Security Note

Android Devices

Published: 2016-12-22
SWD-20161213103414452

Contents

Document revision history

1

Date	Description
22 December 2016	• Updated the Connecting to a VPN and Protecting work data in transit using BlackBerry Secure Connect Plus topics with information about the new per-app VPN feature. • Updated BES12 product names to BlackBerry UEM product names throughout the document.

Introduction

2

Managing Android devices with BlackBerry UEM provides your organization with many security features, including:

- Commands to lock devices, change device passwords, and delete information from devices
- Password and device controls
- Control of network connectivity
- Abillity to enforce device compliance
- Work app management
- Certificate-based authentication
- Microsoft Exchange gatekeeping
- Full-disk encryption
- Address space layout randomization
- Compliance enforcement on rooted devices
- IT policy rule for device encryption

Secure device management

3

BlackBerry UEM offers several management options (activation types) for Android 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.

The activation type that you choose depends on the type of device and your organization's security requirements. There are activation types for:

- All Android devices
- Android for Work devices
- Samsung KNOX Workspace devices

BlackBerry devices powered by Android, such as PRIV and DTEK50, can use the activation types for all Android devices, as well as the activation types for Android for Work devices.

The security features that are available on a device depend on the type of Android device and its BlackBerry UEM activation type.

Using the BlackBerry UEM Client

The BlackBerry UEM Client allows BlackBerry UEM to communicate with devices.

To activate Android 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

The app uses a FIPS-validated cryptographic module to encrypt all of the data that it stores directly and writes indirectly to files.

Ensuring device compliance

You can use compliance profiles to encourage users to follow your organization’s standards for the use of most devices. A compliance profile defines the device conditions that aren't acceptable in your organization. You can specify whether certain conditions are permitted on Android devices, such as:

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

A compliance profile specifies information, such as:

- 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 is 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 Android 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. 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 for 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. For example, devices ignore rules that apply only to other devices or to a different device OS.

Data at rest

4

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

Encrypting device data

Encryption is used to protect data that's stored on Android devices. Depending on the device type and activation type, BlackBerry UEM supports encryption for data on devices, including:

- IT policy rules for device encryption
- A default rule for Android for Work devices that encrypts all device data during activation (For more information about data encryption for Android for Work, visit https://support.google.com/work/android.)
- A default rule for Samsung KNOX Workspace devices that encrypts the KNOX Workspace using AES-256 encryption during activation. (For more information about data encryption for Samsung KNOX Workspace, visit https://www.samsungknox.com/en/products/knox-workspace/technical.)
- A rule that encrypts all data in the work space and media card on Secure Work Space devices
- Native full-disk encryption offered on Android devices, which ensures that all of a device's data is stored in an encrypted form and accessible only to users who enter an encryption PIN or password

Android devices also offer other encryption and data protection features. For more information, see the Android documentation from Google.

Protecting device memory

Address space layout randomization makes it more difficult for attackers to exploit a device and run their own code. This technique randomizes the location of system components in memory so that attackers find it difficult to know where a vulnerability exists. BlackBerry UEM supports the native address space layout randomization offered on Android.

Trusted Boot verification

Trusted Boot is a Samsung KNOX feature that can verify the kernel and OS when a device is started. Trusted Boot verifies the integrity of a device with a KNOX Workspace so that you know that it isn't running unauthorized firmware. If a user installs

unauthorized firmware, Trusted Boot fuses the KNOX warranty bit, the KNOX Workspace becomes inaccessible, and you can no longer manage the device using Samsung KNOX. Also, if the device is encrypted, it becomes unusable.

By default, Trusted Boot verification is turned off, but you can turn on Trusted Boot verification using the "Enable Trusted Boot verification" IT policy rule. For more information about Trusted Boot, visit https://www.samsungknox.com/en/products/knox-workspace.

TIMA support

TIMA verifies that the device kernel has not been compromised during runtime. For Samsung KNOX Workspace devices, BlackBerry UEM supports the following aspects of TIMA:

- TIMA CCM, which stores client certificates that apps can use to encrypt, decrypt, sign, and verify content. TIMA CCM is similar to a smart card. BlackBerry UEM automatically stores Wi-Fi certificates, certificates required for connectivity with the BlackBerry Infrastructure, shared certificates, user certificates, and user credentials in the TIMA CCM. Only allowed apps in the KNOX Workspace that know the certificate alias can access a certificate that's stored in the TIMA CCM. CA certificates are stored in the certificate store in the KNOX Workspace, not the TIMA CCM. This feature is available for devices that support KNOX 2.1 or later.
- TIMA keystore, which stores the keys used to encrypt the KNOX Workspace and provides apps with services for generating and maintaining cryptographic keys.

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 and control password requirements, such as complexity and length, to ensure that a device meets the requirements of your organization. BlackBerry UEM also provides management options for a lost device, including the ability to lock it remotely. You can do this, for example, if a device is lost or if a user forgets their password.

Deleting 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. BlackBerry UEM allows you to send data wipe commands to devices, or require that devices delete data after a specific time or under specific conditions. For example:

- You can send a command to a device requiring that it delete all of its work data.
- If a user types the work space password incorrectly more times than device settings or BlackBerry UEM allow, the device deletes all work space information and the work space is removed from the device.
- You can send a command to a device requiring that it delete all of its device data.

- If a device is password-protected and the user types the device password incorrectly more times than BlackBerry UEM allows, the device deletes all user information and app data, including information in the work space, and returns the device to factory defaults.

Users can also trigger a data wipe on their devices by using device security options to wipe their devices.

Managing apps on devices

You can use BlackBerry UEM to manage and monitor apps that your organization wants to make available on Android 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.

Depending on the activation type, you can also manage personal apps on devices. You can create a list of restricted apps that you don't want users to install. For example, you can prevent users from installing malicious apps or apps that require a lot of resources.

Data in transit

5

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

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

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

Protecting data in transit over the BlackBerry Infrastructure

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

- BlackBerry UEM sends internal apps and all device management data, such as IT policies, profiles, and IT administration commands, to devices through the BlackBerry Infrastructure, even when the device is connected to a work VPN or work Wi-Fi network.
- Data sent between a device and your organization's mail, web, and content servers travels through BlackBerry UEM and the BlackBerry Infrastructure only when BlackBerry Secure Connect Plus 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 Android devices, it always sends the data through the BlackBerry Infrastructure, even when the device is connected to a work Wi-Fi network or work VPN.

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

How BlackBerry UEM authenticates with the BlackBerry Infrastructure

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

- When BlackBerry UEM sends device management data to an Android 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 Android devices using BlackBerry Secure Connect Plus, BlackBerry UEM uses SRP to authenticate with the BlackBerry Infrastructure and then establishes a secure IP tunnel using DTLS between BlackBerry UEM and the device.

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

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

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

Data flow: Authenticating BlackBerry UEM with the BlackBerry Infrastructure to send device management data

1. BlackBerry UEM connects to the BlackBerry Infrastructure and initiates a TLS connection.
2. The BlackBerry Infrastructure sends an authentication certificate to BlackBerry UEM.
3. BlackBerry UEM performs the following actions:
    - Verifies that the authentication certificate is signed by a trusted CA
    - Verifies the name of the server in the BlackBerry Infrastructure to establish the TLS connection

- Sends a data packet that contains its unique SRP ID and SRP authentication key to the BlackBerry Infrastructure to claim the SRP ID

4. The BlackBerry Infrastructure verifies the SRP ID and SRP authentication key sent by BlackBerry UEM and performs one of the following actions:
   - If the credentials are valid, sends a confirmation to BlackBerry UEM to complete the authentication process and configure an authenticated SRP connection
   - If the credentials aren't valid, stops the authentication process and closes the SRP connection

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

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

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

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

How devices connect to the BlackBerry Infrastructure

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

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

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

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

1. An Android 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

Android devices can connect to your organization's resources such as mail servers, web servers, and content servers, using several communication methods. For example, by default, devices that use BlackBerry Secure Connect Plus to connect to your organization's resources use the following communication methods (in order):

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

Connecting to a VPN

If your organization's environment includes VPNs, such as IPsec VPNs or SSL VPNs, and an Android device and its activation type supports VPN profiles, you can configure it to authenticate with a 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 the VPN concentrator, which acts as the gateway to your organization's network. Each device includes a built-in VPN client that supports several VPN concentrators. Depending on the VPN solution, a client app may need to be installed on the device. The VPN client on the device supports the use of strong encryption to authenticate itself with the VPN concentrator. It creates an encrypted tunnel between the device and the VPN concentrator that the device and your organization's network can use to communicate.

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

You can use per-app VPN for Android for Work devices 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, such as 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 work data in transit using BlackBerry Secure Connect Plus

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

For Samsung KNOX Workspace, all work space apps use the secure tunnel. For Android for Work devices, you can allow all apps to use the tunnel or specify apps using per-app VPN. This tunnel gives users access to work resources behind your organization's firewall while ensuring the security of data using standard protocols and end-to-end encryption.

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

If you configure per-app VPN for BlackBerry Secure Connect Plus, the configured apps always use a secure tunnel connection through BlackBerry Secure Connect Plus, even if the app can connect to the work Wi-Fi network or VPN specified in a Wi-Fi or VPN profile.

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

BlackBerry Secure Connect Plus offers the following advantages:

- The IP traffic that is sent between devices and BlackBerry UEM is encrypted end to end using AES-256, ensuring the security of work data.

- BlackBerry Secure Connect Plus provides a secure, reliable connection to work resources when a device user can't access the work Wi-Fi network or VPN.
- BlackBerry Secure Connect Plus is installed behind your organization's firewall, so data travels through a trusted zone that follows your organization's security standards.

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

Protecting communication with devices using certificates

A certificate is a digital document that binds the identity and public key of a certificate subject. Each certificate has a corresponding private key that's stored separately. A CA signs the certificate to verify that it can be trusted.

Depending on the activation type, Android devices can use certificates to:

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

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

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-

How the certificate is added	Description
	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 device. The administrator must have access to the certificate and private key to send the client certificate to the user.

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. Android devices with activation types that support SCEP 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. The password is sent to the devices to allow the devices to make the certificate request. If you use a static challenge password, all SCEP requests from devices use the same challenge password.

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

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

Managing certificates that a device enrolls using SCEP

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

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

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

Data flow: Enrolling a client certificate to a device using BlackBerry UEM as a proxy for the SCEP request

You can use BlackBerry UEM as a proxy for SCEP requests sent from Android devices to the CA. If the CA is behind your firewall, using BlackBerry UEM as a proxy allows you to enroll client certificates to devices without exposing the CA outside of the firewall.

1. BlackBerry UEM sends a SCEP profile that is assigned to the user or associated with an assigned Wi-Fi, VPN, or email profile to the device.
2. The device generates a SCEP request and sends it to the BlackBerry Infrastructure.
3. The BlackBerry Infrastructure sends the SCEP request to BlackBerry UEM.
4. BlackBerry UEM updates the URL for the SCEP request and sends the SCEP request to the CA.
5. The CA issues the certificate and sends it to BlackBerry UEM.
6. BlackBerry UEM sends the SCEP request to the BlackBerry Infrastructure.
7. The BlackBerry Infrastructure sends the SCEP request to the device.
8. The device adds the certificate and corresponding private key to the keystore.

Sending CA certificates to devices

You might need to distribute CA certificates to Android 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 an S/MIME-protected email message is received.

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

Protecting email messages

Devices support using Exchange ActiveSync to synchronize email messages, calendar entries, contacts, and other organizer data with your organization’s mail server. BlackBerry 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.

Extending email security

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

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

BlackBerry UEM and some Android devices and activation types support S/MIME.

S/MIME

You can extend messaging security for BlackBerry UEM and permit users to sign, encrypt, or sign and encrypt messages using S/MIME when they use a work email account that supports S/MIME-protected messages on Android devices and activation types that support S/MIME. 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.

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

Data flow: Sending an email message from an Android device using S/MIME encryption

1. A user sends an email message from an Android 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. Sends the encrypted message to the mail server

2. The mail server sends the S/MIME-encrypted message to the recipient.
3. The recipient decrypts the S/MIME-encrypted message using the recipient's S/MIME private key.

Related resources

6

For more information, read the following documents:

Title	Description	Web address
BlackBerry UEM Administration Guide	• Feature details and the devices that support them • Activation types • 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
BES12 Cloud Security Note	• BES12 Cloud infrastructure security • BlackBerry data center security • Data in transit security	http://help.blackberry.com/en/bes12-cloud-security/current/bes12-cloud-security-note/BES12-Cloud-latest-Security-Note-en.pdf
Policy Reference Spreadsheet	• IT policy rule names, descriptions, and details	http://help.blackberry.com/detectLang/blackberry-uem/current/policy-reference-spreadsheet-zip/
BlackBerry powered by Android Security Guide	Security features of BlackBerry devices powered by Android, such as PRIV and DTEK50	http://help.blackberry.com/en/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
Android information	Android for Work security	https://www.google.com/work/android/
	Samsung KNOX Workspace security	https://www.samsungknox.com/en/products/knox-workspace/technical

Glossary

7

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
CCM	Client Certificate Management
DTLS	Datagram Transport Layer Security
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standards
HMAC	keyed-hash message authentication code
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.
LDAP	Lightweight Directory Access Protocol
NDES	Network Device Enrollment Service
PIN	personal identification number
S/MIME	Secure Multipurpose Internet Mail Extensions
SCEP	simple certificate enrollment protocol
SHA	Secure Hash Algorithm
SRP	Server Routing Protocol
SRP ID	The SRP ID is a unique identifier that an EMM solution from BlackBerry uses to identify itself to the BlackBerry Infrastructure during SRP authentication.
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TIMA	ARM TrustZone based Integrity Measurement Architecture
TLS	Transport Layer Security

UDP	User Datagram Protocol
UEM	Unified Endpoint Manager
VPN	virtual private network

Legal notice

8

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

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

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

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

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

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

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

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

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

Published in Canada