



PINsafe
Reference Manual
Version 3.8

Contents

Table of Contents

Introduction..... 5

Getting Started with PINsafe 3.7..... 6

 Setting the PINsafe Database..... 6

 Setting the Internal Database..... 7

 Setting the Database Mode..... 7

 Configuring Slave Mode..... 7

 Configuring Synchronized Mode..... 8

 To use this mode go to the Mode->General screen and select Synchronized and then click apply.....8

 Configuring the user repositories..... 8

 Using the XML Repository..... 8

 License Key..... 10

Integration..... 11

 Integrating with an external database 12

 Integrating with user repositories..... 14

 Using Groups with User Repositories..... 14

 Importing Disabled State..... 16

 Ignoring Fully Qualified (FQ) name changes..... 16

 Marking missing users as deleted..... 16

 Considerations for multiple repositories..... 17

 Configuring the XML Repository..... 17

 Configuring an Active Directory Repository..... 18

 Configuring Other LDAP Directory Servers as Repositories.....25

 Other repository types..... 28

 Deleting a Repository..... 28

 Integrating with Transport Classes..... 29

 Configuring transports in shared database PINsafe installations..... 30

 How to integrate PINsafe with a GSM Modem..... 31

 How to integrate PINsafe with an SMS service Provider..... 32

 Integrating via SMTP..... 33

 Integrating with Agents using Agent-XML..... 34

 Using the User ChangePIN application..... 35

 How to integrate PINsafe with an IIS Website..... 37

 How to write an Agent..... 40

 Integrating using RADIUS..... 40

 RADIUS Groups..... 42

 How to integrate a VPN with PINsafe using RADIUS..... 43

PINsafe Manual

Two Stage RADIUS Authentication.....	44
Integrating with 3rd Party Authentication systems.....	48
Integrating with other Authentication Servers.....	49
Peering PINsafe servers.....	49
PINsafe as a RADIUS proxy.....	51
Multiple PINsafe servers using a single database.....	52
Operation & Maintenance.....	53
Tasks.....	53
Data Migration.....	56
Job.....	56
Session Clean Up.....	56
Peer Synchronization.....	57
Inactive User Check.....	57
PIN expiry check.....	57
Logs and Alarms.....	58
XML Logging.....	58
Syslog.....	59
SMTP (email) Logging.....	59
Administrator's Guide.....	61
Setting Policies.....	61
User Policies.....	69
Single Channel.....	70
Dual Channel.....	71
Alerting Users.....	71
Managing Users.....	73
Adding User Groups.....	73
Adding Users.....	74
Appendix A Building and Deploying PINsafe server.....	80
Upgrading from PINsafe version 3.2 onwards.....	80
Architecture.....	82
PINsafe Deployment.....	83
Protecting the PINsafe Admin Console.....	83
Configuring the filter.....	83
Activating the Filter.....	86
Filter in operation.....	87
Session Sharing.....	87
Appendix B Windows Installation of the Java Comm API.....	88
Appendix C Active Directory/LDAP Groups and Attributes.....	89
User rights.....	89

PINsafe Manual

Simple AD Group and Attribute example.....	90
More Complex AD Group and Attribute example	91
Appendix D PINsafe Installation details.....	95
Appendix E Setting Schedules and CRON Strings.....	96
INDEX.....	97

Introduction

This document provides a general overview of PINsafe version 3.8, its key features and a quick start guide to the Administration console. It also covers what you should know about your installation of PINsafe and how to support and maintain your installation of PINsafe.

The key new features are

1. New Mobile Client provisioning model, to increase security.
2. New inbound SMS authentication to increase security and reduce costs.
3. New inbuilt reporting capability.
4. New account management options, eg time-limited account locks
- 5.

More details can be found within the associated Release Bulletin, available from www.swivelsecure.com

An important part of this document is the record of the installation, covered in Appendix D PINsafe Installation details. It is recommended that this section is completed at the time of installation and kept with the server or elsewhere where it can be found easily if required. A copy of the installation record needs to be sent to Swivel Secure for their records; this can be sent to

e-mail support@swivelsecure.com
fax +44 1937 547 590

Getting Started with PINsafe 3.8

This guide assumes that there is a PINsafe Version 3.8 server installed and running. Information about building and deploying a PINsafe server is available in Appendix A Building and Deploying PINsafe server.

This section follows the steps required to get a basic PINsafe installation up and running.

There are three fundamental settings that need to be completed to get a PINsafe server up and running.

1. The PINsafe Database
2. The Database mode of operation
3. Any associated user repositories

Setting the PINsafe Database

PINsafe needs a database to store PINsafe account information. This can be an internal or an external database.

On install the PINsafe server comes with a shipping database; this is a single user read-only database that has the user account:

Username: admin

PIN: 1234

Whilst this option is selected as the database it will only be possible to login to the admin console using these details.

Therefore to log in for the first time, enter admin in the username field, click on start session, then enter the first four digits of the Turing image into the OTC field, then click log-in. (The password field should be blank)

The first stage in getting started with PINsafe is to configure the database that you wish to use to store PINsafe account details. This can either be the internal database that comes with PINsafe or it can be a separate external database. PINsafe supports a range of SQL/JDBC databases: consult with your reseller or with Swivel for more details.

In deciding what database to use you need to evaluate the relative merits of the two approaches.

Factor	Internal Database	External Database
Simplicity	Very simple, single-click deployment.	Requires some database set-up and configuration
Flexibility	No Flexibility	Flexible solution allowing multiple PINsafe and Multiple Database servers as required
Performance	Local database means good performance.	Performance needs to be considered but PINsafe is not a

PINsafe Manual

		particularly database intensive application
Availability	Availability determined by the server it is deployed on. Difficult to back-up database, therefore not easy to support site resilience	Available can be improved by using database clustering technologies. External database easier to back-up and replicate
Security	Internal and encrypted	All sensitive data is encrypted. Encrypted database drivers can also be used.

It is assumed that an external database will be more appropriate to larger, multi-site installations and the internal database for use for single site installations. For details integrating with an external database refer to [Integrating with an external database](#) .

Username Case Sensitivity

You can select whether usernames are case sensitive or not. You may need to set usernames to be case insensitive if that is what the users are used to (eg Windows usernames are not case sensitive). When user names are not case sensitive a user with a username of Chris can authenticate a Chris, chris,chrIS etc.

NOTE: Case sensitivity is also affected by settings in your database, if you use an external database. If you require case-sensitive passwords, you also need to ensure that your database is set to be case sensitive.

Setting the Internal Database

To use PINsafe's internal database go to the Database menu, select Internal from the drop down menu, then click apply. There may be a slight delay as PINsafe creates the tables in the database. You then need to create an admin account, see [Configuring the user repository](#). If another database type is required refer to the section on [Database Integration](#)

Setting the Database Mode

PINsafe supports two different database modes; synchronized and slave. Synchronized will mean that the PINsafe server will synchronize with a user repository (e.g. Active Directory) in order to create (or delete) accounts from the PINsafe server. A PINsafe server running in slave mode will not create or remove accounts from the database but will act as an authentication server for all the accounts that exist in the database. A slave PINsafe server relies on another PINsafe server to add and remove accounts.

Configuring Slave Mode

In slave mode there is no user repository. When configuring PINsafe to use slave mode it is therefore important that the database that you have defined has users (and admin users) already in it. Once you select the slave mode you should go to the user admin screen to ensure that the users exist on the server.

Configuring Synchronized Mode

To use this mode go to the Mode->General screen and select Synchronized and then click apply.

The next stage is to configure the repository.

Configuring the user repositories

PINsafe supports multiple user repositories. The initial repository is the internal XML repository, which can be edited within the PINsafe Administration Console. Additional repositories can be defined, repositories can be LDAP based (eg Active Directory) or SQL based (eg MySql Database).

If you are using a user repository it is important that you create an Administrator user to prevent you being locked out of the admin console. If you are unfamiliar with PINsafe, it is recommended that you use the internal XML repository initially.

Using the XML Repository

To use the XML repository, you need to go to the Repository->Servers screen and add an XML repository. You need to give the XML repository a name. Repository names need to be unique within a PINsafe installation, therefore if you have two PINsafe servers connected to the same database, they cannot both have an XML repository called LOCAL.

The XML repository is also a special case because you can add/edit users for this repository from the PINsafe user administration screen.

Go to Repository->Servers to confirm that this repository has been configured. It should be the first (initially, the only) repository in the list, and should appear in the menu below the Groups heading:

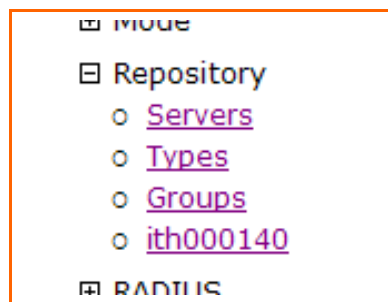



Figure 1. Repository menu

Go to Repository->Groups to configure the repository groups. Initially, two groups are defined – PINsafeUsers and PINsafeAdministrators. Make sure that each group definition for this repository is the same as the group name, as shown below:

Repository > Groups 

Please enter the repository group information to be used by the PINsafe server. This includes group privileges and Active Directory/LDAP definition. For XML repository, please copy the group name into the definition.

	Single	Dual	Swivlet	Admin	Helpdesk	PINless	
Name: <input type="text" value="PINsafeUsers"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Definitions:							<input type="button" value="Delete"/>
PINsafe1: <input type="text" value="PINsafeUsers"/>							
Name: <input type="text" value="PINsafeAdministrators"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Definitions:							<input type="button" value="Delete"/>
PINsafe1: <input type="text" value="PINsafeAdministrators"/>							
Name: <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Definitions:							
PINsafe1: <input type="text"/>							
							<input type="button" value="Apply"/> <input type="button" value="Reset"/>

Figure 2. Repository Groups Definition

Go to user administration screen and select .

The XML repository is shipped with an existing user of admin, with a PIN of 1234, so you will see this account appear on the list of users.

It is recommended that you open a new browser window, navigate to the admin console and log on using this new account before you exit the existing admin console session.

You can create new Admin level accounts by selecting on the User Administration screen and creating a new user that is a member of the PINsafe Administrators group. You can then synchronise PINsafe with the repository to create the PINsafe account. Remember to reset the PIN of the new Admin user that you have created.

NOTE: Unlike previous versions of PINsafe, this repository is always available, even when you add another repository. Therefore, you need to ensure that you change the PIN for the admin user, or else delete or disable this user.

License Key

PINsafe comes with a 5 user evaluation license. To operate a live PINsafe server you need a valid licence key obtained from your reseller or from Swivel Secure. Once you have this license key enter this key on the Server -> License screen. The licence will be for a fixed number of users; i.e. accounts on the PINsafe server. If you need additional users and therefore additional licences, you can purchase a new licence key for the new total of licences required. The new license key is a replacement for the existing one and therefore you simply need to overwrite the license key.

With the repository and database configured and the license installed you are now have a working PINsafe server that you can start to integrate with your IT infrastructure.

Integration

The integration tasks for PINsafe depend on the specifics on the installation and the technology with which PINsafe is required to operate. There are a number of potential integration points including:-

Databases:

PINsafe can be configured to use an external database.

User Repository

PINsafe comes with its own user repository but it can also be configured to work with an external user repositories such as Active Directory

Agents

Agents are the integration points between PINsafe and what it is that PINsafe is being used to protect. Agents use PINsafe's Agent-XML API to integrate with PINsafe.

Radius

PINsafe also can act as a RADIUS server, so an alternative method of integration is to configure PINsafe to accept authentication requests from a RADIUS (NAS) client.

Third Party Authentication

PINsafe is an open authentication platform in that it can be used in conjunction with other authentication technologies. PINsafe has a third party API to support this interaction.

Transport

PINsafe sends security strings to end users via a transport layer implemented by a transport class. Different classes allow for security strings to be sent via different methods, e.g. SMTP, SMS. Transport classes can also be configured to send alert information to users, e.g. to inform them that their PINsafe account has been created.

Logs

PINsafe can be configured to send logs to external systems including syslog and SMTP. These integration points are described in more details below.

Integrating with an external database

nb PINsafe is shipped with the PINsafe software required to interface with many popular database but does not include any licences/drivers for those databases. It is up to the user to obtain any required database licences. PINsafe supports opensource databases such as MySQL and PostGres. If you purchase PINsafe as a HA Active-Active Appliance, MySql is pre-installed and is appropriately licensed.

This section describes the stages required to configure at PINsafe to work with an external database. Most databases will require similar steps; we use MySQL5 as an example.

The first stage is to create a database that PINsafe can use to create the tables it needs and store the data. This database needs to support the UTF8 character set.

You then need to ensure that PINsafe can connect to that database, eg that all firewalls have the required port open (3306 being the default).

Obtain the required database drivers for the database.

Copy these drivers onto the PINsafe server under the webapps/pinsafe/WEB-INF/lib directory.

Restart the PINsafe server

Now go to the Database configuration screen and enter the details of the database and the drivers that you have configured. See the example below.

The screenshot shows a configuration form for a database connection. The fields are as follows:

- Identifier: MySQL 5
- Class: com.swiveltechnologies.user.database.MySQL5Dat
- Driver: com.mysql.jdbc.Driver
- URL: jdbc:mysql://192.168.0.156:3306/pinsafe
- Username: fred
- Password: [masked with four dots]

A "Delete" button is located to the right of the Password field.

Figure 3. Selecting MySQL5 Database in PINsafe CON in Sys Tray

Once you have entered this information select your chosen database from the drop-down list, then click Apply. PINsafe will now try and create the tables in the database. Check the log

PINsafe Manual

files to see if there are any errors. If, for any reason, PINsafe could not open the new database, the database setting reverts to the existing setting to prevent the user being locked out.

If the database tables were created successfully you will see a Database Opened message.

Once the new database has been created, it is important to synhchronize with the user repository to ensure that an admin account is created so that the admin console can be accessed. Remember to set the PIN of this account to a known value.

Integrating with user repositories


PINsafe comes with an XML repository that can be used to store user accounts. However, enterprises may already have a user repository, e.g. Active Directory, for user accounts, and this can be integrated with PINsafe.

The integration means that PINsafe will synchronise with the external user repository to ensure that the user accounts on PINsafe match those within the external user repository. To ensure that the two data stores remain synchronized, PINsafe can be configured to synchronize with the external repository at regular intervals, e.g. once an hour, or synchronisations can be instigated manually.

Using Groups with User Repositories

PINsafe grants users rights dependent on the groups to which they belong within the repository.

To configure groups, go to the Repository > Groups screen, will look something like the following:

Repository>Groups 

Please enter the repository group information to be used by the PINsafe server.
This includes group privileges and Active Directory/LDAP definition. For XML repository, please copy the group name into the definition.

	Single	Dual	Swivlet	Admin	Helpdesk	PINless
Name: <input style="width: 150px;" type="text" value="PINsafeUsers"/> Definitions: PINsafe1: <input style="width: 150px;" type="text" value="PINsafeUsers"/> AD: <input style="width: 150px;" type="text" value="CN=PINsafe,OU=Groups,DC=test,DC=local"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete						
Name: <input style="width: 150px;" type="text" value="PINsafeAdministrators"/> Definitions: PINsafe1: <input style="width: 150px;" type="text" value="PINsafeAdministrators"/> AD: <input style="width: 150px;" type="text" value="CN=PINsafeAdmins,OU=Groups,DC=test,DC=local"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete						
Name: <input style="width: 150px;" type="text"/> Definitions: PINsafe1: <input style="width: 150px;" type="text"/> AD: <input style="width: 150px;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Apply Reset						

Figure 4. Repository Groups definition with Active Directory

With a group name and then a definition for that group for each repository defined on the PINsafe server

There are two parts to defining a new group: defining what rights the group has, and mapping the group to user groups within the repositories.

This screen defines six basic rights:

- **Single** – connect using single-channel authentication
- **Dual** – connect using dual-channel authentication
- **Swivlet** – use the Swivlet application
- **Admin** – administer the entire PINsafe configuration
- **Helpdesk** – administer PINsafe users
- **PINless** – user has no PIN, just a password

When planning what groups are required, in addition to the above functions, the following need to be taken into account:

- Server Agents
- Transport classes
- RADIUS NAS
- RADIUS Groups
- Third Party authentication

When planning the groups, there is no need to define a different group for each function. If, for example, all dual-channel users use the same transport class, then the same group can be used for both functions. Also, users can be members of multiple groups. The exception to this is that a user cannot have more than one transport class.

Each group must have a unique name. Group names are just labels within the configuration, and should be descriptive of the group's purpose.

Having determined what groups are required, the next step is to define the mapping to the repositories.

This is slightly different for the XML repository than for Active Directory or LDAP. For Active Directory and LDAP repositories, the definition is the full-qualified domain name (FQDN) representing the user group within the repository. This group must exist within the repository: defining groups and group membership of Active Directory and LDAP repositories depends on the repository you are using, and is outside the scope of this document – see the appropriate documentation for your directory server. For the XML repository, the group definition is just a label for the user edit screen (and within the XML file). You would normally just copy the group name as the XML repository group definition.

It is not necessary to give a definition for every group for every repository. If a definition is left blank, then no users from the respective repository will be members of the respective group. This goes for the XML repository as well as other repositories.

Refer to Appendix B to see example Active Directory, LDAP and XML repository groups and attributes.

Importing Disabled State

If, as is the case with Active Directory, the repository supports the principle of disabled accounts, PINsafe can take account of this when synchronising with the repository. If Import disabled state is set to Yes, then if the account is disabled in the repository it will be disabled within PINsafe. If Import disabled state is set to No, then a user account can be manually disabled from the User Administration screen by clicking on the user account, selecting policy and then selecting Disabled.

If Import Disabled state is set to Yes, it is not possible to manually disable accounts.

Ignoring Fully Qualified (FQ) name changes.

Repositories such as Active Directory have a concept of fully-qualified names and account names. The fully-qualified name uniquely identifies the object within the repository and the account name is an attribute, such as sAMAccountName, that the user then uses as a username.

For example the fully qualified name may be.

CN=test, CN=User, OU=IT, DC=swivel, DC=com

But the PINsafe account name will be created using the sAMAccountName, test.

If the account is moved within the repository, the fully qualified name changes, e.g.

CN=test, CN=User, OU=Admin, DC=swivel, DC=com

If you set Ignore FQ name changes to Yes, if the fully qualified account name changes but the account name remains the same PINsafe will ignore this change and the associated PINsafe account will not be modified. If Ignore FQ name change is set to No, then the existing PINsafe account will be deleted and a new PINsafe account will be created for that user.

Marking missing users as deleted.

PINsafe users group membership within the user-repository to determine the users rights within PINsafe. If a user is removed from a group it is assumed that the user should be removed from PINsafe. However it is recognized that the user (or even the whole group) may have been removed in error. If this has happened the accounts will be lost and the only way to get them back would be to re-provision the accounts and allocate those users new PINs.

Since version 3.5, it is now possible to not automatically delete users that are missing from the repository. If this option is chosen the missing account will not be deleted, but merely disabled.

If, in subsequent jobs, the account re-appears, (the error being rectified), the account is re-enabled without the user needing to be assigned a new PIN. If there is a requirement to delete the account, it can be purged from the User List screen on the admin console.

Considerations for multiple repositories

PINsafe has the ability to support multiple repositories. If you are planning on using multiple repositories, you should be aware that usernames must be unique across all repositories. For example, it is not possible to have a user called admin in the XML repository and one also called admin in an Active Directory repository. If you are not going to be using the XML repository, it is advisable to remove all users from it, both from the point of view of security and of simplifying synchronization of the Active Directory. If it is going to be difficult to guarantee uniqueness of username across multiple repositories, it might be advisable to use email address, for example, as the login name instead.

Configuring the XML Repository

A new installation of PINsafe has a single repository, based on an XML file. It starts with a single user, "admin", with a PIN of 1234. This user can be removed or disabled, but at the very least it is strongly recommended that the PIN is changed.

It is not normally necessary to modify the configuration of the XML repository, except possibly to change the synchronisation schedule, but the details for doing so are given here.

Select Repository, and then the name of the XML repository, which should be the name of the PINsafe server.

The configuration screen should look like this:

Repository > ptest ⓘ

Please enter the details for the XML repository.

Username attribute:

PIN attribute:

Password attribute:

Synchronization schedule: Every at minutes past the hour

Figure 5.XML Repository configuration

Username, initial PIN and Initial password are provided for compatibility with other repositories, but there is little point in changing these.

It may well be worthwhile, however, changing or removing the synchronization schedule. Since XML repository users can be added and edited within the administration console, it is easy to synchronize the repository manual after making changes. Having an automatic synchronization, therefore, serves little purpose. To remove it, set the schedule to never.

Configuring an Active Directory Repository

Swivel provides a class for the integration of PINsafe with an Active Directory. This class acts as an interface between the PINsafe and the external active directory user repository.

To set-up PINsafe to integrate with Active Directory

1. Set up the required groups within Active Directory and add users to those groups. See Appendix C Active Directory/LDAP Groups and Attributes.
2. Add the Active Directory server as a repository on PINsafe
3. Configure the interface between PINsafe and AD
4. Configure the group definitions for the repository
5. Synchronise the users into PINsafe.

Note that the repository name and type cannot be changed once you have added the server – you must delete the server, and add a new one to rename it.

1 Set up Groups


Groups need to be created in AD that represent different user roles within PINsafe, eg users, helpdesk user, admin users etc , refer to Appendix C Active Directory/LDAP Groups and Attributes

2 Add Repository

Go the Repository > Servers screen. Add a new server by entering an appropriate name in the blank entry at the bottom of the list. From the drop down options select Active Directory, and then click Apply.

3 Configure Interface

The next stage is configure the connection to the AD server. In order to do this you must have an AD domain user account and password and the PINsafe server must be able to access the server via the selected port.


Repository > adtest 

Please enter the details for accessing Active Directory.

Hostname/IP:

Username:


Password:


Allow self-signed certificates: 


Username attribute:


PIN attribute:

Password attribute:

Import disabled state: 

Ignore FQ name changes: 

Mark missing users as deleted: 

Port: 



Synchronization schedule: Every  at  minutes past the hour

Figure 6.AD Repository configuration

Select the repository name from the left hand menu and complete the form: The entries required are summarised in the table below:

PINsafe Manual

Parameter	Meaning
Host/IP	The hostname or IP address of the Domain Controller that PINsafe will connect to.
Username	This username needs to be a fully qualified username for a user within the Active Directory domain that has the required privileges.
Password	Input the password associated with the above account
Synchronization schedule	Set the synchronisation schedule. This determines how often PINsafe will update its user list from Active Directory. See Appendix E Setting Schedules and CRON Strings for details.
Allow self-signed certificates	See Port
Username attribute	Set the username attribute; this is the attribute within the Active Directory repository that will form the username within PINsafe. The default for this is sAMAccountName. This is generally the most appropriate as it is the username that will be used for other, Windows based, authentication
Port	Select the required port number. If you are using SSL for the connection between PINsafe and Active Directory you need to select Port 636 and decide whether to accept self-signed certificates. If you are connecting to a multi-domain AD installation you may need to use Global Catalogue LDAP (3268) or its SSL equivalent (3629).
Initial PIN/Password	Optionally set the attributes within active directory that will form in the initial values for password and PIN.
Import Disabled/Ignore FQDN	Set the flags to import disabled state and ignore FQ name changes as described earlier.
Mark missing users as deleted	If a user account no longer exists in the repository, do not delete the account but mark it as deleted. Accounts can be re-enabled or purged from the admin console.

Figure 7.AD Values

Click  then go to the User Admin screen and click 

At this stage we have not defined what groups within active directory we are interested in so no users will be synched across. Go to the log viewer: if you have connected successfully you will see a message saying synch started and synch completed.

If this was not successful you will see an error in the log; for example

14:22:23 20 December 2006	ERROR	192.168.0.13 admin: Exception occurred during repository attribute query, object: , attribute: defaultNamingContext, exception: javax.naming.AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data 525, vece]
------------------------------------	-------	---

Indicates the username or password were not valid.

14:25:27 20 December 2006	ERROR	192.168.0.13 admin: Exception occurred during repository attribute query, object: , attribute: defaultNamingContext, exception: javax.naming.CommunicationException: 192.168.0.199:389 [Root exception is java.net.NoRouteToHostException: No route to host]
------------------------------------	-------	--

Indicates the server could not be reached.

Once you have confirmed that you can connect to the AD server; you need to set up the repository groups.

4 Configure Groups

Go to Repository > Groups

Assuming you have not added new groups, there will be just the two groups defined: PINsafeUsers and PINsafeAdministrators. The definitions for the AD server will be blank. You can enter fully-qualified domain names for the appropriate groups in the Active Directory which represent normal users and administrators but it is recommended that the Browse feature is used.

Figure 8. Repository Groups definition with Active Directory

This feature allows the repository to be browsed and the required group to be selected.

Figure 9. Using browse feature to select a group

Once the group has been selected go to User Administration and select .

This will then create PINsafe accounts associated with the active directory accounts, including PINsafe accounts with admin rights for active directory accounts that belong to the relevant group, if any. These accounts will be listed on the User Admin screen.

Assuming you have created an administrator account in this repository, select it. Select RESET PIN for the account and enter a new PIN. Make a note of this PIN.

The server is now configured to pull in user information from the Active Directory. There are two ways of instigating the pull of this data:

- | | |
|---------------|---|
| Manually | By going to the User Administration screen and selecting User Sync. |
| Automatically | The schedule for a given repository is set on the configuration screen for that repository, as described above. |

After you have synchronised with the AD repository you should see the accounts that have been created in the User Administration screen. **Remember to reset the PIN on any new admin accounts that you have created, if they are not created automatically.**

Configuring Other LDAP Directory Servers as Repositories

Swivel provides a class for the integration of PINsafe with other LDAP directory servers. This has been tested for use with OpenLDAP, Sun Directory Server, Novell eDirectory and IBM Tivoli Directory Server, and will probably work with most other LDAP-compatible repositories that implements group membership according to the LDAP recommendations ([RFC 2256](#)).

The steps for other LDAP repositories are the same for Active Directory

To set-up PINsafe to integrate with an LDAP repository

1. Set up the required groups within LDAP and add users to those groups. See Appendix C Active Directory/LDAP Groups and Attributes.
2. Add the LDAP server as a repository on PINsafe
3. Configure the interface between PINsafe and LDAP
4. Configure the group definitions for the repository
5. Synchronise the users into PINsafe.

Note that the repository name and type cannot be changed once you have added the server – you must delete the server, and add a new one to rename it.

1 Set up Groups

Groups need to be created in LDAP that represent different user roles within PINsafe, eg users, helpdesk user, admin users etc , refer to Appendix C Active Directory/LDAP Groups and Attributes

2 Add Repository

Go the Repository > Servers screen. Add a new server by entering an appropriate name in the blank entry at the bottom of the list. From the drop down options select Simple LDAP, and then click Apply.

3 Configure Interface

The next stage is to ensure that you can connect to the directory server. In order to do this you must have a valid user account and password for the directory server and the PINsafe server must be able to access the server via LDAP (by default port 389, but most servers allow this to be changed on installation).

Enter the details of the directory server and the account you are using. Note that the username may need to be fully qualified.

Repository > LDAP ⓘ

Please enter the LDAP configuration details

Administrator:	<input type="text" value="cn=Admin,ou=test,o=lo"/>
Password:	<input type="password" value="•••••"/>
Server:	<input type="text" value="LDAPServer"/>
Port:	<input type="text" value="389"/>
Base DN:	<input type="text"/>
Synchronization schedule:	<input type="text" value="0 0 * * * ?"/>
Username attribute:	<input type="text" value="uid"/>
Initial PIN attribute:	<input type="text"/>
Initial password attribute:	<input type="text"/>
Base Search Context:	<input type="text"/>
Group ObjectClass Name:	<input type="text" value="groupOfNames"/>
User ObjectClass Name:	<input type="text" value="inetOrgPerson"/>
Member attribute name:	<input type="text" value="member"/>
Member group attribute name:	<input type="text"/>
Import disabled state:	<input type="text" value="No"/> ▼
Ignore FQ name changes:	<input type="text" value="No"/> ▼
User disabled flag name:	<input type="text" value="disabled"/>
User enabled flag name:	<input type="text"/>
Use SSL:	<input type="text" value="SSL Off"/> ▼

Figure 10. Configuration for LDAP repository

The values are explained in the table below.

PINsafe Manual

Parameter	Meaning
Administrator	The distinguished name of the LDAP user credentials to access the server. This username needs to be a fully qualified username for a user within the LDAP server that has the required privileges
Password	The LDAP user's password
Server	The name or IP address of the server hosting the directory service
Port	The port on which LDAP is running
Base DN	The base distinguished name of the LDAP server
Synchronization Schedule	How often the PINsafe repository is updated from the directory server (see Appendix E Setting Schedules and CRON Strings for details on this)
Username attribute	The name of the attribute on a user object to use as the PINsafe user name. The default for this is uid. This is the most appropriate attribute if users are implemented as inetOrgPerson objects, or custom extensions to that object class
Initial PIN attribute	The name of the attribute on a user object to use as the initial PIN for a user
Initial password attribute	The name of the attribute on a user object to use as the initial password for a user
Base Search Context	The sub-context on the LDAP server in which all users and groups exist
Group ObjectClass Name	The name of the LDAP object class representing a group. For most servers, this will be groupOfUniqueNames, but groupOfNames is a possibility, or you may have created a custom schema.
User ObjectClass Name	The name of the LDAP object class representing a user. inetOrgPerson is the standard schema, but you may have created a custom schema.
Member attribute name	<p>The name of the attribute on a group object that contains the names of members. If the group object class is groupOfUniqueNames, this will be uniqueMember. If groupOfNames, then member.</p> <p>The simple LDAP implementation assumes that group membership is represented by a multi-valued attribute on the group. If your directory server works differently, you will not be able to use Simple LDAP, and will need a custom repository class.</p>
Member group attribute name	The name of the attribute on a group object that contains the names of member groups. This is only relevant in cases where individual members and group members are added with different attributes, as in the case of the IBM Tivoli Directory Server. If this is omitted, it is assumed to be the same as the member attribute name.
Import disabled state	Whether or not to import the PINsafe disabled state from the LDAP repository. If this is set to Yes, the following attribute is used to decide whether or not a user is disabled.
User disabled/enabled flag name	The name of the attribute on a user that indicates that the user is disabled or enabled. The inetOrgPerson schema does not allow for such an attribute, so to implement disabling users, you would need a custom schema. The use of two properties allows disabling to be handled in one of two ways: either a disabled flag is set to indicate that the user is

PINsafe Manual

	disabled, or an enabled flag is set to indicate that the user is enabled. If no such flag exists, the user is assumed to be active.
Ignore FQ name changes	Whether or not to treat an LDAP user object as the same user if the fully-qualified name changes, but the PINsafe username remains the same.
Import Disabled/Ignore FQDN	Set the flags to import disabled state and ignore FQ name changes as described earlier.
Use SSL	Whether or not the server uses SSL for authentication

Figure 11.LDAP Values

The server is now configured to pull in user information from the LDAP repository. The settings can be tested using the "browse in window" option, this should display the contents of the directory.

At this stage no groups within the repository are defined, so no users will be synched across.

4 Configure Groups.

Go to Repository > Groups

Groups from LDAP repositories can be browsed and selected in the same way as described for Active Directory.

Other repository types

Currently PINsafe can pull user information from LDAP based user repositories. However the PINsafe architecture allows for new repository types, eg SQL based, to be easily developed. Therefore if you have a requirement to pull information from a repository not covered by this manual contact support@swivelsecure.com

Deleting a Repository

A repository can be deleted by going to the Repository > Servers screen and clicking on the Delete button next to the appropriate repository. However, by default this only removes the repository definition from the current PINsafe server, and not from the PINsafe database. Neither does it remove users in that repository. To change this, on the Repository > Servers page, change the flag labelled "Delete users with server" to "Yes".

The reason for including this option is to allow for the possibility of repositories being configured on more than one PINsafe server.

If you unintentionally delete a repository with Delete users with server set to "No", you can add the repository back in again (i.e. use the same name), change the flag, and delete it again.

Integrating with Transport Classes

A transport class is the mechanism by which a security string is delivered to the end user for dual-factor authentication. The default method for this is via SMS and PINsafe comes with a class that enable this via a GSM Modem. However the transport class can be used to interface PINsafe with any suitable mechanism for carrying the string. PINsafe comes with a number of pre-defined transports to choose from; others are available and new ones can be developed as required.

To use a transport class you need to configure destination attributes on PINsafe. These represent a mapping of an attribute name to its definition within the connected repositories. For example to send security strings to a mobile phone an attribute called phone is required; this would map to phone for the local XML repository and telephoneNumber (or Mobile) for Active Directory.

Transport>Attributes

Please enter the repository attributes for the transport types (e.g. Email, Mobile Phone).

Name:	<input style="background-color: yellow;" type="text" value="phone"/>		
Attribute:		<input type="button" value="Delete"/>	
local:	<input type="text" value="phone"/>		
activeDirectory:	<input type="text" value="telephoneNumber"/>		
<hr/>			
Name:	<input style="background-color: yellow;" type="text" value="email"/>		
Attribute:		<input type="button" value="Delete"/>	
local:	<input type="text" value="email"/>		
activeDirectory:	<input type="text" value="Mail"/>		

Figure 12.Setting Transport Attributes

Once the attributes have been defined they can be used as part of the transport definition; as shown in the table below.

Identifier	A name for the transport; this is especially important where multiple PINsafe servers are sharing a database; see below
Class	The class that implements this interface
Strings per Message	For some transports you may wish to configure them to send multiple security strings within the same message. You can specify this here.
Destination Attribute	This is the attribute within the repository that will be used as the destination for the user. This will be one of the previously defined transport attributes.
Repository Group	The group in the repository that users will be a member of in order to use this transport to send their security stings.
Alert Repository Group	The group in the repository that users will be a member of in order to use this transport to send alert messages to.

Configuring transports in shared database PINsafe installations

When a repository is synchronised with PINsafe, the PINsafe database stores the name of the transport that the user has been allocated. Where you have multiple PINsafe servers connecting to the same database it is important that the transport configurations are consistent across the servers. The easiest approach is to ensure that the configuration is identical; however this is not the only approach and some extra resilience can be achieved.

For example, you can have two PINsafe servers: one that uses a GSM modem to send SMS messages and another that is part of the same installation that uses an SMS provider. To achieve this, you would need to configure a transport called SMS on both servers and associate that transport with the same groups on both servers. However on one server the calls would be the GSM Modem class and on the other server it would be the class associated with the SMS provider.

NB: You can only use transports that use the same destination attribute.

NB: You need to configure transports on PINsafe servers that are operating in Slave mode, even though they do not have a repository. The group definitions entered on the transport-general screen are not important but the transports still need to be configured.

How to integrate PINsafe with a GSM Modem

PINsafe supplies a transport class that allows PINsafe to send text messages via an AT compatible GSM modem. (The GSM modem obviously needs a valid SIM card and GSM coverage). The transport class operates the modem by sending AT Modem commands via the serial port. Therefore, before configuring the PINsafe server, an AT Compatible modem needs to be connected to the serial port.

To configure the PINsafe server to use the modem:

1. Go to the Transport > General tab.
2. Ensure that the modem class details are entered on the screen as shown below.
3. Enter a repository group name for the class, e.g. modem, if you are using the XML repository.
4. Click Apply.
5. Once this entry has been made, the transport will appear in the left hand pane under the Transport heading. You can then configure the modem interface as required from the Transport > GSM Modem screen.
6. To configure the modem interface select the serial port that you are going to use and set the other parameters to match those of the modem.
7. Configure the modem and connect it to the selected serial port.

Notes on Modems

Swivel Secure can recommend a number of modems that we have tested with PINsafe.

It is recommend that you configure the modem to a specific baud rate rather than using autobauding. You can effect this change by connecting to the modem via a terminal emulation program such as minicom (Linux) or Winterm (Windows) and typing the commands

```
AT+IPR=9600 (for 9600 baud)
```

```
AT&W To save the settings
```

The modem should respond with OK after each command

It is also recommend using hardware handshaking.

How to integrate PINsafe with an SMS service Provider

As an alternative to using a GSM Modem, PINsafe can be configured to use an SMS service provider. To do this you need to obtain an account with an SMS provider that can deliver SMS messages to the PINsafe user base. There are a number of such providers.

A transport class is required to act as an interface between PINsafe and the SMS provider; it receives messages from PINsafe and forwards them to the SMS provider in whatever format that the SMS provider requires.

Swivel has produced classes to work with a number of SMS providers including iTagg (www.itagg.com) and Clickatell (www.clickatell.com)

To configure PINsafe to use an SMS service provider.

1. Obtain an account from an SMS provider for which there is a transport class available.
2. Go to the Transport > General tab.
3. Ensure that the SMS provider class details are entered on the screen as shown below.
4. Select a Repository group name for the class, eg smsUser. All members of this Repository Group will have their security strings sent to them via the SMS provider.
5. Select an Alert Repository group name for the class, eg smsUserAlert. All members of this Repository Group will have system alerts sent to them via the SMS provider.
6. Click Apply.

The screenshot shows a configuration window with the following fields and values:

- Identifier: iTagg
- Class: com.swiveltechnologies.pinsafe.transport.ITaggTransport
- Strings per message: 1
- Destination attribute: phone
- Repository group: smsuser
- Alert repository group: smsAlert

The Alert repository group dropdown menu is expanded, showing the following options: ---NONE---, PINsafeAdministrators, PINsafeUsers, Pinless, pid, smsAlert (highlighted), smsuser, and smtp2.

Figure 13. Configuring an SMS provider transport class

7. Once this entry has been made, the transport identifier (eg iTagg) will appear in the left hand pane under the Transport heading. You can then configure this interface as

required from the Transport > iTagg screen.

8. In order to configure users to use this transport to receive their security strings, users need to be members of the appropriate repository group. If you are using the XML repository you can effect this by going to the User Administration screen, selecting a user, and selecting smsUser as their transport group.

Integrating via SMTP

Integrating with e-mail is a special case for integration. This is because PINsafe requires integration with an e-mail server to send e-mail alarm messages. Therefore the actual integration details such as mail server IP address are specified in the Server -> SMTP screen. See SMTP (email) Loggin

Integrating with Agents using Agent-XML

An agent is a piece of software residing outside the PINsafe platform but which communicates with the PINsafe platform to manage authentication. There are a number of ready made agents available, and new agents can generally be created very easily.

Agents communicate with PINsafe via the Agent-XML interface.

This section covers how PINsafe can be integrated with agents to support using PINsafe with external applications such as websites. Any external application that needs to use the Admin API (new in Version 3.4) needs to be defined as an agent on PINsafe.

How to integrate PINsafe with an external agent.

The PINsafe server will only service authentication requests from trusted agents.

The configuration of PINsafe to work with an external agent therefore consists of adding the details of the agent to the PINsafe trusted agent list. To do this go to the Agents screen, by clicking on Agents in the left hand navigation bar. Then enter a name for the agent, the IP address of the agent and then a shared secret.

- The IP address can be a single IP address or a range of IP addresses.

A range of IP addresses is specified using Classless Inter-Domain Routing (CIDR) notation, whereby you define an IP address but then specify how many bits actually are significant in terms of the network address. For example specifying 192.123.123.120 / 24 would allow authentication from any IP address in the range 192.123.123.xxx as only the first 24 bits of the IP address are required to match.

In order for authentication requests to be processed, the source IP address of the request and the shared secret presented by the agent need to match the details entered on this screen.

Server > Agents ⓘ

Please enter the details for any PINsafe agents below. Agents are permitted to access the authentication services of the PINsafe server via the AgentXML interface.

Agents: Name:

Hostname/IP:

Shared secret:

Group:

- ANY---
- PINsafeAdministrators
- PINsafeUsers

Figure 14.Screen shot of Agent Configuration Screen

It is possible to associate agents with groups within PINsafe. When you configure an agent, if you leave the group selection as "ANY", then any PINsafe user will be able to authenticate via this agent. If a group is specified then the user must be a member of that group in order to authenticate via this agent. The agent groups are similar to other groups in PINsafe. For more details on groups, see section .

Using the User ChangePIN application

One of the most common agents deployed with PINsafe is the Change PIN application. This is an application that allows user to reset their own PINs. This application will come pre-configured as part of an appliance purchase.

This application can be deployed on the same server as the PINsafe server or on a different server, but in either case it must be configured as an agent on the PINsafe server.

The change pin application is usually supplied as a .war file. To install the application copy the changepin.war file to the webapps folder underneath the Apache Tomcat directory and then restart tomcat.

The settings for the Change PIN application are created by editing the settings.xml file under the webapps\changepin\WEB-INF directory.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="ssl">>false</entry>
<entry key="server">localhost</entry>
<entry key="port">8080</entry>
<entry key="context">pinsafe</entry>
<entry key="secret">secret</entry>
<entry key="redirect">http://www.google.com</entry>
</properties>
```

<entry key="ssl">>false</entry>

This sets whether to use ssl to connect to the PINsafe server or not; default is not to use ssl.

<entry key="server">localhost</entry>

This tells the changepin application the server name or IP address of the PINsafe server. The default setting is localhost; this appropriate for installations where the Change PIN application is installed on the same server as PINsafe.

<entry key="port">8080</entry>

This is the port number being used by the PINsafe server. The default is 8080; this will need to be changed if the PINsafe server is using any other port, e.g. if it is using ssl for which the default port number is 8443.

<entry key="context">pinsafe</entry>

PINsafe Manual

This sets the context that pinsafe servers are available on. The default is PINsafe; generally the only time this would need to be changed is where there are multiple PINsafe instances sharing the same Apache TOMCAT servlet container.

<entry key="secret">secret</entry>

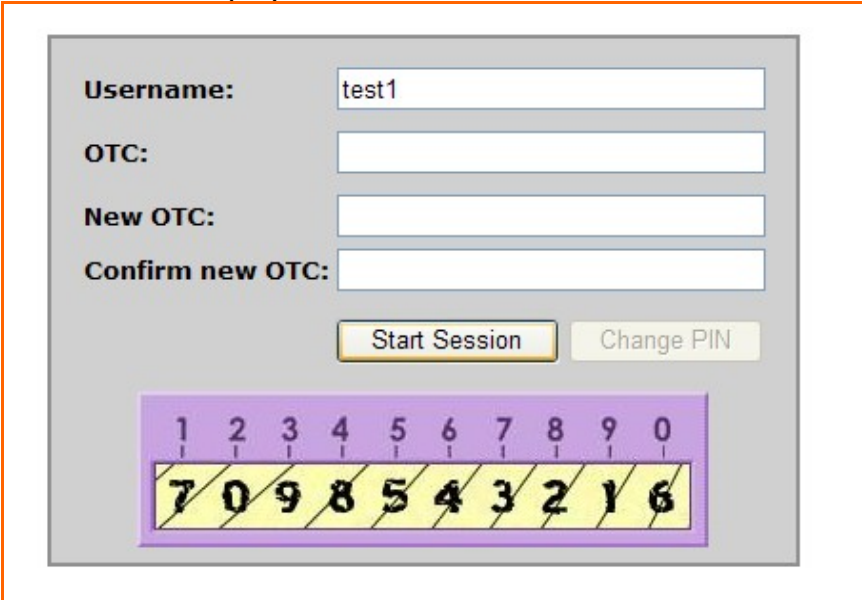
This is the shared secret that needs to match the setting on the PINSafe server for the change PIN agent. This should be changed to a suitably random setting.

<entry key="redirect">http://www.google.com</entry>

The redirect value is a url to where the user will be redirected once they have successfully changed their PIN; this is an optional setting.

You should now be able to use the Change PIN application. Go to <http://<ipaddress>:8080/changepin>

The Change PIN form will be displayed.



The screenshot shows a web form for changing a PIN. It has four input fields: 'Username:' with the value 'test1', 'OTC:', 'New OTC:', and 'Confirm new OTC:'. Below these fields are two buttons: 'Start Session' and 'Change PIN'. At the bottom of the form is a Turing image consisting of a grid of numbers. The top row of the grid contains numbers 1 through 0. The bottom row contains a distorted sequence of numbers: 7, 0, 9, 8, 5, 4, 3, 2, 1, 6.

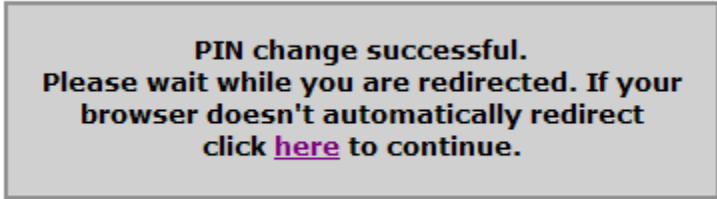
Figure 15.Change PIN screen shot

Enter a username and select Start Session; if the user is configured as a single channel user then a Turing image will be displayed.

Alternatively, if the user is a dual channel user, they may already have been sent a security string via SMS.

To change their PIN, the user must enter their one-time code based on their current PIN and then their new one-time code; therefore in the above example if the user has a PIN of 2378 that they wish to change to 9243 they would enter 0932 in the OTC box and 1089 the New OTC and confirm new OTC boxes.

To change their PIN, the user would then select change PIN.



At which point they will be redirected to the defined redirect page if one was defined. If you check the PINsafe logs you should also see the corresponding entries.

16:52:01 03 January 2007	INFO	192.168.0.13 changepin: Change PIN successful for user: test1.
16:51:47 03 January 2007	INFO	192.168.0.13 changepin: Session started for user: test1.

How to integrate PINsafe with an IIS Website.

In this instance the Agent is implemented using an ISAPI Filter. This filter needs to be installed on the web server hosting the site to be protected. For information about filtering within IIS go to the Microsoft web site. <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iissdk/html/22e3fbfb-1c31-41d7-9dc4-efa83f813521.asp>

To install the PINsafe ISAPI filter you need to run the install PINsafeIISFilter.exe on the IIS server. Make a note of the location the application is installed in (default is C:\Program Files\PINsafe IIS Filter).

The configuration of the filter is achieved by running the configuration application, accessible from

Start-All Programs – PINsafe IIS Filter – Filter Configuration

The configurable Items are summarised below:

PINsafe Server

- Hostname/IP server** The IP address or hostname of the PINsafe server, which must be visible to IIS
- Port:** The port that the PINsafe server services requests on; default 8080
- Context:** The web application context in which the PINsafe server is installed, usually pinsafe
- Secret:** The shared secret between this agent and the PINsafe server. Needs to match value entered as part of PINsafe config
- SSL Enable:** Selected if SSL is being used between the agent and PINsafe, otherwise false.
- Permit Self-Signed:** Select if self-signed certificates are allowed.

Authentication

- Idle Time:** The connection idle time (in seconds) after which re-authentication will be required.

PINsafe Manual

- Username Header:** If the username needs to be included in the http header, what attribute will it be given
- Channels:** What channels will be used, this will determine what buttons are presented on the authentication page, eg if you select Single Channel a get Image button will be included
- Display Password Field:** This will include a password field if a password is being used as well as the PIN based authentication
- Permit self-reset** This will allow users to perform a self-reset via this agent.

Exclusions

- Addresses** Comma separated list of IP addresses that are exempt from the requirement to perform PINsafe authentication. Partial addresses such as "192.168" may be entered.
- Paths** Comma separated list of paths that are exempt from the requirement to perform PINsafe authentication. Partial paths may be entered, for example "/images/" would allow access to "/images/logo.png" and "/images/staff.jpg"

Inclusions

- Included Paths** Comma separated list of paths that require PINsafe authentication. If any paths are entered, then only those paths will be subject to PINsafe authentication and any path exemptions will be ignored. Partial paths may be entered.

Misc

- Default Path** The default location to redirect a user to following login if no other destination is available. Setting this value is recommended as it will allow users who have navigated directly to the login page to access the protected resource
- Logout Path:** A path that causes the cookie to be deleted and authentication to be required on any subsequent request. This must be a path protected by the IIS filter
- Virtual web path:** The virtual web path for the IIS filter authentication pages

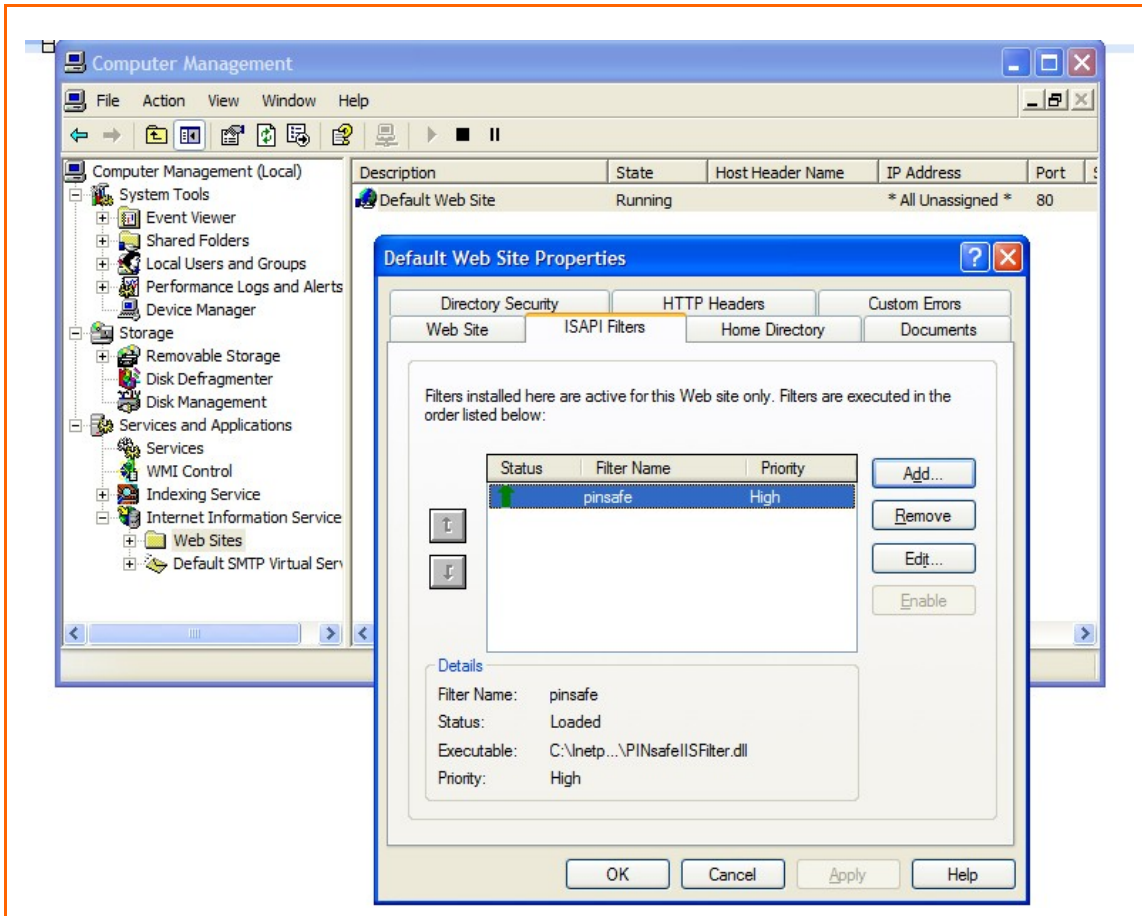


Figure 16. Screenshot of IIS filter installation

Once the filter has been configured, it can be applied to the web site.

In the Control Panel, select Administrative Tools, then Internet Information Services.

Navigate to the default web site (assuming that is the one you want the filter to apply to), right-click on it and select Properties.

Select the ISAPI filters tab, and click Add.

Enter the name "PINsafe IIS filter" (you can call it what you like). Click the Browse button, and navigate to the installation folder noted earlier. Select PINsafeIISFilter.dll and click OK.

Back in the main IIS management console, right-click again on the web site, select New, then Virtual Directory.

When prompted for an alias, enter "pinsafe". On the next screen, when prompted for a directory, click Browse and navigate to the "Web" directory underneath the filter installation directory. On the next screen, ensure that Read and Run scripts are enabled.

Once the virtual directory has been created, right-click on it and select Properties. On the Virtual Directory tab, click the Remove button next to Application name, then click OK.

Once the filter has been applied to the website, when a user attempts to access part of the

website protected by PINsafe, PINsafe will prompt them to authenticate. IIS may need to be restarted for filter settings to take affect.

How to write an Agent

The Change PIN application and the IIS filter are two examples of PINsafe agents that use the PINsafe Agent-XML API. The Agent-XML API is a simple XML- based API that enables integrators to develop their own agents. This can provide for a very flexible authentication solution.

Swivel can provide a range of samples to help support this integration, for example how to make authentication requests from within a jsp. For more details e-mail support@swivelsecure.com

How to use the custom attribute

It is possible to assign a custom attribute to a user from the user admin screen. When a user successfully authenticates via the Agent-XML interface, this custom attribute is returned. This can be used to add granularity to the access rights granted on successful authentication.

When using the XML repository, this custom attribute can be set manually. When using Active Directory the custom attribute can be mapped to an Active Directory attribute.

Integrating using RADIUS

PINsafe can operate as a RADIUS server for working with external systems such as SSL VPNs.

NB: In order to authenticate via RADIUS, a user must be a member of the RADIUS users' group as defined on the Repository->Groups page.

How to configure PINsafe to operate as a RADIUS server.

In order to integrate PINsafe with an external system the PINsafe RADIUS server first needs to be enabled and then configured to receive authentication requests from the external systems, or Network Access Server (NAS) using RADIUS terminology.

The RADIUS server is configured by going to the Radius-> Server config page. Enter the required configuration details and then select Apply.

RADIUS>Server

Please enter the details for the RADIUS server.

Server enabled:	<input type="text" value="Yes"/>
IP address:	<input type="text"/>
Authentication port:	<input type="text" value="1812"/>
Accounting port:	<input type="text" value="1813"/>
Maximum no. sessions:	<input type="text" value="50"/>
Permit empty attributes:	<input type="text" value="No"/>
Filter ID:	<input type="text" value="No"/>
Additional RADIUS logging:	<input type="text" value="Both"/>
Enable debug:	<input type="text" value="No"/>
Radius Groups:	<input type="text" value="Yes"/>
Radius Group Keyword:	<input type="text" value="POLICY"/>

Figure 17.RADIUS server configuration

Notes on RADIUS configuration.

1. The IP address needs to be the 'internal' IP address of the PINsafe server; this is the address to which the RADIUS server will bind. If you leave this setting blank the RADIUS server will process all inbound RADIUS requests received.
2. If you use different ports other than the default of 1812 and 1813, you will need to open up these ports on the appliance; see IPTables.
3. If you set Filter ID to YES the users username will be returned in the RADIUS Filter ID field of the RADIUS authentication response

- Additional RADIUS logging will add RADIUS log events to the PINsafe logs; therefore if a user authenticates via RADIUS there will be a log event for the successful RADIUS authentication and then another log entry for the PINsafe authentication, as the example shows below.

12:13:08 03 January 2007	INFO	RADIUS: <158> Access-Accept(2) LEN=63 192.168.0.151:32859 Access-Request by greenford succeeded
12:13:08 03 January 2007	INFO	192.168.0.151 Aventail: Login successful for user: greenford.

RADIUS Groups

Cisco, and other VPN vendors, use information passed back within a RADIUS Access-Accept response to determine what access policy to apply to the user.

PINsafe can now support this form of operation for a number of vendors.

To implement this feature, set the RADIUS Groups setting to yes. The RADIUS group keyword can be used to filter the groups that are returned. Eg if you set the keyword to POLICY on group names that contain the word policy in their names will be returned.

This prevents irrelevant group information being returned. If this field is left blank then a list of all the groups of which the user is a member is returned. The format used to return the group list is set for each NAS.

On the NAS screen you select the relevant vendor from the Vendor (Groups) option.

Once the Radius Server is configured and enabled, it can be configured to accept requests from a NAS. This is achieved by selecting the Radius->NAS page and entering the details. These settings are the same as those for an agent, name, IP address, shared secret and group.

You can also specify that the NAS will use a secure RADIUS (EAP) protocol from the drop down list, the options are LEAP and EAP-MD5

RADIUS>NAS ⓘ

Please enter the details for any RADIUS network access servers. A NAS is authentication services of the PINsafe server via the RADIUS interface.

NAS: Identifier:

Hostname/IP:

Secret:

EAP protocol:

Group:

Authentication Mode:

Vendor (Groups):

Change PIN warning:

Two Stage Auth:

Figure 18. NAS configuration screen

For authentication requests to be processed by PINsafe they need to come from the IP address specified in the NAS configuration, the shared secret needs to match that specified in the NAS configuration and be sent to the IP address specified in the PINsafe Server Configuration.

How to integrate a VPN with PINsafe using RADIUS.

In order to configure a VPN to use PINsafe for authentication the VPN needs to be configured to make authentication requests against the PINsafe server. This method for doing this depends on the VPN concerned so you need to consult the relevant documentation for the specific VPN. Swivel Secure will be able to provide you with specific instructions for a range of VPNs.

The basis of the configuration is basically to ensure that.

1. The VPN server needs to send authentication requests to the IP address and port number on which the PINsafe Radius server is operating.
2. The VPN server needs to have its shared secret (and realm, if specified) set to match that on the NAS configuration screen.

This is all the configuration that is required for use with a VPN. If TURING image is being used and you require the TURING image to be integrated into the VPN log on page; the log-on page needs modification.

Two Stage RADIUS Authentication

One mode of operation for RADIUS integration is to use a two stage approach.

The user initially submits their username and password. If the password is correct PINsafe responds with a RADIUS-Challenge which indicates to the VPN that additional credentials are required. If the user is a dual channel user and PINsafe is set to on-demand authentication, the user will also be sent an SMS security string.

The VPN will then prompt for the additional credentials, in this case the one-time code. When the one-time code is entered it is submitted to PINsafe via RADIUS. PINsafe then checks the one-time code and if it is correct the user authenticates successfully.

This mode of operation has been successfully tested with Checkpoint, Cisco and Citrix products.

How to use single channel with a VPN

In order to use single channel authentication with a VPN, the user needs to be able to obtain a TURING image, perform the OTC extraction using their PIN and then enter these details onto the VPN authentication page.

One way of delivering a security string to the user is to modify the VPN log-on page so that it incorporates a TURING image; like the example below. Some VPNs accommodate this form of integration; others require some customization and others make this impossible. PINsafe have a number of these customizations available off the shelf.

However there are a number of ways of delivering the security string in a TURING image that do not require the VPN log-on page to be modified and thus are a very low-touch integration.

User Portal

One solution to delivering the security strings is to use a user-portal web application to allow the user to obtain a TURING image via a web browser.

Swivel can supply a user-portal which can be hosted on any servlet container, including the server on which PINsafe is running. It acts as an authentication agent for PINsafe and can be used to deliver security strings to the end-user and also for functions such as allowing the user to change their PIN numbers. It is easily branded and customised.

The beauty of this solution is that it does not require a client to be installed on the user's laptop, all they need is a standard browser.

Users can bookmark this page and even have it on their desktop as a bookmark. Users can be sent the URL of the portal as part of the provisioning of PINsafe.

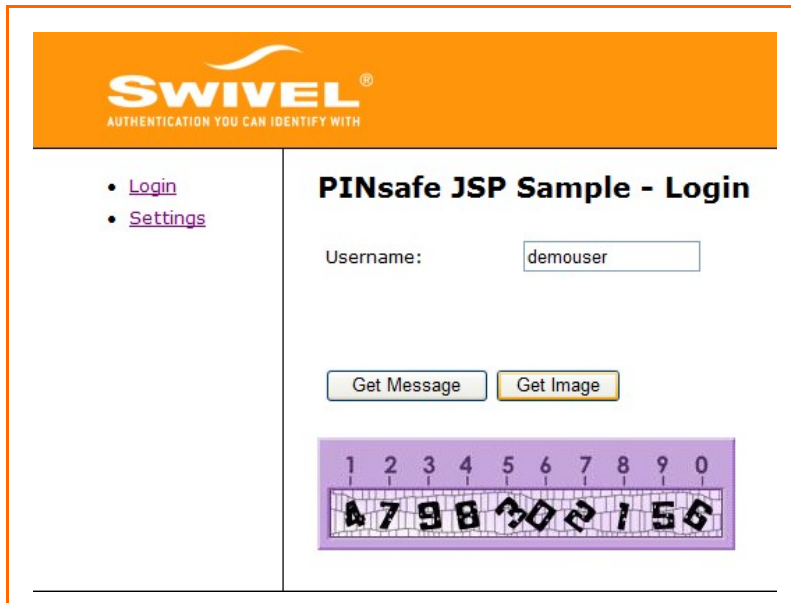


Figure 19. User Portal screen shot

To authenticate the user opens a browser at the portal’s URL, enter their username (although this could be pre-filled, stored in a cookie). They select get image and the image is presented to them. The user performs the one-time code extraction and enters the one-time code into the VPN log-on form.

SysTray Utility

Another way to deliver the TURING image to the end-user is to use the PINsafe SysTray utility. This is a small client that resides in the users System Tray.

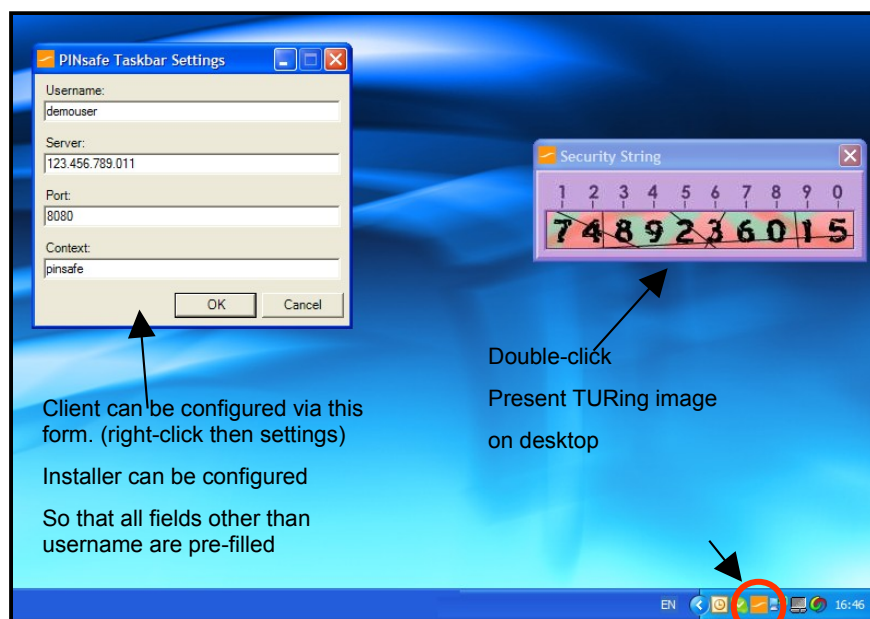


Figure 20. Screenshot of Systray Utility

PINsafe Manual

The application can be manually configured to retrieve TURING images from any PINsafe server, for any user. It can also be pre-configured so that the user need only enter their username. Once the application is configured, users can obtain a security string merely by double-clicking on the PINsafe icon in the system tray (or by right-clicking and selecting get image)

The application is small and easy to distribute; it can be provided with its own windows installer.

The user of the systray application gives a true soft-token like experience.

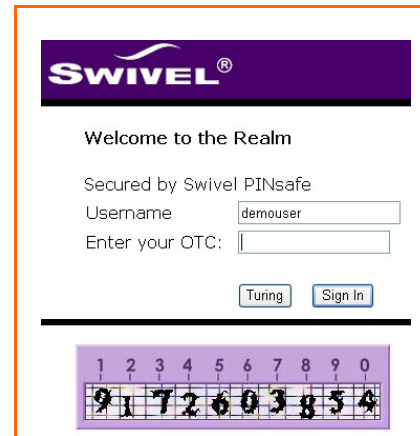
These two options are not mutually exclusive: a single PINsafe server can accommodate both alternatives.

How to incorporate a TURING image into a VPN log on page.

Figure 21. Example VPN screenshot

If you wish to integrate a TURING image with a VPN log on page then the VPN configuration needs modification.

The implementation of these modifications again depend on the VPN itself: some VPNs allow you to easily customize the log on page, for others it is more involved.



The log on page needs to

1. Have a "Start Session" or "TURING" button.
2. The user enters their username and then selects this button
3. This then fetches the Turing Image; this will be in the format

http://PINsafe_IP_Address:8080/pinsafe/SCImage?username=demouser

It is recommended that the request for the image is proxied via the VPN or via other means so that port 8080 on the PINsafe server does not need to be opened up to the internet.

4. The user can then enter their OTC and select Sign In; this will then allow the VPN to use the username and extracted OTC to authenticate against the PINsafe server.

Integrating with 3rd Party Authentication systems

PINsafe can be integrated with 3rd party authentication systems via its third party API. If this is required, a class needs to be developed that implements PINsafe third party API, and interfaced to the third-party authentication system. The details of developing such as class are outside the scope of this document.

Assuming that this class exists, PINsafe can be configured to use the third-party authentication system, via this class, for some or all users.

To configure PINsafe to do this you need to go to the Sever>Third Party Authentication screen.

Enter an identifier for the Authentication, the class (that needs to be installed on the PINsafe server), repository group that the user of the third party system will be associated with and any license key required by the third party system.

Once this configuration is in place the authentication process will be.

1. Agent submits authentication request, including credentials required by the third party system.
2. The PINsafe server checks the user PINsafe credentials.
3. If this stage of authentication is successful and the user is a member of the repository group associated with the third party authentication class, the PINsafe server makes an authentication request to the third party system, passing the required credentials.
4. The third party class returns a success code and, if this stage of authentication is also successful, successfully authenticates the user.

Integrating with other Authentication Servers

There are two ways in which PINsafe servers can interact, enabling users from one server to authenticate to another: using peering, or by sharing a database.

Peering PINsafe servers

It is possible to deploy a number of PINsafe servers as a set of peers. Every user has an account on one of the PINsafe peers, however but they can authenticate to any one of the PINsafe servers.

For example, if a business has a London office and a New York office, running separate Active Directories and SSL VPNs a PINsafe server can be installed in each office. Each PINsafe server can be configured as a peer to the other.

In this configuration, a London-based user can authenticate to the New York VPN; the New York PINsafe detects that the user is served by the London server and proxies the authentication request to the London PINsafe server.

The London PINsafe server checks the user's credentials and returns the results to the New York server that, as a result, can allow or deny access.

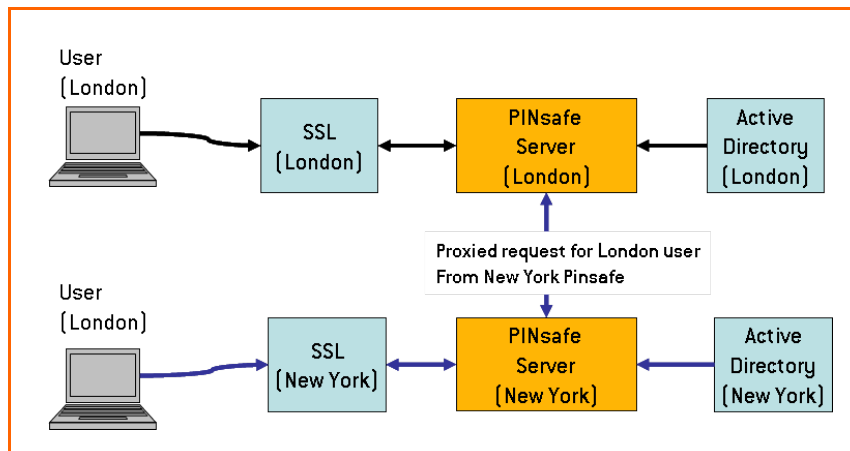


Figure 22. Example of peering for multi-office installation

Another application of this is to support the inter-working of different user repositories, although this configuration is deprecated by Version 3.3's ability to connect to multiple repositories. One PINsafe server can be configured to work with Active Directory, another to work with the XML repository. The two servers can be configured as peers so that a user from either user repository can authenticate to a VPN (or web application) authenticating via either PINsafe server.

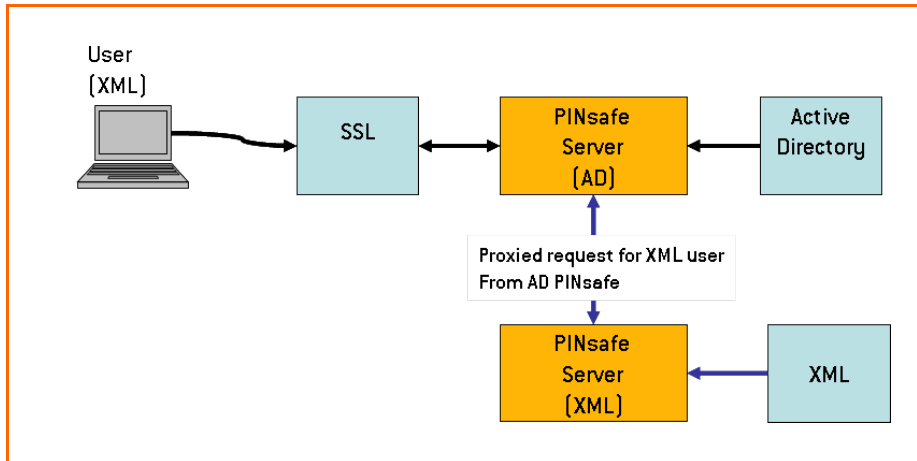


Figure 23.Example of peering fro multi-repository installation

It is possible to deploy both these servers on the same PINsafe appliance, thus avoiding increased hardware costs.

To implement peering, each PINsafe Peer must know the IP address, context and port details of every other PINsafe server in the peering network. Each PINsafe server also has a shared secret used for authentication. To make authentication requests, the requesting server must present the shared secret to authenticate itself to its peer.

To set up this relationship, enter the details on the Server->Peers screen on each PINsafe server. Using the London/New York example, on the London PINsafe server the following would be entered.

Server > Peers

Please enter the details for any peer PINsafe servers below.

Peers: Name:

Hostname/IP:

HTTP port:

SSL:

Context:

RADIUS authorisation port:

RADIUS accounting port:

Shared secret:

Figure 24.Example Peer configuration screen

And then on the New York server would be entered

The screenshot shows a configuration form for a peer server. The fields are as follows:

- Name: London
- Hostname/IP: pinsafe.company.co.uk
- HTTP port: 8080
- SSL: No
- Context: pinsafe
- RADIUS authorisation port: 1812
- RADIUS accounting port: 1813
- Shared secret: [masked]

Figure 25. Example Peer configuration screen

Peering can be used for RADIUS and agent XML authentication solutions. An inbound RADIUS request will be proxied via RADIUS to a peer PINsafe server as required. Similarly an Agent-XML based authentication request will be proxied via the Agent-XML interface.

Peering works by each peer keeping a record of the user-names active on the other servers. This list is updated periodically. How frequently and when this synchronisation takes place is configured on the server>jobs page: see section on Jobs. It is also possible to manual synchronise a peer from the user admin screen by pressing the Peer Sync button.

PINsafe as a RADIUS proxy

The RADIUS proxy option allows PINsafe to work alongside other authentication servers to allow end-users to support a hybrid authentication model. This can be useful when users are being migrated from a token to a PINsafe based solution.

The screenshot shows the 'Server>Peers' configuration page. The fields are as follows:

- Name: test
- Hostname/IP: 192.168.0.10
- HTTP port: 8080
- SSL: No
- Context: pinsafe3.5
- RADIUS authentication port: 1812
- RADIUS accounting port: 1813
- Shared secret: [masked]
- RADIUS Proxy: Unknown User

A 'Delete' button is visible at the bottom right of the form.

Figure 26. Setting PINsafe as a RADIUS Proxy

PINsafe can be configured to proxy to an external RADIUS server if the user is not a PINsafe user or if the submitted credentials appear to be a Token Passcode.

This feature is configured on the Server->Peers screen.

Multiple PINsafe servers using a single database

From PINsafe 3.2, it is possible for multiple PINsafe servers to share a database. This was possible in 3.2, but it would require that the repository on each server was configured identically. With the introduction of multiple repositories, it is now possible for different PINsafe servers to synchronise with different repositories, but for all servers to authenticate all users on all repositories.

In order to accomplish this, it is necessary to select an external database: the internal database is always local to the PINsafe server, so cannot be shared between multiple instances. All that is required, therefore, is that the database URL is the same on all PINsafe servers.

When repositories are synchronized into a shared database, the users can be authenticated by any PINsafe server using that database, even if the user belongs to a repository that is not defined on that server. All repositories will be displayed in the User Administration screen, whether or not the repositories are defined on a particular PINsafe server. The only difference is that users cannot be synced if the repository is not defined.

When connecting repositories to PINsafe servers sharing a database, the repository name must be unique. If the same name is used for repositories on two different PINsafe servers, it is assumed that they actually refer to the same repository. If this is not the case, it could cause users to be deleted every time the user sync runs. This is why the XML repository on each PINsafe server is named from the server name, rather than simply being called "XML", for example.

One consideration here is that the username must be unique over all repositories within the database. It is not possible to have a user called, for example, "admin" in one repository, and another also called "admin" in a different repository, even if those repositories are synchronized on different servers.

Operation & Maintenance

This section refers to PINsafe running on a server, rather than as an appliance. For details of the operation and maintenance of appliances refer to the appliance How To guides.

Tasks

Log files:

Tomcat creates a number of log-files under *usr/local/apache-tomcat-x.x-xx/logs*.

It is recommended that the older instances of these files are deleted to prevent them using up too much disk space.

How to perform back-ups of the PINsafe server

To back up the user and configuration data for the server, the easiest approach is to back up the webapps folder under the Tomcat directory.

usr/local/apache-tomcat-x.x-xx/webapps

Where x.x-xx is the tomcat version number.

This will back up all the user and system data required by PINsafe.

To ensure against sever hardware failure and to facilitate quick restore it is recommended that this back up should be stored on a remote server.

Saving the configuration

PINsafe has a save configuration feature that allows the current configuration to be saved to an xml file. This provides a useful record of the PINsafe configuration and can be useful for fault diagnosis

How to perform automated backups

The following guidelines are a suggested way of performing backups automatically in way that can be integrated with any existing enterprise back-up processes and systems.

This approach uses a back up script to copy the required files to a SAMBA share that allows the back-ups to be copied via the local network to remote server.

Creating a Samba Share:

This is a very quick guide to creating a public share using SAMBA, no security policies have been added to the share. It is being used as a form of access from your global backup server.

Firstly at the console, log in as root.

Start the x-display by typing *startx*

Once the graphical interface has started select *Applications – System Settings – Server Settings – Samba*

Select *Add*

In the Directory browse to and create a new folder called *PINsafeBackup* in the */home/swivel* directory. Then select the new folder as the samba share directory.

N.B. The backup script provided later presumes a */home/swivel/PINsafeBackup* folder exists, if you change this folder here remember to change the backup script to match

Select *Read* and *Allow access to everyone*

In the *Preferences – Server Settings - Security* menu item, set the Authentication Mode to *Share*

In the *Applications – System Settings – Server Settings – Services* menu item tick the *smb* service box and also select *Start Service*

You should now be able to access the share via a client machine pointing to //<server_ip>/PINsafeBackup where <server_ip> is the PINsafe server's IP address.

Writing a simple script to back up PINsafe:

Log on to the console as root.

Use an editor to create a file */home/swivel/backup.sh*

Enter the following code: **NB** replace the tomcat-x.x-xx version with the correct version number running on your server.

```
#!/bin/bash
/etc/init.d/tomcat stop
cd /usr/local/apache-tomcat-x.x-xx/webapps
tar --create \
--file=/home/swivel/PINsafeBackup/Backup.tar |
--label= `Backup` |
--verbose \
pinsafe
/etc/init.d/tomcat start
```

To make the script executable type:

```
chmod a+x /home/swivel/backup.sh
```

Running this script temporarily halts the PINsafe server and therefore prevents users authenticating via PINsafe during back-ups.

Running the script

To run the script manually, do the following:

```
/home/swivel/backup.sh
```

There should appear a new tar file called Backup.tar in your SAMBA share.

How often should I perform back-ups?

It is recommended that this script be run after the first user repository synchronization and then on a regular (e.g. weekly) basis. How regularly it is run depends on how often users and PINs change.

The script can be run as a cron job. The use of a SAMBA share means that this data can then be pulled from the machine and stored elsewhere to conform to any back-up routines/infrastructure that may already be in place.

These instructions are only a guideline and we would recommend you further your investigations into backup.

Restoring from Backup

If you should need to restore your server from a backup, carry out the following:

Log into the server as root and stop Tomcat:

```
/etc/init.d/tomcat stop
```

Delete the pinsafe folder from within the tomcat webapps directory

```
cd /usr/local/apache-tomcat-x.x-xx/webapps
```

```
rm -rf pinsafe
```

Copy and extract the backup file

```
cp /home/swivel/PINsafeBackup/Backup.tar /usr/local/jakarta-tomcat-x.x-xx/webapps
```

```
tar -xvf /usr/local/jakarta-tomcat-x.x-xx/webapps
```

```
Backup.tar
```

Restart Tomcat and check PINsafe is running and your settings are correct.

```
/etc/init.d/tomcat start
```

In a browser point to the admin console: http://server_ip:8080/pinsafe.

How to perform disaster recovery

In the event of a hardware failure or other scenario that requires a new server to be installed and brought up to the last recorded configuration of the live server.

1. Install PINsafe and associated software from the disks supplied as part of the install.
2. Restore the latest back-up copy of the webapps folder to webapps
3. Restart the tomcat server

Data Migration

The data migration feature allows you to move data from one database to another. For example if you want to change from using the internal database to an external database you can.

1. Prepare the new database
2. Add the details of the database to the Database – General screen.
3. Choose the Migrate option and select the new target database
4. Enter Migrate and click apply.

The data will be moved to the new database so you can use the new database without needing to re-provision users.

Job

There are a number of processes (or jobs) that the server needs to run on a regular basis. These handle such things as synchronizing to the user repository and checking for any accounts that should be locked due to inactivity.

For the most part these settings can be left to their default values but there may be reasons why an administrator would want to change these settings. When choosing these settings the administrator needs to balance the requirement to synchronize data regularly and the resultant loading on the server. Where possible these tasks should be scheduled to run during the server's quiet period.

Session Clean Up

The session clean-up job is used to invalidate, after a given time, any security strings that have been requested by the user.

For example a session is deemed to have started when a TURing image is requested. The security string presented within that security string is only valid for as long as the session is valid. The length of time for which the session is valid is set by the session clean-up time: if it is set to 120 seconds the user will have 2 minutes in which to use the security string to authenticate. If they attempt to authenticate with that security string after that time their authentication will fail.

The same setting also applies to security strings delivered by SMS messages when they have been explicitly requested by the user, e.g. via a GET MESSAGE button. SMS messages sent automatically, after an authentication attempt, do not expire in this way.

The following jobs can be set using *cron* notation, this is described in Appendix E Setting Schedules and CRON Strings

Peer Synchronization

This is similar to the user repository synchronization, only it refers to a server synchronizing its list of users with other peer servers within its peer network. Every time this job is run, the server will request an up to date user list from its peer servers.

Inactive User Check

If there are policies in place on the server to lock accounts that have been inactive for more than a certain time then this job will detect those inactive accounts and lock them.

PIN expiry check

If there are policies in place on the server that limit how long a PIN is valid for, this job will go through the user list and check to see the last time the PIN was changed and then either do nothing, send out a PIN expiry warning or lock out the account.

Audit Log tidy

PINsafe maintains an log of user activity for the users for a pre-determined period (as set on the Policy-General screen. The audit log tidy job deletes audit log entries that are now longer required to maintain this log.

Logs and Alarms

PINsafe generates a range of log events and alarms they consist of the following options.

- XML Log files written to the local PINsafe server
- Log files written to Syslog
- Alarm events sent as emails to a specified email address.

XML Logging

XML logs are generated for a number of system events. They have varying levels of severity: FATAL, ERROR, WARNING and INFO. You can set the level of logging: setting the level to INFO will mean all events of severity INFO and above will be recorded.

Logging > XML

Please specify how the server logs events to local XML files. These may be viewed or downloaded using the log viewer.

Level:

Filesize (KB):

File count:

Debug enabled:

Figure 27. Screen for configuring XML Logging

The log events are written to files on the PINsafe server at <tomcat>\webapps\pinsafe\WEB-INF\logs.

If you are running a backup script like the one described earlier in this manual then these log files can be included in that back up to provide a longer term log of system activity.

A log file is written to (as pinsafe.log) until it reaches the file size specified on the Logging > XML screen. This file is then renamed to pinsafe.log.1, a new pinsafe.log is created and writing resumes to that file. This process repeats, creating pinsafe.log.2, pinsafe.log.3 etc.

The number of log files used is determined by the File Count entry. Once this count is reached, the oldest log file on the server is overwritten.

If debug is enabled, debug logs are created that give much more detailed information about the processes running within the server. This setting creates large log files and has an impact on the performance on the server and therefore should only be used for fault

diagnosis. Debug logs are written to a separate file, <tomcat>\webapps\pinsafe\WEB-INF\logs\debug.log

The contents of the XML log files can be viewed via the PINsafe Administration interface, Log Viewer screen and can be downloaded from the PINsafe server to a local machine.

Syslog

As an alternative or addition to writing XML log files locally, PINsafe can also write log files remotely by using the Syslog logging feature.

Logging>Syslog ⓘ

Please enter the details of an external syslog server to which PINsafe logging events should be delivered.

Syslogs: Host:

Level: ▾

Facility: ▾

Host:

Level: ▾

Facility: ▾


Figure 28.Syslog configuration screen

The logging level is set in the same way as for XML logging. The additional information required for Syslog is the host(s) to which the logs will be written and the syslog facility to be used.

SMTP (email) Logging

Certain events can be emailed to operational managers. These are system errors, account lock-outs and account creations and deletions. The configuration screen for this feature is shown below.

To use SMTP logging you must have access to a suitable SMTP mail-server. The details for this server must be entered on to the Server > SMTP screen.


Logging>SMTP 

Please select which logging events are delivered as emails.

From:	<input type="text" value="PINsafe"/>
Send errors:	<input type="button" value="No"/>
Errors address:	<input type="text"/>
Errors subject:	<input type="text" value="PINsafe Error"/>
Send account locks:	<input type="button" value="No"/>
Account locks address:	<input type="text"/>
Account locks subject:	<input type="text" value="PINsafe Account Locke"/>
Send User Account Create/Delete:	<input type="button" value="No"/>
Account audit address:	<input type="text"/>
Account create subject:	<input type="text" value="PINsafe Account Creat"/>
Account delete subject:	<input type="text" value="PINsafe Account Delet"/>

Figure 29.SMTP Logging configuration screen

Administrator's Guide

This section concentrates on explaining how the PINsafe server is administered. It covers all the common tasks that an administrator would normally undertake. **NB** A full on-line help admin reference guide is provided as part of the Swivel distribution. Clicking the  icon will open a web browser with some help pages relating to that aspect of PINsafe.

This section assumes all the required integration tasks described earlier in this document have been completed.

Setting Policies

There are a number of policies relating to account/PIN management, for example PIN length and PIN validity periods. There are two modes of operation for PINsafe: standard and PINless; these two modes are explained below:

Standard


Users are assigned a PIN. They are sent a random security string and use their PIN to extract a one-time code.

PINless

Users do not have a PIN, they are sent a random one-time code which they enter to authenticate.

Both modes can be supported on a PINsafe server. Group memberships are used to define which mode a user uses. To make a group PINless, check the PINless property for the group in the Repository > Groups page.

PINsafe Manual

Repository>Groups 

Please enter the repository group information to be used by the PINsafe server.
This includes group privileges and Active Directory/LDAP definition. For XML repository, please copy the group name into the definition.

	Single	Dual	Swivlet	Admin	Helpdesk	PINless	
Name: <input type="text" value="PINsafeUsers"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Delete"/>
Definitions:							
ith000140: <input type="text" value="PINsafeUsers"/>							
LDAP: <input type="text" value="cn=PINsafeUsers,dc=test,dc=local"/>							
Name: <input type="text" value="PINsafeAdministrators"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Delete"/>
Definitions:							
ith000140: <input type="text" value="PINsafeAdministrators"/>							
LDAP: <input type="text" value="cn=PINsafeAdmins,dc=test,dc=local"/>							
Name: <input type="text" value="PINlessUsers"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Delete"/>
Definitions:							
ith000140: <input type="text" value="PINlessUsers"/>							
LDAP: <input type="text" value="cn=PINlessUsers,dc=test,dc=local"/>							
Name: <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Definitions:							
ith000140: <input type="text"/>							
LDAP: <input type="text"/>							

Figure 30.Groups screen, showing PINless user group

Some policies apply to both PIN and PINless users, other are specific.

The general policies are set on the Policy > General screen.

Policy>General ⓘ

Please enter the policies to apply to authentication.

Security string type:

Auto. set credentials on user creation:

Maximum login tries:

Inactive account expiry (days):

Non-Existent Users appear to be:

Audit Log length (days):

Figure 31.General Policy Screen

Security String Type

You can set the security string to be Numbers and/or Letters. You can have upper or lower case characters or a mixture of both. Mixed case is not recommended for TURING images as it can be difficult to differentiate between characters such as lower case l and number 1, even without the obfuscation.

You can even have a mixture of upper case letters and numbers. In order to make this option usable, letters that can easily be confused with numbers are not used. Therefore, if in doubt, a character is a number.

If the SMS delivery of security strings is used, then it is recommended that numbers are used for security strings.



Figure 32.Alpha-numeric security string; first character is an 8

Maximum login tries

This is the maximum number of consecutive failed login attempts that a user can have before their account is locked out. See account unlocking accounts.

Inactive account expiry

If an account is not used for a specified period, it will become locked. This setting allows you to specify that period (in days). If this is set to 0 then the user account never expires due to inactivity.

Auto Credential setting

If you set this parameter to YES, then whenever a new account is created, PINsafe will automatically create a PIN for them. If a password is also required, this will also be generated. See Adding User Groups for more details.

Non-Existent Users appear to be

When a TURING image is requested for a user that does not exist, PINsafe will still produce an image. This is to prevent a user determining which username are valid accounts. You can specify the type of image that is presented when a image for a non-existent user is requested.

Therefore if all your users have PINs you should set this to PINned. If all your users are PINless, this should be set to PINless and if you have a mixture of user you should set this value to mixed.

Audit Log Length

PINsafe maintains a audit log of user activity; that can be extracted/interrogated by the Admin API. This setting dictates how long the activity records are maintained.

PIN and OTC Policies

PIN and OTC policies are set on the Policy > PIN and OTC screen. PINs within the PINsafe product are the prime authentication credential and administrators may wish to replicate existing password management policies within PINsafe.

Policy > PIN and OTC ⓘ

Please enter the policies to apply to PINs.

Minimum PIN size:	<input type="text" value="4"/>
PIN expiry (days):	<input type="text" value="0"/>
PIN expiry warning (days):	<input type="text" value="7"/>
Require PIN change after auto. setting:	<input type="text" value="No"/>
Require PIN change after admin. reset:	<input type="text" value="No"/>
PINless OTC length:	<input type="text" value="6"/>
Maximum repeated PIN digits:	<input type="text" value="0"/>
Allow numerical sequences for PIN:	<input type="text" value="Yes"/>
Auto-reset PIN on expiry:	<input type="text" value="Yes"/>
PIN change grace period (days):	<input type="text" value="0"/>

Figure 33. PIN Policy Screen

From this screen you can set the minimum PIN size (from 4 to 10 characters). You can also set a PIN expiry period. This determines how long a PIN is valid for: for example setting this figure to 90 days will ensure that users will need to change their PIN at least every 90 days. Setting this value to 0 (zero) would mean that the PINs would never expire.

You can ensure that users are warned about their impending PIN expiry. Setting the PIN expiry warning will determine how many days in advance the users will be prompted to change their PIN. The content and delivery of the warning will depend on which alert group the user is a member of.

Another PIN policy that PINsafe can implement is to require a PIN change after the user has had a PIN auto-created (e.g. via auto credential creation) or where a user has had their PIN changed by the Administrator. Where these policies are in-force, a user must authenticate and then change their PIN: the PINs that have been created for them will only work once.

For PINless users, you can set a policy of how long the one-time code should be. This is set to 6 as a default, but can be from 4 to 8 digits.

For PINs you can also set policies on what PINs are valid. There are two optional policies that can be enforced:

- Maximum repeated digits. This indicates the maximum number of repeated digits that are allowed in the PIN. This allows the administrator to define what PINs are valid. E.g. it allows them to enforce a no repeated digits policy.
- Allow series. This sets whether ascending or descending arithmetic series are allowed as PINs. For example not allowing such series would prevent 1234, 2468, 6543 etc from being set as PIN numbers.

Administrators should be aware that enforcing these policies does reduce the number of possible valid PIN combinations and if they wish to enforce them all, they may wish to consider increasing the PIN length. These policies are enforced when users set their own PINs via the change PIN function and also when PINs are generated by PINsafe. An administrator can override these policies and manually set any PIN number.

If you can specify the behaviour for when a PIN is due to expire. If you set Auto-reset PIN on expiry to Yes, a few days (set by the grace period) before a user's PIN expires, they are automatically sent a new PIN. If this is not set, the account will become locked.

Password Policies



Policy > Password ⓘ

Please enter the policies to apply to passwords.

Require password: No ▾

Password mask: adsxxx

Check Password with Repository: No ▾

Apply Reset

Figure 34.Password Policy Screen

Passwords are an optional part of the PINsafe authentication model. If required the Administrator can ensure that all accounts have a password as well as a PIN associated with them. If passwords are required then if auto-credential creation is set, PINsafe will create a random password for the user. The random password will conform to the password mask. The password mask allows administrators to ensure that certain character types are included in the password in the specified order where: a = alpha, d = digit and s = special character. An example of a password conforming to the above password mask would be r4p&dl2a.

Another way of using passwords with PINsafe is to use the password that the user has from their AD account (or other repository type). If the "Check Password with Repository" option is set to true, when a user attempts to authenticate no does PINsafe check their OTC, but also checks the password they submitted against their repository. To do this the PINsafe server must be able to connect to the user's repository.

User self-reset



Policy > Self-Reset

Please enter the policies to apply to user self-reset.

Allow user self-reset: ▾

Maximum self-reset tries:

Figure 35. Self Reset Policy Screen

PINsafe supports a self-reset policy, whereby if a user's account has been locked they can unlock it. They do this by being sent an unlock code via their alert transport; they then enter this code to authenticate. The above screen enables this feature and stipulates the maximum number of reset tries a user is allowed.

User Policies

Along with the server-wide policies the Administrator can set policies for individual users. To access this feature the Administrator can go to the User Administration screen and select a user and then select the Policy button. This will bring up the following screen for that user.

Username:	fred
Created:	16:07:13 20 April 2006
Last login:	16:08:51 20 April 2006
Last PIN change:	N/A
Last self-reset:	N/A
Disabled:	<input type="checkbox"/>
Change PIN at first login:	<input type="checkbox"/>
PIN never expires:	<input type="checkbox"/>
<input type="button" value="Reset"/>	<input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>

Figure 36. User Policy Screen

This screen shows the status of the user, when they were created on the system and when they last logged-in etc. The Administrator can also, from this screen, implement the following policies.

Disabled: If an account is disabled a user cannot authenticate. Accounts can only be enabled again from this screen. Administrators may wish to disable accounts when a user no longer requires access but they wish to retain the information associated with that account. This feature is not available if the import disabled state on the repository->general screen has been set to Yes.

Change PIN: The Administrator can ensure that the a user has to change their PIN at their next login; i.e. their PIN will only be valid for one authentication

Never Expires: The PIN for this account will never expire; this takes precedence over any server-wide PIN policy. Administrators may wish to use this feature for admin accounts.

Single Channel

The Servers > Single Channel screen allows the Administrator to specify how single channel security strings are presented to the user. From this screen you can specify whether the security string image will be displayed as a TURING, PATTERN or BUTTON image and whether the security string images will be animated. In this screen you can also determine whether to allow session creation via username. This means allowing a user to request a TURING image from any URL, for example by pasting

`http://<pinsafe url>/pinsafe/SCImage?username=<username>` into a web browser.

This provides flexibility in terms on security string delivery but does require that port 8080 is opened up on the PINsafe server. See Protecting the PINsafe Admin Console

Dual Channel

The Server > Dual Channel screen determines how dual channel security strings are delivered. The default model for dual channel security strings is that a new security string is sent whenever a user attempts to authenticate, thus ensuring that the user always has a valid security string to use.

An alternative is to only send a security string to the user when they explicitly request one; this is the on-demand authentication mode that can be enabled from this screen. If this mode is used the security string sent to the user is only valid for as long as the session time-out (clean-up) period specified on the server > jobs screen.

On-demand delivery means that a user can request a new security string at any time even when on-demand authentication is not enabled. This request is made via make a GET to <http://<pinsafe url>/pinsafe/DCMessage?username=<username>>

The request to send a dual channel security string can be via an agent configured on the PINsafe server; alternatively PINsafe can be configured to allow the request for a security string to be instigated from any IP address in a similar way to requesting TURING images. This is enabled by setting Allow message request by username to Yes.

You can also configure PINsafe to return a confirmation image when a security is requested by setting Confirmation image on message request to Yes. This will return an image to indicate to the user whether the message request has been received successfully by PINsafe.



Figure 37. Message Request Confirmation Image

This allows for a dual channel image to be requested in the same way as a TURING image from within JavaScript as well as providing useful feedback to the end-user. Note that the confirmation image confirms that PINsafe has received the request not that the image has been sent.

Alerting Users

The Transport > Alerts screen can be used to determine for which events users receive alerts. Alerts will be sent to the user based on which Alert Transport group to which they belong.

Transport > User Alerts ⓘ

Please select which alerts are delivered to users.

PIN expiry warning: ▾

PIN change required: ▾

PIN changed: ▾

Account locked: ▾

Device key allocated: ▾

Figure 38.Alert Configuration Screen

Managing Users

This section covers the management of users within the PINsafe server; including the addition and removal of users, changing PINs and Passwords and unlocking accounts.

Adding User Groups

The model for handling functionality within groups has been changed for PINsafe 3.3, to accommodate the multiple repository facility. In earlier versions of PINsafe, there were eight fixed groups on the Repository > Groups page, plus a group for each agent, transport class, third party authentication and RADIUS NAS. The group name was typed in, and the syntax had to be specific to the repository type.

In the new model, groups are all defined on the Repository > Groups page. Rather than being associated with a single function, each group can have as many functions as desired. Also, groups can be defined across multiple repositories. As many groups as are necessary can be defined. A new installation will have just two groups: normal users and administrators. However, as many groups can be defined as are necessary to give the desired access control.

To define a new group, all that is necessary is to enter a unique group name in the Name field in the blank section at the bottom of the Repository > Groups page. However, for that group to be useful, two additional pieces of information are required:

- What functionality the group is to have
- How the group maps to a group within each repository

Standard functionality is defined by setting the checkboxes for the group:

- **Single** – connect using single-channel authentication
- **Dual** – connect using dual-channel authentication
- **Swivlet** – use the Swivlet application
- **Admin** – administer the entire PINsafe configuration
- **Helpdesk** – administer PINsafe users
- **PINless** – user has no PIN, just a password

For users of previous versions of PINsafe, these represent 6 of the 8 standard groups previously defined. There is no equivalent of the PINsafe users group, as a member of any of the defined groups is by definition a PINsafe user. The RADIUS group is also unnecessary, as in order to be a RADIUS user, a user must be a member of a NAS group.

To define additional functionality, a group must be selected on the appropriate agent, transport class, third party authentication or NAS. The groups on these forms are now drop-down boxes showing all defined groups, so you must add a group on the Repository > Groups page to correspond to the required functionality. For this reason, it is possible to define a group but not tick any of the boxes.

To associate a repository group with a PINsafe group, you must enter something in the definition field for each repository. For the XML repository, simply copy the group name into

PINsafe Manual

the definition field. For Active Directory or LDAP, you will need to enter the fully-qualified domain name (FQDN) for the repository group. Leaving a definition field blank means that no users of that particular repository will be members of the appropriate group. There is no requirement to enter a definition for every repository in every group, although for the group to be useful, there must be a definition for at least one repository. Conversely, it is not necessary to define a separate group for each repository: if the functionality is the same for groups within different repositories, they can be defined as the same group within PINsafe.

The Repository > Groups admin page will look something like the following:

The screenshot shows the 'Repository > Groups' admin page. It features a table with columns for 'Name', 'Definitions', and channel options: 'Single', 'Dual', 'Swivlet', 'Admin', 'Helpdesk', and 'PINless'. There are three rows of data, each with a 'Delete' button. The first row is for 'PINsafeUsers', the second for 'PINsafeAdministrators', and the third for 'PINlessUsers'. The fourth row is empty. At the bottom right, there are 'Apply' and 'Reset' buttons.

Name:	Single	Dual	Swivlet	Admin	Helpdesk	PINless	
<input type="text" value="PINsafeUsers"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Delete"/>
Definitions: ith000140: <input type="text" value="PINsafeUsers"/> LDAP: <input type="text" value="cn=PINsafeUsers,dc=test,dc=local"/>							
<input type="text" value="PINsafeAdministrators"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Delete"/>
Definitions: ith000140: <input type="text" value="PINsafeAdministrators"/> LDAP: <input type="text" value="cn=PINsafeAdmins,dc=test,dc=local"/>							
<input type="text" value="PINlessUsers"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="Delete"/>
Definitions: ith000140: <input type="text" value="PINlessUsers"/> LDAP: <input type="text" value="cn=PINlessUsers,dc=test,dc=local"/>							
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Definitions: ith000140: <input type="text"/> LDAP: <input type="text"/>							

Figure 39. Repository Groups page

Adding Users

To add users to PINsafe you need to add them to an appropriate group within the repository and synchronise PINsafe with that repository. If you have set Auto Create credentials to Yes, the user will be automatically sent a message with their account details in it. If Auto Create is not set you will need to manually reset or send out their PIN.

When adding users to the PINsafe server you need to consider the following:-

- What rights will they have, e.g. will they be able to use single channel, dual channel or both
- How will security strings be delivered to them
- How will their PIN (and Password) be created and delivered to them.

The implementation of these will be achieved by ensuring that the user is a member of an appropriate user group. See the previous section for details.

Allocating users to authentication methods

If the user accounts are being synchronized with Active Directory, the user must be a member of the correct group(s) within Active Directory to be able to use the associated authentication methods within PINsafe. The Repository > Groups screen will show of which Active Directory groups the user must be a member. Different authentication options may be associated with different groups within Active Directory or, as in the example below, all users will have access to all authentication types.

Repository > Groups

Please enter the repository group information to be used by the PINsafe server. This includes group privileges and Active Directory/LDAP definition. For XML repository, please copy the group name into the definition.

	Single	Dual	Swivlet	Admin	Helpdesk	PINless
Name: PINsafeUsers Definitions: ith000140: PINsafeUsers LDAP: cn=vpnsslusers,ou=group,dc=banquecramer,dc=ch	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Name: PINsafeAdministrators Definitions: ith000140: PINsafeAdministrators LDAP: cn=vpnssladmins,ou=group,dc=banquecramer,dc=ch	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Name: <input type="text"/> Definitions: ith000140: <input type="text"/> LDAP: <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: Delete, Apply, Reset

Figure 40. Simple Active Directory Group Structure

In addition you can specify that one or more groups for users will operate “PINlessly”. To implement this, simply make sure that the PINless box is checked for the appropriate group(s).

Allocating Users to Transports

Users need to be associated with transport classes for the delivery of security strings and for system alerts, e.g. notification of PIN.

The Transport > General screen shows which groups are associated with which transports. It also shows the destination attribute; therefore the Administrator needs to ensure that this attribute is set for the user.

Identifier:	<input type="text" value="GSM Modem"/>
Class:	<input type="text" value="com.swiveltechnologies.pinsafe.transport.GsmTran"/>
Strings per message:	<input type="text" value="1"/>
Destination attribute:	<input type="text" value="phone"/>
Repository group:	<input type="text" value="GSMModemUsers"/>
Alert repository group:	<input type="text" value="GSMModemUsers"/>

Figure 41. Screen showing AD groups associated with GSM Modem transport.

The Administrator may wish to use different transports for alerts from security string delivery.

Allocating Users to Agents

It is possible to configure PINsafe so that only certain users can authenticate via certain agents. When an agent is added to PINsafe it may have had a group associated with it. If this is the case then the user must be placed in that group in order for that user to be able to authenticate via that agent. If no group is specified, any user can authenticate using that agent.

Creating the account

Once the user has been made a member of the relevant groups the repository can be synchronised with PINsafe; this can either be done manually via the User Admin screen or automatically be setting up a job to perform this. (Server-Jobs, see Operation & Maintenance)


PINsafe will create a new account; if auto-credentials create is enabled, PINsafe will also create a username (and password) if required and send them to the user via their allocated Alert transport.

Unlocking Accounts

Accounts can be locked or disabled. If a user's account is locked or disabled they will not be able to authenticate via PINsafe.

You can configure PINsafe to send an email to an administrator to inform them when an account has become locked. See Logs and Alarms.

The main status screen on PINsafe immediately indicates if there are locked or disabled accounts on the PINsafe server.

PINsafe Status 

Licensed to	
Licensed users	5
User accounts	3
Locked user accounts	1
Disabled user accounts	1
Active user repository	XML
RADIUS server enabled	No
Server IP address	127.0.0.1
Server hostname	ITH000136

Figure 42. PINsafe Status Screen

The entries for the Locked and Disabled are hyperlinks to the user administration page; clicking on these links will take you to a list of all Locked accounts and all Disabled accounts respectively.

On the User Administration screen, locked accounts are shown in **bold** and disabled accounts are in *italics*.

test10	▼	✓	✓	✓	✓	✓	
test11	▼	✓	✓	✓	✓	✓	
<i>test12</i>	▼	✓	✓	✓	✓	✓	
test13	▼	✓	✓	✓	✓	✓	
test14	▲	✓	✓	✓	✓	✓	
<input type="button" value="Edit"/> <input type="button" value="Policy"/> <input type="button" value="Reset PIN"/> <input type="button" value="Reset Pwd"/> <input type="button" value="Resend"/> <input type="button" value="Unlock"/> <input type="button" value="Delete"/>							
test15	▼	✓	✓	✓	✓	✓	

Figure 43. Accounts listed on User Administration screen

To unlock an account, click on the account in question and then on Unlock. To enable a disabled account, click on the Policy button and uncheck the disabled checkbox.

Viewing and Sending Security Strings

Username	Admin	Helpdesk	Single	Dual	Swivlet	PINless
admin	✓	✓	✓	✓	✓	
helpdesk		✓	✓	✓	✓	
test	✓	✓	✓	✓	✓	

Figure 44.Accounts listed showing Send String option

The user can be sent a new security string from the admin console by selecting the user and clicking the Send String button. Selecting the View Strings option allows a helpdesk user to view the security string that has been sent to the user.

Username: test

Single Channel

1	2	3	4	5	6	7	8	9	0
2	5	9	0	3	1	8	4	6	7

Dual Channel

1	2	3	4	5	6	7	8	9	0
7	2	1	4	8	6	5	3	0	9

Figure 45.View Strings screen

Selecting Show on the single channel option will create and display a new single channel string. Selecting Refresh on the Dual Channel option will generate a new dual channel string for the user and instigate the sending of this security string to the user.

PINsafe Manual
Resetting/Resending Credentials

You can manually set a PIN to a known value if required by selecting the Reset PIN option. Alternatively you can make PINsafe create a new PIN for a user and set that new PIN to the user via their Alert Transport if they have one configured.

This is useful where a user has forgotten their PIN or lost the credentials alert message. It is recommended that the logs are checked to ensure that the new PIN message has been successfully despatched.

Appendix A Building and Deploying PINsafe server

Upgrading from PINsafe version 3.2 onwards

These instructions refer to standalone PINsafe servers only, separate instructions apply for upgrading HA appliances, contact support@swivelsecure.com for more details.

Upgrading from version 3.2/3.3 should be transparent. Both the user database and the configuration will be upgraded automatically. To upgrade from an existing installation of PINsafe 3.2,3.3 and 3.4 follow the following procedure:

1. Stop the Tomcat Server (service tomcat5 stop).
2. It is **highly recommended** that you take a copy of the entire ...\- 3. Back up the PINsafe configuration by taking a copy of ...\- 4. Back up the PINsafe User Repository by taking a copy of ...\- 5. Back up the PINsafe user data by taking a copy everything under ...\- 6. Back up any customized transport, user repository classes residing on the PINsafe server.
- 7. Start the Tomcat Server (service tomcat5 start)
- 8. Remove the pinsafe.war file from webapps, ensuring that you have a back-up copy. This should undeploy pinsafe and the pinsafe folder should be deleted
- 9. Stop Tomcat. If the webapps\pinsafe folder has not been deleted manually delete it.
- 10. Copy the new pinsafe.war file to the webapps folder
- 11. Start the Tomcat server(service tomcat5 start): this will deploy the PINsafe application.
- 12. Stop the server
- 13. Copy the backed-up config.xml file from step 3 to ...\- 14. If you are using an XML repository, restore the backed-up copy from step 4 to ...\- 15. If you are using an internal database, restore the database files backed up in step 5 to ...\- 16. Ensure that the ownerships and permissions on the file that you have restored are correct

```
drwxrwxr-x  2 swivel swivel  4096 Dec  8 12:13 db
```

For example to change the ownership of data run the chown command from the WEB-INF directory.

```
chown -R swivel:swivel db
```

To change the permission of data run the chmod command from the WEB-INF directory

```
chmod -R 775 db
```

17. Restart the server.

After upgrading you will see that any repository you had will exist on the new installation and it will be named after the associated hostname (or hostname followed by context in the case of the XML repository). Therefore if you had an AD repository in 3.2 you will have an XML repository in 3.3 named after the AD server's hostname (or IP address)

If you had an AD repository on your 3.2 installation you will now have the option to add an XML repository. It is recommended that you do this as this gives you the ability to create admin accounts whilst you are working on the installation

Upgrading from PINsafe version 3.1

To upgrade from PINsafe version 3.1, follow the same procedure as above, except that you should NOT restore config.xml in step 11. Configurations from versions earlier than 3.2 cannot be upgraded automatically. Instead, you should follow the following steps after completing step 15 above.

1. Log into the administration console using the username "admin" and the PIN 1234.
2. You will now have the new version (running under /pinsafe) running alongside the existing version (now running under /pinsafeold). You can then cut and paste configuration settings from one to the other.

NB: You may want to delete the user sync job whilst performing the configuration as if the repository synchronizes prior to the repository groups being configured then user accounts may be deleted. To do this, go to the Repository section and select the last sub-entry: this should be labelled with the PINsafe server computer name. Delete the Synchronization Schedule entry and click Apply.

Architecture

The PINsafe application runs within a JSP/Servlet Container, Apache Tomcat being the default that is recommended, specifically version 5.5.23. PINsafe has also had some testing under Tomcat 6 and Jetty 6.1, and no problems have been observed; however, these containers are not yet recommended for use with PINsafe, and earlier versions of Tomcat (prior to version 5) or Jetty are known not to be compatible.

PINsafe also requires a Java JRE. Specifically, Java JRE 1.6 is recommended, and is the minimum requirement. Certain configurations of the product the Java Communication API needs to be installed: more details in the installation section.

PINsafe needs a database server to store user data and credentials. An internal database server is provided, but there is also the option to use an external database server. The list of currently supported database servers can be found in the Database > General section of the administration console. Note that in order to use any of these databases you will need the appropriate JDBC driver. These are not provided with PINsafe because of licensing regulations, but can usually be obtained free of charge from the database manufacturer.

PINsafe can use its own repository for sourcing user accounts, or can be configured to work with an existing Active Directory or other LDAP-based user repository: see "How to guides" in the Appendix.

An important part of this document is the record of the installation, covered in Appendix D PINsafe Installation details. It is recommended that this section is completed at the time of installation and kept with the server or elsewhere where it can be found easily if required. A copy of the installation record needs to be sent to Swivel Secure for their records; this can be sent to

e-mail support@swivelsecure.com

fax **+44 1423 858172**

PINsafe can be purchased as an Appliance or software only. If an Appliance is shipped with PINsafe, all software will come pre-loaded, there is an Appliance User guide that covers the appliance specific configuration issues such as changing IP addresses etc.

Please note that the installation should only be attempted by someone comfortable with this kind of installation. Also if you install PINsafe on your own hardware platform and OS that you should take all the necessary steps to security harden the installation.

Before you deploy and start PINsafe, ensure you have the following software installed:

- Java runtime environment (JRE) Version 1.6, available from www.sun.java.com
- Tomcat v5.5 available from <http://tomcat.apache.org/> Version 5.5.23 recommended.
- Java Communications API if you intend using a GSM MODEM (follow the Java Comm

API installation instructions) See [Appendix A](#) for instructions. This is available from <http://java.sun.com/products/javacomm/downloads/index.html>

- The PINsafe distribution (.war) file

If you have an appliance the default Linux password is lockbox. This applies for root and the user swivel. These passwords should be changed using the linux passwd command.

PINsafe Deployment

This section refers to a “self-install”, an Appliance comes with the software pre-installed. To deploy and start PINsafe perform the following steps:

1. Place the war file in Tomcat's webapps folder
2. Start Tomcat
3. Browse to http://PINsafe_server_IP_address:portnumber/pinsafe (<http://localhost:8080/pinsafe> for example)
4. The default administrator is 'admin' with a PIN of '1234' so enter admin in the username click start session, then enter the first 4 digits of the security string. Click login.

Protecting the PINsafe Admin Console

In order for users to retrieve TURING images from PINsafe, the PINsafe server needs to be accessible via the internet; this requires the opening up of port 8080 by default.

As the PINsafe admin console is also on port 8080, measures need to be taken to protect the admin pages from unauthorised access. Frequently a customer will have a proxy that they can configure to proxy the inbound image requests. Where this is not available (and even where it is) the Admin-Console filter can ensure that access to the PINsafe Admin Console is only available from a predefined set of IP addresses.

The PINsafe Admin-Console Filter is an implementation of a [J2EE Servlet Filter](#) that is deployed against the Admin-Login servlet.

Configuring the filter

The filter configuration is controlled by two files found in the WEB-INF folder:

filter.properties	Determines the way the filter behaves when access is denied or granted
ranges.xml	List of IP ranges that can access the Admin Console

PINsafe Manual

These files are read as TOMCAT initializes the filter; therefore changes to these files will only take affect after TOMCAT has been restarted.

Editing filter.properties

The default filter.properties file is shown below.

```
#
# Admin Console Filter Localization
#
# Commented lines will result in no message being logged
#
# ALLOWED = Access Allowed
DENIED = Access Denied
ERROR = Page Not Found
# FILTERING = Filtering
STATUS = 404
```


The entries are as follows:

Entry	Meaning	Default
ALLOWED	Message written to TOMCAT console with request IP address when the filter allows access.	Commented out; filter is silent
DENIED	Message written to TOMCAT console with request IP address when the filter denies access.	Access Denied
ERROR	Message reported back to browser when access is denied. If not set, no response is sent and the browser will eventually time out.	Page Not Found
FILTERING	Message written to TOMCAT console followed by address ranges as TOMCAT initializes the filter.	Commented out; filter is silent
STATUS	The http status code reported back when access is denied. This should match the error message.	404

Editing ranges.xml

The ranges.xml file holds the list of IP addresses that are allowed to access the admin console.

The default ranges.xml file is shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE properties (View Source for full doctype...)>
<properties version="1.0">
<entry key="anyone">0/0</entry>
<entry key="localhost">127.0.0.1/255.255.255.255</entry>
</properties>
```

The default configured ranges are named "anyone" and "localhost" and represent access from any IP address and localhost only respectively.

An address range is specified as an IP address followed (optionally) by a mask. The mask can be a single integer representing the number of significant address bits that must match for access to be allowed or it can be an IP-style dotted decimal. Both styles are present in the default file, but further examples are shown below.

IP Range	Meaning
0/0	A /0 mask means that no bits need to match in the address. This allows access from all IP addresses.
123.123.123.123/0	
127.0.0.1/32	A /32 mask means all 32 bits must match. The equivalent dotted-decimal is
127.0.0.1/255.255.255.255	255.255.255.255. Specifying no mask is
127.0.0.1	the same as specifying a /32 mask.
192.168.0.0/24	Access will be allowed from any address
192.168.0.0/255.255.255.0	on the 192.168.0 subnet.

The default entries allow access from all IP addresses. Removing the entry for “anyone” will restrict access to localhost. Further ranges can be added to ease administration. All ranges should have a unique name.

Activating the Filter

The filter is applied to the admin console by specifying the filter-servlet relationship in the web.xml file found in the webapps/pinsafe/WEB-INF folder. In versions of PINsafe that have the filter bundled there is no need to change this file. If the filter is being used with a 3.1.x version of pinsafe then the web.xml file will need editing.

The segment that needs inserting is in the web.xml.fragment file and is shown below.

```
<filter>
  <filter-name>AdminConsoleFilter</filter-name>
  <filter-class>com.swiveltechnologies.filter.AdminConsoleFilter</filter-class>
</filter>
<filter-mapping>
  <filter-name>AdminConsoleFilter</filter-name>
  <servlet-name>AdminLogin</servlet-name>
</filter-mapping>
```

The <filter> element describes the filter and the <filter-mapping> element applies it to the AdminLogin Servlet and the fragment needs inserting at the top of the web.xml file, before the first servlet definition, as illustrated below.

```
<filter>
  <filter-name>AdminConsoleFilter</filter-name>
  <filter-class>com.swiveltechnologies.filter.AdminConsoleFilter</filter-class>
</filter>
<filter-mapping>
  <filter-name>AdminConsoleFilter</filter-name>
  <servlet-name>AdminLogin</servlet-name>
</filter-mapping>
<servlet>
  <servlet-name>QuartzInitializer</servlet-name>
</servlet>
```

To activate these new settings TOMCAT must be restarted.

Filter in operation

When someone attempts to access any part of the admin console they are redirected to the admin log-in page. At this point the filter intercepts the request and checks to see if the IP address is on the allowed list. If it is not it returns the error code and message defined in the filter.properties file.

Session Sharing

PINsafe will use multicast for session sharing, therefore no IP addresses need specifying. PINsafe will use session sharing if there is a cache.xml defined under the webapps/pinsafe/WEB-INF/classes. It is recommended that anyone wishing to use session sharing consult with a Swivel Technician for advice as there are certain requirements on the network infrastructure.

Appendix B Windows Installation of the Java Comm API

1. unzip the file javacomm20-win32.zip into the root of C:

This will produce a hierarchy with a top level directory commapi.

This example assumes that you have installed the J2SE version 6 and has been installed into C:\Program Files\Java\jdk1.6.0_06

2. Copy win32com.dll to your Java\jdk....\jre\bin directory.

C:\>copy c:\commapi\win32com.dll to C:\Program Files\Java\jdk1.6.0_06\jre\bin

3. Copy comm.jar to your Java\jdk....\jre\lib\ext directory.

C:\>copy c:\commapi\comm.jar to C:\Program Files\Java\jdk1.6.0_06\jre\lib\ext

4. Copy javax.comm.properties to your Java\jdk....\jre\lib directory.

C:\>copy c:\commapi\javax.comm.properties to C:\Program Files\Java\jdk1.6.0_06\jre\lib

5. Go to Environment Variable and add the Java\jdk....\bin to 'path'

C:\Program Files\Java\jdk1.6.0_06\bin

TESTING

The Comm API also comes with a number of samples that can be used to confirm the Comm API has been installed correctly.

One of these samples is called BlackBox.

To use Blackbox add BlackBox.jar to the CLASSPATH in Environment Variables

C:\commapi\samples\BlackBox\BlackBox.jar

To run BlackBox, open a command prompt and go to C:\commapi\samples\BlackBox. Then enter 'java BlackBox'

C:\commapi\samples\BlackBox>java BlackBox

Appendix C Active Directory/LDAP Groups and Attributes

Using Active Directory groups to specify how users are managed is a quick and flexible way to manage PINsafe users. You can create a set of groups in such a way that different user groups have a range of different user experiences and rights within PINsafe, or if you have a very simple PINsafe installation you can use just two or three different groups to very simply manage your PINsafe users.

Note that although this section refers consistently to Active Directory, all comments apply also to repositories configured as Simple LDAP. Note also that the groups defined within PINsafe (as of version 3.3) can refer to a single group within each of the defined repositories, or can refer to a single repository only.

The considerations that should be taken into account when planning integration with Active Directory are:

What authentication modes are to be used and whether all users are going to be able to use all methods

- Dual Channel
- Single Channel
- A mixture of the two

What delivery method is to be used for alerts (e.g. account creation) and dual channel authentication, and are all users going to use the same method.

How is the user PIN to be created?

Have all the Active Directory accounts been fully populated with information, e.g. Mobile phone numbers (without +, e.g. 4412345678), Email addresses

Plan your Active Directory Groups. Ideally, by using a hierarchy of groups, users should be able to be assigned a member to one group to give all the requirements for PINsafe.

User rights

The following standard rights are defined on the PINsafe server. Each group can be assigned any combination of these rights.

Admin	Members of groups with this right can configure PINsafe
Helpdesk	Members of groups with this right can manage users, e.g. reset PINs, passwords etc. Users with the Admin right automatically also have this right.
Single	Members of groups with this right can authenticate via the single channel (TURING image) interface.
Dual	Members of groups with this right can authenticate using dual channel authentication, e.g. using SMS messages
Swivlet	Members of groups with this right can authenticate using the PINsafe mobile client.
PINless	Members of groups with this right will be PINless. They

PINsafe Manual
will use one-time passcodes rather than security strings
and one-time codes.

In addition groups will need to be defined for the transports that users are going to use, the agents via which the users will be allowed to authenticate, which RADIUS NAS can be used to authenticate, and the use of third party authentication methods.

Simple AD Group and Attribute example

A simple PINsafe installation may be where TURING image authentication is being used to authenticate a VPN. All users will be single channel users. All users will be sent alerts via e-mail. All users will authenticate via the same NAS. The same group of users will configure and operate PINsafe so there is no requirement for separate helpdesk/admin roles. All users will be PINless.

These requirements can be met by creating a simple set of two groups.

Group name	Example Active Directory definition
PINsafeUsers	CN=PINSafeUsers, OU=pinsafe, DC=example, DC=com
PINsafeAdministrators	CN=PINsafeAdministrators, OU=pinsafe, DC=example, DC=com

The PINsafeUsers group will be given the Single right, allowing them to authenticate using single channel. They will also be given the PINless right. The PINsafeAdministrators group will be given the Admin right. Since this also includes HelpDesk rights, there is no need to tick both.

Authentication for the PINsafeAdministrators group can be handled in one of two ways: either the PINsafeAdminstrators group is itself a member of the PINsafe users group within Active Directory, in which case they automatically get the Single and PINless rights, or else the group can be explicitly given these rights.

The Repository -> Groups screen will look as shown below (this example assumes the administrators group is a sub-group of the users group):

	Single	Dual	Swivlet	Admin	Helpdesk	PINless
Name: <input type="text" value="PINsafeUsers"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions:	<input type="button" value="Delete"/>					
ith000140: <input type="text" value="PINsafeUsers"/>						
AD: <input type="text" value="CN=PINSafeUsers, OU=pinsafe, DC=example, DC=c"/>						
Name: <input type="text" value="PINsafeAdministrators"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Definitions:	<input type="button" value="Delete"/>					
ith000140: <input type="text" value="PINsafeAdministrators"/>						
AD: <input type="text" value="CN=PINsafeAdministrators, OU=pinsafe, DC=examp"/>						

Figure 46.Simple repository groups example

On the Transport->General screen the email (SMTP) transport will be configured as follows:

The screenshot shows a configuration form for an SMTP transport. The fields are as follows:

Identifier:	SMTP
Class:	com.swiveltechnologies.pinsafe.transport.SmtTra
Strings per message:	1
Destination attribute:	mail
Repository group:	---NONE---
Alert repository group:	PINsafeUsers

Figure 47.Simple repository groups example – transport page

On the RADIUS > NAS screen, a single NAS will need to be defined, as follows:

The screenshot shows a configuration form for a single NAS. The fields are as follows:

NAS: Identifier:	NAS1
Hostname/IP:	192.168.0.111
Secret:	•••••
EAP protocol:	None
Group:	PINsafeUsers

Figure 48.Simple repository groups example – RADIUS NAS page

With this set up, to add a normal user to PINsafe you just need to add them to the PINsafeUsers group and synchronize. To create an Administrator, add a user to the PINsafeAdministrators group and synchronize.

NOTE: When multiple PINsafe servers are using the same repository it is very important that either the group definitions are the same for both PINsafe servers, or if the servers are sharing the same database, that the repository is only defined on one of the PINsafe servers. Users will still be able to authenticate on the other server.

More Complex AD Group and Attribute example

In this example it is assumed that PINsafe is being to authenticate a number of different users groups in a number of different methods.

In this case PINsafe is being used to authenticate access a website and a VPN. All users can use the VPN but only a subset of users can authenticate to the websites.

All users can use single channel authentication; some users can use dual-channel (SMS) authentication

Dual channel users will be sent alerts to their mobile phone, single channel users via email.

PINsafe Administrators are dual channel users but Helpdesk users are single channel only.

This is a group structure that can support these requirements:

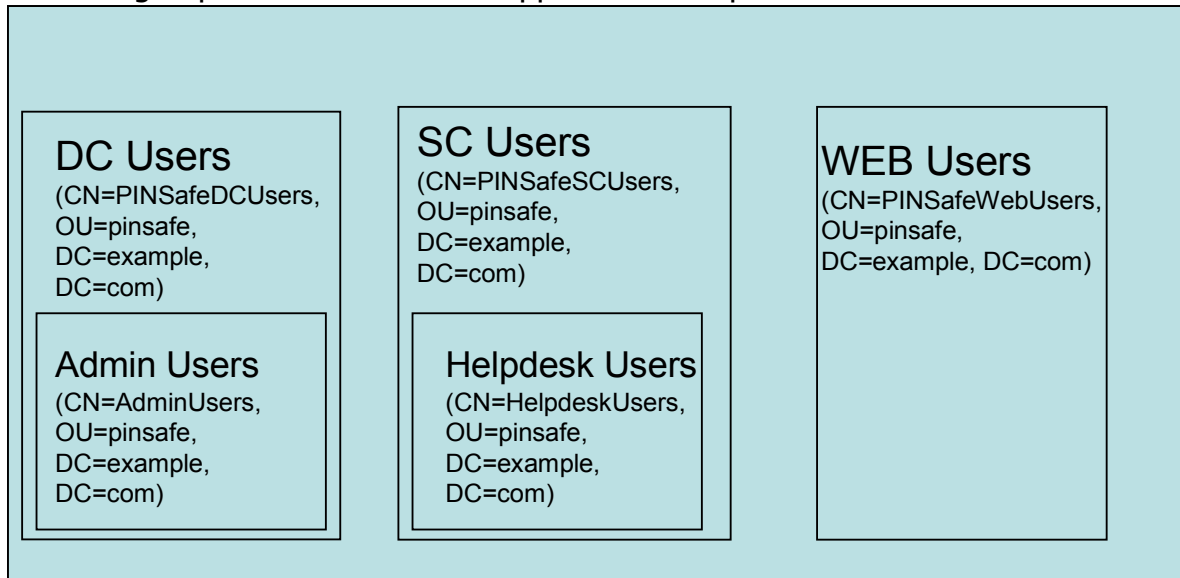


Figure 49. More complex repository groups example – AD structure

(If you are familiar with earlier versions of PINsafe, note that in 3.3, there is no need to define a group that encloses all of the groups above).

The single channel group (SC Users) is the group which contains users that can only authenticate via single channel. In other words, SC Users and DC Users are distinct: no users are members of both of these groups, but all users must be members of one of these two groups.

The Admin users group can be a member of the dual-channel (DC) users group and the Helpdesk group can be a member of the SC Users group.

A separate group for those users that can authenticate to the website also needs to be created. This may contain members of both DC Users and SC Users.

With this group structure in place the PINsafe server would use these groups in the following ways. On the repository -> groups page there would be the following settings

PINsafe Manual

	Single	Dual	Swivlet	Admin	Helpdesk	PINless
Name: <input type="text" value="DC Users"/> Definitions: ith000140: <input type="text" value="DC Users"/> AD: <input type="text" value="CN=PINSafeDCUsers, OU=pinsafe, DC=example, DC="/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
						<input type="button" value="Delete"/>
Name: <input type="text" value="Admin Users"/> Definitions: ith000140: <input type="text" value="Admin Users"/> AD: <input type="text" value="CN=AdminUsers, OU=pinsafe, DC=example, DC=cor"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
						<input type="button" value="Delete"/>
Name: <input type="text" value="SC Users"/> Definitions: ith000140: <input type="text" value="SC Users"/> AD: <input type="text" value="CN=PINSafeSCUsers, OU=pinsafe, DC=example, DC="/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
						<input type="button" value="Delete"/>
Name: <input type="text" value="HelpDesk Users"/> Definitions: ith000140: <input type="text" value="HelpDesk Users"/> AD: <input type="text" value="CN=HelpdeskUsers, OU=pinsafe, DC=example, DC="/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
						<input type="button" value="Delete"/>
Name: <input type="text" value="WEB Users"/> Definitions: ith000140: <input type="text" value="WEB Users"/> AD: <input type="text" value="CN=PINSafeWebUsers, OU=pinsafe, DC=example, DC="/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 50. More complex repository groups example – group definitions

Note that the WEB Users group does not have any rights defined on this page. It must be defined here, though, so that it can be used on other pages.

So that single channel users will have alerts, including on account creation, e-mailed to them, and dual channel users will have alerts sent to them via SMS, the Transport > General screen would include the following entries:

for SMTP:

Destination attribute	Mail
Repository Group	NONE
Alert Repository Group	SC Users

for a GSM Modem (or SMS provider):

Destination attribute	telephoneNumber
Repository Group	DC Users
Alert Repository Group	DC Users

To restrict website access to only those users that are in the WEB users group, the agent associated with the website would include the following entry.

Group	WEB Users
-------	-----------

Despite the variety of user-types, users can, for the most part, be added to PINsafe just by making them a member of the appropriate AD group. The only exception is that users that need to be able to access via the website need to be added to the WEB Users group as well as either the Single Channel or Dual Channel group.

Appendix D PINsafe Installation details.

General

Date of Install
Installation company name
Engineer's name
Customer Contact (inc email/phone)

PINsafe Server Details

Appliance	Yes/No
Appliance serial number(s)	
High Availability	Yes/No
License Installed	Yes/No
PINsafe version	
OS	
IP Address	
Default gateway	
DNS	
Language	English
RADIUS	Yes/No
Change PIN	Yes/No
User self reset.	Yes/No
PINsafe Backup details	

Support Arrangements

Hardware

OS

Software

Customer Sign-off

The installation has been completed to my satisfaction in accordance with the details given above.
I understand the level of support I am entitled to as explained above.

Signature _____

Date: _____

Name _____

on Behalf of (company)

Appendix E Setting Schedules and CRON Strings

With the exception of the session clean up setting, tasks can be scheduled using a *cron* syntax. Most schedules can be set up by using the drop-down menu items on the synchronisation setting screen.

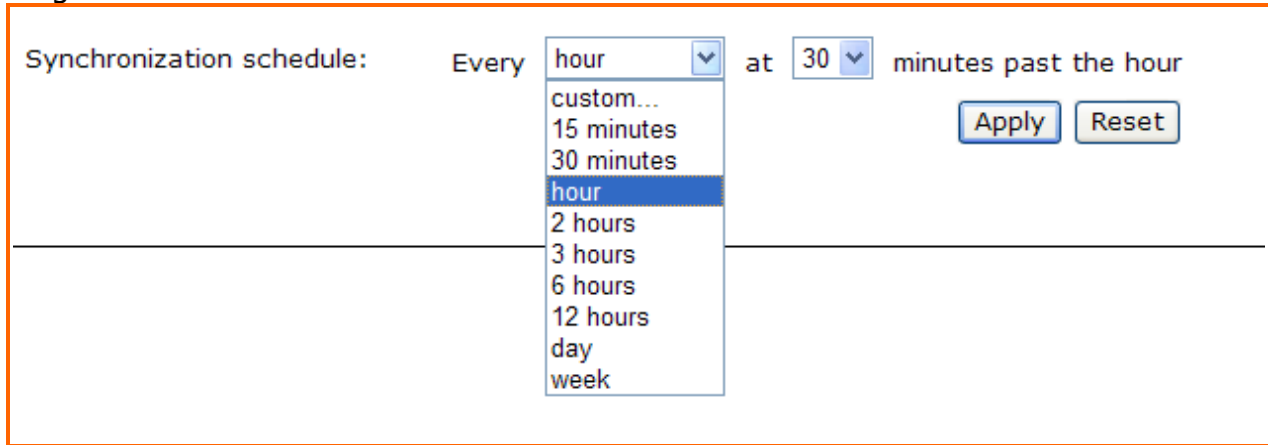


Figure 51. Selecting Schedules

If you select the custom option you can explicitly set the schedule using the *cron* syntax.

The use of the cron-like syntax gives a great deal of flexibility in scheduling these tasks. The settings require the following fields:

Field Name	Allowed Values	Allowed Special Characters
Seconds	0-59	, - * /
Minutes	0-59	, - * /
Hours	0-23	, - * /
Day-of-month	1-31	, - * ? / L W C
Month	1-12 or JAN-DEC	, - * /
Day-of-Week	1-7 SUN-SAT	- * ? / L C #
Year (Optional)	empty, 1970-2099	, - * /

These fields determine when the job is to be run. An asterisk (*) in any field is a wildcard and means that the task will be run for all values of that field. A question-mark (?) means that the setting is not specified, this setting is applied to either the day-of-month and day-of-week as you cannot specify both of these parameters.

Therefore to schedule a job to run every hour, on the hour the settings would be

0 0 * * * ?

Whereas to run a job 3 AM every Sunday would be

0 0 3 ? * 1

INDEX

Active DIrectory.....	SMTP.....	57
Examples.....	Peering.....	47
85	Configuration.....	48
Agents.....	RADIUS.....	38
groups.....	LEAP.....	40
33	ranges.xml.....	81
change PIN.....	Repository.....	
33	XML.....	8
Clickatell.....	support.....	5, 78
30	SysTray Utility.....	43
custom attribute.....	Upgrade.....	
38	from 3.1.....	77
disaster recovery.....	User Repository.....	
53	Active Directory.....	17
EAP-MD5.....	Integration.....	28
40	VPN.....	
filter.....	Integration.....	45
activating.....		
82		
filter.properties.....		
80		
Global Catalogue.....		
20		
IIS.....		
Configuring with PINsafe.....		
37		
iTagg.....		
30		
JRE.....		
78		
Logging.....		

PINsafe Manual

Document Version

- 3.1.4.1 18th October 2006
- 3.1.4.2 19th October 2006, RADIUS and IP table advice added.
- 3.2 31st Jan 2007, Manual for PINsafe version 3.2
- 3.3 12th July 2007, Manual for PINsafe version 3.3
- 3.3 Update 1 19th Nov 2007, 3.3 Update 1
- 3.4 28th April 2008, Manual for PINsafe Version 3.4
- 3.5 20th October 2009, Manual for Version 3.5
- 3.6 9th Jun 2009, For Version 3.6
- 3.6.1 Minor amendments for Version 3.6.1
- 3.7 Updates for Version 3.7. January 2010