

ProSight Duo Two-factor Authentication

Single-click Two-Factor Authentication Solutions: Identity Validation and Device Trust for Secure Access to Applications



Progent's *ProSight Duo* family of managed services incorporates technology from Duo, a Cisco company, to offer two-factor authentication (2FA) for secure access to any application located anywhere, including Microsoft 365 and GSuite. 2FA, a key element of zero trust security, uses out-of-band ID validation to provide a layer of protection beyond passwords. This guards against the most common causes of security breaches like phishing, social engineering, brute-force password attacks, and stolen credentials. Duo's Mobile push technology saves time and hassle by allowing users to verify their identity simply by tapping the "Approve" button on their personal device.

Two-factor Authentication

80% of security breaches involve compromised passwords. All service offerings in Progent's *ProSight Duo* line of access security products can mitigate your reliance on passwords by supporting two-factor authentication. With 2FA, when you log into a protected online account and enter your password you are asked to verify your identity via a device that only you possess and that uses a different ("out-of-band") network channel. A broad range of devices can be used as this second form of authentication including a smart phone or watch, a hardware token, a landline phone, etc. You can register multiple verification devices.

Products Available with *ProSight Duo* Service Plans

Progent's *ProSight Duo* line of subscription-based managed service offerings consist of *ProSight Duo MFA*, *ProSight Duo Access*, and *ProSight Duo Beyond*. Progent's cybersecurity experts can help you determine which version of *ProSight Duo* is the best fit for your environment.

ProSight Duo MFA Features:

- Two-factor authentication with push, passcode or callback options
- Duo Mobile to push single-tap authentication for Android, iOS, Apple Watch
- Authentication via a Universal 2nd Factor (U2F) USB device or biometrics
- User self-enrollment and self-management
- Traditional 2FA via a passcode generated by a token, mobile device, or network administrator
- Cloud-based single sign-on (SSO) for all applications via an MFA-protected dashboard

ProSight Duo Access Features:

- All the features of *ProSight Duo*
- Unified Endpoint Visibility shows every networked device, not just managed devices
- Flag and track high-risk devices
- Duo Device Health application for laptops and desktops
- Health-based policy enforcement for laptops, desktops and mobile devices

ProSight Duo Beyond Features:

- All the features of *ProSight Duo MFA* and *ProSight Duo Access*
- Detection of corporate-owned vs. BYOD laptops, desktops and mobile devices
- Detection of third-party agents such as anti-virus running on devices
- Secure access to on-prem websites/apps and SSH servers without VPN credential management
- Verification of both user and device trust
- Limit mobile access to apps based on enrollment in mobile device management systems (MDMs)

Contact Progent About Two-factor Authentication and Endpoint Trust Solutions

For more information, call 800-993-9400 or send email to information@progent.com



FEATURES

- Two-factor authentication (2FA) for any app at any location.
- Single-tap authentication with iOS, Android, and Apple Watch
- Passcode authentication for hardware or software token, landline phone, etc.
- Support for U2F USB devices and biometrics
- Dashboard for visibility of all devices accessing applications
- Policy enforcement based on app, network, user group
- Policy enforcement based on laptop, desktop, mobile device
- Detection of corporate-owned vs. BYOD endpoints
- Secure access to on-premises websites and apps plus SSH servers without requiring VPN credential management

BENEFITS

- Make sure only authorized users and secure devices can access applications
- Save time and reduce hassle with single-tap authentication
- Build a strong foundation for a modern zero-trust environment
- Avoid damage resulting from compromised passwords or spoofed phone calls
- Continuous verification of user and device compliance
- Support for modern network models with cloud, on-prem, mobile, and hybrid access plus corporate and BYOD endpoints
- Enforce least-privileged access policies to comply with zero trust access security standards