BLACKBERRY UNIFIED ENDPOINT MANAGER (UEM)
12.7
SUPPLEMENTAL PROCEDURES

Version 1, Release 1

11 December 2017

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

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. SECURITY READINESS REVIEW

1.1 General

When conducting a BlackBerry Unified Endpoint Manager (UEM) 12.7 Security Readiness Review (SRR), the Team Lead and the assigned Reviewer identify security deficiencies and provide data from which to predict the effectiveness of proposed or implemented security measures associated with UEM 12.7.

1.2 Mobile Policy Review

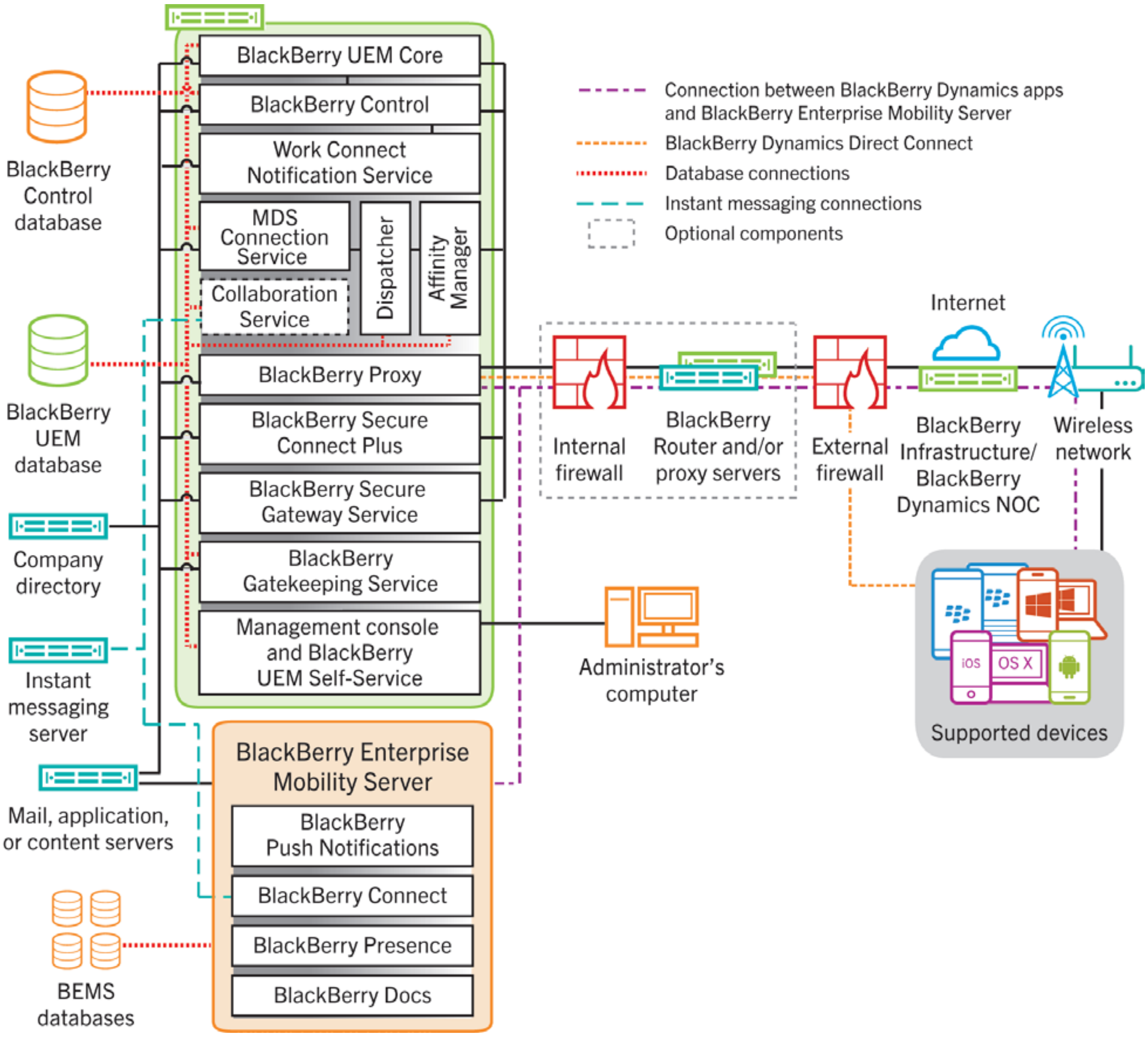
Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website located at: http://iase.disa.mil/stigs/mobility/Pages/policies.aspx.

Use the Mobility Policy STIG and the CMD Management Policy STIG to review the UEM 12.7 asset.

2. UEM SECURITY AND CONFIGURATION INFORMATION

2.1 Architecture

Figure 2-1: UEM Architecture


BlackBerry UEM Core
BlackBerry Control
Work Connect Notification Service
MDS Connection Service
Dispatcher
Affinity Manager
Collaboration Service
BlackBerry Proxy
BlackBerry Secure Connect Plus
BlackBerry Secure Gateway Service
BlackBerry Gatekeeping Service
Management console and BlackBerry UEM Self-Service
BlackBerry Control database
BlackBerry UEM database
Company directory
Instant messaging server
Mail, application, or content servers
BEMS databases
BlackBerry Enterprise Mobility Server
BlackBerry Push Notifications
BlackBerry Connect
BlackBerry Presence
BlackBerry Docs
Connection between BlackBerry Dynamics apps and BlackBerry Enterprise Mobility Server
BlackBerry Dynamics Direct Connect
Database connections
Instant messaging connections
Optional components
Internet
Internal firewall
BlackBerry Router and/or proxy servers
External firewall
BlackBerry Infrastructure/ BlackBerry Dynamics NOC
Wireless network
Administrator's computer
iOS
OS X
Supported devices

2.1.1 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 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 your organization's firewall to allow outbound two-way connections over these ports.

Table 2-1: 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	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. BlackBerry UEM must be able to access this port to support devices running BlackBerry 10 OS version 10.3 or later.

Table 2-2: 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.

Port (TCP)	Description
1620	The port that the BlackBerry UEM Core uses to send SNMP notifications in an IPv4 environment.
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 443	The ports that BlackBerry UEM Self-Service and the management console listen on for HTTPS connections. 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.
8091	The secure SSL port that the BlackBerry Work Connect Notification Service listens on.
8093	The port that the administration console uses to connect to the BlackBerry UEM Core.
8102	The port that the BlackBerry UEM Core uses to check the status of BlackBerry Secure Connect Plus.
8448	The port that is used for internal communication between the BlackBerry UEM Core and the management console and BlackBerry UEM Self-Service.
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.
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). **Note**: BlackBerry UEM must be able to access port 8889 to support devices running BlackBerry 10 OS version 10.3 or later.
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.
8900	The secure SSL port that the BlackBerry Gatekeeping Service listens on.

Port (TCP)	Description
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 push encryption is turned on.
11001	The port that BlackBerry Secure Connect Plus uses to listen for signaling requests from the BlackBerry Infrastructure.
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 devices are moved from BlackBerry UEM10 to BlackBerry UEM.
38085	The port that supports Secure Work Space traffic from iOS and Android devices through the BlackBerry UEM Core and BlackBerry Infrastructure to connect to work resources.
38086	The port that your organization’s TCP proxy server or the BlackBerry Router listens on for data that BlackBerry UEM sends to the APNs.

2.2 Identification and Authentication

2.2.1 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.

2.2.2 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.

2.3 Maintenance

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

2.4 Media Protection

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

2.5 System and Communication Protection

2.5.1 Cryptographic Support

BlackBerry UEM uses the BlackBerry Cryptographic Java Module cryptographic modules, validated under FIPS 140-2 Certificate number 2504, for all cryptographic support. Data in transit between BlackBerry UEM and the BlackBerry mobile devices is protected using AES-256 encryption.

2.5.1.1 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.

2.5.2 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.

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.

3. OPERATIONAL CONSIDERATIONS

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

3.1.1 General

In the DoD environment, mobile devices that store or process sensitive DoD information must be configured to support a work-only processing environment where no personal applications or data are installed or configured to support 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, and Android for Work[1]. 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.

3.1.2 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.

3.1.3 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.

[1] Section 3.2 describes all data separation/container technologies supported by UEM.

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

3.1.3.1 Android for Work

UEM supports two activation types for Android for Work 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 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.

3.1.3.2 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.

3.1.3.3 Other Android

For Non-Samsung Knox and Android for Work devices, the “MDM controls” activation type should be used with Blackberry Dynamics to provide requisite data separation between work and personal data.

3.1.4 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 are 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.

3.1.5 macOS

macOS STIGs are developed by the DoD macOS Consensus Group, which consists of key stakeholders in the DoD. The macOS STIG allows an MDM to deploy configuration profiles on DoD macOS platforms.

3.2 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. It should be noted that a specific data separation technology is usually tied to a specific device activation type.

Table 3-1: Device and Data Separation

Device OS	Description
Android	• Android for Work • 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)

3.3 Activation Types Supported by UEM

Table 3-2 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 3.1 and the BlackBerry OS 10.x STIG for more information.

Table 3-2: UEM Supported Device Activation Types

Activation Type	Description	Devices
Work and personal – Corporate	This activation type provides control of work data on devices while making sure that there is privacy for personal data. When a device is activated, a separate work space is created on the device and the user must create a password to access the work space. Work data is protected using encryption and password authentication. All work data from any previous activations is deleted. You can control the work space on the device using commands and IT policies, but you 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	BlackBerry 10

Activation Type	Description	Devices
	personal data. When a device is activated, the personal space and all work data from any previous activation is removed, a work space is installed, and the user must create a password to access the device. Work data is protected using encryption and password authentication. You can control the device using 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 work space is created on the device and the user must create a password to access the work space. Work data is protected using encryption and password authentication. All work data from any previous activations is deleted. You can control both the work space 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 work space is not installed on the device, and there is no added security for work data. You 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 you 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 PRIV and DTEK50, Windows 10, Windows 10 Mobile
User privacy	You 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	iOS, Android

Activation Type	Description	Devices
	provided. Devices activated with User privacy are activated on BlackBerry UEM and can use services such as Find my Phone and Root Detection, but administrators cannot control device policies.	
Work and personal – user privacy (Android for Work)	This activation type maintains privacy for personal data but lets you 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 for Work
Work and personal – user privacy (Android for Work – Premium)	This activation type maintains privacy for personal data but lets you 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. You must use this activation type if you want to support BlackBerry Secure Connect Plus with the features of the Work and personal - user privacy (Android for Work) activation type.	Android for Work
Work space only (Android for Work)	This activation type lets you 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 for Work
Work space only (Android for Work – Premium)	This activation type lets you 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	Android for Work

Activation Type	Description	Devices
	encryption and a method of authentication such as a password. During activation, the device installs the BlackBerry UEM Client automatically and grants it Administrator permissions. Users cannot revoke the Administrator permissions or uninstall the app. You must use this activation type if you want to support BlackBerry Secure Connect Plus with the features of the Work space only (Android for Work) activation type.	
Work and personal – full control (Samsung Knox)	This activation type lets you manage the entire device using commands and the KNOX MDM and KNOX Workspace IT policy rules. This activation type creates a separate work space on the device and the user must create a password to access the work space. Data in the work space 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 lets you 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 work space on the device and the user must create a password to access the work space. Data in the work space 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 lets you 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 work space. 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