

## Sectigo PKI Enterprise Use Case: VPN

Replacing multi-factor authentication for VPN access with certificate-based authentication improves the user experience and helps ensure the highest standards of security and identity. But using manual processes to manage the certificates required for VPN access across large numbers of employees is labor intensive, technically demanding, and error prone. To fully protect and ensure the authenticity of your VPN, your security team needs to:

- Issue, revoke, and replace digital certificates quickly, reliably, and scalably
- Monitor authorized VPN users and terminate access as needed
- See and control the entire certificate lifecycle through a single user interface

Sectigo can 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. Moreover, Sectigo Certificate Manager supports all trust models and can be used to manage certificates issued through Sectigo's public certificate authority (CA) and from your own private PKI.

Leveraging Sectigo Certificate Manager for VPN will improve the user experience and enable your security team to benefit from:

- **Scalable certificate issuance.** Sectigo Certificate Manager issues certificates automatically, making it easy to use PKI to ensure security for your user base, whether it's tens, hundreds, or thousands of people. That 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 specific workflow and environment, including automation standards like SCEP (Simple Certificate Enrollment Protocol) and EST (Enrollment over Secure Transport), as well as Sectigo's Microsoft CA proxy agent.
- **Full certificate lifecycle management.** Sectigo Certificate Manager provides automatic certificate renewal and replacement, so users can enjoy seamless access. In addition, you can also easily revoke certificates, for example, when an employee leaves your organization and access needs to be terminated.
- **Enhanced visibility and reporting.** View the status of all certificates in use across your VPN through a single pane of glass, enabling you to see expiration dates and minimize or eliminate service disruptions.

With certificate-based authentication, VPN users won't have to remember passwords, change them every few months, or worry that they will be stolen or compromised. 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](http://www.sectigo.com).