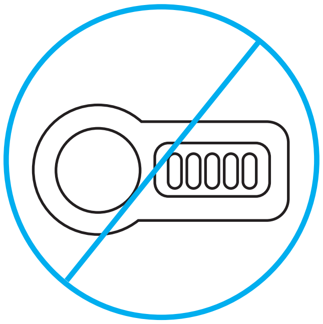
VPN AUTHENTICATION by BLACKBERRY

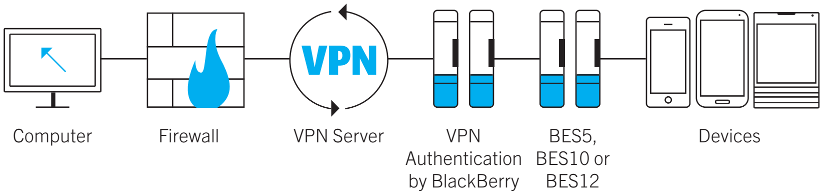
Turn a managed iOS, Android and BlackBerry device into a security token and ditch the key fob. VPN Authentication by BlackBerry streamlines secure access to corporate data and apps when and where your employees need them.

ZERO UPFRONT COSTS. NO MORE LOST KEY FOBS, PASSWORD RESETS, AND FEWER UNHAPPY SUPPORT CALLS.



Introducing your new VPN token. Your smartphone.

Stop depending on outdated one-time password (OTP) tokens that result in another device to carry and another password to remember. With VPN Authentication by BlackBerry®, an iOS, Android™ or BlackBerry® device replaces your organization's expensive OTP hardware solution with PKI-based two-factor security that helps reduce overall costs. With a touch of the screen, the smartphone allows access to your organization's VPN.



Reduce cost and hassle

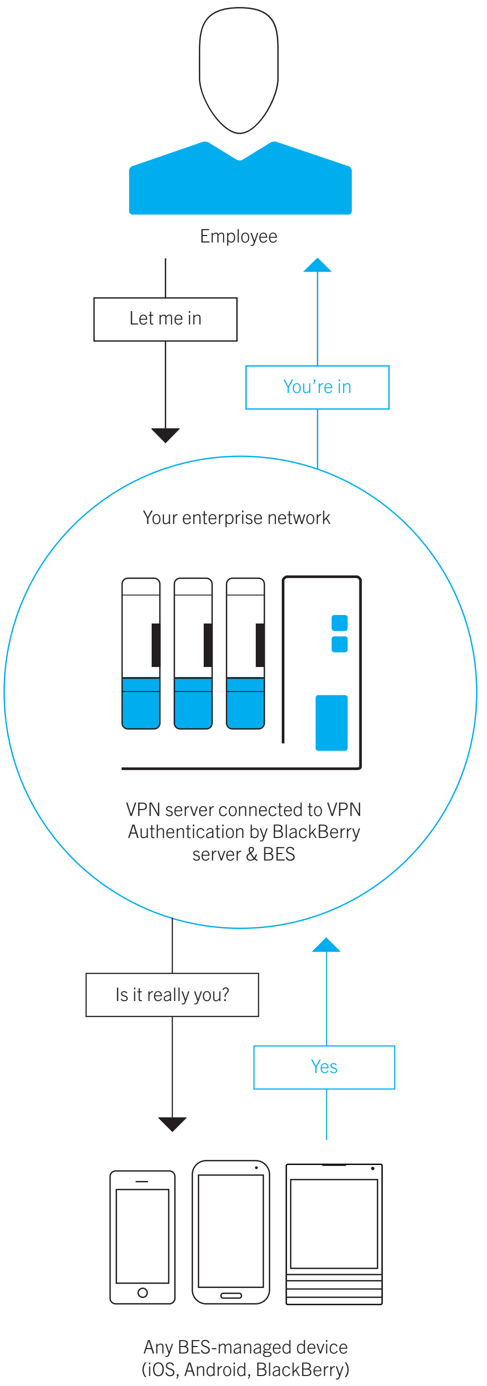
VPN Authentication by BlackBerry works with the managed iOS, Android and BlackBerry devices you already have deployed, offering superior value and equivalent or better security. And, by eliminating support required for synchronization problems and PIN resets through the helpdesk, it helps reduce support costs and employee downtime.

Scalable and Secure

VPN Authentication by BlackBerry takes a hybrid approach – the security and flexibility of on-premise software combined with modern PKI-based encryption, meeting or improving current authentication. And, you can quickly deploy and securely control VPN access and configuration of user profiles.

BlackBerry | ENTERPRISE

VPN AUTHENTICATION by BLACKBERRY



Employee
Let me in
You're in
Your enterprise network
VPN server connected to VPN Authentication by BlackBerry server & BES
Is it really you?
Yes
Any BES-managed device (iOS, Android, BlackBerry)

Flexible authentication options

Because the security needs of no two organizations are alike, VPN Authentication by BlackBerry can be customized to an organization's policies and requirements. Tailor the level of authentication for different user groups.

When your primary goal is	Choose this authentication	Required user actions
Usability	Simple	Device prompts user to accept the VPN connection. If the device is locked, a password is required.
A mix of usability and security	Forced authentication on device	User is always prompted to provide device password. VPN connection is accepted on device after log in.
Security	Active Directory credential authentication before device contact	User enters their Active Directory credentials on the endpoint first (computer/ tablet), and then accepts on device.

VPN Authentication by BlackBerry consists of two components:

1. Server – Install VPN Authentication by BlackBerry on the same hardware or VM image as your BlackBerry® Enterprise Server 5 (BES5), BlackBerry® Enterprise Service 10 (BES10) or BES12. For the best performance, install the server on its own computer or VM image.

2. Client App – Your employees may install the client app on any iOS, Android, BlackBerry® 10 or BlackBerry OS device managed by BES5, BES10 or BES12. App updates can be pushed to devices from the app stores.

Experience

For employees:

1. Employees use the VPN Authentication by BlackBerry app for one tap access to connect to a VPN via computer
2. The device prompts the employee to confirm their identity
3. Access is granted upon confirmation

For IT:

1. Install the on-premise VPN Authentication Server for integration with your existing VPN server (optional: use Enterprise Identity by BlackBerry® for comprehensive identity and access management)
2. Use BES to setup and configure users to use VPN Authentication by BlackBerry
3. Push the VPN Authentication by BlackBerry app to iOS, Android and BlackBerry devices and you are ready to go

Note: You can run VPN Authentication by BlackBerry alongside your existing one-time password (OTP) authentication solution.

For more information, visit **blackberry.com/vpnauthentication**