Uffici Regno Unito & Irlanda
Nord
1200 Century Way
Thorpe Park
Leeds
LS15 8ZA

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

Sud
Pinewood
Chineham Business Park
Chineham, Basingstoke
RG24 8AL

USA & APAC Office
Seattle
Swivel Secure, Inc.
1001 4th Ave #3200
Seattle, WA 98154

+1 949 480 3626 (Tempo Pacifico)
Numero verde: 866.963.AUTH (2884)
usa@swivelsecure.com

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

+351 215 851 487
portugal@swivelsecure.com

Spagna
Calle Punto Mobi 4,
28805 Alcala de Henares
Madrid

+34 911 571 103
espana@swivelsecure.com

AuthControl Sentry®

Protezione delle identità con l'autenticazione intelligente

Con la tecnologia PINsafe® al centro per massima sicurezza e l'autenticazione basata sul rischio fornisce un controllo dinamico con il pluripremiato AuthControl Sentry®, che offre una soluzione intelligente di autenticazione a più fattori per le aziende.

swivelsecure

www.swivelsecure.com

AuthControl Sentry® l'autenticazione intelligente a più fattori

Distribuito in oltre 52 pæsi ed implementato in tantissime imprese, tra cui la finanza, il governo, il sistema sanitario, nel settore di educazione e produzione. AuthControl Sentry® fornisce per organizzazioni con una vera autenticazione a più fattori, una soluzione intelligente per prevenire l'accesso non autorizzato ad applicazioni e dati.

AuthControl Sentry® ha la flessibilità per supportare una serie di requisiti architettonici e la capacità di garantire la massima adozione, con un'ampia scelta di diversi fattori di autenticazione. Utilizzando l'applicazione mobile oppure l'ultima biometria tramite il lettore fingerprint, AuthControl Sentry® è la soluzione per la sicurezza informatica.

Cattura il codice QR per visualizzare il diagramma intero di AuthControl Sentry®, l'autenticazione completa a più fattori e la soluzione stakeholder.

Cosa lo rende differente

- Tecnologia PINsafe® brevettata per massima sicurezza – vedi pagina 8
- Supporta on-premise e cloud per tutti tipi di architettura
- Con un'unica locazione e un'unica cloud a più livelli, garantisce un ottima personalizzazione e un ottimo controllo.
- Autenticazione basata sul rischio e single sign-on come standard
- Si integra perfettamente con centinaia di applicazioni
- Garantisce la massima adozione con una grande varietà di metodi d'autenticazione - fino a dieci fattori!

Autentica l'accesso per tutti stakeholder, se tramite il login a Office 365, eCommerce, o l'accesso al ERP per il controllo delle scorte.

✓ Dipendenti ✓ Clienti

✓ Fornitori

Architettura

Supporta on-premise e cloud per un'architettura modificabile

Non ci sono restrizioni con AuthControl Sentry®. È progettato per autenticare l'accesso alle applicazioni che sono ospitate nella cloud o on-premise, indipendentemente dal fattore se l'utente è un cliente, un dipendente o un fornitore che richiede l'accesso.

Architettura on-premise

Accedere ai sistemi interni tramite il nostro Agente Active Directory - un'applicazione software installata localmente, che elimina la necessità di condividere sua Active Directory tramite internet, pur mantenendo la sincronizzazione dell'account dell'utente.

Architettura basata su cloud

Un IP fisso: Ogni cliente AuthControl riceve un IP fisso, dedicato per le proprie istanze virtuali. Non c'è nessuna risorsa condivisa, nessun interfaccia di programmazione delle applicazioni e nessun portale d' ingresso o database condiviso.

Un'offerta specifica: AuthControl Cloud offre una macchina virtuale specifica. Non ci sono opzioni multi-tenant condivise, in modo da poter aspettarsi la gestione e il controllo totale; significa che hanno la flessibilità di configurare la soluzione per soddisfare le vostre esigenze.

Un firewall privato: Offriamo servizi firewall specifici e indipendenti per ogni cliente, dando la sicurezza adeguata e gli elenchi di controllo degli accessi su misura.

Caratteristiche

Single sign-on come standard

La funzionalità Single sign-on (SSO) per AuthControl Sentry® è una funzionalità che fornisce agli utenti la possibilità di accedere a tutte le loro applicazioni con un unico processo di autenticazione, garantendo che gli utenti lavorano in modo efficiente e senza compromettere sicurezza.

Sicurezza continua

Swivel Secure offre un Unifi ed Portal agli utenti per garantire l'accesso fluido. Utilizzando questo singolo punto di accesso, i privilegi degli utenti possono essere gestiti e il comportamento può essere monitorato con l'audit per migliorare la sicurezza e garantire la responsabilità.

Conveniente

Utilizzando il SSO è possibile di ottenere risparmi significativi. Ad esempio, la necessità di chiamate relative di password ai banchi di supporto ITche vengono sradicati. La produttività aumenta, dove gli utenti effettuano l'accesso a un punto per accedere a tutte le loro applicazioni– risparmio di tempo

Intuitivo

SSO è stato progettato per aumentare l'efficienza, consentendo agli utenti di accedere a tutte le loro applicazioni con un'unica autenticazione di successo, attraverso il Policy-Engine che è basato sul rischio. Se gli utenti stanno accedendo alle applicazioni tramite una VPN, on-premise o una cloud, verranno automaticamente inoltrati ad eseguire l'autenticazione utilizzando l'intuitivo SSO con la funzionalità all'interno del Unified Portal.

Distribuire AuthControl Sentry® per l' autenticazione:

- Stakeholder - dipendenti, fornitori e clienti
- Accesso ad applicazioni come Office 365, Salesforce o SAP
- Un mercato verticale e specifico, così come la società finanziaria

Caratteristiche

Autenticazione basata sul rischio come standard

L'autenticazione basata sul rischio (RBA, Risk-Based Authentication) è una funzionalità di AuthControl Sentry®, progettata per richiedere automaticamente il livello appropriato per accedere alle applicazioni. Basato su parametri impostati nel Policy Engine, il sistema RBA richiede il livello di autenticazione appropriato per accedere alle applicazioni in base all'utente, il suo dispositivo e l'applicazione.

Dinamico ed intelligente

Si adatta alle circostanze dell'utente, incluso:

- A quali applicazioni cercano di accedere
- Quale appartenenza al gruppo hanno
- Da dove accedono all'applicazione
- Quale dispositivo stanno utilizzando

Il policy-engine

Basato su un sistema a punti, il motore dei criteri di autenticazione consente agli amministratori di impostare i parametri per utente, per applicazione.

- Appartenenza al gruppo
- Applicazione a cui si accede
- Indirizzo IP
- Ultima autenticazione
- X.509 Cert.
- Dispositivo
- Posizione fisica (GeoIP)
- Velocità Geografica

Autenticazione basata sul rischio: Esempio 1

L'Assistente agli acquisti è arrivato in Asia sud-orientale per visitare un fornitore. Ha appena terminato un pasto in un ristorante e si rende conto che ha dimenticato di controllare la scorta di componenti per un incontro il giorno seguente. Mentre aspettava, pensava di fare il login al sistema ERP, usando suo dispositivo mobile aziendale

Sistema ERP	
Richiede 120 punti	
LAN	0
IP conosciuto	0
Dispositivo gestito	50
Intervallo IP (Asia)	-100
Autenticazione richiesta	
U&P	10
Mobile App	60
Impronta digitale	20

Risultato: senza successo
Anche provando ad utilizzare un dispositivo aziendale per accedere all'ERP, la gamma IP la riporta a -100 punti a causa della sua posizione. Questa volta non gli sarà concesso l'accesso all'ERP, indipendentemente dal suo desiderio di utilizzare l'autenticazione a più fattori.

Autenticazione basata sul rischio: Esempio 2

Il Sales Manager lavora oggi in ufficio e desidera di accedere al CRM per creare un'opportunità dopo una riunione. Con il suo laptop aziendale sta accedendo all'applicazione che si trova on-premise

Sistema CRM	
Richiede 120 punti	
LAN	50
IP conosciuto	50
Dispositivo gestito	50
Intervallo IP (Italia)	50
Autenticazione richiesta	
U&P	10
App per dispositivi mobili	60
Impronta digitale	20

Risultato: con successo
Il Sales Manager supera chiaramente i punti di cui ha bisogno per accedere al CRM. Una volta autenticato, può utilizzare il Single sign-on (SSO) per accedere anche ad altre applicazioni. Riceve una chiamata dall'assistente acquisti, è in grado di accedere al sistema ERP e fornisce la quantità con il numero di parte che gli viene assegnato.

Massima flessibilità e controllo

Il Policy engine consente di creare nuove regole e combinare norme già esistenti. Oltre di questo fornisce un meccanismo per supportare una serie di scenari con una complessità crescente.

Caratteristiche

Portale utente

Il portale utente è una funzionalità di AuthControl Sentry®, progettato per fornire agli amministratori una soluzione configurabile per garantire l'autonomia agli utenti per le attività basate all' auto-amministrazione.

Il portale utente fornisce agli amministratori la capacità di consentire agli utenti l'accesso diretto di: Eseguire requisiti regolari come la modifica o reimpostazione di un PIN o di dare a disposizione l'app mobile.

Dare a disposizione l'app mobile

Oltre a consentire agli utenti di modificare e reimpostare il PIN, l'app mobile può anche essere sottoposta senza sforzo. Viene inviato un messaggio di posta elettronica all'utente, indicando i passaggi per eseguire il provisioning dell'app mobile e un codice QR per la configurazione. Una volta distribuito, gli utenti saranno in grado di autenticare l'accesso a tutte le loro applicazioni che utilizzano: - Con il codice monouso (OTC) o - Notifica PUSH

Self-service

Il Portale utenti self-service riduce il costo, che di solito è associato con la disposizione del supporto per queste azioni.

Maggiore efficienza

Il portale utente di Swivel Secure è progettato per offrire agli utenti una maggiore efficienza nell'esecuzione dei requisiti di base, tra cui:

- Modifica del PIN
- Reimpostazione del PIN
- Provisioning di app per dispositivi mobili
- Re-sincronizzazione degli hardware token.

È possibile applicare restrizioni per garantire che si verifichino alcune attività di sorveglianza, garantendo che le azioni siano conformi ai protocolli di sicurezza

Tecnologia

PINsafe® tecnologia brevettata

PINsafe® è la tecnologia brevettata alla base dei fattori di autenticazione dell'immagine PINpad®, PICpad e TURing, che fanno parte di una serie di fattori di autenticazione, disponibili con AuthControl Sentry®: La soluzione di autenticazione a più fattori progettata per proteggere dall' accesso non autorizzato alle applicazioni, reti e dati.

Come funziona PINsafe®?

A ogni utente viene rilasciato un numero PIN, che tuttavia questo PIN esatto non viene mai digitato.

Quando un utente deve eseguire l'autenticazione in modo sicuro, gli viene inviato una stringa di sicurezza di 10 cifre, una sequenza di caratteri o numeri. La stringa di sicurezza può essere visualizzata come grafica (TURing, PINpad® o PICpad) o inviata via e-mail o tramite verifica SMS.

Utilizzando il PIN come indicatore posizionale, è possibile estrarre un codice monouso per l'autenticazione.

Potrebbe mostrarmi un esempio?

L'esempio seguente mostra che il PIN è 1370. In quest' occasione la stringa di sicurezza è 5721694380, quindi il codice di accesso è 5240. In quest' occasione la stringa di sicurezza è 5721694380, così il suo codice login è 5240.

La stringa di sicurezza può essere integrata con tanti dispositivi ed applicazioni in diversi modi per una flessibilità completa, incluso:

- Accesso a Windows
- Accesso remoto con F5, Citrix Netscaler e Cisco VPN
- Accesso Web con OWA, Apache e Microsoft ILS

PINsafe® impedisce all'utente di dover inserire il proprio PIN, in più impedisce qualsiasi infiltrazione come ad esempio attacchi man-in-the-middle.

Fattori

Fattori di autenticazione

Swivel Secure offre un'ampia gamma di fattori di autenticazione per garantire che ogni distribuzione offra la massima adozione in tutta l'organizzazione.

Lo stesso, se sceglie di eseguire l'autenticazione utilizzando l'OTC sull'app mobile AuthControl Mobile®, un token hardware tradizionale o anche utilizzando la sua impronta digitale, AuthControl Sentry® di Swivel Secure offre la massima sicurezza e configurabilità per soddisfare le esigenze di sicurezza della sua azienda.

AuthControl Mobile®: OTC

Ogni volta che richiede di effettuare l'autenticazione, è sufficiente utilizzare l'OTC visualizzato nell'App. Poiché esistono 99 codici, la funzione OTC è abbastanza versatile da essere utilizzata offline. Una volta inserito il codice, verrà concesso l'accesso alla sua domanda.

Fattore immagine: PINpad®

Un codice di 10 cifre è presentato sotto forma di una griglia numerica nel web browser dell'utente.

L'utente fa semplicemente clic sulle immagini che rappresentano il pin. Ogni immagine su cui si fa clic trasmette quindi un diverso codice TC a AuthControl Sentry® per autenticare l'utente.

Fattore immagine: PICpad

PICpad è un fattore di autenticazione che trascende le solite opzioni per la diversificazione linguistica dei dipendenti e dei clienti.

Utilizzando gli stessi principi di PINpad®, PICpad visualizza i simboli anziché i numeri, fornendo un significato cœrente in ambienti multinazionali

AuthControl Mobile®: PUSH

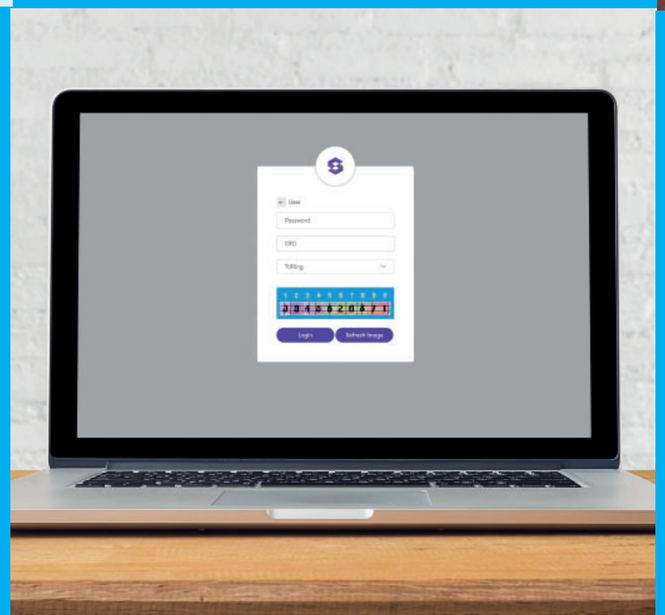
Semplicemente premendo un pulsante nell'app mobile è possibile confermare l'autenticazione con la notifica inviata direttamente al suo cellulare.

Distribuisce rapidamente la funzionalità Swivel One Touch® con una configurazione minima.

Fattore immagine: TURing

Un codice di 10 cifre è presentato sotto forma di un'immagine rettangolare nel browser web dell'utente. L'utente prende quindi i numeri rappresentati dal pin.

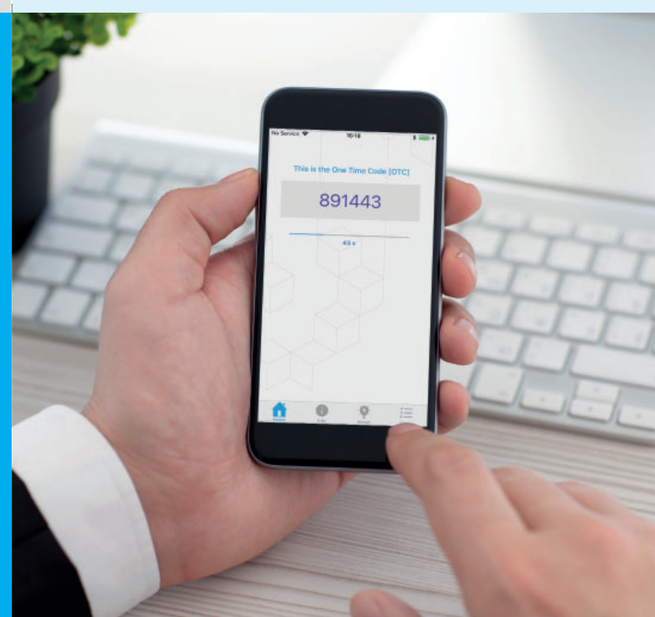
Esempio: se il PIN è 1370, prende semplicemente il primo, terzo, settimo e decimo carattere dall'immagine presentata.



AuthControl Mobile®: OATH

Il soft token OATH è un token basato sul tempo che conta da 0 a 60, simile al hardware token tradizionale utilizzato per accedere ad applicazioni tramite la VPN.

OATH, il compatibile soft token fornisce all'utente un codice a sei cifre per l'autenticazione.



Cellulare: SMS

Per proteggere l'OTC (tramite SMS) da intercettazioni fraudolenti, l'SMS è protetto da PINsafe®. Ciò significa che l'SMS contiene una stringa di sicurezza di due sequenze alfanumeriche e, se combinato con il PIN dell'utente, fornisce il proprio OTC.

Biometria: impronte digitali

Il riconoscimento delle impronte digitali è disponibile per il provider di credenziali AuthControl® che utilizza il framework biometrico di Windows 10 e il controller di accesso alle impronte digitali NITGEN.

Gli utenti possono eseguire l'autenticazione utilizzando il controller di impronte digitali NITGEN o il lettore di impronte digitali incorporato nel proprio computer portatile.

AuthControl Voice

Chiamando l'utente, AuthControl Voice vocalizza un codice monouso (OTC) o una notifica PUSH (YES o NO) per autenticare l'accesso alle applicazioni.
L'OTC consegnato vocalmente al telefono viene quindi digitato nella finestra richiesta.

Hardware token

L'hardware token fornisce agli utenti un codice monouso (OTC) in modo che possano accedere in modo sicuro all'applicazione.

Ogni volta che si preme il pulsante sull'hardware token, fornisce un nuovo codice per garantire la protezione ad accessi non autorizzati.

swivelsecure

Integrazioni

AuthControl Sentry® è una delle soluzioni più flessibili sul mercato, integrandosi con centinaia di applicazioni e software appliance tramite RADIUS, ADFS, SAML e la nostra proprietarà API - AgentXML.

Lo stesso se accede a Salesforce, o effettua l'autenticazione con l'app per dispositivi mobili o preferisce di accedere a Windows Credential Provider utilizzando un autenticatore di immagini; AuthControl Sentry® supporta un'ampia gamma per applicazioni e dispositivi, offrendo la flessibilità e la l'efficienza richiesta per l'autenticazione in una soluzione continuità in tutta l'organizzazione.

Licenze

Piani di licenza flessibili e modelli di prezzi adatti per tutte le organizzazioni. La licenza viene calcolata specificamente in base all'utente

Licenze utente

Piani di licenza flessibili e modelli di prezzi adatti a tutte le organizzazioni.

- Le licenze per AuthControl Sentry® sono per utente
- In ogni licenza TUTTI i fattori di autenticazione sono inclusi.
- MFA, SSO e RBA sono inclusi nel AuthControl Sentry®
- Contratto disponibile a 1, 3, 5 o 7 anni o con condizioni perpetue

On-Premise

È disponibile una licenza permanente per le soluzioni locali o per quelle ospitate in una cloud privata. Il prezzo è per utente, a scala, a partire da soli 10 utenti. Il prezzo è cumulativo, quindi è un modo estremamente conveniente per acquistare un volume di licenze, piuttosto che un modello scaglionato. È il modo ideale per le organizzazioni che desiderano CAPEX, il costo di servizio in anticipo e con un numeri di utenti stabili.

Cloud

Le licenze in abbonamento sono disponibili per le distribuzioni cloud e consentono alle organizzazioni di soddisfare i requisiti degli utenti in base alle modifiche della domanda. Nessun costo iniziale e con un contratto flessibile, senza penalità e con risoluzione. Idealmente adatto alle organizzazioni che vogliono OPEX il costo di un servizio e numeri di utenti variabili.

Opzioni di licenza

Usa la tabella seguente per confrontare le opzioni per le licenze locali e cloud.

Tipo di licenza	On-Premise	Cloud
Autenticazione basata sul rischio	✓	✓
Integrazioni (SAML/ADFS/RADIUS)	✓	✓
Applicazioni on-premise e cloud	✓	✓
Tutti i fattori di autenticazione	✓	✓
Agente AD e AD Sync	✓	✓
Portale unificato con Single sign-On	✓	✓
Reporting	✓	✓
Appliance (fisico/virtuale)	✓	✗
Immagine AWS di Amazon	✗	✓
24x7x365	Opzionale	✓

Assistenza & Supporto

Per garantire che le organizzazioni abbiano accesso al supporto tecnico e alle funzionalità più recenti, offriamo livelli di supporto Standard e Premium per gli utenti della piattaforma di autenticazione. Sono inoltre disponibili servizi professionali per l'aggiornamento, la distribuzione, la migrazione e l'integrazione complessa.

Contratto di manutenzione del livello di ingresso

Orario di supporto: 8/5. Accesso ad aggiornamenti software, aggiornamenti e correzioni di bug.

Contratto di manutenzione standard

Orario di supporto: 24/5. Swivel Secure offre supporto 24 ore su 24 durante i giorni lavorativi.

Contratto di manutenzione Premium

Ore di supporto: un vero servizio 24 ore su 24, 7 giorni su 7, ideale per le organizzazioni o aziende che richiedono immediatament il supporto di esperti. requiring expert support immediately.

Servizi professionali

Swivel Secure fornisce una gamma di servizi professionali per le organizzazioni che richiedono risorse tecniche su misura per la distribuzione dell'autenticazione a più fattori e si garantisce la compatibilità con sistemi, connessioni e hardware.

Servizio (TAM)Technical Account Manager

Il nostro servizio TAM offre una guida proattiva e una gestione centralizzata del servizio, dando la garanzia di un vantaggio nella gestione di prioritaria all'interno di ogni canale di supporto.

Ha bisogno di aggiornare suo Swivel Secure appliance?

Swivel Secure riconosce alcuni dei problemi che possono verificarsi durante un aggiornamento e offre un servizio di aggiornamento sviluppato per garantire che il servizio e l'azienda presentano disturbi minimi.

Possiede un'infrastruttura di rete altamente complessa che richiede numerose integrazioni?

Il nostro team di ingegneri esperti lavora a stretto contatto con i vostri team di architetti tecnici e di erogazione dei servizi per garantire:

- Qualsiasi progetto proposto è adattato all'architettura di rete
- Il progetto soddisfa i requisiti organizzativi di architettura e controllo delle modifiche

Ha bisogno di integrare un nuovo dispositivo RADIUS o SAML senza precedenti articoli di integrazione su cui lavorare?

Il nostro team di sviluppatori software può essere a disposizione per:

- Valutare e sviluppare nuove integrazioni
- Facilitare i nuovi plugin
- Rispondere alle richieste di funzionalità per migliorare continuamente il software.