AuthControl Sentry®

Escritório UK & Ireland Norte
1200 Century Way
Thorpe Park,
Leeds
LS15 8ZA

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

Sul
Pinewood
Chineham Business Park
Chineham, Basingstoke
RG24 8AL

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

+1 949 480 3626 (Pacific Time)
Toll Free: 866.963.AUTH (2884)
usa@swivelsecure.com

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

+351 215 851 487
portugal@swivelsecure.com

Espanha
Calle Punto Mobi 4,
28805 Alcala de Henares
Madrid

+34 911 571 103
espana@swivelsecure.com

Protegemos identidades com autenticação inteligente

Centrada na nossa tecnologia PINsafe® para máxima segurança e autenticação baseada no risco proporcionando controle dinâmico, a nossa solução premiada AuthControl Sentry® oferece uma solução de autenticação multifator inteligente para todas as empresas e tipos de negócio.

swivelsecure

www.swivelsecure.com

AuthControl Sentry® Autenticação inteligente de vários fatores

Implantado em mais de 52 países, implementado em todas as empresas, incluindo finanças, governo, saúde, educação e fabricantes, AuthControl Sentry® fornece às organizaçõe uma verdadeira autenticação multi-fator, entregando uma solução inteligente para evitar acesso não autorizado a aplicativos e dados.

Capture o código QR para ver o diagrama completo do AuthControl Sentry®, a solução de autenticação multifator completa para as partes interessadas.

AuthControl Sentry® tem flexibilidade para suportar uma ampla gama de requisitos arquitetônicos, capacidade de assegurar a máxima adoção, com uma ampla escolha de fatores de autenticação. Utilizando o aplicativo móvel ou a mais recente Biometria, através do leitor de impressões digitais, AuthControl Sentry® consolida-se como uma solução líder em ciber segurança.

O que o torna diferente

- Tecnologia patenteada PINsafe® para a máxima segurança - consulte a página 8
- Suporta on-premise e Cloud para todas as arquiteturas
- Instancia cloud privada, garante personalização e controle otimizados
- Autenticação baseada em risco e logon único como padrão
- Integra-se perfeitamente com centenas de aplicações
- Garante adoção máxima com uma extensa gama de métodos de autenticação - até dez fatores!

Autenticar o acesso para todas as partes interessadas, quer acedendo ao Office 365, transações através de eCommerce, ou para aceder ao seu ERP para controle de stock.

- ✓ Funcionários
- ✓ Clientes
- ✓ Fornecedores

Arquitetura

Suporta on-premise e cloud para arquitetura variável

Não há restrições com AuthControl Sentry®. Foi projetado para autenticar acesso a aplicativos, estejam eles hospedados na Cloud ou on-premise, seja o utilizador um cliente, funcionário ou fornecedor que está a solicitar acesso.

Arquitetura On-premise

Aceda aos seus sistemas internos através do nosso Agente do Active Directory, um aplicativo de software instalado localmente que elimina a necessidade de compartilhar o seu Active Directory através da Internet, mantendo a sincronização da conta do utilizador.

Arquitetura baseada na Cloud

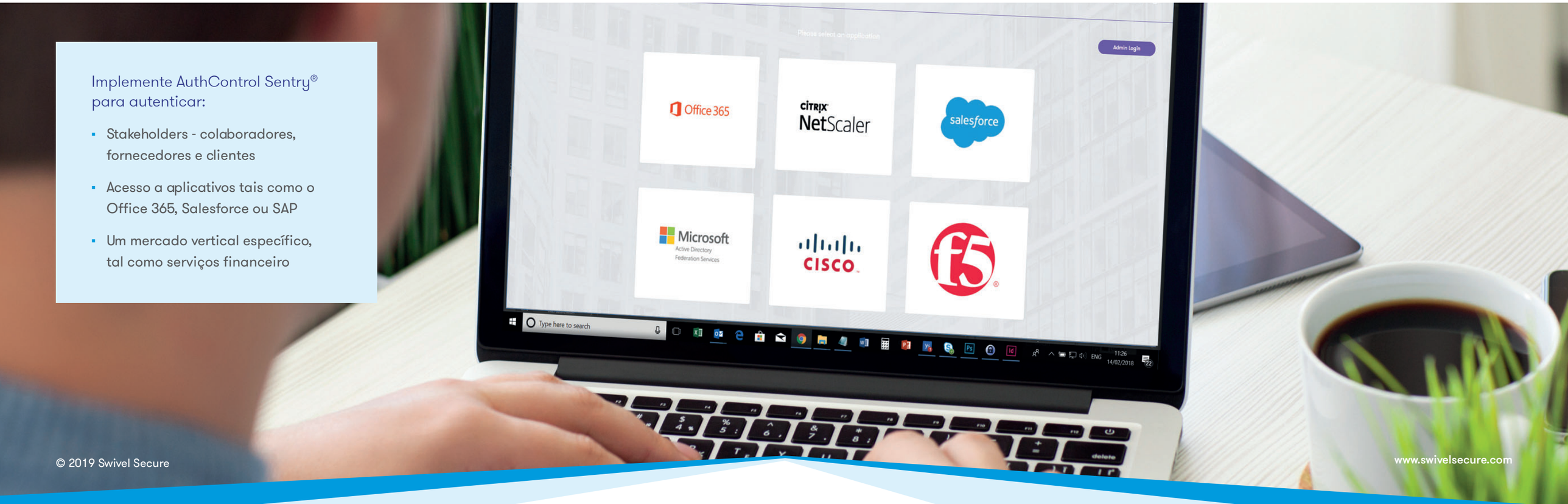
IP Fixo: Cada cliente de AuthControl recebe um IP fixo dedicado para a sua própria instância virtual. Não há recursos compartilhados, nenhuma interface de programação de aplicativos, nenhum portal de entrada, ou banco de dados compartilhado.

Uma oferta dedicada: AuthControl Cloud oferece uma máquina virtual dedicada. Não há opções compartilhadas com vários utilizadores, como tal tem a gestão e o controle total, o que significa que tem a flexibilidade de configurar a solução para atender às suas necessidades específicas.

Uma firewall privada: Oferecemos firewalls dedicadas e independentes para cada cliente, permitindo listas de controle de acessos e segurança personalizadas.

Implemente AuthControl Sentry® para autenticar:

- Stakeholders - colaboradores, fornecedores e clientes
- Acesso a aplicativos tais como o Office 365, Salesforce ou SAP
- Um mercado vertical específico, tal como serviços financeiro



Características

Single sign-on como padrão

A funcionalidade (SSO) para AuthControl Sentry® é um recurso que fornece aos utilizadores a capacidade de aceder a todos os seus aplicativos, com um único processo de autenticação, garantindo que os utilizadores trabalhem de forma eficiente sem comprometer a segurança.

Segurança contínua

Swivel Secure fornece um Portal Unificado para fornecer acesso sem atrito aos seus utilizadores. Ao usar esse ponto único de acesso, os privilégios dos utilizadores podem ser geridos e o comportamento pode ser monitorizado para fins de auditoria, aprimorando a segurança e fornecendo responsabilidade.

Econômico

É possível economizar significativamente utilizando SSO, pois a necessidade de chamadas ao suporte IT relacionadas com passwords é erradicada. A produtividade aumenta, os utilizadores entram em um único local para aceder a todos os seus aplicativos - economizando tempo.

Intuitivo

SSO foi projetado para aumentar a eficiência, permitindo aos utilizadores aceder a todos os seus aplicativos com uma única autenticação bem sucedida, através do mecanismo de políticas baseadas no risco. Independentemente de os utilizadores estarem a aceder a aplicativos através da VPN, on-premise ou Cloud, serão direcionados automaticamente para a autenticação usando o SSO intuitivo, funcionalidade incluida no Portal Unificado.

Características

Autenticação baseada em risco como padrão

A autenticação baseada em risco (RBA) é um recurso dinâmico do AuthControl Sentry®, projetado para solicitar automaticamente o nível apropriado de autenticação para aceder aos aplicativos. Com base nos parâmetros definidos no mecanismo de políticas, RBA solicitará o nível apropriado de autenticação para aceder aos aplicativos com base no utilizador, no seu dispositivo e na aplicação.

Dinâmico e Inteligente

Adapta-se às circunstâncias do utilizador Incluindo:

- Quais os aplicativos que estão a tentar aceder
- A que grupo pertencem
- Onde estão a aceder às aplicações
- Qual o dispositivo que estão a utilizar

O mecanismo de política

Com base em um sistema de pontos, o mecanismo de política da autenticação adaptativa permite que os administradores definam parâmetros por utilizador, por aplicativo.

- Pertencer a um determinado grupo
- Aplicações a serem acedidas
- Endereço de IP
- Última autenticação
- X.509 Certificado
- Dispositivo
- Localização física (GeoIP)
- Geo Velocity

Autenticação baseada em risco: exemplo 1

O Assistente de Compras voou para o Sudeste Asiático com o seu Gerente de compras para visitar um fornecedor. Quando terminou a sua refeição no restaurante percebeu que se tinha esquecido de verificar o stock de componentes para uma reunião no dia seguinte. Pensou que entraria rapidamente no sistema ERP, usando o dispositivo móvel da sua empresa.

Sistema ERP	
Requer 120 pontos	
LAN	0
Known IP	0
Managed Device	50
IP Range (Asia)	-100
Autenticação Requerida	
U&P	10
App Móvel	60
Fingerprint	20

Resultado - Tentativa fracassada
Apesar de estar a usar um dispositivo emitido pela empresa para aceder ao ERP, é atribuído -100 pontos tendo en conta a localização do IP. Não terá acesso ao ERP, independentemente de estar disposta a usar a autenticação multifator.

Autenticação baseada em Risco : Exemplo 2

O gerente de vendas está a trabalhar hoje no escritório, quer aceder ao CRM para criar uma oportunidade após uma reunião. Está a usar o laptop fornecido pela empresa e está aceder à aplicação que está localizada on-premise.

Sistema CRM	
Requer 120 Pontos	
LAN	50
Known IP	50
Managed Device	50
IP Range (Portugal)	50
Autenticação Requerida	
U&P	10
App Móvel	60
Fingerprint	20

Resultado – Autenticação efetuada com sucesso
O gerente de vendas excede claramente os pontos que precisa para aceder ao CRM. Depois de se ter autenticado, pode usar o single sign-on (SSO) para aceder a outras aplicações. Recebe uma chamada do Assistente de Compras, pode aceder ao sistema ERP e fornecer a quantidade relativa à referência que lhe está a ser dada.

Máxima flexibilidade e controle

O mecanismo de políticas permite que sejam criadas novas regras e que sejam combinadas com as regras existentes, além de fornecer um mecanismo para suportar uma variedade de cenários com complexidade crescente.

Características

Portal do Utilizador

O Portal do Utilizador é um recurso do AuthControl Sentry®, projetado para fornecer aos administradores uma solução configurável para oferecer autonomia aos utilizadores para tarefas básicas de autogestão.

O Portal do utilizador fornece aos administradores a capacidade de fornecer acesso direto aos utilizadores, permitindo que executem requisitos regulares, como alterar ou redefinir o PIN, ou provisionar a móvel app.

Provisionar a móvel app

Além de permitir que os utilizadores alterem e redefinam seu PIN, o aplicativo para dispositivos móveis também pode ser provisionado sem esforço. Um e-mail é enviado ao utilizador, detalhando as etapas para provisionar o aplicativo móvel, e um código QR para configuração. Uma vez implantados, os utilizadores podem autenticar o acesso a todos os seus aplicativos regulares usando: - O código único (OTC) ou - Notificação PUSH

Self service

O Portal self-service do utilizador visa reduzir os custos geralmente associados aos pedidos de suporte ao Helpdesk.

Maior eficiência

O Portal do Utilizador Swivel Secure foi projetado para oferecer maior eficiência para os utilizadores executarem requisitos básicos, incluindo:

- Alteração de PIN
- Redefinir PIN
- Provisionamento da App Móvel
- Ressincronização de tokens de hardware.

Restrições podem ser implantadas para garantir que algum controle ocorra, garantindo que as ações estejam de acordo com os protocolos de segurança.

Tecnologia

Tecnologia patenteada PINsafe®

PINsafe® é a tecnologia patenteada por trás da imagem, os fatores de autenticação PINpad®, PICpad e TURing, fazem parte da gama de fatores de autenticação disponíveis com o AuthControl Sentry®, a solução de autenticação multifator projetada para proteger as organizações contra acesso não autorizado aos seus aplicativos, redes e dados.

Como funciona o PINsafe®?

Cada utilizador recebe um número PIN - no entanto, esse PIN exato nunca é digitado.

Quando um utilizador precisa autenticar com segurança, é lhe enviada uma chave de segurança de 10 dígitos - uma sequência aleatória de caracteres ou números. A sequência de segurança pode ser exibida como um gráfico (TURing, PINpad® ou PICpad) ou enviada por e-mail ou por SMS.

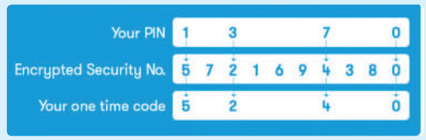
Usando o PIN como um indicador posicional, pode ser extraído um código único para. autenticação.

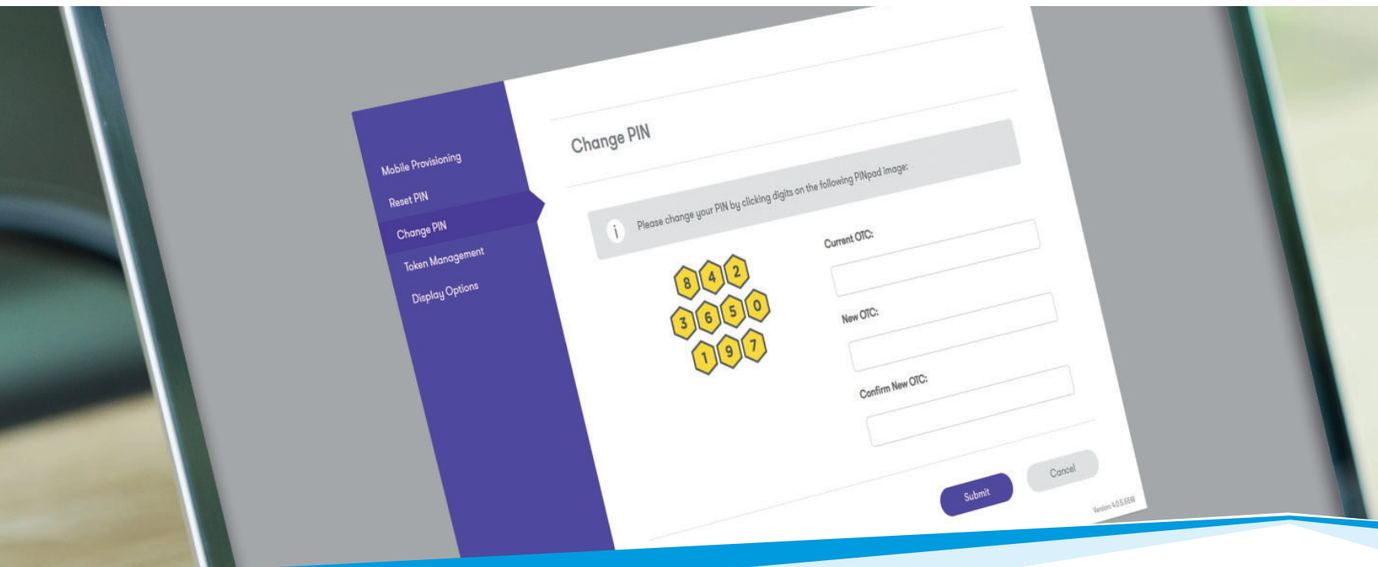
Pode-me mostrar um exemplo?

O exemplo abaixo mostra que o seu PIN é1370. Neste exemplo a chave de segurança é 5721694380, portanto, o seu Código para login é 5240.

A chave de segurança pode ser integrada com vários dispositivos e aplicativos, de várias formas, para flexibilidade total. Incluindo:

- Fazer login no Windows
- Acesso remoto com F5, Citrix Netscaler e Cisco VPN
- Acesso à Web com OWA, Apache e Microsoft ILS





Com PINsafe® o utilizador não insere o seu PIN, evita assim qualquer infiltração, tais como ataques man-in-the-middle

Fatores

Fatores de Autenticação

Swivel Secure fornece uma ampla gama de fatores de autenticação para garantir que cada implementação forneça a máxima adoção em toda a organização.

Pode optar por autenticar utilizando o OTC na app móvel (AuthControl Mobile®), com um token de hardware tradicional ou até mesmo usando a sua impressão digital, AuthControl Sentry®. Swivel Secure oferece segurança e configurabilidade para atender às necessidades de segurança da sua empresa.

AuthControl Mobile®: OTC

Sempre que lhe for solicitada autenticação, basta usar o OTC exibido no aplicativo. A função OTC é suficientemente versátil para ser usada offline, existem 99 códigos prontos a ser utilizados.
Depois de o código ser inserido, terá acesso ao seu aplicativo.

Fator de imagem: PINpad®

Um código de 10 dígitos é apresentado na forma de uma grelha numérica no navegador da Web do utilizador.
O utilizador simplesmente clica nas imagens que representam o seu PIN.
Cada imagem clicada transmite então um código TC diferente para AuthControl Sentry® autenticar o utilizador.

Fator de imagem: PICpad

O PICpad é um fator de autenticação que transcende as opções usuais de diversificação de idiomas tanto para funcionários como para clientes.

Usando os mesmos princípios do PINpad®, o PICpad exibe símbolos em vez de números, fornecendo um significado cœrente em ambientes multinacionais

AuthControl Mobile®: PUSH

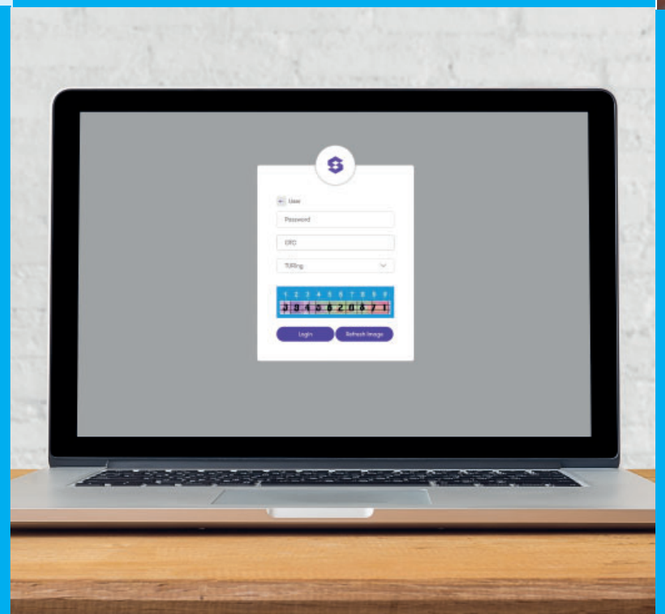
Basta pressionar um botão no aplicativo móvel para confirmar a autenticação com a notificação enviada diretamente para seu telemóvel.

Implemente a funcionalidade Swivel One Touch® rapidamente, com uma configuração mínima necessária.

Fator de imagem: TURing

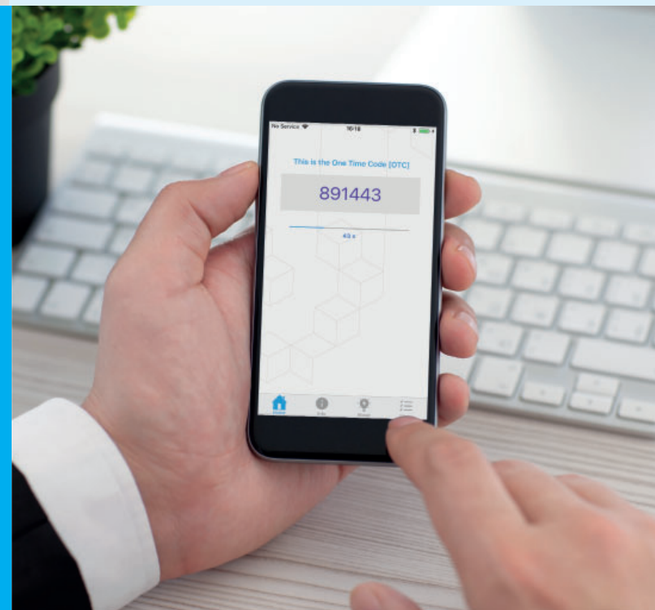
Um código de 10 dígitos é apresentado na forma de uma imagem retangular no navegador da web do utilizador.
O utilizador então extrai os números representados pelo seu PIN.

Exemplo: Se o PIN for 1370, basta simplesmente utilizar a posição 1o, 3o, 7o e 10o dos caracteres da imagem apresentada.



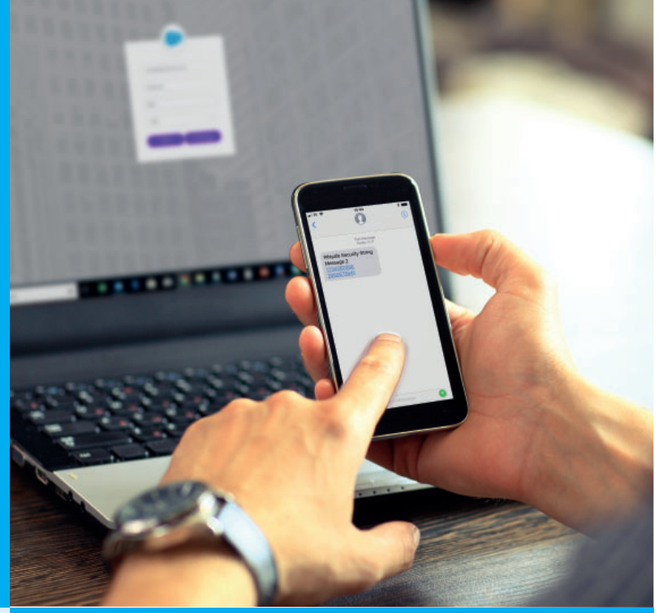
AuthControl Mobile®: OATH

O soft token OATH é um token baseado no tempo que conta de 0 a 60, semelhante ao token de hardware tradicional usado para aceder aos aplicativos através da VPN.
O soft token compatível com OATH fornece ao utilizador um código de seis dígitos para se autenticar.



Mobile: SMS

Para proteger o OTC (através de SMS) contra interceptação fraudulenta, o SMS é protegido pelo PINsafe®. Isso significa que o SMS contém uma sequência de caracteres de segurança de duas sequências alfanuméricas e, quando combinado com o PIN do utilizador fornece o seu OTC.



Biometria: impressão digital

O reconhecimento de impressão digital está disponível para o AuthControl Credential® Provider usando a estrutura biométrica do Windows 10 e o controlador de acesso por impressão digital NITGEN. Os utilizadores podem autenticar usando o controlador de impressão digital NITGEN ou seu leitor de impressão digital embutido no seu laptop.

AuthControl Voz

Quando liga ao utlizador, AuthControl Voz vocaliza um código único (OTC) ou uma notificação PUSH (YES ou NO) para autenticar o acesso aos aplicativos. O OTC emitido vocalmente pelo telefone é então digitado na janela, mediante solicitação.

Hardware token

O token de hardware fornece aos utilizadores um código único (OTC) para que possam aceder com segurança ao aplicativo. Sempre que o botão do token de hardware é pressionado, fornece um novo código, garantindo que o acesso não autorizado seja evitado.

swivelsecure

Integrações

AuthControl Sentry® é uma das soluções mais flexíveis do mercado, integrando com centenas de aplicativos, softwares e appliance através de RADIUS, ADFS, SAML e a nossa própria API proprietária - AgentXML.

Se necessita aceder ao Salesforce, autenticar com o aplicativo móvel ou fazer login no Windows Credential Provider usando um autenticador de imagem, AuthControl Sentry® oferece suporte a uma ampla variedade de aplicativos e dispositivos, fornecendo a flexibilidade e a eficiência necessárias para autenticação contínua para toda a organização.

Licenciamento

Planos de licenciamento flexíveis e modelos de preços adequados para todas as organizações. O licenciamento é cobrado por utilizador.

Licenciamento de Utilizadores

Planos de licenciamento flexíveis e modelos de preços adequados para todas as organizações.

- Licenças para AuthControl Sentry® são por utilizador
- Cada licença inclui todos os fatores de autenticação
- MFA, SSO e RBA estão incluídos no AuthControl Sentry®
- Disponível como contratos de 1, 3, 5 ou 7 anos ou com licenciamento perpétuo

On-Premise

Licença perpétua está disponível para soluções on-premise ou hospedadas numa Cloud privada. O preço é por utilizador, numa escala variável, a partir de apenas 10 utilizadores. O preço é cumulativo, portanto, é uma maneira extremamente econômica de comprar um volume de licenças, em vez de um modelo escalonado. Idealmente adequado para organizações que desejam capex, o custo de um serviço inicial e com um números de utilizadores estáveis.

Cloud

O licenciamento por subscrição está disponível para implantações na Cloud permite que as organizações exibam seus requisitos de utilizador à medida que a necessidade é alterada. Sem custos iniciais e com um contrato e rescisão flexível e sem penalização. Idealmente adequado para organizações que querem OPEX o custo de um serviço e com númers de utilizadores variáveis.

Opções de licenciamento

Use a tabela abaixo para comparar as opções de licenciamento on-premise e na Cloud.

Tipo de licença	On-Premise	Cloud
Autenticação baseada em risco	✓	✓
Integrações (SAML/ADFS/RADIUS)	✓	✓
On-Premise & Aplicações Cloud	✓	✓
Todos os Fatores de Autenticação	✓	✓
AD Agent & AD Sync	✓	✓
Portal Unificado com Single sign-on	✓	✓
Relatórios	✓	✓
Appliance (física/Virtual)	✓	✗
Imagem Amazon AWS	✗	✓
24x7x365	Opcional	✓

Serviço & Suporte

Para garantir que as organizações tenham acesso ao suporte técnico e aos recursos mais recentes, oferecemos níveis de suporte Standard e Premium para os nossos utilizadores da plataforma de autenticação. Serviços profissionais também estão disponíveis para atualização, implantação, migração e integrações complexas.

Contrato de manutenção Standard

Horas de suporte: 8/5. Acesso a atualizações de software, atualizações e correções de bugs.

Contrato de Manutenção Standard

Horas de suporte: 24/5. Swivel Secure Presupõe suporte 24 horas durante a semana de trabalho como standard.

Contrato de Manutenção Premium

Horas de suporte: um verdadeiro serviço 24/7, ideal para organizações empresariais que exigem suporte especializado imediato.

Serviços profissionais

Swivel Secure fornece uma gama de Serviços Profissionais para organizações que necessitam de recursos técnicos adicionais ou sob medida ao implementar a autenticação multifator e garantir a compatibilidade com sistemas, conexões e hardware.

Technical Account Manager (TAM) Service

Nosso serviço TAM oferece orientação proativa e gestão centralizada de serviços, garantindo que beneficia de tratamento prioritário em todos os canais de suporte.

Necessita de atualizar a sua appliance Swivel Secure?

Swivel Secure reconhece alguns problemas que podem ocorrer durante uma atualização, oferece serviço de atualização desenvolvido para garantir um mínimo de interrupção no serviço e na sua empresa.

Tem uma infraestrutura de rede altamente complexa que requer inúmeras integrações?

A nossa equipa de engenheiros especializados trabalha em conjunto com suas equipas de Arquitetos Técnicos e de Prestação de Serviços para garantir:

- Qualquer design proposto é adaptado à sua arquitetura de rede
- O design atende à sua arquitetura organizacional e altera os requisitos de controle

Precisa integrar um novo dispositivo RADIUS ou SAML sem nenhum artigo de integração anterior para trabalhar?

A nossa equipa de desenvolvedores de software pode estar disponível para:

- Avaliar e desenvolver novas integrações
- Facilitar novos plugins
- Resposta a solicitações de recursos para melhorar continuamente o software.