BlackBerry 2FA

Installation and Upgrade Guide

Server

Contents

What is the BlackBerry 2FA server?

The BlackBerry 2FA server is an optional component of BlackBerry 2FA that is deployed when the product is used in conjunction with RADIUS-based systems like most VPNs, or it is used with custom services like web applications and SIP client applications that call the product's external REST API endpoint. The BlackBerry 2FA server is not required in deployments that use only BlackBerry Enterprise Identity, but it can be deployed in cases where you want to use two-factor authentication for both cloud services supported by Enterprise Identity and the other supported systems.

Installing the BlackBerry 2FA server

You can install the BlackBerry 2FA server on the same computer as an EMM solution from BlackBerry, but, for maintainance and availability reasons, this configuration is not recommended.

For information about software requirements and supported mobile device operating systems, see the BlackBerry 2FA server compatibility matrix content.

Environment requirements

Item	Requirement
VPN gateway	Any of the VPN gateways listed in the BlackBerry 2FA server compatibility matrix content.
Custom services	Services like web applications and SIP client applications must be configured to call the BlackBerry 2FA server's external REST API endpoint.
EMM solution from BlackBerry	Any of the EMM solutions listed in the BlackBerry 2FA server compatibility matrix content.
Company directory	Microsoft Active Directory and users with Microsoft Active Directory accounts and valid email addresses.

Hardware requirements

Item	Requirement
RAM	2 GB
CPU	2 cores Both the RAM and CPU requirements are designed to allow for a connection to one instance of BlackBerry UEM and a sustained rate of approximately 30 requests per minute.
Virtual machines	You can install the BlackBerry 2FA server on a virtual machine. Due to known issues generating random numbers on virtual machines, you must configure the hypervisor to provide access to hardware sources of randomness to the guest virtual machine that runs the BlackBerry 2FA server. Otherwise, you may see delays in secure transactions between the BlackBerry 2FA server and the EMM solution from BlackBerry.

Software requirements

Item	Requirement
Operating system (64-bit)	Any of the operating systems listed in the BlackBerry 2FA server compatibility matrix content.
Java Runtime Environment	Java Runtime Environment 8 for Windows x64 (bundle 151 or later).
Domain	For MS-CHAP authentication support, the computer must be part of the domain that users are authenticated on.
Browser	Any of the browsers listed in the BlackBerry 2FA server compatibility matrix content.
Other considerations	BlackBerry 2FA supports IPv4 for TCP/IP connections only.

Configure permissions for the service account

A service account is a Windows account that runs the BlackBerry 2FA server. The service account must be a member of the local Administrators group on the computer that you install BlackBerry 2FA on, and it must have the appropriate permissions.

You can use the service account that the EMM solution from BlackBerry uses to install BlackBerry 2FA. Otherwise, create a service account in your company directory or a local Windows account on the computer that you want to install BlackBerry 2FA on.

1. On the taskbar, click **Start > Administrative Tools > Local Security Policy**.
2. In the left pane, expand **Local policies**.
3. Click **User rights agreement**.
4. Configure the **Log on as a service** permission for the service account.

Install or upgrade the BlackBerry 2FA server

Complete the following steps to install the BlackBerry 2FA server or upgrade the server from an older version.

Whether you are using BlackBerry UEM Cloud or an on-premises instance of BlackBerry UEM, the BlackBerry 2FA server is installed on-premises.

For the latest compatibility information, see the BlackBerry 2FA server compatibility matrix content.

Before you begin:

- On the computer that will run the BlackBerry 2FA server, download and install the latest Java Runtime Environment 8 for Windows x64 (bundle 151 or later). It must be installed in the default location: `C:\Program Files\Java\jre1.8.0_<bundle>`.
- If there is a previous version of the BlackBerry 2FA server configured on the computer, then the configuration settings are automatically saved and restored when the latest.
- If you install the BlackBerry 2FA server on a computer that has more than one NIC, verify that the production NIC is first in the bind order in the Windows network settings.

- On the computer that will host the BlackBerry 2FA server, download the BlackBerry 2FA server for Windows software from https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B.

1. Log in to the computer that you want to install or upgrade the BlackBerry 2FA server on using an account with local administrator privileges. To upgrade a server, you must use the same service account that was used during the original installation. You can find the service account information from the BlackBerry 2FA service in Services.msc.

2. Unzip the BlackBerry 2FA server software to a folder and double-click **Setup.exe**. If a Windows message appears and requests permission for the file to make changes to the computer, click **Yes**.

3. Select a language and click **OK** .

4. Click **Next**.

5. Select a country or region and read the license agreement. To accept it, select **I accept the terms of the license agreement** and click **Next**.

6. Verify that the installation requirements are met. Click **Next** .

7. Verify that **BlackBerry 2FA Service** and **Register as Windows service** are selected.

8. In the **Other components** section, select **BlackBerry 2FA app files**. You only need to install the app files on the first instance of the BlackBerry 2FA server that you install. Make sure the BlackBerry 2FA app is installed on your users' BlackBerry 10 devices after you install and configure the BlackBerry 2FA server. For more information, see the BlackBerry 2FA server configuration content.

9. In the **Service account** dialog box, type the information for the service account that the BlackBerry 2FA server can use to run.

10. Click **Install**.

11. Complete the instructions on the screen.

12. If a version of the BlackBerry 2FA server is already running on the computer, it will be automatically uninstalled. If a system restart is required, then you must run Setup.exe again to resume the upgrade.

13. Click **Next**.

14. Click **Close**.

After you finish: Add a BlackBerry 2FA server to BlackBerry UEM

Add a BlackBerry 2FA server to BlackBerry UEM

You must generate and download an activation file to enable communication between the BlackBerry 2FA server and BlackBerry UEM. You must to store the activation file in the BlackBerry 2FA installation directory.

If you are using BlackBerry UEM Cloud and have a proxy server in a DMZ, you must configure the proxy in the activation file before you restart the BlackBerry 2FA server to activate it. After you restart the server, and the server has been successfully added to BlackBerry UEM, the activation file is removed from the installation directory.

Before you begin: Install or upgrade the BlackBerry 2FA server

1. In the BlackBerry UEM management console, on the menu bar, click **Settings** > **External integration** > **BlackBerry 2FA server**.

2. Click ＋.

3. Click **Generate and download**. Save the file to `<install_dir>\bb2fa-config\`. Only the last activation file that you download is valid.

4. If you are using BlackBerry UEM Cloud and have a proxy in a DMZ, open the activation file and enter the proxy information. If you have a BlackBerry Connectivity Node installed, you can match the proxy settings. For example:

```
proxy.dmz.type=ROUTER_SOCKS5
  proxy.dmz.bcpHosts=my.proxy.host.name
  proxy.dmz.bcpPort=3102
  proxy.dmz.socks.authtype=NoAuth
```

5. To restart the BlackBerry 2FA service, complete the following task:
   a) In a command prompt window, run **services.msc**.
   b) Right-click **BlackBerry 2FA Service** > **Stop**.
   c) Right-click **BlackBerry 2FA Service** > **Start**.
6. In the BlackBerry UEM management console, click **Check status** to verify the server was successfully activated.

After you finish: Configure the BlackBerry 2FA server from the UEM management console. For more information, see the BlackBerry 2FA server configuration content.

BlackBerry 2FA server ports

The following table provides a list of the default ports that the BlackBerry 2FA server uses. Unless specified, you can change them in the bb2fa-config.json file located in the *<install_dir>*/bb2fa-config folder.

When you install several BlackBerry 2FA servers to configure high availability, the same port numbers are configured for each server. If a defined listening port is not available, the BlackBerry 2FA server writes an error message to the log file after you configure and start the server.

Port	Purpose
1812	This is the inbound UDP port that the BlackBerry 2FA server uses as the primary port for RADIUS communication with VPN gateways.
5443	This is the inbound HTTPS port that the BlackBerry 2FA server's external REST API endpoint uses to receive responses custom services.
8828	This is the HTTP inbound configuration port from UEM. The BlackBerry 2FA server uses port 8828 for the first BlackBerry UEM instance that you add and then increments by one for each additional instance.
8886	This is the outbound port that the BlackBerry 2FA server uses to send a request for user authentication.
10000 and above	This is the inbound port that the BlackBerry 2FA server uses to receive device confirmation responses from BlackBerry UEM. Device confirmation requests and responses are supported for all device types. The BlackBerry 2FA server uses port 10000 for the first BlackBerry UEM instance that you add and then increments by one for each additional instance.

Uninstall the BlackBerry 2FA software

You can use the uninstall application to remove the BlackBerry 2FA software from a computer. The uninstall application also removes the log files for the existing installation.

1. Do one of the following:

   - Click **Start > All Programs > BlackBerry 2FA > Uninstall**.
   - Browse to `<install_dir>` or `C:\Program Files\BlackBerry\BlackBerry 2FA` and run **Uninstall_BlackBerry_2FA_Server.exe**

2. Complete the instructions on the screen.

3. Restart the computer.

After you finish:

- Optionally, delete the groups that you created in BlackBerry UEM to support BlackBerry 2FA.
- Optionally, on your VPN gateway, delete the VPN profile that you created for BlackBerry 2FA.

Glossary

API	application programming interface
CA	certification authority
DNS	Domain Name System
ECDH	Elliptic Curve Diffie-Hellman
EAP	Extensible Authentication Protocol
EMM	Enterprise Mobility Management
FQDN	fully qualified domain name
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IP	Internet Protocol
IT policy	An IT policy consists of various rules that control the security features and behavior of devices.
IKE	Internet Key Exchange
MAM	mobile application management
MDM	mobile device management
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NAS	network-attached storage
NTLM	NT LAN Manager
OTP	one-time password
PAP	Push Access Protocol
RADIUS	Remote Authentication Dial In User Service
REST	Representational State Transfer
SAML	Security Assertion Markup Language
SIP	Session Initiation Protocol

SSL	Secure Sockets Layer
TLS	Transport Layer Security
UEM	Unified Endpoint Manager
VPN	virtual private network

Legal notice

©2018 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Android and G Suiteare trademarks of Google Inc. Apache log4j is a trademark of The Apache Software Foundation. Barracuda is a trademark of Barracuda Networks, Inc. Boxis including without limitation, either a trademark, service mark or registered trademark of Box, Inc. Cisco and Cisco AnyConnect are trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Citrix and NetScaler are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.F5 and BIG-IP iOS is a trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. Java and JavaScript are trademarks of Oracle and/or its affiliates. Microsoft, Active Directory, Internet Explorer, SQL Server, Windows, and Windows Phone are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Salesforce is a trademark of salesforce.com, inc. and is used here with permission.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 on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry 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 websites (collectively the "Third Party Products and Services"). BlackBerry 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 BlackBerry 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 BLACKBERRY 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 BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY 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 BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY 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 BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY 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 BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY 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 BlackBerry'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 BlackBerry'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 BlackBerry and BlackBerry 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 BlackBerry.

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

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East