BlackBerry 2FA

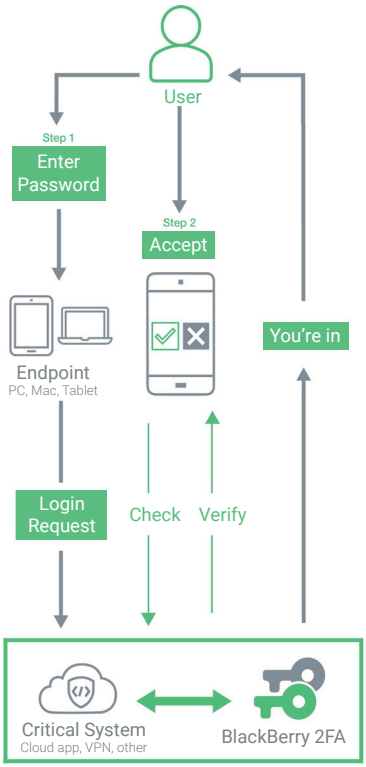
BlackBerry 2FA

The Challenge: Critical enterprise systems – especially cloud services – are more exposed than ever before because of the growing threat of cybercrime. Passwords alone are not enough for the expanding number of endpoints in your network. Two-factor authentication for cloud apps and VPNs is a top priority for today's organizations. Yet many two-factor systems are complicated and error-prone, place heavy burdens on IT, and fail to secure cloud and other services.

The Solution: BlackBerry® 2FA offers strong, high-security user authentication that safeguards cloud and standards-based services – while still protecting your existing VPN.

Two-factor authentication is vital for protecting your company's high-value systems, whether it's critical cloud services like Microsoft® Office 365™ and Salesforce®, or your VPN. There's a growing awareness in today's organizations that legacy two-factor authentication solutions are deficient. The user experience is complex and frustrating, and they don't adequately protect cloud services.

BlackBerry 2FA uses Certificate-Based Authentication of devices, meeting or exceeding the level of security offered by legacy systems – but with lower cost and better user experience.

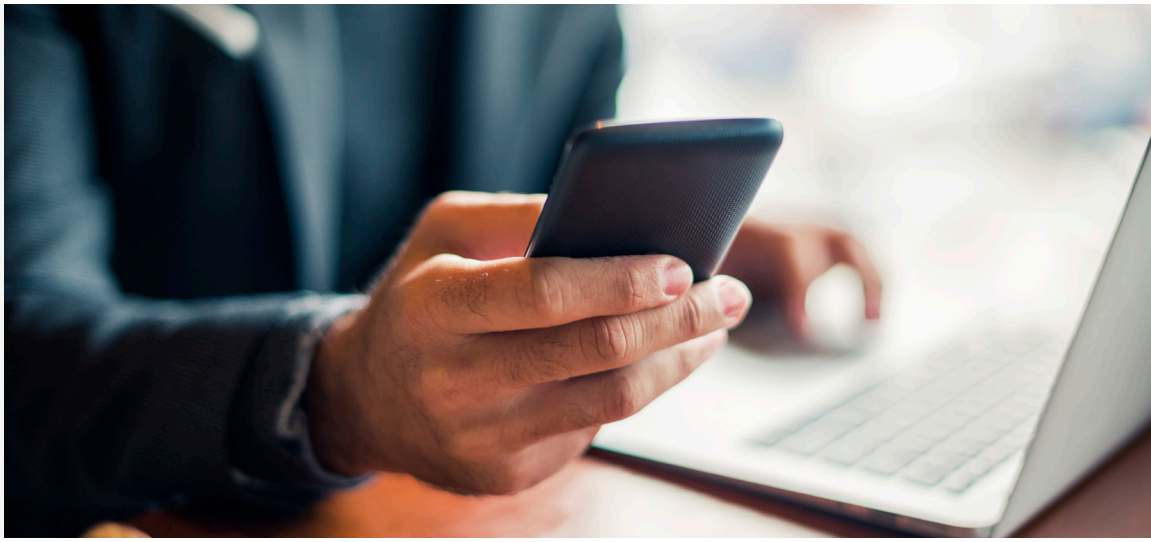


Provide a Superior End-User Experience

BlackBerry 2FA delivers a positive user experience, and supports a wide range of employee devices (iOS, Android™, and BlackBerry). Once employees have registered one or more mobile devices, they can access critical systems simply by entering their usual password and clicking OK on a registered mobile device to authenticate.

It's a simple, high-security solution, with an improved user experience compared with legacy two-factor authentication systems. BlackBerry 2FA:

- Eliminates the frustration of complex authentication processes
- Removes the need to remember PINs, carry additional devices, or manually transcribe codes from tiny screens
- Provides a superior, one-click user experience
- Enables access to critical systems, even in emergencies
- Allows for the use of multiple, preferred devices



Support Any Type of User: With BlackBerry 2FA, you can provide two-factor authentication to every type of user inside and outside your organization—from traditional employees and part-time contractors to partners. It supports unmanaged devices and devices managed by a third party, so it can easily map onto almost any device external users may have. If they have a device, you can provision r emote users without requiring any new hardware.

BlackBerry 2FA supports affordable, standards-based hardware tokens for users without mobile devices, or users unwilling to put software on their devices. Compared with legacy hard tokens on the market, the tokens supported by BlackBerry 2FA are designed to be less expensive, have longer battery life (typically double), and are available through a wide range of vendors.

Lower Your Operating Costs: BlackBerry 2FA has low up-front costs, with no new authentication devices or infrastructure required. Legacy two-factor authentication systems are expensive to maintain. They often have high maintenance or subscription fees, in addition to high operational costs due to complex provisioning and heavy use of IT resources for resolving user issues.

BlackBerry 2FA virtually eliminates help desk requests that occur frequently with legacy two-factor authentication systems, such as forgotten PINs and lost hard token devices. User errors are also drastically decreased.

Easy to Deploy and Scalable: With BlackBerry 2FA, deployment is simple. It allows automatic provisioning to devices managed by BlackBerry® UEM, and a simple activation procedure for users with other devices. In either case, no IT support is required. There are no new physical devices to ship, and no seed files to manage. And you can easily set up BlackBerry 2FA on as many devices as users have.

BlackBerry 2FA also offers flexible deployment options. You can choose to make the move to BlackBerry 2FA all at once with simple, quick deployment. Or you can opt to deploy in a chosen number of users, then work in parallel with your legacy system and easily scale up as desired.

BlackBerry 2FA integrates with BlackBerry® UEM, allowing for better device security, and increasing your trust and confidence in the BYOD model. It can also coexist with other mobility solutions. The integration with UEM simplifies the provisioning process.

Equip Users to Self-Rescue: BlackBerry 2FA offers optional features that can ensure users always have access to your cloud services, VPN, or other systems they need to keep working – without involving IT. Users can authenticate when offline, or even pre-authenticate ahead of planned network connectivity loss – for example, heading into an area of poor network coverage or air travel.

For device loss, users can self-rescue via a portal, with the option of self-issuing a new authentication device.

Compatibility

- Popular VPN/VDI systems (e.g. Cisco, Citrix, others)
- RADIUS systems
- SAML 2.0 services*
- OIDC services*
- Services federated with Microsoft Azure AD*
- Various BlackBerry products*

Authentication

- Internal and external users
- Push authentication
- Software OTP tokens
- OATH TOTP-compliant hardware tokens
- Contextual authentication*
- Password and 2FA processing can be kept on-premises

Devices

- Android, iOS, BB 10
- BlackBerry UEM-managed
- Unmanaged/BYOD
- Managed by third-party solutions

* Requires use of BlackBerry Enterprise Identity

About BlackBerry

BlackBerry is securing a connected world, delivering innovative solutions across the entire mobile ecosystem and beyond. We secure the world's most sensitive data across all end points – from cars to smartphones – making the mobile-first enterprise vision a reality. Founded in 1984 and based in Waterloo, Ontario, BlackBerry operates offices in North America, Europe, Middle East and Africa, Asia Pacific and Latin America. The Company trades under the ticker symbols "BB" on the Toronto Stock Exchange and "BBRY" on the NASDAQ. For more information, visit www.blackberry.com.