BLACKBERRY BES 12.5.x MDM SUPPLEMENTAL PROCEDURES

Version 1, Release 2

28 October 2016

Developed by BlackBerry and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. SECURITY READINESS REVIEW

1.1 General

When conducting a BlackBerry Enterprise Service (BES) 12.5.x Mobile Device Manager (MDM) 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 BES 12.5.

1.2 Mobile Policy Review

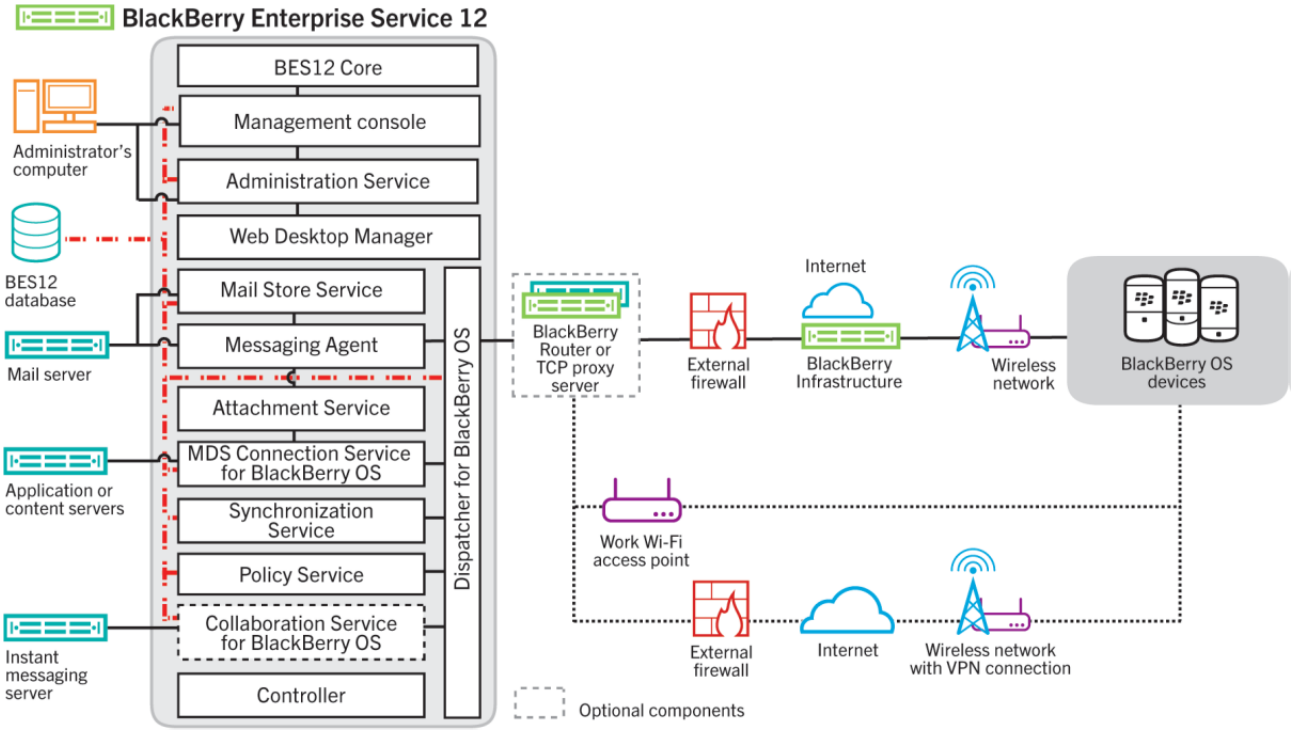
Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website located at http://iase.disa.mil/stigs/mobility/Pages/policies.aspx.

Use the Mobility Policy STIG and the CMD Management Policy STIG to review the BES 12.5 asset.

2. BES SOFTWARE SECURITY AND CONFIGURATION INFORMATION

2.1 Architecture

Figure 2-1: BES12 EMM Solutions



2.1.1 Required Firewall and Port Configurations for BES12

BES12 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. BES12 requires the following configurations on the host-based or appliance firewall:

- DNS
  - Support for resolving IP addresses into host names
- Proxy Firewall
  - If your organization uses a proxy firewall, a proxy that does not change incoming or outgoing data (transparent proxy)
- The 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)
- BES12 Self-Service and BES12 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 ports required for the BES12 Self-Service and BES12 Management Console are not available, or need to be changed for any reason, the ports can be reconfigured using the BES12 Configuration tool.

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

Table 3-1: Outbound Ports

From	To	Port (TCP)
BlackBerry 10 iOS Android Windows devices	BlackBerry Infrastructure	443
BES12	BlackBerry Infrastructure	3101
iOS	APNs	5223
Android	GCM	5228 5229 5230

Note: BES12 uses port 8889 for identity management for BlackBerry 10 devices and to handle SCEP requests for BlackBerry Secure Connect Plus. BES12 must be able to access this port to support devices running BlackBerry 10 OS version 10.3 or later.

Table 3-2: Listening Ports

Port (TCP)	Description
1610	The port that the BES12 Core uses to provide SNMP monitoring data.
1611	The port that SNMP clients can use to query monitoring data for BlackBerry Secure Connect Plus.
1620	The port that the BES12 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 BES12 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.

Port (TCP)	Description
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 BES12 Core.
8102	The port that the BES12 Core uses to check the status of BlackBerry Secure Connect Plus.
8448	The port that is used for internal communication between the BES12 Core and the management console and BES12 Self-Service.
8881	The port that BES12 uses to receive management requests for BlackBerry 10 devices. The connection uses mutual authentication with ECC certificates.
8882	The port that BES12 uses to receive enrollment requests for BlackBerry 10 devices.
8883	The port that BES12 uses to receive enrollment requests for iOS, Android, and Windows Phone devices.
8884	The port that BES12 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 BES12 uses to receive management requests for iOS devices. The connection uses mutual authentication with RSA certificates.
8887	The port that BES12 uses for authenticated connections to check the status of BES12 instances.
8889	The port that the BES12 Core uses for identity management for BlackBerry 10 devices and to handle SCEP requests for BlackBerry Secure Connect Plus (the BES12 Core acts as the CA). **Note**: BES12 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.
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 you turn on push encryption.
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 BES12 Core listens on to route email notification traffic through the BlackBerry Infrastructure to the APNs for iOS devices.
38083	The port that the BES12 Core listens on for migration requests when you move devices from BES10 to BES12.
38085	The port that supports Secure Work Space traffic from iOS and Android devices

Port (TCP)	Description
	through the BES12 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 BES12 sends to the APNs.

2.2 Identification and Authentication

2.2.1 Passwords

Authentication to BES12 can be configured to use local authentication or an enterprise authentication mechanism, such as Active Directory. 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 BES12 console, passwords are obfuscated. The STIG requires the BES 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 BES12 is encrypted.

The BES12 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. BES 12 access should be limited to only systems that enforce local CAC authentication.

2.2.2 Certificates

Management of certificates on the server hosting BES12, 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 BES12. If a self-signed certificate was used, 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 BES12 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 Mobile Operating System 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 BES12.

2.4 Media Protection

Access to and control of removable media and other storage used by BES12 is managed by the host operating system.

2.5 System and Communication Protection

2.5.1 Cryptographic Support

BES12 uses the BlackBerry Cryptographic Java Module cryptographic modules, validated under FIPS 140-2 Certificate number 2504, for all cryptographic support. Data in transit between BES12 and the BlackBerry mobile devices is protected using AES-256 encryption.

2.5.1.1 Public Key Cryptography

BES12 supports software-based asymmetric key technology. Certificates can be managed by BES12. BES 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 BES12 and any storage of data used by and/or created by the BES12 are managed by the host operating system. This includes storage and protection of any keys, certificates, and/or protected classified information.

BES12 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 BES12 prevent the user from loading uncontrolled software or software from non-approved locations.