BlackBerry Device Service

Feature and Technical Overview

Version: 6.0

BlackBerry

Published: 2012-02-16
SWD-20120216115342889

Contents

1 About the BlackBerry Device Service....4
Comparing BlackBerry Device Service with the BlackBerry Enterprise Server and BlackBerry Enterprise Server Express....4
2 Architecture....6
Architecture: BlackBerry Device Service....6
Architecture: BlackBerry Web Desktop Manager....8
3 Components and features....10
BlackBerry Administration Service....10
BlackBerry Mobile Fusion Studio....10
Application management features....11
Managing applications....11
Managing software configurations....11
Message synchronization features....12
Managing email profiles....12
BlackBerry Mail Store Service....13
Contact information that the BlackBerry Mail Store Service stores in the BlackBerry Configuration Database....13
BlackBerry MDS Connection Service....14
BlackBerry Web Desktop Manager....14
4 Data flows....16
Data flow: Activating user accounts using BlackBerry Web Desktop Manager....16
Data flow: Sending configuration updates to tablets....17
Data flow: Sending application updates to tablets....18
Data flow: Sending and receiving email on a BlackBerry PlayBook tablet using Microsoft ActiveSync....19
5 Related resources....20
6 Glossary....22
7 Legal notice....23

About the BlackBerry Device Service

1

The BlackBerry Device Service permits you to manage the work perimeter on BlackBerry PlayBook tablets that run BlackBerry Tablet 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 the BlackBerry Mobile Fusion Studio. The 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.

Comparing BlackBerry Device Service with the BlackBerry Enterprise Server and BlackBerry Enterprise Server Express

The following table compares the features of the BlackBerry Device Service with the BlackBerry Enterprise Server and BlackBerry Enterprise Server Express.

Feature	BlackBerry Device Service	BlackBerry Enterprise Server Express	BlackBerry Enterprise Server
Supported devices	BlackBerry PlayBook tablets	BlackBerry smartphones	BlackBerry smartphones
Supported messaging servers	Supports configuration of a Microsoft ActiveSync client on the tablet to provide direct synchronization with messaging servers that support Microsoft ActiveSync	• Microsoft Exchange • IBM Lotus Domino	• Microsoft Exchange • IBM Lotus Domino • Novell GroupWise
Supported operating systems	• Windows Server 2008 R2 (64-bit only) • Windows Server 2008 R2 SP1 (64-bit only)	• Windows Server 2003 SP2 (32-bit or 64-bit) • Windows Server 2003 R2 SP2 (32-bit or 64-bit) • Windows Server 2008 SP2 (32-bit or 64-bit) • Windows Server 2008 R2	• Windows Server 2003 SP2 (32-bit or 64-bit) • Windows Server 2003 R2 SP2 (32-bit or 64-bit) • Windows Server 2008 SP2 (32-bit or 64-bit) • Windows Server 2008 R2

Feature	BlackBerry Device Service	BlackBerry Enterprise Server Express	BlackBerry Enterprise Server
		• Windows Server 2008 R2 SP1 • Windows Small Business Server 2003 • Windows Small Business Server 2008 • Windows Small Business Server 2011 Standard	
Instances in one BlackBerry Domain	• Only one BlackBerry Device Service instance is supported in a BlackBerry Domain • BlackBerry Device Service instances are not supported in a BlackBerry Domain that includes BlackBerry Enterprise Server Express or BlackBerry Enterprise Server instances	• Multiple BlackBerry Enterprise Server Express instances and versions are supported in a BlackBerry Domain • BlackBerry Enterprise Server instances are not supported in a BlackBerry Domain that includes BlackBerry Enterprise Server Express or BlackBerry Device Service instances	• Multiple BlackBerry Enterprise Server instances and versions are supported in a BlackBerry Domain • BlackBerry Enterprise Server Express instances are not supported in a BlackBerry Domain that includes BlackBerry Enterprise Server or BlackBerry Device Service instances
Administrative roles	• Preconfigured administrative roles only	• Preconfigured administrative roles only	• Preconfigured administrative roles • Custom administrative roles
IT policies	• Default IT policy • Custom IT policies • Reduced set of IT policy rules	• Default IT policy • Custom IT policies • Reduced set of IT policy rules	• Default IT policy and specific preconfigured IT policies • Custom IT policies • Full set of IT policy rules
BlackBerry enterprise instant messaging clients	Not supported	Not supported	Supported
High availability	Not supported	Not supported	Supported

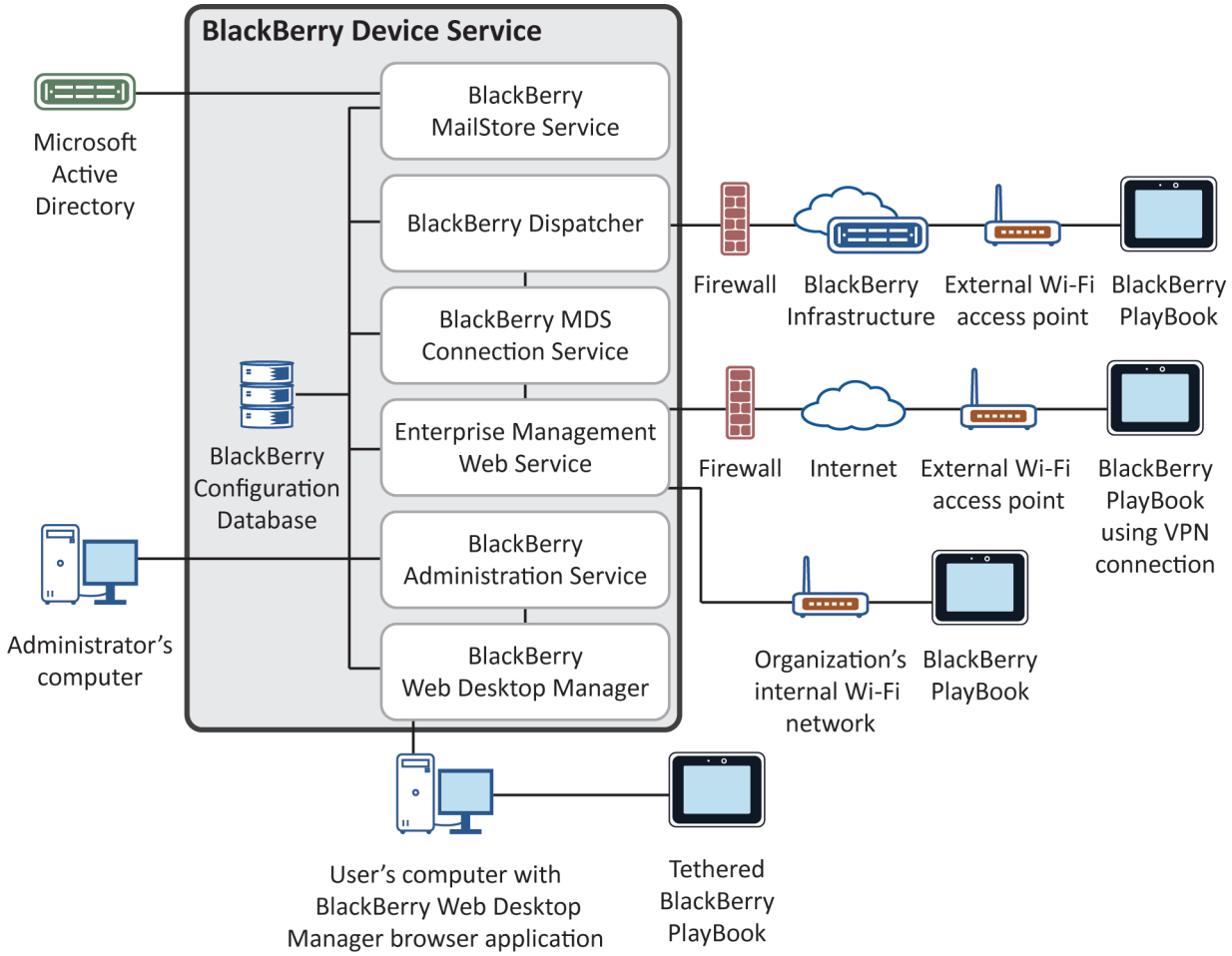
Architecture

2

Architecture: BlackBerry Device Service

The BlackBerry Device Service consists of various components that are designed to help you perform the following actions:

- Install and manage your organization's applications on BlackBerry PlayBook tablets.
- Protect your organization's data and applications on tablets



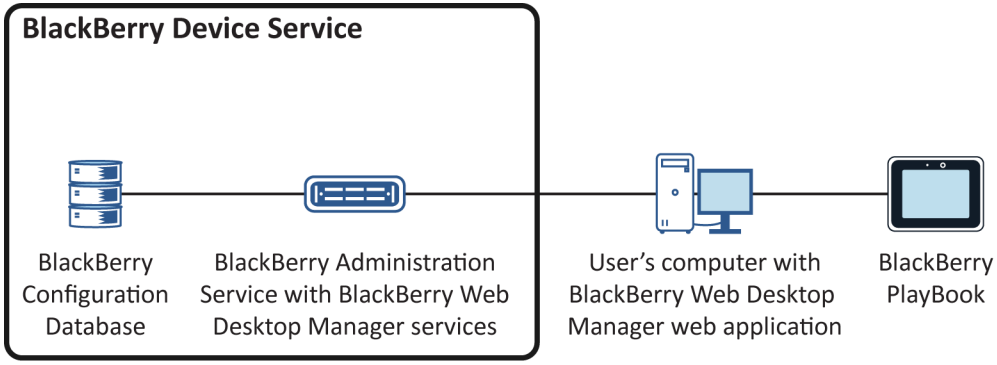
Component	Description
BlackBerry Administration Service	You can use the BlackBerry Administration Service to manage the BlackBerry Device Service and the user accounts and tablets that are associated with it. You can manage user accounts and assign groups, administrative roles, software configurations, email profiles, and IT policies to user accounts. The BlackBerry Administration Service connects to the BlackBerry Configuration Database.
BlackBerry Configuration Database	The BlackBerry Configuration Database is a relational database that contains user account information and configuration information (such as connection details) that the BlackBerry Device Service components use.
BlackBerry Mail Store Service	The BlackBerry Mail Store Service connects to the Microsoft Active Directory in your organization's environment and retrieves user information that the BlackBerry Administration Service requires to activate user accounts. You can add a user account to the BlackBerry Device Service only if the user account exists in your organization's Microsoft Active Directory.
Enterprise Management Web Service	The Enterprise Management Web Service is a set of web services that communicates commands, configuration information, IT policies, VPN profiles, Wi-Fi profiles, and email profiles between the BlackBerry Administration Service and the Enterprise Management Agent on the tablets.
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service provides a secure connection between the Enterprise Management Agent on the tablets and the Enterprise Management Web Service in the BlackBerry Device Service. The connection is used when the tablet is not connected to your organization's Wi-Fi network or VPN.
BlackBerry Dispatcher	The BlackBerry Dispatcher maintains a connection with the BlackBerry Infrastructure over the Internet. The BlackBerry Dispatcher is responsible for compressing and encrypting and for decrypting and decompressing data that travels over the Internet to and from the tablets.
BlackBerry Web Desktop Manager	The BlackBerry Web Desktop Manager is a web application that permits users to activate and manage tablets.
Microsoft Active Directory	The BlackBerry Mail Store Service obtains user account information from the Microsoft Active Directory that is required to create user accounts in the BlackBerry Device Service.
organization's Wi-Fi network	After a tablet is activated on the BlackBerry Device Service, communication between the BlackBerry Device Service and the tablet can occur over your organization's Wi-Fi network when the tablet is within a wireless coverage area and enabled for access as may be required by your organization's network security policies.
external Wi-Fi access point	Depending on your organization's network configuration, communication can occur between the BlackBerry Device Service and tablets that are located

Component	Description
	outside the firewall and connected to the Internet over an external Wi-Fi connection.
firewall	The BlackBerry Device Service requires an outbound-initiated, bidirectional connection through port 3101 on the firewall and over the Internet to the BlackBerry Infrastructure to transport data to and from the tablets.
Internet	The Internet transports data between the BlackBerry Infrastructure and the BlackBerry Device Service. Depending on your organization's network configuration, the tablets may also communicate with the BlackBerry Device Service using a VPN connection over the Internet.

Architecture: BlackBerry Web Desktop Manager

The BlackBerry Web Desktop Manager is a web application that allows BlackBerry PlayBook tablet users to perform certain management tasks on their tablets.

The BlackBerry Web Desktop Manager consists of server-side services that are installed with the BlackBerry Administration Service and components that are installed on the users' computers. By default, when tablet users open the BlackBerry Web Desktop Manager for the first time, the browser prompts them to accept a client authentication certificate and install the required RIMWebComponents.cab file. The RIMWebComponents.cab file provides theBlackBerry Device Manager and USB drivers that users require to use the BlackBerry Web Desktop Manager. The connection between the server and the browser uses HTTPS authentication.



Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service is a web application that is part of the BlackBerry Device Service. You can use the BlackBerry Administration Service to manage user accounts.

Component	Description
	The BlackBerry Administration Service and BlackBerry Web Desktop Manager services provide the server-side services for the BlackBerry Web Desktop Manager web application.
BlackBerry Configuration Database	The BlackBerry Configuration Database is a relational database that contains configuration information, such as BlackBerry Device Service connection details and user account information.
User's computer with BlackBerry Web Desktop Manager web application	The BlackBerry Web Desktop Manager web application includes the BlackBerry Device Manager and USB drivers that are installed on the user's computer.

Components and features

3

BlackBerry Administration Service

The BlackBerry Administration Service is a web application that you use to manage user accounts and to assign user groups, administrative roles, email profiles, software configurations, and IT policies to user accounts. You can open the BlackBerry Administration Service console in a browser on a computer that can access the computer that hosts the BlackBerry Administration Service. You can share administrative duties with multiple administrators who can access the BlackBerry Administration Service at the same time using unique user names and passwords.

Feature	Description
BlackBerry Administration Service authentication or external authentication	Administrators that log in to the BlackBerry Administration Service must provide user names and passwords. You can use unique user names and passwords or you can use external authentication, which permits administrators to log in to the BlackBerry Administration Service using the same information that administrators use to access your organization's Microsoft Active Directory.
Management of user accounts	The BlackBerry Administration Service provides access to features for managing user accounts, including Microsoft ActiveSync configuration options and IT policy options.
Ability to assign user accounts to multiple groups	Groups permit you to share administrative roles, IT policies, and other configuration settings among similar user accounts so that you can set the properties one time for the group instead of setting the properties individually for each user. You can assign a user account to more than one group so that the user account inherits the properties of every group that the account belongs to. You can also assign groups to other groups to share the properties of the parent group.
Options for viewing the BlackBerry Domain	You can find and manage BlackBerry Device Service components using the Server view or Component view.

BlackBerry Mobile Fusion Studio

The BlackBerry Mobile Fusion Studio is designed to make managing user accounts across multiple BlackBerry Domains more organized and efficient. The BlackBerry Mobile Fusion Studio is an administration interface that allows you to administer BlackBerry smartphones and BlackBerry PlayBook tablets. The BlackBerry Mobile Fusion Studio provides organizations with a single tool to manage many common day-to-day tasks that are associated with the BlackBerry Administration Service.

The BlackBerry Mobile Fusion Studio links to the associated BlackBerry Administration Service console so that you can use the BlackBerry Administration Service console to perform tasks that the BlackBerry Mobile Fusion Studio does not support. For more information, see the BlackBerry Mobile Fusion Studio documentation.

The BlackBerry Mobile Fusion Studio allows you to do the following:

- Use a single interface to manage smartphones and tablets
- Manage multiple domains
- Add and activate accounts
- Lock and delete data from devices remotely

You can connect to the BlackBerry Mobile Fusion Studio using the same browsers that the BlackBerry Administration Service supports.

Application management features

Managing applications

You can use the BlackBerry Device Service to install and manage third-party applications on BlackBerry PlayBook tablets. You can specify the versions of the applications that you want to install, update, or remove, and you can specify which applications are required or optional on tablets. If you specify that an application is optional, the BlackBerry Device Service makes the application available to the user for installation on the Work tab in the BlackBerry App World storefront. If you specify that an application is required, the application is automatically installed on the tablet and the user cannot remove it.

When you use the BlackBerry Device Service to manage applications, the applications are considered work applications and are installed in the work perimeter on tablets. The applications can only access work data and interact with other work applications that are also located in the work perimeter. The applications have read-only access to personal data and cannot interact with personal applications that are located in the personal perimeter. You cannot manage or remove the personal applications that BlackBerry PlayBook users installed on their tablets.

Application developers can use various development tools to create, test, and package applications so that you can install them on the tablets in your organization's environment. For more information about the development tools, visit www.blackberry.com/developers.

Note: The work perimeters on tablets do not support Android Runtime applications.

Managing software configurations

You can use software configurations to bundle applications so that the applications can be installed on BlackBerry devices. When you create a software configuration, you can specify the following:

- Versions of the work applications that you want to install on devices
- Applications that are required or optional

After you create a software configuration, you can assign it to a group or individual user accounts. The BlackBerry Administration Service creates a deployment job to make the required applications available for devices to download and install. A deployment job consists of a number of tasks. Each task manages the delivery of a specific object (for example,

an application) by communicating with the appropriate BlackBerry Device Service components. The BlackBerry PlayBook tablet automatically installs required applications in the work perimeter after the tablet downloads them.

Deployment jobs are not created for optional applications. Optional applications are made available in the Work tab on the BlackBerry App World storefront. Users can choose whether they want to download, install, or remove optional applications.

To remove application from devices, you can remove the application from a software configuration.

Message synchronization features

You can extend your organization's messaging environment to BlackBerry PlayBook tablets in two ways:

- You can allow BlackBerry PlayBook tablet users to connect to your organization's messaging server using Microsoft ActiveSync. You can manage email profile settings for Microsoft ActiveSync using the BlackBerry Administration Service.
- If you are using the BlackBerry Enterprise Server or BlackBerry Enterprise Server Express to manage BlackBerry smartphones, you can also allow tablet users to use the BlackBerry Bridge. The BlackBerry Bridge allows users to connect their tablets to their smartphone to access email, calendars, BlackBerry Messenger, files, and other data on the tablet. For details, see the information about BlackBerry Bridge in the *BlackBerry PlayBook Tablet User Guide*.

Managing email profiles

You can use email profiles to specify how BlackBerry PlayBook tablets connect to your organization's messaging server and synchronize email messages and organizer data using Microsoft ActiveSync. You can add email profiles to user accounts.

Email profiles include the following settings.

Setting	Description
Type	This setting specifies the type of email account for the email profile.
Server name	This setting specifies the name of the messaging server.
Use SSL	This setting specifies whether SSL is allowed when the tablet connects to the messaging server.
Push enabled	This setting specifies whether the messaging server can push email messages and organizer data to the tablet.
Days to synchronize	This setting specifies the number of days prior that the tablet synchronizes with.
Interval between synchronizations	This setting specifies how often the tablet checks the messaging server for notifications and email messages that the messaging server does not push to the tablet.

Setting	Description
Email synchronization	This setting specifies whether the tablet synchronizes email messages with the messaging server.
Calendar synchronization	This setting specifies whether the tablet synchronizes calendar entries with the messaging server.
Contact synchronization	This setting specifies whether the tablet synchronizes contacts with the messaging server.

BlackBerry Mail Store Service

The BlackBerry Mail Store Service connects to the Microsoft Active Directory in your organization's environment and retrieves the contact information that the BlackBerry Administration Service requires to search for user accounts.

The BlackBerry Mail Store Service performs the following actions:

- Synchronizes your organization's contact list with the BlackBerry Configuration Database
- Updates the contact list in the BlackBerry Configuration Database every 24 hours automatically
- Permits the BlackBerry Administration Service to access user account information that is stored in the Microsoft Active Directory
- Exposes an API that the BlackBerry Administration Service can use to connect to the BlackBerry Mail Store Service
- Searches for contact information on behalf of the BlackBerry Administration Service

Contact information that the BlackBerry Mail Store Service stores in the BlackBerry Configuration Database

The BlackBerry Mail Store Service synchronizes contact information from the Microsoft Active Directory with the BlackBerry Configuration Database. The BlackBerry Mail Store Service updates the contact information in the BlackBerry Configuration Database daily.

Contact information	Database property name	Description
Address type	Type	This property specifies whether the address is for a user account or distribution list.
Display name	DisplayName	This property specifies the display name for the user account.
Email address	MailboxSMTP	This property specifies the email address for the user account.
Mailbox path	MailboxKey	This property specifies the unique mailbox path.

Contact information	Database property name	Description
Messaging server path	ServerName	This property specifies the path to the messaging server.

BlackBerry MDS Connection Service

The BlackBerry MDS Connection Service provides a secure connection between the Enterprise Management Agent on BlackBerry PlayBook tablets and the Enterprise Management Web Service in the BlackBerry Device Service. The BlackBerry Device Service and tablet use the connection when the tablet is not connected to an enterprise Wi-Fi network or a VPN and the following situations occur:

- You need to send IT administration commands to the tablet
- A BlackBerry PlayBook tablet user browses to work resources (for example, your organization's Intranet) using HTTP or HTTPS
- A user sends or receives email messages, calendar entries, or organizer data for the user's work email account using Microsoft ActiveSync
- A work application on the tablet needs to access work resources on your organization's network

The connection that the BlackBerry MDS Connection Service makes to the Enterprise Management Agent uses the BlackBerry Infrastructure to provide security. For example, if the BlackBerry MDS Connection Service sends IT administration commands to a tablet, the BlackBerry MDS Connection Service can connect to the tablet using the BlackBerry Infrastructure and push the IT administration command to the tablet.

BlackBerry Web Desktop Manager

The BlackBerry Web Desktop Manager is a web application that provides tablet management features to BlackBerry PlayBook tablet users. Users can connect their BlackBerry PlayBook tablets to computers using a USB connection, and log in to BlackBerry Web Desktop Manager to activate and manage tablets. Users can also log in to the BlackBerry Web Desktop Manager to change their password or delete their data remotely in case the tablet is lost or stolen.

Feature	Description
Access from anywhere	Users can access tablet management and configuration capabilities from any computer that can access the intranet.
Customizable interface	You can customize the appearance of the UI to match your organization's requirements. You can customize the font colors, logo, and the help.
Tablet activation	Users can use the BlackBerry Web Desktop Manager to activate their tablets. The activation process uses Microsoft ActiveX controls. Users must open BlackBerry Web Desktop Manager in Microsoft Internet Explorer to activate their tablets.

Feature	Description
Simplified administration	The web UI does not require you to deploy, support, and maintain client-side software.

Data flows

4

Data flow: Activating user accounts using BlackBerry Web Desktop Manager

When you activate user accounts, you associate the work perimeter on BlackBerry PlayBook tablets with user accounts in the BlackBerry Device Service and establish a secure communication channel between the tablets and the BlackBerry Device Service so that BlackBerry PlayBook tablet users can access your organization's resources.

1. An administrator adds a user account to the BlackBerry Administration Service from the account information in the organization's Microsoft Active Directory.
2. A user performs the following actions:
   a Connects a tablet to a computer using a USB cable.
   b Browses to BlackBerry Web Desktop Manager using Windows Internet Explorer and logs in.
3. If necessary, the browser downloads and installs the BlackBerry Device Communication Components. The BlackBerry Device Communication Components are Microsoft ActiveX controls that permit the BlackBerry Administration Service to communicate with a tethered tablet.
4. The BlackBerry Device Communication Components send the tablet PIN to the BlackBerry Administration Service over an HTTPS connection to start the activation process.
5. The BlackBerry Administration Service receives the tablet PIN and performs the following actions:
   a Stores the tablet PIN in the BlackBerry Configuration Database.
   b Generates an activation password. The administrator and user cannot view the activation password.
   c Sends the activation password, user ID, and the server name and port of the Enterprise Management Web Service to the Enterprise Management Agent.
6. The Enterprise Management Agent creates the work perimeter.
7. The Enterprise Management Agent and Enterprise Management Web Service generate a shared symmetric key using the activation password and EC-SPEKE. The shared symmetric key is designed to help protect the CSR and response.
8. The Enterprise Management Agent performs the following actions:
   a Generates a key pair for the certificate.
   b Creates a PKCS#10 CSR that includes the public key of the key pair.
   c Sends the CSR to the Enterprise Management Web Service.
9. The Enterprise Management Web Service performs the following actions:
   a Retrieves the user ID, work perimeter ID, tablet PIN, and your organization’s name from the BlackBerry Configuration Database.

   b Packages a client certificate using the information it retrieved and the CSR that the Enterprise Management Agent sent.
   c Signs the client certificate using the enterprise management root certificate.
   d Sends the client certificate, enterprise management root certificate, and the Enterprise Management Web Service URL to the Enterprise Management Agent.

10. The Enterprise Management Agent stores the client certificate, enterprise management root certificate, and the authentication certificate for the Enterprise Management Web Service in its key store.
11. The Enterprise Management Agent and Enterprise Management Web Service generate the device transport key using ECMQV and the long-term public keys in the client certificate and the authentication certificate for the Enterprise Management Web Service.
12. The Enterprise Management Agent stores the device transport key in its key store.
13. The Enterprise Management Web Service performs the following actions:
   a Stores the device transport key in the BlackBerry Configuration Database.
   b Sends the IT policy, SRP information, profiles, and software configurations to the tablet over TLS.
14. The Enterprise Management Agent sends an acknowledgment that it received the IT policy and other data to the Enterprise Management Web Service over TLS. The activation process is complete.

The elliptic curve protocols used during activation use the NIST-recommended 521-bit curve.

Data flow: Sending configuration updates to tablets

You can configure administrative commands, application information, IT policies, email profiles, Wi-Fi profiles, and VPN profiles for BlackBerry PlayBook tablets using the BlackBerry Administration Service. This configuration information is sent to the Enterprise Management Agent on the work perimeter of the tablet over a secure, preauthenticated connection through the Enterprise Management Web Service.

1. You complete one of the following actions in the BlackBerry Administration Service:
   - Select an IT command such as wipe work perimeter, wipe entire device, full device lock, or lock work perimeter and change password for a tablet
   - Remove a tablet from a user account
   - Assign or change an IT policy
   - Assign or change a VPN profile or Wi-Fi profile
   - Assign or change Microsoft ActiveSync configuration settings
   - Assign or change email configuration settings
   - Assign or change root certificates
2. If data conflicts exist, the BlackBerry Administration Service uses predefined reconciliation rules to resolve the conflicts. Updates are applied in the BlackBerry Device Service and the BlackBerry Administration Service identifies objects that must be shared with the tablet.

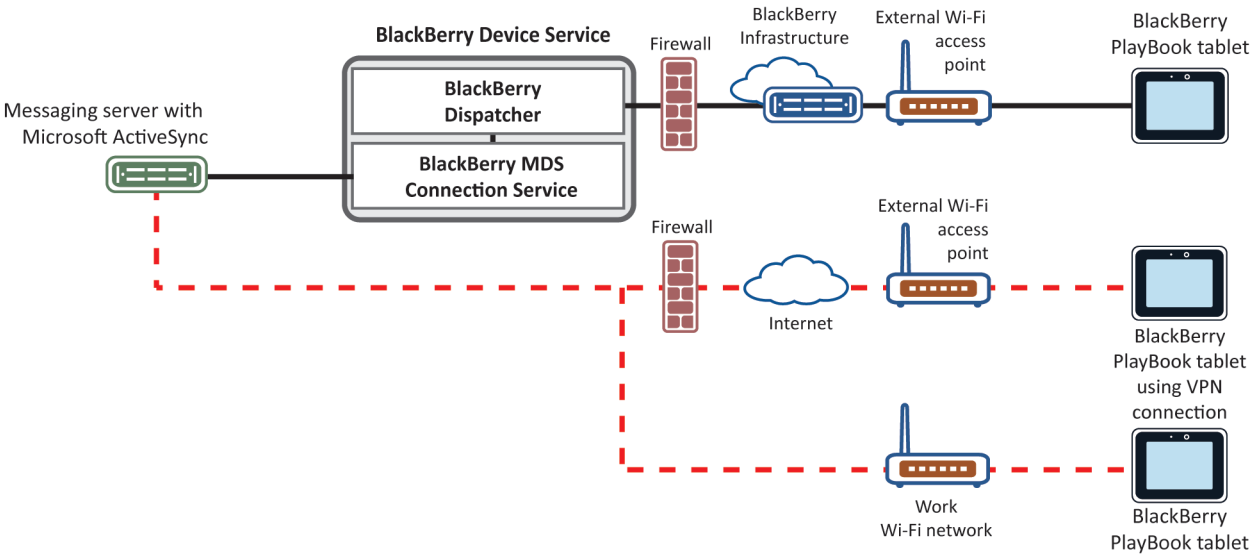
3. The Enterprise Management Web Service notifies the Enterprise Management Agent on the tablet that there is an update.
4. The Enterprise Management Agent polls the Enterprise Management Web Service for the update.
5. The Enterprise Management Web Service sends the configuration updates to the Enterprise Management Agent.
6. The Enterprise Management Agent retrieves the configuration updates and communicates with the Perimeter Manager on the tablet to apply the new or updated configuration on the work perimeter of the tablet.

Data flow: Sending application updates to tablets

You use software configurations to specify applications that are required or optional for the work perimeter of the BlackBerry PlayBook tablets. Required applications are installed in the work perimeter after the tablet receives them. Optional applications can be downloaded and installed to the work perimeter. Applications that are not listed as required or optional can only be installed in the personal perimeter.

1. You complete one of the following actions in the BlackBerry Administration Service:
   - Create a software configuration and assign it to a user account or a group the user account belongs to
   - Update a software configuration that is already assigned to the user account
   - Update application information
2. If data conflicts exist, the BlackBerry Administration Service uses predefined reconciliation rules to resolve the conflicts. Updates are applied in the BlackBerry Device Service and the BlackBerry Administration Service identifies objects that must be shared with the tablet.
3. The Enterprise Management Web Service notifies the Enterprise Management Agent on the tablet that there is an update.
4. The Enterprise Management Agent on the tablet polls the Enterprise Management Web Service for updates.
5. The Enterprise Management Web Service sends the update to the Enterprise Management Agent.
6. If a required application was added or updated, the Enterprise Management Agent accesses the URL that is specified in the application information to download and install the required application to the work perimeter.
7. If the list of optional applications changed, the Work tab in the BlackBerry App World storefront displays the updated list and the user can download and install the application.

Data flow: Sending and receiving email on a BlackBerry PlayBook tablet using Microsoft ActiveSync



1. The tablet issues an HTTPS request to the messaging server and requests that the messaging server notifies the tablet if any items change in the folders that are configured to synchronize.
2. The tablet stands by. The synchronization time can be adjusted, depending on your messaging server. Some messaging servers do not support HTTP sessions that are 15 minutes. For more information, go to

   http://technet.microsoft.com/en-us/

   to read article 182270.
3. The messaging server checks for any new or changed items and notifies the tablet when items change or new items come into the user's mailbox. The notification contains the name of the folder that has the new or changed item.
4. The tablet issues a synchronization request for the folder.
5. The messaging server synchronizes the changed files with the tablet.
6. When the synchronization is complete, the tablet issues another request to start the whole process over.
7. If there are no new or changed items during this interval, the messaging server sends a "HTTP 200 OK" message to the tablet.
8. The tablet issues a new PING request.

Related resources

5

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

Resource	Information
BlackBerry Device Service and BlackBerry Mobile Fusion Studio Installation and Configuration Guide	• System requirements • Installation instructions • Instructions to add or remove MDM domains from BlackBerry Mobile Fusion Studio
BlackBerry Administration Service Help and *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 and 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 Tablet 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 BlackBerry Bridge app • 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 Device Service Policy Reference Guide	• Description of available IT policy rules and profile settings

Resource	Information
BlackBerry Device Service Release Notes	• Description of known issues and potential workarounds

Glossary

6

BlackBerry Domain	A BlackBerry Domain consists of the BlackBerry Configuration Database with its users and the BlackBerry Device Service that connects to it.
BlackBerry MDS	BlackBerry® Mobile Data System
CSR	certificate signing request
ECMQV	Elliptic Curve Menezes-Qu-Vanstone
EC-SKEPE	Elliptic Curve – Simple Password Exponential Key Exchange
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IT administration command	An IT administration command is a command that you can send over the wireless network to protect sensitive information on a BlackBerry device or delete all BlackBerry device data.
IT policy	An IT policy consists of various IT policy rules that control the security features and behavior of BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager.
IT policy rule	An IT policy rule permits you to customize and control the actions that BlackBerry smartphones, BlackBerry® PlayBook™ tablets, the BlackBerry® Desktop Software, and the BlackBerry® Web Desktop Manager can perform.
messaging server	A messaging server sends and processes messages and provides collaboration services, such as updating and communicating calendar and address book information.
NIST	National Institute of Standards and Technology
PIN	personal identification number
PKCS	Public-Key Cryptography Standards
SRP	Server Routing Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
VPN	virtual private network

Legal notice

7

©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.

IBM, Domino, and Lotus, are trademarks of International Business Machines Corporation. Microsoft, Active Directory, ActiveSync, Microsoft ActiveX, Internet Explorer and Windows are trademarks of Microsoft Corporation. Novell and GroupWise are trademarks of Novell, Inc. Wi-Fi is a trademark of the Wi-Fi Alliance. All other brands, product names, company names, trademarks, and service marks are the properties of their respective owners.

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

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