Universal Device Service

Version: 6.1

Installation and Configuration Guide

BlackBerry®

Published: 2013-02-11
SWD-20130211171025279

Contents

1 Related resources 5
2 About the Universal Device Service 6
3 Planning a Universal Device Service installation 7
Installing the Universal Device Service with other software 7
Installing all Universal Device Service components on one computer 8
Installing the Core Module 8
Installing the Communication Module 8
Installing the Console services 8
Universal Device Service connection types and port numbers for all devices 9
Universal Device Service connection types and port numbers for iOS devices 10
4 Requirements 11
System requirements: iOS devices and Android devices 11
System requirements: Firewall 12
System requirements: Your organization's environment 13
Hardware requirements: Universal Device Service 13
Hardware requirements: All Universal Device Service components on one computer 14
Hardware requirements: Management Database 14
Hardware requirements: Universal Device Service distributed deployment 15
Software requirements: Universal Device Service and components 16
Software requirements: Database server 17
Software requirements: Browser 17
Supported features and environments 18
5 Preinstallation tasks 19
Requesting an SSL certificate for the Communication Module 19
Create a CSR 19
Submit the CSR to a certification authority 20
Complete the CSR 20
Remove the WebDAV Publishing role service 21
Installing the Universal Device Service on Windows Small Business Server 21
Update the 8.3 naming convention settings 21
Configuring connections for the Management Database 22
Specifying database permissions to create the Management Database 22
Create a Management Database 23
Applications that are installed with the Universal Device Service 24
6 Installing the Universal Device Service software 26

Prerequisites: Installing the Universal Device Service software ... 26
Install the Universal Device Service software ... 26
Install the Communication Module in the DMZ ... 29
7 Postinstallation tasks ... 31
Test the Universal Device Service installation ... 31
Best practice: Running the Universal Device Service ... 31
Log in to the Administration Console ... 32
Configuring database permissions using Microsoft SQL Server roles ... 32
Configure minimum database permissions for the Windows account or Microsoft SQL Server account ... 33
Using BlackBerry Mobile Fusion Studio with the Universal Device Service ... 33
8 Removing the Universal Device Service software ... 35
Remove the Universal Device Service software ... 35
9 Troubleshooting the Universal Device Service installation process ... 36
The JRE 6 Update 31 installation failed ... 36
10 Glossary ... 37
11 Legal notice ... 38

Related resources

1

To read the following guides or additional related material, visit www.blackberry.com/go/serverdocs.

Resource	Information
Universal Device Service Feature and Technical Overview	• Architecture diagram • Descriptions of features and components • Data flows
What's New in Universal Device Service 6.1 Job Aid	• Summary of new features, enhancements, and updates in Universal Device Service 6.1
Universal Device Service Release Notes	• Descriptions of known issues and potential workarounds
Universal Device Service Upgrade Guide	• System requirements • Upgrade instructions
Universal Device Service Administration Guide	• Instructions for creating user accounts, groups, and administrator accounts • Instructions for activating devices • Instructions for creating and assigning IT policies and profiles • Instructions for managing applications on devices

About the Universal Device Service

2

The Universal Device Service is designed to permit you to manage devices that run iOS or Android OS in your organization's environment.

If you activate devices using the Universal Device Service, you can use the Universal Device Service to:

- Manage devices using the IT policies and IT administration commands that the devices support
- Configure profiles for devices so that you can control the connections to your organization's environment (VPN profiles for iOS devices, Wi-Fi profiles, certificate profiles, and email profiles for iOS devices and Android devices; email profiles for Android devices require TouchDown and Universal Device Service 6.1 MR1 or later)
- Provision and manage work applications on devices
- View the device inventory for your organization

To provide a single interface for helpdesk administrators to manage all the devices in your organization's environment, you can connect BlackBerry Mobile Fusion Studio to the Universal Device Service.

You can purchase and download the Universal Device Service from www.blackberry.com/support/downloads.

Planning a Universal Device Service installation

3

You can install all Universal Device Service components on one computer, or you can install specific components on separate computers. You should consider any effect on system resources before you decide where to install the components.

You can install all components on one computer if you do not plan to activate many devices, if you determine that the computer can manage the volume of traffic for the Universal Device Service components, and if it is acceptable that the computer is located in the DMZ.

If you plan to install components on separate computers, you must install the Core Module first.

For more information about supported deployment options, see the *Universal Device Service Feature and Technical Overview*.

Installing the Universal Device Service with other software

You can install the Universal Device Service on the computer that hosts BlackBerry Mobile Fusion Studio.

The Universal Device Service is not supported if you install the software on a computer that hosts any of the following products:

- BlackBerry Device Service
- BlackBerry Enterprise Server
- BlackBerry Enterprise Server Express

Installing all Universal Device Service components on one computer

You can install all Universal Device Service components on one computer, and you can install the database server on the same computer or use an existing database server in your organization's environment (local or remote).

During the installation process, if you select the basic installation option, the setup application installs Microsoft SQL Server Express, creates the Management Database and automatically configures it. If you select the advanced installation option, you can choose to install Microsoft SQL Server Express or use an existing database server in your organization's environment.

Installing the Core Module

The Core Module connects to the Management Database, communicates with services in your organization's environment, and sends notifications to devices.

You can install the Core Module with the Communication Module and Console services, with the Console services, or by itself on a separate computer. If you plan a distributed deployment, you must install the Core Module first.

Installing the Communication Module

The Communication Module listens for connections from devices over the Internet. You can install the Communication Module with the Core Module and Console services or by itself on a separate computer. The computer that you install the Communication Module on must be accessible from the Internet (for example, a computer that is located in the DMZ).

Installing the Console services

You can install the Console services with the Core Module and Communication Module, with the Core Module, or by itself on a separate computer.

The Console services includes the following components:

Component	Description
Administration Console	A web application that permits you to manage the iOS devices and Android devices in your organization
Scheduler	Services that manage scheduled tasks for the Universal Device Service
BlackBerry Web Services	Web services that support communication with the BlackBerry Directory Sync Tool and BlackBerry Mobile Fusion Studio

Universal Device Service connection types and port numbers for all devices

The following connection types and port numbers allow communication between Universal Device Service components and incoming connections from iOS devices and Android devices.

Item	Communication protocol	Default port number	Connection
Administration Console	HTTPS	8443	Incoming connections from browsers
BlackBerry Web Services	HTTPS	8082	Incoming connections from the BlackBerry Directory Sync Tool and BlackBerry Mobile Fusion Studio
Communication Module	HTTPS	443	Incoming connections from devices that use the Internet or a work Wi-Fi network
Core Module	HTTPS	8081	Incoming connections from the Communication Module, Administration Console, Scheduler, and BlackBerry Web Services
Management Database	TCP	1433	Incoming connections to the database server that hosts the Management Database (if you configured the database server to use static ports)
BlackBerry Infrastructure	TCP	3101	Outgoing connections to the BlackBerry Infrastructure to validate the SRP information

Item	Communication protocol	Default port number	Connection
SMTP gateway	TCP	25	If you enable SMTP, outgoing connections to the SMTP gateway for email messages

Universal Device Service connection types and port numbers for iOS devices

The following connection types and port numbers allow communication between the Universal Device Service, Apple, and iOS devices. You cannot configure the port numbers that are used to communicate with APNs or the Apple Root Certification Authority.

Item	Communication protocol	Default port number	Connection
BlackBerry Infrastructure	HTTPS	443	Outgoing connections to the BlackBerry Infrastructure to request a signed CSR from Research In Motion when you configure the APNs certificate
Apple Push Notification service	TCP TCP	2195 5223	Outgoing connections from the Core Module to APNs Outgoing connections from iOS devices that use a work Wi-Fi network to APNs
Apple Root Certification Authority	HTTPS and HTTP	443 and 80	Outgoing connections to the Apple Root Certification Authority to check the certificate revocation list

Related information

System requirements: Firewall, 12

Requirements

4

System requirements: iOS devices and Android devices

The Universal Device Service is designed to offer support for iOS devices and Android devices. You can determine the compatibility of the mobile operating system with the Universal Device Service based on the device's operating system version. Features that the Universal Device Service supports may vary based on device hardware, operating system or API limitations imposed by OEM vendors, or other restrictions.

Item	Requirement
iOS devices	Any of the following mobile operating systems: • iOS 4.3 • iOS 5.0 • iOS 5.1 • iOS 6.0 (Universal Device Service 6.1 MR1 or later is required)
Android devices	Any of the following mobile operating systems: • Android OS 2.2 • Android OS 2.3.*x* • Android OS 3.*x*.*x* • Android OS 4.0.*x* • Android OS 4.1.*x* (Universal Device Service 6.1 MR1 or later is required)

System requirements: Firewall

For more information about the range of IP addresses for the BlackBerry Infrastructure, visit www.blackberry.com/go/kbhelp to read article KB03735.

Requirements to manage all devices

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)
Communication Module	• Port 443 is open to allow incoming HTTPS connections from iOS devices and Android devices that use the Internet or a work Wi-Fi network • The computer that hosts the Communication Module must have a publicly accessible DNS name
BlackBerry Infrastructure	• Port 3101 is open to allow outgoing TCP connections to the BlackBerry Infrastructure to validate the SRP information

Requirements to manage iOS devices

You cannot configure the port numbers that are used to communicate with APNs or the Apple Root Certification Authority. For more information about the range of IP addresses for APNs, visit developer.apple.com to read *IP Address Range Used by the Push Service*, in article TN2265.

Item	Requirement
BlackBerry Infrastructure	• Port 443 is open to allow outgoing HTTPS connections to the BlackBerry Infrastructure to request a signed CSR from Research In Motion when you configure the APNs certificate
Apple Push Notification service	• Port 2195 is open to allow outgoing TCP connections from the Core Module to APNs

Item	Requirement
	• Port 5223 is open to allow outgoing TCP connections from iOS devices that use a work Wi-Fi network to APNs
Apple Root Certification Authority	• Port 80 (HTTP) and port 443 (HTTPS) are open to allow outgoing connections to the Apple Root Certification Authority to check the certificate revocation list

Related information

Universal Device Service connection types and port numbers for all devices, 9
Universal Device Service connection types and port numbers for iOS devices, 10

System requirements: Your organization's environment

To add users from your organization's directory to the Universal Device Service, you can enable Microsoft Active Directory in the Administration Console.

Item	Requirement
Directory service	Microsoft Active Directory

Hardware requirements: Universal Device Service

You must consider the memory and disk space requirements for the Universal Device Service deployment option that you choose.

If you install the Universal 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 *Universal Device Service Performance Calculator*.

Hardware requirements: All Universal Device Service components on one computer

The following guidelines apply to the computer that you install the Universal Device Service and Universal Device Service components on, excluding the Management Database. If you install the Management Database on the computer that hosts the Universal Device Service, the disk space requirements for the Management Database are 4 MB of disk space plus 40 KB for each user.

Number of devices	Requirement
1 to 150	• One processor, 2.33 GHz Intel Xeon 5140 (Dual Core) • 4 GB of available memory • 1 GB of disk space plus 35 MB per hour
150 to 500	• One processor, 3 GHz Intel Xeon 5160 (Dual Core) • 4 GB of available memory • 1 GB of disk space plus 35 MB per hour
500 to 1000	• One processor, 1.86 GHz Intel Xeon E5320 (Quad Core) • 6 GB of available memory • 1 GB of disk space plus 35 MB per hour
1000 to 2000	• One processor, 2.66 GHz Intel Xeon X5560 (Quad Core) • 8 GB of available memory • 1 GB of disk space plus 35 MB per hour **Note:** If you install the Management Database on the computer that hosts the Universal Device Service, you should use one processor, 2.93 GHz Intel Xeon X5570 (Quad Core).

Hardware requirements: Management Database

The following guidelines apply to the computer that you install the Management Database on.

Number of devices	Requirement
1 to 150	• One processor, 1.6 GHz Intel Xeon 5110 (Dual Core) • 4 GB of available memory • 4 MB of disk space plus 40 KB for each user
150 to 500	• One processor, 1.86 GHz Intel Xeon 5128 (Dual Core) • 4 GB of available memory • 4 MB of disk space plus 40 KB for each user
500 to 1000	• One processor, 2.33 GHz Intel Xeon 5140 (Dual Core) • 4 GB of available memory • 4 MB of disk space plus 40 KB for each user
1000 to 2000	• One processor, 2.83 GHz Intel Xeon E5440 (Quad Core) • 4 GB of available memory • 4 MB of disk space plus 40 KB for each user

Hardware requirements: Universal Device Service distributed deployment

The following guidelines apply to a distributed deployment of the Universal Device Service with up to 10,000 devices.

Component	Requirement
Core Module	• One processor, 2.93 GHz Intel Xeon 5570 (Quad Core) • 4 GB of available memory • 200 MB of disk space plus 10 MB per hour
Communication Module	• One processor, 2 GHz Intel Xeon E5335 (Quad Core) • 4 GB of available memory • 200 MB of disk space plus 25 MB per hour
Console services	• One processor, 1.6 GHz Intel Xeon 5110 (Dual Core)

Component	Requirement
	• 4 GB of available memory • 600 MB of disk space plus 100 KB per hour
Management Database	• One processor, 1.86 GHz Intel Xeon L5609 (Quad Core) • 4 GB of available memory • 4 MB of disk space plus 40 KB for each user

Software requirements: Universal Device Service and components

The following requirements apply to the computer that you install the Universal Device Service on, or if you install remote Universal Device Service components, the computer that you install the Core Module on and the computer that you install the Communication Module on.

Item	Requirement
Operating system	Any of the following operating systems (localized operating systems are not supported): • Windows Server 2008 SP2 (64-bit) • Windows Server 2008 R2 • Windows Server 2008 R2 SP1 • Windows Small Business Server 2011 For Windows Server 2008 SP2, Microsoft hotfix 2379016 is installed
Software framework	• Microsoft .NET Framework 3.5 SP1 (for Windows Server 2008 SP2) • Microsoft .NET Framework 4.0 (for all operating systems)
Web server	Microsoft IIS 7.0 or 7.5

Software requirements: Database server

Item	Requirement
Database management system	Any of the following database management systems: • Microsoft SQL Server 2008 SP3 (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 SP3 (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)
Database connectivity	To support database connectivity for the Management Database, you must configure the following settings: • TCP/IP protocol is enabled • Named Pipes protocol is disabled

Software requirements: Browser

The following requirements apply to the browser that you use to log in to the Administration Console.

Item	Requirement
Browser	• Windows Internet Explorer 8.0 or 9.0 • Mozilla Firefox 10 or later • Google Chrome 12 or later • Safari 5 for Mac or later
Browser settings for Windows Internet Explorer	To support browser access, you must configure the following settings:

Item	Requirement
	• Support for JavaScript • Cookies turned on • Support for TLS or SSL (verify that TLS 1.2 is disabled) • The Administration Console website is assigned to the trusted websites security zone For Windows Internet Explorer 8, you must install the following Microsoft hotfixes: • Microsoft hotfix 2647516 (in some environments, the Administration Console does not display the user list if this hotfix is not installed) • Microsoft hotfix 2675157 (the Administration Console does not display the Available Settings pane if this hotfix is not installed) **Note:** If Windows Internet Explorer Enhanced Security Configuration is turned on, some areas of the Administration Console might not function correctly.
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

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.

Preinstallation tasks

5

Requesting an SSL certificate for the Communication Module

You must provide an SSL certificate when you install the Communication Module. You should use an SSL certificate that is issued by a certification authority that is already trusted by iOS devices and Android devices. If you choose to use an SSL certificate that is not trusted by iOS devices by default, you must provide the certification authority certificate to the user to install as a trusted root certificate before the user can activate any iOS devices. If you choose to use an SSL certificate that is not trusted by Android devices by default, the user receives a warning that the certificate for the server is not trusted when the user activates any Android devices. The user has the option to continue with activation or return to the Mobile Fusion Client home screen. The Universal Device Service does not support self-signed certificates.

For more information about the certificates that are trusted by iOS devices, visit support.apple.com to read article HT4415 for iOS 4 or article HT5012 for iOS 5.

For more information about the certificates that are trusted by Android devices, check the “Trusted CA” section of the Android device.

Create a CSR

You must perform the following actions on the computer that hosts Microsoft IIS.

1. Open Internet Information Services (IIS) Manager.
2. Click the server name.
3. Double-click **Server Certificates**.
4. Click **Create Certificate Request**.
5. Specify the required information for the certificate. Click **Next**.

   In the **Common name** field, you must specify the publicly accessible DNS name of the computer that you install the Communication Module on (for example, domain.example.com). The common name can contain the wildcard character that is denoted by an asterisk (*), but the Universal Device Service supports SSL certificates that match only a single level of subdomain as defined in the RFC 2818 standard. For example, *.example.com matches domain.example.com but not mdm.domain.example.com.

6. Select **Microsoft RSA SChannel Cryptographic Provider** and the bit length. Click **Next**.

7. Specify a location and file name for the CSR. Click **Finish**.

Submit the CSR to a certification authority

The CSR that you create must be signed with the SHA-2 algorithm by a certification authority.

1. Submit the CSR to an external certification authority or your organization's certification authority. Contact the certification authority for details and follow the instructions.
2. Save the signed certificate that you receive from the certification authority.

After you finish: Copy the signed certificate to the computer that hosts Microsoft IIS.

Complete the CSR

You must perform the following actions on the computer that hosts Microsoft IIS.

1. Open Internet Information Services (IIS) Manager.
2. Click the server name.
3. Double-click **Server Certificates**.
4. Click **Complete Certificate Request**.
5. Specify the location of the signed certificate and in the **Friendly name** field, type a display name.
6. Click **OK**.
7. Double-click the certificate that you installed.
8. In the **Certificate** window, on the **Details** tab, click **Copy to File**.
9. In the **Certificate Export Wizard**, click **Next**.
10. Select **Yes, export the private key**. Click **Next**.
11. Select **Personal Information Exchange - PKCS # 12 (.PFX)**. Click **Next**.
12. Type and confirm a password. Click **Next**.
13. Specify a location and file name for the SSL certificate. Click **Next**.
14. Click **Finish**.

After you finish: Copy the .pfx file for the SSL certificate to the computer that you install the Communication Module on.

Remove the WebDAV Publishing role service

If Microsoft IIS is already installed on the computer that you install the Universal Device Service on, you must remove the WebDAV Publishing role service.

1. On the taskbar, click **Start** > **Administrative Tools** > **Server Manager**.
2. In the left pane, click **Roles**.
3. In the **Web Server (IIS)** section, click **Remove Role Services**.
4. Clear the **WebDAV Publishing** check box.
5. Apply your changes.

Installing the Universal Device Service on Windows Small Business Server

If you install the Universal Device Service on Windows Small Business Server, you must perform the following actions:

- Configure a custom port for the Communication Module. The default port number for the Communication Module is reserved by Windows Small Business Server. For more information, see System requirements: Firewall.
- If you plan to use the advanced installation option, configure database connectivity. For more information, see Software requirements: Database server.
- Update the 8.3 naming convention settings.

Update the 8.3 naming convention settings

To support the 8.3 version of long file names, you can specify whether NTFS generates a short file name that follows the 8.3 naming convention (for example, a maximum of eight characters for the file name, a period (.), and a maximum of three characters for the extension). By default, 8.3 name creation is disabled on Windows Small Business Server. You must update the 8.3 naming convention settings to avoid potential issues with long file names during the Universal Device Service installation process.

1. On the taskbar, click **Start** > **Run**.
2. Type **regedit**.
3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\File System.
4. Change **NtfsDisable8dot3NameCreation** to **2**.
5. Click **OK**.
6. Restart Windows Small Business Server.

Configuring connections for the Management Database

The database for the Universal Device Service is the Management Database. You create the Management Database when you install the Core Module or when you run the CreateDB executable.

The Core Module can connect to the Management Database on the database server using Windows authentication or Microsoft SQL Server authentication. By default, the Core Module logs in to the Management Database using the Windows account that you use to complete the installation process or the Microsoft SQL Server account that you specify during the installation process.

Specifying database permissions to create the Management Database

Depending on the database option and the type of authentication that you select, you might need to assign database creator permissions to the Windows account that you use to complete the installation process or the Microsoft SQL Server account that you specify during the installation process. You can configure database permissions using Microsoft SQL Server roles.

Database option	Database permission
Install Microsoft SQL Server Express during the Universal Device Service installation process	• If you choose Windows authentication, the setup application automatically assigns the required database permissions to the Windows account. • If you choose Microsoft SQL Server authentication, you must add the Microsoft SQL Server account to the dbcreator server role.
Use an existing Microsoft SQL Server in your organization's environment	• You must add the Windows account or Microsoft SQL Server account to the dbcreator server role.

Create a Management 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 create the Management Database instead of using the setup application. After you create the Management 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 create the Management Database, you must log in to the computer using a Windows account that has database creator permissions.
2. Copy the Universal Device Service installation files to the database server that you want to configure as the host server for the Management Database.
3. Extract the contents to a folder on the computer.
4. Navigate to <*extracted_folder*>\Database.
5. Open the **UDSMgmt.cfg** file in a text editor.
6. Change the file to include information that is specific to your organization's environment.
7. Save and close the file.
8. Open a command prompt window.
9. Change the directory to <*extracted_folder*>\Database.
10. Type **CreateDB.exe UDSMgmt.cfg**.

UDSMgmt.cfg properties

Property	Description
DATABASE_NAME	This property specifies the name of the Management Database.
CMD	This property specifies the type of action that the CreateDB executable must complete (for example, install or upgrade the Management Database).
SERVER	This property specifies the name of the database server that hosts the Management Database. If a database instance hosts the Management 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.

Property	Description
SCRIPT_ROOT	This property specifies the path to the DBInstallScripts folder.
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.
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.

Applications that are installed with the Universal Device Service

You can use the Universal Device Service installation process to install third-party applications.

Application	Universal Device Service components that the application is installed with
JRE 6 Update 31	• Console services
Microsoft IIS 7.0 or 7.5	• Core Module • Communication Module
Microsoft Web Deploy 2.0	• Core Module • Communication Module
Microsoft SQL Server 2008 R2 Express (if it is selected during the installation process)	• Core Module

Application	Universal Device Service components that the application is installed with
Microsoft .NET Framework 3.5 SP1 (if you select Microsoft SQL Server 2008 R2 Express and the operating system is Windows Server 2008 R2)	• Core Module

Installing the Universal Device Service software

6

Prerequisites: Installing the Universal Device Service software

Verify that you have the following information available for the Universal Device Service software:

- Universal Device Service CAL key
- SRP host
- SRP identifier
- SRP authentication key

On the computer that you install the Universal Device Service on, verify the following items for the Windows account that you use to install the Universal Device Service:

- Verify that the account is assigned local administrator permissions and the permission "Log on as a batch job".
- Verify that the password for the account does not contain spaces.

Install the Universal Device Service software

1. Log in to the computer that you want to install the Universal Device Service on using the Windows account that has correct permissions on the computer.
2. In the BlackBerry Mobile Fusion installation files, double-click **Autorun.exe**. If a message appears and requests permission for the Autorun.exe to make changes to the computer, click **Yes**.
3. On the BlackBerry Mobile Fusion installation screen, click **Install** for the Universal Device Service software.
4. In the **License agreement** dialog box, perform the following actions:

a. In the **Customer information** section, specify information for your organization and select your country or region.

b. In the **License agreement** section, read the license agreement. To accept the license agreement, select **I accept the terms of the license agreement**.

c. Click **Next**.

5. In the **Installation options** dialog box, perform one of the following actions:
   - If you want to install all Universal Device Service components and the database server on the computer, select the **Basic installation** option. Click **Next** and go to step 8.
   - If you want to select the Universal Device Service components to install on the computer or use an existing database server in your organization's environment, select the **Advanced installation** option. Click **Next**.
6. In the **Setup type** dialog box, perform the following actions:

   a. Select **Create a Management Database**.

   b. If you do not have a database server in your organization's environment, select **Install and use Microsoft SQL Server 2008 R2 Express Edition on this computer**. Otherwise, select **Use an existing Microsoft SQL Server in your organization's environment**.

   c. Click **Next**.
7. In the **Setup options** dialog box, select the Universal Device Service components that you want to install. Click **Next**.
8. In the **Universal Device Service CAL and SRP information** dialog box, perform the following actions:

   a. In the **CAL key** field, type the Universal Device Service CAL key.

   b. In the **SRP authentication information** section, type the SRP identifier and SRP authentication key.

   c. In the **SRP host** and **SRP authentication information** sections, click **Verify** to verify that the information is correct.

   d. Click **Next**.
9. In the **Preinstallation checklist** dialog box, read and verify the information. Click **Next**.
10. 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 Windows account that you used in step 1.

    b. Click **Next**.
11. In the **Summary** dialog box, verify that the information is correct. Click **Install**.
12. In the **Installation** dialog box, when the installation status is complete for the Universal Device Service and any third-party applications, click **Next**.
13. If you chose the basic installation option, in the **Database information** dialog box, when the setup application finishes creating the Management Database, click **Next** and go to step 15.
14. If you chose the advanced installation option, in the **Database information** dialog box, perform the following actions:

a. In the **Microsoft® SQL Server® name** field, type the name of the computer that hosts the database server.

b. In the **Database name** field, type a name for the Management Database.

c. If you configured the database server to use static ports, select the **Static** option. If the static port number is not port 1433, in the **Port** field, type the port number.

d. By default, the setup application uses Windows authentication to connect to the Management Database. If you select SQL authentication, specify login information for the Microsoft SQL Server account that has correct permissions on the database server.

e. Click **Next**.

15. In the **Core Module information** dialog box, perform the following actions:

a. In the **Name** field, specify the FQDN of the computer that you install the Core Module on or the DNS name (if you created a DNS record for the computer that hosts the Core Module). You cannot specify an IP address.

b. Type and confirm a password for the Core Module. The components in the Universal Device Service domain use this password to connect to the Core Module and you must specify this password when you install remote components.

c. In the **Website information** section, in the drop-down list, click **Create a website**. If necessary, in the **Website port** field, change the default port number.

d. Click **Next**.

16. If you chose the basic installation option, or if you chose the advanced installation option and chose to install the Communication Module, in the **Communication Module information** dialog box, perform the following actions:

a. In the **Communication Module** section, specify the publicly accessible DNS name of the computer that you install the Communication Module on. The name that you specify for the Communication Module must be accessible over the Internet and you cannot specify an IP address.

b. In the **Website information** section, in the drop-down list, click **Create a website**. If necessary, in the **Website port** field, change the default port number.

c. In the **SSL certificate** section, specify the location and password for the SSL certificate that you obtained from a certification authority (the signed certificate that you exported to a .pfx file).

d. Click **Next**.

17. If you chose the basic installation option, or if you chose the advanced installation option and chose to install the Console services, in the **Administration settings** dialog box, perform the following actions:

a. In the **Port settings** section, if necessary, change the default port number for the Administration Console and BlackBerry Web Services.

b. In the **Keystore settings** section, type and confirm a password to encrypt the keystore files for the Administration Console and BlackBerry Web Services.

c. In the **Administrator account settings** section, type and confirm a password for the administrator account. You use the login information that you specify to log in to the Administration Console for the first time.

18. In the **Finalize installation** dialog box, the setup application finishes installation tasks. If you chose to install the Console services, the Universal Device Service services start automatically. Click **Next**.
19. In the **Console addresses** dialog box, click **Finish**. If you chose to install the Console services, the setup application exports the Administration Console web address to a .txt file. If you chose the advanced installation option, the setup application also exports the Core Module URL to the same .txt file.

Install the Communication Module in the DMZ

Before you begin: Install the Core Module in your organization's environment and copy the Core Module URL from the .txt file that you export after the installation process completes.

1. Log in to the computer that you want to install the Communication Module on using the Windows account that has correct permissions on the computer.
2. In the BlackBerry Mobile Fusion installation files, double-click **Autorun.exe**. If a 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 Universal Device Service software.
4. In the **License agreement** dialog box, perform the following actions:
   a. In the **Customer information** section, specify information for your organization and select your country or region.
   b. In the **License agreement** section, read the license agreement. To accept the license agreement, select **I accept the terms of the license agreement**.
   c. Click **Next**.
5. In the **Installation options** dialog box, select the **Advanced installation** option. Click **Next**.
6. In the **Setup type** dialog box, perform the following actions:
   a. Select **Use an existing Management Database** .
   b. Select **You already have a Core Module connected to the database**.
   c. Specify the Core Module URL that you copied.
   d. Type the password that you specified when you installed the Core Module.
   e. Click **Next**.
7. In the **Setup options** dialog box, select only the Communication Module. 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 Windows 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. In the **Installation** dialog box, when the installation status is complete for the Universal Device Service and any third-party applications, click **Next**.
12. In the **Communication Module information** dialog box, perform the following actions:

    a. In the **Communication Module** section, specify the publicly accessible DNS name of the computer that you install the Communication Module on. The name that you specify for the Communication Module must be accessible over the Internet and you cannot specify an IP address.

    b. In the **Website information** section, in the drop-down list, click **Create a website**. If necessary, in the **Website port** field, change the default port number.

    c. In the **SSL certificate** section, specify the location and password for the SSL certificate that you obtained from a certification authority (the signed certificate that you exported to a .pfx file).

    d. Click **Next**.

13. In the **Finalize installation** dialog box, the setup application finishes installation tasks. Click **Next**.
14. In the **Console addresses** dialog box, click **Finish**. If you already installed the Console services, the setup application exports the Administration Console web address to a .txt file.

Postinstallation tasks

7

Test the Universal Device Service installation

1. On the computer that hosts the Console services, in Windows Services, verify that the services for the Universal Device Service are running.
2. In the Windows Event Viewer and log files that are located in <*drive*>:\Program Files (x86)\Research In Motion \Universal Device Service\Logs, check for error messages.
3. In Microsoft IIS, check that the websites for the Core Module and Communication Module are started.
4. In the Administration Console, add a test user account.
   If you can add a test user account, the connection from the Core Module to the Management Database is open.

After you finish: For troubleshooting information, visit www.blackberry.com/support.

Best practice: Running the Universal Device Service

Best practice	Description
Do not change the startup type for the Universal Device Service services.	When you install or upgrade the Universal Device Service, the setup application configures the startup type for the Universal Device Service services as either automatic or manual. To avoid errors in the Universal Device Service, do not change the startup type for the Universal Device Service services.
Do not change the account information for the Universal Device Service services.	When you install or upgrade the Universal Device Service, the setup application configures the account information for the Universal Device Service services.

Best practice	Description
	Do not change the account information for the Universal Device Service unless the Universal Device Service documentation specifies that you can.

Log in to the Administration Console

To open the Administration Console, you can use a browser on any computer that has access to the computer that hosts the Administration Console. When you install the Universal Device Service, you specify the login information that you use to log in to the Administration Console for the first time.

1. In the browser, type **https://*<server_name>*:*<port>*** , where *<server_name>* is the fully qualified domain name of the computer that hosts the Administration Console. The default port for the Administration Console is port 8443.
2. In the **User name** field, type your username.
3. In the **Password** field, type your password.
4. Click **Log in**.

Configuring database permissions using Microsoft SQL Server roles

The Universal Device Service setup application requires the Windows 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 Management Database. After the installation or upgrade process completes, you can change the database permissions for the Windows account or Microsoft SQL Server account to the minimum permission that the Universal Device Service requires to run.

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

Database role	Description
db_owner	The setup application requires this role to upgrade the Management Database. This role is the default permission in Microsoft SQL Server for running the Universal Device Service.

Database role	Description
rim_db_uds_server	The setup application or the CreateDB executable creates the role automatically when it creates the Management Database. This role is the minimum permission in Microsoft SQL Server for running the Universal Device Service.

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

You can configure minimum database permissions for the Windows account or Microsoft SQL Server account that the Universal Device Service uses to connect to the Management Database.

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

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

Using BlackBerry Mobile Fusion Studio with the Universal Device Service

BlackBerry Mobile Fusion Studio is a web application that administrators who are assigned to either the Senior Helpdesk role or Junior Helpdesk role can use. BlackBerry Mobile Fusion Studio is a single administrative interface that allows you to perform common administrative tasks for BlackBerry smartphones, BlackBerry PlayBook tablets, iOS devices, and Android devices. The following Universal Device Service settings must be configured before you can use the BlackBerry Mobile Fusion Studio:

- Microsoft Active Directory settings
- SMTP settings

You must also edit the template for the activation email message.

For more information about configuring these settings, see *Universal Device Service Administration Guide*.

Removing the Universal Device Service software

8

Remove the Universal Device Service software

1. On the taskbar, click **Start** > **Control Panel**.
2. Click **Uninstall a program**.
3. Click **Universal Device Service**.
4. Click **Uninstall**.

After you finish: You can remove third-party software that the setup application installed during the Universal Device Service installation process (for example, you can remove the JRE software from the computer).

Related information

Applications that are installed with the Universal Device Service, 24

Troubleshooting the Universal Device Service installation process

9

The JRE 6 Update 31 installation failed

This message appears when the Universal Device Service setup application cannot complete the JRE software installation process.

Possible solution

If McAfee VirusScan Enterprise 8.8 is installed on the computer, verify that Patch 1 is installed.

1. Open the VirusScan Enterprise console.
2. Click **Help** > **About McAfee VirusScan Enterprise**.
3. If **Installed Patches** is not **1**, check for software updates from McAfee and install the patch.
4. Restart the setup application.

Possible solution

Install JRE 6 Update 31 manually.

1. Download JRE 6 Update 31 from www.java.com.
2. Open a command prompt window.
3. Type ***<path to file>\<filename>*** **STATIC=1**.
4. Close the command prompt window.
5. Restart the setup application.

Note: You must have an Internet connection available during the JRE software installation process.

Glossary

10

APNs	Apple Push Notification service
CAL	Client Access License
CSR	certificate signing request
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
FQDN	fully qualified domain name
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IIS	Internet Information Services
IP address	An Internet Protocol (IP) address is an identification number that each computer or mobile device uses when it sends or receives information over a network, such as the Internet. This identification number identifies the specific computer or mobile device on the network.
JRE	Java Runtime Environment
NTFS	New Technology File System
OEM	original equipment manufacturer
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SRP	Server Routing Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VPN	virtual private network
WebDAV	Web Distributed Authoring and Versioning

Legal notice

11

©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.

Apple, Mac, and Safari are trademarks of Apple Inc. Android and Google Chrome are trademarks of Google Inc. Intel and Xeon are trademarks of Intel Corporation. McAfee and VirusScan are trademarks of McAfee, Inc. Microsoft, ActiveSync, Active Directory, Internet Explorer, SQL Server, Windows, and Windows Server are trademarks of Microsoft Corporation. Mozilla and Firefox are trademarks of Mozilla Foundation. TouchDown is a trademark of NitroDesk Inc. 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