Protecting identities with intelligent authentication

swivelsecure

Privacy Notice
Mobile App
IOS

Swivel Secure Limited
1200 Century Way, Thorpe Park, Leeds, LS15 8ZA
T +44 113 486 0123 E hq@swivelsecure.com

www.swivelsecure.com

Contents

Version History

Release Date	Description	Version	Author
11/11/2020	Initial Creation	V0	Stela Bordin
18/07/2022	Creation Item 4.1., 4.2., 4.3.	V1	Stela Bordin

1. Scope

All data subjects whose personal data is collected through our Mobile App - IOS, in line with the requirements of the General Data Protection Regulation Europe (GDPR EU & GDPR UK).

2. Responsibilities

2.1. The Data Protection Officer is responsible for ensuring that this notice is made available to data subjects prior to Swivel Secure Limited collecting/processing their personal data.

2.2. All Employees and contractors of Swivel Secure Limited who interact with data subjects are responsible for ensuring that this notice is drawn to the data subject's attention and their consent to the processing of their data is secured.

3. Privacy Notice

3.1. Who are we?

Swivel Secure is a pioneering network security solutions provider. Founded in 2001, Swivel Secure protects thousands of organisations in over 54 countries. Our authentication platform is recognised as a leading standard in authentication technology and is the solution of choice for prominent global organisations. Offering a wide range of authentication options, the Swivel Secure platform delivers two-factor authentication via Mobile Apps, SMS, OATHTokens, Telephony and Strong authentication through integrated in-browser imagery.

Our specialities are: Software Development, Two Factor Authentication, IT Security, SaaS, Tokenless Authentication, Strong Authentication, VPN authentication, Cloud authentication, VDI authentication, and Web application authentication.

The award-winning AuthControl Sentry delivers multi-factor authentication (MFA), combined with single sign-on and risk-based authentication for intelligently securing cloud and on-premise architecture. 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.

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

Swivel Secure has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Swivel Secure and its sub-processors.

Our Data Protection Officer and data protection representatives can be contacted directly here: dataprivacy@swivelsecure.com

The personal data we would like to collect from you is:

Personal Data: Username.

4. Our Solution – AuthControl Mobile App (IOS)

How do users obtain an account?

The company to which the user belongs decides if they will use the mobile application as part of their user authentication. The process consists of providing a specific provision code to use the application. It is not a public process.

How do users obtain a QR code?

As mentioned above, the company to which the user belongs decides if they will use the mobile application or not. A QR Code is generated internally and the user receives it in their corporate email.

4.1. AuthControl Mobile Sentry (AMS)

AMS works with OATH online, PIN (online or offline) and PIN (online or offline) + PUSH policies.

Oath online mimics physical tokens and relies on connectivity with the Swivel Secure appliance.

PIN online shows a One-Time-Code that relies on connectivity with the Swivel Secure appliance.

PIN offline shows a One-Time Code that does not rely on connectivity with the Swivel Secure appliance.

PIN (online or offline) + PUSH shows a One-Time-Code accordingly and the option for PUSH notification.

There are at least three different methods by which the user can provision using AMS. They are the below:

4.2. AuthControl Mobile MSP ("AMM")

AMM works with OATH online + PUSH, PIN (online or offline) and PIN (online or offline) + PUSH policies and provision users from different appliances in one single application.

Oath online + PUSH mimics physical tokens and relies on connectivity with the Swivel Secure appliance and the option for PUSH notifications.

PIN online shows a One-Time-Code that relies on connectivity with the Swivel Secure appliance.

PIN offline shows a One-Time Code that does not rely on connectivity with the Swivel Secure appliance.

PIN (online or offline) + PUSH shows a One-Time-Code accordingly and the option for PUSH notification.

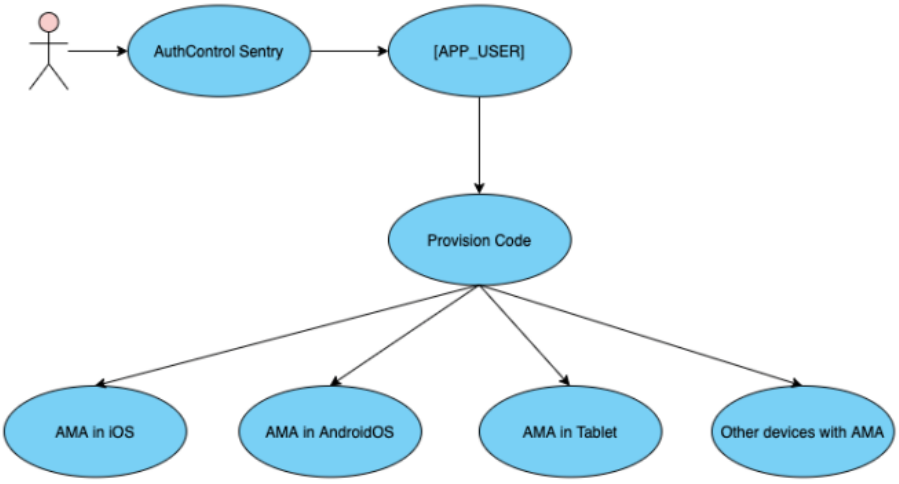
There are at least 6 different provisioning on which the user can provision policies available for AMM. They are the below:

4.3. AuthControl Mobile Authenticator ("AMA")

AMA is restricted to the OATH offline policy.

Oath offline mimics physical tokens and does not rely on connectivity with the Swivel Secure appliance.

The best scenario to use the AMA provisioning policy is the one-to-many provision process. With a single provision code users can provision as many devices as necessary. Example:



4.4. The purpose for which we collect Personal Data

Swivel Secure collects data from you through our **AuthControl Mobile (IOS)**. You provide the data directly into the application, where it will be used only for the purpose of providing authentication to our multi-factor solution.

If you choose not to provide the data required to provide you with a product or feature, you will not be able use that product or feature. Likewise, where we need to collect personal data by law or to enter into or carry out a contract with you, and you do not provide the data, we will not be able to enter into the contract; or if this relates to an existing product you're using, we may have to suspend or cancel it. We will notify you if this is the case at the time.

The table below describes which personal data we collect and the lawful basis for processing this data. We have processes in place to ensure that only those in our organisation who need to access your data can do so.

PII	Collected by	Original Source	For how long is the data retained?	How do we protect the data
Username	Sentry Core	Customers Company Directory/Manually entered	Until the user uninstalls the app and erases the data on the device **For Android:** Manual user configuration on the device **For IOS:** There is a button to remove the user and delete the data	By downloading the application, the customer agrees with the terms of data processing, which informs you of the data that will be kept and, in compliance with this policy, how you can delete it.

4.5. How we use Personal Data

Under the GDPR EU & GDPR UK, personal data is defined as:

"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

In the case of our mobile apps, the data Swivel Secure collects is to:

- Provide mobile authentication.

We will process (collect and use) the information you provide in a manner compatible with the GDPR EU & GDPR UK.

4.5.1. Biometric Data

Our **AuthControl Mobile App (IOS)** may request access to the camera, to authenticate with Face ID. The request can be requested for the exclusive purpose of authenticating the user in a secure manner using Face ID. The app is restricted to users of a single company and it is unique to each user.

4.5.2. Protection of Children

This **AuthControl Mobile App (IOS)** is not intended for users under the age of 18, and we have no intention of collecting personally identifiable information from children (i.e., individuals under the age of 18). If a parent or guardian learns that a child has provided us with personally identifiable information, that child's parent or guardian should contact us. And send a request marked "Privacy-Urgent" to DataProtection@swivelsecure.com if they would like the information submitted by the child deleted from our database. We will use all reasonable efforts to delete such information from our database. Swivel Secure may have liability to you in case of failure to comply with the law or this policy in handling the onward transfer of your Information to third parties.

4.6. Reasons we share Personal Data

Since we only collect authentication data, we follow the established general security policy of never sharing such data.

4.6.1. Biometric Data

Since Swivel Secure does not store Face ID in the internal database, we do not share the data with third parties except with the system provider, which is Apple (you can find the Privacy Policy in this link).

4.7. How do we protect the data

Swivel Secure maintains a comprehensive information security management program that contains administrative, technical, and physical safeguards. Also, the customer can agree with the terms of data processing by **AuthControl Mobile App (IOS)**, which informs that the data will be kept logged and in compliance with this policy, how can delete it.

4.8. How we delete the data

Our application does not store any data. What can do is an "unprovision" the authentication placed by the user or delete the application directly from the mobile phone.

4.9. Our legal basis for processing the personal data

Any legitimate interests pursued by us, or third parties we use, are as follows:

If you are an individual in the European Economic Area (EEA), we collect and process information about you only where we have a legal basis or bases for doing so under applicable EU laws. The legal bases depend on the products and services that your organisation has purchased from Swivel Secure, how such products and services are used, and how you choose to interact and communicate with Swivel Secure website and systems. This means we collect and use your Personal Data only where:

- We need it to operate and provide you with our products and services, provide customer support and personalised features, and to protect the safety and security of our products and services;
- It satisfies a legitimate interest of Swivel Secure (which is not overridden by your data protection interests), such as for research and development, to provide information to you about our products and services that we believe you and your organisation may find useful, and to protect our legal rights and interests;
- You give us consent to do so for a specific purpose; or
- We need to comply with a legal obligation.

If you have consented to our use of Personal Data about you for a specific purpose, you have the right to change your mind at any time, but this will not affect any processing that has already taken place. Where we are using your Personal Data because we or a third party (for example, your employer) have a legitimate interest to do so, you have the right to object to that use; however, in some cases, this may mean that you no longer use our products and services.

If we require your consent for this activity, you may withdraw consent at any time by the company website https://swivelsecure.com/right-to-erasure/.

5. Disclosure

Swivel Secure Limited will not pass on your personal data to third parties without first obtaining your consent as reported in the Purchase Agreement.

5.1. Under what circumstances will Swivel Secure contact me?

Our aim is not to be intrusive, and we undertake not to ask irrelevant or unnecessary questions. Moreover, the information you provide will be subject to rigorous measures and procedures to minimise the risk of unauthorised access or disclosure.

5.2. Retention period

The app will retain your Personal Data until the user uninstalls the app and erases the data on the device. For IOS: There is a button to remove the user and delete the data.

5.3. Your rights as a data subject

At any point while we are in possession of or processing your personal data, you, the data subject, have the following rights:

- Right of access – you have the right to request a copy of the information that we hold about you. Right of rectification – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- Right to be forgotten – in certain circumstances you can ask for the data we hold about you to be erased from our records.
- Right to restriction of processing – where certain conditions apply to have a right to restrict the processing.
- Right of portability – you have the right to have the data we hold about you transferred to another organisation.
- Right to object – you have the right to object to certain types of processing such as direct marketing. Right to object to automated processing, including profiling – you also have the right to be subject to the legal effects of automated processing or profiling.
- Right to judicial review: in the event that the organisation refuses your request under rights of access, we will provide you with a reason as to why. You have the right to complain as outlined in Clause 5.4 below.

At your request, we can confirm what information we hold about you and how it is processed. If we do hold personal data about you, you can request the following information:

- Identity and the contact details of the person or organisation that has determined how and why to process your data. In some cases, this will be a representative in the EU.
- Contact details of the data protection officer, where applicable.
- The purpose of the processing as well as the legal basis for processing.
- If the processing is based on the legitimate interests of Swivel Secure Limited or a third party, information about those interests.
- The categories of personal data collected, stored and processed.
- Recipient(s) or categories of recipients that the data is/will be

disclosed to.

- If we intend to transfer the personal data to a third country or international organisation, information about how we ensure this is done securely. The EU has approved sending personal data to some countries because they meet a minimum standard of data protection. In other cases, we will ensure there are specific measures in place to secure your information.
- How long the data will be stored.
- Details of your rights to correct, erase, restrict or object to such processing. Information about your right to withdraw consent at any time.
- How to lodge a complaint with the supervisory authority.
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether you are obliged to provide the personal data and the possible consequences of failing to provide such data.
- The source of personal data if it was not collected directly from you.
- Any details and information of automated decision making, such as profiling, and any meaningful information about the logic involved, as well as the significance and expected consequences of such processing.

5.4. Complaints

In the event that you wish to make a complaint about how your personal data is being processed by Swivel Secure Limited (or third parties as described in 5 above), or how your complaint has been handled, you have the right to lodge a complaint directly with the supervisory authority and Swivel Secure Limited's Data Protection Officer.

The details for each of these contacts are:

Controller contact details:

1200 Century Way,
Thorpe Park Leeds,
LS15
8ZA UK

DataPrivacy@swivelsecure.com

+44 (0)1134 860 123
+44 (0)1134 860 111

Document owner and approval

The Data Protection Officer/GDPR Owner is the owner of this document and is responsible for keeping it up to date.