BLACKBERRY (BB) UNIFIED ENDPOINT MANAGEMENT (UEM) SUPPLEMENTAL PROCEDURES

Version 2, Release 1

22 January 2021

Developed by BlackBerry and DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

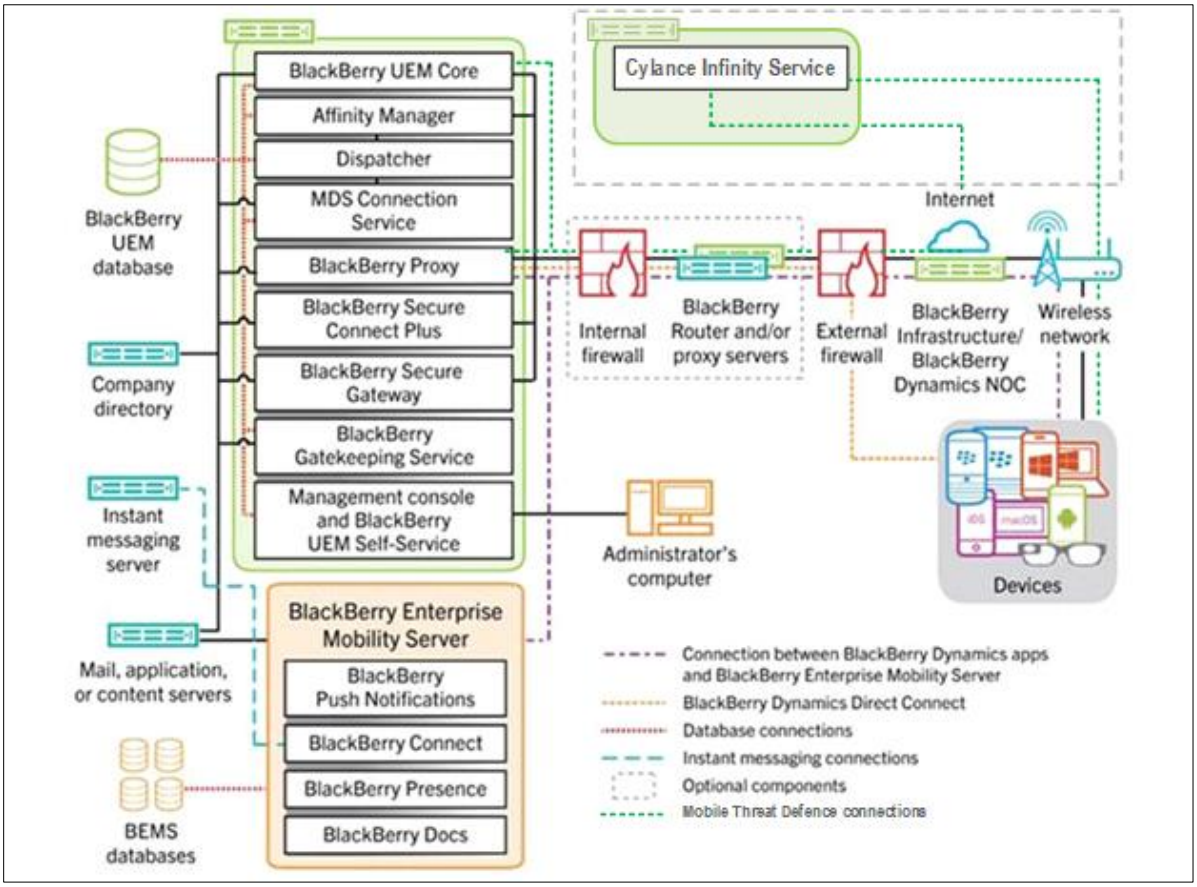
LIST OF FIGURES

Page

1. UEM SECURITY AND CONFIGURATION INFORMATION

1.1 Architecture

Figure 1-1: UEM Architecture



1.1.1 Network Configuration

BlackBerry UEM requires an outbound-initiated, bidirectional connection through port 3101 on the firewall and over the internet to the BlackBerry Infrastructure to transport data to and from the devices. BlackBerry UEM requires the following configurations on the host-based or appliance firewall:

- DNS
  - Support for resolving IP addresses into host names
- Proxy Firewall
  - If the user's organization uses a proxy firewall, a proxy that does not change incoming or outgoing data (transparent proxy) should be used
- BlackBerry Infrastructure
  - Exclusive use of port 3101 to open and maintain an outbound-initiated, bidirectional TCP/IP connection to the BlackBerry Infrastructure

  - Use of port 443 to register activation information with the BlackBerry Infrastructure (outgoing HTTPS connection)
- BlackBerry UEM Self-Service and BlackBerry UEM Management Console
  - Use of ports 8000 and 443

  Note: If port 443 is not available, the setup application tries to use port 8008. If port 8008 is not available, the setup application assigns a port value from the range of 12000 to 12999.

If the default ports required for the BlackBerry UEM Self-Service and BlackBerry UEM Management Console are not available, or need to be changed for any reason, the ports can be reconfigured using the BlackBerry UEM Configuration tool.

Configure the organization's firewall to allow outbound two-way connections over these ports.

Table 1-1: Outbound Ports

From	To	Port (TCP)
BlackBerry 10 iOS Android Windows devices	BlackBerry Infrastructure	443
BlackBerry UEM	BlackBerry Infrastructure	3101
iOS	APNs	5223
Android	GCM Note: FCM will replace GCM.	5228 5229 5230

Note: BlackBerry UEM uses port 8889 for identity management for BlackBerry 10 devices and to handle SCEP requests for BlackBerry Secure Connect Plus.

Table 1-2: Listening Ports

Port (TCP)	Description
1610	The port that the BlackBerry UEM Core uses to provide SNMP monitoring data.
1611	The port that SNMP clients can use to query monitoring data for BlackBerry Secure Connect Plus.
1612	The default port that is used for SNMP monitoring for the BlackBerry Secure Gateway. This port can be changed in the management console.
1613	The default port that is used for SNMP monitoring for the BlackBerry Cloud Connector.
1620	The port that the BlackBerry UEM Core uses to send SNMP notifications in an IPv4 environment.

Port (TCP)	Description
3202	The port that the active BlackBerry Affinity Manager listens on for RCP connections from the BlackBerry Dispatcher.
3203	The port that the BlackBerry Dispatcher listens on for BIPPe connections from the BlackBerry MDS Connection Service.
8000	The ports that BlackBerry UEM Self-Service and the management console listen on for HTTPS connections.
443	If 443 is not available, the setup application tries to use port 8008. If port 8008 is not available, the setup application assigns a port value from the range of 12000 to 12999.
8085	The port that the active BlackBerry Affinity Manager listens on for REST notifications.
8087	The primary BlackBerry UEM components and any BlackBerry Connectivity Node instances send BlackBerry Secure Gateway traffic to this port.
8095	This port is reserved for secure REST communication between external systems and BlackBerry UEM plug-ins.
8100	The BlackBerry UEM Core uses this port to check the status of the UEM management console.
8102	The BlackBerry UEM Core uses this port to check the status of BlackBerry Secure Connect Plus.
8103	The BlackBerry UEM Core uses this port to obtain the status of the BlackBerry Secure Gateway. The status is displayed in the management console.
8182	The BlackBerry UEM Core uses this port to obtain the status of the BlackBerry Collaboration Service.
8448	The port that is used for internal communication between the BlackBerry UEM Core and the management console and BlackBerry UEM Self-Service.
8543	Defines the listening port for UI Certificate Based Authentication service. The default value is 8543.
8881	The port that BlackBerry UEM uses to receive management requests for BlackBerry 10 devices. The connection uses mutual authentication with ECC certificates.
8882	The port that BlackBerry UEM uses to receive enrollment requests for BlackBerry 10 devices.
8883	The port that BlackBerry UEM uses to receive enrollment requests for iOS, Android, and Windows Phone devices.
8884	The port that BlackBerry UEM uses to receive management requests for iOS, Android, and Windows Phone devices. The connection uses mutual authentication with RSA certificates.
8885	An additional port that BlackBerry UEM uses to receive management requests for iOS devices. The connection uses mutual authentication with RSA certificates.

Port (TCP)	Description
8887	The port that BlackBerry UEM uses for authenticated connections to check the status of BlackBerry UEM instances.
8889	The port that the BlackBerry UEM Core uses for identity management for BlackBerry 10 devices and to handle SCEP requests for BlackBerry Secure Connect Plus (the BlackBerry UEM Core acts as the CA).
8890	The port that BlackBerry Secure Connect Plus and the BlackBerry Gatekeeping Service use to obtain configuration and authorization data and certificates. The BlackBerry Gatekeeping Service also uses this port for gatekeeping operations.
8891	Certain BlackBerry Infrastructure services use this mutually authenticated port to connect with BlackBerry UEM.
8892	When BlackBerry Secure Connect Plus and the BlackBerry Gatekeeping Service are installed with the primary BlackBerry UEM components, they use this port to obtain configuration and authorization data and certificates. The BlackBerry Gatekeeping Service also uses this port for gatekeeping operations.
8893	This port supports connections to the BlackBerry UEM Core from the BlackBerry 2FA app on BlackBerry 10 devices (10.3.2 or earlier).
8894	The BlackBerry UEM Core health can be collected on this port. This functionality is available only for deployments of BlackBerry UEM Cloud.
8895	The BlackBerry UEM Core uses this port to receive requests from external services such as BEMS, BlackBerry Connect, and BlackBerry Workspaces.
8896	BlackBerry UEM listens on this port for REST requests from BlackBerry Dynamics apps. This port uses GDAuthToken-based authentication.
8897	BlackBerry UEM listens on this port when the user is upgrading to BlackBerry UEM version 12.8 so that it can communicate with Windows Phone 8 devices. For more information, visit http://support.blackberry.com/kb to read article KB48098.
8900	The secure SSL port that the BlackBerry Gatekeeping Service listens on.
10080	The HTTP port that the BlackBerry MDS Connection Service listens on for enterprise push data.
10443	The HTTPS port that the BlackBerry MDS Connection Service listens on for enterprise push data. This port is used when the user turns on push encryption.

Port (TCP)	Description
11001	The port that BlackBerry Secure Connect Plus uses to listen for signaling requests from the BlackBerry Infrastructure.
17080	BlackBerry Proxy listens on this port for connections from application servers. **Note**: The default port must be used. The setup application does not assign an alternate port if the default port is not available.
17317	BlackBerry Control listens on this port for container management data. **Note**: The default port must be used. The setup application does not assign an alternate port if the default port is not available.
17433	BlackBerry Proxy listens on this port for SSL connections from application servers. **Note**: The default port must be used. The setup application does not assign an alternate port if the default port is not available.
17443	BlackBerry Control listens on this port for HTTP connections. **Note**: The default port must be used. The setup application does not assign an alternate port if the default port is not available.
17443	BlackBerry Control listens on this port for SSL connections. **Note**: The default port must be used. The setup application does not assign an alternate port if the default port is not available.
17533	BlackBerry Proxy listens on this port for SSL connections. **Note**: The default port must be used. The setup application does not assign an alternate port if the default port is not available.
18084	The port that applications can use to send data to the BlackBerry Web Services.
38082	The port that the BlackBerry UEM Core listens on to route email notification traffic through the BlackBerry Infrastructure to the APNs for iOS devices.
38083	The port that the BlackBerry UEM Core listens on for migration requests when the user moves devices from BES10 to BlackBerry UEM.
38086	The port that the user's organization's TCP proxy server or the BlackBerry Router listens on for data that BlackBerry UEM sends to the APNs.
38087	The BlackBerry UEM Core listens on this port to route traffic for BlackBerry Enterprise Identity through the BlackBerry Infrastructure.

1.2 Identification and Authentication

1.2.1 Passwords

Authentication to BlackBerry UEM can be configured to use local authentication or an enterprise authentication mechanism, such as Active Directory. The STIG requires that UEM administrators use Active Directory-managed authentication. Management and protection of local server accounts and their access, as well as enforcement of required password rules and policies, is managed by the host operating system. When logging on to the BlackBerry UEM console, passwords are obfuscated. The STIG requires the BlackBerry UEM to be configured to use an enterprise authentication mechanism.

Negotiated keys/passwords are negotiated through established and approved key agreement schemes using FIPS-validated cryptographic modules. All communication between the mobile device and BlackBerry UEM is encrypted.

The BlackBerry UEM server does not currently support the functionality to block access to specific servers and/or network shares; however, this can be accomplished through the corporate infrastructure through BlackBerry Mobile Data System (MDS) and corporate Wi-Fi/VPN, which should be directed through a proxy server to allow these controls. BlackBerry UEM access should be limited to only systems that enforce local Common Access Card (CAC) authentication.

1.2.2 Certificates

Management of certificates on the server hosting BlackBerry UEM, including verification, validation, and protection, is the responsibility of the host operating system.

A DoD PKI-issued certificate must be used during the installation of BlackBerry UEM. If a self-signed certificate was used during server installation, it must be replaced with a DoD PKI-issued certificate.

Certificate verification and handling of email security-related tasks, such as confirmation of certificate validity, is not configured on the BlackBerry UEM server. Device-side certificate and security functions relating to the mobile email client are built into the mobile operating system and are addressed in the applicable operating system Security Requirements Guide (SRG) and related documentation.

1.3 Maintenance

Access management and control for nonlocal maintenance and diagnostic sessions are managed by the host operating system and are out of scope for BlackBerry UEM.

1.4 Media Protection

Access to and control of removable media and other storage used by BlackBerry UEM are managed by the host operating system.

1.5 System and Communication Protection

1.5.1 Cryptographic Support

BlackBerry UEM uses the BlackBerry Cryptographic Java Module cryptographic modules, validated under FIPS 140-2 Certificate number 3391, for all cryptographic support. Data in transit between BlackBerry UEM and the BlackBerry mobile devices is protected using AES-256 encryption.

1.5.1.1 Public Key Cryptography

BlackBerry UEM supports software-based asymmetric key technology. Certificates can be managed by BlackBerry UEM. The BlackBerry UEM administrator can use CA Certificate profiles to publish required DoD certificates, including DoD root and intermediate certificates to be stored in the certificate store on the BlackBerry mobile device. Public key cryptography is used during the activation process when using the Web Desktop Manager.

1.5.2 System Protection

Protection of the BlackBerry UEM and any storage of data used by and/or created by the BlackBerry UEM are managed by the host operating system. This includes storage and protection of any keys, certificates, and/or protected classified information.

BlackBerry UEM does not contain a device integrity system, as the BlackBerry mobile OS is designed to be tamper resistant. The kernel performs an integrity test when the BlackBerry mobile OS starts, and if the integrity test detects damage to the kernel, the device does not start.

The UEM client applications installed on third-party devices perform integrity tests when the application starts, such as Attestation device integrity checking for Samsung devices, as well as compliance checks for jailbroken or rooted devices.

In addition to the kernel protection, the system controls built into the BlackBerry mobile OS and BlackBerry UEM prevent the user from loading uncontrolled software or software from non-approved locations.

2. OPERATIONAL CONSIDERATIONS

2.1 Management of iOS, Android, Windows, and macOS Devices in the DoD Environment

2.1.1 General

In the DoD environment, mobile devices that store or process sensitive DoD information must be configured to support either a work-only processing environment where no personal applications or data are installed or two processing environments: one for work applications and data and one for personal applications and data. When work and personal processing environments are used, personal applications must not be able to access work data. The Mobile Device Fundamentals Protection Profile (MDFPP) defines technical requirements for data separation between the work and personal processing environments.

BlackBerry UEM supports a broad range of technologies and activation types that provide data separation features compliant with the MDFPP, including iOS-managed and -unmanaged apps, Samsung Knox[1], and Android Enterprise[2]. DISA-developed operating system STIGs are MDM product independent and therefore do not contain UEM-specific configuration and activation type information. The sections below provide additional information needed when using UEM to manage DoD iOS, Android, Windows, and macOS mobile devices.

2.1.2 Apple iOS

UEM supports the following additional security-related controls not described in the latest iOS STIG. The AO must decide how best to implement these additional controls in their environment.

- Compliance enforcement of jailbroken devices
- Connectivity to the DoD network via BlackBerry Secure Connect Plus

The "MDM controls" activation type supported by UEM is the same as the environment assumed by the iOS STIG. Personal and work data is separated using the native iOS-managed and -unmanaged app concept. BlackBerry Dynamics can also be used to provide an alternate method for meeting DoD requirements for data separation between work and personal data. The "User privacy" activation type should not be used because it does not support MDM control of the device.

[1] Samsung will be deprecating Knox for enterprise mobile security. In future updates, Workspace Advanced Profile Owner (PO) will replace Knox BYOD, and Knox BYOD will automatically convert to Workspace Advanced PO. Workspace Advanced Device Owner (DO) with Knox will replace Knox COM.
[2] Section 2.2 describes all data separation/container technologies supported by UEM.

2.1.3 Android

UEM supports the following additional security-related controls not described in the latest Samsung with Knox STIG. The AO must decide how best to implement these additional controls in their environment.

- Compliance enforcement of rooted devices
- Connectivity to the DoD network via BlackBerry Secure Connect Plus

2.1.3.1 Android Enterprise

UEM supports two activation types for Android Enterprise devices for the DoD environment: "Work and personal – user privacy" and "Work space only". When the Work and personal activation type is used, DoD policy requires that specific device-level, MDM-managed controls be available: device unlock password; personal data encryption; ability to enable/disable microphone, camera, and radios; and ability to allow/disallow personal app installation.

2.1.3.2 Samsung Android with Knox

The "Work and personal – full control" and "Work space only" activation types supported by UEM are the same as the environments assumed by the Samsung Android Knox STIG. Work and personal data are separated via the Knox container.

2.1.3.3 Other Android

For non-Samsung Knox and Android Enterprise devices, the "User Privacy" activation type should be used with Blackberry Dynamics to provide requisite data separation between work and personal data.

2.1.4 Windows

For Windows 10 Mobile, the "MDM controls" activation type supported by UEM is the same as the environment assumed by the Windows 10 Mobile STIG. Personal and work data is separated using Windows Information Protection (WIP).

In the DoD, UEM cannot be used to manage domain-joined Windows 10 devices because the Windows 10 STIG does not allow MDM management of Windows 10 devices. The Windows 10 STIG requires Active Directory management of Windows 10 platforms. Windows STIGs are developed by the DoD Windows Consensus Group, which consists of key stakeholders in the DoD.

2.1.5 macOS

The macOS STIG is developed by DISA and Apple. The macOS STIG allows an MDM to deploy configuration profiles on DoD macOS platforms.

2.2 Data Separation and Container Technologies

UEM supports a number of technologies that are compliant with MDFPP requirements for data separation of work and personal processes. A specific data separation technology is usually tied to a specific device activation type.

Table 2-1: Device and Data Separation

Device OS	Description
Android	• Android Enterprise • Knox Workspace • BlackBerry Dynamics applications
BlackBerry 10	• BlackBerry Balance
iOS	• iOS-managed open in BlackBerry Dynamics applications
macOS	• BlackBerry Dynamics applications
Windows 10	• BlackBerry Dynamics applications • Windows Information Protection (WIP)

2.3 Activation Types Supported by UEM

Table 2-2 lists all device activation types by supported operating system for UEM.

Note: Some activation types in the list are not allowed in the DoD environment. See Section 2.1 and the BlackBerry OS 10.x STIG for more information.

Note: Support for Samsung Knox policies on Android Enterprise for all BlackBerry UEM activations, Samsung Knox, is now available to Samsung Knox devices when the devices are activated with an Android Enterprise activation type. Samsung Knox devices that are activated with an Android Enterprise activation type now have Samsung Knox policies applied. Even though devices already activated with a Samsung Knox activation type continue to work, the Android Enterprise activation types are recommended for new activations.

Table 2-2: Android Enterprise Activation Supported Types

Activation Type	Description
Samsung Knox activation type	Android Enterprise activation type
Work and personal – full control (Samsung Knox)	Work and personal – full control (Android Enterprise fully managed device with work profile) Knox MDM policies applied to the device. If Knox policies are required to be applied in the workspace, select "When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus". **Note**: For all non-Samsung devices, such as Google Pixel, the AE activation type needed should be used.
Work and personal – user privacy (Samsung Knox)	Work and personal – user privacy (Android Enterprise): **No Knox** policies are applied to the device. If required in the workspace, select "When activating Android Enterprise devices enable premium UEM functionality such as BlackBerry Secure Connect Plus".
Work space only (Samsung Knox)	Workspace only (Android Enterprise): Knox MDM policies applied to the device. If Knox policies are required to be applied in the workspace, select "When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus".

Table 2-3: UEM Supported Device Activation Types

Activation Type	Description	Devices
Work and personal – Corporate	This activation type provides control of work data on devices while ensuring privacy for personal data. When a device is activated, a separate workspace is created on the device, and the user must create a password to access the workspace. Work data is protected using encryption and password authentication. All work data from any previous activations is deleted. The user can control the workspace on the device using commands and IT policies but cannot control any aspects of the personal space on the device.	BlackBerry 10
Work space only	This activation type provides full control of the device and does not provide a separate space for personal data. When a device is activated, the personal space and all work data from any previous activation is removed, a workspace is installed, and	BlackBerry 10

Activation Type	Description	Devices
	the user must create a password to access the device. Work data is protected using encryption and password authentication. The user can control the device using commands and IT policies.	
Work and personal – Regulated	This activation type provides control of both work and personal data. When a device is activated, a separate workspace is created on the device and the user must create a password to access the workspace. Work data is protected using encryption and password authentication. All work data from any previous activations is deleted. The user can control both the workspace and the personal space on the device using commands and IT policies.	BlackBerry 10
MDM controls	This activation type provides basic device management using device controls made available by iOS. A separate workspace is not installed on the device, and there is no added security for work data. The user can control the device using commands and IT policies. During activation, users must install a mobile device management profile on the device. On OS X, the device and the user are set up as separate entities on BlackBerry UEM. Separate communication channels are established between BlackBerry UEM and the device and BlackBerry UEM and the user account, allowing the user to manage the device and the user separately. • For Knox, applies to the Knox MDM IT policies • For Windows devices, provides basic device management using device controls made available by Windows 10 and Windows 10 Mobile	iOS, macOS, all Android devices including Motion, KeyONE, KeyTWO, PRIV, Motion, DTEK50 and DTEK60, Windows 10, and Windows 10 Mobile
User privacy	The user can use the User privacy activation type to provide basic control of devices while making sure that users' personal data remains private. With this activation type, no separate container is installed on the device, and no added security for work data is provided. Devices activated with User privacy are activated on BlackBerry UEM and can use services	iOS, Android

Activation Type	Description	Devices
	such as Find my Phone and Root Detection, but administrators cannot control device policies.	
Work and personal – user privacy (Android Enterprise)	This activation type maintains privacy for personal data but allows the user to manage work data using commands and IT policy rules. This activation type creates a work profile on the device that separates work and personal data. Work and personal data are both protected using encryption and password authentication. This activation type does not support BlackBerry Secure Connect Plus.	Android Enterprise
Work and personal – user privacy (Android Enterprise – Premium)	This activation type maintains privacy for personal data but allows the user to manage work data using commands and IT policy rules. This activation type creates a work profile on the device that separates work and personal data. Work and personal data are both protected using encryption and password authentication. The user must choose this activation type if they want to support BlackBerry Secure Connect Plus with the features of the Work and personal – user privacy (Android Enterprise) activation type.	Android Enterprise
Work space only (Android Enterprise)	This activation type allows the user to manage the entire device using commands and IT policy rules. This activation type requires the user to reset the device to factory settings before activating. The activation process installs a work profile and no personal profile. The user must create a password to access the device. All data on the device is protected using encryption and a method of authentication such as a password. This activation type does not support BlackBerry Secure Connect Plus.	Android Enterprise
Work space only (Android Enterprise – Premium)	This activation type lets the user manage the entire device using commands and IT policy rules. This activation type requires the user to reset the device to factory settings before activating. The activation process installs a work profile and no personal profile. The user must create a password to access the device. All data on the device is protected using encryption and a method of authentication such as a password. During activation, the device installs the	Android Enterprise

Activation Type	Description	Devices
	BlackBerry UEM Client automatically and grants it Administrator permissions. Users cannot revoke the Administrator permissions or uninstall the app. The user must choose this activation type if they want to support BlackBerry Secure Connect Plus with the features of the Workspace only (Android Enterprise) activation type.	
Work and personal – full control (Samsung Knox)	This activation type allows the user to manage the entire device using commands and the Knox MDM and Knox Workspace IT policy rules. This activation type creates a separate workspace on the device, and the user must create a password to access the workspace. Data in the workspace is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. This activation type supports the logging of device activity (SMS, MMS, and phone calls) in BlackBerry UEM log files.	Samsung Knox devices that support Knox Workspace
Work and personal – user privacy (Samsung Knox)	This activation type maintains privacy for personal data but allows the user to manage work data using commands and IT policy rules. This activation type does not support the Knox MDM IT policy rules. This activation type creates a separate workspace on the device, and the user must create a password to access the workspace. Data in the workspace is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. The user must also create a Screen lock password to protect the entire device and will not be able to use USB debugging mode.	Samsung Knox devices that support Knox Workspace
Work space only (Samsung Knox)	This activation type allows the user to manage the entire device using commands and the Knox MDM and Knox Workspace IT policy rules. This activation type removes the personal space and installs a workspace. The user must create a password to access the device. All data on the device is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint.	Samsung Knox devices that support Knox Workspace

2.4 Purebred PKI Extension Management

BlackBerry extends the certificate-based authentication provided by Purebred PKI services to the devices and applications that are managed with BlackBerry UEM. Purebred is supported across all key platforms used by the Department of Defense (DoD), such as native iOS, Android, Android Enterprise, Samsung Knox, Windows 10, and BlackBerry 10.

Purebred (derived credentials) deployments are enabled by extending the certificate-based authentication provided by PKI services to the devices and apps that are managed with BlackBerry UEM. To connect BlackBerry UEM to the app-based PKI solution, the UEM and device need to be configured.

The application must be installed on a device that communicates with a certification authority (CA) to enroll certificates and add them to the device. DoD can use the Purebred app-based PKI solution to provide certificates for use by BlackBerry Dynamics apps.

To use an app-based PKI solution with iOS devices, the user must add a connection between BlackBerry UEM and the PKI provider. This task is not required to use an app-based PKI solution with only Android devices.

If the PKI app that retrieves certificates from the CA is not a BlackBerry Dynamics app, the BlackBerry UEM Client communicates with the PKI app to get the certificates and provide them to BlackBerry Dynamics apps. Verify that the app that retrieves certificates for use by BlackBerry Dynamics apps is in the app list in BlackBerry UEM.

Additional information is available at https://docs.blackberry.com/en/endpoint-management/blackberry-uem/12_11/administration/pki-certificates/jth1399034187513

2.4.1 Android

Purebred enables the DoD to authenticate mobile identity. The Purebred application can be deployed by UEM administrators into the workspace.

Once deployed, the device user needs to use it and follow whatever process Purebred has defined for users to obtain their keys/certificates. These keys/certificates are placed in the Android native key store and can then be used by any application (including the dynamics apps) that is deployed into the work space. The dynamics applications can be configured to use the keys from the native key store (via the user credential profile in UEM).

2.4.2 iOS

On iOS, to enable third-party apps to use derived credentials, leverage the key sharing interface of the Purebred application. The key sharing interface uses Apple’s document provider extensions to share PKCS 12 objects between a key management application and an application for which keys are to be used. Sample code that identifies this is available at https://github.com/purebred.

For iOS 13, in the email Exchange payload, set the following to “True” to allow users to select Purebred-issued credentials for signed and encrypted email:

SMIMESigningUserOverrideable;

SMIMESigningCertificateUUIDUserOverrideable;

SMIMEEncryptByDefaultUserOverrideable;
SMIMEEncryptionCertificateUUIDUserOverrideable

2.5 Mobile Threat Defense

BlackBerry UEM includes device management and a compliance infrastructure that includes malware and unsafe URL detection. This leverages an AI and machine learning engine called Infinity identified in Figure 1-1: UEM Architecture. Additionally, BlackBerry applications monitor and enforce security standards at the device and user level. This feature and function are fully integrated into existing components of the overall UEM server and device architecture. CylanceINFINITY is an evolution to whitelisting or blacklisting. This service is not enabled by default. See the product overview for more information.

Note: BlackBerry UEM also includes enterprise infrastructure that manages adaptive security requirements and behaviors of user devices and work applications. BlackBerry Intelligent Security (BIS) enables BlackBerry UEM to apply device configurations to enable user behaviors that make it easier to access work applications and resources securely. This service is not enabled by default. See the product overview for more information.

2.6 Samsung Knox Dual Layer Data-at-Rest (DAR)

When the user is not using the Samsung device, all data in the Knox Workspace is locked and cannot be accessed by apps running in the background. In an Activation profile, a user can specify whether to use the default Dual DAR app or an internal app to encrypt the workspace. Devices that support Samsung Knox Dual DAR encryption can now have Knox Workspace data secured using two layers of encryption.