

# **TANLock 3 Deployment Manual**

**Technical sales and deployment guide**

**Document status – Draft first PR 8<sup>th</sup> Sept 2019**

## Contents

<b>1</b>	<b>TANlock Introduction &amp; Setup</b>	<b>3</b>
1.1	Different TANlock Modules	3
1.1.1	Items delivered in the box	5
1.1.2	Factory default configuration for TANlock 3	6
1.2	TANlock Introduction	8
1.2.1	How to restore to the factory default configuration	10
1.3	TANlock Explorer configuration tool	12
1.3.1	Installing TANlock Explorer tool	12
1.3.2	Logging into TANlock Explorer	14
1.3.3	TANlock – Basic Lock Information	16
1.3.4	TANlock – Launching the Cockpit	19
1.3.5	TANlock – Cockpit Info Tab	20
1.3.6	TANlock Cockpit – User	21
1.3.7	TANlock Cockpit – Network Tab	22
1.3.8	TANlock Cockpit – Config Tab	23
1.3.9	TANlock Cockpit – SNMP Tab	25
1.3.10	TANlock Cockpit – LDAP	26
1.3.11	TANlock Cockpit - HTTP	27
1.3.12	TANlock Cockpit - Syslog	30
1.3.13	TANlock Cockpit - Service	30
1.3.14	TANlock – Restore ‘Config’	33
1.3.15	TANlock File Explorer	34
1.3.16	TANlock Statics	38
1.3.17	TANlock Log	38
1.3.18	TANlock Upload firmware	42

# 1 TANlock Introduction & Setup

A TANlock is a networked IoT (Internet of Things) device and consideration should be given to the security of the network links and remote access available to and from the assigned lock IP address.

It is recommended that TANlock is not directly connected to any production networks.

It may be connected to the corporate network, more specifically a monitoring and administration network that hosts the servers monitoring or managing the organization. It should be isolated via a firewall allowing only specific protocol to and from the TANlock network.

## 1.1 Different TANlock Modules







TANlock 3 is a modular system that can use changeable modules to provide for different authentication methods.

New authentication methods and features can be integrated into the lock so that can it can adjust to the current market requirements.

Changeable modules allow sites that may currently have Pin Pad TANlocks deployed and in the future need to upgrade some locks to a Fingerprint model to just replace the module and not the whole lock.

### TANlock Modules

		<b>Pin Pad.</b> Set the user ID and pin length to give a combination for a single pin. Default user ID 3 digits, Password 3 digits. User has a 6-digit pin to open the lock. User IDs and Pins can be dynamically created. Dynamically creating PINs requires 3 <sup>rd</sup> party management software.
		<b>RFID</b> The TANlock can be configured with the RFID card credentials of a user. 13.54Mhz ISO 14443a, 14443b, 15693, Legic prime, are supported.  The TANlock RFID chip supports most card types. However, RFID building access cards tend to be proprietary.

		<p><b>RFID + PinPad</b>  Allows the setup of two factor authentication so that an RFID Card + Pin is required. Either a single user can provide both or multiple users need to provide their authentication credentials.  Two Factor can be  RFID + RFID, RFID+Pin, Pin+Pin, Pin+RFID</p>
		<p><b>QR Code</b>  This integrates with a backend 3<sup>rd</sup> party management server using the Web API.  The user uses a mobile phone App to scan the QR or Barcode after authenticating via the App.</p>
		<p><b>TouchDisplay Pad</b>  Displays a keypad with text display. Selectable digits 0 – 9  User enters their PIN to unlock the TANlock.</p>
		<p><b>Fingerprint reader</b>  Scans the user fingerprint and matches it against a stored list of templates. Multiple fingers for a single user can be scanned and stored.  Separate registration and management software is included as part of the solution.</p>
		<p><b>Hand Vein Scan</b>  Requires separate Micro-computer to store, match and register vein scans.  Supplied as a complete solution with the management software to store and validate the hand scans.</p>
<p>TANlockExplorer is FATH software. Optimum Paths Visual Data Center is one example of 3<sup>rd</sup> Party software.  Note, All TANlocks regardless of the module type can be configured to use two-factor authentication.</p>		

Two integral parts of TANlock 3 are

- Firmware (OS)
- TANlockExplorer tool

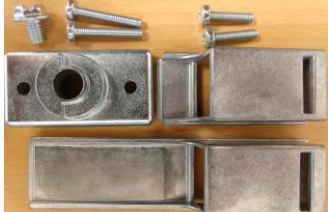



New firmware releases may add new features as well as provide software updates.

The TANlockExplorer tool provides a simple management interface to configure the TANlock and allow user authentication credentials to be created and stored directly on the lock.

Allowing user credentials to be directly created from the TANlockExplorer tool allows small deployments of 2 – 20 locks that customers can deploy and manage at short notice.

### 1.1.1 Items delivered in the box

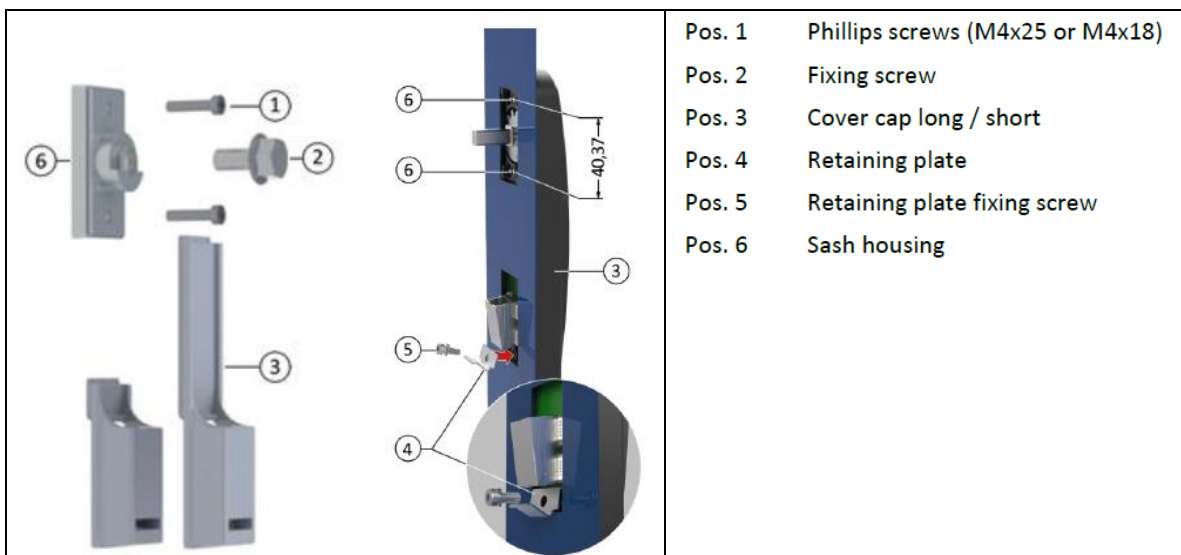
The TANlock is delivered as a package with the following components

<p>Phillips screws (M4x25 &amp; M4x18) Fixing screw Sash housing Cover cap long/short</p>	
<p>TANlock 3 motherboard, POE and module view</p>	
<p>TANlock 3 external handle with authentication module (RFID only module shown)</p>	
<p>TANlock 3 replaceable modules. Ribbon cable and 4 screws are the only requirements for replacing the module. Modules are always installed and connected in delivered products.</p>	

The following are not included, ethernet cable, locking CAM.

The existing locking CAM from the current enclosure may be used or a different locking CAM can be ordered from FATH depending on the enclosure type and fitting required.

### TANlock assembly



Custom adapters for different enclosure styles exist, however, if a custom adapter is required to fit a specific enclosure type that does not exist it can be designed and developed by inhouse FATH Mechanical engineers.

### 1.1.2 Factory default configuration for TANlock 3

TANlock is shipped with an initial base configuration.

All TANlocks have the same delivered base configuration and need to be customized to the specific end user environment.

Each customer requirement, from lock module to network integration and lock management may be different but the basic setup for each customer will be similar.

The default setting for the base TANlock 3 configuration is shown in the table below. The base config is modified using the TANlockExplorer tool.

<b>User</b>		
	Create/Delete/Clear	No users defined by default unless an RFID module is being used. Some have a sample card and user defined.
<b>Network</b>		
	IP Address	192.168.0.90 (default IP)
	Subnet Mask	255.255.255.0 (default mask)
	Gateway	Not defined
	DNS	Not defined
	Enable DHCP client	Not enabled by default
	VLAN	Not selected, VID 1
	NTP	Not selected, not defined
<b>Config</b>		
	Device name	lock1
	Keypad Timeout	5 sec
	Auth. Fail Timeout	1 sec
	User ID Length	3
	Pin Length	3
	Door open Detection, Ext 1 & Ext 2	Selected
	Two-factor authentication	Not selected
	Nodelink over TCP	Selected
<b>SNMP</b>		
	SNMP	Not selected
	Trap Destination	Not defined
	Community Read String	public
	Community write String	private
<b>LDAP</b>		
	LDAP	Not selected
	Sample settings filled in	Modify to customer requirements
	Two Way	Not selected (Allows 2 <sup>nd</sup> search)
<b>HTTP</b>		
	API-Key	lab

	HTTP (Port 80)	Selected
	HTTPS (Port 443)	Selected
	Web API	Not selected
	RESTful API	Not selected
	HTTP Event	Not selected
<b>Syslog</b>		
	Syslog	Not selected
	Syslog Server	Not defined
<b>Service</b>		
	Service Tab (visible, depends on Firmware version)	No selections available at 'Config' Cockpit user level. Need to login at 'Service' user level to activate options.
	Passwords, Config Cockpit, Service Cockpit, cftp, ftp, ftp-update	Set but not displayed. cftp & ftp use a username 'root'. ftp-update account uses a username 'update'.
<b>Access</b>		
	Config Cockpit password	91174 (default 'Config' password)
	Service Cockpit password	15973 (default 'Service' password)
	TANlockExplorer TCP port	1328/TCP

The TANlockExplorer tool may present different tabs depending on the firmware version being used and the password (permission level) used to access the tool.

There are two modes of access, 'Config' and 'Service'.

The 'Service' tab may be visible when logged into the 'Config interface' but changes within the Service tab can only be made when logged in with the 'Service' password.

Only experienced users should have access to the 'Service' password, it should not be used for general administration. Do not log in using the 'Service' password unless you need a feature that is only available in the 'Service' mode.

The only features that are restricted to the 'Service' mode are

- Changing the lock to 'Firstboot/Service' mode ready for transport.
- Opening the lock using TANLockExplorer without requiring specific user credentials.
- Changing the administration passwords.

The default passwords should be changed when the TANlock is installed at the customer location.

If you lose the 'Service' password, then you might not be able to reset the other passwords. This may depend on the firmware version currently installed.

Do NOT lose the 'Service' password.

## 1.2 TANlock Introduction

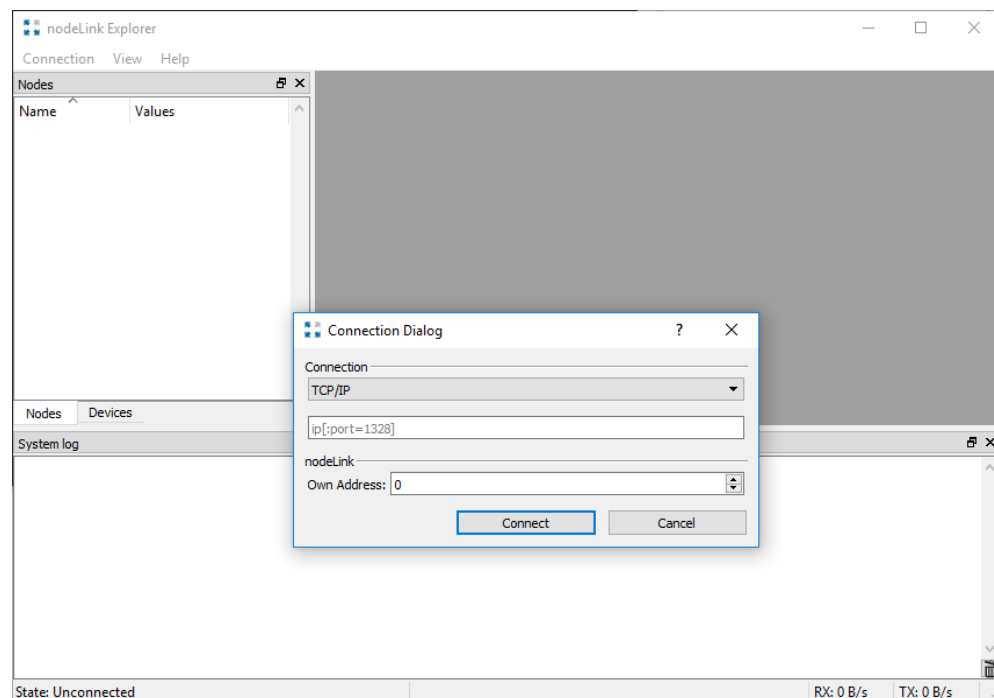
The TANlock initial setup can be completed using the TANlockExplorer tool over a network link connecting to the default IP address 192.168.0.90 if DHCP has not been enabled. If a network link is not available, then the initial setup can be completed using the serial connection with a USB-C type cable.

The TANlockExplorer tool is only supported in Microsoft Windows 10. It may work for earlier versions but is not officially supported.

All TANlocks are currently delivered pre-configured with the IP address 192.168.0.90 and use a TANlockExplorer 'Config Cockpit' password of 91174.

If DHCP service on the lock is enabled an accessible DHCP server must be available to assign an IP address and complete the initial setup.

The TANlockExplorer tool is available from the support website.



TANlocks are delivered factory packed in a box with a metal cover cap and assembly kit unless they are pre-installed in the enclosure or cabinet.

TANlocks, when not purchased as an integrated part of the enclosure do not come with the locking CAM as this is already part of the rack enclosure that the current lock uses.

When retrofitting a TANlock it will usually work without modification and should work with the standard CAM supplied with the enclosure or cabinet. Customized adapters and different locking CAMs are available if required for specific enclosures from some manufacturers.



The lock when delivered might be in one of two states, a state known as 'First Boot', also referred to as 'Service mode' or if configured in an enclosure it might come locked with a sample RFID card to open it.

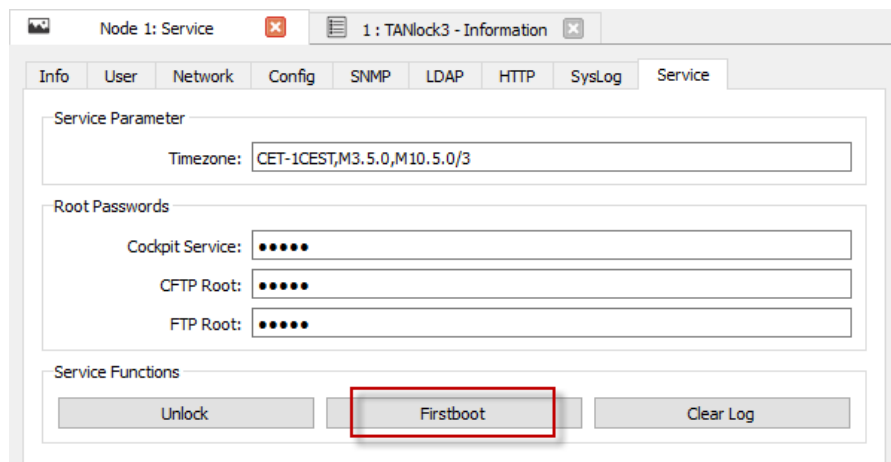
'First boot' or 'Service mode' means that the locking latch is not engaged, and the locking lever cannot be locked in place. The locking latch will reset to the lock position when power is first applied to the TANlock.

If the lock has an RFID module then it may come with a demonstration RFID card and the lock handle will be in a locked state. Use the card to open the lock once connected to a power source. Alternatively, it may have a 6 digit PIN set to unlock it, for example 123412.

In either case, First Boot or supplied with a sample RFID card the TANlock can be installed into the rack enclosure without the problem of locking the door and not being able to open the door again without adding user credentials.

In 'Service' mode there normally a plastic tag holding the lever arm in place and this should not be removed until the lock is ready to be powered on and configured.

If you remove the plastic holding tag, then make sure it is put back until the lock is ready to be powered on to complete the basic configuration.



In order to set a TANlock in 'First Boot' mode you need to be logged in using the 'Service' account password.

You normally only do this when removing the lock from the current installed location to relocate it. It is sometimes referred to as 'Transport mode'.

Once the TANlock has been deployed and connected to the POE switch if the TANlock loses connectivity due to physical switch, port, or network cable failure then the lock can be powered using a USB-C type cable with a battery pack or directly from a laptop USB port.

Providing the TANlock has power then it can be unlocked.

Some TANlock authentication modules, QR code, Fingerprint & Hand Vein Scan can only function correctly when integrated with 3<sup>rd</sup> party management software to control access and to register users or remotely unlock the TANlock.

If you have a small site, 20 – 40 locks then it is possible to just use the TANlockExplorer tool to manage your installation.

Log events can be sent to a syslog server and SNMP traps sent to a central SNMP monitoring server.

Kiwi syslog works quite well for receiving both syslog and SNMP trap events. Most sites will likely already have a network monitoring and management solution like SolarWinds, HP Openview, WhatsUp Gold, Optimum Path Visual Data Center, Sunbird DCIM, that can be used to send or forward the snmp traps to.

There is no limit to the number of locks that the TANlockExplorer can manage.

Third party management software like Optimum Paths 'Visual Data Center' or Sunbird DCIM, for managing Data Center environments can be used to manage the TANlock as another integrated device.

TANLock can be treated as just another device that can be added to the Visual Data Center database.

For building management systems then the TANlock can be integrated as a managed device for example, Prowatch is a common global building management system.

The HTTP API commands allow TANlock to be easily integrated into many 3<sup>rd</sup> party software solutions.

The TANlock 3 uses HTTPS to secure the communicate between the Management software and the lock.

Integrating with 3<sup>rd</sup> party software only needs the software to be able to send https commands to the TANlock and be able to process JSON objects that are returned as responses to the API commands.

It is not difficult for software developers that understand web page management to integrate TANlocks into their software.

### 1.2.1 How to restore to the factory default configuration

There is currently no reset button to restore to a factory delivered base firmware and default configuration.

There is a 'Restore' config option within the TANlockExplorer in both 'Config' and 'Service' mode to restore the configuration parameters to the initial delivery base configuration.

There is currently no option to restore the firmware version back to the factory delivered firmware version.

The critical files that contain the core configuration needed for the basic configuration and defined user credentials are the following

```
/config/config.txt  
/config/users.bak  
/config/users.json
```

If you overwrite the config.txt file with a backup version and then reset the TANlock then it will reboot using the file last copied to /config/config.txt.

You need the 'Service' password to have access to the File explorer tool within TANlockExplorer which allows file downloads and edits on the TANlock file system. Alternatively, you can use the root FTP password to ftp a copy of the files from the TANlock to a safe location.

In normal operation of the TANlock there is no requirement to edit files on the TANlock filesystem without the guidance of technical support.

The actual configuration from lock to lock is very similar in most end user deployments therefore a config.txt file from one lock can often be used as a replacement for another.

The config.txt file may contain information for a specific module type therefore it is not necessarily 100% compatible between different TANlock authentication module types.

If the users are defined locally in the '/config/users.json' file and multiple locks need the same user settings to be defined on multiple locks, then this file can be copied between locks.

However, it is easier to write a batch job and use the Web API and the 'curl' command line tool to configure the same credentials on multiple locks. This assumes that the Web API commands are enabled.

```
curl -k https://<IP Address>/<api-key>/user/create/<user>/<pin>
```

For example

```
curl -k https://192.168.0.90/lab/user/create/123/123  
curl -k https://192.168.0.91/lab/user/create/123/123  
curl -k https://192.168.0.92/lab/user/create/123/123  
curl -k https://192.168.0.93/lab/user/create/123/123  
curl -k https://192.168.0.94/lab/user/create/123/123  
curl -k https://192.168.0.95/lab/user/create/123/123
```

The -k option suppresses error messages for SSL self-signed certificates.

Note: the IP address/hostname part of a URL is not encrypted in https but the rest of the URL is .../lab/user/create/123/123.

In a customer environment the API-Key may be unique to each TANlock and the batch commands generated by 3<sup>rd</sup> Party Management software.

The management software would have a database of all lock details including the unique API-Key and can easily generate the API commands. The https commands would only be originating from a single known source IP address in most environments.

In some customer environments they may not want to store user credentials on every lock.

The 'users.json' file may be empty and user credentials dynamically created by the 3<sup>rd</sup> party Management software adding and deleting users as and when they are needed.

Not storing the users in the 'users.json' file is perhaps the most secure type of customer deployment as there are no stored credentials on the TANlocks.

With no static credentials' users cannot share their authentication details as each access event to open a lock would require a unique onetime code.

Even when using an RFID card, it is possible to program a card ID on the lock dynamically just before it is needed. This takes planning and 3<sup>rd</sup> party software integration but once setup as a standard procedure is easy to control user access.

Check references to *Zero Key TANlock* & *Dynamic Key TANlock* both methods only create the user TANlock credentials as they are required. To make use of dynamic onetime authentication 3<sup>rd</sup> party management software is required.

The TANlockExplorer tool does not use *Zero* or *Dynamic Key TANlock* functionality as it cannot dynamically create different passwords each time a user needs to open a lock.

Dynamically creating TANs (Transaction authentication Numbers) requires the methods for user interaction with 3<sup>rd</sup> party software to be defined and managed externally using remote Web API commands.

## 1.3 TANlock Explorer configuration tool

### 1.3.1 Installing TANlock Explorer tool

In production environments you might have one or two virtual PC's that the TANlockExplorer tool is installed on located in a segmented network with restricted access to specific destinations.

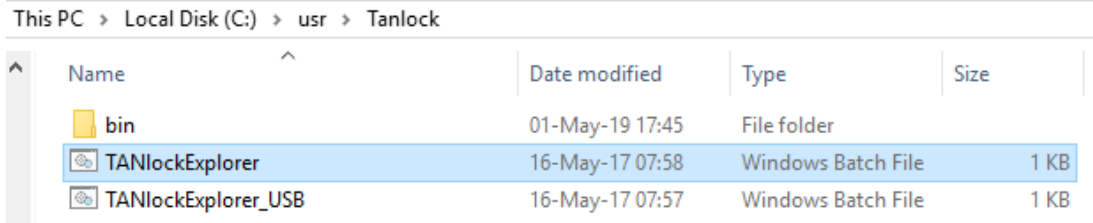
The zip files for TANlock can be installed in any directory as the files are all self-contained and do not need windows shared libraries or add registry entries to the Windows 10 operating system.

In this example TANlockExplorer has been extracted to a directory c:\usr\TANlock.

To start the application, select either the TANlockExplorer or TANlockExplorer\_USB batch file depending on how you would like to access the lock. The \_USB batch file just provides an option to select 'Serial' as well as TCP/IP from the pulldown connection type menu.

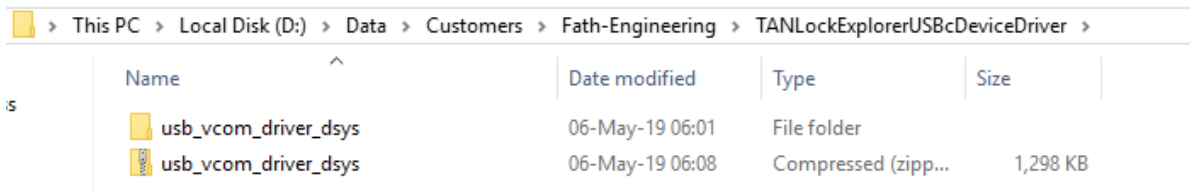
TANlockExplorer\_USB.bat file contains a single line

‘.\bin\tANlockExplorer.exe --view-all-tty’

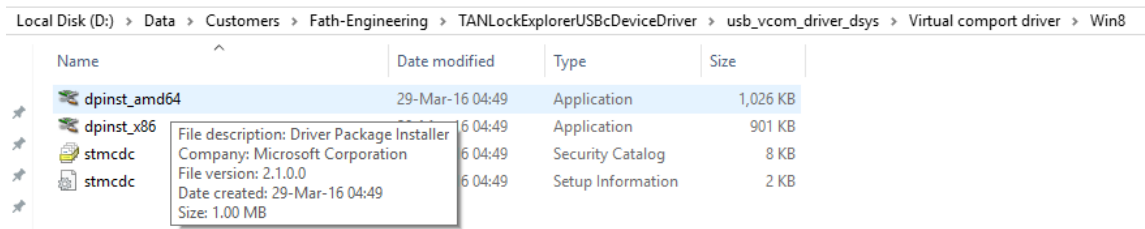


To use the USB interface version the device driver must be installed otherwise the TANlock 3 device will not be recognized as a serial USB coms device when connected.

Install the device driver before connecting the USB-C cable to the TANlock.

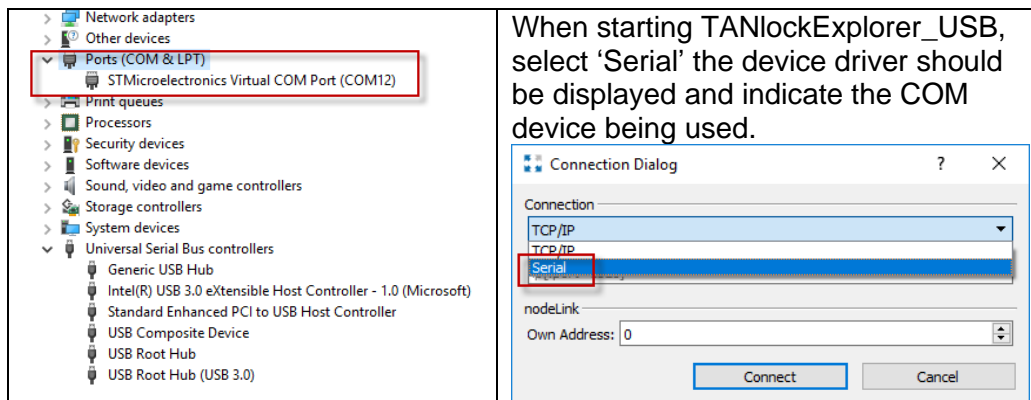


If you are using Windows 10 64-bit install try using the windows 8 driver.



The zip file containing the device driver is available from TANlock support or as a download from [www.tanlock.com](http://www.tanlock.com). Once unzipped, run the installer.

After installation the device driver should be visible in the list of devices in Windows ‘Device Manager’.



If you cannot see the device in the list after selecting 'Serial' then the device driver may not be correctly installed or recognized by Windows.

Alternatively, you may be using a USB-C cable that only works for power transfer and not data. This will also result in the COM port not being listed in the Connection Dialog.

Try using a different USB-C cable, one that you know works for data transfer before trying to reinstall or debug issues with the device driver.

### 1.3.2 Logging into TANlock Explorer

The default IP address of the TANlock is 192.168.0.90 unless DHCP is enabled.

Set the ethernet interface of the PC/laptop to an IP address in the 192.168.0.0/24 network, for example 192.168.0.42.

Check that the network cable is connected between the PC and the TANlock via the switch and complete a ping test.

```
C:\usr\TANlock>ping 192.168.0.90

Pinging 192.168.0.90 with 32 bytes of data:
Reply from 192.168.0.90: bytes=32 time<1ms TTL=255
Reply from 192.168.0.90: bytes=32 time<1ms TTL=255
Reply from 192.168.0.90: bytes=32 time<1ms TTL=255
Reply from 192.168.0.90: bytes=32 time<1ms TTL=255

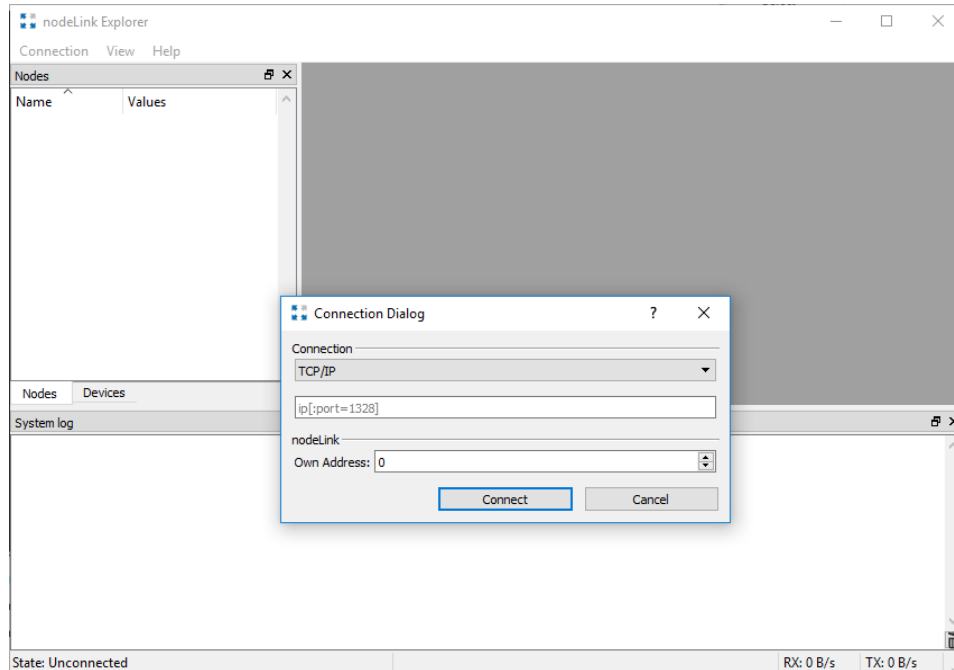
Ping statistics for 192.168.0.90:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\usr\TANlock>
```

When started, the application will prompt for the IP address of the TANlock. This example starts with a default TANlock base configuration so uses 192.168.0.90.

If you do not know the status of the TANlock or the configured IP address, you will need to use the serial connection to obtain that information before trying anything over a network link. If DHCP is enabled, you may be able to determine the IP address assigned and connect to that instead of using the serial cable link.

**There is NO reset button to restore back to a factory default config with IP address 192.168.0.90.**



Enter the IP address of the lock you want to manage or pulldown the TCP/IP and Serial menu option and select Serial.

Although TANlock can use DHCP to automatically assign an IP address for most deployments it will often be easier to keep track of the TANlocks and the associated rack location if static IP addresses are used. For initial setup DHCP might be easier to start with and then change to static IP addresses.

A DHCP server would need to be available on the network or via a routed link and the 'ip helper' command configured on the gateway to relay the DHCP requests to the server if DHCP is required.

Customers using DHCP in a production deployment would need to use 3<sup>rd</sup> Party management software that could discover the devices using SNMP and extract the attributes that would identify the lock and possibly work out the location.

You can run the following Web API command to get the Serial number and MAC address of the lock.

```
curl -k https://<IP Address>/<API-Key>/info

C:\usr\tanlock>curl -k https://192.168.0.90/lab/info
{
  "software": "06",
  "hardware": "02",
  "serialno": "5200010288",
  "macaddr": "00:18:79:00:0D:49",
  "time": "Sat Jan 1 09:53:51 2000",
  "user": "",
  "sensor": {
    "lock": true,
    "handle": false,
    "motor": true,
  }
}
```

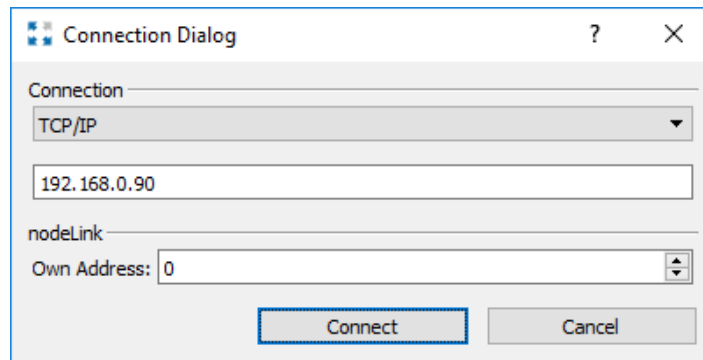
```

        "temperature": 0
    },
    "external": {
        "ext_11": false,
        "ext_12": false,
        "relais_0": false,
        "relais_1": false
    }
}
C:\usr\tanlock>

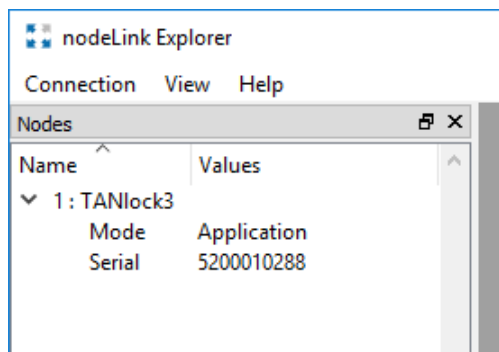
```

Using DHCP would also have to have a consistent user authentication model that was used across all locks as it would be difficult to identify individual locks to set specific user credentials.

It is easy to manage static IP address space used via a spreadsheet or IP address management tool like VitalQIP.



Once connected the basic details and serial number will be displayed.

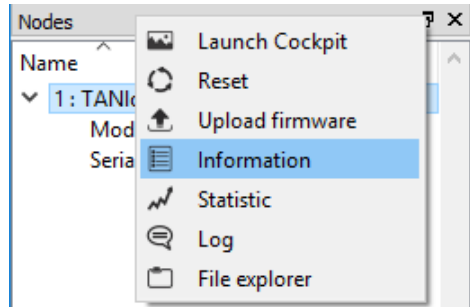


To make it easier to identify the lock and rack when you connect the hostname of the lock might include the cabinet number and location.

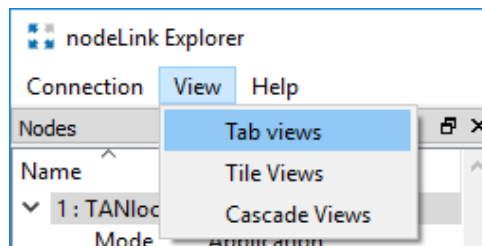
### 1.3.3 TANlock – Basic Lock Information

Select 'Information' from the popup menu

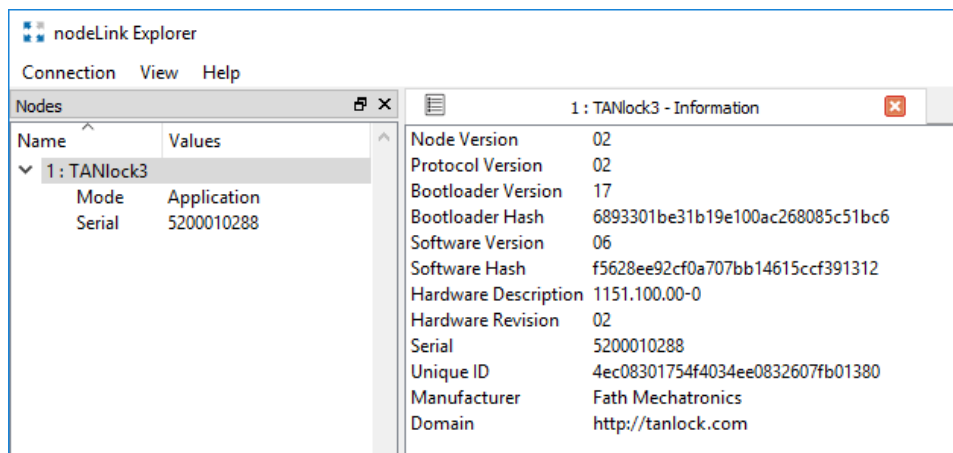




Change to Tab views as this displays the information in a clearer format on the display.



The basic information of the lock is displayed. You do not need a password to display the basic lock information shown below.



The Bootloader and the Software Version are of specific interest. This will show the firmware version currently installed. In this example firmware version 06 is being used.

Use the TANlock.com website to review the latest details and features of the firmware versions available. Each release of firmware will have a changelog document that details the changes and updates.

It is not necessary to always upgrade to the latest firmware. Only upgrade if a update has been added that is required for your environment.

For warranty and support purposes you should keep track of the serial numbers of the TANlocks you have installed.

You do not need a password to display the 'Information' tab.

A key password that must be kept safe and secure and recoverable is the 'Service' password.

The 'Service' password might be different for every lock in a customer environment.

Many sites use TACACs or RADIUS to centrally store and manage network device passwords for different users. TANlock does not support TACACs or RADIUS.

There is only a few accounts and passwords and multiple administrators with their own login are not required for a TANlock.

Something to consider for the 'Service' password since you must keep it secure and not lose it might be to create a relationship with the TANlock serial number.

The TANlock serial number is always unique.

For example, administrators might use a spreadsheet to keep track of serial number, IP address, location and warranty information.

In the spreadsheet, it might also be possible to create a unique but recoverable 'Service' password.

For example,

Cell G5 = Serial number

Cell H5=TRUNC((G5\*210567967456353)/133458761238) = 16232154

Then take the 5 digits from the right, =RIGHT(H5,5) = 32154

TRUNC removes the digits after the decimal point.

The multiplier & divisor need to be large numbers otherwise the same password might be created for some consecutive serial numbers.

It would not be difficult to work out the formulae used if you know enough passwords, but any formulae can be used so long as the method is known to the administrators and the numbers are large.

This is just a method of making the Service password recoverable if you change it from the default and use a different password for every lock. The passwords can be alpha numeric so could be more complex and use an MD5 Hash and then use the digits from the MD5 Hash.

Doing something like this means that no end user can forget the 'Service' password if every lock needs a unique password as it can be calculated from the serial number. Just do not lose the formulae used to create the number!

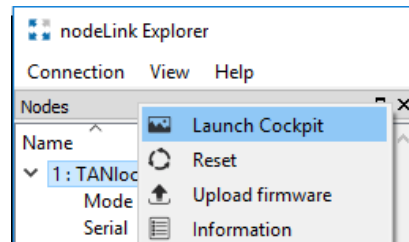
In a customer environment the serial numbers and 'Service' passwords are likely to be stored in a secure central database by the administrators.

This is one administration task that needs to be considered by end users.

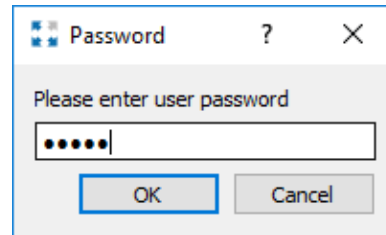
For managing a small number of locks this is not an issue but for managing 100's of locks then this may be something that needs to be integrated into the 3<sup>rd</sup> party management software.

### 1.3.4 TANlock – Launching the Cockpit

Use the 2<sup>nd</sup> mouse button, select the TANlock to display the popup menu and select 'Launch Cockpit'.



Enter the 'Config' password, the default password is '91174'.

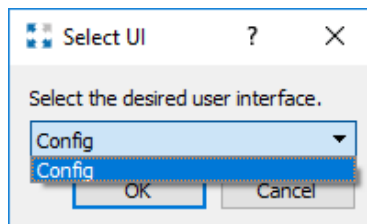


Once this password has been changed by the local administrator if it is lost then the only way to recover it is to use the 'Service' level password which will allow it to be reset.

If you lose the 'Service' level password, then that is a problem. The passwords for different levels are stored in the 'config.txt' file for each lock.

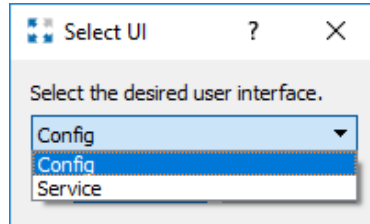
When passwords are changed a copy of the passwords should be stored in a safe recoverable location or a method of recovering the passwords should be implemented.

There is only one option to select when using the base level password, 'Config', select OK to open the TANlock configuration tool options.



If you had entered the 'Service' level password then there would be two options in the pulldown list, 'Config' and 'Service'.

The 'Service' User Interface (UI) displays some extra settings to allow resetting passwords.

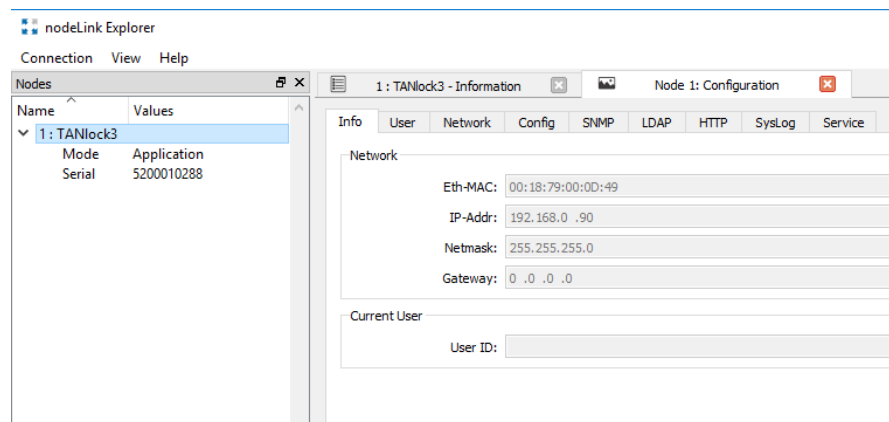


### 1.3.5 TANlock – Cockpit Info Tab

The 'Cockpit' is where most of the initial configuration of the TANlock is completed.

It is also possible to use the Web API commands to manage some aspects of the lock but setting parameters like network and server parameters are still restricted to the Cockpit.

The info tab displays the current network interface details.



The 'Current User' shows the last user to authenticate with the lock. If the value is blank try selecting refresh, if the value stays blank then it is likely that an RFID card was used but not authorized therefore no user is listed.

If you change any value in the tabs you may have to select the refresh button to see the updated values.

Make sure you select 'Save' and then reset (reboot) the lock for any changes to take effect.

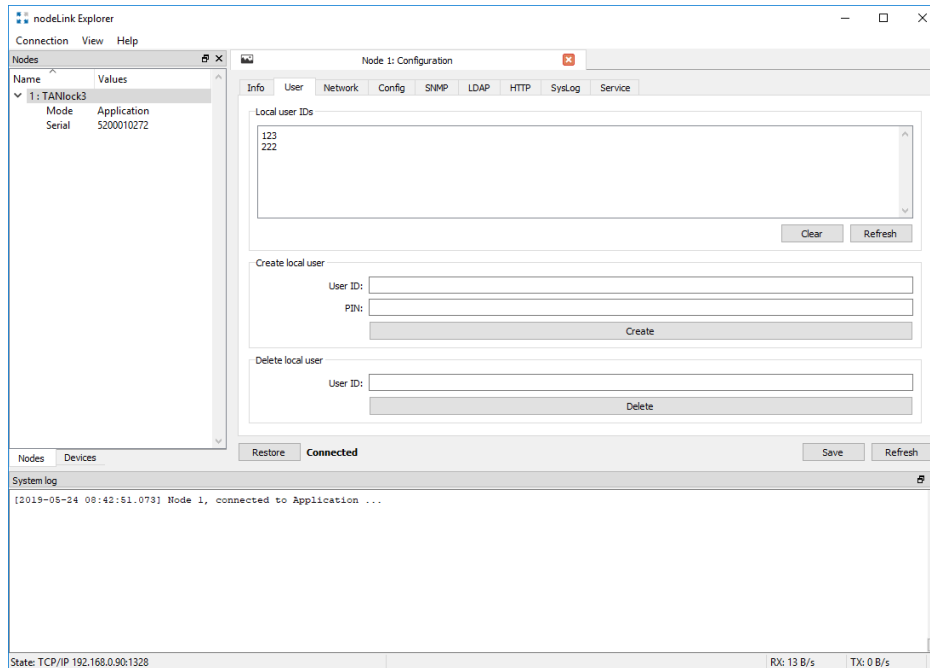
The only tab you can make changes to that does not require a reset/reboot is the 'User' tab as users are stored in a different file to the configuration.

### 1.3.6 TANlock Cockpit – User

Users can be managed either via the Web API (if enabled) or directly from the TANlockExplorer. The User tab was added in firmware version 05.

For customers that have a small number of TANlock 3 products installed then TANlockExplorer may be the only management software that is required.

Log events for access control can be sent to a syslog server like SolarWinds Kiwi syslog server.



If you have the same user credentials to be replicated on multiple TANlocks then this can either be completed by editing each lock and adding the user credentials or by using a batch job via the web.

```
C:\usr\bin>curl -k https://<IP address>/<API Key>/user/create/123/123
```

The user credential format '3 character/3 character' will depend on the settings for 'User ID length' and 'Pin length' set in the 'Config' Tab.

The default value is set to use 3 digits for the 'User ID length' and 3 digits for the 'PIN length'.

A user does not need to know they are using a User ID and PIN as they only know to use a 6-digit number when using the Pin Pad module to open the lock.

From a user point of view, they have a 6-digit PIN number.

If RFID cards are used then users do not need to know what length of PIN authentication is being used.

A user will just position a card over the TANlock reader to authenticate and open the lock.

Whoever has the card can open the lock.

There is an option to enable two factor Authentication where an RFID card + PIN is needed to open the lock to prevent someone using a lost/stolen/borrowed RFID card.

Alternatively two RFID cards might be required.

### 1.3.7 TANlock Cockpit – Network Tab

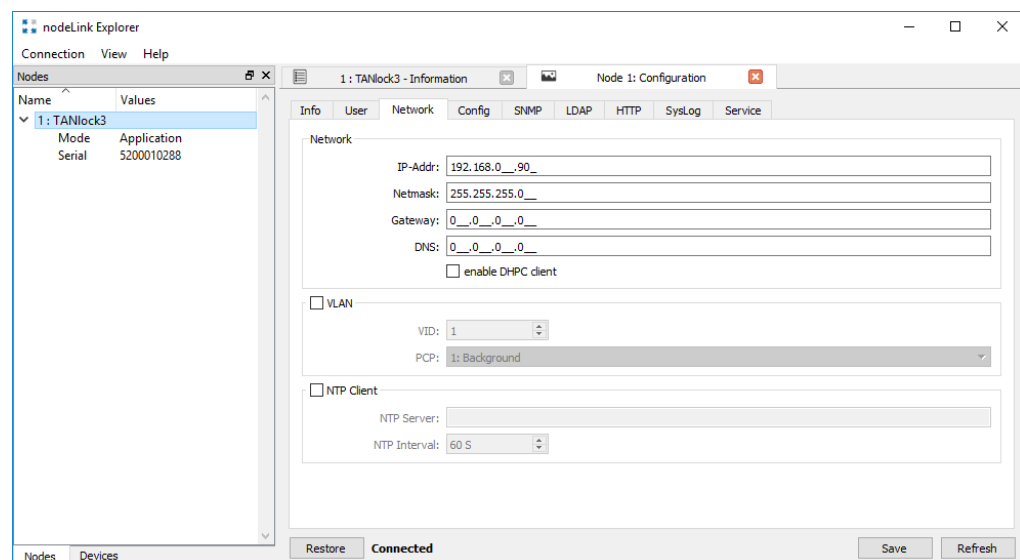
In this tab the network settings are configured.

Most deployments will find it easier to manage all the locks and the rack locations using static IP addresses unless using 3<sup>rd</sup> Party management software to discover and manage the locks.

Using DHCP for the initial deployment can be a useful option if you know the MAC address of the lock so you can identify it at the switch and know which address it has been allocated.

Even using 3<sup>rd</sup> party DCIM software still leaves the problem of keeping track of the exact lock location for, building, floor, rack enclosure, front or back.

Using DHCP to assign IP addresses means there must be some method of tracking the DHCP IP address with the serial number of the lock and the rack door location so that log events can identify which rack door is opened. This might be available in the 3<sup>rd</sup> Party Data Center Management software.



If the switch network port being used for the TANlock is on a port configured as a trunk then the VLAN ID can be set and packets sent to the switch will be VLAN tagged.

For most installs the VLAN ID will not be required. The port on the switch will be assigned to a specific VLAN.

To ensure that the lock keeps correct time an NTP server should be defined. Firewall rules or ACLs at the next gateway may be needed to allow the TANlock network to connect using ntp (port 123/UDP).

To keep configurations simple the next hop gateway is often used as the time source. The next hop gateway would need to be configured as a time source.

### 1.3.8 TANlock Cockpit – Config Tab

Each TANlock should be given a unique device name this might be

location+racknumber+<front/back>

of the rack or just a simple name like 'tanlock1, tanlock2,...'.

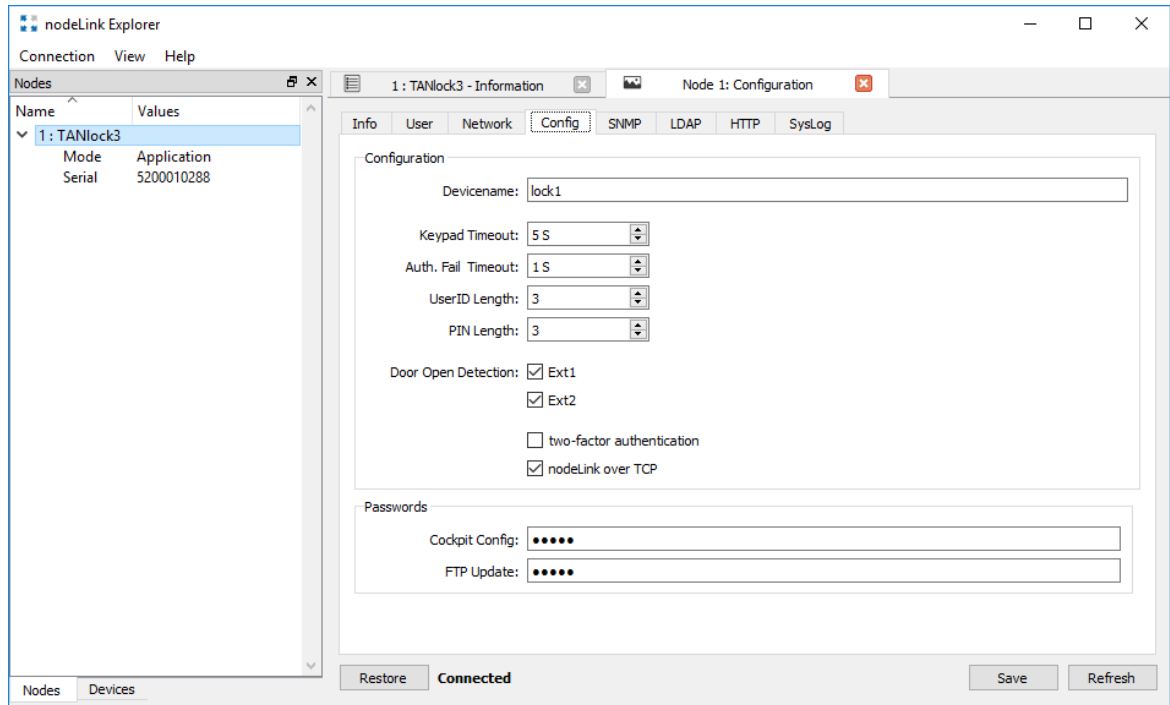
Even numbered locks might be the front and odd numbered might be the back. In some installs there may just be one TANlock for an enclosure as it depends if front and back door access is required.

A naming convention may already exist for customer devices and this is just another device that needs to follow the naming format.

**Keypad Timeout**, after entering a PIN on the keypad this is the time a user is allocated to select the open button (tick). A user that fails to select the open button within the timeout period will need to enter their pin again. Default is 5 seconds.

**Auth. Fail Timeout**, this is the time delay between authentication attempts after a failed authentication. If this value is set to 20 seconds and a failed authentication occurs then the red light will illuminate for 20 seconds and block authentication attempts. Default 1 second.

**User ID length and Pin length**, this setting determines the overall pin length for user authentication regardless of the type of authentication being used. Default value 3.



**two-factor Authentication**, will require two different user credentials to open the TANlock. Default is disabled.

This will work for a PIN Pad and RFID only modules as well as an 'RFID + PIN Pad' module.

For example, if a TANlock has an RFID Module only then it would require two cards to be scanned before unlocking.

If a PIN Pad only TANlock module is used, then two PINs are needed.

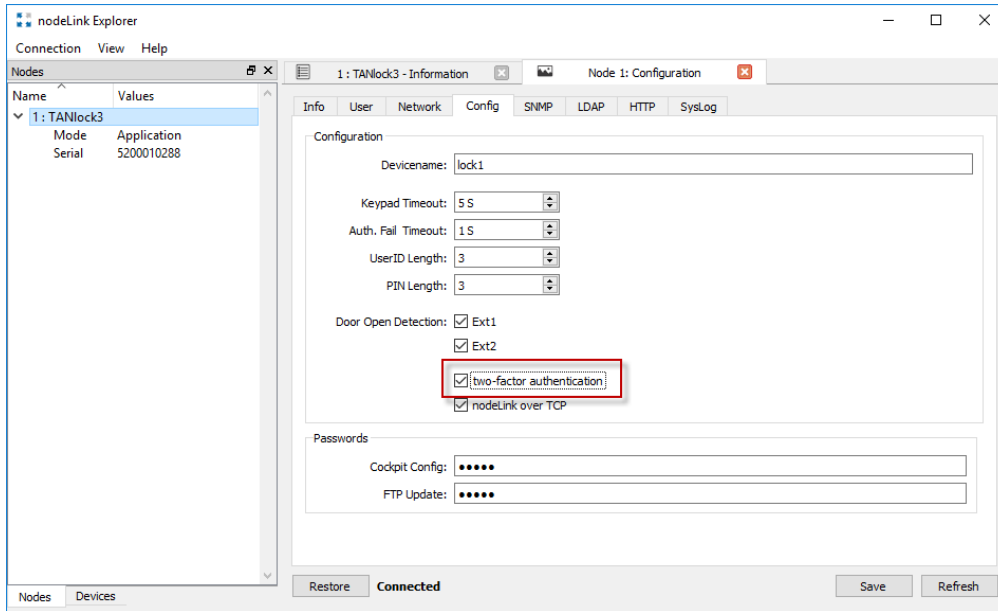
If a TANlock has an RFID + PIN Pad module then the 'two-factor' could be

- RFID card + PIN
- RFID card 1 + RFID card 2
- PIN + PIN
- PIN + RFID Card.

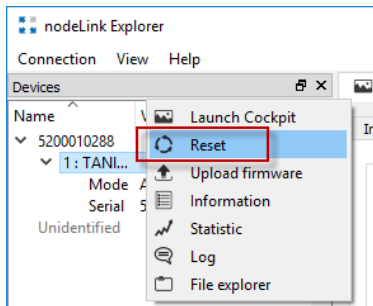
After selecting the 'two-factor authentication' option the TANlock must be reset (rebooted) for the change to take effect.

To change back to single factor authentication then unselect the 'two-factor authentication' option and reset (reboot) the lock.





After setting two-factor authentication make sure the config is saved and lock reset.



The default setting is to not use 'two-factor authentication'.

Note the two factor Authentication could be RFID Card swipe at the lock and remote open command using the Web API from a central command controller, like the NOC.

For example, a user calls the Data Center NOC to get permission to open a rack door, NOC user logs into rack lock management software and enters the rack details requested and selects to open the lock.

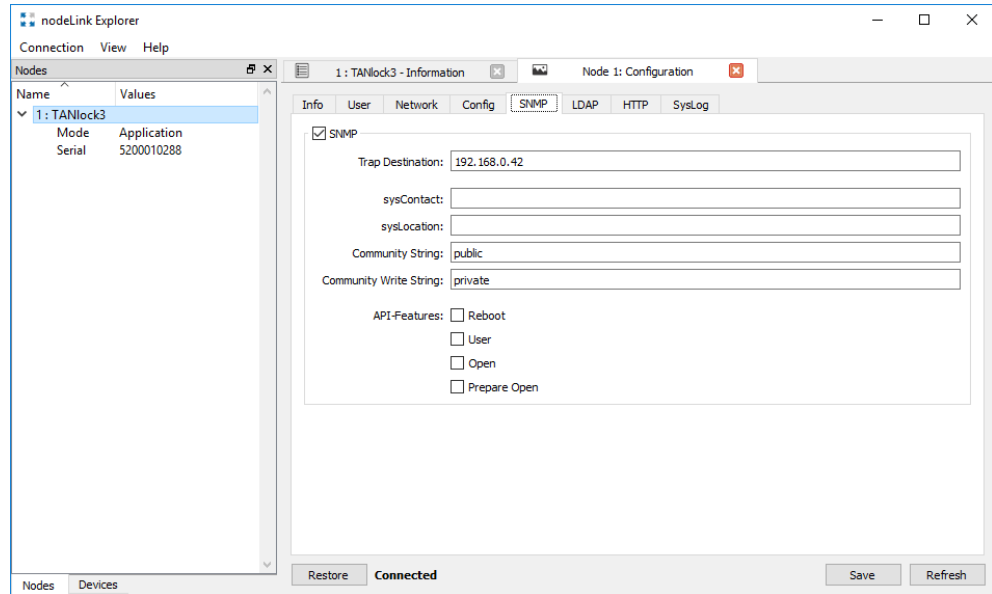
The management software can send a remote open command or a prepare to open command which then allows the user to locally open the lock.

### 1.3.9 TANlock Cockpit – SNMP Tab

If SNMP is not enabled, then the SNMP daemon will not be started and queries for SNMP MIB variables will not work. The 3<sup>rd</sup> Party software management tools tends to use the SNMP attributes to poll the status of the lock attributes and receive SNMP traps when authentication and open/close events occur.

If SNMP traps are to be sent for events, like user authentication, open and close handle events then set the IP address of the SNMP server to send the events to.

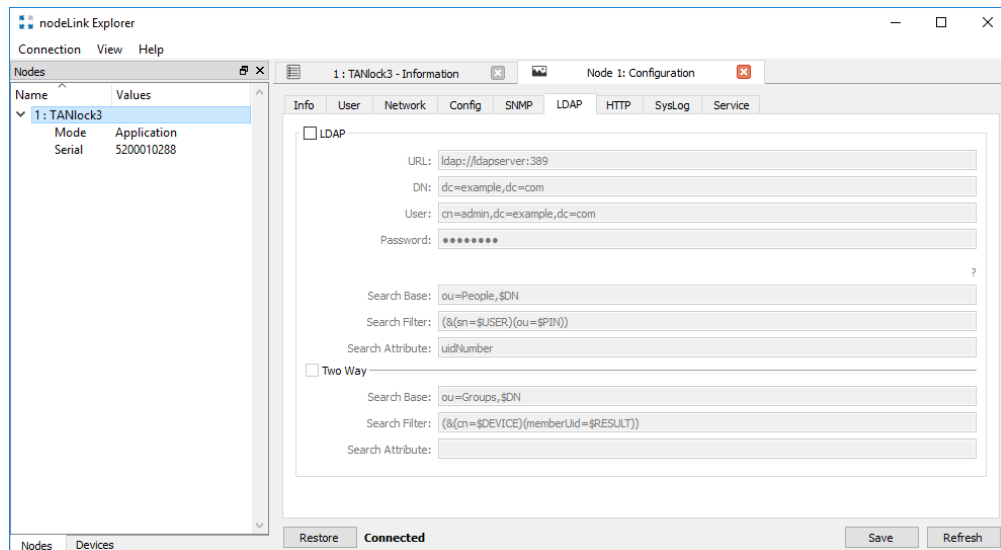
If you need to use the FQDN (fully qualified Domain Name) instead of the IP address, make sure that a DNS server has been set in the 'Network' tab and that the locks can connect to the DNS server which may be located anywhere on the routable network.



SNMP V1 and V2 is supported.  
SNMP 3 is not currently supported. This will require a firmware update in the future.

### 1.3.10 TANlock Cockpit – LDAP

The TANlock can use an external LDAP server like ApacheDS (<https://directory.apache.org/apacheds/>) or Microsoft Active Directory to match attributes to centrally store the user credentials.



If LDAP is enabled and the server details are correctly configured, then the user credentials are searched first in the LDAP database and then if not found the local lock database is searched.

The settings in the configuration fields for using ApacheDS and Microsoft AD are different.

Setting the parameters incorrectly may cause the lock to reset.

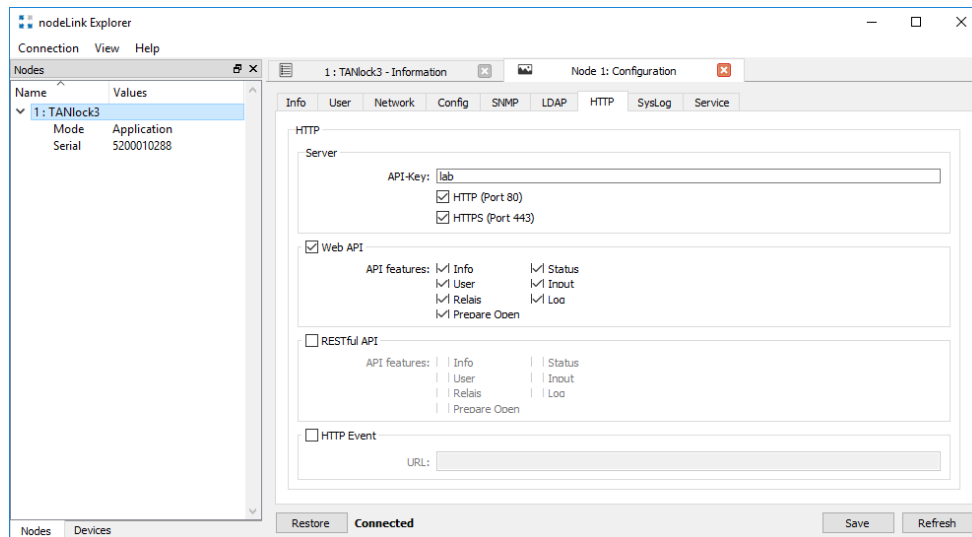
### 1.3.11 TANlock Cockpit - HTTP

The HTTP Tab controls the Web API commands that are enabled and the connection method HTTP or HTTPS.

For some deployments the HTTP web API commands may not be needed are not enabled.

In some environments TANlockExplorer may be the only management tool required and remote configuration of users or remote opening via the web API is not required.

If you do not want the TANlock to be remotely opened via 3<sup>rd</sup> party software or URL commands, then do not enable the 'input' API option.



#### Server

This applies to the web server running on the TANlock. The web server has very limited capability and tailored to specific API commands to manage the lock.

**API-Key**, this is an optional unique string associated with each lock. For some sites this may be the same for every lock and others it may be unique for each lock. FATH Mechatronics recommend that a unique API-Key is used for each lock. Using a unique API-Key means that administrators need to keep track of the lock and matching API-Key. However, if the locks are managed by 3<sup>rd</sup> party central software this should not be a problem as the software will maintain an internal database of the details.

HTTP – Select HTTP to allow clear text HTTP traffic to the lock IP address.  
HTTPS – Select HTTPS allow encrypted HTTP traffic to the lock IP address.

**FATH Mechatronics recommend that you only enable HTTPS.**

The SSL certificate is a self-signed certificate and therefore communications between the management server and the lock are susceptible to MITM (Man In The Middle) attacks.

However, the network the TANlocks are assigned will most likely be a closed private network so the only attackers should be local administrators and network users.

It is not really practical to try and deploy a signed certificate on the TANlock but this may be an option if there is a certificate authority server accessible in the network infrastructure.

**Web API** – Select this to use the Web interface commands via http or https commands from a command line or web browser.  
This is the main interface used by 3<sup>rd</sup> Party management applications to interface with the Lock for creating users and generating remote open events.

The 3<sup>rd</sup> party management software can also interface with the lock using SNMP get/set but is not meant for creating user credentials.

The Web API has a very limited number of commands. This means 3<sup>rd</sup> party software vendors can develop API interfaces between their software and TANlocks in a relatively short time.

A typical web interface command line request might be

```
curl -k https://192.168.0.90/<API-Key>/help  
curl -k https://192.168.0.90/<API-Key>/info  
curl -k https://192.168.0.90/<API-Key>/user/create/123/123  
curl -k https://192.168.0.90/<API-Key>/user/delete/123
```

'**curl**' is a free command line tool that can be used to send https requests to a server.

The -k option suppresses the error messages that would occur if the https server uses a default self-signed SSL certificate.

**RESTful API** – Select this if your programming environment requires non state information to be stored on the lock web server.

Extract from - <https://restfulapi.net/>

REST is acronym for REpresentational State Transfer. It is architectural style for **distributed hypermedia systems** and was first presented by Roy Fielding in 2000 in his famous [dissertation](#).

Like any other architectural style, REST also does have it's own **6 guiding constraints** which must be satisfied if an interface needs to be referred as **RESTful**. These principles are listed below.

## Guiding Principles of REST

1. **Client-server** – By separating the user interface concerns from the data storage concerns, we improve the portability of the user interface across multiple platforms and improve scalability by simplifying the server components.
2. **Stateless** – Each request from client to server must contain all of the information necessary to understand the request, and cannot take advantage of any stored context on the server. Session state is therefore kept entirely on the client.
3. **Cacheable** – Cache constraints require that the data within a response to a request be implicitly or explicitly labeled as cacheable or non-cacheable. If a response is cacheable, then a client cache is given the right to reuse that response data for later, equivalent requests.
4. **Uniform interface** – By applying the software engineering principle of generality to the component interface, the overall system architecture is simplified and the visibility of interactions is improved. In order to obtain a uniform interface, multiple architectural constraints are needed to guide the behavior of components. REST is defined by four interface constraints: identification of resources; manipulation of resources through representations; self-descriptive messages; and, hypermedia as the engine of application state.
5. **Layered system** – The layered system style allows an architecture to be composed of hierarchical layers by constraining component behavior such that each component cannot “see” beyond the immediate layer with which they are interacting.
6. **Code on demand (optional)** – REST allows client functionality to be extended by downloading and executing code in the form of applets or scripts. This simplifies clients by reducing the number of features required to be pre-implemented.

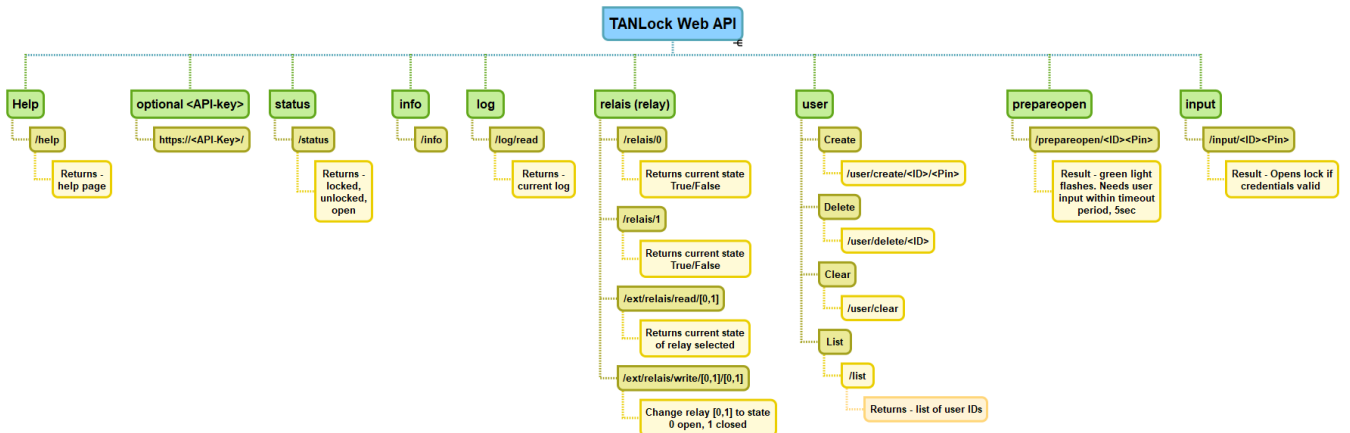
## HTTP Event

Enter a URL that events will be sent to that can handle the data being sent.

This could be anything which just processes the event details and emails an alert or generates an SMS message each time a lock is opened.

## Summary of the Web API commands.

Note the only command that does not have the option of using the API-Key in the URL is the '/help'.



New API sub commands may be added in updated firmware releases as new features are introduced.

For a summary of the current commands and examples of the format to use then use

<https://192.168.0.90/help>

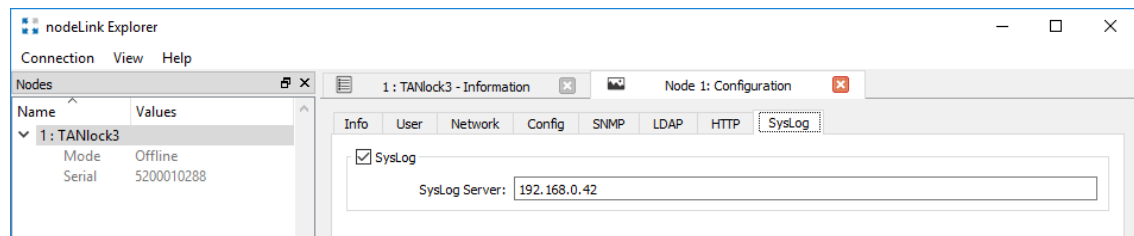
If you have not enabled the Web API then the help request URL will not return anything.

### 1.3.12 TANlock Cockpit - Syslog

In this tab the IP address or FQDN of the syslog server can be set.

For environments that use a small number of TANlocks a simple syslog server can be used. For example, Kiwi syslog, rsyslog, logstash.

For 3<sup>rd</sup> party management software solutions, they are likely to have both syslog & SNMP servers integrated as part of their software solution.



A common problem with syslog servers is information gets logged but never analyzed.

Many sites are now integrating SIEM (Security Information & Event Management) software where syslog events are logged to a central server and reports generated at regular intervals looking for specific types of events.

For any log data to be meaningful the date and time stamp must be correct.

Make sure the NTP server option is set and that the NTP server is accessible.

### 1.3.13 TANlock Cockpit - Service

This tab is not usually used in general day to day operations of the TANlock.

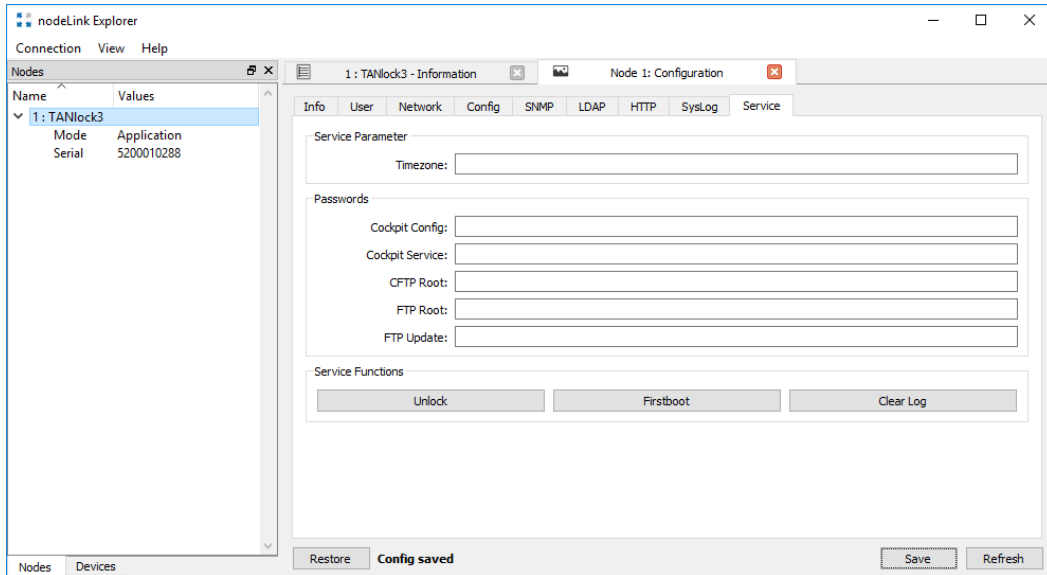
It can be used for the following

- To change all the default passwords.
- To unlock the lock independent of the defined users on the lock.
- To put the TANlock into service mode (First boot) for safe transport with the lock latch in the unlock position.
- To clear the log file that is stored on the TANlock.

The log file on the TANlock is a revolving log file and overwritten every 1000 entries.

To put the lock back into normal mode after selecting 'Firstboot' so that the latch will lock, disconnect the power supply and then reconnect the power.

Removing and reconnecting power completes a first boot cycle and moves the locking latch to the correct position'.



The default base 'Config' mode password for TANlockExplorer is 91174.

This only gives access to the basic 'config' parameters.

The default password to access the 'Service' mode is 15973.

The password can be either plain text or stored as an MD5 Hash. The default is plain text.

```
Plaintext password or
md5-hash
Syntax: "MD5:<hex-
hash>"
```

To generate and store the password in the /config/config.txt file in MD5 format then generate an MD5 hash for the password you want to use.

You need an MD5 hash program.

Some systems have one installed by default, however, Microsoft Windows does not.

New password for 'Config mode' to be '12345'.

```
D:\Data\Customers>md5 -d12345
827CCB0EEA8A706C4C34A16891F84E7B
```

Take the MD5 hash output and paste it into the password field for the 'Cockpit Config' password. This can only be done if you are logged into 'Service' mode.

Info	User	Network	Config	SNMP	LDAP	HTTP	SysLog	Service
Service Parameter								
Timezone: CET-1CEST,M3.5.0,M10.5.0/3								
Passwords								
Cockpit Config: MD5:827CCB0EEA8A706C4C34A16891F84E7B								
Cockpit Service: 15973								
CFTP Root: 15973								
FTP Root: 15973								
FTP Update: 91174								
Service Functions								
Unlock			Firstboot			Clear Log		

If you check the /config/config.txt file, (see File explorer) then the password is now stored as the MD5 hash and not simple cleartext.

This is a more secure method of deploying TANlocks in a production environment but adds a level of overhead that some sites may not want or need.

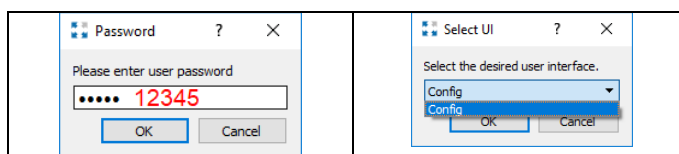
This may be a requirement for audit compliance for environments that need to be PCI-DSS or HIPPA compliant. General rule for those environments, passwords cannot be stored in plain text format.

```

config = {
  access = {
    cftp = {
      user = {
        root = "15973"
      }
    },
    cockpit = {
      config = "MD5:827CCB0EEA8A706C4C34A16891F84E7B",
      service = "15973"
    },
    ftp = {
      user = {
        root = "15973",
        update = "91174"
      }
    }
  },
}

```

Test using the password to login to 'Config' mode Cockpit.



The TANlockExplorer dialog takes the password '12345' converts it to an MD5 hash and it is the MD5 hash that is passed over the network so even if the network traffic is monitored then the password is relatively secure.

In future the initial base configuration may use MD5 by default. This change in behavior will not affect the use of the default passwords shipped with the TANlock.



**Service Mode Password** - If the 'Service' mode password is changed and lost then it cannot be recovered by FATH Mechatronics.

However, it is possible to reset the config of the TANLock back to the basic delivery config.txt if you know the 'Config' mode password.

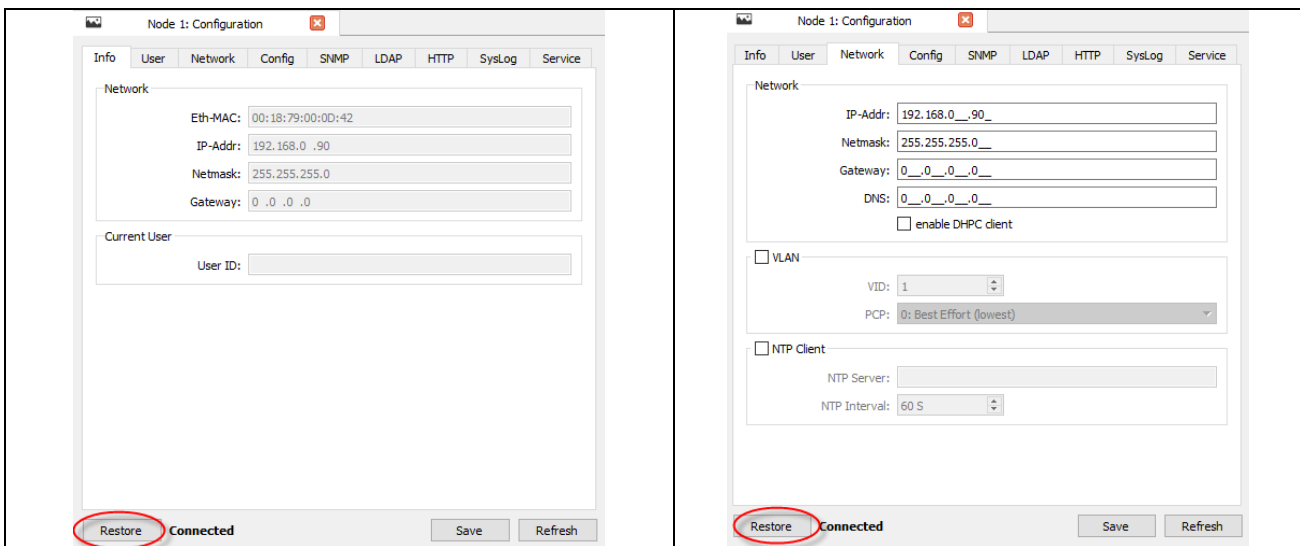
Make sure a copy of the 'Service' password for each lock is stored in a secure location.

If the passwords for Cockpit, CFTP root, FTP root, FTP Update have been changed and lost then it may be problematic to get the passwords back without affecting the normal operation of the lock.

The default passwords use numeric only characters, but any alphanumeric character can be used, 0-9, a-z, uppercase/lowercase.

### 1.3.14 TANLock – Restore 'Config'

There is an option in each of the Config tabs to restore the config to an initial base configuration. The restore can be done from either 'Config' or 'Service' mode.



This will restore a base config.txt file when logged in with either the 'Config' or 'Service' mode password.

**Do not select the restore unless you really do want to reset the lock configuration back to the initial base configuration.**

This will include unselecting the Web API commands and resetting the IP address of the lock back to 192.168.0.90. It will also reset all passwords back to the default delivery passwords.

- You will need to select 'Restore'.
- Check and change any of the tab config parameters.
- Save the config.
- Reset the lock.

- You may also need technical support to reconfigure the config.txt file to enable RFID cards to work.

Any 'Restore' config operation is best done when using the TANlockExplorer\_USB interface.

If you restore and save the config while connected via a network link, then you will lose connectivity as the IP address will change back to the initial configuration IP address of 192.168.0.90.

The users.json file will also be restored to the original so all the locally defined users will be lost and need to be recreated.

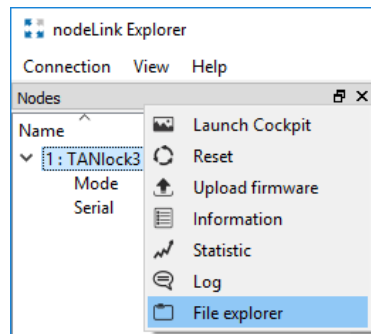
The 'restore' config is an option if you have lost the 'Service' password but know the base 'Config' password.

At least you can get full control back over the lock, but it will need to be reconfigured and this usually needs to be completed by connecting locally via the USB interface.

### 1.3.15 TANlock File Explorer

Only trained administrators should have access to the File explorer within the TANlockExplorer tool as it is possible to delete or accidentally move files/directories that are critical to the locks normal function.

This is not a function that will be required on a regular basis and probably only needed during initial setup for an unusual situation or to help with a technical issue and edit the /config/config.txt file under the guidance of Technical support.



By default, the passwords for all admin accounts are in clear text unless MD5 hash format has been used.

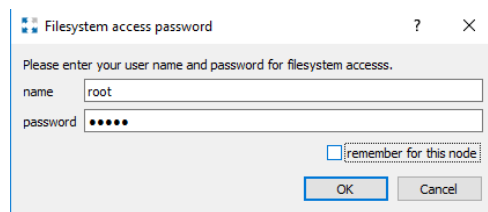
The MD5 hash format can be set within the 'Service' tab so there is no reason to directly edit the file to set secure passwords.

```
config = {
  access = {
    cftp = {
      user = {
        root = "15973"
      }
    },
    cockpit = {
      config = "91174",
      service = "15973"
    },
    ftp = {
      user = {
        root = "15973",
        update = "91174"
      }
    }
  },
}
```

The passwords for all admin type users are stored in the file /config/config.txt.

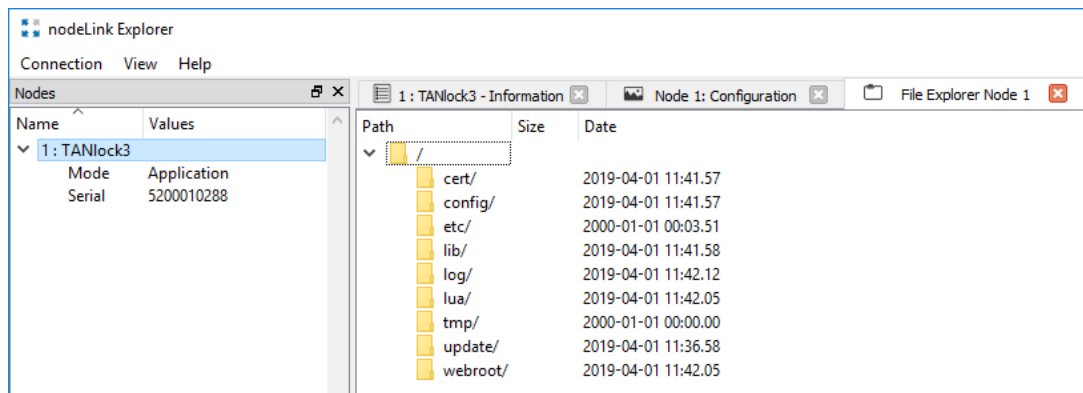
Enter the username - 'root' and the password for cftp.

This is the console FTP password and gives full access to the filesystem. Be very careful not to move or delete files as this may break the lock.



The File Explorer tab will be started, it allows file Edits, Downloads, Copy, Move and Delete.

It is possible to accidentally delete a block of text while editing a file and that will corrupt the file and cause problems with the lock if you save the file and do not notice the deleted section.



The main config file is /config/config.txt. This is a useful file to have a backup copy stored in a safe location for at least one of your TANlocks.

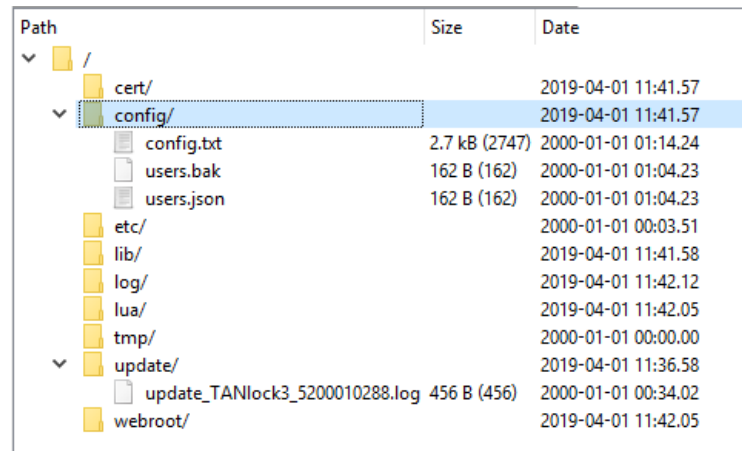
If you need to edit the config.txt file, then it is better to ftp it to a local PC, edit it and put it back.

This file, with some restrictions, is portable between TANlocks but not 100% compatible with each lock.

Some settings in the file are specific to the authentication module type installed in the lock and may cause problems if parameters are incorrectly set.

If you are unsure of the configuration content and the TANlock authentication module then always check with technical support before implementing the change.

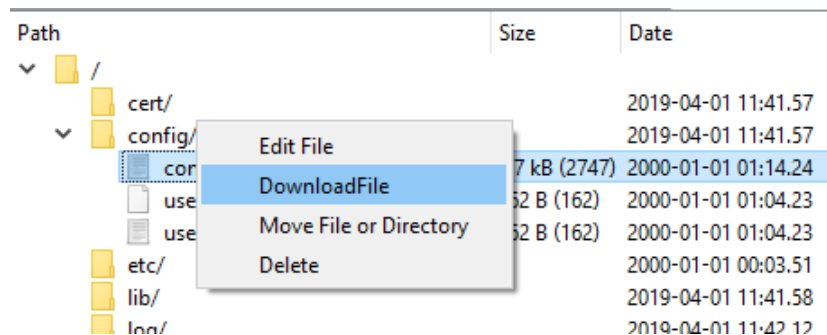
Technical support will be able to confirm the file does not contain conflicts that will cause problems with the authentication module being used.



Path	Size	Date
/		
cert/		2019-04-01 11:41:57
config/		2019-04-01 11:41:57
config.txt	2.7 kB (2747)	2000-01-01 01:14:24
users.bak	162 B (162)	2000-01-01 01:04:23
users.json	162 B (162)	2000-01-01 01:04:23
etc/		2000-01-01 00:03:51
lib/		2019-04-01 11:41:58
log/		2019-04-01 11:42:12
lua/		2019-04-01 11:42:05
tmp/		2000-01-01 00:00:00
update/		2019-04-01 11:36:58
update_TANlock3_5200010288.log	456 B (456)	2000-01-01 00:34:02
webroot/		2019-04-01 11:42:05

The defined users are in 'users.json' and the last version of 'users.json' is stored in 'users.bak'.

The users.json file contains the user and pin details. **This file should NOT be copied off the lock and stored externally.**



Path	Size	Date
/		
cert/		2019-04-01 11:41:57
config/		2019-04-01 11:41:57
config.txt	2.7 kB (2747)	2000-01-01 01:14:24
users.bak	162 B (162)	2000-01-01 01:04:23
users.json	162 B (162)	2000-01-01 01:04:23
etc/		2000-01-01 00:03:51
lib/		2019-04-01 11:41:58
log/		2019-04-01 11:42:12

The expanded directory paths for a firmware version 06 should look like the following.

Path	Size	Date
▼ /		
▼ cert/		2019-04-01 06:41:57
ca.crt	2.6 kB (2612)	1999-12-31 19:20:55
server.crt	1.2 kB (1194)	1999-12-31 19:20:54
server.key	1.7 kB (1704)	1999-12-31 19:20:54
▼ config/		2019-04-01 06:41:57
config.txt	3.0 kB (2958)	1999-12-31 22:11:33
users.bak	48 B (48)	1999-12-31 23:19:54
users.json	48 B (48)	1999-12-31 23:19:54
etc/		1999-12-31 19:03:51
▼ lib/		2019-04-01 06:41:58
> cgilua/		2019-04-01 06:41:59
json.lua	17.3 kB (17346)	1999-12-31 19:20:56
jsonrpc.lua	4.2 kB (4185)	1999-12-31 19:21:02
luaprint.lua	4.8 kB (4755)	1999-12-31 19:21:02
preload.lua	200 B (200)	1999-12-31 19:20:56
▼ log/		2019-04-01 06:42:12
events_0.log	32.7 kB (32745)	1999-12-31 20:00:04
events_1.log	18.4 kB (18363)	1999-12-31 22:11:42
log_0.txt	262.1 kB (262122)	1999-12-31 21:11:37
log_1.txt	3.8 kB (3831)	1999-12-31 21:11:38
▼ lua/		2019-04-01 06:42:05
mod/		1999-12-31 19:21:03
main.lua	573 B (573)	1999-12-31 19:21:03
tmp/		1999-12-31 21:11:38
▼ update/		2019-04-01 06:36:58
update_TANlock3_5200010288.log	1.6 kB (1602)	1999-12-31 19:21:04
▼ webroot/		2019-04-01 06:42:05
help/		2019-04-01 06:42:06
index.htm	2.8 kB (2813)	1999-12-31 19:21:04
tanlock3_1.11.mib	10.5 kB (10465)	1999-12-31 19:21:04

You can fetch the TANlock MIB database from the webroot directory and view the attributes using a tool like 'iReasoning MIB Browser'.

Using a tool like 'iReasoning' or 'snmpwalk' may be the first step that 3<sup>rd</sup> party software developers use as many of the monitoring values need for the lock status can be read as SNMP attributes.

You can only use SNMP with the TANlock if it is enabled in the SNMP tab and the read community string has been set.

SNMP  
 Trap Destination: 192.168.0.42  
 sysContact:   
 sysLocation:   
 Community String: public  
 Community Write String: private  
 API-Features:  Reboot  
 User  
 Open  
 Prepare Open

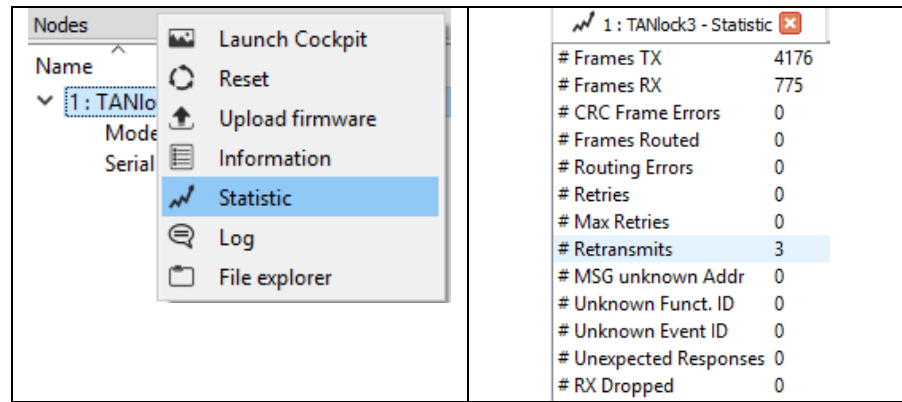
Setting the 'Trap Destination' is optional but in many environments a central SNMP monitoring server will exist and depending on the network infrastructure and security policy the TANlock may be able to send traps to the central server.

Monitored trap events often have alerts like email or SMS associated with them so that quick responses can be actioned in the event of a critical event.

3<sup>rd</sup> party management software will use SNMP to monitor MIB attributes and process SNMP Traps to react to changes in the lock status.

### 1.3.16 TANlock Statics

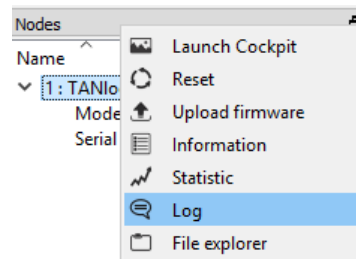
This is just basic statistics related to network connectivity to the TANlock.



This information is also available from the SNMP server running on the TANlock as attributes that can be fetched using the SNMP get command.

### 1.3.17 TANlock Log

The log is a useful debugging tool within the TANlockExplorer tool and can be used to easily identify the details of an RFID card to find the card UID.



There is an internal log stored on the TANlock that is a revolving log limited to 1000 entries. The oldest entries are over written when the log is full.

**To view the internal detailed log events, you must directly connect to the lock using TANlockExplorer.**

The TANlock can log to a syslog server and send SNMP trap events for user authentication and lock open/close events to store the logs centrally.

The log events and traps are not as detailed when sent to a central syslog server.

There is an option in the bottom right corner to delete the current local TANlock log file (dustbin icon).

Log Node 1 (Connected)						
System time	Timestamp	Line	Module	Context	Function	Text
2019-05-30 12:10:36.585	03259931	927	http_mod_web...	HTTP_WRK00	http_mod_web...	WEBAPI-API called with '/input/123123'
2019-05-30 12:11:07.445	03290796	927	http_mod_web...	HTTP_WRK01	http_mod_web...	WEBAPI-API called with '/lab/input/123123'
2019-05-30 12:11:07.445	03290797	865	http_mod_web...	HTTP_WRK01	_handler_call	RESOURCE: '/123123'
2019-05-30 12:11:07.445	03290798	312	lock	APP	_on_input	AUTH: input=123123, len=6
2019-05-30 12:11:07.445	03290798	360	lock	APP	_on_input	AUTH: user_id=123, pin=123
2019-05-30 12:11:07.445	03290799	386	lock	APP	_on_input	AUTH: LOCAL request
2019-05-30 12:11:07.445	03290799	398	lock	APP	_on_input	AUTH: MASTER request
2019-05-30 12:11:07.445	03290799	413	lock	APP	_on_input	AUTH: success=FALSE
2019-05-30 12:11:07.492	03290850	131	log	APP	_log_event	LOG: auth failure
2019-05-30 12:11:07.492	03290852	188	logapi	APP	_file_open	using logfile '/log/events_0.log'
2019-05-30 12:15:01.353	03524242	131	log	ERFC:PROCESS	_log_event	LOG: local user created: 123
2019-05-30 12:15:01.353	03524242	188	logapi	ERFC:PROCESS	_file_open	using logfile '/log/events_0.log'
2019-05-30 12:15:16.006	03539357	927	http_mod_web...	HTTP_WRK02	http_mod_web...	WEBAPI-API called with '/lab/input/123123'
2019-05-30 12:15:16.006	03539357	865	http_mod_web...	HTTP_WRK02	_handler_call	RESOURCE: '/123123'
2019-05-30 12:15:16.006	03539359	312	lock	APP	_on_input	AUTH: input=123123, len=6
2019-05-30 12:15:16.006	03539359	360	lock	APP	_on_input	AUTH: user_id=123, pin=123
2019-05-30 12:15:16.006	03539359	386	lock	APP	_on_input	AUTH: LOCAL request
2019-05-30 12:15:16.006	03539360	131	log	APP	_log_event	LOG: auth success via local user uid=123
2019-05-30 12:15:16.006	03539362	188	logapi	APP	_file_open	using logfile '/log/events_0.log'
2019-05-30 12:15:16.131	03539490	413	lock	APP	_on_input	AUTH: success=TRUE
2019-05-30 12:15:16.746	03540089	250	lock	APP	_event_hal_un...	UNLOCK
2019-05-30 12:15:16.746	03540089	131	log	APP	_log_event	LOG: unlocked
2019-05-30 12:15:16.747	03540089	188	logapi	APP	_file_open	using logfile '/log/events_0.log'

Example, detailed local lock log entries attempting to authenticate via sending input using the Web API.

```

2019-05-30 12:10:36.585 03259931 927 htt p_mod_webapi HTTP_WRK00 http_mod_webapi_call WEBAPI-API called with
'/input/123123'
2019-05-30 12:11:07.445 03290796 927 http_mod_webapi HTTP_WRK01 http_mod_webapi_call WEBAPI-API called with
'/lab/input/123123'
2019-05-30 12:11:07.445 03290797 865 http_mod_webapiHTTP_WRK01 _handler_call RESOURCE: '/123123'
2019-05-30 12:11:07.445 03290798 312 lock APP _on_input AUTH: input=123123, len=6
2019-05-30 12:11:07.445 03290798 360 lock APP _on_input AUTH: user_id=123, pin=123
2019-05-30 12:11:07.445 03290799 386 lock APP _on_input AUTH: LOCAL request
2019-05-30 12:11:07.445 03290799 398 lock APP _on_input AUTH: MASTER request
2019-05-30 12:11:07.445 03290799 413 lock APP _on_input AUTH: success=FALSE
2019-05-30 12:11:07.492 03290850 131 log APP _log_event LOG: auth failure
2019-05-30 12:11:07.492 03290852 188 logapi APP _file_open using logfile '/log/events_0.log'
2019-05-30 12:15:01.353 03524242 131 log ERFC:PROCESS log_event LOG: local user created: 123
2019-05-30 12:15:01.353 03524242 188 logapi ERFC:PROCESS _file_open using logfile
'/log/events_0.log'
2019-05-30 12:15:16.006 03539357 927 http_mod_webapiHTTP_WRK02 http_mod_webapi_call WEBAPI-API called with
'/lab/input/123123'
2019-05-30 12:15:16.006 03539357 865 http_mod_webapiHTTP_WRK02 _handler_call RESOURCE: '/123123'
2019-05-30 12:15:16.006 03539359 312 lock APP _on_input AUTH: input=123123, len=6
2019-05-30 12:15:16.006 03539359 360 lock APP _on_input AUTH: user_id=123, pin=123
2019-05-30 12:15:16.006 03539359 386 lock APP _on_input AUTH: LOCAL request
2019-05-30 12:15:16.006 03539360 131 log APP _log_event LOG: auth success via local user uid=123
2019-05-30 12:15:16.006 03539362 188 logapi APP _file_open using logfile '/log/events_0.log'
2019-05-30 12:15:16.131 03539490 413 lock APP _on_input AUTH: success=TRUE
2019-05-30 12:15:16.746 03540089 250 lock APP _event_hal_unlock UNLOCK
2019-05-30 12:15:16.746 03540089 131 log APP _log_event LOG: unlocked
2019-05-30 12:15:16.747 03540089 188 logapi APP _file_open using logfile '/log/events_0.log'
2019-05-30 12:15:16.746 03540089 131 log APP _log_event LOG: unlocked
2019-05-30 12:15:16.747 03540089 188 logapi APP _file_open using logfile '/log/events_0.log'

```

The log entries above show that the first call to open the lock was ignored. No response or acknowledgement event.

The second call to open the lock used the **correct API-Key <lab>** but the user credentials are not valid.

A user 123 was created.

A call to open the lock with the Web API for user 123 was successful.

If you scan a new RFID card then you can obtain the card UID details.

In the example log below for an RFID card swipe since user id length and Pin length has been set to 3 then the program calculated the user ID as **cf6** and the password as **6d0**.

The card UID is **fcb60162d**.

The user ID/PIN are case sensitive. If you use a mobile app to display the card UID it will likely display everything in uppercase for clarify.

The TANLock expects the card UID to be in lowercase.

```
2019-05-30 14:08:22.643 00031698 278 rfidmod rfidmod _scan_cb +++ RFID uid=fcb6016d
2019-05-30 14:08:22.643 00031698 305 rfidmod rfidmod _scan_cb => UserID : cf6
2019-05-30 14:08:22.643 00031698 314 rfidmod rfidmod _scan_cb => PIN : 6d0
2019-05-30 14:08:22.643 00031698 312 lock APP _on_input AUTH: input=cf66d0, len=6
2019-05-30 14:08:22.643 00031698 360 lock APP _on_input AUTH: user_id=cf6, pin=6d0
2019-05-30 14:08:22.643 00031699 386 lock APP _on_input AUTH: LOCAL request
2019-05-30 14:08:22.643 00031699 398 lock APP _on_input AUTH: MASTER request
2019-05-30 14:08:22.643 00031699 413 lock APP _on_input AUTH: success=FALSE
2019-05-30 14:08:22.690 00031750 131 log APP _log_event LOG: auth failure
2019-05-30 14:08:22.690 00031753 188 logapi APP _file_open using logfile '/log/events_0.log'
2019-05-30 14:08:22.830 00031885 1041 snmpapi APP snmpapi_trap_send SNMP_TRAP: event=6
2019-05-30 14:08:22.830 00031885 1015 snmpapi APP snmpapi_trap_state_chaned SNMP_TRAP: STATE_CHANGED
```

For standard Mifare 1K cards with a 4 Byte UID then the user ID and PIN length would normally be set to 8 digits because there will be 8 hexadecimal characters.

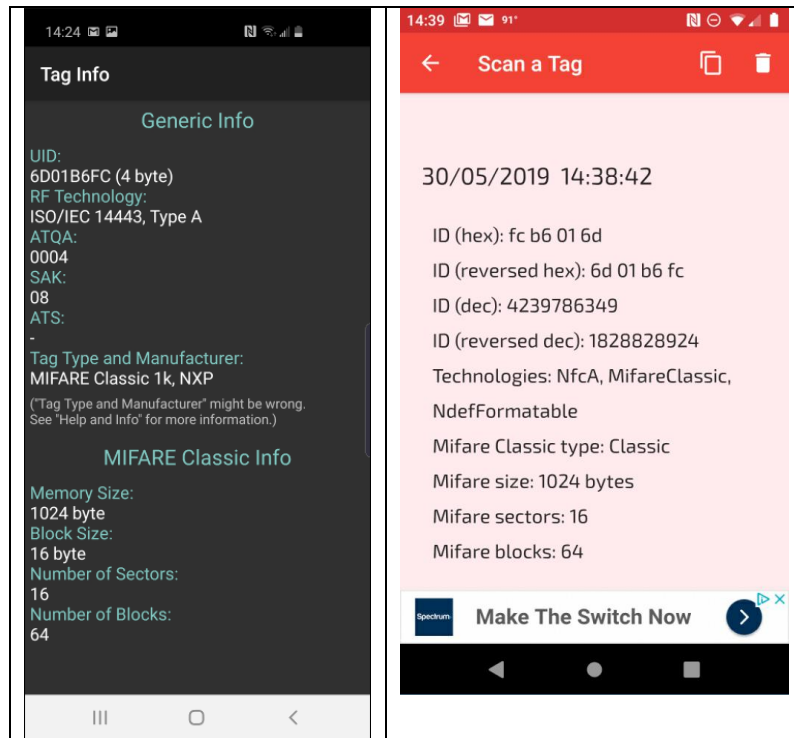
Each byte being 2 hexadecimal characters.

Setting the user ID and PIN length to 8 digits may not be practical if using 'Two factor authentication' (RFID+PIN) as it would require the user to swipe the RFID card and then type in a 16 digit PIN.



The following shows an RFID card read using the phone App 'MCT Mifare Classic Tools' & 'NFC Reader'.

Both apps need NFC turned on to be able to read the RFID card.



There is no standard for how the UID will be read and displayed, uppercase, lowercase, big endian, little endian.

Some readers will use big endian and read the first byte from the left and others will use little endian to read the first byte from the right.

This is one reason why different vendors RFID card systems installed in a building using Weigand protocol might not work with each other unless the software application is adjusted for reading the card correctly for the format being used.

This is not normally a problem as it's a software programming issue and relatively easy to adjust to the different formats.

The only thing that matters is how the TANlock firmware sees the card UID.

The detailed debug log on the TANlock can be used to provide the user ID and PIN that the software calculates and can then be set using the TANlockExplorer tool, Web API or 3<sup>rd</sup> party management software.

Any RFID enabled TANlock can be used to read and debug the details of a new card.

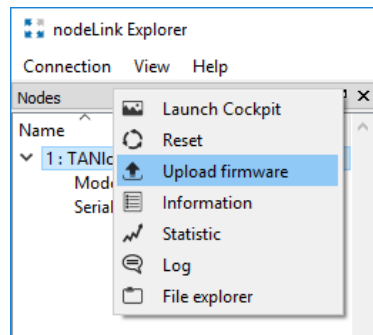
If using a PIN Pad TANlock, then a 3 digit user ID and Pin is set so that the user has to enter a total of 6 digits.

The end user does not need to know that the 6 digits are split into a user ID part and a PIN part.

To a user, there are 6-digits that make up their PIN to provide access.

### 1.3.18 TANlock Upload firmware

This option allows the upload of a new version of the firmware to the Lock.



An alternative and preferred method is to use an FTP client like WINSCP or FileZilla.

There is an 'update' account that can be used with the FTP client to upload the firmware.

The default password for the 'update' account is the same as the 'Config' Cockpit password.

Username: update, Default Password: 91174

```
config = {
  access = {
    cftp = {
      user = {
        root = "15973"
      }
    },
    cockpit = {
      config = "91174",
      service = "15973"
    },
    ftp = {
      user = {
        root = "15973",
        update = "91174"
      }
    }
  },
}
```

Before uploading the file make sure you know the MD5 and/or SHA1 Hash of the file you are about to upload.

You may have to install an MD5/SHA1 tool to create MD5 Hashes.

```
D:\Data\Customers\Fath-Engineering\Firmware-Updates\TANlock3>dir
Volume in drive D has no label.
Volume Serial Number is DA0E-8798
```

```
Directory of D:\Data\Customers\Fath-Engineering\Firmware-Updates\TANlock3
```

```

14-Jun-19 12:26 <DIR>      .
14-Jun-19 12:26 <DIR>      ..
12-May-19 04:07 <DIR>      05c-log-errors
10-May-19 08:45          495,640 1151.100.00-0_TANlock3_05a_20190510.ddc
12-May-19 03:09          496,832 1151.100.00-0_TANlock3_05c_20190510.ddc
14-May-19 05:15          497,088 1151.100.00-0_TANlock3_05d_20190513.ddc
10-May-19 09:27          486,856 1151.100.00-0_TANlock3_05_20190429.ddc
06-Jun-19 01:32          533,952 1151.100.00-0_TANlock3_06_20190528.ddc
23-May-19 16:23 <DIR>      chkdir
                    5 File(s)      2,510,368 bytes
                    4 Dir(s)    28,932,706,304 bytes free

```

```

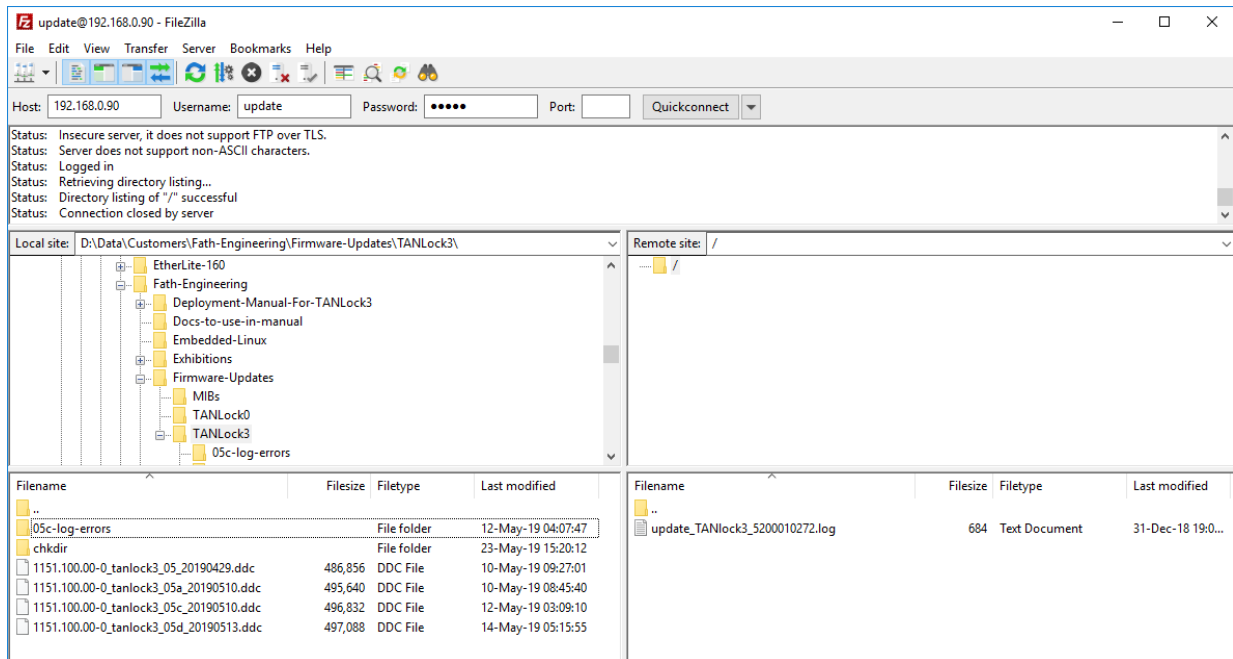
D:\Data\Customers\Fath-Engineering\Firmware-Updates\TANlock3>c:\usr\bin\md5 *.ddc
8D318E22C5BDC3223FBD4E087AA053DF 1151.100.00-0_TANlock3_05_20190429.ddc
DDF3FD3A1C8F58BF950B4B539999C8AC 1151.100.00-0_TANlock3_05a_20190510.ddc
AC87E274C671943C07C2CFFA2FD95DBF 1151.100.00-0_TANlock3_05c_20190510.ddc
B42ED0748FA2BF0E25FCAF09501ACDED 1151.100.00-0_TANlock3_05d_20190513.ddc
F1B0622FDA5A26A0233343508BF4E031 1151.100.00-0_TANlock3_06_20190528.ddc

```

```
D:\Data\Customers\Fath-Engineering\Firmware-Updates\TANlock3>
```

The update account is limited to the directory that the firmware update needs to be located.

It is critical that the complete file is uploaded before the lock is reset or loses power.



Once the file is uploaded and validated then doing a reset of the lock will automatically upgrade the firmware during the reboot process.

Reconnect back to the lock using TANlockExplorer and check that the lock information shows the updated firmware version number.