key of the recipient.
   d. If the device is connected to the BlackBerry Infrastructure, the device uses BlackBerry transport layer encryption to encrypt the PGP encrypted message.
   e. The device sends the encrypted message to BlackBerry UEM.
2. If the device is connected to the BlackBerry Infrastructure, BlackBerry UEM decrypts the BlackBerry transport layer encryption.
3. BlackBerry UEM sends the PGP encrypted message to the mail server.
4. The mail server sends the PGP encrypted message to the recipient.
5. The recipient's device decrypts the PGP encrypted message using the recipient's PGP private key.

Retrieving PGP keys from a Symantec Encryption Management Server

If your organization’s environment includes a Symantec Encryption Management Server, you can require BlackBerry 10 device users to enroll their devices with this server using the “Symantec Encryption Management Server address” setting in the Email profile. You can also specify whether users must use their work email address or their Microsoft Active Directory credentials to enroll devices with this server. Users must submit their enrollment information and then devices must enroll, authenticate, and communicate with the specified server before users can use PGP protection on their devices.

After users enroll their devices with the server, devices can access PGP keys and PGP key status, as well as retrieve and enforce the email policy of the Symantec Encryption Management Server for all email messages that the user sends.

IBM Notes email encryption

If your organization's environment includes IBM Notes or IBM Domino, BlackBerry 10 devices that have IBM Notes Traveler installed can send and receive email messages that are encrypted using IBM Notes email encryption.

When users send, forward, or reply to email messages, users can indicate whether the Notes Traveler server must encrypt the message before it sends the message to recipients. Devices and the Notes Traveler server send all data to each other over a TLS connection.

Users can turn on IBM Notes email encryption using device settings.

For more information about supported Notes Traveler versions, http://help.blackberry.com/detectLang/blackberry-uem-compatibility-matrix/current/.

Message classification

Message classification allows your organization to specify and enforce secure email policies and add visual markings to email messages on BlackBerry 10 devices. You can use BlackBerry UEM to provide BlackBerry 10 device users with similar options for message classification that you make available on their computer email applications. You can define the following rules to apply to outgoing messages, based on the messages' classifications:

- Add a label to identify the message classification (for example, Confidential)
- Add a visual marker to the end of the subject line (for example, [C])
- Add text to the beginning or end of the body of an email (for example, This message has been classified as Confidential)
- Set S/MIME or PGP options (for example, sign and encrypt)
- Set a default classification

For devices that are running BlackBerry 10 OS version 10.3.1 and later, you can use message classification to require users to sign, encrypt, or sign and encrypt email messages, or add visual markings to email messages that they send from their devices. You can use BlackBerry UEM to specify a message classification configuration file to send to a user’s device. The device then interprets and implements the contents of the message classification configuration file. When the user either replies to an email message that has message classification set or composes a secure email message, the message classification configuration determines the classification rules that the device must enforce on the outgoing message.

Users can raise, but not lower, the message classification levels on their devices. The message classification levels are determined by the secure email rules of each classification.

Providing devices with single sign-on access to your organization's network

You can allow the browser and apps in the work space on BlackBerry 10 devices to authenticate automatically with domains and web services in your organization’s network.

Single sign-on authentication can use a user’s login information or certificate. Certificate-based authentication is supported for BlackBerry 10 devices. After you assign a single sign-on profile to a user, the user's login information is saved on the device the first time they access a domain specified in the profile. The user's saved credentials are used automatically when the user tries to access any of the domains specified in the profile. The user isn't prompted again for credentials until the user's password changes or the certificate expires.

BlackBerry UEM supports the following single sign-on authentication types: Kerberos, NTLM, and certificate-based authentication.

Using Kerberos to provide single sign-on from devices

If your organization uses Kerberos to provide single sign-on access, you can provide users with single sign-on access to your organization's resources from the browser and apps in the work space on their BlackBerry 10 devices.

When Kerberos is used with devices, if a valid TGT is available on the devices, users aren't prompted for login information when they access your organization's internal resources from the browser and apps in the work space. If users are connected to your organization using a VPN connection, the VPN gateway must permit traffic to the KDC to pass through for users to have access without providing login information.

To use Kerberos with devices, you specify your organization's Kerberos configuration file in a single sign-on profile.

Cryptography on devices

8

BlackBerry 10 devices support various types of cryptographic algorithms, codes, protocols, and APIs.

Symmetric encryption algorithms

Algorithm	Key length (in bits)	Modes
AES	128, 192, 256	CBC, CFB, ECB, OFB, CTR, CCM/CCM*, GCM, Key Wrap (RFC 3394)
AES	512	XTS
Blowfish	up to 256	CBC, CFB, ECB, OFB
Camellia	128, 192, 256	CBC, ECB
CAST	40 to 128	CBC, CFB, ECB, OFB
DES	56	CBC, CFB, ECB, OFB
DESX	184	CBC, CFB, ECB, OFB
RC2	up to 256	CBC, CFB, ECB, OFB
RC4	up to 256	—
Triple DES	112, 168	CBC, CFB, ECB, OFB

Asymmetric encryption algorithms

Algorithm	Supported curve or key length (in bits)
ECIES	secp192r1, secp256r1, secp384r1, secp521r1, sect163k1, sect283k1
RSA PKCS#1 v1.5 / PKCS#1 v2.1 (OAEP)	512, 1024, 2048, 4096

Hash algorithms

Algorithm	Digest size (in bits)
AES-MMO	128
MD2	128
MD4	128
MD5	128
MDC-2	128
RIPEMD-160	160
SHA-1	160
SHA-2	224, 256, 384, 512

Message authentication codes

Codes	Key length (in bits)
AES-XCBC-MAC	128
CMAC-AES	28, 192, 256
HMAC-MD5	128
HMAC-SHA-1	160
HMAC-SHA-2	224, 256, 384, 512
HMAC-RIPEMD-160	160

Signature algorithms

Algorithm	Supported curve or key length (in bits)
DSA (FIPS 186-3)	1024, 2048, 3072
ECDSA	secp192r1, secp256r1, secp384r1, secp521r1, sect163k1, sect283k1
ECQV	secp192r1, secp256r1, secp384r1, secp521r1, sect163k1, sect283k1
RSA PKCS#1 v1.5 / PKCS#1 v2.1 (PSS)	512, 1024, 2048, 4096

Key agreement algorithms

Algorithm	Supported curve or key length (in bits)
DH	1024, 2048, 3072
ECDH	secp192r1, secp256r1, secp384r1, secp521r1, sect163k1, sect283k1
ECMQV	secp192r1, secp256r1, secp384r1, secp521r1, sect163k1, sect283k1

Cryptographic protocols

BlackBerry 10 devices support various Internet, VPN, and Wi-Fi security protocols.

Internet security protocols

- DTLS 1.0
- SSL 2.0
- SSL 3.0

- TLS 1.0
- TLS 1.1
- TLS 1.2

VPN security protocols

- IKE
- IKEv2
- IPsec

Wi-Fi security protocols

- WEP
- WPA-Personal
- WPA-Enterprise
- WPA2-Personal
- WPA2-Enterprise

Cipher suites for SSL/TLS connections

BlackBerry 10 devices support various cipher suites for direct mode SSL/TLS when they open SSL/TLS connections to the BlackBerry Infrastructure or to web servers that are internal or external to your organization. The following cipher suites are supported:

- TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_DSS_WITH_DES_CBC_SHA
- TLS_DHE_DSS_WITH_SEED_CBC_SHA
- TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_SEED_CBC_SHA
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_RC4_128_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_RC4_128_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_PSK_WITH_3DES_EDE_CBC_SHA
- TLS_PSK_WITH_AES_128_CBC_SHA
- TLS_PSK_WITH_AES_256_CBC_SHA
- TLS_PSK_WITH_RC4_128_SHA
- TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
- TLS_RSA_EXPORT_WITH_RC4_40_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_SEED_CBC_SHA

Cryptographic libraries

- BlackBerry OS Cryptographic Library
- OpenSSL

VPN cryptographic support

Protocol	Authentication types	IKE IPSec DH group	IKE IPSec cipher	IKE IPSec hash	IKE PRF
IKE	PSK, PKI, XAUTH-PSK, XAUTH-PKI	1, 2, 5, 7 to 26	DES (56-bit key), Triple DES (168-bit key), AES (128, 192, 256-bit keys)	AES-XCBC, MD5, SHA-1, SHA-256, SHA-384, SHA-512	AES-XCBC, HMAC-MD5, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512
IKEv2	PSK, PKI, EAP-TLS, EAP-MS-CHAPv2	1, 2, 5, 7 to 26	DES (56-bit key), Triple DES (168-bit key), AES (128, 192, 256-bit key)	AES-XCBC, MD5, SHA-1, SHA-256, SHA-384, SHA-512	AES-XCBC, HMAC-MD5, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512

Wi-Fi cryptographic support

Cryptographic protocol	Encryption	EAP outer method	EAP inner method
WEP	RC4	—	—
WPA	TKIP	PEAP, EAP-TTLS, EAP-FAST, EAP-TLS, EAP-AKA, EAP-SIM	MSCHAPv2, EAP-GTC, PAP

Cryptographic protocol	Encryption	EAP outer method	EAP inner method
WPA2	TKIP, CCMP (AES)	PEAP, EAP-TTLS, EAP-FAST, EAP-TLS, EAP-AKA, EAP-SIM	MSCHAPv2, EAP-GTC, PAP

Related resources

9

For more information about using BlackBerry UEM to manage BlackBerry 10 devices, visit http://help.blackberry.com/detectLang/blackberry-uem-products/current/. Here, you can find information such as how to activate BlackBerry 10 devices, and manage them with IT policies, profiles, and IT administration commands.

Glossary 10

AES	Advanced Encryption Standard
AES-CCMP	Advanced Encryption Standard Counter Mode CBCMAC Protocol
AES-XCBC	Advanced Encryption Standard extended cipher block chaining
AES-XCBC-MAC	Advanced Encryption Standard extended cipher block chaining message authentication code
API	application programming interface
ARC4	Alleged Rivest's Cipher 4
BlackBerry signing authority system	The BlackBerry signing authority system is used by third-party developers to cryptographically sign their applications.
BlackBerry UEM instance	A BlackBerry UEM instance refers to one installation of the BlackBerry UEM Core and all associated BlackBerry UEM components that communicate with it. The components can be installed on the same server or multiple servers. There can be more than one BlackBerry UEM instance in a BlackBerry UEM domain.
CA	certification authority
CAC	Common Access Card
CAST	Carlisle Adams Stafford Tavares
CBC	cipher block chaining
CCKM	Cisco Centralized Key Management
CCM	Client Certificate Management
CFB	cipher feedback
CKIP	Cisco Key Integrity Protocol
CTR	Counter
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EAP-AKA	Extensible Authentication Protocol Authentication and Key Agreement
EAP-FAST	Extensible Authentication Protocol Flexible Authentication via Secure Tunneling

EAP-GTC	Extensible Authentication Protocol Generic Token Card
EAP-SIM	Extensible Authentication Protocol Subscriber Identity Module
EAP-MS-CHAP	Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol
EAP-TLS	Extensible Authentication Protocol Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol Tunneled Transport Layer Security
EAPoL	Extensible Authentication Protocol over LAN
ECB	electronic code book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Standard
ECMQV	Elliptic Curve Menezes-Qu-Vanstone
EDE	Encryption-Decryption-Encryption
FIPS	Federal Information Processing Standards
GCC	GNU Compiler Collection
GCM	Galois/Counter Mode
HMAC	keyed-hash message authentication code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
IT policy	An IT policy consists of various rules that control the security features and behavior of devices.
LAN	local area network
LED	light-emitting diode
MD	Message Digest Algorithm
MD5	Message-Digest Algorithm, version 5
MDC	Modification Detection Code
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NVRAM	nonvolatile random access memory
OBEX	Object Exchange

OFB	output feedback
PAC	Protected Access Credential
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail
PFX	Personal Information Exchange
PIV	Personal Identity Verification
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PSK	pre-shared key
RC	Rivest's Cipher
RFC	Request for Comments
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
SCEP	simple certificate enrollment protocol
SHA	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
space	A space is a distinct area of the device that enables the segregation and management of different types of data, applications, and network connections. Different spaces can have different rules for data storage, application permissions, and network routing. Spaces were formerly known as perimeters.
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
Triple DES	Triple Data Encryption Standard
UDP	User Datagram Protocol
UEM	Unified Endpoint Manager
VPN	virtual private network
WebDAV	Web Distributed Authoring and Versioning
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
XEX	Xor-Encrypt-Xor

XML	Extensible Markup Language
XTS	XEX-based Tweaked CodeBook mode with CipherText Stealing

Legal notice

Android is a trademark of Google Inc. Cisco is a trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. IBM, Domino, and Notes are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. IEEE, 802.11, 802.11i, and 802.1X are trademarks of the Institute of Electrical and Electronics Engineers, Inc. Microsoft, Active Directory, and Outlook are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Nginx is a trademark of Nginx Software Inc. OpenSSL is a trademark of the The OpenSSL Software Foundation, Inc. PGP is a trademark of PGP Corporation. RSA is a trademark of RSA Security. Symantec is a trademark or registered trademark of Symantec Corporation or its affiliates in the U.S. and other countries. Wi-Fi, WPA, and WPA2 are trademarks of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available 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
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada