



WIRELESS STIG BLACKBERRY SECURITY CHECKLIST

Version 5, Release 2.2

15 September 2008

Developed by DISA for the DoD

Database Reference Number: _____

CAT I: _____

Database entered by: _____ Date: _____

CAT II: _____

Technical Q/A by: _____ Date: _____

CAT III: _____

Final Q/A by: _____ Date: _____

CAT IV: _____

TOTAL: _____

UNCLASSIFIED

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

Site Name: _____ Date of Wireless

SRR: _____

Wireless Reviewer		Phone/Location		
Previous SRR (circle)	Y N	Date of Previous SRR		
Number of Current Open Findings				
Site Name				
Address				
Phone				
Position	Name	Phone Number	Email	Area of Responsibility
IAM				
IAO				
BlackBerry Administrator				

This page is intentionally left blank.

TABLE OF CONTENTS

	Page
SUMMARY OF CHANGES.....	X
1. INTRODUCTION.....	1
2. BLACKBERRY COMPLIANCE REQUIREMENTS.....	4
2.1 Wireless Policy – Applicable to all Devices.....	4
WIR0010 All Wireless systems must have DAA approval.....	4
WIR0011 Personally owned PEDs are used	5
WIR0016 Maintain an equipment list of all approved PED devices.....	6
WIR0030 Document equipment in the SSP.....	7
WIR0072 Wireless network devices must be physically protected	7
WIR0076 Require signed user agreement	8
WIR0180 Wireless devices allowed into SCIFs must be DCID compliant.....	11
WIR0225 CTTA coordination and proper separation required	12
2.2 System Security Requirements	13
WIR0012 Display required DoD logon banner on PDA / Smartphone	13
WIR0371 PDAs/Smartphones with cameras must be approved	13
WIR0372 PDAs and Smartphones with cameras not allowed in classified areas.....	14
WIR1010 Establish CMI procedures for wireless email devices.....	15
WIR1015 Establish disposal procedures for wireless email devices	16
WIR1020 Do not use wireless email for classified messages	16
WIR1030 Scan BlackBerry devices using the AutoBerry tool.....	17
WIR1040 Do not connect BlackBerry servers to classified DoD networks	18
WIR1050 BlackBerry users must receive required training	19
WIR1070 Use only BES email solution	21
WIR1080 Install BES using approved architecture	22
WIR1090 Required actions if wireless email handheld is lost or stolen	25
WIR1100 Authenticated login procedures to unlock a wireless email device.....	26
WIR1110 Password Keeper configuration must be compliant.....	28
WIR1130 Control of BlackBerry applications (Part I)	29
WIR1131 Control of BlackBerry applications (Part II).....	32
WIR1132 Control of BlackBerry applications (Part III)	34
WIR1140 Bluetooth usage must be compliant	35
WIR1150 Bluetooth Smart Card Reader usage must be compliant	36
WIR1160 Secure wireless email servers using operating system STIG.....	40
WIR1170 Comply with provisioning requirements for wireless email devices.....	41
WIR1180 Do not allow users to install or remove applications.....	42
WIR1190 Do not install Onset Technologies METAmessgae software	43
WIR1200 Digitally sign email emergency and/or critical email notifications.....	44
WIR1210 Configure wireless email auto signature as required.....	45
WIR1220 If Text Messaging or Instant Messaging are used, enable security	46
WIR1230 Setup of BlackBerry Wi-Fi security controls.....	47

WIR1240 The wireless carrier Internet browser is disabled	50
WIR1250 Implement BES and BlackBerry handheld configuration settings	51
WIR1260 Configure Master Key on the BES	52
WIR1280 Data-at-Rest encryption is enabled on all wireless email devices	53
3. BES AND BLACKBERRY DEVICE SECURITY INFORMATION	54
3.1 Creating IT Policies	54
3.2 Creating an Activation Password.....	55
3.3 BlackBerry Application Security.....	55
3.3.1 Application Security Controls.....	56
3.3.1.1 IT Policy Controls.....	57
3.3.1.2 Software Configuration Controls.....	58
3.3.1.3 Application Control Policies.....	59
3.3.2 Configuring BlackBerry MDS Services Security.....	63
3.3.2.1 Configuring BlackBerry Authentication To Web Servers.....	64
3.3.2.2 Data Encryption	64
3.3.2.3 BlackBerry MDS Connection Service Properties.....	65
3.3.2.4 BlackBerry MDS Integration Service Security.....	67
3.4 S/MIME Configuration.....	67
3.5 PGP Encryption	68
3.6 Managing Encryption Keys	68
3.7 Maintenance Configuration	69
3.7.1 Logging.....	69
3.7.2 BES Alert Settings	71
3.7.3 System Backup.....	72
3.7.4 BES Monitoring Tools.....	73
3.8 Content Protection	73
3.9 Password Keeper Settings.....	73
3.10 Bluetooth Security Settings.....	74
3.11 Bluetooth Smart Card (CAC) Reader	74
3.12 Forcing BlackBerry Device Software Updates.....	74
3.13 Firewall Requirements	75
3.13.1 BES Architecture	75
3.13.2 BlackBerry Host Based Firewall Non-Segmented Architecture	75
3.13.3 Segmented Architecture.....	78
3.14 BlackBerry IP Modem	80
3.15 Disposal of BlackBerry Handhelds.....	81
3.16 Use of “Team” BlackBerrys	81
3.17 RIM Bluetooth Smart Card Reader Connections to PCs.....	81
3.18 Using Software Certificates	82
3.19 BlackBerry Use with Wireless LANs.....	83
3.19.1 Wi-Fi Connection to a DoD Operated Enterprise WLAN System.....	84
3.19.2 Wi-Fi Connection to a Public Hot Spot WLAN System	84
3.19.3 Wi-Fi Connection to a Home WLAN System	84
3.19.4 BlackBerry Wi-Fi Security Controls	85
3.19.5 Instructions for Installing a BlackBerry Device Certificate	85

3.19.6	BlackBerry Wi-Fi Voice over IP (VoIP)	86
3.20	Antivirus Support on BlackBerry Devices	86
3.21	AutoBerry Tool	86
3.22	BlackBerry Instant Messaging	87
3.23	Additional BlackBerry Applications and Services	87
3.23.1	Documents To Go	87
3.23.2	BlackBerry Mobile Voice System (MVS)	87
3.23.3	BlackBerry Web Desktop Manager	87
APPENDIX A. REFERENCES		90
APPENDIX B. BLACKBERRY DISPOSAL PROCEDURES		93
APPENDIX C. BES IT POLICY RULES AND CONFIGURATION SETS		95
APPENDIX D. HANDHELD SOFTWARE CONFIGURATION SETTINGS		164
APPENDIX E. CAC DIGITAL CERTIFICATE PROVISIONING		171
APPENDIX F. VMS PROCEDURES		174
APPENDIX G. BLACKBERRY CONFIGURATION FOR GROUP EMAIL ACCOUNTS		177

TABLE OF TABLES

	Page
Table 3-1. Activation Password Security.....	55
Table 3-2. HTTP Properties.....	65
Table 3-3. Proxy Properties.....	65
Table 3-4. TLS and HTTPS Properties.....	65
Table 3-5. Log Properties.....	66
Table 3-6. BES Alert Setting.....	72
Table 3-7. Host-Based Firewall Architecture Ports, Protocols and Services for Non-Segmented Architecture On BES.....	78
Table 3-8. Host-Based Firewall Architecture Ports, Protocols and Services for Segmented Architecture On BES Router.....	78
Table 3-9. Host-Based Firewall Architecture Ports, Protocols and Services for Segmented Architecture On BES.....	80
Table C.1. BES IT Policy Rules in Order Listed in BES.....	143
Table C.2. BES IT Policy Rules in Alphabetical Order.....	151
Table C.3. WLAN Configuration Set.....	154
Table C.4. VPN Configuration Set.....	157
Table C.5. Configuration Settings for Application Control Policy Rules.....	160
Table C.6. Configuration Settings for MDS Integration Service Device Policy Rules.....	162
Table D.1. BlackBerry Handheld Software Configuration Settings.....	169
Table E-1. VMS Asset Matrix.....	175

TABLE OF FIGURES

	Page
Figure 2-1. Example BlackBerry Network Architecture.....	23
Figure 2-2. Segmented BlackBerry Network Architecture.....	24
Figure 3-1. Determine if a Wireless Update is Successful.....	59
Figure 3-2. Deny All Application Control Policy.....	60
Figure 3-3. Optional Application Control Policy.....	61
Figure 3-4. Assigning Application Control Policies to Applications.....	62
Figure 3-5. BlackBerry Connections to Enclave Servers.....	64
Figure 3-6. Screen Shot – LDAP Configuration.....	66
Figure 3-7. Screen Shot – OCSP Configuration.....	67
Figure 3-8. Screen Shot – Selecting Master Key Algorithm.....	68
Figure 3-9. Screen Shot – Configuring Global BES Logs.....	70
Figure 3-10. Screen Shot – Configuring component BES Logs.....	71
Figure 3-11. Screen Shot – Configuring BES Alert.....	72
Figure 3-12. Screen Shot – Setting Password Keeper password.....	74

This page is intentionally left blank.

SUMMARY OF CHANGES

GENERAL CHANGES:

The previous release was Version 5, Release 2.1, dated 15 November 2007

SECTION CHANGES

SECTION 1. INTRODUCTION

Minor editorial changes.

SECTION 2. BLACKBERRY COMPLIANCE REQUIREMENTS

All checks were reordered into two new subsections: 2.1 Wireless Policy and 2.2 System Security Requirements.

Minor editing changes were completed on the following checks: WIR0010, WIR 1010, WIR1015, WIR1020, WIR1040, WIR1090, WIR1110, WIR1130, WIR1140, WIR1150, WIR1170, WIR1200, WIR1250, & WIR1260.

WIR 1030 – This is a new check that describes requirements for BlackBerry users and Administrators to run the DoD developed AutoBerry tool on site managed BlackBerry devices.

WIR1050 – This is a new check. All user training requirements from all BlackBerry checks have been consolidated into this check.

WIR1070 – Added clarification regarding connections of BlackBerry devices to more than one email system.

WIR1080 – Major changes to this requirement. The DMZ architecture has been removed because it was determined to be impractical. A new, segmented architecture has been defined.

WIR1130 – This check has been completely revised and now is Part I of the three part application security control requirements.

WIR1131 and WIR1132 – These checks are new. They are Part II and Part III of the three part application security control requirements.

WIR1220 – This check has been modified to add BlackBerry Instant Messaging security requirements.

WIR1230 – This is a new check. This check describes requirements for the BlackBerry Wi-Fi Service.

WIR1270 – This check has been deleted. It is no longer applicable because the BES automatically updates the BlackBerry Master Key every 30 days.

SECTION 3. BES SECURITY RELATED CONFIGURATIONS

Section 3.1 – Added new information on the IT Policy export / import tool in the BlackBerry resource kit and the DISA developed STIG compliant IT policy file.

Section 3.3 – This is a new section that covers security controls for applications used on BlackBerry devices, including applications and content servers located on the enclave network and accessed by site managed Blackberry devices.

Section 3.6 – Updated to state that the AES algorithm is now required for the BlackBerry Master Key.

Section 3.7 – Minor updates.

Section 3.13 – Updated to correspond to the changes to WIR1080. IP filtering must now be configured on the host-based BES firewall for connections to enclave servers.

Section 3.14 – Minor update.

Section 3.18 – Added requirements for the BlackBerry password when software certificates are used on the BlackBerry.

Section 3.19 – This is a new section on security controls for using Wi-Fi with BlackBerry devices. Requirements for Wi-Fi VoIP connections are also described.

Section 3.20 – This is a new section that describes BlackBerry antivirus protections.

Section 3.21 – This is a new section that describes the AutoBerry tool.

Section 3.22 – This new section describes BlackBerry Instant Messaging security controls.

Section 3.23 – This is new section that describes Documents to Go.

APPENDIX A. REFERENCES

Updated to remove outdated references and added new references.

APPENDIX B. BLACKBERRY DISPOSAL PROCEDURES

No changes.

APPENDIX C. BES IT POLICY RULES

Added new IT Policy rules to Table C.1 that were released in versions 4.1.5 and 4.1.6 of the BES.

Obsolete IT Policy rules have been removed from Table C.1.

The following IT Policy rules have been changed from the previous version of this document. Types of changes include status of the rule (Required or Optional), configuration setting of the rule, or finding Security Category Code.

<u>Policy Group</u>	<u>Policy Rule</u>
BlackBerry Smart Card Reader	Disable Auto Reconnect To BlackBerry Smart Card Reader
BlackBerry Smart Card Reader	Maximum Number of PC Pairings
Browser	Disable Auto Synchronization in Browser
Browser	MDS Browser Use Separate Icon
Common	Disable Kodiak PTT
Common	Disable Voice-Activated Dialing
Device-Only	Allow Peer-to-Peer Messages
Device-Only	Default Browser Config UID
Device-Only	User Can Change Timeout
S/MIME Application	S/MIME Allowed Content Ciphers
Security	Disable 3DES Transport Crypto
Security	Disable Peer-to-Peer Normal Send
Security	Disable Public Photo Sharing Applications
SIM Application Toolkit	Disable Network Location Query
SIM Application Toolkit	Disable SIM Call Control
SIM Application Toolkit	Disable SIM Originated Calls

Tables C.2, C.3, C.4, C.5, and C.6 are new.

APPENDIX D. HANDHELD SOFTWARE CONFIGURATION SETTINGS

Added new check to Table D.1 on BlackBerry Auto Signature (this check was previously in Table C.1).

APPENDIX E. CAC DIGITAL CERTIFICATE PROVISIONING

Added requirement to load BlackBerry PIV drivers.

APPENDIX F. VMS PROCEDURES

Section has been updated.

APPENDIX G. BLACKBERRY CONFIGURATION FOR GROUP EMAIL ACCOUNTS

No changes.

1. INTRODUCTION

This Checklist provides security policy and configuration requirements for the use of BlackBerry wireless email in the Department of Defense (DoD). Guidance in this document applies to all BlackBerry systems, including BlackBerry handheld devices and the BlackBerry Enterprise Server (BES).

This checklist serves as both a security review checklist and a configuration guide. Information Assurance Officers (IAOs), Security Managers (SMs), System Administrators (SAs), device users, and security readiness reviewers, each with varying experience levels, should use this document to ensure the security of BlackBerry implementations. Thus, the format of each section is tailored to meet these various needs.

Section 2 lists all BlackBerry system security checks and will be used by IAOs, SMs, and SAs for performing self-assessments and by DISA FSO to perform Security Readiness Reviews (SRRs).

Section 3 and Appendices B, C, D, E, and G are intended for experienced BES administrators who have completed BES 4.1 for Microsoft Exchange Administrator training. SAs should also consult Appendix A for a listing of various Research in Motion (RIM) configuration guides and other documents. The configuration settings (or actions) in Section 3 and Appendices C and D are classified as either “Required” or “Optional”. “Required” configuration settings are mandatory for all installations of DoD BES for Microsoft Exchange and for BlackBerry Handheld Software. “Optional” settings are the recommended and preferred configuration for installations of DoD BES 4.1 for Microsoft Exchange and BlackBerry Handheld Software. “Optional” configuration settings may not be possible at all DoD installations because of operational or network constraints.

Appendix F provides procedures used by SAs and SRR reviewers when registering and updating assets in the DoD Vulnerability Management System (VMS).

This checklist covers configuration requirements for BES versions 4.1 up to SP6 and BlackBerry Handheld Software version 4.0 to 4.5. Earlier versions of software are not authorized for use in DoD. Note that all configuration procedures listed in this checklist are for BES version 4.1.6 and BlackBerry Handheld Software version 4.2 and may vary for other versions.

This checklist has the minimum “baseline” BlackBerry security guidance for DoD. Combatant Commanders/Services/Agencies (CC/S/A) may direct more secure configuration settings based on operational requirements.

For our NATO customers using this document:

The term “classified” used in this document refers to US Government classifications of Confidential, Secret and Top Secret. NATO BlackBerry deployments are permitted to carry information bearing a NATO classification of “NATO restricted” and should be treated in a similar manner as US Government information marked Unclassified//For Official Use Only. The security guidance provided in this document can be directly applied to NATO

BlackBerry deployments with the understanding that “NATO Restricted” information should not be equated to US Government-defined “classified” information.

This page is intentionally left blank.

2. BLACKBERRY COMPLIANCE REQUIREMENTS

2.1 Wireless Policy – Applicable to all Devices

Perform these checks for all wireless devices (Classified or Unclassified) that are used to process, transmit, store, or connect to DoD information or Enclave resources. Perform these general checks first, and then perform checks in Section 2.2.

For VMS users: These policies are listed in VMS under the Non-Computing Assets, Wireless Policy asset posture. The reviewer should create one non-computing asset for the site BlackBerry system (e.g. Fort Smith BlackBerry System).

WIR0010 All Wireless systems must have DAA approval

VMS Vulnerability Key: V0008283

Long Name: The IAO will ensure all wireless systems including associated peripheral devices, operating system, applications, network/PC connection methods, and services are approved by the DAA prior to installation and use for processing DoD information.

Severity: CAT I

Checks: Work with the site POC to verify documentation. Performed with WIR0016 (equipment list).

1. Request copies of written DAA approval documentation.
 - A signed wireless inventory list, SSAA/SSP, or DAA approval documents as proof of compliance.
 - DAA approval letter and SSAA/SSP may be a general statement of approval rather than list each device.
2. Verify DAA approval for each device used (i.e., wireless connection services, peripherals, and applications).

Mark this check as a finding for any of the following reasons.

Wireless systems, devices, services, or accessories are in use but DAA approval letter(s) do not exist.

If in the judgment of the reviewer, configuration differs significantly from that approved by the DAA approval letter.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR0011 Personally owned PEDs are used

VMS Vulnerability Key: V0015872

Long Name: The IAO will ensure personally owned PEDs are not used to transmit, receive, store, or process DoD information unless approved by the DAA and the owner signs a forfeiture agreement in case of a security incident.

Severity: CAT III

Checks: Interview the IAO.

1. Ask if users are using personally owned devices such as PDAs, Blackberries, laptops, or home computers to access sensitive Enclave resources. Access to publicly available resources in the DMZ can be accessed via personal devices, depending on the INFOCON level.
2. If personally owned devices are allowed, verify written DAA approval exists and the SSAA is annotated.
3. Verify a **forfeiture agreement** is being used at the site and users are trained to report security incidents on personally owned devices.
4. Mark as a finding if:
 - a. CAT I finding if personally owned devices are used for classified access.

Hint: This check includes any non-DoD owned or approved devices such as computers, PEDs/PDAs, and wireless NICs. This applies to administrative and end-user access. Use of personally owned devices is discouraged but may be approved by DAA.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR0016 Maintain an equipment list of all approved PED devices

VMS Vulnerability Key: V0008284

Long Name: The IAO will maintain a list of all DAA approved wireless and non-wireless PED devices that store, process, or transmit DoD information. The list will be stored in a secure location.

Severity: CAT III

Checks:

1. Verify existence of site wireless equipment list.
2. Determine the process for updating the list and keeping it current. The list should indicate date of last update.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR0030 Document equipment in the SSP

VMS Vulnerability Key: V0008297

Long Name: The IAO will ensure wireless devices connecting directly or indirectly (e.g., hotsync, ActiveSync, wireless) to the network are added to the site System Security Plan (SSP).

Severity: CAT III

Checks: Review the SSP.

1. Wireless network devices such as access points, laptops, PEDs, and wireless peripherals (keyboards, pointers, etc.) that use a wireless network protocol such as Bluetooth, 802.11, or proprietary protocols must be documented in the SSP.
2. A general statement in the SSP permitting the various types of wireless network devices used by the site is acceptable rather than a by-model listing (e.g., a statement that “wireless devices of various models are permitted but only when configured in accordance with the Wireless STIG or other such specified restriction”).

Mark as a finding if a DAA approved SSP does not exist or if it is not updated.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR0072 Wireless network devices must be physically protected

VMS Vulnerability Key: V0014894

Long Name: The NSO will ensure all network devices such as Intrusion Detection System (IDS), routers, servers, Remote Access System (RAS), firewalls, WLAN access points, etc. are located in a secure room with limited access or otherwise secured to prevent tampering or theft.

Severity: CAT II

Checks: The NSO will ensure all network devices such as, Intrusion Detection System (IDS), routers, servers, Remote Access System (RAS), firewalls, WLAN access points, etc. are located in a secure room with limited access or otherwise secured to prevent tampering or theft.

Hint: For BlackBerry, this check is for the BlackBerry Enterprise Server.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR0076 Require signed user agreement

VMS Vulnerability Key: V0013982

Long Name: For mobile and remote users of the DoD enclave and resources, the IAM will develop a written security policy or checklist for secure wireless remote access to the site and an agreement between the site and remote user. These documents will include relevant security requirements, including (but not limited to) the following.

The agreement will contain the type of access required by the user (privileged, end-user, etc.).

The agreement will contain the responsibilities, liabilities, and security measures (e.g., malicious code detection training) involved in the use of the wireless remote access device. Incident handling and reporting procedures will be identified along with a designated point of contact.

The remote user can be held responsible for damage caused to a Government system or data through negligence or a willful act.

The policy will contain general security requirements and practices and are acknowledged and signed by the remote user.

If classified devices are used for remote access from an alternative work site, the remote user will adhere to DoD policy in regard to facility clearances, protection, storage, distributing, etc.

Government owned hardware and software is used for official duties only. The employee is the only individual authorized to use this equipment.

DoD CIO Memorandum "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," dated 9 May 2008 requires the following additional information in all User Agreements:

***STANDARD MANDATORY NOTICE AND CONSENT PROVISION
FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS***

***By signing this document, you acknowledge and consent that when you access
Department of Defense (DoD) information systems:***

You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

You consent to the following conditions:

- The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the U.S. Government may inspect and seize data stored on this information system.

- Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
- This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
- Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
 - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
 - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
 - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
 - Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
 - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
 - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (Le., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
- All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

Severity: CAT III

Checks:

1. Inspect a copy of the site's user agreement.
2. Verify user agreement has the minimum elements described in the STIG policy.
3. User agreements are particularly important for mobile and remote users since there is a high risk of loss, theft, or compromise thus, this signed agreement is a good best practice to help ensure the site is making the user is aware of the risks and proper procedures.

Mark as a finding if site user agreements do not exist or are not compliant with the minimum requirements.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR0180 Wireless devices allowed into SCIFs must be DCID compliant

VMS Vulnerability Key: V0012072

Long Name: The IAO will ensure wireless devices are not permitted in a permanent, temporary, or mobile SCIFs unless approved in accordance with Director Central Intelligence Directive (DCID) 6/9 or 6/3.

Severity: CAT I

Checks: Work with the traditional reviewer or interview the IAO or SM.

1. Determine if site SCIF security policy/procedures allow users to bring wireless PEDs into SCIFs.
2. If No, determine if procedures are in place to prevent users from bringing PEDs into SCIFs and users are trained on this requirement. Posted signs are also evidence of compliance.
3. If Yes,
 - b. Determine if site has written procedures that describe what type of PEDs and under what type of conditions (e.g., turned off, SCIF mode enabled)
 - c. If PED devices are allowed, then users should receive proper training on the handling of these devices in a SCIF.
4. Mark this as a finding if:
 - d. Required procedures or training policies are not in place or
 - e. Required user training has not been documented.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR0225 CTTA coordination and proper separation required

VMS Vulnerability Key: V0012106

Long Name: The IAO will ensure wireless devices are not operated in areas where classified information is electronically stored, processed, or transmitted unless:

- Approved by the DAA in consultation with the Certified TEMPEST Technical Authority (CTTA).
- The wireless equipment is separated from the classified data equipment the distance determined by the CTTA and appropriate countermeasures, as determined by the CTTA, are implemented.

Severity: CAT II

Checks: Review documentation. Work with the traditional security reviewer to verify the following.

1. If classified information is not processed at this site, or site has a written procedure prohibiting the use of wireless devices in areas where classified data processing occurs, then mark as not a finding.
2. Ask for documentation showing the CTTA was consulted about operation and placement of wireless devices. Acceptable proof would be coordination signature or initials of the CTTA on the architecture diagram. IAW DoD policy, the CTTA must have a written separation policy for each classified area.
3. Review written policies, training material, or user agreements to see if wireless usage in these areas is addressed.
4. Verify proper procedures for wireless device use in classified areas is addressed in training program.
5. Mark as a finding if any of the following is found.
 - o CTTA has not designated a separation distance in writing
 - o DAA has not coordinated with the CTTA
 - o Users are not trained or made aware (using signage or user agreement) of procedures wireless device usage in and around classified processing areas.

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

2.2 System Security Requirements

The following requirements apply to BlackBerry system components.

WIR0012 Display required DoD logon banner on PDA / Smartphone

VMS Vulnerability Key: V0015399

Long Name: The IAO will ensure all PDAs and Smartphones display the following banner during device unlock/logon: "I've read & consent to terms in IS user agreement."

Severity: CAT III

Checks: Work with the SA to review the configuration of the PDA security management server or security policy configured on the PDA.

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR0371 PDAs/Smartphones with cameras must be approved

VMS Vulnerability Key: V0004840

Long Name: The IAO will ensure PDAs and Smartphones with digital cameras (still and video) are allowed in a DoD facility only if specifically approved by site physical security policies.

Severity: CAT III

Checks: Work with traditional reviewer to review site's physical security policy.

- Verify that it addresses PDA devices with embedded cameras.
- Mark this as a finding if there is no written physical security policy outlining whether wireless phones with cameras are permitted or prohibited on or in this DoD facility.

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR0372 PDAs and Smartphones with cameras not allowed in classified areas

VMS Vulnerability Key: V0012165

Long Name: The IAO will ensure PDAs or Smartphones with digital cameras (still and video) are not allowed in any SCIF or other area where classified documents or information is stored, transmitted, or processed.

Severity: CAT I

Checks: Work with the traditional reviewer to interview the Security Manager.

1. Review site's physical security policy.
2. Verify that users are informed of this policy by reviewing user agreement, posted signs, or training material.
3. Powering off, removal of batteries, or blocking IR ports is not acceptable for disabling camera functionality, as this method has not been tested for efficacy.

Mark as a finding if a written policy and user training does not prohibit these devices in classified areas. (Note that training requirements are verified in WIR1050 check.)

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1010 Establish CMI procedures for wireless email devices

VMS Vulnerability Key: V0015605

Long Name: The IAO will ensure that if a Classified Message Incident (CMI) occurs on a wireless email device or system the following actions are completed:

- In accordance with DoD policy, all components must establish Incident Handling and Response procedures. A Classified Message Incident (CMI) or “data spill” occurs when a classified email is inadvertently sent on an unclassified network and received on a wireless email device. BlackBerry devices are not authorized for processing classified data.
- The BlackBerry Enterprise Server (BES) and Microsoft Exchange server are handled as classified systems until they are sanitized according to appropriate procedures.
- The BlackBerry handheld is handled as a classified device and must be destroyed according to DoD guidance for destroying classified equipment. Currently, there is no reliable method for sanitizing BlackBerry handhelds after a CMI.

Severity: CAT II

Checks:

1. Interview the IAO.
2. Verify classified incident handling, response, and reporting procedures are documented in site BlackBerry procedures or security policies.

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1015 Establish disposal procedures for wireless email devices

VMS Vulnerability Key: V0014938

Long Name: The IAO will ensure that prior to disposing of a BlackBerry handheld device, for example, if the BlackBerry is transferred to another DoD or other government agency, the procedures found in Appendix B will be followed.

Severity: CAT III

Checks: Interview the IAO. Verify proper procedures are being followed and the procedures are documented.

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1020 Do not use wireless email for classified messages

VMS Vulnerability Key: V0014016

Long Name: The IAO will ensure BlackBerry devices and systems are not used to send, receive, store, or process classified messages.

Severity: CAT I

Checks: Interview the IAO.

Verify written policy and training material exists (or requirement is listed on signed user agreement) that states that wireless devices (or specifically BlackBerry devices) must not be used to transmit classified information. (Note that training requirements are verified in WIR1050 check.)

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1030 Scan BlackBerry devices using the AutoBerry tool

VMS Vulnerability Key: V0016340

Long Name: The IAO will ensure that all site managed BlackBerry devices are scanned with the DoD AutoBerry tool using the following schedule:

- Scan immediately after BlackBerry is provisioned or reprovisioned (this is the “control” or “baseline” scan).
- Scan before and after BlackBerry user travels OCONUS (if BlackBerry user is based within CONUS) and perform a comparison of the two scans.
- Scan at least every 90 days if BlackBerry user is based OCONUS and compare current scan results to the previous scan.
- BlackBerry devices of executives, senior managers, and staff in sensitive positions should be scanned at least every 90 days and results from the current scan compared to the previous scan. Commanders, DAAs, or IAOs will designate BlackBerry users who meet this criteria.
- All other BlackBerry devices should be scanned at least once every 6 months and results from the current scan compared to the previous scan.

The following requirements also apply:

- The results of all AutoBerry scans will be maintained by either the site BlackBerry administrator or IAO.
- AutoBerry scans can be conducted by either the site BlackBerry administrator or by each BlackBerry user. If conducted by the BlackBerry user, the results and mitigation actions reported by the tool will be provided to the site IAO or BlackBerry administrator.
- The IAO will verify that mitigation actions recommended by the AutoBerry tool after a scan (e.g. wipe BlackBerry) are completed by the BlackBerry administrator or user.
- The site IAM should designate the length of time that a site maintain the results of individual BlackBerry scans (at least 1 year is recommended). Control or Baseline scans should be maintained until a BlackBerry device is decommissioned.

Severity: CAT II

Checks: Interview the IAO and BlackBerry Administrator.

- Determine if the site is conducting required control or baseline scans and is saving the results of the scans.
- Determine if the site has any executives, senior managers, and staff in sensitive positions. If yes, determine if AutoBerry scans are conducted as required on BlackBerry devices of these users and the scan results are maintained by the site IAO or BlackBerry administrator.
- If the site is located CONUS, determine if the site has BlackBerry users that travel OCONUS. If yes, determine if AutoBerry scans are conducted as required on BlackBerry devices of these users and the scan results are maintained by the site IAO or BlackBerry administrator.

- If the site is located CONUS, determine if AutoBerry scans are conducted at least every 6 months on site BlackBerry devices and the scan results are maintained by the site IAO or BlackBerry administrator.
- If the site is located OCONUS, determine if AutoBerry scans are conducted at least every 90 days on site BlackBerry devices and the scan results are maintained by the site IAO or BlackBerry administrator.
- Determine if AutoBerry recommended mitigation actions are completed on site BlackBerry devices. The IAO or BlackBerry administrator should be saving records of scan results and mitigation actions.
- Mark as a finding if any requirements are not being met by the site.

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1040 Do not connect BlackBerry servers to classified DoD networks

VMS Vulnerability Key: V0011832

Long Name: The IAO will ensure that the BlackBerry Enterprise Server (BES) is not connected to classified DoD networks or information systems.

Severity: CAT I

Checks:

If possible, work with the traditional security reviewer to determine compliance. Verify the BES is connected to an unclassified network.

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1050 BlackBerry users must receive required training

VMS Vulnerability Key: V0016735

Long Name: The IAO and site BlackBerry system administrator will ensure that all BlackBerry users receive training on the following topics before they are issued a BlackBerry device:

- Requirement that personally owned PEDs are not used to transmit, receive, store, or process DoD information unless approved by the DAA and the owner signs forfeiture agreement in case of a security incident. See WIR0011 for additional information.
- Procedures for wireless device usage in and around classified processing areas. (WIR0180 and WIR0225)
- Requirement that PEDs with digital cameras (still and video) are not allowed in any SCIF or other area where classified documents or information is stored, transmitted, or processed. (WIR0372)
- Procedures when a CMI occurs. (WIR1010)
- Requirement that wireless two-way email devices and systems are not used to send, receive, store, or process classified messages. (WIR1020)
- Procedures for conducting and AutoBerry scan and requirements to report the results of the scan to site IAO or BlackBerry administrator and to complete mitigation actions recommended by the tool after the scan. (WIR1030)
- Requirement that that BlackBerry devices and systems are not connected to classified DoD networks or information systems. (WIR1040)
- Requirement that a user immediately notify appropriate site contacts (e.g. IAO, BES administrator, supervisor, etc.) when their BlackBerry has been lost or stolen. (WIR1090)
- If the use of the BlackBerry Keeper is approved by the DAA, users are trained on password configuration and change requirements. (WIR1110)
 - Passwords must be changed at least every 90 days.
- Bluetooth Smart Card Reader usage and security issues. (WIR1150)
 - Secure pairing procedures.
 - Perform secure pairing immediately after the SCR is reset.
 - Select a strong reader connection password (during initial pairing of the SCR with a BlackBerry, the user is required to select a connection password). Select at least an eight character password.
 - Accept only Bluetooth connection requests from devices they control.
 - Monitor Bluetooth connection requests and activity in order to detect possible attacks and unauthorized activity.
 - When SCR is used with PC, users with PC administrative rights will not disable the RIM Bluetooth Lockdown tool on the PC.
- Procedures on how to sign emergency and critical email notifications. (WIR1200)
- If SMS or test messaging is approved by the DAA, IA awareness training material should include SMS/MMS security issues. (WIR1220)

When BlackBerry Wi-Fi Service is authorized for use, the following training will be completed (WIR1230):

- Procedures for setting up a secure Wi-Fi connection.

- Approved connection options (e.g. enterprise, home)
- Requirements for home Wi-Fi connections.

When group or team BlackBerrys are used, the following training will be completed by all team BlackBerry users (WIR1250):

- BlackBerry device configuration procedures when transferring a BlackBerry to a new team member.

Note: Listing training requirements in the User Agreement is an acceptable procedure for informing/training users on many of the required training topics.

Severity: CAT III

Checks:

- Review site BlackBerry training material to see if it contains the required content.

Note: Some training content may be listed in the User Agreement signed by the user.

- Verify that site training records show that BlackBerry users received required training and training occurred before the user was issued a BlackBerry. Check training records for approximately 5 users, picked at random.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1070 Use only BES email solution

VMS Vulnerability Key: V0014021

Long Name: The IAO will ensure only the BlackBerry Enterprise Server (BES) email solution (version 4.0.0.4 (version 4.0 with Service Pack 2) or later) is used. The BlackBerry Desktop Redirector, BlackBerry Connect, and BlackBerry Professional Services Software are not authorized for use.

Note: The purpose of this requirement is to ensure a STIG compliant IT policy is enforced on all DoD BlackBerry devices. This requirement applies to the DoD email (primary) email account received on the BlackBerry device. All DoD BlackBerry devices must be managed via an STIG compliant IT policy pushed from a BES.

DAAAs may authorize users to connect BlackBerry devices to additional, secondary email accounts (e.g. Verizon email) based on mission needs. Use IT Policy rule **Allow Other Message Services, Service Exclusivity policy group** to control connections to secondary email accounts.

Severity: CAT I

Checks: Interview IAO and BlackBerry system administrator.

- Verify that the BES is part of the site's BlackBerry architecture and the site uses BES version 4.0.0.4 or later. From the BlackBerry Manager applet, select Help to view the version number.
- Determine if the site authorizes users to connect BlackBerry devices to additional, secondary email accounts (e.g. Verizon email) based on mission needs. If yes, verify that the DAA has approved this service. Ask to see documentation of DAA approval.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1080 Install BES using approved architecture

VMS Vulnerability Key: V0014022

Long Name: The IAO will ensure that the Wireless Email system is set up with the required system components and software installed on the handheld device.

- The BES is installed and configured using either the architecture shown in Figure 2.1 (non-segmented architecture) or alternate segmented architecture shown in Figure 2-2.
- The BES and all other systems providing BlackBerry services (e.g., email server and LDAP server) are protected behind a corporate firewall.
- The BES has a host based firewall (e.g., McAfee Personal Firewall, Norton Personal Firewall) and/or dedicated hardware firewall (e.g., Cisco, Netscreen) with the following required statements or rules.
 - Internal traffic from the BES is limited to internal systems used to host the BlackBerry services (e.g., email and LDAP servers) and DAA approved back-office application and content servers. Communications with other services, clients, and/or servers are not authorized.
 - Internet traffic from the BES is limited to only those specified BlackBerry services (e.g., BlackBerry SRP server, OCSP, SSL/TLS, HTTP, and LDAP). All outbound connections are initiated by the BlackBerry system and/or service.
 - Firewall settings listed in Section 3.13 of the BlackBerry Security Checklist will be implemented, including blocking connections to web proxy servers and back-office application and content servers unless the server IP address is on the firewall list of trust IP addresses and subnets.

Severity: CAT I

Checks: Interview the IAO and system administrator and review system network diagrams.

Verify that logical connectivity complies with the requirements of one of the approved architectures (the drawings in Figure 2.1 or Figure 2.2 (of the BlackBerry Security Checklist) show example architectures).

Verify the firewall configuration meets approved architecture configuration requirements (or have the network reviewer do the review of the firewall). Use Table 3-7 in the BlackBerry Security Checklist when using the non-segmented architecture and Tables 3-8 and 3-9 when using the segmented architecture for required firewall rules.

Verify that the firewall is configured to block connections to internal servers unless the server IP address is included on the list of trusted networks. IP addresses of the enclave web proxy server and authorized back-office application and content servers that the BES connects to should be included on this list. Mark as a finding if a list of trusted networks by IP address is not configured on the BES host-based firewall.

Mark as a finding if a BES is not used. Mark as a finding if the BES is used but the required firewalls and communication flow is not configured in accordance with the architecture.

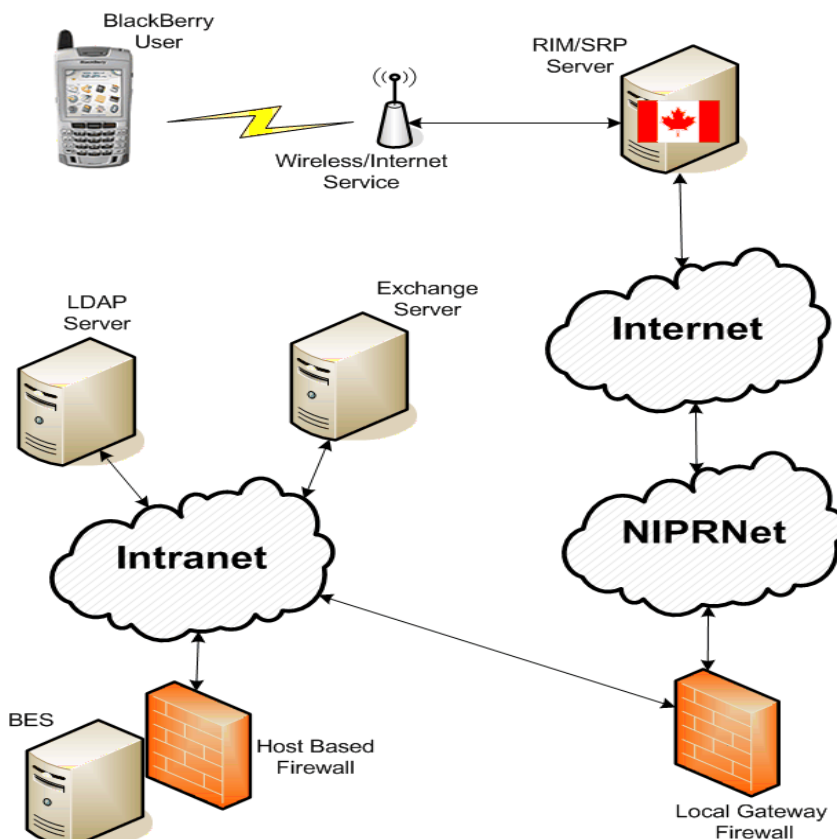


Figure 2-1. Example BlackBerry Network Architecture

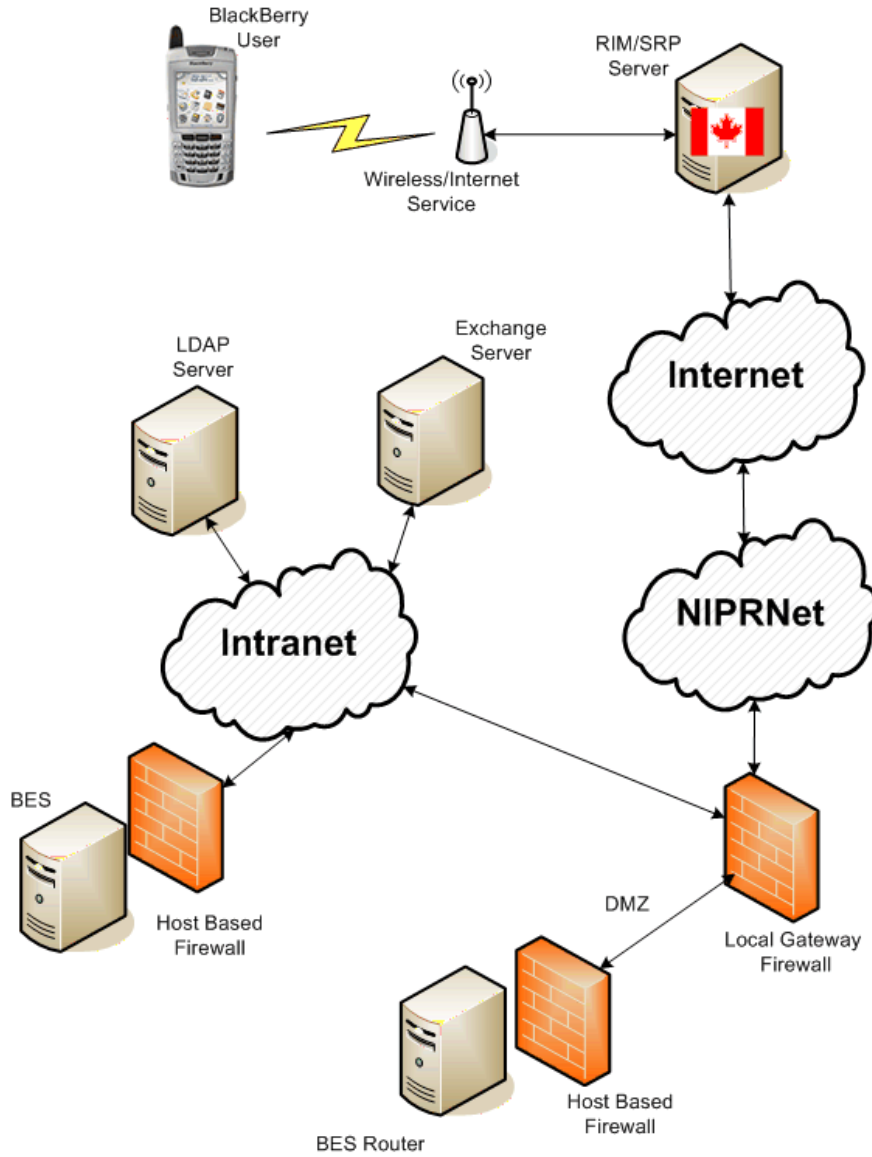


Figure 2-2. Segmented BlackBerry Network Architecture

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1090 Required actions if wireless email handheld is lost or stolen

VMS Vulnerability Key: V0003544

Long Name: The IAO will ensure the wireless email system administrator sends a “Wipe” or “Kill” command to the device and removes the device from the wireless email management server, when a wireless email device is reported lost or stolen.

If a wireless email device is lost or stolen, the device must be immediately disabled to prevent unauthorized use or access. Once the device is deemed unrecoverable, the device should be permanently removed from the server and SA should contact the service provider to cancel the service.

In addition, BlackBerry users should be trained to immediately notify appropriate site contacts (e.g., IAO, BES administrator, supervisor, etc.) when their BlackBerry has been lost or stolen.

Severity: CAT III

Checks: Interview the IAO. Review written policies. Verify that proper procedures are followed when devices are lost or stolen. (Note that training requirements are verified in WIR1050 check.)

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1100 Authenticated login procedures to unlock a wireless email device

VMS Vulnerability Key: V0003545

Long Name: The IAO will ensure BlackBerry devices are protected by authenticated login procedures to unlock the device. Either CAC or Password authentication is required.

When Password authentication is used, the following procedures will be enforced.

- The device password is set to five or more characters. The system security policy must be configured to enforce this policy. If five characters are used, both a letter (lower or upper case) and a number must be used in all device passwords. The wireless email server must be configured to enforce this policy. If six or more characters are used, numbers only, letters only (either lower or upper case), or a combination of numbers and letters may be used for the password. It is recommended that eight or more characters be used.
- The number of incorrect passwords entered before a device wipe occurs is set to 10 or less. The system security policy must be configured to enforce this policy.
- The password is changed at least every 90 days. The system security policy must be configured to enforce this policy.

Note: When software certificates are used on a BlackBerry device, CTO 07-15 Revision 1 requires that the password used to unlock the certificate store meet the following requirements: Password length equals 15; password complexity: at least one upper case letter, lower case letter, number, and special character must be included in the password. Software certificates are saved in the BlackBerry keystore, which has the same password as the device unlock password.

- When software certificates are used on a BlackBerry, the BlackBerry password must be set to meet the requirements of CTO 07-15 Revision 1. The following BES IT Policy rules must be set as follows:

IT Policy Group	IT Policy Rule	Required Setting
Minimum Password Length	Device-Only	15
Password Pattern Checks	Device-Only	3

When CAC authentication is used to unlock the BlackBerry, the following IT Policy rules should be configured as follows:

IT Policy Group	IT Policy Rule	Required Setting
Maximum Password Age	Device-Only	0
Minimum Password Length	Device-Only	6
Password Pattern Checks	Device-Only	0 or <blank>
Password Required	Device Only	True
Force Smart Card Two Factor Authentication	Security	True
Required Password Pattern	Security	N, n, or #

Severity: CAT I

Checks: Interview the IAO and administrator.

- Verify CAC authentication or PIN authentication is used.
- Determine if software certificates are used on the BlackBerry to sign and encrypt email or for WiFi network authentication.
- If Password authentication is used, verify correct settings.
- If software certificates are used, verify correct IT policy rule settings.

These policies are given in Appendices B and are reviewed as part of check WIR1250. The reviewer should lower to a CAT II **if no** configuration settings designated as CAT I **remain in an Open status**. The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status**.

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1110 Password Keeper configuration must be compliant

VMS Vulnerability Key: V0011865

Long Name: The IAO will ensure that when the Password Keeper is enabled on the BlackBerry device, the DAA has reviewed and approved its use, and the application is configured to enforce the following password rules.

Require use of eight or more characters. The Password Keeper must be configured to enforce this policy.

Set the number of incorrect passwords entered before a device wipe occurs to 10 or less. The Password Keeper must be configured to enforce this policy.

Set local policy to require a change of password at least every 90 days.

Severity: CAT III

Checks: Interview the IAO.

1. Ask if users are allowed to use Password Keeper on their handheld devices. If Password Keeper is used, review the DAA approval documentation regarding this.
2. Work with the IAO to view the Password Keeper configuration on a sampling of BlackBerry devices using this application. On BlackBerry, go to Applications/Password Keeper. The Password Keeper icon may also be installed directly on the BlackBerry home screen. Verify the following Password Keeper setting (have user log into Password Keeper, then click menu and select **Options**)
 - Verify **Random Password Length** is set to 8 or more.
 - Verify **Password Attempts** is set to 10 or less.
3. Verify that users are trained on password change requirement (90 days or less) by reviewing user agreement or training materials. (Note that training requirements are verified in WIR1050 check.)

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1130 Control of BlackBerry applications (Part I)

VMS Vulnerability Key: V0007078

Long Name: The IAO will ensure that the following application security controls are implemented on the site BlackBerry system (BES and BlackBerry devices):

- If non-baseline BlackBerry applications are used on site BlackBerry devices, the DAA has approved the use of these applications.

Note: see section 3.3.1 of the BlackBerry Security Checklist for a definition and list of “Baseline” BlackBerry applications. Essentially, baseline BlackBerry applications are applications found on almost all BlackBerry devices after initial provisioning. Baseline applications do not require application control policies.

- The site does not allow BlackBerry users to access and download applications directly from application repositories located on a network drive. Applications will be installed on BlackBerry devices only under direct control of the BlackBerry administrator during initial provisioning of the BlackBerry or by using software configurations.
- The BES has been set up to require BlackBerry users to authenticate directly with enclave application and content servers.

Note: This configuration setting should be implemented for all DoD BES installations, including sites that have not deployed enclave application and content servers for BlackBerry systems.

- If the BlackBerry MDS Integration Service is installed on the BES (to manage connections to BlackBerry MDS Runtime applications), a default BlackBerry MDS Integration Service device policy will be configured on the BES.
- The BES is configured to prohibit users from downloading unsigned BlackBerry MDS Runtime applications.
- The BES must be configured to require trusted connections to enclave application or web push servers. Push servers are set up to push content to BlackBerry users, (e.g., Remedy Ticket notification system).

Severity: CAT II

Checks: Perform the following checks:

- 1) Determine if there are non-baseline BlackBerry applications installed on site BlackBerry devices by performing the following (review a sample of 2-3 site BlackBerrys):
 - a) Look at what applications installed on the BlackBerry desktop.
 - b) Look at what applications installed in the BlackBerry **Applications** folder.
 - c) Look at the list of applications found at

Settings>Options>Advanced Options>Applications

- d) Make a list of non-baseline BlackBerry applications found on site BlackBerry devices. Compare the name of each application found on the BlackBerry to the list of baseline BlackBerry applications found at the end of Section 3.3.1 in the BlackBerry Security Checklist. If a found application is not on the list of baseline BlackBerry applications, it is a non-baseline application. Make a list of all non-baseline applications found on site BlackBerry devices.
- 2) Verify DAA has approved the use of all non-baseline applications found on site BlackBerry devices. Approval can be in a memo, documented in the SSAA/SSP, or other documentation. Mark as a finding if non-baseline applications are found that are not on the list of applications approved by the DAA.
- 3) Verify the site does not allow users to download applications to their BlackBerry from an application repository. Interview the IAO and BlackBerry administrator and determine if a site application repository has been set up at the site. Mark as a finding if an application repository is used (CAT III).
- 4) Check to see if the BlackBerry MDS Integration Service is installed on the BES (to manage connections to BlackBerry MDS Runtime applications) by looking at the left pane in the BlackBerry Manager. Ask the BlackBerry SA to show that the BlackBerry MDS Integration Service is or is not installed. If the BlackBerry MDS Integration Service **is installed**, perform the following checks:
 - a) Verify that each BES User Group has been assigned a BlackBerry MDS Integration Service device policy:
 - i) In the BlackBerry Manager, click on one of the user groups listed in the left pane
 - ii) Click on the **Group Configuration** tab at the top of the screen.
 - iii) Click on the **MDS Integration Service** and write down the name of the BlackBerry MDS Integration Service device policy assigned to that BES User Group
 - iv) Complete the previous steps for all user groups
 - v) Mark as a finding if any BES User Group is not assigned a BlackBerry MDS Integration Service device policy
 - b) Verify that a **BlackBerry MDS Integration Service** device policy assigned to each BES User Group has been configured correctly:
 - i) In the BlackBerry Manager, in the left pane, click on the **BlackBerry MDS Integration Service**
 - ii) On the **MDS Integration Services** tab, click **Edit Properties**
 - iii) Click **Devices Policies**
 - iv) Select a device policy that has been assigned to a BES User Group and verify the policy has been configured as shown in Table C-6 of the BlackBerry Security Checklist. Mark as a finding (CAT III) if the device policy has not been configured correctly.
 - v) Repeat the previous steps for all device policies.

- c) Verify the BES is configured to not allow users to install unsigned BlackBerry Integration Service applications, using the following procedure:
 - i) In the BlackBerry Manager, in the left pane, click on the BlackBerry MDS Integration Service
 - ii) On the MDS Integration Services tab, click Edit Properties
 - iii) In the left pane click **General**
 - iv) Click **Allow Unsigned Applications**
 - v) Verify the configuration setting is **False**
 - d) Mark as a finding (CAT III) if the setting is not set as required
- 5) Verify that the site has configured the BES to require trusted connections to Push enclave application or web servers, using the following procedure:
- a) In the BlackBerry Manager, click the BlackBerry MDS Connection Service in the left pane
 - b) On the **Connection Service** tab, click **Edit Properties**
 - c) Click **TLS/HTTPS**
 - d) Verify **Allow Untrusted HTTPS Connections** is set to **False**
 - e) Verify **Allow Untrusted TLS Connections** is set to **False**
 - f) Mark as a finding (CAT III) if any of these settings are not correct
 - g) Verify a keystore file has been set up (webserver.keystore) at the following location on the BES: <drive>:\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\webserver. Look for the keystore file.
 - h) Mark as a finding (CAT III) if the keystore file is not found.

The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status.**

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1131 Control of BlackBerry applications (Part II)

VMS Vulnerability Key: V0016341

Long Name: The IAO will ensure that an application white list has been configured on the BES to control all non-baseline applications installed on site BlackBerry devices.

Severity: CAT III

Checks: Perform the following checks:

Check the BES to see if an application control White List has been configured on the BES. Do the following checks:

- 1) Review each BES User Group and make a list of the software configuration assigned to each group:
 - a) In the BlackBerry Manager, click on one of the user groups listed in the left pane
 - b) Click on the **Group Configuration** tab at the top of the screen.
 - c) Write down the name of the software configuration listed as the **Group Configuration Name**
 - d) Complete the previous steps for all user groups
 - e) Mark as a finding if any BES User Group is not assigned a software configuration.
- 2) For each software configuration assigned to each BES User Group, do the following checks:
 - a) In the BlackBerry Manager, click **BlackBerry Domain** in the left pane
 - b) Click **Software Configurations** tab
 - c) In the **Configuration Name** list, double click on one of the software configurations that was assigned to a BES User Group.
 - d) Expand the Application Software tree
 - e) Write down the name of the Application Control Policy that has been assigned to the **Application Software** group. It will be listed in the **Policy** column to the right of the **Delivery** column.
 - f) Write down the name of the Application Control Policy that has been assigned to each application listed in the **Application Software** group. It will be listed in the **Policy** column to the right of the **Delivery** column for each application.
 - g) Mark as a finding if an application control policy has not been assigned to the **Application Software** group or to each application listed in the **Application Software** group.
- 3) Repeat the following steps for each software configuration assigned to each BES User Group.
 - a) For each application control policy assigned to the **Application Software** group of each software configuration, check to see that the application control policy has been configured exactly as shown in Figure 3-2 of the BlackBerry Security Checklist. This is a **Deny All** application control policy. Mark as a finding if one or more of the application control policies reviewed in this step are not configured as required.
 - b) For each application control policy assigned to each application listed in the **Application Software** group of each software configuration, if the application is a non-baseline

application and **has not been approved by the DAA**, the **Deny All** application control policy must be assigned to the application. Mark as a finding if the non-DAA approved applications listed in a software configuration do not have the **Deny All** application control policy assigned to them.

- c) For each application control policy assigned to each application listed in the **Application Software** group of each software configuration, if the application is a non-baseline application and **has been approved by the DAA**, check to see that the application control policy has been configured as specified in Table C-5 of the BlackBerry Security Checklist. Mark as a finding if one or more of the application control policies reviewed in this step are not configured as required.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1132 Control of BlackBerry applications (Part III)

VMS Vulnerability Key: V0016343

Long Name: The IAO will ensure that if the site provides BlackBerry users access to “back-office” applications and content servers located on the site network enclave, the following controls will be implemented:

- All enclave application and content servers that are accessed by BlackBerry users will implement CAC authentication.
- The BES host-based firewall is set to block connections to back-office application and content servers unless the server IP address is on the firewall list of trust IP addresses and subnets.

Note: BlackBerry back-office application and content servers include J2ME application servers, SOAP web services, and web servers.

Severity: CAT II

Checks: Ask The BlackBerry SA if the site provides BlackBerry users access to “back-office” applications and content servers located on the site network enclave. If the response is “Yes” ask for a list of all enclave servers BlackBerry users can access and then perform the following checks:

- Verify CAC authentication has been implemented on each server. Have the Windows reviewer assist with the review of each server. Mark as a finding if CAC authentication has not been implemented on each server.
- Verify the BES host based firewall has been configured as required. This check should have been performed during the review of check WIR1080. Confirm this requirement was reviewed.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1140 Bluetooth usage must be compliant

VMS Vulnerability Key: V0014198

Long Name: The IAO will ensure a wireless email device, which has a Bluetooth radio, applies the following Bluetooth controls.

- Bluetooth data transmissions, such as syncing to the desktop or transfer of data files, on wireless email devices are disabled except for the Bluetooth CAC reader (i.e., Bluetooth Smart Card Reader (SCR)). Only DISA tested and approved Bluetooth SCRs may be used (listed in WIR1150).
- Bluetooth for voice transmissions, such as the Bluetooth ear bud, is not authorized. Both the Bluetooth Handsfree and Headset profiles must be disabled. Users should use wired hands-free devices.

Severity: CAT II

Checks:

Reviewed as part of WIR1250 check.

The reviewer must raise this to a CAT I finding if **any** configuration setting designated as CAT I **remains in an Open status**. The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status**.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1150 Bluetooth Smart Card Reader usage must be compliant

VMS Vulnerability Key: V0011866

Long Name: The IAO will ensure that when RIM Bluetooth Smart Card Readers (SCR) or the Apriva Bluetooth SCR is used in the organization, the following procedures will be followed.

1. BlackBerry Handheld Software version 4.1.0.294 or later is used on all BlackBerry devices.
2. Only the RIM Bluetooth SCR or the Apriva BT100-C or BT200 Bluetooth SCRs are used with RIM BlackBerry devices. Bluetooth SCRs from other manufacturers have not undergone a DoD security evaluation with BlackBerrys and are not approved by DISA. The SCR is not used with PCs, cell phones, PDAs, or non-RIM PDAs with BlackBerry software installed (BlackBerry Connect).
3. When the RIM Bluetooth SCR is used as a PC SCR, the requirements listed in Section 3.18 of the Wireless STIG BlackBerry Security Checklist must be followed. Apriva Bluetooth SCRs are not approved for use with DoD PCs.
 - The DAA must approve the use of a Bluetooth smart card reader with command/site PCs.
 - Required version of BlackBerry Smart Card Reader software application installed on the PCs is v4.2.0.95 or later.
 - Required version of SCR drivers installed on the SCR is **PLATFORM** 1.5.0.81 or later and **APPS** is version 4.2.0.95 or later. Earlier versions will not be used for PC connections.
 - **Note:** BlackBerry Smart card reader software version 1.5.1 Hot Fix #2, Package Version 4.2.0.31 contains all required versions of SCR software for the PC and SCR.
 - Separate BlackBerry Account Groups should be created: one for users that are authorized to use the RIM BlackBerry Smart Card Reader with their PCs and one for users that are NOT authorized to use the RIM BlackBerry Smart Card Reader with their PCs (or do not have a RIM BlackBerry Smart Card Reader).
 - At the time of the publication of this document, the use of the BlackBerry Smart Card Reader for authentication with PCs is only authorized with PCs that have Microsoft Windows XP. The Microsoft Vista Bluetooth stack has not yet been tested with the BlackBerry Smart Card Reader to determine if Bluetooth device pairing can be done in a secure manner and meets DoD security requirements.
 - Bluetooth radios installed in site PCs must be Class 2 or 3. Class 1 (100 mW) Bluetooth radios are not allowed.

Note for IAOs: To determine the “class” rating of the Bluetooth radio, look under the specification section of the Bluetooth Network Interface Card manual, which can be downloaded from the laptop vendor’s web site or the Bluetooth dongle vendor’s web site. Nearly all internal laptop Bluetooth radios are Class 2 or 3 and many Bluetooth dongle radios are Class 1.

4. Separate BlackBerry account groups are set up for users of the SCR and for users that do not use the SCR. The IT Policy rules for the Bluetooth group policy will be set as indicated in Table C-1 for each BlackBerry account group.
5. The Bluetooth device property **Trusted** field should be set to “Ask.” This is the default value. This property is set on the BlackBerry device in the Bluetooth Device Properties immediately after the Bluetooth pairing connection alert.
6. Users are trained how to perform the following (checked in WIR1050):
 - Perform secure pairing immediately after the SCR is reset.
 - Select a strong reader connection password (during initial pairing of the SCR with a BlackBerry, the user is required to select a connection password). Select at least an eight character password.
 - Accept only Bluetooth connection requests from devices they control.
 - Monitor Bluetooth connection requests and activity in order to detect possible attacks and unauthorized activity.

Severity: CAT III

Checks: Interview the IAO and wireless email system administrator.

1. Verify that the BlackBerry SA places users with or without card readers in separate BlackBerry account groups.
 - In BlackBerry Manager, select **BlackBerry Domain** in the left pane.
 - Select **User Group List** tab.
 - Check **Group Description** and have BES Admin shows required user groups.
2. Verify the Bluetooth device property **Trusted** field should be set to “Ask.” To check (or change), do the following: On the BlackBerry, Select Options/Bluetooth/Smart Card Reader/Device Properties.
3. Verify that if the RIM BlackBerry Smart Card Reader is used as a PC SCR the following requirements are met:
 - The DAA has approved the use of the RIM BlackBerry Smart Card Reader with site PCs. Have the IAO provide documentation showing DAA approval (letter, memo, SSP, etc.)
 - Verify the correct version of BlackBerry SCR software (v4.2.0.95 or later) has been installed on a sample of PC at the site (3 or more PCs should be checked).
 - On the PC, go to **Start>Control Panel>Add or Remove Programs>Select BlackBerry Smart Card Reader v1.5.1** and click the **Click here for support information** link. Verify that the **Version:** field says **4.2.0.95 (Platform 1.5.0.81)** or later.

- Verify the RIM Bluetooth Lockdown tool is installed and configured correctly:
 - On the PC, go to **Start>Control Panel>Add or Remove Programs>** Select **BlackBerry Smart Card Reader v1.5.1** and click the **Change/Remove** button.
 - In the first pop-up dialog box click **Next** button.
 - In the next dialog box verify that **Modify** is selected and click the **Next** button.
 - In the next dialog box click the **Next** button.
 - In the next dialog box (**Restrict Bluetooth Functionality**), verify that the checkbox is checked. Click the **Cancel** button and cancel installation.

- Interview the IAO and verify the site Windows group security policy is set to restrict the capability of the PC user to disable, remove, or change the configuration of the RIM Bluetooth Lockdown tool.
- Verify all PC users with administrative account rights to their PC have been trained to never disable the RIM Bluetooth Lockdown tool on their PC. PC Administrators should NEVER change any Bluetooth settings followings implementation of Bluetooth lockdown. (Note that training requirements are verified in WIR1050 check.)
- Verify separate BlackBerry Account Groups have been created: one for users that are authorized to use the RIM BlackBerry Smart Card Reader with their PCs and one for users that are NOT authorized to use the RIM BlackBerry Smart Card Reader with their PCs (or do not have a RIM BlackBerry Smart Card Reader).
 - In BlackBerry Manager, select **BlackBerry Domain** in the left pane.
 - Select **User Group List** tab.
 - Check **Group Description** and have BES Admin shows required user groups.

- Note:** Recommend 3 BlackBerry account groups be created:
 1. BlackBerry users without a smart card reader.
 2. BlackBerry users with a smart card reader, but not authorized to use the smart card reader to connect to their PC.
 3. BlackBerry users with a smart card reader and authorized to use the smart card reader to connect to their PC.

- Verify the correct version of BlackBerry SCR has been installed on a sample of SCRs:
 - On the RIM SCR, with the Bluetooth radio turned off, press and hold the **Action** button.
 - “rEsetIng” appears on the screen.
 - During the resetting sequence, the **PLATFORM** and **APPS** versions will be displayed. Verify the correct versions are installed. (1.5.0.81 or later for **PLATFORM** and 4.2.0.95 or later for **APPS**)

- Interview the IAO and SA and verify that the RIM BlackBerry SCR is not used with Windows Vista. BlackBerry users with Vista on their PCs must be put in the BlackBerry users group not authorized to use the BlackBerry SCR with their PCs.
- Interview the IAO and verify Bluetooth radios are disabled or removed in all PCs (check a sample) where users do not have a RIM BlackBerry Smart Card Reader Bluetooth radios will be disabled either by removing the radio from the PC and/or by Windows group policy.
- Interview the IAO to verify only Bluetooth Class 2 or 3 radios are used by in site PCs. Have the IAO or site BlackBerry administrator show for a sample of PCs the Bluetooth radio is not a Class 1 radio by providing a copy of the Bluetooth radio specification sheet.

4. Required BES setting are reviewed during WIR1250 check. The reviewer must raise this to a CAT II finding if **any** configuration setting designated as CAT II **remains in an Open status**.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1160 Secure wireless email servers using operating system STIG

VMS Vulnerability Key: V0014199

Long Name:

The IAO will ensure that all host servers and computers where the BlackBerry Enterprise Server (BES) are installed, are hardened in accordance with the appropriate operating system STIG.

Severity: CAT II

Checks: Work with the OS reviewer or check VMS for last review of each host BES computer asset. Verify that there are no outstanding CAT I findings associated with each host server.

Mark as a finding if CAT I findings are open for the host computer operating system or if a SRR or site self-check was not performed for the host computers.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1170 Comply with provisioning requirements for wireless email devices

VMS Vulnerability Key: V0011868

Long Name:

1. The IAO will ensure that a BlackBerry system administrator performs a “Wipe (or Nuke) Handheld” command on all new or reissued BlackBerry handheld devices and that all BlackBerry, wireless carrier, and system software is reloaded on the BlackBerry from a trusted source and the site BlackBerry IT policy is pushed to the device before issuing it to DoD personnel and placing the device on a DoD BlackBerry network.
2. When wireless activation is performed, the activation password is passed to the user in a secure manner (e.g., activation password is encrypted and emailed to an individual).

Severity: CAT III

Checks: Interview the IAO. Verify required procedures are followed.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1180 Do not allow users to install or remove applications

VMS Vulnerability Key: V0014478

Long Name: The IAO will ensure that wireless email users do not install or remove applications and/or software on their handheld device unless under the direction and supervision of an authorized BlackBerry system administrator.

Severity: CAT I

Checks:

- IT Policy rules set in the BES. Reviewed as part of WIR1250 check. The reviewer should lower to a CAT II **if only** configuration settings designated as CAT II **remain in an Open status** and all other requirements in this check are met.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1190 Do not install Onset Technologies METAMessage software

VMS Vulnerability Key: V0011870

Long Name: The IAO will ensure Onset Technologies METAMessage software is not installed on DoD BlackBerry devices or on the BES.

Severity: CAT I

Checks:

- Check a sample of BlackBerry devices (**Settings>Options>Advanced Options>Applications**) to ensure the METAMessage application is not loaded on the BlackBerry device.
- On the BES, have the BlackBerry Administrator show that the site software configurations do not have the METAMessage application in any software configuration package.
 - o **In the BlackBerry Manager, select BlackBerry Domain** in the left pane
 - o Select the **Software Configurations** tab
 - o Select a sample of listed software configurations to check. For each, do the following;
 - Select a configuration to review
 - Click on **Edit Configuration**
 - Expand the list under **Application Software** and check to ensure METAMessage is not listed

The Metamessage application allows the user to open and create Microsoft Office files such as MS Word or Excel attachments or documents. These documents can then be sent via email, saved, or printed. This application presents a security risk and is not allowed for use in DoD. Verify this software application is not used by interviewing the IAO or reviewing a sampling of the devices.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1200 Digitally sign email emergency and/or critical email notifications

VMS Vulnerability Key: V0011871

Long Name: The IAO will ensure that all wireless email emergency and/or critical email notifications are digitally signed and verified to ensure the authenticity of the sender.

Severity: CAT III

Checks:

1. Check the BES IT policy rule for the S/MIME Application policy group (checked as part of WIR1250). The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status** and all other requirements in this check are met.
2. Verify that S/MIME is configured such that users may sign messages.
Check a sample of BlackBerry devices:
 - Verify S/MIME application and Smart Card Reader drivers are installed on the device:
 - On the BlackBerry go to **Settings>Options>Advanced Options>Applications**.
 - Look for the following applications:
 - S/MIME Support Package
 - PIV Drivers (optional)
 - BlackBerry Smart Card Reader
 - DoD Root Certificates
 - Verify Certificates are configured on the BlackBerry:
 - **Settings>Options>Security Options>Certificate Servers** – GDS and OCSP servers should be listed.
 - **Settings>Options>Security Options>Certificate** - DoD Root certificates should be listed.
 - **Settings>Options>Security Options>S/MIME** – User’s public keys should be loaded.
3. Verify that if software certificates are used on the BlackBerry device, the DAA has approved their use (letter, memo, SSP, etc.).

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1210 Configure wireless email auto signature as required

VMS Vulnerability Key: V0011872

Long Name: The IAO will ensure that if wireless email auto signatures are used, the signature message does not disclose that the email originated from a mobile device (e.g., “Sent From My Wireless Handheld”).

Severity: CAT III

Checks:

1. Note that the site can disable the use of auto signature via an IT policy rule (checked as part of WIR1250).
2. If allowed, check a sample of BlackBerry devices:
 - Open the BlackBerry email folder.
 - Highlight the date line at the top of the list of messages.
 - Click the menu button.
 - Select **Options**, then **Email Settings**.
 - Check the contents of “Auto Signature” text box to verify compliance.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1220 If Text Messaging or Instant Messaging are used, enable security

VMS Vulnerability Key: V0011873

Long Name: The IAO will ensure the following security requirements for text messaging (Short Message Service (SMS), Multi-media Messaging Service (MMS), Pin-To-Pin messaging, and other text messaging services) and Instant Messaging (IM) are followed:

- When BlackBerry Messenger (PIN-to-PIN messaging) is used S/MIME encryption must be implemented.
- When SMS is used, users are trained on security risks of SMS. (verified in WIR1050)
- MMS will not be used.
- When BlackBerry Instant Messaging is used, only connections to DoD IM servers will be allowed. The DoD IM system must meet the security requirements of the Instant Messaging STIG.

Severity: CAT III

Checks:

1. Verify S/MIME function enabled for BlackBerry Messenger (PIN-to-PIN messaging) (checked as part of WIR1250 check).
2. Verify S/MIME Support Package is installed. Check a sample of BlackBerry devices (see WIR1200, #3 for the procedure).
3. Verify MMS is not enabled on the BES (verified during WIR1250 check review).
4. Interview the IAO or BlackBerry Administrator and determine if BlackBerry Instant Messaging is used on site managed Blackberry devices. If yes, determine what server the BlackBerry Instant Messaging system connects to.
 - The server should be managed by a DoD site.
 - The IM system must be compliant with the Instant Messaging STIG. Verify that a security review has been conducted on the site IM system and recorded in VMS.
 - Mark as a finding if requirements are not met.

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

WIR1230 Setup of BlackBerry Wi-Fi security controls

VMS Vulnerability Key: V0016058

Long Name: The IAO will ensure that BlackBerry Wi-Fi¹ security controls are implemented as follows:

- If BlackBerry Wi-Fi Service is authorized for use at the site, the following conditions apply:
 - The DAA has approved the service.
 - The site SSP/SSAA shows BlackBerry Wi-Fi services as part of the site IT infrastructure and documents what connection options are approved for use: Connection to a site DoD operated wireless LAN system and/or home WLAN system. Connections to public and hotel Wi-Fi hotspots are not authorized.
 - A BlackBerry WLAN IT policy has been set up for the site on the BES and is configured as shown in Table C1 of this checklist.
 - One or more WLAN profiles have been defined and assigned to users.
 - If some BlackBerry users have been approved to use their home WLAN system to receive BlackBerry email, the following conditions apply:
 - The home WLAN system has been set up for WPA2 Personal.

Note to IAO: Home users that have Wi-Fi systems that are not capable of being configured for WPA2 Personal will not be authorized to use the home connection option.

 - BlackBerry security awareness training provided to BlackBerry users shall include information on the proper use of BlackBerry Wi-Fi Services.
 - The site BlackBerry User Agreement shall contain an acknowledgment on when and where BlackBerry Wi-Fi services can be used and user responsibilities for following security requirements.
- If BlackBerry Wi-Fi service is not authorized for use at the site, the following conditions apply: A BlackBerry WLAN IT policy has been set up for the site on the BES and is configured as shown in Table C2 of this checklist where the policy rule **Disable WLAN** is set to **TRUE**.

Severity: CAT III

Checks: Interview the IAO and determine if the site has approved the use of BlackBerry Wi-Fi Service.

- If BlackBerry Wi-Fi Service has been approved, do the following:

¹ The terms Wi-Fi, and WLAN are used interchangeably in this document. Both terms are used in RIM's BlackBerry documentation. The term "Wi-Fi" is used in this document when referencing a BlackBerry document or BlackBerry configuration setting. The term WLAN is used in the Wireless STIG and other DoD wireless documents and is also by RIM to label various wireless configuration settings in the BES.

- Verify DAA approval by reviewing an approval letter, memo, or SSP. Mark as a finding if the site uses BlackBerry Wi-Fi service but there is no evidence of DAA approval.
- Verify the BlackBerry Wi-Fi Service is listed in the site SSP. In addition, the SSP should list what connection options are approved:
 - Connection to a DoD operated WLAN system
 - Connections to home WLAN systems.
 - Connections to public or hotel hotspots Wi-Fi hotspots will not be approved.
 - Mark as a finding if the DAA has approved the BlackBerry Wi-Fi Service, but required documentation is not in the SSP.
- Verify a site WLAN IT policy has been configured on the BES. (Verified as part of WIR1250 check).
- Verify the site has set up one or more WLAN profiles and assigned those profiles users authorized to use the BlackBerry Wi-Fi Service. Each user authorized to use the BlackBerry Wi-Fi Service should be assigned a WLAN profile and the profile should be properly configured.
 - Ask the IAO or BlackBerry SA for names of site BlackBerry users that have been authorized to use BlackBerry Wi-Fi Service and verify that these users have been assigned a WLAN profile. Verify that authorized users have been assigned a WLAN profile as follows (select 2 or 3 users to check):
 - In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**
 - On the **All Users** tab, double-click the user account to which you want to verify a WLAN profile has been assigned
 - In the Properties for the user account, click **WLAN Configuration**
 - Double-click **WLAN Configuration Sets** to see if a WLAN profile has been assigned to the user account. If **Yes**, write down the name of the profile. If **No**, mark as a finding.
 - Next, determine if the assigned WLAN profile has been configured as required.
 - In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
 - On the **Global** tab, click **Edit Properties**.
 - Click **WLAN Configuration**.
 - In the **WLAN Configuration Administration** section, double-click **WLAN Configuration Sets**.
 - Double-click the profile that you want to check.
 - In the left pane, click one of the following options: **WLAN Settings** or **Associations**
 - Verify rules are set as shown in table C.3 (only rules with “Required” settings need to be verified)

- Mark as a finding if the WLAN profile has not been configured as required.
- If some BlackBerry users have been approved to use BlackBerry Wi-Fi service with their home Wi-Fi network verify the following:
 - The site has determined that cellular coverage is not available at the home of each approved home user. Ask the site IAO or BlackBerry administrator how this verification was performed. Ask to review support documentation for a sample of approved users.
 - The site has verified the home Wi-Fi system of the home user supports WPA Personal and the user has verified their system is configured for WPA Personal. Ask the site IAO or BlackBerry administrator how this verification was performed. Ask to review support documentation for a sample of approved users.
- BlackBerry security awareness training includes information on the proper use of BlackBerry Wi-Fi Services. (Note that training requirements are verified in WIR1050 check.)
- Verify the site BlackBerry User Agreement contains an acknowledgment on when and where BlackBerry Wi-Fi services can be used and user responsibilities for following security requirements.
- If BlackBerry Wi-Fi Service HAS NOT been approved, do the following:
 - Verify a site WLAN IT policy has been configured on the BES and the policy rule **Disable WLAN** is set to **TRUE**. (Verified as part of WIR1250 check).

The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status** and all other requirements in this check are met.

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1240 The wireless carrier Internet browser is disabled

VMS Vulnerability Key: V0011875

Long Name: The IAO will ensure that all Internet browsers are disabled and removed from the BlackBerry device except for the BlackBerry internet browser.

Severity: CAT III

Checks:

- Review a sampling of handheld devices and verify that the Wireless Carrier's internet browser, web portal browser, and all other browsers (Yahoo, etc.) are not installed on the BlackBerry device. The only browser installed should be the BlackBerry browser. Go to the BlackBerry device Home screen and verify only the Blackberry browser is present.

Settings>Options>Advanced Options>Browser

Verify the BlackBerry Browser is set as the default browser.

- Check that other browsers are not allowed by IT policy configuration (checked as part of WIR1250 check).

The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status** and all other requirements in this check are met.

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1250 Implement BES and BlackBerry handheld configuration settings

VMS Vulnerability Key: V0011876

Long Name: The IAOWill ensure that all required wireless email server and handheld device configuration settings are implemented.

See requirements listed in Section 3 and Appendices C, D, and G.

Severity: CAT II

Checks: Verify the BlackBerry administrator has used the configuration settings list in Section 3 and Appendix C of the *Wireless STIG, BlackBerry Security Checklist* as follows:

1. Appendix C, Table C.1 Verify all required IT policy rules have been set on the BES. Open findings should be marked against the check number listed in the table for the IT policy rule found to be in “Open” status. The IT Policy settings can be checked as follows:
 - In the BlackBerry Manager, click **BlackBerry Domain** (left pane)
 - On the **Global** tab, click **Edit Properties**.
 - Click **IT Policy**.
 - In the **IT Policy Administration** section, double click **IT Policies**.
 - Double-click an IT Policy to check.
 - Click **Properties**.
 - Select each policy group in turn, and check the setting of each rule in the policy group.
2. Appendix C, Tables C.3 and C.4. Ask the BlackBerry system administrator if the site uses WLAN and/or VPN configuration sets to configure WLAN and VPN settings on Wi-Fi enabled BlackBerry devices. If yes, verify that the WLAN and/or VPN configuration sets are set up as required in Table C.1 and C.2. The configuration sets can be viewed as follows:
 - In the BlackBerry Manager, click **BlackBerry Domain** (left pane)
 - On the **Global** tab, click **Edit Properties**.
 - Click **WLAN Configuration**.
 - In the **WLAN Configuration Administration** section, double-click **WLAN Configuration Sets** (or **VPN Configuration Sets**).
 - Double click a profile to check.
 - In the left pane, click either **WLAN Settings** or **Associations** (or **VPN Settings**) and check settings with Table C.1.
3. Appendix D, Table D.1. A sample of BlackBerry devices should be checked. Open findings should be marked against the check number listed in the table for the IT policy rule found to be in “Open” status. Appendix d contains instructions on how to verify correct setting on a BlackBerry.

4. Appendix G. If team or Group BlackBerrys are used, ensure procedures in Appendix G have been followed. Verify group/team BlackBerry users have been trained on how to configure the BlackBerry before it is transferred to a new user. (Note that training requirements are verified in WIR1050 check.)

The reviewer must raise this to a CAT I finding if **any** configuration setting designated as CAT I **remains in an Open status**. The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status**.

Note: Open checks in Appendix C and D should be marked against the check number listed in the table for the “Open” IT Policy rule.

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1260 Configure Master Key on the BES

VMS Vulnerability Key: V0011877

Long Name: The IAO will ensure that the Master Key is configured on the BES for AES encryption.

Note: The following BlackBerry devices have BlackBerry Handheld Software versions earlier than 4.0, which uses 3DES encryption instead of AES: 5820, 5810, 5790, 957, 950, 857, and 850. These older BlackBerry devices should not be used in the DoD since they cannot support some required BlackBerry security features.

Severity: CAT III

Checks: Work with the BlackBerry SA to view the BES configuration setting. In the Supported Encryption Algorithms section verify that **AES** is selected.

- In BlackBerry Manager, click on a BES to review
- Select the **Server Configuration** tab
- Click on **Edit Properties**
- Click on **General** in **Properties** list
- Check Encryption Algorithm setting. Verify the setting is correct.

SRR/ECV Finding (circle one):

OPEN NOT A FINDING NOT REVIEWED NOT APPLICABLE

Comments:

WIR1280 Data-at-Rest encryption is enabled on all wireless email devices

VMS Vulnerability Key: V0012164

Long Name: The IAO will ensure that Data-at-Rest encryption is enabled on all wireless push email handheld devices.

Note: When Content Protection is enabled in BES 4.1.4 and earlier, the BES system administrator cannot remotely unlock a BlackBerry device and remotely reset the device password.

Severity: CAT III

Checks

- Work with BlackBerry SA to verify that IT Policy rules are set in accordance with Appendix C. (Checked as part of WIR1250 check.)
- In addition to checking the IT Policy Rule settings, a sample on BlackBerry devices may also be checked as follows:
 - o **Settings>Options>Security Options>General Settings>Content Protection**
 - o Verify **Content Protection** is set to **Enabled**
 - o Verify the setting cannot be changed

SRR/ECV Finding (circle one):

OPEN

NOT A FINDING

NOT REVIEWED

NOT APPLICABLE

Comments:

3. BES AND BLACKBERRY DEVICE SECURITY INFORMATION

3.1 Creating IT Policies

IT policies are a collection of rules that are used by the BlackBerry Enterprise Server (BES) to define how mail is handled and what functions are available on the BlackBerry device. There are over 300 possible policy rules, which are grouped into over 40 policy groups. Table C.1, BES IT Policy Rules, lists all required and optional BlackBerry IT policy settings which are directly or indirectly related to the security of the BlackBerry system. Table D.1, BlackBerry Handheld Software 4.0-4.6 Configuration Settings, lists device settings related to the security of the device.

All new users are assigned to the base or “default” policy. The BES administrator can define customized IT policies and assign users to specific policies based on their roles, jobs, or other needs of the organization.

Note: Users can only be members of one IT policy at a given time.

Steps to create a new IT policy:

- In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
- On the **Global** tab, click **Edit Properties**.
- Select **IT Policy**.
- In the **IT Policy Administration** section, double-click **IT Policies**.
- Click **New**.
- Double-click **IT Policy Name**
- Type a name for the new policy.
- Configure the IT policy rules by performing the following steps:
 - In the left pane, click a policy group.
 - In the right pane, double-click the IT policy rule.
 - Set a value for the IT policy rule.
- Click **OK**.

After the new IT Policy is created, the next step is to assign users to the policy as follows:

- In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
- On the Global tab, click **Edit Properties**.
- Click **IT Policy**.
- In the **IT Policy Administration** section, double-click **IT Policy to User Mapping**.
- In the left pane, click a user account.
- In the right pane, select the desired IT policy.
- Click **OK**.

Note: With the release of BES 4.1.5, RIM provided a new tool in the BlackBerry Resource Kit called “BlackBerry IT Policy Import and Export Tool” for importing and exporting IT policies on the BES. This tool can be used by DoD agencies to configure an agency wide STIG compliant IT policy, which then can be distributed to all subordinate BES sites.

Note: DISA has developed a STIG compliant BlackBerry IT Policy file that can be exported and installed on DoD BlackBerry Enterprise Servers. The file can be found on the IASE web site with this checklist.

3.2 Creating an Activation Password

When a BES administrator uses wireless enterprise activation, the administrator creates an Activation Password on the user's BlackBerry account. A secure method must be used to provide this password to the user (e.g., similar to methods used to provide network passwords to network users).

Configuration or Action	Setting	
	Required	Optional
Activation Password	Passed to user by secure method	
Password Expiration Time		Recommend 12 hours or less

Table 3-1. Activation Password Security

Setup the Activation Password using the following steps.

1. In the BlackBerry Manager, in the left pane, select a BES.
2. On the **Users** tab, select a user account.
3. Click **Service Access**.
4. Click **Set Activation Password**.
5. Type in shared password and retype it to confirm.
6. In the **Password Expires** box, type-in an expiration time.
7. Select **OK**.
8. Provide user password by secure method.

3.3 BlackBerry Application Security

The BlackBerry has become much more than a just wireless email device over the past couple of years. Many industry, Federal Government, and DoD agencies are viewing mobile devices as an extension of the desktop computer, both providing access to the same applications and services. Research In Motion (RIM) has released a number of tools for developing business, productivity, and entertainment applications and has added new capabilities to BlackBerry MDS Services for managing and securing applications and content servers located behind the enclave firewall.

Today, almost any application or service a DoD BlackBerry user can access on their office PC can be accessed from their BlackBerry device, including Lotus Sametime Connect, Jabber Instant Messenger, and Remedy Trouble Tickets. Also, applications can be quickly developed for many DoD business processes; for example weapon inventory management, flight line maintenance procedure checklists, and TDY expense tracking.

BlackBerry applications can generally be characterized as standalone, network applications, or RIM applications, each with the following characteristics:

- Standalone applications
 - Installed as a cod file on the BlackBerry
 - Operates within its own sandbox on the BlackBerry
 - Does access data or resources external to the BlackBerry
 - Can access public BlackBerry APIs
 - Can access controlled BlackBerry APIs if application code is signed by vendor key provided by RIM
- Network applications
 - Installed as a cod file on the BlackBerry
 - Can access data and resources on the BlackBerry, Intranet, and network enclave via the MDS
 - Can access public BlackBerry APIs
 - Can access controlled BlackBerry APIs if application code is signed by vendor key provided by RIM
- RIM applications
 - Developed and signed by RIM key
 - Can access data and resources on the BlackBerry
 - Can access both public, controlled, and private APIs on the BlackBerry
 - Can access low level hardware interfaces

Client applications use the BlackBerry MDS Services, a component of the BES, to access applications and content servers located in the DoD network enclave via the BlackBerry MDS Runtime, BlackBerry JAVA Virtual machine, or BlackBerry Browser.

Note: RIM uses the term “Third-Party Application” to designate any application not developed by RIM and not signed by a RIM digital signature key. Any application developer that wants to access BlackBerry controlled application program interfaces (APIs) that are considered “sensitive” (for example core and cryptographic APIs) must register their application with RIM and have their application signed by a vendor key provided by RIM. Applications that have not been signed by a RIM provided key cannot access controlled BlackBerry APIs.

3.3.1 Application Security Controls

Deploying and using applications and connecting to internal DoD network web services must be done in a secure manner so that the security posture of the BlackBerry device and DoD network are not compromised. Security features available for the deployment and use of applications on BlackBerry devices and connecting to web services include:

- BlackBerry Internal Protections
 - Java Virtual Memory (VM) Sandboxing – stops applications from reading memory outside of their assigned memory area.

- Code signing – only applications that have an approved digital signature can run on the BlackBerry.
- IT Policy Rules
 - Enforces a system wide security policy rule.
 - Takes precedence over an Application Control policy.
- Software Configurations
 - Used to define which applications are allowed or restricted.
 - Used to assign an application control policy to an application.
 - Required applications cannot be removed by user.
- Application Control Policy
 - A default policy is assigned to all applications unless a per-application policy is created and assigned to specific applications.
 - Defines application access to BlackBerry resources (USB connector, GPS, Internet, Address Book, phone, Bluetooth radio, BlackBerry keystore, Intranet connections, etc.).
 - Defines if an application is allowed to be installed on site managed Blackberry devices.
- BlackBerry MDS Integration Service Device Policies
 - Used to control how users access and use BlackBerry RMDS Runtime Applications on their BlackBerry devices.
- CAC Authentication for Servers
 - Back-office enclave applications and content servers that are accessed by BlackBerry users should be configured to require digital certificate based authentication (CAC) of BlackBerry users.
- BES Host-based Firewall
 - The firewall should be configured to allow access to only DAA approved enclave applications and content servers by implementing IP address access control on the firewall.
- Distribution of Applications
 - Applications installed on BlackBerry devices should be distributed only under direct control of the BlackBerry administrator during initial provisioning of the BlackBerry or by using software configurations. Application repositories should not be used in the DoD.
- Security for Push Applications and Web Servers
 - When push applications or web servers located in the enclave are used to push application data and content to site managed BlackBerry devices, trusted connections must be set up between the application and the BlackBerry MDS Connection Service. (A trusted server is a server that has its digital certificate stored in the BES keystore. See Chapter 9, page 64 – 68, of the Administration Guide, BlackBerry Enterprise server for Microsoft Exchange, Version 4.1 Service Pack 5 for more information.)

3.3.1.1 IT Policy Controls

The following BES IT Policy rules are used to control applications on the BlackBerry (the required or recommended DoD configuration is listed after each policy):

- Allow External Connections
 - Required BlackBerry Security Checklist Setting: FALSE
- Allow Internal connections
 - Recommended BlackBerry Security Checklist Setting: TRUE
- Allow 3rd Party Apps to Use Serial Port
 - Recommended BlackBerry Security Checklist Setting: FALSE
- Disallow Third Party Application Download
 - Required BlackBerry Security Checklist Setting: TRUE

3.3.1.2 Software Configuration Controls

Software configurations are defined to install or remove applications on BlackBerry devices and to assign application control policies to allowed applications.

Note: When the IT Policy rule “**Disallow Third Party Application Download**“ is set to **TRUE**, applications cannot be downloaded and installed via the wireless network (i.e., Over-the-Air (OTA) install). In this case, software configurations should be pushed to BlackBerry devices via the BES BlackBerry Manager or BlackBerry Desktop Manager. In some cases, it may not be practical to push a critical software configuration via the BES BlackBerry Manager or BlackBerry Desktop Manager; for example, when a critical update must be installed within a short time period, it is not practical to require users to return their BlackBerry devices to the system administrator to load updates, or users may not have access to the BlackBerry Desktop Manager. In these cases, BES system administrators should follow the following procedure for pushing critical updates to BlackBerry users over the wireless network:

- Create a software configuration with the critical application or software update.
- Change the site BlackBerry IT Policy by setting “**Disallow Third Party Application Download**” to **FALSE**.
- It is recommended that the BES System Administrator send an email to all BlackBerry users and send a message to all site managed BlackBerry devices using the BlackBerry Enterprise Server “Send Message” function prior to pushing the software update to site managed BlackBerrys informing users of the planned wireless software update and requesting that BlackBerry devices be turned on during the time period the update will be pushed out.
- Push the software configuration policy via a wireless update.
- BES System Administrators are required to change the IT policy back to the required configuration as soon as possible after all site managed BlackBerry devices have been updated but no later than 72 hours after the site IT policy was changed. It is recommended that if all site managed BlackBerry devices have not been updated within 36 hours, the BES System Administrator should contact BlackBerry users whose devices have not been updated and their managers to determine why the update has not taken place and facilitate actions to have remaining BlackBerry devices updated as soon as possible. See Figure 3.1 for screen shot showing how to determine if a wireless software update has been received on a site managed BlackBerry device. Site managed

BlackBerrys that cannot be updated with the 72 hour period should be scheduled for a future update when they are available.

- Change the site BlackBerry IT Policy back to the required policy by setting “**Disallow Third Party Application Download**” to **TRUE** and push the new IT policy to all site managed BlackBerry devices.
- Add the new application to the application “White List” described in section 3.3.1.3.
- See the “Quick Reference Guide – BlackBerry Enterprise Server Wireless Push of DoD Root CA Application” located at <https://www.us.army.mil/suite/page/474113> for detailed instructions on this procedure.

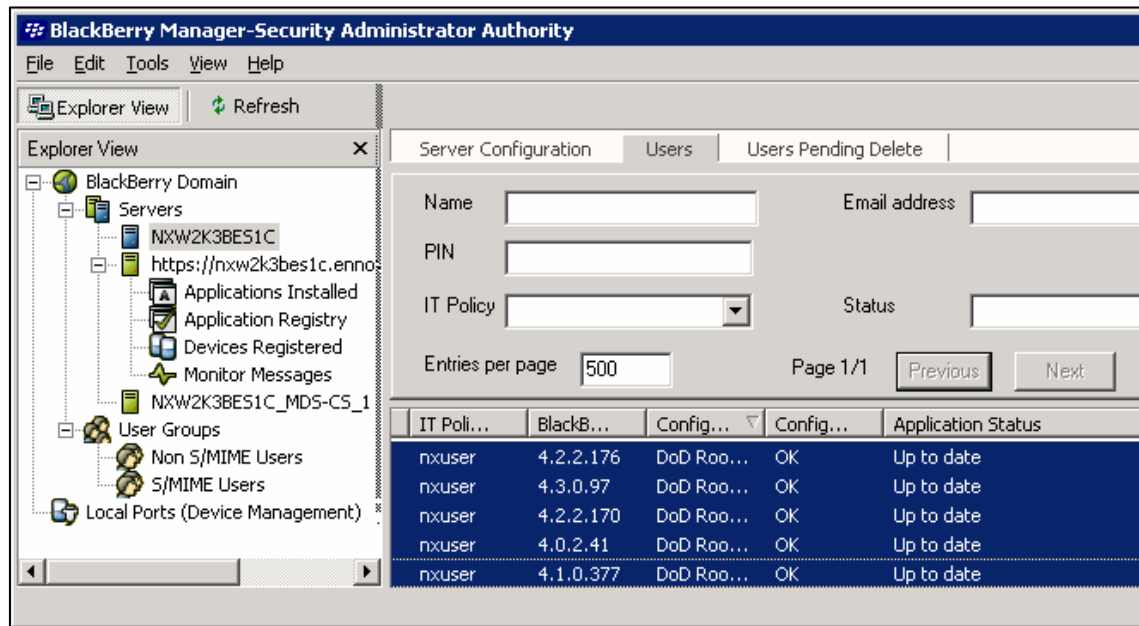


Figure 3-1. Determine if a Wireless Update is Successful

A software configuration can be used to specify required applications on site managed BlackBerry devices using the following procedures:

- Set up a software configuration for each type of BlackBerry device managed by the site.
- Set up an Application Control Policy where the **Disposition** rule is set to **Required**. Name this policy **Force Install**.
- Assign the **Force Install** policy to each required application in each software configuration.
- Assign the software configurations to user groups or individual users.

3.3.1.3 Application Control Policies

Application control policies are used to control what applications can be installed or removed on site managed BlackBerry devices and to control allowable actions of approved applications. A white list of approved applications should be developed using the procedure in BlackBerry

document KB10858 (www.BlackBerry.com). Complete the following steps for creating an application white list:

1. Create an Application Control Policy that denies the installation of all applications. See Figure 3-2.
2. Create an Optional Application Control Policies that restrict actions by approved applications. See Figure 3-3. See the next paragraph for more information on creating application control policies for applications authorized for use by site BlackBerry users.
3. Create a Software Configuration for each type of BlackBerry device assigned to the site. See Figure 3-4.

Assign the Deny All Application Control Policy to the **Application Software** group and then assign Optional application control policies to each required application.

4. Assign a software configuration to a BlackBerry smartphone user or group.
5. Verify the delivery of the software configuration.

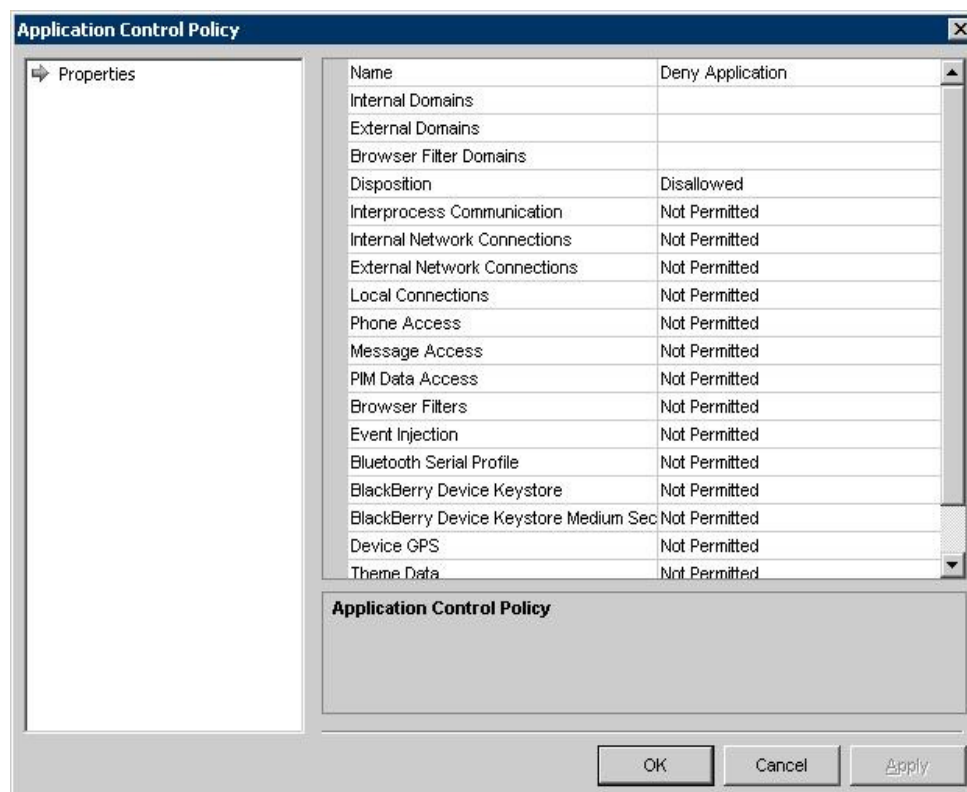


Figure 3-2. Deny All Application Control Policy

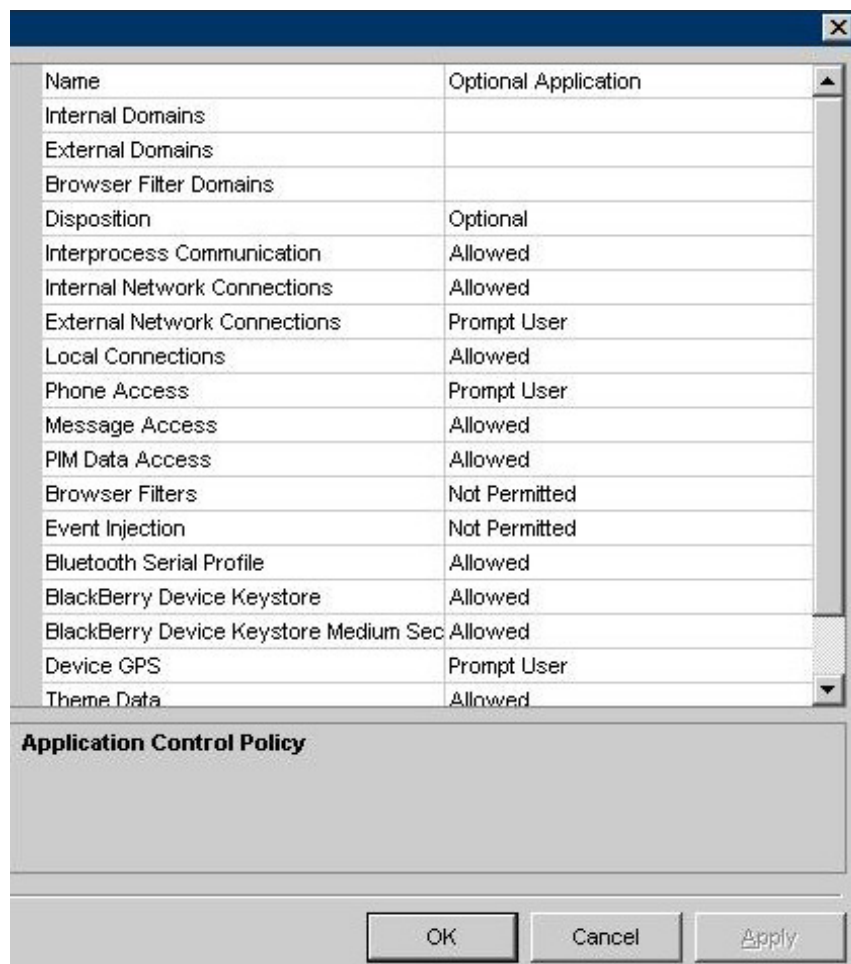


Figure 3-3. Optional Application Control Policy

- MemoPad
- Messages
- Password Keeper
- Phone
- Tasks
- BlackBerry Maps
- BlackBerry S/MIME Support
- BlackBerry Smart Card Reader
- Media
- PIV Driver
- Push to Talk
- Search
- Send Voice Note
- TTY Support
- Voice Dialing

All application control policy rules should be set to “Not Permitted” by default and set to “Allowed” or “Prompt User” only if required for application operation. Only properties required by each application should be allowed.

See page 34 in the “Administration Guide, BlackBerry Enterprise Server for Microsoft Exchange, Version 4.1 Service Pack 6” for information on creating application control policies and page 177 in the “Policy Reference Guide, BlackBerry Enterprise Server, Version: 4.1 | Service Pack: 6 (Document Version 31)” for a detailed description of each application control policy rule.

3.3.2 Configuring BlackBerry MDS Services Security

The BlackBerry MDS Services is a component of the BlackBerry Enterprise Server (BES) and consists of two services: the BlackBerry MDS Connection Service and the BlackBerry MDS Integration Service. The BlackBerry MDS Connection Service enables users to access the Internet, an organization’s Intranet, and connect to application and content servers located on the enclave network. The BlackBerry MDS Integration Service provides application-level integration for BlackBerry® MDS Runtime Applications on BlackBerry devices. Key BlackBerry MDS Services security issues are authentication of the BlackBerry user, access control to only authorized services and connections, and encryption of data between the BlackBerry device and the MDS or data/application server.

Note: Before configuring the BlackBerry MDS Services, determine which DoD servers, Intranet sites, Internet web services, and applications will be accessible to device users.

Figure 3.5 shows how BlackBerry MDS Runtime applications, JAVA applications, and BlackBerry browser applications can be used to provide connections to enclave applications and content servers via the BlackBerry MDS Services. See Chapter 9 of the BlackBerry Admin Guide version 4.1.6 for a detailed description.

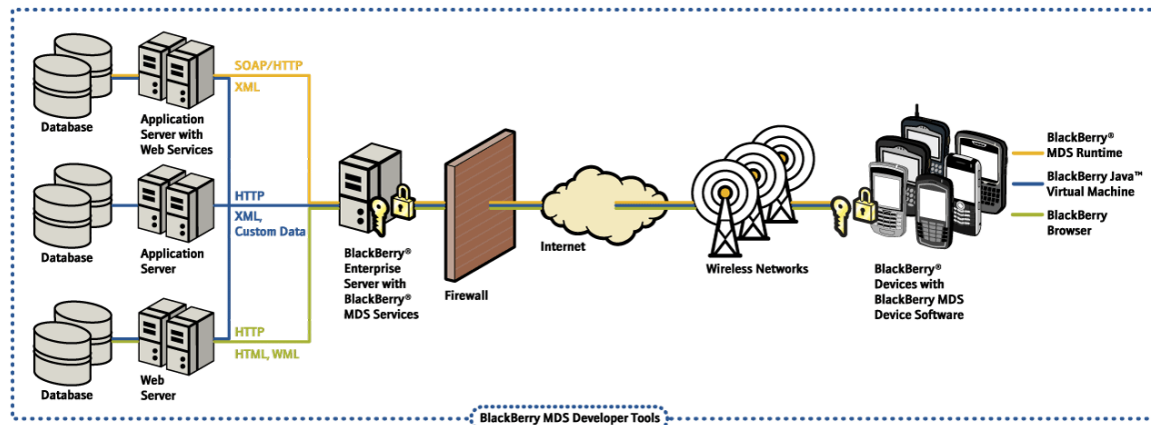


Figure 3-5. BlackBerry Connections to Enclave Servers

3.3.2.1 Configuring BlackBerry Authentication To Web Servers

When connections to enclave applications and content servers are set up in a DoD enclave, the following BES configurations are required:

- Configure BlackBerry devices to authenticate with application and web servers directly. Setting up the BlackBerry MDS Connection Service to authenticate with application/web servers on behalf of the BlackBerry user is not permitted because the BlackBerry MDS Connection Service does not support either NTLMv3 or CAC/certificate based authentication. See Page 62, BlackBerry Admin Guide v4.1.6 for detailed instructions (set **Support HTTP Authentication to False**).
- Create a key store on the BES so the BlackBerry MDS Connection Service can accept HTTPS connections from trusted push application/web servers. See Page 66, BlackBerry Admin Guide v4.1.6 for detailed instructions.
- Configure the BlackBerry MDS Connection Service to disable connections from untrusted push application/web servers. See Page 68, BlackBerry Admin Guide v4.1.6 for detailed instructions (set **Allow Untrusted HTTPS Connections to False** and set **Allow Untrusted TLS Connections to False**).
- Configure the BlackBerry MDS Connection Service to use OCSP to retrieve the status of certificates of web servers. See Page 69, BlackBerry Admin Guide v4.1.6 for detailed instructions. See Figure 3.7 in this checklist for required OCSP configuration.

3.3.2.2 Data Encryption

When data is sent between the BlackBerry MDS Connection Service and the BlackBerry device it is encrypted using the same data encryption processes that are used to encrypt wireless email between the BES and the BlackBerry device. In addition, SSL or TLS security encryption can be enabled for those application servers that require secure connections.

3.3.2.3 BlackBerry MDS Connection Service Properties

The following tables and figures show security related BlackBerry MDS Connection Service properties and *required* or *optional* configuration settings for those properties.

HTTP Properties

HTTP Properties		
MDS Property	Setting	
	Required	Optional
Support HTTP Authentication	FALSE	
Authentication Timeout		3600000
Support HTTP Cookie storage		FALSE
HTTP handheld connection timeout (milliseconds)		120000
HTTP server connection timeout (milliseconds)		120000
Maximum number of redirects		5

Table 3-2. HTTP Properties

Proxy Properties

Proxy Properties		
MDS Property	Setting	
	Required	Optional
Proxy Mappings		Specify required mappings

Table 3-3. Proxy Properties

TLS/HTTPS Properties

TLS and HTTPS Properties		
MDS Property	Setting	
	Required	Optional
Allow Untrusted HTTPS Connections		FALSE
Allow Untrusted TLS Connections		FALSE

Table 3-4. TLS and HTTPS Properties

Logs Properties

Logs Properties		
MDS Property	Setting	
	Required	Optional
Logging Level Detail		HTTP logs, TLS Logs

Table 3-5. Log Properties

Note: A sound best practice is for each site to keep logs for 30 days. Logs can be kept 7 days or less on the BES server and then archived offline.

CRL Properties

The Certificate Revocation List (CRL) should not be configured on a DoD BES. The BES is limited to configuration of only one CRL connection. The current DoD PKI has over 20 CRL locations. OCSP must be configured instead.

LDAP Properties

Only one LDAP can be defined at the BES level. See Figure 3.6. Additional connections to different LDAPs would be configured through the BlackBerry Desktop Manager.

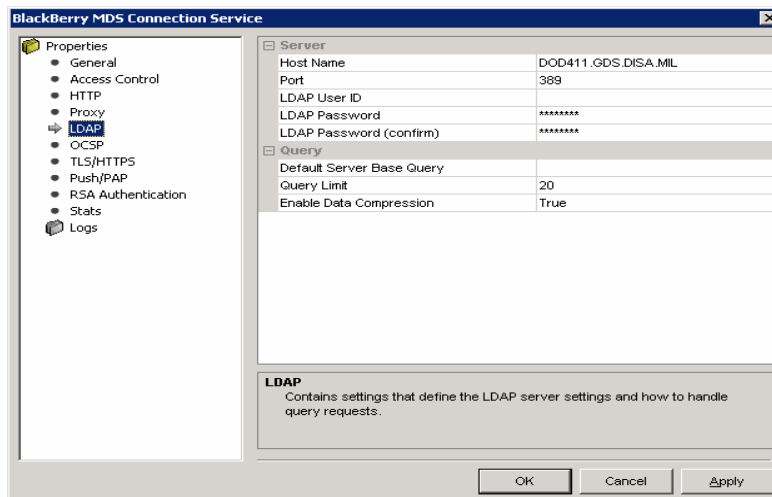


Figure 3-6. Screen Shot – LDAP Configuration

OCSP Properties

OCSP provides certificate validation services for all DoD PKI issued certificates in one location. Configure as shown in Figure 3.7.

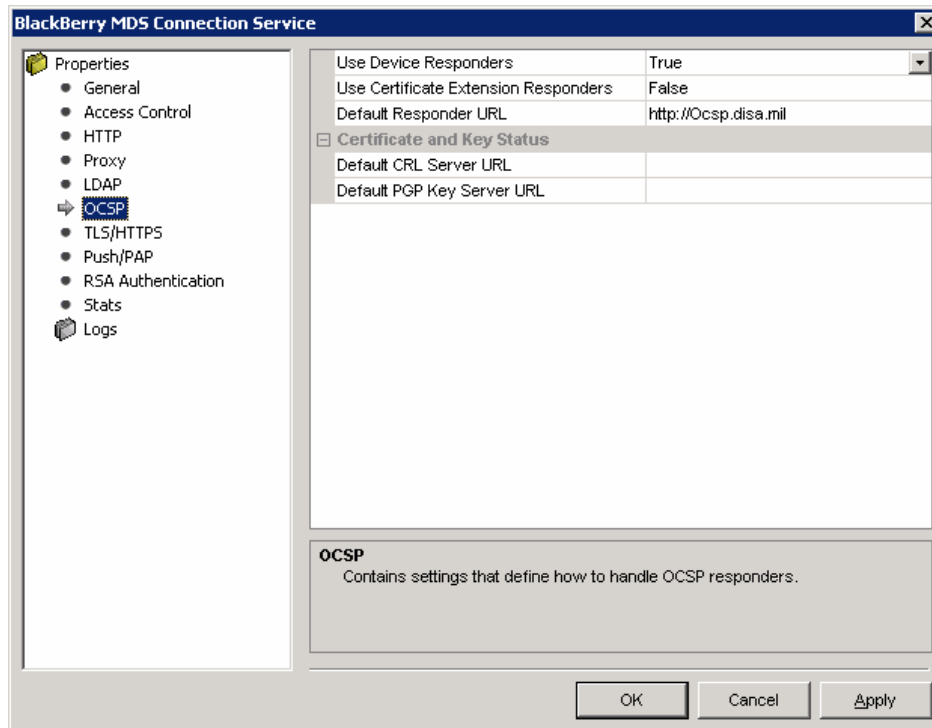


Figure 3-7. Screen Shot – OCSP Configuration

3.3.2.4 BlackBerry MDS Integration Service Security

When the BlackBerry MDS service is installed on the BES, a default BlackBerry MDS Integration Service device policy should be set. Table C-6 shows recommended and required settings for the BlackBerry MDS Integration Service device policy.

3.4 S/MIME Configuration

The BlackBerry S/MIME Support Package (SSP), provides the capability for users to send and receive S/MIME email messages from their BlackBerry devices when S/MIME is enabled on their BES.

Table C.1, IT Policy Rules, lists all S/MIME related *Required* and *Optional* BlackBerry IT policy settings.

For S/MIME Pin-to-Pin messaging (BlackBerry Messenger), do the following:
Set Allow Peer-to-Peer Messages to **TRUE**
Set Disable Peer-to-Peer Normal Send to **TRUE**
Have recipient PIN listed in address book entry

The following recommended change should be made to the default S/MIME configuration of the BES so that “Signed” messages are not also encrypted, by default:

Change "**Enable S/MIME Encryption on Signed and Weakly Encrypted Messages**" from "**TRUE**" (default setting) to "**FALSE**."

3.5 PGP Encryption

PGP encryption should not be used on DoD BlackBerry systems. S/MIME is the standard email encryption package for DoD BlackBerry systems.

3.6 Managing Encryption Keys

Both 3DES and AES encryption are available on the BES for securing data between the BES and the BlackBerry device but AES should be selected as the BES encryption algorithm. BlackBerry devices that use BlackBerry handheld software earlier than version 4.0 do not support the AES algorithm and should not be used because required security features cannot be supported.

Select Master Key Algorithm

Select the Master Key on the BES as follows:

1. In the BlackBerry Manager, right-click a server and select a **BlackBerry Enterprise Server** in left pane
2. In the right pane, select **Edit Properties**
3. Select **General** tab
4. In the Security section, click **Encryption Algorithm: AES**

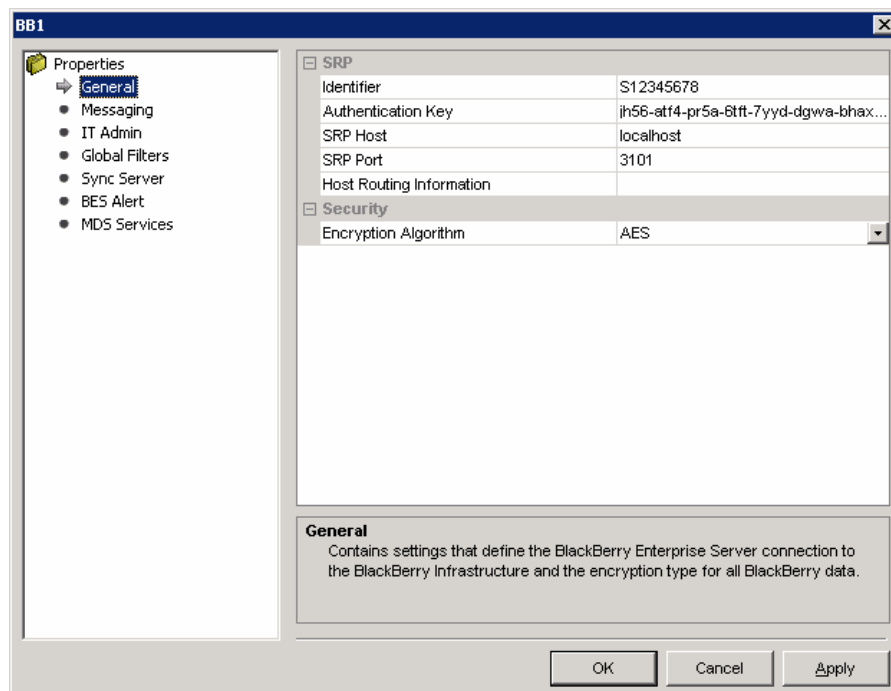


Figure 3-8. Screen Shot – Selecting Master Key Algorithm

The following IT Policies apply to the selection and protection of Master Keys. Table C.1, IT Policy Rules, lists all related *Required* and *Optional* BlackBerry IT policy settings.

Security policy group
Disable 3DES Transport Crypto
Force Content Protection of Master Keys

3.7 Maintenance Configuration

3.7.1 Logging

BlackBerry Enterprise Server event logs are a key tool for monitoring BlackBerry system security events and the BES should be configured to log system events. Logs can be configured to record Global events (all log files on the BES) or at the component/service level. BES components include Router, Dispatcher, Messaging Agent, Controller, Attachment Service, Synchronization Service, Mobile Data Service, Policy Service, and Database.

Steps to configure global BES logs:

1. Start > Programs > BlackBerry Enterprise Server > BlackBerry Server Configuration
2. Select Logging tab
3. Modify desired parameters:
 - **Log Root Location** Type the desired root folder for logs, or click browse
 - **Log file prefix** Type the desired custom prefix to add to all log file names
 - **Create daily log folder** Type **Yes** if daily log files are desired
4. Select **OK**

Steps to configure component BES logs:

1. Start > Programs > BlackBerry Enterprise Server > BlackBerry Server Configuration
2. Select Logging tab, then select a Server component or service
3. Modify desired parameters:
 - **Debug log identifier** Type new default four letter identifier for component
 - **Debug daily log file** Type **Yes** if daily log files are desired
 - **Debug log level** Select level of logging
 - **Debug log size** Select value of maximum log size
 - **Debug log auto-roll** Select if new log file is created when component is restarted or the maximum log size is reached.
 - **Debug log maximum** Select maximum log age in days
 - **Daily file age** Select maximum log age in days. Select at least one day longer than period logs are moved to offline storage (e.g., select 8 days if standard procedures is to move Daily logs on BES to offline storage every 7 days).
4. Select **OK**
5. Restart the component

Note: RIM recommends that 30 days of daily log files be maintained for each component or service for system troubleshooting purposes. No more than seven days of logs should be

maintained on the same server that the BES is installed on, therefore the BES administrator should move logs to offline storage every 7 days or less.

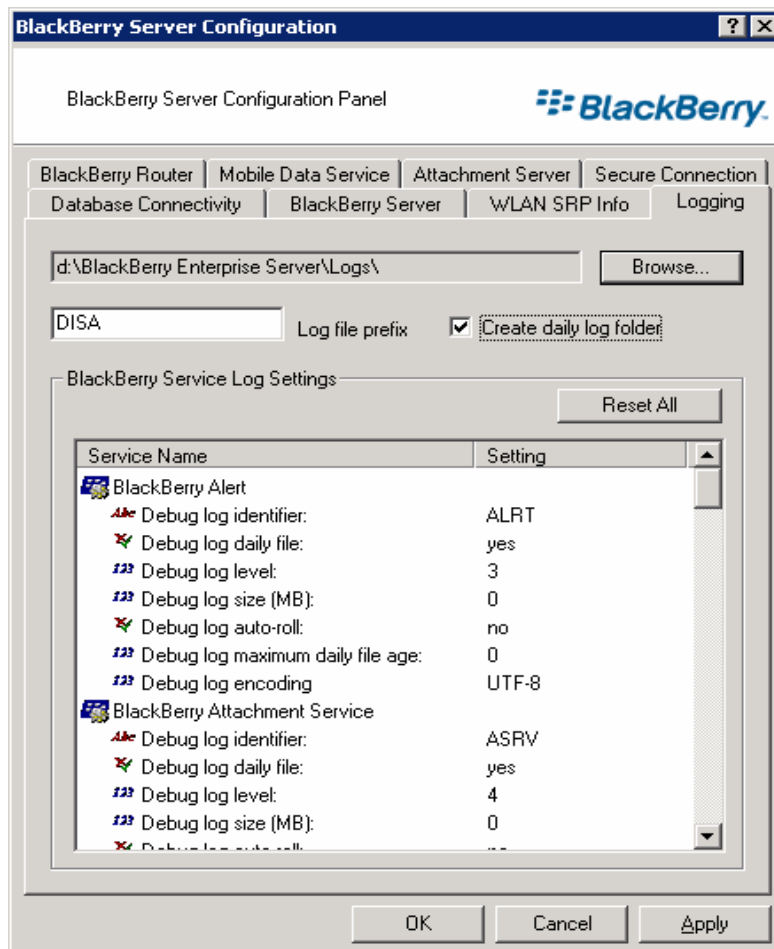


Figure 3-9. Screen Shot – Configuring Global BES Logs

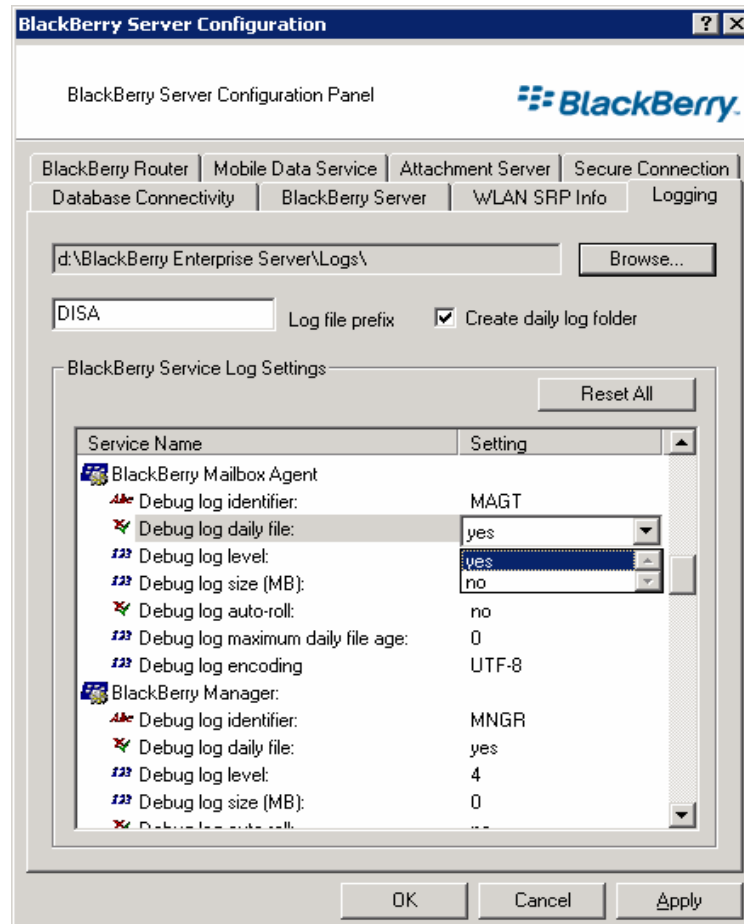


Figure 3-10. Screen Shot – Configuring component BES Logs

3.7.2 BES Alert Settings

The BES Alert Tool monitors the Microsoft Windows Event log and sends selected users email messages containing alert notifications when certain events are recorded in the Event log. Types of events monitored include critical, errors, warnings, and information.

Critical messages are generated by events that affect the operation of the BES.

Error messages are generated by events that affect email redirection for all BlackBerry users.

Warning messages are generated by events that affect email redirection for one or more (but not all) BlackBerry users.

Informational events are generated by any action performed by the BES.

When selecting **Critical**, includes **Critical** messages only.

When selecting **Error**, includes **Critical** and **Error** messages.

When selecting **Warning**, includes **Critical**, **Error**, and **Warning** messages.

When selecting **Informational**, includes **Critical**, **Error**, **Warning**, and **Informational** messages.

BES Alert Setting		
Configuration or Action	Setting	
	Required	Optional
BES Alert		Critical, Error or Warning

Table 3-6. BES Alert Setting

To configure the BES Alert, follow the instructions under **Set the default event monitoring level** on page 2 of the *User Guide, BlackBerry Enterprise Server Alert Tool*.

To define a BES Alert message recipient, follow the instructions under **Define a notification recipient** on page 2 of the *User Guide, BlackBerry Enterprise Server Alert Tool*.

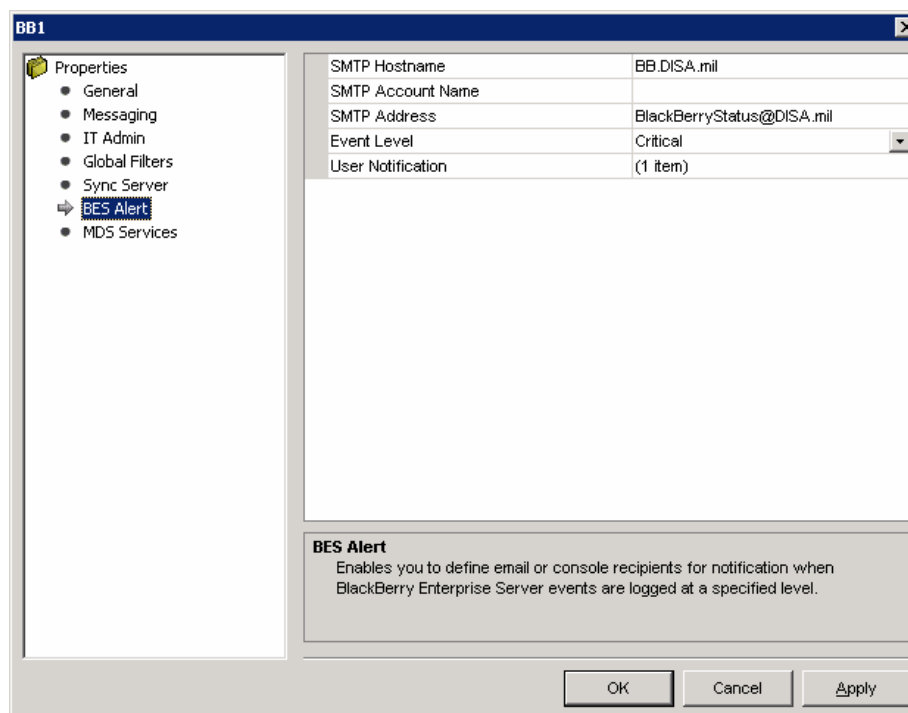


Figure 3-11. Screen Shot – Configuring BES Alert

Information on configuring BES Alert can be found in the RIM document *User Guide, BlackBerry Enterprise Server Alert Tool*.

3.7.3 System Backup

Full system backups should be performed regularly on BES data to protect the BlackBerry system against system data loss or unavailability. The following BES data should be backed up:

- BES registry settings
- Log files
- Attachment service executables and supporting files
- Microsoft Exchange user mailbox information and hidden BlackBerry files

The BlackBerry Backup tool is used to manage data backup and recovery. Procedures for using the tool are found in Appendix D of the BlackBerry Enterprise Server for Microsoft Exchange, Version 4.0, Maintenance Guide.

3.7.4 BES Monitoring Tools

The BlackBerry Enterprise Server resource Kit has a number of tools for analyzing, monitoring, and troubleshooting the BES. BES System administrators should consider using these tools to continually monitor the status of the BES. Information on these tools can be found in the RIM document: *BlackBerry Enterprise Server Resource Kit, version 4.1 Service Pack 5, User Guide for the BlackBerry Analysis, Monitoring, and Troubleshooting Tools*.

3.8 Content Protection

Content Protection encrypts data stored on the BlackBerry handheld device using 256-bit AES encryption. The following items are encrypted on the BlackBerry device: Email, Calendar, MemoPad, Tasks, Contacts, Auto Text, and BlackBerry Browser.

Content Protection can be enabled either by an IT Policy configuration setting or by selecting the Content Protection option on the BlackBerry device. In DoD, Content Protection should be enabled via an IT Policy configuration setting.

Note: When using BES version 4.1.4 and earlier or BlackBerry handheld software version 4.4 and earlier, and Content Protection is enabled, the BES system administrator *cannot* remotely unlock a BlackBerry device and remotely reset the device password, which may be a critical mission requirement at some DoD facilities. Version 4.5 of the BlackBerry handheld software is only available for 8xxx and higher series BlackBerrys.

Table C.1, IT Policy Rules, lists the *Required* and *Optional* BlackBerry IT policy settings.

3.9 Password Keeper Settings

Password Keeper is a third party application provided by RIM that can be installed on the BlackBerry handheld device. This application allows users to create and store passwords. The use of Password Keeper should be reviewed and approved by the local DAA. Passwords are stored using 256-bit AES encryption using the BlackBerry FIPS 140-2 certified encryption module. Passwords in the Password Keeper can be copied and pasted into other applications but the password is unencrypted while it resides in the BlackBerry handheld device clipboard.

When Password Keeper is enabled, the user must configure the application to enforce the following rules.

- Require use of a eight or more character password.
- Set the number of incorrect passwords entered before a device wipe occurs to 10 or less.
- Change the password at least every 90 days.

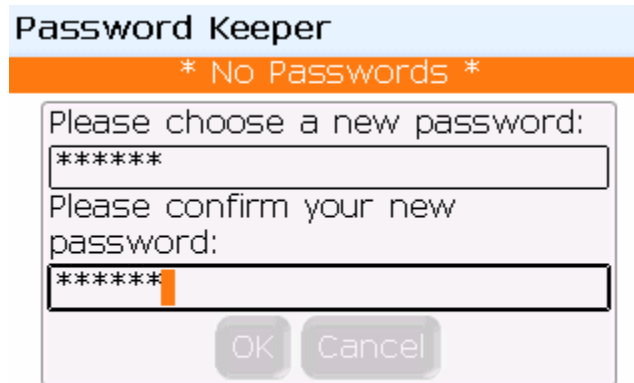


Figure 3-12. Screen Shot – Setting Password Keeper password

3.10 Bluetooth Security Settings

Bluetooth wireless voice and data connections can be established between the BlackBerry handheld device and any other device with Bluetooth wireless capabilities. There are significant security issues with Bluetooth, therefore, Bluetooth should only be used as follows:

- Voice connection to a Bluetooth cell phone headset is prohibited due to Bluetooth security issues. Wired handsfree devices should be used.
- Data connections for the Bluetooth smart card reader (see section 3.11). Only DISA tested and approved Bluetooth CAC readers may be used.

Table C.1, IT Policy Rules, lists the *Required* and *Optional* BlackBerry IT policy settings.

3.11 Bluetooth Smart Card (CAC) Reader

The Bluetooth Smart Card Reader significantly improves the ease of use of the Common Access Card (CAC) with the S/MIME Support Package. When configured properly, the Bluetooth Smart Card Reader provides a secure wireless data connection between the smart card reader and BlackBerry device or between the smart card reader and PC. (See section 3.17 for information on using the BlackBerry SCR with PCs.)

Table C.1, BES IT Policy Rules, lists the required and optional BlackBerry IT policy settings.

Note: Organizations should set up separate IT policy groups for users that use the Bluetooth Smart Card Reader (SCR) and for users that do not use the Bluetooth SCR.

3.12 Forcing BlackBerry Device Software Updates

A critical component of a DoD BlackBerry system security posture is ensuring all BlackBerry devices have up-to-date software and application loads on the handheld devices. Therefore

BlackBerry system administrators will include rules in each IT policy users are assigned to that force upgrades to site managed BlackBerry devices.

The following IT Policy applies to software updates on BlackBerry devices. Table C.1, BES IT Policy Rules, lists the *Required* and *Optional* BlackBerry IT policy settings.

Desktop Only policy group
Force Load Count
Force Load Message

3.13 Firewall Requirements

3.13.1 BES Architecture

DoD security policy requires isolation of the BES host server from the site's Internal LAN (also referred to as the Internal Enclave LAN) by installing a host-based firewall on the BES host server or installing a firewall between the BES and the Internal LAN. The BES and Exchange Servers must be placed on the same segment of the Internal LAN to facilitate communications. The BES also needs to communicate with other resources (e.g., email, LDAP, and OSCP servers; and authorized back-office web servers, SOAP web services, and J2ME applications) which may be located in various segments or security domains within the site's architecture. This section describes the configuration requirements of the host-based firewall located on the BES.

3.13.2 BlackBerry Host Based Firewall Non-Segmented Architecture

In this architecture, all systems used to host BlackBerry services (e.g., email server and LDAP server) are protected behind an Internal Enclave firewall and added protection is achieved by use of a host based firewall installed on the BES server. The BES server is located directly on the Internal Enclave LAN on the same network segment as the Exchange Server.

The Local Gateway Firewall depicted in Figure 2.1 is an Internal Enclave firewall which creates a separate security domain for the site's Internal LAN. Specific firewall rules implemented on the BES host-based firewall will vary based on the BES services used. The server will need to communicate with the LDAP server, OSCP, BlackBerry SRP, Exchange Server, SQL Server, and any other authorized resources (e.g., back-office application and content servers) not installed directly on the BES. Careful testing prior to deployment of the BES server will be needed to ensure proper operation while remaining compliant with DoD ports, protocols, and services policies.

In accordance with DoD policy, the administrator must configure the host-based firewall policy to deny unneeded incoming and outgoing ports and services by default. In addition, connections to internal network back-office application and content servers should be blocked except for connections to authorized servers by implementing a list of trusted IP addresses. Furthermore, firewall filtering rules will be documented; security alerts must be monitored; and a firewall audit log must be maintained. The firewall used for this functionality must be robust and have the capability to block both incoming and outgoing traffic.

In general, the host based firewall rules must be configured to implement the following policies:

- Internal traffic from the BES is limited to internal systems used to host the BlackBerry services (e.g., email, LDAP servers, and authorized back-office application and content servers). Communications with other services, clients, and/or servers are not authorized.

- Internet traffic from the BES is limited to only specified BlackBerry services (e.g., BlackBerry SRP server, OCSP, SSL/TLS, HTTP, and LDAP). All outbound connections are initiated by the BlackBerry system and/or service.

The following table lists the default or standard ports for the needed services used for BES and BlackBerry device communications in a segmented network. Although it is possible to configure TCP/UDP to use non-standard or unregistered ports for these communications, this is not recommended as it will cause unexpected results at various internal or external boundaries in the DoD Enclave.

Note: The following table is intended as a starting point and is provided by request of field sites and reviewers to facilitate firewall configuration. Use additional references from RIM, Microsoft, and DISA STIGs to tailor the firewall rule configuration to the site’s specific architecture.

Service	Protocol	Default Port	Comments
Outgoing data connections, using SRP, to BlackBerry Infrastructure.	TCP	3101	Both the Local Gateway Firewall and the Enclave Perimeter firewall outbound rules must be configured to allow this port outbound to Internet via NIPRNet (DoD Network). (Must traverse PPS CAL boundaries 12, 10, 6, 4, and 2 when configured in compliance with the requirements of this checklist.)
Incoming and outgoing connections from the Desktop Manager utility installed on a PC with the handheld device attached. Used to sync the BlackBerry to the BES.	TCP	4101	Incoming and outgoing connections on the Internal Enclave (Intranet) to/from the BES (i.e., not outgoing to the Internet).
Incoming and outgoing connection to the Microsoft SQL server for BlackBerry Configuration Database	TCP	1433	Needed only if SQL is on a separate server from BES.

Service	Protocol	Default Port	Comments
Outgoing connections to the Enclave web proxy server	HTTP, HTTPS	8080, 8443	For BlackBerry browser connections to the Internet if permitted by local policy. Some sites have opted to place all application and web proxy services into an Internal Enclave DMZ network. If the DAA has approved access to these applications, then the FA will update all appropriate firewall rules to allow the BES access. List IP address of the web proxy server in the host-based BES firewall list of trusted IP addresses and subnets.
Outgoing connections to Enclave application, and content servers (J2ME servers, SOAP web services, and web content servers)	HTTP, HTTPS	8080, 8443	For approved/authorized connections to Internal Enclave application servers. If the DAA has approved access to these applications, then the FA will update all appropriate host-based BES firewall rules to allow the BES access, including listing IP address of the servers in the firewall list of trusted IP addresses and subnets.
Outgoing connection to trusted OCSP	HTTP	80	To obtain PKI certificate information.
Connections between BES and BlackBerry Messaging Agent – Incoming data connections to the BlackBerry Dispatcher – Incoming system log connections to the BlackBerry Controller	TCP UDP	5096 4070	
Outgoing system log connections from the BlackBerry MDS Connection Service to the SNMP agent	UDP	4071	
For connections between the BES and the Enclave Microsoft Exchange Server.			
RPC endpoint mapper	TCP	135	
Microsoft Exchange System Attendant service	TCP	135	

Service	Protocol	Default Port	Comments
Name Service Provider Interface (NSPI)	TCP	135	
Microsoft Exchange Information Store	TCP	135	

Table 3-7. Host-Based Firewall Architecture Ports, Protocols and Services for Non-Segmented Architecture On BES

3.13.3 Segmented Architecture

In the segmented network architecture (see Figure 2-2) the BES Router is installed in a DMZ of the enclave border firewall. A host-based firewall must be installed on the server with the BES router and configured as described in the Desktop Application STIG.

When the segmented network architecture is used, the host-based firewall on the BES router and the DMZ must be configured as shown in Figure 3-8.

Service	Protocol	Default Port	Comments
Incoming from the BES locked on the enclave. Outgoing data connections, using SRP, to BlackBerry Infrastructure.	TCP	3101	Both the Local Gateway Firewall and the Enclave Perimeter firewall outbound rules must be configured to allow this port outbound to Internet via NIPRNet (DoD Network) and inbound from the enclave. (Must traverse PPS CAL boundaries 12, 10, 6, 4, and 2 when configured in compliance with the requirements of this checklist.)
Incoming and outgoing connections from the Desktop Manager utility installed on a PC with the handheld device attached. Used to sync the BlackBerry to the BES.	TCP	4101	Incoming and outgoing connections on the Internal Enclave (Intranet) to/from the BES (i.e., not outgoing to the Internet).
Outgoing system log connections from the BlackBerry MDS Connection Service to the SNMP agent	UDP	4071	

Table 3-8. Host-Based Firewall Architecture Ports, Protocols and Services for Segmented Architecture On BES Router

When the segmented architecture is used, the host-based firewall on the BES should be configured as shown in Figure 3-9.

Service	Protocol	Default Port	Comments
Outgoing data connections, to the BES Router located in the DMZ.	TCP	3101	
Incoming and outgoing connections from the Desktop Manager utility installed on a PC with the handheld device attached. Used to sync the BlackBerry to the BES.	TCP	4101	Incoming and outgoing connections on the Internal Enclave (Intranet) to/from the BES (i.e., not outgoing to the Internet).
Incoming and outgoing connection to the Microsoft SQL server for BlackBerry Configuration Database	TCP	1433	Needed only if SQL is on a separate server from BES.
Outgoing connections to the Enclave web proxy server	HTTP, HTTPS	8080, 8443	For BlackBerry browser connections to the Internet if permitted by local policy. Some sites have opted to place all application and web proxy services into an Internal Enclave DMZ network. If the DAA has approved access to these applications, then the FA will update all appropriate firewall rules to allow the BES access. List IP address of the web proxy server in the host-based BES firewall list of trusted IP addresses and subnets.
Outgoing connections to Enclave application, and content servers (J2ME servers, SOAP web services, and web content servers)	HTTP, HTTPS	8080, 8443	For approved/authorized connections to Internal Enclave application servers. If the DAA has approved access to these applications, then the FA will update all appropriate host-based BES firewall rules to allow the BES access, including listing IP address of the servers in the firewall list of trusted IP addresses and subnets.
Outgoing connection to trusted OCSP	HTTP	80	To obtain PKI certificate information.

Service	Protocol	Default Port	Comments
Connections between BES and BlackBerry Messaging Agent	TCP	5096	
– Incoming data connections to the BlackBerry Dispatcher	UDP	4070	
– Incoming system log connections to the BlackBerry Controller			
Outgoing system log connections from the BlackBerry MDS Connection Service to the SNMP agent	UDP	4071	
For connections between the BES and the Enclave Microsoft Exchange Server.			
RPC endpoint mapper	TCP	135	
Microsoft Exchange System Attendant service	TCP	135	
Name Service Provider Interface (NSPI)	TCP	135	
Microsoft Exchange Information Store	TCP	135	

Table 3-9. Host-Based Firewall Architecture Ports, Protocols and Services for Segmented Architecture On BES

3.14 BlackBerry IP Modem

A BlackBerry can be used as an “IP” modem or “tethered modem” to provide a wireless Internet connection for a laptop computer. In some cases, this is less expensive than buying a broadband wireless card and setting up a separate broadband wireless account. In order to use the BlackBerry IP modem feature, the following IT Policy rules must be configured as indicated:

Disable IP Modem - FALSE
 Disable Radio When Cradled – 0

Note: Most wireless carriers disable the capability for using the BlackBerry browser to directly set up a tethered connection to a laptop via an Internet connection, forcing subscribers to buy a higher priced “BlackBerry Data Service Plus Tethered” service. Procedures for setting up IP modem service on a laptop are available from each wireless carrier or on several web sites, including <http://forums.crackberry.com/f33/ip-modem-installation-procedures-6633/>.

3.15 Disposal of BlackBerry Handhelds

Appendix B provides required BlackBerry sanitization procedures to follow prior to disposing of BlackBerry devices (e.g., donating to a charity, selling as excess inventory).

3.16 Use of “Team” BlackBerrys

Appendix G provides security requirements and procedures for setting up and using “team” BlackBerrys. A “team” BlackBerry is configured to receive email for a group email account and is shared between team members (e.g., a help desk team where the on-call team member will have the team BlackBerry).

3.17 RIM Bluetooth Smart Card Reader Connections to PCs

The RIM BlackBerry Smart Card Reader (i.e. CAC reader) is designed to connect to both the BlackBerry and to PCs with Bluetooth radios. DoDD 8100.2 requires strong security controls when Bluetooth is used in the DoD, therefore if the RIM BlackBerry Smart Card Reader is used as a PC smart card reader, the following security controls must be implemented:

- The DAA must approve the use of the RIM BlackBerry Smart Card Reader with site PCs.
- Separate BlackBerry Account Groups will be created: one for users that are authorized to use the RIM BlackBerry Smart Card Reader with their PCs and one for users that are NOT authorized to use the RIM BlackBerry Smart Card Reader with their PCs (or do not have a RIM BlackBerry Smart Card Reader). The IT Policy rule settings for the Bluetooth Smart card reader policy group will be set for each account group as indicated in Table C.1.

Note: Recommend 3 BlackBerry account groups be created:

1. BlackBerry users without a smart card reader.
 2. BlackBerry users with a smart card reader, but not authorized to use the smart card reader to connect to their PC.
 3. BlackBerry users with a smart card reader and authorized to use the smart card reader to connect to their PC.
- The BlackBerry SCR will only be used with PCs that have Windows XP SP2 (or later) installed. Using the RIM BlackBerry Smart Card Reader with Windows Vista is not approved since DoD testing of the Vista Bluetooth stack has not been completed and configuration procedures for Vista have not been developed. BlackBerry users with Vista on their PCs must be put in the BlackBerry users group not authorized to use the BlackBerry SCR with their PCs.
 - Bluetooth radios must be disabled in all PCs where users do not have a RIM BlackBerry Smart Card Reader or the use of the RIM BlackBerry Smart Card Reader has not been approved by the DAA. Bluetooth radios will be disabled either by removing the radio from the PC and/or by Windows group policy.

- Only Bluetooth Class 2 or 3 radios must be used by the PC. Class 1 (100 mW) Bluetooth radios are not allowed. Also, Bluetooth controllers on the PC must support 128-bit Bluetooth encryption.

Note: Many vendors do not disclose the class of the Bluetooth radio in their product data or specification sheets, therefore the vendor's technical support office may need to be contacted for this information. For laptops, look under the specification section of the Bluetooth Network Interface Card manual, which can be downloaded from the laptop vendor's web site or the Bluetooth dongle vendor's web site.

- Only RIM BlackBerry Smart Card Reader operating system version 1.5.1 (platform 1.5.0.81) or later will be installed on the smart card reader and BlackBerry Smart Card reader software application version 4.2.0.88 or later will be installed on the Bluetooth enabled PC.
- **Note:** RIM indicates 4.2.0.88 refers to the reader driver version and 1.5.0.81 refers to the reader operating system version.) In addition, the RIM Bluetooth Lockdown tool will be installed and enabled (check **Restrict Bluetooth Functionality**) during installation of the BlackBerry Smart Card Reader Software. Installation should be performed by the authorized BlackBerry system administrator.
- The site Windows group security policy will set to restrict the capability of the PC user to disable, remove, or change the configuration of the RIM Bluetooth Lockdown tool.
- Users with administrative account rights to their PC must be trained to never disable the RIM Bluetooth Lockdown tool on their PC. PC Administrators should NEVER change any Bluetooth settings followings implementation of Bluetooth lockdown.

Note: The RIM Bluetooth smart card reader will not operate unless the Bluetooth radio in the PC uses the Microsoft Windows Bluetooth stack. Some Bluetooth USB adapters do not use the Windows Bluetooth stack and install an alternate Bluetooth stack when the adapter drivers are installed on the PC (or provide the option to install an alternate Bluetooth stack). Additional information can be found at the following we site: <http://hellalame.com/bluetooth.htm>.

3.18 Using Software Certificates

DoD PKI issued digital certificates are used to digitally sign and encrypt email. When using PKI digital certificates with a handheld device (e.g., BlackBerry, Windows Mobile Smartphone), a user's digital certificates can be stored either on the handheld (soft certificates) or on their Common Access Card (CAC) (hard certificates). Software certificates are defined as any PKI certificate that does not require the presence of a common access card, smart card, or alternate hardware token for the certificate to be used for digital signature or encryption operations.

Software certificate use by end users must be approved by the Component DAA, and remain in use only for the minimum time necessary to comply with the hardware token requirement. Approval of software certificate usage by the DAA can be for general use cases, for groups of individuals, or for organizations to preclude DAA's approving individual end user instances of software certificate usage.

The current JTF-GNO position is that they prefer the usage of CAC for S/MIME requirements for BlackBerry devices, but the use of software certificates is not precluded if requirements of JTF-GNO Communications Tasking Order (CTO) 07-15 Revision 1 are met:

- Passwords to open software certificate stores must be at least 15 characters long.
- Passwords to open software certificate stores must consist of at least one of each of the following: upper case letter, lower case letter, special character, and number.

Note: Software certificates are saved in the BlackBerry keystore, which has the same password as the device unlock password. Therefore, when software certificates are used on a BlackBerry, the BlackBerry password must be set to meet the requirements of CTO 07-15 Revision 1. The following BES IT Policy rules must be set as follows:

IT Policy Group	IT Policy Rule	Required Setting
Minimum Password Length	Device-Only	15
Password Pattern Checks	Device-Only	3

3.19 BlackBerry Use with Wireless LANs

Several BlackBerry models are Wi-Fi enabled providing access to both voice and data services over cellular and Wi-Fi networks. The BlackBerry Wi-Fi service can be used to connect to DoD WLAN networks, public Wi-Fi hotspots, or home WLAN networks. The primary purpose of the BlackBerry Wi-Fi service is to provide an alternate wireless connection to the BES when cellular service is not available (for example in buildings like the Pentagon) but it can also be used for voice services such as when Unlicensed Mobile Access (UMA) services are available from the mobile network service provider and connections to the Internet. It is also possible for a BlackBerry user to connect simultaneous to both cellular and Wi-Fi networks, for example, when using the cellular connection for a telephone call while connected to the BES for email via a Wi-Fi connection. Wi-Fi enabled BlackBerrys also include a VPN client that provides a secure connection to enterprise networks. The VPN client provides FIPS 140-2 encryption and is both Wi-Fi and WPA2 certified but it does not support smart card (e.g. CAC) authentication.

The following Wi-Fi connections options are available for connecting Wi-Fi enabled BlackBerry devices to a DoD BES (see *BlackBerry Enterprise Server Wi-Fi Implementation Supplement* for more information.):

- Direct connection to the BES router via a Wi-Fi connection to a DoD network WLAN access point (with or without a VPN connection).
- Direct connection to the BES router via the Internet using a Wi-Fi connection to a home or hot spot WLAN access point (with or without a VPN connection).

- Connection to the BlackBerry mobile network via the Internet using a Wi-Fi connection to a home or hot spot WLAN access point.

DoD security requirements for WLAN systems can be found in the following documents: DoDD 8100.2; ASD-NII Memorandum, Subject: Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies in the Department Defense (DoD) Global Information Grid (GIG), 2 June 2006 and Draft DoD Instruction 0000.00, Remote Access to Assigned Enclaves for DoD Remote Access Users with Government Furnished Mobile Devices, v1.0 (scheduled for a Sept. 2008 release). Based on the requirements found in these documents, the following Checklist sections describe conditions that apply for the use of the BlackBerry Wi-Fi Service.

3.19.1 Wi-Fi Connection to a DoD Operated Enterprise WLAN System

Connections to DoD operated Enterprise WLAN access points are authorized if the DoD WLAN system is fully compliant with the Wireless STIG. This service must be approved by the DAA and documented in the Site Security Plan (SSP). A BlackBerry Wi-Fi profile should be set up as described below. See information below for installing a device digital certificate on the BlackBerry to support EAP-TLS authentication.

3.19.2 Wi-Fi Connection to a Public Hot Spot WLAN System

Connections to public hotspots, including hotel hotspots is prohibited. Requirements listed in the draft DoD remote access policy for connections to public internet access points cannot be currently met (external device and special purpose operating system connection products are not available) and FIPS 140-2 connections are not available.

3.19.3 Wi-Fi Connection to a Home WLAN System

Connections to home WLAN systems can be used under the following conditions:

- The DAA has approved this service when cellular service is not available inside or outside the home. It is recommended that prior to the DAA granting approval, switching to an alternate cellular carrier be considered.
- The home WLAN system is configured according to DoD requirements:
 - WPA2 Personal security is implemented on the home WLAN system.
- Connection is made to the BlackBerry Mobile Network only.
 - Direct connection to the BES via an Internet connection should not be used (with or without a VPN connection).

Note: Non-VPN connections to the DoD enclave violate DoD network security requirements and the BlackBerry VPN client does not support CAC authentication.

- When a direct connection to the BES is not available, a Wi-Fi enabled BlackBerry will automatically establish an SSL connection to the BlackBerry mobile network via an Internet connection.
- The home network firewall (usually part of the wireless router) must be configured to allow an outbound TCP connection on port 443.

3.19.4 BlackBerry Wi-Fi Security Controls

BlackBerry Wi-Fi security controls are set by using WLAN IT policy rules and by setting up WLAN configuration sets that define WLAN profiles.

- A baseline WLAN IT policy should be set up for all DoD BlackBerry enterprises. WLAN IT Policy rules are used to configure WLAN configuration settings that apply to all site managed Wi-Fi enabled BlackBerry devices. If the BlackBerry VPN is required, a baseline VPN IT policy should also be set up. Required and optional configurations setting for the WLAN IT policy group and VPN IT policy group are found in table C.1.
- WLAN configuration sets should be used to set up custom BlackBerry Wi-Fi profiles for individual users or groups of users. The BlackBerry Wi-Fi profile (and the BlackBerry VPN profile, if used) should be configured on the BES and not the BlackBerry device to control the use of WLAN and VPN connections. WLAN configuration sets are used to configure WLAN configuration settings that apply to individual BlackBerry accounts. WLAN and VPN Configuration Set rules are found in Tables C.3, and C.4, respectively.
- Instructions for setting up a WLAN or VPN IT Policy rules and WLAN and VPN Configuration Sets can be found in the *BlackBerry Enterprise Server Wi-Fi Implementation Supplement*.
- When both WLAN IT Policy rules and WLAN configuration sets are used, Wi-Fi enabled BlackBerry devices will follow global WLAN rules in the WLAN IT Policy and WLAN profile settings that have been assigned to specific user account associated with the BlackBerry.

3.19.5 Instructions for Installing a BlackBerry Device Certificate

The DoD wireless policy (DoDD 8100.2) states DoD wireless LAN systems must use EAP-TLS authentication, which requires a digital certificate to be installed on the WLAN client or for a user to use CAC authentication². *BlackBerry Enterprise Server Wi-Fi Implementation Supplement* provides instructions for installing a device or supplicant private digital certificate on the BlackBerry. The BlackBerry also supports EAP-TLS via smart card based PKI authentication (i.e. CAC). The WLAN system manual should be consulted for instructions for configuring certificates on the system for new clients.

DoD sites setting up BlackBerry Wi-Fi connections should contact their local PKI support office for information on obtaining PKI certificates for their BlackBerry devices.

Note: When software certificates are used, the BlackBerry password must meet the requirements of CTO 07-15 Revision 1. See Section 3.18 and WIR1100 for more information.

² Research In Motion claims that CAC authentication with EAP-TLS is supported on the BlackBerry but this capability has not been tested by DISA.

3.19.6 BlackBerry Wi-Fi Voice over IP (VoIP)

Wi-Fi VoIP systems provide the capability to use mobile phones over a site's VoIP system. DoD Wi-Fi VoIP systems must meet the security requirements of both the Wireless STIG and the Internet Protocol Telephony and Voice Over Internet Protocol STIG. The BlackBerry Enterprise Server provides IT policy controls for setting up connections to Wi-Fi VoIP systems.

3.20 Antivirus Support on BlackBerry Devices

DoD Instruction 8500.2, Information Assurance (IA) Implementation, Feb 6, 2003, requires virus protection on mobile computing devices. In DoDI 8500.2, IA control ECVP-1 states: "All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates."

For some IT systems this requirement is met by using antivirus applications installed on the computer (e.g., IT systems with the Windows operating system). The BlackBerry Enterprise System meets the virus protection requirement of DoDI 8500.2 by a combination of IT policies, application control policies, and code signing to contain malware and control its ability to install itself on the BlackBerry device and gain access to device resources, applications, and data and access the DoD network. This Checklist includes specific BlackBerry Enterprise Server (BES) and BlackBerry device configuration requirements to ensure BlackBerry Enterprise System malware controls are implemented.

BlackBerry virus protection features have been tested by NSA and DISA and were approved by the DISN Security Accreditation Working Group (DSAWG) in 2006 as meeting DoD security requirements when the initial release of this Checklist was approved.

Additional information on BlackBerry malware protections can be found in the following RIM document: *Protecting the BlackBerry device platform against malware, BlackBerry Enterprise Server 4.0 and later*.

3.21 AutoBerry Tool

AutoBerry is a DoD developed tool that scans a BlackBerry and determines if any changes have been made to files on the device from a previous control scan (modified, deleted, or new file). Based on changes found, the tool then determines an Information Assurance (IA) threat status and provides a list of actions that should be implemented; for example, no action required, wipe BlackBerry.

AutoBerry can be downloaded from the following DoD web sites:

<https://powhatan.iiee.disa.mil/tools/autoberry/> - DoD CAC required.

www.iad.nsa.smil.mil/resources/library/tools/index.cfm.

3.22 BlackBerry Instant Messaging

BlackBerry Enterprise Server software version 4.1.5 is designed to provide support for the following instant messaging platforms:

- BlackBerry® Instant Messaging for Microsoft® Office Live Communications Server 2005 for Microsoft® Office Communicator
- BlackBerry® Instant Messaging for Microsoft Office Live Communications Server 2005 for Microsoft® Windows® Messenger
- BlackBerry® Instant Messaging for IBM® Lotus® Sametime®
- BlackBerry® Client for IBM® Lotus® Sametime®
- BlackBerry® Instant Messaging for Novell® GroupWise® Messenger

The Instant Messaging STIG provides security guidance on the use of instant messaging applications in the DoD. DoD BlackBerry devices can be used to connect to any DoD managed IM server or system that meets the requirements of the Instant Messaging STIG.

3.23 Additional BlackBerry Applications and Services

3.23.1 Documents To Go

Documents To Go is a BlackBerry application that is used to view, edit, and create Microsoft Word, Excel, and PowerPoint files and attachments on the BlackBerry smartphone.

The standard version of Documents To Go is included in the BlackBerry device software version 4.5 update. The premium version can be purchased from InTact Technology. Microsoft documents can be viewed and edited with the standard edition of Documents To Go. The premium edition is required to create documents.

There are no required DoD security controls for Documents To Go.

3.23.2 BlackBerry Mobile Voice System (MVS)

BlackBerry MVS Services are a component of the BES (version 4.1.4 and later) that provides the capability for a BlackBerry to send and receive telephone calls through the corporate telecom system.

DoD security controls have not yet been defined for BlackBerry MVS Services but are expected to be included in the next release of this checklist (sometime during the first half of CY 2009). DoD sites that are considering implementing BlackBerry MVS Services should contact DISA FSO (fso_spt@disa.mil) for guidance on required security controls.

3.23.3 BlackBerry Web Desktop Manager

BlackBerry Web Desktop Manager is a web version of BlackBerry Desktop Manager. It provides many of the same functions as BlackBerry Desktop Manager, including enabling users

to manage and configure their BlackBerry devices to receive messages and perform maintenance related tasks (for example, backup and restore, define email settings, and load new applications). Blackberry Web Desktop Manager requires the installation of the BlackBerry Administration Service either on the same computer the BES is installed on or on a separate server.

DoD security controls have not yet been defined for BlackBerry Web Desktop Manager but are expected to be included in the next release of this checklist (sometime during the first half of CY 2009). DoD sites that are considering implementing BlackBerry Web Desktop Manager should contact DISA FSO (fso_spt@disa.mil) for guidance on required security controls.

This page is intentionally left blank.

APPENDIX A. REFERENCES

A.1 Primary References

RIM frequently moves the online location of BlackBerry documents. The web links below were valid at the time of publication of this document. If a web link does not work, search for the document at <http://www.BlackBerry.com/support>.

Feature and Technical Overview, BlackBerry Enterprise Server for Microsoft Exchange, Version: 4.1 | Service Pack: 6,

<http://na.blackberry.com/eng/support/docs/subcategories/?userType=2&category=BlackBerry+Enterprise+Server+for+Microsoft+Exchange>

50

Installation Guide, BlackBerry Enterprise Server for Microsoft Exchange, Version 4.1 Service Pack 6,

<http://na.blackberry.com/eng/support/docs/subcategories/?userType=2&category=BlackBerry+Enterprise+Server+for+Microsoft+Exchange>

Placing the BlackBerry Enterprise Solution in a segmented network, BlackBerry Enterprise server version 4.0 and later,

<http://na.BlackBerry.com/eng/atalgance/security/>

Restricting Bluetooth technology on Bluetooth enabled computers, 2007 RIM document,

<http://www.BlackBerry.com/knowledgecenterpublic/livelink.exe?func=ll&objId=1371440&objAction=browse&sort=name44>

RIM Document KB13504, New features in BlackBerry Smart Card Reader 1.5.1, Aug 13, 2007, http://www.BlackBerry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB13504&sliceId=SAL_Public&dialogID=23986423&stateId=0%20%2023984672

BlackBerry Smart Card Reader Security Technical Overview, Release 1.5,

<http://na.BlackBerry.com/eng/atalgance/security/products/smartcardreader/>

BlackBerry with the S/MIME Support Package, White Paper, Version 4.2

<http://na.BlackBerry.com/eng/atalgance/security/products/smime.jsp>

Policy Reference Guide, Version 31, (for BES 4.1.6).

<http://na.BlackBerry.com/eng/atalgance/security/>

BlackBerry Enterprise Solution, Security Technical Overview, for BlackBerry Enterprise Server Version 4.1 Service Pack 5 and BlackBerry Device Software Version 4.5,

<http://na.BlackBerry.com/eng/atalgance/security/>

BlackBerry Enterprise Server Wi-Fi Implementation Supplement, 25 July 2007,
http://www.BlackBerry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8067/645045/7963/810874/1369381/Wi-Fi_Implementation_Supplement.pdf?nodeid=1369382&vernum=0

Protecting the BlackBerry device platform against malware, BlackBerry Enterprise server 4.0 and later, <http://www.blackberry.com/security>

BlackBerry Enterprise Server Resource Kit, version 4.1 Service Pack 5, User Guide for the BlackBerry Analysis, Monitoring, and Troubleshooting Tools,
<http://na.BlackBerry.com/eng/support/docs/subcategories/?userType=2&category=BlackBerry+Enterprise+Server+Resource+Kit>

A.2 Additional References

Preliminary Security Evaluation of RIM's BlackBerry-to-Smart Card Reader Bluetooth Interface, Headquarters Army Materiel Command (AMC) Report, 7 April 2006 (FOUO).

Technical Evaluation of RIM's Smart Card Reader, BlackBerry Bluetooth Support, and Bluetooth Headsets; NSA; I332-013R-2006 ; 12 May 2006 (SECRET).

DoD Directive 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2004.

ASD-NII Memorandum, Subject: Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies in the Department Defense (DoD) Global Information Grid (GIG), 2 June 2006.

Draft DoD Instruction 0000.00, Remote Access to Assigned Enclaves for DoD Remote Access Users with Government Furnished Mobile Devices, V1.0.

This page is intentionally left blank.

APPENDIX B. BLACKBERRY DISPOSAL PROCEDURES

Detailed Procedures for Sanitizing DoD BlackBerry Devices Prior to Disposal³

1. Load the default or generic BlackBerry IT Policy on the BlackBerry.
 - a. Wipe the old IT Policy from the registry on the desktop by performing the **Desktop Registry Clear Procedure**.
 - b. Obtain a generic policy.bin file (One example can be found here: (<http://voicecareaustralia.com.au/dumpster/BlackBerry/files/policy.bin>)).
 - c. Place the downloaded file in the following directory on the desktop computer used to load software on the BlackBerry (computer where **BlackBerry Desktop Manager** is loaded): **C:\Program Files\Research In Motion\BlackBerry**.
 - d. Sync the BlackBerry device with the Desktop Manager – the existing IT Policy will now be erased from the device.
2. Obtain and install Javaloader.exe on the computer where **BlackBerry Desktop Manager** is loaded (can be found at <http://www.BlackBerry.com/developers/downloads/jde/index.shtml> - installs as part of the JDE – javaloader.exe is a DOS application).
3. Wipe contents of the BlackBerry device:
 - a. Connect BlackBerry device to USB cable/computer and run “**javaloader –usb wipe**” command from DOS prompt. This will completely erase the contents of the BlackBerry device.
 - b. Allow device to reset (will not be functional at this point).

Desktop Registry Clear Procedure

1. Go to Start button, select run, then type **regedit**
2. Find the following registry key: **HKEY_Current_Users\Software\Research In Motion\BlackBerry\PolicyManager**
3. **Right-click** the above registry key and select **New ->String Value**
4. **Type** the word **Path** in the value field
5. **Double-click** the **Path** key from above and enter the following in the Value data field: **C:\Program Files\Research In Motion\BlackBerry\policy.bin**
6. Close **regedit**

³ This procedure assumes no classified information is on the BlackBerry. This procedure should not be used for sanitizing BlackBerrys after a Classified Message incident (CMI).

This page is intentionally left blank.

APPENDIX C. BES IT POLICY RULES AND CONFIGURATION SETS

C.1 BES IT POLICY RULES

NOTE: Not all IT Policy rules listed in this table are available for all versions of BES software 4.0 – 4.1.6 and Handheld software versions 4.0 – 4.7. See *Policy Reference Guide, BlackBerry Enterprise Server, Version: 4.1 | Service Pack: 6 (Document Version 31)* and *BlackBerry Enterprise Server, Wi-Fi Implementation Supplement* for more information.

Note: In the table below, “Required” IT Policy rule settings must be implemented by all DoD BlackBerry systems. “Optional” IT Policy rule settings are recommended settings and may be changed to meet mission requirements.

Note: The number in parenthesis found in the Comments column for each IT Policy rule refers to the BES version the rule was initially released in. IT Policy Rules without BES release versions were released prior to BES 4.1.3

Note: *Policy Reference Guide, BlackBerry Enterprise Server, Version: 4.1 | Service Pack: 6 (Document Version 31)* and *BlackBerry Enterprise Server, Wi-Fi Implementation Supplement* provide detailed descriptions of each BlackBerry IT policy group and rule. These documents list BES IT policy groups and rules in alphabetical order. The IT Policy manager in the BES lists IT policy groups and rules in random order. At the request of DoD BlackBerry Administrators, Table C.1 has been reorganized and now lists BlackBerry IT policy groups and rules in the order found in the BES IT Policy Manager to make it easier to use the table when configuring the BES for STIG compliance. Table C.2 lists all Blackberry IT policy groups and rules in alphabetical order and provides a cross reference to the location of a specific rule in Table C.1.

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
Device-Only Items								
1.1	Password Required	Device-Only	TRUE			I	WIR1100	

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
1.2	Allow Peer-to-Peer Messages	Device-Only		TRUE	If Peer-to-Peer messaging (e.g., Pin-to-Pin messaging) allowed, than "Disable Peer-to-Peer Normal Send" must be set to "TRUE" to require S/MIME encrypted Peer-to-Peer messaging	III	WIR1220	

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
1.6	Maximum Password Age	Device-Only	90 days or less		Set to 0 only if CAC authentication is enabled for device unlock	III	WIR1100	
1.7	User Can Change Timeout	Device-Only	FALSE			III	WIR1250	
1.8	Password Pattern Checks	Device-Only	-Choose any selection EXCEPT "No Restriction" and <blank> -Choose any available selection -Choose "3" -Choose "0" or <blank>		If password length of 5 is used. If password length of 6 or more is used (except as noted for software certificates) If software certificates are used on the BlackBerry When implementing CAC authentication for BlackBerry unlock.	I	WIR1100	
1.9	Enable Long Term Timeout	Device-Only	TRUE			III	WIR1250	
1.10	Allow SMS	Device-Only		FALSE	If set to TRUE, IA Awareness training must include SMS/MMS security issues.			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
1.11	Allow BCC Recipients	Device-Only		TRUE				
1.12	Home Page Address	Device-Only		<blank>	Default setting. (4.1.5)			
1.13	Home Page Address is Read-Only	Device-Only		<blank>	Default setting.			
1.14	Enable WAP Config	Device-Only		FALSE	TRUE only if operational requirement			
1.15	Default Browser Config UID	Device-Only		<blank>	Default setting			
Desktop-Only Items								
2.1	Message Prompt	Desktop-Only		<blank>	Default setting			
2.2	Show Application Loader	Desktop-Only	FALSE			II	WIR1180	
2.3	Force Load Count	Desktop-Only	1		Requires software update to be installed.	III	WIR1250	
2.4	Synchronize Messages Instead Of Importing	Desktop-Only		TRUE	Default setting			
2.5	Message Conflict Mailbox Wins	Desktop-Only		TRUE	Default setting			
2.6	Disable Wireless Calendar	Desktop-Only		FALSE	Default setting			
2.7	Auto Backup Enabled	Desktop-Only		FALSE	Default setting			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
2.8	Auto Backup Frequency	Desktop-Only		7	Default setting			
2.9	Auto Backup Include All	Desktop-Only		TRUE	Default setting			
2.10	Auto Backup Exclude Messages	Desktop-Only		FALSE	Default setting			
2.11	Auto Backup Exclude Synchronization	Desktop-Only		FALSE	Default setting			
2.12	Show Web Link	Desktop-Only		FALSE	Default setting			
2.13	Web Link URL	Desktop-Only		<blank>	Default setting			
2.14	Web Link Label	Desktop-Only		<blank>	Default setting			
2.15	Forward Messages In Cradle	Desktop-Only		TRUE	Default setting			
2.16	Do Not Save Sent Messages	Desktop-Only		FALSE				
2.17	Force Load Message	Desktop-Only	Add notification message. See comments for example.		“BlackBerry device handheld software update is available. Update required by DoD policy.”	III	WIR1250	
Global Items								
3.1	Allow Phone	Global		TRUE	Default setting			
3.2	Allow Browser	Global		TRUE	Default setting.			
Common policy group								

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
4.1	Lock Owner Info	Common	Select to 1 (Lock Information text) or 3 (Lock both Name and Information text)			III	WIR0012	
4.2	IT Policy Notification	Common	TRUE			III	WIR1250	
4.3	Confirm On Send	Common		<blank>	Factory default setting.			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
4.4	Set Owner Info	Common	Follow guidance in comment		DoD CIO Memorandum "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," dated 2 Nov 2007 requires the following message be displayed: "I've read & consent to terms in IS user agreement." DoD BlackBerry sites should consider adding the following optional message: "If this BlackBerry is found, please call the following phone number xxx-xxx-xxxx." When called, the phone number should not identify itself as a DoD organization.	III	WIR0012	

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
4.5	Set Owner Name	Common	Leave blank or follow guidance in comment		DoD BlackBerry sites should consider using the following message: "If this BlackBerry is found, please call the following phone number xxx-xxx-xxxx." When called, the phone number should not identify itself as a DoD organization.	III	WIR1250	
4.6	Disable MMS	Common	TRUE			III	WIR1220	
4.7	Disable Voice-Activated Dialing	Common		FALSE				
4.8	Disable Kodiak PTT	Common		FALSE				
4.9	Disable Voice Note Recording			FALSE	Factory default setting. (4.1.5)			
Password policy group								
5.1	Set Password Timeout	Password	15			II	WIR1100	
5.2	Set Maximum Password Attempts	Password	10 (or less)		Default setting	I	WIR1100	
5.3	Suppress Password Echo	Password	TRUE		Default setting	III	WIR1100	

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
5.4	Maximum Password History	Password	3 or more			III	WIR1100	
5.5	Duress Notification Address	Password		<blank>	Default setting			
5.6	Periodic Challenge Time	Password		60	Default setting. Note: When 'Enable Long Term Timeout' is set to TRUE, this rule will be automatically set to 60.			
5.7	Forbidden Passwords	Password	List forbidden passwords based on local security policies		For example: "password"	III	WIR1100	
Email Messaging policy group								
6.1	Enable Wireless Message Reconciliation	Email Messaging		TRUE	Default setting.			
6.2	Attachment Viewing	Email Messaging		TRUE	Default setting.			
6.3	Prepend Disclaimer	Email Messaging		<blank>	Default setting.			
6.4	Keep Message Duration	Email Messaging		-1	Default setting.			
6.5	Keep Saved Message Duration	Email Messaging		-1	Default setting.			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
6.6	Maximum Native Attachment MTH total attachment size	Email Messaging		<blank>	Default setting.			
6.7	Maximum Native Attachment MTH attachment size	Email Messaging		<blank>	Default setting. (4.1.5)			
6.8	Allow Auto Attachment Download	Email Messaging		FALSE	Default setting.			
6.9	Disable Notes Native Encryption Forward and Reply	Email Messaging		TRUE				
6.10	Notes Native Encryption Password Timeout	Email Messaging		<blank>	Default setting. (4.1.5)			
6.11	Maximum Native Attachment MTH attachment size	Email Messaging		<blank>	Default setting.			
6.12	Disable Rich Content Email	Email Messaging		FALSE	Default setting. (4.1.5)			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
6.13	Inline Content Requests	Email Messaging		Manual Only	(4.1.5)			
6.14	Disable Manual Download of External Images	Email Messaging		FALSE	Default setting. (4.1.5)			
6.15	Disable Form Submission	Email Messaging		FALSE	Default setting. (4.1.5)			
Security policy group								
7.1	Lock on Smart Card Removal	Security		FALSE	Default setting			
7.2	Force Smart Card Two Factor Authentication	Security		FALSE TRUE	Default setting. When implementing CAC authentication for BlackBerry unlock.			
7.3	Disable Untrusted Certificate Use	Security		FALSE	Default setting			
7.4	Disable Revoked Certificate Use	Security	TRUE			III	WIR1200	
7.5	Disable Message Normal Send	Security		FALSE	Default setting Set to TRUE only if S/MIME messaging is required for all email messages (forces users to send signed and/or encrypted S/MIME messages)			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
7.6	Disable Peer-to-Peer Normal Send	Security	TRUE		Forces S/MIME encryption for Peer-to-Peer messages when "Allow Peer-to-Peer Message" set to "TRUE"	III	WIR1220	
7.7	Disable Key Store Low Security	Security	TRUE		This rule is labeled "Disable Security Data Low Security" in the BES	III	WIR1200	
7.8	Key Store Password Maximum Timeout	Security	60 or less (15 is the recommended setting)		Do not select 0	III	WIR1250	
7.9	Certificate Status Cache Timeout	Security	7			III	WIR1200	
7.10	Disallow Third Party Downloads	Security	TRUE			I	WIR1180	
7.11	Force Lock When Holstered	Security		TRUE				
7.12	Allow Third Party Apps Use Serial Port	Security		FALSE	Use TRUE if third-party applications are allowed and serial port access required by approved applications			
7.13	Content Protection Strength	Security	Stronger or Strongest			III	WIR1280	

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
7.14	Allow Internal Connections	Security		TRUE	Default setting			
7.15	Allow External Connections	Security		FALSE	Change to True only if approved applications require external connections			
7.16	Allow Split-Pipe Connections	Security	FALSE		Default setting	II	WIR1250	
7.17	Disable Invalid Certificate Use	Security	TRUE			III	WIR1200	
7.18	Disable Weak Certificate Use	Security	TRUE			III	WIR1200	
7.19	Trusted Certificate Thumbprints	Security		<blank>	Default setting			
7.20	Disable Key Store Backup	Security		FALSE	Default setting			
7.21	Certificate Status Maximum Expiry Time	Security	168 or less			III	WIR1200	
7.22	Disable Stale Status Use	Security		FALSE	Default setting			
7.23	Disable Cut/ Copy/ Paste	Security		FALSE	Default setting			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
7.24	Disable Radio When Cradled	Security		2 - Radio disabled when the connected USB device enumerates 0 - Radio not disabled when USB device is connected	Forces radio to turn off when BlackBerry is connected to a PC but allows radio to be on when connected to a travel charger. Use this setting when IP modem is used.			
7.25	Disable Forwarding Between Services	Security		FALSE	Default setting			
7.26	FIPS Level	Security	1 (FIPS 140-2 Level 1)		Default setting. This rule applies only to BlackBerry Software versions 4.0.0 through 4.2.1	I	WIR1250	
7.27	Allow Outgoing Call When Locked	Security		FALSE	Default setting			
7.28	Disable Unverified CRLs	Security	TRUE			III	WIR1200	

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
7.29	Security Service Colors	Security		<blank>	Default setting. Site can choose message background colors.			
7.30	Disable 3DES Transport Crypto	Security		TRUE	Forces AES encryption			
7.31	Disable Persisted Plaintext	Security		FALSE	Default setting			
7.32	Minimal Signing Key Store Security Level	Security	Medium Security or High Security		Default setting	III	WIR1250	
7.33	Minimal Encryption Key Store Security Level	Security	Medium Security or High Security		Default setting	III	WIR1250	
7.34	Desktop Backup	Security		0 (All BlackBerry device databases)	Default setting			
7.35	Disable Unverified Certificate Use	Security		FALSE	Default setting			
7.36	Disable IP Modem	Security		FALSE	Default setting			
7.37	Allow Smart Card Password Caching	Security		FALSE	Default setting			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
7.38	Disable GPS	Security		FALSE	Default setting (4.1.5)			
7.39	Force Content Protection of Master Keys	Security	TRUE			I	WIR1250	
7.40	Force LED Blinking When Microphone Is On	Security	TRUE			III	WIR1250	
7.41	Force Include Address Book In Content Protection	Security	TRUE			III	WIR1280	
7.42	Message Classification	Security		(No items)	Default setting. Sites should consider using Unclassified, Sensitive But Unclassified (SBU), Personal Identifiable Information (PII), etc.			
7.43	Disable Stale Certificate Status Checks	Security		FALSE	Default setting			
7.44	Disable External Memory	Security		TRUE	Select FALSE if external memory cards allowed			
7.45	Disable USB Mass Storage	Security		TRUE				

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
7.46	External File System Encryption Level	Security	4 - Encrypt to Device Key (including multi-media directories)			III	WIR1280	
7.47	Disable Media Manager FTP Access	Security		FALSE	Default setting			
7.48	Disable Smart Password Entry	Security		FALSE	Default setting			
7.49	Force Smart Card Two Factor Challenge Response	Security		FALSE	Default setting			
7.50	Secure Wipe if Battery Low	Security		FALSE	Default setting			
7.51	Secure Wipe Delay After Lock	Security		<blank>	Default setting			
7.52	Secure Wipe Delay After IT Policy Received	Security		<blank>	Default setting			
7.53	Firewall Block Incoming Messages	Security	MMS Messages	SMS Messages		III	WIR1220	
7.54	Required Password Pattern	Security		<blank> Use N, n, or #	Default setting When implementing CAC authentication for BlackBerry unlock.			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
7.55	Require Secure APB Messages	Security		FALSE	Default setting			
7.56	Password Required for Application Download	Security	TRUE		(4.1.4)	III	WIR1250	
7.57	Allow Resetting of Idle Timer	Security	FALSE		(4.1.4)	II	WIR1250	
7.58	Remote Wipe Reset to Factory Defaults	Security	TRUE		If a finding, mark either WIR1090 or WIR1100 (4.1.4)	II	WIR1090 or WIR1100	
7.59	Allow Screen Shot Capture	Security		TRUE	(4.1.4)			
7.60	Disable Public Photo Sharing Applications	Security	TRUE		(4.1.4)	III	WIR1250	
7.61	Disable Geo-Tagging of Photos	Security		FALSE	Default setting (4.1.4)			
7.62	Message Classification Title	Security		<blank>	Default setting. (4.1.4)			
7.63	Firewall Whitelist Addresses	Security		<blank>	Based on site policy, site can specify a list of allowed email addresses or domains. (4.1.5)			
7.64	Weak Digest Algorithms	Security		<blank>	Default setting. (4.1.5)			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
7.65	Maximum Smart Card User Authentication Certificate Status Check Period	Security		<blank>	Default Setting. (4.1.5)			
7.66	Security Transcoder Cod File Hashes	Security	<blank>		Default setting. (4.1.5)	III	WIR1250	
7.67	Disable Public Social Networking Applications	Security	TRUE		(4.1.5)	III	WIR1250	
S/MIME Application policy group								
8.1	S/MIME Minimum Strong RSA Key Length	S/MIME Application	1024		Default setting	III	WIR1200	
8.2	S/MIME Minimum Strong DH Key Length	S/MIME Application	1024		Default setting	III	WIR1200	
8.3	S/MIME Minimum Strong ECC Key Length	S/MIME Application	163		Default setting	III	WIR1200	
8.4	S/MIME Force Digital Signature	S/MIME Application		FALSE	Default setting. Set to TRUE based on local policy.			
8.5	S/MIME Force Encrypted Messages	S/MIME Application		FALSE	Default setting			
8.6	S/MIME Force Smartcard Use	S/MIME Application		TRUE	When smart card capability is available			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
8.7	S/MIME Blind Copy Address	S/MIME Application		<blank>	Default setting.			
8.8	S/MIME Allowed Content Ciphers	S/MIME Application	0 (AES-256 bit) 1 (AES-192 bit) 2 (AES-128 bit)			III	WIR1200	
8.9	S/MIME Minimum Strong DSA Key Length	S/MIME Application	1024		Default setting	III	WIR1200	
8.10	Entrust Messaging Server (EMS) Email Address	S/MIME Application	<blank>		Default setting	III	WIR1200	
8.11	S/MIME Allowed Encrypted Attachment Mode	S/MIME Application		Automatic	Default setting. (4.1.5)			
8.12	S/MIME Allowed Encryption Types	S/MIME Application	Certificate based-only		(4.1.6)	III	WIR1200	
PGP policy group								
9.1	All Policy Group Rules	PGP			Set at default value. DoD does not use PGP encryption.			
Memory Cleaner policy group								

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
10.1	Memory Cleaner Maximum Idle Time	Memory Cleaner		20				
10.2	Force Memory Clean When Idle	Memory Cleaner		TRUE				
10.3	Force Memory Clean When Holstered	Memory Cleaner		TRUE				
TLS Application policy group								
11.1	TLS Disable Weak Ciphers	TLS		2 (prompt user on the BlackBerry device)	Default setting			
11.2	TLS Disable Untrusted Connection	TLS		2 (prompt user on the BlackBerry device)	Default setting			
11.3	TLS Minimum Strong RSA Key Length	TLS		1024	Default setting			
11.4	TLS Minimum Strong DH Key Length	TLS		1024	Default setting			
11.5	TLS Minimum Strong ECC Key Length	TLS		163	Default setting			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
11.6	TLS Disable Invalid Connection	TLS		2 (prompt user on the BlackBerry device)	Default setting			
11.7	TLS Restrict FIPS Ciphers	TLS	TRUE			III	WIR1250	
11.8	TLS Minimum Strong DSA Key Length	TLS		1024	Default setting			
11.9	TLS Device Side Only	TLS		FALSE	Default setting. Set to TRUE only if device-side TLS is available			
WTLS Application policy group								
12.1	WTLS Disable Weak Ciphers	WTLS		2 (prompt user on the BlackBerry device)	Default setting			
12.2	WTLS Disable Untrusted connection	WTLS		2 (prompt user on the BlackBerry device)	Default setting			
12.3	WTLS Minimum Strong RSA Key Length	WTLS		1024	Default setting			
12.4	WTLS Minimum Strong DH Key Length	WTLS		1024	Default setting			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
12.5	WTLS Minimum Strong ECC Key Length	WTLS		163	Default setting			
12.6	WTLS Disable Invalid Connection	WTLS		2 (prompt user on the BlackBerry device)	Default setting			
12.7	WTLS Restrict FIPS Ciphers	WTLS	TRUE		Default setting	III	WIR1250	
Browser policy group								
13.1	MDS Browser Title	Browser		BlackBerry Browser	Default setting. Use default or specify a name			
13.2	Disable Java Script in Browser	Browser		FALSE	Default setting			
13.3	Allow IBS Browser	Browser	FALSE			III	WIR1240	
13.4	MDS Browser JavaScript Enabled	Browser		FALSE	Default setting			
13.5	MDS Browser Style Sheets Enabled	Browser		FALSE	Default setting			
13.6	MDS Browser HTML Tables Enabled	Browser		FALSE	Default setting			
13.7	MDS Browser BSM Enabled	Browser		TRUE	Default setting			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
13.8	Download Images URL	Browser		<blank>	Default setting			
13.9	Download Themes URL	Browser		<blank>	Default setting			
13.10	Download Tunes URL	Browser		<blank>	Default setting			
13.11	Disable Auto Synchronization in Browser	Browser		FALSE	Default setting			
13.12	MDS Browser Use Separate Icon	Browser		TRUE				
13.13	MDS Browser Domains	Browser		<blank>	Default setting			
13.14	Allow Application Download Services	Browser	FALSE		(4.1.5)	III	WIR1250	
13.15	Allow Hotspot Browser	Browser	Disallow		(4.1.6)	III	WIR1240	
SIM Application Toolkit policy group								
14.1	Disable SIM Call Control	SIM Application Toolkit		TRUE				
14.2	Disable Network Location Query	SIM Application Toolkit		TRUE				
14.3	Disable SIM Originated Calls	SIM Application Toolkit		TRUE				

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
TCP Toolkit policy group								
15.1	TCP APN	TCP		<blank>	Default setting. Set if using TCP APN			
15.2	TCP Username	TCP		<blank>	Default setting. Set if using TCP APN			
15.3	TCP Password	TCP		<blank>	Default setting. Set if using TCP APN			
PIM Synchronization policy group								
16.1	Disable All Wireless Synchronization	PIM Synchronization		FALSE	Default setting			
16.2	Disable Address Wireless Synchronization	PIM Synchronization		FALSE	Default setting			
16.3	Disable Calendar Wireless Synchronization	PIM Synchronization		FALSE	Default setting			
16.4	Disable Memopad Wireless Synchronization	PIM Synchronization		FALSE	Default setting			
16.5	Disable Task Wireless Synchronization	PIM Synchronization		FALSE	Default setting			
16.6	Disable Wireless Bulk Loads	PIM Synchronization		FALSE	Default setting			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
16.7	Disable PIN Messages Wireless Synchronization	PIM Synchronization		TRUE	Default setting			
16.8	Disable SMS Messages Wireless Synchronization	PIM Synchronization		TRUE	Default setting			
16.9	Disable Phone Call Log Wireless Synchronization	PIM Synchronization		FALSE	Default setting			
16.10	Disable Enterprise Activation Progress	PIM Synchronization		TRUE	Default setting			
Bluetooth policy group								
17.1	Disable Bluetooth	Bluetooth	TRUE, FALSE		Set to FALSE when using Bluetooth Smart Card Reader, otherwise, setting should be TRUE	II	WIR1140	
17.2	Disable Pairing	Bluetooth	TRUE, FALSE		Set to FALSE for users in IT policy group with Bluetooth Smart Card Reader. Set to TRUE for users in IT policy group without Bluetooth SCR.	II	WIR1140	

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
17.3	Disable Headset Profile	Bluetooth	TRUE			II	WIR1140	
17.4	Disable Handsfree Profile	Bluetooth	TRUE			II	WIR1140	
17.5	Disable Serial Port Profile	Bluetooth	TRUE, FALSE		Set to FALSE for users in IT policy group with Bluetooth Smart Card Reader. Set to TRUE for users in IT policy group without Bluetooth SCR.	II	WIR1140	
17.6	Disable Discoverable Mode	Bluetooth	TRUE			II	WIR1140	
17.7	Allow Outgoing Calls	Bluetooth	Only when unlocked			III	WIR1250	
17.8	Disable Address Book Transfer	Bluetooth	TRUE			III	WIR1140	
17.9	Disable Desktop Connectivity	Bluetooth	TRUE		Default setting	III	WIR1140	
17.10	Disable Wireless Bypass	Bluetooth	TRUE		Default setting.	II	WIR1140	
17.11	Require Password for Enabling Bluetooth Support	Bluetooth	FALSE		Default setting. Rule must be set to FALSE for SCR operation.	III	WIR1140	

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
17.12	Require Password for Discoverable Mode	Bluetooth	TRUE			III	WIR1140	
17.13	Require Encryption	Bluetooth	TRUE			II	WIR1140	
17.14	Disable File Transfer	Bluetooth	TRUE			II	WIR1140	
17.15	Require LED Connection Indicator	Bluetooth	TRUE			III	WIR1140	
17.16	Disable Dial-Up Networking	Bluetooth	TRUE			II	WIR1140	
17.17	Force CHAP Authentication Bluetooth Link	Bluetooth	FALSE		Default setting. (4.1.4)	II	WIR1140	
17.18	Disable Advanced Audio Distribution Profile	Bluetooth	TRUE		(4.1.4)	II	WIR1140	
17.19	Disable Audio/Video Remote Control Profile	Bluetooth	TRUE		(4.1.4)	II	WIR1140	
17.20	Minimum Encryption Key Length	Bluetooth		<blank>	Default setting. (4.1.5)			
17.21	Limit Discoverable Time	Bluetooth	FALSE		Default setting. (4.1.5)	III	WIR1140	

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
17.22	Disable SIM Access Profile	Bluetooth	TRUE		Default setting. (4.1.6)	II	WIR1140	
VoIP policy group								
18.1	Allow VoIP	VoIP		FALSE				
18.2	VoIP Allow BlackBerry Device Changes	VoIP		FALSE	(4.1.5)			
18.3	SIP Realm	VoIP		<blank>	Default setting. (4.1.5)			
18.4	SIP User ID	VoIP		<blank>	Default setting. (4.1.5)			
18.5	SIP User Password	VoIP		<blank>	Default setting. (4.1.5)			
18.6	SIP Server Type	VoIP		<blank>	Default setting. (4.1.5)			
18.7	SIP Server Name	VoIP		<blank>	Default setting. (4.1.5)			
18.8	SIP Server Port	VoIP		<blank>	Default setting. (4.1.5)			
18.9	SIP User Display Name	VoIP		<blank>	Default setting. (4.1.5)			
18.10	SIP Domain	VoIP		<blank>	Default setting. (4.1.5)			
18.11	SIP Server Transport	VoIP		<blank>	Default setting. (4.1.5)			
18.12	SIP Registration Timeout	VoIP		<blank>	Default setting. (4.1.5)			
18.13	SIP RTP Media Port	VoIP		<blank>	Default setting. (4.1.5)			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
18.14	SIP Local Port	VoIP		<blank>	Default setting. (4.1.5)			
18.15	SIP Authentication ID	VoIP		<blank>	Default setting. (4.1.5)			
18.16	VoIP Emergency Number	VoIP		<blank>	Default setting. (4.1.5)			
18.17	VoIP Enable Call Hold	VoIP		<blank>	Default setting. (4.1.5)			
18.18	VoIP Enable Unattended Call Hold	VoIP		<blank>	Default setting. (4.1.5)			
18.19	VoIP Enable Attended Call Transfer	VoIP		<blank>	Default setting. (4.1.5)			
18.20	Disable VoIP User Profiles	VoIP		<blank>	Default setting. (4.1.5)			
Smart Dialing policy group								
19.1	Enable Smart Dialing Policy	Smart Dialing		FALSE				
19.2	Smart Dialing Allow Device Changes	Smart Dialing		FALSE				
19.3	Set Local Country Code	Smart Dialing		<blank>	Default setting			
19.4	Set Local Area Code	Smart Dialing		<blank>	Default setting			
19.5	Set National Number Length	Smart Dialing		<blank>	Default setting			
VPN policy group								

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
20.1	Enable VPN	VPN		FALSE	Default setting (4.1.3)			
20.2	VPN Allow Handheld Changes	VPN		TRUE	Default setting (4.1.3)			
20.3	VPN Vendor Type	VPN		<blank>	Default setting (4.1.3)			
20.4	VPN Gateway Address	VPN		<blank>	Default setting (4.1.3)			
20.5	VPN Group Name	VPN		<blank>	Default setting (4.1.3)			
20.6	VPN Group Password	VPN		<blank>	Default setting (4.1.3)			
20.7	VPN User Name	VPN		<blank>	Default setting (4.1.3)			
20.8	VPN User Password	VPN		<blank>	Default setting (4.1.3)			
20.9	VPN DNS Configuration	VPN		TRUE	Default setting (4.1.3)			
20.10	VPN Primary DNS	VPN		<blank>	Default setting (4.1.3)			
20.11	VPN Secondary DNS	VPN		<blank>	Default setting (4.1.3)			
20.12	VPN Domain Name	VPN		<blank>	Default setting (4.1.3)			
20.13	Use VPN Xauth Certificates	VPN		FALSE	Default setting (4.1.3)			
20.14	VPN Xauth Type	VPN		<blank>	Default setting (4.1.3)			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
20.15	VPN IKE DH Group	VPN		Group 7	Default setting (4.1.3)			
20.16	VPN IKE Cipher	VPN		<blank>	Default setting (4.1.3)			
20.17	VPN IKE Hash	VPN		<blank>	Default setting (4.1.3)			
20.18	VPN PFS	VPN		TRUE	Default setting (4.1.3)			
20.19	VPN IPSEC Cipher and Hash	VPN		SHA1 Hash and AES128 Cipher	Default setting (4.1.3)			
20.20	VPN Allow Password Save	VPN		TRUE	Default setting (4.1.3)			
20.21	VPN NAT Keep Alive	VPN		1	Default setting (4.1.3)			
20.22	VPN Password Hidden on Input	VPN		FALSE	Default setting (4.1.3)			
20.23	VPN Disable Prompt for Credentials Re-Entry	VPN		FALSE	Default setting (4.1.3)			
20.24	Disable VPN User Profiles	VPN		FALSE	Default setting (4.1.3)			
20.25	VPN Minimal Certificate Encryption Key Security Level	VPN		1 (Low Security)	Default setting (4.1.3)			
WLAN policy group								

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
21.1	WLAN Allow Handheld Changes	WLAN	FALSE		(4.1.3)	III	WIR1230	
21.2	WLAN Link Security	WLAN	EAP-TLS		(4.1.3)	III	WIR1230	
21.3	WLAN SSID	WLAN		Type in the SSID of approved WLAN systems	Default setting (4.1.3)			
21.4	WLAN Default Key ID	WLAN		1	Default setting (4.1.3)			
21.5	WLAN WEP Key 0	WLAN		<blank>	Default setting (4.1.3)			
21.6	WLAN WEP Key 1	WLAN		<blank>	Default setting (4.1.3)			
21.7	WLAN WEP Key 2	WLAN		<blank>	Default setting (4.1.3)			
21.8	WLAN WEP Key 3	WLAN		<blank>	Default setting (4.1.3)			
21.9	WLAN Preshared Key	WLAN		<blank>	Default setting (4.1.3)			
21.10	WLAN User Name	WLAN		<blank>	Default setting (4.1.3)			
21.11	WLAN User Password	WLAN		<blank>	Default setting (4.1.3)			
21.12	WLAN DHCP Configuration	WLAN		TRUE	Default setting (4.1.3)			
21.13	WLAN IP Address	WLAN		<blank>	Default setting (4.1.3)			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
21.14	WLAN Subnet Mask	WLAN		<blank>	Default setting (4.1.3)			
21.15	WLAN Primary DNS	WLAN		<blank>	Default setting (4.1.3)			
21.16	WLAN Secondary DNS	WLAN		<blank>	Default setting (4.1.3)			
21.17	WLAN Default Gateway	WLAN		<blank>	Default setting (4.1.3)			
21.18	WLAN Minimal EAP-TLS Certificate Encryption Key Security Level	WLAN	2 or 3 (Medium or High Security)		This rule is obsolete in BES 4.1.4 and later (4.1.3)	III	WIR1230	
21.19	WLAN Enable Authentication Page	WLAN		FALSE	Default setting (4.1.3)			
21.20	Disable WLAN	WLAN	FALSE or TRUE		Most DoD sites should set to FALSE. Set to TRUE if DAA has approved the use of WLAN services with BlackBerry devices (see WIR1230 for more information) (4.1.3)	III	WIR1230	
21.21	WLAN Password Hidden on Input	WLAN		FALSE	Default setting (4.1.3)			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
21.22	Disable WAN-Only Mode	WLAN		FALSE	Default setting (4.1.3)			
21.23	Disable WAN-Preferred mode	WLAN		FALSE	Default setting (4.1.3)			
21.24	Disable GAN-Only Mode	WLAN		FALSE	Default setting (4.1.3)			
21.25	Disable GAN-Preferred Mode	WLAN		FALSE	Default setting (4.1.3)			
21.26	Disable GAN Selection Mode Editing	WLAN		FALSE	Default setting (4.1.3)			
21.27	WLAN Disable Prompt for Credentials Re-entry	WLAN		FALSE	Default setting (4.1.3)			
21.28	Disable WLAN User profiles	WLAN		FALSE	(4.1.3)			
21.29	GAN WLAN Threshold	WLAN		<blank>	Default setting (4.1.3)			
21.30	GAN WLAN Threshold	WLAN		<blank>	Default setting (4.1.3)			
21.31	GAN Signal Strength threshold	WLAN		<blank>	Default setting (4.1.3)			
21.32	GAN Signal Quality Threshold	WLAN		<blank>	Default setting (4.1.3)			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
21.33	Disable WLAN Access to BES	WLAN		TRUE	Disables access to BES from DoD WLAN network			
				FALSE	To allow access to BES from DoD WLAN (4.1.3)			
AMS policy group								
22.1	AMS AG Registration URL	AMS		<blank>	Default setting. (4.1.5)			
22.2	AMS AG Messaging URL	AMS		<blank>	Default setting. (4.1.5)			
On-Device Help policy group								
23.1	On-Device Help Links	On-Device help		<blank>	Default setting			
23.2	On-Device Help Group Label	On-Device help		<blank>	Default setting			
BlackBerry Smart Card Reader policy group								
24.1	Maximum Connection Heart Beat Period	BlackBerry Smart Card Reader		<blank>	Default setting. If set to 1, 2, or 5 seconds, battery performance decreases.			
24.2	Maximum BlackBerry Disconnected Timeout	BlackBerry Smart Card Reader		<blank>	Default setting.			
24.3	Maximum BlackBerry Long Term Timeout	BlackBerry Smart Card Reader		<blank>	Default setting.			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
24.4	Maximum BlackBerry Bluetooth Traffic Inactivity Timeout	BlackBerry Smart Card Reader		<blank>	Default setting.			
24.5	Maximum Smart Card Not Present Timeout	BlackBerry Smart Card Reader		<blank>	Default setting			
24.6	Maximum Number of BlackBerry Transactions	BlackBerry Smart Card Reader		<blank>	Default setting			
24.7	Maximum Bluetooth Range	BlackBerry Smart Card Reader	50% or less			III	WIR1150	
24.8	Maximum PC Disconnect Timeout	BlackBerry Smart Card Reader	0 <blank>		Use this setting for BlackBerry Account groups where BlackBerry SCR is not allowed to connect to a PC Default setting. Use this setting for BlackBerry Account groups where BlackBerry SCR is allowed to connect to a PC	II	WIR1150	

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
24.14	Maximum Bluetooth Encryption Key Regeneration Period	BlackBerry Smart Card Reader		<blank>	Default setting (4.1.4)			
24.15	Force Erase Key on PC Standby	BlackBerry Smart Card Reader		FALSE	Default setting	III	WIR1150	
24.16	Disable Auto Reconnect To BlackBerry Smart Card Reader	BlackBerry Smart Card Reader		Check "Disable Auto Reconnect On BlackBerry" Check "Disable Auto Reconnect PC"	(4.1.4)			
BlackBerry MDS Integration Service policy group								
25.1	Disable MDS Runtime	BlackBerry MDS Integration Service		FALSE	Default setting			
25.2	Lowest BlackBerry MDS Integration Service Security Version Allowed	BlackBerry MDS Integration Service		2				

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
25.3	Verify BlackBerry MDS Integration Service Certificate	BlackBerry MDS Integration Service	TRUE		Default setting	II	WIR1250	
25.4	Disable Activation With Public BlackBerry MDS Integration Service	BlackBerry MDS Integration Service	TRUE			II	WIR1250	
25.5	Disable User Initiated Activation With Public BlackBerry MDS Integration Service	BlackBerry MDS Integration Service	TRUE			II	WIR1250	
Secure Email policy group								
26.1	Disable Certificate Address Checks	Secure Email		FALSE	Default setting			
26.2	Canonical Certificate Domain Name	Secure Email		<blank>	Default setting Enter the Domain name (if this field is used)			
Device IOT Application policy group								
27.1	Device Diagnostic App Disable	Device IOT Application		FALSE	Default setting			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
27.2	Set Diagnostic Report Email Address	Device IOT Application		<blank>	Default setting			
27.3	Set Diagnostic Report PIN Address	Device IOT Application		<blank>	Default setting			
Camera policy group								
28.1	Disable Camera	Camera		TRUE				
28.2	Disable Video Recorder	Camera		TRUE	(4.1.5)			
Location Based Services policy group								
29.1	Disable BlackBerry Maps	Location Based Services		FALSE	Default setting			
29.2	Enable Enterprise Location Tracking	Location Based Services		FALSE	Default setting (4.1.3)			
29.3	Enterprise Location Tracking User Prompt Message	Location Based Services		“Your location is now being tracked at the server”	Default setting. (4.1.3)			
29.4	Enterprise Location Tracking Interval	Location Based Services		15	Default setting. (4.1.3)			
RIM Value Added Applications policy group								
30.1	Disable RIM Value-Added Applications	RIM Value-Added Applications		TRUE	(4.1.6)			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
30.2	Disable Ecommerce Content Optimization Engine	RIM Value-Added Applications		TRUE	(4.1.6)			
30.3	Disable BlackBerry Wallet	RIM Value-Added Applications		TRUE	(4.1.6)			
30.4	Disable Lotus Connections	RIM Value-Added Applications		TRUE	(4.1.6)			
30.5	Lotus Connections Dogear Server	RIM Value-Added Applications		<blank>	(4.1.6)			
30.6	Lotus Connections Profile Server	RIM Value-Added Applications		<blank>	(4.1.6)			
30.7	Lotus Connections Communities Server	RIM Value-Added Applications		<blank>	(4.1.6)			
30.8	Lotus Connections Blogs Server	RIM Value-Added Applications		<blank>	(4.1.6)			
30.9	Lotus Connections Activities Server	RIM Value-Added Applications		<blank>	(4.1.6)			
Application Center policy group								

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
31.1	Disable Application Center	Application Center	TRUE		Applies to BlackBerry devices with software version 4.6 and higher (4.1.6)	III	WIR1250	
31.2	Disable Carrier Directory	Application Center	TRUE		Applies to BlackBerry devices with software version 4.6 and higher (4.1.6)	III	WIR1250	
Desktop policy group								
32.1	Desktop Password Cache Timeout	Desktop		10	Default setting.			
32.2	Desktop Allow Desktop Add-Ins	Desktop		FALSE	TRUE may be required for some applications			
32.3	Desktop Allow Device Switch	Desktop	FALSE			II	WIR1250	
32.4	Disable Media Manager			FALSE	Default setting. (4.1.5)			
32.5	Disable Check For Updates Link	Desktop		TRUE	(4.1.5)			
32.6	Disable Media Synchronization	Desktop		FALSE	Default setting. (4.1.5)			
32.7	Override Check For Updates URL	Desktop		<blank>	(4.1.5)			
Service Exclusivity policy group								
33.1	Allow Other Message Services	Service Exclusivity		FALSE				

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
33.2	Allow Other Browser Services	Service Exclusivity	FALSE			III	WIR1240	
33.3	Allow Public Yahoo! Messenger Services	Service Exclusivity	FALSE			III	WIR1240	
33.4	Allow Public AIM Services	Service Exclusivity	FALSE			III	WIR1240	
33.5	Allow Public ICQ Services	Service Exclusivity	FALSE			III	WIR1240	
33.6	Allow Public IM Services	Service Exclusivity	FALSE			III	WIR1240	
33.7	Allow Public Google Talk Services	Service Exclusivity	FALSE			III	WIR1240	
33.8	Allow other Calendar Services	Service Exclusivity		FALSE	(4.1.5)			
33.9	Allow Public WLM Services	Service Exclusivity	FALSE		(4.1.5)	III	WIR1240	
Enterprise Voice Client policy group								
34.1	Disable Enterprise Voice Client	Enterprise Voice Client		FALSE	Default setting. (4.1.4)			
34.2	Reject Non-Enterprise Voice Calls	Enterprise Voice Client		FALSE	Default setting. (4.1.4)			
34.3	Lock Outgoing Line	Enterprise Voice Client		FALSE	Default setting. (4.1.4)			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
34.4	Disable DTMF Fallback	Enterprise Voice Client		FALSE	Default setting. (4.1.5)			
Firewall policy group								
35.1	Restrict Incoming Cellular calls	Firewall		<blank>	Default setting. (4.1.5)			
35.2	Restrict Outgoing Cellular Calls	Firewall		<blank>	Default setting. (4.1.5)			
Certificate Synchronization policy group								
36.1	Random Source URL	Certificate Sync		<blank>	Default setting			
36.2	User can Disable Automatic RNG Initialization	Certificate Sync		FALSE	(4.1.5)			
Wireless Software Upgrades policy group								
37.1	Allow Non Enterprise Upgrade	Wireless Software Upgrades	FALSE		Default setting Software upgrades should only come from trusted DoD source (4.1.4)	III	WIR1250	
37.2	Disallow Device User Requested Upgrade	Wireless Software Upgrades		TRUE	(4.1.4)			
37.3	Disallow Device User Requested Rollback	Wireless Software Upgrades		TRUE	(4.1.4)			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
37.4	Disallow Patch Download Over WAN	Wireless Software Upgrades	TRUE		Software upgrades should only come from trusted DoD source (4.1.4)	III	WIR1250	
37.5	Disallow Patch Download Over Roaming WAN	Wireless Software Upgrades	TRUE		Software upgrades should only come from trusted DoD source (4.1.4)	III	WIR1250	
37.6	Disallow Patch Download Over International Roaming WAN	Wireless Software Upgrades	TRUE		Software upgrades should only come from trusted DoD source (4.1.4)	III	WIR1250	
37.7	Disallow Patch Download Over Wi-Fi	Wireless Software Upgrades	TRUE		Software upgrades should only come from trusted DoD source (4.1.4)	III	WIR1250	
BlackBerry Messenger policy group								
38.1	Disable BlackBerry Messenger	BlackBerry Messenger		FALSE	Default setting			
38.2	Messenger Audit Email Address	BlackBerry Messenger		<blank>	Default setting			
38.3	Messenger Audit UID	BlackBerry Messenger		<blank>	Default setting			
38.4	Messenger Audit Report Interval	BlackBerry Messenger		24	Default setting			
38.5	Messenger Audit Max Report Interval	BlackBerry Messenger		168	Default setting			

BES IT POLICY RULES								
Rule Ref No.	Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
			Required	Optional				
38.6	Disallow Forwarding of Contacts	BlackBerry Messenger		FALSE	Default setting (4.1.6)			
Instant Messaging policy group								
39.1	Disallow File Transfer Types	Instant Messaging	“*?”		This setting disallows all file types. (4.1.6)	III	WIR1250	
39.2	Disable Emailing Conversation	Instant Messaging		FALSE	Default setting. (4.1.6)			
39.3	Disable Saving Conversation	Instant Messaging		FALSE	Default setting. (4.1.6)			
Document To Go policy group								
40.1	Disable Documents To Go	Documents To Go		FALSE	Default setting. (4.1.5)			
40.2	Hide Documents To Go Premium Feature Menus	Documents To Go		<blank>	Default setting. (4.1.5)			
40.3	Hide Documents To Go Communications Menus	Documents To Go		<blank>	Default setting. (4.1.5)			
BlackBerry Unite! policy group								
41.1	Disable BlackBerry Unite! Applications	BlackBerry Unite!	TRUE		(4.1.6)	III	WIR1250	
41.2	Disable Download Manager	BlackBerry Unite!	TRUE		(4.1.6)	III	WIR1250	

Table C.1. BES IT Policy Rules in Order Listed in BES

C.2 BLACKBERRY IT POLICY RULES CROSS REFERENCE TABLE

Table C.2 lists all BES IT policy groups and rules in alphabetical order as found in *Reference Guide, BlackBerry Enterprise Server, Version: 4.1 | Service Pack: 6 (Document Version 31)* and *BlackBerry Enterprise Server, Wi-Fi Implementation Supplement*. To find the required STIG configuration for a specific IT policy rule, locate the rule in Table C.2, determine the Table C.1 reference number for the rule and then locate the rule in Table C.1.

Policy Rule	Table C.1 Ref No.
AMS policy group	
AMS AG Messaging URL	22.2
AMS AG Registration URL	22.1
Application Center policy group	
Disable Application Center	31.1
Disable Carrier Directory	31.2
BlackBerry MDS Integration Service policy group	
Disable Activation With Public BlackBerry MDS Integration Service	25.4
Disable MDS Runtime	25.1
Disable user Initiated Activation With Public BlackBerry MDS Integration Service	25.5
Lowest BlackBerry MDS Integration Service Security Version Allowed	25.2
Verify BlackBerry MDS Integration Service Certificate	25.3
BlackBerry Messenger policy group	
Disable BlackBerry Messenger	38.1
Disallow Forwarding of Contacts	38.6
Messenger Audit Email Address	38.2
Messenger Audit Max Report Interval	38.5
Messenger Audit Report Interval	38.4

Policy Rule	Table C.1 Ref No.
Messenger Audit UID	38.3
BlackBerry Smart Card Reader policy group	
Disable Auto Reconnect To BlackBerry Smart Card Reader	24.16
Force Erase All Keys on BlackBerry Disconnected Timeout	24.13
Force Erase Key on PC Standby	24.15
Maximum BlackBerry Disconnected Timeout	24.2
Maximum BlackBerry Bluetooth Traffic Inactivity Timeout	24.4
Maximum BlackBerry Long Term Timeout	24.3
Maximum Bluetooth Encryption Key Regeneration Period	24.14
Maximum Bluetooth Range	24.7
Maximum Connection Heart Beat Period	24.1
Maximum Number of BlackBerry Transactions	24.6
Maximum Number of PC Pairings	24.12
Maximum PC Bluetooth Traffic Inactivity Timeout	24.10
Maximum Number of PC Transactions	24.11

Policy Rule	Table C.1 Ref No.
Maximum PC Disconnect Timeout	24.8
Maximum PC Long Term Timeout	24.9
Maximum Smart Card Not Present Timeout	24.5
BlackBerry Unite! Policy group	
Disable Download Manager	41.2
Disable BlackBerry Unite! Applications	41.1
Bluetooth policy group	
Allow Outgoing Calls	17.7
Disable Address Book Transfer	17.8
Disable Advanced Audio Distribution Profile	17.18
Disable Audio/Video Remote Control Profile	17.19
Disable Bluetooth	17.1
Disable Desktop Connectivity	17.9
Disable Dial-Up Networking	17.16
Disable Discoverable Mode	17.6
Disable File Transfer	17.14
Disable Handsfree Profile	17.4
Disable Headset Profile	17.3
Disable Pairing	17.2
Disable Serial Port Profile	17.5
Disable SIM Access Profile	17.22
Disable Wireless Bypass	17.10
Force CHAP Authentication Bluetooth Link	17.17
Limit Discoverable Time	17.21

Policy Rule	Table C.1 Ref No.
Minimum Encryption Key Length	17.20
Require Encryption	17.13
Require LED Connection Indicator	17.15
Require Password for Discoverable Mode	17.12
Require Password for Enabling Bluetooth Support	17.11
Browser policy group	
Allow Application Download Services	13.14
Allow Hotspot Browser	13.15
Allow IBS Browser	13.3
Disable Auto Synchronization in Browser	13.11
Disable Java Script in Browser	13.2
Download Images URL	13.8
Download Themes URL	13.9
Download Tunes URL	13.10
MDS Browser BSM Enabled	13.7
MDS Browser Domains	13.13
MDS Browser HTML Tables Enabled	13.6
MDS Browser JavaScript Enabled	13.4
MDS Browser Style Sheets Enabled	13.5
MDS Browser Title	13.1
MDS Browser Use Separate Icon	13.12
Camera policy group	

Policy Rule	Table C.1 Ref No.
Disable Camera	28.1
Disable Video Recorder	28.2
Certificate Sync policy group	
Random Source URL	36.1
User can Disable Automatic RNG Initialization	36.2
Common policy group	
Confirm On Send	4.3
Disable Kodiak PTT	4.8
Disable MMS	4.6
Disable Voice-Activated Dialing	4.7
Disable Voice Note Recording	4.9
IT Policy Notification	4.2
Lock Owner Info	4.1
Set owner Info	4.4
Set Owner Name	4.5
Desktop Only Items	
Auto Backup Enabled	2.7
Auto Backup Exclude Messages	2.10
Auto Backup Exclude Sync	2.11
Auto Backup Frequency	2.8
Auto Backup Include All	2.9
Disable Wireless Calendar	2.6
Do Not Save Sent Messages	2.16
Force Load Count	2.3
Force Load Message	2.17
Forward Messages In Cradle	2.15
Message Conflict Mailbox Wins	2.5
Message Prompt	2.1

Policy Rule	Table C.1 Ref No.
Show Application Loader	2.2
Show Web Link	2.12
Synchronize Messages Instead Of Importing	2.4
Web Link Label	2.14
Web Link URL	2.13
Desktop policy group	
Desktop Allow Desktop Add-Ins	32.2
Desktop Allow Device Switch	32.3
Desktop Password Cache Timeout	32.1
Disable Check For Updates Link	32.5
Disable Media Manager	32.4
Override Check For Updates Link	32.6
Device IOT Application policy group	
Device Diagnostic App Disable	27.1
Set Diagnostic Report Email Address	27.2
Set Diagnostic Report PIN Address	27.3
Device-Only items	
Allow BCC Recipients	1.11
Allow Peer-to-Peer Messages	1.2
Allow SMS	1.10
Default Browser Config UID	1.15
Enable Long Term Timeout	1.9
Enable WAP Config	1.14

Policy Rule	Table C.1 Ref No.
Home Page Address	1.12
Maximum Password Age	1.6
Home Page is Read-Only	1.13
Maximum Security Timeout	1.5
Minimum Password Length	1.3
Password Pattern Checks	1.8
Password Required	1.1
User Can Change Timeout	1.7
User Can Disable Password	1.4
Documents To Go policy group	
Disable Documents To Go	40.1
Hide Documents To Go Communications Menus	40.3
Hide Documents To Go Premium Feature Menus	40.2
Email Messaging policy group	
Allow Auto Attachment Download	6.8
Attachment Viewing	6.2
Disable Form Submission	6.15
Disable Manual Download of External Images	6.14
Disable Notes Native Encryption Forward and Reply	6.9
Disable Rich Content Email	6.12
Enable Wireless Message Reconciliation	6.1
Inline Content Requests	6.13
Keep Message Duration	6.4
Keep Saved Message Duration	6.5

Policy Rule	Table C.1 Ref No.
Maximum Native Attachment MTH attachment size	6.7
Maximum Native Attachment MTH total attachment size	6.6
Notes Native Encryption Password Timeout	6.10
Prepend Disclaimer	6.3
Maximum Native Attachment MTH attachment size	6.11
Enterprise Voice Client policy group	
Disable DTMF Fallback	34.4
Disable Enterprise Voice Client	34.1
Lock Outgoing Line	34.3
Reject Non-Enterprise Voice Calls	34.2
Firewall policy group	
Restrict Incoming Cellular calls	35.1
Restrict Outgoing Cellular Calls	35.2
Global items	
Allow Browser	3.2
Allow Phone	3.1
Instant Messaging policy group	
Disallow File Transfer Types	39.1
Disable Emailing Conversation	39.2
Disable Saving Conversation	39.3
Location Based Services policy group	

Policy Rule	Table C.1 Ref No.
Disable BlackBerry Maps	29.1
Enable Enterprise Location Tracking	29.2
Enterprise Location Tracking User Prompt Message	29.3
Enterprise Location Tracking Interval	29.4
Memory Cleaner policy group	
Force Memory Clean When Holstered	10.3
Force Memory Clean When Idle	10.2
Memory Cleaner Maximum Idle Time	10.1
On-Device Help policy group	
On-Device Help Links	23.1
On-Device Help Group Label	23.2
Password policy group	
Duress Notification Address	5.5
Forbidden Passwords	5.7
Maximum Password History	5.4
Periodic Challenge Time	5.6
Set Maximum Password Attempts	5.2
Set Password Timeout	5.1
Suppress Password Echo	5.3
PIM Synchronization policy group	
Disable Address Wireless Synchronization	16.2
Disable All Wireless Sync	16.1
Disable Calendar Wireless Synchronization	16.3

Policy Rule	Table C.1 Ref No.
Disable Enterprise Activation Progress	16.10
Disable Memopad Wireless Synchronization	16.4
Disable Phone Call Log Wireless Synchronization	16.9
Disable PIN Messages Wireless Synchronization	16.7
Disable SMS Messages Wireless Synchronization	16.8
Disable Task Wireless Synchronization	16.5
Disable Wireless Bulk Loads	16.6
PGP Application policy group	
All Policy Group Rules	9.1
RIM Value-Added Applications policy group	
Disable BlackBerry Wallet	30.3
Disable Ecommerce Content Optimization Engine	30.2
Disable RIM Value-Added Applications	30.1
Disable Lotus Connections	30.4
Lotus Connections Activities Server	30.9
Lotus Connections Blogs Server	30.8
Lotus Connections Communities Server	30.7
Lotus Connections Dogear Server	30.5
Lotus Connections Profile Server	30.6

Policy Rule	Table C.1 Ref No.
S/MIME Application policy group	
Entrust Messaging Server (EMS) Email Address	8.10
S/MIME Allowed Content Ciphers	8.8
S/MIME Allowed Encrypted Attachment Mode	8.11
S/MIME Allowed Encryption Types	8.12
S/MIME Blind Copy Address	8.7
S/MIME Force Digital Signature	8.4
S/MIME Force Encrypted Messages	8.5
S/MIME Force Smartcard Use	8.6
S/MIME Minimum Strong DH Key Length	8.2
S/MIME Minimum Strong ECC Key Length	8.3
S/MIME Minimum Strong DSA Key Length	8.9
S/MIME Minimum Strong RSA Key Length	8.1
Secure Email policy group	
Canonical Certificate Domain Name	26.2
Disable Certificate Address Checks	26.1
Security policy group	
Allow External Connections	7.15
Allow Internal Connections	7.14

Policy Rule	Table C.1 Ref No.
Allow Outgoing Call When Locked	7.27
Allow Resetting of Idle Timer	7.57
Allow Screen Shot Capture	7.59
Allow Smart Card Password Caching	7.37
Allow Split-Pipe Connections	7.16
Allow Third Party Apps Use Serial Port	7.12
Certificate Status Cache Timeout	7.9
Certificate Status Maximum Expiry Time	7.21
Content Protection Strength	7.13
Desktop Backup	7.34
Disable 3DES Transport Crypto	7.30
Disable Cut/ Copy/ Paste	7.23
Disable External Memory	7.44
Disable Forwarding Between Services	7.25
Disable Geo-Tagging of Photos	7.61
Disable GPS	7.38
Disable Invalid Certificate Use	7.17
Disable IP Modem	7.36
Disable Key Store Backup	7.20
Disable Key Store Low Security	7.7

Policy Rule	Table C.1 Ref No.
Disable Media Manager FTP Access	7.47
Disable Message Normal Send	7.5
Disable Peer-to-Peer Normal Send	7.6
Disable Persisted Plaintext	7.31
Disable Public Photo Sharing Applications	7.60
Disable Public Social Networking Applications	7.67
Disable Radio When Cradled	7.24
Disable Revoked Certificate Use	7.4
Disable Smart Password Entry	7.48
Disable Stale Certificate Status Checks	7.43
Disable Stale Status Use	7.22
Disable Untrusted Certificate Use	7.3
Disable Unverified Certificate Use	7.35
Disable Unverified CRLs	7.28
Disable USB Mass Storage	7.45
Disable Weak Certificate Use	7.18
Disallow Third Party Downloads	7.10
External File System Encryption Level	7.46
FIPS Level	7.26

Policy Rule	Table C.1 Ref No.
Firewall Block Incoming Messages	7.53
Firewall Whitelist Addresses	7.63
Force Content Protection of Master Keys	7.39
Force Include Address Book In Content Protection	7.41
Force LED Blinking When Microphone Is On	7.40
Force Lock When Holstered	7.11
Force Smart Card Two Factor Authentication	7.2
Force Smart Card Two Factor Challenge Response	7.49
Key Store Password Maximum Timeout	7.8
Lock on Smart Card Removal	7.1
Maximum Smart Card User Authentication Certificate Status Check Period	7.65
Message Classification	7.42
Message Classification Title	7.62
Minimal Encryption Key Store Security Level	7.33
Minimal Signing Key Store Security Level	7.32
Password Required for Application Download	7.56
Required Password Pattern	7.54
Remote Wipe Reset to Factory Defaults	7.58

Policy Rule	Table C.1 Ref No.
Require Secure APB Messages	7.55
Secure Wipe Delay After IT Policy Received	7.52
Secure Wipe Delay After Lock	7.51
Secure Wipe if Battery Low	7.50
Security Service Colors	7.29
Security Transcoder Cod File Hashes	7.66
Trusted Certificate Thumbprints	7.19
Weak Digest Algorithms	7.64
Service Exclusivity policy group	
Allow Other Browser Services	33.2
Allow other Calendar Services	33.8
Allow Other Message Services	33.1
Allow Public AIM Services	33.4
Allow Public Google Talk Services	33.7
Allow Public ICQ Services	33.5
Allow Public IM Services	33.6
Allow Public WLM Services	33.9
Allow Public Yahoo! Messenger Services	33.3
SIM Application Toolkit policy group	
Disable Network Location Query	14.2
Disable SIM Call Control	14.1

Policy Rule	Table C.1 Ref No.
Disable SIM Originated Calls	14.3
TCP policy group	
TCP APN	15.1
TCP Password	15.3
TCP Username	15.2
TLS policy group	
TLS Device Side Only	11.9
TLS Disable Invalid Connection	11.6
TLS Disable Untrusted Connection	11.2
TLS Disable Weak Ciphers	11.1
TLS Minimum Strong DH Key Length	11.4
TLS Minimum Strong DSA Key Length	11.8
TLS Minimum Strong ECC Key Length	11.5
TLS Minimum Strong RSA Key Length	11.3
TLS Restrict FIPS Ciphers	11.7
Smart Dialing policy group	
Enable Smart Dialing Policy	19.1
Set Local Area Code	19.2
Set Local Country Code	19.3
Set National Number Length	19.4
Smart Dialing Allow Device Changes	19.5
VoIP policy group	
Allow VoIP	18.1
Disable VoIP User Profiles	18.20
SIP Authentication ID	18.15

Policy Rule	Table C.1 Ref No.
SIP Domain	18.10
SIP Local Port	18.14
SIP Registration Timeout	18.12
SIP Realm	18.3
SIP RTP Media Port	18.13
SIP Server Name	18.7
SIP Server Port	18.8
SIP Server Transport	18.11
SIP Server Type	18.6
SIP User Display Name	18.9
SIP User ID	18.4
SIP User Password	18.5
VoIP Allow BlackBerry Device Changes	18.2
VoIP Emergency Number	18.16
VoIP Enable Attended Call Transfer	18.19
VoIP Enable Call Hold	18.17
VoIP Enable Unattended Call Hold	18.18
VPN policy group	
Enable VPN	20.1
VPN Allow Handheld Changes	20.2
VPN Vendor Type	20.3
VPN Gateway Address	20.4
VPN Group Name	20.5
VPN Group Password	20.6
VPN User Name	20.7
VPN User Password	20.8
VPN DNS Configuration	20.9
VPN Primary DNS	20.10
VPN Secondary DNS	20.11

Policy Rule	Table C.1 Ref No.
VPN Domain Name	20.12
Use VPN Xauth Certificates	20.13
VPN Xauth Type	20.14
VPN IKE DH Group	20.15
VPN IKE Cipher	20.16
VPN IKE Hash	20.17
VPN PFS	20.18
VPN IPSEC Cipher and Hash	20.19
VPN Allow Password Save	20.20
VPN NAT Keep Alive	20.21
VPN Password Hidden on Input	20.22
VPN Disable Prompt for Credentials Re-Entry	20.23
Disable VPN User Profiles	20.24
VPN Minimal Certificate Encryption Key Security Level	20.25
Wireless Software Upgrades policy group	
Allow Non Enterprise Upgrade	37.1
Disallow Device User Requested Rollback	37.3
Disallow Device User Requested Upgrade	37.2
Disallow Patch Download Over International Roaming WAN	37.6
Disallow Patch Download Over Roaming WAN	37.5

Policy Rule	Table C.1 Ref No.
Disallow Patch Download Over WAN	37.4
Disallow Patch Download Over Wi-Fi	37.7
WLAN IT policy group	
WLAN Allow Handheld Changes	21.1
WLAN Link Security	21.2
WLAN SSID	21.3
WLAN Default Key ID	21.4
WLAN WEP Key 0	21.5
WLAN WEP Key 1	21.6
WLAN WEP Key 2	21.7
WLAN WEP Key 3	21.8
WLAN Preshared Key	21.9
WLAN User Name	21.10
WLAN User Password	21.11
WLAN DHCP Configuration	21.12
WLAN IP Address	21.13
WLAN Subnet Mask	21.14
WLAN Primary DNS	21.15
WLAN Secondary DNS	21.16
WLAN Default Gateway	21.17
WLAN Minimal EAP-TLS Certificate Encryption Key Security Level	21.18
WLAN Enable Authentication Page	21.19
Disable WLAN	21.20
WLAN Password Hidden on Input	21.21
Disable WAN-Only Mode	21.22

Policy Rule	Table C.1 Ref No.
Disable WAN-Preferred mode	21.23
Disable GAN-Only Mode	21.24
Disable GAN-Preferred Mode	21.25
Disable GAN Selection Mode Editing	21.26
WLAN Disable Prompt for Credentials Re-entry	21.27
Disable WLAN User profiles	21.28
GAN WLAN Threshold	21.29
GAN WLAN Threshold	21.30
GAN Signal Strength threshold	21.31
GAN Signal Quality Threshold	21.32
Disable WLAN Access to BES	21.33
WTLS policy group	
WTLS Disable Invalid Connection	12.6
WTLS Disable Untrusted connection	12.2
WTLS Disable Weak Ciphers	12.1
WTLS Minimum Strong DH Key Length	12.4
WTLS Minimum Strong ECC Key Length	12.5
WTLS Minimum Strong RSA Key Length	12.3
WTLS Restrict FIPS Ciphers	12.7

Table C.2. BES IT Policy Rules in Alphabetical Order

C.3 WLAN CONFIGURATION SETS

WLAN Configuration Set					
Setting	Setting		Comments	Security Category Code (CAT)	Related Check Number
	Required	Optional			
WLAN Allow Handheld Changes	FALSE			III	WIR1230
WLAN Link Security	EAP-TLS			III	WIR1230
WLAN SSID		Type in the SSID of approved WLAN systems	Default setting		
WLAN Default Key ID		1	Default setting		
WLAN WEP Key 0		—	Default setting		
WLAN WEP Key 1		—	Default setting		
WLAN WEP Key 2		—	Default setting		
WLAN WEP Key 3		—	Default setting		
WLAN Preshared Key		—	Default setting		
WLAN User Name		—	Default setting		

WLAN Configuration Set					
Setting	Setting		Comments	Security Category Code (CAT)	Related Check Number
	Required	Optional			
WLAN User Password		—	Default setting		
WLAN DHCP Configuration		TRUE	Default setting		
WLAN IP Address		—	Default setting		
WLAN Subnet Mask		—	Default setting		
WLAN Primary DNS		—	Default setting		
WLAN Secondary DNS		—	Default setting		
WLAN Default Gateway		—	Default setting		
WLAN Minimal EAP-TLS Certificate Encryption Key Security Level	2 or 3		This rule is obsolete in BES 4.1.4 and later	III	WIR1230
WLAN Enable Authentication Page		FALSE	Default setting		
WLAN Hard Token Required		FALSE	Default setting		
WLAN Token Serial Number		—	Default setting		
WLAN Profile Visibility		0	Default setting		

WLAN Configuration Set					
Setting	Setting		Comments	Security Category Code (CAT)	Related Check Number
	Required	Optional			
WLAN Profile Editability		0	Default setting		
WLAN Allow Password Save	FALSE		Default setting	III	WIR1230
WLAN Roaming Threshold		0	Default setting		
WLAN Server Subject		—	Default setting		
WLAN Server SAN		—	Default setting		
WLAN Inner Authentication Mode		0	Default setting		
WLAN Protected Access Credential Key		—	Default setting		
WLAN Domain Suffix		—	Default setting		
WLAN Allow AP to AP Handover		TRUE	Default setting		
Associated VoIP Configuration		—	Default setting		
Associated VPN Configuration		—	Default setting		

Table C.3. WLAN Configuration Set

C.4 VPN CONFIGURATION SETS

VPN Configuration Set					
Setting	Setting		Comments	Security Category Code (CAT)	Related Check Number
	Required	Optional			
Enable VPN		FALSE	Default setting		
VPN Allow Handheld Changes		TRUE	Default setting		
VPN Vendor Type		—	Default setting		
VPN Gateway Address		—	Default setting		
VPN Group Name		—	Default setting		
VPN Group Password		—	Default setting		
VPN User Name		—	Default setting		
VPN User Password		—	Default setting		
VPN DNS Configuration		TRUE	Default setting		
VPN Primary DNS		—	Default setting		
VPN Secondary DNS		—	Default setting		

VPN Configuration Set					
Setting	Setting		Comments	Security Category Code (CAT)	Related Check Number
	Required	Optional			
VPN Domain Name		—	Default setting		
Use VPN Xauth Certificates		FALSE	Default setting		
VPN Xauth Type		0	Default setting		
VPN IKE DH Group		7	Default setting		
VPN IKE Cipher		0	Default setting		
VPN IKE Hash		0	Default setting		
VPN PFS		TRUE	Default setting		
VPN IPSEC Cipher and hash		3	Default setting		
VPN Allow Password Save		TRUE	Default setting		
VPN NAT Keep Alive		1	Default setting		
VPN Hard Token Required		FALSE	Default setting		
VPN Token Serial Number		—	Default setting		
VPN Minimal Certificate Encryption Key Security Level		1	Default setting This rule is obsolete in BES 4.1.4 and later		
VPN Profile Visibility		0	Default setting		

VPN Configuration Set					
Setting	Setting		Comments	Security Category Code (CAT)	Related Check Number
	Required	Optional			
VPN Profile Editability		0	Default setting		
VPN IP Address		0	Default setting		
VPN Subnet Mask		—	Default setting		
Suppress VPN Banner		TRUE	Default setting		

Table C.4. VPN Configuration Set

C.5 APPLICATION CONTROL POLICY RULES

Configuration Settings for Application Control Policy Rules						
Setting	Setting			Comments	Security Category Code (CAT)	Related Check Number
	Required	Recommended	Default			
Internal Domains		Null Value	Null Value	Set to recommended value unless application requires access to this service		
External Domains		Null Value	Null Value	Set to recommended value unless application requires access to this service		
Browser Filter Domains		Null Value	Null Value	Set to recommended value unless application requires access to this service		
Disposition	Specify Required or Not Permitted for each application		Optional		II	WIR1131
Interprocess Communications		Not permitted	Allowed	Set to recommended value unless application requires access to this service		
Internal Network Connections		Null Value	Prompt User	Set to recommended value unless application requires access to this service		

Configuration Settings for Application Control Policy Rules						
Setting	Setting			Comments	Security Category Code (CAT)	Related Check Number
	Required	Recommended	Default			
External Network Connections		Null Value	Prompt User	Set to recommended value unless application requires access to this service		
Local Connections		Not Permitted	Allowed	Set to recommended value unless application requires access to this service		
Phone Access		Not Permitted	Prompt User	Set to recommended value unless application requires access to this service		
Message Access		Not Permitted	Allowed	Set to recommended value unless application requires access to this service		
PIM Data Access		Not Permitted	Allowed	Set to recommended value unless application requires access to this service		
Browser Filters		Not Permitted	Not Permitted	Set to recommended value unless application requires access to this service		
Event Injection		Not Permitted	Not Permitted	Set to recommended value unless application requires access to this service		

Configuration Settings for Application Control Policy Rules						
Setting	Setting			Comments	Security Category Code (CAT)	Related Check Number
	Required	Recommended	Default			
Bluetooth Serial Profile		Not Permitted	Allowed	Set to recommended value unless application requires access to this service		
BlackBerry Device Keystore		Not Permitted	Allowed	Set to recommended value unless application requires access to this service		
BlackBerry Device Keystore Medium Security		Not Permitted	Allowed	Set to recommended value unless application requires access to this service		
Device GPS		Not Permitted	Prompt User	Set to recommended value unless application requires access to this service		
Theme Data		Not Permitted	Allowed	Set to recommended value unless application requires access to this service		
User Authenticator		Not Permitted	Allowed	Set to recommended value unless application requires access to this service		

Table C.5. Configuration Settings for Application Control Policy Rules

C.6 BLACKBERRY MDS INTEGRATION SERVICE DEVICE POLICY RULES

Configuration Settings for MDS Integration Service Device Policy Rules						
Setting	Setting			Comments	Security Category Code (CAT)	Related Check Number
	Required	Recommended	Default			
Allow Runtime Upgrade by User	False		False		III	WIR1130
Allow Discovery by User	False		True		III	WIR1130
Allow Application Install by User	0		2		III	WIR1130
Allow Push Application Install		True	True			
Allow Application Delete by User	False		True		III	WIR1130
Allow External Access		0	0			
Allow Access to Multiple Domains	False		False		III	WIR1130
Queue Limit for Inbound Application Messages		8	8			

Configuration Settings for MDS Integration Service Device Policy Rules						
Setting	Setting			Comments	Security Category Code (CAT)	Related Check Number
	Required	Recommended	Default			
Queue Limit for Outbound Application Messages		16	16			

Table C.6. Configuration Settings for MDS Integration Service Device Policy Rules

This page is intentionally left blank.

APPENDIX D. HANDHELD SOFTWARE CONFIGURATION SETTINGS

BLACKBERRY HANDHELD SOFTWARE CONFIGURATION SETTINGS						
Rule	Setting Required	Optional	Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
Options/Bluetooth/Paired Devices list/select each paired device/click Device Properties						
Device Name	Leave default value			III	WIR1250	
Trusted	Ask			III	WIR1250	
Encryption	Enabled		May not be able to configure on device if corresponding BES IT Policy rule is configured	III	WIR1250	
“Don’t ask this again” checkbox	Do Not Check		Located on the connection alert dialog box	III	WIR1250	
Options/Bluetooth/Options menu item						
Device Name	Select name that does not identify user, organization, location, or device in any way			III	WIR1250	
Discoverable	No		May not be able to configure on device if corresponding BES IT Policy rule is configured	II	WIR1140	

BLACKBERRY HANDHELD SOFTWARE CONFIGURATION SETTINGS						
Rule	Setting Required	Optional	Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
Allow Outgoing Calls	If Unlocked		May not be able to configure on device if corresponding BES IT Policy rule is configured	III	WIR1250	
Address Book Transfer	Disabled		May not be able to configure on device if corresponding BES IT Policy rule is configured	III	WIR1250	
Options/Security Options/Smart Card						
Lock on Card Removal		Disabled	May not be able to configure on device if corresponding BES IT Policy rule is configured			
PIN Caching		Disabled	May not be able to configure on device if corresponding BES IT Policy rule is configured			
Options/Security Options/Smart Card/Registered Reader Drivers/BlackBerry/Driver Settings						
Reader LED – Low Battery	Enabled			III	WIR1150	
Reader LED – Pairing	Enabled			III	WIR1150	
Reader LED – Traffic	Enabled			III	WIR1150	

BLACKBERRY HANDHELD SOFTWARE CONFIGURATION SETTINGS						
Rule	Setting Required	Optional	Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
Reader Setting – Connection Heartbeat Period		None	May not be able to configure on device if corresponding BES IT Policy rule is configured			
Reader Setting – Power Off Timeout		None				
Reader Setting – Power saving Mode		Partial				
Reader setting – Bluetooth Range	2 or less		May not be able to configure on device if corresponding BES IT Policy rule is configured	III	WIR1150	
Erase Key After – Disconnected Timeout		None	May not be able to configure on device if corresponding BES IT Policy rule is configured			
Erase Key After – Long Term Timeout		None	May not be able to configure on device if corresponding BES IT Policy rule is configured			
Erase Key After – Inactivity Timeout		None	May not be able to configure on device if corresponding BES IT Policy rule is configured			

BLACKBERRY HANDHELD SOFTWARE CONFIGURATION SETTINGS						
Rule	Setting Required	Optional	Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
Erase Key After – Card Not Present timeout		None	May not be able to configure on device if corresponding BES IT Policy rule is configured			
Erase Key After – Number of Transactions		None	May not be able to configure on device if corresponding BES IT Policy rule is configured			
Options/Owner						

BLACKBERRY HANDHELD SOFTWARE CONFIGURATION SETTINGS						
Rule	Setting Required	Optional	Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
Name	Leave blank or follow guidance in comment		<p>May not be able to configure on device if corresponding BES IT Policy rule is configured</p> <p>DoD BlackBerry sites should consider using the following message: "If this BlackBerry is found, please call the following phone number xxx-xxx-xxxx." When called, the phone number should not identify itself as a DoD organization.</p>	III	WIR1250	

BLACKBERRY HANDHELD SOFTWARE CONFIGURATION SETTINGS						
Rule	Setting Required	Optional	Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
Information	Leave blank or follow guidance in comment		<p>May not be able to configure on device if corresponding BES IT Policy rule is configured</p> <p>DoD BlackBerry sites should consider using the following message: "If this BlackBerry is found, please call the following phone number xxx-xxx-xxxx." When called, the phone number should not identify itself as a DoD organization.</p>	III	WIR1250	
Open Email Application/Menu/Options/Email Settings						
Auto signature		Add disclaimer message (e.g., "For government Use Only" or signature block)	If used, disclaimer message must not include "Sent from my BlackBerry handheld" or similar message.	III	WIR1210	

Table D.1. BlackBerry Handheld Software Configuration Settings

This page is intentionally left blank.

APPENDIX E. CAC DIGITAL CERTIFICATE PROVISIONING

1. Initial Provisioning of BlackBerry for S/MIME

Complete the following steps for setting up a BlackBerry with S/MIME support:

- Load BlackBerry Handheld and carrier software on BlackBerry.
- Load S/MIME software on BlackBerry.
- Load Smart Card Reader drivers on BlackBerry.
- Load PIV drivers on BlackBerry.
- Load user digital certificates on BlackBerry.
- Load DoD Root certificates on BlackBerry (to get the latest root certificates, use the BlackBerry browser and connect to www.dodpke.com/jad and download Root Certificate file.)
- Load BlackBerry Smart Card Reader drivers on Bluetooth SCR.

Download the following documents from the DoD PKE web portal for additional information:

BlackBerry QRC Importing Smart Card Certs.pdf
BlackBerry SMIME and SCR for CAC Setup.pdf

These documents are located at <https://gesportal.dod.mil/sites/dodpke/>, select the “Knowledge Base Library” link, select the “Wireless” folder, then the “BlackBerry” folder.

2. Loading New CAC Public Certificates on a BlackBerry

Method #1

Follow the following procedure for loading certificates from a new CAC on a previously provisioned BlackBerry:

- Load new certificates by following the procedures found in BlackBerry QRC Importing Smart Card Certs.pdf (see #1 above).
- Remove old certs from BlackBerry as follows:
 - Connect BlackBerry to computer where BlackBerry Desktop Manager is installed with USB cable.
 - Launch the BlackBerry Desktop Manager.
 - Click on “Certificate Sync.”

- Under the “Personal Certificates” tab, uncheck all old certificates.
- Click “Synchronize.”

Method #2

- Remove old certs from BlackBerry as follows:
 - Go to **Settings>Options>Security Options>Certificates**
 - Select each user certificate in turn (there may be three) and go to **Menu>Delete**
- Add new CAC certificate pointers to the BlackBerry as follows:
 - Place new CAC in BlackBerry SCR
 - Go to **Settings>Options>Security Options>S/MIME**
 - Select **Menu>Import smart card certs**, then follow prompts

For additional information or assistance on BlackBerry PKI issues, contact the DoD PKE office at pke_support@disa.mil or visit their web site at <https://gesportal.dod.mil/sites/dodpke/>.

This page is intentionally left blank.

APPENDIX F. VMS PROCEDURES

The following information applies only to teams and sites that use VMS to enter and track DoD assets. When conducting a BlackBerry SRR, the Team Lead and the assigned Reviewer identify security deficiencies and provide data from which to predict the effectiveness of proposed or implemented security measures associated with the BlackBerry system and operating environment.

Both the Reviewer and the SA will create, maintain, and track assets in VMS. The reviewer will use the Asset and Finding Maintenance screen to perform these functions. The SA will use the By Location navigation chain to perform the same function. When Reviewers access the Asset and Finding Maintenance screen, the Navigation pane displays a white Visits folder. Expand this Visits folder to display its subfolders. Each subfolder represents an individual visit in VMS that is assigned for review. Click (+) to expand the visit and display the location summaries for the visit. Within the location, BlackBerry assets are tracked using the Computing and Non-Computing asset types.

Use the following matrix to select the appropriate asset type for each BlackBerry asset. The reviewer or SA must enter the entire asset posture including non-wireless related applications and services installed on the BES.

VMS Asset Matrix		
Wireless Technology	VMS Asset Type	ASSET POSTURE
All wireless devices (Wireless email servers and handheld devices) A non-computing asset is created to apply all general wireless policy checks in Section 2.1 of the Checklist.	Non-Computing	<p>NETWORK POLICY REQUIREMENTS -> WIRELESS POLICY</p> <p><i>Note:</i> These checks apply to the network or concern site policy rather than to a specific wireless device.</p> <p>The reviewer should create one non-computing asset for the BlackBerry system at the site. Example asset name: Site Q BlackBerry System.</p>
BlackBerry Enterprise Server NOTE: Only configure asset for applications installed on the same server as the BES application. There are no checks for LDAP	Computing	<p>Operating System -> Windows. Expand and select version then service pack installed.</p> <p>Application -BlackBerry Enterprise Server Application ->Antivirus. Expand and select version. Application - Expand and select other applications installed on same server to capture the entire asset posture of the server (e.g., SQL, Exchange, Browsers, Office Automation, etc).</p> <p>Role - Member Server</p>

VMS Asset Matrix		
Wireless Technology	VMS Asset Type	ASSET POSTURE
BlackBerry Client Devices	Computing	<i>NOTE:</i> Do not mark as a workstation <i>NOTE:</i> Do not enter IP or MAC address Network -> Data Network -> Wireless -> BlackBerry Client

Table E-1. VMS Asset Matrix

This page is intentionally left blank.

APPENDIX G. BLACKBERRY CONFIGURATION FOR GROUP EMAIL ACCOUNTS

Procedures for Setting up and Using a “Team” BlackBerry

Introduction

When a BlackBerry has been set up for a group email account and will be shared by a group or “team” (e.g., help desk team) the BlackBerry must be configured and operated consistent with DoD BlackBerry security requirements. This paper describes required procedures.

References

1. BlackBerry QRG Importing Software Certs.pdf, found on the DoD PKE web site at <https://www.us.army.mil/suite/doc/8461655> . (CAC and DKO account required to access document.)
2. BlackBerry QRG Importing Smart card Certs.pdf, found on the DoD PKE web site at <https://www.us.army.mil/suite/doc/8461656> . (CAC and DKO account required to access document.)

Note: Contact the DoD PKE Office at pke_support@disa.mil for support in getting access to these references.

Step 1 – Install Group Email Account Shared Email Encryption Key on BlackBerry

- a. Have Team Lead follow local procedures to request a software certificate from the local RA. Request group/role attributes for the group email account.
- b. Get the private email encryption key and save on floppy diskette or thumb drive. The team lead must select a master password to protect the key and the password should only be known to the team lead.
- c. Install private email encryption key for group email account on the PC used as the Desktop Manager for the Team BlackBerry. (See Reference 1, Steps 5-16)

Once the two new .cer files have been created, publish the group email account certificates to the GAL using local procedures.

- d. Mark key as exportable. (See Reference 1, Step 9)
- e. Export key to the BlackBerry. (See Reference 1, Steps 17-19)
- f. Re-install private email encryption key to the desktop a second time (see paragraph c above) and mark as non-exportable. (See Reference 1, follow procedure described at the end of page 6)

- g. If BlackBerry Desktop Manager and private group email encryption key is installed on every team member's PC then there will be less disruption when a member of the team departs the group. This minimizes the security risk when a member of the group leaves, thus requiring the group email certificate keystore password to be changed. Each team member then selects their own certificate keystore password to protect the certificates on their PC.

Step 2 - Install Team Member certificates on BlackBerry

Load the digital certificates of each team member on the BlackBerry. (See Reference 2)

STEP 3 – Incorporate BlackBerry Team Procedures in Site BlackBerry SOP/CONOPS

The following procedures must be included in the site BlackBerry SOP or CONOPS:

- a. Each "team" member is required to logon to the BlackBerry with their CAC.
- Configure the BlackBerry or BES to require CAC authentication for device unlock. Do one of the following:
 - Put Team BlackBerry in a separate IT Policy group on the BES and enable “**Force Smart Card Two Factor Authentication.**”

Or

 - On team BlackBerry, Enable “**User Authentication**” (e.g. CAC authentication) as follows⁴: **Options>Security Options>General Settings>click on User Authentication>select Change Option>change option to Enabled>click User Authentication>select Save>when prompted, enter BlackBerry password under Enter Handheld Password (or Enter Password) and enter CAC PIN of current team member using BlackBerry under Enter Authenticator Password.**

Note: Both the BlackBerry password and the CAC PIN need to be entered when unlocking the BlackBerry.
 - Procedure for changing Team BlackBerry user:
 - The **User Authentication Password** must be changed to the new user's CAC PIN as follows:
 - Current user unlocks the BlackBerry
 - Current user selects **Options>Security Options>General Settings>click on User Authentication>select Change Option>Change Password>** when prompted, enter BlackBerry password under **Enter Handheld Password** and enter CAC PIN of current team member using BlackBerry under **Enter Authenticator Password**
 - When **New Password** prompt is on screen, hand BlackBerry to new user.

⁴ This procedure may vary slightly, depending on the BlackBerry model and version of Handheld Software installed.

- New user enters CAC PIN and then reenters PIN to verify new Authentication Password.
- b. Each “team” member is to be trained on how to sign and encrypt email messages on the BlackBerry.
- c. BlackBerry team members are prohibited from storing personal or individually sensitive information on the team BlackBerry.
- d. A "Master Station Log" will be used to document who currently has possession of the team BlackBerry and when the BlackBerry was passed from one team member to another. Procedures for maintaining and inspecting the log will also be included in the site BlackBerry SOP or CONOPS.
- e. Completion of BlackBerry user training will be documented.

This page is intentionally left blank.