UK & Ireland Offices
North
Equinox 1
Audby Lane
Wetherby, Leeds
LS22 7RD

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

South
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 (Pacific Time)
Toll Free: 866.963.AUTH (2884)
usa@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

Spain
Av. Juan Carlos I, nº 13 – 2ª
planta (Torre Garena)
Alcalá de Henares
28806 Madrid

+34 911 571 103
espana@swivelsecure.com

AuthControl Sentry®

Protecting identities with intelligent authentication

With PINsafe® technology at the core for ultimate security and risk-based authentication providing dynamic control, the award winning AuthControl Sentry® delivers an intelligent multi-factor authentication solution for business.

swivelsecure

www.swivelsecure.com

swivelsecure

AuthControl Sentry® Intelligent Multi-factor Authentication

Deployed in over 52 countries and implemented in across enterprises including finance, government, healthcare, education, and manufacturing, AuthControl Sentry® provides organisations with true multi-factor authentication, delivering an intelligent solution to prevent unauthorised access to applications and data.

AuthControl Sentry® has the flexibility to support a range of architectural requirements and the ability to ensure maximum adoption, with a wide choice of authentication factors. Whether utilising the mobile application, or the latest in biometrics via the fingerprint reader, AuthControl Sentry® establishes itself as a leading solution in cybersecurity.

Capture the QR code to see the full diagram of AuthControl Sentry®, the complete multi-factor authentication stakeholder solution.

What makes it different

- Patented PINsafe® technology for ultimate security – see page 8
- Supports on-premise and cloud for all architecture
- A single tenancy and single tiered cloud solution, ensures optimised customisation and control
- Risk-based authentication and single sign-on as standard
- Integrates seamlessly with hundreds of applications
- Ensures maximum adoption with an extensive range of authentication methods - up to ten factors!

Authenticate access for all stakeholders, whether its logging onto Office 365, transacting through eCommerce, or accessing your ERP for stock control.

✓ Employees ✓ Customers

✓ Suppliers

Architecture

Supports on-premise and cloud for changeable architecture

There are no restrictions with AuthControl Sentry®. It's designed to authenticate access to applications whether they're hosted in the cloud or on-premise, and whether the user is a customer, an employee, or a supplier requesting access.

On-premise architecture

Access internal systems via our Active Directory Agent, a locally installed software application that removes the need to share your Active Directory across the Internet, whilst maintaining user account synchronisation.

Cloud based architecture

A fixed IP: Each AuthControl customer receives a dedicated fixed IP for their own virtual instance. There is no shared resource, no shared application programming interface and no shared entry portal or shared database.

A dedicated offering: AuthControl Cloud gives you a dedicated virtual machine. There are no shared multi-tenanted options, so you can expect total management and control which means you have the flexibility to configure the solution to meet with your exacting needs.

A private firewall: We offer dedicated and independent firewalls for each customer, allowing tailored security and access control lists.

Deploy AuthControl Sentry® for authenticating:

- Stakeholders - employees, suppliers, and customers
- Access to applications such as Office 365, Salesforce or SAP
- A specific vertical market such as financial services

swivelsecure

Features

Single sign-on as standard

Single sign-on (SSO) functionality for AuthControl Sentry® is a feature providing users with the ability to access all of their applications, with a single authentication process, ensuring users work efficiently without compromising security.

Continuous security

Swivel Secure provides a Unified Portal to deliver frictionless access for your users. By using this single point of access, users' privileges can be managed and behaviour can be tracked for auditing purposes, enhancing security and providing accountability.

Cost effective

Significant savings can be achieved by utilising SSO, as the necessity for password-related calls to IT support desks are eradicated. Productivity increases, where users are logging into one point to access all of their applications – saving time.

Intuitive

SSO is designed to increase efficiency by allowing users to access all of their applications with a single successful authentication, through the risk-based policy engine. Whether users are accessing applications through a VPN, on-premise, or cloud, they will automatically be directed to authenticate using the intuitive SSO functionality within the Unified Portal.

Features

Risk-based authentication as standard

Risk-based authentication (RBA) is a dynamic feature of AuthControl Sentry®, designed to automatically request the appropriate level of authentication to access applications. Based on parameters set in the policy engine, RBA will request the appropriate level of authentication to access applications based on the user, their device and the application.

Dynamic & intelligent

Adapts to the user's circumstances including:

- What applications they are trying to access
- What group membership they have
- Where they are accessing the applications from
- What device they are using

The policy engine

Based on a points system, the adaptive authentication policy engine enables administrators to set parameters per user, per application.

- Group membership
- Application being accessed
- IP address
- Last authentication
- X.509 Cert
- Device
- Physical location (GeoIP)
- Geo Velocity

Risk-based authentication: Example 1

The Purchasing Assistant has flown to South East Asia to visit a supplier with the Purchasing Manager. She has just finished a meal in a restaurant and realises she forgot to check the stock of some components for a meeting the following day. She thought she'd quickly login to the ERP system, using her company-issued mobile device.

ERP system	
Requires 120 points	
LAN	0
Known IP	0
Managed Device	50
IP Range (Asia)	-100
Authentication required	
U&P	10
Mobile App	60
Fingerprint	20

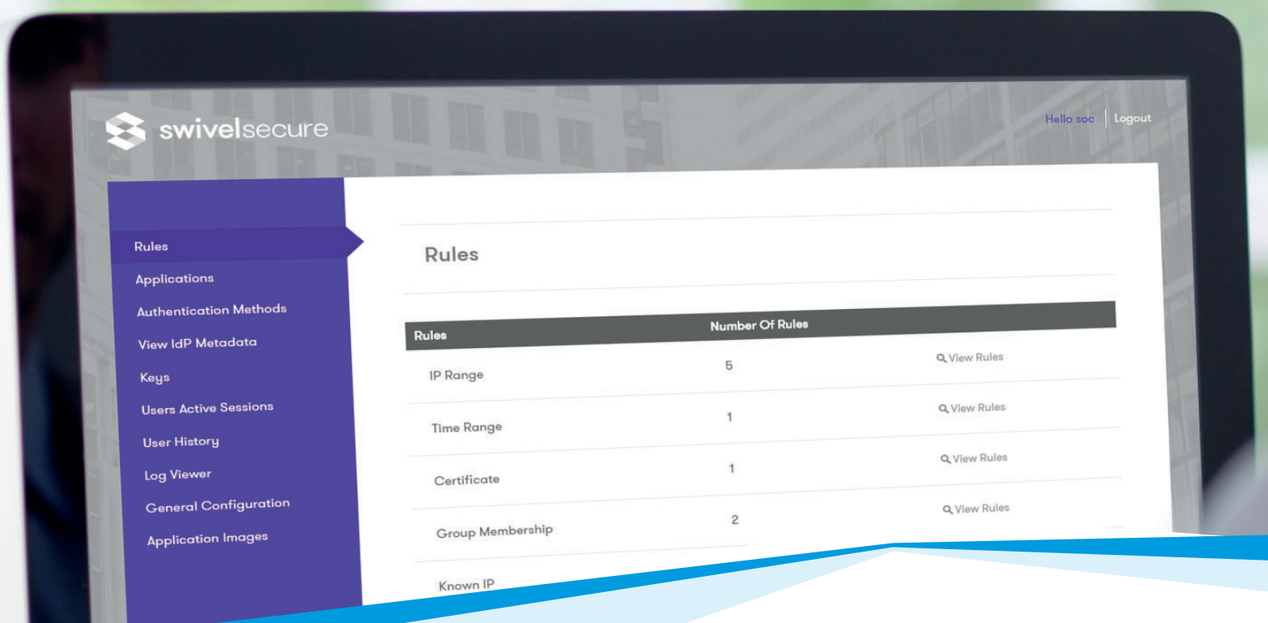
Result – Unsuccessful
Although she is trying to use a company-issued device to access the ERP, the IP range sets her back -100 points because of her location. She will not be granted access to the ERP this time, independently of her willing to use multi-factor authentication.

Risk-based authentication: Example 2

The Sales Manager is working in the office today and wants to access the CRM to create an opportunity following a meeting. He is using his company-issued laptop and is accessing the application which is located on-premise.

CRM system	
Requires 120 points	
LAN	50
Known IP	50
Managed Device	50
IP Range (US)	50
Authentication required	
U&P	10
Mobile App	60
Fingerprint	20

Result – Successful
The Sales Manager clearly exceeds to the points he needs to access the CRM. Once he is authenticated, he can use single sign-on (SSO) to access other applications. He receives a call from the Purchasing Assistant and is able to access the ERP system, and provides the quantity with the part number he is given.



Ultimate flexibility & control

The Policy engine allows you to create new rules and combine existing rules, as well as providing a mechanism to support a range of scenarios with increasing complexity.

Features

User Portal

The User Portal is a feature of AuthControl Sentry®, designed to provide administrators with a configurable solution to deliver autonomy to users for basic self-administration tasks.

The User Portal provides administrators with the capability of giving users direct access, allowing them to execute regular requirements such as changing or resetting a PIN, or provisioning the mobile app.

Provisioning the mobile app

As well as allowing users to change and reset their PIN, the mobile app can also be provisioned effortlessly. An email is sent to the user detailing the steps to provision the mobile app, and a QR code for configuration. Once deployed, users can authenticate access to all of their regular applications using: - The one-time code (OTC) or - PUSH notification

Self service

The self-service User Portal reduces any related cost usually associated with providing support for these actions is redeemed.

Greater efficiency

Swivel Secure's User Portal is designed to deliver greater efficiency for users to execute basic requirements including:

- Changing their PIN
- Resetting their PIN
- Mobile app provisioning
- Hardware token resynchronisation.

Restrictions can be deployed to ensure some policing occurs, ensuring actions are in accordance with security protocols.

swivelsecure

Technology

PINsafe® patented technology

PINsafe® is the patented technology behind the image authentication factors PINpad®, PICpad and TURing, part of the range of authentication factors available with AuthControl Sentry®, the multi-factor authentication solution designed to protect organisations from unauthorised access to their applications, networks and data.

How does PINsafe® work?

Each user is issued a PIN number – however this exact PIN is never typed in.

When a user needs to securely authenticate, they're sent a 10-digit security string – a random sequence of characters or numbers. The security string can be displayed as a graphic (TURing, PINpad® or PICpad) or sent via email or through SMS verification.

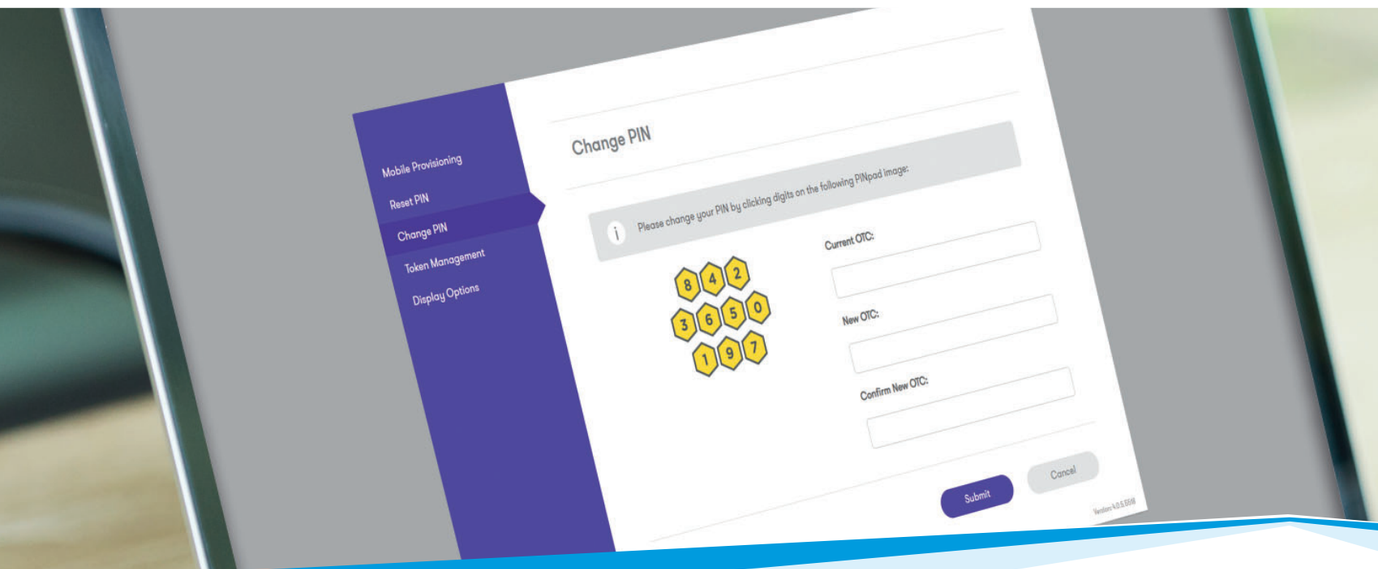
By using the PIN as a positional indicator, a one-time code for authentication can be extracted.

Can you show me an example?

The example below shows your PIN is 1370. On this occasion the security string is 5721694380, so your login code is 5240.

The security string can be integrated with many devices and applications, in a variety of ways for complete flexibility. Including:

- Logging into Windows
- Remote access with F5, Citrix Netscaler and Cisco VPN
- Web access with OWA, Apache, and Microsoft ILS



As PINsafe® prevents the user from ever having to enter their PIN, it prevents any infiltration such as man-in-the-middle attacks.

Factors

Authentication factors

Swivel Secure provides an extensive range of authentication factors to ensure each deployment provides maximum adoption across your whole organisation.

Whether you choose to authenticate utilising the OTC on the mobile app (AuthControl Mobile®, a traditional hardware token or even using your fingerprint, Swivel Secure's AuthControl Sentry® provides ultimate security and configurability to suit your business' security needs.

AuthControl Mobile®: OTC

Each time you are challenged to authenticate, simply use the OTC displayed in the App. As there are 99 codes, the OTC function is versatile enough to be used offline. Once the code has been entered, you will be granted access to your application.

Image factor: PINpad®

A 10-digit code is presented in the form of a number grid in the user's web browser. The user then simply clicks on the images that represent their PIN. Each image clicked then transmits a different OTC code to AuthControl Sentry® to authenticate the user.

Image factor: PICpad

PICpad is an authentication factor that transcends the usual options for language diversification of both employees and customers.

Using the same principles as PINpad®, PICpad displays symbols instead of numbers, providing a coherent meaning in multi-national environments

AuthControl Mobile®: PUSH

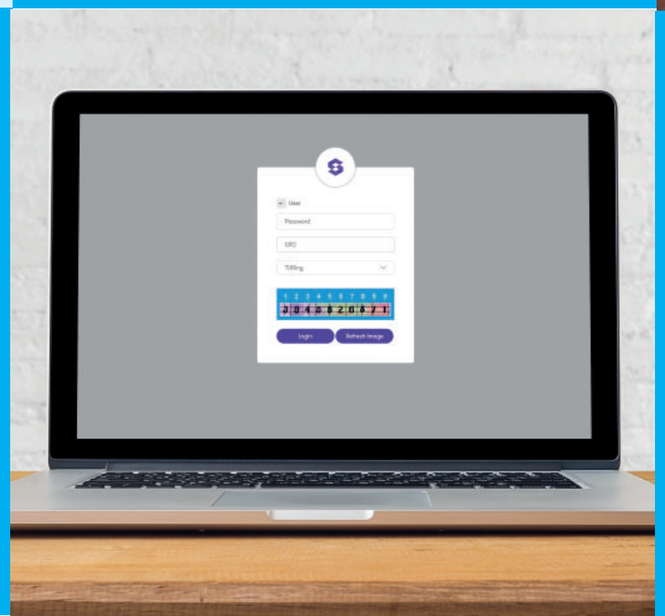
Simply by pressing a button in the mobile app you can confirm authentication with the notification sent directly to your mobile.

Deploy Swivel One Touch® functionality quickly with minimal configuration required.

Image factor: TURing

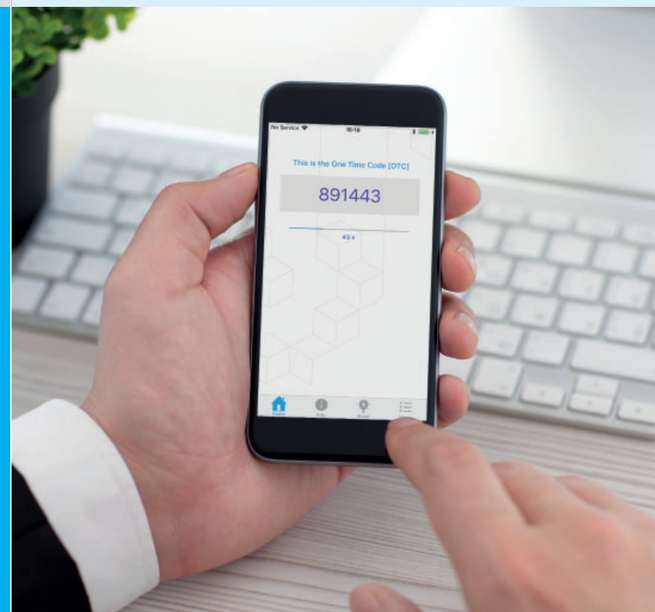
A 10-digit code is presented in the form of a rectangular image in the user's web browser. The user then takes from it the numbers represented by their PIN.

Example: If their PIN is 1370, then they simply take the 1st, 3rd, 7th, and 10th character from the presented image.



AuthControl Mobile®: OATH

The OATH soft token is a time-based token counting from 0 to 60, similar to the traditional hardware token used to access applications though the VPN. The OATH compliant soft token provides the user with a six digit code to authenticate.



Mobile: SMS

To protect the OTC (through SMS) from fraudulent interception, the SMS is protected by PINsafe®. This means the SMS contains a security string of two alphanumerical sequences, and when combined with the user's PIN provides their OTC.

Biometrics: fingerprint

Fingerprint recognition is available for AuthControl Credential® Provider using the Windows 10 biometric framework and the NITGEN fingerprint access controller. Users can authenticate using the NITGEN fingerprint controller or their embedded fingerprint reader in their laptop.

AuthControl Voice

By calling the user, AuthControl Voice vocalises either a one-time code (OTC) or a PUSH notification (YES or NO) to authenticate access to applications. The OTC delivered vocally over the telephone is then typed into the window upon request.

Hardware token

The hardware token provides users with a one-time code (OTC) so they can securely access their application. Every time the button on the hardware token is pressed, it provides a new code, ensuring unauthorised access is prevented.

swivelsecure

Integrations

AuthControl Sentry® is one of the most flexible solutions on the market, integrating with hundreds of applications and appliance software through RADIUS, ADFS, SAML and our own proprietary API – AgentXML.

Whether you need to access Salesforce, authenticating with the mobile app, or logging into Windows Credential Provider using an image authenticator, AuthControl Sentry® supports an extensive range of applications and devices, providing the flexibility and efficiency required for seamless authentication throughout the entire organisation.

Licensing

Flexible licensing plans and pricing models suitable for all organisations. Licensing is charged on a per named user basis.

User Licensing

Flexible licensing plans and pricing models suitable for all organisations.

- Licenses for AuthControl Sentry® are per user
- Each license is inclusive of ALL authentication factors
- MFA, SSO & RBA are including in AuthControl Sentry®
- Available as 1, 3, 5 or 7 year contracts or with perpetual terms

On-Premise

A perpetual license is available for on-premise solutions, or those hosted in a private cloud. Pricing is per user, on a sliding scale, starting from just 10 users. Pricing is cumulative, therefore it is an extremely cost effective way to buy a volume of licenses, rather than a staggered model. Ideally suited to organisations that want to CAPEX the cost of a service upfront, and with stable user numbers.

Cloud

Subscription licensing is available for Cloud deployments, and allows organisations to flex their user requirements as demand changes. No upfront costs and with a flexible and penalty free contract and termination. Ideally suited to organisations that want to OPEX the cost of a service, and with variable user numbers.

Licensing options

Use the table below to compare options for on-premise and cloud licensing.

Type of License	On-Premise	Cloud
Risk-based Authentication	✓	✓
Integrations (SAML/ADFS/RADIUS)	✓	✓
On-Premise & Cloud Applications	✓	✓
All Authentication Factors	✓	✓
AD Agent & AD Sync	✓	✓
Unified Portal with Single sign-on	✓	✓
Reporting	✓	✓
Appliance (Physical/Virtual)	✓	✗
Amazon AWS Image	✗	✓
24x7x365	Optional	✓

Service & Support

To ensure organisations have access to technical support and the latest features, we offer Standard and Premium levels of support for our authentication platform users. Professional services are also available for upgrading, deployment, migration and complex integration.

Entry Level Maintenance Agreement

Support hours: 8/5. Access to software upgrades, updates and bug fixes.

Standard Maintenance Agreement

Support hours: 24/5. Swivel Secure offers 24hr support during working days as standard.

Premium Maintenance Agreement

Support hours: A true 24/7 service, ideal for enterprise organisations requiring expert support immediately.

Professional Services

Swivel Secure provide a range of Professional Services for organisations requiring additional or bespoke technical resources when deploying multi-factor authentication and ensuring compatibility with systems, connections and hardware.

Technical Account Manager (TAM) Service

Our TAM service delivers proactive guidance and centralised service management, ensuring you benefit from priority handling within every channel of Support.

Need to upgrade your Swivel Secure appliance?

Swivel Secure recognise some of the issues that can occur during an upgrade, and offer an upgrade service developed around ensuring there is minimal disruption to the service and your business.

Have a highly complex network infrastructure requiring numerous integrations?

Our team of expert engineers work closely with your Technical Architects and Service Delivery teams to ensure:

- Any design proposed is tailored to your network architecture
- The design meets your organisational architectural and change control requirements

Need to integrate a new RADIUS or SAML device with no previous integration article to work against?

Our team of software developers can be on hand to:

- Assess and develop any new integrations
- Facilitate new plugins
- Respond to feature requests to continuously improve the software.