BlackBerry 2FA

Overview

Contents

About BlackBerry 2FA

BlackBerry 2FA protects access to your organization's critical resources using two-factor authentication. The product uses a password that users enter and a secure prompt on their mobile device each time they attempt to access resources. BlackBerry 2FA also supports the use of standards-based One-Time Password (OTP) tokens.

You manage BlackBerry 2FA users from the BlackBerry UEM Cloud or BlackBerry UEM management console. You can also use BlackBerry 2FA on devices that aren't managed by BlackBerry UEM Cloud or BlackBerry UEM. BlackBerry 2FA supports iOS and Android devices that have only a BlackBerry Dynamics container, devices managed by third-party MDM systems, or unmanaged devices.

You can use BlackBerry 2FA to protect a wide variety of systems, including VPNs, RADIUS-compatible systems, custom applications using a REST API, and SAML-compliant cloud services when they are used in conjunction with BlackBerry Enterprise Identity.

Configuring BlackBerry 2FA for use with mobile devices is straightforward. The first authentication factor, the password, can be a user's directory or container password. The second authentication factor, the device prompt, requires an app on the device that triggers a secure validation of the device. For iOS and Android devices, BlackBerry 2FA is included in the BlackBerry UEM Client. They are either installed during activation or you must have users install them. For managed BlackBerry 10 devices, you must deploy a separate BlackBerry 2FA app or have users install it.

Configuring BlackBerry 2FA for users without mobile devices is also straightforward. Standards-based OTP tokens are registered in the BlackBerry UEM console and issued to users. The first authentication factor is the user's directory password, and the second authentication factor is a dynamic code that appears on the token's screen. For more information, see the Administration content for BlackBerry 2FA.

The BlackBerry 2FA server is an optional component that is deployed when the product is used in conjunction with RADIUS-based systems like most VPNs, or it is used with apps calling the product's REST API. The BlackBerry 2FA server is not required in deployments that use only Enterprise Identity, but it can be deployed in cases where you want to use two-factor authentication for both cloud services and the other supported systems. For more information, see the BlackBerry 2FA server compatibility matrix content, BlackBerry 2FA server installation and upgrade content, and the BlackBerry 2FA server configuration content.

Direct Authentication

You can enable BlackBerry 2FA Direct Authentication so that when users want to authenticate to your organization's resources, they start the authentication process from their devices instead of receiving a confirmation prompt and without using a One-Time Password. When you enable Direct Authentication feature for users, users must use their directory password to log in to your organization's resources within the time limit that you specify.

Users can access the direct authentication feature from the BlackBerry UEM Client on Android and iOS devices and the BlackBerry 2FA app on BlackBerry 10 devices.

OTP tokens

BlackBerry UEM supports the use of One-Time Password (OTP) tokens through BlackBerry 2FA service. The OTP tokens feature provides a secure authentication scheme for users who do not have a mobile device or have a mobile device that does not have sufficient connectivity to support the real-time BlackBerry 2FA device notifications. When using an OTP instead of a device notification as the second factor of authentication, the OTP is provided in the same channel as the user's password, and their mobile device is not signaled.

You can enter the OTP code with the username or the password.

- When using an OTP code with the username, after the username, you type a comma (,) then the OTP code with no spaces between them. For example, if the username is "janedoe" and code is "555123", it should be entered as "janedoe,555123". Using this method, users can easily verify the code that they entered.
- When using an OTP code with the password, the code precedes the user's password. For example, if the code is "555123" and the password is "AbCdeF", it should be entered as "555123AbCdeF".

Software tokens

You enable software OTP tokens for users in the BlackBerry 2FA profile that you assign to them. The software token can be found in the BlackBerry UEM Client app by swiping through its home screen.

Hardware tokens

To manage hardware OTP tokens in BlackBerry UEM, the user must have a BlackBerry 2FA profile assigned to them.

For more information about the latest supported hardware tokens, see the BlackBerry 2FA server compatibility matrix.

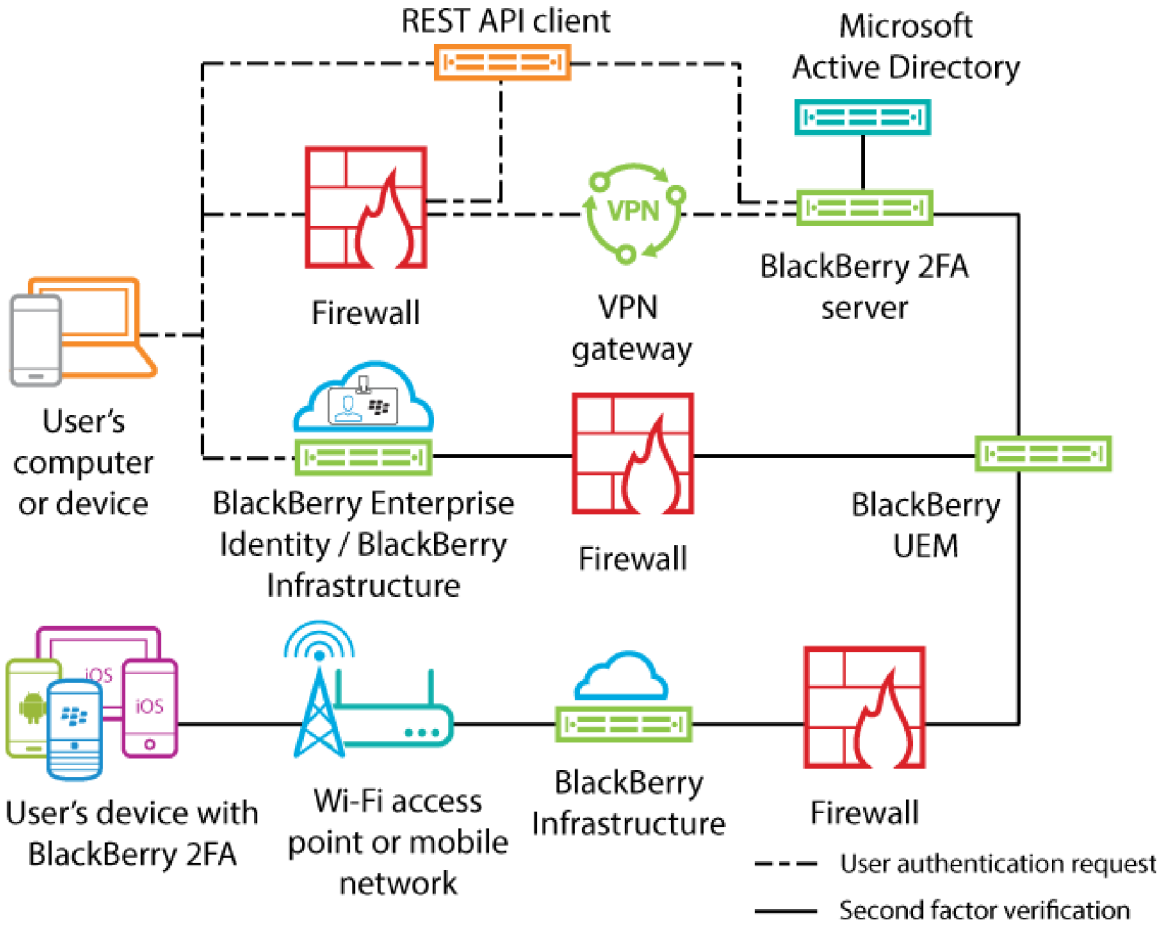
Preauthentication and self-rescue

BlackBerry 2FA Preauthentication and self-rescue are features that allow users to authenticate to your organization's resources for a predetermined period with only a single factor. These features are enabled and configured independently.

Preauthentication should be used when the user expects to have no device access or no network coverage for a short period of time (for example, when they are on an airplane). Users can request Preauthentication from the their device, or administrators can enable it through the BlackBerry UEM management console. BlackBerry recommends using the software OTP feature instead whenever possible because it retains full two-factor security, even though it is less user-friendly.

Self-rescue should be used when a user has lost their device or has no device access for a longer period of time such as a day or more (for example, the user lost their device and is waiting for a replacement). Users can access the self-rescue feature from BlackBerry UEM Self-Service, which means that it can only be enabled if the user is connected to the organization's network.

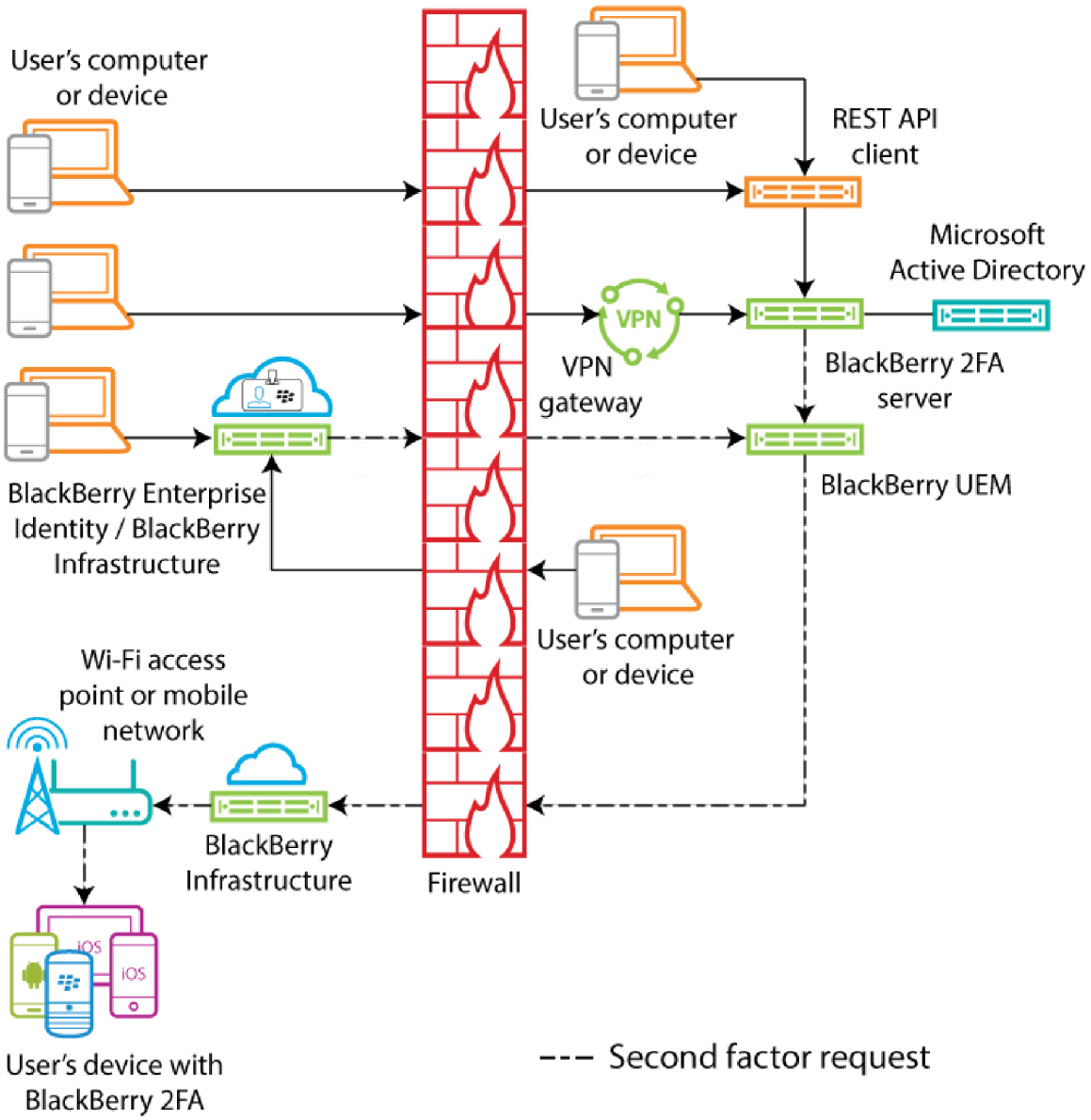
Architecture: BlackBerry 2FA



Component	Description
User's computer or device	A user's computer or device is any computer or device, from inside or outside a firewall, that is used to connect to a resource that requires two-factor authentication.
BlackBerry 2FA server	The BlackBerry 2FA server connects to BlackBerry UEM to find the devices associated with a user and to send authentication requests to the BlackBerry 2FA app that's installed on devices.
VPN gateway (optional)	The VPN gateway is a computer that accepts VPN connections to your organization's network. **Note:** This feature requires the BlackBerry 2FA server.

Component	Description
REST API client (optional)	The REST API client is a customer-defined, on-premises service that authenticates users who access it through the BlackBerry 2FA server's REST API. **Note:** This feature requires the BlackBerry 2FA server.
BlackBerry Enterprise Identity (optional)	BlackBerry Enterprise Identity provides single sign-on (SSO) to cloud services, such as Box, Salesforce, and G Suite. Enterprise Identity connects directly to the BlackBerry 2FA service in BlackBerry UEM or BlackBerry UEM Cloud.
BES12, or BlackBerry UEM, BlackBerry UEM Cloud	BlackBerry UEM also manages BlackBerry 2FA user configuration through the BlackBerry 2FA profile and the use of one-time password (OTP) tokens.
User's device with BlackBerry 2FA	For iOS and Android devices, BlackBerry 2FA is included in the BlackBerry UEM Client. For BlackBerry 10 devices, users install the BlackBerry 2FA app.

Authentication requests through BlackBerry UEM



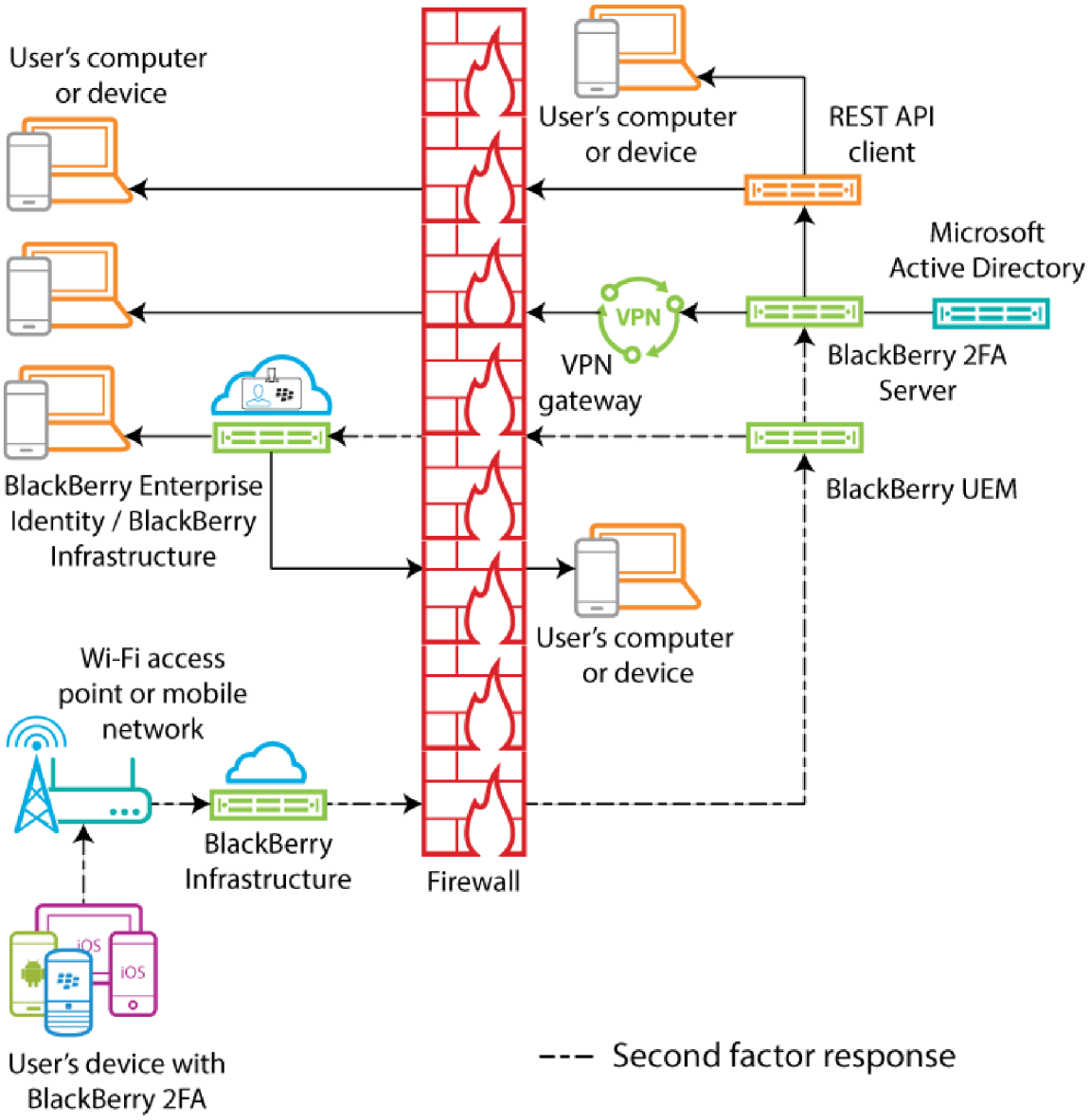
To initate an authentication request, a user performs one of the following actions:

- Accesses the login interface for a custom service on a computer or device at work and enters their login information
- Accesses the login interface for a custom service on a computer or device outside work and enters their login information
- Opens a VPN client on a computer or device outside work and enters their login information
- Accesses the login interface of a service that is configured to use BlackBerry Enterprise Identity for authentication on a computer or device outside work and enters their login information
- Accesses the login interface of a service that is configured to use BlackBerry Enterprise Identity for authentication on a computer or device at work and enters their login information

The user receives a prompt on their device to confirm that they want to authenticate. Depending on the authentication options configured for the user, they may be required to enter their device or secure container password before they can acknowledge the prompt.

The diagram does not show the data flow for authentication requests that use one-time password (OTP) tokens.

Authentication responses through BlackBerry UEM

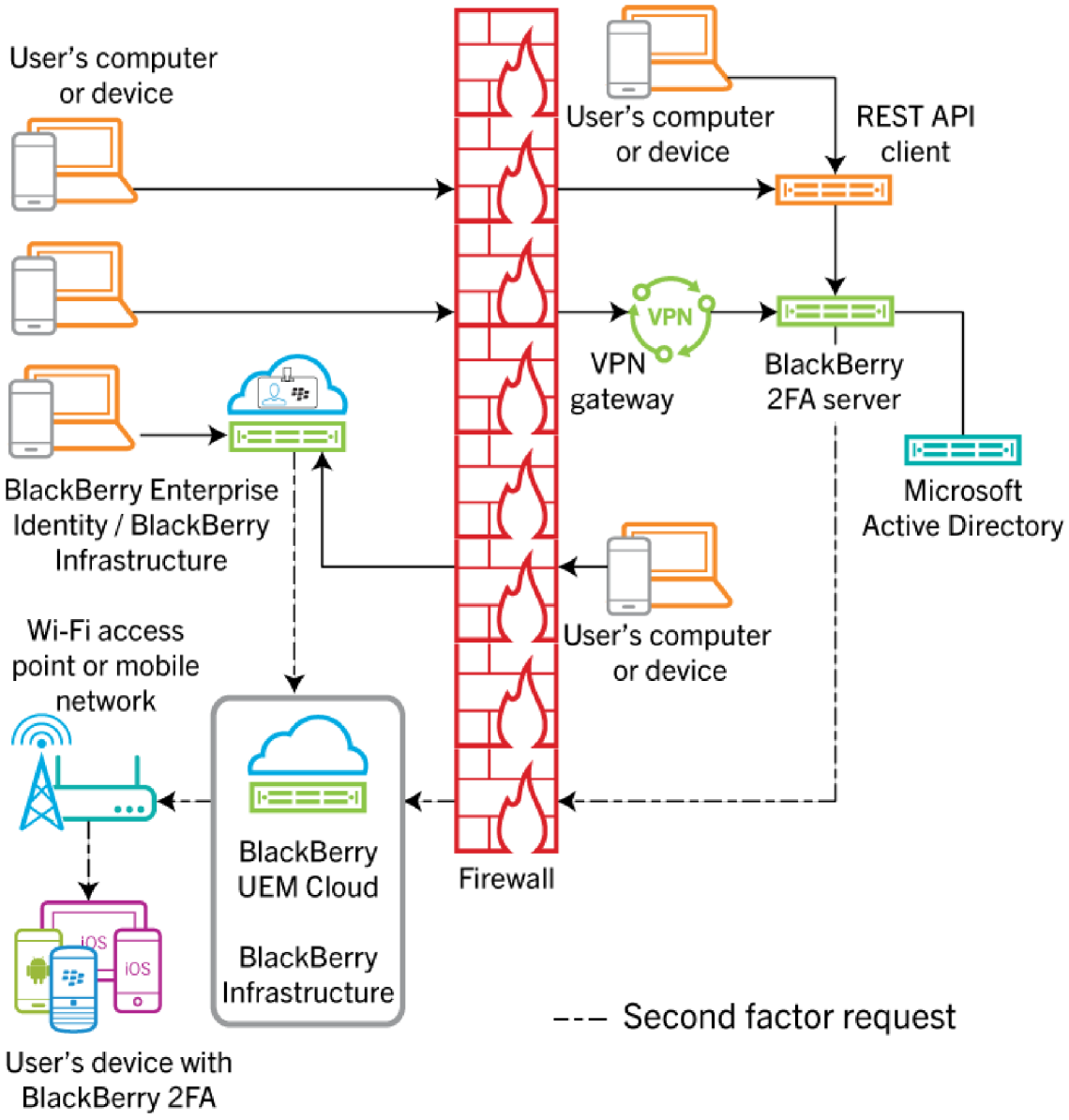


In all the responses shown, the user confirms the authentication prompt on their device, and the response travels back to BlackBerry Enterprise Identity or the BlackBerry 2FA server. The user's directory password is verified if the

authentication options for the user require it. After it is verified, the user receives a message on their device that the prompt response was sent successfully.

The diagram does not show the data flow of authentications using one-time password (OTP) tokens.

Authentication requests through BlackBerry UEM Cloud



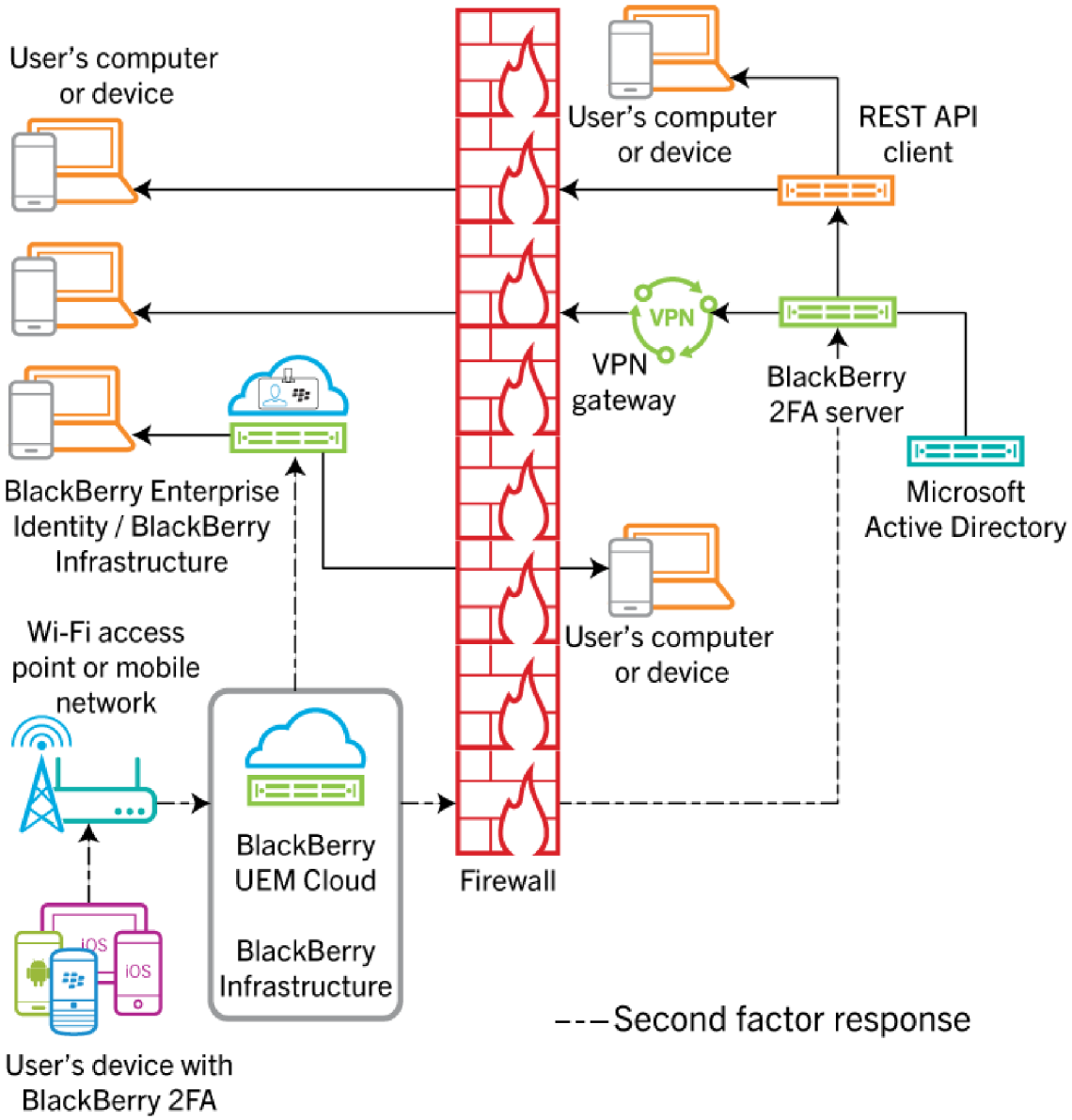
To initate an authentication request, a user performs one of the following actions:

- Accesses the login interface of a service that is configured to use BlackBerry Enterprise Identity for authentication on a computer or device outside work and enters their login information
- Accesses the login interface of a service that is configured to use BlackBerry Enterprise Identity for authentication on a computer or device at work and enters their login information

The user receives a prompt on their device to confirm that they want to authenticate. Depending on the authentication options configured for the user, they may be required to enter their device or secure container password before they can acknowledge the prompt.

The diagram does not show the data flow for authentication requests that use one-time password (OTP) tokens.

Authentication responses through BlackBerry UEM Cloud



In all the responses shown, the user confirms the authentication prompt on their device, and the response travels back to BlackBerry Enterprise Identity. The user's directory password is verified if the authentication options for the user require it. After it is verified, the user receives a message on their device that the prompt response was sent successfully.

The diagram does not show the data flow of authentications using one-time password (OTP) tokens.

Legal notice

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
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada