Swivel Appliance User Guide Version 2.0.14

Last Revision January 2012

Contents

Introduction

This document provides a quick start guide for the Swivel Appliance. It covers issues related specifically to the Swivel Appliance as supplied by Swivel rather than the software configuration of Swivel. This is covered by the Swivel Reference Manual.

The appliance has two network interfaces. The primary interface is eth0, labelled Gb[1] on the back panel (circled in red below)

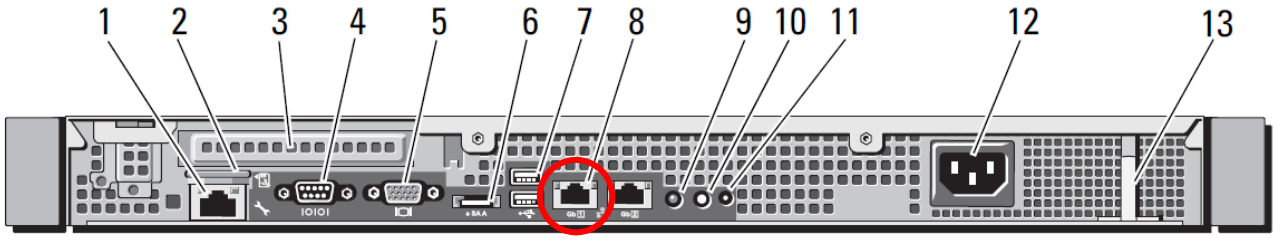


Figure 1. Rear Panel (taken from DELL manual)

The recommended approach for configuring the Swivel Appliance is to use the Console Maintenance Interface (CMI). After the configuration has been applied there is graphical tool (Webmin) which may be used to view the configuration and settings via a web browser.

The default IP address for the machine is 192.168.0.35 for a standalone appliance and 192.168.0.36 and .37 for the primary and standby servers of a HA pair.

These may be changed as part of the pre-installation or installation.

What is on the Appliance?

The Swivel Appliance includes the Swivel application and all the associated software required for it to operate. In addition it includes the High Availability (HA) packages required for your chosen HA solution (if applicable).

The appliance includes the following additional applications:

- Change PIN Allows users to set their own PINs
- Reset PIN Allows users to request a new PIN should they forget their PIN
- Proxy A proxy application that allows access to the Swivel Admin Console to be isolated from other network traffic.

The Swivel Appliance comes with a pre-installed self-signed certificate allowing Swivel to operate over encrypted https connections.

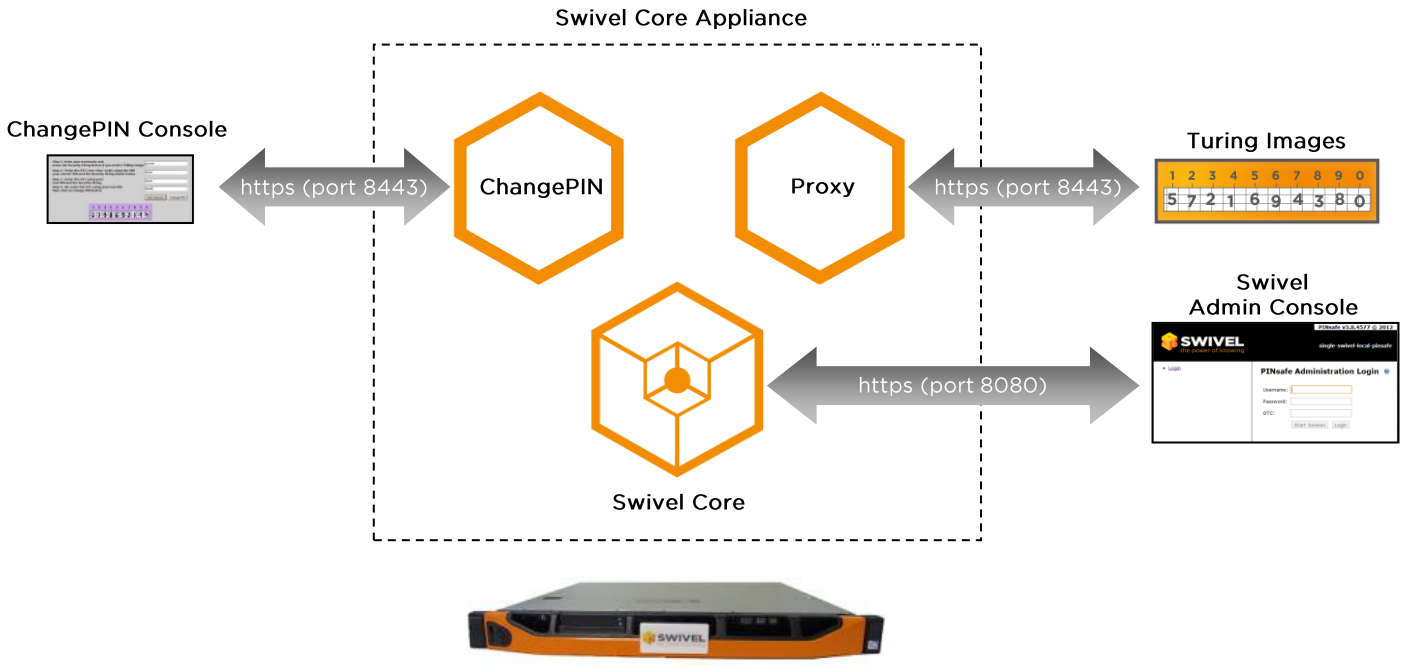


Figure 2. Swivel Appliance Applications

All external requests into the Swivel can be routed via port 8443 and via the Proxy. The internal traffic, i.e. the Swivel Admin Console, is served on port 8080. Port 8181 is used for communication between the Swivel and the other bundled applications. Port 8181 is only available to applications hosted on the appliance.

Assuming a default IP address of 192.168.0.36, the default URL mapping for a Swivel Appliance is as follows:

https://192.168.0.36:8080/pinsafe	Swivel Admin Console
https://192.168.0.36:8080/pinsafe/AgentXML	Agent-XML direct access
https://192.168.0.36:8443/proxy/AgentXML	Security strings access for Midlet
https://192.168.0.36:8080/pinsafe/SCImage	Direct image Servlet
https://192.168.0.36:8443/changepin	ChangePIN application
https://192.168.0.36:8443/resetpin	Reset pin application
https://192.168.0.36:8443/proxy/SCImage	Image request via proxy
https://192.168.0.36:10000	Appliance Administration (Webmin)

In addition to the Swivel software and ancillary applications there are two administration interfaces on the Appliance. These interfaces are used for installation and maintenance of the Swivel Appliance.

These two interfaces are:

Console Management Interface (CMI)

This is a text-based interface that can be accessed locally of via SSH. It is accessed by logging-on as the *admin* user. It provides access to the main appliance settings, eg IP addresses. It also allows appliances to be backed-up and restored. This interface will primarily be used by engineers installing a Swivel Appliance.

Webmin

Webmin provides a web-based graphical interface for viewing the status of a Swivel Appliance. It also allows for some configuration by allow the editing of a range of text-based configuration files and the changing of firewall rules.

Console Management Interface

The following steps are required to configure the appliance for the local network infrastructure using the Console Management Interface (CMI).

Getting Started

Too access the CMI log onto the appliance either locally or via an SSH session (port 22) using the account name **admin** and the password **lockbox.**

The appliance comes with a default **admin** account. This accounts has the default password **lockbox**. Using the console screen or an SSH client login as **admin**.

The appliance will then run the CMI. You can change the password for the **admin** account, using menu options 'Advanced Menu -> Admin Menu -> Change admin password'

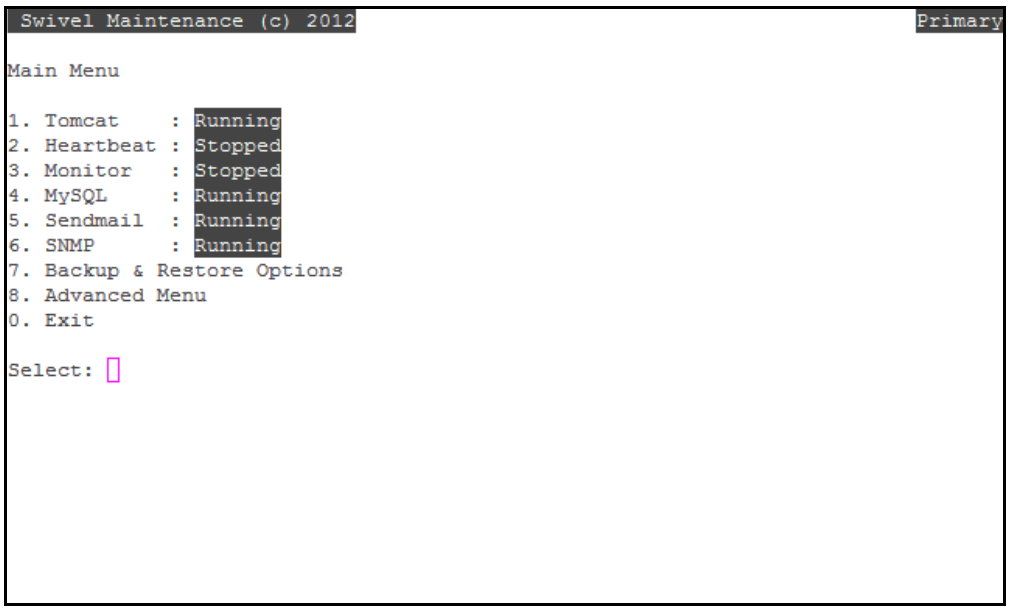


Figure 3. CMI status screen

Once you have accessed the CMI, the first task you may need to perform is to change the IP address. There are a number of IP addresses that need configuring on a Swivel Appliance installation, but setting of the physical address of the appliance will probably be the first.

To change this address, you first need to stop the Tomcat and MySQL services. The top-level screen shows the status of these services.

Figure 4. Tomcat status screen

To stop a service select it (e.g. by pressing "1" for Tomcat). Then select the stop option.

Once these services are stopped you can navigate to the change IP address option from the status screen by selecting:

Advanced Menu -> Networking -> IPs & Routing -> Change Appliance IPs.

If you have not stopped Tomcat, you may be prompted to do so at this point.

On this screen you can enter the new appliance IP addresses. You can also set the standby and virtual ip addresses at this stage if you wish (if you have a HA pair). **Note: Pressing return without entering a value leaves the settings unchanged.**

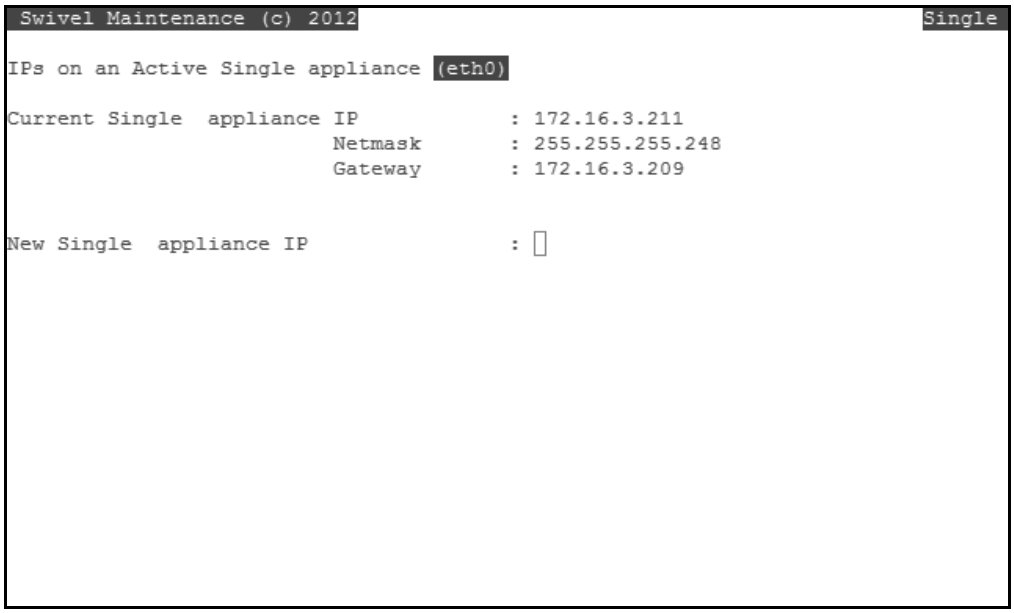


Figure 5. Changing the Appliance IP Address(es)

Overview

The CMI has the following standard functionality:

Tomcat	Start, Stop and Restart for the Tomcat service
Heartbeat	Start, Stop and Status for the Heartbeat service
Monitor	Start and Stop for the Monitor service
MySQL (A/A or DR)	Control MySQL DB
DRBD (A/P only)	Start, Stop and Status for the DRBD service
Sendmail	Start, Stop and Status for the Sendmail service
SNMP	Start, Stop and Status for the SNMP service
Backup & Restore Options	Backup and restore options for Swivel and the appliance
Advanced Options	Maintenance and installation options

Tomcat

The menu allows the service to be started or stopped. An option to restart the service is also available. The CMI will report on the current state of the service as either running or stopped.

Heartbeat

The menu allows the service to be started or stopped. The Status option will report on the service as either running, or stopped. If the service is running and a virtual IP has been configured, it will be displayed along with the IP address of the appliance that is currently in control of the virtual IP.

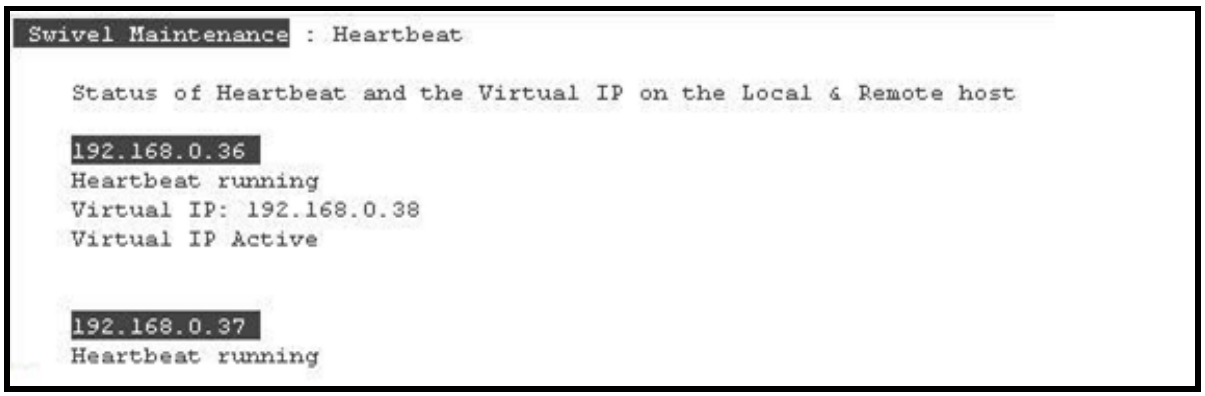


Figure 6. Heartbeat Status Screen

Monitor

The monitor service is used to determine if Tomcat is running on a HA machine. The menu allows the service to be started or stopped. The CMI will report on the current state of the service as either running or stopped. The service should be stopped when performance upgrades etc to prevent an fail-over.

MySQL

The menu allows the service to be started or stopped. The status option will report on the service as

either running, or stopped. When checking on the status of the service both appliances in the HA solution will be queried. In addition it is possible to stop the slave DB which is used as part of the DB replication configuration.

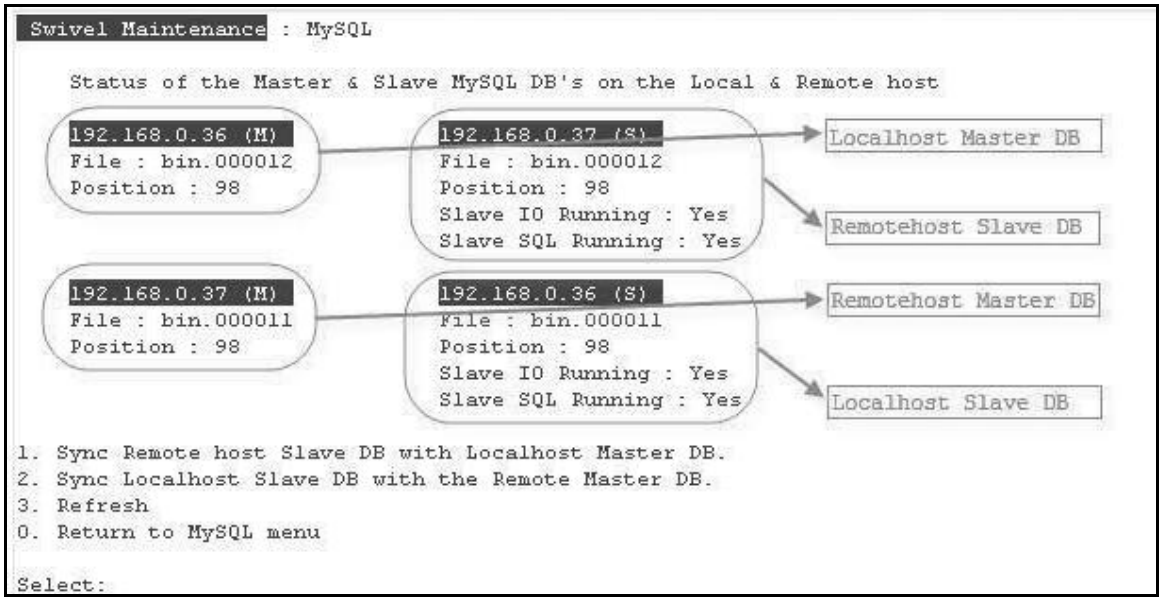


Figure 7. Replication Status Screen

The status check screen enables the user to resolve various issues which may occur with a replicated database HA solution. The screen above shows the status of a healthy HA pair. The Files and positions between the to servers agree and the Slave IO and Slave SQL show as running.

There are menu options available that may correct any anomalies.

Option 1. Sync Remote host Slave DB with Localhost Master DB

Compares the File and Position records on the Slave DB Remote appliance with the File and Position records on the Master DB Local appliance. If they are different this option will resynchronise the pointers and copy data from the Local Master DB to the Remote Slave DB.

Option 2. Sync Localhost Slave DB with Remote Master DB

Compares the File and Position records on the Slave DB Local appliance with the File and Position records on the Master DB Remote appliance. If they are different this option will resynchronise the pointers and copy data from the Remote Master DB to the Local Slave DB.

Option 3. Refresh

Refresh the screen to reflect changes made by the synchronisation options.

The MySQL command Line provides access to the MySQL interface. Caution should be used with this option, and the user should be following direct instruction from Customer Support. Incorrect use of the MySQL interface could cause Swivel to stop authenticating requests.

DRBD

DRBD is the disk replication service used by Active-Passive HA installations.

The menu allows the service to be started or stopped. The status option will report on the service as either running, or stopped. When checking on the status of the service both appliances in the HA solution will be queried.

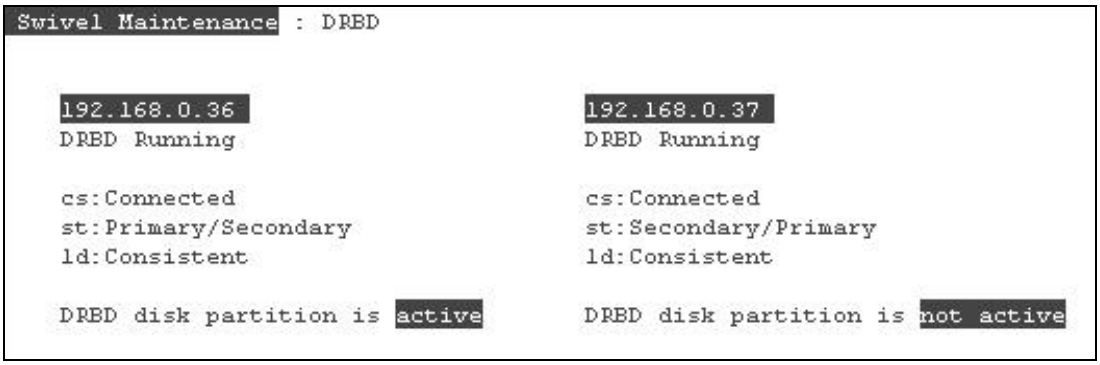


Figure 8. DRBD Status screen showing “healthy” status

The Status screen allows the user to check quickly and easily if the DRBD service is running, the HA pairs are connected and that they are in a Consistent state.

The CMI enables the user to resolve various issues which may occur with a DRBD HA solution.

> Option 1. Synchronise Remote host to Localhost
>
> The CMI automatically evaluates the states of the DRBD service. If the databases are not in a consistent state the option to synchronise them will be offered.

Sendmail

The menu allows the service to be started or stopped. The status option will report on the service as either running, or stopped.

SNMP

The menu allows the service to be started or stopped. The status option will report on the service as either running, or stopped.

Backup & Restore

The CMI features comprehensive backup and restore functions. There are three main backups that may be taken:

- Full backup including appliance configuration and PINsafe (Swivel) application
- Backup PINsafe (Swivel) and PINsafe (Swivel) configuration files
- Backup network configuration files.

Each backup may be restored, using the appropriate menu option or copied to a different Swivel Appliance.

- Backups are automatically purged after a defined period of days. They may also be manually purged if required.
- A bare metal recovery CD may be manually created to help with the restore process.

Advanced Functionality

The CMI has the following advanced functionality:

Menu Item	Description
Version Information	Displays version information relevant for the Swivel Appliance
Default Running Services	Enables services to be automatically started/stopped after a reboot
Change Hostnames	Change an appliance hostname
Change IPs & Routing	Change a network card IP address, and associated routing
Change NIC speeds	Change a network card speed
Change DNS Servers	Change DNS IP address on an appliance
RAID status	Shows the RAID status of the appliance drives and controller
Admin Menu	Options to reboot, or shutdown the appliance. Restart the NICs, and to change various system passwords
Command Line	Provide access to the Linux command line

Version Information

Menu to view the version numbers of the core applications applicable to Swivel. Includes 'open source' software Tomcat, MySQL and Webmin and the versions of Java, Swivel, and the Appliance.

Default Running Services

Menu to check if services (Tomcat, Mon, Heartbeat, DRBD, Sendmail, SNMP & MySQL) will automatically start following a reboot. Functionality controls if a service should start automatically after a reboot.

Change Hostname

Menu to allow the hostname to be changed on an appliance. In an HA pair installation each server must have its own and its partners hostnames configured correctly.

Change IP Address

Includes menu options to view or change the range of IP address settings that apply to the appliance and other appliances within the same installation.

These include:

Appliance Addresses

	Item	Default Value
1.	IP Address	192.168.0.36 (192.168.0.37 for standby appliance)
2.	NetMask	255.255.255.0
3.	Broadcast Address	192.168.0.255
4.	Default Gateway	192.168.0.254
5.	Other appliance in HA pair	192.168.0.37 (192.168.0.36 for standby appliance)
6.	Virtual IP	192.168.0.38

MySQL Addresses

	Item	Default Value	
1.	Primary Replication IP	172.16.0.1	
2.	Network Address	172.16.0.0	
3.	Broadcast Address	172.16.0.255	
4.	Other appliance in HA pair	172.16.0.2	
5.	Disaster Recovery	192.168.0.35	Separate menu

Addresses used for Replication should not normally be changed as the servers are often connected via a crossover cable or VLAN. This option should only be used by experienced users.

Change NIC Speeds

Menu to allow the speed of the network interfaces (NIC) to be changed.

Change DNS Servers

Menu to change the DNS servers used by the appliance. Currently only two DNS servers may be configured.

RAID Status

Menu to view the current status of the RAID drives and controller on the appliance.

Admin Menu

Menu to provide several miscellaneous administration level tasks:

- Reboot or shutdown the appliance.
- Reset the network interfaces.
- Change various system level passwords

Command Line

Menu to allow a user access to the Linux command prompt. The command prompt should only be used by an experienced user following the directions of Swivel or Reseller/Distributor Support.

Users need to enter a password known only to Resellers/Distributors in response to the disclaimer shown after choosing this option.

Webmin Swivel Appliance Configuration

Webmin provides a browser based graphical interface for configuring the Swivel appliance.

Accessing Webmin

Log in to Webmin at its default address of https://<IPaddress>:10000 where the IP address is the address of the Swivel appliance. By default this will be 192.168.0.35 for a stand-alone appliance, and 192.168.0.36 and 192.168.0.37 for an HA pair.

A warning may be shown on the browser about the certificate of the URL not being valid. Ignore the warning and proceed to the website.

The Webmin login page should be displayed.

Figure 9. Webmin Sign-on Page

Enter the username **admin** and the password **lockbox**.

This is the default setting and should be changed. Refer to the changing passwords section.

After a successful login the Webmin status page will be displayed. The status screen presents top level status information for the appliance and a navigation window showing the sections available

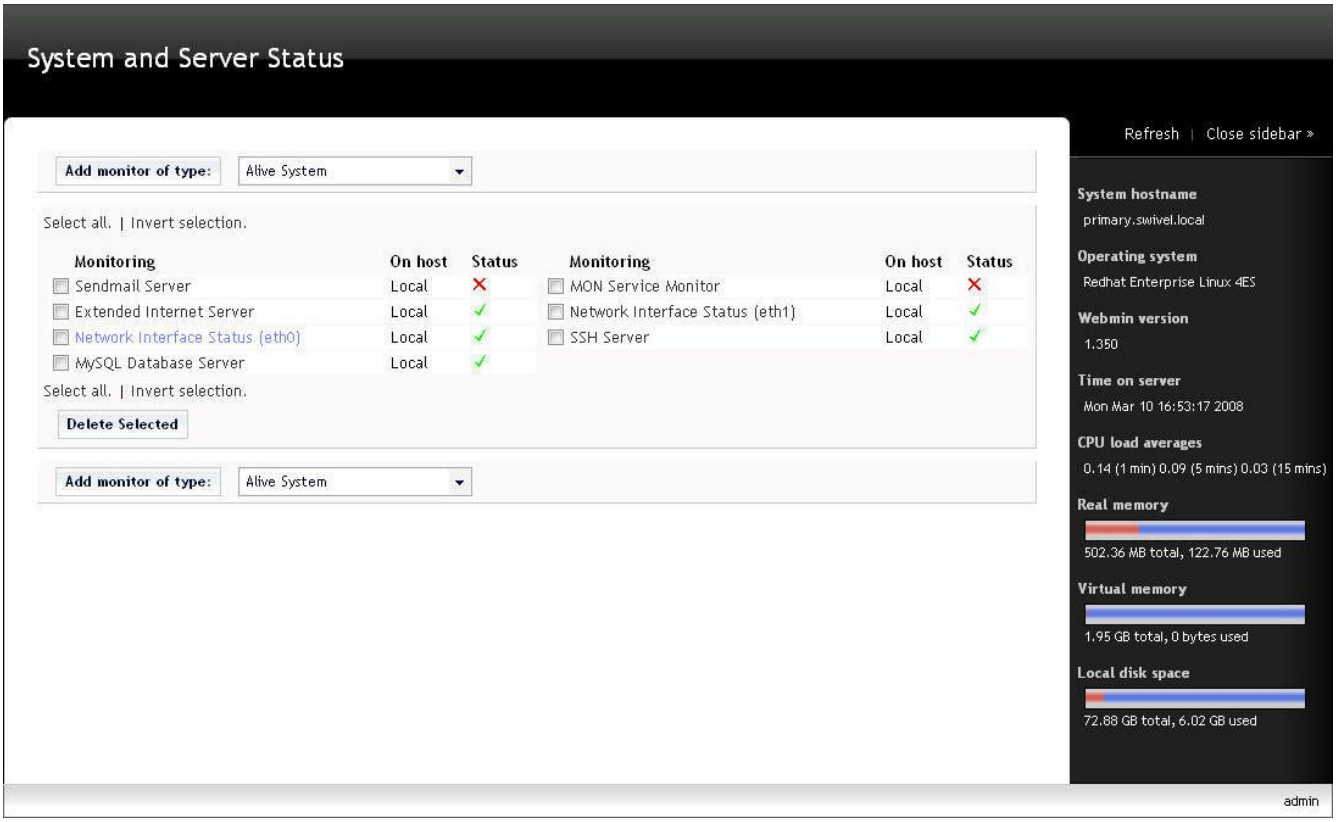


Figure 10. Webmin Status Page

Common Tasks

This section lists the most commonly accessed tasks in the Webmin interface.

Changing the Webmin password for the admin user
There is a default Webmin account called **admin** with a password of **lockbox**. This should be changed. Select the Webmin option in the navigation menu, expanding the options, and select Webmin Users.

Select the **admin** user by clicking on the word **admin**. The management window opens for the account.

To change the password, on the password line select 'Set to' and enter a new value for the account password.

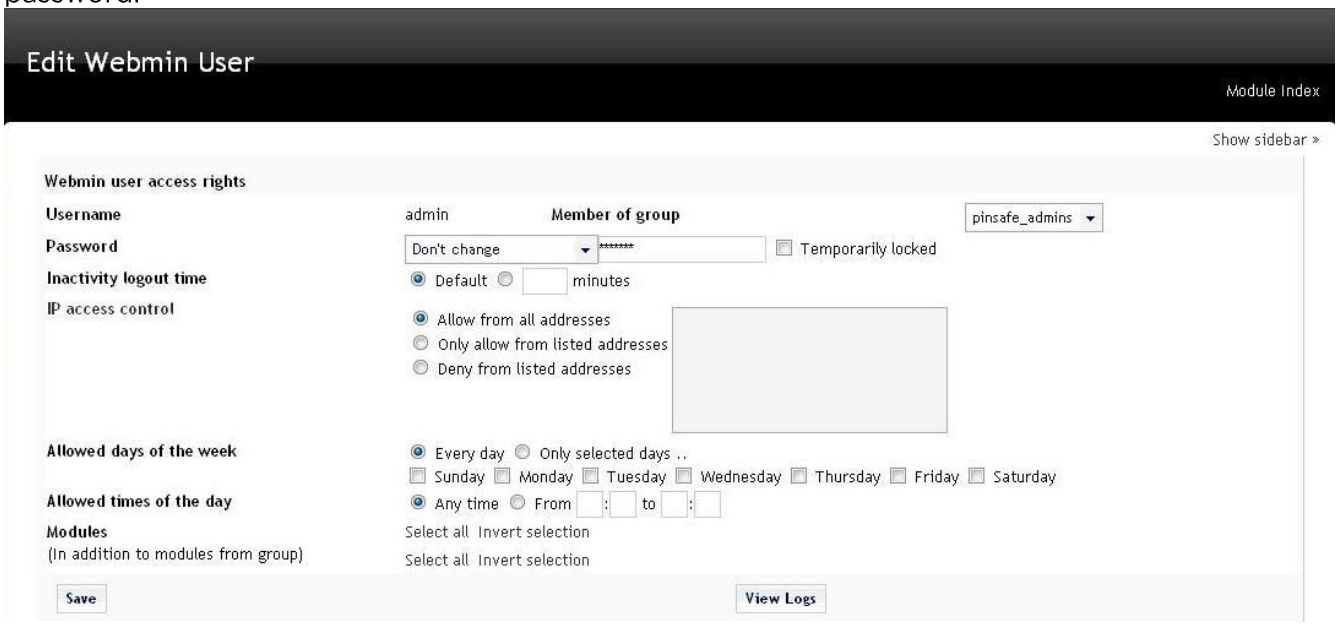


Figure 11. Editing Webmin User

Then select 

The password is now set to the new value.

Other values can be set on this screen to restrict when and from where this account can access Webmin i.e. a list of IP addresses coupled with days of the week and valid access hours.

Nb The Webmin "admin" account is separate for the CMI "admin" account. Changing the password for this account on Webmin will not change it for the CMI admin account and vice versa

Viewing the appliance IP address

This section describes how to view the IP address of the Swivel appliance. If the appliance is part of an HA pair, or a DR solution then the IPs used in the MySQL DB replication will also be visible.

To view an appliance IP address you need to navigate to Networking-> Network Configuration. Select the Network Interface icon

Network Interfaces

This will bring up the Network Interface configuration screen.

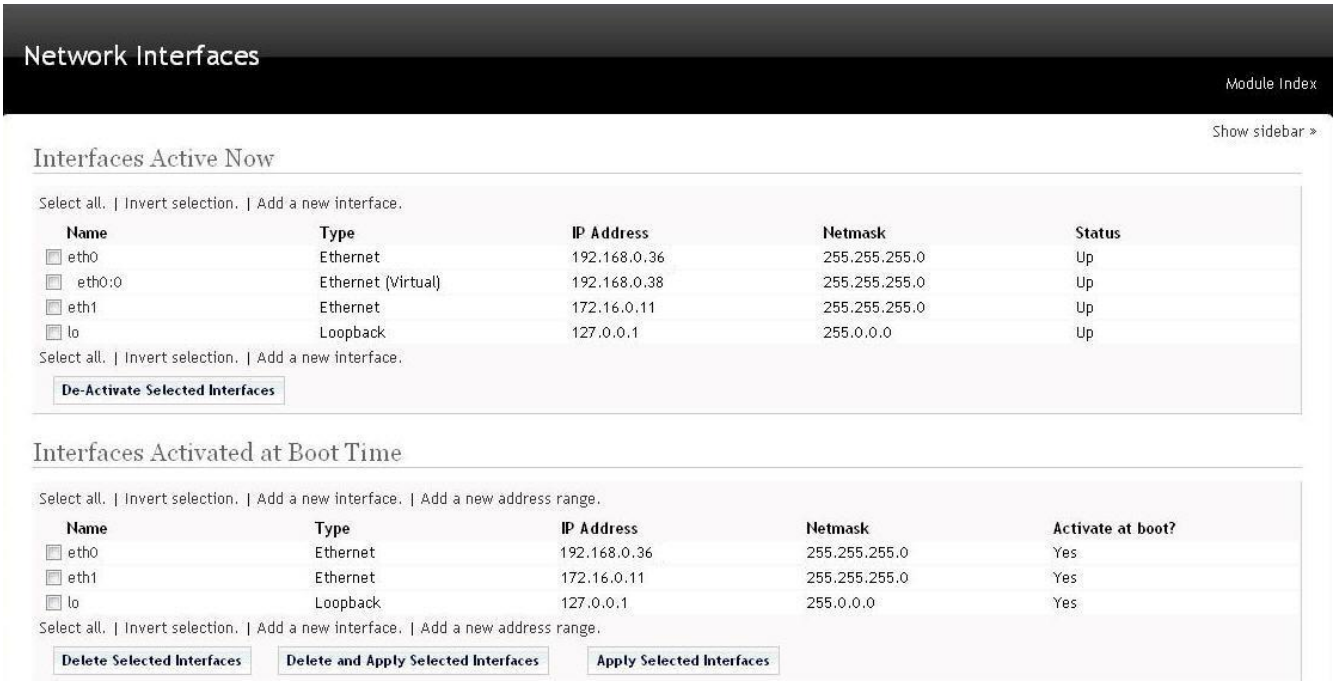


Figure 12. Network Configuration Screen

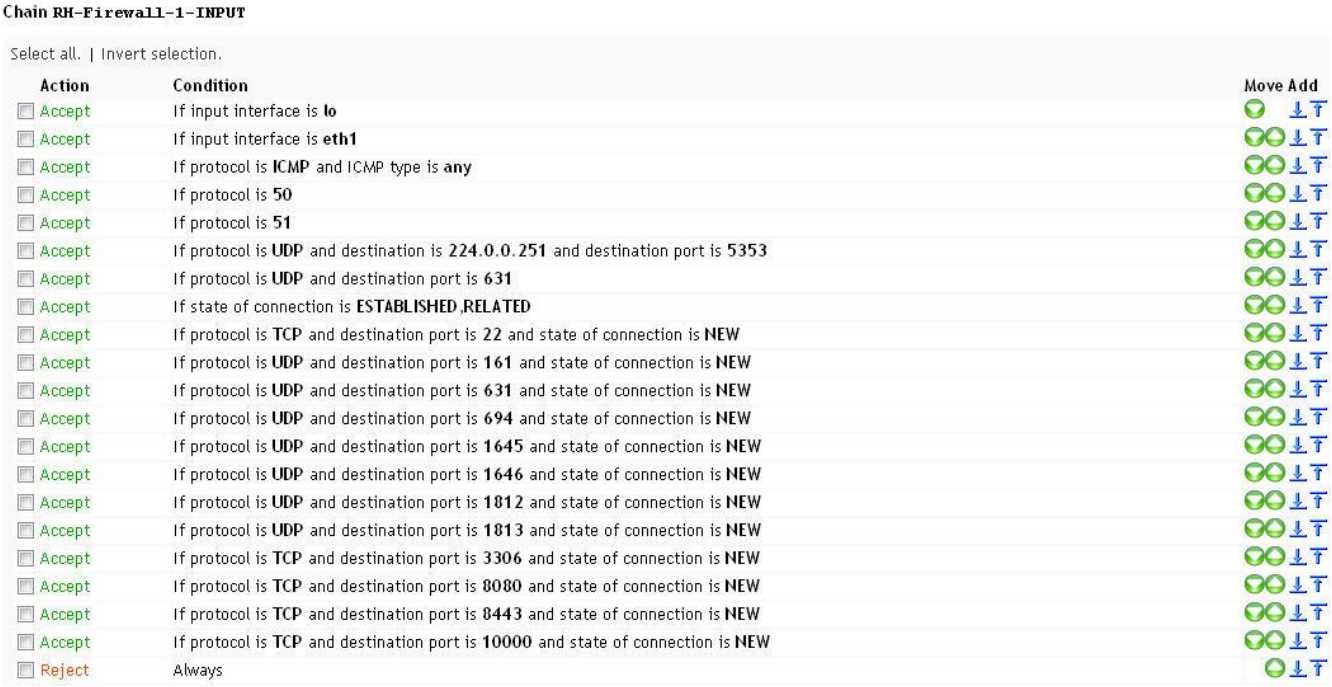
This screen has two sections. The top section displays the IP addresses that the appliance is currently using. The lower section will display the IP addresses the appliance will use following a reboot. These two sections should be the same.

Firewall Changes

The appliance has a pre-configured firewall. Webmin allows changes to the firewall if required. For example if the RADIUS server needs to run on a different port then the firewall will require a change.

Firewall settings can be accessed from the Networking -> Linux Firewall section.

To change an existing rule, scroll down the firewall screen to the **Chain RH-Firewall-1-INPUT** section and click on the Accept of the line associated with the rule to be changed.



Chain RH-Firewall-1-INPUT

Select all. | Invert selection.

Action	Condition	Move Add
Accept	If input interface is **lo**	
Accept	If input interface is **eth1**	
Accept	If protocol is **ICMP** and ICMP type is **any**	
Accept	If protocol is **50**	
Accept	If protocol is **51**	
Accept	If protocol is **UDP** and destination is **224.0.0.251** and destination port is **5353**	
Accept	If protocol is **UDP** and destination port is **631**	
Accept	If state of connection is **ESTABLISHED,RELATED**	
Accept	If protocol is **TCP** and destination port is **22** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **161** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **631** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **694** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **1645** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **1646** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **1812** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **1813** and state of connection is **NEW**	
Accept	If protocol is **TCP** and destination port is **3306** and state of connection is **NEW**	
Accept	If protocol is **TCP** and destination port is **8080** and state of connection is **NEW**	
Accept	If protocol is **TCP** and destination port is **8443** and state of connection is **NEW**	
Accept	If protocol is **TCP** and destination port is **10000** and state of connection is **NEW**	
Reject	Always	

Figure 13. Firewall List of Rules

This will open a screen that allows the rule to be changed. For example to change the RADIUS port to 1814 click on the Accept of the line

> If protocol is **UDP** and destination port is **1812** and state of connection is **NEW**

This brings up the following screen:

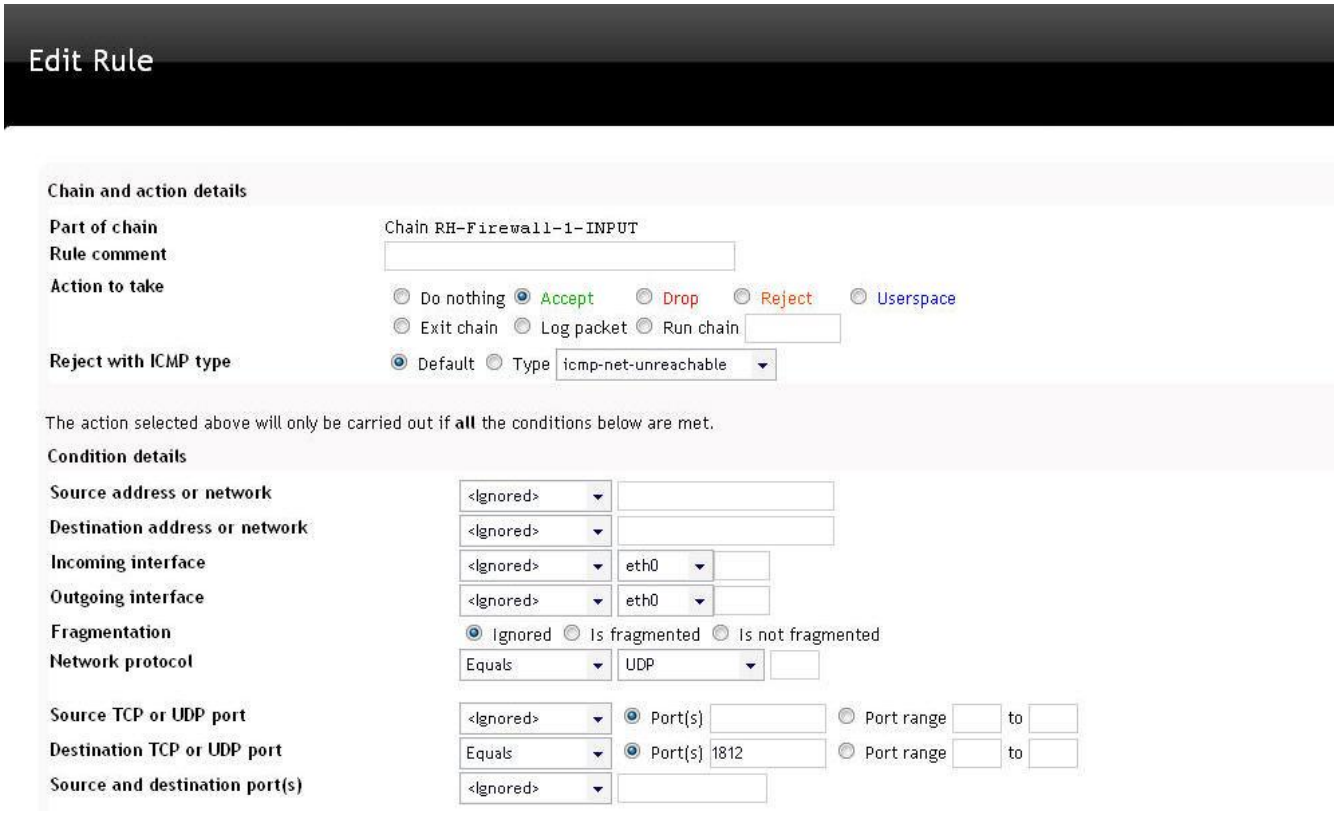


Figure 14. Editing a firewall rule

1. On this screen change the port number to 1814 and select **'save'**.

2. Then on the first firewall screen select **'Apply Configuration'**. This will apply the new rule

The easiest way to create a new firewall rule is to clone an existing firewall rule:

1. Select a rule that is similar to the new required rule, e.g. to allow ssh access on port 222 and port 22 select the default port 22 rule:.

   If protocol is **TCP** and destination port is **22** and state of connection is **NEW**

2. Select **'Clone rule'** at the bottom of the screen.

3. This will create a copy of that rule. Then edit the elements that are different for this rule, e.g. change the port from 22 to 222. Then select **'Clone'** which creates a new rule, with the new port number.

Action	Condition	Move Add
Accept	If input interface is **lo**	
Accept	If input interface is **eth1**	
Accept	If protocol is **ICMP** and ICMP type is **any**	
Accept	If protocol is **50**	
Accept	If protocol is **51**	
Accept	If protocol is **UDP** and destination is **224.0.0.251** and destination port is **5353**	
Accept	If protocol is **UDP** and destination port is **631**	
Accept	If state of connection is **ESTABLISHED,RELATED**	
Accept	If protocol is **TCP** and destination port is **22** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **161** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **631** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **694** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **1645** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **1646** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **1812** and state of connection is **NEW**	
Accept	If protocol is **UDP** and destination port is **1813** and state of connection is **NEW**	
Accept	If protocol is **TCP** and destination port is **3306** and state of connection is **NEW**	
Accept	If protocol is **TCP** and destination port is **8080** and state of connection is **NEW**	
Accept	If protocol is **TCP** and destination port is **8443** and state of connection is **NEW**	
Accept	If protocol is **TCP** and destination port is **10000** and state of connection is **NEW**	
Reject	Always	
Accept	If protocol is **TCP** and destination port is **222** and state of connection is **NEW**	

Figure 15. Updated firewall, showing new rule for port 222

Move this rule to the most appropriate place in the chain using the arrows on the right hand side of the screen as the order for the rules are important.

Disabling the firewall

To disable the firewall for any reason e.g. for installation/testing, from the Networking->Linux Firewall screen, select the first Action under the Incoming Packets (INPUT) section. Change the action from Run Chain to Accept. Save and apply the changes.

Starting and Stopping Tomcat

To start and stop Tomcat access the Servers->PINsafe screen. On this screen there are buttons to stop
Tomcat, start Tomcat and restart Tomcat.

Configuring SSL

The Swivel appliance runs over ssl as standard using a pre-installed, self-signed certificate. To change the certificate, edit the Tomcat server.xml file. The use of ssl is determined by the connector definitions.
An ssl connector is defined as shown

```
< Connector address="0.0.0.0" port="8080" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" keystoreFile="/home/swivel/.keystore"
keystorePass="lockbox" />
```

To change this to non-SSL this definition needs to be replaced with

```
< Connector address="0.0.0.0" port="8080" />
```

Similarly for the ancillary apps, in the same file

```
< Connector address="0.0.0.0" port="8443" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" keystoreFile="/home/swivel/.keystore"
keystorePass="lockbox" />
```

Is replaced with

```
< Connector address="0.0.0.0" port="8443" >
```

PINsafe Tasks

There is a Swivel specific section in Webmin covering a range of Swivel specific functions.

Tomcat
There are buttons to start, stop and restart the Tomcat service. Additionally there is a button that allows the editing of the Tomcat server.xml file. Editing this file changes certain aspects of the Tomcat installation, for example to run Swivel on ports other than the defaults of ports 8080/8443.

Note: In an Active/Passive HA config using disk replication, stop Tomcat with the Tomcat stop button. However Tomcat should be restarted using the heartbeat restart command.

Editing Swivel config files
All the files can be opened within a text editor for modification. Only authorised or trained personnel should make any alterations to the config files. Errors made in these files may prevent Swivel operating correctly.

config.xml
The config.xml file defines how the Swivel application will be deployed. Normally there is no need to edit this file.

ranges.xml
This file determines what IP addresses can access the Swivel Admin Console. It comprises a list of IP addresses and IP address ranges; refer to the Swivel manual for more details.

ChangePIN Config – settings.xml

This file defines the parameters for the ChangePIN application. It is recommended that the default value for the shared secret is changed, remembering to also change it on the Swivel appliance on the agent->configuration screen.

```
<?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">192.180.0.35</entry>
<entry key="imageport">8443</entry>
<entry key="imagessl">true</entry>
<entry key="secret">secret</entry>
<entry key="explicit">false</entry>
<entry key="redirect">http://www.google.com</entry>
</properties>
```

Set ssl to true if you are using https for the authentication.

This is the server used for authentication requests

The port used for authentication requests

The context (directory) of the Swivel server

The context of the image server

The IP address of the image server, localhost will not work

The port used to request images

Set to true if using https to retrieve the images

The shared secret between changepin and Swivel

If explicit is set to true, user enters their new PIN (rather than OTC)

URL to which users is redirected after completing change PIN

Reset PIN Config

This file defines the parameters for the reset PIN application. It is recommended that the default value for the shared secret is changed.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM
"http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="ssl">false</entry>                                  Set ssl to true if you are using https for the authentication.
<entry key="server">localhost</entry>                           This is the server used for authentication requests
<entry key="port">8181</entry>                                  The port used for authentication requests
<entry key="context">pinsafe</entry>                            The context (directory) of the Swivel appliance
<entry key="secret">secret</entry>                              The shared secret between reset PIN and Swivel
<entry key="redirect">http://www.google.com</entry>             URL to which users is redirected after completing change PIN
</properties>
```

Proxy Config

The Swivel appliance has a proxy that proxies inbound requests on port 8080 to the Swivel application running on port 8181. This allows the admin console traffic and the authentication traffic to run over separate ports.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM
"http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="ssl">false</entry>                                  Set ssl to true if you are using https for the authentication.
<entry key="server">localhost</entry>                           This is the server used for authentication requests
<entry key="port">8181</entry>                                  The port used for authentication requests
<entry key="context">pinsafe</entry>                            The context (directory) of the Swivel server
<entry key="secret">secret</entry>                              The shared secret between the proxy PIN and Swivel
</properties>
```

HA Configuration

The Cluster resources screen defines the nodes in the cluster, the resources they share and the actions taken in the event of a switchover.

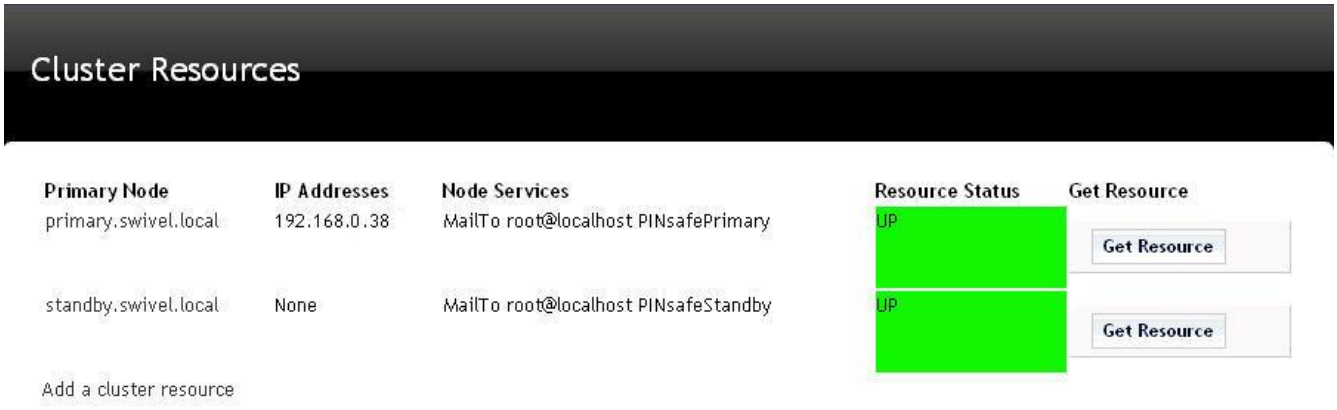


Figure 16. Cluster Resources Screen

The resources shared by a cluster will depend on the type of HA config that is installed. If it is an Active/Active solution then the only shared resource is the virtual IP address (as in the above example). If the configuration is Active/Passive then there will also be a shared disk partition.

SSL Configuration

It is recommended that SSL is used for connecting to Swivel. Therefore a suitable certificate needs installing on the appliance(s) and SSL configuration needs to be completed. This should be done on-site in order to ensure that the SSL certificates are set up properly for the client.

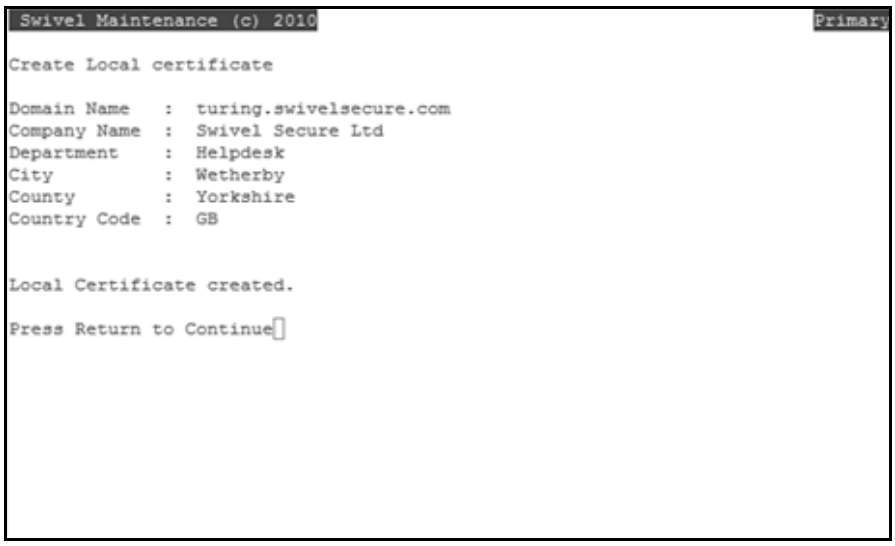
1. Create a local certificate

From the Certificate Management menu, select the Create a local Certificate option.
Note: With a certificate renewal you just need to Generate a CSR on the existing cert, without creating a new cert. You will need to enter the alias of the existing keypair when selecting the cert to generate a csr for. Usually this is 'swivel'.

Here is a screen shot of the first screen you encounter when selecting the Create a local Certificate option. At the time of writing this article, most CAs (Certificate Authorities) require at least 2048 bit key size.

You are next prompted to provide information on the site-name (URL of the Swivel Turing image that the certificate will be securing), company name and location information.

Once all of the information has been entered (including correct country code) you will be presented with the information for review and confirmation that the certificate has been created.



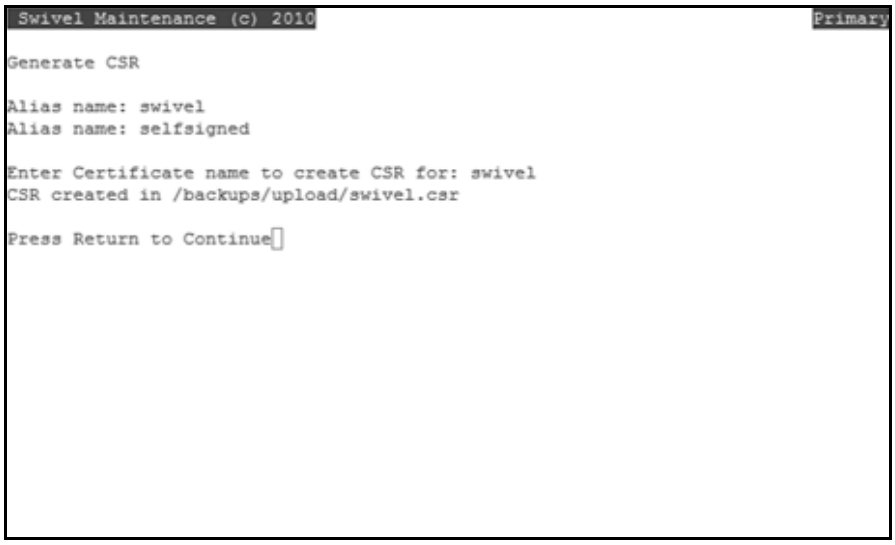
Now you have created a local Certificate, you can generate a CSR (Certificate Signing Request) from it.

2. Generate a CSR

Before performing this step, please ensure you have successfully created a local certificate, as detailed in the previous section.

To generate a CSR (Certificate Signing Request) from the new local certificate, select the Generate CSR menu option from the Certificate Management menu screen. You will be presented with the following screen.

You need to enter the alias swivel as shown in the next screen shot, as this is the alias used by the Certificate Management software when you create a local certificate.



You now need to copy the certificate signing request file you just generated, from the appliance, so that you may send it to your Certificate Signing Authority. For more information on how to copy files to and from the Swivel appliance, see the Copying appliance files How to Guide.
The CSR is created under /backups/upload as <certificate alias>.csr where <certificate alias> in this case would be swivel, e.g. swivel.csr

3. Apply for the Certificate

Request the certificate from the certificate provider via their website. You should receive an email response once the certificate has been signed. You need to look for "Tomcat" or "Java" keystore compatible formats. This is fairly crucial, otherwise you will create further complications translating the certificate to the correct format and this may require command line work.

4. Import the Certificate

Copy your certificate, and any intermediate certificates you require, to the appliance, under /backups/upload. See Copying appliance files How to Guide
Next, on the Certificate Management menu of the appliance, import the intermediate certificates. Ensure they are given aliases that do not already exist in the keystore.

Now import the new certificate, making sure you use the alias that was used to generate the CSR, i.e. "swivel".

5. Check that the certificate is valid

Check the certificate using the View keystore option. The length of the certificate chain should equal the number of certificates you have installed (including intermediates) plus one (for the root certificate). Also, the certificate type should be "privateKeyEntry", not "trustedCertEntry".

6. Delete the old selfsigned alias if it exists

If there is still an alias "selfsigned" in the keystore, delete it, or Swivel may use that instead of the new certificate. Use the delete certificate option for this. Do not delete the local certificate created in step 1.

7. Restart Tomcat

Restart Tomcat to register the new certificate. Check access to the Swivel administration console, and that there is no certificate error.

For more information on the Appliance Certificate process, please refer to the knowledgebase:
http://kb.swivelsecure.com/wiki/index.php/SSL_Certificate_PINsafe_Appliance_How_to_Guide