Upgrade Guide

BlackBerry Device Service

Version: 6.1

BlackBerry®

Published: 2012-07-23
SWD-20120723181152216

Contents

1 Related resources 5
2 About the BlackBerry Device Service 7
3 Planning a BlackBerry Device Service upgrade 8
Upgrade implications for the BlackBerry Configuration Database 8
4 Requirements 9
System requirements: Your organization's environment 9
System requirements: Firewall 9
System requirements: VPN hardware 10
Hardware requirements: BlackBerry Device Service 11
Software requirements: BlackBerry Device Service and components 13
Software requirements: BlackBerry Device Service 14
Software requirements: Database server 14
Software requirements: Browser 15
Software requirements: Email app, Calendar app, and Contacts app 17
Installation considerations 17
Supported features and environments 17
Unsupported environments 18
5 Preupgrade tasks 19
Upgrade implications for BlackBerry PlayBook tablet users 19
Identify users that must update their BlackBerry PlayBook tablets 19
Backing up the BlackBerry Configuration Database 20
Performing a test upgrade of the BlackBerry Configuration Database 20
Perform a test upgrade of the BlackBerry Configuration Database 20
Verifying database permissions to upgrade the BlackBerry Configuration Database 22
Upgrade a BlackBerry Configuration Database 22
Connecting to an existing BlackBerry Configuration Database 24
6 Upgrading the BlackBerry Device Service software 25
Prerequisites: Upgrading the BlackBerry Device Service software 25
Upgrade the BlackBerry Device Service software 25
7 Postupgrade tasks 28
Best practice: Running the BlackBerry Device Service 28
Import the SSL certificate for the messaging server to the BlackBerry Administration Service 29
Log in to the BlackBerry Administration Service 29
There is a problem with this website's security certificate 30

Configuring database permissions using Microsoft SQL Server roles 31
Configure minimum database permissions for the service account or Microsoft SQL Server account 32
8 Glossary 33
9 Legal notice 34

Related resources

1

To read the following guides, visit www.blackberry.com/go/serverdocs.

Resource	
BlackBerry Device Service Feature and Technical Overview	• Architecture diagrams • Descriptions of features and components • Data flows
BlackBerry Device Service Installation and Configuration Guide	• System requirements • Installation instructions
BlackBerry Device Service Administration Guide	• Instructions for creating user accounts, groups, roles, administrator accounts, and so on • Instructions for activating BlackBerry PlayBook tablets • Instructions for creating and sending IT policies and profiles • Instructions for sending and managing applications on tablets
BlackBerry Web Desktop Manager User Guide	• User instructions for activating tablets • User instructions for protecting a lost tablet
BlackBerry Device Service and BlackBerry PlayBook Tablet Security Technical Overview	• Description of the security maintained by the BlackBerry Device Service, BlackBerry Infrastructure, and tablet to protect data and connections • Description of the BlackBerry PlayBook OS • Description of how work data is protected on tablets when you use the BlackBerry Device Service
BlackBerry Bridge App and BlackBerry PlayBook Tablet Security Technical Overview	• Description of how work data is protected on tablets when you use the BlackBerry Bridge app

Resource	
	• Description of how work data is protected when it is in transit between a tablet and a BlackBerry smartphone • Description of attacks that the BlackBerry Bridge pairing process is designed to prevent
BlackBerry PlayBook Tablet Print To Go Security Note	• Description of how data is protected when using Print To Go • Instructions for preventing the use of Print To Go
BlackBerry Device Service Policy Reference Guide	• Descriptions of available IT policy rules and profile settings
BlackBerry Device Service Release Notes	• Descriptions of known issues and potential workarounds

About the BlackBerry Device Service

2

The BlackBerry Device Service permits you to manage the work perimeter on BlackBerry PlayBook tablets that run BlackBerry PlayBook OS 2.0 or later.

The BlackBerry Device Service allows you to:

- control the connections the tablet makes to your organization's environment, including connections to your organization's Wi-Fi networks and Microsoft ActiveSync
- install and manage your organization’s applications on tablets
- protect your organization’s data and applications on tablets

You can install the BlackBerry Device Service with BlackBerry Mobile Fusion Studio. BlackBerry Mobile Fusion Studio provides a simplified administrative console for your organization's helpdesk administrators.

You can download the BlackBerry Device Service from www.blackberry.com/support/downloads.

Planning a BlackBerry Device Service upgrade

3

You upgrade the BlackBerry Device Service software by replacing the existing version and upgrading the BlackBerry Configuration Database. After you upgrade the BlackBerry Device Service, existing user accounts are active and no additional administrative actions are required.

You can upgrade BlackBerry Device Service 6.0 to the latest version.

Upgrade implications for the BlackBerry Configuration Database

When you upgrade the BlackBerry Device Service to the latest version, you must also upgrade the BlackBerry Configuration Database to the latest version. The setup application upgrades the BlackBerry Configuration Database automatically so that the database and BlackBerry Device Service components run the same version. If you do not want to use the setup application to upgrade the BlackBerry Configuration Database, you can run the database upgrade scripts on the database server.

Requirements

4

System requirements: Your organization's environment

Item	Requirement
Directory service	• Microsoft Active Directory that is running at a domain functional level that is set to Windows Server 2003 or later • BlackBerry Device Service users must have a Microsoft Active Directory account

BlackBerry PlayBook OS	• PlayBook OS 2.0 or later
	• PlayBook OS 2.1 or later is required if you want to use the following features:
	  • SCEP profiles to obtain certificates for certificate-based authentication
	  • Activation over the Wi-Fi network

System requirements: Firewall

For more information about activation data flows, see the *BlackBerry Device Service Feature and Technical Overview*.

Item	Requirement
DNS	• Support for resolving IP addresses into host names
Proxy firewall	• If your organization uses a proxy firewall, a proxy that does not change incoming or outgoing data (transparent proxy)

Item	Requirement
BlackBerry Infrastructure	• Exclusive use of port 3101 to open and maintain an outbound, bidirectional TCP/IP connection to the BlackBerry Infrastructure

Enterprise Management Web Service	• Exclusive use of port 8081 and port 8444 on the computer that hosts the BlackBerry Device Service to permit communication with the Enterprise Management Web Service. If users do not use the BlackBerry Infrastructure to activate their BlackBerry PlayBook tablets, port 8081 and port 8444 must also be open for the connection that users use for activation:
	  • Wired connection (connection between a tablet and a computer using a USB cable)
	  • VPN or work Wi-Fi network configured for the BlackBerry Device Service
	
	Note: If port 8081 and port 8444 are already in use, see the *BlackBerry Device Service Administration Guide* to find out how to change the ports required by the Enterprise Management Web Service.

System requirements: VPN hardware

If your organization's environment includes VPNs, you can configure a BlackBerry PlayBook tablet to authenticate with the VPN so that it can access your organization's network. The BlackBerry MDS Connection Service is used when the tablet is not connected to a VPN or work Wi-Fi network that is configured for the BlackBerry Device Service.

BlackBerry PlayBook OS 2.0 or later supports the following IPsec VPN hardware:

- Any gateway from Check Point
- Cisco VPN 3000 Series Concentrator
- Cisco PIX Firewall
- Cisco IOS Easy VPN
- Any appliance in the Cisco ASA Series
- Any gateway in the Juniper SRX Series
- Any gateway in the Juniper NetScreen Series
- Any Windows Server with RRAS and IPsec configured that supports IKEv2
- Any VPN server that supports IKEv2

PlayBook OS 2.0 or later supports the following SSL VPN hardware:

- Any gateway in the Juniper SA Series
- Any gateway in the Juniper MAG Series

For more information, visit www.blackberry.com/go/kbhelp to read article KB28128.

Hardware requirements: BlackBerry Device Service

The following guidelines apply to the computer that you install the BlackBerry Device Service and BlackBerry Device Service components on, including the BlackBerry Configuration Database. Disk space requirements are for the BlackBerry Device Service and approximately 1 month of log files.

The size of log files for the BlackBerry Device Service and BlackBerry Device Service components varies based on the number of users in your organization's environment and the level of user activity. It is a best practice to monitor and control the amount of disk space that the BlackBerry Device Service log files take up. For more information about configuring logging, visit www.blackberry.com/go/serverdocs to read the *BlackBerry Device Service Administration Guide*.

If you install the BlackBerry Device Service on the computer that hosts BlackBerry Mobile Fusion Studio, you must also consider the memory and disk space requirements for BlackBerry Mobile Fusion Studio.

For more information about calculating hardware requirements, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Device Service Performance Calculator*.

Note: The BlackBerry Device Service hardware requirements are lower when BlackBerry PlayBook tablets connect to a VPN or work Wi-Fi network.

Requirements for 1 to 500 users

Environment	Requirement
Email messages and app downloads (VPN or work Wi-Fi network)	• One processor, 1.6 GHz Intel Xeon 3000 Series or Intel Xeon 5100 Series (Dual Core) • 3 GB of available memory • 10 GB of disk space
Email messages only	• One processor, 1.6 GHz Intel Xeon 3000 Series or Intel Xeon 5100 Series (Dual Core) • 3 GB of available memory • 10 GB of disk space

Environment	Requirement
Email messages and 2 MB app downloads per user	• One processor, 2 GHz Intel Xeon 3000 Series or Intel Xeon 5100 Series (Dual Core) • 4 GB of available memory • 10 GB of disk space
Email messages and 10 MB app downloads per user	• One processor, 2.33 GHz Intel Xeon 3000 Series or Intel Xeon 5100 Series (Dual Core) • 4 GB of available memory • 10 GB of disk space

Requirements for 500 to 2000 users

Environment	Requirement
Email messages and app downloads (VPN or work Wi-Fi network)	• One processor, 2 GHz Intel Xeon 3000 Series or Intel Xeon 5100 Series (Dual Core) • 3 GB of available memory • 15 GB of disk space
Email messages only	• One processor, 2 GHz Intel Xeon 3000 Series or Intel Xeon 5100 Series (Dual Core) • 4 GB of available memory • 15 GB of disk space
Email messages and 2 MB app downloads per user	• One processor, 2.66 GHz Intel Xeon 3000 Series or Intel Xeon 5100 Series (Dual Core) • 4 GB of available memory • 25 GB of disk space
Email messages and 10 MB app downloads per user	• One processor, 2.5 GHz Intel Xeon 5400 Series (Quad Core) • 5 GB of available memory • 25 GB of disk space

Requirements for 2000 to 5000 users

Environment	Requirement
Email messages and app downloads (VPN or work Wi-Fi network)	• One processor, 2 GHz Intel Xeon 3000 Series or Intel Xeon 5100 Series (Dual Core) • 4 GB of available memory • 30 GB of disk space
Email messages only	• One processor, 2 GHz Intel Xeon 3000 Series or Intel Xeon 5100 Series (Dual Core) • 5 GB of available memory • 30 GB of disk space
Email messages and 2 MB app downloads per user	• One processor, 2.5 GHz Intel Xeon 5400 Series (Quad Core) • 5 GB of available memory • 50 GB of disk space
Email messages and 10 MB app downloads per user	• One processor, 2.53 GHz Intel Xeon 5500 Series (Quad Core) • 6 GB of available memory • 50 GB of disk space

Requirements for 5000 to 10,000 users

Environment	Requirement
Email messages and app downloads (VPN or work Wi-Fi network)	• One processor, 2.5 GHz Intel Xeon 5400 Series (Quad Core) • 5 GB of available memory • 60 GB of disk space

Software requirements: BlackBerry Device Service and components

Software requirements: BlackBerry Device Service

To install the BlackBerry Device Service, any of the following operating systems:

- Windows Server 2008 SP2 (64-bit)
- Windows Server 2008 R2
- Windows Server 2008 R2 SP1

Software requirements: Database server

Item	Requirement
Database management system	Any of the following database management systems: • Microsoft SQL Server 2008 SP2 (32-bit or 64-bit) • Microsoft SQL Server 2008 R2 (32-bit or 64-bit) • Microsoft SQL Server 2008 R2 SP1 (32-bit or 64-bit) • Microsoft SQL Server 2008 Express SP2 (32-bit or 64-bit) • Microsoft SQL Server 2008 R2 Express (32-bit or 64-bit) • Microsoft SQL Server 2008 R2 SP1 Express (32-bit or 64-bit)
Collation setting	To configure collation settings, the following conditions: • Database server collation configured to default case-insensitive • BlackBerry Configuration Database collation configured to default case-insensitive • Default collations are suggested but non-default collations are supported (for more information, visit www.blackberry.com/go/kbhelp to read articles KB04785 and KB15534)
Database connectivity	TCP/IP network protocols turned on
Database transactional replication	To support database transactional replication for the BlackBerry Configuration Database, the following conditions: • Database server must be Microsoft SQL Server 2008 SP2 or Microsoft SQL Server 2008 R2

Item	Requirement
	• Database server that hosts the replicated database must use the same version and build as the database server that hosts the primary database

Software requirements: Browser

The following requirements apply to the browser that you use to log in to the BlackBerry Administration Service and BlackBerry Web Desktop Manager.

Item	Requirement
Browser	• Windows Internet Explorer 8.0 and 9.0 (32-bit) • Mozilla Firefox 10 or later • Google Chrome 12 or later • Safari 5 for Mac or later Windows Internet Explorer 8 or later provides optimal support for BlackBerry Web Desktop Manager features and BlackBerry Administration Service features. **Note:** If users use a wired connection to activate their BlackBerry PlayBook tablets (connection between a tablet and a computer using a USB cable), they must use Windows Internet Explorer.

Browser settings for Windows Internet Explorer	To support browser access, you must configure the following settings:
	• Language preferences that display encoded web pages
	• Microsoft hotfix 955839 is installed on the computer to make sure that the correct time zones are displayed
	• If you are using Windows XP (64-bit), Microsoft hotfix 968730 is installed on the computer
	• Verify that the Windows firewall does not block incoming connections to RIMProxy.exe
	• To support Microsoft ActiveX, the following settings are enabled:
	  • Automatic prompting for Microsoft ActiveX controls
	  • Download signed Microsoft ActiveX controls
	  • Run Microsoft ActiveX controls and plug-ins

Item	Requirement

	• Script Microsoft ActiveX controls marked safe for scripting
	• Support for JavaScript
	• Cookies turned on
	• Support for TLS or SSL
	• The SSL certificate is installed to permit trusted connections to the BlackBerry Administration Service
	• If you do not configure single sign-on authentication for the BlackBerry Administration Service, the BlackBerry Web Desktop Manager website and BlackBerry Administration Service website are assigned to the local intranet or trusted websites zone
	• If you configure single sign-on authentication for the BlackBerry Administration Service
	  • The BlackBerry Web Desktop Manager and BlackBerry Administration Service websites are assigned to the local intranet zone
	  • Enable Integrated Windows Authentication is selected

Browser settings for Firefox, Google Chrome, and Safari	To support browser access, you must configure the following settings: • Support for JavaScript • Cookies turned on • Support for TLS or SSL • The SSL certificate is installed to permit trusted connections to the BlackBerry Administration Service Single sign-on authentication for the BlackBerry Administration Service is not supported by Google Chrome.

Software requirements: Email app, Calendar app, and Contacts app

To allow users to use the Email app, Calendar app, and Contacts app to connect to your organization's messaging server, you can enable Microsoft ActiveSync for any of the following messaging servers that support Microsoft ActiveSync.

Item	Requirement
Microsoft Exchange	For Microsoft Exchange, any of the following messaging servers: • Microsoft Exchange Server 2003 • Microsoft Exchange Server 2007 (Microsoft ActiveSync enabled by default) • Microsoft Exchange Server 2010 (Microsoft ActiveSync enabled by default) For more information, visit technet.microsoft.com to read *Managing an Exchange ActiveSync Server*.
IBM Lotus Domino	For Lotus Domino, any messaging server that supports IBM Lotus Notes Traveler. For more information, visit www.ibm.com/support to read about IBM Lotus Notes Traveler.

Installation considerations

Supported features and environments

Item	Description
Virtual environment	For more information about supported virtual environments, visit www.blackberry.com/go/kbhelp to read article KB29661.

Item	Description
IP	BlackBerry Device Service components support only IPv4 for TCP/IP connections.
Remote access	The BlackBerry Device Service and BlackBerry Device Service components support remote access by administrators who use Remote Desktop Connection.

Unsupported environments

Item	Description
DMZ	The BlackBerry Device Service and BlackBerry Device Service components do not support installation in a DMZ. For information about configuring the BlackBerry Device Service to connect to an existing BlackBerry Router, visit www.blackberry.com/go/kbhelp to read article KB29748.
Mixed environment	You cannot connect the BlackBerry Device Service and the BlackBerry Enterprise Server or BlackBerry Enterprise Server Express to the same BlackBerry Configuration Database. To run the BlackBerry Device Service and the BlackBerry Enterprise Server or BlackBerry Enterprise Server Express in the same organization, you can configure one BlackBerry Configuration Database for the BlackBerry Device Service, and another BlackBerry Configuration Database for the BlackBerry Enterprise Server instances or BlackBerry Enterprise Server Express instances.

Preupgrade tasks

5

Upgrade implications for BlackBerry PlayBook tablet users

If you upgrade the BlackBerry Device Service before all BlackBerry PlayBook tablet users update their BlackBerry PlayBook tablets to BlackBerry PlayBook OS 2.1 or later, users with tablets running an earlier version of PlayBook OS can continue to use their tablets but work apps on the tablet and the associated application data are removed. Required apps are automatically resent to users, but application data is permanently lost. Users must manually download and install any optional apps again on the Work tab in the BlackBerry App World storefront.

Identify users that must update their BlackBerry PlayBook tablets

You can check the software version of the BlackBerry PlayBook tablets that are managed by your organization's BlackBerry Device Service domain.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Click **Export all results**.
4. Click **Download file** and specify a location to save the file.

After you finish: Notify users with tablets running a software version earlier than 2.1 to update their tablets to BlackBerry PlayBook OS 2.1 or later to avoid work app and data loss.

Backing up the BlackBerry Configuration Database

You must back up the BlackBerry Configuration Database so that you can restore it if the BlackBerry Device Service upgrade process does not complete. You can use the backup and restore tools that are a part of Microsoft SQL Server to back up the BlackBerry Configuration Database.

For more information, see the Microsoft documentation for Microsoft SQL Server.

Performing a test upgrade of the BlackBerry Configuration Database

You can perform a test upgrade of the BlackBerry Configuration Database to help you identify and address potential issues that might occur during the database upgrade without affecting your production environment. You can also find out how long it takes to upgrade the BlackBerry Configuration Database.

When you perform a test upgrade of the BlackBerry Configuration Database, you back up the BlackBerry Configuration Database, restore the backup version of the BlackBerry Configuration Database to a database server that does not host the BlackBerry Configuration Database, and then run the CreateDB executable.

Perform a test upgrade of the BlackBerry Configuration Database

This task should be performed by a database administrator with the appropriate permissions to back up, restore, and upgrade the BlackBerry Configuration Database.

Before you begin: Verify that you configured the correct permissions on the database server that you want to perform a test upgrade of the BlackBerry Configuration Database on.

1. Log in to the computer that hosts the BlackBerry Configuration Database.
2. Back up the BlackBerry Configuration Database.
3. Log in to a computer that hosts a database server that you want to perform a test upgrade of the BlackBerry Configuration Database on.

4. Restore the backup version of the BlackBerry Configuration Database.
5. Copy the BlackBerry Device Service installation files to the database server.
6. Extract the contents to a folder on the computer.
7. Navigate to <*extracted_folder*>\Database.
8. Open the **BDSMgmt.cfg** file in a text editor.
9. Change the file to include information that is specific to your organization's environment.
10. Change CMD=Install to CMD=Upgrade.
11. Save and close the file.
12. Open a command prompt window.
13. Change the directory to <*extracted_folder*>\Database.
14. Type **CreateDB.exe BDSMgmt.cfg**.

BDSMgmt.cfg properties

Property	Description
CMD	This property specifies the type of action that the CreateDB executable must complete (for example, install or upgrade the BlackBerry Configuration Database).
DATABASE_NAME	This property specifies the name of the BlackBerry Configuration Database.
SERVER	This property specifies the name of the database server that hosts the BlackBerry Configuration Database. If a database instance hosts the BlackBerry Configuration Database, follow the format *database_server_name* *database_instance_name*.
USERID	If you use database authentication, this property specifies the username for the database account that has database creator permissions.
PASSWORD	If you use database authentication, this property specifies the password for the database account.
SCRIPT_ROOT	This property specifies the path to the DBInstallScripts folder. By default, this folder is in the same root folder that the CreateDB.exe file is located in.
LOG_DIR	This property specifies the path to the folder that you can create log files in. By default, this folder is in the same root folder that the CreateDB.exe file is located in.

Property	Description
DBMS	This property specifies the database management system that your organization uses.
DB_FILE_DIR	This property specifies an existing folder that you can save the database files in. By default, this folder is the same folder that the Microsoft SQL Server tempdb file is located in.
BACKUP_DIR	This property specifies an existing folder that you can save the database backup in. By default, this folder is the same folder that the Microsoft SQL Server database files are located in.
BES_TYPE	For the BlackBerry Device Service, this property must be set to BDS.

Verifying database permissions to upgrade the BlackBerry Configuration Database

The BlackBerry Device Service connects to the BlackBerry Configuration Database on the database server using the login information that you specified during the installation process (Windows authentication or Microsoft SQL Server authentication). If you want to use the setup application to upgrade the BlackBerry Configuration Database, the Windows account or Microsoft SQL Server account must have permissions on the database server to upgrade the BlackBerry Configuration Database.

You can configure database permissions using Microsoft SQL Server roles. You must verify that the Windows account or Microsoft SQL Server account is a member of the db_owner database role for the BlackBerry Configuration Database.

Upgrade a BlackBerry Configuration Database

If the security requirements of your organization do not allow applications to have permissions to create or upgrade databases, you can run the CreateDB executable on the database server to upgrade the BlackBerry Configuration Database instead of using the setup application. After you upgrade the BlackBerry Configuration Database using the CreateDB executable, you can run the setup application using a Windows account that has minimum permissions on the database server.

Before you begin: Verify that you configured the correct permissions on the database server.

1. Log in to the computer that hosts the database server. If you use a Windows account to upgrade the BlackBerry Configuration Database, you must log in to the computer using a Windows account that is a member of the db_owner database role for the BlackBerry Configuration Database.
2. Copy the BlackBerry Device Service installation files to the database server that hosts the BlackBerry Configuration Database.
3. Extract the contents to a folder on the computer.
4. Navigate to <*extracted_folder*>\Database.
5. Open the **BDSMgmt.cfg** file in a text editor.
6. Change the file to include information that is specific to your organization's environment.
7. Change CMD=Install to CMD=Upgrade.
8. Save and close the file.
9. Open a command prompt window.
10. Change the directory to <*extracted_folder*>\Database.
11. Type **CreateDB.exe BDSMgmt.cfg**.

BDSMgmt.cfg properties

Property	Description
CMD	This property specifies the type of action that the CreateDB executable must complete (for example, install or upgrade the BlackBerry Configuration Database).
DATABASE_NAME	This property specifies the name of the BlackBerry Configuration Database.
SERVER	This property specifies the name of the database server that hosts the BlackBerry Configuration Database. If a database instance hosts the BlackBerry Configuration Database, follow the format *database_server_name* *database_instance_name*.
USERID	If you use database authentication, this property specifies the username for the database account that has database creator permissions.
PASSWORD	If you use database authentication, this property specifies the password for the database account.
SCRIPT_ROOT	This property specifies the path to the DBInstallScripts folder. By default, this folder is in the same root folder that the CreateDB.exe file is located in.
LOG_DIR	This property specifies the path to the folder that you can create log files in.

Property	Description
	By default, this folder is in the same root folder that the CreateDB.exe file is located in.
DBMS	This property specifies the database management system that your organization uses.
DB_FILE_DIR	This property specifies an existing folder that you can save the database files in. By default, this folder is the same folder that the Microsoft SQL Server tempdb file is located in.
BACKUP_DIR	This property specifies an existing folder that you can save the database backup in. By default, this folder is the same folder that the Microsoft SQL Server database files are located in.
BES_TYPE	For the BlackBerry Device Service, this property must be set to BDS.

Connecting to an existing BlackBerry Configuration Database

You can connect only one BlackBerry Device Service to the BlackBerry Configuration Database. If you need to install the BlackBerry Device Service on a new computer and connect to an existing BlackBerry Configuration Database that you created or upgraded (for example, a disaster recovery situation), you can open a command prompt window, navigate to the BlackBerry Device Service installation files and type setup.exe /r.

Upgrading the BlackBerry Device Service software

6

Prerequisites: Upgrading the BlackBerry Device Service software

- Delete inactive user accounts from the BlackBerry Device Service.
- Back up the BlackBerry Configuration Database.
- If you perform the upgrade process on a computer that has more than one NIC, verify that the production NIC is first in the bind order in the Windows network settings.
- If you configured database replication for the BlackBerry Configuration Database, turn off database replication during the upgrade process to avoid possible errors.
- Verify that the Windows account that you use to upgrade the BlackBerry Device Service software is the same account that you used to install the BlackBerry Device Service software.

Upgrade the BlackBerry Device Service software

Before you upgrade the BlackBerry Device Service software, you must stop all BlackBerry Device Service services. During the BlackBerry Device Service upgrade process, you might need to restart the computer.

Before you begin:

- Verify that the service account that you use to upgrade the BlackBerry Device Service software has local administrator permissions on the computer that you perform the upgrade process on.
- The upgrade process deletes the IT policy rules in the Certification Authority Profile rule group. Document the existing IT policy settings in this rule group before you start the upgrade process so that you can create new SCEP profile

settings after the upgrade process is complete. For more information, see the *BlackBerry Device Service Policy Reference Guide*.

1. Log in to the computer using the service account that runs the BlackBerry Device Service services.
2. In the BlackBerry Mobile Fusion installation files, double-click **Autorun.exe**. If a Windows message appears and requests permission for Autorun.exe to make changes to the computer, click **Yes**.
3. On the BlackBerry Mobile Fusion installation screen, click **Install** for the BlackBerry Device Service software.
4. In the **License agreement** dialog box, perform the following actions:
   a. In the **License agreement** section, read the license agreement. To accept the license agreement, select **I accept the terms in the license agreement**.
   b. Click **Next**.
5. In the **Database information** dialog box, verify that the information is correct and select the check box to back up the database if you want the setup application to back up the BlackBerry Configuration Database before any database upgrades. Click **Next**.
6. If you see a warning message about BlackBerry PlayBook tablets running a software version earlier than 2.1, all users did not update their tablets to BlackBerry PlayBook OS 2.1 or later. Perform one of the following actions:
   - Click **Yes** to continue the upgrade process. Users can continue to use their tablets but work apps on the tablet and the associated application data are removed. For more information, see Upgrade implications for BlackBerry PlayBook tablet users.
   - Click **No** to cancel the upgrade process. You must notify users to update their tablets to PlayBook OS 2.1 or later to avoid work app and data loss. For more information, see Identify users that must update their BlackBerry PlayBook tablets.
7. In the **Setup information** dialog box, review the BlackBerry Device Service components that the setup application upgrades on the computer. Click **Next**.
8. In the **Preinstallation checklist** dialog box, read and verify the information. Click **Next**.
9. In the **Accounts and Folders** dialog box, perform the following actions:
   a. In the **Windows® account information** section, in the **Password** field, type the password for the service account that you used in step 1.
   b. Click **Next**.
10. In the **Summary** dialog box, verify that the information is correct. Click **Install**.
11. If the setup application prompts you to restart the computer, click **Yes**. Otherwise, click **Continue**.
12. If you restart the computer, log in to the computer using the service account that you used in step 1.
13. In the **Administration settings** dialog box, perform the following actions:
    a. In the **BlackBerry Administration Service domain name** section, verify the name that you use to access the BlackBerry Administration Service. If you created a DNS record for the computer that hosts the BlackBerry Administration Service, you can specify the DNS name.

b. Click **Next**.

14. In the **Start services** dialog box, click **Start Services**. When all the BlackBerry Device Service services start, click **Next**.
15. In the **Console addresses** dialog box, click **Finish**. By default, the setup application exports the BlackBerry Administration Service and BlackBerry Web Desktop Manager web addresses to a .txt file.

After you finish:

- To use SCEP profiles to obtain certificates for certificate-based authentication, create new SCEP profile settings in the BlackBerry Administration Service. For more information, see the *BlackBerry Device Service Administration Guide*.

Postupgrade tasks

7

Best practice: Running the BlackBerry Device Service

Best practice	Description
Do not change the startup type for the BlackBerry Device Service services.	When you install or upgrade the BlackBerry Device Service, the setup application configures the startup type for the BlackBerry Device Service services as either automatic or manual. For example, the setup application configures the startup type for the BlackBerry Mail Store Service to manual. To avoid errors in the BlackBerry Device Service, do not change the startup type for the BlackBerry Device Service services.
Do not change the account information for BlackBerry Device Service services.	When you install or upgrade the BlackBerry Device Service, the setup application configures the account information for the BlackBerry Device Service services. Do not change the account information for the BlackBerry Device Service unless the BlackBerry Device Service documentation specifies that you can.
Run the BlackBerry Configuration Panel as an administrator.	Consider the following guidelines to run the BlackBerry Configuration Panel: • Log in to the computer with a user account that is in the Administrators group on the Windows Server. • Right-click the BlackBerry Configuration Panel icon and click Run as administrator.

Import the SSL certificate for the messaging server to the BlackBerry Administration Service

If your organization's environment does not allow anonymous access to your messaging server and requires an SSL certificate to authenticate with the messaging server, you must import the SSL certificate to the BlackBerry Administration Service web.keystore file so that you can send an activation email message to a user. For more information about activation, see the *BlackBerry Device Service Administration Guide*.

For more information about using the keytool, visit docs.oracle.com/javase/6/docs/technotes/tools/windows/keytool.html.

Before you begin: Copy the SSL certificate for your organization's messaging server to the computer that hosts the BlackBerry Administration Service.

1. On the computer that hosts the BlackBerry Administration Service, in <*drive*>:\Program Files (x86)\Research In Motion\BlackBerry Device Service\BAS\bin, back up the **web.keystore** file.
2. Open a command prompt window (run as administrator).
3. Change the directory to <*drive*>:\Program Files (x86)\Java\<*JRE_version*>\bin.
4. Type **keytool -importcert -keystore "<*drive*>:\Program Files (x86)\Research In Motion\BlackBerry Device Service\BAS\bin\web.keystore" -file "<*certificate_filename*>.cer" -alias mailserver**.
5. When you receive a prompt, type the SSL password that you specified when you installed the BlackBerry Administration Service.
6. When you receive a prompt to trust the certificate, type **yes**.
7. In Windows Services, restart the BlackBerry Administration Service services.

Log in to the BlackBerry Administration Service

You can use the BlackBerry Administration Service to manage the BlackBerry Device Service and the user accounts and tablets that are associated with it. To open the BlackBerry Administration Service, you can use a browser on a computer that has access to the computer that hosts the BlackBerry Device Service. You can set an administrator account to use

Microsoft Active Directory or BlackBerry Administration Service credentials to log in to the BlackBerry Administration Service.

When you install the BlackBerry Device Service, you specify the credentials that you use to log in to the BlackBerry Administration Service for the first time.

1. In the browser, type **https://*<server_name>*/webconsole/login**, where *<server_name>* is the name of the computer that hosts the BlackBerry Administration Service.
2. In the **User name** field, type your user name.
3. In the **Password** field, type your password.
4. Perform one of the following actions:
   - In the **Log in using** drop-down list, click **BlackBerry Administration Service**.
   - In the **Log in using** drop-down list, click **Active Directory** and type the Microsoft Active Directory domain in the **Domain** field.
5. Click **Log in**.
6. Install the RIMWebComponents.cab add-on if you are prompted to do so.

There is a problem with this website's security certificate

Description

This message appears when you try to navigate to the BlackBerry Administration Service using Windows Internet Explorer 8 or later.

Possible solution

Add the web address for the BlackBerry Administration Service to the list of trusted web sites in Windows Internet Explorer, and install the certificate for the BlackBerry Administration Service in the certificate store of your computer.

1. In Windows Internet Explorer, navigate to the BlackBerry Administration Service console.
2. Click **Continue to this website (not recommended)**.
3. On the **Tools** menu, click **Internet Options**.
4. On the **Security** tab, click **Local Intranet**.
5. Click **Sites**.
6. Click **Add** to add the console to the list of trusted web sites.
7. Click **Close**.
8. Click **OK**.

9. In the browser window, on the toolbar, click **Certificate Error**.
10. Click **View certificates**.
11. Click **Install certificate**. The Certificate Import Wizard opens.
12. Complete the instructions in the Certificate Import Wizard. If you are trying to log in to the BlackBerry Administration Service using a computer that runs Windows Vista, perform the following actions in the Certificate Import Wizard:
    a In the **Certificate Store** dialog box, click **Place all certificates in the following store**.
    b Click **Browse**.
    c Click **Trusted Root Certification Authorities**.
    d Click **OK**.
13. Close and reopen the browser.

Configuring database permissions using Microsoft SQL Server roles

The BlackBerry Device Service setup application requires the service account or Microsoft SQL Server account that it uses during the installation or upgrade process to have permissions on the database server to create or upgrade the BlackBerry Configuration Database. After the installation or upgrade process completes, you can change the database permissions for the service account or Microsoft SQL Server account to the minimum permission that the BlackBerry Device Service requires to run.

When you change the database permissions, you can use Microsoft SQL Server security to minimize the operations that the service account or Microsoft SQL Server account can perform on the BlackBerry Configuration Database. The following table describes the Microsoft SQL Server roles that are required by the setup application and the BlackBerry Device Service.

Database role	Description
db_owner	The setup application requires this role to upgrade the BlackBerry Configuration Database. This role is the default permission in Microsoft SQL Server for running the BlackBerry Device Service.
rim_db_bes_server	The setup application or the CreateDB executable creates this role automatically when it creates the BlackBerry Configuration Database. This role is the minimum permission in Microsoft SQL Server for running the BlackBerry Device Service.

Configure minimum database permissions for the service account or Microsoft SQL Server account

You can configure minimum database permissions for the service account or Microsoft SQL Server account that the BlackBerry Device Service uses to connect to the BlackBerry Configuration Database.

Before you begin: Add a different Windows account or Microsoft SQL Server account to the db_owner database role for the BlackBerry Configuration Database.

1. Open the Microsoft SQL Server Management Studio.
2. Expand **Microsoft SQL Server** > **Security** > **Logins**.
3. Right-click the service account or Microsoft SQL Server account and click **Properties**.
4. Click **User Mapping** and select the BlackBerry Configuration Database.
5. In the **Database role membership** section, select **rim_db_bes_server**.
6. Remove all other database role memberships except public.
7. Apply your changes.

Glossary

8

BlackBerry MDS	BlackBerry Mobile Data System
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.
DNS	Domain Name System
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
JRE	Java Runtime Environment
LAN	local area network
NIC	network interface card
RRAS	Routing and Remote Access service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	virtual private network

Legal notice

9

©2012 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

Mac and Safari are trademarks of Apple Inc. Check Point is a trademark of Check Point Software Technologies Ltd. Cisco, Cisco IOS, and PIX are trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Google Chrome is a trademark of Google Inc. IBM, Domino, Lotus, and Lotus Notes are trademarks of International Business Machines Corporation. Intel and Xeon are trademarks of Intel Corporation. Juniper and NetScreen are trademarks of Juniper Networks, Inc. Microsoft, ActiveSync, Active Directory, ActiveX, Internet Explorer, SQL Server, Windows, Windows Server, and Windows Vista are trademarks of Microsoft Corporation. Mozilla and Firefox are trademarks of Mozilla Foundation. Java, JavaScript, and JRE are trademarks of Oracle and/or its affiliates. Wi-Fi is a trademark of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at www.blackberry.com/go/docs is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites (collectively the "Third Party Products and Services"). RIM does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE

HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

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.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

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

Research In Motion UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada