AR8x application note

This guide provides simple steps to quickly start using your new Nordic ID AR or Sampo S2 RFID reader and a high-level overview of the configuration and monitoring options available for your reader.

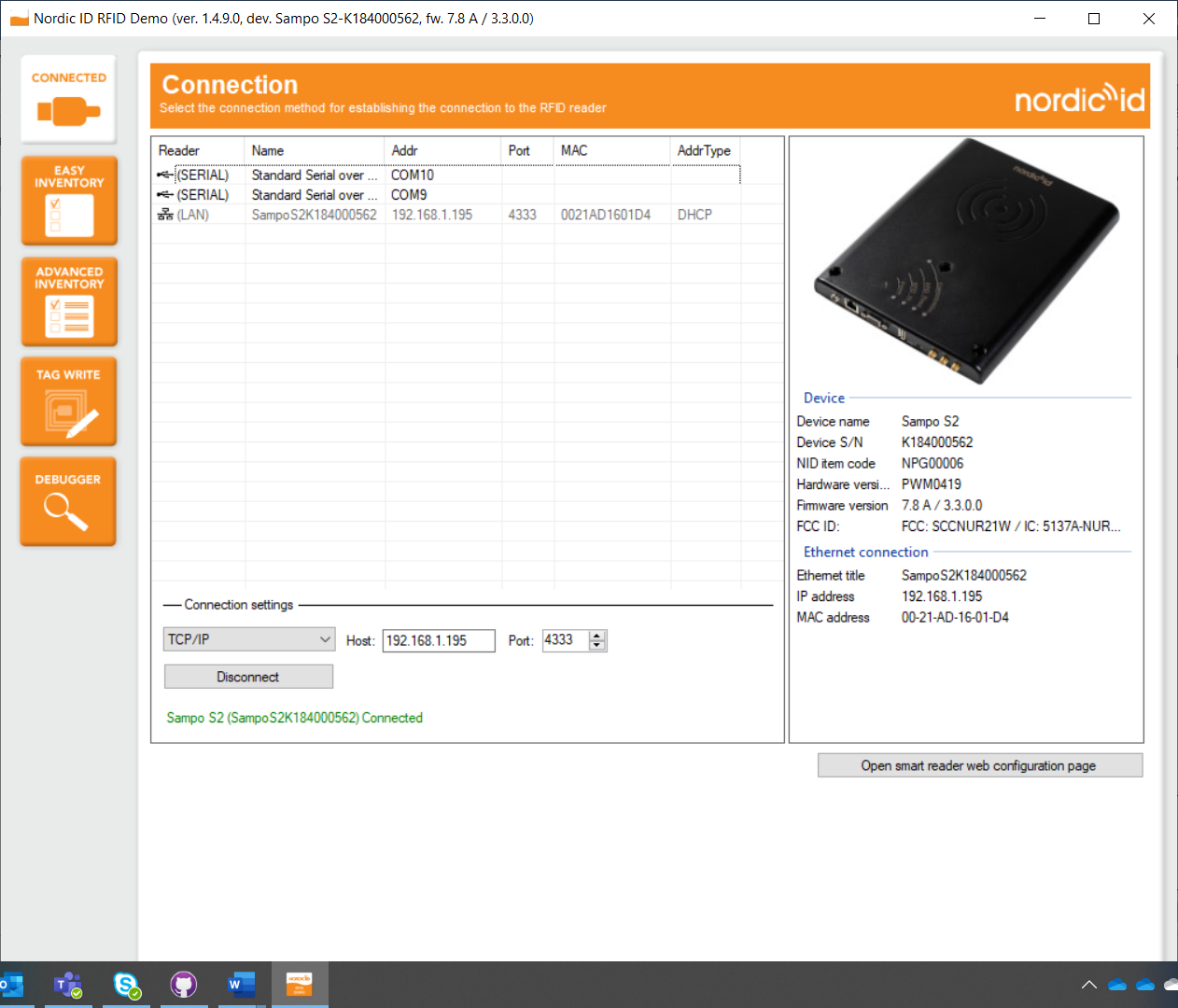
1. Getting started

Now that you have a brand-new Nordic ID AR8x device in front of you, the first step is to plug in the ethernet cable to the device. The other end of the cable should be connected to a DHCP-enabled network. Ensure your PC has Bonjour Print Services installed (install if needed). If your ethernet setup does not have power over ethernet, plug in the power cable to the device and connect it to a power outlet.

In case your network requires static IP address, then connect also the USB cable to your device and download the Nordic ID RFID Configurator and install it to your PC. Once it has been installed, start it and plug in the USB also to your PC. Choose the USB connection option from the RFID Configurator and it’ll connect to your device. Then you should be able to change the network settings on your device using the RFID Configurator. After you have applied the mentioned settings, unplug the power from your device and plug it in again to ensure that the settings are applied.

Once the device has powered up, check from the label (found from the bottom of the device) for the dashboard URL in the form of ([*http://hostname.local*](http://hostname.local)), your device hostname will be a combination of the device name and its serial (e.g. SampoS2K184000562). Alternatively, the device will use the MAC address in case the device name and serial are not known, check the label again for the MAC-address of the device. Let’s assume that the address you are seeing is 00-12-34-56-78-90. Take the last 3 values from the MAC and you should have 56-78-90. This last 3 bytes of the MAC is used as a part of the hostname for the device by default. The address is formatted as ar8x567890 where the first 4 characters are for identifying the device type and the last 6 are from the MAC address. You can test this configuration by performing a ping from your PC using the following command: *ping ar8x567890.local*

If the ping receives replies properly, you should be able to access the web configuration on the device through a web browser as well. The address would then be something like this: <https://ar8x567890.local> or <http://sampos2k184000562.local> Use URL from the label found the bottom of the device and open it in your web browser.

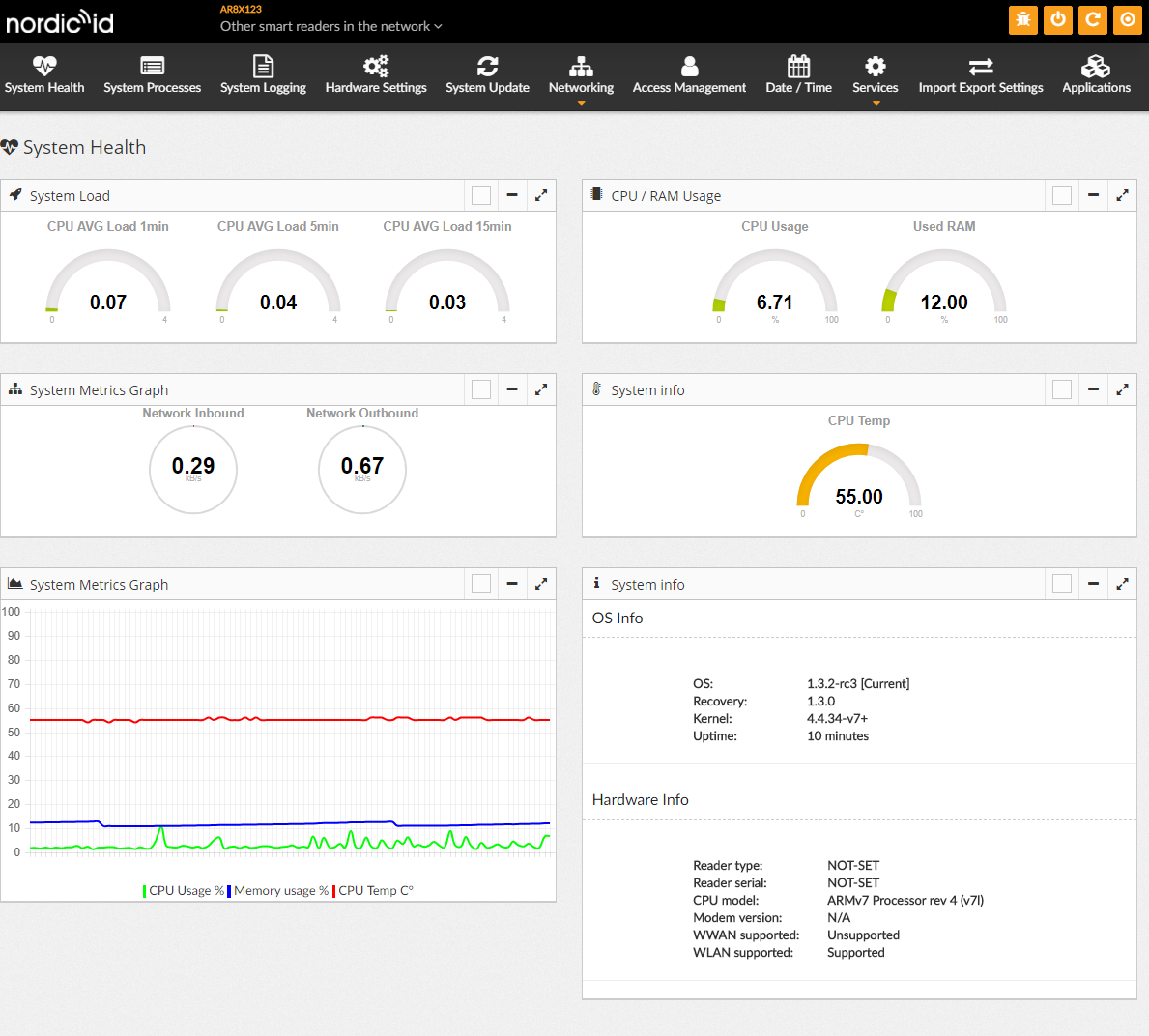


You can also find out the IP address using the RFID Demo software. In case you already know the IP-address of the device (from setting the static IP or other reasons), you can also access device by using the IP-address (like <http://192.168.1.195/>) instead of the <http://sampos2k184000562.local>.

Since self-signed certificates are used on the platform, your browser will most likely prompt you that there’s a “problem with this website’s security certificate”. Depending on your browser, you’ll need to click “Continue to this website (not recommended)” or other similar buttons.

If you can reach the device, you should be prompted with a username and password request. The default the configuration is **admin** & **admin**. The password can be changed in the Web Config view.

After the above steps have been completed successfully, you should see a view similar to this in your web browser:



The following table outlines the main features of the Web config UI.

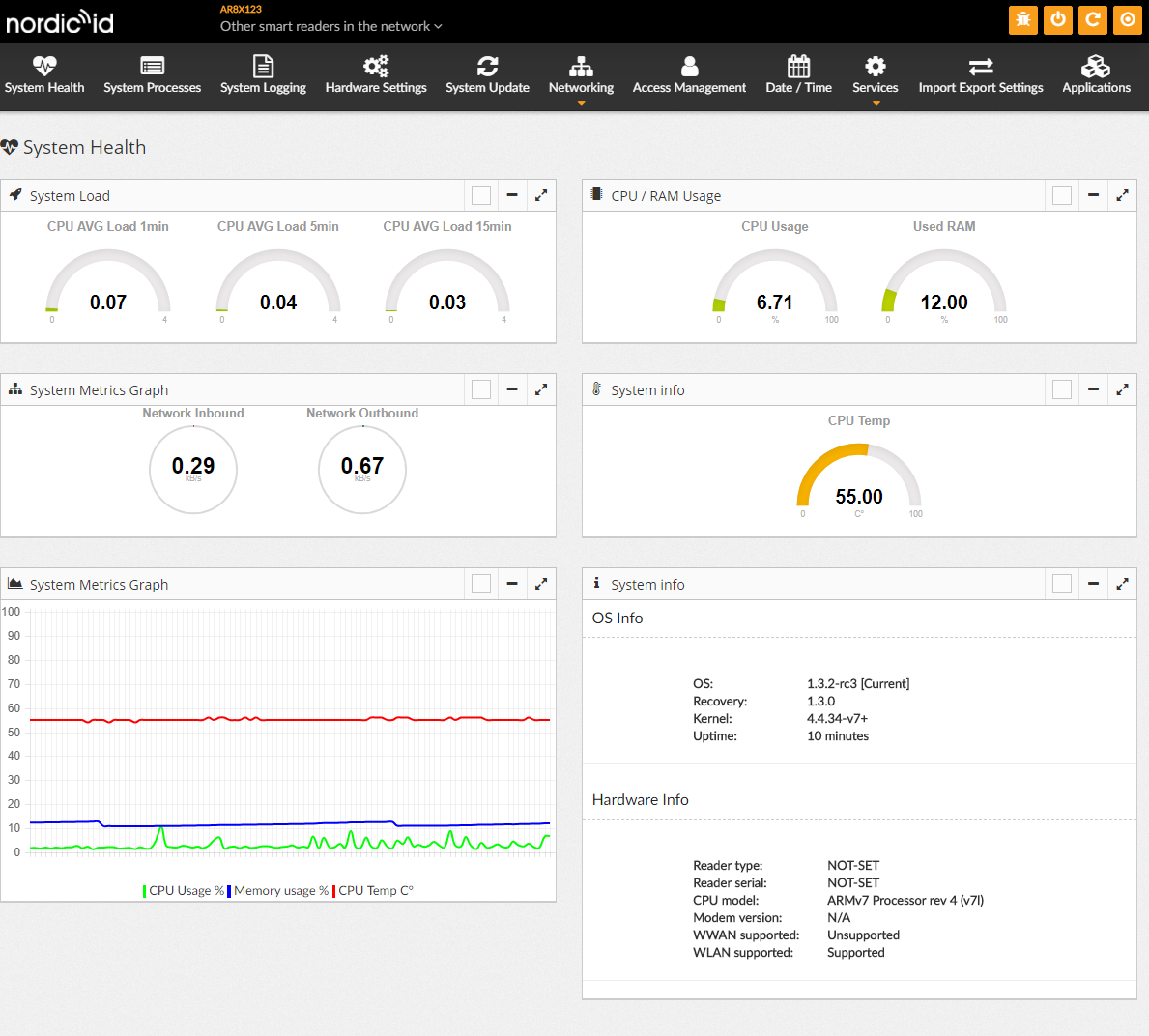
|  |  |
| --- | --- |
| **BUTTON-ACTIONS** | |
| **System Health** | Loads the system health page which displays realtime system info |
| **System Processes** | Displays the currently running processes of the device along with the CPU/RAM usage etc. |
| **System Logging** | Allows viewing the log files available in the /var/log directory |
| **Hardware Settings** | Options to configure the CPU governors, frequency limit for the CPU and to turn on/off the HW modules. On this page, you can also define how the device uses the USB port (i.e. as HID output or for the NUR module uses it to communicate with client applications etc.) and define udev rules for any devices you plug into the reader. |
| **System Update** | Used for updating the firmware for the platform |
| **Networking** | **General**  Disable/Enable network interfaces Configure IP-settings for interfaces Set Wifi to Client/Access point mode  **Wi-Fi**  Configure the wifi profiles  **3G** (if supported)  Configure the WWAN settings for the 3G module  **Wi-Fi Access point**  Settings Define the access point settings Clients List the connected clients along with their details |
| **Access Management** | Manage the web app admin access |
| **Date/Time** | Configure the current system time, timezone and NTP settings |
| **Services** | * System Services Enable/disable the predefined list of system services * NUR Service Configure the NUR service * MQTT Settings Configure Mosquitto MQTT broker * Radea Configure Radea settings if you have access to its services * Task Scheduling Schedule reader reboot or other tasks |
| **Import Export Settings** | Allows copying the current settings from the device and/or importing settings from another device, this view also allows to factory reset the device. |
| **Applications** | * Manage Manage installed applications and access their settings * Upload Upload & install new applications   See **AN002\_AR8x\_appinterface.docx** for more information |

1. available CONFIGURATION and info tools

In this chapter, we describe the tools available in the Web config UI. The backend of the web config can be accessed also using HTTP GET/POST requests. See **AN003\_AR8x\_webservice.docx** for more information.

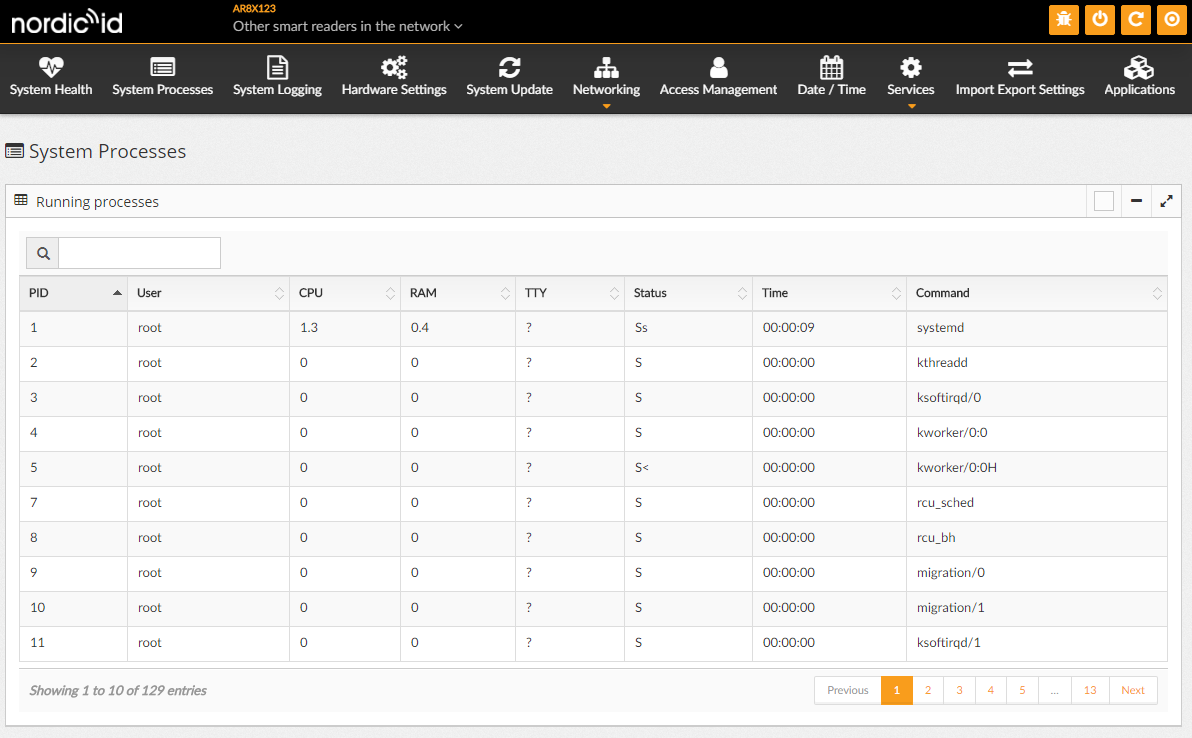
* 1. SYSTEM HEALTH

System health-page shows device-specific information and device performance monitoring details.



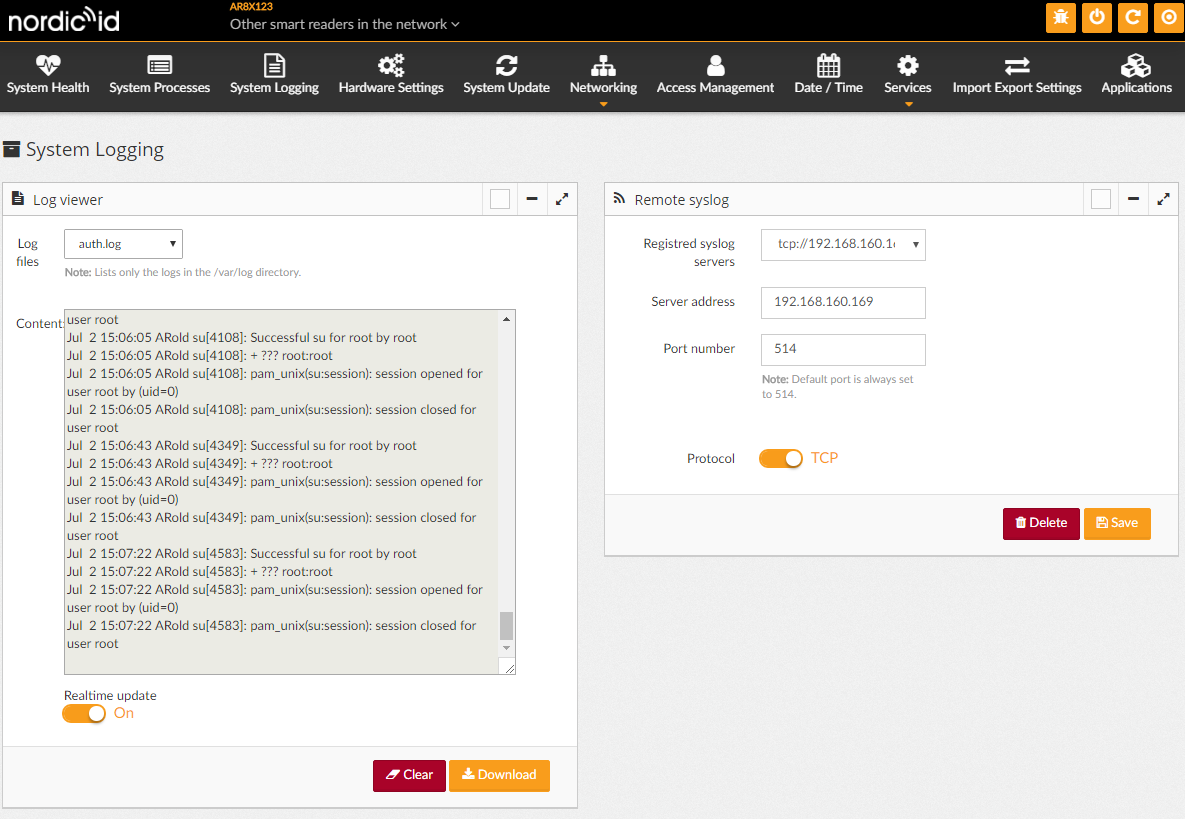
* 1. System processes

System processes list all the currently running processes and show details for them.



* + 1. system LOGging

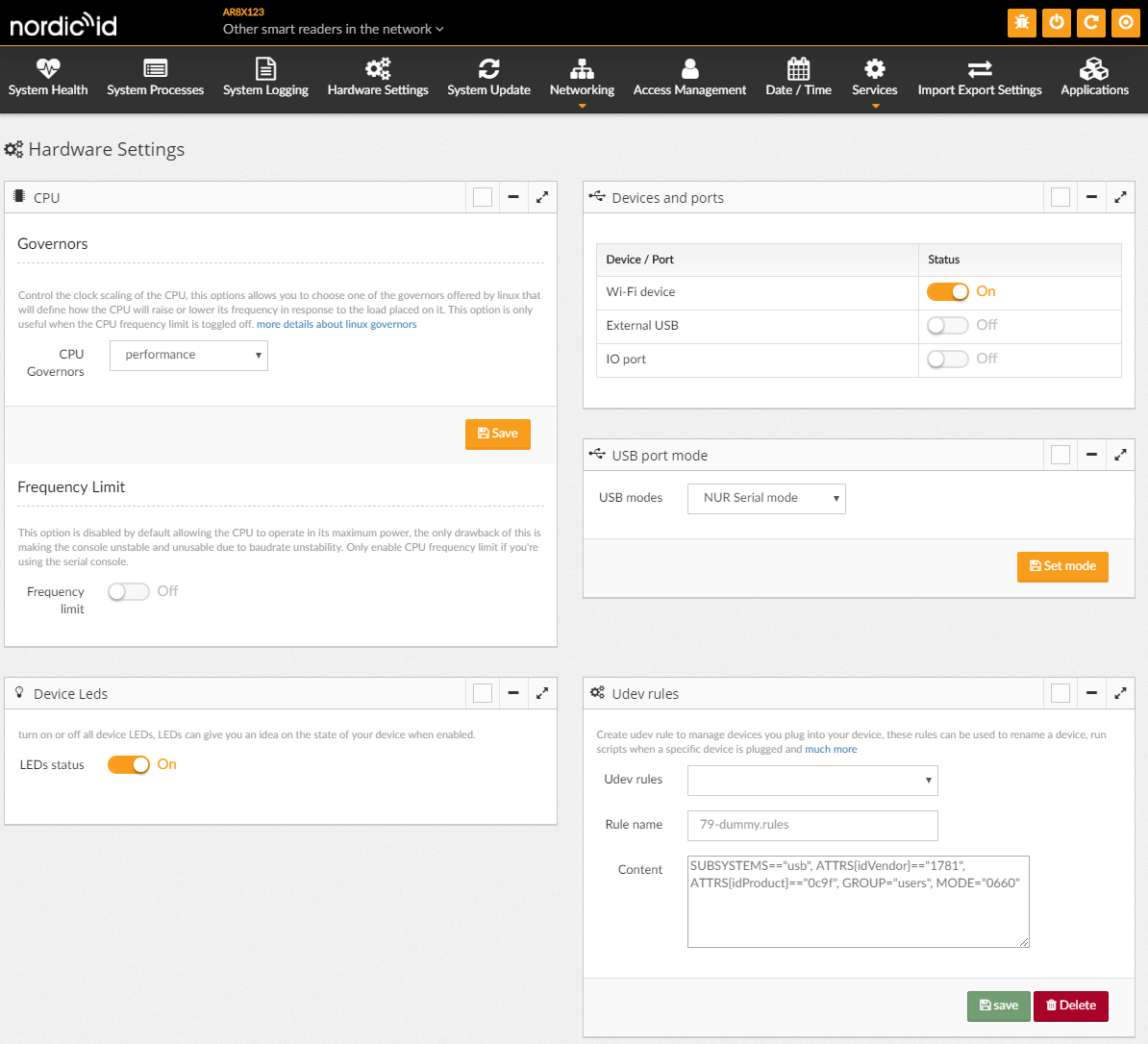
On the Logs-page, you retrieve the list of the available log-files and view their contents. If your applications should also display their log content here, make sure that they write their log to /var/log. Keep in mind that /var/log is mounted to temporary file storage so the content will be lost during system reboot.



This view can be also used for configuring the remote logging settings in case that is required.

* 1. HARDWARE Settings

On HW management you can define the CPU Governor setting & frequency limits for the CPU. Note that the CPU frequency limit is to allow serial console connections to the device, otherwise, it is recommended that the limit is disabled. The view allows also toggling the power for 3G & wifi interfaces as also +5VDC on the D15 port and the external USB port. In this view users can define udev rules for any device they plug into the reader, udev rules can also be used to run scripts more details can be found on the page.

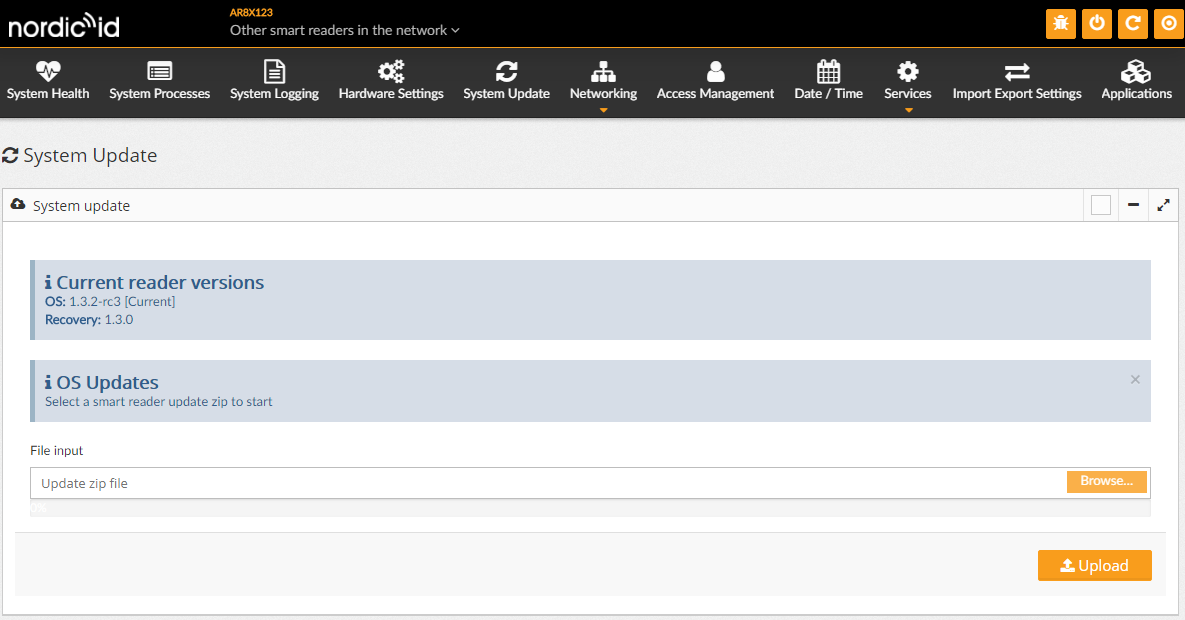


* 1. SYSTEM UPDATE

The OS and also the recovery image can be updated through the web config. The System Update accepts only zip-files which are created by Nordic ID to ensure correct contents for the update. Please see <https://www.nordicid.com/support/downloads/> for more SW updates.

When updating the OS or the recovery image, first choose the file from your PC and then upload it. After the upload has finished, the backend will verify the contents. If the verification succeeds, you need to click the “Install”-button (Upload => Install) to apply the update. At this step, the device will restart itself so it might take a while before the update tool notifies you that the update has finished.

The device upgrading procedure takes around 7 minutes, so watch the LEDs because the IP address might change after the update procedure depending on the network configuration. If the IP address has changed, then the web page keeps spinning even the communication LED blinks for telling that the device is up and running and waiting for the new connection. You can also watch the RFID Demo/Configurator because the device appears on the list when the upgrading procedure is finished.



* 1. NETWORKing

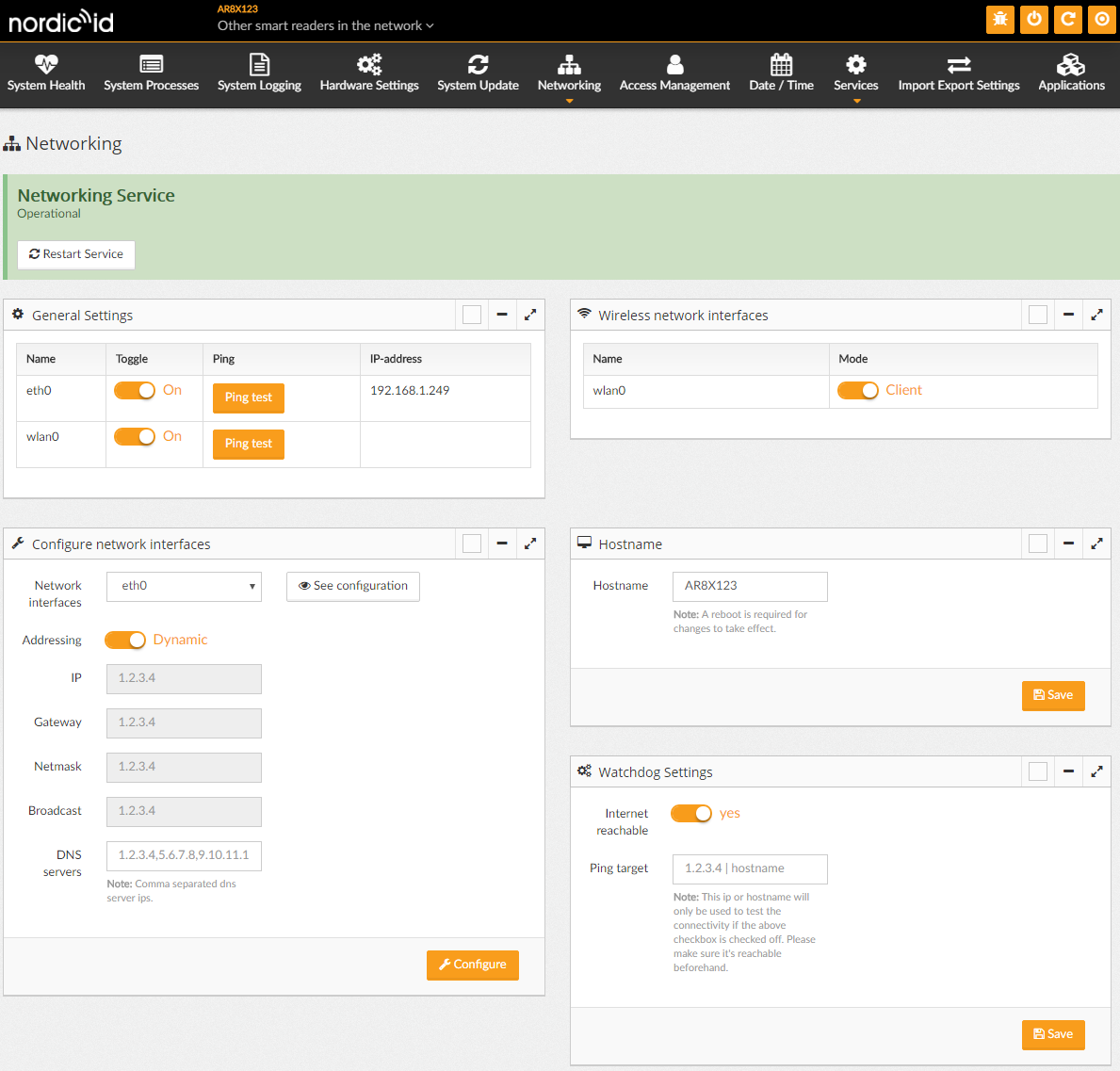
Network settings allow you to change the ethernet and WLAN adapter TCP/IP settings as also change the WPA Supplicant settings or the wifi access point settings in case the interface is to be used as such.

* + 1. General

On the general settings sections, you can toggle the state of each available network adapter as also define which wifi interfaces are to be used in access point mode.

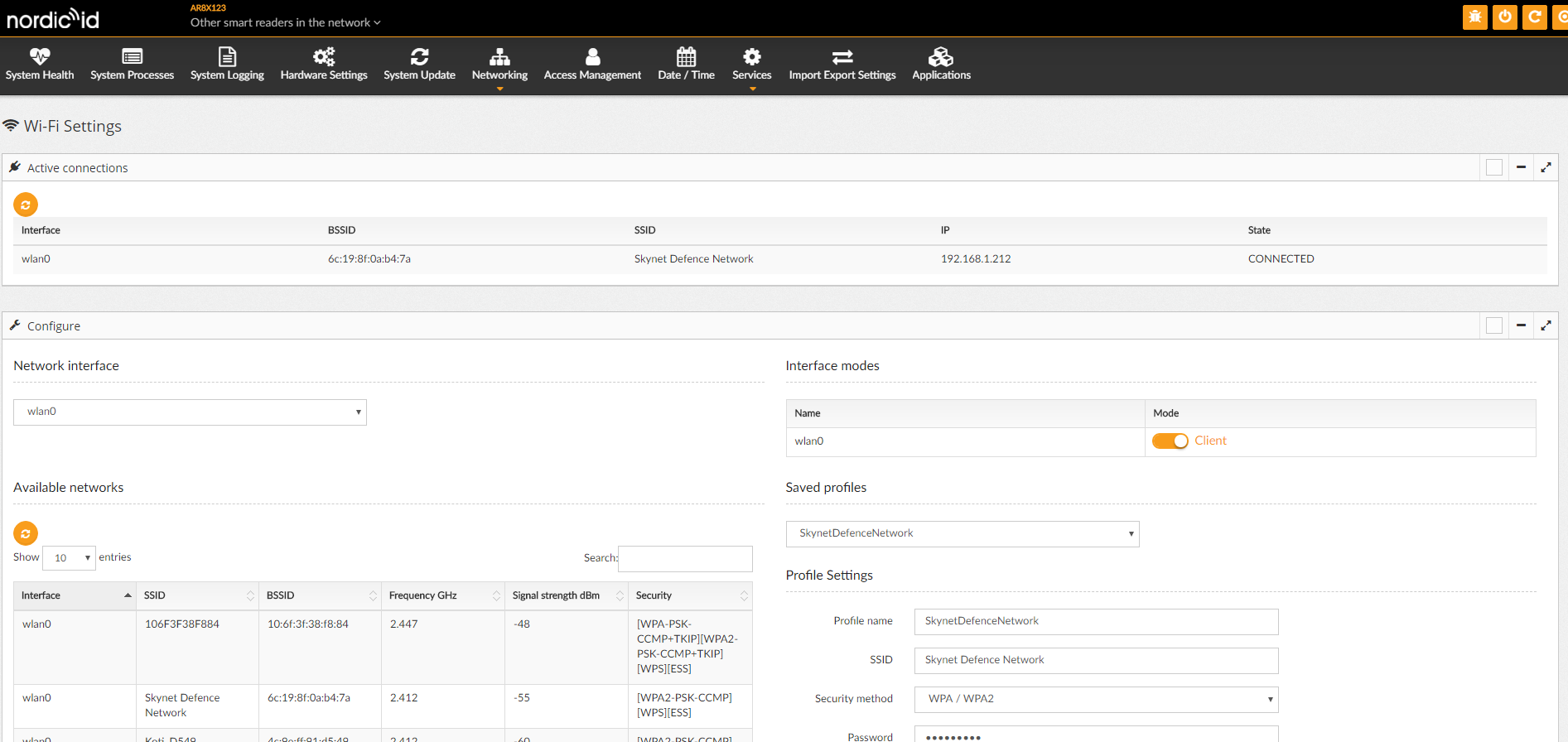
The view allows also changing the IP settings for each interface and also changing the hostname of the reader (requires a reboot for the hostname change to take effect).

On the same page, you will be able to configure the networking watchdog to check for internet connectivity if that’s applicable or configure it to check the connection to a network of any device in the network.



* + 1. Wi-fi

Wifi settings allow you to create/remove network profiles for each wifi interface and browse the available networks when using the interface in client mode.

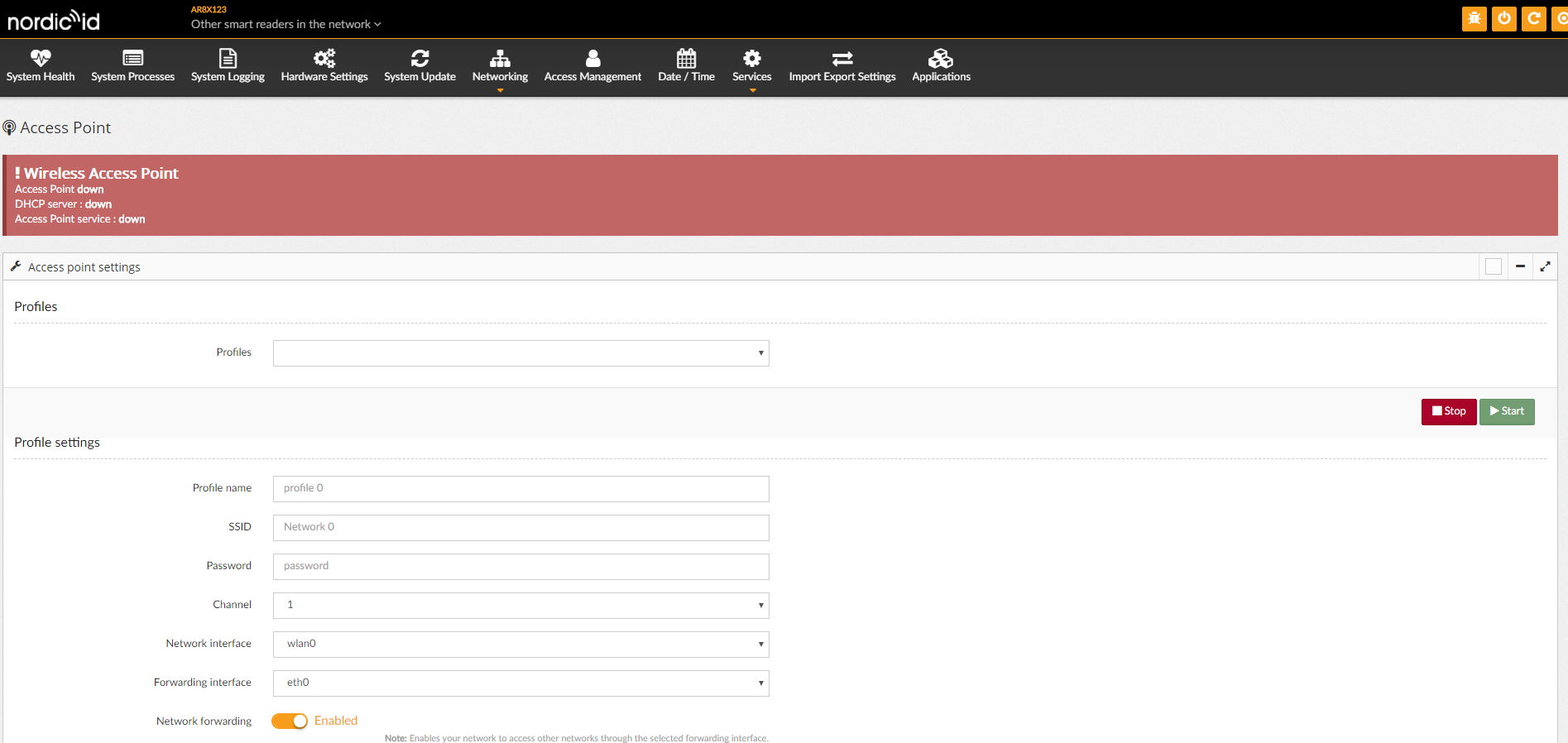


* + 1. 3G

If your device is equipped with a 3G module, you can also access its configuration through the Web UI. On the configuration view, you can define the access point settings and the pin code for your SIM card.

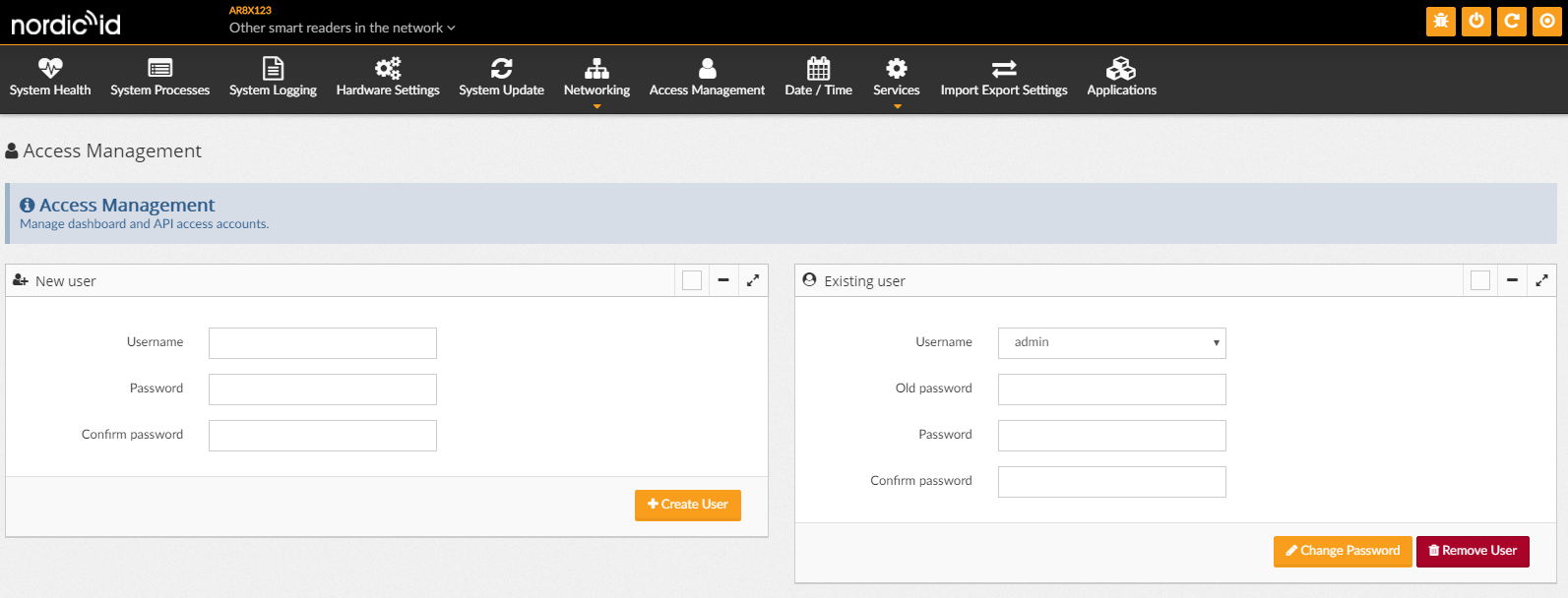
* + 1. wi-fi ACCESS POINT

On the access point view, you can see a list of the connected clients and configure the access point settings.



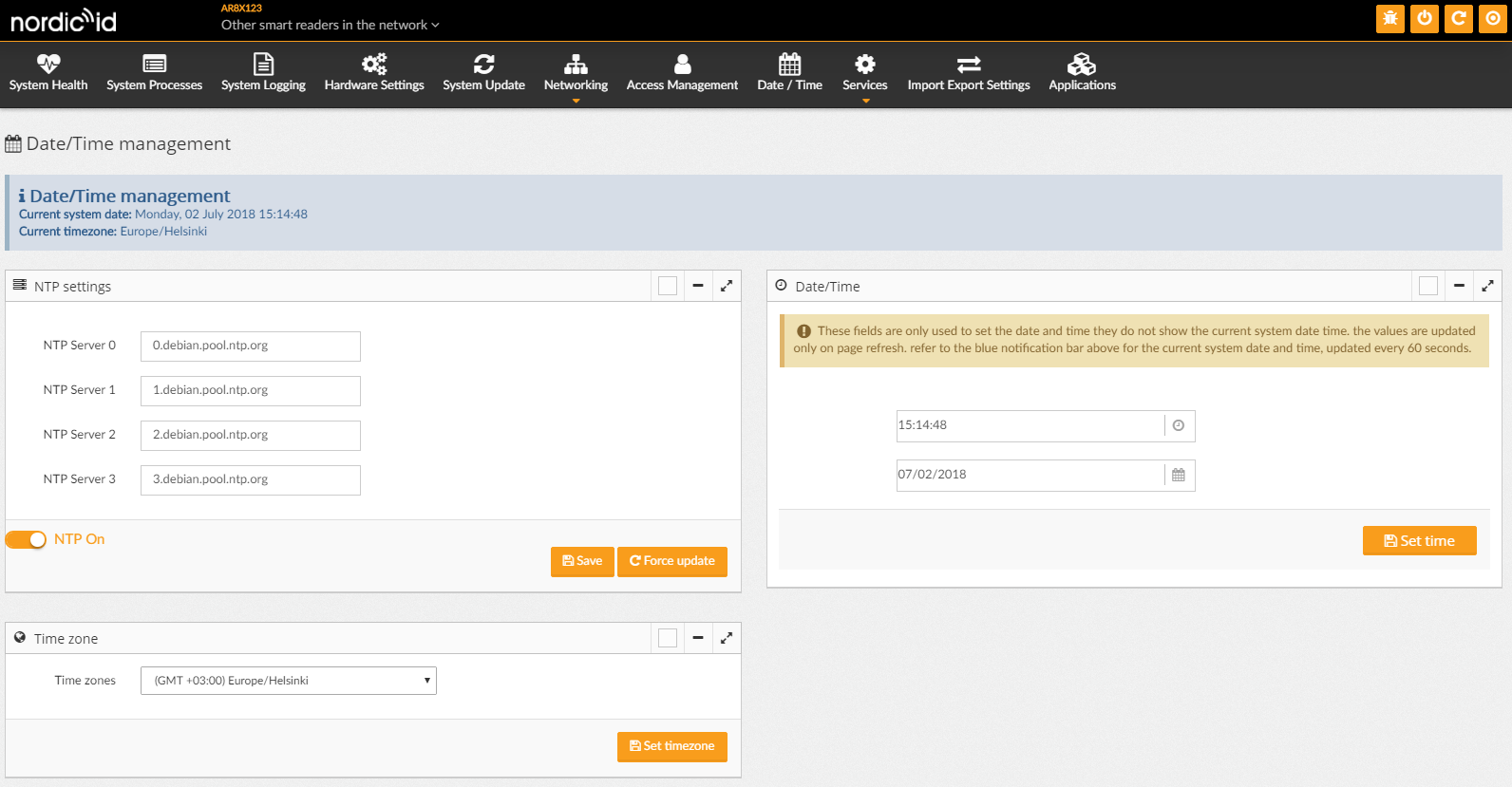
* 1. access MANAGEMENT

On the user management view, you can edit the admin password and add new users. These login credentials are only for accessing the reader dashboard and use the API provided with it.



* 1. Date / Time

The Date & Time configuration allows you to configure the RTC, timezone, system time for the device and also configure the NTP settings for the device.

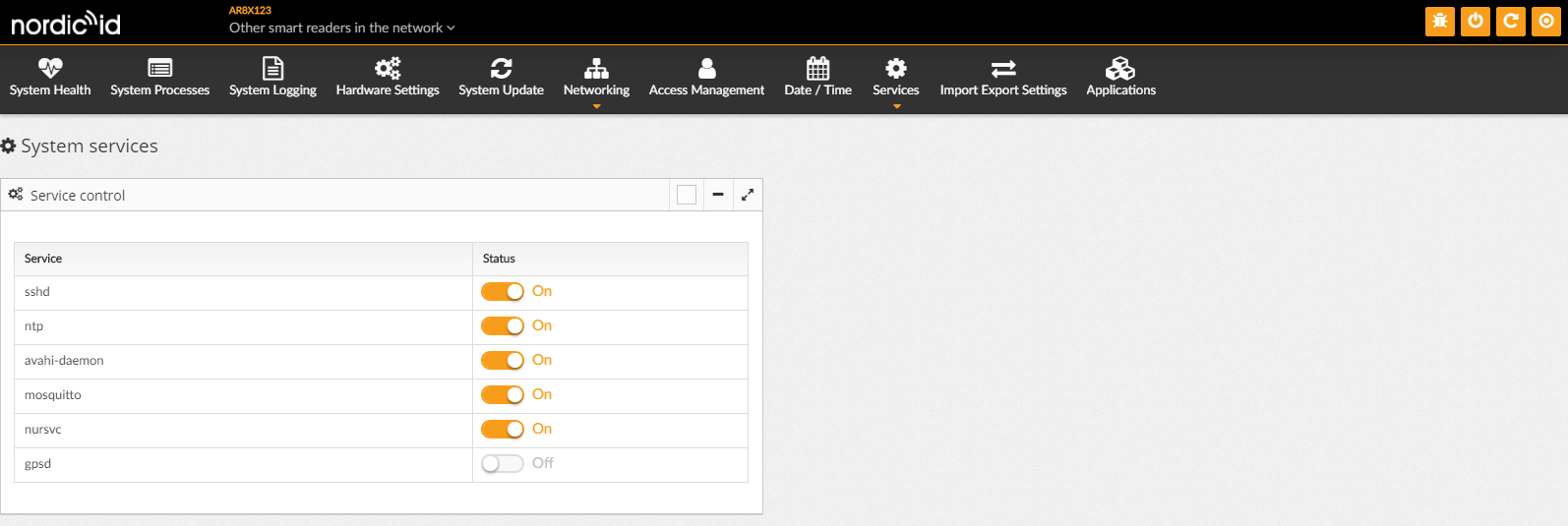


* 1. SERVICES

System services provide a view where you can configure certain system services as also enable/disable them.

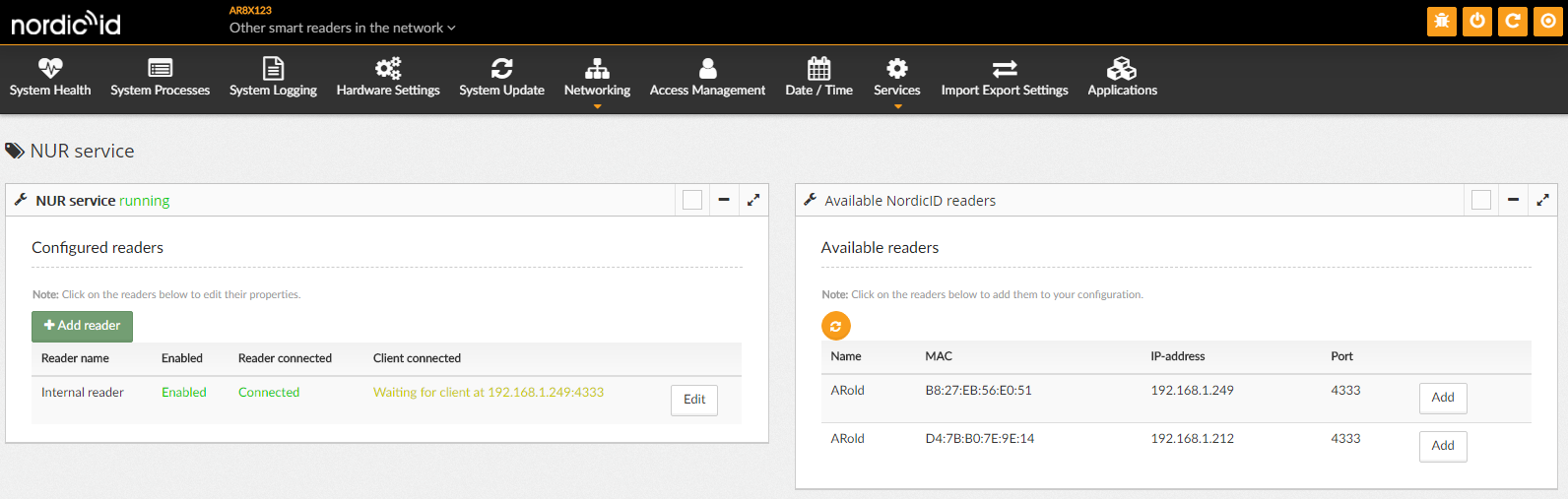
* + 1. system services

On general settings, you can enable/disable sshd, avahi-daemon, mosquitto and nursvc. By default, sshd is **Off**, and the others are **On**. Keep in mind that if you decide to turn off the nursvc, applications and other services are unable to access the NUR (Nordic ID UHF RFID) module inside the reader.



* + 1. NUr Service

The Nur service acts as a proxy between the internal reader module and the client applications. The service handles the communication due to the reason that some of the IO features on the platform are accessed via the OS and others through the NUR module. This service can be also used to route the communication to other Nordic ID readers, for example in a situation where you have 1 Sampo S2 and multiple Sampo S1’s and instead of finding the IP address for each device, you would only be connecting to the Sampo S2 IP using the individual port for each S1 instance.

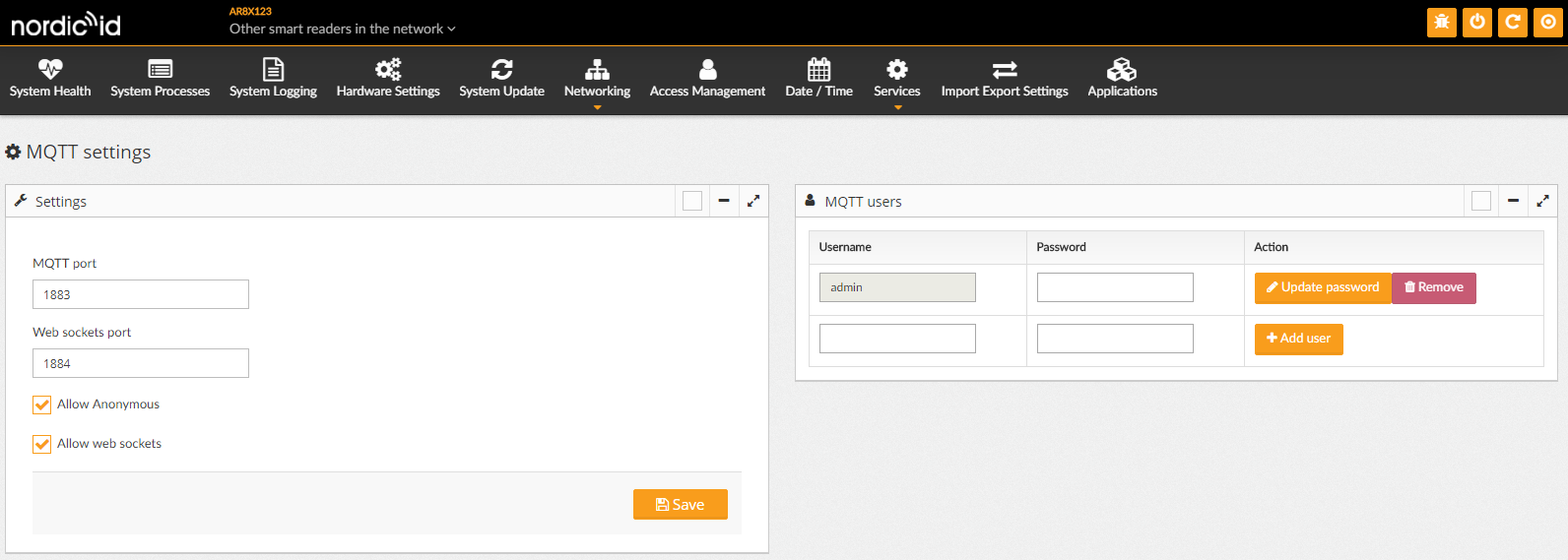


The view allows also configuring the “default” UHF settings for each instance, meaning that when the proxy opens the connection, it’ll apply the configured settings for the reader. Then when client applications connect, the settings are already in use.

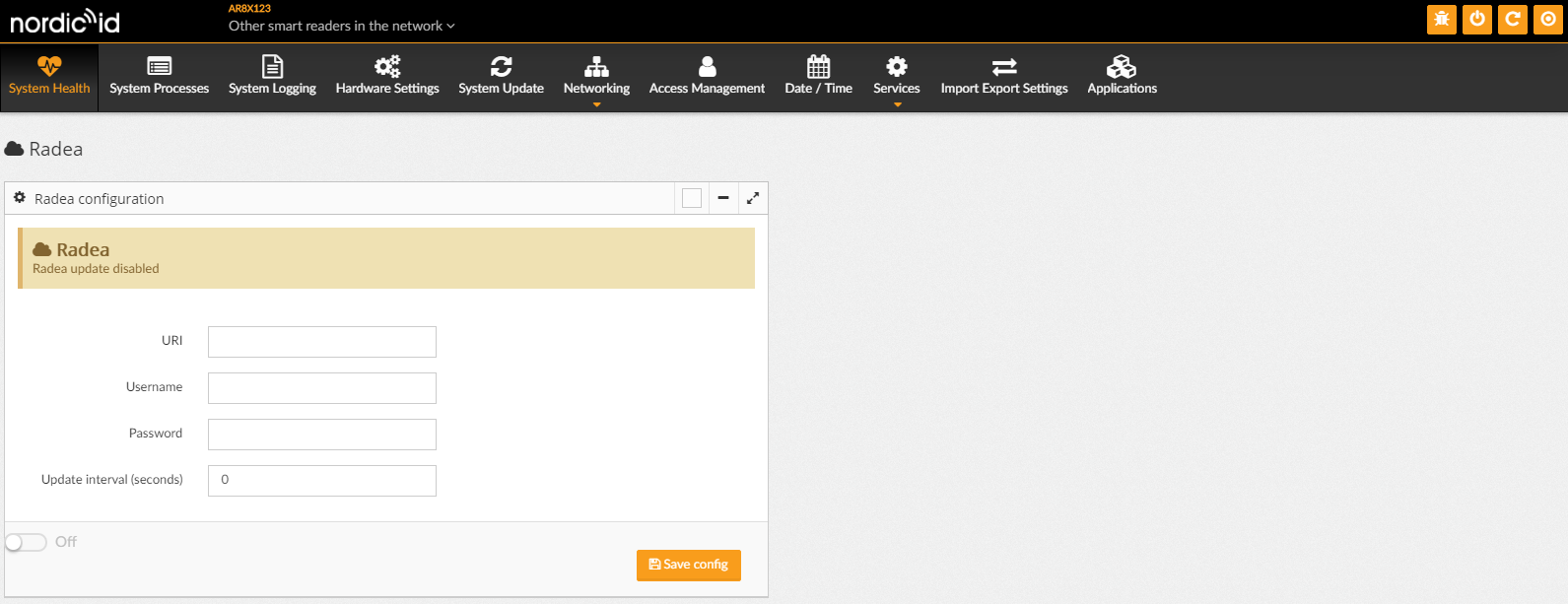
By default, the service will connect only to the internal reader module. This particular configuration cannot be removed, only the enabled/disabled state can be toggled. See **AN006\_AR8x\_NurSvc.docx** for more information.

* + 1. mqtt service

On the mosquitto view, you can configure the settings for the MQTT service on the device. By default, the MQTT port is set to 1883 and for web sockets access 1884. Anonymous connections are enabled by default, but you can also configure login details for the MQTT to limit who can view the MQTT messages.

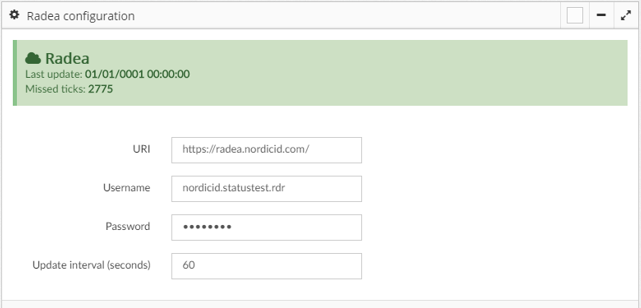


* + 1. Radea



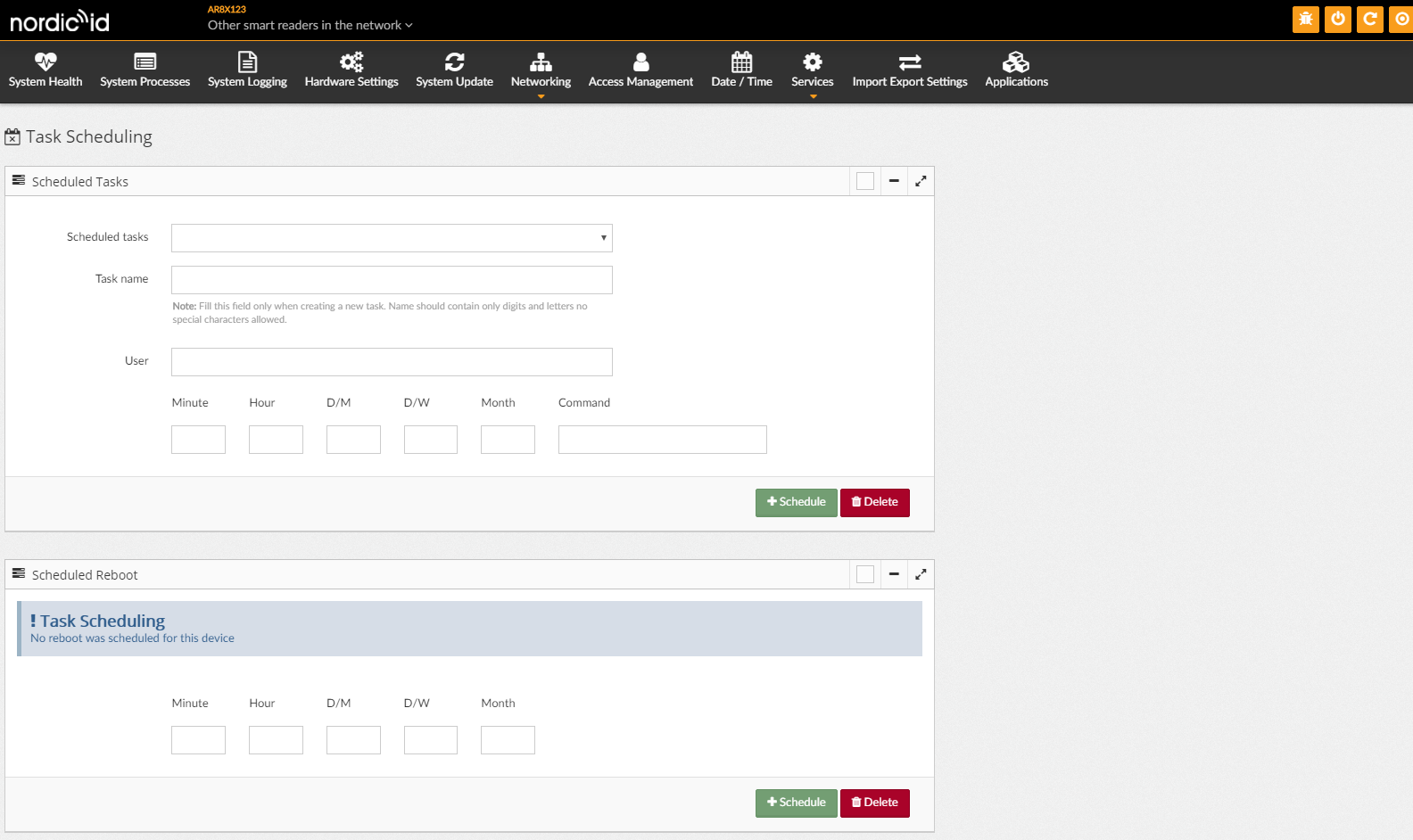
In this view; accessible from the ***Services*** sub-menu, you can configure and enable Radea metrics update; this will make the reader send different health and performance metrics to the cloud where you will be able to visualize performance graphs, changes made on the device and many other useful metrics with a timestamp allowing you to make better decisions and get an idea on what is going on in all your Radea enabled devices throughout the day.

The configuration for this feature requires specifying the Radea instance URL you want the updates to be sent to, a device username and password given after you registered your reader with the RADEA API. The final parameter is the Update interval which specifies the period between two Radea metric pushes.



The view will also let you know when was the last RADEA metric push and the number of missed pushes since then which will be reset to 0 after a successful push. In the screenshot above the reader was unable to push its metrics it shows the default date (01/01/0001 00:00:00) and failed to push 2775 times.

* + 1. Task scheduling



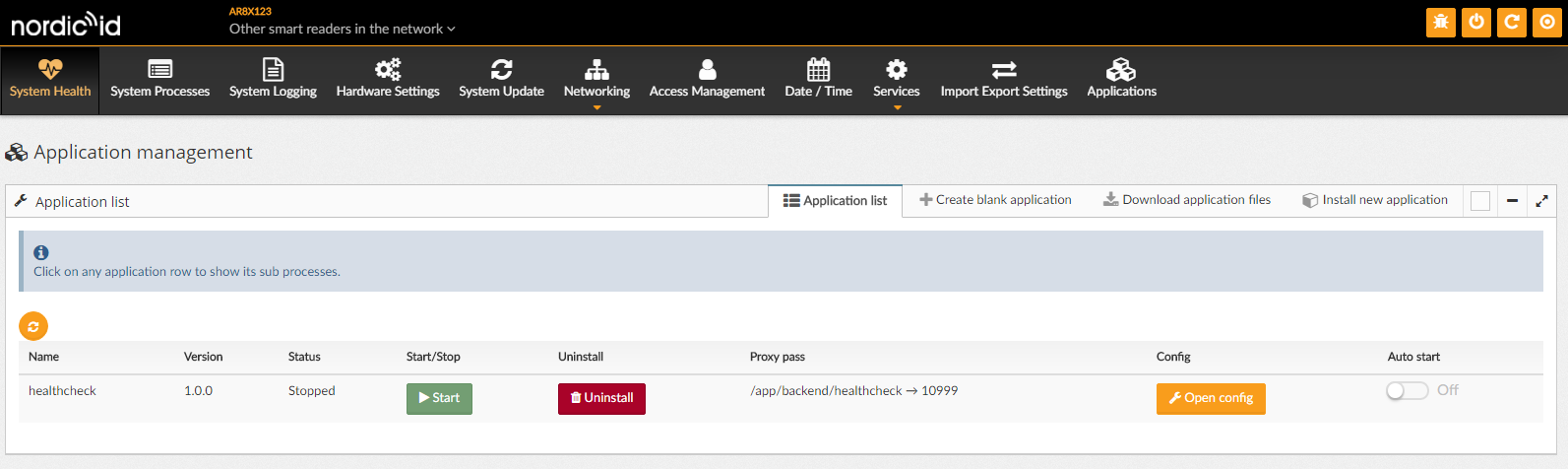
This view allows you to define and schedule tasks and device reboots, it uses the Linux job scheduler (cron). For more details on how to use this feature, you can go through documentation online e.g [centos documentation](https://www.centos.org/docs/5/html/5.2/Deployment_Guide/s2-autotasks-cron-configuring.html). Give your task a name, define the user the task should be run under, the task or command and the timing settings and schedule. For scheduling reboot, all you need to do is define the timing. Everything else is handled by the device.

* 1. APPLICATIONS

The Applications-tool allows you to configure and monitor installed applications See **AN002\_AR8x\_appinterface.docx** for more details.

* + 1. MANAGE

Manage-view allows you to start/stop/uninstall your application as well as open your own web management view for the application (if available). Management view also lists all the processes which have been started for each application.



Possible actions in this view are:

* + Start the application
  + Stop the application
  + Uninstall the application
  + Reset password (used for SSH communication)
  + Set applications to auto start
  + Open the configuration (if installed from the application zip-file). Keep also in mind that if the “backend” for the application configuration is not yet running, the configuration will most likely be unable to communicate with any backend service.
  + Kill individual process started by the application (app user)
  + Download application files
  + Create a “Blank” application for development purposes (e.g. for getting SSH connection)
    1. UPLOAD

Install new application tab allows you to upload your application zip-packages to the platform. Details of the package format can be found from **AN002\_AR8x\_appinterface.docx**

