

PINsafe Version 3.6 Release Bulletin

1 Introduction

This release bulletin relates to Version 3.6 of the PINsafe platform. The following features have been added

- Multiple Security Strings per message: It is now possible to send multiple security strings within a single text message. At the time of authentication the user is shown which string to use to authenticate.
- Animated TURING images: It is now possible to animate the TURING, BUTTOn and PATTErn images as increased resistance to malware attacks.
- In built repository browser: PINsafe 3.6 now has an inbuilt repository browser that can view the contents of any LDAP based repository to which PINsafe is integrated. This speeds up initial configuration and subsequent fault analysis
- Agent/NAS authentication modes: It is now possible to configure Agents and NASs to only allow certain authentication modes, eg dual channel only.
- Auto PIN-Reset: It is now possible to automatically resend a user a new PIN when their PIN expires, rather than locking the account.
- Idle Status: Accounts that are locked because the user has been idle are now distinguishable from accounts that are locked for other reasons
- Account Expiry: It is now possible to set expiry dates on accounts in the XML repository.

Known Issues with Version 3.6

- Certain features, eg Agent/NAS authentication modes, do not work with peers. The peering feature is deprecated.
- **Some older PINsafe installations may also need to upgrade the version of Java to user PINsafe 3.6, Java Version 6.0_06 is recommended**
- Check Password with Repository only works for PAP RADIUS
- Using Windows-style syslog entries (\\server\device) within Linux causes ALL logging to fail.

Version 3.6 History

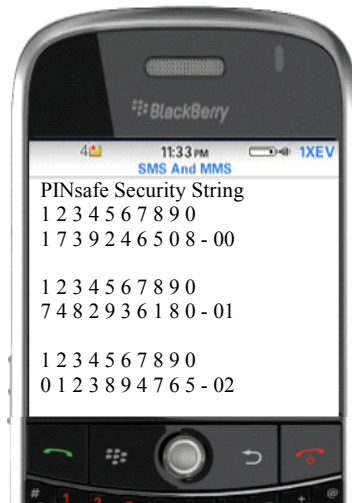
Build 3275 First release

2 Multi-String SMS Model

This new mode of operation for dual-channel authentication enables users to be sent security strings in batches rather than one at a time. This feature uses SMS messages concatenation so that the single batch of security strings is sent using two separate SMS messages, but these messages appear as a single message in the user's SMS inbox.

The user experience is as follows:

1. The user is sent a single text message containing a number of security strings, eg 10.



2. When the user wishes to authenticate they indicate that they wish to authenticate using SMS, and the log-in page informs them which security string from within the message they have been sent, they should use. In this example this is shown by the 02 in the field after the OTC field

PINsafe - Login

Username:	<input type="text" value="fred"/>
Password:	<input type="password" value="••••••••"/>
OTC:	<input type="text" value="••••"/> - <input type="text" value="02"/>
	<input type="button" value="Get Index"/> <input type="button" value="Login"/>

3. So in this example if the user's PIN was 2468, they would enter 1397 as their OTC, the -02 being added automatically
4. The next time they authenticate they will be prompted to use the next string.
5. The user will be sent a new batch of strings after they have used their last string.

In fact the user can use any string later in the sequence than the one prompted for, however if they do this they need to specify which string they are using by appending the index to the one-time code. In the above example the user may choose to use the last string to authenticate, in which case they would enter the one-time code based on the last string followed by -09.

This would be a means by which a user can instigate the sending of a new set of strings.

It is also possible to configure PINsafe to allow a user to request a new set of security strings at any time.

Benefits:

This feature means that 10 authentications can be supported via a single message (sent using 2 concatenated text messages). This reduces the SMS costs for this form of authentication by up to 80%

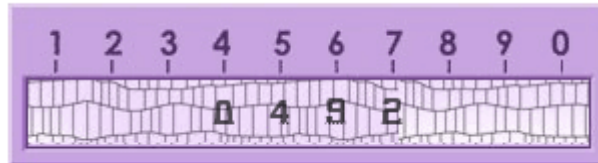
This also means that a user can have up to 10 security strings available to them; lessening concerns about lack of mobile phone coverage at the point of authentication.

3 New Single-Channel Image Options

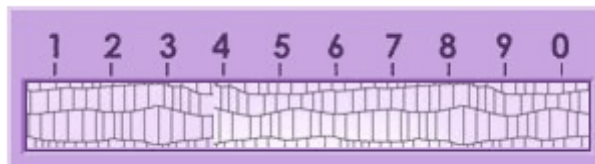
A number of new image options have been made available in PINsafe Version 3.6.

These are all available from the Server → Single Channel screen.

These include the ability for images to be animated, so that only a subset of the characters with the security string are visible at any one time.



Additionally you can specify how many times the image is shown and then optionally ensure that no characters remain on display.



Benefits

These features provide resistance against forms of malware attack. Additional resistance to OCR type attacks is provided by being able to mixed fonts and text positioning and also to adjust the contrast (Alpha value) of the strings.

These animated images also make shoulder-surfing attacks harder as the security string digits are only visible for a relative short time.



4 LDAP Repository Browser

It is now possible to browse LDAP repositories from within PINsafe; this assists with installations and post-install fault-diagnosis.

The browser can be accessed in two ways. Firstly from the repository definition screen and secondly from the Repository->Group Definition screen.

Repository name: adtest

Path: OU=PINsafeDemo,DC=test,DC=local

[Up a level](#)

Groups:

CN=PINsafe_Admin	Select
CN=PINsafe_Resellers_ES	Select
CN=PINsafe_Resellers_GE	Select
CN=PINsafe_Resellers_PT	Select
CN=PINsafe_Resellers_UK	Select
CN=PINsafe_SMS	Select
CN=PINsafe_Users	Select

Users:

[CN=Customer Test](#)

The browser can navigate throughout directory structure and see the number of users in any given group and then list them. For individual accounts the browser can display the attributes associated with account.

User attributes: CN=Test User,OU=PINsafeDemo,DC=test,DC=local

Attribute	Value(s)
cn:	Test User
displayName:	Test User
name:	Test User
sn:	User
givenName:	Test
sAMAccountName:	Test.User
userPrincipalName:	Test.User@test.local
mail:	(none)
telephoneNumber:	(none)
mobile:	(none)

Benefits

The ldap browser resides on the same machine as the PINsafe application and uses the same ldap credentials to bind to the LDAP server, it is a reliable way to prove that PINsafe has the the required access to the directory server. It can be used to:

- Diagnose issues with routes and firewalls
- Diagnose issues with account permissions and credentials
- Confirm group definitions for use on the PINsafe server
- Confirm attribute definitions for Transports.

5 Agent/NAS Authentication Modes

It is now possible to restrict agents or NASs to specific authentication modes. So, for example, if PINsafe is being used to authenticate a number of different services some dual channel some single channel, you can explicitly state what form of authentication each agent can allow.

Server>Agents

Please enter the details for any PINsafe agents below. Agents are permitted to access the AgentXML interface.

Agents: Name:	<input type="text" value="local"/>
Hostname/IP:	<input type="text" value="127.0.0.1"/>
Shared secret:	<input type="password" value="●●●●●●●●●●"/>
Group:	<input type="text" value="--ANY--"/>
Authentication Modes:	<input type="text" value="Dual Channel Only"/> <input type="button" value="Delete"/>

This is the same for RADIUS → NASs

RADIUS>NAS

Please enter the details for any RADIUS network access server via the RADIUS interface.

NAS: Identifier:	<input type="text" value="VPN1"/>
Hostname/IP:	<input type="text" value="vpn.swivel.test"/>
Secret:	<input type="password" value="●●●●●●●●"/>
EAP protocol:	<input type="text" value="None"/>
Authentication Mode:	<input type="text" value="Single Channel"/>
Group:	<input type="text" value="--ANY--"/>
Change PIN warning:	<input type="text" value="No"/>

The default is to allow any mode of authentication.

Benefit

This allows different levels of authentication to be required for access to different services, allowing appropriate levels of security to be implemented.

6 Auto PIN Change

Users of PINsafe may have a policy that requires users to change their PINs on a regular basis. Up until version 3.6, if a user did not change their PIN in time, their account would become locked.

As an alternative PINsafe version 3.6 can automatically send the user a new PIN in the event of their current PIN expiring.

This removes any helpdesk overhead and avoids the user being locked. It does not mean that the user cannot subsequently set their own PIN if this is still required.

Benefits

Reduces management costs, prevents users becoming locked.

7 Idle Accounts

Accounts that have become locked due to lack of use can now be distinguished from accounts that have been locked due to other reasons. The status of "Inactive" can now be used to filter users on the user admin screen and accounts locked due to inactivity are shown underlined rather than **bold** for accounts locked for other reasons.

Max No. Users: (3 users in this repository)

Users per page:

Repository:

State:

Username:

Members of group:

View:

Username	Admin	Helpdesk	Single	Dual	Swivlet	PINless
<u>test2</u>	✓	✓	✓	✓	✓	

Benefits

Being able to identify idle accounts can help manage licence usage as well as identify possible issues with the provisioning (or de-provisioning) of users.

8 Automatic Account Expiry

When manually adding accounts to PINsafe, via the XML repository, it is now possible to set an expiry date for this account.

Username:	<input type="text" value="test"/>
First name:	<input type="text" value="test"/>
Last name:	<input type="text" value="user"/>
Email address:	<input type="text" value="test.user@test.com"/>
Phone number:	<input type="text"/>
Custom attribute:	<input type="text"/>
Expiry Date:	<input type="text" value="05-06-2009"/>
Server groups:	
PINsafeAdministrators	<input checked="" type="checkbox"/>
PINsafeUsers	<input checked="" type="checkbox"/>
<input type="button" value="Reset"/>	<input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>

In the example above, this account is set to expiry on the 5th June. The first time that the repository is synchronised on or after that date, the account will be removed from the repository and therefore deleted from (or marked as deleted in) the database

Benefits:

This allows for the creation of temporary accounts, eg for short-term contractors, that expiry automatically.