SecurID™

MFA for Your VPN

Three Keys To Getting It Right

Your VPN Deserves More Than a Username and Password

Back in the day, only a handful of users needed remote access via a virtual private network (VPN). And only the most critical of those were provided with enhanced security, via some form of token. Today, not only employees but also contractors, vendors, audit team members, partners, and sometimes even customers need access to your VPN. But far too many organizations still rely on usernames and passwords alone—leaving themselves them far too vulnerable.

In today's modern VPN era, you need to offer easy, frictionless and secure access to a diverse and growing population of users. You must be sure that they are who they say they are, and offer the appropriate levels of access to each one, every time.

Mobile multi-factor authentication (MFA) from SecurID can prevent unauthorized access to your VPN—and make it easy and cost-efficient for legitimate users to authenticate.

How easily can you distinguish **legitimate users from malicious actors?**

Three Keys To Using MFA To Secure Your VPN Access

1 Power accurate step-up authentication with risk analytics

Look for a MFA solution that can discern when access risk is high and when it's not—and respond accordingly. User-behavior analytics, relevant threat intelligence and machine learning make it possible to step up authentication when access risk warrants it, rather than inconveniencing low-risk users with unnecessary requests for additional authentication. A robust policy engine can put flexible controls in the hands of your security teams.

2 Offer each user the most convenient authentication option

Employees, contractors and partners. At the office, at home, in coffee shops, on airplanes. They all need easy, secure VPN access—but not all the same way. To give users convenient VPN access without compromising security, your MFA solution needs to offer a range of sign-in options, including mobile push-to-approve, one-time passcodes, biometrics, and hardware and software tokens.

3 Keep it simple for both users and admins

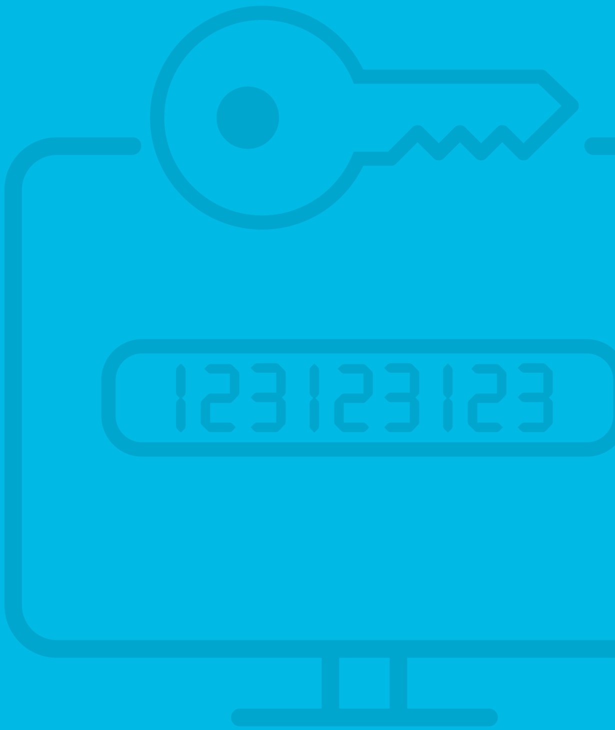
Spare yourself the grief of multiple MFA solutions. A MFA solution that can extend beyond VPN to other access scenarios—such as third-party cloud applications—gives users a single, seamless access experience, and you one secure solution to manage.

More Than Tokens

SecurID provides a host of sophisticated authentication options to secure your VPN

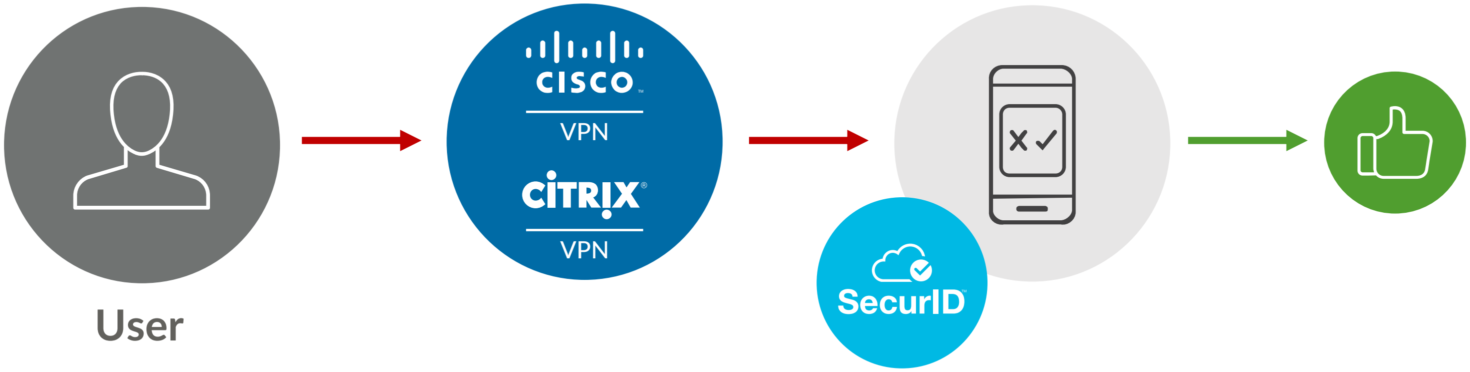
SecurID provides the widest range of authenticators, letting you extend modern MFA to more VPN users—and allowing them to choose from push notification, biometrics, hardware and software tokens, and more. SecurID makes it easy to manage different authenticators for different users, and to balance security, convenience and cost.

- Push
- Mobile OTP
- Biometrics
- Text Message
- Voice Call
- Hardware Token
- Software Token
- FIDO
- Wearables



How It Works

SecurID makes it easy to use mobile authentication to protect access to your VPN and support digital business.



1
User needs to access apps and data on the network via VPN

2
Identity authenticated with a simple mobile push

Identity assurance requested from SecurID

3
Access granted

About SecurID

SecurID, an RSA business, is the trusted identity platform for 13,000 organizations around the world, managing 50 million identities and providing secure, convenient access to 30 million users. SecurID empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, SecurID connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to **securid.com**.

SecurID™
An RSA Business