# Password Management VOS1, VOS2

This page contains information about the system password management on VOS1 and VOS2 platforms. On VOS1 and VOS2, passwords are used to protect the System Mode Overview from unauthorized use. The initial password value is set on the factory and can be set/changed by the deployment process.

## Overview

### Data Structure

Password database location:

- /mnt/flash/system/passwords_db
- /mnt/flash/system/passwords_db.sha (cryptographic signature, contains a HMAC that is generated using a h.w OTP key) Both files are binary files. Sys-mode Password database file can be accessed by system users (sysN), but not regular users (usrN).

### Password Change History

The Password database content history is not accessible.

The Password database file modification date is only modified after a password change. This date can be used to get the last date when passwords were modified (value or expiration state is changed).

Example:

```
root@Raptor:~# su - usr1usr1@Raptor:~$ stat /mnt/flash/system/passwords_dbFile:
/mnt/flash/system/passwords_dbSize: 2088 Blocks: 8 IO Block: 4096 regular fileDevice: 14h/20d Inode: 21275
Links: 1Access: (0660/-rw-rw----) Uid: ( 0/ root) Gid: ( 616/ system)Access: 2020-10-13
00:04:17.000000000Modify: 2020-10-13 00:05:35.000000000Change: 2020-10-13 00:05:35.000000000
```

### System Passwords

"passwords_db" stores hashed values of system passwords listed below:

| Password type | Description |
|---|---|
| supervisor | Full access to all System mode functionality. Supervisor password is also used to protect Rescue menu |
| maintenance | View settings and perform diagnostics either at the customer site or a repair depot. Does not allow changes to the device |
| level1, level2 | These optional logins have System mode access limits defined by the security policy file. Note that the Level1 and Level2 login acts as a subset of the usr1 account |
| keyload1, keyload2 | These passwords requested to initiate key loading |
| switch1, switch2 | These passwords requested to activate devices when Anti Removal Switches (ARS) are activated (e.g. UX300 and UX100 Installation) |

## Password Value Guidelines

- The password entered should be a minimum of 7 digits.
- The new password entered should not match the previous password.
- The new password entered should not match the default password.

## Password Value Entering

During the input of passwords and key components into the POI keypad, if a button is not pressed every 60 seconds an inactivity time-out is implemented such that the device will exit the sensitive state.

Password Entry timeouts for 5 seconds on wrong password entry.

The entered password is not stored. Once a full password is entered, or password entry is canceled/timed out, the password is cleared from memory immediately.

## Password Value Validation

**Trident and Engage:**

When the user is logging in, the value entered in UI is hashed (SHA-256) and the hashed value is compared with the value stored in the database (that is already hashed using the same hash type).

If the user logins into the sysmode, and enters a password value, that is less than 7 digits, then - even if the hash of this password value entered is the same as stored on the device:

- the password state is changed to ''expired'',
- the sysmode prompts the user to enter a new password value that should be at least 7 digits long.

A new password (if it is entered via the UI) can not be equal to the old value. A new password must be entered twice for validation.

> Password length validation doesn't affect DEV mode devices to keep the possibility to use the default factory password that is 6 digits long.

## Password Value Expiring

It is a PCI requirement for passwords allowing access to sensitive areas of the system to expire when the unit is shipped from the factory.

The first login after the unit leaves the factory forces the operator to change the password.

The password expiration state can be changed by password change packages (Password update (V/OS2), Supervisor password Reset).

If the password is expired, then during login user is forced to change the password.

Maintenance mode - Does not require expired passwords as there is no ability to access sensitive areas or clear tamper codes. Allows the password to be reset to the default.