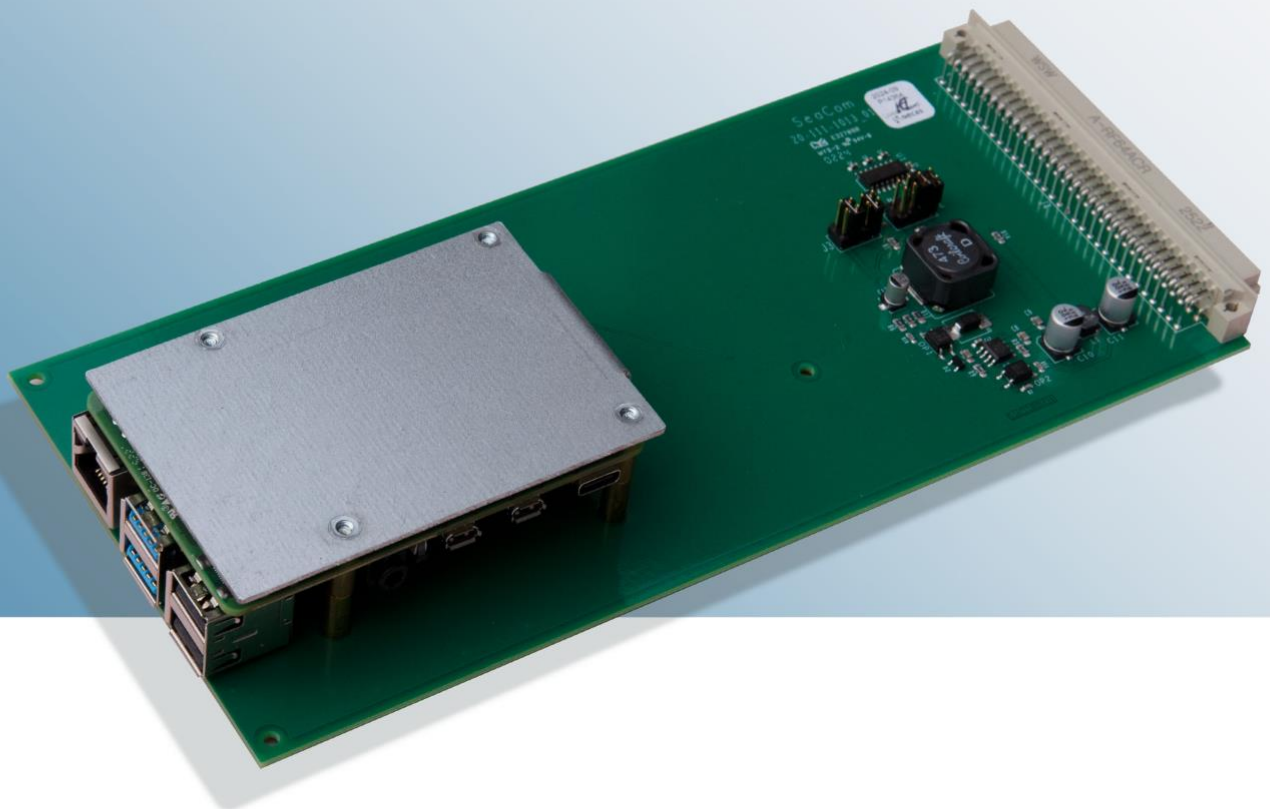


LSP CS

OS 03.00 Manual



The LSP CS is running our Cyber Secure version of Linux OS03.00. It s used as the central processor of our PABX systems. This manual covers the use of the OS 03.00 and its Cyber Security capabilities.

TMN20250520CJ01_W02 LSP OS03.00 Manual

1. Introduction

The Alphaconnect / SeaCom PABX systems need a Central Processor to be executing the Central Processor software. For this we are using a Raspberry-Pi5, a power-full single board mini computer.

The package of hardware and OS (operating system) we call the LSP (Linux System Processor). And when the operating system is rev 03.00 we call it LSP CS, CS standing for Cyber Secure.

The LSP need a carrier board for physical mounting and for its power supply. For the Alphaconnect / SeaCom 3000 the LSP is carried on the internal backplane, and for our 19" PBX systems, the LSP is carried on the CP3 card.

The subject for this manual is how to use the LSP CS with OS 03.00, and how to use the Cyber Security capabilities of this OS.

Below an overview of the content of this short manual:

- Quick guide in how to connect the LSP
- Overview of the Cyber Security
- Using the OS

1.1 The LSP

The LSP is a credit card sized computer.



1.2 Specifications

- Credit card sized
- Processor Broadcom BCM2712
- 2.4GHz quad-core 64-bit Arm Cortex-A76
- SDRAM 4GB
- USB 3.0 ports,
- Gigabit Ethernet
- Power consumption 2W

1.2.1 Ports

The main ports are the Ethernet port and the USB ports.



1.3 Hard disk

The OS is stored in the 32 Gbyte micro SD card. This card is removable for service and development purpose, but will normally not leave its slot in the LSP.

The SD card is divided into 3 partitions:

- Boot partition 512 Mbyte
- OS 16 Gbyte
- Data 12 Gbyte

1.3.1 Boot and OS partitions

These partitions are used for the Linux operating system. They are both write protected by an overlay file system. This mean that whenever the LSP is restarted, the OS returns to its factory default settings.

1.3.2 Data partition

The data partition holds data that should not be restored to factory default after a reboot. This is for example the customized log files and the data used by the telephone system itself and user names and passwords.

2. Quick guide to OS 03.00

This chapter gives a quick introduction to how to use the LSP with OS 03.00.

Make your first login, get access to the PABX configuration files and set up a VNC debugging using SSH tunnel.

These steps are all you need for the basic use of the system.

How to make Cyber Security will be described in the following chapters.

2.1 Connecting to a network

The LSP is connected to an Ethernet as any other computer or network device. The LPS act as a DHCP client, meaning that the network must offer an IP address.

The addresses distributed by the server MUST be in the range 192.168.x.x

2.2 NTP

It is essential for the Cyber Security system that access to NTP (Network Time) is given, so the local network must have an NTP time server or give access to 0.dk.pool.ntp.org via an internet connection.

2.3 SSH

The heart the OS 03.00 security capabilities is SSH (Secure SHell).

Secure SHell is a cryptographic network protocol used to securely access and manage devices over an unsecured network.

It allows users to log into another computer remotely, execute commands, and transfer files. SSH encrypts the session to prevent eavesdropping, connection hijacking, and other attacks.

Authentication is done with user name and password, and the SSH protocol features secure file transfer and tunneling, which we will see how to use later in this manual.

2.4 Service computer

All tasks are carried out from a service computer connected to the same local network as the LSP. In the following all screenshots and examples are related to a computer running Windows.

2.5 Tool software

To access the OS 03.00 we need some tool software running on the service computer. Except for the PingTool they all relies on the security capabilities of the SSH protocol.

- PingTool
- Putty
- WinSCP
- WinVNC

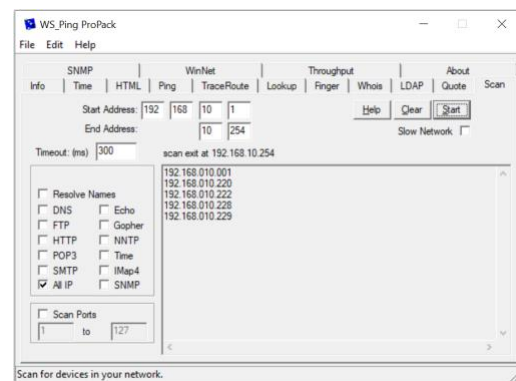
These tools are well known freeware and can be downloaded from the web or from

www.seacom.dk/products.

2.5.1 Ping Tool

Wspingpr.exe

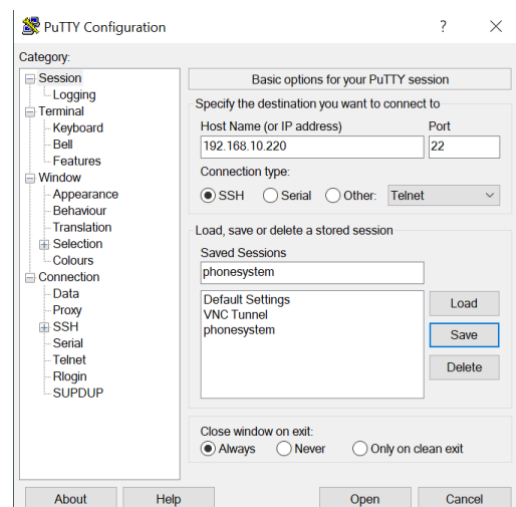
This is a nice to have tool for finding computers on a network.



2.5.2 Putty

Putty.exe

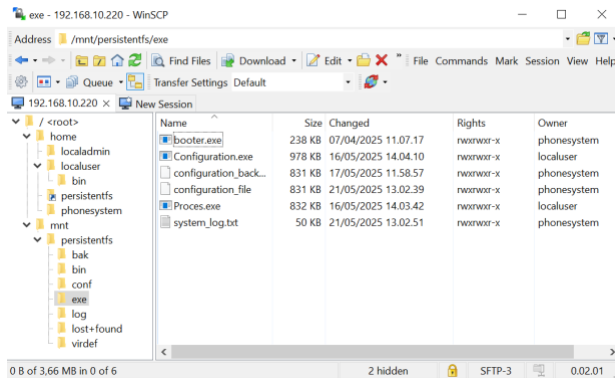
This is an SSH terminal window software.



2.5.3 WinSCP

WinSCP.exe

This is a Secure File transfer tool using SSH for authenticating users and encrypting data when transferred:



2.5.4 VNC Viewer

VNC.Viewer.exe

This is a remote desktop client that can connect the VNC server on the LSP via an SSH tunnel.



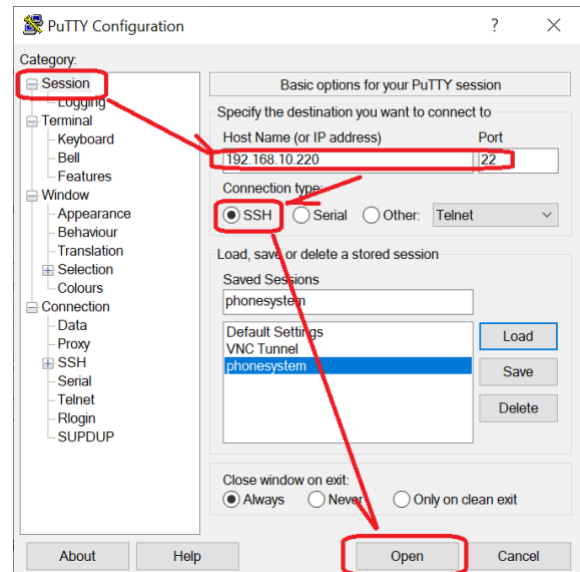
2.6 Finding the IP address of the LSP

The first thing to do is to find the IP address of the LSP. Start by having NOT connected the LSP to the network.

Then use the Ping Tool to scan the network for active devices. Remember or write down the list. Next connect the LSP and wait a couple of minutes. Then again use the Ping Tool to find which address was added. The address added is likely to be the LSP.

2.7 First time login using Putty

Now start up Putty on the service computer, and enter the IP address of the LSP:



Press open.

You should now see a login window prompting for first a user name and then a password.

When the LSP comes from factory, there is only one user and one password:

Username: **localuser**

Password: **13qe!#QE**

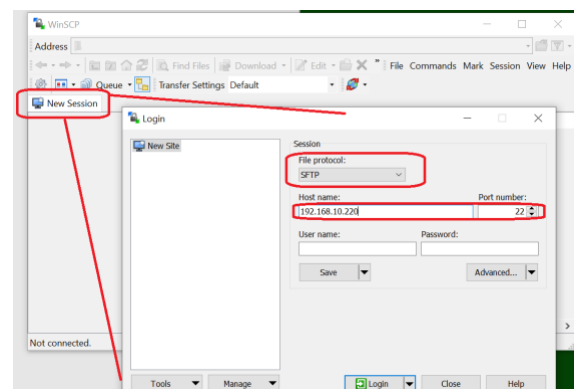
Now you are logged in as **localuser**

Use command **exit** to close down the connection.

2.8 Log in using WinSCP

In order to access the files that are used for the PABX Central Processor, we will need to log in using WinSCP.

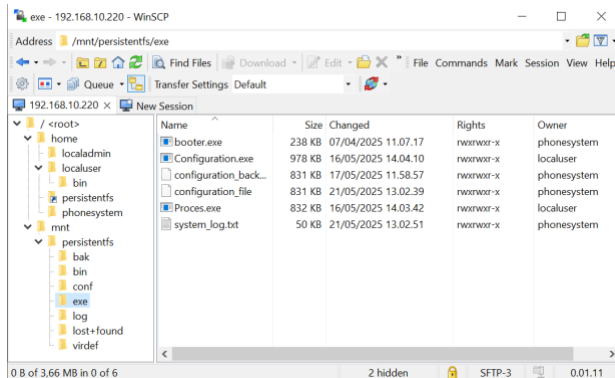
WinSCP is a Windows implementation of the Secure Copy. The SCP is a part of the SSH suite, and we can securely make file transfers between the LSP and the service computer.



Press LOGIN and You will be prompted for user name and password:

Username: **localuser**
Password: **13qe!#QE**

When logged in using WinSCP You will see a browser window like below.



Navigate to: **/home/persistentfs/exe**

Here you will find these files:

Name	Size	Changed
booter.exe	238 KB	07/04/2025 11.07.17
Configuration.exe	978 KB	16/05/2025 14.04.10
configuration_back...	831 KB	17/05/2025 11.58.57
configuration_file	831 KB	21/05/2025 13.02.39
Proces.exe	832 KB	16/05/2025 14.03.42
system_log.txt	50 KB	21/05/2025 13.02.51

You are familiar with programming the SeaCom systems, so you will see the files that you already know.

Copy out the **Configuration.exe** and the **configuration_file** to a work folder on the service computer. Now launch the Configuration.exe on the service computer and create the required updates to the configuration_file. Remember to save the result as **configuration_file_new**.

Go back to the WinSCP and copy over the **configuration_file_new** to the LSP.

The file will quickly be erased again, showing that it is accepted by the PABX CP system. Use F5 to refresh the file list.

This is basically all that we need to program and install a PBX system.

2.9 Using SSH tunneling of VNC

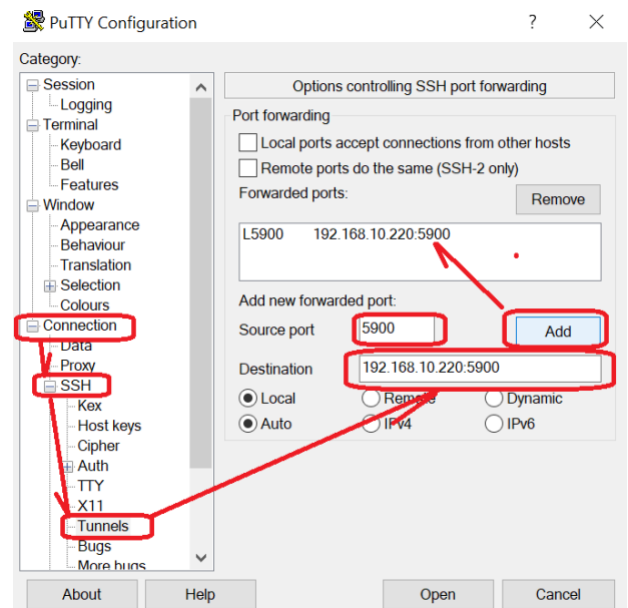
When installing and commissioning a PBX system, then it is nice to have a remote desktop connection to the LSP.

Fortunately this is also possible via SSH using the tunnelling, which is a part of the SSH suite.

In this way we can use the fully Cyber Secure SSH protocol to set up a remote desktop.

Open Putty and find the left side page. Connction/SSH/Tunnels.

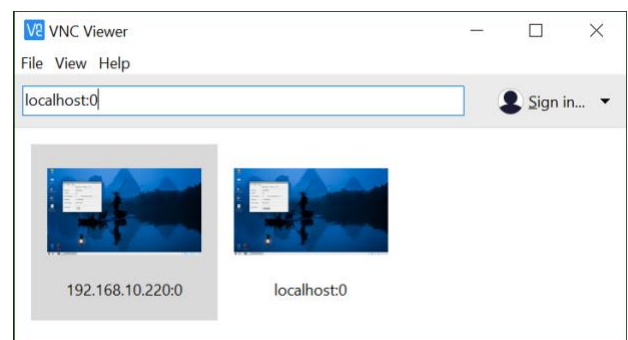
Enter the IP address of the LSP and use port number 5900 which is the port used by VNC.



Press Open and you will be prompted for user name and password:

Username: **localuser**
Password: **13qe!#QE**

Then open the VNC-Viewer on the service PC, and now use **localhost:0** as target.



You will be prompted again for user name and password:

Username: **localuser**
Password: **13qe!#QE**

The remote desktop should show up.

3. Cyber Security

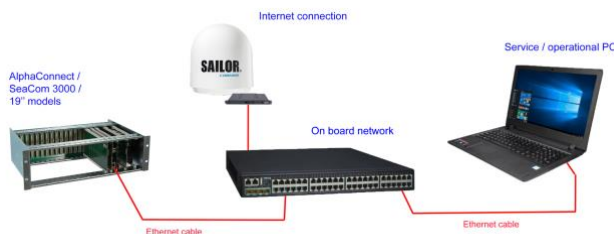
The remaining part of this manual covers the features and capabilities of the OS 03.00 with respect to Cyber Security.

This chapter gives an overview of the Cyber Security strategy and its components.

The following chapters will describe how each part shall be used and configured.

The OS 0300 is our cyber secure operating system. It can be used by the newest Alphaconnect Classic and the CP3 card in 19" systems.

With this OS we are able to securely participate in networks like the one shown below:



The PABX systems can be permanently connected to the on board network, allowing for both local on board service, as well as remote service via a satellite internet connection.

This is possible due to a completely rearranged and updated version of our LSP and the operating system: OS 03.00

3.1 Components of the CS strategy

Cyber Security is obtained by a set of functions and features installed in the OS 03.00:

- Firewall
- User management
- Enforcement of strong user passwords
- 2 person authentication for remote access
- SSH (Secure SHell)
- SCP (Secure Copy)
- Encrypted communication
- Malicious code detection
- Intrusion detection and blocking
- System audit and reports
- Event logging
- E-mail alerts
- Write protected OS
- Strategy for system backup and restore

The following paragraphs describes each part of the strategy.

3.2 Fire wall

The OS 03.00 has a firewall installed. The firewall is set up to completely block all network traffic, except for local access to SSH at port 22.

With this we make sure that nothing, except SSH from local on board computers, will be accepted by the LSP.

The system administrator is given the option to open the firewall temporarily for external SSH and for a local VNC when needed.

The firewall is also used by the security module **fail2ban**, to enforce blocking of IP addresses when suspicious activity is detected.

3.3 User management

A user management system is used. This allows for adding users with real names, and thereby make a much better logging of acts and behaviors. When managing users, it is essential opening only access to parts of the system that each user has the privileges to visit.

The use of personal names for login instead of shared names like "administrator" gives a much stronger recording of user activities and makes users behave more responsible.

Users are given the right to access the **exe** folder, and to use WinSCP for modifying the PABX configuration files. Nothing else.

3.4 Administrator

A user can turn into administrator provided the password is known.

The administrator can use the user management system, open the firewall temporarily for external SSH access and read and analyze the log files.

3.5 SSH

All access to the system goes via the Ethernet port using SSH (Secure Shell). SSH is a network protocol that provides administrators and users with a secure way to access a remote computer over an unsecured network. SSH uses encrypted user authentication and data transfer.

The SSH is a command line interface. There will be no graphical user interface and no browser based administration.

3.5.1 Users and user authentication

The SSH protocol includes a user name/password authentication when logging in.

The below rules for passwords are in force:

- Strong passwords with length of min 8 chars and two character classes.
- Minimum password complexity
- Blocking on 3 unsuccessful login attempts

- Log in notifications are sent by e-mail to system administrator.

3.5.2 2-person authentication

When the system is to be accessed from remote via unsecure networks, not only 2 factors, but 2 persons need to be involved. The administrator on board will need to manually open the firewall for external access, with a 2 hour timeout, and the external user need to use own credentials for logging in to the now 2 hours open system.

3.5.3 Encryption

SSH uses strong encryption algorithms to secure the data exchanged between the client and the server. A public key system is used.

3.5.4 Secure Data Transmission

SSH encrypts the entire session, including login credentials, commands, and the output sent back from the server.

3.5.5 Remote Command Execution

SSH will give you a command line window for both local network and remote connection.

3.5.6 SCP

A part of the SSH suite is SFTP (Secure File Transfer Protocol). This allows for secure log in and secure file transfers over unsecure networks. The file transfer is needed to be able to update the telephone system configuration file.

3.5.7 Tunneling

Running VNC remote desktop is possible in a secure way by using the tunneling feature of the SSH protocol. Once You have set up the secure SSH connection, a VNC remote desktop can be launched, communicating via the SSH encrypted communication, using the tunneling (port forwarding) feature.

3.5.8 Brute-force protection

SSH is set up to limit number of login attempts to 3 whereafter the user is blocked for 10 minutes. This will make automated log in trials very slow.

3.5.9 Session time-out

A session timeout is closing down an SSH session when idle for more than 10 minutes

3.6 Malicious code protection

Once every week, we are running a scanning of the full OS in order to detect if any malicious code should have been introduced.

Alerts are sent by e-mail to system administrator in case infections are found.

3.7 Intrusion detection and blocking

A **fail2ban** system is in use. This system is set up to monitor suspicious activity on the network, and if detected, the IP address from which the attack is coming is banned in the firewall for a period. These are the rules

- 5 failed SSH logins bans for 1 hour
- Repeating offenders will be banned permanently
- Syn-flood banned for 1 hour

5 failed login attempts will ban the IP address for 1 hour. If the same address tries to login more than 5 times but fails, the address will be permanently banned.

On a syn-flood attack, the address will be banned for 1 hour.

3.8 Audit records

An audit logging system is installed. This allows for detailed tracking of events in the system.

The system is set up to monitor core files and folders in the OS:

- /etc - configuration files for the system and installed applications.
- /bin - core command line utilities for booting the system
- /sbin - core administrative executables
- /usr/bin - user programs like nano, crome
- /usr/bin/sudo - sudo usage
- /etc/crontab - timed actions file

The audit system logs detailed information on events in the monitored folders into the **/var/log/audit/audit.log** file.

A regular scan of the audit log is carried out by a script file that analyses and reports to the **audit.log** file and sends an e-mail alert if issues are found. When issues are found, the system administrator is given right to read the log files and to do a more detailed study of the suspicious events.

3.9 Event logging

A set of OS 03.00 specific log files are found. In these files we log these events:

- System boot
- Adding, deleting users
- Users log in via SSH
- Changing the firewall
- Log file storage low
- Virus scan reports
- Banned network activity
- Audit events summary
- Update of the telephone configuration file

3.10 E-mail alerts

OS 03.00 send signals about events via e-mail to the administrator on board the vessel.

The below events are alerted via e-mail:

- System boot
- Users log in via SSH
- Log file storage failure
- Virus detected
- Banned network activity
- Audit events

3.11 NTP for keeping time

The validity of the timestamps on log records is ensured by using the NTP protocol to read time from an internet time server. All timestamps are UTC.

3.12 Write protected OS

The OS 03.00 is installed on a disk with a file system overlay. This means that the system can be restored from a cyber attack simply by rebooting the system.

Updates to the system, like adding users and modifying crontab etc. will be in force until a system reboot is carried out. After a reboot, the factory version of the OS will come into operation again. There are methods of making changes persistent.

3.13 Backup and restore after a cyber attack

When the system is finally installed on board, a full backup of the complete system can be made using a disk imager software like **Win32_disk_imager**. This is an easy a manageable way of making a complete system backup including the telephone system configuration file.

4. System management

This chapter describes how to access the system for installation and daily management, and it gives an introduction to the tools installed for Cyber Security purposes.

4.1 Users

Log in to the system is always done using a user name/password. The system comes with a default user installed:

User: `localuser` Passwd: `13qe!#QE`

Users are to be installed by their real names, and they must update their password to an own chosen password. Users have rights limited to access to the `../exe` folder holding the PABX CP software and configuration.

4.2 Administrator

A user can take administrator rights by first logging into own user account, and then a log in to user `localadmin` using the command `su - localadmin`

Factory credentials are:

User: `localadmin` Passwd: `1q2w3e!Q"W#E`

It is not possible to add more administrators, and it is not possible to log in to the `localadmin` directly via SSH or SCP.

Administrators are given all rights.

The following paragraphs describes tools that can be used by administrators only.

4.3 User management

The administrator can add users to the system. It is strongly recommended to add users on real names, rather than just using the default `localuser` as a shared user name.

The below commands are available to the administrator:

- `user_add <name>`
- `user_delete <name>`
- `user_disable <name>`
- `user_enable <name>`
- `user_list`

Default password for a new user is: `13qe!#QE`

The new user should change this immediately on the first login by issuing the command: `passwd`

4.4 Managing SSH sessions

The administrator can manage SSH sessions using these two commands:

- `ssh_show`
- `ssh_killall`

4.5 Firewall management

Commands are given to the administrator for managing the firewall:

- `fw_opensshremote`
- `fw_openvnclocal`
- `fw_close`

`fw_opensshremote` will open the firewall for SSH at port 22 also for IP addresses outside the local area network 192.168.x.x.

There is a 2 hour timeout whereafter the firewall will return to its default state.

`fw_openvnclocal` will open the firewall for VNC at port 5900 for local address IP's 192.168.x.x.

There is a 2 hour timeout whereafter the firewall will return to its default state.

`fw_close` is the command for returning the firewall to its default rules, which is open to local IP addresses SSH on port 22 only.

4.6 Inspecting log files

OS 03.00 specific log files are stored in the folder `/home/persistentfs/log`. This is in the persistent disk partition, so log files will stay also after rebooting. The files can be downloaded to the service computer by WinSCP and be inspected by a normal text editor.

4.6.1 OS 03.00 custom log files

The below log files are found:

- `boot.log`
- `usermanagement.log`
- `user_login.log`
- `firewall.log`
- `diskspace.log`
- `virscan.log`
- `fail2ban.log`
- `audit.log`
- `configuration.log`

4.6.2 Audit log file

The audit system track detailed information about file changes in selected core OS folders.

The raw log file is stored in `/var/log/audit/audit.log`

The audit system includes a tool: `ausearch` used to search in the log file for specific events.

Example: `sudo ausearch -ts today` shows events from today. Using `ausearch` is beyond the scope of this manual.

4.7 E-mail alerts

The person being administrator shall be able to receive e-mails from the system. This is the only way notification, alarms and alerts are send out.

The e-mail address is configured in the file:

`/home/persistentfs/conf/email.conf`

Its content look like:

```
#This is where to enter the e-mail address of the administrator
EMAIL="info@seacom.dk"
```

The OOS 03.00 sends e-mail alerts to the administrator on these events:

- System boot
- Users log in via SSH
- Log file storage failure
- Virus detected
- Banned network activity
- Audit events

The administrator need to take care when such an e-mail is received.

This chapter describes each alert and describes how to handle the alerts.

4.7.1 System boot

ALERT: Reboot on <hostname>

The system shall not reboot under normal operation, so a reboot alert is a warning that something is wrong, maybe with the power supply of the system.

4.7.2 Users log in via SSH

LOGIN: <user name>

Information about a user logging in to the system. This will be OK, if we know that service work is in progress, but not OK if we don't expect anyone to log in.

4.7.3 Log file storage failure

WARNING: Low diskspace on <hostname>

Warning about more the 80% usage of the available disk space.

The administrator should take care and delete log files in the disk that is affected.

4.7.4 Virus detected

SECURITY ALERT: Malware detected

The Virus scan detected a virus or malware. This is a serious security warning, and immediate action shall be taken.

The best way is to use the recovery SD card image and perform a full recovery to a virus free state.

4.7.5 Banned network activity

SECURITY ALERT: banned IP address

The fail2ban has blocked an IP address due to too many failures or syn-flood attack. It is not a critical warning, as the attacker is blocked, but it is an indication of something going on and that network security in general shall be checked.

4.7.6 Audit events

SECURITY ALERT: Audit report from <hostname>

The audit system is like a surveyance camera overlooking core folders in the OS.

In normal operation there will be no alerts or warnings from the audit system.

If anything is touched intentionally, like adding users or opening the firewall, then there will be response from the audit, that can be ignored.

The audit system gives a warning that someone is touching the system files. This is not to be the case in normal operation, so audit events shall be immediately investigated.

4.8 System backup

The administrator shall keep a system backup to be used in case of a Cyber Attack. It will be possible to create a full backup to an USB disk using the command: `sudo dd if=/dev/mmcblk0`

`of=/media/phonesystem/bak/OS300_01.img bs=4M status=progress`

But it is really not recommended to backup a live operating system. It is better to close down gracefully and then make a full copy of the SD card using an SD card reader and the tool software like **Win32DiskImager**.

SD cards are so low priced that a backup copy can easily be created on delivery of a system.

5. Commissioning OS 03.00

When installing a PABX system with LSP + OS 03.0, there are a few but important steps to follow:

- Configure the e-mail address of the administrator in the file:
Log in as `localadmin` and
`nano /home/persistentfs/conf/email.conf`
- Change default passwords of `localuser` and `localadmin`.
`su – localadmin`
`passwd`
`su – localuser`
`passwd`
- Add the users that should have user rights and administrator rights by their real names
- Make sure that the above users log in and update their passwords.
- Give the `localadmin` password to those that should have the right to be administrator
- Make a complete backup of the OS to be used for recovering from Cyber Attack.