Dynabook Europe GmbH

Stresemannallee 4b, 41460 Neuss, Germany
PHONE:+ 49(0)2131 52508-20
FACSIMILE:+ 49(0)2131 52508-99

Supervisor Registration Utility for Windows
[TsuRuWin]
Version 1.18

User Guide

Index

Document Revision: 1.18-DBE

1. Outline

Text-based Supervisor Registration Utility for Windows [TsuRuWin] **[v1.18]**

The 'TsuRuWin.exe' utility (TsuRuWin) can be used by a supervisor to register the BIOS password, set the user policy, restrict the use of specific devices or limit the ability to boot from specific devices.

2. Requirements

Before being able to use TsuRuWin, it is necessary to do the following:

- **Verify that the PC model supports TsuRuWin**.
  (*verify with your regional sales rep or system engineer*)
- **Install the dynabook System Driver**
  (*old name: the Toshiba System Driver, the Toshiba Value Added Package*)
  (*at least the ACPI-Compliant Value Added Logical and General Purpose Device Driver is necessary*)
  or,
  when Windows PE, load the TVALZ.sys driver.
  (*add the driver into a WIM image using 'DISM /Add-Driver'* ***OR*** *load the driver using 'drvload' command at startup of Windows PE*)

NOTE: If a 64-bit (AMD64) version of Windows PE, you must use 'TsuRuWin64.exe' instead of 'TsuRuWin.exe'

3. How to Use

1. **Edit 'TsuRuWin.ini' file using a text editor**
   (e.g. using Notepad). In the following, Step 3 is mandatory.
2. **Modify [ModelNumber] section - Enter Model Number**
   (only 1 model number per line number or model family by using an '*' (asterisk symbol, means wildcard) after the first six characters as in the sample below **OR** you can remove all Model Numbers and TsuRuWin will be active for ALL units the utility is installed on.
3. **Modify [Supervisor] section - Enter the supervisor password.**

   NOTE: *You can set the supervisor password here if you do not already have one set*

   ➔ OldPswd:
   Currently registered supervisor password. (*Required when change / update / delete*)
   ➔ NewPswd:
   Newly registered / changed supervisor password. (*Required when register / change / update*)

For example:

A) **Register when no supervisor password is registered**

```
[Supervisor]
NewPswd = <New Supervisor Password to be registered>
```

B) **Change supervisor password**

```
[Supervisor]
OldPswd = <Old Supervisor Password to be deleted>
NewPswd = <New Supervisor Password to be registered>
```

C) **Update settings**

```
[Supervisor]
OldPswd = <Current supervisor password>
NewPswd = <Current supervisor password>       (This must be the same as 'OldPswd')
```

D) **Delete Supervisor password**

```
[Supervisor]
OldPswd = <Old Supervisor Password to be deleted>
```

4. **Modify options after '='** (*equal symbol*)

Enable option	→	**1 = Enabled**
Disable option	→	**0 = Disabled**

ⓘ **NOTE:** **[Supervisor] section is mandatory. Other sections are optional.**

Unnecessary options and sections must be commented out by putting ";" (semicolon symbol) at the beginning of the line or the BIOS changes will not take effect. This also includes the User password if it is not being used or configured.

Each password string can be described by the encoded password string instead of plain text.
The encoded password string can be generated at the following website:

- https://www.biospw.com/tsb/encoder/

⚠ WARNING:
If one or more items listed in [DeviceLock] section has a value of '0', 'BiosSetup' in [UserPolicy] section must also be set to '0', otherwise the BIOS SETUP screen will be corrupted.

5. **Save the ini and executable file to any location you wish on the storage.**

4. How to Execute

1. **Open a Command Prompt in windows and browse to the location of the saved ini and executable file** (*it is recommended, to open CMD prompt with admin permissions*)

2. **Type `'tsuruwin'`**
   <Options> (case-insensitive):

   /V - *Verbose mode*
   /Y - *Do not ask to confirm whether to execute*
   /E - *Waiting for a key input when error occurs*
   /? - *Help*

   You can specify your own named ini file after options. (*if omitted, 'tsuruwin.ini' is assumed*)
   Example: `tsuruwin /y mypswd.ini`

3. **Please reboot your computer**

5. 'TsuRuWin.ini' Sample

Definition = Highlighted text

NOTE:
The bold value of the following options shows the default value.

WARNING:
Some options may not be supported depending on the PC model.

```
[ModelNumber]
1             =          XXX123-AAAA1
2             =          YYY456-*

[Supervisor]
OldPswd       =          OLD SUPERVISOR PASSWORD
NewPswd       =          NEW SUPERVISOR PASSWORD

[User]
OldPswd       =          OLD USER PASSWORD
NewPswd       =          NEW USER PASSWORD

[UserPolicy]
RegistPswd               =1        - 1: Allow to register user password
DeletePswd               =1        - 1: Allow to delete user password
ChangePswd               =1        - 1: Allow to change user password
NoLockPswd               =1        - 0: Lock user password if user password verification exceeds max retry counts
NoReqRgPswd              =1        - 0: BIOS will request the user to register or change user password on next boot
MaxChekTry               =3        - Maximum try count to verify user password (1-15), or unlimited
                                    (i.e. MaxChekTry = Unlimited)
MinPswdLen               =1        - Minimum length of user password (1-15) (Maximum length of password is fixed to 50)
BiosSetup                =1        - 1: Allow to setup BIOS SETUP (synonymous with SYSTEM SETUP)
BiosUpdate               =1        - 1: Allow to update the BIOS
NotViewMode              =1        - 0: Show the BIOS SETUP screen with View Mode (only when BiosSetup=0)
```

```
RegDelHDDpw     =1     - 1: Allow to register and remove the HDD password
ChangeHDDpw     =1     - 1: Allow to change the HDD password
S4LockHDDpw     =1     - 0: Try automatic unlocking of the HDD security at the time of return from S4
S5LockHDDpw     =1     - 0: Try automatic unlocking of the HDD security at the time of boot from S5
ActivateTPM     =1     - 1: Allow to configure ‘TPM Enable/Disable’ in BIOS SETUP
OwnerClrTPM     =1     - 1: Allow to configure ‘Clear TPM Owner’ in BIOS SETUP
BTcert          =1     - 1: Allow to Bluetooth authentication
BTcertMode      =1     - 1: Treat Bluetooth as a Simple token
                       - 0: Two factor authentication of Bluetooth authentication and
                       BIOS password authentication is required
FPcert          =1     - 1: Allow to Fingerprint authentication
EnSmartCard     =1     - 1: Allow to Smart Card authentication
NoBootMenu      =1     - 0: Show the boot menu at booting with the F12 key
RmBiosUp        =1     - 1: Allow to Remote BIOS Update (If not allowed, supervisor password authentication
                       may be required at remote BIOS update)
S4WolPwAuth     =1     - 1: When Wake On LAN (WoL) occurs from hibernation (S4) state, BIOS password
                       authentication and/or HDD password authentication are required
S5WolPwAuth     =1     - 1: When Wake On LAN (WoL) occurs from power off (S5) state, BIOS password
                       authentication and/or HDD password authentication are required

[TokenPolicy]
CreateToken     =1     - 1: Allow to create user token
RemoveToken     =1     - 1: Allow to remove user token

[DeviceLock]
IoCOM           =1     - 1: Enable Serial (RS-232C) Port
IoPRT           =1     - 1: Enable Parallel (Printer) Port
IoFIR           =1     - 1: Enable Infrared (IrDA) Port
IoIntFDD        =1     - 1: Enable Internal Floppy Disk Drive
IoExtPS2        =1     - 1: Enable PS/2 Connector (external PS/2 Mouse and Keyboard)
IoODD           =1     - 1: Enable Optical Disc Drive (internal CD-ROM drive, CD/DVD/ Blu-ray multi-drive)
Io2ndHDD        =1     - 1: Enable Second Hard Disk Drive
IoBluetooth     =1     - 1: Enable Bluetooth (except for SD/USB Bluetooth)
IoMODEM         =1     - 1: Enable Internal Modem
IoUSB           =1     - 1: Enable USB Connector
IoLAN           =1     - 1: Enable Internal LAN (disabling this item, boot from the internal LAN is also disabled)
IoPCCard        =1     - 1: Enable PC Card Slot (disabling this item, boot from a PC Card ATA is also disabled)
IoSD            =1     - 1: Enable SD Card Slot (disabling this item, boot from SD memory card is also disabled)
```

```
IoIEEE1394      =1      - 1: Enable i.LINK (IEEE1394) Connector
IoExpCard       =1      - 1: Enable ExpressCard Slot
IoTdODD         =1      - 1: Enable Tablet Multi Dock Optical Disk Drive
IoTdHDD         =1      - 1: Enable Tablet Multi Dock Hard Disk Drive
IoWiredLAN      =1      - 1: Enable Internal Wired LAN
IoWlessLAN      =1      - 1: Enable Internal Wireless LAN
IoWlessWAN      =1      - 1: Enable Internal Wireless WAN
IoMediaSlot     =1      - 1: Enable Internal Media slot
IoCFSlot        =1      - 1: Enable Internal Compact Flash (CF) Slot
IoESATA         =1      - 1: Enable eSATA Connector (or eSATA portion of an eSATA+USB connector)
IoWebcam        =1      - 1: Enable Internal Webcam
IoWiGig         =1      - 1: Enable Internal Wireless Gigabit
IoTBolt         =1      - 1: Enable Thunderbolt Connector
IoMic           =1      - 1: Enable Microphone
Boot1stHDD      =1      - 1: Enable boot from First Hard Disk Drive
Boot2ndHDD      =1      - 1: Enable boot from Second Hard Disk Drive
BootODD         =1      - 1: Enable boot from Optical Disc Drive
BootFDD         =1      - 1: Enable boot from Floppy Disk Drive
BootLAN         =1      - 1: Enable boot from Internal LAN
BootATA         =1      - 1: Enable boot from PC Card ATA
BootUSB         =1      - 1: Enable boot from USB Memory (USB Flash Memory and USB Hard Disk Drive)
BootESATA       =1      - 1: Enable boot from eSATA device

[HDD] – WARNING: HDD password cannot be reset if forgotten.
OldMasterPswd   =       OLD MASTER HDD PASSWORD
NewMasterPswd   =       NEW MASTER HDD PASSWORD
OldUserPswd     =       OLD USER HDD PASSWORD
NewUserPswd     =       NEW USER HDD PASSWORD

[OwnerString] - If user password is set, the following entries will be displayed during password login.
1               =       1st line
2               =       (Empty line)
3               =       3rd line
```

OR to delete:

```
[OwnerString]
1               =
```

6. Optional

- **Scrambling ini file**

  An ini file has passwords in plain text and can be read by anyone.
  You can avoid this by using the scrambling function:

  ```
  % tsuruwin /scramble
  ```

  (*where 'tsuruwin.ini' exists in the same directory*)
  Then scrambled 'tsuruwin.ins' is generated.

  NOTE:

  - You can rename 'tsuruwin' part, but must not rename the extension '.ins' since TsuRuWin find that '*.ins' is scrambled
  - 'tsuruwin.ins' that already exists is overwritten if `'tsuruwin /scramble'` is executed.
  - `/V` option does not show password info if '*.ins' is used.
  - Anyone cannot de-scramble from '*.ins' to '*.ini'.
  - Anyone cannot modify any 1-bit in '*.ins' since TsuRuWin detects tampering.

- **Embedding ini file into executable file**

  You can embed scrambled ini file (*.ins) into executable file itself:

  ```
  % tsuruwin /scramble mypswd.ini
  ```

  Then 'mypswd.exe' is generated.

  NOTE:

  - You can distribute or carry only this 'mypswd.exe' without 'TsuRuWin.exe' and 'mypswd.ini'.
  - You can rename 'xxxx' part in 'xxxx.exe'.
  - If there is the same named exe file, previous exe file is backed up to '*.bak'.
  - You can identify ini-file-embedded exe file with `/?` option.
  - If `/scramble` option appears, it does not have ini information.
  - Original 'TsuRuWin.exe' has been signed by Microsoft Authenticode certificate for dynabook / Toshiba. However, generated ini-file-embedded exe file, that digital signature is not embedded (*that is removed*).

- **Password protection for scrambled ini file**

  When scrambling ini file, by adding a password, you can protect it more safely.

  ```
  % tsuruwin /scramble:pswd
  ```

  Then 'tsuruwin.ins' (that is protected by password ‘pswd’) is generated.

  At execution, you must specify both password and ‘*.ins’.

  ```
  % tsuruwin /scramble:pswd tsuruwin.ins
  ```

  If password ‘pswd’ is correct, it is executed.

  And also you can embed scrambled ini file (that is protected by password) into executable file itself.

  ```
  % tsuruwin /scramble:secret pwsetup.ini
  ```

  Then ‘pwsetup.exe' (that is protected by password ‘secret’) is generated.

  At execution, you must specify password.

  ```
  % pwsetup /scramble:secret
  ```

  If password ‘secret’ is correct, it is executed.