Table of Contents

1 V3 & V4 Appliance Quick Start.....1

1.1 Quick Start.....1

1.2 Accessing Appliance Menus.....1

1.3 Updating Appliance.....1

1.4 Webmin.....2

1.5 Setting Hostname IP Address.....2

1.6 Starting and Stopping Tomcat.....2

1.7 Accessing the Swivel Applications.....2

2 V4 Appliance Reference.....3

2.1 Introduction.....3

2.2 Main Menu.....3

2.3 Tomcat Menu.....3

2.4 Network Menu.....4

2.5 Appliance Menu.....5

2.6 Backup and Restore.....6

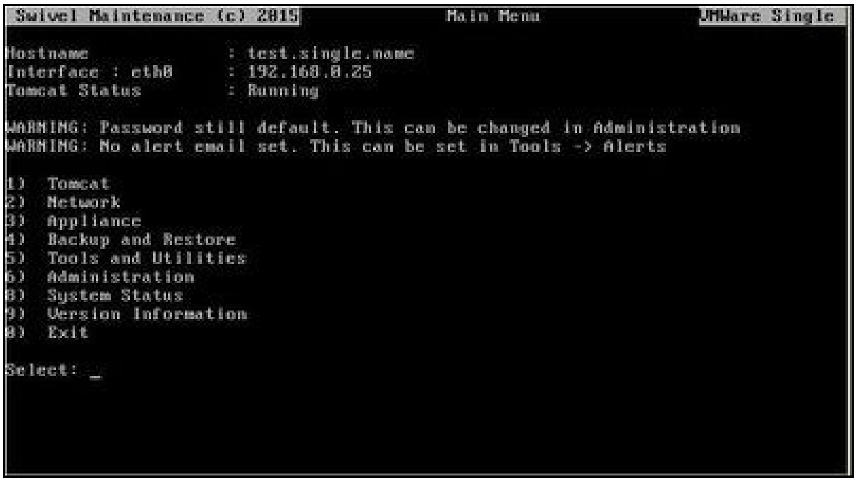
2.7 Tools and Utilities.....7

2.8 Administration.....8

2.9 High Availability (HA).....8

1 V3 & V4 Appliance Quick Start

1.1 Quick Start



```
 Swivel Maintenance (c) 2015              Main Menu              VMWare Single

Hostname             : test.single.name
Interface : eth0     : 192.168.0.25
Tomcat Status        : Running

WARNING: Password still default. This can be changed in Administration
WARNING: No alert email set. This can be set in Tools -> Alerts

1)  Tomcat
2)  Network
3)  Appliance
4)  Backup and Restore
5)  Tools and Utilities
6)  Administration
8)  System Status
9)  Version Information
0)  Exit

Select: _
```

This guide is a quick start guide to the **Version 3 and 4** Swivel Secure Appliances.

A reference guide that describes the meaning for all the menus is also available here for version 3 and here for version 4.

The appliance will come with a pre-configured IP address depending on appliance type:

Stand-alone (192.168.0.35)

HA Primary (192.168.0.36)

HA Standby (192.168.0.37)

Amazon/Cloud (DHCP)

If this IP address is compatible with your network you can plug an ethernet cable into eth0 (labelled Gb1) and access the appliance via SSH.

Alternatively you can access by plugging in an ethernet cross-over cable into eth0

1.2 Accessing Appliance Menus

To access the appliance menus you secure-shell onto the appliance. From a Windows machine you can use a terminal emulator capable of SSH connections, such as putty. From a Linux machine you can simply use the ssh command. SSH access is via the standard port 22.

When you access the appliance you will be prompted for a username and password. The default settings for this are:

- V3 and V4.0 appliances:

username:admin

password:lockbox

- V4.1 and later appliances:

username:admin

password:securebox

Once you have logged on you will be presented with the top level menu. Sub-menus are accessed by simply pressing the number of the item required followed by <Enter>

On certain actions you will be asked to enter Y to continue. Entering any other character or just entering return will cause the action to be cancelled. To maintain compatibility with v2, entering ?yes? will also work.

NOTE Refer to our PuTTY How To Guide for detailed instructions and screenshots.

1.3 Updating Appliance

Important You should update an appliance prior to installation to ensure it is running the optimum versions and settings

A reference guide that details the options available for Appliance updating is available.

1.4 Webmin

You can find the Webmin guide here.

1.5 Setting Hostname IP Address

If you are using an Cloud-based appliance, IP addresses must be set by DHCP.

You will need to set the IP address(es) of the appliance. To do this use the access the Network Menu and do the following

1. Use the change hostname to set the hostname. Recommended to make this a meaningful, eg swivel.yourcompany. If this appliance is part of an HA installation include the appliance type eg primary.swivel.yourcompany.
2. Set the Network settings for ETH0. This is the main interface, you may not need to change the ETH1 settings as this is used for database replication (ref Setting up HA)
3. Set DNS servers. This may not be required at this stage but will be required if the Swivel Appliance will need to perform DNS resolution, eg for sending emails or SMS messages via named hosts.

1.6 Starting and Stopping Tomcat

Swivel applications run within Tomcat so you will only be able to access them when Tomcat is running. Tomcat will start automatically when the appliance starts and the status of Tomcat is shown on the main screen and on the Tomcat menu screen.

Should you need to manually start or stop Tomcat, this is possible from the Tomcat menu.

1.7 Accessing the Swivel Applications

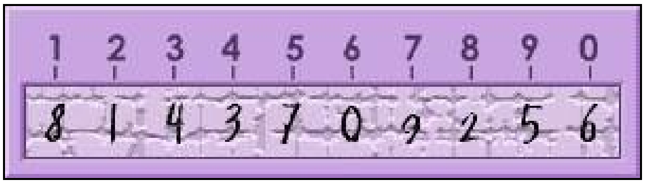
With the ETH0 address set to <IP Address> you will be able to access the following applications from a browser:

Swivel Core admin console https://<IP Address>:8080/pinsafe. For version 4, this should be https://<IP Address>:8080/sentry.

Swivel User (Self Service) Portal https://<IP Address>:8443/userportal

Swivel Proxy https://<IP Address>:8443/proxy

- The Swivel Proxy has no user interface but acts as a proxy for image and message requests e.g. https://<IP Address>:8443/proxy/SCImage?username=test should result in a TURing image being displayed.



2 V4 Appliance Reference

2.1 Introduction

This is a reference guide for Version 4 of the Swivel Appliance. It describes the function of each menu.

It should be used in conjunction with the How to guides and quick start guide.

2.2 Main Menu

1	Tomcat
2	Network
3	Appliance
4	Backup and Restore
5	Tools and Utilities
6	Administration
7	High Availability
8	System Status
9	Version Information
0	Exit

Most of the items on this menu have sub-menus described below. The exception are:

Version Information: Lists versions of the installed software on this appliance.

Exit: Logs out of the Console. **0** will always return to the previous menu from all sub-menus.

Note that the High Availability menu is not shown on stand-alone appliances.

2.3 Tomcat Menu

1	Start/Stop	Start or Stop Tomcat as required
2	Restart	If Tomcat is running it will be stopped and the restarted. If Tomcat is not running, it will be started
3	HTTPS	Sub menu that allows you to Enable or Disable https on either port 8080 or 8443 as required. Requires Tomcat Restart to take effect
4	Certificates	Opens a menu for managing certificates
5	SSL Protocols	Opens a menu to enable or disable SSL protocols

2.3.1 HTTP(s) Menu

1	Enable/Disable HTTPS on Port 8080	Enables or disables HTTPS for Swivel Core (port 8080)
2	Enable/Disable HTTPS on Port 8443	Enables or disables HTTPS for Sentry and auxiliary applications (port 8443)

2.3.2 Certificates Menu

1	Create Local Certificate	Use this option to Generate a Local Certificate, which can then be signed by a Certificate Authority.

2	Generate CSR	Generate a Certificate Signing Request from an existing certificate alias.
3	Import to New/Existing Alias	Sub-menu to import a Certificate Response from a Certificate Authority on top of the existing alias that the Certificate Signing Request was generated from, or to import a trusted root certificate.
4	View Keystore	View the contents of the Keystore, either by selecting one alias in particular or choose to view everything.
5	Delete Certificate from Keystore	Delete a certificate from the Keystore by selecting a particular alias name.
6	Generate Self-Signed Certificate	Use this option to Generate a Self-Signed Certificate.
7	Clone Certificate	This option can be used to clone a Certificate by specifying the alias name of the certificate you wish to clone and providing a new alias name for the clone. This is useful for backing up aliases prior to making changes such as importing responses
8	Import / Roll Back to Previous Keystore	Each time a change is made to a Keystore, a backup is created. This option allows you to rollback to one of those backups and they are labelled according to date and time. You can also use this option to import from an external keystore, which MUST include the private key, and can be either a Java Keystore or a PKCS#12 (PFX) file. If you do not have a certificate in either of these formats, please see SSL Solutions for further suggestions.
9	Change Keystore Password	Use this option to change the password for the certificate keystore

2.3.2.1 Import Menu

1	Import to New Alias	Import a trusted root certificate
2	Import Response to Existing Alias	Import a certificate response to an alias that has previously been used to generate a CSR

NOTE:

- All trusted root certificates **MUST** be imported **before** the response which they have been used to sign.
- Certificates must be uploaded to /backups/upload prior to using this menu.

2.3.3 SSL Protocols Menu

1	Enable/Disable TLSv1.0

As the caption for this menu states, TLSv1.0 is deprecated and insecure, but is required by some legacy applications. Use this option under advice from your reseller or Swivel Secure support.

2.4 Network Menu

1	Change Hostname	Set the hostname of the appliance.
2	Change IP address	Displays a sub-menu to change the IP address of either of the network interfaces
3	Change Default Gateway	Change the default gateway IP address
4	NIC Settings	Allows for the setting of the bit rate negotiation for the network interfaces. Default is Auto-Negotiation
5	DNS	Allows for the adding and removal of DNS servers for the appliance to use for domain-name resolution.
6	HTTP Proxy	If the Swivel Appliance has to make outbound http connections via an http proxy, those proxy settings can be set here. This includes proxy IP Address, Port and username/password if required.
7	NTP Servers	The Swivel appliances run an NTP Daemon. This menu allows you to edit the list of NTP servers that this daemon will use to keep the Appliance server time accurate.

8	Route Configurations	This allows you to create custom routes, see below
9	Restart Interfaces	Restart the Network interfaces. This may be required to allow new settings to take effect

2.4.1 Route Configurations Menu

1	Show Route Table	This displays the default rules for routing traffic. Typically it will show that the default route (for destination IP 0.0.0.0) to be routed via the gateway defined under the Network menu
2	Add Route	By default outbound traffic will be routed via the defined gateway. You can specify exceptions to this rule by adding custom routes to the routing table. For example if you require traffic to IP addresses 12.19.19.xxx to be routed via the gateway 172.1.1.1 you would create the route IP address 12.19.19.0 Netmask 255.255.255.0 Gateway 172.1.1.1
3	Delete Route	You can delete one or all of the custom routes that you have added. This will have no effect on the default routing table.

2.5 Appliance Menu

1	Default running services	The default running services are those services that will start automatically when the appliance boots. It is recommended that you only start the services your required as starting non-configured services can increase boot times.
2	Start/Stop Services	Manually start or stop any of the Appliance services
3	SMTP Server	Configure an SMTP server to which to send Appliance alerts
4	Set Database to Shipping	Sets the Swivel Core database to Shipping Mode to allow access using default credentials. A Tomcat restart is required

2.5.1 Default Running Services

	Service	Description	Default
1	Tomcat	Host server for Swivel Applications	ON
2	Sendmail	Required to use Appliance as a mail relay server	ON
3	SNMP	For Network Management (if required)	OFF
4	Database	Appliance Database service	ON
5	Webmin	Web based GUI alternative for Appliance management	OFF
6	Heartbeat	Use for HA installations to determine status of peer appliance	OFF
7	Database	Use for HA installations to determine status of peer application server	OFF

2.5.2 Start/Stop Services

	Service	Description
1	Tomcat	Host server for Swivel Applications
2	Sendmail	Required to use Appliance as a mail relay server

3	SNMP	For Network Management (if required)
4	Database	Appliance Database service
5	Webmin	Web based GUI alternative for Appliance management
6	Heartbeat	Use for HA installations to determine status of peer appliance
7	Database	Use for HA installations to determine status of peer application server

2.5.3 SMTP Server

1	Enable/Disable SMTP	Enable of Disable the sending of alerts via email
2	Change SMTP server	Select this option to enter a hostname or IP address of the SMTP server you wish to relay email to, from the appliance.
3	Enable Authentication	Enable authentication for the SMTP server if it is currently disabled. You will be prompted to enter a valid username and password.
3	Change Username and Password	If authentication is enabled for the SMTP server, change the username and password for SMTP authentication.
4	Disable Authentication	Disable authentication for the SMTP server, if it is currently enabled.

2.6 Backup and Restore

1	Backup	This option takes you to the Backup submenu. From here you can choose from a multitude of manual Backup types.
2	Restore	This option takes you to the Restore submenu. From here you can choose from a multitude of Restore types.
3	Purge Old Backups	Use this option to get to the Purge menu. Here you can define how many days to retain backups and manually purge them
4	Configure FTP	Use this option to define your FTP server details. You can also manually send the latest backup to your FTP server.

2.6.1 Backup Menu

1	Full Backup	This option takes a full backup of the Swivel Application including the Swivel configuration, database, Tomcat certificate keystore. The Appliance settings are also backed up.
2	Application Only Backup	This option takes a backup of the items necessary to restore the application. the Tomcat configuration and keystore, the Swivel home folder contents, and the Tomcat webapps and the database.
3	System Only Backup	This option takes a backup of the items more central to the system than the application. Effectively, it?s everything in the full backup that isn?t in the application backup (and the tomcat config and keystore).
4	Create Restore Point	This option takes a full backup which is never purged and has an assigned name.

2.6.2 Restore Menu

1	Full Restore	This option lets you restore from any full backup present in /backups/swivel.

2	Application Only Restore	This option lets you restore only appliance-level files from any full or appliance backup present in /backups/swivel.
3	System Only Restore	This option lets you restore only system-level files from any full or system backup present in /backups/swivel.
4	Restore Point Restore	This option lets you restore from any restore point backup present in /backups/restore.
5	Restore from Older Version	This option lets you restore from v2 backups present in /backups/old

2.6.3 Configure FTP Menu

1	Modify FTP Server	Modify the features of the assigned FTP server: server, destination folder, user, password
2	Delete FTP Server	Delete the assigned FTP server, and stop sending backups using FTP.
3	Forcibly Send Latest Backup Over FTP	Send backups to the FTP server manually. If backups aren?t being sent, the error message from this command could be helpful in debugging the problem.

2.7 Tools and Utilities

1	Ping Host or IP Address	Allows you to ping a hostname or IP address to test DNS and network connectivity
2	NS Lookup	Performs a DNS lookup on a hostname
3	Telnet	Attempts a telnet session to a remote host and port
4	Trace-Route	Lists the hops between the appliance and a remote host
5	Command Line	Allows access to the command line. Requires command line password: contact support@swivelsecure.com
6	Collect Support logs	Collects log information and sends to an email address. Requires SMTP server to be set
7	Alerts	This shows a sub-menu to enable an email alert to be sent if there is a disk space warning. (See Disk Space)

2.7.1 Alerts

1	SMTP Server Menu	Shows the SMTP Server menu detailed above
2	Change Alert Email	Changes the email address the alerts are sent to
3	Change From Address	Changes the email address the alerts appear to come from
4	Send Test Email	Sends a test email according to the settings above
5	Show Disk Space Menu	Shows the following sub-menu

2.7.2 Disk Space

1	Status	Shows the current usage of the Appliance disk partitions
2	Change Disk Space Warning Levels	Allows you to set the level at which a warning will be sent indicating that the partition has gone above capacity expected for normal operation
3	Add New Disk to Check	Allows you to add a new partition to be have its usage monitored

4	Remove a Disk from Check	Remove a disk from the list to be checked
5	Restore to Default	Restores the partition usage thresholds back to their default settings.

2.8 Administration

1	Change Admin Password	Changes the password required to access the Appliance Menus. If you do change this password **please keep a secure record**. if you lose this password Swivel Secure may not be able to regain access to the appliance
2	Add Certificates	It is possible to use certificate-based authentication to access the Appliance. This menu allows you to add that certificate
3	Deauthorize Default Certificates	Remove the ability to log on to the appliance using the default certificates stored in /root/.ssh. Ensure you have some other way of logging in before doing this!
4	Reboot	Reboots the appliance.
5	Shutdown	Shutdown the appliance. Use with caution if remote from appliance
6	Update Appliance	Shows a sub-menu to install appliance updates

2.8.1 Update

1	Settings	Changes the update settings
2	Update CMI Menu	Applies any required updates to the appliance CMI menus
3	Update System	Applies any required updates to the operating system
4	Update Swivel Core Products	Applies any required updates to the Swivel products
5	Install Swivel Sentry	Installs Sentry SSO if not already installed
8	Install/Update Package	Allows you to install or update a package manually. **USE WITH CARE**.
9	Flush Cache	Clears any temporary files left by previous updates

2.8.1.1 Update Settings

1	Enable External Repository Access	Enable/Disable the direct use of CentOS repositories, rather than the Swivel mirror
2	Yum Proxy	Configure a proxy server to enable access to yum.swivelsecure.net

2.9 High Availability (HA)

1	Set Peer IP	In an HA configuration there are two servers that act as peers and possibly others that act as Disaster Recovery. Peer servers replicate data between each other (Master-Master replication) This menu option allows you to set the details of the appliance that is the peer appliance in the HA pair. You can set The Peer Hostname Needs to match the setting set on the peer appliance Peer IP addresses for ETH0 and ETH1 By default the database replication traffic is routed via eth1. If required it can be routed of ETH0 by using the change replication interface option
2	Set DR IP	A DR Appliance has Master-Slave replication. This means changes made on this appliance will be replicated across to the DR Appliance

		but changes made on the DR appliance will not be reflected back. This menu allows you to add a DR Appliance to this Appliance so that database replication logs will be available to the configured DR Appliance. You can add up to 2 DR Appliances. All that is required is to enter the IP address of the DR appliance
3	Database Replication	Start and Stop replication and view the status. see Database Replication
4	Virtual IP	An HA pair can share a virtual IP address. If this is enabled then by default primary server will respond to that IP address. In the event that the primary server goes off-line the standby server will respond. The switchover is initiated via Mon or Heartbeat services. See Virtual IP
5	Advanced	Change hostnames, IPs for HA. Not usually required as defaults will usually be ok or changes will be made when setting Peer IP address in HA menu

2.9.1 Database Replication

1	Status	Replication will take place between peers and between peers and DRs. This menu will allow you to view the status of replication between this appliance and its peer or its DR The status will show if the Remote Appliance is reading the database changes made locally and (in the case of a peer) vice-versa
2	Start/Stop Reading updates	Starts or stops the reading of updates from the remote peer. Equivalent to starting and stopping the slave.
3	Database Replication	Start and Stop replication and view the status. see Database Replication
4	Repair Replication	If replication stops (or has never started) this option allows the databases to be brought into to line and for replication to start. To do this select the database that you want to be the version to use. This data will be copied to both servers and replication will be re-started.

2.9.2 Virtual IP

1	Set Email Address	An email alert will be sent in the event of a failover of the VIP from one server to the other (requires SMTP server to be set up). This sets the destination email address for this alert
2	Change Virtual IP	This sets the value for the virtual IP. This needs setting on both peer appliances.
3/4	Add/Remove Ping Nodes	One way that will be used to determine which Appliance should be responding on the virtual IP is to compare how many ping nodes each server can ping. The default gateway is usually a ping node but others can be added. The same number of ping nodes should be set on both appliances
5	Start/Stop Mon	Mon monitors whether the Swivel core is running on the peer appliance
6	Start/Stop Heartbeat	Heartbeat monitors whether the peer appliance is contactable via either network interface