Reference Document: Security Behind BlackBerry

www.blackberry.com

Contents

Executive Summary

This reference document is based on the webcast entitled “Security Behind BlackBerry®.” Click here to view the webcast, or visit the BlackBerry Resource Center at:

http://resourcecenter.blackberry.com/index.php?cp=0&page=details&eventSelected=299

The goal of this document is to provide a better understanding of the security tools that come preinstalled with the BlackBerry solution. This document describes how to use these tools to better secure a BlackBerry deployment.

Webcast Summary

The following pages summarize the essential topics from the webcast entitled “Security Behind BlackBerry.”

The Value of Real-Time Information Delivery

Having access to information in real time is important. A study of mobile devices shows that users save time by having access to information at any time and in any place. When mobile devices are used, team efficiency increases by 29%. Direct cost savings are achieved through decreased RAS (Reliability, Availability, Serviceability), mobile phone and PDA (personal digital assistant) and pager usage. This study shows that 94% of users improved their ability to manage their inbox and 93% were able to convert downtime into productive time. In fact, typical users recover about an hour of downtime per day by catching up on email or setting up other types of sessions while in a cab, waiting for a meeting to start or waiting for elevators. These users make use of snippets of time during the day to be more productive. Recovering an hour of downtime every day also gives users more free time in the evening.

While having access to information allows users to recover downtime, security is equally important. For example, suppose an organization expands its existing corporate network. As a result, instead of just being a fairly localized environment that network now spans the globe. There are public network access points (kiosks) to the organization’s network available anywhere in the world. These kiosks are unlocked and provide full access to the network. This means confidential information is being sent to kiosks located all over the world.

Now suppose this kiosk is small enough to fit in the palm of a user’s hand or wear on a belt. This kiosk works almost anywhere in the world, is constantly connected to the organization’s network and is outside the organization’s firewall.

Mobile devices are powerful tools that extend beyond email. Users expect to have real-time access to information. They expect to have mobile devices that provide access to email, contacts and corporate data within the network. Users expect the ability to download existing applications and build new applications to run on mobile devices. This means an organization must expand its existing security boundaries to cover mobile devices. In other words, traditional security boundaries must be expanded to match user reality.

Security is no longer just a competitive concern. Security is about the ability to meet regulatory requirements. For example, public companies in the United States and companies in the financial industry must meet Sarbanes-Oxley (SOX) or Graham-Leach-Biliey legislative requirements. Any organization in the healthcare industry that handles patient information must meet HIPAA requirements. If an organization is unable to protect information, this can result in receiving fines or a jail sentence. Other industries face different compliance regulations with regard to the types of products that they can use. For example, there can be certification requirements for products. Finally, in a supply-chain environment, the partners with which an organization works may demand that proper solutions are in place to protect the partners’ data from being compromised.

Beyond any requirements that an organization might have to meet, information increasingly is becoming more sensitive and accessible thanks to mobile devices, so data must be secure and organizations must have the ability to prove that data is secure. It is not a good strategy to trust any vendor’s assurance that a product is secure. Instead, it is each organization’s responsibility to make sure the appropriate security is in place.

Benefits of the BlackBerry Platform

In the BlackBerry solution, security is not an afterthought. Security is one of the pillars of the BlackBerry solution.

Any type of mobile solution has many different components that must be included when establishing security. With the BlackBerry solution, there is no need to worry about the end points. The BlackBerry solution includes the BlackBerry device as well as the BlackBerry Enterprise Server™, which communicates with the device. It is an organization’s responsibility to make sure it can protect the data on those systems and any data transmitted between the device and the server. It is also important to ensure that users can maintain flexible access to this data. Therefore, the user is not responsible for keeping the BlackBerry device in a secure state.

As any type of solution grows, new technology and features will be added to that solution. This means an organization must ensure that these new features do not compromise the existing security of the product. For example, adding Bluetooth® to a product can open up a host of new attack vectors for people tempted to compromise the solution. Therefore, when considering adding a product like Bluetooth, be sure to add it in a secure manner and do not compromise what is already in place.

As previously mentioned, Research In Motion (RIM) has focused on security issues, including securing the BlackBerry device and data as it is sent between the device and the BlackBerry Enterprise Server. RIM ensures that its products work with various Internet standards, including S/MIME, TLS, Secure Sockets Layer (SSL) and PKI.

A BlackBerry device or any other mobile device is typically a corporate asset. Therefore, when the device is used within a corporation, that organization must ensure that corporate policies can also be applied to BlackBerry devices. For example, an organization may have established policies for acceptable use and security, which are applied to all other network appliances. Applying these policies to BlackBerry devices is essential.

RIM takes a holistic approach to securing BlackBerry devices. Security begins with hardware. RIM produces its own hardware, writes its own operating systems and the core applications. As a result, RIM can use the hardware as a trust anchor. When producing hardware at the manufacturing plant, a secure boot ROM is installed into that hardware. The secure boot ROM is then used to verify that only RIM-validated operating systems are allowed to be loaded onto the system. Without this type of trust anchor, an attacker could load software onto a user’s device and that user might never know this has happened. The trust anchor makes it possible to have confidence in the BlackBerry solution.

The operating system and applications are verified by the hardware. When a verified operating system is loaded onto the BlackBerry device, the operating system can ensure that any applications loaded afterwards have also been created and signed by RIM and have not been modified by an unauthorized user. This establishes a chain of trust because this process validates that no application has been corrupted or tampered with before it was installed on the device. Only authentic and authorized applications are allowed to run. Applications from third parties can be centrally managed by the BlackBerry Enterprise Server administrator and wirelessly deployed to all BlackBerry devices within an organization.

The BlackBerry Enterprise Server provides administrative control over all aspects of the platform, giving the administrator full control over applications, configuration and transport. The administrator can manage all options centrally and update all BlackBerry devices instantly and wirelessly.

When thinking about security, it is important to establish some ground rules. A BlackBerry device has more constraints than a laptop, although the BlackBerry device manages scarcity effectively. A BlackBerry device has limited computing power, storage, network capacity, network performance and battery life. It is necessary to juggle all of these constrained resources in order to provide the optimum user experience without compromising security.

It may seem counter-intuitive, but battery life is important to security. For example, suppose an organization tries to use a very chatty network protocol to protect transactions that go between a server and a device. As the number of packets sent increases, the battery life decreases. Faster processors and increased memory will use battery life at a faster rate. Higher data speeds require network capacity utilization.

An organization must ensure that security protocols are optimized as much as possible. This step is not just to ensure that the security protocols are more secure and have fewer bugs but also that they use the resources available in the most optimal manner possible. This results in using as little battery life and network capacity as possible.

As networks grow, it is easy to assume that network capacity will continue to grow without bounds and the problem with sending data will disappear. However, while larger networks provide more capacity, the problem is that they also support more users, including those using more bandwidth-intensive applications, such as streaming video. While the pipe may be bigger for sending information on the network, the information being sent through the pipe is larger as well. The net result is that the capacity does not change.

Battery life and network capacity do not follow Moore’s Law. An 8% to 10% increase in lithium ion technology for battery life is considered to be very good. Battery life does not have the same kind of growth rate as components like processors. It is important to take care in using available resources.

Mobile Security

Jack Gold is an industry analyst who examines the wireless industry. He was interviewed by *Computerworld* in June 2006 about mobile security. He listed nine main areas of concern that any customer evaluating a solution should consider. The following sections address Gold’s nine areas of concern, which include:

- Password protection
- Mobile management system
- User’s window into the organization
- Encryption of information
- Security standards for data travelling between devices and servers
- Virus and firewall protections
- Administrative control of a lost device
- Logging information
- Security must be comprehensive

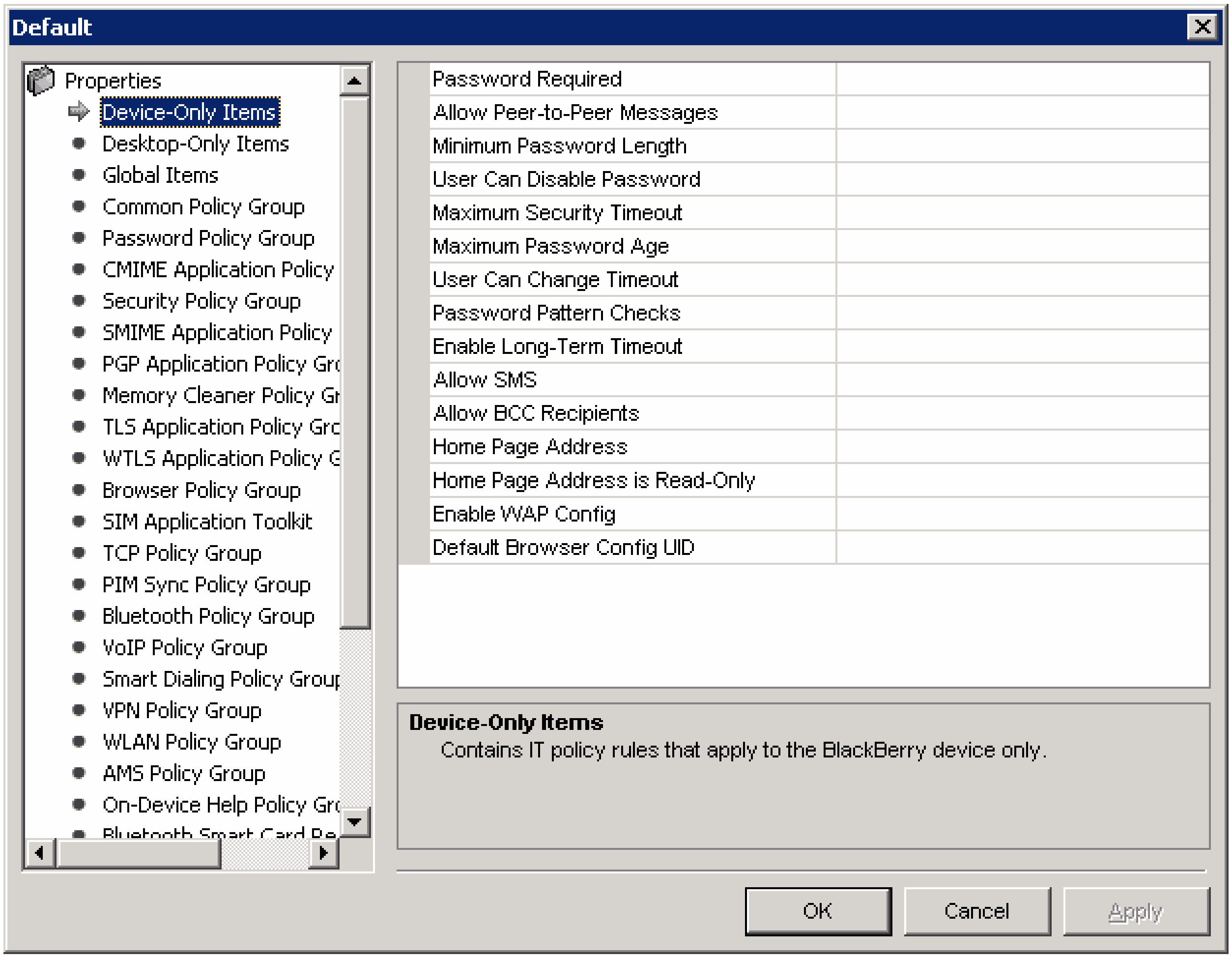
Password Protection

The first area of concern is enforcing password protection. Because users carry a mobile device, it is easy to lose. For example, users have walked away from a restaurant and accidentally left a mobile device or cell phone on a table. Therefore, it is essential for an administrator to have the ability to enforce password protection and other types of authentication from a central location. This way, it is not up to the user to solve the problem of password protection. Instead, this task is something that the administrator can do on behalf of the user by ensuring that password protection is set up on all BlackBerry devices.

With the BlackBerry device, there is the concept of IT policy. This concept makes it possible for an administrator to set a variety of properties that determine the ways in which a device can operate and be used. The administrator centrally sets these policies on specific or all BlackBerry devices. Policies are pushed over the air and applied automatically to the devices. The user does not have to do anything.

The administrator has a variety of policies that can be applied for passwords. These policies range from simply specifying whether a password needs to be used to more complex policies that give the administrator the ability to establish the period of time a password can cache on the device, complex rules for a password's appearance and specific formats for passwords. The administrator can set these policies and ensure that they are enforced on a user's device. Then if a device is lost, it is more difficult for an unauthorized user to access information on the device.

As shown in Figure 1 and Figure 2, IT policy items are split into various groups.

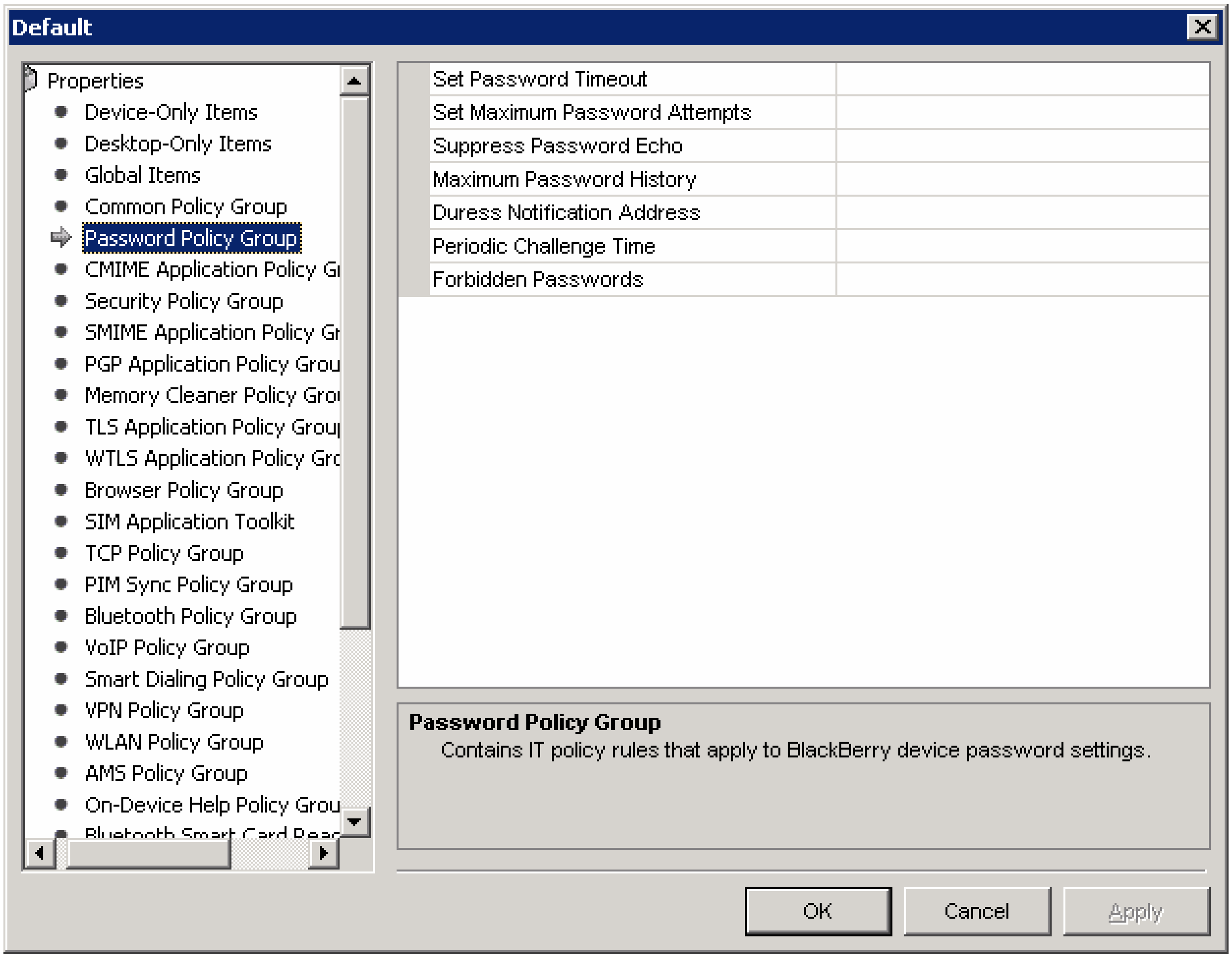


Properties
- Device-Only Items
- Desktop-Only Items
- Global Items
- Common Policy Group
- Password Policy Group
- CMIME Application Policy
- Security Policy Group
- SMIME Application Policy
- PGP Application Policy Gro
- Memory Cleaner Policy Gr
- TLS Application Policy Gro
- WTLS Application Policy G
- Browser Policy Group
- SIM Application Toolkit
- TCP Policy Group
- PIM Sync Policy Group
- Bluetooth Policy Group
- VoIP Policy Group
- Smart Dialing Policy Grour
- VPN Policy Group
- WLAN Policy Group
- AMS Policy Group
- On-Device Help Policy Gro
- Bluetooth Smart Card Re

Password Required
Allow Peer-to-Peer Messages
Minimum Password Length
User Can Disable Password
Maximum Security Timeout
Maximum Password Age
User Can Change Timeout
Password Pattern Checks
Enable Long-Term Timeout
Allow SMS
Allow BCC Recipients
Home Page Address
Home Page Address is Read-Only
Enable WAP Config
Default Browser Config UID

Device-Only Items
Contains IT policy rules that apply to the BlackBerry device only.

Figure 1. IT policy groups



- Properties
  - Device-Only Items
  - Desktop-Only Items
  - Global Items
  - Common Policy Group
  - Password Policy Group
  - CMIME Application Policy G
  - Security Policy Group
  - SMIME Application Policy Gr
  - PGP Application Policy Grou
  - Memory Cleaner Policy Grou
  - TLS Application Policy Grou
  - WTLS Application Policy Gro
  - Browser Policy Group
  - SIM Application Toolkit
  - TCP Policy Group
  - PIM Sync Policy Group
  - Bluetooth Policy Group
  - VoIP Policy Group
  - Smart Dialing Policy Group
  - VPN Policy Group
  - WLAN Policy Group
  - AMS Policy Group
  - On-Device Help Policy Grou
  - Bluetooth Smart Card Reac

Set Password Timeout	
Set Maximum Password Attempts	
Suppress Password Echo	
Maximum Password History	
Duress Notification Address	
Periodic Challenge Time	
Forbidden Passwords	

Password Policy Group
Contains IT policy rules that apply to BlackBerry device password settings.

Figure 2. IT Policy groups

At a minimum, it is a good practice to enable passwords for all BlackBerry device users. There is also a way to set the timeouts for how often a user must type in the password. Setting timeouts is controlled by administrators to allow them to meet their corporate security policies.

Along the same lines, if there are features on a BlackBerry device that the administrator does not like, IT policy can be used to shut those features off. For example, if the corporate policy is to not allow Bluetooth, then the administrator can shut off the Bluetooth radio. Or if Bluetooth is used only for connecting to headsets, then the administrator can shut off the other Bluetooth profiles, such as the serial port profile or the handsfree profile.

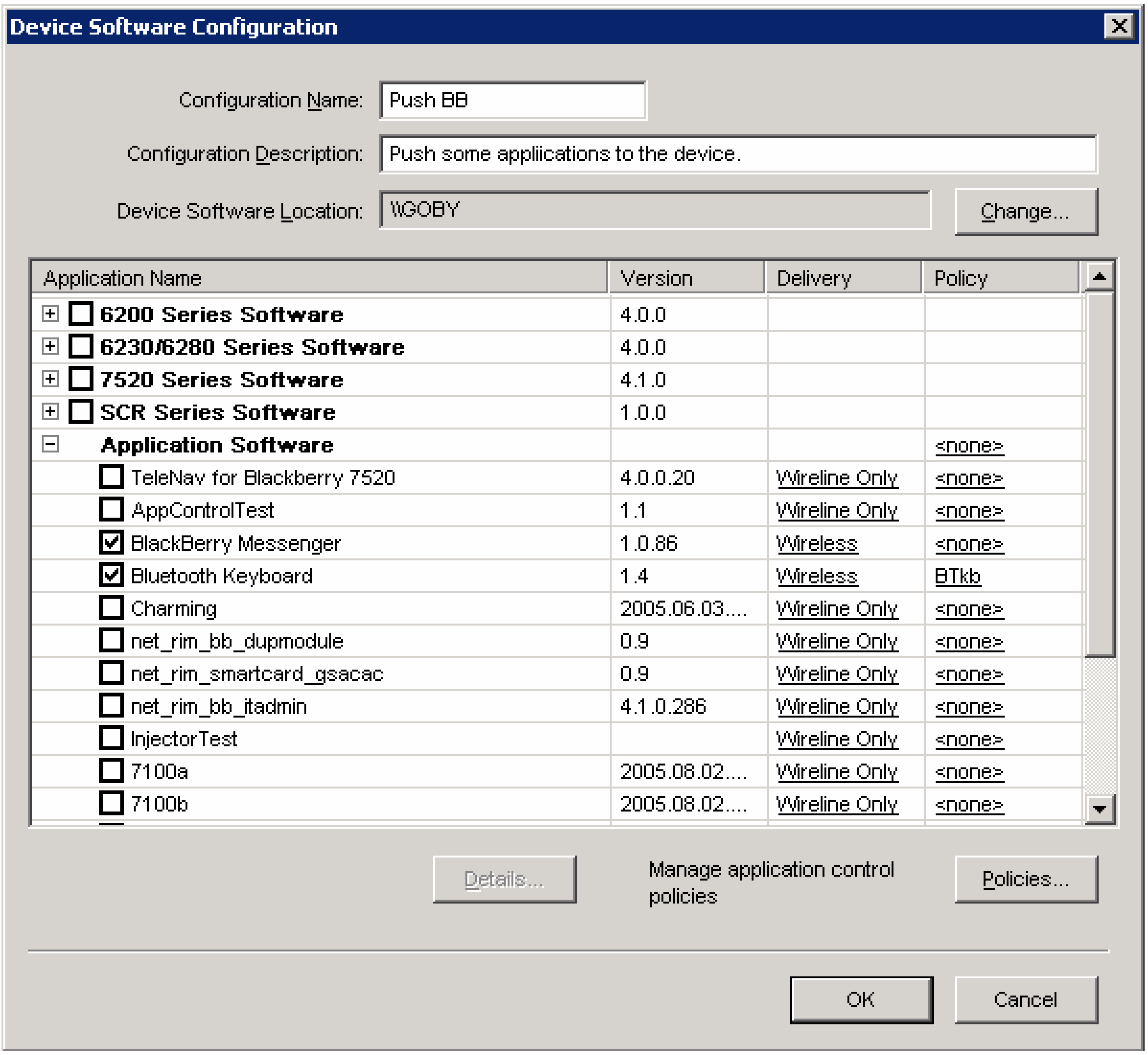
Mobile Management System

A mobile management system that enforces reasonable data security policies on the widest possible range of mobile, wireless devices should be installed. A mobile device is a corporate asset that needs to be controlled just like any other corporate asset. The administrator has many options for controlling BlackBerry devices.

As previously mentioned, IT policy lets the administrator set specific limitations on the ways in which users are allowed to use their BlackBerry devices. Furthermore, an administrator using device configuration can specify the types of applications that need to be on the device so that it will be allowed onto the network. For example, an organization in the real estate industry might have a Multiple Listing Service (MLS) application that all users need to have on their BlackBerry device. The administrator can specify that the MLS application is required on all the users' devices by using the management console.

When an administrator specifies that an application is required, that application is pushed out automatically over the air to the users. This means the application shows up on their BlackBerry devices and users cannot delete the application because it is required.

In addition to having the ability to decide which applications are and are not allowed, the administrator can establish limitations for applications on the BlackBerry device. This is possible by using the Application Control, which is the native solution that RIM provides for managing the risk of malware on the BlackBerry device. The Application Control is illustrated in Figure 3.


Device Software Configuration
Change...
Details...
Manage application control policies
Policies...
OK
Cancel

Configuration Name: Push BB

Configuration Description: Push some appliications to the device.

Device Software Location: \\GOBY

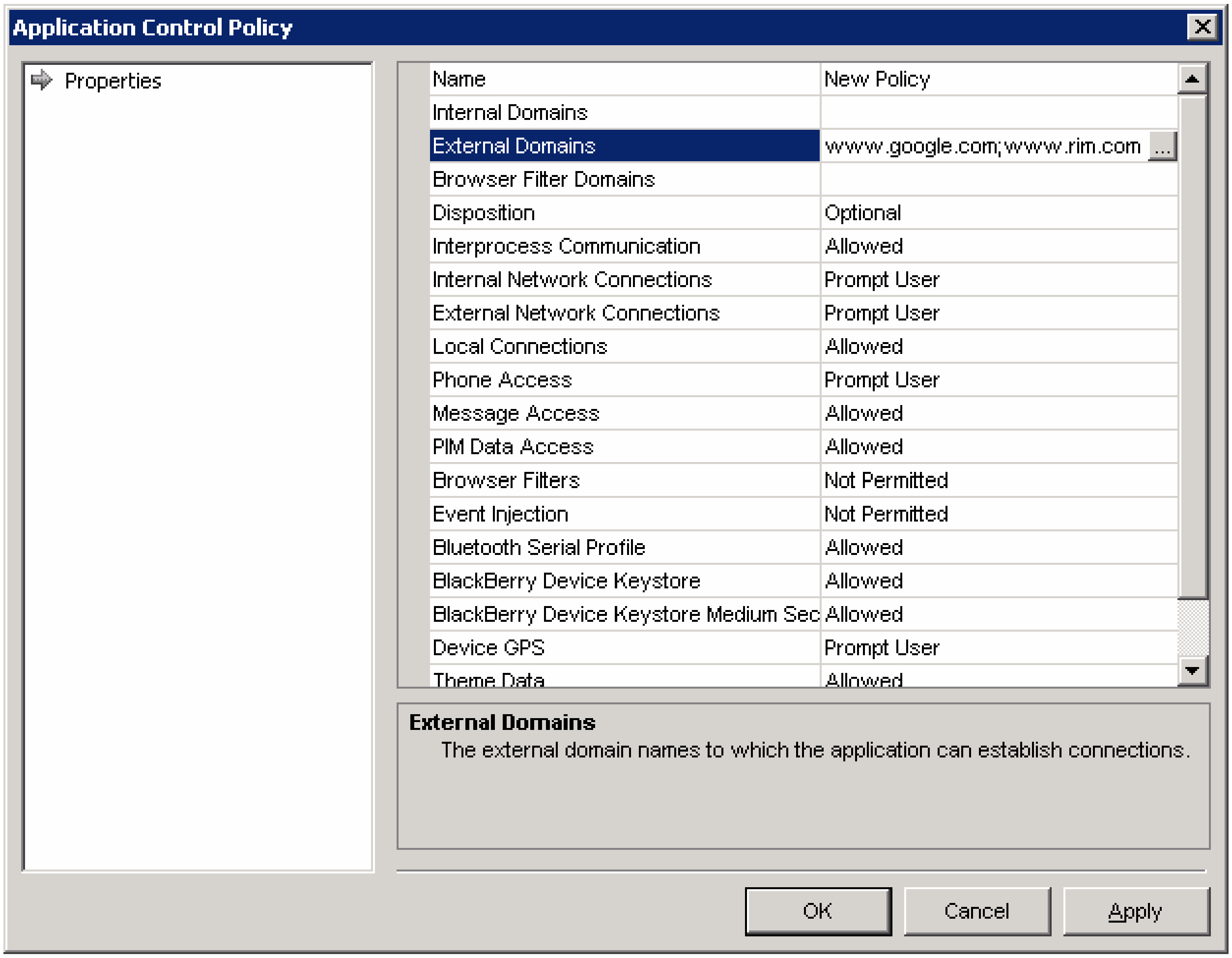
Application Name	Version	Delivery	Policy
⊞ □ **6200 Series Software**	4.0.0		
⊞ □ **6230/6280 Series Software**	4.0.0		
⊞ □ **7520 Series Software**	4.1.0		
⊞ □ **SCR Series Software**	1.0.0		
⊟ **Application Software**			<none>
□ TeleNav for Blackberry 7520	4.0.0.20	Wireline Only	<none>
□ AppControlTest	1.1	Wireline Only	<none>
☑ BlackBerry Messenger	1.0.86	Wireless	<none>
☑ Bluetooth Keyboard	1.4	Wireless	BTkb
□ Charming	2005.06.03....	Wireline Only	<none>
□ net_rim_bb_dupmodule	0.9	Wireline Only	<none>
□ net_rim_smartcard_gsacac	0.9	Wireline Only	<none>
□ net_rim_bb_itadmin	4.1.0.286	Wireline Only	<none>
□ InjectorTest		Wireline Only	<none>
□ 7100a	2005.08.02....	Wireline Only	<none>
□ 7100b	2005.08.02....	Wireline Only	<none>

Figure 3. Use Application Control to limit the risk of malware

User's Window into the Organization

Users need to have a window into the organization in order to access different types of information. An organization is likely to want some control over what mobile users are allowed to access through their devices. For example, the organization may want to limit access to Internet sites. Or there might be concern that, for example, in a situation in which specific web servers host sales information, users should not be allowed access to that information from their BlackBerry devices.

As shown in Figure 4, the administrator can use the Application Control to grant specific access to specific devices and limit the types of internal and external domains to which they are allowed to connect.



Name	New Policy
Internal Domains	
External Domains	www.google.com;www.rim.com
Browser Filter Domains	
Disposition	Optional
Interprocess Communication	Allowed
Internal Network Connections	Prompt User
External Network Connections	Prompt User
Local Connections	Allowed
Phone Access	Prompt User
Message Access	Allowed
PIM Data Access	Allowed
Browser Filters	Not Permitted
Event Injection	Not Permitted
Bluetooth Serial Profile	Allowed
BlackBerry Device Keystore	Allowed
BlackBerry Device Keystore Medium Sec	Allowed
Device GPS	Prompt User
Theme Data	Allowed

External Domains
The external domain names to which the application can establish connections.

Figure 4. Application Control limits domains

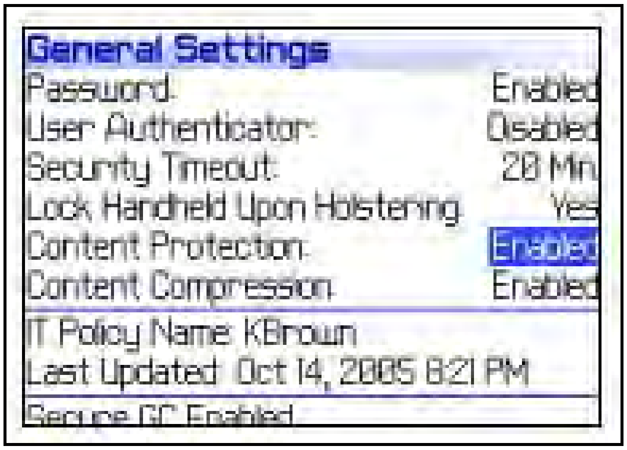
For example, a mobile device may be allowed to access only a certain set of web servers in a company. These web servers are used only for hosting customer information, meaning CRM information. That is a powerful strategy, because it allows travelling salespeople to have access to their customer information, which is probably one of the main reasons they should have a BlackBerry device. At the same time, these users should not have access to Human Resources information, which is very sensitive information that should stay within that department.

An administrator can also set up extra authentication on web services. The BlackBerry solution provides out-of-the-box support for RSA SecurID®, which is used to limit access to authorized users. When using RSA SecurID for limiting access to web servers, users will receive those prompts from their device. They will have to enter the RSA SecurID token number in order to be granted access to the web service from their devices.

Encryption of Information

The need for encryption of information is essential, whether it is on a BlackBerry device or being sent to or from the device. Solutions are different in the mobile world vs. the wired world. In the mobile world, information is broadcast from a device, which has a radio. The BlackBerry solution provides several out-of-the-box solutions to protect data at rest (data stored on the device) and data in motion (data in transit between the device and the backend server).

Content protection is offered for data at rest. With content protection, all user data on the BlackBerry device is stored in an encrypted format. This is something that the administrator can enforce for a user and that the user can enforce as well. Figure 5 shows the Content Protection setting as Enabled.



General Settings

Password:	Enabled
User Authenticator:	Disabled
Security Timeout:	20 Min
Lock Handheld Upon Holstering	Yes
Content Protection:	Enabled
Content Compression:	Enabled

IT Policy Name: KBrown
Last Updated: Oct 14, 2005 8:21 PM

Secure GC Enabled

Figure 5. Enabling content protection

For data in motion, Advanced Encryption Standard (AES) and Triple DES encryption are supported for protecting data that goes between the BlackBerry device and the server.

When making the decision to use AES or Triple DES encryption, it is important to understand the history of each. When the first BlackBerry device was sold in 1999, Triple DES was the de facto standard for protecting information worldwide, whether in the financial or the government sector Triple DES is what RIM uses for protecting any information sent between the BlackBerry device and the server. In 2001 the United States government created a new algorithm called AES for protecting government information. As the industry moved to using AES for protecting information, RIM added support for use in protecting the BlackBerry solution. BlackBerry Enterprise Server v4.0 included support for AES. Using AES with a BlackBerry device requires having BlackBerry Enterprise Server v4.0 and BlackBerry Device Software v4.0. RIM still supports Triple DES for legacy reasons. Organizations that have BlackBerry devices and servers that are all v4.0 or later should use AES, because it is a more secure and efficient algorithm than Triple DES.

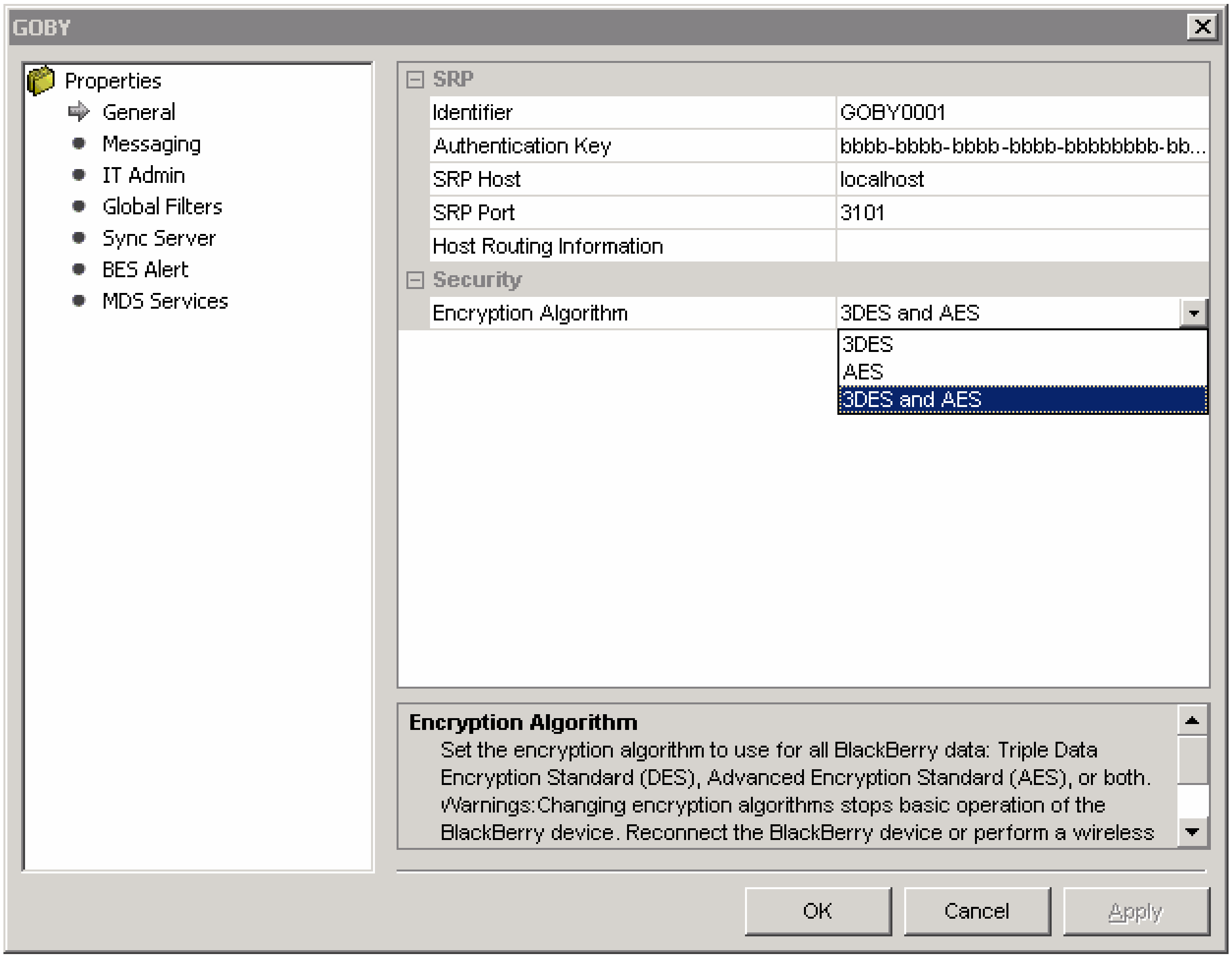
For organizations that have concerns beyond protecting data at rest and data in motion, there are add-ons, such as S/MIME and PGP. These add-ons address a need for more secure email being sent between organizations. This kind of need goes beyond the concern of sending information between a corporate server and the BlackBerry device.

If an organization already is using S/MIME and PGP, then it should use them with the BlackBerry solution to make it possible for BlackBerry device users to read any S/MIME-encrypted or PGP-encrypted messages they receive. Whether it is necessary to use S/MIME and PGP with the BlackBerry solution depends on the organization. When sending a message from a BlackBerry device to a user outside the organization, that message is sent from the BlackBerry device to the organization’s mail server. That connection is protected using BlackBerry transport encryption. But when the message is sent from the organization’s mail server to another organization’s mail server, that message traverses the Internet in the same way as a message sent from a desktop. For an extra level of assurance with regard to protecting information as it travels over the Internet, then use S/MIME or PGP within the organization from desktops and BlackBerry devices.

Security Standards for Data Travelling between Devices and Servers

There is a need to enforce security standards for any data that travels between BlackBerry devices and backend servers. As previously mentioned, the BlackBerry solution provides the administrator with many controls.

The administrator has the ability to specify the types of algorithms used to protect information sent between the BlackBerry device and the BlackBerry Enterprise Server. The BlackBerry Manager provides fine-grained control over the security settings of deployed BlackBerry devices. For example, in Figure 6, the administrator can choose the algorithm to be used for the BlackBerry transport encryption. In this case, administrators can choose between using Triple DES or AES. Alternatively, they can use both, for example, if the organization has a mix of older devices in the environment.



SRP

Identifier	GOBY0001
Authentication Key	bbbb-bbbb-bbbb-bbbb-bbbbbbbb-bb...
SRP Host	localhost
SRP Port	3101
Host Routing Information	

Security

Encryption Algorithm	3DES and AES

Encryption Algorithm

Set the encryption algorithm to use for all BlackBerry data: Triple Data Encryption Standard (DES), Advanced Encryption Standard (AES), or both. Warnings:Changing encryption algorithms stops basic operation of the BlackBerry device. Reconnect the BlackBerry device or perform a wireless

Figure 6. Use the BlackBerry Manager to set security for BlackBerry devices

Virus and Firewall Protections

There is also the need for virus and firewall protections on mobile devices. It is becoming more and more common to see reports in the media of different types of malware specifically designed for mobile devices. Many types of malware in the past have been focused on the Symbian operating system but there is now malware, such as Red Browser, specifically targeted at Java™ devices, which includes BlackBerry devices. To protect against malware, RIM provides out-of-the-box support for the Application Control.

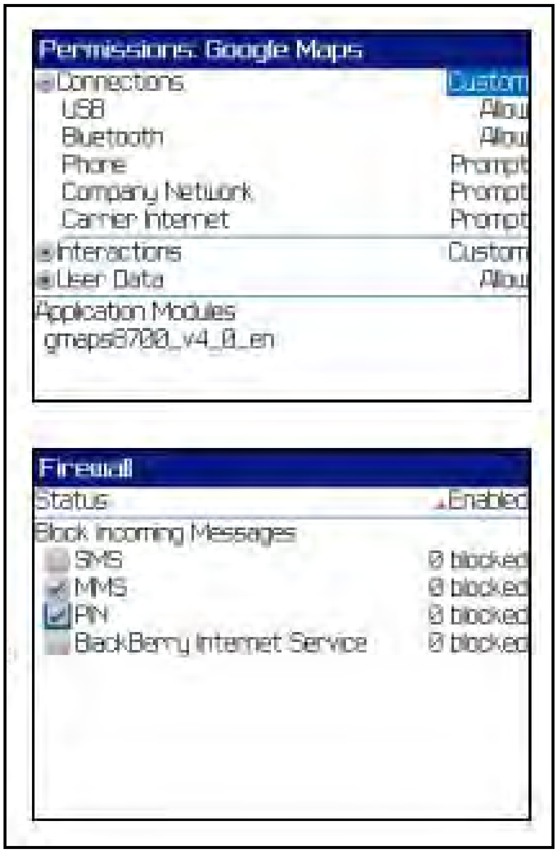
When trying to protect a device against malware or viruses, there are two tasks that should be performed. The first task is detection. This means determining if an application is malware. The second is containment. Once an application has been determined as malware, containment means preventing that malware from causing harm to the BlackBerry device.

Detection is very difficult in the mobile world. This is because detection requires either having a large database of information stored on a BlackBerry device (which does not work well because the device is space-constrained) or access to backend servers (which can perform signature checking). Accessing a server is not always possible when using a mobile device because that device may not be in a coverage area that allows access.

Therefore, the focus is on containment. By using the Application Control, the administrator can control the following elements:

- User data that can be accessed
- Device resources that can be accessed
- Connections that can be made

Figure 7 illustrates the settings on the BlackBerry device that can be made with Application Control for containment of malware.



Permissions: Google Maps

Connections Custom
USB Allow
Bluetooth Allow
Phone Prompt
Company Network Prompt
Carrier Internet Prompt
Interactions Custom
User Data Allow

Application Modules
gmaps8700_v4_0_en

Firewall

Status Enabled

Block Incoming Messages
☐ SMS 0 blocked
☑ MMS 0 blocked
☑ PIN 0 blocked
☐ BlackBerry Internet Service 0 blocked

Figure 7. Using Application Control to contain the threat of malware

Suppose a user's BlackBerry device has a game, and the user wants that application to access the Internet in order to send high game scores to other players or to a web site. However, the organization is not comfortable with the game accessing the phone, the corporate network or user data (such as email or the user's address book). Using Application Control, the administrator can specify default configurations for the tasks that applications can and cannot perform on the BlackBerry device and then set specific configurations. On the other hand, when an application is trusted, the administrator can specify looser controls on that application because some due diligence has already been performed. The application is known as a safe application that can be deployed in the organization’s network.

The user also has the ability to set the user settings. When the administrator sets controls for the device, this translates to setting minimum-security controls for the device. The user can specify more stringent controls that further limit the settings specified by the administrator. For example, although the administrator might be comfortable specifying that any application downloaded by the user can access Bluetooth, the user may not want any application to access Bluetooth. The user can limit applications by default from accessing Bluetooth.

Using Application Control provides an effective containment mechanism. If a user downloads malware, it cannot do anything to harm the device because the malware has been sandboxed, meaning it only has access to its own resources and cannot access any of the user’s or the company’s resources.

In the upcoming release of BlackBerry Device Software v4.2, there is the ability for the user to set up a firewall on the device for blocking unwanted incoming messages. For example, if users are concerned about Short Message Service (SMS) SPAM, then they can shut off receiving SMS on their devices. The device will receive the message, but the user will never see it. Therefore, incoming spam messages are hidden. Using the firewall application, users can control SMS, Multimedia Messaging Service (MMS), PIN-to-PIN messages and email coming from the BlackBerry Internet Service™. Like any other BlackBerry device feature, the administrator can also control these settings.

Administrative Control of a Lost Device

With any mobile device, there is a constant concern about losing BlackBerry devices, as previously mentioned. The administrator needs to have the ability to control a device effectively when it is no longer in the designated user’s hands.

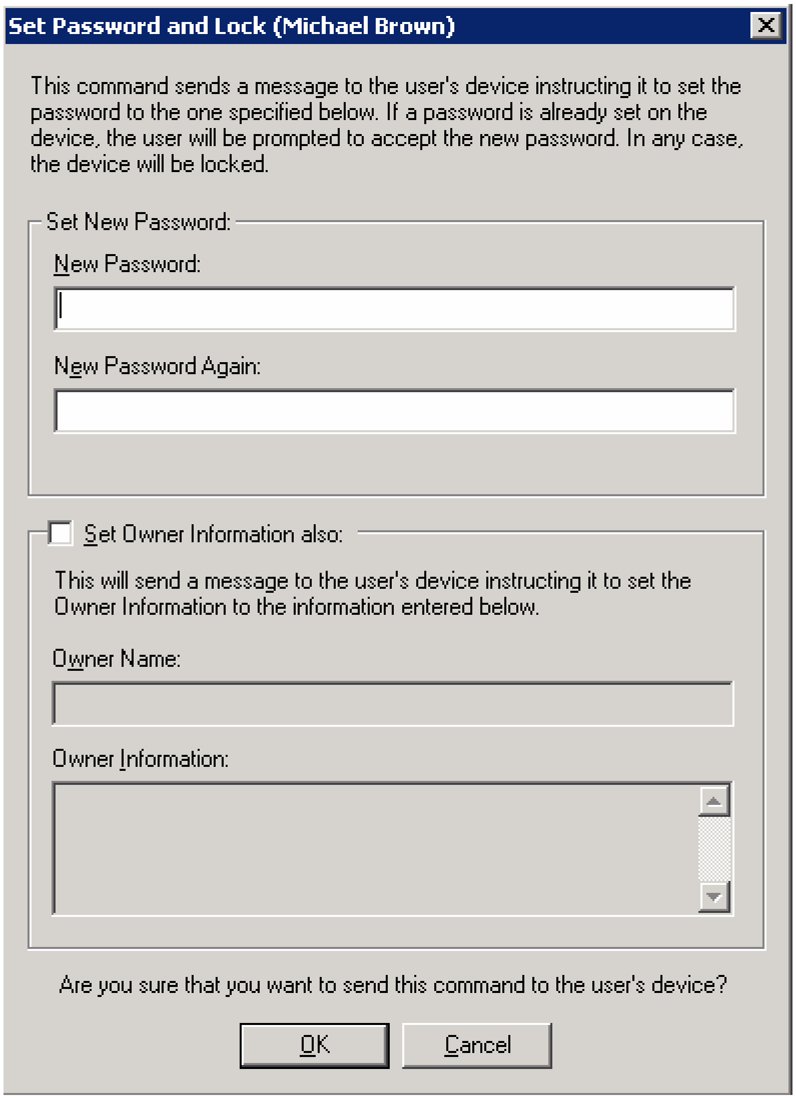
By using IT commands the administrator can perform the following tasks:

- Set owner information.
- Remotely lock a BlackBerry device.
- Reset that device’s password.
- Send a Kill command to wipe all the data from that device.

Setting owner information means the administrator can enter information into the BlackBerry device that can be seen by anyone who finds that device. This information is the name of the company that owns the device and the address to which it should be returned.

The administrator can also remotely lock a device. If someone picks up a lost device, it is not possible to use it without entering a password that unlocks the device. This provides another level of assurance.

As shown in Figure 8, the administrator has the ability to set a new password for a device.



This command sends a message to the user's device instructing it to set the password to the one specified below. If a password is already set on the device, the user will be prompted to accept the new password. In any case, the device will be locked.

This will send a message to the user's device instructing it to set the Owner Information to the information entered below.

Are you sure that you want to send this command to the user's device?

Figure 8. Setting a new password for a BlackBerry device

If a user is certain that the device is lost, and the administrator is concerned about information on the device falling into the wrong hands, it is possible to send a Kill command over the air. When the device receives this Kill command, that command automatically wipes all user information from the device. The execution of the Kill command returns the device to its factory default state. Therefore, the administrator has an over-the-air ability to lock down and kill any devices that go missing or are believed to be compromised within the organization.

When the Kill command is sent from the server, it is addressed to a specific BlackBerry device by using the personal identification number (PIN) of that device. If the device is lost and the battery dies before that device can receive the Kill command, then the device cannot receive or respond to the Kill command. The BlackBerry Enterprise Server reports whether a command has been received.

If the same user gets a new device, there is no need to worry. The Kill command will not be sent to that user’s new device because the Kill command is addressed to only the lost device.

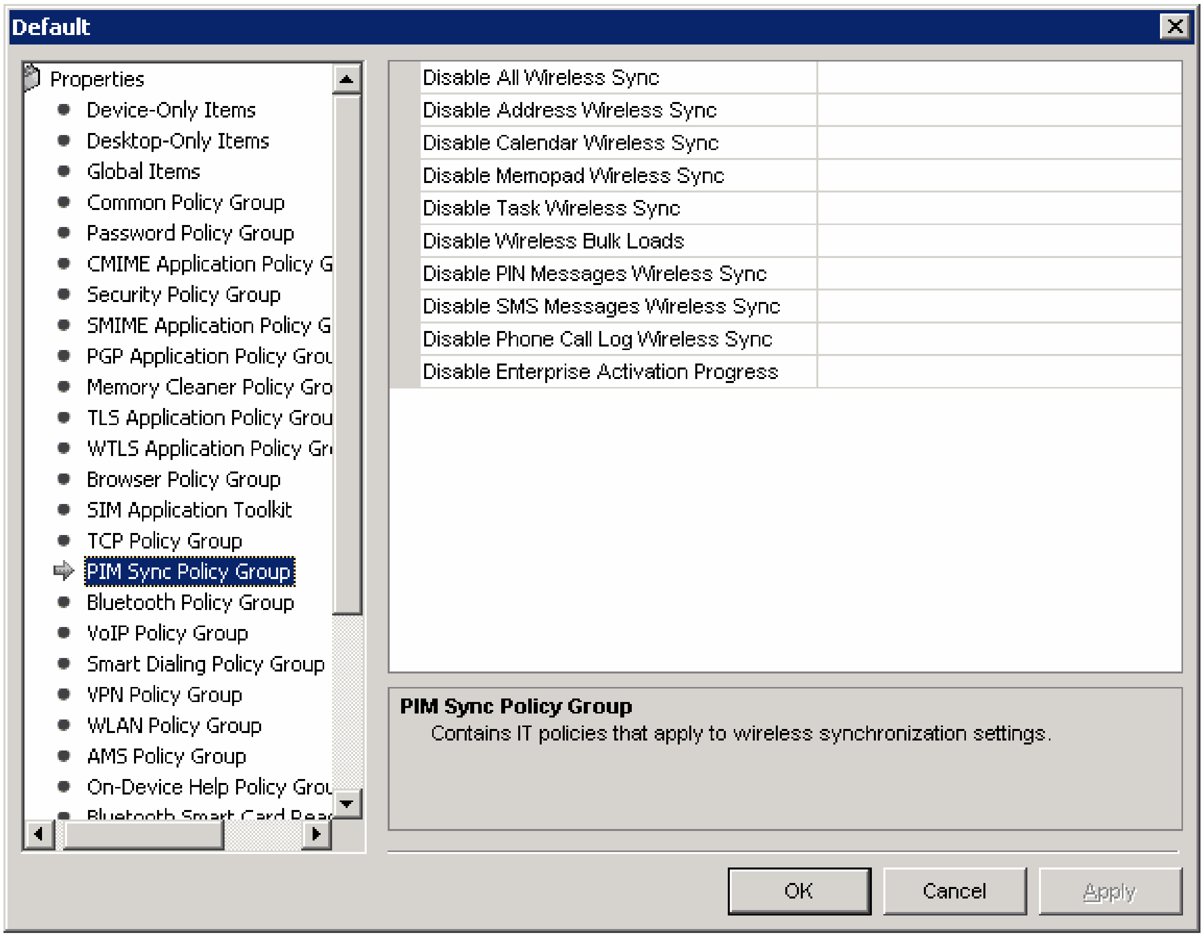
If an employee loses a BlackBerry device but finds it within a few minutes, there should be no security problem with that device as long as a password was set. If there is any concern that someone might have tampered with the device, such as trying to read information or installing an application onto the device, it is a good practice to wipe the device by using a Kill command or by using the security options and selecting Wipe Device. This will remove all user information from the device. Alternatively, the BlackBerry Enterprise Server console can be used to wipe all information (including applications) from the device and then reload a known set of applications back onto the device. Losing a BlackBerry device is similar to losing a laptop and being concerned about whether it has been tampered with. When a laptop is lost, most people will wipe the laptop and re-image it. The same approach should be taken when a BlackBerry device is lost for more than a few minutes.

Logging Information

Because the BlackBerry solution is a network appliance, an organization’s existing network login capabilities apply to traffic sent from the BlackBerry device. The administrator also can log specific BlackBerry device usage. Having logged information available allows an organization to stay within its compliance regulations. The administrator can turn on the ability to log the following information:

- PIN-to-PIN messages
- Peer-2-Peer messages
- SMS and MMS messages
- Information about any phone calls made from the device

Figure 9 illustrates examples of logging information.



Disable All Wireless Sync	
Disable Address Wireless Sync	
Disable Calendar Wireless Sync	
Disable Memopad Wireless Sync	
Disable Task Wireless Sync	
Disable Wireless Bulk Loads	
Disable PIN Messages Wireless Sync	
Disable SMS Messages Wireless Sync	
Disable Phone Call Log Wireless Sync	
Disable Enterprise Activation Progress	

PIM Sync Policy Group
Contains IT policies that apply to wireless synchronization settings.

Figure 9. Logging information

Educating Users

It is important to educate users and corporations about the security concerns for the products they use and how to address those concerns. With the BlackBerry solution, the goal is to provide all the information about security related to BlackBerry products from one central location—www.blackberry.com/security. This clearinghouse provides security-related product information for the BlackBerry solution, security White Papers outlining the BlackBerry solution, add-on products information, protocol information, third party certifications and information about the RIM security response team that handles security vulnerabilities and discusses remediation strategies.

Security Must be Comprehensive

Security must be comprehensive, ranging from password controls to logging mechanisms to protecting devices from malware and viruses. The BlackBerry solution strives to be comprehensive by giving the administrator the tools to control a device and its applications, as well as the different elements involved in a BlackBerry solution.

The BlackBerry solution provides encryption to ensure confidentiality in the following ways:

- AES or Triple DES encryption is provided for all data transmitted to and from a BlackBerry device.
- AES encryption is provided for protecting all data stored on a BlackBerry device.
- Well-known and studied schemes, including AES, Triple DES, Elliptic Curve Cryptography (ECC) and SkipJack, are supported.
- Module self-tests and integrity checks are provided.

Robust remote IT management is provided by wireless administration, configuration management, remote device lock, the Kill command and data wipe. The administrator has strict control of more than 200 device options from the server. The Internet security standards that are supported include S/MIME, PGP, Transport Layer Security (TLS), SSL and Java. Full application control gives the administrator the ability to allow or disallow third party applications. The administrator also has granular IT controlled access to APIs and user data.

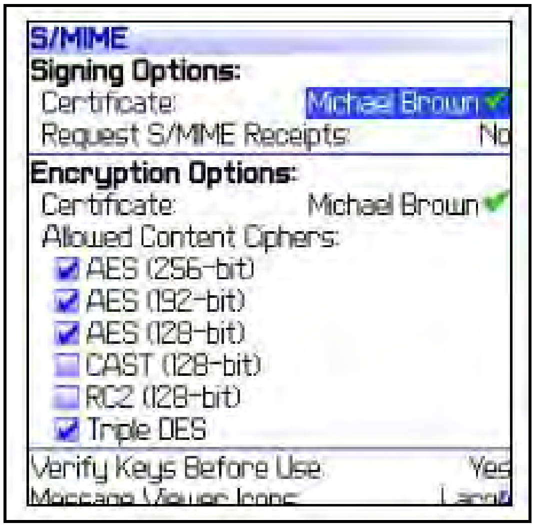
Security Extensions

RIM also offers solutions for an organization’s specific needs, such as the use of secure email. For example, suppose an organization uses S/MIME for signing and encrypting email, whether communicating within the organization or with external organizations. This is supported with the BlackBerry solution through the add-on S/MIME support package. This package includes the following features:

- Compatibility with Microsoft® Exchange (BlackBerry Enterprise Server v3.5 and higher) and IBM® Lotus® Domino® (BlackBerry Enterprise Server v4.1 SP2)
- Ability to send and receive signed and/or encrypted messages directly from the BlackBerry device
- Complete PKI support with OTA Lightweight Directory Access Protocol (LDAP), Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL)
- Can be used to protect PIN-to-PIN messages
- Fully controlled through IT Policy
- Smartcard support (including the Department of Defense’s Common Access Card (CAC))

The BlackBerry solution is the only S/MIME client available for mobile devices that supports elliptic curves. Out-of-the-box support is available for NSA Suite B, which is a set of algorithms that the United States’ National Security Agency created for protecting secret and top secret information.

RIM also supports PGP, which is very similar to S/MIME in that it is a secure email product for signing and encrypting messages. Options for signing and encryption are illustrated in Figure 10.



S/MIME
Signing Options:
Certificate: Michael Brown ✓
Request S/MIME Receipts: No
Encryption Options:
Certificate: Michael Brown ✓
Allowed Content Ciphers:
☑ AES (256-bit)
☑ AES (192-bit)
☑ AES (128-bit)
□ CAST (128-bit)
□ RC2 (128-bit)
☑ Triple DES
Verify Keys Before Use: Yes
Message Viewer Icons: Large

Figure 10. Signing and encryption options

There is full support for Exchange and Lotus Domino. The BlackBerry solution is also a fully-compliant PGP satellite product. This means organizations using the PGP Universal Server v9.0.2 or higher can use the BlackBerry device within that environment.

The BlackBerry Smart Card Reader

A smart card is a wearable peripheral. Smart cards are small and lightweight, have long battery life and provide easy operation. Some organizations use smart cards for secure email, secure storage of certificates and private keys or two-factor authentication. Smart cards are used as an extra mode of authentication for logical access control to an organization's network appliances.

The BlackBerry Smart Card Reader™ provides a wireless solution for using smart cards with BlackBerry devices. The BlackBerry Smart Card Reader uses the proven RIM secure Java Virtual Machine (JVM) with a FIPS-140-2 validated encryption module for protecting data that goes between the BlackBerry device and the BlackBerry Smart Card Reader. Rather than relying on Bluetooth for security, an AES-256 encrypted channel is layered on top of Bluetooth to protect information transmitted.

The administrator has a significant amount of control around how to use smart cards with the BlackBerry device. Using the IT Policy, the administrator can force the user to always log in using a smartcard. If using S/MIME, then the administrator can make it necessary to use smart cards with S/MIME. This makes it impossible to use soft certificates from a user's desktop. Instead, users can only use private keys that are stored on the smart card itself.

Like any BlackBerry products, the BlackBerry Enterprise Server administrator can specify IT policies through the BlackBerry Enterprise Server to control the BlackBerry Smart Card Reader. There are always security concerns with regard to Bluetooth, and RIM has taken pains to protect information sent across the Bluetooth link. The BlackBerry Smart Card Reader has been involved in extensive security audits conducted by Booz Allen Hamilton, commissioned by the United States Army, where the product passed the test.

There is out-of-the-box support for Safenet 330 cards, which is what the Canadian federal government uses. There is also support for the Common Access Cards (CAC) used by the U.S. Department of Defense. In addition, all of the tools needed to write drivers for any smart card are available through the BlackBerry Java Development Environment (BlackBerry JDE). Therefore, any third party can develop a driver that can be used with its own smart cards for use with BlackBerry devices.

Communication without Compromise

The focus at RIM is “trust, but verify.” Through a variety of BlackBerry security validations, the goal is to offer better assurances that the BlackBerry solution performs in the way it is promised to perform. For example, in the United Kingdom, the BlackBerry device is the first and only mobile device that has been through the CAPS program, which is an invitation-only program run by CESG. The BlackBerry solution has been approved for use for restricted information in Her Majesty’s Government in the United Kingdom. RIM has been involved in the FIPS 140-2 program in the United States and Canada for many years, and all BlackBerry products go through that process. This program ensures that the cryptography used on BlackBerry devices is implemented correctly. Other governments that have approved the BlackBerry solution include Australia, New Zealand and Austria. The BlackBerry solution has also been approved for restricted communications within NATO.

Figure 11 shows countries and their security validation approval of the BlackBerry solution, as well as countries in which certifications are in progress.

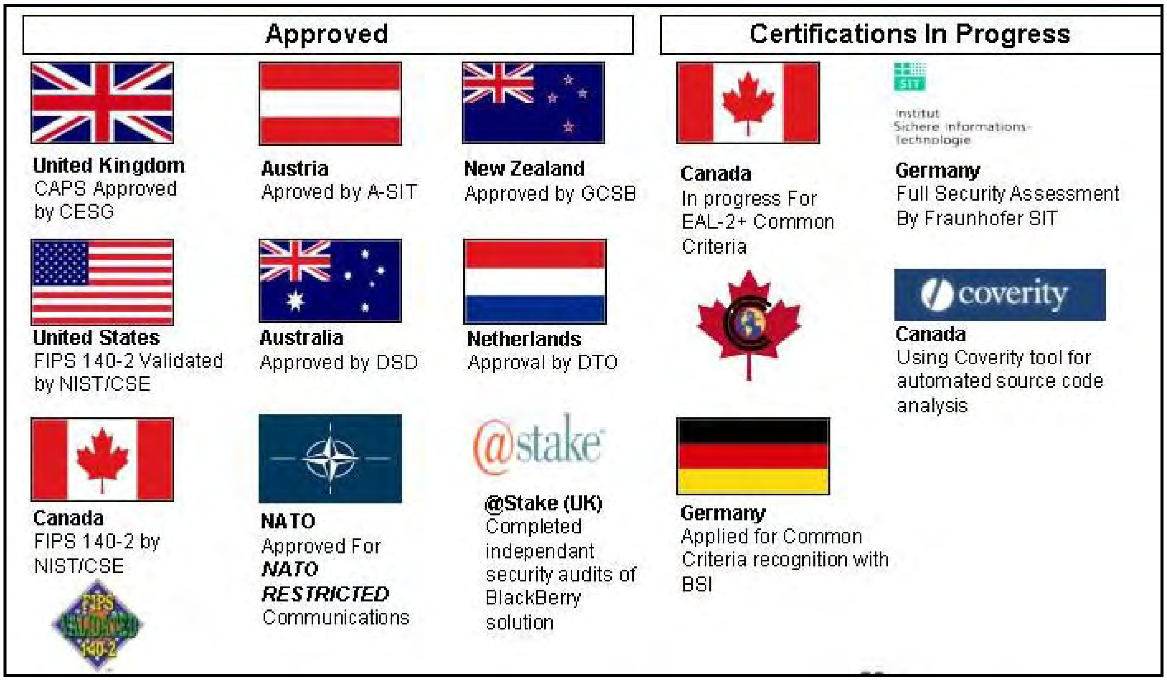


Figure 11. BlackBerry security validations

RIM is involved in the Common Criteria program and has a product going through for EAL-2+ certification. RIM is also involved in a very detailed security assessment being run by the Fraunhofer Institute in Germany. Finally, RIM uses the Coverity tool for automated source code analysis. This provides analysis to fix many common issues that can plague software products such as memory leaks and buffer overflows. Being involved in as many certification processes as possible, whether third party or government-initiated, gives RIM customers the best assurance that the BlackBerry solution is handling their users’ data properly.

Each version of software has new security features. RIM works hard to lock down any security issues. However, while a new version of software offers new features, it might also have new issues. If an organization is comfortable with a version of software that has proven to be stable, then when considering a new version of that software it is important to evaluate its new features.

An organization’s desire for specific features and security improvements will influence the decision whether to upgrade.

Summary

As mobile devices become more common and more powerful, security becomes a more important consideration. The BlackBerry solution provides an advantage because security has always been a priority in product design. RIM has the advantage of producing the hardware, software and operating system for the BlackBerry solution. However, any organization must take the appropriate steps to make sure it can protect data on the BlackBerry Enterprise Server and the BlackBerry devices that are deployed. These steps include ensuring security when adding new technology or products other than the BlackBerry solution. Furthermore, corporate policies should be applied to the BlackBerry solution.

Analyst Jack Gold has described nine areas of concern that customers should consider before purchasing mobile devices. These concerns are password protection, mobile management system, the user’s window into the organization, encryption of information, security standards for data travelling between devices and servers, virus and firewall protections, administrative control of a lost device, logging information and comprehensive security. This document describes the way in which the BlackBerry solution addresses each of these concerns.

Additional Resources

To determine which version of the server has various security improvements, look at the release notes associated with a product. There is also a BlackBerry Security White Paper available at www.blackberry.com/security and new versions of that White Paper correspond with new releases. It contains a “What’s New?” section that lists the security features in a new product.

*Check with service provider for availability, roaming arrangements and service plans. Certain features outlined in this document require a minimum version of BlackBerry Enterprise Server software, BlackBerry Desktop Software, and/or BlackBerry Device Software. May require additional application development. Prior to subscribing to or implementing any third party products or services, it is your responsibility to ensure that the airtime service provider you are working with has agreed to support all of the features of the third party products and services. Installation and use of third party products and services with RIM's 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. You are solely responsible for determining whether such third party licenses are required and are responsible for acquiring any such licenses. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use these products and services until all such applicable licenses have been acquired by you or on your behalf. Your use of third party software shall be governed by and subject to you agreeing to the terms of separate software licenses, if any, for those products or services. Any third party products or services that are provided with RIM's products and services are provided "as is". RIM makes no representation, warranty or guarantee whatsoever in relation to the third party products and services and RIM assumes no liability whatsoever in relation to the third party products and services even if RIM has been advised of the possibility of such damages or can anticipate such damages.

The 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; D,445,428; D,433,460; D,416,256. Other patents are registered or pending in various countries around the world. Please visit www.rim.net/patents.shtml for a current listing of applicable patents.

This document is provided "as is" and Research In Motion Limited (RIM) assumes 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 AFFILIATED COMPANIES AND THEIR 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 and/or third party web sites ("Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, 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 in any way. Any dealings with third parties, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third party. RIM shall not be responsible or liable for any part of such dealings.