

## PINsafe Version 3.5 Release Bulletin

### 1 Introduction

This release bulletin relates to Version 3.5 of the PINsafe platform. The following features have been added

- Session Sharing; the ability for security sessions (TURING images) to be shared across an HA pair
- Users "mark as deleted" so that accounts mistakenly deleted can be recovered without need to re-issue a new PIN
- Improved user admin screen to provide more listing and searching options
- Easier setting of job schedules
- Ability to specify whether Helpdesk users are global or restricted to their own repository

**This release also addresses the following issues.**

- All passwords that are part of the configuration are now stored in an encrypted form in the config.xml file.
- Under certain circumstances PINsafe would misleadingly report an Array Index out of bounds exception during RADIUS authentication
- Stack traces, when they occur, are now written to the log files
- It is now possible to instigate a user-sync job via an Agent-XML API call.
- The restriction of only allowing one Syslog server to be defined has been removed.
- It is now possible to delete all users from a repository.
- Adding a user to the XML repository that duplicates an existing user in another repository, then deleting that user, no longer results in the original user being deleted. A consequence of this change is that users deleted from the XML repository are not deleted from the PINsafe database until the next User Synchronisation.

### Known Issues with Version 3.5

- Upgrading to 3.5 is not supported for PostGres
- Certain special characters cause problems in Open LDAP and Novell e-Directory

- When user peering, only users that are in repositories to which PINsafe is connected will be peered

None of these features are urgent patches and users need only upgrade if they need any of these new features

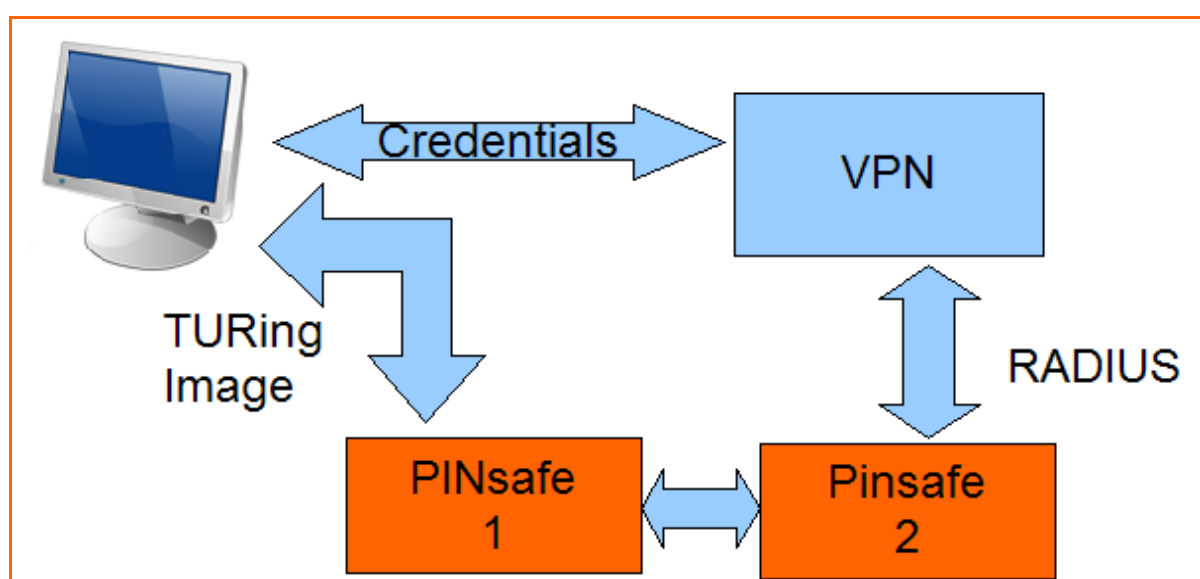
### Version 3.5 History

Build First release r2842

## 2 Session Sharing

For Active-Active HA pairs, when using single channel or on-demand dual channel, it has been a requirement that the user authenticate to the same server from which they load-retrieved the security string. This has prevented PINsafe servers from being deployed in a truly load-balanced way.

Version 3.5 of the PINsafe software now removes this requirement. Now when a session is started on one PINsafe server, that session is shared with the other PINsafe server, so that either server can accept the subsequent authentication request.



**Figure 1** Session sharing means if PINsafe server 1 supplied the TURING image the VPN can still authenticate the user via PINsafe 2

The mechanism for this is that the sessions that are "in progress", ie where a user has requested an image or message, but not yet authenticated, are stored in a cache that is shared between the two servers. In a similar way to the way that the databases are shared.

The session sharing can, but need not be, used with an Active-Active pair. Clearly to support the use of this feature there must be sufficient bandwidth, with low-enough latency, between the two servers.

The use of session sharing is determined by an .xml file within the PINsafe application.

### 3 Mark as Deleted

There has been incidents in the past where AD administrators have made changes within the AD domain that have had adverse affects on the PINsafe installation. For example moving groups, renaming domains or containers.

These changes have resulted in PINsafe removing a number of accounts, as these accounts are no longer members of the specified PINsafe groups.

To limit the impact of such changes it is now possible to configure PINsafe to mark accounts as deleted when they appear to have been removed from the PINsafe group. An account that is marked as deleted is still retained on the system, although it is disabled.

Please enter the details for accessing Active Directory.

Hostname/IP:	<input type="text" value="192.168.0.165"/>
Username:	<input type="text" value="Administrator@test.loc"/>
Password:	<input type="password" value="....."/>
Allow self-signed certificates:	<input type="button" value="No"/> ▾
Username attribute:	<input type="text" value="cn"/>
PIN attribute:	<input type="text" value="cn"/>
Password attribute:	<input type="text" value="cn"/>
Import disabled state:	<input type="button" value="No"/> ▾
Ignore FQ name changes:	<input type="button" value="Yes"/> ▾
Mark missing users as deleted:	<input type="button" value="Yes"/> ▾

**Figure 2** Setting the mark as deleted option. This option is set on a per-repository basis

If, in a subsequent sync job, the account reappears, the account is re-enabled, the user will still be able to use their existing PIN. If the account really does need to be deleted, then all Mark as deleted accounts can be purged from the system.

<input type="button" value="Search"/> <input type="button" value="Reset"/> <input type="button" value="Purge"/> <input type="button" value="Undelete"/> <input type="button" value="User Sync"/>							
Username	Admin	Helpdesk	Single	Dual	Swivlet	PINless	
1234	✓	✓	✓	✓	✓	✓	
a1	✓	✓	✓				
<del>abadmin</del>	✓	✓	✓	✓	✓	✓	
adhelp	✓	✓	✓	✓	✓	✓	
BillyBob	✓	✓	✓	✓	✓	✓	
graham	✓	✓	✓	✓	✓	✓	
test10	✓	✓	✓	✓	✓	✓	

**Figure 3** User list showing users marked as deleted

This means in the event of the mistakenly deletion of accounts, the mistake can be rectified without needing to issue new PINs to the affected users.

As a consequence of this change, the restriction that all users cannot be deleted from a repository has been removed since if all users in a repository are removed in error, they can now be restored.

Note that this option is disabled by default. Administrators are encouraged to enable it for increased data safety.

It should be observed that users marked as deleted still count towards the total user count.

## 4 Improved User Admin Screen

The User Admin screen has always had the ability to list users and apply a range of filters to that list. 3.5 adds a filter for restricting a search to a specific group.

Max No. Users: 500 (5 users in this repository)  
 Users per page: 100  
 Repository: adtest  
 State: All  
 Username: Contains  
 Members of group: two (selected), ---ANY---, special, PINsafeAdministrators, PINsafeUsers  
 View: two (selected), special, PINsafeAdministrators, PINsafeUsers

Buttons: Search, Reset, Purge, Undelete, User Sync

Username	two	special	PINsafeAdministrators	PINsafeUsers
1234	✓		✓	✓
adhelp	✓		✓	✓
BillyBob	✓		✓	✓
graham	✓		✓	✓

**Figure 4** Setting the user list to only show members of a specific group. These features are particularly useful when diagnosing

Version 3.5 also adds options for listing different sets of user attributes. For example, you can list the transports that a user is assigned to use, along with their destination attributes, eg email address and telephone number.

View: Transport

Buttons: Search, Reset, Purge, Undelete, User Sync

Username	Security String		Alerts	
	Transport	Destination	Transport	Destination
1234	iTagg	447817360285	SMTP	c.russell@swivelsecure
a1				
adhelp				
BillyBob	iTagg	4478171234567	SMTP	bb@swivelsecure.com
graham				

**Figure 5** user list, showing the transports associated with each user

You can also list the groups of which they are a member. These features are particularly useful when diagnosing issues related to repository integration.

View: Groups ▾

Search Reset Purge Undelete User Sync

Username	two	special	PINsafeAdministrators	PINsafeUsers
1234 ▾	✓		✓	✓
a1 ▾		✓		
adhel ▾	✓		✓	✓
BillyBob ▾	✓		✓	✓
graham ▾	✓		✓	✓

**Figure 6** User list showing group membership

## 5 Easier Job Scheduling

Previously the setting of job schedules for repository synchronisation etc were specified using a cron string format eg:

0 0 \* \* \* ? meant run the job on the hour every hour.

Version 3.5 adds a tool to help with the setting of these jobs so that you can easily specify commonly used schedules.

Import disabled state: No

Ignore FQ name changes: Yes

Mark missing users as deleted: Yes

Port: 389 (Dc)

Synchronization schedule: Every hour at 17 minutes past the hour

Apply Reset

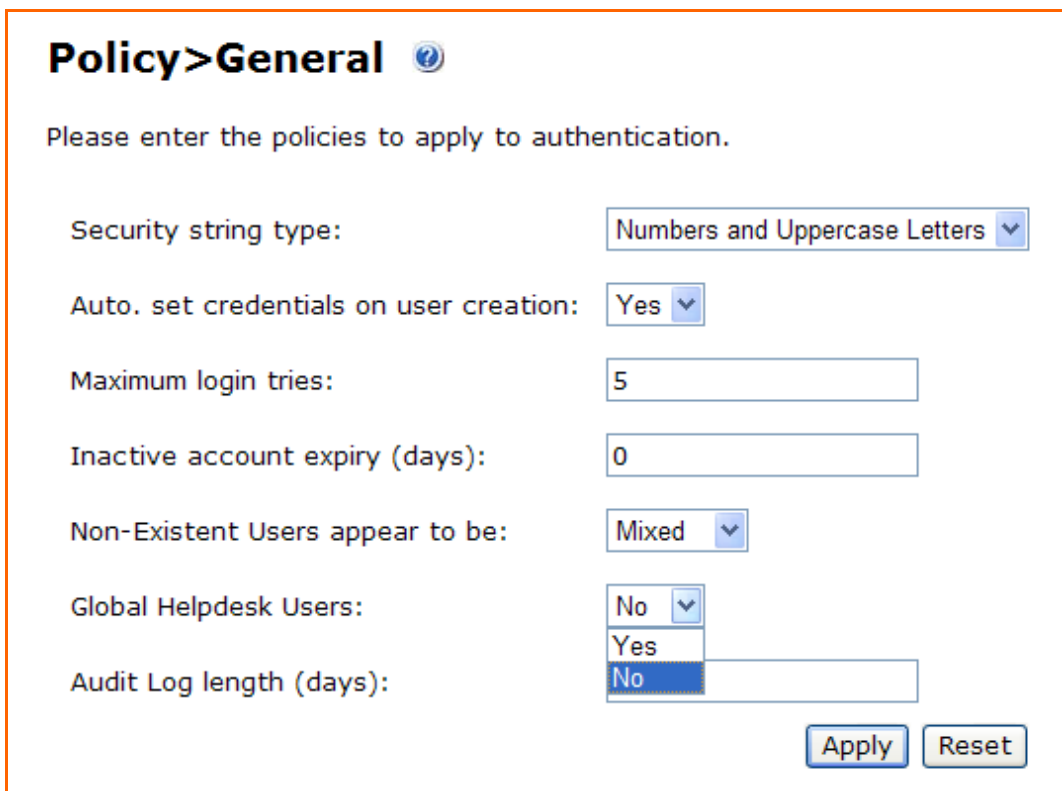
**Figure 7** Setting Job Schedule

It is also possible to specify the schedule using the existing cron format, by selecting custom, so no flexibility has been lost.

## 6 Helpdesk users

Version 3.4 introduced the concept of a delegated helpdesk user. This meant that a helpdesk user could only manage the accounts that were in the same repository as their account.

Version 3.5 makes this an optional feature, so that if required PINsafe can allow a helpdesk account to manage all the accounts on the system. This is implemented by selecting Global Helpdesk Users to Yes on the Policy General screen.



**Policy > General** ⓘ

Please enter the policies to apply to authentication.

Security string type:	<input type="text" value="Numbers and Uppercase Letters"/>
Auto. set credentials on user creation:	<input type="text" value="Yes"/>
Maximum login tries:	<input type="text" value="5"/>
Inactive account expiry (days):	<input type="text" value="0"/>
Non-Existent Users appear to be:	<input type="text" value="Mixed"/>
Global Helpdesk Users:	<input type="text" value="No"/>
Audit Log length (days):	<input type="text" value="No"/>

**Figure 8** Setting Global Helpdesk Policy