USA & APAC Office
Irvine
Swivel Secure, Inc.
1340 Reynolds Ave. #116-285
Irvine, CA 92614

+1 949 480 3626 (Pazifische Zeitzone)
Gebührenfrei: 866.963.AUTH (2884)
usa@swivelsecure.com

UK & Ireland Offices
Norden
1200 Century Way
Thorpe Park
Leeds
LS15 8ZA

HQ: +44 (0)1134 860 123
Support: +44 (0)1134 860 111
hq@swivelsecure.com

EMEA Offices
Portugal
Estrada de Alfragide,
N.º 67, Alfrapark – Lote H, Piso 0,
2614-519 Amadora

+351 215 851 487
portugal@swivelsecure.com

Spanien
Calle Punto Mobi, 4,
28805 Alcalá de Henares,
Madrid, Spain

+34 911 571 103
espana@swivelsecure.com

AuthControl Sentry®

Schutz von Identitäten durch intelligente Authentifizierung

Mit der PINsafe® Technologie im Mittelpunkt für ultimative Sicherheit und risikobasierte Authentifizierung mit dynamischer Steuerung, bietet die preisgekrönte AuthControl Sentry® eine intelligente Multi-Faktor-Authentifizierungslösung für Unternehmen.

swivelsecure

www.swivelsecure.com

swivelsecure

AuthControl Sentry® Intelligente Multi-Faktor-Authentifizierung

In über 54 Ländern eingesetzt, in Unternehmen einschließlich Finanzwesen, Regierung, Gesundheitsversorgung, Bildung und Manufraktur. AuthControl Sentry® bietet Organisationen mit echter Multi-Faktor-Authentifizierung, eine intelligente Lösung zur Verhinderung unautorisierter Zugriffe auf Anwendungen und Daten.

Erfassen Sie den QR-Code, um das gesamte Diagramm von AuthControl Sentry® zu sehen, die vollständige Multi-Faktor-Authentifizierung Stakeholder-Lösung.

AuthControl Sentry® hat die Flexibilität eine Reihe architektonischer Anforderungen zu unterstützen und die Fähigkeit, eine maximale Adoption mit einer großen Auswahl an Authentifizierungsfaktoren zu gewährleisten. Ob Nutzung der mobilen Anwendung oder der neuesten Biometrie über den Fingerabdruckleser, etabliert sich AuthControl Sentry® als führende Lösung in Computer- und Netzsicherheit.

Was macht es anders

- Patentierte PINsafe®-Technologie für ultimative sicherheit – siehe Seite 8
- Unterstützt On-Premise und Cloud für alle Architekturen
- Eine einzelne Pacht und eine einzelne mehrstufige Cloud Lösung, sorgt für eine optimierte Individualisierung und Kontrolle
- Risikobasierte Authentifizierung und Single sign-on als standard
- Integriert sich nahtlos in hunderte von Anwendungen
- Gewährleistet maximale Adoption durch ein umfangreiches Angebot an Authentifizierungs-methoden - bis zu zehn Faktoren!

Authentifizieren des Zugriffs für alle Stakeholder, egal ob durch Einloggen auf Office 365, eCommerce oder durch Zugriff auf Ihr ERP zur Bestandskontrolle.

- ✓ Mitarbeiter
- ✓ Kunden
- ✓ Lieferanten

Architektur

Unterstützt on-premise und Cloud für veränderbare Architektur

Es gibt keine Einschränkungen mit AuthControl Sentry®. Es wurde, um den Zugriff auf Anwendungen zu authentifizieren, unabhängig davon, ob sie in der Cloud oder on-premise gehostet sind und unabhängig davon, ob es sich beim Benutzer um einen Kunden, einen Mitarbeiter oder um eine Zugangsanfrage eines Lieferanten handelt.

On-premise Architektur

Zugriff auf interne Systeme über unseren Active Directory Agenten, eine lokal installierte Softwareanwendung, die die Notwendigkeit beseitigt, Ihre Active Directory über das Internet teilen zu müssen, während Ihre Benutzerkonten-Synchronisierung jedoch erhalten bleibt.

Cloud-basierte Architektur

Eine feste IP: Jeder AuthControl Kunde erhält eine für Ihn dedizierte, feste IP für seine eigenen virtuellen Angelegenheiten. Es gibt keine freigegebene Ressource, keine freigegebene Anwendungsprogrammierschnittstelle und kein freigegebenes Eingangsportal oder freigegebene Datenbank.

Ein spezielles Angebot: AuthControl Cloud stellt Ihnen eine dedizierte virtuelle Maschine bereit. Es gibt keine mehrinstanzenfähigen Optionen, sodass totales Management und Kontrolle gewährleistet werden kann. Das bedeutet, dass Sie die Flexibilität haben, die Lösung so zu konfigurieren, dass sie Ihren anspruchsvollen Bedürfnissen gerecht werden.

Eine private Firewall: Wir bieten engagierte und unabhängige Firewalls für jeden Kunden, maßgeschneiderte Sicherheits- und Zugriffskontrolllisten.

Funktionen

swivelsecure

Einmaliges Anmelden als standard

SSO-Funktionalität (Single Sign-On) für AuthControl Sentry® ist eine Funktion, die Benutzern die Möglichkeit bietet, mit einem einzigen Authentifizierungsprozess auf alle Ihre Anwendungen zuzugreifen und sicherzustellen, dass die Arbeit der Benutzer effizient ist, ohne Kompromisse bezüglich der Sicherheit einzugehen.

Kontinuierliche Sicherheit

Swivel Secure bietet ein Unifi ed Portal zum reibungslosen Zugriff für Ihre Benutzer. Durch die Verwendung dieser Single Point of Access können die Berechtigungen der Benutzer verwaltet und verfolgt werden; für Prüfungszwecke, für die Verbesserung der Sicherheit und der Rechenschaftspflicht.

Kostengünstig

Erhebliche Einsparungen können durch SSO erzielt werden, indem die Notwendigkeit für passwortbezogene Anrufe an IT-Support-Desks ausgelöscht werden. Die Produktivität steigt, wenn sich der Benutzer an einem Punkt anmeldet, um auf alle Anwendungen zuzugreifen – Zeitersparnis

Intuitiv

SSO wurde entwickelt, um die Effizienz zu steigern, indem Benutzern der Zugriff auf alle Seine Anwendungen mit einer einzigen erfolgreichen Authentifizierung, das risikobasierte Policy-Engine gewährleistet wird. Ob Benutzer über ein VPN auf Anwendungen zugreifen, on-premise oder Cloud, werden sie automatisch zur Authentifizierung mit dem intuitiven SSO Funktionalität innerhalb des Unified Portals geleitet

Bereitstellen von AuthControl Sentry® für authentifizierung:

- Stakeholders - Mitarbeiter, Lieferanten, und Kunden
- Zugriff auf Anwendungen wie Office365, Salesforce oder SAP
- Ein spezifischer vertikaler Markt wie der des Finanzwesens

Eigenschaften

Risikobasierte Authentifizierung als standard

Die risikobasierte Authentifizierung (RISK-based Authentication, RBA) ist ein dynamisches Merkmal von AuthControl Sentry®; entwickelt, um automatisch den entsprechenden Grad der Authentifizierung für den Zugriff auf Anwendungen einzuschätzen. Basierend auf Parameter, die im Policy-Engine festgelegt sind, wird RBA die Anfrage der entsprechenden Authentifizierungsebene anfordern, um auf Anwendungen zuzugreifen, basierend auf dem Benutzer, deren Gerät und Anwendung.

Dynamisch & intelligent

Passt sich den Umständen des Benutzers an, einschließlich:

- Welche Anwendungen versucht wird zuzugreifen.
- Welche Gruppenmitgliedschaft sie haben
- Von wo sie auf die Anwendungen zugreifen
- Welches Gerät Sie verwenden

Das Policy-Engine

Basierend auf ein Punktesystem erlaubt das Authentifizierungsrichtlinienmodul Administratoren Parameter pro Benutzer, pro Anwendung zu setzen.

- Gruppenmitgliedschaft
- Anwendung, auf die zugegriffen wird
- IP-Adresse
- Letzte Authentifizierung
- X.509 Cert
- Gerät
- Physischer Standort (GeoIP)
- Geo-Geschwindigkeit

Risikobasierte Authentifizierung: Beispiel 1

Der Einkaufsassistent ist zu einem Lieferanten nach Südostasien geflogen. Sie hat gerade eine Mahlzeit in einem Restaurant beendet und merkt, dass sie vergessen hat, den Bestand kommender Komponenten für ein Meeting am nächsten Tag zu überprüfen. Während sie auf das Taxi wartete, dachte sie, dass sie sich schnell mit ihrem von der Firma bereitgestellten mobilen Endgerät in das ERP-System einloggen würde.

ERP-system	
Benötigt 120 Punkte	
LAN	0
Bekannte IP	0
Verwaltetes Gerät	50
IP-Bereich (Asien)	-100
Authentifizierung erforderlich	
U&P	10
Mobile App	60
Fingerabdruck	20

Ergebnis – erfolglos

Obwohl sie versucht, ein von einem Unternehmen ausgestelltes Gerät für den Zugriff auf das ERP zu verwenden, setzt der IP-Bereich aufgrund ihres Standorts 100 Punkte zurück. Diesmal wird ihr kein Zugriff auf das ERP gewährt, unabhängig von ihrer Bereitschaft, die Multi-Faktor-Authentifizierung zu verwenden.

Risikobasiert Authentifizierung: Beispiel 2

Der Sales Manager arbeitet heute im Büro und möchte auf das CRM zugreifen, um die Möglichkeit zu erstellen, an einem Meeting teil zu nehmen. Er verwendet seinen von der Firma gelieferten Laptop und greift auf die Anwendung zu, die sich vor Ort befindet.

CRM-system	
Benötigt 120 Punkte	
LAN	50
Bekannte IP	50
Verwaltetes Gerät	50
IP-Bereich (Deutschland)	50
Authentifizierung erforderlich	
U&P	10
Mobile App	60
Fingerabdruck	20

Ergebnis – erfolgreich

Der Sales Manager übertrifft deutlich die Punkte, die er für den Zugriff auf das CRM benötigt. Nach der Authentifizierung kann er mit Single Sign-On (SSO) auf andere Anwendungen zugreifen. Er erhält einen Anruf vom Einkaufsassistenten, kann auf das ERP-System zugreifen und gibt die Menge mit der Teilenummer an, die er erhält.

Ultimative Flexibilität & Kontrolle

Das Richtlinienmodul erlaubt Ihnen neue Regeln und bestehende Regeln zu kombinieren, sowie das Bereitstellen eines Mechanismus, welcher eine Reihe von Szenarien mit zunehmender Komplexität zu unterstützt.

Eigenschaften

Benutzerportal

Das Benutzerportal ist ein Feature von AuthControl Sentry®, entwickelt um Administratoren mit einer konfigurierbaren Lösung, Autonomie an die Benutzer zu liefern und grundlegende Selbstverwaltungsaufgaben zur Verfügung zu stellen.

Das Benutzerportal gibt Administratoren die Möglichkeit, Benutzern direkten Zugang zu gewähren, durch: Regelmäßige Anforderungen wie das Ändern oder Zurücksetzen eines PIN oder das Bereitstellen der mobilen App.

Bereitstellung der mobilen App

Außerdem können Benutzer ihren PIN ändern und zurücksetzen. Auch mit der mobilen App kann dies mühelos vorgenommen werden. Eine E-Mail wird an den Benutzer gesendet, in der die Schritte zur Bereitstellung der mobilen App und einen QR Code für die Konfiguration angegeben werden. Nach der Bereitstellung können Benutzer auf alle regulären Anwendungen zugreifen mit: - Dem Einmalcode (OTC) oder - PUSH-Benachrichtigung

Self-service

Das Self-Service-Benutzerportal reduziert alle Kosten, die in der Regel durch Bereitstellung des Supports anfallen, um diese Aktionen durchzuführen

Mehr Effizienz

Das Benutzerportal von Swivel Secure wurde entwickelt, um Benutzern eine höhere Effizienz bei der Ausführung grundlegender Anforderungen zu bieten, darunter:

- Ändern des PIN
- Zurücksetzen des PIN
- Bereitstellung mobiler Apps
- Hardware token Resynchronisierung.

Es können Einschränkungen eingesetzt werden, um sicherzustellen, dass einige Überwachungsmaßnahmen stattfinden und um sicherzustellen, dass die Aktionen mit den Sicherheitsprotokollen in Einklang stehen.

Technologie

swivelsecure

PINsafe® patentierte technologie

PINsafe® ist die patentierte Technologie hinter den Bildauthentifizierungsfaktoren PINpad®, PICpad und TURing, welche Teil einer Serie von Authentifizierungsfaktoren sind, die mit AuthControl Sentry®, der Multi-Faktor-Authentifizierungslösung zum Schutz von Authentifizierungsfaktoren zur Verfügung stehen. Somit wird Organisationen der Schutz ihrer Anwendungen, Netzwerke und Daten vor nicht autorisierten Zugriffen gewährleistet.

Wie funktioniert PINsafe®?

Jeder Benutzer erhält eine PIN-Nummer. Dieser spezifische PIN wird jedoch nie eingegeben.

Wenn sich ein Benutzer sicher authentifizieren muss, wird er eine 10-stellige Sicherheitsz-eichenfolge gesendet – eine zufällige Reihe an Zeichen oder Zahlen. Die Sicherheitszeichenfolge kann als Grafik (TURing, PINpad® oder PICpad) angezeigt oder per E-Mail oder per SMS-Überprüfung gesendet werden.

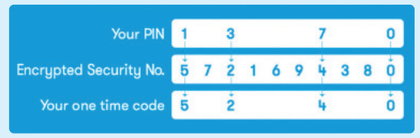
Durch die Verwendung des PIN als Positionsindikator kann ein einmaliger Code für die Authentifizierung extrahiert werden.

Können Sie mir ein Beispiel zeigen?

Das folgende Beispiel zeigt, dass Ihre PIN 1370 ist. Bei dieser Gelegenheit ist die Sicherheitszeichenfolge 5721694380, so dass Ihr Login-Code 5240 ist.

Die Sicherheitszeichenfolge kann in viele Geräte und Anwendungen integriert werden und das auf vielfältige Weise für Flexibilität. einschließlich:

- Anmelden bei Windows
- Remote-Zugriff mit F5, Citrix Netscaler und Cisco VPN
- Webzugriff mit OWA, Apache und Microsoft ILS



Da PINsafe® verhindert, dass der Benutzer jemals seine PIN eingeben muss, verhindert es jegliche Infiltration, wie z. B. Man-in-the-middle-Angriffe.

Faktoren

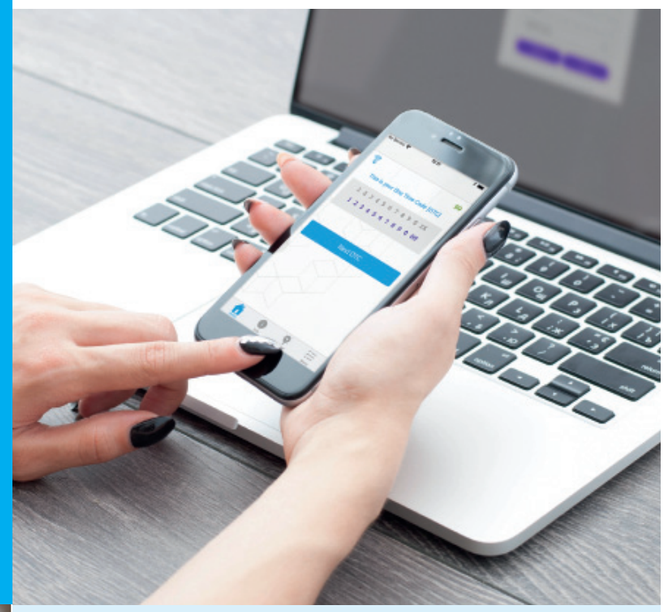
Authentifizierungsfaktoren

Swivel Secure bietet eine umfangreiche Palette von Authentifizierungsfaktoren, um sicherzustellen, dass jede Bereitstellung eine maximale Adoption in Ihrem gesamten Unternehmen bietet.

Ganz gleich, ob Sie sich für die Authentifizierung mit dem OTC in der mobilen App AuthControl Mobile® für ein herkömmliches Hardware-Token oder sogar Ihr Fingerabdruck entscheiden, den Ihnen AuthControl Sentry® von Swivel Secure bereitstellt, Ihren Unternehmen wird ultimative Sicherheit und Konfigurierbarkeit der Sicherheitsanforderungen geboten.

AuthControl Mobile®: OTC

Jedes Mal, wenn Sie aufgefordert werden, sich zu authentifizieren, verwenden Sie einfach die OTC, die in der App angezeigt wird. Da es 99 Codes gibt, ist die OTC-Funktion vielseitig genug, um offline verwendet zu werden. Sobald der Code eingegeben wurde, erhalten Sie Zugriff auf Ihre Anwendung.



Bildfaktor: PINpad®

Ein 10-stelliger Code wird in Form eines Zahlenrasters im Webbrowser des Benutzers angezeigt.

Der Benutzer klickt dann einfach auf die Bilder, die seine PIN darstellen. Jedes angeklickte Bild überträgt dann einen anderen TC-Code an AuthControl Sentry®, um den Benutzer zu authentifizieren.

Bildfaktor: PICpad

PICpad ist ein Authentifizierungsfaktor, der über die üblichen Optionen der Sprachdiversifizierung von Mitarbeitern und Kunden hinausgeht.

Mit den gleichen Prinzipien wie PINpad® zeigt PICpad Symbole anstelle von Zahlen an, was in multinationalen Umgebungen eine kohärente Bedeutung bietet.

AuthControl Mobile®: PUSH

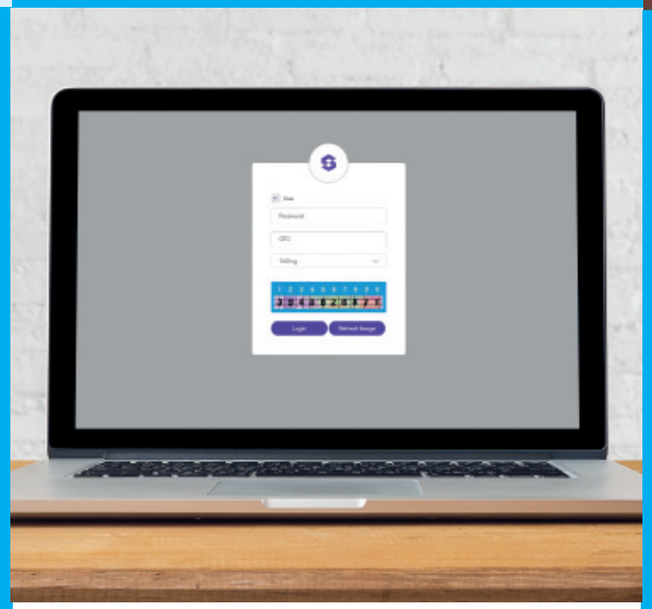
Einfach durch Drücken einer Taste in der mobilen App können Sie die Authentifizierung mit der Benachrichtigung bestätigen, die direkt an Ihr Handy gesendet wird.

Stellen Sie die Swivel One Touch®-Funktionalität schnell bereit, da eine minimale Konfiguration erforderlich ist.

Bildfaktor: TURing

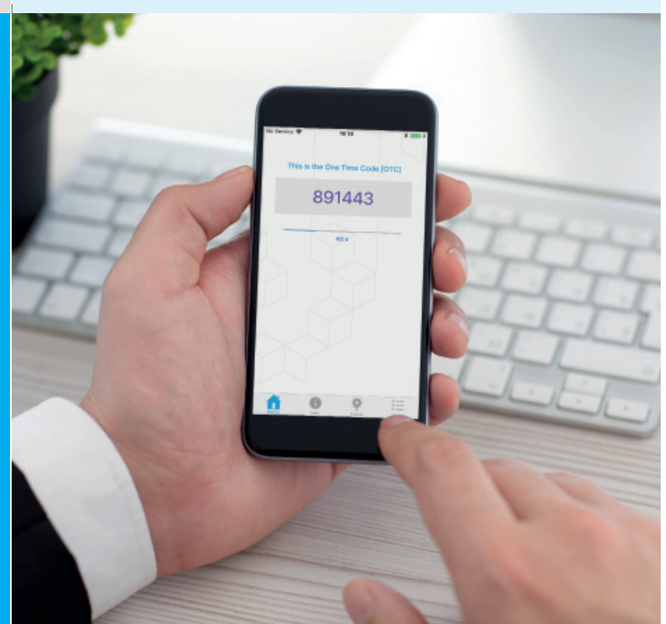
Ein 10-stelliger Code wird in Form eines rechteckigen Bildes im Webbrowser des Benutzers angezeigt. Der Benutzer nimmt dann die Zahlen, aus welche sein PIN besteht.

Beispiel: Wenn ihr PIN 1370 ist, dann nehmen sie einfach das 1., 3., 7. und 10. Zeichen aus dem dargestellten Bild.



AuthControl Mobile®: OATH

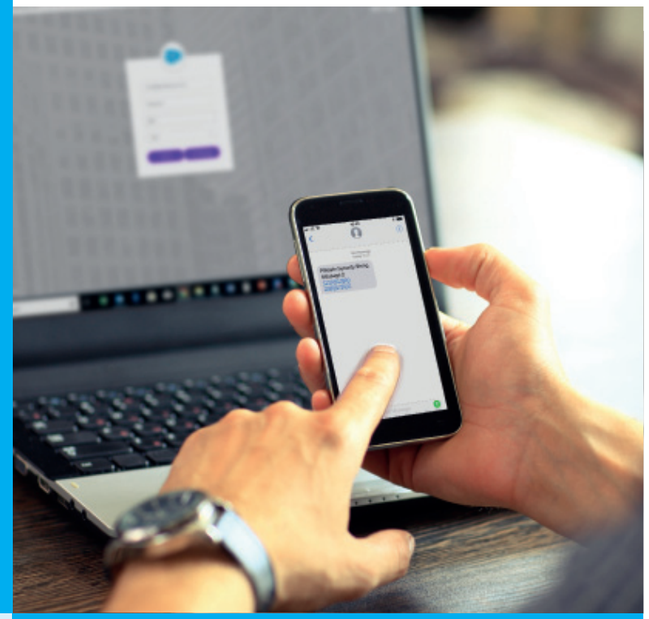
Das OATH-Softtoken ist ein zeitbasiertes Token, das von 0 bis 60 gezählt wird, ähnlich dem herkömmlichen Hardwaretoken, auf dem über das VPN auf Anwendungen zugegriffen werde kann. Das OATH-kompatible Softtoken stellt dem Benutzer einen sechsstelligen Code zur Authentifizierung zur Verfügung.



Mobil: SMS

Um die OTC (über SMS) vor betrügerischem Abfangen zu schützen, ist die SMS durch PINsafe® geschützt.

Dies bedeutet, dass die SMS eine Sicherheitszeichenfolge von zwei alphanumerischen Sequenzen enthält und in Kombination mit dem PIN des Benutzers ihren OTC bereitstellt.



Biometrie: Fingerabdruck

Die Fingerabdruckerkennung ist für AuthControl-Credential® Anbieter verfügbar, welche das biometrische Windows 10-Framework und den NITGEN-Fingerabdruckzugriffscontroller verwenden.

Benutzer können sich mit dem NITGEN-Fingerabdruckcontroller oder ihrem eingebetteten Fingerabdruckleser in ihrem Laptop authentifizieren.

AuthControl Voice

Durch Anrufen des Benutzers erkennt AuthControl Voice die Stimme entweder durch einen einmaligen Code (OTC) oder einer eine PUSH-Benachrichtigung (JA oder NEIN) zur Authentifizierung des Zugriffs auf

Anwendungen. Der über das Telefon gesprochene OTC wird dann auf Wunsch ins Fenster eingegeben.

Hardwaretoken

Das Hardwaretoken bietet Benutzern einen einmaligen Code (OTC), damit diese sicher auf Ihre Anwendung zugreifen können.

Jedes Mal, wenn die Taste auf Ihrem Hardware-Token gedrückt wird, wird ein neuer Code zur Verfügung gestellt, um sicherzustellen, dass unbefugter Zugriff verhindert wird.

swivelsecure

Integrationen

AuthControl Sentry® ist eine der flexibelsten Lösungen auf dem Markt und integriert sich mit hunderten von Anwendungen und Appliance-Software über RADIUS, ADFS, SAML und unsere eigene proprietäre API – AgentXML.

Ganz gleich, ob Sie auf Salesforce zugreifen, sich mit der mobilen App authentifizieren oder sich über einen Bildauthentifikator bei Windows Credential Provider anmelden müssen; AuthControl Sentry® unterstützt eine breite Palette von Anwendungen und Geräten und bietet so die Flexibilität und Effizienz, die für eine reibungslose Authentifizierung im gesamten Unternehmen erforderlich ist.

Lizenzierung

Flexible Lizenzpläne und Preismodelle, für alle Organisationen geeignet. Die Lizenz wird auf Basis eines bestimmten Benutzers berechnet.

Benutzerlizenzierung

Flexible Lizenzpläne und Preismodelle, für alle Organisationen geeignet.

- Lizenzen für AuthControl Sentry® sind pro Benutzer
- Jede Lizenz beinhaltet ALLE Authentifizierungsfaktoren
- MFA, SSO & RBA sind in AuthControl Sentry enthalten®
- Erhältlich als 1, 3, 5 oder 7 Jahre oder mit unbefristeten Laufzeiten

On-Premise

Eine unbefristete Lizenz ist für lokale Lösungen oder solche verfügbar, die in einer privaten Cloud gehostet werden. Die Preise sind pro Benutzer, auf einer gleitenden Skala, beginnend mit 10 Benutzern. Die Preise sind kumulativ, daher ist es eine äußerst kostengünstige Möglichkeit, ein Volumen von Lizenzen zu kaufen, anstatt ein gestaffeltes Modell. Ideal und geeignet für Organisationen, die die Kosten eines Dienstes im Voraus CAPEX und mit stabilen Nutzerzahlen wollen.

Cloud

Die Abonnementlizenzierung ist für Cloud-Bereitstellungen verfügbar und ermöglicht es Organisationen, ihre Benutzeranforderungen, wenn sich die Anforderungen ändern, zu erfüllen. Keine Vorabkosten und mit einem flexiblen und straffreien Vertrag und Kündigung. Ideal und geeignet für Organisationen, die die Kosten eines Dienstes OPEX und mit variablen Benutzernummern wollen.

Lizenzierungsoptionen

Verwenden Sie die folgende Tabelle, um Optionen für die lokale und Cloud-Lizenzierung zu vergleichen.

Art der Lizenz	On-Premise	Cloud
Risikobasierte Authentifizierung	✓	✓
Integrationen (SAML/ADFS/RADIUS)	✓	✓
On-Premise- & Cloud-Anwendungen	✓	✓
Alle Authentifizierungsfaktoren	✓	✓
AD Agent & AD Sync	✓	✓
Einheitliches Portal mit Single sign-on	✓	✓
Reporting	✓	✓
Appliance (physisch/virtuell)	✓	✗
Amazon AWS-Image	✗	✓
24x7x365	Optional	✓

Service & Support

Um sicherzustellen, dass Unternehmen Zugang zu technischem Support und den neuesten Funktionen haben, bieten wir Benutzern Standard- und Premium-Support für unsere Authentifizierungsplattform an. Professionelle Dienste sind auch für Upgrades, Bereitstellung, Migration und komplexe Integration verfügbar.

Einstiegslevel Wartungsvertrag

Support-Stunden: 8/5. Zugriff auf Software-Upgrades, Updates und Fehlerbehebungen.

Standard Wartungsvertrag

Support-Stunden: 24/5. Swivel Secure bietet standardmäßig 24 Stunden Support an Werktagen an.

Premium Wartungsvertrag

Support-Stunden: Ein echter 24/7-Service, ideal für Unternehmen, die sofort kompetente Unterstützung benötigen.

Professionelle Dienstleistungen

Swivel Secure bietet eine Reihe professioneller Dienste für Organisationen, die zusätzliche oder maßgeschneiderte technische Ressourcen bei der Bereitstellung der mehrstufigen Authentifizierung und der Sicherstellung der Kompatibilität mit Systemen, Verbindungen und Hardware einschließt.

Technischer Account Manager (TAM)-Dienst

Unser TAM-Service bietet proaktive Beratung und zentralisiertes Service-Management, um sicherzustellen, dass Sie von der bevorzugten Handhabung innerhalb jedes Support-Kanals profitieren.

Möchten Sie Ihre Swivel Secure-Appliance aktualisieren?

Swivel Secure erkennt einige der Probleme, die während eines Upgrades auftreten können, und bietet einen Upgrade-Service an, der entwickelt wurde, um sicherzustellen, dass der Service und Ihr Unternehmen nur minimal gestört werden.

Verfügen Sie über eine hochkomplexe Netzwerkinfrastruktur, die zahlreiche Integrationen erfordert?

Unser Team von erfahrenen Ingenieuren arbeitet eng mit Ihren technischen Architekten und Service-Lieferungs Teams zusammen, um sicherzustellen:

- Jeder vorgeschlagene Entwurf ist auf Ihre Netzwerkarchitektur zugeschnitten
- Das Design erfüllt Ihre organisatorischen, architektonischen und Änderungs-Kontrollanforderungen

Möchten Sie ein neues RADIUS- oder SAML-Gerät ohne vorherigen Integrationsartikel integrieren, um dagegen zu arbeiten?

Unser Team von Software-Entwicklern kann zur Verfügung stehen, um:

- Bewerten und Entwickeln neuer Integrationen
- Neue Plugins erleichtern
- Reagieren Sie auf Feature-Anforderungen, um die Software kontinuierlich zu verbessern.