swivelsecure

Swivel Secure is considered one of the strongest multifactor authentication platforms in the market. Choose Swivel Secure and feel safe in your security access and identity management.

GARTNER DESCRIBES US AS A COMPANY WITH

'The broadest range of user deployment options for strong authentication in the market place'

SOURCE QUOTE: GARTNER

Cloud applications have made network and application access control more important than ever before. You need to ensure the right people in your organisation access the correct applications in the most simple and intelligent way possible.

Swivel Secure controls access to your network enabling you to define levels of control to each user based on their status, risk and role by simplifying the login process to both cloud and on premise applications.

AUTHCONTROL SENTRY™

Swivel Secure's AuthControl Sentry™ is a multi-factor authentication platform trusted to authenticate your users at the traditional network or cloud perimeter.

Swivel Secure has designed AuthControl Sentry™ which provides the user with:

- The ability to host your authentication system wherever you want: in our cloud, your cloud, or your data centre.
- Delivers risk and role-based authentication to match your authentication method to your level of risk.
- The option of choosing single sign-on or adaptive authentication, as needed.
- A choice of licence options, from one year to perpetuity.
- The ability to change to any token (authentication method).

KEY FEATURES

SINGLE TENANT

AuthControl Sentry™ gives you a dedicated virtual machine in the cloud or on premise. There are no shared, multi-tenanted options, as we believe your security should be at the forefront of our service. We also ensure all AuthControl Cloud customers receive a dedicated fixed IP for their own virtual instance.

ADAPTIVE AUTHENTICATION

Adaptive Authentication adapts to your needs and gives you the best user experience whilst maintaining appropriate levels of access security. Swivel Secure do this by allowing you to choose the appropriate authentication strength and access method depending on the user's circumstances, and the data accessed. The users have the ability to:

- Control and restrict user access times
- Control which user devices have access to which data
- Control access from specified locations

POLICY ENGINE

The policy engine allows you to determine what form of authentication is appropriate for any given user. Using a set of rules and a points system, you can allocate the level of security required on a per-user, per-application basis.

A HIGHLY CONFIGURABLE SERVICE

Whatever you need to access and whatever devices you use, we can guarantee a secure user experience with a wide choice of authentication access methods including mobile apps, SMS, hardware tokens, and voice and desktop clients and image challenges.

- **Authentication Methods**
  Authenticate users via username and password, web-based PINpad or TURing image, mobile app, SMS, OATH token or voice.
- **Access Rules**
  Set access rules based on group, service, IP address, time, date, day, device, operating system, last authentication, X.509 certification or physical location.
- **Automatic Configuration**
  If a particular service has a new requirement for two-factor authorisation, the portal will enable it without having to specifically integrate it into the service or VPN.
- **Adaptive Login**
  If a user has already authenticated once during the day, the policy settings can be configured to allow subsequent access via username and password only.

SIMPLIFIED TRAINING

Having a standard login portal and process means that once a user knows how to access one service they know how to access any service.

ROUND-THE-CLOCK SUPPORT

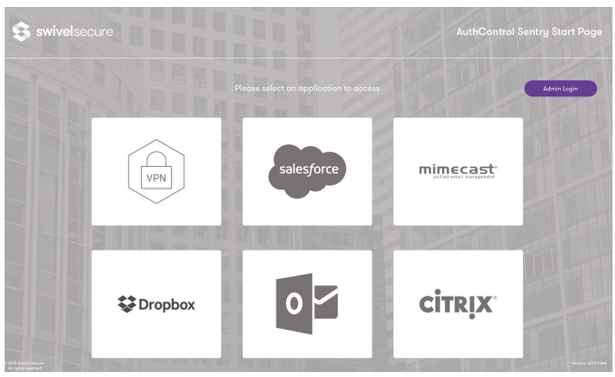
Swivel Secure provides anything up to 24/7 support, with specific service-level agreements to suit your circumstances.

WHY CHOOSE AUTHCONTROL SENTRY™?

There is no shared resource, no shared application programming interface and no shared entry portal. You're unique and we believe your cloud service should be too.

Central Access Point - Unified Access Portal

Swivel Secure's AuthControl Sentry™ brings to you a new unified access portal which is a central access point for all users whether they are via VPN or Cloud applications. This is one single portal to access local services and almost any cloud application including Office365, Salesforce, Google and Dropbox.



The Unified Access Portal is for centralised access and single sign on.

This portal, the authentication engine and the flexible token licensing model Swivel Secure combine to allow users true Single-Sign-On and "risk and role" based authentication in a cost effective manner.

AuthControl Sentry™ allows a simple and realistic rollout of identity management at no additional cost. Swivel Secure's wide range support of user repositories and protocols include: MS AD, ADFS, SAML, RADIUS, LDAP, Databases and more!

Easy to use secure access – Single Sign On

To make life easy and simplify administration, AuthControl Sentry™ provides a seamless and unified approach to authentication. All authentication requests can be routed and controlled via our single sign-on page, based on risk policies you define.

By giving your users one sign-on, to all their applications/services in your business, whether they are connecting to applications locally or via a virtual private network (VPN) or the cloud, it means they do not have to log in several times and can get straight to work.

Cost–Effective Authentication

AuthControl Sentry™ gives you savings through seamless integration and utilisation of your existing infrastructure. Our automated processes for self-service account management significantly reduce IT management time and costs.

Once AuthControl Sentry™ has been purchased there are no expensive additional module options. All the functionality is available and the AuthControl Sentry™ license allows all our integrations, and authentication methods to be used for a single user price. We don't charge extra, if your usage alters. One user, many methods.

Use AuthControl Sentry™ to apply the right level of authentication based on who the user is, the service the user is trying to access or the IP address they are using, so your business can always run at maximum efficiency.

With around 50% of help-desk calls being password related, having a single sign on significantly reduces IT management costs and time. Your savings will only grow as your users use an increasing number of services and systems.

Intelligent Security

Our intelligent, adaptive authentication combines authentication with a risk-and-rules-based policy engine working in tandem with the single sign-on page to ensure access to your data remains safe. Adaptive authentication ensures the user is challenged at the appropriate strength based on a defined RISK profile, ensuring your data is only accessed when and where it should be.

Having one sign-on means users are less likely to have to rely on simple, easy-to-remember passwords because of the need to have so many. Single sign-on means it is easy to track usage and mark privileges, creating an audit trail in the event of an internal breach.

Manageability

Securing access to multiple services requires management and integration with a wide variety of technologies. Our unified approach means validation to all of these goes through a single authentication portal. Access to internal systems is via our Active Directory Agent, a locally installed software application that removes the requirement to share your Active Directory across the internet, whilst maintaining user account synchronisation.

Leading Versatility

AuthControl Sentry™ is the only solution on the market with full two-factor and strong image-based authentication. This is used to support the widest range of business use cases.

Comprehensive Administration and Help Desk

With AuthControl Sentry™ you get automated processes for account management and self-service, saving help desk time. You can also enjoy various support options, from standard business hours to all day round-the-clock support. Swivel Secure provides anything up to 24/7 support, with specific service-level agreements to suit your circumstances.

A Range of Hosting Options

AuthControl Sentry™ is available on premise, or in a private or public cloud, helping solve your authentication challenges irrespective of the size and complexity of your organisation.

Easy to Integrate, Scale and Buy

AuthControl Sentry™ offers you easy integration with Remote Authentication Dial-In User Service, Security Assertion Mark-up Language and Active Directory Federation Services. You can add or remove users at will, and go from 25 users to 25,000 within minutes.

You can gain all this with no upfront capital expenditure, taking advantage of a range of commercial models.

Swivel Secure offer multiple choices for user access to AuthControl Sentry™ using Adaptive Authentication.

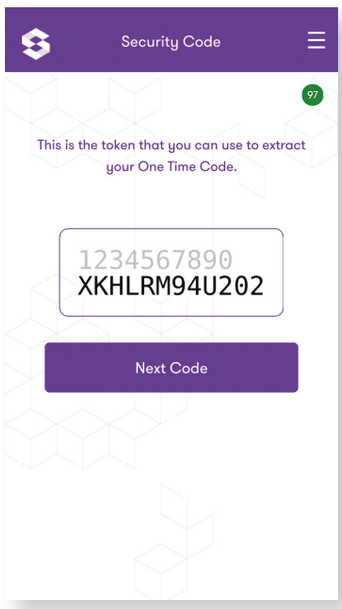
It's no easy task to provide intelligent, secure authentication across the wide variety of systems and endpoints for your company's use every day.

That's why AuthControl Sentry™ covers the widest possible range of configuration profiles with an easy-to-deploy, easy-to-use, single sign-on process. Use Sentry to control access via mobile devices, web browsers, desktop client software, SMS, tokens or voice.

AUTHCONTROL MOBILE™ – MOBILE DEVICE SOFT TOKEN

Authenticate your employees using any mobile device or operating system such as Apple, Android, Microsoft, and BlackBerry. Our mobile clients offer:

- **Increased productivity.** Our app generates a one-time code on demand and works with or without network coverage. This is so your employees can work even without a network connection. One-time codes can be protected with a personal identification number (PIN).
- **Ease of use.** One-touch push authentication allows for fast and simple workflows by authenticating at the press of a key. A notification appears asking users to accept or reject the authentication, with no codes required.
- **Simple management.** The app provides direct access to your support desk, via email or a phone call. While a six-digit one-time code is typically used, a range of lengths can be set during configuration.
- **Affordability.** AuthControl Sentry™ is free to download, with no additional ongoing charges other than normal data costs.

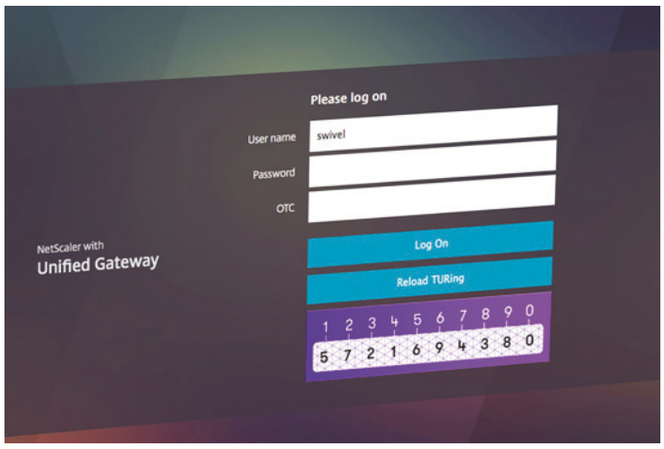


AUTHCONTROL BROWSER™ – BROWSER BASED AUTHENTICATION

Using image-based challenges allows you to leverage a web browser as the authentication factor, helping you solve business challenges relating to the security of, and access to, your data. With our browser-based client you get:

- **Multiple methods.** The image challenge is available as a grid of numbers (PINpad) or a rectangular image (TURing). Each time the image is presented the challenge is changed by displaying the characters in a different order, altering the font or changing the background.
- **Sentry Security.** Sentry Security takes authentication beyond a simple one-time code challenge and uses intelligent authentication to decide if and how a user should be authenticated. Sentry uses a PIN to create unique one-time codes.
- **TURing.** This is a single image used to represent the security string. The TURing image uses placeholders to help the user extract their one-time code. Since the PIN is never entered as part of the login process, the user's PIN is always safe.
- **PINpad.** With PINpad, users simply click on the images representing their PIN. Each number on the PINpad has a second hidden number, which is transmitted as a one-time code.
- **Strong authentication.** Our client provides enhanced security over the use of a username and password alone by creating a changing credential without deploying a two-factor authentication challenge.
- **Reduced costs.** With no physical or soft token to manage, the total cost of ownership and management of our image-based service is lower than any comparable full two-factor authentication service.
- **Simple management.** With no SMS to send, app to download or token to provide, the image-based solution is the fastest and simplest authentication factor on the market to deploy and use.
- **Personalised branding.** PINpad icons and TURing images can be tailored to the colours of your choice.

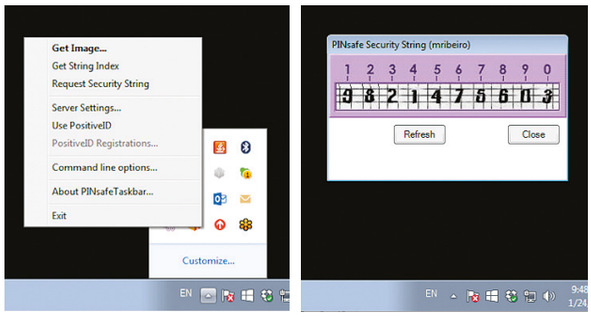
TURing



PINpad

AUTHCONTROL TASKBAR™ – WINDOWS CLIENT SOFTWARE USING TURING OR PINPAD

AuthControl Taskbar is a soft token for Windows 7, 8 and 10 which uses your computer as your token.

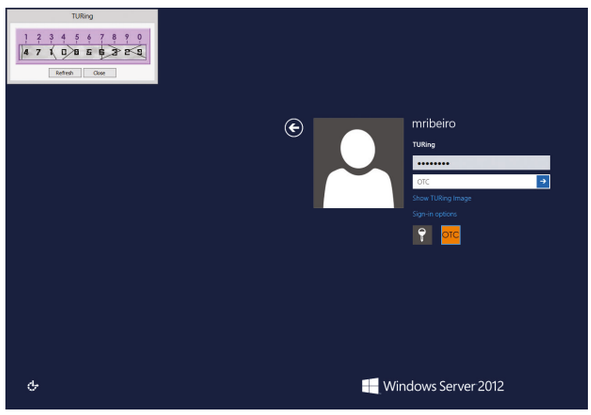


Use it now for:

- **Easy configuration.** Pinsafe can be configured and provisioned with a single click. The desktop client remains conveniently available in the Windows system tray, showing the number of remaining codes.
- **Increased productivity.** The desktop client can provide one-time codes whilst offline, so there is no need for a network connection to provide authentication and access.
- **Maximum security.** One-time codes can be protected with a PIN and nothing is stored on the client, so even if you lose a computer you do not lose your credentials.

AUTHCONTROL DESKTOP™

AuthControl Desktop allows you to add Swivel Secure's authentication solution to the Windows login process. You can use this to control access at local, remote and screen unlock level to the machine. It supports online and offline authentication and also allows you to have enhanced control of Microsoft's Direct access technology. This is done by using a simple security layer added to its inherent automation.



AUTHCONTROL SMS™

SMS remains a powerful way to use existing mobile devices for authentication. AuthControl Sentry™ gives you:

- **Flexibility.** AuthControl Sentry™ is able to send a one-time code via SMS either on demand or after each authentication. This user-centric approach ensures seamless integration of security into the working environment.
- **In-bound SMS.** To defeat man-in-the-middle attacks, the user can be shown a one-time code on screen and then text that code to a known SMS number, along with their PIN, to complete the authentication challenge.
- **Sentry Security.** Sentry combines the use of registered PINs with a random security string to give an extra level of protection and neutralises the risk of code interception during transit, or if phones are lost or stolen.

- **Improved return on investment.** Using mobile phones allows you to capitalise on an existing investment and reduces the need for physical tokens. SMS is easy to deploy, manage and use.
- **Multiple vendor support.** Swivel Secure supports a wide variety of internet-based SMS gateways; the option to use a GSM modem or an email-to-SMS service is also supported.
- **Efficient deployment.** Delivery of one-time codes is very fast and allows rapid deployment to the user base. SMS is supported by all phone manufacturers and devices.
- **Multiple codes.** Sentry provides the option to deliver multiple one-time codes via a single text, to reduce cost and counter network coverage issues.
- **Policy-controlled one-time code length.** While a six-digit one-time code is typically used, a range of code lengths can be set during configuration.
- **No SMS management.** Each SMS message sent by Sentry replaces the previous one, ensuring users always know the correct code to use.
- **Reduced costs.** Direct SMS billing between you and the SMS provider means no upfront costs or management fees are involved.
- **Customisable messages.** The message included with your one-time code can be tailored to provide a greeting or directions for use.
- **Minimal risk.** Use SMS as a second factor for authentication and protect against identity theft and Internet breaches.

AUTHCONTROL KEYFOB TOKEN™

"keyfob" type hardware tokens let you authenticate wherever, whenever. Physical tokens don't require charging, a phone signal or data coverage. Our token security gives you:

- **Protocol support.** We cover all token protocols, including time-based one-time password algorithms and hash message authentication code-based one-time passwords, with Open Authentication (OATH) challenge-response algorithm support. We even support other vendor's tokens so your existing token investment is protected!
- **Ease of use.** While our mobile app and SMS offerings are completely user friendly, for sheer simplicity a hardware token is tough to beat. Simply pick it up, press the button and read the one-time code shown on screen.
- **Cost-effective security.** Our tokens are affordable, at a fraction of the price of similar tokens provided by leading competitors.
- **Managed costs.** Physical tokens have a fixed cost, with no variable extras or usage-based costs from third parties.

AUTHCONTROL VOICE™

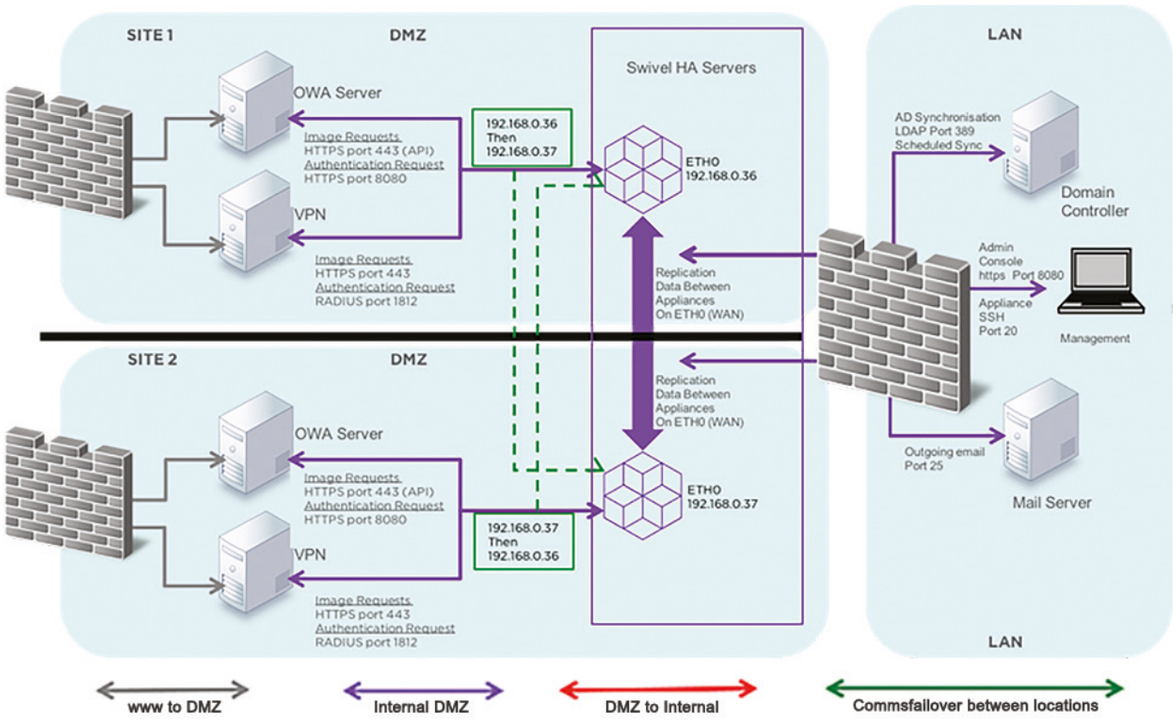
Using phone numbers as a second factor for authentication provides a strong level of security while allowing global access. It's an easy way to protect against identity theft, internet breaches and keep your company data protected.

Using our voice authentication gives you:

- **Reduced costs.** Direct voice billing between you and the voice provider means no upfront costs or management fees are involved, and no requirement for a mobile phone or physical token. Telephone numbers are a universal, stable and affordable way to authenticate.
- **Efficient deployment.** Delivery of one-time codes via voice is fast and allows a rapid deployment to the user base. There is nothing to buy, manage or provision, providing a suitable number to call the user on is stored in Lightweight Directory Access Protocol.
- **Vendor support.** We offer tried-and-tested technical voice delivery via the voice verification leader Nexmo, and are able to support multiple voice service providers directly.
- **Secure environments.** Voice enables authentication in restricted locations when a mobile or a physical token may not be allowed.

The authentication challenge can be configured in multiple ways:

- Requesting a PIN. The user enters their PIN on the phone keypad and then a one-time code is read out. The call disconnects, leaving the user to type in the code.
- Requesting a PIN and then disconnecting the call, after which the login process automatically completes with no further action required.
- Asking the user to press the # key and then disconnecting the call. The login process automatically completes, with no further interaction from the user required.
- Giving the user a one-time code and then disconnecting the call. The user then types in the code.



HOW AUTHCONTROL SENTRY™ WORKS

- **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. You're unique and we believe your cloud service should be too.
- **Active Directory integration**. Access to internal systems is via our Active Directory Agent, a locally installed software application that removes the requirement to share your Active Directory across the Internet, whilst maintaining user account synchronisation.
- **Comprehensive administration**. With our expert team maintaining the infrastructure, the only thing left for you to manage are the integrations, policies and users. All administration is via our simple-to-use, comprehensive graphical user interface.
- **A dedicated offering**. Our AuthControl Cloud gives you a dedicated virtual machine. There are no shared, multi-tenanted options, as we believe your security should be at the forefront of our service.
- **A private firewall**. We offer dedicated and independent firewalls for each customer, allowing tailored security and access control lists.
- **Single sign on**. To make life easy and simplify administration, Sentry provides a seamless and unified approach to authentication. All authentication requests can be routed and controlled via our single sign-on page, based on risk policies you define.

For more information, visit www.swivelsecure.com today.