

# PINsafe Appliance Active/Active Installation Guide

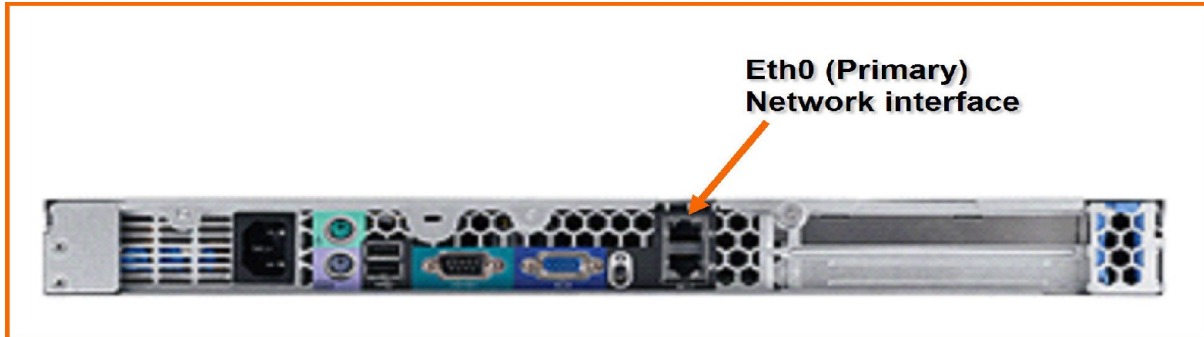
## Contents

Introduction.....	3
Configuration.....	4
Connection.....	4
Network (Primary Appliance).....	4
Services.....	4
PINsafe – Testing (1).....	5
Network (Standby Appliance) .....	5
Database Replication (Primary Appliance).....	5
PINsafe – Testing (2).....	6
Virtual IP.....	6
Virtual IP – Cont.....	7
PINsafe – Testing (3).....	8

## Introduction

This document provides a quick start guide for the PINsafe Active/Active appliance. It covers issues related specifically to the PINsafe appliance as supplied by Swivel Secure rather than the software configuration of PINsafe. This is covered by the PINsafe User Manual.

The appliance has two network interfaces. The primary interface is eth0, labelled **1** on the back panel.



The recommended way to configure the appliance is to use the pre-installed console application (CMI), in combination with the graphical admin tool Webmin. The CMI is useful for diagnostic issues, initial installation and any reconfiguration task.

The default IP addresses for the HA pair are 192.168.0.36 for the primary and 192.168.0.37 for the standby. Whilst both appliances are always active, for the purpose of this document we will refer to one appliance as Primary, and the other as Standby. This is merely a naming convention, and does not necessarily reflect their mode of operation.

With an Active/Active scenario both appliances will require configuring separately. The same process and steps should be followed for each appliance.

# Configuration

## Connection

The appliance may be configured using the console, or via ssh (port 22) over network connection. To configure the appliance using a network connection, connect the primary interface (labelled 1) to either a PC via a cross-over cable or to a switch/hub. If connecting directly to an existing network ensure that the default IPs on the appliance will not conflict with an existing network device.

## Network (Primary Appliance)

To change the IP addresses on the appliance the following information will be required:

Description	Default IP	New IP
IP Address	192.168.0.36	
Network Address	192.168.0.0	
Broadcast Address	192.168.0.255	
Default Gateway	192.168.0.1	
Other appliance in the HA Pair	192.168.0.37	
Virtual IP (if required)	192.168.0.38	

To change the IP address of the appliance:

- Login to the appliance locally or via ssh, as user **'admin'**, and use the default password.
- The Console Management Interface (CMI) application will automatically start.
- On the entry screen, check the status of the MySQL and Tomcat services, they must be stopped before you can change the IP address. To stop a service select the menu item associated with that service then select the stop option.
- Select 'Advanced Options ->Change IPs and Routing -> Change Appliance IPs'.
- Follow the on screen prompts, all information is required, and then confirm the changes.
- Reboot the appliance (Advanced Options -> Admin ->Reboot appliance)
- Connect to the appliance (remembering to change the settings on your ssh client as required) and check the new settings using the CMI application.
- Exit the CMI application.

## Services

The appliance shipped by Swivel Secure, by default, will automatically start MySQL and Tomcat. Based upon the installation type additional services and applications will need to be configured if required.

## PINsafe – Testing (1)

- Navigate to the PINsafe admin page on the Primary appliance. By default this will be on <https://192.168.0.36:8080/pinsafe>, however if the IP address has been changed navigate to the new IP address. Always use HTTPS in the browser.
- Use the Admin account, and click 'Start Session'. A Turing image should be displayed.

SWIVEL<sup>®</sup>  
AUTHENTICATION YOU CAN IDENTIFY WITH

PINsafe

default

• [Login](#)

### PINsafe Administration Login

Username:

Password:

OTC:

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

- Use the default PIN of '1234' and login.
- Configure PINsafe. For additional help configuring PINsafe refer to the 'PINsafe User Manual'.

## Network (Standby Appliance)

- Configure the Standby appliance, by following the processes outlined for the Primary appliance, with the following changes:
  - Use <https://192.168.0.37:10000>, for the default Webmin GUI URL
  - Use <https://192.168.0.37:8080/pinsafe>, for the default PINsafe URL.

## Database Replication (Primary Appliance)

- Use an SSH client, or the appliance console and connect to the appliance.
- Login to the appliance as user '**admin**', and use the default password.
- Select 'MySQL -> Status of Master/Slave'.
- Check the DB pointers and log files on the Primary Master match those on the Standby Slave and that the DB pointers and log files on the Standby Master match those on the Primary Slave. If they do not match, or more help is required, then use the guide '[How to Synchronise DB pointers](#)' to resolve the problem.
- The DB pointers and log files must be synchronised before continuing.

## PINsafe – Testing (2)

- On the primary appliance use the PINsafe administration pages to:
  - Configure a MySQL DB using the default settings unless you have change them, as shown below. (The password being pinsafe).

Identifier:	<input type="text" value="MySQL 5"/>
Class:	<input type="text" value="com.swiveltechnologies.pinsafe.user.database.MySQL5Database"/>
Driver:	<input type="text" value="com.mysql.jdbc.Driver"/>
URL:	<input type="text" value="jdbc:mysql://localhost/pinsafe_rep"/>
Username:	<input type="text" value="pinsafe"/>
Password:	<input type="password" value="••••••"/>

- Create an XML repository
- Change the Mode to 'Synchronised'
- Create a user on the primary appliance.
- On the standby appliance login to the administration pages and check that the repository and user created on the primary appliance has been created on the standby appliance.
- Delete the user using the standby appliance.
- On the primary appliance login to the administration pages and check that the user has been deleted.

## Virtual IP

If a virtual IP is required then on the Primary appliance then the heartbeat service needs to be started.

- Use an SSH client, or the appliance console and connect to the appliance.
- Login to the appliance as user '**admin**', and use the default password.
- Select 'Heartbeat -> Start'. (Wait for a few minutes for the IP to be allocated).
- Select 'Heartbeat -> Status' and check that the IP address is active on the Primary appliance.

```
Swivel Maintenance : Heartbeat

Status of Heartbeat and the Virtual IP on the Local & Remote host

192.168.0.36
Heartbeat running
Virtual IP: 192.168.0.38
Virtual IP Active

192.168.0.37
Heartbeat running
```

- Ping the Virtual IP address from any device on the same network, and ensure it responds.
- Navigate to the Webmin admin console. By default this will be <https://192.168.0.36:10000>, however if the IP address has been changed navigate to the new IP address. Always use HTTPS in the browser.
- Select menus: 'Servers -> PINsafe'.
- Click on the button 'Edit ChangePIN Config File'

## Virtual IP – Cont

### Editing file

`/usr/local/apache-tomcat-5.5.20/webapps2/changeip/WEB-INF/settings.xml`

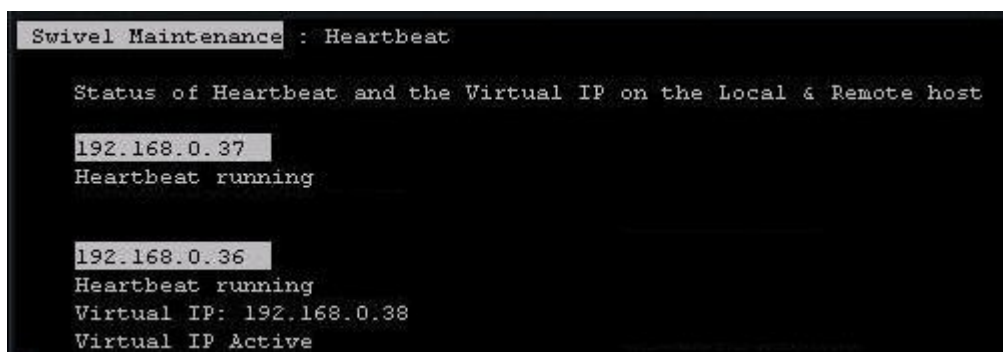
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="ssl">>false</entry>
<entry key="server">localhost</entry>
<entry key="port">8181</entry>
<entry key="context">pinsafe</entry>
<entry key="imagecontext">proxy</entry>
<entry key="imageserver">192.168.0.38</entry>
<entry key="imageport">8443</entry>
<entry key="imagesssl">>true</entry>
<entry key="secret">secret</entry>
<entry key="explicit">>false</entry>
<entry key="redirect">http://www.google.co.uk</entry>
</properties>
```

Save

- Change the imageserver IP address to be the Virtual IP specified previously, and save the file.

On the Standby appliance:

- Use an SSH client, or the appliance console and connect to the appliance.
- Login to the appliance as user '**admin**', and use the default password.
- Select 'Heartbeat -> Start'
- Select 'Heartbeat -> Status' and check that the IP address is active on the Primary appliance.



```
Swivel Maintenance : Heartbeat

Status of Heartbeat and the Virtual IP on the Local & Remote host

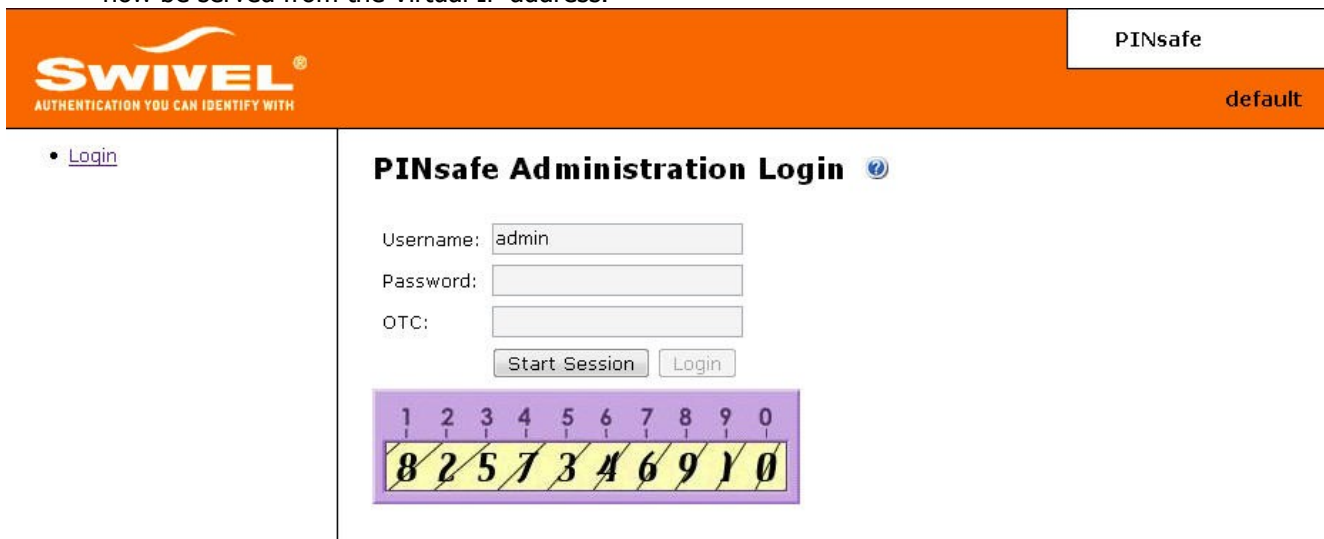
192.168.0.37
Heartbeat running

192.168.0.36
Heartbeat running
Virtual IP: 192.168.0.38
Virtual IP Active
```

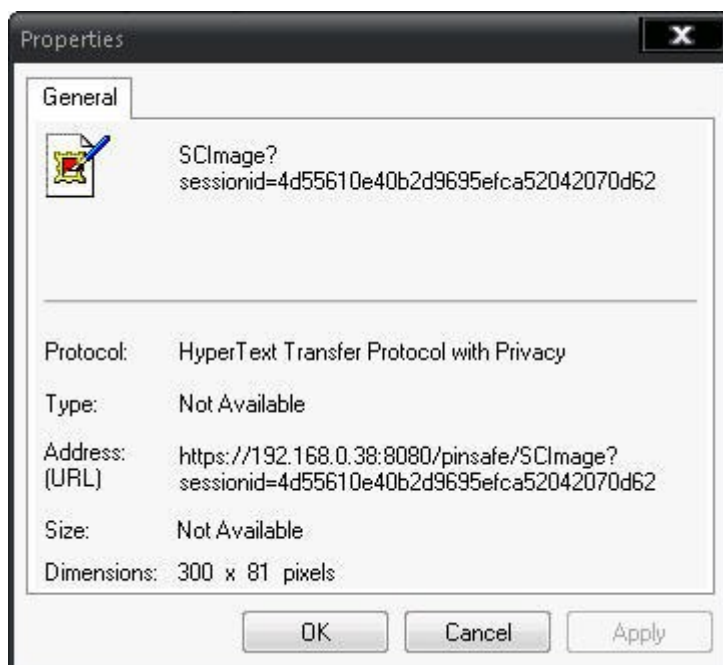
- Navigate to the Webmin admin console. By default this will be <https://192.168.0.37:10000>, however if the IP address has been changed navigate to the new IP address. Always use HTTPS in the browser.
- Click on the button 'Edit Changepin Config File'
- Change the IP address to be the virtual IP specified previously. Save the file.

## PINsafe – Testing (3)

- Navigate to the PINsafe admin page on using the Virtual IP. By default this will be on <https://192.168.0.38:8080/pinsafe>, however if the IP address has been changed navigate to the new IP address. Always use HTTPS in the browser.
- Use the Admin account, and click 'Start Session'. A Turing image should be displayed. This image should now be served from the Virtual IP address.



- Using the Admin PIN log in.
- Confirm the 'Server Address' on the Status page matches the Virtual IP address.
- Connect to primary appliance on <https://192.168.0.36:8080/pinsafe>, however if the IP address has been changed navigate to the new IP address. Always use HTTPS in the browser.
- Use the Admin account, and click 'Start Session'. A Turing image should be displayed. Right click on the image and select 'Properties'. Check that the image source matches the Virtual IP address.



- Connect to primary appliance on <https://192.168.0.37:8080/pinsafe>, however if the IP address has been changed navigate to the new IP address. Always use HTTPS in the browser.
- Use the Admin account, and click 'Start Session'. A Turing image should be displayed. Right click on the image and select 'Properties'. Check that the image source matches the Virtual IP address.



