BlackBerry UEM

Security Note

Contents

Document revision history

Date	Description
22 December 2016	Updated BES12 product names to BlackBerry UEM product names throughout the document.

Introduction

BlackBerry Unified Endpoint Manager is a comprehensive, scalable, and secure device management solution from BlackBerry that allows you to manage various devices for your organization. You can manage BlackBerry, iOS, OS X, Android, and Windows devices all from a unified interface.

BlackBerry UEM is an on-premises solution that you install in your organization's environment and includes many security features that allow you to strike the right balance between offering your employees their choice of device while keeping your business data secure. Each BlackBerry UEM instance encrypts all of the data that it stores directly and writes indirectly to files using a FIPS-validated cryptographic module. BlackBerry UEM includes the following security features:

- An architecture that provides secure connectivity to your organization's resources
- A software development model that focuses on security
- Administration commands, IT policy rules, and profiles
- Encryption to protect your data while it's at rest and in transit
- Password and device controls
- Network connectivity controls
- Device compliance enforcement
- App management
- Certificate-based authentication

This guide provides a high-level description of various BlackBerry UEM security features. However, BlackBerry UEM manages many different devices and not all security features are supported on all devices. Each device type, OS version, and device management option provides its own set of security features that BlackBerry UEM can help you manage. For more information about each feature and the devices that support it, visit http://help.blackberry.com/detectLang/blackberry-uem/current/administration-guide-pdf to read the *BlackBerry UEM Administration Guide*.

Managing device security

BlackBerry UEM provides a number of device management features. The available features depend on the device type and the device management options you choose when activating devices.

Activating devices

Device activation associates a device with a user account in BlackBerry UEM and establishes a secure communication channel between the device and BlackBerry UEM through the BlackBerry Infrastructure. After a device is activated, you can manage the device using BlackBerry UEM.

To help secure the activation process, a user must enter a password to activate a device. You can specify how long an activation password remains valid before it expires. You can also specify the default password length for the automatically generated password that's sent to users in the activation email message.

By default, users are registered with the BlackBerry Infrastructure when they are added to BlackBerry UEM. Information sent to the BlackBerry Infrastructure is sent and stored securely. You can turn off user registration with the BlackBerry Infrastructure if you don't want to send user information to BlackBerry. The benefit of registration is that users don't have to enter the server address when they're activating a device; they only need to enter their email address and password. Depending on the device, the Enterprise Management Agent or the BlackBerry UEM Client communicates with the BlackBerry Infrastructure to retrieve the server address. A secure connection is established with BlackBerry UEM with minimal user input.

Activation types configure the level of control you have over activated devices. For example, you can have full control over a device that your organization issues to a user or you can make sure that you have no control over the personal data on a device that a user owns and brings to work. The activation types that your organization can use depend on the device types that you manage and on the licenses that you purchase.

Protecting work apps and data with work spaces

When devices are activated on BlackBerry UEM, depending on the activation type, a work space may be created on the device. 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. Devices with both a work space and a personal space allow your organization to maintain stricter controls over work apps and data while allowing your users to have control over personal data and apps. BlackBerry UEM supports several work space options including:

- BlackBerry Balance on BlackBerry 10 devices
- Secure Work Space on iOS and Android devices
- Android for Work on Android devices
- Samsung KNOX Workspace on Samsung devices

Managing apps on devices

You can use BlackBerry UEM to manage and monitor apps that your organization wants to make available on devices. You can specify apps that are required on devices and use compliance profiles to specify the action taken if the user doesn’t install the app. You can also specify optional apps that users are allowed to install in the work space and restricted apps that users aren’t allowed to install. For example, you can prevent users from installing malicious apps or apps that require a lot of resources. For some devices, you can also manage personal apps.

Ensuring device compliance

You can use compliance profiles to encourage users to follow your organization’s standards for the use of devices. A compliance profile defines the device conditions that aren't acceptable in your organization. Depending on the OS and version, you can specify whether the following conditions are permitted:

- Jailbroken or rooted devices
- Restricted device software version is installed
- Non-assigned or restricted app is installed
- Required app isn't installed

A compliance profile specifies the following information:

- Conditions that make a device non-compliant with BlackBerry UEM
- Notifications that users receive if a device violates the compliance conditions, and the amount of time that users have to correct the issue
- Action that's taken if the user doesn't correct the issue, including limiting a user’s access to the organization's resources, deleting work data from the device, or deleting all data from the device

Locating devices

You can set up location service profiles to help locate devices that have been lost or stolen. You can view the current locations of the devices on a map in the management console and allow users to locate their devices on a map in BlackBerry UEM Self-Service. For some devices, you can also log the device location history.

Using IT policies to manage devices

An IT policy is a set of rules that restrict or allow features and functionality on devices. IT policy rules can manage the security and behavior of devices. The device OS determines the list of features that can be controlled using IT policies and the device activation type determines which rules in an IT policy apply to a specific device.

BlackBerry UEM 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. Devices ignore rules in an IT policy that don't apply to them.

When you configure IT policy rules, they can restrict or allow device and work space features and functionality. The IT policy rules available for each device are determined by the device type, the OS, and version. You can use IT policy rules to control such things as:

- Device and work space password requirements
- Device features such as the camera or location services
- Connections that use Bluetooth wireless technology or NFC

Using the BlackBerry UEM Client

The BlackBerry UEM Client allows BlackBerry UEM to communicate with devices. The BlackBerry UEM Client uses a FIPS-validated cryptographic module to encrypt all of the data that it stores directly and writes indirectly to files.

To activate these devices using BlackBerry UEM, users must first install the BlackBerry UEM Client on devices. After users activate their devices, the BlackBerry UEM Client allows them to do the following:

- Verify whether their devices are compliant with your organization's standards
- View the IT policy rules and profiles that have been assigned to their user accounts
- Deactivate their devices

Sharing information with Google data centers

BlackBerry UEM doesn’t send any of your organization’s work data, such as work email messages or other work data for Android for Work devices, to Google data centers. The work space on Android for Work devices isn’t backed up and sent to Google data centers.

When BlackBerry UEM creates user accounts, it sends only users’ display names and email addresses to Google. Google uses this information to activate devices with Android for Work and set up Google Play for Work. Google is also aware of the internal and public apps that you’re managing on Android for Work devices and which users the apps are assigned to.

Protecting data at rest

BlackBerry UEM supports various methods that you can use to keep data private and secure while it's stored on devices, including password authentication, encryption, and data wipes.

Protecting data with passwords

Device and work space passwords protect your organization's data and user information that's stored on devices. You can use BlackBerry UEM to enforce password protection on devices.

You use IT policy rules to set the password requirements for devices. Each device type supports several IT policy rules for controlling device and work space password requirements. You can set requirements such as password length and complexity, password expiration, the period of inactivity before the device or work space requests a password, and the result of incorrect password attempts.

Depending on the features a device supports, you can use BlackBerry UEM IT administration commands to lock devices remotely and change their passwords. You can do this, for example, if a device is lost or if a user forgets their password. If the device has a work space, you can also change the work space password.

Storing passwords in the BlackBerry UEM database

BlackBerry UEM stores administrative passwords and activation passwords in the BlackBerry UEM database. The passwords are encrypted and stored in a secure manner.

The BlackBerry UEM management console passwords that administrators use for direct authentication are stored in the database using the following form:

```
<Hex Encoded Hash>:<Hex Encoded Salt>

where:
<HexEncodedSalt> = HEX(<salt>)
<HexEncodedHash> = HEX(<hash>)
<salt> = random 4 byte salt
<hash> = HASH(<plaintext>, <salt>, SHA-512, 100 iterations)
```

BlackBerry UEM validates the password that an administrator uses to log in as follows:

- Uses the username to search for the hashed password
- Uses the salt to hash the supplied password
- Compares the computed hash of the passwords to determine whether the supplied password is valid

Passwords that an administrator uses to connect to Microsoft Active Directory or an LDAP directory, as well as device activation passwords, are encrypted using a 256-bit AES/CBC/PKCS5Padding encryption scheme and stored in the database.

Protecting data with encryption

BlackBerry UEM protects data at rest using encryption. Each BlackBerry UEM instance encrypts all of the data that it stores directly and writes indirectly to files using a FIPS-validated cryptographic module.

BlackBerry UEM also helps protect data at rest on devices using encryption. BlackBerry UEM supports both full device and work space encryption offered by various device types, either by default or when activated on

BlackBerry UEM. You can also use IT policy rules to force some devices to encrypt data in the work space, personal space, or on media cards.

Wiping data on devices

To protect your organization's data and user information on devices, you can use BlackBerry UEM to control when a device must wipe its data. For example, you can use IT administration commands and IT policy rules to require that a device deletes device data, work data, or the work space after a specific time or under specific conditions. You can do this to protect your data on a device that's lost and unlikely to be recovered or on a personal device when a user no longer works at your organization.

Users can also trigger a data wipe on their devices by making too many incorrect password attempts, for example, or using device security options to wipe their devices.

Protecting data in transit

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

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

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

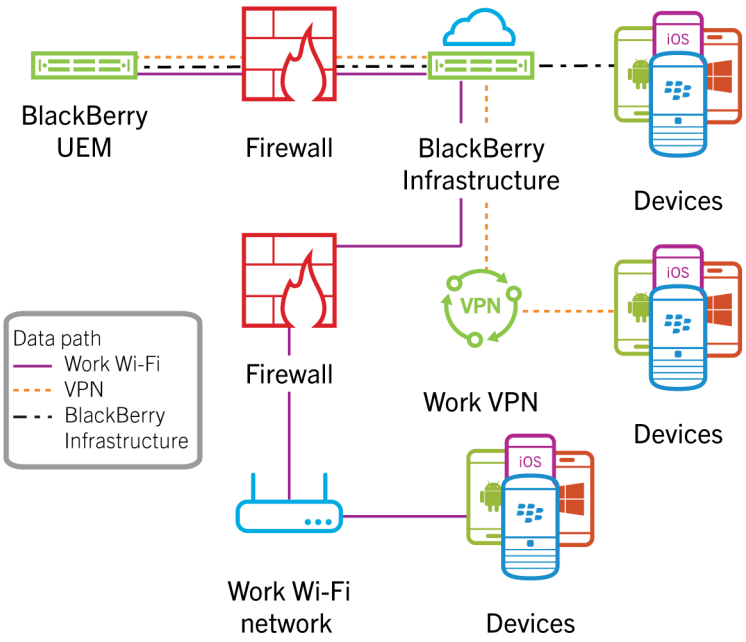
Protecting data in transit over the BlackBerry Infrastructure

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

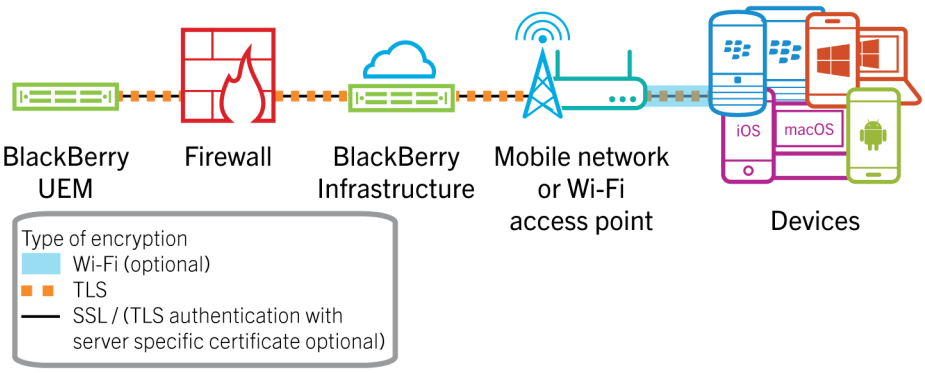
- BlackBerry UEM sends internal apps and all device management data, such as IT policies, profiles, and IT administration commands, to devices through the BlackBerry Infrastructure, even when the device is connected to a work Wi-Fi network or work VPN.
- Data sent between a device and your organization's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

Protecting device management data sent between BlackBerry UEM and devices

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



During the activation process, a mutually authenticated TLS connection is established between BlackBerry UEM and a device. If a device uses the BlackBerry UEM Client, BlackBerry UEM establishes the connection with the app or client. When BlackBerry UEM needs to send configuration information to a device, BlackBerry UEM and the device use the TLS connection to protect the data. The following diagram shows the encryption that's used when BlackBerry UEM sends device management data to devices through the BlackBerry Infrastructure:



How BlackBerry UEM authenticates with the BlackBerry Infrastructure

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

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

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

SRP is a proprietary point-to-point protocol that runs over TCP/IP. BlackBerry UEM uses SRP to contact the BlackBerry Infrastructure and open a connection. When BlackBerry UEM and the BlackBerry Infrastructure open a connection, they can authenticate with each other, exchange configuration information, and send and receive data.

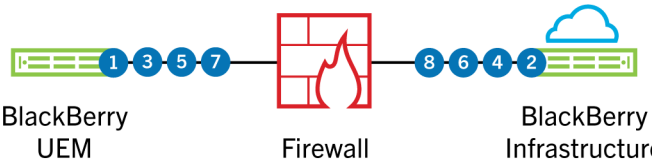
Data flow: Authenticating BlackBerry UEM with the BlackBerry Infrastructure when sending device management data to devices

This data flow shows how BlackBerry UEM authenticates with the BlackBerry Infrastructure when BlackBerry UEM sends device management data to a device. It also applies to how BlackBerry UEM authenticates with the BlackBerry Infrastructure when BlackBerry UEM sends work data from your organization’s mail, web, and content servers to Secure Work Space devices using enterprise connectivity.

1. BlackBerry UEM connects to the BlackBerry Infrastructure and initiates a TLS connection.
2. The BlackBerry Infrastructure sends an authentication certificate to BlackBerry UEM.
3. BlackBerry UEM performs the following actions:
   - Verifies that the authentication certificate is signed by a trusted CA
   - Verifies the name of the server in the BlackBerry Infrastructure to establish the TLS connection
   - Sends a data packet that contains its unique SRP ID and SRP authentication key to the BlackBerry Infrastructure to claim the SRP ID
4. The BlackBerry Infrastructure verifies the SRP ID and SRP authentication key sent by BlackBerry UEM and performs one of the following actions:
   - If the credentials are valid, sends a confirmation to BlackBerry UEM to complete the authentication process and configure an authenticated SRP connection
   - If the credentials aren't valid, stops the authentication process and closes the SRP connection

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

This data flow shows how BlackBerry UEM authenticates with the BlackBerry Infrastructure when BlackBerry UEM sends work data from your organization's mail, web, and content servers to BlackBerry 10 devices through the BlackBerry Infrastructure using enterprise connectivity. It also applies to how BlackBerry UEM authenticates with the BlackBerry Infrastructure when BlackBerry UEM sends work data from your organization's mail, web, and content servers to devices using BlackBerry Secure Connect Plus.



1. BlackBerry UEM connects to the BlackBerry Infrastructure and initiates a TLS connection.
2. The BlackBerry Infrastructure sends an authentication certificate to BlackBerry UEM.
3. BlackBerry UEM performs the following actions:
   - Verifies that the authentication certificate is signed by a trusted CA
   - Verifies the name of the server in the BlackBerry Infrastructure to establish the TLS connection
   - Sends a data packet that contains its unique SRP ID and SRP authentication key to the BlackBerry Infrastructure to claim the SRP ID
4. The BlackBerry Infrastructure sends a random challenge string to BlackBerry UEM.
5. BlackBerry UEM sends a challenge string to the BlackBerry Infrastructure.
6. The BlackBerry Infrastructure hashes the challenge string it received from BlackBerry UEM with the SRP authentication key using HMAC with the SHA-1 algorithm. The BlackBerry Infrastructure sends the resulting 20-byte value to BlackBerry UEM as a challenge response.
7. BlackBerry UEM hashes the challenge string it received from the BlackBerry Infrastructure with the SRP authentication key and sends the result as a challenge response to the BlackBerry Infrastructure.
8. The BlackBerry Infrastructure performs one of the following actions:
   - Accepts the challenge response and sends a confirmation to BlackBerry UEM to complete the authentication process and configure an authenticated SRP connection
   - Rejects the challenge response

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

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

How devices connect to the BlackBerry Infrastructure

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

If an attacker tries to impersonate the BlackBerry Infrastructure, devices prevent the connection. Devices verify whether the public key of the TLS certificate for the BlackBerry Infrastructure matches the private key of the root certificate that's preloaded on devices (BlackBerry 10 or BlackBerry devices powered by Android only) during the manufacturing process or installed on other devices during the activation process. If a user accepts a certificate that isn't valid, the connection can't open unless the device can also authenticate with a valid BlackBerry UEM instance.

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

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

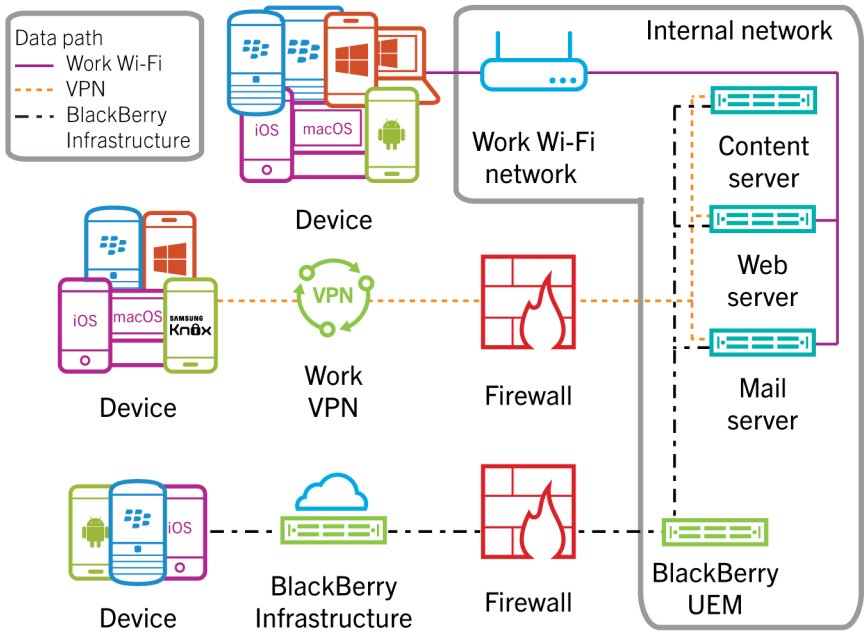
1. A device sends a request to the BlackBerry Infrastructure to open a TLS connection.
2. The BlackBerry Infrastructure sends its TLS certificate to the device.
3. The device verifies the TLS certificate using a root certificate preloaded on the device during the manufacturing or activation process.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

How devices connect to your resources

Devices can connect to your organization's resources, such as mail, web, and content servers, using several communication methods. For example, by default, devices that use enterprise connectivity or BlackBerry Secure Connect Plus to connect to your organization's resources use the following communication methods (in order). By default, work apps on devices can also use any of these communication methods to access the resources in your organization's environment.

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

The following diagram shows the communication methods that devices can use to connect to your organization's network:

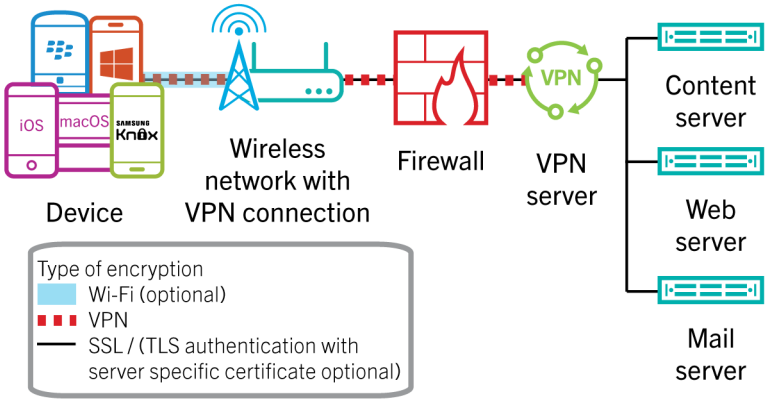


Connecting to a VPN

A VPN provides an encrypted tunnel between a device and the network. BlackBerry UEM supports VPN profiles on most devices. If your organization's environment includes VPNs, such as IPsec VPNs or SSL VPNs, you can configure devices to authenticate with a VPN to access your organization's 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 the VPN concentrator, which acts as the gateway to your organization's network. Each device includes a built-in VPN client that supports several VPN concentrators. Depending on the VPN solution, a client app may be required 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.

In a VPN connection, devices connect to your organization's resources through any wireless access point or a mobile network, your organization's firewall, and your organization's VPN server. Wi-Fi encryption is used if the wireless access point is set up to use it. Devices can use either password- or certificate-based authentication to connect. The following diagram shows how devices connect to your organization's resources over a VPN connection and the encryption that's used for the connection:



Additional VPN features, such as VPN on demand and per-app VPN, are supported on some devices. VPN on demand allows you to specify whether a device connects automatically to a VPN in a particular domain. Client certificates provide authentication for the user's device when accessing the particular domain. For example, you can specify your organization's domain to allow users access to your intranet content using VPN on demand.

Per-app VPN allows you to specify which work apps and secured apps on devices must use a VPN for their data in transit. Per-app VPN helps decrease the load on your organization's VPN by enabling only certain work traffic to use the VPN (for example, accessing application servers or web pages behind the firewall). This feature also supports user privacy and increases connection speed for personal apps by not sending the personal traffic through the VPN.

Protecting communication with devices using certificates

A certificate is a digital document that binds the identity and public key of a certificate subject. Each certificate has a corresponding private key that's stored separately. A CA signs the certificate to verify that it can be trusted. Depending on the device capabilities and activation type, devices can use certificates to:

- Establish a secure connection with BlackBerry UEM
- Authenticate using SSL/TLS when they connect to web pages that use HTTPS
- Authenticate with a work mail server
- Authenticate with a work Wi-Fi network or VPN

- Encrypt and sign email messages using S/MIME protection

Many certificates used for different purposes can be stored on a device. Client certificates can be provided to devices in several ways:

How the certificate is added	Description
During device activation	BlackBerry UEM sends certificates to devices during the activation process. Devices use these certificates to establish secure connections between the device and BlackBerry UEM.
SCEP profiles	You can create SCEP profiles that devices use to connect to, and obtain client certificates from, your organization's CA using a SCEP service. Devices can use these certificates for certificate-based authentication from the browser and to connect to your work Wi-Fi network, work VPN, and work mail server.
User credential profiles	If your organization uses Entrust or OpenTrust software products to issue and manage certificates, you can create user credential profiles that devices use to get client certificates from your organization's CA. Devices use these certificates for certificate-based authentication from the browser, and to connect to your work Wi-Fi network, work VPN, and work mail server.
Shared certificate profiles	A shared certificate profile specifies a client certificate that BlackBerry UEM sends to devices. BlackBerry UEM sends the same client certificate to every user that the profile is assigned to. The administrator must have access to the certificate and private key to create a shared certificate profile.
Sending client certificates to individual user accounts	To send a client certificate to the devices for an individual user, you can add a client certificate to a user account. BlackBerry UEM sends the certificate to the user's devices. The administrator must have access to the certificate and private key to send the client certificate to the user.
User import	Users can import client certificates into the device's certificate store using device settings. Certificates intended for use by the work browser or for sending S/MIME-protected messages from the work email account can be imported from the file system on the device or from a network location that's accessible from the work space.
Smart cards	Users can import S/MIME and SSL certificates to their devices from a smart card.

Enrolling client certificates to devices using SCEP

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

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

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

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

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

Sending CA certificates to devices

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

When the certificates for the CAs that issued your organization's network and server certificates are stored on devices, the devices can trust your networks and servers when they make 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 they receive an S/MIME-protected email message.

Protecting access to your organization’s mail server

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

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

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

You can configure Microsoft Exchange to block devices from using Exchange ActiveSync unless the devices are explicitly added to an allowed list. Devices that aren't on the allowed list can't access work email and organizer data. In BlackBerry UEM, you can set up Microsoft Exchange gatekeeping to control which devices are automatically added to the allowed list on your Microsoft Exchange Server. If you use Microsoft Exchange gatekeeping, when a user who's assigned an email profile activates a device, the device is automatically added to the allowed list in Microsoft Exchange. A device is automatically removed from the allowed list if you remove the email profile from the user account, if the device violates the settings in the assigned compliance profile, or if the device is deactivated.

Extending email security

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

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

S/MIME

You can extend messaging security for BlackBerry UEM and permit device users to sign, encrypt, or sign and encrypt messages using S/MIME when they use a work email account and a device that supports S/MIME-protected messages. BlackBerry UEM allows you to control S/MIME options on devices. For example, you can specify whether devices can send S/MIME-protected email messages.

BlackBerry UEM lets you configure LDAP server settings and send them to devices so that users don’t have to manually import S/MIME certificates. Users can then search for and retrieve recipients' S/MIME certificates from LDAP servers over the wireless network. To authenticate with LDAP certificate servers, devices might use simple, Kerberos, or password authentication. BlackBerry UEM also lets you configure settings to determine the status of S/MIME certificates using OCSP, HTTP, HTTPS, or LDAP.

PGP

You can extend messaging security for BlackBerry UEM and permit device users to sign, encrypt, or sign and encrypt messages using PGP protection when they use a work email account and a device that supports PGP protected messages. BlackBerry UEM allows you to control PGP options on devices. For example, you can specify whether devices can send PGP protected email messages.

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

Message classification

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

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

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

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

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

You can provide the browser and apps on devices with single sign-on access so they can authenticate automatically with domains and web services in your organization’s network. Single sign-on authentication can use a user’s login information or certificate.

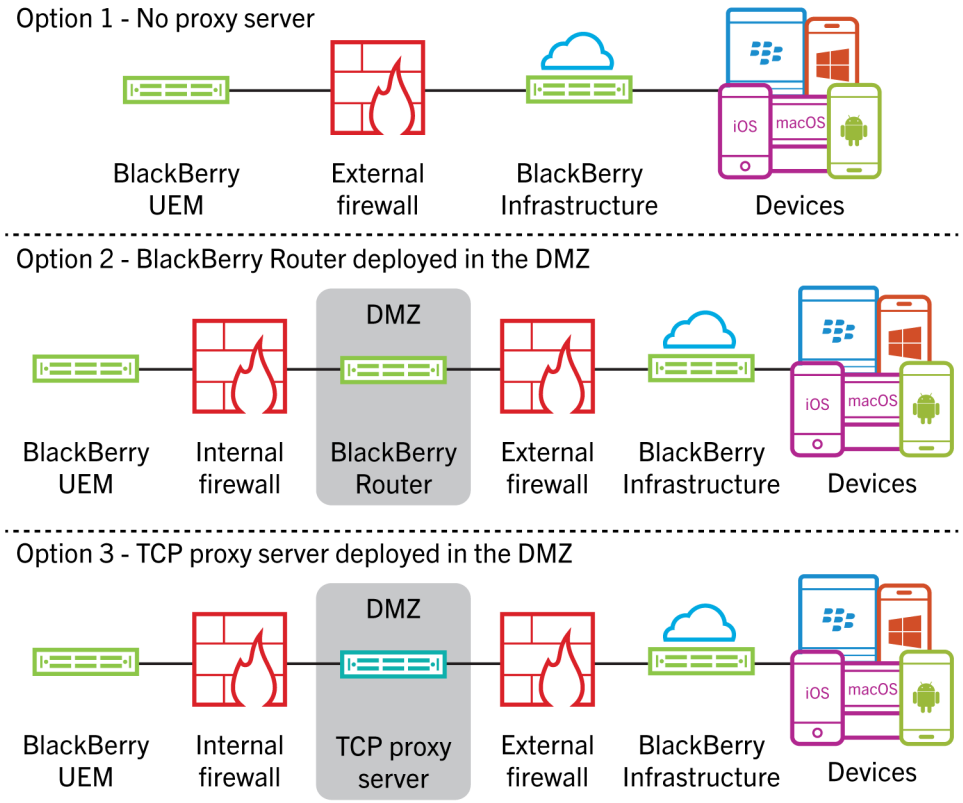
You can use BlackBerry UEM to assign a single sign-on profile to a user. The user’s login information is then saved on the device the first time they access a domain specified in the profile. The user’s saved credentials are used automatically when the user tries to access any of the domains specified in the profile. The users isn’t prompted again for credentials until the user’s password changes or the certificate expires. BlackBerry UEM supports Kerberos, NTLM, and certificate-based authentication types.

Using DMZs to protect connections to BlackBerry UEM

By default, BlackBerry UEM connects directly to the BlackBerry Infrastructure. However, if your organization's security policy requires that internal systems don’t connect directly to the Internet, you can use a proxy server to act as an intermediary between BlackBerry UEM and the BlackBerry Infrastructure. You can install the BlackBerry Router to act as a proxy server, or use a TCP proxy server.

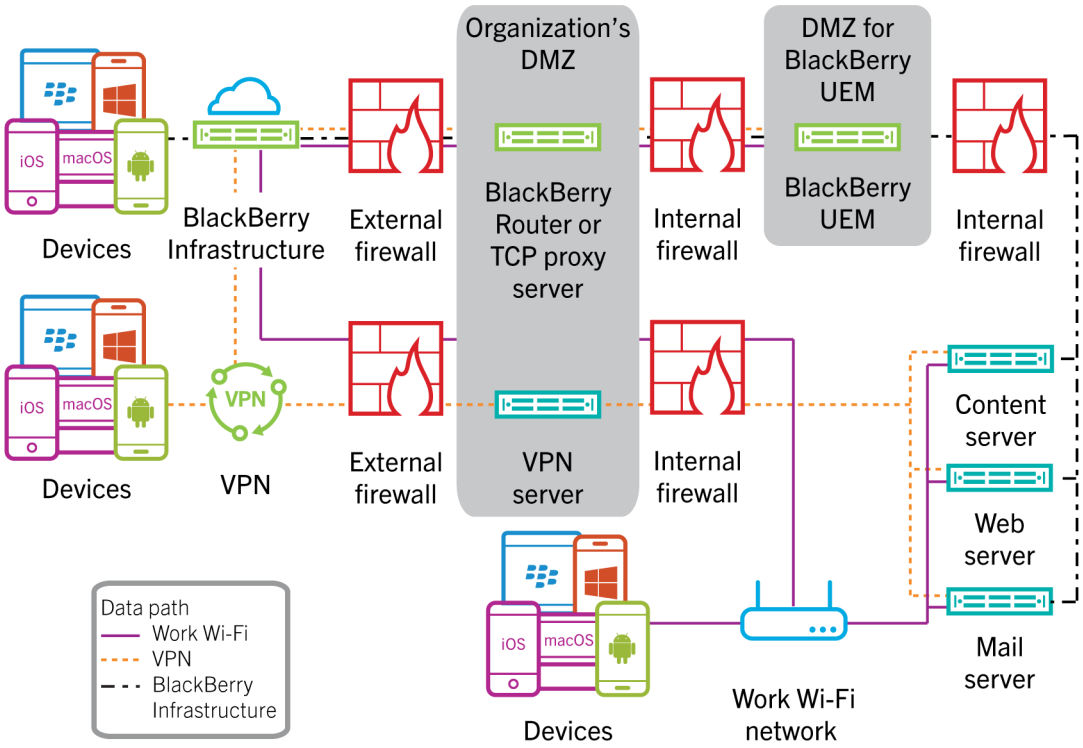
The proxy server can be installed outside your organization’s firewall, in the DMZ. This provides an extra level of security for BlackBerry UEM because only the proxy server connects to BlackBerry UEM from outside the firewall, and all connections to the BlackBerry Infrastructure between BlackBerry UEM and devices go through the proxy server.

The following diagram shows the options for using a proxy server with BlackBerry UEM:



When BlackBerry UEM detects a BlackBerry Router, it identifies the IP address of the computer that hosts the BlackBerry Router and writes the IP address to the BlackBerry UEM database.

If your organization's security policies require more granular control over the resources that BlackBerry UEM has access to, you can also install BlackBerry UEM in its own DMZ. The following diagram shows how you can install the proxy server in your organization’s DMZ and install BlackBerry UEM in a separate DMZ:


Organization's DMZ
DMZ for BlackBerry UEM
iOS
macOS
Devices
BlackBerry Infrastructure
External firewall
BlackBerry Router or TCP proxy server
Internal firewall
BlackBerry UEM
Internal firewall
VPN
Devices
VPN
External firewall
VPN server
Internal firewall
Content server
Web server
Mail server
Data path
Work Wi-Fi
VPN
BlackBerry Infrastructure
Devices
Work Wi-Fi network

Related resources

For more information, read the following documents:

Title	Description	Web address
BlackBerry UEM Administration Guide	• Feature details and the devices that support them • Device activation • App management • Device compliance • IT policies, profiles, and administration commands • VPN and Wi-Fi configuration • Certificate management • Secure email	http://help.blackberry.com/detectLang/blackberry-uem/current/administration-guide-pdf
BlackBerry 10 Devices Security Note	• BlackBerry UEM management of devices • Hardware root of trust • OS security • Data at rest security • Data in transit security • Cryptography on devices	http://help.blackberry.com/detectLang/blackberry-uem-security/current/blackberry-10-security-note/BlackBerry-10-Devices-latest-Security-Note-en.pdf
BlackBerry Corporate Infrastructure Security Note	• BlackBerry policies • Security organizations • Physical and environmental security • Human resources • Access control • Communications and operations management • Systems development and maintenance • Disaster recovery and business continuity • Incident response and management	http://help.blackberry.com/detectLang/blackberry-uem-security/current/infrastructure-security-note/BlackBerry-Corporate-Infrastructure-latest-Security-Note-en.pdf
BES12 Cloud Security Note	• BES12 Cloud infrastructure security • BlackBerry data center security • Data in transit security	http://help.blackberry.com/detectLang/bes12-cloud-security/current/bes12-cloud-security-note/BES12-Cloud-latest-Security-Note-en.pdf

Title	Description	Web address
BlackBerry powered by Android Security Guide	• Device security • Data in transit security • Device management • BlackBerry enterprise mobility solutions	http://help.blackberry.com/detectLang/security-guide-for-blackberry-powered-by-android/latest/security-guide-for-blackberry-powered-by-android-pdf/BlackBerry-powered-by-Android-latest-Security-Guide-en.pdf
Policy Reference Spreadsheet	• IT policy rule names, descriptions, and details	http://help.blackberry.com/detectLang/blackberry-uem/current/policy-reference-spreadsheet-zip/
Android for Work information	• How Android for Work protects your apps and data • Data encryption for Android for Work	http://www.google.com/work/android/
Samsung KNOX Workspace information	• How Samsung KNOX Workspace protects your apps and data • Data encryption for Samsung KNOX Workspace	http://www.samsungknox.com/en/products/knox-workspace/technical
iOS information	• iOS device security	http://www.apple.com/business/docs/iOS_Security_Guide.pdf

Glossary

AES	Advanced Encryption Standard
BlackBerry UEM instance	A BlackBerry UEM instance refers to one installation of the BlackBerry UEM Core and all associated BlackBerry UEM components that communicate with it. The components can be installed on the same server or multiple servers. There can be more than one BlackBerry UEM instance in a BlackBerry UEM domain.
CA	certification authority
CBC	cipher block chaining
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.
DoS	denial of service
DTLS	Datagram Transport Layer Security
FIPS	Federal Information Processing Standards
HMAC	keyed-hash message authentication code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
IT policy	An IT policy consists of various rules that control the security features and behavior of devices.
LAN	local area network
LDAP	Lightweight Directory Access Protocol
NDES	Network Device Enrollment Service
NFC	Near Field Communication

NTLM	NT LAN Manager
OCSP	Online Certificate Status Protocol
PKCS	Public-Key Cryptography Standards
RFC	Request for Comments
SCEP	simple certificate enrollment protocol
SHA	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
space	A space is a distinct area of the device that enables the segregation and management of different types of data, applications, and network connections. Different spaces can have different rules for data storage, application permissions, and network routing. Spaces were formerly known as perimeters.
SRP	Server Routing Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of communication protocols that is used to transmit data over networks, such as the Internet.
TLS	Transport Layer Security
UEM	Unified Endpoint Manager
VPN	virtual private network

Legal notice

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

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

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

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

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

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

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

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario

Canada N2K 0A7

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

Published in Canada