Australian Government
Department of Defence
Intelligence and Security

PROTECT

Defence Signals Directorate

Blackberry Hardening Guide

July 2011

Table of Contents

Overview

Introduction

This document provides technical guidance on how to harden the BlackBerry Enterprise Server (BES) and BlackBerry handheld devices produced by Research in Motion (RIM).

Versions

This document relates to BES versions up to and including 5.0.3.

Settings and features listed in this document that are non-existent in the version of the BES or device being used may be disregarded.

Policy relating to the use of Portable Electronic Devices (PEDs) by Australian government agencies can be found in the Australian Government Information Security Manual (ISM).

Contents

This publication contains the following sections:

Technical Guidance

Overview

Introduction

The information in this section is provided to give some technical guidance to agencies installing a BlackBerry solution consistent with Australian Government ICT security requirements as stated in the previous section.

Please note that this guide is mandatory if you are connecting your BlackBerry solution to a RESTRICTED/PROTECTED level network, and only guidance for lower classification networks. For lower classification networks you need to remain compliant to the ISM and the Consumer Guide. For RESTRICTED/PROTECTED you need to remain compliant to the ISM, Consumer Guide and this Hardening Guide.

Other software platforms

This guidance is derived from the results of the DSD review in which the BES was installed upon a Microsoft (MS) Windows 2008 R2 Server, configured to function with Microsoft Exchange Server 2007.

Certain aspects of the following guidance are therefore limited to these software versions. Where this occurs, agencies implementing BlackBerry solutions on other platforms are encouraged to apply comparable strategies to address the identified issues.

Currency

Some of the information in this section, particularly with respect to current patches and URL locations, may become outdated. Although all such information is accurate at the time of publishing, agencies are advised to confirm that they have the latest information available when installing their BlackBerry systems.

Contents

This chapter contains the following topics:

Network Architecture

General principles	Distributing services will help to mitigate the effects of any future exploits and to improve availability, as will hardening the system by keeping permitted services and open ports to the minimum required.
Configuring the external firewall	The only traffic that should be passing through the firewall located between the Internet and the BlackBerry router is an agency-initiated connection to RIM's network operations centre. **Action:** Configure the external firewall to permit only a single, outbound-initiated but bi-directional connection on port 3101 between the router and RIM.
Attachment Service	The separation of the Attachment Service allows agencies to reduce the consequences of a successful attack against the Service by immediately isolating it from the network. **Action:** Install the BlackBerry Attachment Server on a separate server to the BES.
Network diagram	Please see the RIM document entitled *Placing the BlackBerry Enterprise Solution in a Segmented Network* for details on our recommended network solution. http://www.blackberry.com/solutions/resources/Placing_the_BlackBerry_Enterprise_Solution_in_a_Segmented_Network.pdf

BES Installation

Patching the host operating system

Although the RIM installation guides do not provide advice on the level of vendor security patching that should be applied to either the BES's underlying operating system or the Microsoft Exchange server, best practice indicates that production servers be installed with the most current vendor cumulative patches and security hot fixes.

Information relating to patching levels is available from Microsoft's TechNet.

Action: Apply relevant patches:
- Microsoft Windows 2003 Server – SP2,
- Microsoft Windows 2008 Server – SP2,
- Microsoft Windows 2008 Server R2 – SP1 Beta, and
- Any hot fixes released since these service packs.

Default Windows share

The default configuration for the BES, using a Microsoft Windows operating system, provides a Windows share of C:\ which is not required for BES functionality.

Action: Remove the C:\ share.

BES file share

Installing BES automatically creates a common network directory share for holding BlackBerry handheld software configuration files. These files are used to configure handhelds with the agency's IT policy; unauthorised modification to the files could reduce the security of handhelds.

Action: Set the handheld configuration files for Read Only access.

Additional hardening

A complete hardening guide and assessment is beyond the scope of this review as there are a number of server configurations that could be utilised. However, to ensure that the BES is protected against known vulnerabilities, agencies should ensure at minimum the vendor best security practice guidelines are followed. These guides will assist administrators in identifying the required patching levels and help to determine the necessary functions, services and file shares.

Action: Harden the Microsoft Windows Server supporting the BES platform in accordance with the vendor security guides, prior to installing any BlackBerry system.

Guides such as Microsoft's Baseline Security Analyser (MSBSA) are available from:
URL: www.microsoft.com/technet/security/tools/mbsahome.mspx

Continued on next page

BES Installation, Continued

SQL Server 2005

The BES relies on configuration information being held in a Microsoft-compliant relational database. During BES installation the operator is given the choice of installing Microsoft's SQL Server 2005 Express Edition SP3 or using an existing Microsoft SQL Server database.

The configuration database may also be hosted on a separate SQL Server. This server may reside within the corporate network with the appropriate firewall opened to allow traffic on port 1433 between the BES and the database server. This reduces the risks associated with hosting this information in the DMZ

Action: The SQL Server component of the BES should also be maintained to appropriate service pack levels and patched. More information is available from:
URL:http://www.microsoft.com/sqlserver

Browser

The BES requires Internet Explorer (IE) to be installed to allow viewing and navigation of locally stored RIM help files. However, the BES has no functional requirement for this IE installation to be aware of any external gateway allowing it to establish connections to the Internet, and to do so would greatly increase the risk to the system.

Note: The BES configuration manager, not the IE installation, is the service that allows the BES to conduct Internet requests made from BlackBerry handhelds.

Action: Ensure that all relevant IE Service Packs and hot fixes have been applied to IE.

Action: Ensure that the server is not able to make connections to the Internet via the agency's default gateway.

Action: Install a personal firewall to the BES with rules that allow the BES applications to communicate whilst explicitly denying IE.

Continued on next page

BES Installation, Continued

Exchange environment

The BES can be used with the following Exchange servers in the Microsoft Windows environment.

Action: Apply Microsoft cumulative Service Packs and hot fixes for the version of Microsoft Exchange used prior to connection to the BES. At the time of publication the current service packs for Microsoft Exchange were:

a. MS Exchange Server 2003 - SP2
b. MS Exchange Server 2007 - SP3
c. MS Exchange Server 2010 - SP1 Beta

BlackBerry Administration Service

RIM has changed how administrators control the BES, by introducing a web-based front end. With this web-based front end also comes a web desktop application that allows general users to administer their own BlackBerry.

DSD recommends considering restricting the web-service to only BES administrator computers, and disabling the web desktop application if there is no business requirement.

Action: Restrict BAS access to administrator computers and disable web desktop application if not required.

Additional information

RIM provides a comprehensive guide on preparing and installing the system to operate in a functioning environment.

Action: Review the guide designed for the version of software that you intend to install, available from:
URL: http://www.blackberry.com/knowledgecenterpublic

RIM also provides a current series of hot fixes to address application efficiency and to mitigate against BES security issues. Australian service providers may provide local websites with this information and/or provide an update alert feature. A generic entry to this information is also available at:
URL: https://www.blackberry.com/Downloads/entry.do?

Action: Periodically check for and apply Service Packs and hot fixes to the BES Server as they become available.

Bluetooth Peripherals

Available peripherals

BlackBerry handhelds may incorporate Bluetooth functionality allowing pairing with headsets and hands-free car sets.

These peripherals are designed to allow hands-free voice communications only.

If agencies require a less risky hands-free option, the use of an earpiece and jack is recommended.

Recommended process

The risks of using Bluetooth within the context of BlackBerry handheld voice communications can be partially mitigated by using the process detailed below.

Step	Action
1	Ensure that, as a minimum, BES Version 4 Service Pack 3 is installed. This will provide the Bluetooth IT Policy group with the option to disallow Bluetooth Discovery mode on the handheld.
2	Create a separate Bluetooth IT Policy Group on the BES for users that will be using Bluetooth. This policy should reflect all other agency IT policy settings with the exception of: • Bluetooth Policy Group: Disable Bluetooth = FALSE, • Bluetooth Policy Group: Disable Headset profile = FALSE, • Bluetooth Policy Group: Disable Pairing = TRUE, and • Bluetooth Policy Group: Disable Discovery Mode = TRUE.
3	Create a separate IT Policy for users that will not be using the Bluetooth peripherals: • Bluetooth Policy Group: Disable Bluetooth = TRUE.
4	Create a Bluetooth configuration IT Policy that represents the agency IT policy with the exception that: • Bluetooth Policy Group: Disable Bluetooth = FALSE, • Bluetooth Policy Group: Disable Headset profile = FALSE, • Bluetooth Policy Group: Disable Pairing = FALSE, and • Bluetooth Policy Group: Disable Discovery Mode = FALSE.
5	Within the confines of a controlled environment, set the handheld Bluetooth setting to Discoverable mode under the Bluetooth options menu. This will allow the device to be paired with a BlackBerry headset.

Continued on next page

Bluetooth Peripherals, Continued

Recommended process (continued)

Step	Action
6	Follow the RIM guide for pairing to the BlackBerry headset and ensure that: • encryption with the paired device is used, • the device is set to non-discoverable mode, and • the handheld's Bluetooth device name is set.
7	Apply the Bluetooth IT Policy Group to the Handheld which disallows pairing to other devices.
8	Create a set of standard operating procedures for Bluetooth enabled users that are designed to educate them on the exploitability of Bluetooth and the manner in which they are to operate this function. Content may include: • attempts to pair additional devices to the handheld are forbidden, • if prompted to pair with another Bluetooth device the user is to deny all requests and report such information to system administrators, and • the functionality is to be used only when a hands-free environment is required, and the functionality should be turned off whenever this is not the case.

S/MIME & PGP

Using S/MIME or PGP

The introduction of Secure Multipurpose Internet Mail Extension (S/MIME) or PGP, using the OpenPGP message Format, would ensure that end-to-end encryption using a DSD Approved Cryptographic Protocol (DACP) is applied to emails between all users, including the BlackBerry handheld. The use of S/MIME or PGP on an enterprise email system would therefore mitigate some of the risks introduced by a BlackBerry system.

BlackBerry networks are able to handle S/MIME or PGP and its introduction would decrease the attractiveness of all sources of email content information, including the BES.

Considerations

If S/MIME or PGP is used, the network owner has to allow the traversal of encrypted information through their firewall to the mail server. Methods of dealing with the agency's email filtering and anti-virus protection requirements at the workstation, rather than just the gateway environment, would then need to be implemented.

Action: Consider the introduction of S/MIME or PGP to the enterprise wide mail network.

APB Messages

All Points Bulletin message functionality

The BlackBerry Enterprise Server management console allows the ability for an administrator to send general alerts to all handsets, a group or an individual. This can be useful to notify users of outages or other general information.

Action: Consider sending only UNCLASSIFIED information with little or no identifying information of the organisation or operations when using this feature.

Application Policy Settings

Third Party application control

Agencies have the ability to control what applications are installed on BlackBerry handsets through the use of IT Policy Settings, which will control use of all third party applications, and Application Control Policies which will allow more granular control of permissions for each application or group of applications.

Action: If no third party applications are required a default policy with all options to Not Permitted should be used. Furthermore, control policies should be created for required applications to enforce the minimum features required.

BES IT Policy Settings

Overview

Introduction

The BlackBerry solution provides users with a broad range of options, approximately 500 IT policy settings, aimed at delivering end user functionality and flexibility.

To ensure that security is also addressed by these settings, DSD has reviewed the available settings and determined appropriate values.

Other settings

This section does not contain the full list of settings. Those setting not included here were not considered by DSD to have a direct impact on security and therefore are left up to the discretion of each agency.

Settings

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Application Center	Disable Application Center	No	Specify whether to disable the BlackBerry® Application Center on the BlackBerry device. Set this rule to Yes to prevent the user from accessing the BlackBerry Application Center.	4.1.6	Yes	Yes	
BlackBerry Messenger	Disable BlackBerry Messenger	No	Specify whether the BlackBerry® Messenger is turned off on the BlackBerry device.	4.0.2	Agency decision		Set to "Yes" if you are not allowing Peer-to-peer messaging
BlackBerry Messenger	Disallow Forwarding Of Contacts	No	Specify whether a user can forward contacts using BlackBerry Messenger.	4.1.6	Agency decision		Only UNCLASSIFIED contacts may be sent using BlackBerry Messenger
BlackBerry Messenger	Messenger Audit Email Address	NULL	Type the address to which the BlackBerry device sends BlackBerry Messenger audit reports. If this rule is empty, the BlackBerry Messenger turns off auditing and does not send reports.	4.0.2	Agency decision		If the Agency wants to audit messages, set to a valid email
BlackBerry Unite!	Disable Download Manager	No	Specify whether to prevent the BlackBerry® Download Manager for BlackBerry® Unite!™ from running on BlackBerry devices. This rule applies only to BlackBerry devices with BlackBerry Unite! Applications installed.	4.1.6	Yes	Yes	
BlackBerry Unite!	Disable Unite! Applications	No	Specify whether to prevent BlackBerry Unite! Applications from running on BlackBerry devices. This	4.1.6	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			rule applies only to BlackBerry devices with BlackBerry Unite! Applications installed.				
Bluetooth	Disable Address Book Transfer	No	Specify whether to prevent the BlackBerry device from exchanging address book data with supported Bluetooth enabled devices.	4.0.3	Agency decision		Only UNCLASSIFIED information may be sent over Bluetooth
Bluetooth	Disable Bluetooth	No	Specify whether support for Bluetooth technology is turned off on the BlackBerry device. If the Bluetooth wireless radio is active when the BlackBerry device receives this IT policy rule, the BlackBerry device must be reset manually for the change to take effect	4.0.0	Agency decision		DSD recommends only enabling Bluetooth to people who use their BlackBerrys with Bluetooth devices
Bluetooth	Disable Desktop Connectivity	Yes	Specify whether the BlackBerry device can use Bluetooth technology to connect to the BlackBerry® Desktop Manager.	4.0.3	Yes	Yes	
Bluetooth	Disable Dial-Up Networking	No	Specify whether a Bluetooth enabled BlackBerry device can use the Bluetooth Dial-Up Networking Profile (DUN).	4.0.6	Yes	Yes	
Bluetooth	Disable Discoverable Mode	No	Specify whether to prevent a Bluetooth enabled BlackBerry device user from turning on Discoverable mode on their BlackBerry device. Note: A BlackBerry device with Discoverable mode turned on can be discovered by other Bluetooth enabled devices in range of the BlackBerry device.	4.0.1	Yes	Yes	See the Bluetooth guide for more information
Bluetooth	Disable File Transfer	No	Specify whether the Bluetooth enabled BlackBerry device can	4.0.6	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			exchange files with compatible Bluetooth OBject EXchange (OBEX) devices.				
Bluetooth	Disable Handsfree Profile	No	Specify whether to prevent a Bluetooth enabled BlackBerry device from using the Bluetooth Hands Free Profile (HFP) required to enable wireless voice capabilities with most car kits and some headsets.	4.0.0	Agency decision		See the Bluetooth guide for more information
Bluetooth	Disable Headset Profile	No	Specify whether to prevent a Bluetooth enabled BlackBerry device from using the Bluetooth Headset Profile (HSP) required to enable wireless voice capabilities with most headsets and some car kits.	4.0.0	Agency decision		See the Bluetooth guide for more information
Bluetooth	Disable Pairing	No	Specify whether to prevent a Bluetooth enabled BlackBerry device from establishing a relationship (in other words, pairing) with another Bluetooth device. Note: Set this rule to Yes to prevent the BlackBerry device user from pairing with subsequent Bluetooth devices after the BlackBerry device pairs with an approved Bluetooth device (for example a headset).	4.0.0	Yes	Yes	See the Bluetooth guide for more information
Bluetooth	Disable Serial Port Profile	No	Specify whether to prevent a Bluetooth enabled BlackBerry device from using the Bluetooth Serial Port Profile (SPP) required to establish a serial connection between the BlackBerry device and a Bluetooth peripheral using a serial	4.0.0	Yes	Yes	See the Bluetooth guide for more information

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			port interface.				
Bluetooth	Disable SIM Access Profile	No	Specify whether to prevent a Bluetooth enabled BlackBerry device from using SIM Access Profile (SAP). Some car kits require SAP to share the SIM card when the car kit initiates dialing.	4.1.6	Yes	Yes	See the Bluetooth guide for more information
Bluetooth	Disable Wireless Bypass	Yes	Specify whether a Bluetooth enabled BlackBerry device can perform wireless bypass over Bluetooth.	4.0.3	Yes	Yes	See the Bluetooth guide for more information
Bluetooth	Limit Discoverable Time	No	Specify whether the BlackBerry device user can set the Bluetooth discoverable mode option to have no time limit. Set this rule to Yes to permit the user to set the Bluetooth discoverable mode option to have a time limit of 2 minutes or to turn off Bluetooth discoverable mode. The BlackBerry device uses this IT policy rule only if the Disable Discovery Mode IT policy rule is set to No.	4.1.5	Yes	Yes	See the Bluetooth guide for more information
Bluetooth	Require Encryption	No	Specify whether a Bluetooth enabled BlackBerry device uses Bluetooth encryption on all connections. Set to Yes to force Bluetooth enabled BlackBerry devices to use Bluetooth encryption on all connections. Note: Requiring Bluetooth encryption on all connections might restrict compatibility with other Bluetooth	4.0.4	Yes		This may cause compatibility issues with some Bluetooth devices. If this is the case then it can be disabled

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			enabled devices.				
Bluetooth	Require LED Connection Indicator	No	Specify whether the LED is required to flash when the BlackBerry is connected to another Bluetooth device.	4.0.6	Agency decision		
Bluetooth	Require Password for Discoverable Mode	No	Specify whether the BlackBerry device requires that the user type the security password to enable Discoverable mode. Set to Yes to require the BlackBerry device to prompt the user for the security password to make the BlackBerry device discoverable by other Bluetooth devices. Set to No to permit the BlackBerry device user to turn on Discoverable Mode without entering the security password.	4.0.3	Yes	Yes	
Bluetooth	Require Password for Enabling Bluetooth Support	No	Specify whether the BlackBerry device requires that the user type the security password to enable Bluetooth support. Set to Yes to require the BlackBerry device to prompt the user for the security password when enabling Bluetooth support. Set to No to permit the BlackBerry device user to enable Bluetooth support without typing the security password.	4.0.3	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Browser	Allow Application Download Services	Yes	Specify whether application download service icons appear on the BlackBerry device when the wireless service provider assigns a service and the appropriate service books are present on the BlackBerry device. Set this rule to No to hide all application download service icons.	4.1.5	No	Yes	
Browser	Allow Hotspot Browser	Allow	Specify whether the hotspot browser is available on a Wi-Fi enabled BlackBerry device. Set this rule to Disallow to prevent access to the hotspot browser. Set this rule to Only for Hotspot Login to allow access to the hotspot browser only for the purpose of authentication to the hotspot.	4.1.6	Disallow	Yes	
Browser	Allow IBS Browser	Yes	Specify whether the Internet Browsing Service (IBS) browser icon appears on the BlackBerry device when the service provider provisions the IBS browser and the appropriate service books are present. Set this rule to No to hide the IBS browser icon.	4.0.1	No	Yes	
Browser	Disable Java Script in Browser	No	Specify whether to prevent JavaScript® execution in the BlackBerry Browser.	4.0.0	Agency decision		DSD recommends to have the same policy as with your corporate desktop policy
Browser	MDS Browser JavaScript Enabled	No	Specify whether JavaScript is enabled by default in the BlackBerry Browser.	4.0.2	Agency decision		DSD recommends to have the same policy as with your corporate desktop

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
							policy
Browser	MDS Browser Title	BlackBerry Browser	Type the name that appears on the BlackBerry device Home screen for the BlackBerry Browser icon.	3.6.0	Agency decision		
Camera	Disable Photo Camera	No	Specify whether the ability to take still pictures with the camera is turned off on the BlackBerry device.	4.0.6	Agency decision		Set to "Yes" if you are not allowed cameras on your work area
Camera	Disable Video Camera	No	Specify whether the ability to record video with the camera is turned off on the BlackBerry device. Set this rule to Yes to turn off the video camera feature.	4.1.5	Agency decision		Set to "Yes" if you are not allowed cameras on your work area
Common	Disable Kodiak PTT	No	Specify whether to prevent the BlackBerry device user from using Kodiak® Instant Calling, or Push to Talk (PTT) functionality on supported BlackBerry devices.	4.0.6	Yes	Yes	
Common	Disable MMS	No	Specify whether to prevent the BlackBerry device user from using Multimedia Messaging Service (MMS) functionality on the BlackBerry device. Set this IT policy rule to Yes to hide MMS functionality on the BlackBerry device. Note: To block incoming MMS messages, set the Firewall Block Incoming Messages IT policy rule in the Security policy group.	4.0.0	Agency decision		MMS can be enabled however only UNCLASSIFIED information may be sent
Common	Disable Voice Note Recording	No	Specify whether the voice note recording feature on the BlackBerry device is turned on. Set this rule to Yes to turn off the voice note	4.1.5	Agency decision		Only UNCLASSIFIED voice recordings may be saved

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			recording feature and prevent applications on the BlackBerry device from accessing it.				
Common	IT Policy Notification	No	Specify if warnings of IT policy changes are displayed to the BlackBerry device user.	4.0.0	Yes		
Common	Lock Owner Info		Specify whether users can change specified fields in the Owner options screen of the BlackBerry device. 1: Lock Information text 2: Lock Name text 3: Lock both Name and Information text. Note: You can use this rule to lock the text defined in the Set Owner Info and Set Owner Name rules. If you set this rule, the specified fields can be modified only if you change the values of those rules and the BlackBerry device receives the IT policy again, or if you send a Set Owner Information IT Admin command to the BlackBerry device.	4.0.0	"Lock both Name and Information text"		
Common	Set Owner Info		Type the owner information that is set on the BlackBerry device. Use the Lock Owner Info rule to prevent the BlackBerry device user from editing this information. Warning: This information is overwritten by the Set Owner Information IT Admin command.	4.0.0	Agency decision		Include sufficient information to enable a lost handset to be returned, with no further identifying information.
Common	Set Owner Name		Type the owner name that is set on the BlackBerry device. Use the Lock Owner Info rule to prevent the BlackBerry device user from editing this information. Warning: This	4.0.0	Agency decision		Include as little identifying information as necessary.

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			information is overwritten by the Set Owner Information IT Admin command.				
Desktop	Allow Blackberry Desktop Software Statistics	Yes	Specify whether to allow BlackBerry® Device Software to send statistical information to Research In Motion	5.0.0	No	Yes	
Desktop	Allow External Device Software Servers	No	Specify whether to allow BlackBerry® Device Software updates from software servers that are hosted externally. This rule does not apply to users running on BlackBerry® Enterprise Server for Novell® GroupWise®.	4.1.7	No	Yes	
Desktop	Desktop Allow Desktop Add-ins	Yes	Specify whether the BlackBerry Desktop Software enables the user to configure and execute desktop add-ins (third-party COM-based extensions that access the BlackBerry device databases during synchronization). This rule does not apply to users running on BlackBerry Enterprise Server for Novell GroupWise.	3.6.0	No		If an agency requires a desktop add-in, they may perform a risk assessment
Desktop	Desktop Allow Device Switch	Yes	Specify whether the BlackBerry Desktop Software allows users to switch BlackBerry devices. For users running on BlackBerry Enterprise Server for Novell GroupWise, this rule only applies in conjunction with BlackBerry® Web Desktop Manager.	3.6.1	No	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Desktop	Disable Media Manager	No	Specify whether the media manager tool of the BlackBerry Desktop Manager is available. This rule does not apply to users running on BlackBerry Enterprise Server for Novell GroupWise.	4.0.6	Agency decision		If an agency has a need for multimedia on the handset, they may set this to "No"
Desktop	Disable Media Synchronization	No	Specify whether BlackBerry Media Sync is available. This rule does not apply to users running on BlackBerry Enterprise Server for Novell GroupWise.	4.1.6	Agency decision		If an agency has a need for multimedia on the handset, they may set this to "No"
Desktop	Generate Encrypted Backup Files	No	Specify whether to require the user to generate encrypted backup files. This rule does not apply to users running on BlackBerry Enterprise Server for Novell GroupWise.	4.1.7	Yes	Yes	
Desktop Only items	Auto Backup Enabled	No	Specify whether the option to automatically backup data and encryption keys on the BlackBerry device is turned on. Set this rule to Yes to update the status in the backup and restore settings of the BlackBerry Desktop Software. For users running on BlackBerry Enterprise Server for Novell GroupWise, this rule only applies in conjunction with BlackBerry Web Desktop Manager.	3.5.0	Yes		
Desktop Only items	Auto Backup Include All	Yes	Specify whether all data is included in automatic backups. If this rule is set to Yes, the "Backup all BlackBerry device application data" radio button in Backup and Restore Options of the BlackBerry Desktop Manager will be selected. For users	3.5.0	Yes		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			running on BlackBerry Enterprise Server for Novell GroupWise, this rule only applies in conjunction with BlackBerry Web Desktop Manager.				
Desktop Only items	Force Load Count	no limit	Specify the number of times a BlackBerry device user can decline when prompted to update the BlackBerry device before the update is forced. To disable the forced update functionality, set this rule to -1. For users running on BlackBerry Enterprise Server for Novell GroupWise, this rule only applies in conjunction with BlackBerry Web Desktop Manager version 1.0 or 1.0.1.	3.5.0	3	Yes	If the BES admin pushes out an update, the user can delay the update up to a maximum of 3 times.
Desktop Only items	Force Load Message	NULL	Type the message that appears when the BlackBerry device prompts users are to update to a later version of the BlackBerry Device Software. Note: The BlackBerry device uses this rule only if you also set the Force Load Count rule to a positive number. For users running on BlackBerry Enterprise Server for Novell GroupWise, this rule only applies in conjunction with BlackBerry Web Desktop Manager version 1.0 or 1.0.1.	3.5.0	Agency decision		Agency may decide to put BES Admin details here to contact to make sure the update is valid
Desktop Only items	Message Prompt	NULL	Type a message to prompt the user each time the BlackBerry Desktop Software starts. This rule does not apply to users running on	3.5.0	Agency decision		Agency may decide to remind users that they are working on an official work

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			BlackBerry Enterprise Server for Novell GroupWise.				device
Desktop Only items	Show Application Loader	Yes	Specify whether the BlackBerry device user has access to the application loader in the BlackBerry Desktop Software. For users running on BlackBerry Enterprise Server for Novell GroupWise, this rule only applies in conjunction with BlackBerry Web Desktop Manager version 1.0 or 1.0.1.	3.5.0	No	Yes	
Desktop Only items	Show Web Link	No	Specify whether the BlackBerry device user has access to the Web Link icon in the BlackBerry Desktop Software. Note: The icon will only appear if the default URL is set using the WebLinkURL rule. This rule does not apply to users running on BlackBerry Enterprise Server for Novell GroupWise.	3.5.0	No	Yes	
Device IOT Application	Set Diagnostic Report Email Address		Type the destination email address of the diagnostic report. One or multiple email addresses can be specified here. The email addresses are separated by a comma.	4.0.6	Agency decision		
Device IOT Application	Set Diagnostic Report Pin Address		Type the destination PIN address of the diagnostic report. One or multiple PIN addresses can be specified here. The PIN addresses are separated by a comma.	4.0.6	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Device only items	Allow Peer-to-Peer Messages	Yes	Specify whether the user can send PIN messages from the BlackBerry device. Set this rule to No to hide PIN messaging functionality on the BlackBerry device. Note: To block incoming PIN messages, set the Firewall Block Incoming Messages IT policy rule in the Security policy group.	3.5.0	Agency decision		Peer-to-Peer messaging can be enabled however only UNCLASSIFIED information may be sent
Device only items	Allow SMS	Yes	Specify whether the BlackBerry device permits sending Short Message Service (SMS) messages (text messaging). Set this rule to No to hide text messaging functionality on the BlackBerry device. Note: To block incoming text, or SMS, messages, set the Firewall Block Incoming Messages IT policy rule in the Security policy group.	3.5.0	Agency decision		SMS can be enabled however only UNCLASSIFIED information may be sent
Device only items	Enable Long-Term Timeout		Specify whether the BlackBerry device locks after a predefined period of time, regardless of whether the BlackBerry device has been idle or in use during that interval. Set this rule to Yes to force the BlackBerry device to lock automatically after 60 minutes. Note: You can use the Periodic Challenge Time rule to shorten the timeout interval.	3.5.0	Yes	Yes	
Device only items	Enable WAP Config		Specify whether the user can see and use the WAP browser icon on the BlackBerry device (when the Internet service provider provisions the WAP browser and the	3.5.0	No	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			appropriate service books are on the BlackBerry device). Set this rule to No to hide the WAP Browser icon on the BlackBerry device.				
Device only items	Home Page Address		Type the URL of the BlackBerry device browser's home page. Note: If you do not specify a URL, the BlackBerry device uses the browser's default home page URL.	3.5.0	Agency decision		Agency may set this to their intranet or internet home page
Device only items	Home Page Address is Read-Only		Specify whether the BlackBerry device user can modify the URL address of the browser home page.	3.5.0	Agency decision		
Device only items	Maximum Password Age		Type the number of days until a BlackBerry device security password expires and the BlackBerry device prompts the user to set a new password. Note: Set this rule to 0 to prevent the BlackBerry device security password from expiring. Rule dependency: The BlackBerry device uses this rule only if a security password is set. To require a security password, set the Password Required rule to Yes.	3.5.0	90	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Device only items	Maximum Security Timeout		Specify the maximum time, in minutes, that a BlackBerry device user can set as the security timeout value (the number of minutes of BlackBerry device user inactivity allowed before the security timeout occurs and the BlackBerry device requires the user to type the BlackBerry device password to unlock the BlackBerry device). The BlackBerry device user can set any timeout value that is less than or equal to the maximum value unless you set the User Can Change Timeout rule value to No. The maximum security timeout value available by default on the BlackBerry device is 60 minutes. Use the Set Password Timeout rule to set a specific timeout value. Rule dependency: The BlackBerry device uses this IT policy rule only if the Password Required rule is set to Yes.	3.5.0	10	Yes	
Device only items	Minimum Password Length		Type the minimum required length, in characters, of the BlackBerry device security password. This rule only controls the minimum password length, not the maximum password length. The maximum password length is 32 characters. Rule dependency: The BlackBerry device uses this rule only if a security password is set. To require a security password, set the	3.5.0	7 or 12	Yes	As per ISM: Length of 12 if no complexity; or 7 with at least 3 of the following: lowercase (a-z), uppercase (A-Z), digits (0-9), and punctuation and special characters

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			Password Required rule to Yes. Warning: If the FIPS Level rule is set to 2, then the BlackBerry device ignores this rule and explicitly requires a minimum password length of five characters.				
Device only items	Password Pattern Checks	No restriction	Specify a character pattern that the BlackBerry device security password must match. Rule dependency: The BlackBerry device uses this rule only if a security password is set. To require a security password, set the Password Required rule to Yes. Warning: If you select option 2 or option 3, password pattern checking is disabled on 95x/85x BlackBerry devices.	3.5.0	"No Restriction" or "At least 1 alpha, 1 numeric, and 1 special character"	Yes	As per ISM: If Minimum password length is set to 12, "No restriction"; otherwise "At least 1 alpha, 1 numeric, and 1 special characteer"
Device only items	Password Required	No	Specify whether the BlackBerry device requires a security password. Set this rule to Yes to require the user to enter a security password to unlock the BlackBerry device. Rule dependency: If you set this rule to Yes, you should set the User Can Disable Password rule to No to prevent the BlackBerry device user from disabling this rule. Warning: If the FIPS Level rule is set to 2, the BlackBerry device explicitly requires a security password and ignores this rule's setting.	3.5.0	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Device only items	User Can Disable Password	Yes	Specify whether the user can disable the requirement for a BlackBerry device security password. Set this rule to No to prevent users from disabling the security password requirement on the BlackBerry device. Rule dependency: The BlackBerry device uses this rule only if a security password is set. To require a security password, set the Password Required rule to Yes.	3.5.0	No	Yes	
Documents To Go	Disable Documents To Go	No	Specify whether users can open files or attachments using the Documents To Go® application on the BlackBerry device.	4.1.5	Agency decision		
Documents To Go	Hide Documents To Go Communication Menus	No	Specify whether users can register the Documents To Go application with DataViz®, check for software updates from DataViz, and use the premium edition of the Documents To Go application on the BlackBerry device. If you set the Disable Documents To Go IT policy rule to Yes, the BlackBerry device ignores this rule.	4.1.5	Yes	Yes	
Documents To Go	Hide Documents To Go Premium Feature Menus	No	Specify whether to hide the premium DataViz Documents To Go features that are not available on BlackBerry devices that are running the standard edition of the Documents To Go application. If you set the Disable Documents To Go IT policy rule to Yes, the BlackBerry device ignores this rule.	4.1.5	Yes		If you have purchased Premium Features, then set this to "No".

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Email Messaging	Confirm External Image Download	No	Specify whether the BlackBerry device displays a confirmation dialog box when a BlackBerry device user clicks the Get Images link in an HTML-formatted email message.	5.0.0	Yes		
Email Messaging	Disable Form Submission	No	Specify whether the BlackBerry device user can submit forms embedded in email.	4.1.5	Agency decision		
Email Messaging	Disable Notes Native Encryption Forward And Reply	No	Specify whether to prevent a BlackBerry device user from forwarding and replying to received IBM® Lotus Notes® encrypted messages on their BlackBerry devices. If you set this rule to Yes, BlackBerry device users cannot forward or reply to received IBM Lotus Notes encrypted messages on their BlackBerry devices. By default, a BlackBerry device user with support for reading IBM Lotus Notes encrypted messages enabled on the BlackBerry device can forward or reply to an encrypted message that the BlackBerry device has received, decrypted, and decompressed. The BlackBerry® Enterprise Server for IBM® Lotus® Domino® decrypts the message before the BlackBerry device sends the message to the recipient as plain text.	4.1.3	Agency decision		
Email Messaging	Disable Rich Content Email	No	Specify whether the BlackBerry Enterprise Server sends email messages to the BlackBerry device	4.1.5	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			in Rich Content (HTML) format.				
Email Messaging	Inline Content Requests	Automatic Allowed	Specify whether the BlackBerry device can send messages with inline content and request inline content in received messages automatically, or if the BlackBerry device user must manually request inline content on the BlackBerry device.	4.1.5	Agency decision		
Email Messaging	Keep Message Duration	-1	Specify the maximum length of time, in days, that the BlackBerry device keeps messages. Note: Set this IT policy rule to 0 or -1 to keep messages on the BlackBerry device indefinitely.	4.0.6	Agency decision		
Email Messaging	Keep Saved Message Duration	-1	Specify the maximum length of time, in days, that the BlackBerry device keeps saved messages. Note: Set this IT policy rule to 0 or -1 to keep saved messages on the BlackBerry device indefinitely. Set this rule to -2 to delete saved messages and turn off the ability to save messages on a BlackBerry device that is running BlackBerry Device Software version 4.5 or later.	4.0.6	Agency decision		
Email Messaging	Maximum Native Attachment MFH Attachment Size	3145728	Specify the maximum size (in bytes) of a single native attachment that can be uploaded from the BlackBerry device.	4.0.6	Agency decision		
Email Messaging	Maximum Native Attachment MFH Total Attachment Size	5242880	Specify the total size (in bytes) of all native attachments that can be uploaded from the BlackBerry device.	4.0.6	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Email Messaging	Maximum Native Attachment MTH Attachment Size	10240	Specify the maximum size (in kilobytes) of a single native attachment that can be downloaded to the BlackBerry device. A value of 0 indicates that the ability to download native attachments is turned off on the BlackBerry device.	4.1.5	Agency decision		
Email Messaging	Notes Native Encryption Password Timeout	-1	Specify the maximum length of time (in minutes) that the BlackBerry device stores the IBM Lotus Notes .id password that the user types. Set this rule to -1 to store Notes .id passwords that the user types indefinitely. Set this rule to 0 to never store the password that the user types.	4.1.5	30	Yes	
Email Messaging	Prepend Disclaimer	NULL	Type a disclaimer to appear at the beginning of all email messages that the user composes and sends using the BlackBerry device.	4.0.5	Agency decision		Agencies may want to have a disclaimer on outgoing emails
Email Messaging	Require Notes Native Encryption For Outgoing Messages	No	Specify whether all email messages sent from a BlackBerry device that uses email services capable of IBM Lotus Notes encryption must be encrypted. If necessary, the user is prompted for encryption credentials (the Notes Native Encryption password) on the BlackBerry device. Note that the BlackBerry device does not perform the encryption. This IT policy rule ensures that the BlackBerry device configures messages that it sends for IBM Lotus Notes encryption by the BlackBerry Enterprise Server.	5.0.0	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			This IT policy rule does not affect messages sent from the BlackBerry device using email services that are not capable of IBM Lotus Notes encryption.				
Global items	Allow Browser	Yes	Specify whether the user can use the BlackBerry Browser included on the BlackBerry device. Set this rule to No to hide the BlackBerry Browser icon on the BlackBerry device.	3.5.0	Agency decision		All traffic that goes through the Browser is run through the BES, and thus the agency's internet proxy. You can also access the intranet through the browser.
Global items	Allow Phone	Yes	Specify whether the phone functionality on the BlackBerry device is available to the user. Set this IT policy rule to No to prevent users from making and receiving any phone calls except emergency calls from their BlackBerry devices. The phone icon is still visible to users on their BlackBerry devices.	3.5.0	Agency decision		Phone can be enabled however only UNCLASSIFIED information may be communicated

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Global items	Auto Signature		The functionality provided by this rule is now provided by server-side Disclaimer text settings. Setting this policy rule will not prevent a user from changing their Auto Signature text on BlackBerry devices running 4.0 and later software. Please refer to the BlackBerry Enterprise Server Administration Guide for information on how to set disclaimer text. Type the signature attached automatically to the BlackBerry device user's outgoing messages. For users running on BlackBerry Enterprise Server for Novell GroupWise, this rule only applies in conjunction with BlackBerry Web Desktop Manager.	3.5.0	Agency decision		Agencies may want to have a disclaimer on outgoing emails
Instant Messaging	Disable Saving Conversation	No	Specify whether a user can save an instant messaging conversation into the device memory or media card on the BlackBerry device.	4.1.6	Agency decision		
Instant Messaging	Disallow File Transfer Types	NULL	Specify the types of files that the BlackBerry device user cannot transfer when using instant messaging. Specify the file extensions in a comma-delimited format (for example, "bat, exe, mp3"). Set this rule to "Null / " to allow all file types. Set this rule to "*" to prevent all file types.	4.1.6	Agency decision		
Instant Messaging	Maximum File Transfeer Size	6 MB	Specify the maximum size (in bytes) of files that a collaboration client can send to an instant messaging server. The permitted range is 0 through 6 MB.	5.0.1	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Location Based Services	Disable BlackBerry Maps	No	Specify whether the BlackBerry® Maps functionality is available (turned on) on the BlackBerry device.	4.0.6	Yes		
Location Based Services	Enable Enterprise Location Tracking	No	Specify whether to turn on Enterprise Location Tracking. Set this rule to Yes to turn on the reporting of a device's location back to the BES.	4.1.3	Agency decision		
Location Based Services	Enterprise Location Tracking Interval	15	Type the interval, in minutes, after which a device will report location back to the BlackBerry Enterprise Server.	4.1.3	Agency decision		
MDS Integration Service	Disable Activation With Public BlackBerry MDS Integration Service		Specify whether to prevent BlackBerry devices from connecting to public BlackBerry MDS Integration Service.	4.0.6	Yes	Yes	
MDS Integration Service	Disable User-Initiated Activation with the BlackBerry MDS Integration Service	No	Specify whether to prevent the BlackBerry device user from initiating activation with the BlackBerry MDS Integration Service. Set this rule to Yes to prevent the user from specifying the BlackBerry MDS Integration Service to connect to on the BlackBerry device.	4.0.6	Yes	Yes	
On-Device Help	On-Device Help Group Label		Type the label to use when grouping multiple On-Device Help links.	4.0.3	Agency decision		
On-Device Help	On-Device Help Links		Type the links to add to the On-Device Help index page using the format "uri1|label1|...|uriN|labelN". If you specify multiple links, you should also set the On-Device Help	4.0.3	Agency decision		Agency may wish to have a link to corporate support

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			Group Label rule.				
Password	Duress Notification Address	NULL	Type the message account address that receives notification when users type their BlackBerry device security passwords under duress (in other words, users indicate that they are unlocking their BlackBerry devices against their will). Warning: If you do not specify an email address, the BlackBerry device does not respond to passwords entered under duress. Warning: To prevent a party who has stolen the unlocked BlackBerry device from receiving a response to the duress notification on the BlackBerry device, the message account you specify to receive duress notification messages should be active and not have an out of office or other auto-reply function set. Rule dependency: The BlackBerry device uses this rule only if a security password is set. To require a security password, set the Password Required rule to Yes. Warning: If you set this IT policy rule, the set maximum number of password attempts is effectively reduced by half; each time the user types a password to unlock the BlackBerry device, the BlackBerry device must confirm whether the password attempt is either the	4.0.0	Agency decision		If you set this policy, then the number of password attempts is halved. Agencies should keep this in mind when setting this and the "Set Maximum Password Attempts" policy

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			correct password or the correct duress password.				
Password	Forbidden Passwords	NULL	Type a list of comma-separated string values representing words that users are not permitted to use within their passwords. Rule dependency: The BlackBerry device uses this rule only if a security password is set. To require a security password, set the Password Required rule to Yes. Note: The BlackBerry device automatically prevents common letter substitutions. For example, if you include "password" in the forbidden passwords list, users cannot use "p@ssw0rd", "pa$zword", or "password123" on the BlackBerry device.	4.0.2	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Password	Maximum Password History	0	Set the maximum number of previous passwords against which the BlackBerry device can check new passwords to prevent reuse of the old passwords. Note: Set this rule to 0 to prevent the BlackBerry device from checking for reused passwords. Rule dependency: The BlackBerry device uses this rule only if a security password is set. To require a security password, set the Password Required rule to Yes.	3.6.0	8	Yes	
Password	Periodic Challenge Time		If you set the Enable Long-Term Timeout IT policy rule to Yes, the security timeout interval is turned on and set to 60 minutes. The security timeout is the time elapsed, in minutes, after which the BlackBerry device locks and prompts the user to type the BlackBerry device password, regardless of whether the BlackBerry device has been idle or in use during that interval. Type a periodic challenge time to shorten or extend the security timeout interval to a value in the range of 1 to 1440 minutes (24 hours). Note: To disable the security timeout, set the Enable Long-Term Timeout IT policy rule to No and do not set a Periodic Challenge Time. Rule dependency: The BlackBerry device uses this rule only if a security password is set. To require a security password, set the	4.0.0	840	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			Password Required rule to Yes.				
Password	Set Maximum Password Attempts		Set the number of security password attempts (incorrect passwords entered) permitted on the BlackBerry device before the BlackBerry device data is erased and the BlackBerry device is disabled. Default setting: 10 password attempts You can use this rule to lower the number of password attempts. Rule dependency: The BlackBerry device uses this rule only if a security password is set. To require a security password, set the Password Required rule to Yes.	3.6.0	5	Yes	If the Duress Notification Address policy is set, you may need to change this value to "10"

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Password	Set Password Timeout		Specify the amount of time, in minutes, of BlackBerry device user inactivity allowed before the security timeout occurs and the BlackBerry device requires the user to type the password to unlock the BlackBerry device. Note: The default security timeout interval is 2 minutes of inactivity for BlackBerry Device Software versions earlier than 4.7 and 30 minutes of inactivity for BlackBerry Device Software versions 4.7 and later. Rule dependencies: The BlackBerry device uses this rule only if the Password Required rule is set to Yes. If you do not set the User Can Change Timeout rule to No, the BlackBerry device user can set the password timeout to one of a range of values. The maximum security timeout value available by default on the BlackBerry device is 60 minutes.	3.6.0	5	Yes	
Password	Suppress Password Echo		Set this rule to Yes to prevent the echoing (printing to the screen) of characters typed into the security password screen after the user had entered a set number of incorrect passwords when attempting to unlock the BlackBerry device. Rule dependency: The BlackBerry device uses this rule only if a security password is set. To require a security password, set the	3.6.0	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			Password Required rule to Yes. Note: You can set the number of incorrect password attempts that the BlackBerry device permits before password echoing (if permitted) occurs, using the Set Maximum Password Attempts rule. Note: If the FIPS Level rule is set to 2, then the BlackBerry device ignores this rule and explicitly prevents password echoing.				
PGP Application	PGP Allowed Content Ciphers	All supported algorithms	Specify the content ciphers that the BlackBerry device can use to encrypt PGP® messages. Warning: To maintain compatibility with most PGP clients, enable at least one of Triple DES and CAST. Warning: If the FIPS Level rule is set to 2, then the setting of this rule is ignored and the BlackBerry device is explicitly permitted to use AES (256-bit), AES (192-bit), AES (128-bit) and 3DES.	4.0.2	All EXCEPT CAST	Yes	
PGP Application	PGP More All and Send More	Manual	Specify the mode that a BlackBerry device uses to retrieve the complete text of an email message when a user replies to or forwards that email message.	5.0.1	Automatic	Yes	
PGP Application	PGP Universal Server Address	NULL	Type the URL of a PGP Universal Server that your organization uses to enforce a secure email policy and access PGP keys and key status. When BlackBerry devices with the PGP Support Package installed receive this rule set to a PGP Universal Server URL, they must	4.0.2	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			enroll, authenticate, and communicate with the specified PGP Universal Server to send PGP messages.				
RIM Value-Added Applications	Allow Edits to BlackBerry Social Network Application Policy URL for Lotus Quickr	Yes	Specify whether a user can change the URL for the BlackBerry Social Networking Application Proxy for IBM Lotus Quickr on a BlackBerry device.	4.1.7	No	Yes	
RIM Value-Added Applications	Allow TiVo for BlackBerry	Yes	Specify whether the TiVo for BlackBerry application on the BlackBerry device is turned on.	4.1.7	No	Yes	
RIM Value-Added Applications	BlackBerry Social Network Application Proxy URL for Lotus Connections	NULL	Specify the URL of the server that hosts the BlackBerry Social Networking Application Proxy URL for Lotus Connections	5.0.1	Agency decision		
RIM Value-Added Applications	BlackBerry Social Network Application Proxy URL for Lotus Quickr	NULL	Specify the URL of the server that hosts the BlackBerry Social Networking Application Proxy URL for Lotus Quickr	4.1.7	Agency decision		
RIM Value-Added Applications	Disable BlackBerry Wallet	No	Specify whether to prevent BlackBerry® Wallet from running on the BlackBerry device.	4.1.6	Yes		
RIM Value-Added Applications	Disable Ecommerce Content Optimization Engine	No	Specify whether to prevent the E-Commerce Optimization Engine from running on the BlackBerry device.	4.1.6	Yes		
RIM Value-Added	Disable Lotus Connections	No	Specify whether to prevent IBM® Lotus® Connections from running	4.1.6	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Applications			on the BlackBerry device.				
RIM Value-Added Applications	Lotus Connections Activities Server	NULL	Specify the server address of the server that hosts IBM Lotus Connections Activities. If this rule is not set, users can enter the server information manually. If this rule is set, users are only allowed to use the specified server information.	4.1.6	Agency decision		
RIM Value-Added Applications	Lotus Connections Blogs Server	NULL	Specify the server address of the server that hosts IBM Lotus Connections Blogs. If this rule is not set, users can enter the server information manually. If this rule is set, users are only allowed to use the specified server information.	4.1.6	Agency decision		
RIM Value-Added Applications	Lotus Connections Communities Server	NULL	Specify the server address of the server that hosts IBM Lotus Connections Communities. If this rule is not set, users can enter the server information manually. If this rule is set, users are only allowed to use the specified server information.	4.1.6	Agency decision		
RIM Value-Added Applications	Lotus Connections Dogear Server	NULL	Specify the server address of the server that hosts IBM Lotus Connections Dogear. If this rule is not set, users can enter the server information manually. If this rule is set, users will only be allowed to use the specified server information.	4.1.6	Agency decision		
RIM Value-Added Applications	Lotus Connections Profiles Server	NULL	Specify the server address of the server that hosts IBM Lotus Connections Profiles. If this rule is not set, users can enter the server information manually. If this rule is	4.1.6	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			set, users are only allowed to use the specified server information.				
S/MIME Application	Entrust Messaging Server (EMS) Email Address	NULL	Type the email address for your organization's Entrust® Messaging Server (EMS).	4.0.3	Agency decision		
S/MIME Application	S/MIME Allowed Content Ciphers	All supported algorithms	Specify the content ciphers that the BlackBerry device can use to encrypt S/MIME messages Warning: To maintain compatibility with most S/MIME clients, enable at least one of Triple DES or an RC2 cipher. Warning: If the FIPS Level rule is set to 2, then the setting of this rule is ignored and the BlackBerry device is explicitly permitted to use AES (256-bit), AES (192-bit), AES (128-bit) and 3DES.	4.0.3	AES (256-bit), AES (192-bit), AES (128-bit) and 3DES		
S/MIME Application	S/MIME More All and Send Mode	Manual	Specify the mode that a BlackBerry device uses to retrieve the complete text of an email message when a user replies to or forwards that email message.	5.0.1	Automatic	Yes	
Secure Email	Canonical Certificate Domain Name	NULL	Specify the domain name that is used for the email addresses contained in certificates issued within the organization. This rule is intended for use in organizations where users' certificates contain a long-lived email address but they typically send email from a shorter-lived email address with the same username component and a different domain component. Note:	4.0.6	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			Both the short-lived and long-lived email addresses will be used when searching for certificates for use with secure email.				
Security	Allow External Connections	Yes	Specify whether applications can initiate external connections (for example, to WAP, SMS, or other public gateways) on the BlackBerry device.	3.6.0	No	Yes	
Security	Allow Resetting of Idle Timer	No	Specify whether the BlackBerry will allow third party applications to reset the device's idle timer, bypassing the security timeout.	4.1.4	Yes		
Security	Allow Screen Shot Capture	Yes	Specify whether the BlackBerry device will allow applications to capture screen shots. This applies to RIM applications and third party applications.	4.1.4	No	Yes	
Security	Allow Split-Pipe Connections	No	Specify whether applications can open both internal and external connections simultaneously. Note: If you set this rule to Yes, applications can surreptitiously collect data from inside the firewall and send it outside the firewall without any auditing, introducing a possible security issue.	3.6.0	No	Yes	
Security	Allow Third Party Apps to Access Screen Contents	Yes	Specify whether a third-party application on a BlackBerry device can access the data that is displayed on the device screen.	5.0.3	Agency Decision	No	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Security	Allow Third Party Apps to Use Serial Port	Yes	Specify whether third-party applications on the BlackBerry device can use the serial port, IrDA, or USB ports.	3.6.0	No	Yes	
Security	Allowed Authentication Mechanisms	Allowed	Specify which types of authentication mechanisms the BlackBerry device user can turn on. The authentication mechanisms control access to the BlackBerry device. Authentication mechanisms considered "Other" can be controlled using the User Authenticator API application control setting. This IT policy rule takes priority over the Force Smart Card Two Factor Authentication IT policy rule. For example, if this IT policy rule prevents smart card authentication but the Force Smart Card Two Factor Authentication IT policy rule is set to Yes, smart card authentication is not enforced.	5.0.0	None	Yes	
Security	Certificate Status Maximum Expiry Time		Type the maximum length of time, in hours, that a certificate status can remain on the BlackBerry device before it should be updated in the Certificate Synchronization Manager and in the BlackBerry device key store. By default a certificate status can remain indefinitely on the BlackBerry device.	4.0.0	4	Yes	
Security	Content Protection of Contact List	Allowed	Specify whether a user can choose to encrypt the contact list on a BlackBerry device when content protection is turned on.	4.0.6	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Security	Content Protection Strength	NULL	Specify whether content protection is turned on by selecting the cryptography strength that the BlackBerry device uses to encrypt content that it receives while it is locked. When content protection is turned on, BlackBerry device content is always protected with the 256 bit AES encryption algorithm. If the BlackBerry device is locked when it receives content, the BlackBerry device randomly generates the content protection key (a 256 bit AES encryption key) and an ECC key pair, derives an ephemeral 256 bit AES encryption key from the BlackBerry device password, and uses the ephemeral key to encrypt the content protection key and the ECC private key. Strong: Provides good security and performance. This setting is adequate for most situations. Stronger: Provides better security, but slower performance. If you use this setting, RIM recommends that you set the Minimum Password Length IT policy rule to 12 characters. Strongest: Provides the best security, but with the slowest performance. If you use this setting, RIM recommends that you request that the user set a password of at least 21 characters. Note: Set this rule to prioritize either encryption	4.0.0	Strong	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			strength or decryption time. When the BlackBerry Enterprise Server decrypts the message using the BlackBerry device master encryption key, it uses the ECC public key in the decryption operation first, followed by a 256 bit AES decryption operation. The ECC decryption operation adds time to the decryption process. Rule dependency: The BlackBerry device uses this IT policy rule only if the Password Required rule is set to True. Note: If you do not set this rule, the BlackBerry Enterprise Server does not force content protection on the BlackBerry device; if the user enables content protection on the BlackBerry device, it forces the Strong setting, which is the Default setting.				
Security	Content Protection Usage	Yes	Specify whether you or a BlackBerry device user can turn on content protection for a BlackBerry device	5.0.2	Yes	Yes	
Security	Disable 3DES Transport Crypto	No	Specify whether to prevent the BlackBerry device from using the Triple DES algorithm to encrypt and decrypt packets that the BlackBerry device and the BlackBerry Enterprise Server that sends the IT policy send between them. Set this IT policy rule to Yes to require the BlackBerry device and the	4.0.0	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			BlackBerry Enterprise Server to use the AES algorithm to encrypt and decrypt the communication between them.				
Security	Disable BlackBerry App World	No	Specify whether the BlackBerry App World application is turned off on the BlackBerry device.	4.1.7	Yes	Yes	
Security	Disable External Memory	No	Specify whether to prevent the expandable memory (microSD) feature from working on supported BlackBerry devices.	4.0.6	Agency decision		
Security	Disable Forwarding Between Services	No	Specify whether to prevent the BlackBerry device user from forwarding or replying to a message on the BlackBerry device using an email account or messaging service that is associated with a BlackBerry Enterprise Server or BlackBerry Internet Service that is different from the service that delivered the original message. For example, use this IT policy rule to prevent forwarding or replying to a PIN message with an email message, and replying to an email message with a PIN message.	4.0.0	Yes	Yes	
Security	Disable Invalid Certificate Use	No	Specify whether to prevent the BlackBerry device user from sending a message using a certificate that is expired or not valid. Set this rule to No to force the BlackBerry device to warn the user that the certificate is expired or not valid. The BlackBerry device does	3.6.0	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			not prevent the user from sending the message.				
Security	Disable Key Store Backup	No	Specify whether to prevent the BlackBerry device user from backing up certificates and private keys in the BlackBerry device key store.	4.0.0	Yes	Yes	
Security	Disable Key Store Low Security	No	Specify whether to prevent a BlackBerry device user frrom setting the key store security to low.	4.0.0	Yes	Yes	
Security	Disable Media Manager FTP Access	No	Specify whether to disable access to the file transfer protocol channel from the media manager tool of the BlackBerry Desktop Manager.	4.0.6	Yes		
Security	Disable Persisted Plain Text	No	Specify whether to prevent applications from persisting the plain text form of a content protected object in the persistent store (for example, the file system). Set this rule to Yes to enable the BlackBerry device to write information about the application in the BlackBerry device Event Log, and then reset, returning the BlackBerry device to a valid known state. Warning: If you set this rule to Yes, all applications might not work. RIM recommends this setting only for very security-conscious customers who need assurance that sensitive data cannot be persisted in plain text form.	4.0.0	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Security	Disable Public Photo Sharing Applications	No	Specify whether to prevent public photo sharing applications (for example, Flickr) on the BlackBerry device from uploading photos to public servers.	4.1.4	Agency decision		
Security	Disable Public Social Networking Applications	No	Specify whether to prevent public social networking applications on the BlackBerry device from accessing public social networking services (for example, Facebook).	4.1.5	Agency decision		
Security	Disable Revoked Certificate Use	No	Specify whether to prevent the BlackBerry device user from sending messages that are encrypted using revoked certificates. Set this rule to No to force the BlackBerry device to warn the user that the certificate is revoked. The BlackBerry device does not prevent the user from sending the message.	3.6.0	Yes	Yes	
Security	Disable Smart Password Entry	No	Specify whether to prevent the user from using smart password entry on the BlackBerry device when using two factor authentication. If you set the IT policy rule to Yes, the BlackBerry device resets any knowledge of the user's numeric passwords if the user is currently using smart password entry. If you set this IT policy rule to No, the user cannot use smart password entry on the BlackBerry device when using two factor authentication. If the user is using two-factor authentication and their BlackBerry device	4.0.6	Yes		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			password or authenticator password is numeric, smart password entry enables the BlackBerry device to remember whether the last password that the user typed in a password field was numeric and if it was, the next time that the user types the password the BlackBerry device applies a numeric filter so that the user does not have to press the Alt key to type the numbers. By default, the BlackBerry device stores knowledge of the user's numeric passwords only if the user is using smart password entry.				
Security	Disable Stale Status Use	No	Specify whether to prevent the BlackBerry device user from sending a message that is encrypted using a certificate with a stale status. Set this rule to No to force the BlackBerry device to warn the user that the certificate is stale. The BlackBerry device does not prevent the user from sending the message.	4.0.0	Yes	Yes	
Security	Disable Untrusted Certificate Use	No	Specify whether to prevent the BlackBerry device user from sending messages that are encrypted with certificates that the BlackBerry device does not trust. Set this rule to No to force the BlackBerry device to warn the user that the certificate is not trusted. The BlackBerry device does not prevent the user from sending the	3.6.0	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			message.				
Security	Disable Unverified Certificate Use	No	Specify whether to prevent the BlackBerry device user from sending messages that are encrypted with a certificate that the BlackBerry device cannot verify. If this rule is set to No, the user is warned about, but not prevented from, using an unverified certificate.	4.0.0	Yes	Yes	
Security	Disable Unverified CRLs	No	Specify whether to prevent the BlackBerry device user from accepting unverified CRLs on the Mobile Data Service when checking the status of a certificate.	4.0.0	Yes	Yes	
Security	Disable USB Mass Storage	No	Specify whether to prevent the USB Mass Storage feature from working on supported BlackBerry devices. If you set this IT policy rule to Yes, the BlackBerry device cannot use an external file system connected to the USB port. This means that the ability to transfer files to an external file system using the Media Manager with BlackBerry Desktop Manager Version 4.2.2 and 4.3 is turned off.	4.0.6	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Security	Disable Weak Certificate Use	No	Specify whether to prevent the BlackBerry device user from sending a message using a certificate that has a weak corresponding public key. Set this rule to No to force the BlackBerry device to warn the user that the certificate has a weak corresponding public key. The BlackBerry device does not prevent the user from sending the message. Note: Use the IT policy rules provided for each secure messaging application (WTLS, TLS, S/MIME, PGP) to set the minimum strength for each type of encryption key (RSA, DH, DSA, ECC). Note: Use the Weak Digest Algorithms IT policy rule to set the digest algorithms that the BlackBerry device considers weak.	3.6.0	Yes	Yes	
Security	Disallow Third Party Application Downloads	No	Specify whether applications that are not digitally signed by the Research In Motion® signing authority system are permitted on the BlackBerry® device if the user tries to download the applications or the BlackBerry® Enterprise Server or another party sends the applications to the device. This rule prevents the user from installing unsigned third-party applications over the wireless network or when the BlackBerry device is connected to the BlackBerry® Desktop	3.6.0	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			Manager or application loader tool.				
Security	Encryption on On-Board Device Memory Media Files	Allowed	If a media card is inserted in the BlackBerry device, this rule specifies whether the media files that are located in the media card are encrypted to the user password and the device-generated key.	4.0.6	Allowed or Required. See notes		If the media data is higher than UNCLASSIFIED, set to "Required"
Security	Enforce FIPS Mode of Operation	No	Specify whether a BlackBerry device must operate in FIPS mode. FIPS are computer-system standards that were developed by the United States federal government.	5.0.3	Yes	Yes	
Security	External File System Encryption Level	NULL	Specify the level of encryption that a BlackBerry device uses to encrypt files that it stores on a media card.	4.0.6	"Encrypt to User Password (including multimedia directories)"	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Security	FIPS Level	FIPS 140-2 Level 1 compliance	Specify the level of Federal Information Processing Standard (FIPS) compliance. Level 1: You can apply Level 1 compliance to Java based BlackBerry devices using BlackBerry Device Software Version 3.3.0 and later. Level 1 compliance affects the BlackBerry Cryptographic Kernel, which is the embedded cryptographic module required for basic operation of the BlackBerry device. Level 2: You can apply Level 2 compliance to Java® based BlackBerry devices using BlackBerry Device Software Version 4.0 and later. Level 2 compliance affects only the BlackBerry Device Software and does not result in the BlackBerry device meeting FIPS 140-2 Level 2 hardware security requirements. Warning: Selecting Level 2 prevents WTLS from using the RC5 cipher, which can result in problems using the WTLS protocol. Set this rule to Level 2 to force all BlackBerry Device Software to operate in a FIPS-compliant mode of operation and enforce the following IT policy rules with these values: Password Required = Yes Minimum Password Length >= 5 characters Suppress Password Echo = True SMIME Allowed Content Ciphers = AES (256-bit) | AES (192-bit) | AES (128-bit)| Triple	4.0.0	FIPS 140-2 Level 2	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			DES TLS Restrict FIPS Ciphers = Yes PGP Allowed Content Ciphers = AES (256-bit) | AES (192-bit) | AES (128-bit)| Triple DES Disallow Third Party Application Downloads = Yes				
Security	Firewall Block Incoming Messages	NULL	Specify whether the firewall on the BlackBerry device blocks, and prevents the BlackBerry device from processing, specific types of incoming messages that bypass your corporate network. If you set this IT policy rule, the BlackBerry device drops the specified type(s) of incoming messages at the firewall and does not display received message notifications for those messages. Note: Users can specify whether to block public PIN messages on the BlackBerry device. Users cannot specify whether to block corporate PIN messages on the BlackBerry device.	4.0.6	BIS	Yes	BES Admin to block all messages that are not needed. E.g. Block SMS messages if SMS messaging is disabled.

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Security	Force Cryptographic Power Analysis Protection	No	Specify whether a BlackBerry device must use algorithms that are protected by cryptographic power analysis (if available).	5.0.3	Yes	Yes	
Security	Force Device Password Entry While User Authentication is Enabled	No	Specify whether a BlackBerry device user must type the BlackBerry device password and credentials for the second-factor authentication method to unlock the device	5.0.0	Yes	Yes	
Security	Force LED Blinking When Microphone Is On	No	Specify whether the BlackBerry device indicates that its microphone is on (for example, when a phone call is in progress or a voice note is being recorded). If you set this rule to Yes, the BlackBerry device LED blinks rapidly when its microphone is on. If you set this rule to No, the BlackBerry device does not indicate that its microphone is on.	4.0.3	Agency decision		
Security	Key Store Password Maximum Timeout	60	Type the maximum number of minutes allowed before the cached key store password times out and the BlackBerry device prompts the user to type the key store password. If you set this rule to 0, the BlackBerry device does not cache the key store password. Note: The BlackBerry device key store is the database that stores the user's private keys. The key store uses a password to protect the user's private keys. By default, the BlackBerry device caches the key	3.6.0	1	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			store password to minimize the number of key store password prompts.				
Security	Login Disclaimer	NULL	Specify the disclaimer that a BlackBerry device can display before a user unlocks the BlackBerry device for the first time after you or a user resets the BlackBerry device.	5.0.1	Agency decision		
Security	Media Card Format on Device Wipe	Allowed	Specify whether a BlackBerry device formats a media card when a user or administrator permanently deletes all data on a BlackBerry device.	5.0.1	Required	Yes	
Security	Message Classification	NULL	Specify the set of message classifications available to users within the enterprise.	4.1.2	Agency decision		
Security	Message Classification Title	NULL	Specify the message classification title that BlackBerry devices will include when users within the organization send messages.	4.1.4	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Security	Minimal Encryption Key Store Security Level	Low security	Specify the minimum security level for the encryption key in the key store. All keys on the BlackBerry device are forced to have the security level you set using this rule as their minimum, but the user can set a higher security level if desired. Low security: The BlackBerry device never prompts the user for their key store password when accessing the encryption key. Medium security: The BlackBerry device only prompts the user for their key store password if the password is cleared from the key store cache. Note: Medium security is the default security level assigned to a private key when it is first loaded on to the device. High security: The BlackBerry device always prompts the user for their password when accessing the encryption key. If the user recently typed the password, the BlackBerry device prompts the user to confirm access to the private key.	4.0.0	High security	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Security	Minimal Signing Key Store Security Level	Low security	Specify the minimum security level for the signing key in the key store. Note: All keys on the BlackBerry device are forced to have the security level you set using this rule as their minimum, but the user can set a higher security level if desired. Low security: The BlackBerry device never prompts the user for their key store password when accessing the signing key. Medium security: The BlackBerry device only prompts the user for their key store password if the password is cleared from the key store cache. Note: Medium security is the default security level assigned to a private key when it is first loaded on to the device. High security: The BlackBerry device always prompts the user for their password when accessing the signing key. If the user recently typed the password, the BlackBerry device prompts the user to confirm access to the private key.	4.0.0	High security	Yes	
Security	Remote Wipe Reset to Factory Defaults	No	Specify whether the BlackBerry device resets itself to factory default settings when it receives the Erase Data and Disable Handheld IT Admin command over the wireless network. Set this IT policy rule to Yes to require the BlackBerry device to permanently delete its stored IT policy and delete all third party applications, in addition to	4.1.4	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			performing the BlackBerry device wipe process.				
Security	Require Secure APB Messages	No	Specify whether the BlackBerry device can receive unsecured messages, including All Points Bulletin (APB) messages, from a BlackBerry Enterprise Server. The BlackBerry device can receive all messages from the BlackBerry Enterprise Server that are not blocked at the firewall on the BlackBerry device unless you set this IT policy to Yes to prevent the BlackBerry device from receiving unsecured messages.	4.0.6	Yes	Yes	
Security	Secure Wipe Delay After IT Policy Received	Disabled	Specify the length of time, in hours, after receiving an IT policy update that the BlackBerry device securely wipes all of its user data. Use this IT policy rule to require a BlackBerry device that cannot receive IT policy updates or IT Admin commands to perform a secure wipe of user data after the length of time specified. Warning: If you set this IT policy rule, set the Policy Resend Interval on the BlackBerry Enterprise Server (in the IT Admin properties) to a value that is lower than this rule setting to prevent unwanted BlackBerry device wiping.	4.0.6	Agency decision		

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
Service Exclusivity	Allow Other Browser Services	Yes	Specify whether users can use other browser services on the BlackBerry device. Set this rule to No to force all browser traffic through your organization's BlackBerry Enterprise Server and prevent users from installing other browser services.	3.5.0	No	Yes	
Service Exclusivity	Allow Other Calendar Services	Yes	Specify whether BlackBerry device users can use calendar services other than the standard calendar application. Set this rule to No to make it mandatory for BlackBerry device users in your organization to send appointments through a BlackBerry Enterprise Server within your organization's environment.	4.1.5	No	Yes	
Service Exclusivity	Allow Other Message Services	Yes	Specify whether users can use other message services on the BlackBerry device. Set this rule to No to force all outbound messages through your organization's BlackBerry Enterprise Server and prevent users from sending outbound messages from other message services. Warning: This rule does not prevent users from receiving inbound messages from other message services.	3.5.0	No	Yes	
Service Exclusivity	Allow Public AIM Services	Yes	Specify whether the public AOL Instant Messenger (AIM) for BlackBerry service is permitted on the BlackBerry device. Set this rule to No to prevent communication using the public AIM service on the	3.6.6	No	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			BlackBerry device.				
Service Exclusivity	Allow Public Google Talk Services	Yes	Specify whether the public Google Talk for BlackBerry service is permitted on the BlackBerry device. Set this rule to No to prevent communication using the public Google Talk service on BlackBerry devices. Note: If you set this rule to No and users have downloaded Google Talk for BlackBerry onto their BlackBerry devices, the Google Talk for BlackBerry icon remains on the Home screen. If users attempt to sign into Google Talk for BlackBerry, a message on their BlackBerry devices indicates that they cannot use Google Talk for BlackBerry.	4.0.4	No	Yes	
Service Exclusivity	Allow Public ICQ Services	Yes	Specify whether the public ICQ service is permitted on the BlackBerry device. Set this rule to No to prevent communication using the public ICQ service on the BlackBerry device.	3.6.6	No	Yes	
Service Exclusivity	Allow Public IM Services	Yes	Specify whether any public instant messaging (IM) for BlackBerry services are permitted on the BlackBerry device. Set this rule to No to disable access to all public IM services on the BlackBerry device, and to prevent communication using any public instant messaging service on the BlackBerry device.	4.0.4	No	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
			Note: This rule applies to all RIM public IM services that were released after the first availability of this rule. To prevent Yahoo! Messenger 1.0 from running on the BlackBerry device, use the Allow Public Yahoo! Messenger Services rule.				
Service Exclusivity	Allow Public WLM Services	Yes	Specify whether the public Windows Live Messenger for BlackBerry service is permitted on the BlackBerry device. Set this rule to No to prevent communication using the public Windows Live Messenger service on BlackBerry devices.	4.1.5	No	Yes	
Service Exclusivity	Allow Public Yahoo! Messenger Services	Yes	Specify whether the public Yahoo! Messenger for BlackBerry service is permitted on the BlackBerry device. Set this rule to No to prevent communication using the public Yahoo! Messenger service on the BlackBerry device.	3.6.4	No	Yes	
TLS Application	TLS Disable Invalid Connection	Prompt user on BlackBerry device	Specify whether the BlackBerry device permits the use of connections to servers with invalid certificates during TLS connections.	3.6.0	Yes	Yes	
TLS Application	TLS Disable Untrusted Connection	Prompt user on BlackBerry device	Specify whether to prevent the BlackBerry device from permitting the use of connections to untrusted servers during TLS connections.	3.6.0	Yes	Yes	
TLS Application	TLS Disable Weak Ciphers	Prompt user on BlackBerry device	Specify whether to prevent the BlackBerry device from permitting the use of weak ciphers during TLS connections.	3.6.0	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
TLS Application	TLS Minimum Strong DH Key Length	512	Specify the minimum DH key size, in bits, that the BlackBerry device permits for use in TLS connections.	3.6.0	1024	Yes	
TLS Application	TLS Minimum Strong DSA Key Length	512	Specify the minimum DSA key size, in bits, that the BlackBerry device permits for use in TLS connections.	3.6.1	1024	Yes	
TLS Application	TLS Minimum Strong ECC Key Length	160	Specify the minimum ECC key size, in bits, that the BlackBerry device permits for use in TLS connections.	3.6.0	163	Yes	
TLS Application	TLS Minimum Strong RSA Key Length	512	Specify the minimum RSA key size, in bits, that the BlackBerry device permits for use in TLS connections.	3.6.0	1024	Yes	
TLS Application	TLS Prevent Unmatched Domain Name	Prompt user on BlackBerry device	Specify whether to prevent a BlackBerry device from opening a TLS connection to a server that has a domain name that does not match any domain names in the server's certificate	5.0.1	Yes	Yes	
TLS Application	TLS Restrict FIPS Ciphers	No	Specify whether the BlackBerry device can use an algorithm with TLS that is not FIPS-compliant. Warning: If the FIPS Level IT policy rule is set to 2, by default, the BlackBerry device ignores this IT policy rule and uses only algorithms that are FIPS-compliant.	3.6.0	Yes	Yes	
Wireless Software Upgrades	Disallow Device User Requested Rollback	No	Specify whether to prevent the BlackBerry device user from requesting rollbacks of previously successful wireless software upgrades.	4.1.4	Yes	Yes	
Wireless Software Upgrades	Disallow Device User Requested Upgrade	No	Specify whether to prevent the BlackBerry device user from requesting available wireless software upgrade packages.	4.1.4	Yes	Yes	

Policy group	IT policy rule	Default value	Description	Minimum version for BlackBerry Enterprise Server	Recommended value	Mandatory for RESTRICTED/ PROTECTED	Notes
WTLS Application	WTLS Disable Invalid Connection	Prompt user on BlackBerry device	Specify whether the BlackBerry device permits the use of connections to servers with invalid certificates during WTLS connections.	3.6.0	Yes	Yes	
WTLS Application	WTLS Disable Untrusted Connection	Prompt user on BlackBerry device	Specify whether the BlackBerry device permits the use of connections to untrusted servers during WTLS connections.	3.6.0	Yes	Yes	
WTLS Application	WTLS Disable Weak Ciphers	Prompt user on BlackBerry device	Specify whether the BlackBerry device permits the use of weak ciphers during WTLS connections.	3.6.0	Yes	Yes	
WTLS Application	WTLS Minimum Strong DH Key Length	512	Specify the minimum DH key size, in bits, that the BlackBerry device permits for use in WTLS connections.	3.6.0	1024	Yes	
WTLS Application	WTLS Minimum Strong ECC Key Length	160	Specify the minimum ECC key size, in bits, that the BlackBerry device permits for use in WTLS connections.	3.6.0	163	Yes	
WTLS Application	WTLS Minimum Strong RSA Key Length	512	Specify the minimum RSA key size, in bits, that the BlackBerry device permits for use in WTLS connections.	3.6.0	1024	Yes	
WTLS Application	WTLS Restrict FIPS Ciphers	No	Specify whether the BlackBerry device can use an algorithm with WTLS that is not FIPS-compliant. Warning: If the FIPS Level IT policy rule is set to 2, by default, the BlackBerry device ignores this IT policy rule and uses only algorithms that are FIPS-compliant.	4.0.0	Yes	Yes	