FAQ
MFA-NG

Welche Systeme sind betroffen?

Die Aktualisierung betrifft Ihre Firewall-Systeme, die den sicheren Fernzugriff über Global Protect (VPN) ermöglichen. Konkret wird das Verfahren, mit dem Sie sich bei diesem Dienst authentifizieren, durch unsere neue, hochmoderne Lösung MFA-NG ersetzt. Dadurch profitieren Sie von einer **erhöhten Sicherheit** und einer **vereinfachten Verwaltung** Ihrer VPN-Verbindungen.

Es ändert sich nur das Authentifizierungsverfahren, die VPN-Einwahl (Global Protect Agent) bleibt dieselbe.

Welche Vorbereitung muss ich als Kunden auf meiner Seite treffen?

Um die neue MFA-NG Lösung zu bestellen, gehen Sie bitte wie folgt vor:

1. **Terminvereinbarung:**
   Buchen Sie einen kostenlosen Termin für die Umstellung.
2. **Ansprechpartner benennen:**
   Bitte benennen Sie einen Ansprechpartner in Ihrem Unternehmen, der den VAPS-Techniker während der Umstellung begleitet und zukünftig als Ansprechpartner für die MFA-NG Lösung fungiert. Dieser benötigt keine tiefgehenden IT-Kenntnisse.
3. **Umstellung**:
   Für die Umstellung benötigt der Ansprechpartner ein Smartphone, auf dem eine entsprechende App installiert werden kann. Nach erfolgreicher Umstellung sollte der Ansprechpartner die Möglichkeit haben, die VPN-Einwahl zu testen, um sicherzustellen, dass alles wie erwartet funktioniert.

Was muss ich während der Umstellung beachten?

Die Umstellung auf die neue MFA-NG Lösung erfolgt für Sie vollkommen transparent. Dank des „in-place updates“ wird die bestehende Authentifizierungsmethode nahtlos durch die neue ersetzt.

- **Keine Unterbrechung:**
  Sie und Ihre Mitarbeiter müssen sich während der Umstellung nicht aus dem VPN abmelden. Die Verbindung bleibt bestehen.
- **Sofortiger Wechsel:**
  Ab dem Zeitpunkt der Umstellung wird bei der nächsten Anmeldung die neue Authentifizierungsmethode verwendet.
- **Keine lästige Verteilung von Zugangsdaten:**
  Es ist keine Verteilung von Zugangsdaten notwendig. Alle Benutzer können sich selbstständig registrieren und die neue Authentifizierung danach benutzen.
- **Ein Ansprechpartner:**
  Wir benötigen lediglich einen Ansprechpartner auf Ihrer Seite, um die Umstellung durchzuführen.

Wichtig: Bitte beachten Sie, dass Sie sich nach der Umstellung bei der nächsten Anmeldung mit Ihren neuen Zugangsdaten authentifizieren müssen.

FAQ
MFA-NG

Was ändert sich bei der Anmeldung?

Mit der neuen MFA-NG Lösung haben Sie mehr Flexibilität bei der Authentifizierung. Sie können zwischen folgenden Optionen wählen:

Option 1: Einfache Anmeldung mit Ihrem Gerät

- **Windows:**
  Nutzen Sie die bereits bekannte Windows Hello oder Windows Hello for Business (WHFB) Funktion.
- **Andere Betriebssysteme:**
  Äquivalente Funktionen anderer Betriebssysteme können ebenfalls genutzt werden.
- **Vorteil:**
  Schnell und bequem, da keine zusätzlichen Geräte erforderlich sind.

Option 2: Authentifizierung mit der AuthN App

- **QR-Code Scan:**
  Scannen Sie einfach den QR-Code auf Ihrem Bildschirm mit der AuthN App.
- **Push-Benachrichtigung:**
  Bestätigen Sie die Anmeldung direkt auf Ihrem Smartphone.
- **Vorteil:**
  Wenn Sie noch kein Windows Hello einsetzen, haben Sie eine bequeme Alternative der Authentifizierung.

Im Vergleich zur alten OTP-Lösung mit MobilPass oder Hardware-Token entfällt das manuelle Eingeben von Codes. Die neue Lösung ist somit nicht nur sicherer, sondern auch komfortabler.

Kann ich meine alten Hardware oder Software Token weiter nutzen?

Nein, leider können Sie Ihre alten Hardware- oder Software-Token nicht mehr für die neue MFA-NG Lösung verwenden. Diese waren **speziell für die alte Authentifizierungsmethode** konzipiert.

Die MFA-NG Lösung bietet Ihnen folgende Vorteile:

- **Mehr Komfort:**
  Sie benötigen kein zusätzliches Gerät wie einen Token.
- **Höhere Sicherheit:**
  Durch die Nutzung von Windows Hello oder vergleichbaren Funktionen wird die Sicherheit Ihres Zugriffs deutlich erhöht.
- **Zukunftsfähigkeit:**
  Die MFA-NG Lösung ist auf dem neuesten Stand der Technik und bietet langfristige Sicherheit.

Wir empfehlen Ihnen dringend, auf die neuen Authentifizierungsmethoden umzusteigen.

Zusätzliche Hinweise:

- **Token-Rückgabe:**
  Geben Sie Ihre alten Token bitte entsprechend den Sicherheitsrichtlinien Ihres Unternehmens zurück.
- **TPM-Chip:**
  Für die Nutzung von Windows Hello oder vergleichbaren Funktionen ist ein **Trusted Platform Module (TPM)** Chip in Ihrem Computer erforderlich. Dieser Chip dient zur sicheren Speicherung von kryptografischen Schlüsseln und ist in modernen Geräten (seit 2016) bereits integriert.

FAQ
MFA-NG

Gibt es auch Hardware Token?

Nein, für die neue MFA-NG Lösung benötigen Sie **keine zusätzlichen Hardware-Token** mehr. Wir haben uns entschieden, auf eine rein **softwarebasierte Lösung** umzustellen, um Ihnen mehr Komfort und Flexibilität zu bieten.

Die Vorteile der neuen Lösung:

- **Keine zusätzliche Hardware:**
  Sie brauchen keinen weiteren physischen Token mehr.
- **Höhere Sicherheit:**
  Die neue Lösung basiert auf den neuesten Sicherheitsstandards und bietet einen robusten Schutz.
- **Mehr Komfort:**
  Die Authentifizierung erfolgt direkt über Ihr Gerät, ohne dass Sie zusätzliche Schritte durchführen müssen.

Warum keine Hardware-Token mehr?

Hardware-Token können verloren gehen oder beschädigt werden. Die neue softwarebasierte Lösung ist **sicherer und einfacher zu verwalten**.

FAQ
MFA-NG

Warum die Umstellung auf unsere neue MFA-NG Lösung sinnvoll ist?

Sie möchten Ihre Unternehmensdaten bestmöglich schützen und gleichzeitig die Arbeit Ihrer Mitarbeiter erleichtern? Dann ist unsere neue MFA-NG Lösung die perfekte Wahl für Sie.

Reduzierung der Angriffsoberfläche:
Stoppen Sie 68% aller Angriffe auf Ihr Unternehmen!

Laut dem aktuellen Verizon Data Breach Report*1 sind 68% aller Cyberangriffe auf gestohlene Zugangsdaten zu- rückzuführen. Mit unserer neuen MFA-Lösung schützen Sie sich effektiv vor diesen Bedrohungen. Durch die Nutzung modernster Authentifizierungsprotokolle sind Sie bestens gerüstet für die Herausforderungen der digitalen Welt.

Zu denen folgende zählen:

- **Nutzung von Cloud Anwendungen**
- **Compliance Anforderung durch Cyber-Versicherungen**
- **Schutz vor Passwort-Phishing**

Beispiel wie MFA gehackt wird:
https://www.youtube.com/watch?v=5rUbRJqUCpE
(Englisch)

*1 https://www.verizon.com/business/de-de/resources/reports/dbir/

Sparen Sie wertvolle Zeit und Ressourcen:

Mit unserer neuen Lösung entfällt der gesamte Verwaltungsaufwand für physische Token. Keine verlorenen oder beschädigten Geräte mehr, die zu zeitaufwendigen Ersatzbestellungen führen. Ihre IT-Abteilung kann sich auf wichtigere Aufgaben konzentrieren, während sich Ihre Mitarbeiter unkompliziert anmelden. Die Zeiten des lästigen Resyncs der Token sind vorbei, **die MFA-NG Lösung benötigt keine Resyncs mehr**.

Weniger Geräte, mehr Komfort:

Mit unserer neuen Lösung benötigen Sie keine zusätzlichen Hardware-Geräte wie Smartphones. Einfach mit einem Gerät anmelden und loslegen!

Sichern Sie Ihre VPN-Einwahl:

Die Zeiten ändern sich, und auch die Anforderungen an IT-Sicherheit steigen kontinuierlich. So wird die alte Lösung in Zukunft nicht mehr unterstützt werden. Wodurch Ihre Mitarbeiter plötzlich keinen Zugriff mehr auf Ihr VPN haben werden. Um diesem Risiko zu entkommen, entscheiden Sie sich heute schon für eine zukunftssichere Lösung und vermeiden Unterbrechungen in Ihrem VPN-Zugangs-Dienst.