BlackBerry Enterprise Server Wireless Software Upgrades

Version: 4.1 | Service Pack: 7

Administration Guide

BlackBerry

Published: 2009-10-30
SWDT207654-207654-1030044737-001

Contents

Upgrading the BlackBerry Device Software over the wireless network

1

Wireless software upgrades

Wireless software upgrades are designed to allow you to manage upgrades of the BlackBerry® Device Software over the wireless network for the BlackBerry devices in your organization.

You can use the BlackBerry® Enterprise Server to send software upgrade packages to users with BlackBerry devices that support wireless software upgrades. To receive upgrade requests that you send over the wireless network, or to download, reject, defer, install, or cancel wireless software upgrades, users are not required to connect their supported BlackBerry devices to their computers.

Sources of software upgrade requests

Source	Description
administrators of the BlackBerry® Enterprise Server	By default, you can use the BlackBerry Manager to view and send wireless software upgrade requests to supported BlackBerry devices.
BlackBerry device users	If you permit, BlackBerry device users can request wireless software upgrades or make cancellation requests using their BlackBerry devices.
wireless service providers	If you permit, wireless service providers can search for, send, and monitor wireless software upgrades using the BlackBerry® Provisioning System administration web site.

Applications that the wireless software upgrade process supports

The wireless software upgrade process supports BlackBerry® Device Software applications that Research In Motion creates. It does not support upgrading instant messaging applications or other third-party applications on the BlackBerry device.

During the wireless software upgrade process, as in the wired software upgrade process, if the upgrade process is upgrading third-party applications on the BlackBerry device, the BlackBerry device deletes all data for third-party applications that are both designed not to use synchronization and designed to use RIM persistent APIs on the BlackBerry device. The upgrade process does not delete third-party applications from the BlackBerry device.

Types of software upgrade packages

Software upgrade packages that Research In Motion makes available on the BlackBerry® Infrastructure can introduce new features and address known software issues on BlackBerry devices.

Type	Description
platform update	• applies to applications on the BlackBerry device other than Java® applications (for example, the software for the JVM, the native support libraries for the JRE, the operating system, and the wireless transceiver) • is typically 500 KB or less • typically requires up to 5 minutes to download over the wireless network
partial software upgrade	• applies to wireless transceiver code • is typically less than 1 MB • typically requires up to 15 minutes to download over the wireless network
complete software upgrade	• applies to existing, complete BlackBerry® Device Software on the BlackBerry device • is typically more than 1 MB • typically requires 1 to 2 hours to download over the wireless network

Approximate duration for downloading and installing wireless software upgrades

The duration of the download and installation process for wireless software upgrades depends on the type of upgrade, size of the software upgrade package, the wireless network conditions, and the network type.

Type of upgrade	Size of upgrade package	Duration of download	Duration of installation for average amount of BlackBerry device data (12 MB)	Duration of installation for large amount of BlackBerry device data (25 MB)
platform update	500 KB	2 minutes	• installing the wireless software update – 5 minutes	• installing the wireless software update – 5 minutes
partial software upgrade	8 MB	15 minutes	• backing up the BlackBerry® device data – 15 to 30 minutes • installing the wireless software upgrade – 30 to 45 minutes • restoring the BlackBerry device data – 15 to 30 minutes	• backing up the BlackBerry device data – 45 minutes • installing the wireless software upgrade – 30 to 45 minutes • restoring the BlackBerry device data – 45 minutes
complete software upgrade	15 MB	30 minutes	• backing up the BlackBerry device data – 15 to 30 minutes • installing the wireless software upgrade – 30 to 45 minutes • restoring the BlackBerry device data – 15 to 30 minutes	• backing up the BlackBerry device data – 45 minutes • installing the wireless software upgrade – 30 to 45 minutes • restoring the BlackBerry device data – 45 minutes

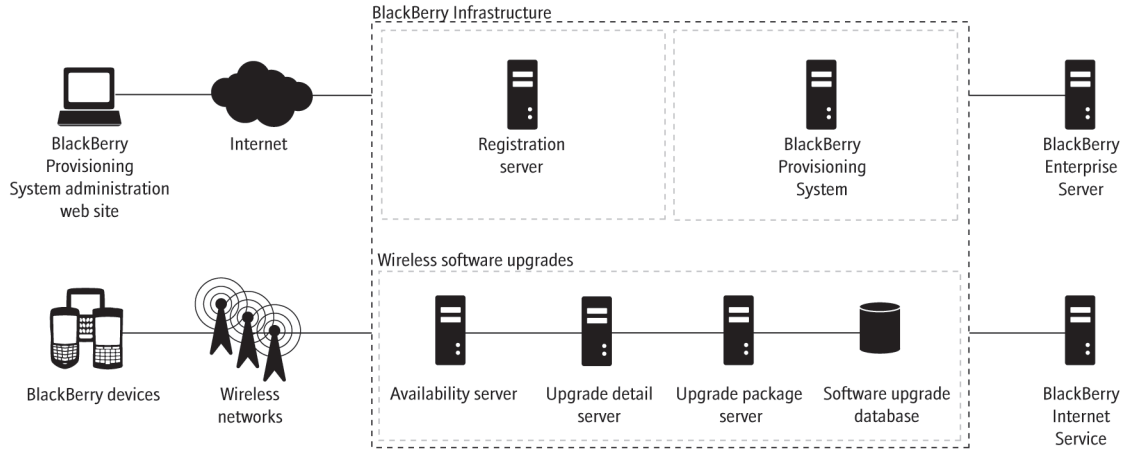
Features of wireless software upgrades

Feature	Description
approval of software upgrade packages that are available	Research In Motion and wireless service providers approve software upgrade packages before RIM makes the software upgrade packages available on the BlackBerry® Infrastructure.
automated detection of when new upgrade packages are available	• The BlackBerry® Enterprise Server contacts the BlackBerry Infrastructure once daily to check for updates to the software upgrade packages. • The BlackBerry Enterprise Server makes new software packages available automatically. • The BlackBerry Manager automatically indicates the BlackBerry devices on which you can apply the software upgrade.
control of wireless software upgrades	If you have the appropriate administrative role and permission on the BlackBerry Enterprise Server, you can perform the following actions: • view and send software upgrade requests only to supported BlackBerry devices to which the software upgrade package applies • control the software upgrade process by permitting or restricting upgrade requests to specific sources and to specific network connection types • send software upgrade requests that users must accept within 72 hours, after which their BlackBerry devices retrieve and install the software packages automatically
automated backup and restoral of data on BlackBerry devices	• The BlackBerry device is designed to back up user data, RIM-provided standard applications (such as contacts, messages, pictures, and ring tones), and existing third-party applications automatically during the software upgrade process. • The BlackBerry device is designed to restore the backed-up user data and applications when the software upgrade process completes.

Architecture: BlackBerry Infrastructure components

Component	Description
BlackBerry® Provisioning System administration web site	The BlackBerry Provisioning System administration web site is the Internet interface of the BlackBerry Provisioning System. Wireless service providers use the administration web site to manage subscribers and BlackBerry devices on their wireless network.
availability server	The availability server is designed to manage and store information about the availability of software upgrade packages. The availability server is designed to provide administrators with information about the latest approved software upgrade packages and recommended upgrade paths. Wireless service providers can access this information using the BlackBerry Provisioning System administration web site.
upgrade package server	The upgrade package server is designed to store and send software upgrade packages to the BlackBerry device. It controls the rate at which subscribers can download software upgrade packages. Research In Motion administrators upload software upgrade packages to this server as they are approved.
upgrade detail server	The upgrade detail server is designed to provide the BlackBerry device with a list of the upgrade files that are needed for a particular wireless software upgrade.
software upgrade database	The software upgrade database is the primary database that contains the software upgrade information and metadata that the BlackBerry® Infrastructure processes.

Components


BlackBerry Infrastructure
BlackBerry Provisioning System administration web site
Internet
Registration server
BlackBerry Provisioning System
BlackBerry Enterprise Server
Wireless software upgrades
BlackBerry devices
Wireless networks
Availability server
Upgrade detail server
Upgrade package server
Software upgrade database
BlackBerry Internet Service

Protecting wireless software upgrades

2

Measures of security for wired and wireless solutions

Measure	Description
confidentiality	Only the intended recipient of data or a message can view the data or the contents of the message.
integrity	The recipient can detect if a third party changed the data or the message in transit between the sender and the recipient.
authenticity	The recipient can identify and trust the identity of the sender.

Controlling wireless software upgrades using the BlackBerry Enterprise Server

By default, only the BlackBerry® Enterprise Server can select software upgrade packages that are available, send them to BlackBerry devices over the wireless network, and request that the BlackBerry device users download the software upgrade packages. Wireless service providers cannot select software upgrade packages and send them to BlackBerry devices unless you allow them to using IT policy.

Administrative roles that can control software upgrade requests

The following administrative roles can perform software upgrade tasks and manage the software upgrade process on a BlackBerry® Enterprise Server:

- security administrator
- enterprise administrator
- device administrator

How the BlackBerry Enterprise Solution authenticates requests for wireless software upgrades

Request source	Description of authentication method
BlackBerry® Enterprise Server	The BlackBerry Enterprise Server and the BlackBerry device are designed to encrypt all of the data sent between them, including data for wireless software upgrades, using standard BlackBerry encryption.
BlackBerry® Infrastructure BlackBerry® Provisioning System administration web site	The BlackBerry device is designed to use digital signature validation to authenticate the following types of data: • control messages that the BlackBerry device receives from the BlackBerry Infrastructure or the administration site that requests the wireless software upgrade • upgrade instructions that the BlackBerry device requests and receives from the BlackBerry Infrastructure or the administration site that sends the wireless software upgrade

Authenticating requests for wireless software upgrades

Before the BlackBerry® Infrastructure sends data about a wireless software upgrade to a BlackBerry device, it performs the following actions:

- generates an ECDSA key periodically, using ECC over a 521-bit curve
- signs the ECDSA key, using a stored root certificate
- signs the software upgrade data using the digitally signed ECDSA key

When the BlackBerry device receives the data, it performs the following actions:

- decrypts the ECDSA key, using a public key common to all BlackBerry devices that support wireless software upgrades
- verifies the digital signature on the ECDSA key, using a stored root certificate

How the BlackBerry device protects the existing BlackBerry Device Software

During the BlackBerry® Device Software update process, security features of the BlackBerry device components are designed to protect the BlackBerry Device Software from an attack by a user with malicious intent. Each time a user turns on the BlackBerry device, specific components on the BlackBerry device are designed to automatically check the authenticity of the operating

system and the integrity of the BlackBerry Device Software. The BlackBerry Device Software must pass these security tests before the user can run the applications on the BlackBerry device, and before the BlackBerry Device Software update can complete successfully.

How the BlackBerry Enterprise Server verifies the BlackBerry Device Software upgrade files

The signing authority system that Research In Motion® provides is designed to authorize and authenticate the code of the software upgrade package by digitally signing the software upgrade package. After the BlackBerry® device user downloads a software upgrade package to the BlackBerry device, the BlackBerry device verifies the digital signature on the software upgrade package before it can install the software upgrade package successfully.

The signing authority system uses code signing to authorize and authenticate the upgraded BlackBerry® Device Software before the user can run any of the upgraded applications on the BlackBerry device.

Battery power requirements for protecting the BlackBerry device against attack

If the battery power level on a BlackBerry® device drops below the required minimum to perform a BlackBerry Device Software update, the BlackBerry device prompts the user to recharge the battery and start the BlackBerry Device Software update process again. This security measure is designed to protect the BlackBerry device against attacks from users with malicious intent who might try to take advantage of low battery power during a BlackBerry Device Software update.

You can set the Secure Wipe If Low Battery IT policy rule to require that the BlackBerry device delete all user data if the BlackBerry device has insufficient battery power to receive IT policy updates or IT administration commands.

How a BlackBerry device protects user data during a BlackBerry Device Software update over the wireless network

When the content protection feature on a BlackBerry® device is turned on, the following measures to encrypt user data take effect:

- the user must type the BlackBerry device password before the BlackBerry® Device Software update process can back up or restore the user data
- the BlackBerry device encrypts stored user data during the BlackBerry Device Software update process

Protection of user data on locked BlackBerry devices

When the content protection feature on BlackBerry® devices is turned on, the BlackBerry devices are designed to protect user data in the following ways:

- use 256-bit AES encryption to encrypt stored data
- use ECC public keys to encrypt data that the BlackBerry devices receive

User data that BlackBerry devices can encrypt when the content protection feature is turned on

Item	Description
AutoText	all text that automatically replaces the text that BlackBerry® device users type
BlackBerry® Browser	• content that web sites or third-party applications push to BlackBerry devices • web sites that users save on their BlackBerry devices • browser cache
calendar	• subject • location • meeting organizer • meeting participants • notes included in calendar items
address book contacts	all contact information except the contact title and category For information about using the Force Include Address Book In Content Protection IT policy rule to prevent users from turning off encryption for the address book, see the *BlackBerry Enterprise Server Policy Reference Guide*.
message list	• subject • email addresses • message body • attachments
memo list	• title • information included in the body of notes
Open Mobile Alliance® DRM applications	keys that identify the BlackBerry devices and SIM cards (if available) that the BlackBerry devices add to DRM forward-locked applications

Item	Description
RSA SecurID® library	the contents of the .sdtid file seed that is stored in flash memory
tasks	• subject • information included in the body of tasks

How the BlackBerry Enterprise Solution controls installation of third-party applications that wireless software upgrades do not support

To send third-party applications to a BlackBerry® device over the wireless network, you must assign a software configuration to the BlackBerry device user and set an application control policy. The BlackBerry device user can then connect to the shared application loader tool, and install or upgrade to the third-party applications that you provide.

The application control policy rules for the BlackBerry® Enterprise Server are designed so that you can permit or prevent the installation of specific third-party applications on the BlackBerry device, and so that you can limit the permissions of third-party applications on the BlackBerry device. You can assign values for an application control policy rule in the application control policy.

Requesting wireless software upgrades 3

Process flow: Requesting a wireless software upgrade from a BlackBerry device

1. The BlackBerry® device user requests a wireless software upgrade.
2. The BlackBerry® Enterprise Server sends information about any available software upgrades to the BlackBerry device.
3. The BlackBerry device user selects one or more software upgrade packages.
4. The BlackBerry device connects to the upgrade detail server.
5. The upgrade detail server determines whether the BlackBerry device can perform the wireless software upgrade. If applicable, the upgrade detail server allows the BlackBerry device to connect to the upgrade package server to retrieve the software upgrade package.

Severity levels for software upgrade requests

Severity level	Description
Mandatory	• use to send a software upgrade package that the BlackBerry® device retrieves and installs automatically if the user does not accept the software upgrade request within 72 hours • might fix one or more software issues that are critical to how the BlackBerry device works • might include one or more important new BlackBerry device features
Critical	• use to send a request that indicates that the user should download and install the wireless software upgrade immediately • might include one or more important new BlackBerry device features • might fix one or more software issues that impact how the BlackBerry device works
High	• use to send a request that indicates that the user should download and install the wireless software upgrade as soon as possible • might include one or more important new BlackBerry device features • might fix one or more software issues that visibly impact BlackBerry device features but are not critical to how the BlackBerry device works

Severity level	Description
Medium	• use to send a request that indicates that the user should download and install the wireless software upgrade as soon as it is convenient to do so • might include one or more new BlackBerry device features • might fix one or more software issues that do not visibly impact BlackBerry device features and are not critical to how the BlackBerry device works
Low	• use to send a request that indicates that the user can download and install the wireless software upgrade when wanted • might include one or more minor new BlackBerry device features • might fix one or more minor software issues

Information that a software upgrade request displays

A software upgrade request provides BlackBerry® device users with the following information about the software upgrade packages that are available:

- software version number
- approximate size of the software upgrade package
- severity level of the software upgrade request, which tells users how soon they should consider upgrading
- description of the software upgrade package

Prerequisites: Requesting wireless software upgrades

- review the BlackBerry® device hardware, software, memory, and battery power requirements for wireless software upgrades
- understand the BlackBerry device behavior that might occur during the software upgrade process

Minimum requirements for wireless software upgrades

- BlackBerry® Enterprise Server version 4.1 SP5 or later
- Supported BlackBerry device models that run BlackBerry® Device Software version 4.5 or later

BlackBerry device memory requirements for BlackBerry Device Software updates over the wireless network

The BlackBerry® device must have 16 MB of RAM and at least 64 MB of flash memory available to start and complete a BlackBerry® Device Software update over the wireless network.

If the amount of available flash memory on the BlackBerry device decreases to less than 400 KB, the BlackBerry device runs the LMM automatically to identify and delete unreferenced and cached data associated with BlackBerry device applications such as the message list, organizer data, and data for third-party applications.

If the update process requires more memory, the LMM deletes medium-priority items such as very old email messages and out-of-date calendar entries.

If the minimum amount of memory required is still not available, the BlackBerry device user must delete items manually.

Battery power requirements for BlackBerry Device Software updates over the wireless network

The battery power level on a BlackBerry® device must be 50% or greater for the BlackBerry device to retrieve an update package over the wireless network. If the battery power level is below the minimum requirement, the update process suspends. The BlackBerry device prompts the user to recharge the battery and start the update process again. If the battery power level returns to 50%, the BlackBerry device resumes retrieving the update package from the BlackBerry® Infrastructure.

The battery power requirement is designed to protect the BlackBerry device against attacks from a potentially malicious user who might try to take advantage of low battery power during a BlackBerry Device Software update.

Best practice: Preventing possible BlackBerry device issues during the BlackBerry Device Software update process

Scenario	Best practice
The BlackBerry® Device Software update process might not complete if the user turns off the BlackBerry device.	Do not turn off the BlackBerry device after the BlackBerry Device Software update process starts.
The BlackBerry Device Software update process might not complete if the user removes the expandable memory from the BlackBerry device.	Do not remove the expandable memory after the BlackBerry Device Software update process starts.

Scenario	Best practice
A user cannot make an emergency call on the BlackBerry device.	Pause or cancel the current BlackBerry Device Software update process to make an emergency call on the BlackBerry device.
A user does not receive incoming calls on the BlackBerry device.	Pause or cancel the current BlackBerry Device Software update process to receive incoming calls on the BlackBerry device.
The BlackBerry device might have slow response times and requires user attention if the content protection feature is turned on.	If the content protection feature is turned on or the BlackBerry device resets after it installs an application, type the password for the BlackBerry device.
The BlackBerry device loses all of its user data if the user starts to update the BlackBerry® Desktop Software.	Do not update the BlackBerry Desktop Software until the BlackBerry Device Software update process completes.

Search criteria for BlackBerry devices

BlackBerry device criteria	Search method
registered with a specific wireless service provider	In the **Carrier** drop-down list, click the name of a wireless service provider.
a specific BlackBerry® device model	In the **Device** drop-down list, click the model number of a BlackBerry device.
currently using a specific BlackBerry® Device Software version	In the **From Version** drop-down list, click the version number of a software upgrade package.
can upgrade to a specific BlackBerry Device Software version	In the **To Version** drop-down list, click the version number of a software upgrade package.
status of a previous upgrade or cancellation request	In the **Upgrade Status** drop-down list, click a status.
sequential number of the command for a previously sent upgrade or cancellation request	In the **Sequence** drop-down list, click a number.
activated on a specific BlackBerry® Enterprise Server	In the **Server** drop-down list, click a BlackBerry Enterprise Server.
application of a specific IT policy	In the **IT Policy** drop-down list, click an IT policy name.

How a user can respond to a software upgrade request

Response	Description
accept the upgrade request	• The BlackBerry® device starts the software download process. • The user can monitor the progress of the wireless software download on the BlackBerry device and can continue to use the BlackBerry device, where permitted by the wireless technology. • When the software download process completes successfully, the BlackBerry device prompts the user to install the software upgrade package.
defer the upgrade request	• A prompt appears on the BlackBerry device every 24 hours, to remind the user to install the software upgrade package.
reject the upgrade request	• The upgrade request process is designed to stop.

Send a software upgrade request

Before you begin: You must log in to the BlackBerry® Enterprise Server using the appropriate administrative role and permission.

1. In the BlackBerry Manager, click **Upgrades**.
2. Use one or more of the fields available to search for BlackBerry devices that meet specific criteria.
3. In the list of applicable BlackBerry devices, select one or more BlackBerry devices.
4. Click **Device Management**.
5. Click **View/Upgrade Software**.
6. In the **Severity** drop-down list, perform one of the following actions:
   - Select a severity level to assign to the software upgrade package.
   - To retain the severity level that the wireless service provider approved when Research In Motion made the software upgrade package available, click **Use Carrier**.
7. Type a message to display to BlackBerry device users, such as a description of the software upgrade package and the reason for the upgrade request.
8. In the **Rollback Cutoff Days** field, change the default number of days for which you are permitted to start a cancellation request after sending the upgrade request.
9. Click **Continue**.
10. In the **Upgrade to Version** drop-down list, click the version number of a software upgrade package.
11. Click **Continue**.

12. Click **OK**.

Restricting wireless software upgrades

4

Preventing wireless software upgrades based on the source of the upgrade request

You can change the BlackBerry® Enterprise Server settings to prevent or allow upgrade requests from sources other than the BlackBerry Enterprise Server.

By default, the BlackBerry Enterprise Server does not allow supported BlackBerry devices to receive upgrade requests from wireless service providers; however, BlackBerry device users can send requests for software upgrade packages from their BlackBerry devices either to the BlackBerry Enterprise Server or to their wireless service providers.

Allow wireless service providers to send software upgrade requests

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click an IT policy.
6. Click **Properties**.
7. Click **Wireless Software Upgrades Policy Group**.
8. Change the Allow Non Enterprise Upgrade IT policy rule setting to **True**.
9. Click **OK**.

Prevent BlackBerry device users from sending software upgrade requests

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click an IT policy.
6. Click **Properties**.
7. Click **Wireless Software Upgrades Policy Group**.
8. Set the Disallow Device User Requested Upgrade IT policy rule to **True**.
9. Click **OK**.

Preventing BlackBerry Device Software updates over the wireless network based on the network connection type

You can prevent BlackBerry® devices from starting or completing BlackBerry® Device Software updates over specific types of network connections. You might choose to place restrictions for the following reasons:

- conserve network bandwith
- prevent added cost of network usage
- verify that BlackBerry Device Software updates only occur over network connections that you consider to be efficient and reliable
- increase security

Upgrading BlackBerry Device Software over a serial bypass connection

After the BlackBerry® Infrastructure sends the BlackBerry® Device Software update package to the BlackBerry® Enterprise Server, the BlackBerry Enterprise Server sends an update request to BlackBerry devices over the wireless network.

To perform the wireless BlackBerry Device Software update over a serial bypass connection, users must connect their BlackBerry devices to computers that run the BlackBerry® Device Manager.

Upgrading BlackBerry Device Software over a Wi-Fi connection

If your organization's environment includes an enterprise Wi-Fi® network and a remote BlackBerry® Router in a DMZ, the environment is designed to bypass the BlackBerry® Infrastructure. If your organization's environment is designed to bypass the BlackBerry Infrastructure and you have the appropriate administrator role and permissions for the BlackBerry® Enterprise Server, you can permit BlackBerry device users to download BlackBerry Device Software update packages over a Wi-Fi connection.

After the BlackBerry Infrastructure sends the BlackBerry® Device Software update package to the BlackBerry Enterprise Server, the BlackBerry Enterprise Server sends an update request to BlackBerry devices over the wireless network. The BlackBerry device users can then update the BlackBerry Device Software.

Prevent BlackBerry device users from downloading software upgrade packages over a Wi-Fi connection

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.

5. Click an IT policy.
6. Click **Properties**.
7. Click **Wireless Software Upgrades Policy Group**.
8. Set the Disallow Patch Download Over WiFi IT policy rule to **True**.
9. Click **OK**.

Prevent BlackBerry device users from downloading software upgrade packages over a WAN connection

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click an IT policy.
6. Click **Properties**.
7. Click **Wireless Software Upgrades Policy Group**.
8. Set the Disallow Patch Download Over WAN IT policy rule to **True**.
9. Click **OK**.

Prevent BlackBerry device users from downloading software upgrade packages over a roaming WAN connection

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click an IT policy.
6. Click **Properties**.
7. Click **Wireless Software Upgrades Policy Group**.
8. Set the Disallow Patch Download Over Roaming WAN IT policy rule to **True**.
9. Click **OK**.

Prevent BlackBerry device users from downloading software upgrade packages over an international roaming WAN connection

1. In the BlackBerry® Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click an IT policy.
6. Click **Properties**.
7. Click **Wireless Software Upgrades Policy Group**.
8. Set the Disallow Patch Download Over International Roaming WAN IT policy rule to **True**.
9. Click **OK**.

Managing wireless software upgrades

5

If you have the appropriate administrative role and permission on the BlackBerry® Enterprise Server, you can perform the following tasks:

- monitor the progress of each software upgrade request
- cancel software upgrade requests within the permitted cancellation request period
- monitor the progress of each cancellation request

Monitoring software upgrade requests and cancellation requests

You can monitor all software upgrade requests and cancellation requests that the BlackBerry® Enterprise Server submits. In the BlackBerry Manager, on the Upgrades tab, you can search for and view software upgrade requests and cancellation requests based on properties of the BlackBerry devices, the BlackBerry Enterprise Servers, and the status of the software upgrade requests and cancellation requests.

Cancel a wireless software upgrade

Before you begin:

- You must log in to the BlackBerry® Enterprise Server using the appropriate administrative role and permission.
- The cancellation request period for the software upgrade request that you want to cancel must not be expired.

1. In the BlackBerry Manager, click **Upgrades**.
2. Use one or more of the available fields to search for BlackBerry devices that meet specific criteria.
3. In the list of applicable BlackBerry devices for which wireless software upgrades are available, select one or more BlackBerry devices.
4. Click **Device Management**.
5. Click **Revert Software Upgrade**.
6. In the **Severity** drop-down list, perform one of the following tasks:
   - Select a severity level to assign to the cancellation request.
   - To retain the severity level that the wireless service provider approved when Research In Motion made the software upgrade package available, click **Use Carrier**.
7. Type a message to display to BlackBerry device users, such as a description of the software upgrade package and the reason for the cancellation request.
8. Click **Continue**.

9. Click **OK**.

The BlackBerry Enterprise Server is designed to cancel the wireless software upgrade completely in 1 to 2 hours. The user can view status information about the cancellation process on the BlackBerry device.

Cancelling wireless software upgrades

To cancel a wireless software upgrade, the BlackBerry® device must have installed the software upgrade successfully and be allowed to accept and complete upgrade cancellation requests.

The default period for you or the BlackBerry device to request the cancellation of a wireless software upgrade is 24 hours after the software upgrade process completes successfully.

Prevent BlackBerry device users from cancelling wireless software upgrades

Before you begin:

- The software upgrade process must complete successfully on the BlackBerry® device.
- The cancellation request period for the software upgrade request that you want to cancel must not be expired.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click an IT policy.
6. Click **Properties**.
7. Click **Wireless Software Upgrades Policy Group**.
8. Set the Disallow Device User Requested Rollback IT policy rule to **True**.
9. Click **OK**.

View upgrade properties for BlackBerry devices

You can view the properties of the BlackBerry® devices for which software upgrade packages are currently available on the upgrade package server or to which you have sent a software upgrade request.

1. In the BlackBerry Manager, click **Upgrades**.
2. In the upper pane, view the default properties for the BlackBerry devices.
   You can select a specific BlackBerry device to view all of its properties in the lower pane of the BlackBerry Manager.

View additional upgrade properties for BlackBerry devices

To view additional properties of BlackBerry® devices for which software upgrade packages are currently available on the upgrade package server, or to which you have sent a software upgrade request, you can add properties columns to the Upgrades tab.

1. In the BlackBerry Manager, click **Upgrades**.
2. On the **Upgrades** tab, right-click any column heading.
3. In the **Show columns related to** drop-down list, click **Device Upgrades**.
4. In the **Available columns** list, click the name of a properties column.
5. To add the column to the properties that the **Upgrades** tab displays, click **Insert**.
6. Repeat steps 4 and 5 for any other Device Upgrades properties that you want to view.
7. Click **OK**.

After you finish: You can change the order in which the columns appear in the BlackBerry Manager.

Upgrade properties for BlackBerry devices

Property	Description
Name	name of the BlackBerry® device user account
PIN	PIN of the BlackBerry device
Home Carrier	name of the wireless service provider with which the BlackBerry device is registered
BlackBerry Device Model	model number or name of the BlackBerry device
Upgrade Status	status of the most recent software upgrade request that the BlackBerry® Enterprise Server sent over the wireless network to the BlackBerry device
Server Name	name of the BlackBerry Enterprise Server on which the BlackBerry device is activated
Command	type of request that the BlackBerry Enterprise Server sent to the BlackBerry device
Destination Version	version of the BlackBerry® Device Software that the BlackBerry device installs when it accepts the software upgrade request or the cancellation request
Download Bytes	size, in bytes, of the software upgrade package that the BlackBerry device installs when it accepts the software upgrade request or the cancellation request
Sequence	sequential number that the BlackBerry Manager assigned to the command
Severity	severity that you or the wireless service provider and Research In Motion assigned to the software upgrade package
Source Version	version of the BlackBerry Device Software that the BlackBerry device runs before accepting the software upgrade request or the cancellation request

Property	Description
Upgrade Status	current status of the request that the BlackBerry Enterprise Server sent to the BlackBerry device
Upgrade Status Time	time that the BlackBerry Enterprise Server received the current upgrade status from the BlackBerry device

Optional upgrade properties for BlackBerry devices

Property	Description
Command	type of request that the BlackBerry® Enterprise Server sends to the BlackBerry device
Destination Version	version of the BlackBerry® Device Software that the BlackBerry device installs when it accepts the software upgrade request or the cancellation request
Download Bytes	size, in bytes, of the software upgrade package that the BlackBerry device installs when it accepts the software upgrade request or the cancellation request
Sequence	sequential number that the BlackBerry Manager assigned to the command
Severity	severity that you or the wireless service provider and Research In Motion assigned to the software upgrade package
Source Version	version of the BlackBerry Device Software that the BlackBerry device runs before accepting the software upgrade request or the cancellation request
Upgrade Status	current status of the request that the BlackBerry Enterprise Server sent to the BlackBerry device
Upgrade Status Time	time that the BlackBerry Enterprise Server received the current upgrade status from the BlackBerry device

Glossary

6

AES
Advanced Encryption Standard

API
application programming interface

DMZ
A demilitarized zone (DMZ) is a neutral subnetwork outside of an organization's firewall. It exists between the trusted LAN of the organization and the untrusted external wireless network and public Internet.

DRM
Digital Rights Management

ECC
Elliptic Curve Cryptography

ECDSA
Elliptic Curve Digital Signature Algorithm

JRE
Java® Runtime Environment

JVM
Java® Virtual Machine

LMM
The Low Memory Manager (LMM) is an application on the BlackBerry device that deletes medium-priority items, such as old email messages and out-of-date calendar entries, when the amount of available flash memory on the BlackBerry device is less than 400 KB.

OMA
Open Mobile Alliance™

PIN
personal identification number

SIM
Subscriber Identity Module

WAN
wide area network

Legal

7

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF RIM OR ANY AFFILIATES OF RIM HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry® Enterprise Server, BlackBerry® Desktop Software, and/or BlackBerry® Device Software.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
Centrum House
36 Station Road
Egham, Surrey TW20 9LF
United Kingdom

Published in Canada