Integration FAQ

Integration FAQ

Q). PINsafe will it work in our environment?

A). These are the questions that need to be asked of those wishing to look at PINsafe:

1. What application is PINsafe to integrate with?

2. What is the user repository, i.e. where is the user data stored?

3. What mechanism will be used to supply the security string?

4. What mechanism will be used to supply the PIN to the user?

5. Where is the user data to be stored?

Q). Will PINsafe integrate with access product X,Y,Z

A). Check the integration guides on the Swivel Secure Website. If it is not listed, then check to see if the access device supports RADIUS, XML authentication, and has a customisable front end, then contact support. Some integrations may be chargeable.

Q). Can PINsafe integrate with multiple Data Sources?

A). Yes, there can be one XML data source but multiple AD, LDAP or SQL data sources.

Q). Can PINsafe integrate with multiple Active Directories?

A). Yes.

Q). Can PINsafe integrate with LDAP?

A). Yes, as a source of user data.

Q). Can PINsafe integrate with SQL databases?

A). Yes, as a source of users, and also for storing user data.

Q). Will PINsafe work with Single Sign On?

A). Yes, if they support RADIUS or XML authentication and the entry point can be modified where required. PINsafe itself is not a Single Sign on Productbut offers strong and two factor authentication to such products.

Q). Is there a limit to the number of Applications?

A). For systems with multiple applications and load balanced systems there are no license limitations.

Q). Is there any concurrent login limit?

A). This is only limited by the hardware and software performance.

Q). What are the costs of implementation?

A). Hardware for the PINsafe server, PINsafe licenses, and if dual channel SMS is used then there will be an ongoing cost for the SMS, and maintenance.

Q). Does PINsafe have any resilience?

A). Yes, the PINsafe appliance has a High Availability option using an Active-Active solution at a single or multiple sites. 2.1.21. Q). Is there a software version

Q). Does PINsafe support double byte code languages?

A). Yes.

Q). How many digits can PINsafe be configured to use?

A). 4 through to 10, default is 4. Note: the more digits that are used, the harder it is for users to remember it without writing it down.

Q). Is there a OTC without a PIN?

A). Yes this is the PINless security string, where there is no PIN extraction, i.e. your OTC is the security string. It is not as secure than using PIN protection, but still an option.

Q). If the string is revealed is the system compromised?

A). No, as the pin number will determine the number and order of the security code to be used.

Q). If the Pin is compromised will the login be compromised?

A). No, if dual channel authentication is used, the security string and username must also be compromised.

Q). Will PINsafe stop a man in the middle attack?

A). The user believes they are authenticating against a legitimate system, often DNS is compromised to do this, and the attack could be fully automated. Using Dual Channel contextual authentication, the user can be asked to verify transactions and will immediately spot any misuse.

Q). Can PINsafe deliver multiple strings?

A). Yes. Management of strings becomes more difficult with multiple strings. The benefit is less SMS texts and so may be cheaper, and also allows logins when no SMS is available. PINsafe 3.6 supports the ability to ask the user for a particular string number.

Q). What OS will PINsafe run on?

A). As PINsafe is a Java? application it will run in Apache Tomcat (but in theory could run in any compatible Servlet Container), and should therefore run on any OS that supports a servlet container, this includes Windows?, Solaris? and Linux.

Q). Can I define my own TURing image?

A). Yes. The backgrounds and fonts to be used are specified in the file turing.xml. The backgrounds for the TURing image, plus the settings for these, are all in the folder WEB-INF\singleChannel. Backgrounds are in the backgrounds sub-folder, and fonts in the fonts sub-folder, The file turing.xml, requires to be edited with the file names in the appropriate list. Backgrounds must be jpgs, but do not have to be the right size, although they must be at least 280 by 33 pixels. If they are larger than this, PINsafe will cut a random rectangle from the image provided.

Q). Can a security string use characters instead of numbers?

A). Yes, and combinations of these in version 3.1.2 onwards.

Q). Do Swivel provide a list of SMS providers?

A). The product has a list of SMS providers in the product. New ones are tested and added over time.

Q). Can I add my own SMS provider?

A). Yes, although there are some configuration strings that need to be set. Contact Swivel for support.

Q). Does PINsafe have its own database?

A). Yes, to store username against the PIN where the internal database is used. An external database can also be used.

Q). What is a PINsafe Agent?

A). An agent is a program that communicates with the PINsafe server, such as the ISAPI filter.

Q). Can the PIN numbers be viewed in the database?

A). No, the PIN numbers are never revealed.

Q). Are PIN numbers encrypted?

A). Yes

Q). Are communications with the PINsafe Server encrypted?

A). Yes if SSL is enabled on the server and requested by the application.

Q). What algorithms are used to generate the security string?

A). The security string is randomly generated using the Sun Java Secure random method. This class provides a cryptographically strong random number generator (RNG) A cryptographically strong random number minimally complies with the statistical random number generator tests specified in FIPS 140-2, Security Requirements for Cryptographic Modules, section 4.9.1. Additionally, SecureRandom must produce non- deterministic output and therefore it is required that the seed material be unpredictable and that output of SecureRandom be cryptographically strong sequences as described in RFC 1750: Randomness Recommendations for Security.

Q). Is it possible to authenticate a User with Password and One Time Code (OTC), even in a e.g. IPSec VPN, where you are not able to integrate a graphical image, but I could get my OTP via SMS or mobile phone client?

A). Yes, select PINsafe as the authentication RADIUS server. PINsafe can also check the AD password entered is correct.