

Deepnet Unified Authentication for VPN Logon

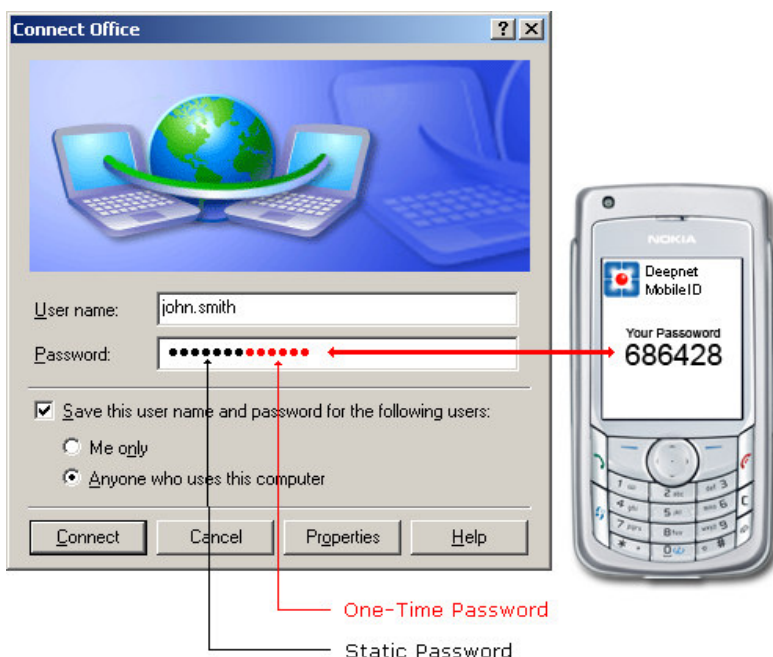
User Authentication is the weak link in VPN security. VPN technology, employing either the Secure Sockets Layer (SSL) or IP Security (IPSec) encryption protocol, is secure but only on the level of data transmission. VPNs typically verify users with only a static password, an approach that offers minimal security as passwords can be easily compromised. Strong user authentication is the only proven method for making VPN remote access secure. Deepnet Authentication for VPN Logon, utilizing one-time passwords generated by portable authentication tokens in a variety of form factors, offers the ultimate security for VPN remote access without compromising the user's experience.

Built-in RADIUS Server

Deepnet Unified Authentication Platform provides a built-in, RFC 2865 compliant RADIUS server. It supports any Network Access Server (NAS) or application that employs RADIUS authentication protocol.

No End-User Software

With Deepnet Authentication for VPN Logon the end-users do not need to install any new software. They will use the same VPN client as they're using now, and simply enter a one-time password or a combination of their static password and one-time password in the place where the password is required.



Multiple Choices of OTP tokens

Deepnet Unified Authentication Platform provides a variety of one-time password tokens, ranging from hardware tokens, software tokens, mobile tokens to USB tokens. These include:

Hardware Tokens

- SafeID
- GridID
- PocketID
- OATH-Compliant OTP tokens
- RSA SecurID

Software Tokens

- MobileID (Desktop)

Mobile Tokens

- MobileID
- QuickID

USB Tokens

- FlashID

Seamless VPN Integration

Deepnet Authentication for VPN integrates with any IPSec and SSL VPN that supports RADIUS, including :

- | | |
|--------------|-------------|
| • Cisco | • Aventail |
| • Nortel | • SonicWave |
| • Checkpoint | • AEP |
| • Juniper | • Whale |
| • WatchGuard | • F5 |