Universal Device Service

Version: 6.2

Release Notes

BlackBerry®

Published: 2012-11-27
SWD-20121127151039072

Contents

1 Related resources 4

2 Fixed issues 5

- Administration fixed issues 5
- Documentation fixed issues 6
- Installation fixed issues 6
- Mobile Fusion Client fixed issues 7
- Profiles fixed issues 7

3 Known issues 9

- Administration known issues 9
- APNs certificate known issues 9
- Documentation known issues 10
- Installation known issues 10
- Logging known issues 13
- Mobile Fusion Client known issues 13
- Profiles known issues 13

4 Legal notice 15

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 6.2 Quick Reference	• Summary of new features, enhancements, and updates in Universal Device Service 6.2
Universal Device Service Installation and Configuration Guide	• System requirements • Installation instructions
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

Fixed issues

2

Administration fixed issues

The Limit time to sync email option was not supported for Microsoft ActiveSync profiles on Android devices. (DT 5907374)
When you added an application definition to a software configuration and assigned it to users, the Application definitions pane on the Library page displayed "0 users" for the application definition. (DT 5881719)
Some iPad devices did not receive updates to assigned work apps, even though the work apps appeared to be installed on the device. (DT 5870855)
Records were not cleared from the database periodically and that allowed the dabatabse to grow to a large size. (DT 5819396)
If you saw an "unhandled exception" error in the Core Module log file, the Core Module could not connect to the Management Database. (DT 5502640)
When you reactivated a device that was already compliant based on the device compliance settings that you configured and the device was still assigned to the same user, the user received an email message about a compliance issue. (DT 5373808)
Senior helpdesk administrators could not assign a certification authority certificate profile or shared certificate profile to a group. (DT 5330055)
The "Disable device backup" IT policy rule was available but was not supported. (DT 5325294)
You must have at least one CAL key for the Universal Device Service. If you tried to delete the last CAL key, the Administration Console did not display a clear error message. (DT 5135115)
Activation emails were not sent if the SMTP configuration used SSL/TLS with a custom port and you specified the IP address of the SMTP server. (DT 5046330)

If you accessed the Administration Console using Windows Internet Explorer 9, some fields were not available on Settings pages. (DT 4387719)

Unicode characters did not appear correctly in the Edit Application Source fields in the Administration Console of the Universal Device Service. (DT 3278388)

Documentation fixed issues

The *Universal Device Service Installation and Configuration Guide* was missing a requirement for the Communication Module. (DT 5329901)

The steps to update device ownership in the device report were not documented. (DT 3818226)

When you deactivate an iOS device, the Work Apps icon changes to a blank icon and remains on the device. The steps to remove the blank icon were not documented. (DT 3688753)

Installation fixed issues

If you used a custom installation folder for the Communication Module in a distributed deployment, the certification authority certificate for the Communication Module and Core Module did not match in Microsoft IIS. (DT 5032723)

In a distributed deployment, if you removed the Universal Device Service components and then reinstalled the components, the CA certificate for the Communication Module and Core Module did not match in Microsoft IIS and you could not activate an iOS device. (DT 3427327)

When you reinstalled or upgraded the Universal Device Service, you had to type the CAL key in the Universal Device Service CAL and SRP information dialog box. (DT 3218781)

Mobile Fusion Client fixed issues

The Mobile Fusion Client turned on the Wi-Fi connection on certain Android devices even when the user had turned it off. (DT 6249460)

If you applied a Compliance profile to a user and the user updated the Mobile Fusion Client on an Android device, the log files recorded unnecessary exception errors. (DT 6224075)

When you assigned a software configuration to iOS devices and the application definition included an application source that was missing "http://" from the application web address, the Mobile Fusion Client stopped responding when users selected that application from the Work Apps tab. (DT 5137370)

When you assigned a shared or user certificate profile and a CA certificate profile to a user with an iOS device and an Android device, if you assigned a Wi-Fi profile with the TLS protocol that used both certificate profiles for authentication, the shared or user certificate profile was displayed twice in the Mobile Fusion Client on the device. (DT 4465152)

When you assigned a defined SCEP profile or an external SCEP profile, the Mobile Fusion Client did not display the SCEP profile on the Profiles tab, but the SCEP profile was displayed in the device settings. (DT 4251590)

When you removed the Mobile Fusion Client from a device, the Universal Device Service continued to send email messages to the device. (DT 3218777)

Profiles fixed issues

When you deleted a group that included certificate profiles, the certificate profiles were removed from the Mobile Fusion Client but were still installed on the device. (DT 5444698)

If you assigned multiple profiles to Android devices or iOS devices (for example, Wi-Fi profile, VPN profile, Microsoft ActiveSync profile, CA certificate profile, shared certificate profile, and SCEP profile), only certificate profiles were displayed in the Mobile Fusion Client after you upgraded the Universal Device Service and users updated the Mobile Fusion Client. (DT 5339506)

When you created a VPN profile and selected IPsec, AnyConnect, Juniper, F5, or Custom as the VPN profile type, if you selected the Enable VPN on demand option, the fields were not labeled correctly. (DT 4386318)

After you assigned a Microsoft ActiveSync profile and activated an iOS device, if you disabled activations for the user, the Microsoft ActiveSync profile was reset and the user did not receive email until they typed the password again. (DT 4292662)

3

Known issues

Administration known issues

When you create a software configuration with an application definition that includes a .ipa file as the application source and assign the software configuration to an iOS device that was activated prior to upgrading the Universal Device Service, the Work Apps icon is not available on the device. (DT 6381810, 4923704)

Workaround: If you want to deploy internally hosted apps (.ipa files), users must activate their iOS devices again.

The error message that the Universal Device Service displays when you try to add a temporary CAL key when a permanent CAL key exists is not descriptive. The error message should state that you cannot add a temporary CAL key if a permanent CAL key exists. (DT 5923963)

After you upgrade the Universal Device Service and users update the Mobile Fusion Client for Android OS, users must reactivate their devices, or wait for 15 minutes before the device can be managed in the Universal Device Service. (DT 5363555)

If you try to add an invalid file type when you create a certification authority certificate profile or shared certificate profile, you return to the Administration Console instead of the certificate profile window. (DT 3866435)

APNs certificate known issues

If you renew an APNs certificate and install it in the Microsoft Management Console without deleting the old certificate, device notifications will fail. (DT 3428471)

Workaround: Delete the old certificate from the Microsoft Management Console before or after installing the renewed certificate. The two certificates will look the same, so check the expiration date on the certificates and delete the older one.

Documentation known issues

If you have a Cisco VPN environment and configure an IPsec VPN profile with XAuth-PSK authentication, some third-party devices may be unable to store the static XAuth passwords. The user is required to enter the XAuth password each time they enable VPN. The steps to allow affected third-party devices to store the XAuth password are not documented in the Universal Device Service documentation.

Workaround: To allow affected third-party devices to store the XAuth password, you can modify the group-policy attributes of the VPN profile in your Cisco VPN system to include the password-storage enable option. For more information, visit www.blackberry.com/go/kbhelp to read KB30353.

The steps to use a Microsoft ActiveSync profile with IBM Lotus Domino are not documented. (DT 3338300)

Workaround: Use the %DisplayName% variable in the ActiveSync settings to allow IBM Lotus Notes users to log in to IBM Lotus Notes Traveler, which allows ActiveSync to access IBM Lotus Domino. Use Microsoft Active Directory to add the user to the directory. Create one IBM Lotus Notes Traveler profile for all Lotus Notes users that uses the %DisplayName% variable to allow the user to access the IBM Lotus Notes Traveler server.

Installation known issues

You cannot install the Universal Device Service on localized Windows operating systems.

If you edit the port binding for the Core Module and change it from all unassigned to a specific IP address, you cannot complete an upgrade of the Universal Device Service. (DT 6352704)

Workaround: Change the port binding back to all unassigned and then retry the upgrade.

If an error occurs and the installation process does not complete, the setup application does not copy the files required to remove the Universal Device Service software and you cannot remove the software. (DT 6069757)

Workaround: Perform the following actions to remove the Universal Device Service software:

1. In the Universal Device Service installation files, navigate to the CDLayout folder and copy the Languages.ini file and Setup.exe file.
2. Navigate to <*drive*>:\Program Files (x86)\Research In Motion\Common Files\Setup and paste the files that you copied.
3. Rename Setup.exe to Uninstaller.exe.

4. Open a command prompt window (run as administrator if necessary) and change the directory to <*drive*>:\Program Files (x86)\Research In Motion\Common Files\Setup.
5. Type **Uninstaller.exe -u UDS**.

When you upgrade the Universal Device Service, the setup application installs the JRE software that is included with the Universal Device Service software and replaces the existing JRE software on the computer, which might be a later version. (DT 6038097)

Workaround: Manually update the JRE software to the latest version.

If you installed the Core Module and Communication Module on separate computers and then you change the Core Module password on each computer using a different Windows account than the account that you used to install the Universal Device Service software, the Universal Device Service does not function correctly. (DT 5947033)

Workaround: Log in to each computer using the Windows account that you used to install the Universal Device Service software, change the Core Module password, and restart all Universal Device Service services.

If you change the port number for the Administration Console when you run the setup application again, you cannot access the Administration Console after the installation process is complete. (DT 5945034)

Workaround: Perform the following actions:

1. Navigate to <*drive*>:\Program Files (x86)\Research In Motion\Universal Device Service\RIM.BUDS.Gui\webapps\ROOT\WEB-INF\classes.
2. In the **config.properties** file, change the **mdm.httpsPort** value to the new port number for the Administration Console.
3. In Windows Services, restart the BlackBerry Administration Console service.

If you restore a backup of the Management Database to a different database server, when you run the setup application on the computer that hosts the Core Module and change the database location, the setup application cannot complete the installation process. (DT 5913978)

Workaround: On the computer that hosts the Core Module, update the location of the database server in the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Research In Motion\Universal Device Service\Setup\Components\DB\ DatabaseServerMachineName.

When you install the Universal Device Service using an existing Management Database from a previous Universal Device Service installation and you install the Console services on a different computer than the previous installation, the Universal Device Service services do not start. (DT 5258563)

Workaround: In Windows Services, start the Universal Device Service services manually.

When you upgrade the Universal Device Service, you cannot change the location of the installation folder even though the setup application allows you to. If you change the installation folder, the upgrade does not complete. (DT 5159223)

On the Installation dialog box, the installation status displays "Complete" for the Universal Device Service components but files are still being copied. (DT 5150525)

The setup application does not allow you to change the ports for the Core Module and the Communication Module when you run the setup application again. (DT 5135101)

When you install the Universal Device Service using an existing Management Database from a previous Universal Device Service installation and you do not specify the correct password for the Core Module, the installation process does not complete. (DT 4416299)

Workaround: Run the setup application again and specify the correct password for the Core Module.

If the password for the Windows account that you use to run the setup application contains spaces, the installation process does not complete. (DT 3673904).

Workaround: Run the setup application using a Windows account with a password that does not contain spaces.

If you install the Universal Device Service on Windows Server 2003 SP2 64-bit or Windows Server 2003 R2 SP2 64-bit, which are unsupported environments, no error message appears and the installation proceeds. (DT 3368096)

After the Universal Device Service is uninstalled, an empty BlackBerry Mobile Fusion folder remains in the Start > All Programs menu. (DT 3367277)

After a reinstallation of the same software bundle, if an administrator creates a custom logs folder, the setup logs and Administration Console logs do not go to the custom logs folder. Instead they are sent to the original default logs folder. (DT 3356497)

If the Windows Installer is in use by another process when you begin installing the Universal Device Service, you do not receive a warning message and the installation does not complete successfully. (DT 3228352)

If you install the Core Module and the Communication Module on a standalone computer, the Finalize Installation dialog box incorrectly lists components that have not been selected for installation. (DT 3202223)

During the installation process, the JRE update installation might fail. (DT 3194315)

Workaround: Install JRE 6 Update 31 manually using the command **jre-6u31-windows-i586.exe /s STATIC=1 or jre-6u31-windows-i586.exe STATIC=1**. Do not use the **/L** switch.

When you change the password for the keystore files using the Universal Device Service Configuration tool and click OK, the Keystore settings tab is blank and the password is not saved. (DT 3189071)

Workaround: Click Apply and then click OK.

The setup application requests login information for the Windows account that you use to install the Universal Device Service components, but the login information is used only if you select Windows authentication to connect to the Management Database. (DT 3164849)

Logging known issues

The logs for the Core Module and Communication Module are moved out of the date folder and into the corresponding component folder, leaving the date folder empty. This usually occurs at 24:00 h when new folders are created. Administrators may not find the log files where they are expected to be. (DT 3238650)

Mobile Fusion Client known issues

In certain circumstances, if a device is deactivated and then activated on a different server, the previous compliance and server name information is displayed in the Mobile Fusion Client. (DT 6278899)

Workaround: Close the Mobile Fusion Client and open it again.

After you upgrade the Universal Device Service and users update the Mobile Fusion Client for Android OS, users must reactivate their Android devices. (DT 5363555)

Application sources that are .ipa files (applications that are internally hosted by your organization) can be assigned only to devices running iOS 5 or later. When you add an application source with a .ipa file, you should select iOS 5.x values for the Platform, otherwise devices running iOS 4.x receive notifications in the Mobile Fusion Client about changes to internally hosted apps. (DT 3836790)

Profiles known issues

On some Android devices, the Microsoft ActiveSync profile that is pushed to the device from the Universal Device Service is not displayed in the list of accounts in Settings > Accounts. (DT 6248124)

In certain circumstances, the Universal Device Service cannot send a Wi-Fi profile to iOS devices. (DT 5925743)

If you create a Microsoft ActiveSync profile or VPN profile that uses variable injection with a defined SCEP profile or an external SCEP profile, you cannot assign the SCEP profile to a group. (DT 5478087)

Workaround: Assign the SCEP profile directly to each user in the group.
All certificates linked by Wi-Fi profile must be assigned directly to Android users or they will not be pushed to the device. (DT 3373692)
When you create a Wi-Fi profile and select Enterprise as the security type, you must type a value in the User name for authentication of the network field, or devices will not be able to install the profile. (DT 2598824)

4

Legal notice

©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, iPad, and iPhone are trademarks of Apple Inc. Cisco and AnyConnect are trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. F5 is a trademark of F5 Networks, Inc. Android is a trademark of Google Inc. IBM, Domino, Lotus, and Lotus Notes are trademarks of International Business Machines Corporation. Juniper is a trademark of Juniper Networks, Inc. Microsoft, ActiveSync, Active Directory, Internet Explorer, Windows, and Windows Server are trademarks of Microsoft Corporation. JRE is a trademark of Oracle and/or its affiliates. Samsung, Galaxy, Samsung Galaxy, and Samsung Galaxy Tab are trademarks of Samsung Electronics Co., Ltd. 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