Universal Device Service

Feature and Technical Overview

Version: 6.0

BlackBerry®

Published: 2012-03-22
SWD-20120322133506407

Contents

1 About the Universal Device Service 4
2 Features 5
3 Architecture 7
Architecture: Universal Device Service installed on one computer 7
Architecture: Universal Device Service with the Communication Module installed in the DMZ 8
Architecture: Universal Device Service installed in a distributed environment 9
4 Data flows 11
Data flow: Activating an iOS device over the wireless network 11
Data flow: Activating an Android device over the wireless network 11
5 Related resources 13
6 Glossary 14
7 Legal notice 15

About the Universal Device Service

1

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 (Wi-Fi profiles and certificate profiles for iOS devices and Android devices, VPN profiles and email profiles for iOS devices)
- 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.

Features

2

Feature	Description
Certificate-based authentication	You can use the Universal Device Service to roll out certificates to devices using certificate profiles or SCEP profiles. The Universal Device Service helps to restrict access to Microsoft ActiveSync, Wi-Fi connections, or VPN connections to devices using certificate-based authentication. Also, this feature helps you to control Microsoft ActiveSync, Wi-Fi connections, or VPN connections on devices because the Universal Device Service can automatically remove profiles and certificates when a device violates one of the predefined compliance policies, for example, compliance policies for jailbroken devices or rooted devices. Certificate-based authentication does not require a proxy server between the device and your organization's messaging server.
Activation and management of devices	To activate a device, you send an email message to the device that contains information about downloading the Mobile Fusion Client. You can manage multiple devices for each user account and view the device inventory for your organization in the Mobile Fusion Client. You can perform the following actions if they are supported by the device: • Activate, lock, and delete information from a device • Reset the device password • Apply profiles and IT policies to a device • Install certificates and configure SCEP on a device
Mobile Fusion Client	The Mobile Fusion Client permits the device to communicate with the Universal Device Service and perform the following actions: • Retrieve device information • Manage device settings • Display messages
Groups	Groups permit you to share roles, IT policies, and other configuration settings among similar user accounts. You can assign a user account to a group so that the user account inherits the properties of the group. You can install and configure the BlackBerry Directory Sync Tool to add user accounts to a group or remove user accounts from a group. For more information about the BlackBerry Directory Sync Tool, see the *BlackBerry Enterprise Server Resource Kit Administration Guide*.
IT policies	An IT policy is a set of IT policy rules that permit you to define password requirements and control applications and functions on a device. You can create and apply an IT policy to a user account or a group of user accounts.

Feature	Description
Management of applications	You can provision and manage work applications on devices.
Profiles	You can use profiles to manage device settings that are supported by the device. You can set up and assign profiles to a user account or a group of user accounts. These profiles are: • The VPN profile permits an device to connect to a VPN. • The Wi-Fi profile permits a device to connect to a wireless access point. • The Microsoft ActiveSync profile permits a device to connect to your organization's email service, if the email service supports Microsoft ActiveSync. • The SCEP profile permits a device to enroll a certificate from a certificate authority that supports the SCEP. • The certification authority certificate profile allows a device to establish a trusted relationship with services that use certificates that are issued by the certification authority.

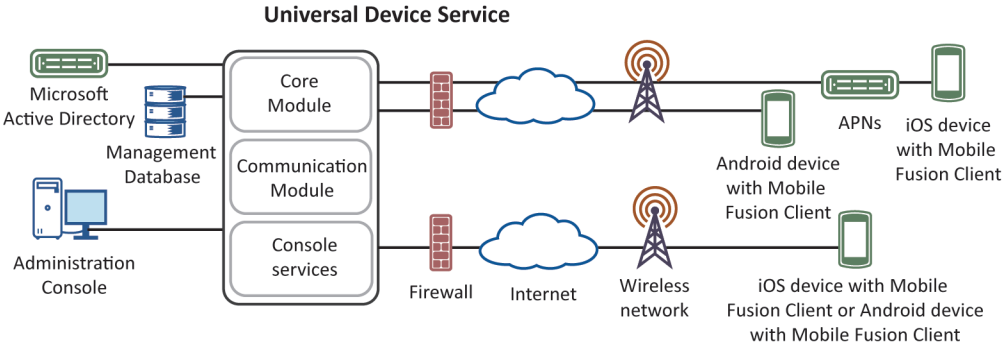
Architecture

3

This section gives you a high-level overview of the architecture of the and how it fits into an existing environment. For more information about system requirements and installation instructions, see the *Universal Device Service Installation and Configuration Guide*.

Architecture: Universal Device Service installed on one computer

You can install the Universal Device Service components on one computer.



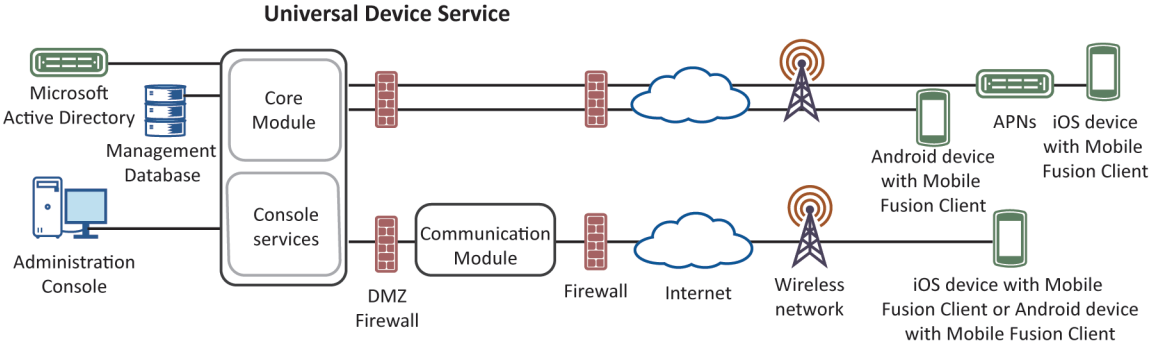
Component	Description
Core Module	The Core Module controls access to the Management Database and communicates with your organization's environment. The Core Module connects to the following services: • The Universal Device Service retrieves user account information from Microsoft Active Directory to create user accounts • The Microsoft ActiveSync profile is configured on iOS devices to allow the devices to access your organization's email service. • The Core Module sends notifications to APNs for an iOS device. These notifications inform the iOS device to contact the Communication Module.
Communication Module	The Communication Module manages Universal Device Service communication. It must be accessible to the Internet so that it can communicate with iOS devices and Android devices.
Console services	You can use Console services to manage user accounts, IT policies, profiles, and devices.
Mobile Fusion Client	The Mobile Fusion Client is installed on devices and communicates with the Communication Module.

Architecture: Universal Device Service with the Communication Module installed in the DMZ

The Universal Device Service components can be installed with the following configuration:

- The Communication Module is installed on a computer in the DMZ.
- The Core Module and the Console services are installed on the same computer behind both the DMZ firewall and your organization's firewall.

The Management Database can be located on the computer that hosts the Core Module or on a separate computer. The Management Database cannot be installed in the DMZ. If the Communication Module is installed in the DMZ, the database cannot be hosted on that same computer.



Component	Description
Core Module	The Core Module controls access to the Management Database and communicates with your organization's environment. The Core Module connects to the following services: • The Universal Device Service retrieves user account information from Microsoft Active Directory to create user accounts. • The Microsoft ActiveSync profile is configured on iOS devices to allow the devices to access your organization's email service. • The Core Module sends notifications to APNs for an iOS device. These notifications inform the iOS device to contact the Communication Module.
Communication Module	The Communication Module manages the Universal Device Service communication. The Communication Module is installed on a computer in the DMZ. It must be able to access the Internet so that it can communicate with iOS devices and Android devices. To prevent an unauthorized user from having direct access to the other Universal Device Service components, the Communication Module is installed on a computer in the DMZ, between the DMZ firewall and your organization's firewall.

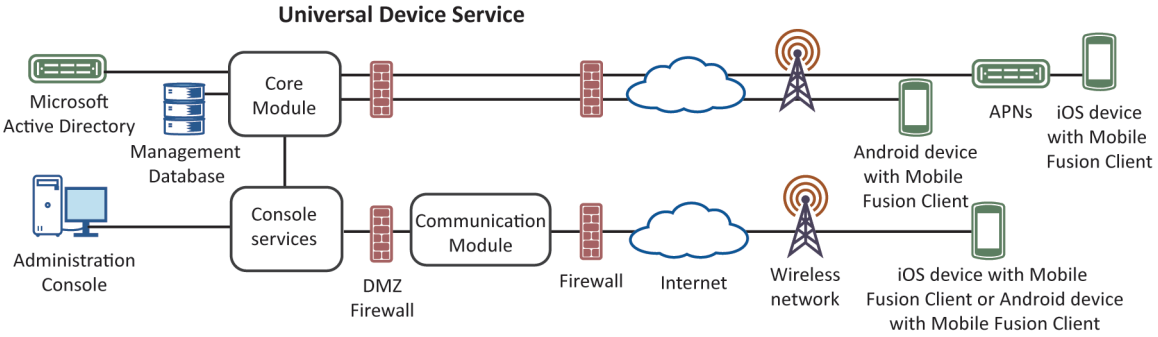
Component	Description
Console services	You can use Console services to manage user accounts, IT policies, profiles, and devices.
Mobile Fusion Client	The Mobile Fusion Client is installed on the device and communicates with the Communication Module.

Architecture: Universal Device Service installed in a distributed environment

You can install the Universal Device Service in a distributed environment with the following components:

- The Communication Module is installed on a computer in the DMZ.
- The Core Module and the Console services are installed on separate computers behind both the DMZ firewall and your organization's firewall.

The Management Database is located on the computer that hosts the Core Module or on a separate computer. The database cannot be installed in the DMZ. If the Communication Module is installed in the DMZ, the database cannot be hosted on that same computer.



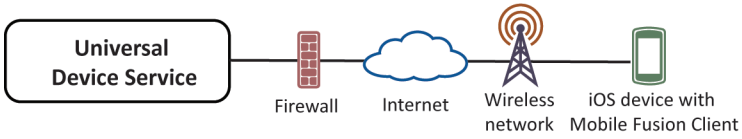
Component	Description
Core Module	The Core Module controls access to the Management Database and communicates with your organization's environment. The Core Module connects to the following: • The Universal Device Service retrieves user account information from Microsoft Active Directory to create user accounts • The Microsoft ActiveSync profile is configured on iOS devices to allow the devices to access your organization's email service. • The Core Module sends notifications to APNs for an iOS device. These notifications inform the iOS device to contact the Communication Module.

Component	Description
Communication Module	The Communication Module manages Universal Device Service communication. The Communication Module is installed on a computer in the DMZ. It must be able to access the Internet so that it can communicate with iOS devices and Android devices. To prevent an unauthorized user from having direct access to the other modules, the Communication Module is installed on a computer in the DMZ, between the DMZ firewall and your organization's firewall.
Console services	You can use Console services to manage user accounts, IT policies, profiles, and devices.
Mobile Fusion Client	The Mobile Fusion Client is installed on devices and communicates with the Communication Module.

Data flows

4

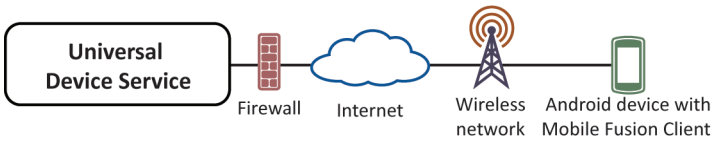
Data flow: Activating an iOS device over the wireless network



1. In the Administration Console, you create a user account and send an email message that contains information about downloading the Mobile Fusion Client to the user.
2. The user performs the following actions:
   - The user receives the email message and installs the Mobile Fusion Client on the device.
   - The user types their organization's name, username, and password and accepts the terms and conditions of the license agreement and then activates the device.

The device is activated and can communicate with the Universal Device Service.

Data flow: Activating an Android device over the wireless network



1. In the Administration Console, you create a user account and send an email message to the user that contains information about downloading the Mobile Fusion Client.
2. The user performs the following actions:
   - The user receives the email and installs the Mobile Fusion Client on the device.
   - The user types their organization's name, username, and password and accepts the terms and conditions of the license agreement and then activates the device.

The device is activated and can communicate with the Universal Device Service.

Related resources

5

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

Resource	Information
Universal Device Service Release Notes	• Description of known issues and potential workarounds
Universal Device Service Installation and Configuration Guide	• System requirements • Installation instructions
Universal Device Service Feature and Technical Overview	• Architecture diagrams • Description of features and components • Data flows
Universal Device Service Administration Guide	• Instructions for creating user accounts, groups, and administrator accounts, and so on • Instructions for activating devices • Instructions for creating and assigning IT policies and profiles • Instructions for managing applications on devices

Glossary

6

APNs	Apple Push Notification service
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.
SCEP	simple certificate enrollment protocol
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.

Apple is a trademark of Apple Inc. Android is a trademark of Google Inc. Microsoft ActiveSync and Microsoft Active Directory are trademarks of Microsoft Corporation. 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
Centrum House
36 Station Road
Egham, Surrey TW20 9LF
United Kingdom

Published in Canada