



Protecting the BlackBerry device platform against malware

BlackBerry Enterprise Server Version 5.0 and later

Technical Overview

Contents

BlackBerry device application platform default behavior	3
Adding third-party Java applications to BlackBerry devices.....	3
Malware vulnerabilities on the BlackBerry device.....	4
Managing the risk of malware attacks.....	4
Using BlackBerry Enterprise Solution tools to contain malware on the BlackBerry device	4
Policy precedence on the BlackBerry device	5
Using IT policy rules to control third-party Java application functionality on the BlackBerry device.....	5
Using application control policy rules to control third-party Java application access	6
Using code signing to limit access to BlackBerry device application data.....	11
Using segmented network architecture to prevent the spread of malware on your corporate network.....	11
Using segmented network architecture to prevent the spread of malware on your Wi-Fi network	12
Related resources	13
Appendix A: Examples of how to prevent potential vulnerability to malware attacks on BlackBerry devices	15
Preventing potential vulnerability to an application proxy attack.....	15
Preventing potential vulnerability to a MAPI attack	15

This document describes the third-party Java application control features of the BlackBerry® Enterprise Solution and provides an overview of how you might use those features and place the BlackBerry Enterprise Solution within your corporate network architecture to contain the threat of malware on your BlackBerry® devices and your corporate network.

See the *BlackBerry Enterprise Solution Security Acronym Glossary* for the full terms substituted by the acronyms in this document.

BlackBerry device application platform default behavior

Java® based BlackBerry devices are designed to provide an open platform for third-party wireless enterprise application development. Using BlackBerry® MDS Studio and the BlackBerry® Java Development Environment (JDE), the BlackBerry Enterprise Solution lets software developers create third-party Java applications for BlackBerry devices. The BlackBerry device supports MIDlets (Java applications that use standard MIDP and CLDC APIs only) and Java applications that use the BlackBerry APIs.

BlackBerry JDE developers can create more powerful, sophisticated applications than are possible with standard Java 2 Platform Micro Edition (J2ME™). A third-party BlackBerry application can perform the following tasks on the BlackBerry device:

- communicate and share persistent storage with other third-party BlackBerry applications
- interact with native BlackBerry applications
- access BlackBerry device user data such as calendar entries, email messages, and contacts

Adding third-party Java applications to BlackBerry devices

By default, Java based BlackBerry devices can download third-party Java applications by performing either of the following actions:

- accessing a web site using the BlackBerry® Browser and choosing to download the application over the wireless network
- running the application loader tool of the BlackBerry® Desktop Manager and choosing to download the application onto the BlackBerry device using a physical connection to the computer

You can also send third-party Java applications to BlackBerry devices wirelessly, and install them on the BlackBerry devices automatically using the application loader remote function. Users can then run these third-party Java applications on their BlackBerry devices, and manage and delete those applications using the application loader tool of the BlackBerry Desktop Manager.

You can provide a trusted application for BlackBerry device users by performing either of the following actions:

- placing the application on a network drive or web server for BlackBerry device users to download over the wireless network or download from a hosted web site over a physical connection to a computer
- placing the application on a network drive and using a software configuration that you define in the BlackBerry Administration Service to push the application to BlackBerry devices over the wireless network

Whether you push third-party Java applications or let BlackBerry device users freely download third-party Java applications onto BlackBerry devices, the BlackBerry Enterprise Solution includes tools designed to let you control the manual or automatic installation of third-party Java applications. It also lets you limit the access of untrusted applications to the BlackBerry devices and their resources to help contain malware attacks on the BlackBerry devices. When trying to download a third-party Java application, the BlackBerry device first downloads a small portion of the application to determine the hash and verify whether the BlackBerry device allows the application to exist and run. The BlackBerry device is designed to prevent unauthorized application code from running.

Malware vulnerabilities on the BlackBerry device

Third-party Java applications that are designed with malicious intent to cause harm to computer systems are commonly known as malware and include the following examples:

- Viruses: replicate themselves by attaching to legitimate applications on a computer
- Trojan horses: disguise themselves as or embed themselves within innocuous-seeming or trusted applications; to succeed, a Trojan horse application depends on the action of the device user, and therefore, it requires successful use of social engineering rather than the ability to exploit flaws in the security design or configuration of the target device
- Worms: replicate themselves to spread across networks and potentially overwhelm computer systems (a worm is self-contained and does not need to be part of another program to spread itself)
- Spyware: designed to log device user activities and personal data and send that information to the attacker

Some malware attacks might target BlackBerry devices. Attackers might use malware to perform attacks that are designed to

- steal personal and corporate data
- create a Denial of Service to make a corporate network unusable
- access a corporate network using corporate BlackBerry devices

Managing the risk of malware attacks

Plan your network architecture and design your security policies to help manage the risk of malware attacks. When you plan and set up your corporate network, you should set security policies to protect the network components, which might have many connections to the Internet and to external systems, as well as network clients such as BlackBerry devices.

Consider separating your corporate network infrastructure into digital zones, or segments, separated by firewalls, and restricting internal and external user access to those zones. You might require multiple security products and methods to protect each gateway from one section of your corporate network to another and to and from the Internet.

To maintain and enforce the corporate network security policies, you also must apply a subset of your security solution and security policies on each BlackBerry device, since BlackBerry devices are an extension of your physical corporate network. Make sure that the security measures you set up are designed to protect your physical corporate network and to protect the security of the BlackBerry devices.

You can use BlackBerry Enterprise Solution tools to help prevent opportunities for attackers to use malware to access your corporate network and BlackBerry devices. See "Appendix A: Examples of how to prevent potential vulnerability to malware attacks on BlackBerry devices" on page 15 for more information about using BlackBerry Enterprise Solution tools designed to prevent specific, potential malware attacks.

Using BlackBerry Enterprise Solution tools to contain malware on the BlackBerry device

On computers, malware prevention requires processes that both detect and contain malware attacks. Detection is the process of determining whether or not a program is malware. Effective malware detection requires a comprehensive and frequently updated local database or a constant connection to a similarly qualified online database. While computers might have access to these databases, current mobile devices do not have enough storage space for a malware database and cannot guarantee a constant connection to the Internet.

The BlackBerry Enterprise Solution is designed to use IT policies, application control policies, and code signing to contain malware by controlling third-party Java application access to BlackBerry device resources and applications. These containment methods are designed to prevent malware that might gain access to the BlackBerry device from causing damage to the BlackBerry device, its applications and its data, or to the corporate network.

The BlackBerry® Enterprise Server provides IT policy rules and application control rules that you can set to control third-party Java applications using the following methods:

- preventing BlackBerry devices from downloading third-party Java applications over the wireless network
- requiring or preventing BlackBerry devices from installing specific third-party Java applications
- controlling the permissions of third-party Java applications that exist on BlackBerry devices

By default, BlackBerry devices can install all third-party Java applications until you use one or all of these methods to control third-party Java applications on BlackBerry devices.

Policy precedence on the BlackBerry device

IT policy rule settings override application control policy rule settings. For example, if you set the Allow Internal Connections IT policy rule to False for BlackBerry devices for which you also set an application control policy that allows a specific application to make internal connections, the IT policy rule setting overrides the application control policy rule setting; the application cannot make internal connections.

The BlackBerry device revokes an application control policy and resets if the permissions of the application to which it is applied become more restrictive. BlackBerry devices running the BlackBerry Device Software Version 4.1 or later let BlackBerry device users make application permissions more, but never less, restrictive than what the BlackBerry Enterprise Server administrator sets.

Using IT policy rules to control third-party Java application functionality on the BlackBerry device

Most of the IT policy rules that the BlackBerry Enterprise Server includes are designed to let you control Research In Motion applications on the BlackBerry device. The BlackBerry Enterprise Server Version 4.1 SP2 or later includes the following IT policy rules that are designed to let you

- prevent BlackBerry devices from downloading third-party Java applications over the wireless network
- specify whether or not applications, including third-party Java applications, on the BlackBerry device can initiate specific types of connections

IT policy rule	Description	Default setting
Disallow Third Party Application Download	<p>Specify whether or not the BlackBerry device can download third-party Java applications. If you set this IT policy rule to True, the BlackBerry devices do not remove previously installed applications.</p> <p>You cannot use this IT policy rule to allow or prevent the downloading of specific applications on the BlackBerry device. For that, you must set application control policy rules.</p> <p>Note: If you set the FIPS Level IT policy rule to FIPS 140-2 Level 2 compliance, the BlackBerry Enterprise Server automatically sets the Disallow Third Party Application Download IT policy rule to True in the same IT policy.</p>	False (The BlackBerry device allows the downloading of all third-party Java applications.)
Allow External Connections	Specify whether or not applications, including third-party Java applications, on the BlackBerry device can initiate external connections (for example, to WAP, SMS, or other public gateways).	True (The BlackBerry device allows all external connections from applications.)
Allow Internal Connections	<p>Specify whether or not applications, including third-party Java applications, on the BlackBerry device can initiate internal connections (for example, to the BlackBerry MDS™ Connection Service)</p> <p>Note: Preventing all internal connections for all third-party Java applications turns off the use of the connection service on the BlackBerry device.</p>	True (The BlackBerry device allows all internal connections from applications.)
Allow Third-Party Apps to Use Serial Port	Specify whether or not third-party Java applications can use the serial port or USB port on the BlackBerry device for communication.	True (The BlackBerry device allows all third-party Java applications to use the BlackBerry device ports.)

See the *BlackBerry Enterprise Server System Administration Guide* for information about setting IT policies. See the *Policy Reference Guide* for more information about using specific IT policy rules.

Using application control policy rules to control third-party Java application access

The BlackBerry Enterprise Server application control policy rules are designed to let you allow or prevent the installation of specific third-party Java applications on the BlackBerry device and to limit the permissions of third-party Java applications, including

- the resources (for example, email, phone, and BlackBerry device key store) that third-party Java applications can access on the BlackBerry device
- the types of connections that a third-party Java application running on the BlackBerry device can establish (for example, local, internal, and external connections)

- whether or not an application can access the user authenticator framework API, which permits the registration of drivers to provide two factor authentication to unlock the BlackBerry device

For example, you can control connections to your internal servers from third-party Java applications on the BlackBerry device using the following process:

1. Do not change the Allow Internal Connections IT policy rule (the default value is True)
2. Create an application control policy that prevents the application to which it is assigned from making internal connections.
3. Apply the application control policy to a software configuration for a user or one or more user groups (when you set application policy rules for user groups, you can limit allowed application behavior to a small subset of trusted BlackBerry device users only)

The BlackBerry device users to which you assign the application control policy cannot use third-party Java applications to send and receive data from internal servers.

Defining software configurations

Before you can set an application control policy on a BlackBerry device, you must set up a software configuration and either install all of the necessary application files on the BlackBerry Enterprise Server or on another computer on which the BlackBerry Enterprise Server administrator tools exist.

A software configuration points to the shared network location of the BlackBerry Device Software that you want to install on a specific BlackBerry device model. Software configurations allow you to remotely add and remove third-party Java applications using the application loader tool on BlackBerry devices that are connected to computers running the BlackBerry Device Manager.

See the *BlackBerry Enterprise Server System Administration Guide* for information about defining software configurations.

Applying application control policies

After you assign a software configuration to a BlackBerry device user, the user can use the application loader tool of the BlackBerry Desktop Manager to install or upgrade to the BlackBerry Device Software that you assign. To control or change the behavior of third-party Java applications on the BlackBerry device, you must set an application control policy and assign application control policy rule values.

If a default application policy does not exist, the user can change application controls on the BlackBerry device. If a default application control policy exists (that is, it is not assigned to a specific application, but is set as a default for third-party Java applications that the BlackBerry device downloads thereafter), the BlackBerry device user cannot change the application controls.

For example, you can set a default application control policy that removes all existing third-party Java applications and blocks third-party Java applications that the user adds thereafter from running on the BlackBerry device. This means that even if a user connects a BlackBerry device with third-party Java applications installed to a BlackBerry Enterprise Server, the BlackBerry device does not allow the third-party Java applications to run.

You can also set one or more application control policies and apply them to trusted third-party Java applications to create an allowed list of applications for specific application behavior. You can create an allowed list of one or more specific applications by setting an application policy to

- allow BlackBerry device users to install only those applications (if the default application policy otherwise prevents users from installing third-party Java applications)
- allow only those applications to perform specific actions (if the default application policy otherwise prevents all third-party Java applications from performing those actions)

The BlackBerry Enterprise Server Version 4.1 SP2 or later includes the following application control policy rules:

Application control policy rule	Description	Default setting
Internal Domains	Specify the internal domain names to which the application can establish a connection.	Null value (not set)
External Domains	Specify the external domain names to which the application can establish a connection.	Null value (not set)
Browser Filter Domains	Specify the domains for which the application can apply browser filters to web page content on the BlackBerry device. For example, you can specify google.com and yahoo.com as domains for which you allow an application to use a search engine browser filter on the BlackBerry device.	Null value (not set)
Disposition	Specify whether the application is optional, required, or not allowed on the BlackBerry device. You can use this application control policy rule to require that the BlackBerry device download a specific application or prevent the BlackBerry device from downloading an unspecified or untrusted application.	Optional
Interprocess Communication	Specify whether or not the application can perform interprocess communication operations. You can use this application control policy rule to prevent two or more applications from sharing data and to prevent one application from using the connection permissions of another application.	Allowed
Internal Network Connections	Specify whether or not the application can make internal corporate network connections. You can use this application control policy rule to allow or prevent the application from sending or receiving data on the BlackBerry device using an internal protocol (for example, using the connection service) or to require that the user respond to a prompt on the BlackBerry device to allow internal connections through the BlackBerry device firewall.	Prompt User
External Network Connections	Specify whether or not the application can make external network connections. You can use this application control policy rule to allow or prevent the application from sending or receiving data on the BlackBerry device using an external protocol (for example, using a WAP gateway, public BlackBerry MDS Services, or TCP), or to require that the user respond to a prompt on their BlackBerry device to allow external connections through the BlackBerry device firewall.	Prompt User
Local Connections	Specify whether or not the application can make local network connections (for example, connections to the BlackBerry device using a USB or serial port).	Allowed

Application control policy rule	Description	Default setting
Phone Access	Specify whether or not the application can make phone calls and access phone logs on the BlackBerry device. You can use this application control policy rule to allow or prevent the application from making calls on the BlackBerry device or to require that the user respond to a prompt on the BlackBerry device to allow the application to make a phone call.	Prompt User
Message Access	Specify whether or not the application can send and receive messages on the BlackBerry device using the email API.	Allowed
PIM Data Access	Specify whether or not the application can access the BlackBerry device PIM APIs, which control access to the user's personal information on the BlackBerry device, including the address book. Note: Allowing the application to access PIM data APIs and use internal and external network connection protocols creates an opportunity for an application to send all of the user's personal data from their BlackBerry device.	Allowed
Browser Filters	Specify whether or not the application can access browser filter APIs to register a browser filter with the browser on the BlackBerry device. You can use this application control policy rule to allow third-party Java applications to apply custom browser filters to web page content on the BlackBerry device.	Not Permitted
Event Injection	Specify whether or not the application can inject synthetic input events, such as pressing keys and performing trackwheel actions, on the BlackBerry device.	Not Permitted
Bluetooth Serial Profile	Specify whether or not the application can access the Bluetooth® Serial Port Profile (SPP) API. Note: If you set the Disable Serial Port Profile IT policy rule to True, the Bluetooth enabled BlackBerry device cannot use the Bluetooth SPP to establish a serial connection to a Bluetooth enabled device.	Allowed

Application control policy rule	Description	Default setting
BlackBerry Device Keystore	Specify whether or not the application can access the BlackBerry device key store APIs. If you set the Minimal Signing Key Store Security Level and the Minimal Encryption Key Store Security Level IT policy rules to high, the BlackBerry device prompts the user for the BlackBerry device key store password each time an application tries to access the user's private key on the BlackBerry device, and the BlackBerry device does not use this application policy control rule.	Allowed
BlackBerry Device Keystore Medium Security	Specify whether or not the application can access key store items at the medium security level (the default level), which requires that the BlackBerry device prompt the user for the BlackBerry device key store password when an application tries to access the user's private key for the first time or when the private key password timeout expires. If you set the Minimal Signing Key Store Security Level and the Minimal Encryption Key Store Security Level IT policy rules to high, the BlackBerry device prompts the user for the BlackBerry device key store password each time an application tries to access their private key, and this application policy control rule is not recognized.	Allowed
Device GPS	Specify whether or not the application can access the BlackBerry device Global Positioning System (GPS) APIs. You can use this application control policy rule to allow or prevent the application from accessing the GPS APIs on the BlackBerry device or to require that the user respond to a prompt on the BlackBerry device to allow access to the GPS APIs.	Prompt User
Theme Data	Specify whether or not the BlackBerry device can use the custom theme applications, which developers can create using the Plazmic CDK, as themes if they exist on the BlackBerry device.	Allowed
User Authenticator API	Specify whether or not the BlackBerry device allows an application to access the user authenticator framework API. The user authenticator framework allows the registration of drivers (currently smart card drivers only) that provide two-factor authentication to unlock the BlackBerry device. This application control policy rule applies to the BlackBerry Device Software and third-party Java applications.	Allowed

See the *BlackBerry Enterprise Server System Administration Guide* for more information about setting application control policies. See the *Policy Reference Guide* for more information about using specific application control policy rules.

Using code signing to limit access to BlackBerry device application data

RIM does not inspect or verify third-party Java applications that run on BlackBerry devices; however, RIM controls the use of BlackBerry device APIs that include sensitive packages, classes, or methods to prevent unauthorized applications from accessing data on the BlackBerry device. Each third-party Java application requires authorization to run on the BlackBerry device. MIDlets cannot access the memory of other applications, or access the persistent data of other MIDlets unless they are digitally signed by the RIM signing authority system.

Before you or a BlackBerry device user can run a third-party Java application that uses the RIM controlled APIs on the BlackBerry device, the RIM signing authority system must use public key cryptography to authorize and authenticate the application code. The third-party Java application developer must visit www.blackberry.com/developers/downloads/jde/api.shtml to register with the RIM signing authority system for access to the controlled APIs and use the BlackBerry Signature Tool, which is a component of the BlackBerry JDE, to request, receive, and verify a digital code signature from RIM for the application.

Third-party Java application developers who create controlled access third-party APIs can act as a signing authority for those APIs. The application developer can download and install the BlackBerry Signing Authority Tool to allow other developers to register for access to the application developer's controlled APIs. Registered developers can use their BlackBerry Signature Tool to request, receive, and verify digital code signatures from the application developer's BlackBerry Signing Authority Tool for their applications.

See the *BlackBerry Signing Authority Tool Administrator Guide* for more information about code signing and third-party Java applications.

Using segmented network architecture to prevent the spread of malware on your corporate network

You can separate a corporate network or LAN into multiple firewall segmented components to create segmented network architecture. Each segment of the corporate network can contain network traffic, which improves the security and performance of the network segment by filtering out data that is not destined for that particular segment. If your corporate security policies enforce the use of segmented network architecture, you can place the BlackBerry Enterprise Solution components in network segments.

To place the BlackBerry Enterprise Solution in multiple network segments, you must install each component on a remote computer and then place each component in its own network segment. Placing the BlackBerry Enterprise Solution components in segmented network architecture is an option designed to prevent the spread of potential attacks from one BlackBerry Enterprise Solution component that exists on a remote computer to another computer within the corporate LAN. In a segmented network, attacks are isolated and contained on one computer. When each BlackBerry Enterprise Solution component resides in its own network segment, you allow remote communications by opening only the port connections that the BlackBerry Enterprise Solution components use.

The BlackBerry Enterprise Solution components authenticate port connections between them over a TCP/IP or UDP/IP connection using SSL or TLS. For certain connections between remote BlackBerry Enterprise Solution components, (for example, between the BlackBerry Dispatcher and the BlackBerry Collaboration Service) the BlackBerry Enterprise Solution provides additional encryption using RIM proprietary protocols. See the *BlackBerry Enterprise Solution Version 4.1 Security Technical Overview* for more information on the RIM protocols.

See *Placing the BlackBerry Enterprise Solution in a Segmented Network* for more information on using segmented network architecture.

Using segmented network architecture to prevent the spread of malware on your Wi-Fi network

Supported Wi-Fi® enabled BlackBerry devices on an enterprise Wi-Fi network bypass the use of SRP by using the BlackBerry Router to send data between the BlackBerry Enterprise Server and the BlackBerry device. After the BlackBerry Router protocol establishes an authenticated connection successfully, the supported Wi-Fi enabled BlackBerry device uses a direct connection to the BlackBerry Enterprise Server using the BlackBerry Router instead of SRP connectivity and authentication.

If you have configured an enterprise Wi-Fi network that uses a VPN solution, when Wi-Fi enabled BlackBerry devices make connections to that network, they might allow the VPN concentrator, which acts as network gateway, to send data directly to the internal network of your organization. The VPN concentrator is the only device connected to the enterprise Wi-Fi network in this scenario. Configure your VPN concentrator to prevent it from opening unnecessary connections to the internal network.

Related resources

Resource	Information
<i>BlackBerry Application Web Loader Developer Guide</i>	<ul style="list-style-type: none"> • installing applications from a web page • using the application web loader on a web server
<i>BlackBerry Enterprise Server System Administration Guide</i>	<ul style="list-style-type: none"> • making BlackBerry Device Software and applications available to BlackBerry device users • assigning application control policies to BlackBerry device user accounts to control applications that exist on BlackBerry devices • assigning IT policies to BlackBerry device users and groups • managing IT policies • setting IT policy rules • managing security features
<i>BlackBerry Enterprise Solution Security Acronym Glossary</i>	<ul style="list-style-type: none"> • understanding full terms substituted by acronyms in this and other security documents
<i>BlackBerry Enterprise Solution Security Technical Overview</i>	<ul style="list-style-type: none"> • preventing the decryption of information at an intermediate point between the BlackBerry device and the BlackBerry Enterprise Server or corporate LAN • managing security settings for all BlackBerry devices • protecting data in transit between the BlackBerry device and the BlackBerry Enterprise Server. • understanding the algorithms that the RIM cryptographic application programming interface (Crypto API) provides • understanding the TLS and WTLS standards that the RIM Crypto API currently supports • understanding the memory scrubbing process that occurs on the BlackBerry device when content protection is turned on

Resource	Information
<p><i>BlackBerry Java Development Environment BlackBerry Application Developer Guide Volume 1: Fundamentals</i></p>	<ul style="list-style-type: none"> • using BlackBerry APIs • using APIs, classes, and methods with limited access • retrieving custom IT policy rules from the IT policy API • installing applications using the BlackBerry Desktop Software • installing applications over the wireless network
<p><i>BlackBerry Java Development Environment BlackBerry Application Developer Guide Volume 2: Advanced Topics</i></p>	<ul style="list-style-type: none"> • using controlled APIs • using code signatures
<p><i>BlackBerry Signing Authority Tool Administrator Guide</i></p>	<ul style="list-style-type: none"> • understanding the BlackBerry Signing Authority Tool implementation of public key cryptography • installing, setting up, and managing the BlackBerry Signing Authority Tool • restricting access to APIs
<p><i>Placing the BlackBerry Enterprise Solution in a Segmented Network</i></p>	<ul style="list-style-type: none"> • using a segmented network implementation of the BlackBerry Enterprise Server • protecting BlackBerry Enterprise Solution components • protecting non-BlackBerry components on the corporate network • understanding BlackBerry Enterprise Server connectivity requirements • customizing the port numbers that the BlackBerry Enterprise Solution uses
<p><i>Policy Reference Guide</i></p>	<ul style="list-style-type: none"> • using BlackBerry Enterprise Server IT policies • using BlackBerry Enterprise Server application control policy rules • using BlackBerry MDS Services policy rules • understanding example IT policies and application control policies
<p><i>Security for BlackBerry Devices with Bluetooth Wireless Technology</i></p>	<ul style="list-style-type: none"> • understanding Bluetooth wireless technology • using and protecting Bluetooth enabled BlackBerry devices • understanding risks of using Bluetooth wireless technology on mobile devices

Appendix A: Examples of how to prevent potential vulnerability to malware attacks on BlackBerry devices

Preventing potential vulnerability to an application proxy attack

A malicious user can use the BlackBerry device in its default configuration to potentially access and attack servers internal to your corporate LAN. An external, malicious server could use a third-party Java application on the BlackBerry device as a proxy to contact servers on your corporate network for which it has IP addresses. A successful attack would result in the attacker making contact with an internal server or a user desktop or laptop computer on your corporate network.

The means by which attacks that proxy the BlackBerry device can occur require the following conditions:

Required condition	Options to prevent condition
Users must be able to download third-party Java applications onto their BlackBerry devices.	Set the Disallow Third Party Application Download IT policy rule to True, or use the other options listed in this table.
The ability to download third-party Java applications onto the BlackBerry device must not be limited to specific, trusted applications.	Assign an application control policy with the Disposition application control policy rule set to Required or Optional for specific, trusted applications only. Assign an application control policy with the Disposition application control policy rule set to Disallowed for unspecified or untrusted applications.
The BlackBerry device must prompt the user to allow HTTP connections from the third-party Java application domain and the protocol that the connections use.	Assign an application control policy with the External Network Connections application control policy rule set to Permitted or Prompt User for specific, trusted applications only. Assign an application control policy with the External Network Connections application control policy rule set to Not Permitted for unspecified or untrusted applications.
Applications on the BlackBerry device must be able to communicate with a target component of the BlackBerry Enterprise Server, or connect to a BlackBerry Enterprise Server component using BlackBerry MDS Services.	Assign an application control policy with the Internal Network Connections application control policy rule set to Permitted or Prompt User for specific, trusted applications only. Assign an application control policy with the Internal Network Connections application control policy rule set to Not Permitted for unspecified or untrusted applications.
Servers on your corporate network must be able to communicate with the malware server.	Use available corporate network security tools to protect your corporate network (for example, set the port numbers on the firewall protecting your corporate network to control outbound access).

Preventing potential vulnerability to a MAPI attack

A successful MAPI attack replaces a legitimate user's BlackBerry device on a BlackBerry Enterprise Server with the attacker's BlackBerry device so that the attacker can receive the legitimate BlackBerry device

user's email messages and access internal servers on your corporate network using the BlackBerry MDS Services (if the IT policy of the attacked BlackBerry device allows).

To perform a MAPI attack, a malicious user must run malware from a computer internal to your corporate network that is designed to replace a BlackBerry device PIN and device transport encryption key with new values. If the attacker knows the PIN of a BlackBerry device and can determine its device transport encryption key, the attacker can use malware to send a preconstructed MAPI request to change the BlackBerry device PIN and device transport encryption key values and send the new values to the Microsoft® Exchange Server. The malware then notifies the attacker that the BlackBerry Enterprise Server has added the BlackBerry device with the new values.

The means by which MAPI attacks can occur require the following conditions:

Required condition	Option to prevent condition
The malicious user must already be added to a BlackBerry Enterprise Server and authorized to use a BlackBerry device.	When the BlackBerry Administration Service starts, it checks your authentication credentials, determines your administrative role, and then displays a list of the tasks that you can complete. Only database users assigned the Security administrator (rim_db_admin_security) role can manage role membership. Only database users assigned the Security administrator, Enterprise administrator, Device administrator, or Senior help desk administrator roles can add BlackBerry device user accounts.
The malicious user must be allowed to switch to a different BlackBerry device.	Set the Desktop Allow Device Switch IT policy rule to False to prevent BlackBerry device users from switching to use other BlackBerry devices.

Part number: 9652937 Version 6

©2010 Research In Motion Limited. All Rights Reserved. The BlackBerry and RIM families of related marks, images, and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, "Always On, Always Connected", the "envelope in motion" symbol, and BlackBerry are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

The Bluetooth word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Research In Motion Limited is under license. Microsoft is either a registered trademark or trademarks of Microsoft Corporation in the United States and/or other countries. Sun, Java, and J2ME are either registered trademarks or trademarks of Sun Microsystems, Inc. in the United States and other countries. Wi-Fi is a trademark of the Wi-Fi Alliance. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

The BlackBerry device and/or associated software are protected by copyright, international treaties and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in various countries around the world. Visit www.rim.com/patents.shtml for a current list of RIM [as hereinafter defined] patents.

This document is provided "as is" and Research In Motion Limited and its affiliated companies ("RIM") assume no responsibility for any typographical, technical, or other inaccuracies in this document. RIM reserves the right to periodically change information that is contained in this document; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this document to you in a timely manner or at all. RIM MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR COVENANTS, EITHER EXPRESS OR IMPLIED (INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY, DURABILITY, TITLE, OR RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE REFERENCED HEREIN OR PERFORMANCE OF ANY SERVICES REFERENCED HEREIN). IN CONNECTION WITH YOUR USE OF THIS DOCUMENTATION, NEITHER RIM NOR ITS RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR CONSULTANTS SHALL BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER BE THEY DIRECT, ECONOMIC, COMMERCIAL, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR INDIRECT DAMAGES, EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA, DAMAGES CAUSED BY DELAYS, LOST PROFITS, OR A FAILURE TO REALIZE EXPECTED SAVINGS.

This document might contain references to third-party sources of information, hardware or software, products or services and, or third-party web sites (collectively the "Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by RIM of the Third-Party Information or the third-party in any way. Installation and use of Third-Party Information with RIM products and services may require one or more patent, trademark, or copyright licenses in order to avoid infringement of the intellectual property rights of others. Any dealings with Third-Party Information, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third-party. You are solely responsible for determining whether such third-party licenses are required and are responsible for acquiring any such licenses relating to Third-Party Information. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use Third-Party Information until all such applicable licenses have been acquired by you or on your behalf. Your use of Third-Party Information shall be governed by and subject to you agreeing to the terms of the Third-Party Information licenses. Any Third-Party Information that is provided with RIM products and services is provided "as is." RIM makes no representation, warranty, or guarantee whatsoever in relation to the Third-Party Information and RIM assumes no liability whatsoever in relation to the Third-Party Information even if RIM has been advised of the possibility of such damages or can anticipate such damages.