Security Technical Overview

BES10 Cloud Solution Market Preview

Published: 2014-04-22
SWD-20140422090823041

Contents

Introduction

Secure

About this guide

BES10 Cloud helps you manage BlackBerry 10, Android, and iOS devices in your organization's environment. This guide describes how BES10 Cloud delivers a higher level of control and security to devices.

This guide is intended for senior IT professionals responsible for evaluating the product and planning its deployment, as well as anyone who's interested in learning more about BES10 Cloud solution security. After you read this guide, you should understand how BES10 Cloud can help protect data at rest, data in transit, and apps for your organization.

What is BES10 Cloud?

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

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

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

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

Key features of BES10 Cloud

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

Key security features of the BES10 Cloud solution

Feature	Description
IT administration commands, IT policies, and profiles	BES10 Cloud provides you with administrative control of device behaviour.
Control of device access to your organization's network	BES10 Cloud allows you to send work Wi-Fi profiles and work VPN profiles to devices so that those devices can connect to your organization's network.
Protection of company directory data	If you allow BES10 Cloud to access your company directory, the BlackBerry Cloud Connector sends your company directory information to BES10 Cloud over a secure TLS connection.
Protection of device user information	You or users can delete work data or all data from devices.
Protection of data between BES10 Cloud and devices	Data that is in transit between BES10 Cloud and devices is protected using transport layer encryption (using AES-256) and TLS.
Protection of work data on BlackBerry 10 devices	BlackBerry devices: • protect work data using XTS-AES-256 encryption. • isolate the work and personal file systems. • isolate work and personal apps.
Protection of personal data on BlackBerry 10 devices	You or users can require that BlackBerry 10 devices encrypt the data stored in the personal file system. The device encrypts the personal data using XTS-AES-256 encryption.
Protection of media card data on BlackBerry 10 devices	You or users can require that BlackBerry 10 devices encrypt the data stored on media cards.
Protection of the BlackBerry 10 OS	The BlackBerry 10 OS: • Protects app data using sandboxing • Protects resources • Manages permissions to access capabilities • Verifies the boot loader code
Enforcement of device standards for iOS and Android devices	Compliance profiles allow you to encourage iOS and Android device users to follow your organization's standards for jailbroken and rooted devices and for required and installed apps.

Hardware and OS security

Hardware root of trust for BlackBerry devices

BlackBerry ensures the integrity of BlackBerry 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 so that it's very difficult to remove or bypass this security. 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 are manufactured by BlackBerry and 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's 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

The base file system is read-only and contains system files. Because the base file system is read-only, the BlackBerry 10 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.

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 BlackBerry 10 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 BlackBerry 10 device 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 BlackBerry 10 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 BlackBerry 10 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 six security mechanisms listed below.

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.

Activating and managing devices

Multiplatform

Activating devices

Device activation associates the device with a user account in BES10 Cloud and establishes a secure communication channel between the device and BES10 Cloud.

BES10 Cloud allows multiple devices to be activated for the same user account. More than one active iOS, Android, and BlackBerry 10 device can be associated with a user account.

All device types consume a license when activated.

By default, a user can activate a device using any of the following connections:

- Over your work Wi-Fi network with a connection to the BlackBerry Infrastructure
- Over any Wi-Fi connection or mobile network using a VPN connection with a connection to the BlackBerry Infrastructure
- Over any Wi-Fi connection or mobile network through the BlackBerry Infrastructure

After the activation process completes, BES10 Cloud can send apps, profiles, and IT policies to the device. If an Exchange ActiveSync profile is configured, the user can send and receive work email messages using the device.

Activating devices over the wireless network

You can allow a user to activate a device over the wireless network using the following methods:

- A work Wi-Fi connection or a VPN connection to the BlackBerry Infrastructure
- Any Wi-Fi connection or mobile network connection through to the BlackBerry Infrastructure

Users can activate a device after they receive an activation email message from BES10 Cloud, or they can log in to BES10 Self-Service and request an activation password.

Your organization's activation information is registered automatically with the BlackBerry Infrastructure. The username and your organization's BES10 Cloud address is sent to and stored in the BlackBerry Infrastructure. Users who activate a BlackBerry 10 device don't need to know the BES10 Cloud address, and only need to provide their work email address and activation password to activate a device. Users who activate an iOS or Android device still require the BES10 Cloud address.

When a BlackBerry 10 user starts the activation process, if the device has been previously activated, the device displays a warning message to indicate that the work apps and data on the device will be deleted. When the user confirms that the device should be activated, the existing work space is deleted and a new work space is created.

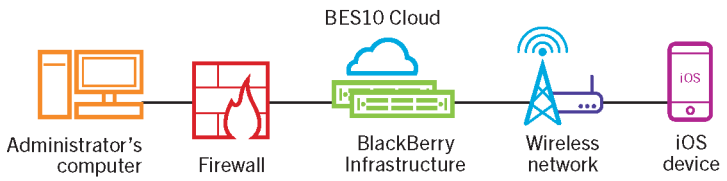
Activation passwords

You can specify the default period of time that an activation password remains valid for before it expires. You can also specify the default password length for the automatically generated password that is sent to users in the activation email message.

The value that you enter for the activation period expiration appears as the default setting in the "Activation period expiration" field when you add a user account to BES10 Cloud.

The activation period expiration can be 1 minute to 30 days, and the length of the automatically generated password can be 4 to 16 characters.

Data flow: Activating an iOS device



1. You perform the following actions:
   a. Add a user to BES10 Cloud as a local user account, or by using the account information retrieved from your company directory
   b. Assign an activation profile to the user
   c. Use one of the following options to provide the user with activation details:
      - Automatically generate a device activation password and send an email with activation instructions for the user
      - Set a device activation password and communicate the username, password, and activation URL to the user directory or by email
      - Don't set a device activation password and communicate the BES10 Self-Service address to the user so that they can set their own activation password
2. The user downloads and installs the BES10 Client on their device. Once installed, the user launches the BES10 Client and enters the activation URL.
3. The BES10 Client establishes a connection to BES10 Cloud.
4. BES10 Cloud prompts the user to accept the BES10 Cloud certificate. This prompt includes information about the SSL certificate, including the Common Name, fingerprint, and whether the certificate is trusted or untrusted. If the certificate has been preinstalled on the device, it will be trusted; otherwise it will be untrusted.
5. The user accepts the certificate and enters their username and password on the device.
6. The BES10 Client sends an activation request to BES10 Cloud. The activation request includes the username, password, device operating system, and unique device identifier.
7. BES10 Cloud performs following actions:
   a. Inspects the credentials for validity
   b. Creates a device instance
   c. Associates the device instance with the specified user account in the BES10 Cloud database
   d. Adds the enrollment session ID to an HTTP session
   e. Sends a successful authentication message to the device
8. The BES10 Client creates a CSR using the information provided by BES10 Cloud and sends a client certificate request over HTTPS.
9. BES10 Cloud performs the following actions:

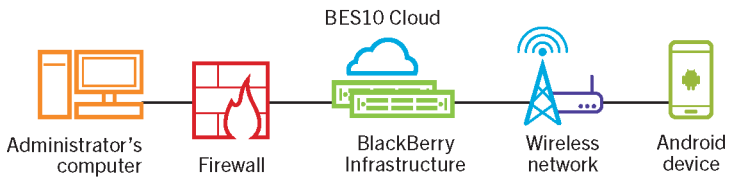
a Validates the client certificate request against the enrollment session ID in the HTTP session

b Signs the client certificate request with the root certificate

c Sends the signed client certificate and root certificate back to the BES10 Client

10. A mutually authenticated TLS session is established between the BES10 Client and BES10 Cloud.
11. The BES10 Client displays a message to inform the user that a certificate must be installed to complete the activation.
12. The user clicks OK and is redirected to the link for the MDM Daemon enrollment.
13. The BES10 Client establishes a connection to the MDM provider in BES10 Cloud.
14. BES10 Cloud provides the MDM profile to the BES10 Client. This profile contains the MDM enrollment URL and the challenge. The MDM profile is wrapped as a PKCS#7 signed message that includes the full certificate chain of the signer, which allows the device to validate the profile. This triggers the enrollment process.
15. The MDM Daemon on the device sends the device profile, including the customer ID, language, and OS version, to BES10 Cloud.
16. BES10 Cloud validates that the request was signed by a CA and responds to the MDM Daemon with a successful authentication notification.
17. The MDM Daemon sends a request to BES10 Cloud asking for the CA certificate, CA capabilities information, and a device issued certificate.
18. BES10 Cloud sends the CA certificate, CA capabilities information, and the device issued certificate to the MDM Daemon.
19. The MDM Daemon installs the MDM profile on the device.
20. The BES10 Client notifies BES10 Cloud of the successful installation of the MDM profile and certificate and polls BES10 Cloud periodically until it acknowledges that the MDM enrollment is complete.
21. BES10 Cloud acknowledges that the MDM enrollment is complete.
22. The BES10 Client requests all configuration information and sends the device and software information to BES10 Cloud.
23. BES10 Cloud stores the device information in the database and sends the requested configuration information to the device.
24. The device sends an acknowledgment to BES10 Cloud that it received the configuration information. The activation process is complete.

Data flow: Activating an Android device



1. You perform the following actions:

a Add a user to BES10 Cloud as a local user account, or by using the account information retrieved from your company directory

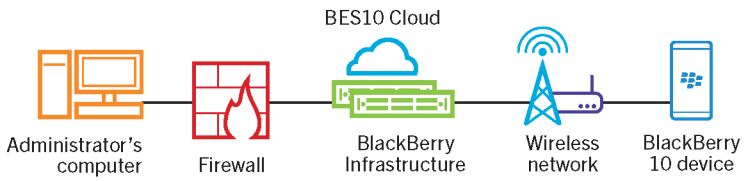
b Assign an activation profile to the user

c Use one of the following options to provide the user with activation details:

- Automatically generate a device activation password and send an email with activation instructions for the user
- Set a device activation password and communicate the username, password, and activation URL to the user directory or by email
- Don't set a device activation password and communicate the BES10 Self-Service address to the user so that they can set their own activation password

2. The user downloads and installs the BES10 Client on their device. Once installed, the user launches the BES10 Client and enters the activation URL.
3. The BES10 Client establishes a connection to BES10 Cloud.
4. BES10 Cloud prompts the user to accept the BES10 Cloud certificate. This prompt includes information about the SSL certificate, including the Common Name, fingerprint, and whether the certificate is trusted or untrusted. If the certificate has been preinstalled on the device, it will be trusted; otherwise it will be untrusted.
5. The user accepts the certificate and enters their username and password on the device.
6. The BES10 Client sends an activation request to BES10 Cloud. The activation request includes the username, password, device operating system, and unique device identifier.
7. BES10 Cloud performs following actions:
   a Inspects the credentials for validity
   b Creates a device instance
   c Associates the device instance with the specified user account in the BES10 Cloud database
   d Adds the enrollment session ID to an HTTP session
   e Sends a successful authentication message to the device
8. The BES10 Client creates a CSR using the information provided by BES10 Cloud and sends a client certificate request to BES10 Cloud over HTTPS.
9. BES10 Cloud performs the following actions:
   a Validates the client certificate request against the enrollment session ID in the HTTP session
   b Signs the client certificate request with the root certificate
   c Sends the signed client certificate and root certificate back to the BES10 Client
10. A mutually authenticated TLS session is established between the BES10 Client and BES10 Cloud.
11. The BES10 Client requests all configuration information and sends the device and software information to BES10 Cloud.
12. BES10 Cloud stores the device information in the database and sends the requested configuration information to the device.
13. The device sends an acknowledgment to BES10 Cloud that it received the configuration information. The activation process is complete.

Data flow: Activating a BlackBerry 10 device



1. You perform the following actions:
   a. Add a user to BES10 Cloud as a local user account, or by using the account information retrieved from your company directory
   b. Assign an activation profile to the user
   c. Use one of the following options to provide the user with activation details:
      - Automatically generate a device activation password and send an email with activation instructions for the user
      - Set a device activation password and communicate the username and password to the user directly or by email
      - Don't set a device activation password and communicate the BES10 Self-Service address to the user so that they can set their own activation password
2. The user types their username and activation password on the device.
3. The Enterprise Management Agent on the device performs the following actions:
   a. Establishes a connection to the BlackBerry Infrastructure
   b. Sends an activation request to the BlackBerry Infrastructure
4. The BlackBerry Infrastructure performs the following actions:
   a. Verifies that the user is a valid, registered user
   b. Retrieves the BES10 Cloud address for the user
   c. Sends the address to the Enterprise Management Agent
5. The Enterprise Management Agent performs the following actions:
   a. Establishes a connection with BES10 Cloud
   b. Generates a shared symmetric key with BES10 Cloud, using the activation password and EC-SPEKE. The shared symmetric key protects the CSR and response.
   c. Creates an encrypted CSR and HMAC by:
      - Generating a key pair for the certificate
      - Creating a PKCS#10 CSR that includes the public key of the key pair
      - Encrypting the CSR using the shared symmetric key and AES-256 in CBC mode with PKCS#5 padding

- Computing an HMAC of the encrypted CSR using SHA-256 and appending it to the CSR

d Sends the encrypted CSR and HMAC to BES10 Cloud

6. BES10 Cloud performs the following actions:
   a Verifies the HMAC of the encrypted CSR and decrypts the CSR using the shared symmetric key
   b Retrieves the username, work space ID, and your organization's name from the BES10 Cloud database
   c Packages a client certificate using the information it retrieved and the CSR that the Enterprise Management Agent sent
   d Signs the client certificate using the enterprise management root certificate
   e Encrypts the client certificate, enterprise management root certificate, and the BES10 Cloud URL using the shared symmetric key and AES-256 in CBC mode with PKCS#5 padding
   f Computes an HMAC of the encrypted client certificate, enterprise management root certificate, and the BES10 Cloud URL and appends it to the encrypted data
   g Sends the encrypted data and HMAC to the Enterprise Management Agent
7. The Enterprise Management Agent performs the following actions:
   a Verifies the HMAC
   b Decrypts the data it received from BES10 Cloud
   c Stores the client certificate and the enterprise management root certificate in its keystore
8. The Enterprise Management Agent and BES10 Cloud perform the following actions:
   a Establish a mutually authenticated TLS connection by verifying both the client certificate and the server certificate for BES10 Cloud using the enterprise management root certificate
   b Generate the device transport key using ECMQV and the authenticated long-term public keys from the client certificate and the server certificate for BES10 Cloud
9. The Enterprise Management Agent stores the device transport key in its keystore.
10. BES10 Cloud stores the device transport key in the database and sends the IT policy, SRP information, profiles, and software configurations to the device over TLS.
11. The Enterprise Management Agent sends an acknowledgment to BES10 Cloud over TLS, that it received the IT policy and other data. The activation process is complete.

The elliptic curve protocols used during the activation process use the NIST-recommended 521-bit curve.

Using IT policies to manage security

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

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

Only one IT policy can be assigned to each user account, and the same IT policy is sent to all of the user's devices. If an IT policy isn't assigned to a user account or to a group that a user belongs to, BES10 Cloud sends the Default IT policy to the user's devices.

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

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

Using compliance profiles to enforce standards for iOS and Android devices

You can use compliance profiles to encourage iOS and Android device users to follow your organization's standards for the use of mobile devices. A compliance profile specifies the device conditions that aren't acceptable in your organization, the notification messages sent to users, and the actions taken if a device is non-compliant.

You can specify whether the following conditions are permitted:

- Jailbroken or rooted device
- Non-assigned app is installed
- Required app isn't installed

You can also specify how BES10 Cloud responds when a device violates compliance rules. Actions can include the following:

- Send an email message to the user
- Display a notification message on the device
- Prevent the user from accessing the organization's resources and apps from the device, either immediately or after a period of time
- Delete work data from the device, either immediately or after a period of time
- Delete all data from the device, either immediately or after a period of time

For more information, see the *BES10 Cloud Administration Guide*.

Data in transit

Secure

How devices connect to your organization's network

You can use Wi-Fi and VPN profiles to configure how devices connect with your organization's network. By default, devices attempt to connect to your organization's network using the following communication methods, in order:

1. Work VPN profiles that you configure (BlackBerry 10 and iOS devices only)
2. Work Wi-Fi profiles that you configure
3. Personal VPN profiles and personal Wi-Fi profiles that a user configures on the device

By default, work apps on the device can also use any of these methods to access the resources in your organization's environment (for example, mail servers, web servers, and content servers).

For more information about configuring Wi-Fi and VPN profiles, see the *BES10 Cloud Administration Guide*.

Protecting Wi-Fi connections

You can use Wi-Fi profiles to send Wi-Fi configuration information, including security settings and any required certificates to devices.

To permit a device to access your work Wi-Fi network, you must send sensitive Wi-Fi information such as encryption keys and passwords to the device using Wi-Fi profiles. After the device receives the sensitive Wi-Fi information, the device encrypts the encryption keys and passwords and stores them in flash memory.

Using a VPN

If your organization's environment includes VPNs, such as IPSec VPNs or SSL VPNs, you can configure BlackBerry 10 and iOS devices to authenticate with the VPN to access your organization's network. A VPN provides an encrypted tunnel between a device and the network.

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 a 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.

Types of encryption used for Wi-Fi and VPN connections

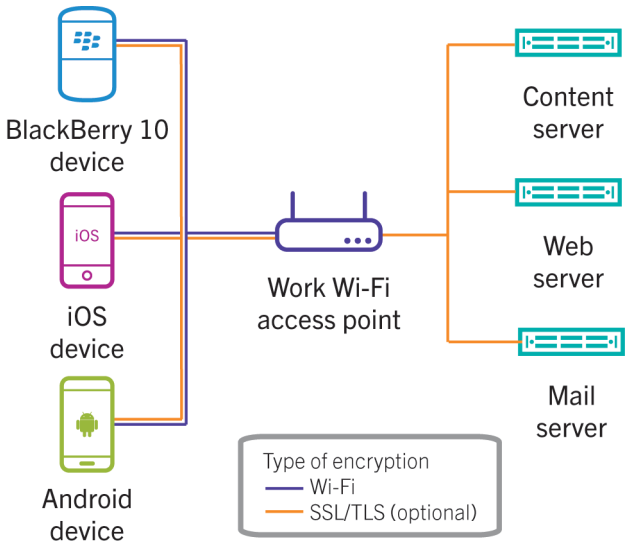
Communication between a device and your organization's resources can use various types of encryption. The type of encryption used depends on the connection method.

Encryption type	Description
Wi-Fi encryption (IEEE 802.11)	Wi-Fi encryption is used for data in transit between a device and wireless access point if the wireless access point was set up to use Wi-Fi encryption.
VPN encryption	VPN encryption is used for data in transit between a device and a VPN server.

Encryption type	Description
SSL/TLS encryption	SSL/TLS encryption is used for data in transit between a device and content server, web server, or mail server in your organization. The encryption for this connection must be set up separately on each server and uses a separate certificate with each server. The server might use SSL or TLS, depending how it is set up.

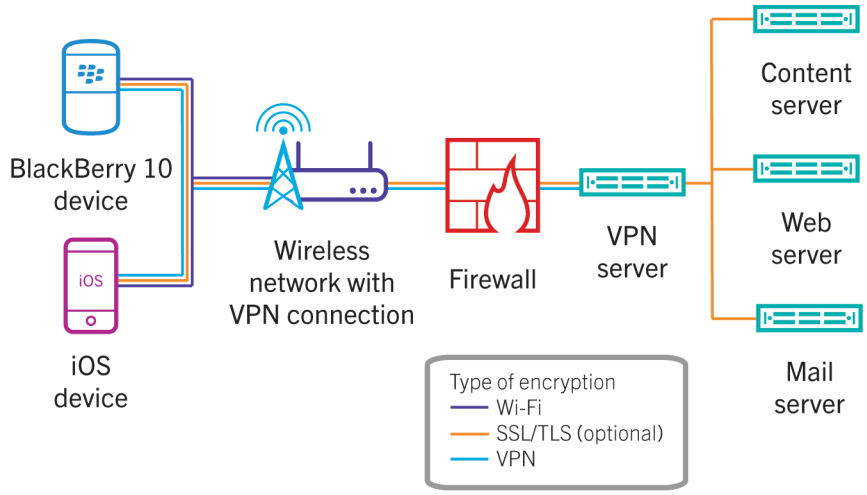
Work Wi-Fi connection

In a work Wi-Fi connection, a device connects to your organization's resources using the settings that you configured in a Wi-Fi profile. Wi-Fi encryption is used if the wireless access point was set up to use it.



VPN connection

In a VPN connection, a BlackBerry 10 or iOS device connects 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 was set up to use it.



Protecting email and organizer data

Devices use Exchange ActiveSync to synchronize email messages, calendar entries, and contacts with your organization’s mail server. You can use Exchange ActiveSync profiles to specify how devices connect to your organization's mail server. Devices can use certificate-based authentication with the mail server.

When users send and receive email messages, the data travels over one of the following communication paths:

- A direct connection from the device to the mail server through your VPN or over your work Wi-Fi network
- A direct connection from the device to a mail server that is located in a DMZ or is exposed to the public network

Messages and organizer data in transit between devices and your mail server aren't routed through BES10 Cloud.

Protecting data in transit between BES10 Cloud and devices

When you send configuration information, such as IT polices, profiles, and app configurations to devices, BES10 Cloud uses SSL to protect the data in transit between itself and devices.

Protecting data in transit between BES10 Cloud and iOS and Android devices

BES10 Cloud protects the data in transit between itself and iOS and Android devices.

During the activation process for iOS and Android devices, a client certificate, signed by the enterprise management root certificate, is issued to the device and a mutually authenticated TLS connection is established between BES10 Cloud and the BES10 Client on the device. When BES10 Cloud sends configuration information to an iOS or Android device, the data is protected by client and server certificates over the mutually authenticated TLS connection.

Related information

Data flow: Activating an iOS device, on page 21
Data flow: Activating an Android device, on page 22

Protecting data in transit between BES10 Cloud and BlackBerry 10 devices

BES10 Cloud protects the data in transit between itself and BlackBerry 10 devices.

During the activation process for BlackBerry 10 devices, an EEC client certificate, signed by the enterprise management root certificate, is issued to the device and a mutually authenticated TLS connection is established between BES10 Cloud and the device. When BES10 Cloud sends configuration information to a BlackBerry 10 device, the data is protected by client and server certificates over the mutually authenticated TLS connection.

Related information

Data flow: Activating a BlackBerry 10 device, on page 24

Protecting data in transit between BES10 Cloud and your company directory

The BlackBerry Cloud Connector is an optional component that you can install behind your organization's firewall to provide a secure connection between BES10 Cloud and your company directory.

If you use the BlackBerry Cloud Connector to give BES10 Cloud access to your company directory, you can create user accounts by searching for and importing user data from the directory and you can allow users to use their directory credentials to access BES10 Self-Service. BES10 Cloud synchronizes user data with the directory daily. You can also start the synchronization process manually for individual users.

For more information about configuring the BlackBerry Cloud Connector, see the *BES10 Cloud Administration Guide*.

Data flow: Establishing a secure connection between BES10 Cloud and the BlackBerry Cloud Connector

1. You download the installation and activation files using the administration console and install the BlackBerry Cloud Connector on a computer that can access the Internet and your company directory.
2. The BlackBerry Cloud Connector establishes a connection with BES10 Cloud and sends an activation request.
3. BES10 Cloud verifies that the activation information is valid.
4. The BlackBerry Cloud Connector and BES10 Cloud generate a shared symmetric key using the activation password and EC-SPEKE. The shared symmetric key protects the CSR and response.
5. The BlackBerry Cloud Connector performs the following actions:
    a. Generates a key pair for the certificate
    b. Creates a PKCS#10 CSR that includes the public key of the key pair
    c. Encrypts the CSR using the shared symmetric key and AES-256 in CBC mode with PKCS #5 padding
    d. Computes an HMAC of the encrypted CSR using SHA-256 and appends it to the CSR
    e. Sends the encrypted CSR and HMAC to BES10 Cloud
6. BES10 Cloud performs the following actions:
    a. Verifies the HMAC of the encrypted CSR and decrypts the CSR using the shared symmetric key
    b. Packages a client certificate using your organization's information and the CSR that the BlackBerry Cloud Connector sent
    c. Signs the client certificate using the enterprise management root certificate
    d. Encrypts the client certificate, enterprise management root certificate, and the BES10 Cloud URL using the shared symmetric key and AES-256 in CBC mode with PKCS #5 padding
    e. Computes an HMAC of the encrypted client certificate, enterprise management root certificate, and the BES10 Cloud URL and appends it to the encrypted data
    f. Sends the encrypted data and HMAC to the BlackBerry Cloud Connector

7. The BlackBerry Cloud Connector performs the following actions:
    a. Verifies the HMAC
    b. Decrypts the data it received from BES10 Cloud
    c. Stores the client certificate and the enterprise management root certificate in its keystore
    d. Establishes a TLS connection with BES10 Cloud
    e. Creates a registration request that includes the tenant ID, the client certificate signed with its private key using SHA1 and ECDSA, and the time stamp of the signing action
    f. Sends the registration request to BES10 Cloud
8. BES10 Cloud performs the following actions:
    a. Validates the registration request
    b. Ensures that the time stamp of the signing action isn't older than 3 minutes
    c. Performs one of the following actions:
        - If the validation is successful, registers the BlackBerry Cloud Connector instance and sends the BlackBerry Cloud Connector an authorization token that the BlackBerry Cloud Connector uses for subsequent connections with BES10 Cloud.
        - If the validation fails, BES10 Cloud closes the TLS connection with the BlackBerry Cloud Connector.

After the BlackBerry Cloud Connector is activated and registration is complete, when BES10 Cloud sends a directory request to the BlackBerry Cloud Connector, a mutually authenticated TLS connection is established using the trusted certificates and the authorization token and the BlackBerry Cloud Connector sends your company directory information to BES10 Cloud over the secure TLS connection.

Managing 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 a device.

A device can use certificates to:

- Authenticate using SSL/TLS when it connects to webpages that use HTTPS
- Authenticate with a work Wi-Fi network or VPN
- Encrypt and sign email messages using S/MIME protection (BlackBerry 10 and iOS devices only)

Sending CA certificates to devices

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

When the CA certificates for 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. For more information see the *BES10 Cloud Administration Guide*.

CA certificate stores on BlackBerry 10 devices

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

Store	Description
Browser certificate store	The work browser on BlackBerry 10 devices uses the certificates in this store to establish SSL connections with servers in your organization's environment. Devices that are running BlackBerry 10 OS version 10.0 also use the certificates in this store to authenticate S/MIME-protected email messages that are received.
VPN certificate store	BlackBerry 10 devices use certificates in this store for VPN connections. You must set the "Trusted certificate source" setting in the VPN profile to "Trusted certificate store" to use the certificates in this store for work VPN connections.
Wi-Fi certificate store	BlackBerry 10 devices use certificates in this store for Wi-Fi connections. You must set the "Trusted certificate source" setting in the Wi-Fi profile to "Trusted certificate store" to use certificates in this store for work Wi-Fi connections.
Enterprise certificate store	Devices that are running BlackBerry 10 OS version 10.1 or later use certificates in this store to authenticate S/MIME-protected email messages that are received.

Sending client certificates to devices

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

Client certificates are used for many purposes, including allowing networks and servers to trust the device when making secure connections and for digital signatures on S/MIME-protected email messages.

You can send client certificates to BlackBerry 10 device users by email, and if users have the BlackBerry Smart Card Reader 2.0 and BlackBerry 10 version 10.2 or later devices, users can also import S/MIME certificates to devices from a smart card.

You can use shared certificate profiles and user certificate profiles to send client certificates to iOS and Android devices. For more information, see the *BES10 Cloud Administration Guide*.

Extending email security

BES10 Cloud and devices support the following secure messaging technologies:

- S/MIME protection: You can extend messaging security for BES10 Cloud and permit BlackBerry 10 and iOS device users to sign, encrypt, or sign and encrypt messages using S/MIME.
- IBM Notes email encryption: If your organization's environment includes IBM Notes or IBM Domino, devices that are running BlackBerry 10 OS version 10.2.1 or later that have IBM Notes Traveler version 9.0.0.1 or later installed can send and receive email messages that are encrypted using IBM Notes email encryption.

About S/MIME

You can extend messaging security for BES10 Cloud and permit users to send and receive S/MIME-protected email messages on BlackBerry 10 and iOS devices. Digitally signing or encrypting messages adds another level of security to email messages that users send or receive from their devices. If they use a work email account that supports S/MIME-protected messages on devices, users can digitally sign, encrypt, or sign and encrypt messages using S/MIME protection.

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 keeps messages confidential. When a user encrypts a message, the device uses the recipient's public key to encrypt the message. The recipient's device uses the recipient's private key to decrypt the message.

If devices don't have S/MIME support turned on, devices can't send signed or encrypted email messages. To send encrypted email messages, a user must have the recipient's public key on their device. To read encrypted email messages, a user must have their private key on their device or on a smart card. If users don't have their private keys on their devices, the devices can't read S/MIME-encrypted messages, and devices display an error message.

S/MIME for BlackBerry 10 devices

You can require BlackBerry 10 devices to sign, encrypt, or sign and encrypt messages using S/MIME protection when users send email messages using a work email address.

Devices support keys and certificates in the following file formats and file name extensions:

- PEM (.pem, .cer)
- DER (.der, .cer)
- PFX (.pfx, .p12)

Users can configure S/MIME preferences on devices in the BlackBerry Hub settings, including choosing certificates and encoding methods. Users can manage certificates on their devices in the "Security and Privacy" section of the "System Settings." Users can store their private keys on their devices or a smart card.

Devices support attachments in S/MIME-protected email messages. Users can view, send, and forward attachments in S/MIME-protected email messages.

Users can 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.

If users don't have their private keys on their devices, the devices can't read S/MIME-encrypted messages, and the devices display the message, "Unable to decode the message because you do not have the corresponding private key."

S/MIME settings for BlackBerry 10 devices

BES10 Cloud uses Exchange ActiveSync profiles to configure S/MIME settings on BlackBerry 10 devices. You can configure the following S/MIME settings:

Setting	Description
S/MIME support	You can specify whether S/MIME is enabled on a device. • Allow: Users can choose whether or not to enable S/MIME on the device. S/MIME isn't enabled on the device and must be enabled by users (default value). • Required: S/MIME is automatically enabled on the device and can't be disabled by users. • Disallow: S/MIME is automatically disabled on the device and can't be enabled by users.
Digitally signed S/MIME messages	You can make digital signing of outgoing messages allowed, required, or disallowed: • Allow: Users can choose whether or not to digitally sign S/MIME messages (default value). • Required: Users must send digitally signed messages. • Disallow: Users can't send digitally signed messages.
Encrypted S/MIME messages	You can make encryption of outgoing messages allowed, required, or disallowed: • Allow: Users can choose whether or not to encrypt messages (default value). • Required: Users must encrypt messages. • Disallow: Users can't encrypt messages.
Encryption algorithms	You can choose any or all of the following encryption algorithms that a device can use to encrypt S/MIME-protected email messages: • AES (256-bit) • AES (192-bit) • AES (128-bit) • Triple DES • RC2

If you set any of the S/MIME settings to "Required," you must make sure that users have their private keys on their devices or smart cards to sign or decrypt messages.

For more information about S/MIME setting descriptions, see the *BES10 Cloud Policy and Profile Reference Guide*. For information about managing S/MIME settings, see the *BES10 Cloud Administration Guide*.

S/MIME profile and device setting dependencies

The following table shows the dependencies between the S/MIME settings that you can configure in BES10 Cloud and the S/MIME settings that users can configure on BlackBerry 10 devices. Depending on what these are set to, the options in the Encoding drop-down list on devices change. Devices ignore the value for some settings if a higher priority setting (for example, the "S/MIME support" setting) conflicts with the value for that setting.

S/MIME support setting	Digitally signed S/MIME messages setting	Encrypted S/MIME messages setting	S/MIME settings on device	Encoding drop-down on device
Allowed	Allowed	Allowed	User can turn S/MIME on or off.	• Plain text • Sign (S/MIME) • Encrypt (S/MIME) • Sign and Encrypt (S/MIME)
	Allowed	Required	S/MIME is on. User can't turn it off.	• Encrypt (S/MIME) • Sign and Encrypt (S/MIME)
	Allowed	Disallowed	User can turn S/MIME on or off.	• Plain text • Sign (S/MIME)
	Required	Allowed	S/MIME is on. User can't turn it off.	• Sign (S/MIME) • Sign and Encrypt (S/MIME)
	Required	Required	S/MIME is on. User can't turn it off.	Sign and Encrypt (S/MIME)
	Required	Disallowed	S/MIME is on. User can't turn it off.	Sign (S/MIME)
	Disallowed	Allowed	User can turn S/MIME on or off.	• Plain text

S/MIME support setting	Digitally signed S/MIME messages setting	Encrypted S/MIME messages setting	S/MIME settings on device	Encoding drop-down on device
				• Encrypt (S/MIME)
	Disallowed	Required	S/MIME is on. User can't turn it off.	Encrypt (S/MIME)
	Disallowed	Disallowed	User can turn S/MIME on or off but can't encrypt or sign messages because the necessary profiles are set to Disallowed.	Plain text
Required	Allowed	Allowed	S/MIME is on. User can't turn it off.	• Sign (S/MIME) • Encrypt (S/MIME) • Sign and Encrypt (S/MIME)
	Allowed	Required	S/MIME is on. User can't turn it off.	• Encrypt (S/MIME) • Sign and Encrypt (S/MIME)
	Allowed	Disallowed	S/MIME is on. User can't turn it off.	Sign (S/MIME)
	Required	Allowed	S/MIME is on. User can't turn it off.	• Sign (S/MIME) • Sign and Encrypt (S/MIME)
	Required	Required	S/MIME is on. User can't turn it off.	Sign and Encrypt (S/MIME)
	Required	Disallowed	S/MIME is on. User can't turn it off.	Sign (S/MIME)
	Disallowed	Allowed	S/MIME is on. User can't turn it off.	Encrypt (S/MIME)

S/MIME support setting	Digitally signed S/MIME messages setting	Encrypted S/MIME messages setting	S/MIME settings on device	Encoding drop-down on device
	Disallowed	Required	S/MIME is on. User can't turn it off.	Encrypt (S/MIME)
	Disallowed (This setting is ignored)	Disallowed (This setting is ignored)	S/MIME is on. User can't turn it off.	• Sign (S/MIME) • Encrypt (S/MIME) • Sign and Encrypt (S/MIME)
Disallowed	Any setting is ignored	Any setting is ignored	S/MIME is off. User can't turn it on.	Plain text

For more information about S/MIME setting descriptions, see the *BES10 Cloud Policy and Profile Reference Guide*. For information about managing S/MIME settings, see the *BES10 Cloud Administration Guide*.

S/MIME certificates and private keys

BlackBerry 10 devices 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, SHA-2, or MD5. 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 can be stored on the device or a smart card.

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
- 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 device using S/MIME encryption

1. A user sends an email message from a BlackBerry 10 device. The device performs the following actions:
   a. Checks the device keystore for the S/MIME certificate of the recipient
   b. Encrypts the email message with the S/MIME certificate of the recipient
   c. If the device is connected to the BlackBerry Infrastructure, uses BlackBerry transport layer encryption to encrypt the S/MIME-encrypted message
   d. Sends the encrypted message to BES10 Cloud.
2. If the device is connected to the BlackBerry Infrastructure, BES10 Cloud decrypts the BlackBerry transport layer encryption.
3. BES10 Cloud sends the S/MIME-encrypted message to the recipient.
4. The recipient decrypts the S/MIME-encrypted message using their S/MIME private key.

Using S/MIME with a smart card

BlackBerry devices that are running BlackBerry 10 OS version 10.2 or later support using S/MIME with a smart card and include tools to import certificates onto devices. To use S/MIME 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.

S/MIME for iOS devices

You can permit iOS device users to sign, encrypt, or sign and encrypt messages using S/MIME protection when users send email messages using a work email address in the native iOS email app. You can't force iOS device users to use S/MIME.

Users can configure S/MIME preferences on devices, including choosing certificates and encoding methods. Users can store their private keys on their devices or a smart card. To use S/MIME, a user must enable S/MIME on the device and specify whether to encrypt, sign, or encrypt and sign emails.

If users don't have their private keys on their devices, the devices can't read S/MIME-encrypted messages, and devices display an error message.

S/MIME settings for iOS devices

BES10 Cloud uses Exchange ActiveSync profiles to configure S/MIME settings on iOS devices. You can configure the following S/MIME settings:

Setting	Description
Use S/MIME	You can specify whether users can use S/MIME to encrypt or sign email messages in the native iOS email app. You can't force users to use S/MIME.
Signing certificate	You can specify the shared certificate profile for a client certificate that users can use to digitally sign S/MIME-protected email messages. If you don't use this setting, users can still import certificates to their devices and use them to digitally sign S/MIME-protected email messages.
Encryption certificate	You can specify the shared certificate profile for a client certificate that users can use to encrypt S/MIME-protected email messages. If you don't use this setting, users can still import certificates to their devices and use them to encrypt S/MIME-protected email messages.

For more information about S/MIME setting descriptions, see the *BES10 Cloud Policy and Profile Reference Guide*. For information about managing S/MIME settings, see the *BES10 Cloud Administration Guide*.

IBM Notes email encryption for BlackBerry 10 devices

If your organization's environment includes IBM Notes or IBM Domino, BlackBerry devices that are running BlackBerry 10 OS version 10.2.1 or later, and that have IBM Notes Traveler version 9.0.0.1 or later 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 their device must encrypt the message before it sends the message to recipients.

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

Data at rest

Securing BlackBerry 10 devices for work and personal use

Your organization can use BlackBerry Balance technology to permit users to use BlackBerry 10 devices for both work and personal use. For example, your organization might want to permit users to activate their personal devices on BES10 Cloud or permit users to use devices that your organization provides for personal use.

BES10 Cloud 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 your organization's apps and data differently from personal apps and data. These features and options have the following benefits:

- Permit your organization to control access to your organization's 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 install and manage your organization's apps on devices
- 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

How work and personal spaces are separated

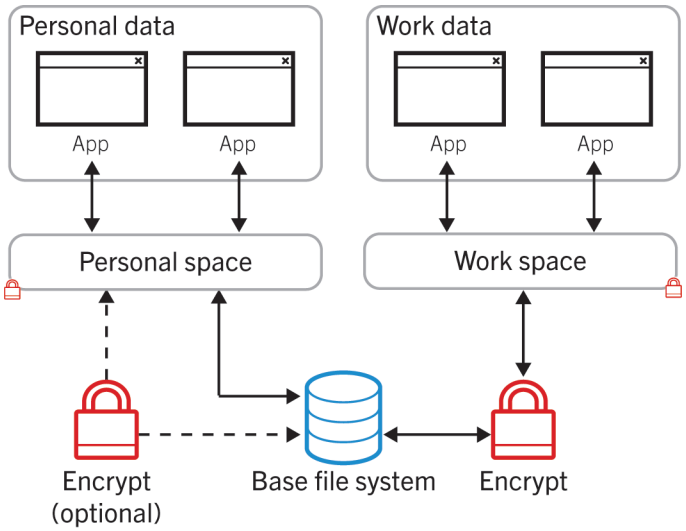
BlackBerry Balance separates and secures work and personal information on BlackBerry 10 devices that are activated on BES10 Cloud. BlackBerry Balance uses separate areas of the device called spaces to separate work and personal activities. A space is a distinct area of the device that enables the segregation and management of different types of data, apps, and network connections. Different spaces can have different rules for data storage, app permissions, and network routing. The separate spaces help users to avoid activities such as accidentally copying work data into a personal app, or displaying confidential work data during a BBM Video chat.

The device encrypts the work space during the activation process. You can use an IT policy rule to require the device to encrypt the personal space separately.

Devices that aren't activated on BES10 Cloud operate only a personal space. When you activate a BlackBerry 10 device on BES10 Cloud, a work space is created on the device. The personal space on the device remains intact during the activation process and any user data, apps, or network connections that the user was using before the device was activated are available to the user in the personal space on the device.

Retaining the original personal space on the device provides users with the opportunity to use devices for activities that your organization's security policies might not otherwise allow, such as downloading videos, playing online multi-player games, and uploading personal photos and Facebook entries, without exposing your organization's content that is stored in the work space.

The work space is a segregated area of the device for work resources that also provides a modified version of the BlackBerry World storefront called BlackBerry World for Work. BlackBerry World for Work contains the apps that your organization allows users to download and use at work. The work space also provides a segregated area of the device where users can create, edit, and save work documents and slide decks.



Securing work and personal apps and data on devices

Security features on both BES10 Cloud and BlackBerry 10 devices help to classify, protect, and manage work and personal apps and data on devices.

How devices classify work and personal apps and data

BlackBerry 10 devices can distinguish between data that is for work use and data that is for personal use. Devices classify data as work or personal data based on the source of the data, and these classifications determine how devices store, protect, and handle data on devices. For example, if data comes from a work account, it is stored in the work space on the device, and if data comes from a personal account, it is 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.

How devices classify apps and data

BlackBerry 10 devices classify work data as any data that is managed by apps in the work space and personal data as any data that is managed by apps in the personal space.

The following table describes each app classification and lists examples of apps that belong to each app classification:

Description	App
Apps that are available only in the work space and display only work data	• BlackBerry World for Work • Any apps deployed by your organization • 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 (with access to work contacts except if prevented by the "Allow personal apps to access work contacts" IT policy rule)

Description	App
	• BBM Video (with access to work contacts except if prevented by the "Allow personal apps to access work contacts" IT policy rule) • BlackBerry Newsstand • BlackBerry Story Maker • BlackBerry World • Calculator • Camera • Compass • Consumer Instant Messaging Apps • Facebook for BlackBerry devices • Phone • SMS text messaging (with access to work contacts except if prevented by the "Allow personal apps to access work contacts" IT policy rule) • Visual voice mail (with access to work contacts except if prevented by the "Allow personal apps to access work contacts" IT policy rule) • Weather • 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. For example, the BlackBerry Hub, Calendar, Contacts, BlackBerry Remember app, and the universal search 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 • Search
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	• Adobe Reader • Browser • Documents To Go

Description	App
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 is 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.	• File Manager • Help • Music • Pictures • Print To Go • Videos

How devices are designed to prevent BlackBerry Runtime for Android apps from accessing work apps and data

BlackBerry 10 devices classify 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. Android apps don't have access to the work apps or work data that are located in the work space.

How BES10 Cloud and devices protect work and personal apps and data

BlackBerry 10 devices protect work data by encrypting the files stored in the work space. Devices can also protect personal data by encrypting the files stored in the personal space if you or a user requires. Devices can also encrypt the files stored on media cards that are inserted in devices; only personal data can be saved to media cards. Devices encrypt only the contents of files; file and directory names aren't encrypted.

You can protect work data on devices further by requiring password protection and controlling when devices wipe their work space.

How devices protect work data

BlackBerry 10 devices encrypt data stored in the work 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 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 is 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 is 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

BlackBerry 10 devices allow the encryption of personal files on devices.

You can use the "Force personal space data encryption" IT policy rule to turn on encryption for the personal space of devices. If the "Force personal space data encryption" IT policy rule is selected, files stored in the personal space of the device are encrypted. If this rule isn't selected, users can choose to encrypt files in the personal space using the "Device Encryption" option in the "Security and Privacy" settings on the device.

If encryption is turned on for the personal space of the device, the device 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 is 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 is embedded in the processor when the processor is manufactured

If the "Force personal space data encryption" IT policy rule is selected, you should also select the "Apply work space password to full device" IT policy rule so that the work space password applies to the entire device. If the "Force personal space data encryption" IT policy rule isn't selected and the user chooses to turn on encryption for the personal space, the device prompts the user to type a new password if the device doesn't already have a password.

Devices can also encrypt all files stored on media cards that are inserted in devices. Users can save only personal data to media cards.

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.

Protecting data on media cards

BlackBerry 10 devices allow users to store only personal data on media cards and that data is stored in an unencrypted format.

Although users can't move or save work files to media cards, if your organization wants to ensure the security of files on them, you can require that devices encrypt all files stored on them using the "Force media card encryption" IT policy rule.

Protecting work data on devices with password rules

To secure work content and resources in the work space on BlackBerry 10 devices, devices require users to set a password for the work space by default. If you don't want users to have to enter a password to access work content and resources in the work space, the "Password required for work space" IT policy rule shouldn't be selected.

You can use IT policy rules to enforce either a password for the work space or the entire device and then control password requirements for that password, such as complexity and length.

Controlling when devices delete all data in the work space

To protect your organization's data on BlackBerry 10 devices, you can delete all work data from the device by wiping the work space and all of its contents. All personal data remains on the device. For example, you can do this if a user no longer works at your organization.

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 BES10 Cloud synchronizes with the user's work email account
BlackBerry Remember	All tasks and memos that BES10 Cloud 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 BES10 Cloud
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

How BES10 Cloud and devices manage work and personal apps and data

BlackBerry 10 devices are designed to separate work data from personal data to prevent users from compromising your organization's data on devices. You can also use BES10 Cloud and IT policy rules to manage work and personal apps and data on devices using the following security features:

- Send work space wallpaper to devices
- Control access to work and personal content on devices
- Manage sharing of work and personal files using the Share option
- Manage how apps open links in the work and personal spaces on devices
- Manage data transferred to and from devices using NFC
- Manage cloud storage apps in the work space on devices
- Transfer work data from devices using Bluetooth profiles
- Prevent users from sharing work data on devices when sharing the screen during BBM Video chats
- Prevent users from using voice control commands on devices
- Prevent users from using voice dictation within work apps on devices
- Control roaming on devices
- Control features on devices
- Control messaging on devices

Sending work space wallpaper to devices

To help users distinguish between the work space and the personal space on BlackBerry 10 devices, the home screen in each space displays different, visually distinct wallpapers by default. This gives users a strong visual indication of which space they are currently working in.

You can choose to apply a customized work wallpaper image file such as your organization's logo, for work space wallpaper. After you specify an image file for a device model, the Enterprise Management Web Service sends the work space wallpaper to the appropriate devices in the BES10 Cloud domain and users can't change their work space wallpaper to a different wallpaper image.

When users are in the work space on devices, they see the work space wallpaper. If you don't send a work space wallpaper image to devices, users can still set a different wallpaper image for the work space using the "Select Wallpaper" option in the "Display" settings, while in the work space. If a user selects an image file as their work space wallpaper, the device saves a copy of the image in case it's deleted or the media card that it's stored on is removed from the device. Users can set the personal space wallpaper using the "Select Wallpaper" option in the "Display" settings while in the personal space.

The work space wallpaper that you send to devices is stored in a protected folder that's separate from the folders that store other wallpaper images and is removed if the work space is removed.

For more information about sending work space wallpaper to devices, see the *BES10 Cloud Administration Guide*.

Controlling app access to work and personal content on devices

Files and data are stored in either the work space or personal space on BlackBerry 10 devices. 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. On devices that are running BlackBerry 10 OS version 10.2.1 or later, 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, visual voice mail, and voice dialing.

Managing sharing of work and personal files using the "Share" option on devices

BlackBerry 10 devices allow users to share personal files with work apps using the "Share" option. If users want to share personal files with work apps, the work space must be unlocked.

Users can share work files only with work apps using the "Share" option.

You can use the “Allow transfer of work data using NFC” and “Allow transfer of work files using Bluetooth OPP” IT policy rules to specify whether users can share work content using NFC or Bluetooth.

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 10 devices. For example, if users click on links in personal email messages, the browser in the personal space will open. In a few cases, work apps will 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 ensure 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 will 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.

Your organization may require that intranet links be opened in the browser in the work space. If you want links in work email messages to always open the browser in the work space make sure the "Allow opening links in work email messages in the personal browser" IT policy rule isn't selected.

Managing data transferred to and from a device using NFC

Data that a BlackBerry 10 device receives from another device 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 the 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 allow or prevent users from sharing work data in a file format (for example, pictures or documents) using NFC using the "Allow transfer of work files using Bluetooth OPP" IT policy rule. Regardless of how this IT policy rule is 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 the “Allow transfer of work data using NFC” IT policy rule to prevent users from sending work data to another NFC-enabled device using NFC.

Managing cloud storage apps in the work space on devices

BlackBerry 10 devices support cloud storage apps in both the work and personal space. By default, users can use cloud storage apps developed by BlackBerry, such as Box and Dropbox, in the work space on devices. After users log in to a cloud storage app in the work space on devices, that cloud file storage is available as a storage option in the work space and the cloud storage app stores its settings and data in the work space file system. Users can then read, write, move, and update data to that location.

On devices that are running versions of BlackBerry 10 OS that are earlier than 10.2.1, you can use the "Allow cloud storage access from work space" IT policy rule to prevent cloud storage apps from being available in the work space.

On devices that are running BlackBerry 10 OS version 10.2.1 or later, Box and Dropbox are no longer installed in the work space by default. Users can use cloud storage apps in the work space only if you add the apps to the available app list using BES10 Cloud, which allows users to download the apps from the BlackBerry World for Work storefront. If a user upgrades their device to BlackBerry 10 OS version 10.2.1 or later, and you haven't allowed these apps, they are removed from the work space during the upgrade.

Transferring work data from devices using Bluetooth

Using Bluetooth wireless technology, users can open wireless connections between a BlackBerry 10 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, 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 the following IT policy rules to prevent users from transferring work data to other Bluetooth enabled devices:

- Allow transfer of work files using Bluetooth OPP
- Allow transfer of work contacts using Bluetooth PBAP or HFP
- Allow transfer of work messages using Bluetooth MAP

Devices use the Bluetooth OPP to send objects to another Bluetooth enabled device. You can use the "Allow transfer of work files using Bluetooth OPP" IT policy rule to prevent a user from using the Bluetooth OPP to send work files and objects such as contacts to another Bluetooth enabled device. Devices also use the Bluetooth OPP to share work data in a file format (for example, pictures or documents) using NFC. When the "Allow transfer of work files using Bluetooth OPP" IT policy rule isn't selected, users can't share work data in a file format using NFC. You can also use the “Allow transfer of work data using NFC” IT policy rule to prevent users from sending work data to another NFC-enabled device using NFC.

Devices use the Bluetooth PBAP and the Bluetooth HFP to send contacts to another Bluetooth enabled device. You can use the "Allow transfer of work contacts using Bluetooth PBAP or HFP" IT policy rule to prevent a user from using the Bluetooth PBAP

and the Bluetooth HFP to send work contacts to another Bluetooth enabled device. If you don't select this rule, devices also can't use the Bluetooth MAP to send work messages to another Bluetooth enabled device.

Devices use the Bluetooth MAP to send messages to another Bluetooth enabled device. You can use the "Allow transfer of work messages using Bluetooth MAP" IT policy rule to prevent a user from using the Bluetooth MAP to send messages from the work space (for example, email messages and instant messages) to another Bluetooth enabled device. If you don't select the "Allow transfer of work contacts using Bluetooth PBAP or HFP" IT policy rule, users can't send work messages to another Bluetooth enabled device using the Bluetooth MAP, regardless of whether or not the "Allow transfer of work messages using Bluetooth MAP" IT policy rule is selected.

By default, if the "Allow transfer of work messages using Bluetooth MAP" IT policy rule is selected, a user can transfer work messages to a Bluetooth enabled device using the Bluetooth MAP following a single password prompt to enter the work space. If you want to require a user to unlock the work space each time the device connects to the Bluetooth enabled device before the device can transfer work messages using the Bluetooth MAP, don't select the "Allow transfer of work messages using Bluetooth MAP without prompt" IT policy rule.

Preventing users from sharing work data on devices when sharing the screen during BBM Video chats

By default, users can share the screen with other BBM Video chat participants during a BBM Video chat when they are in the work space on BlackBerry 10 devices.

You can use the "Allow sharing work data during BBM Video screen sharing" IT policy rule to allow or prevent users from sharing work screens with other BBM Video chat participants during a BBM Video chat. If this rule isn't selected, a 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 voice control

By default, users can use voice control commands on BlackBerry 10 devices. To prevent users from using voice control commands for Email and Calendar apps on devices, set the "Allow voice control" IT policy rule to "Disallow for email and calendar". To allow users to use voice control commands only for voice dialing and, on devices with BlackBerry 10 OS version 10.2 or later, for checking device status, set this rule to "Allow only phone and device status".

For more information, visit blackberry.com/go/kbhelp to read article KB33430.

Preventing users from using voice dictation within work apps on devices

By default, users can use voice dictation in all apps that support this feature on BlackBerry 10 devices.

You can use the "Allow voice dictation in work apps" IT policy rule to allow or prevent users from using voice dictation in work apps.

Controlling roaming

By default, users can use data services over the wireless network when BlackBerry 10 devices are roaming.

You can use the "Allow roaming" IT policy rule to allow or prevent users from using data services over the wireless network when the device is roaming. If this rule isn't selected and the device is connected to a Wi-Fi network, the device can still send and receive data over the Wi-Fi network when the device is roaming.

Controlling features on devices

You can use the following IT policy rules to control certain features on BlackBerry 10 devices:

- Allow lock screen preview of work content
- Allow unified view for work and personal accounts and messages

For more information about these IT policy rules, see the *BES10 Cloud Policy and Profile Reference Guide*.

Controlling messaging on devices

By default, users can set up various messaging methods on BlackBerry 10 devices such as Facebook and text messaging. You can use the following IT policy rules to control what types of messaging users can do on their devices:

- Display indicator for external email addresses
- Display warning message for external email addresses
- External email domain allowed list
- External email domain restricted list
- Allow forwarding or adding recipients to private messages
- Allow IRM-Protected Email Messages

For more information about these IT policy rules, see the *BES10 Cloud Policy and Profile Reference Guide*.

Controlling how work and personal apps connect to networks

BES10 Cloud controls how work and personal apps on BlackBerry 10 devices connect to networks.

Work data traffic and personal data traffic are routed independently, and you can use IT policy rules to control the type of connections that work and personal apps use to connect to networks.

Preventing work apps on devices from using personal networks to connect to the Internet

By default, apps in the work space on BlackBerry 10 devices can't use personal networks to connect to the Internet.

You can use the "Allow work apps to use personal networks" IT policy rule to allow work apps, including organizer apps, to make connections using personal networks if a work Wi-Fi or work VPN connection isn't available or if your organization doesn't send any work Wi-Fi or work VPN profiles to the device.

Preventing personal apps on devices from using your organization's networks to connect to the Internet

By default, apps in the personal space on BlackBerry 10 devices can use your organization's Wi-Fi or VPN network to connect to the Internet.

You can use the "Allow work network usage for personal apps" IT policy rule to allow or prevent all apps in the personal space from using your organization's networks to connect to the Internet. If you prevent all 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.

If the "Allow work network usage for personal apps" IT policy rule is selected, users can still prevent all apps in the personal space from using your organization's network to connect to the Internet using the "Allow Personal Apps to Use Work Networks" option in the "BlackBerry Balance" settings on the device. Users may choose to do this in order to protect their privacy.

Preventing the BBM Video feature on devices from using your organization’s networks

The BBM Video feature is classified as a personal app on BlackBerry 10 devices. By default, if the "Allow work network usage for personal apps" IT policy rule is selected, the BBM Video feature on devices can use your organization’s Wi-Fi network or VPN network for incoming and outgoing video chats.

If you allow personal apps to use your organization's networks to connect to the Internet (by selecting the "Allow work network usage for personal apps" IT policy rule), you can prevent the BBM Video feature from using your organization's networks by making sure that the "Allow BBM Video access to work network" IT policy rule isn't selected.

Protecting data

BES10 Cloud and devices offer the following security features to protect user information:

- Passwords
- Security timeout
- Data wipe
- BlackBerry Link protection
- Backup protection
- Encryption
- Home screen messages
- Smart cards with BlackBerry Smart Card Reader

Passwords

Device passwords protect your organization's data and user information that is stored on devices. You can use BES10 Cloud to enforce password protection on devices.

You can also use BES10 Cloud to lock devices remotely and change or clear their passwords.

BlackBerry 10 device passwords

BlackBerry 10 devices require users to set a work space password by default. If you don't want users to have to enter a password to access work content and resources in the work space, make sure that the "Password required for work space" IT policy rule isn't selected. You can enforce either a work space password or a full device password as follows:

Rule settings	Result
• "Password required for work space" IT policy rule is selected • "Apply work space password to full device" IT policy rule isn't selected	The Work Password (in the "BlackBerry Balance" settings on the device) is used as the work space password and the IT policy rules in the Password rule group apply to the work space password. Users can use their work space password as their device password using the “Use as my device password” option in the "BlackBerry Balance" settings.
• "Password required for work space" IT policy rule is selected • "Apply work space password to full device" IT policy rule is selected	The work 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.

You can use the following IT policy rules to enforce additional password requirements on devices:

- Maximum password age
- Maximum password attempts
- Maximum password history
- Minimum password complexity
- Minimum password length

A user can configure device password settings using the "Device Password" option in the "Security and Privacy" settings on devices. If a user turns on personal data encryption using the "Encryption" option on devices, 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. For devices that are running BlackBerry 10 OS version 10.2 or later, 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.

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

Changing BlackBerry 10 device passwords

You can use BES10 Cloud to lock BlackBerry 10 devices remotely and change their passwords using the "Specify device password, lock device and set message" IT administration command. You can do this, for example, if a device is lost or if a user forgets their password.

This command has different results on devices, depending on their passwords and settings. The following table lists the device conditions and results that this command will have on them:

Conditions	Result
• Device has a work space password • Device does'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
• Device has a work space password • Device has a full device password • The passwords aren't linked by the "Apply Work Space Password to Full Device" IT policy rule or the "Use as my device password" device option	• 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
• Device has a work space password • The work space password is enforced as the full device password by the "Apply Work Space Password to Full Device" IT policy rule	• 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
• Device has a work space 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

Conditions	Result
• The user sets the work space password as the full device password using the "Use as my device password" option	• The passwords are unlinked

If BES10 Cloud 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.

The "Maximum password age" IT policy rule can be used to control how often a user must change the password by specifying the time that can elapse before a device password expires.

A device user can change the work space password in the "BlackBerry Balance" settings on the device. If the "Apply work space password to full device" IT policy rule isn't selected, a user can choose to use the same password for the entire device.

The "Specify device password, lock device and set message" IT administration command can also be used 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.

For more information about sending the “Specify device password, lock device and set message” IT administration command to a device, see the *BES10 Cloud Administration Guide*.

iOS device passwords

You can use the "Password required for device" IT policy rule to require iOS device users to set a device password.

You can enforce additional password requirements on devices using the following IT policy rules:

- Allow simple value
- Require alphanumeric value
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age
- Passcode history
- Maximum number of failed attempts

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

Changing iOS device passwords

You can use BES10 Cloud to lock or unlock iOS devices remotely and clear their passwords. You can do this, for example, if a device is lost or if a user forgets their password.

You can use the "Lock device" IT administration command to lock a device remotely. The user must type the existing device password to unlock the device. You can use this command if a device is lost or stolen.

You can use the "Unlock and clear password" IT administration command to unlock a device and clear the existing password. The user is prompted to create a new device password. You can use this command if a user forgets their device password.

For more information about sending these commands to devices, see the *BES10 Cloud Administration Guide*.

Android device passwords

You can use the "Password requirements" IT policy rule to require Android device users to set a device password and to specify minimum requirements for device passwords.

You can enforce additional password requirements on devices using the following IT policy rules:

- Maximum failed password attempts
- Password expiration timeout
- Password history restriction
- Minimum password length
- Minimum uppercase letters required in password
- Minimum lowercase letters required in password
- Minimum letters required in password
- Minimum numerical digits required in password
- Minimum symbols required in password

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

Changing Android device passwords

You can use BES10 Cloud to lock or unlock Android devices remotely and change or clear their passwords. You can do this, for example, if a device is lost or if a user forgets the password.

You can use the "Lock device" IT administration command to lock a device remotely. The user must type the existing device password to unlock the device. You can use this command if a device is lost or stolen.

You can use the "Unlock and clear password" IT administration command to unlock a device and clear the existing password. The user is prompted to create a new device password. You can use this command if a user forgets their device password.

You can use the "Specify device password and lock" IT administration command to create a new device password and lock a device. When the user unlocks the device, they are prompted to accept or reject the new password. You can use this command if a device is lost or stolen.

For more information about sending these commands to devices, see the *BES10 Cloud Administration Guide*.

Security timeout

You can use BES10 Cloud to require that devices lock after a certain period of inactivity.

For BlackBerry 10 devices, you can use the "Security timeout" IT policy rule to require that a device lock the work space or the entire device after a certain period of inactivity. On devices that have different work space and device passwords, the security timeout of the work space is controlled by the "Security timeout" IT policy rule and the “Lock Work Space After” option (in the "BlackBerry Balance" settings on the device). The security timeout of the entire device is controlled by the “Lock Device After” option (in the "Device Password" settings on the device). On devices that have a work space password that applies to the full device, the security timeout of the entire device is controlled by the "Security timeout" IT policy rule, along with the “Lock Work Space After” option (in the "BlackBerry Balance" settings on the device). The “Lock Device After” option (in the "Device Password" settings on the device) is grayed out.

Work apps (including apps that display work data and personal data in a unified view) on BlackBerry 10 devices 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 period of user inactivity that you specify in the "Security timeout" IT policy rule or specified in the "Password Lock" settings on the device. If you want to prevent apps from doing this, make sure that the "Allow app security timer reset" IT policy rule isn't selected. If the "Allow app security timer reset" IT policy rule is selected, users can still prevent apps from extending the password lock time in the "Device Password" settings on the device.

For iOS devices, the "Maximum auto-lock" IT policy rule can be used to require that devices lock after a certain period of inactivity. The "Maximum grace period for device lock" IT policy rule can also be used to allow users to unlock their devices without entering their passwords after a specified period of inactivity.

For Android devices, the "Maximum inactivity time lock" IT policy rule can be used to require that a device lock after a specified period of inactivity.

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

Data wipe

To protect your organization's data and user information on devices, you can use BES10 Cloud to delete work data or all data on devices.

Users can also delete work data or all data on their devices.

Full device wipe

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 10 • iOS • Android	You can use BES10 Cloud 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, if applicable, returns the device to factory defaults, and removes the device from BES10 Cloud. For BlackBerry 10 devices and Motorola devices that support the Enterprise Device Management API, information on the media card is also deleted. Once you submit this command, an option to remove the device from BES10 Cloud is displayed. You can remove the device from BES10 Cloud if it's possible that the device is unable to connect to the organization's network to receive the

Event	Device type	Description
		command. If the device connects to the organization's network after it has been deleted, only the work data is removed from the device, including the work space, if applicable. For more information about sending this IT administration command, see the *BES10 Cloud Administration Guide*.
• A BlackBerry 10 device user types the device password incorrectly more times than the "Maximum password attempts" IT policy rule allows. • An iOS device user types the device password incorrectly more times than the "Maximum number of failed attempts" IT policy rule allows. • An Android device user types the device password incorrectly more times than the "Maximum failed password attempts" IT policy rule allows.	• BlackBerry 10 • iOS • Android	This command 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 10 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.
A user uses the "Security Wipe" option on the device.	BlackBerry 10	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 10	A user can also use BlackBerry Protect to wipe a device. For more information about BlackBerry Protect, see the *BlackBerry Protect User Guide*.

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

Data flow: Deleting all data on a BlackBerry 10 device

When all data is deleted from a BlackBerry 10 device, the device performs the following actions:

1. The BlackBerry 10 OS overwrites the device memory with zeros.
2. The BlackBerry 10 OS 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.

Work data wipe

To protect your organization's data on devices, devices delete only work data when any of the following events occur:

Event	Device type	Description
You send the “Delete only work data” IT administration command to a device	• BlackBerry 10 • iOS • Android	You can use BES10 Cloud to delete all work data from devices using the "Delete only work data" IT administration command. You can send this command, for example, to a personal device when a user no longer works at your organization, or if a device is lost or stolen. This command deletes work data, including the IT policy, profiles, apps, and certificates that are on a device, and removes the device from BES10 Cloud. On BlackBerry 10 devices, the work space information is deleted and the work space is removed from the device. Once you submit this command, an option to remove the device from BES10 Cloud is displayed. You can remove a device from BES10 Cloud if it's possible that the device is unable to connect to the organization's network to receive the command. If the device connects to the organization's network after it has been deleted, all work data is removed from the device, including the work space, if applicable. A user can still use the device while the work space data is being deleted. For more information about sending this IT administration command, see the *BES10 Cloud Administration Guide*.
A user types the work space password incorrectly more times than the "Maximum password attempts" IT policy rule allows.	BlackBerry 10	The work space information is deleted and the work space is removed from the device. When the device has a different work space and device password, if a user types the device password incorrectly more times than the "Maximum password attempts" IT policy rule allows, the entire device is wiped, including the work space.
A device exceeds the amount of time without connecting to your organization’s network that the "Wipe the work space without network connectivity" IT policy rule allows.	BlackBerry 10	You can use the "Wipe the work space without network connectivity" IT policy rule to specify the number of hours that must elapse when a device doesn't connect to your organization’s network before the device deletes all data in the work space. You can use this rule to make the device delete the data in the work space if the device can't receive updates or commands from BES10 Cloud.
A user uses the "Delete work space" option in the "BlackBerry Balance" settings on the device.	BlackBerry 10	Users can also remove the work space from their devices using the "Delete work space" option in the "BlackBerry Balance" settings.

BlackBerry Link protection for BlackBerry 10 devices

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

- Synchronize music, pictures, videos, 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 personal 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

Users with devices that are running BlackBerry 10 OS version 10.1 or later can also use BlackBerry Link on a computer to:

- Allow remote file access, so that their devices can access files stored in user-selected folders on their computers
- Synchronize contacts and calendar appointments between devices and computers

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

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.

Back up and restore

BlackBerry 10 device users can back up and restore apps and data on devices using BlackBerry Link. Users can back up and restore only personal apps and data on devices. If users try to back up work apps and data, BlackBerry Link displays an error message.

Backup protection

When a BlackBerry 10 device user backs up personal 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.

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.

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 personal 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.

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 devices.

Backup protection for iOS devices

For iOS devices, the “Allow backup” IT policy rule can be used to prevent users from backing up devices to iCloud.

You can use the “Force encrypted backups” IT policy rule to require that backup files are stored in an encrypted format on users’ computers when they back up their devices using iTunes software.

Encryption

BlackBerry 10 devices use encryption to protect the following:

Type of data	Description
Work space data	Devices protect work data by encrypting the files stored in the work space. Work space encryption isn't optional.

Type of data	Description
Personal space data	Devices can protect personal data by encrypting the files stored in the personal space. Personal space encryption is optional. You can use the "Force personal space data encryption" IT policy rule to turn on encryption for the personal space on a device. Users can also turn on personal data encryption using the "Device Encryption" option in the "Security and Privacy" settings on the device.
Media card data	Devices can protect media card data by encrypting the files stored on media cards. Media card encryption is optional. You can use the "Force media card encryption" IT policy rule to turn on media card encryption. Users can also turn on media card encryption using the "Media Card Encryption" option in the "Security and Privacy" settings on the device.

Android devices can use encryption to protect data that is stored on devices. You can use the "Require storage encryption" IT policy rule to specify whether the data storage on an Android device is encrypted.

Home screen message on BlackBerry 10 devices

If BlackBerry 10 devices are lost, you can use the "Specify device password, lock device and set message" IT administration command to set a message that appears on a device's home screen. For example, you can use a home screen message to display contact information that can be used to return the device.

For more information about setting a home screen message on a device, see the *BES10 Cloud Administration Guide*.

BlackBerry Smart Card Reader

You can use the BlackBerry Smart Card Reader 2.0 with devices that are running BlackBerry 10 OS version 10.2 or later to:

- Permit 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

The reader communicates using Bluetooth technology version 1.1 or later and encrypts information on the smart card using AES-256 encryption. The reader stores all encryption keys in RAM only and never writes the keys to flash memory.

To pair devices with the reader, users must install a smart card driver, the BlackBerry Smart Card Reader driver, and, optionally, a smart card authenticator module on their devices.

Opening a secure connection to the BlackBerry Smart Card Reader

A user can open a secure connection between a BlackBerry 10 device and the BlackBerry Smart Card Reader in one of the following ways:

- Clicking "Connect" on the BlackBerry Smart Card Reader options screen on the device
- Trying an action on the device that requires the smart card (for example, importing certificates, signing or decrypting a message, or turning on two-factor authentication)

The reader reconnects automatically to a device that it has previously connected.

The device and reader open a secure connection by using the following pairings:

Pairing	Description
Bluetooth	This pairing creates a Bluetooth encryption key and opens a Bluetooth connection between the device and the reader. For more information about the Bluetooth connection, see the *BlackBerry Smart Card Reader Security Technical Overview*.
Secure pairing	This pairing creates a secure pairing PIN and opens a connection between the smart card and the device. The reader and the device use the secure pairing PIN to encrypt and authenticate the data that they send between them over the application layer. By default, the secure pairing PIN is 8 characters long and is case-sensitive. You can use the "Smart card reader PIN entry mode" IT policy rule to change the format of the secure pairing PIN. During the secure pairing process the following events occur: • The initial key establishment protocol creates a shared device transport key on the device and the reader that they use to encrypt and decrypt the data that they send between them • The connection key establishment protocol creates a shared connection key on the device and the reader that they use to send data between them For more information about the initial key establishment protocol and the connection key establishment protocol, see the *BlackBerry Smart Card Reader Security Technical Overview*. The secure pairing is only deleted if the user removes the reader from the list of Bluetooth paired devices, or the device or reader is wiped.

Unbinding the current smart card from a BlackBerry 10 device

There are two ways to delete the binding between a user's current smart card and a BlackBerry 10 device:

- You 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. You can wipe the device by sending the "Delete all data" IT administration command or the "Delete only work data" IT administration command.
- The 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 BlackBerry 10 device user using a smart card

When users turn on two-factor authentication on BlackBerry 10 devices, they are required to authenticate with their devices using a smart card. Users need to prove their identities by demonstrating two factors:

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

On devices that are running BlackBerry 10 OS version 10.2 or later, users can turn on or turn off two-factor authentication with the smart card by changing the "Smart Card User Authenticator" field in the "Device Password" settings on the device.

When a user 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 has not yet configured a device password, the device forces the user to set a password.
2. The device prompts the user to type the smart card password to turn on two-factor authentication with the installed smart card.

Apps

Managing work apps on BlackBerry 10 devices

You can use BES10 Cloud to install, update, or remove apps that your organization wants to make available as work apps on BlackBerry 10, iOS, and Android devices.

For 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 is 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.

You can change whether iOS apps or Android apps are required or optional. BlackBerry apps can only be optional. You can configure a compliance rule that performs actions when users don't install a required app.

For more information, see the *BES10 Cloud Administration Guide.*

Preventing BlackBerry 10 device users from installing apps using development tools

App developers can use development tools to test apps that they are developing by installing the apps on BlackBerry 10 devices using a USB or Wi-Fi connection.

On BlackBerry devices, you can use the "Restrict development mode" IT policy rule to prevent users from using development tools to install apps on the entire device.

Alternatively, on devices that are running BlackBerry 10 OS version 10.2 or later, you can use the “Allow development mode access to work space” rule to prevent users from using development tools to install apps in 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 devices that are running versions of BlackBerry 10 OS that are earlier than 10.2.1, users can install apps in the personal space only from the BlackBerry World storefront
- On devices that are running BlackBerry 10 OS version 10.2.1 or later, 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

Installing personal apps on BlackBerry 10 devices

On BlackBerry devices that are running versions of BlackBerry 10 OS that are earlier than 10.2.1, users can install apps in the personal space only from the BlackBerry World storefront or by using development mode (if development mode isn't restricted).

On BlackBerry devices that are running BlackBerry 10 OS version 10.2.1 or later, users can install apps in the personal space from various sources such as BlackBerry World, email attachments, downloads through the browser, media cards, and using development mode (if development mode isn't restricted).

Protecting a BlackBerry 10 device from malicious apps

Apps are tested to make sure that they don't interfere with the core functionality of BlackBerry 10 devices before they are approved by BlackBerry and made available on the BlackBerry World storefront. BlackBerry can remove any apps from BlackBerry World that were identified as potentially malicious or don't follow the BlackBerry World Vendor Agreement.

Cryptography

Secure

Cryptography on BlackBerry 10 devices

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

Algorithm	Digest size (in bits)
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

Internet security protocols

- DTLS 1.0
- SSL 2.0
- SSL 3.0
- TLS 1.0
- TLS 1.1

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

Product documentation

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

Provide feedback

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

Glossary

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.
CA	certification authority
CAST	Carlisle Adams Stafford Tavares
CBC	cipher block chaining
CFB	cipher feedback
CSR	certificate signing request
CTR	Counter
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DH	Diffie-Hellman
DMZ	A demilitarized zone (DMZ) is a neutral subnetwork outside of an organization's firewall. It exists between the trusted LAN of the organization and the untrusted external wireless network and public Internet.
DRBG	deterministic random bit generator
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

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
EC-SPEKE	Elliptic Curve – Simple Password Exponential Key Exchange
EDE	Encryption-Decryption-Encryption
FIPS	Federal Information Processing Standards
GCC	GNU Compiler Collection
GCM	Galois/Counter Mode
HFP	Hands-Free Profile
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
IRM	information rights management
IT policy	An IT policy consists of various rules that control the security features and behavior of devices.
MAP	Message Access Profile
MD	Message Digest Algorithm
MDC	Modification Detection Code
MDM	mobile device management
MIME	Multipurpose Internet Mail Extensions
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OFB	output feedback
OPP	Object Push Profile
PAP	Password Authentication Protocol
PBAP	Phone Book Access Profile
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail

PFX	Personal Information Exchange
PIN	personal identification number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PRNG	pseudorandom number generator
PSK	pre-shared key
RC	Rivest's Cipher
RFC	Request for Comments
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
S/MIME	Secure Multipurpose Internet Mail Extensions
SHA	Secure Hash Algorithm
SMS	Short Message Service
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.
SRP	Server Routing Protocol
SSL	Secure Sockets Layer
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
Triple DES	Triple Data Encryption Standard
URI	Uniform Resource Identifier
VPN	virtual private network
WebDAV	Web Distributed Authoring and Versioning
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
xAuth	Extended Authentication
XEX	Xor-Encrypt-Xor
XML	Extensible Markup Language
XTS	XEX-based Tweaked CodeBook mode with CipherText Stealing

Legal notice

PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

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

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

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

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

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada