Sectigo PKI Enterprise Use Case: Windows Hello for Business

Integrating PKI-based authentication with Windows Hello for Business biometrics helps ensure the highest standards of security and identity. But using manual processes to manage the certificates required for Windows Hello for Business across large numbers of employees is labor intensive, technically demanding, and error prone.

To fully protect and ensure the authenticity of devices equipped for Windows Hello for Business, your security team needs to:

- Issue, deploy, renew, and replace digital certificates in your Windows 10 environments quickly, reliably, and scalably
- Monitor authorized Windows Hello for Business users and terminate access as appropriate
- See and control the entire certificate lifecycle through a single user interface

Sectigo offers solutions to help. Sectigo Certificate Manager is a complete management platform that automates end-to-end lifecycle management of digital certificates at scale. It is interoperable with all leading devices, operating systems, protocols, and chipsets and provides visibility and management through a single pane of glass, enabling security administrators to easily and cost-effectively monitor certificates across the enterprise.

Leveraging Sectigo Certificate Manager with Windows Hello for Business will enable your security team to benefit from:

- **Scalable certificate issuance.** Sectigo Certificate Manager issues public-private key pairs automatically, making it easy to use PKI in combination with Windows Hello for Business biometrics to ensure security for your user base—whether that's tens, hundreds, or thousands of people. It minimizes hassles for your security team and frees them for more valuable tasks.

- **Automated certificate deployment.** Sectigo offers a variety of automation options to fit your Windows 10 workflow and environment, including Sectigo's Microsoft CA proxy agent and automation standards like SCEP (Simple Certificate Enrollment Protocol) and EST (Enrollment over Secure Transport).

- **Full certificate lifecycle management.** With Sectigo Certificate Manager, you can automatically renew and replace certificates, so users can enjoy seamless access with Windows Hello for Business. You can also easily revoke certificates, terminating Windows Hello for Business access as needed.

- **Secure key storage.** Certificates are stored on devices using the secure Trusted Platform Module (TPM) or our software-based secure certificate storage.

- **Enhanced visibility and reporting.** Sectigo Certificate Manager allows you to view the status of the certificates in use across your network through a single pane of glass, enabling you to see expiration dates and minimize or eliminate service disruptions.

With Sectigo Certificate Manager, your security team can easily enforce cryptographic security, prevent data loss via unauthorized access, and future-proof your Windows devices equipped with Windows Hello for Business. And Sectigo Certificate Manager can be used to automate issuance and lifecycle management of all other certificates throughout your organization, across a wide variety of use cases, ranging from code signing to web servers and email.

About Sectigo

Sectigo provides purpose-built, automated PKI solutions that secure websites, connected devices, applications, and digital identities. As the largest commercial Certificate Authority trusted by enterprises globally for more than 20 years, and more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape. For more information, visit **www.sectigo.com.**

