Single sign-on:

Single sign-on (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.

Risk-based authentication

Risk-based authentication - is a dynamic feature of AuthControl Sentry®, designed to automatically request the appropriate level of authentication to access applications, configured on a wide range of parameters from GeoIP to Device requesting access.

User Portal

Where users can change / reset their PIN and provision the mobile app. Helps to save on overheads by providing users with autonomy.

Licensing

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 with perpetual terms

Service & Support

Entry Level Maintenance Agreement

Support hours: 9am-5pm, 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.
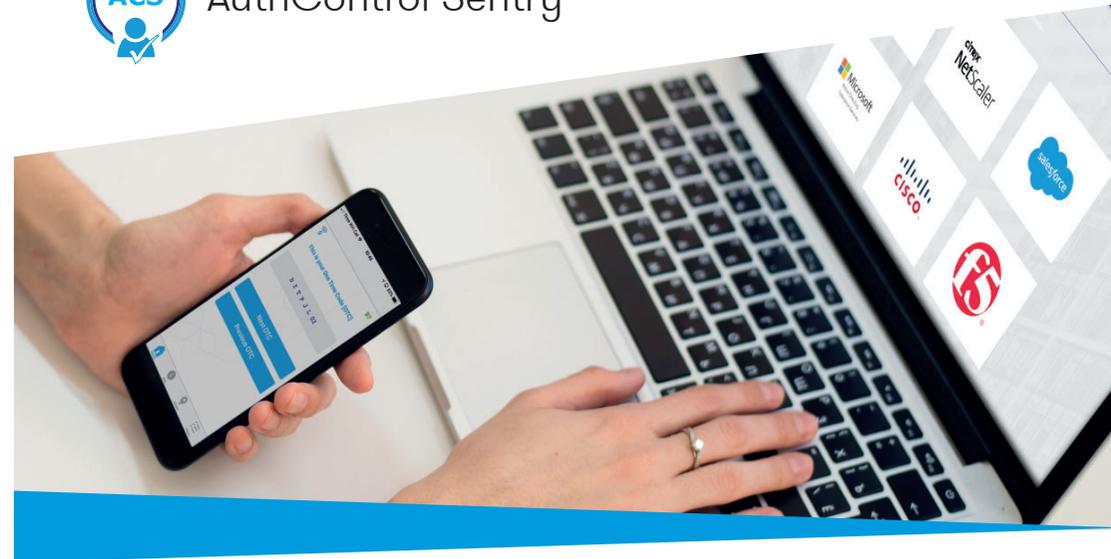
Professional Services

Swivel Secure provides 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.

Search our approved partners

ACS 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 all stakeholders including employees, suppliers and customers.

Deployed in over 54 countries and implemented in enterprises including finance, government, healthcare, education, and manufacturing, AuthControl Sentry® provides organisations with true multi-factor authentication.

What makes AuthControl Sentry® different

✓ Patented PINsafe® technology for ultimate security

✓ 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!

swivelsecure

AuthControl Mobile®:

AuthControl Mobile® provides users with three methods of authenticating including:
- One-time code
- PUSH notification
- OATH soft token

SMS using PINsafe® technology is also available.

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 laptop.
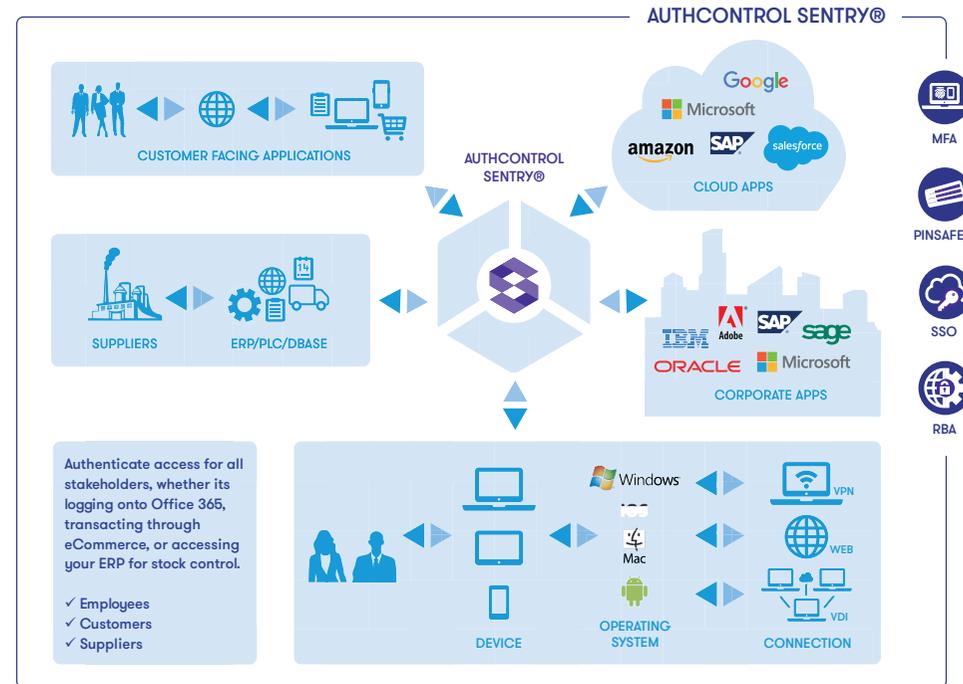
AuthControl Voice

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.

AuthControl Sentry® key features

AuthControl Sentry® delivers key features which are designed to drive efficiency through your business without compromising on security:

AUTHCONTROL SENTRY®

CUSTOMER FACING APPLICATIONS

AUTHCONTROL SENTRY®

Google
Microsoft
amazon SAP salesforce
CLOUD APPS

MFA

PINSAFE®

SUPPLIERS   ERP/PLC/DBASE

IBM Adobe SAP sage
ORACLE Microsoft
CORPORATE APPS

SSO

RBA

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

✓ Employees
✓ Customers
✓ Suppliers

DEVICE

Windows
iOS
Mac
OPERATING SYSTEM

VPN
WEB
VDI
CONNECTION

PINsafe® technology

Is the patented technology behind the image authentication factors PINpad®, PICpad and TURing, part of the range of authentication factors available with AuthControl Sentry®.

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.

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.

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 numbers that represent their PIN. Each image clicked then transmits a different OTC code to AuthControl Sentry® to authenticate the user.

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