Silicon:SAFE

Password:Protect

User Guide

September 2017

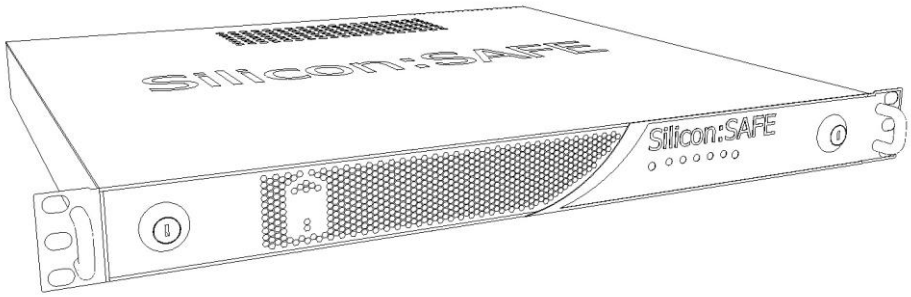

Table of Contents

Feature overview 4
Password:Protect Overview 5
Objective of Document 5
Using Password:Protect 6
Password:Protect Appliance 6
Syslog 6
NTP service 6
Password:Protect Windows Configuration Application 7
Deployment Topologies 8
Master-slave 8
Multi-master 8
Data Striping 9
Hardware Installation and configuration 10
Appliance Installation 11
Windows Configuration Application installation 12
Installation 12
Appliance First-time Setup 13
Appliance ad-hoc configuration 20
Admin 20
Update Admin Password: 20
Password Policies: 20
Services: 21
Analytics: 21
Logging: 21
System 21
Update System password: 22
Settings->Logging: 22
Logging: 22
Restart Options: 22
Workflows 23
Changing network settings 23
Changing Encryption settings 23
Adding an Additional Appliance to a Cluster 23

PSU Failure 24
Fan Failure 24
Temperature Events 24
Disk Events 24
Other Events 24
Notification of Events 24
Disaster recovery 25
Appendices 27
APPENDIX I. Example deployments 27
4 Appliance multi-master setup 27
Striped setup with slave backup 28
Striped setup with multi-master 29

Feature overview

Description	Password:Protect, authentication Appliance
Processor architecture	Quad processor 32 bit ARM CORTEX-M3
Disk storage	Flash Memory
Operating System	None
File system	Proprietary “no-read” key value pair file system
Connectivity	4 x Ethernet, 1 x serial
Networking protocols	Proprietary Snap TCP/UDP protocols implemented in HW
Security	
Data storage	Proprietary “no-read” key value pair file system
Encryption	128bit XXTEA or AES-CBC mode Encryption Cypher with 128bit MD5 HMAC
Data storage and backup	• Data Mirroring • Data mirroring with striping
Physical Intrusion detection	Intrusion switch to detect lid removal
Physical keys required to perform certain functions	• Configuration over serial connection • Disaster recovery, End Of Life
Separate SYSTEM and ADMIN functions	Separate passwords for user and network management functions
Redundancy and resilience	
Number of mirrors	Up to 7 mirrors per striped segment
Load balancing	Via mirror Appliances
Redundancy	Via mirror Appliances
Disaster recovery	Replacement Appliance can be populated from a surviving mirror without loss of service
Data Storage	
Total number of secrets stored	16 million per Appliance (per data segment)
Max number of secrets per account	4 (primary and 3 secondary – e.g. Password, PIN, answer to security question, etc.)
Number of user accounts	• 16 m with 1 secret per account • 8 m with 2 secrets per account • 5.3 m with 3 secrets per account • 4 m with 4 secrets per account
Secret storage types	• Plain text (up to 64 alphanumeric characters) • Hash code (up to 512 bits)
Password Policy	
Minimum password length	Yes
Password expiry	Yes (password expires after *n* days, where *n* is settable via a configuration command)
Suspend/Enable user accounts	Yes
Password reset with temporary password	Yes
Re-use of previous passwords prevention	Yes (*n* previous passwords are checked up to a maximum of 5. *n* is settable via a configuration command)
Partial password Support	Individual characters of a password or PIN can be used to authenticate
Brute Force Attack prevention	
Automatic temporary password suspension	After *n* failed authentication attempts, the password is locked for y seconds. Where n and y are configurable
Rate limiting of account deletions	Minimum time between consecutive Delete commands is settable via a configuration command
IP Access Control List (whitelisting)	Each Ethernet port can restrict connections via an ACL
Remote management	Windows Configuration GUI via Ethernet or serial
General features	
Logging	• Syslog logging over UDP • Detailed event logs on Appliance
Time Service	• Set time via NTP time server support • Set time manually

Password:Protect Overview

Silicon: SAFE's Password:Protect is an impenetrable hardware storage and authentication Appliance that stops dead the bulk theft of usernames and passwords during a cyber-attack on a business.

Instead of storing and validating usernames and passwords using a database or directory service in your network, they are stored and validated by Password:Protect.

The underlying concept behind Password:Protect is breathtakingly simple: hardware that allows secrets to be stored and verified, but never retrieved. Only the results of verification requests can leave the Appliance, never the data itself, like a data non-return valve. Secrets are isolated at the hardware level making it impossible to steal them over the network. Because the Appliance is hardware, it has no operating system to hack, no privileges to circumvent, and data is safe whether encrypted or not. It is impervious to Malware because there is no conventional execution environment in which Malware can run and it is impervious to return oriented programming/stack smashing attacks.

Each Password:Protect Appliance can store millions of login credentials and authenticate thousands of users per minute. Appliances have disaster recovery and high availability features built in. They can be clustered for scalability, load balancing and failover including geographic redundancy.

Objective of Document

The objective of this document is to:

- Provides examples of Deployment Topologies
- Provide a guide to the Password:Protect Windows configuration Application

This document does not cover the SNAP protocol used for communication with Password:Protect.

Using Password:Protect

Password:Protect has been designed from the ground up to run 24/7 with minimal maintenance. A full system requires no backups.

Each Appliance has 4 interfaces, each dedicated to a certain role, and configuration of the Appliances is achieved through the Password:Protect Windows configuration Application.

As a further security measure, the Password:Protect Appliance includes two physical key-switches on the front of the case. These keys, when inserted and turned, allow communication to the Configuration interface via the Serial port. The keys also allow certain restricted functions such as disaster recovery and end of life operations. As communication using the Serial port is unencrypted, for security reasons, the keys should not be left inserted when the Appliance is unattended.

Password:Protect Appliance

The Appliance contains a circuit board providing four interfaces. The interfaces all use an encrypted protocol for communication; this is called SNAP. SNAP is not an acronym, the protocol is named after the card game Snap - when two passwords match; SNAP! All four interfaces use Ethernet for communication except the Configuration interface which can also use Serial.

1) Authentication – this interface is public facing, often via web services. This is the interface on which to send:
   a) Account/Password creation commands
   b) Password authentication commands
   c) Password admin commands
2) Replication – this is only used in data replication between Password:Protect Appliances and is usually connected via a private network. This interface is not used for any other purpose.
3) Repository – this interface stores the password data and is not usually connected to other Appliances. Only in the event of Disaster Recovery is the “new” Appliance temporarily connected to the existing Appliance over this interface.
4) Configuration – this interface handles the configuration commands via the Windows Configuration Application. Alongside the Ethernet port, the communication to this interface can also be made via the Serial port (at 115200 baud). There is however, no encryption when using the Serial port. The Configuration interface also handles Syslog and (S)NTP services.

Syslog

All Password:Protect appliances support the use of a Syslog server to generate real-time diagnostics and event logging.

NTP service

Password:Protect appliances can synchronise time using an SNTP or NTP time server. Although the time can be set manually, it is recommended that an NTP server is used to ensure the time is synchronised between appliances. Especially within the replication, it is important that the units know the correct time as this will ensure user accounts are kept up to date across the deployment. All times should be set in UTC.

Password:Protect Windows Configuration Application

The Password:Protect Windows Configuration Application uses the Configuration interface to setup the Appliance.

For the Ethernet interfaces, the following can be configured:

- Encryption and Signing Keys
- IP Address and Port
- Gateway and Subnet mask
- Service suspension
- TCP transmission timeout and retry
- Accept / Reject ping messages (ICMP)
- View MAC addresses
- Remove error description (Authentication service only)
- Setup IP Whitelists
- Peer IP and ports for replication

Other functions are:

- Set / view License Key
- Set Appliance Name and Location
- Set Session Key timeouts
- Set Login Session timeout
- Set Password Policies
- Set / update the admin and system passwords.
- Retrieve Events and Metrics
- Set / Retrieve Time on Appliance
- IP Address and Port for NTP server
- IP Address and Port for Syslog Monitor
- Commit all configuration changes
- Un-commit all configuration changes
- Send a ping command
- Send Password Admin commands
- Perform Disaster Recovery
- Restart or Power Down Appliance

Deployment Topologies

Appliances have disaster recovery and high availability features built in. They can be clustered for scalability, load balancing and failover including geographic redundancy. Both master-slave and multi-master modes are supported. APPENDIX I contains three example deployments.

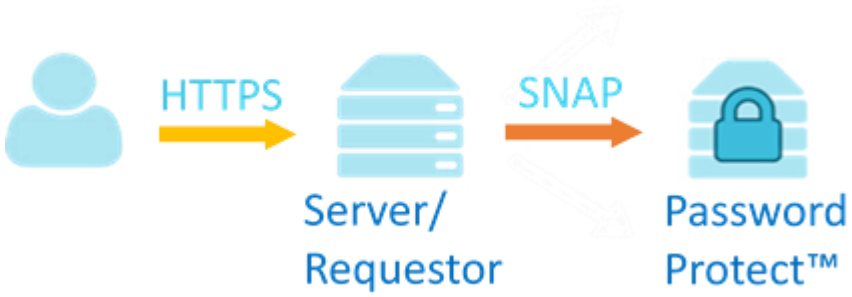

Figure 1 – Password Protect

Master-slave

In master-slave mode, one Appliance is designated as a master and the other(s) are designated as backup slaves. Up to 7 slaves are supported in addition to a master totalling 8 Appliances per cluster. During normal operation, requestors connect to the master Appliance only. Replication ensures that slave devices are kept up to date so that a requestor can fail-over to a slave device in the event of a master becoming unavailable.

Multi-master

In multi-master mode each Appliance can act as a live master thanks to replication of the password repository. Up to 8 multi-masters can exist in a cluster. In multi-master mode, load balancing can be achieved by directing requestors to any master appliance in the cluster.

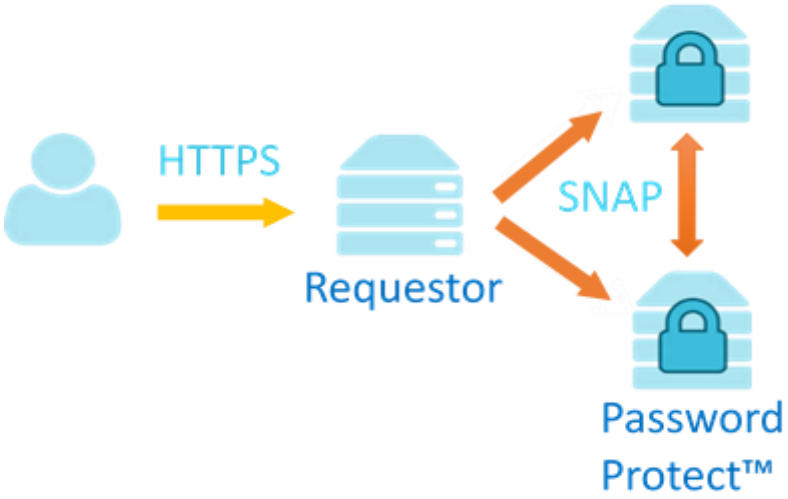

Figure 2 - Clustering Password:Protect appliances

Data Striping

Data can be striped across multiple Appliances. For example two clusters might exist in which half the accounts reside on cluster A and the other half on cluster B. A requestor will have to implement their own connection logic to determine in which cluster a particular account resides, then further connection logic will be required to load balance/failover within the cluster of Appliances.

Striping works in both master-slave and multi-master deployments. In master-slave mode each data stripe comprises a master and up to 7 slave Appliance(s). In multi-master mode, up to 8 master Appliances can exist in each stripe.

For very high authentications rates (> 1000/sec) in which large numbers of requestors are deployed to handle peak demand, data striping can be an effective topology to employ because it allows many requestors to authenticate too many clusters simultaneously. Load balancing and failover to Appliances within each cluster provide resilience.

Figure 3 - Data can be striped to increase throughput

Hardware Installation and configuration

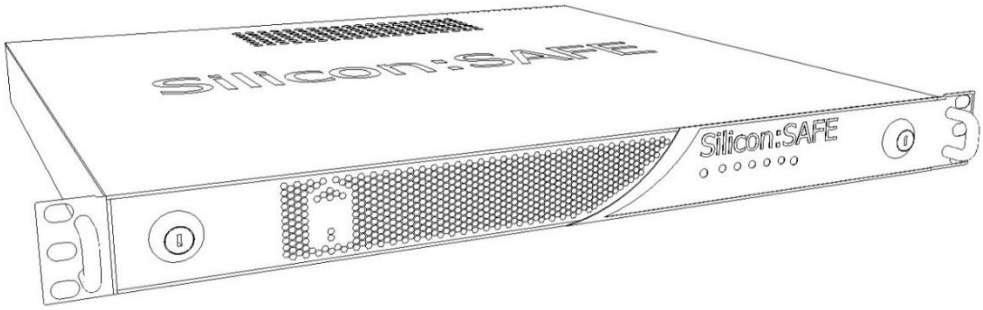

Figure 4 – 19" 1U Password:Protect unit

Password:Protect is a 19" 1U rack-mount Appliance suitable for installation into a standard server cabinet. It features a hot-swappable fully redundant power supply unit (PSU) as standard.

The front panel of the unit includes 2 key-switches, 2 handles and an interface made up of an array of LEDs and switches.

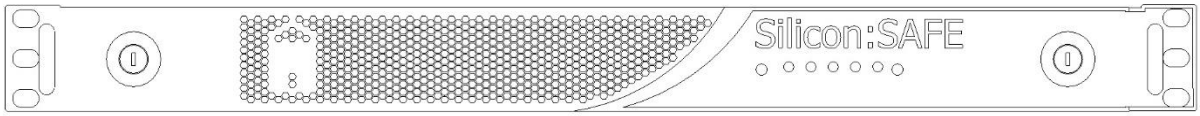

Figure 5 - Front Panel

The front panel interface is shown in more detail in in Figure 6:

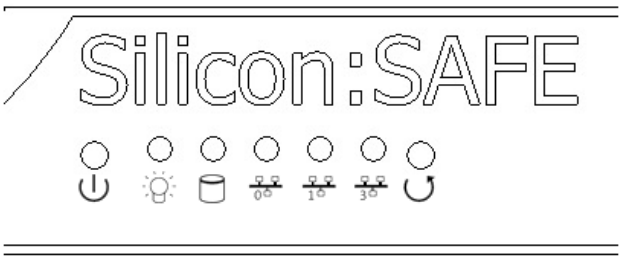

Figure 6 - Front Panel LEDs and Switches

From left to right, the front panel interface consists of:

- Power button
- Power LED [Blue]
- Disk Access LED [Yellow]
- Ethernet 0 (Authentication) LED [Blue]
- Ethernet 1 (Replication) LED [Blue]
- Ethernet 3 (Configuration) LED [Red]
- Restart button

While the unit is powered up, pressing and holding the power button for two seconds before releasing will cause a shut-down. The power button also provides a factory reset facility. Holding the power button for ten seconds (while both key switches are turned) before releasing, will return the Appliance to its factory default setting i.e. all configuration information is reset. This will remove IP addresses so will prevent access to the device over Ethernet. NOTE: the repository is not deleted and the admin and system passwords are also retained. To restart/reset the appliance, the Restart button is used.

While the unit is powered up, the power LED will remain on constantly, and the other LEDs will blink dependant on usage. During regular operation, it is expected that the Authentication and Disk Access LEDs will blink (as users log in) as will the Replication LED (as accounts are replicated across boards). The Configuration LED should only blink while an Admin/System user is logged in and configuring the board via the ethernet.

The rear of the Appliance has two A/C Power jacks (one for each of the redundant PSU modules) and four RJ45 Ethernet sockets. The Eth2 RJ45 socket is not used in normal operation.

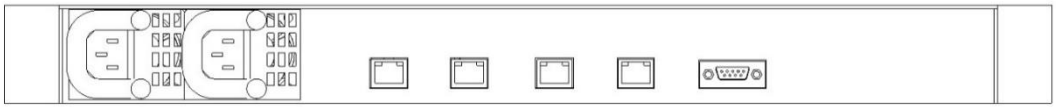

Figure 7 - Back panel

Appliance Installation

A Password:Protect unit should always have power cables plugged in to both of its redundant PSU modules. The Appliance will detect if this is not the case and send Syslog errors if one is missing; The Appliance will continue to function with only a single power connection but redundancy will of course not work.

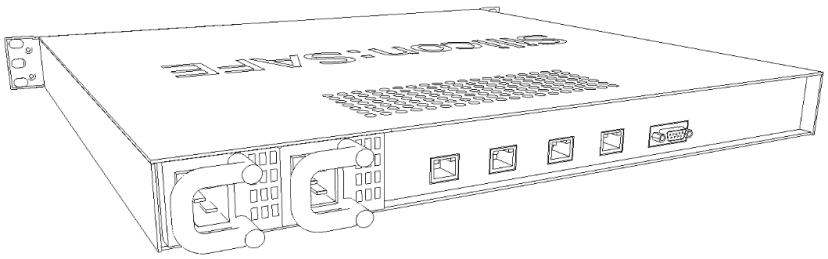

Figure 8 – Rear panel view

All Ethernet cables should be shielded CAT5e as a minimum.

The Authentication service (Eth0) should connect to the network on which the requestor web-server/ directory will reside. The Appliance is designed to cope with being on a busy network, so no special connection needs to be made to the web-server, it may however be advantageous to prevent too much un-related traffic on this network so as not to affect the units performance.

It is highly recommended that the Replication (Eth1) service should be connected to its own physical network, or VLAN, dedicated only to the Replication services of other Password:Protect units.

The Configuration Serial port needs to be connected to a PC/laptop when the Appliance is configured for the first time. Thereafter it can be remotely configured.

Windows Configuration Application installation

The Password:Protect Windows Configuration Application is used to configure each Appliance. This should be installed on a PC/laptop which is able to access the same network as the Configuration interface.

A first-time setup procedure must be followed first to configure each Appliance via the supplied Serial-to-USB cable. This will include programming the network settings, password policy etc. so that the unit is ready to function.

Installation

The setup.msi will install the configuration tool. On starting the installation software, the following page will appear. The installation follows the standard format of any windows application.

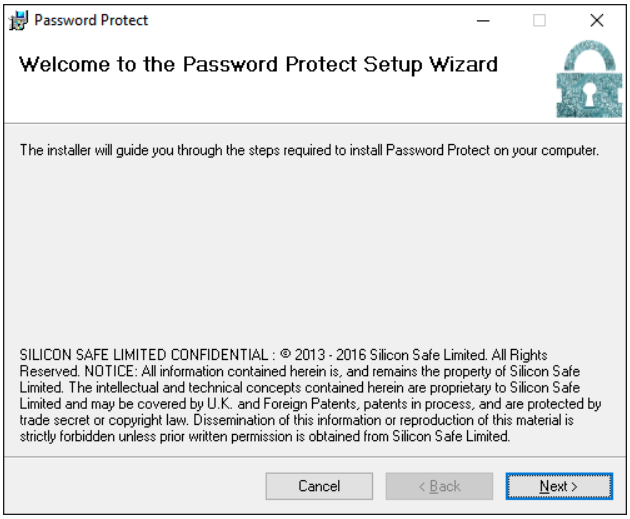

Figure 9 - Windows installer

Appliance First-time Setup

The first connection to an Appliance must be made through the serial port with the supplied USB-to-serial converter – because the Ethernet ports don't have default IP addresses configured.

The Password:Protect Windows Configuration Application will detect that the board is un-configured and run a first time setup wizard. This will ensure that all the necessary parameters will be set. When opened, the Password:Protect Windows Configuration Application will ask for an installation passphrase, this passphrase is used to encrypt the connection details held within the app and will need to be entered every time the program is run. If the password is lost, a reset will have to be carried out which will lose all connection details held locally (this will not affect the Password:Protect Appliances themselves).

Figure 10 - Installation passphrase

The first page that is displayed is the connections list.

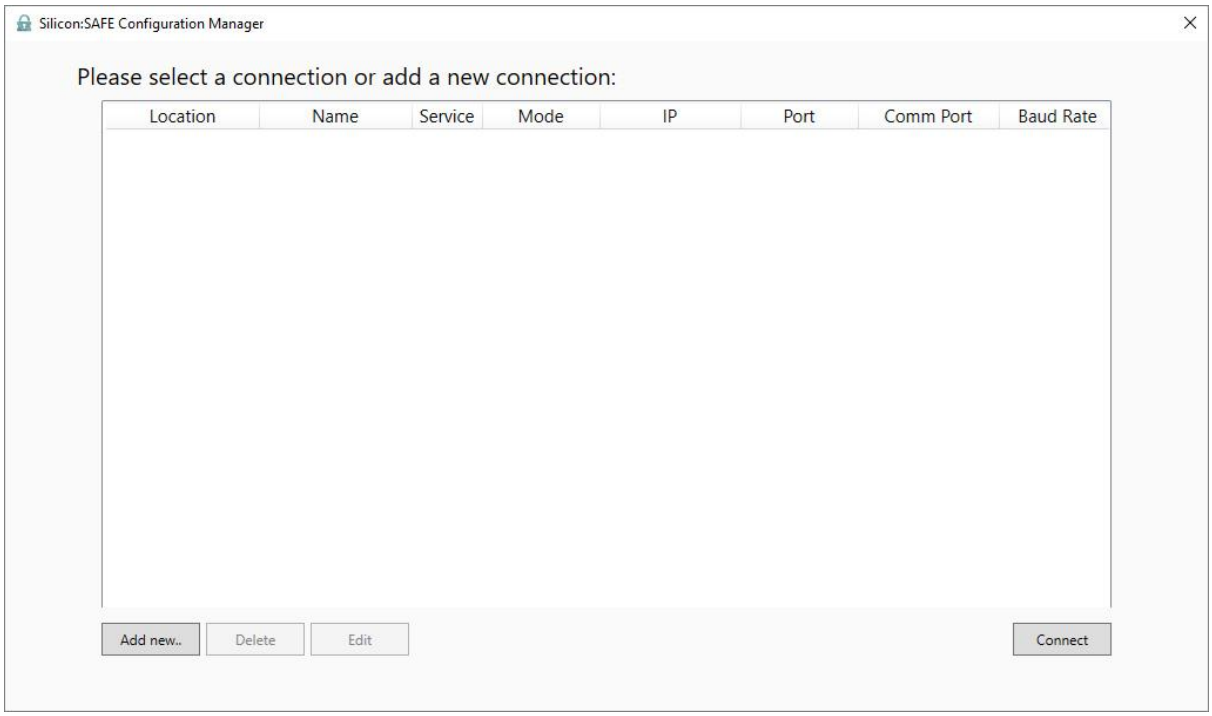

Figure 11 - Connection list

The first connection to add will be the serial port through which the wizard will be completed, before the network settings have been programmed. The COM port will be that of the USB-Serial converter and name and location can be set to help identify the unit in the future.

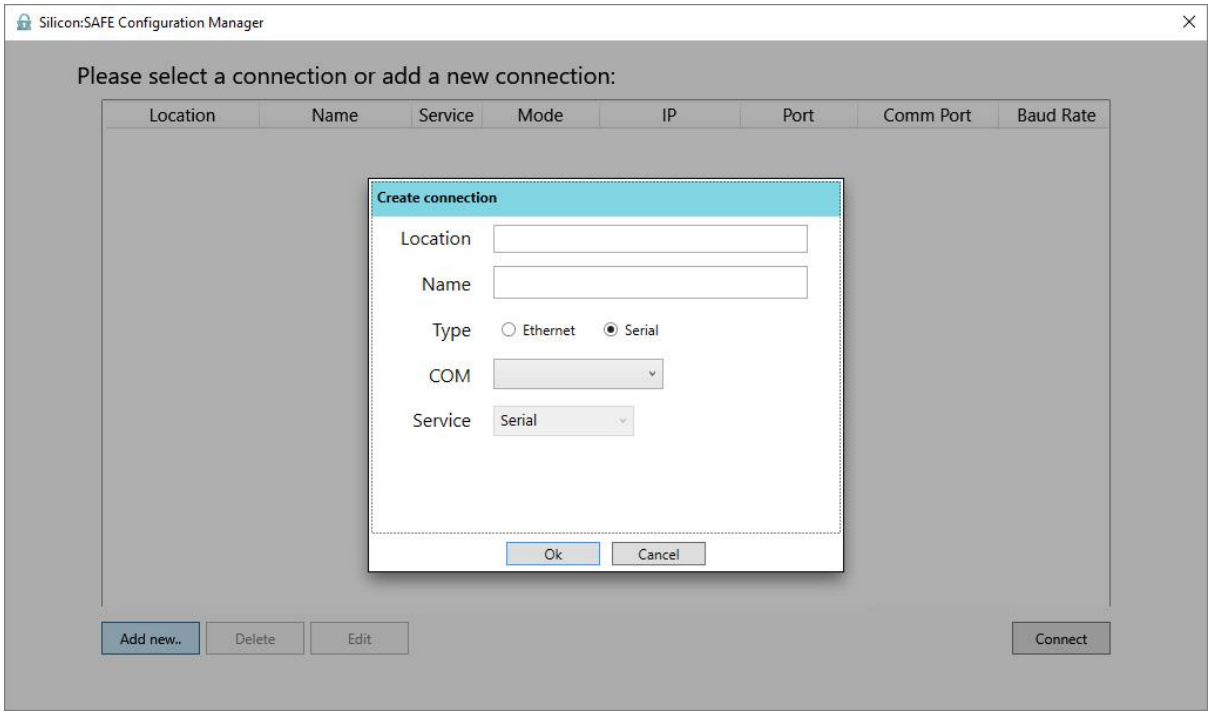

Figure 12 - Add a connection

Once there is a connection listed for the serial port, the board can be accessed and the wizard can begin.

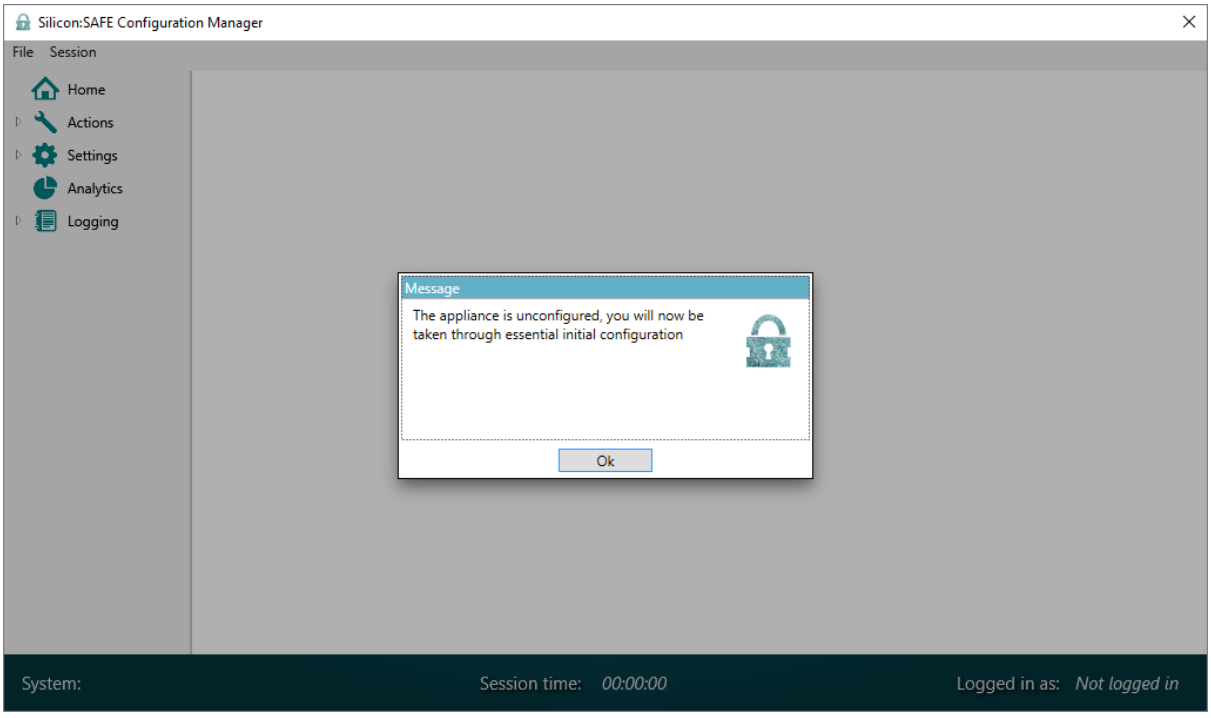

Figure 13 - The Password:Protect Windows App will detect an un-configured board and initiate the first time setup wizard

The first page prompts for the license key provided for the Appliance.

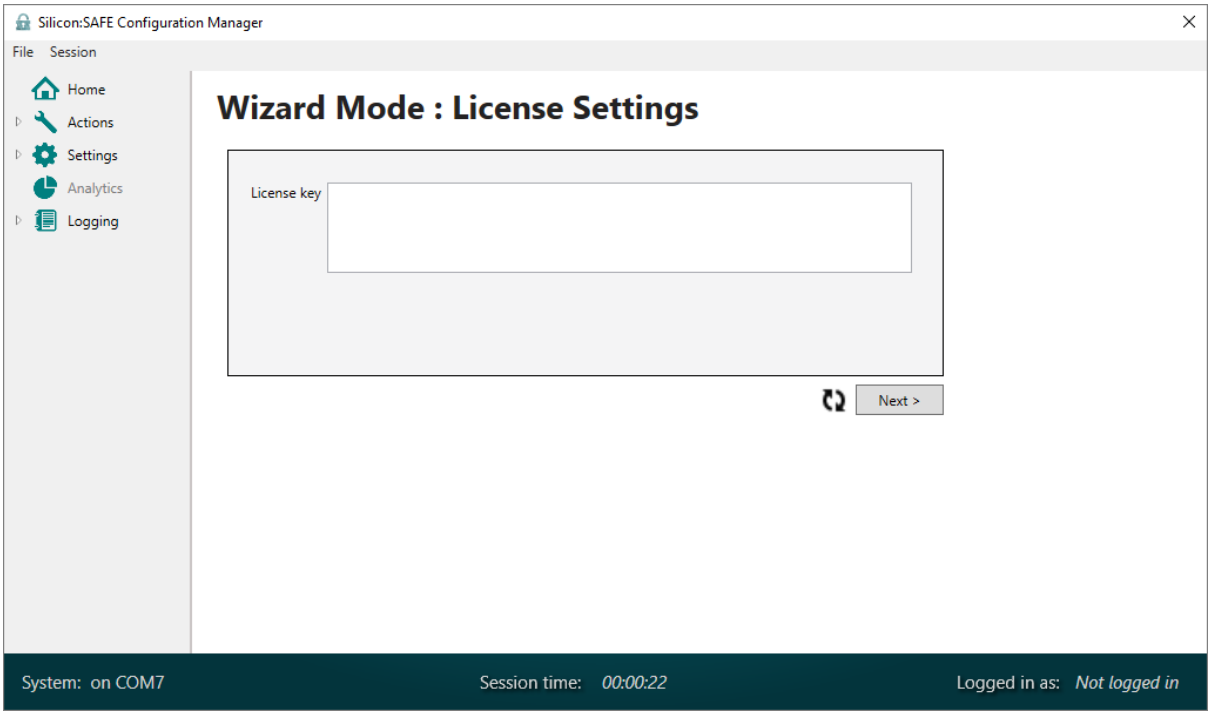

Figure 14 - Each appliance is assigned a unique license key which is needed for operation.

The next page is the password policy page. Here the policy of the deployment can be implemented, including a password expiry time, restrictions on using previous passwords, password length, and max number of failed attempts. Partial passwords can also be enabled, though this does not, by definition, work on hashed password files. It is important to note that the number of secrets refers to the number of passwords defined for each account. It can only be set once and **cannot be changed at a later date!**

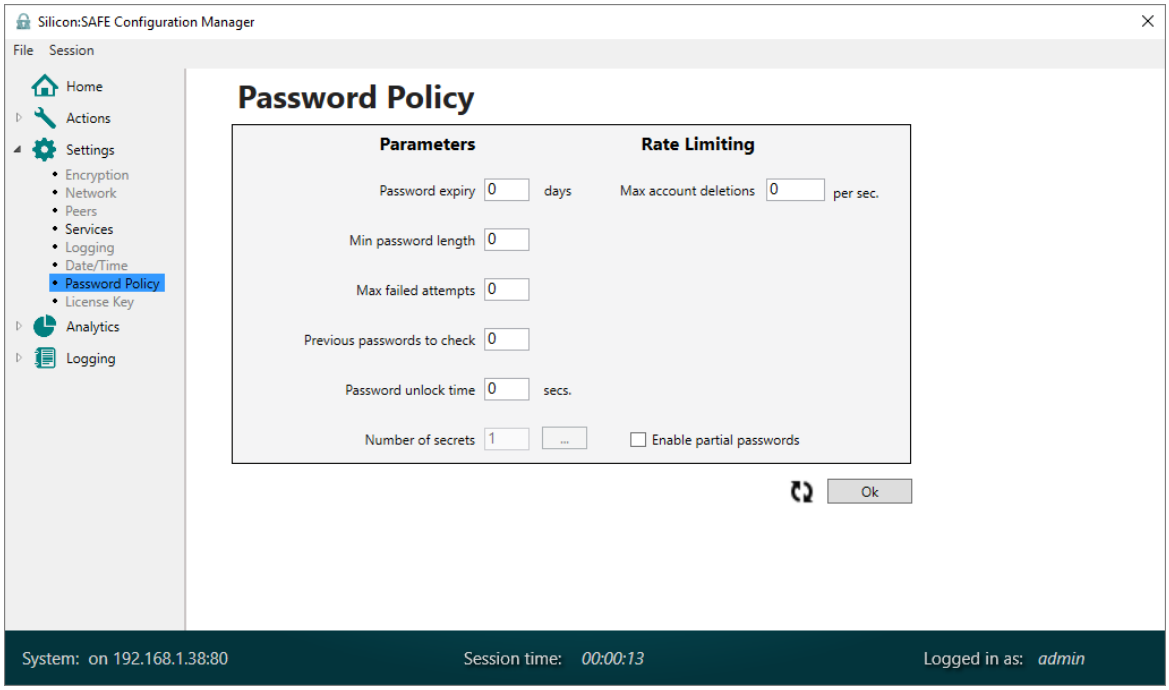

Figure 15 - The password policy dictated by an organisation can largely be implemented on the Password:Protect unit.

With the number of secrets defined, an admin and system account need to be created, these accounts allow ad-hoc configuration through the Configuration interface.

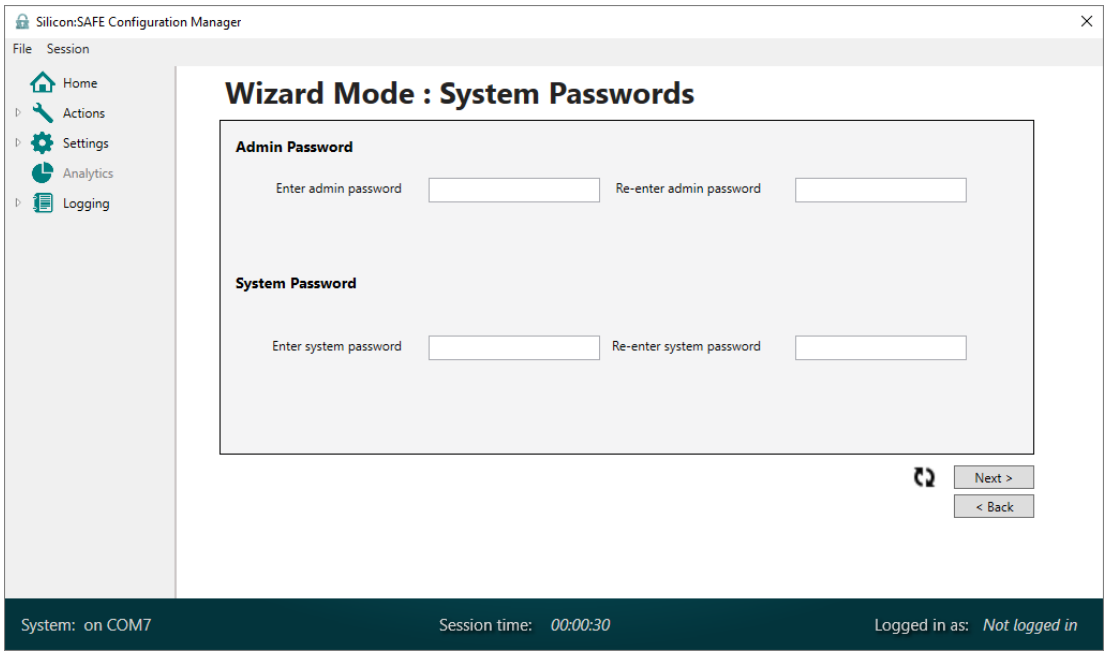

Figure 16 - An admin and a system account are created that give access to certain functions

The Appliance needs to keep time. This can be set manually or an NTP server can be used. The set now button will use the local time on the PC running the Windows Configuration Application.

All appliances in a cluster should use the same time source to reduce clock drift.

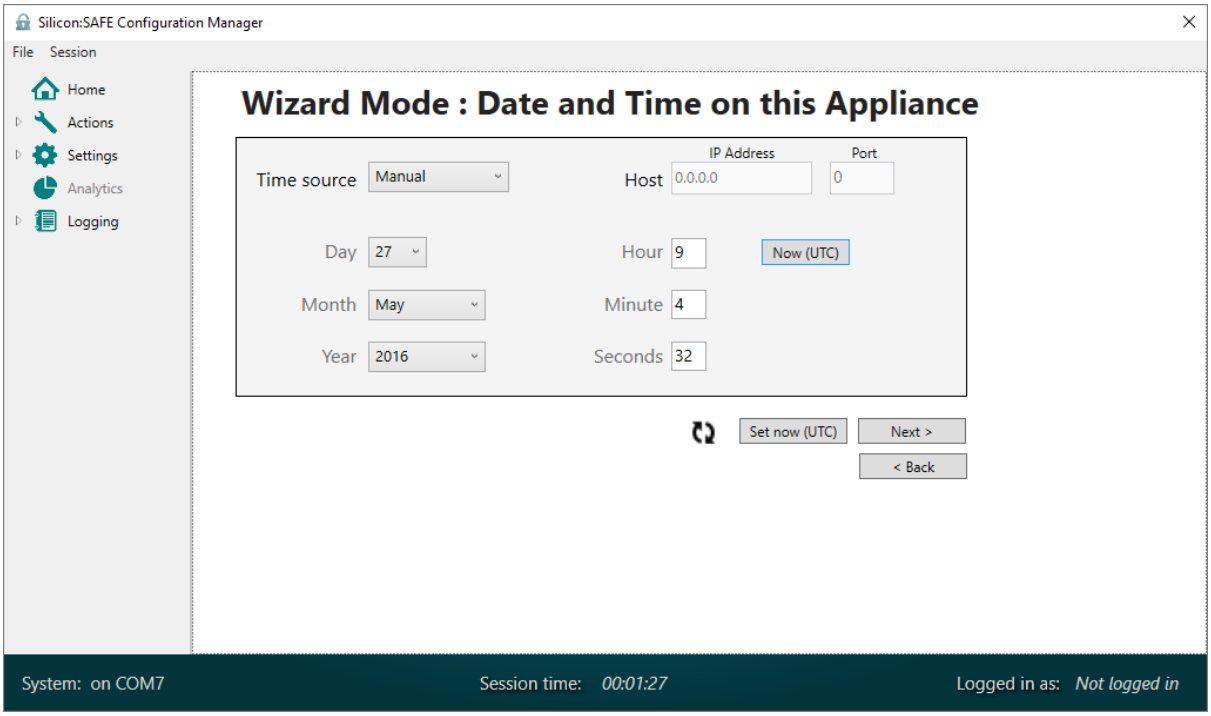

Figure 17 - Both manual or NTP time server settings can be entered

Password:Protect units use symmetric key encryption for all Ethernet interfaces to maintain a secure channel of communication. The 128 bit encryption and HMAC keys need to be set. Each key requires a unique ID (4 digit hex number). It is advised that you create separate keys for each interface.

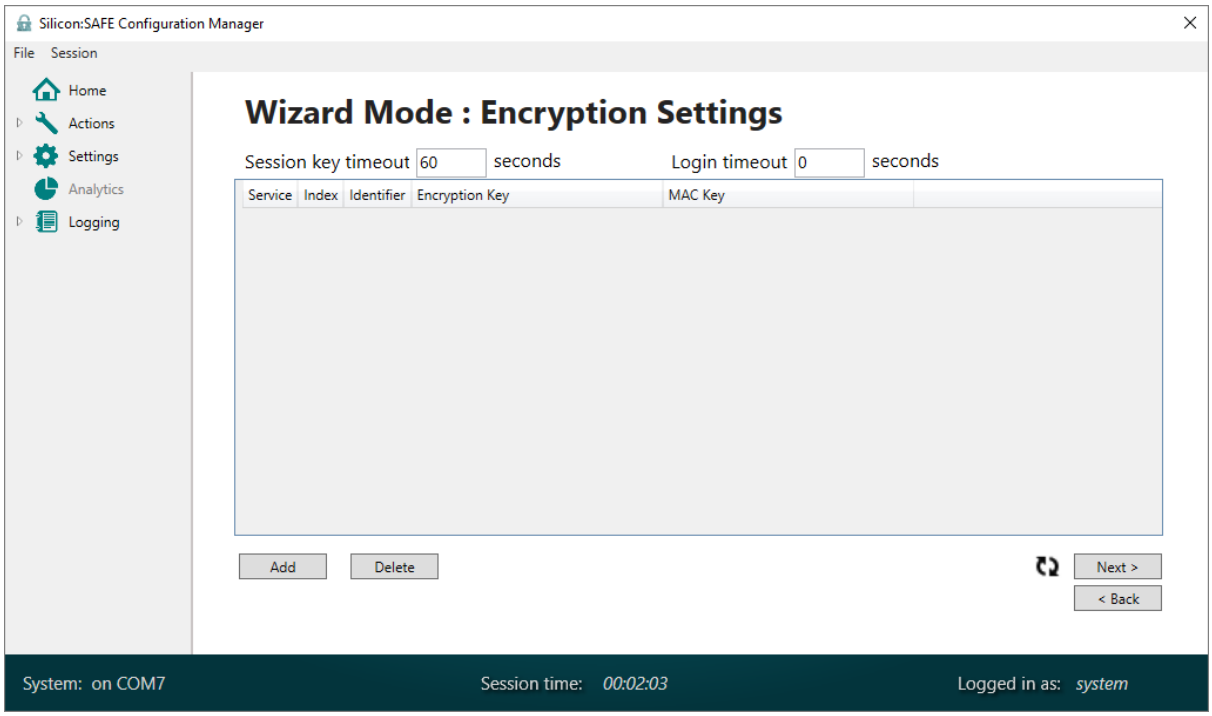

Figure 18 - Communication with the Password:Protect appliance is encrypted using shared keys.

Appliances are shipped without any keys defined so add them as part of the first time setup. More can

Figure 19 - Encryption keys are set manually

be added later, but connection to the configuration interface via Ethernet requires keys.

The '…' button on the right hand side can be used to auto-generate a key. This can be useful to prevent predictable keys. A temporary note should be made of the auto generated keys however so that peers can share keys.

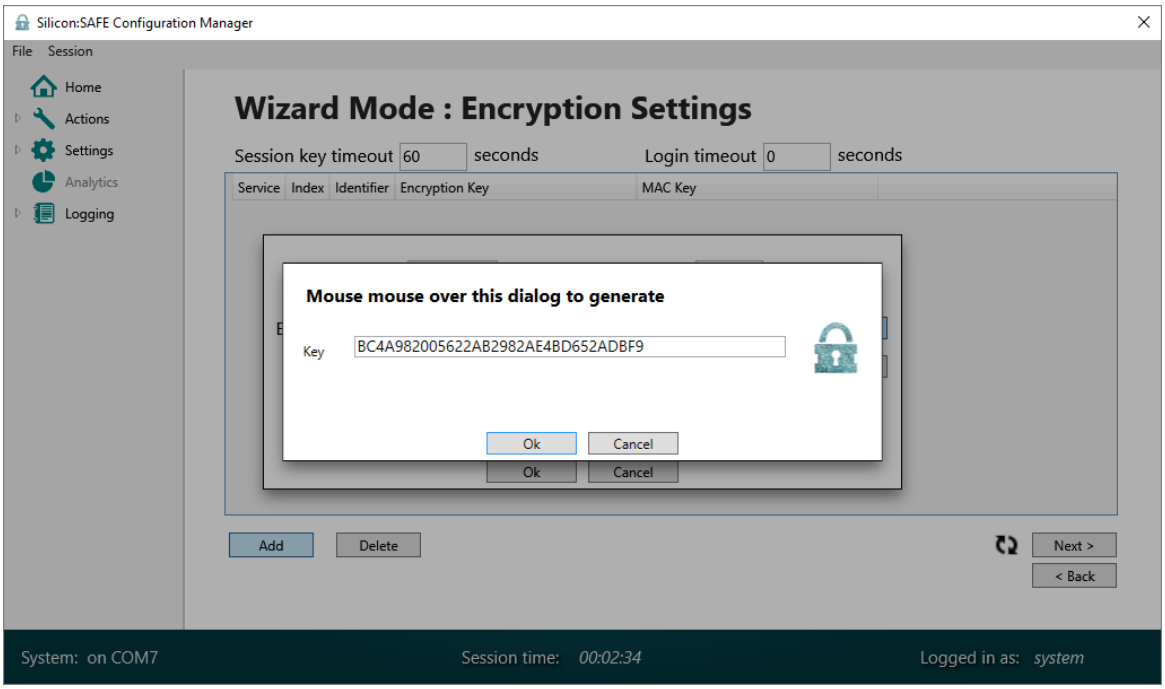

Figure 20 - Keys can be auto-generated

The next page shows the MAC addresses of the 4 interfaces in the Password:Protect unit; these are pre-set into the device and cannot be changed. Users however have control over the IP addresses and ports used, as well as the TCP timeout and retry settings.

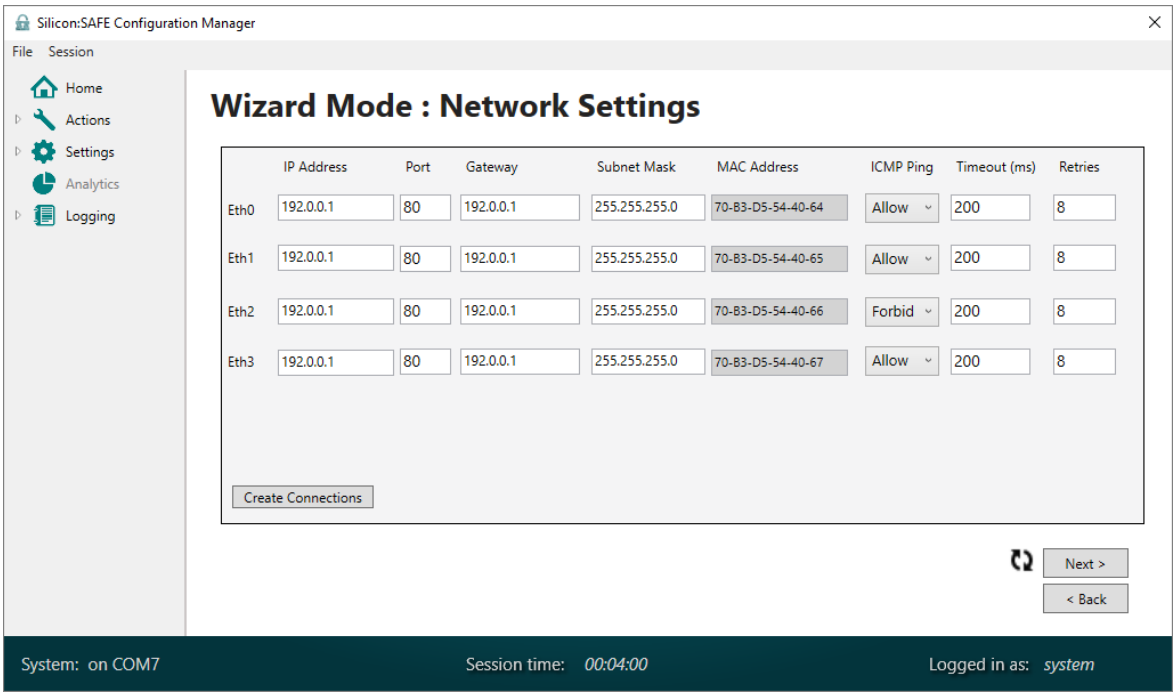

Figure 21 - Network settings

Each Appliance can replicate to up to 7 peers. When adding peers the host IP address and port must be defined, plus the Master key ID of the key to be used must be specified.

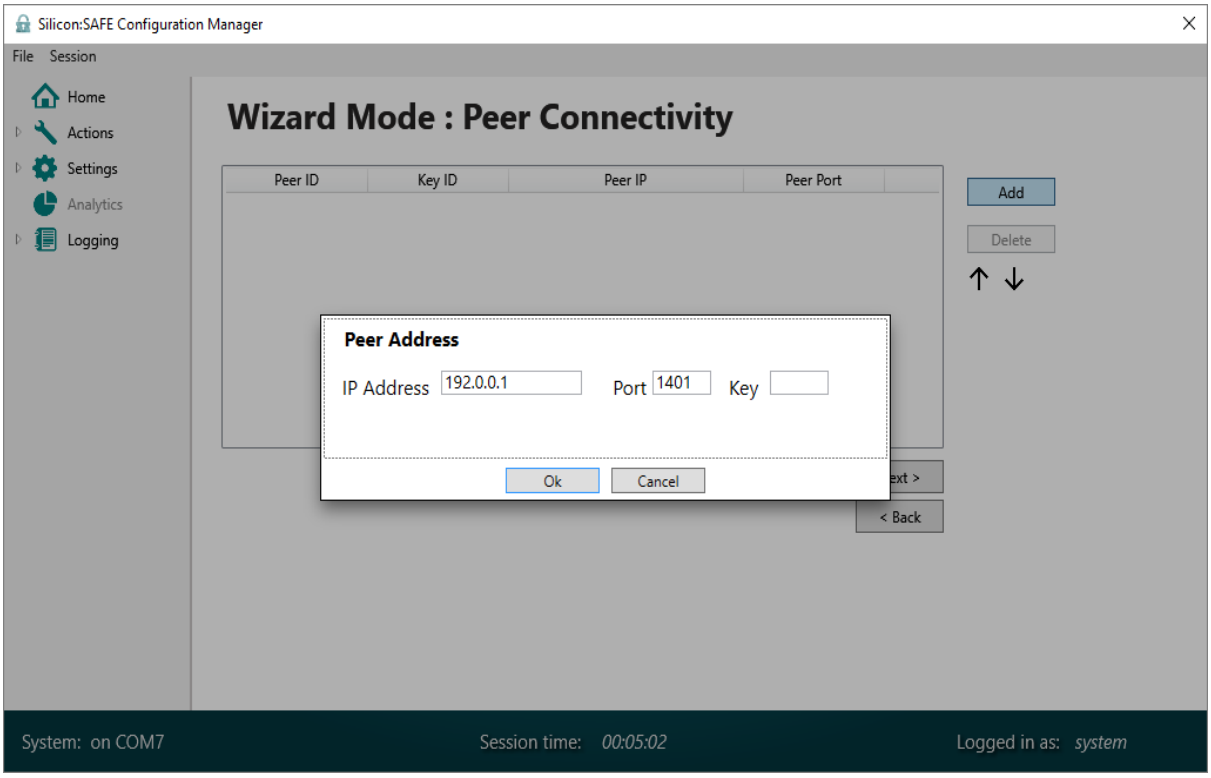

Figure 22 - Adding a peer to the peer table

The last stage is to enable the services. The Authentication, Replication, and Configuration services can all be controlled independently. Only enable a service when the appliance is ready to use it. It is a good idea to enable the Configuration service at the end of the wizard, but the other services can be left disabled at this stage and enabled later during ad-hoc configuration.

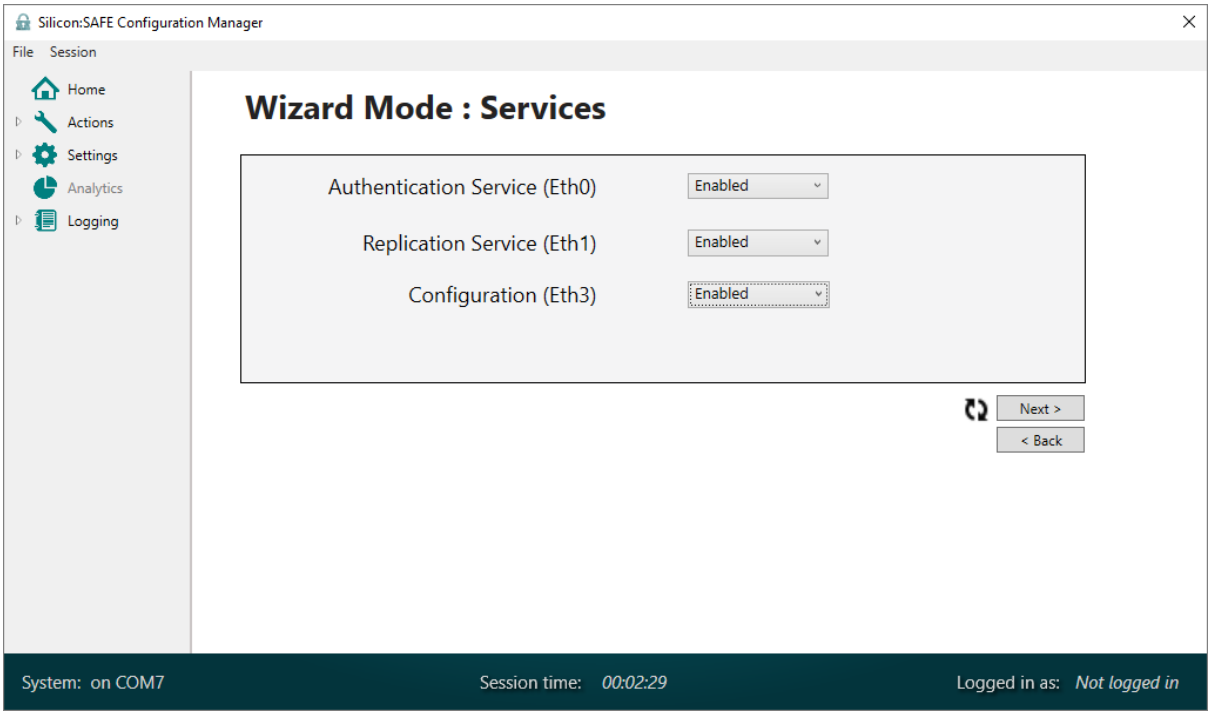

Figure 22 - Enable the services for the Password:Protect appliance

Appliance ad-hoc configuration

The Password:Protect Windows Configuration Application can also be used to perform ad-hoc configuration of Password:Protect Appliances.

The management of a Password:Protect unit is split into two roles. The role of the admin, and the role of the system user.

Note: unless otherwise stated, any change to settings will need to also be made to each Appliance in the cluster.

Admin

The admin user is designed to be the individual in control of user space, the repository and its maintenance. Once logged in as admin, the Configuration Application will highlight the functionality that can be performed as admin user. Other actions associated with the system user will be greyed.

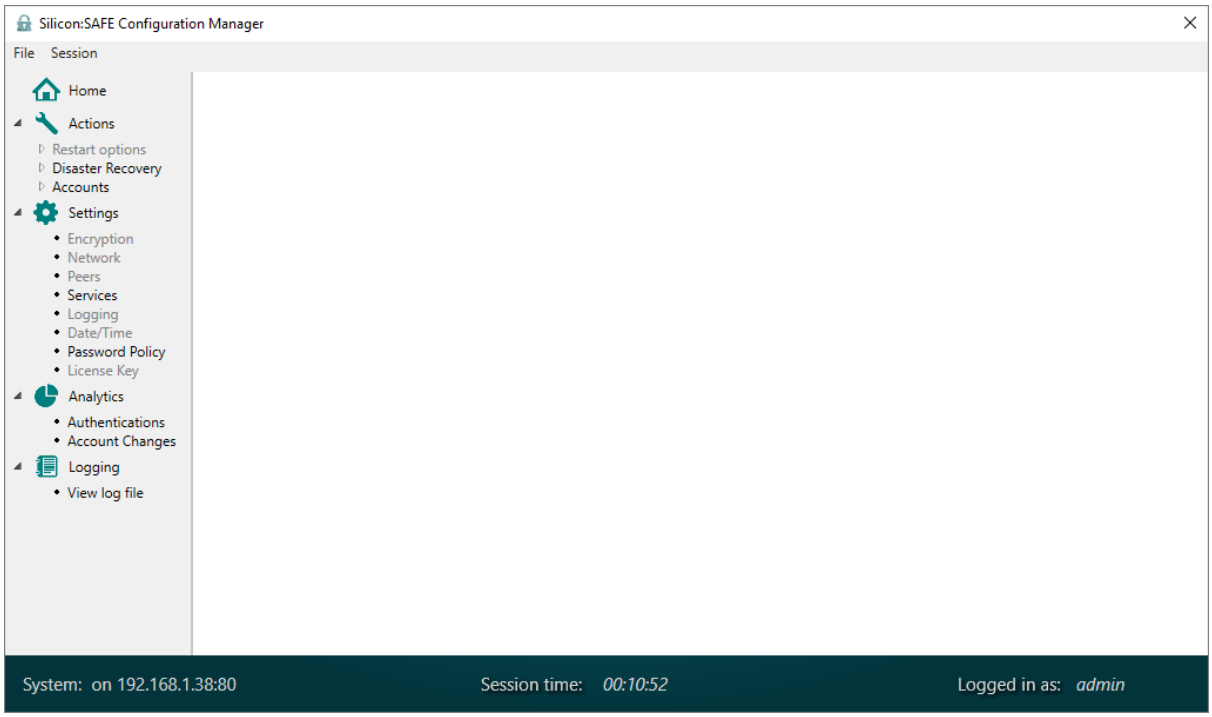

Figure 24 - Configuration menus available to the Admin account

The admin user has permissions to suspend/delete accounts, reset passwords, and control the disaster recovery process in the rare eventuality that an appliance fails (this is covered in the Trouble Shooting section).

The following pages are also available to the admin user:

Update Admin Password:

The old password is required.

Password Policies:

This page is similar to that in the first time setup wizard.

Services:

This page, similar to that in the first time setup wizard and allows services to be enabled/disabled. In addition, the page allows the level of error reporting for the Authentication Service to be either:

Verbose: This will return success (y) or the reason for fail
Restricted: This will only return success (y) or fail (n)

For the three services: Authentication, Replication and Configuration, Ethernet connection White Lists can be setup.

Analytics:

There are two pages:

- Authentications: This page displays the accumulative number of successful and unsuccessful authentications.
- Account Changes: This page displays the accumulative number of successful account creations and deletions

Logging:

This page displays the events for the given range of time. All or some of these events will be displayed in the Syslog, but this will depend on how the Syslog has been configured (covered in the "Settings->Logging:" section.

System

The system user is designed to be the individual responsible for managing the network infrastructure and as such, the deployment of the Password:Protect Appliances. Most of the settings from the wizard are available to the system user post setup.

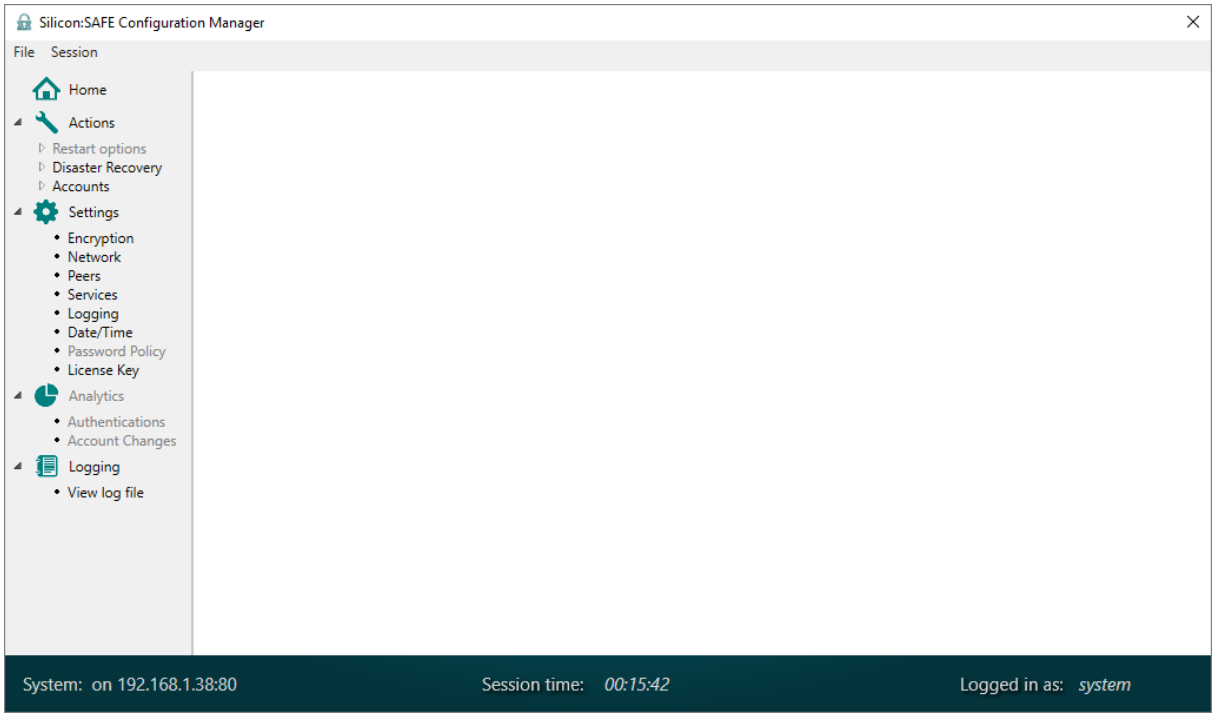

Figure 25 - Configuration menus available to the System account

The Configuration Application will highlight the functionality that can be performed as system user with other functions greyed.

In addition to the pages that appear in the first-time setup wizard, the following pages are also available to the system user:

Update System password:
The old password is required.

Settings->Logging:

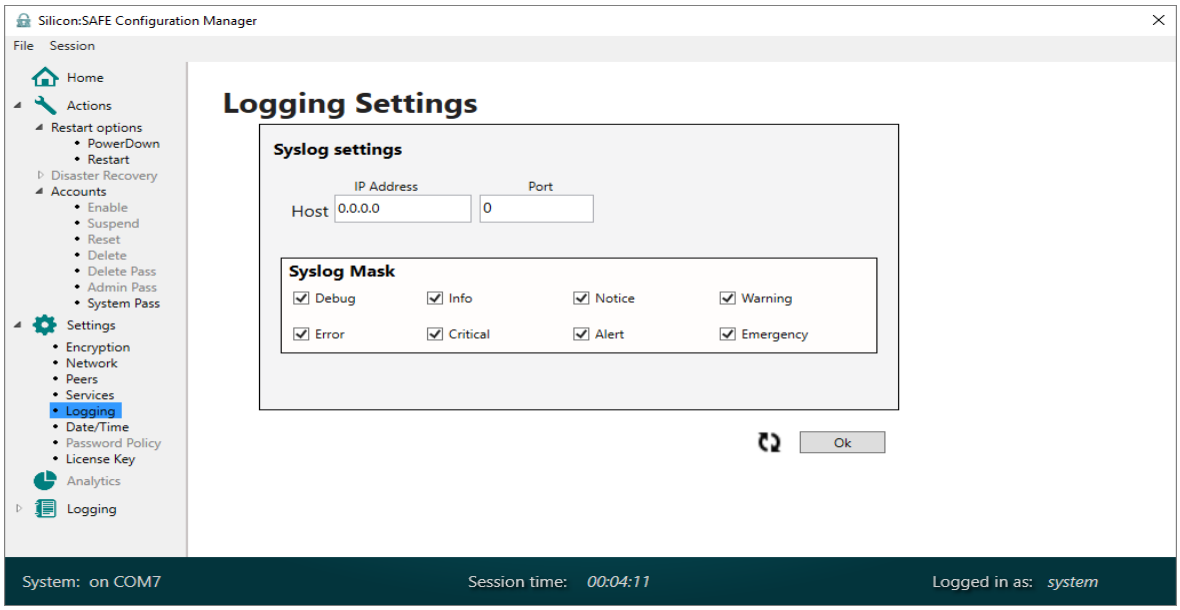

Figure 26- Logging settings

This page provides the IP address and port setting for the Syslog monitor.

The mask provides the selection of what event logs to be sent to the Syslog monitor. By default all events of severity Error or higher are sent to the Syslog monitor.

Logging:
The same page as under admin user

Restart Options:
This allows the appliance to be powered down or restarted. In both cases, the system password is required.

Workflows

Changing network settings

The network setting for an Appliance can be modified by connecting to the configuration port.

Login as a system user.

Using the Settings->Network page, the IP addresses and ports can be modified. Commit the change. It is not necessary to restart the Appliance.

Then for each of the peers of this Appliance, the Peer IP address for the modified Appliance will need to be changed:

Connect to the configuration port and login as system.

From Settings->Peers, modify the appropriate peer address. Commit the change.

From Actions->Restart options->Restart, restart the Appliance.

Changing Encryption settings

To maintain continuity, the deprecated encryption key should be deleted only after all the appliances in the cluster have the new encryption key configured and the server/requestor(s) have been modified to no longer use the old key.

Connect to the configuration port and login as system.

From Settings->Encryption, add the new key(s). Note, within an interface e.g. (Eth0) the key id should be unique. Commit the change.

Adding an Additional Appliance to a Cluster

Configure the Appliance using the first-time setup wizard. However, leave the services all disabled.

On creating the repository, the number of passwords/secrets and those which are hashed should match those for the other Appliances.

The password policies/white lists for the new Appliance should match those for all Appliances in the cluster.

The Peer IP address for the new Appliance will need to be added to the peer table for all the other Appliances in the cluster:
For each of the existing Appliances, connect to the configuration port and login as system.
From Settings->Peers, modify the appropriate peer address. Commit the change.
From Actions->Restart options->Restart, restart the Appliance.

If new encryption keys are given, these should be set on all Appliances in the cluster.
If the repositories in the existing cluster contain accounts then use the Disaster Recovery mechanism (see below) to populate the new Appliance with the accounts from one of the existing Appliances in the cluster. Remember to enable the services on the new Appliance when you are ready.

Trouble Shooting

All events are recorded in the event log and can be seen in the Logging pages of Password:Protect.

Events will include:

- PSU module failure
- Fan failure
- Temperature events
- Disk Events
- Other Events

PSU Failure

A PSU failure is relatively simple to rectify – the PSU used is a hot-swappable redundant unit and fails-over to a backup until the faulty unit is replaced.

Fan Failure

The fans are located inside the enclosure and there is no access to them without removing the lid – this triggers the Intrusion system. A fan replacement will require a Silicon:SAFE service engineer to replace it. The unit will have to go off-line for a short period of time while the fan is replaced. There are however 3 fans built in for redundancy – a single fan failure is not a critical event.

Temperature Events

There are two different temperature events, one a warning, one an alarm. A warning will occur if the ambient temperature changes by more than 2 degrees in 60 seconds, and an alarm will occur if it reaches more than 60 C degrees.

Disk Events

Failure to read and write data to Disk will generate critical events

Other Events

These events include Appliance start-up, internal communication errors and invalid connection attempts. Many of the errors that are generated by the Authentication Service are also displayed as events.

Notification of Events

In addition to the logging pages of the GUI, events are displayed:

If configured, the Syslog server can receive events.

Audible Sound: A buzzer will sound when events have a severity of critical or above. These will include:

- Unable to initialise or format Disk
- Appliance Restart
- Box Tamper

Disaster recovery

Though it is unlikely to ever happen, there is a provision built into the Password:Protect Appliances to allow a replacement Appliance to populate its repository from another Appliance in the cluster.

The new Appliance will need to be taken through the first time setup wizard to configure all the settings to the same values as the failed unit, but the services should not yet be enabled. The disaster recovery procedure then needs to be started from the Password:Protect Windows Configuration Application for both the unit acting as the source, and the unit to be restored. The admin account will need to be used to connect to both Appliances to begin the process.

The source and destination IP addresses and ports are those of the Repository of either Appliance. The cipher dropdown box enables one of the pre-configured keys to be used for encryption, it is important that both units use the same key! The import should be started before the export, and then both Appliances can be left to complete the process, with progress bars viewable in the Windows Application.

The recovery process will take some time, especially for large repositories!

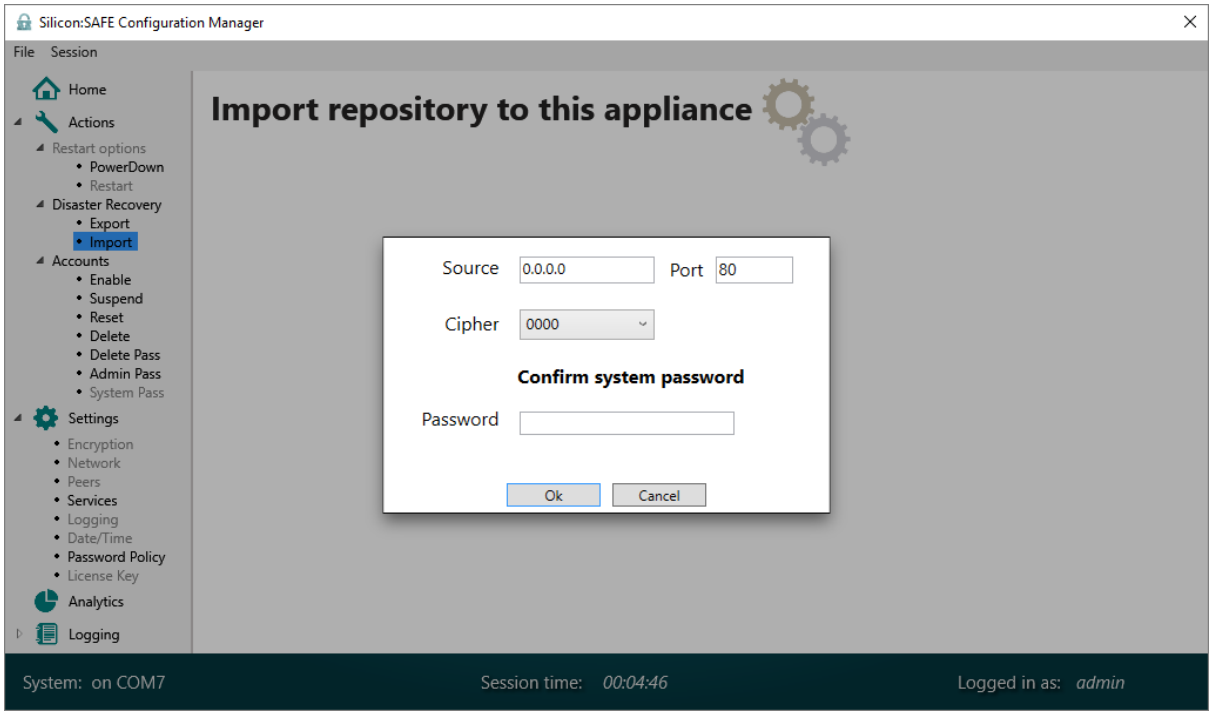

Figure 23 - Disaster recovery slave

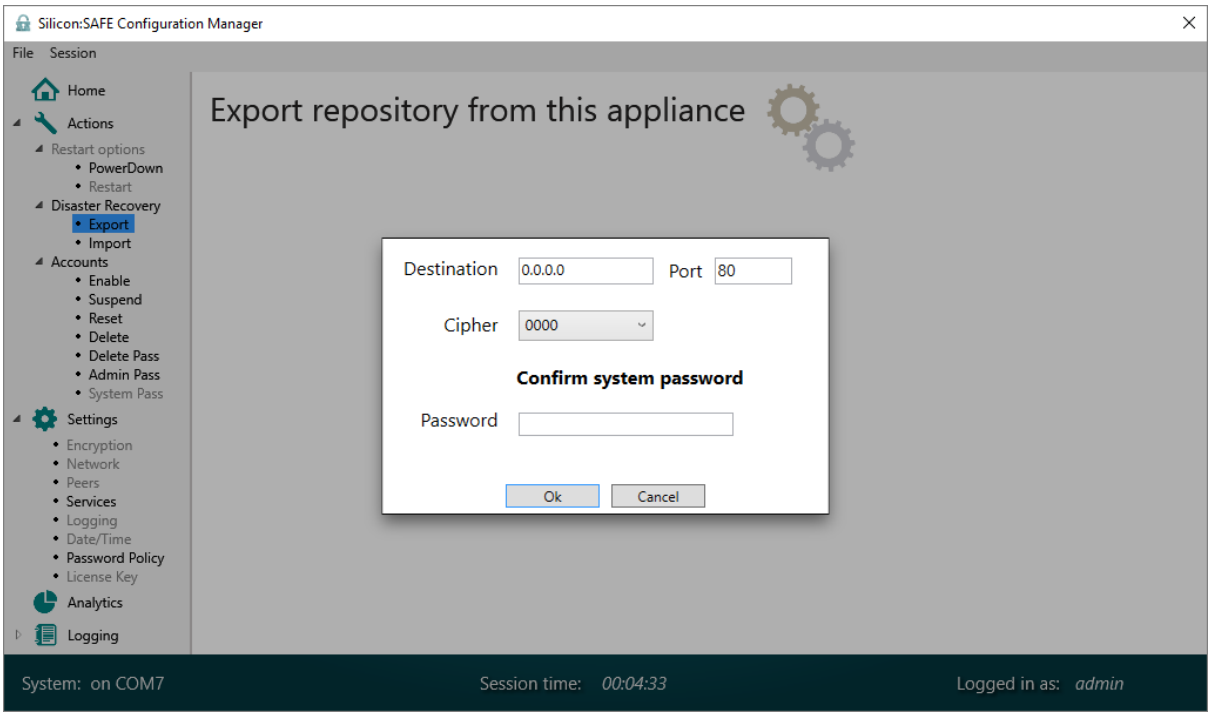

Figure 24 - Disaster recovery master

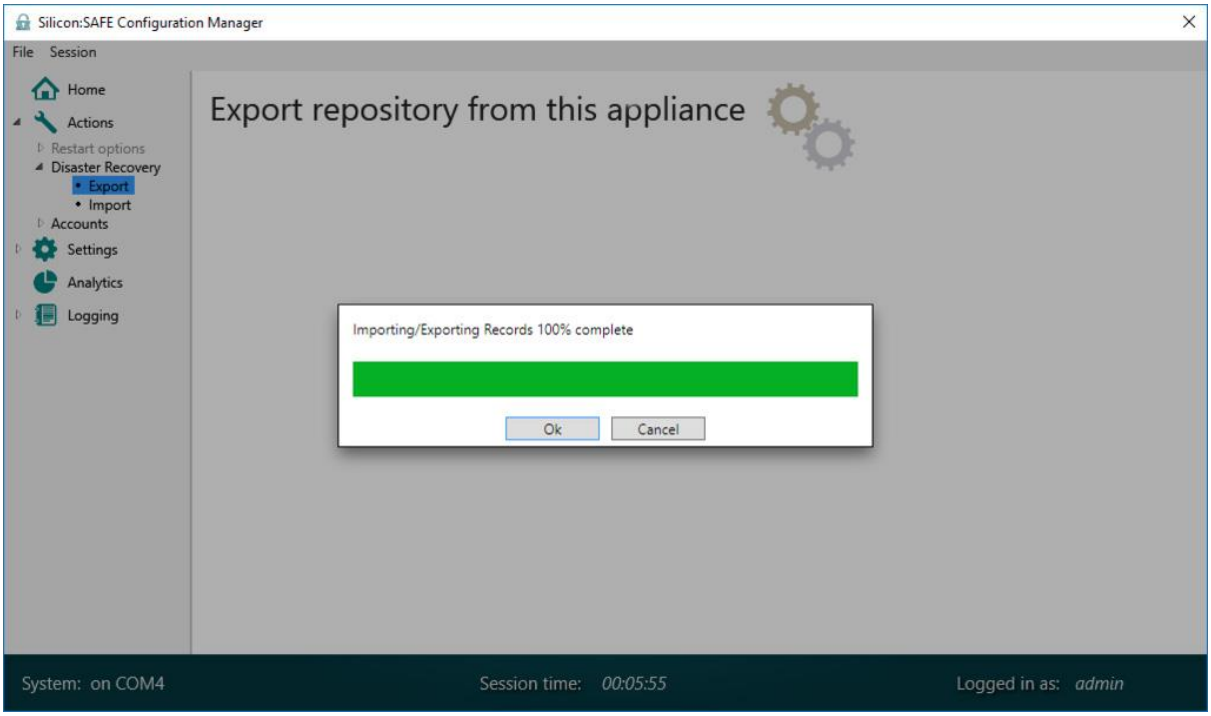

Figure 25 - Disaster recovery

Appendices

APPENDIX I. Example deployments

4 Appliance multi-master setup

The multi-master setup is one of the simplest ways to achieve high throughput and resilience. When behind a load balancer, a cluster of Password:Protect units can share the incoming requests.

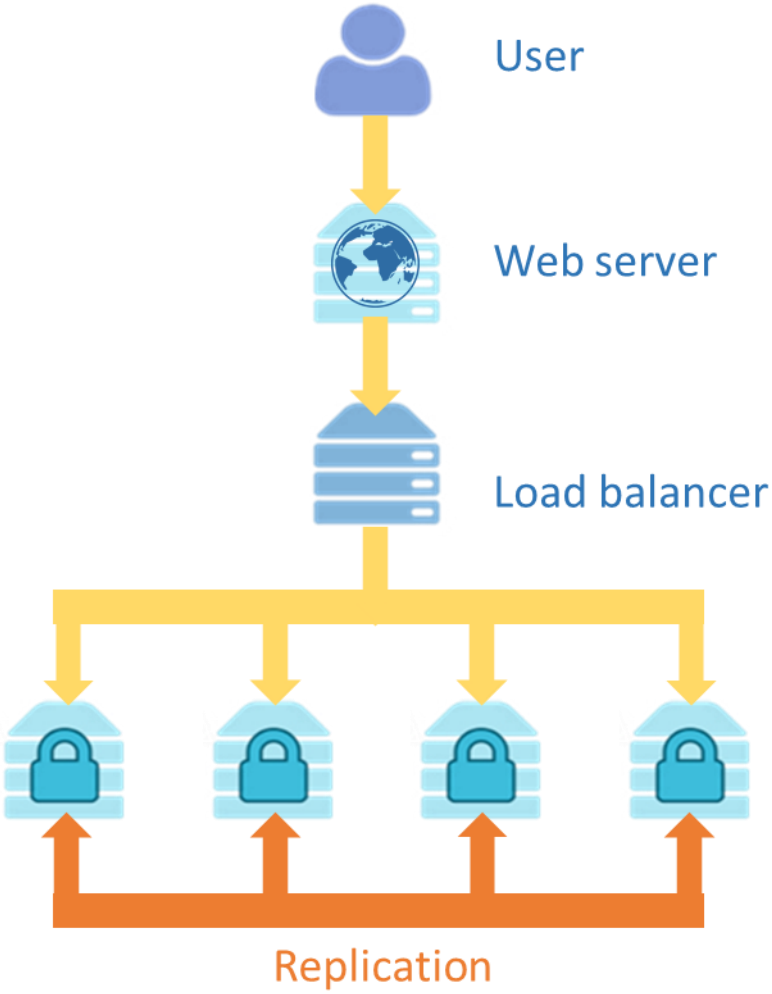

Figure 26 - Multi-master setup

Because accounts are replicated to each Appliance in the cluster, any appliance can be used as a live authentication device.

The setup for this arrangement is quite simple; all four Password:Protect Appliances share exactly the same settings (save for IPs and MAC addresses) and each peer is defined in the peer connection table.

Striped setup with slave backup

An alternative to a multi-master setup is the use of data-striping. User accounts are spread across several clusters according to a user defined algorithm. A crude algorithm would be store accounts with usernames between A to M in one cluster and O to Z in the other). The webserver will check the username and connect to the appropriate cluster. The master-slave arrangement within each cluster

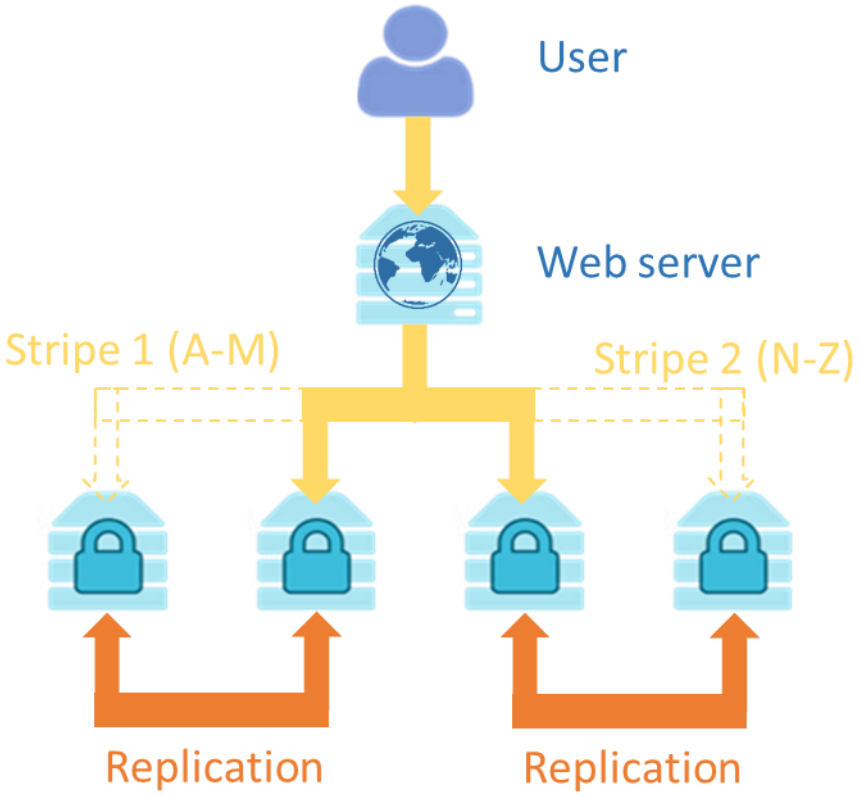

Figure 27 - 2 data stripes, with backup and failover protection

provides failover protection.

When configuring this arrangement, the majority of settings will remain common through all of the Password:Protect units, but each pair will have to have their peers set so as to back up in the master/slave arrangement, and the backup units will have their Authentication services disabled unless they are required to replace the master.

Striped setup with multi-master

Combining multi-master and striping approaches can be used to maximise throughput of a system. This is the suggested approach for customers with greater demands in terms of authentication rate.

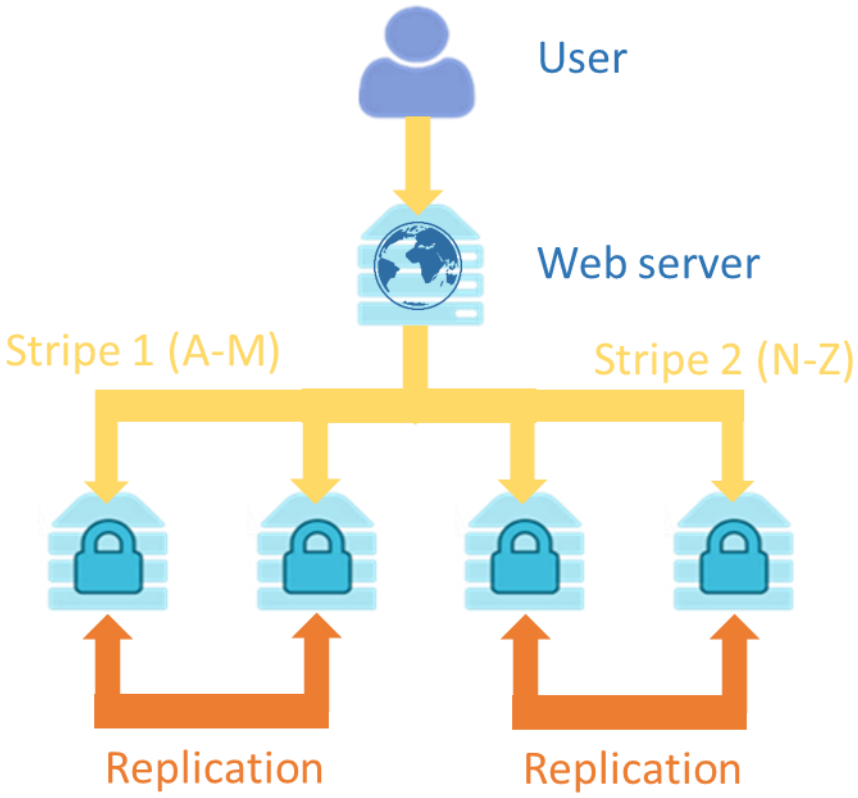

Figure 28 – Striped setup with multi-master stripes.

Each stripe now has two live master Appliances which it can use, and these Appliances replicate account creations and changes to each other.

Connection logic will need to be implemented on the web-server so that it uses both of the units on either stripe, but a load balancer could be introduced that would allow up to 8 Password:Protect Appliances in each stripe (the maximum allowed in each replication group/cluster). This – alongside making more, smaller stripes – allows for near infinite scalability so as to cover all levels of demand.

As ever, all Appliances share settings apart from IP and networking settings, so that the password policy/time/Syslog server/encryption etc. is consistent. All services will be enabled, as all Appliances are live and not simply a backup, and peers will replicate only to other appliances within their stripe.