WebAccess/DMP
Device Management & Provisioning

Updated on: 6 Nov 2018
Document Revision: 1.11
Software Release Version: 1.8

Table of Contents

1 Table of Figures

2 Abbreviations

DMP	WebAccess/DMP client server application
App	Device applications hosted in DMP and available for download to devices.

3 Introduction

WebAccess/DMP (DMP) is a centralised device management and diagnostics platform for Advantech's industrial routers (e.g. SmartStart, SmartFlex, SmartMotion, UR5i, LR77, ICR-3 series, etc.), IoT Gateway (e.g. SmartSwarm) and Wzzard wireless sensor node products. It allows users to remotely access and configure their device estate from anywhere there is a web connection. Depending upon the type of device being managed, it allows remote changes to configuration, application module downloads and device firmware updates. Changes may be applied to a single device or to a group of devices and are either sent to the device as the changes are made in DMP or, if the device is not online at the time of the change, are queued and sent once the device reconnects.

If a device is configured to send its SNMP traps to the hosted application, WebAccess/DMP can also provide diagnostics information on the status of the device, and also the quality of the communications interface it uses to connect.

3.1 Purpose

This manual provides useful information about the functionality available from WebAccess/DMP, and how to access it. It does not however provide detailed information on the significance of each individual configuration field available in each connected device, and the relevant device manual should be consulted for this information.

3.2 General Description

This document is structured along the same lines as the menu system within DMP. Major functional areas, defined by headings in the blue banner line at the top of every DMP screen, are given dedicated chapters, with sub-chapters reflecting the choices available under each option.

NOTE also in the top right hand corner of every screen there is a 'Help' link which calls up this manual.

3.3 Before You Start

There are some things that you need to before you begin:

3.3.1 Remote Device Client

WebAccess/DMP needs a client application to be installed on any remote device that it manages. This can be specified to be included at time of purchase, or alternatively, it can be downloaded from the Advantech website and installed on a device using the local web interface.
This client is also available to be downloaded from within the WebAccess/DMP UI.

3.3.2 Device Firmware Version

For a V3 router it is necessary that the router is running firmware version 5.0.0 (2014-12-02) or later.
For a V2 router it is necessary that the router is running firmware version 5.1.3 (2015-04-24) or later.

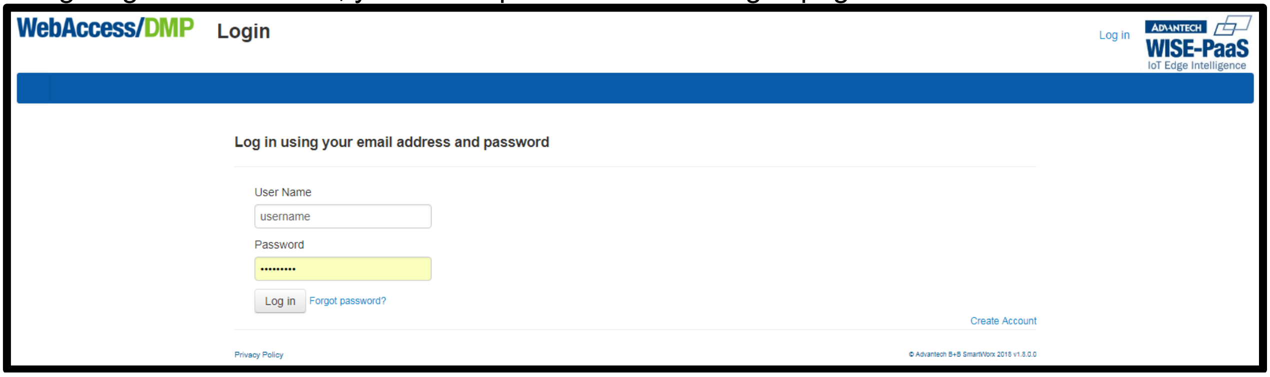
3.3.3 Internet connectivity

The router must be able to connect to the internet so that it can make itself available to WebAccess/DMP. Advantech's routers contain lookup tables of the login credentials for many public cellular APNs and will automatically try to connect using one of these options if ordered with the client pre-installed. If you install the client yourself, then you must also ensure it has the necessary configuration to enable it to connect to the internet before it can be managed by WebAccess/DMP.

4 Authentication

You can access WebAccess/DMP from any browser at https://hub.bb-smartworx.com.

Upon navigating to this address, you will be presented with a log in page as follows:



Log in using your email address and password

User Name
username

Password
••••••••••

WebAccess/DMP
Login
Log in
ADVANTECH WISE-PaaS IoT Edge Intelligence
Log in
Forgot password?
Create Account
Privacy Policy
© Advantech B+B SmartWorx 2018 v1.8.0.0

Figure 1 Login

Enter your user name and password,and click on the Log in button to move into the main program.

If you do not already have a user-account to log-in to, you may use the “Create Account” option.

***NOTE**: In the “normal” workflow, one person in your organisation will create an Account for your organisation: this user is the “account-creation” user. Then that person will create “users” within that account.*
If you are a “user” within a pre-created account, then you will receive an email invitation to join the account.

The first time your organisation’s account-creation user accesses WebAccess/DMP, she will be presented with an End User Licence Agreement (EULA) page, which must be accepted prior to continuing.

4.1 Action of ‘Forgot password?’ link

If you are unable to remember your password, then click on the ‘Forgot password’ link and you will be directed to a screen which prompts for your email address. Enter this information and click on the ‘Reset’ button.
If the email address entered belongs to a valid account user, then an email will be sent to the entered address with instructions on how to reset your password. After you have entered your new password, you will be returned to the Log-in screen.
In cases where the email fails to arrive check with your systems admin to ensure that the smtp server is active. The smtp settings are specified in the web.config of the web application. This is located at c:\inetput\wwwroot\bb\web.config on the web application server. Look for the setting EmailSMTPServerName in this file.

4.2 Action of ‘Create Account’ link

This link enables the “account-creation” user to create an account, for an organisation, on WebAccess/DMP. After entering the required details, the account-creation user will receive a verification email. This email will enable the account-creation user to create a password, and to subsequently access the system.

The “account-creation” user will have the “TP Admin” role by default.
All users with the role “TP Admin” may create other users.
All users created in this way will be associated with the organisation Account that was created by the “account-creation” user.

5 Dashboard

From version 1.5 of WebAccess/DMP, the default Dashboard contains:

5.1 Status Overview

The Status Overview is a visual snapshot summary of the current online/offline status of all of the remote-assets in your Organisation.

By default, this dashboard is intended to show the “worst case status” first:
i.e. Your remote devices that have been offline for the longest, will appear first in the view.

The view may be filtered, using drop-down list options:

Filter 1 options:

- All Devices
- Devices Currently Online
- Devices Currently Offline

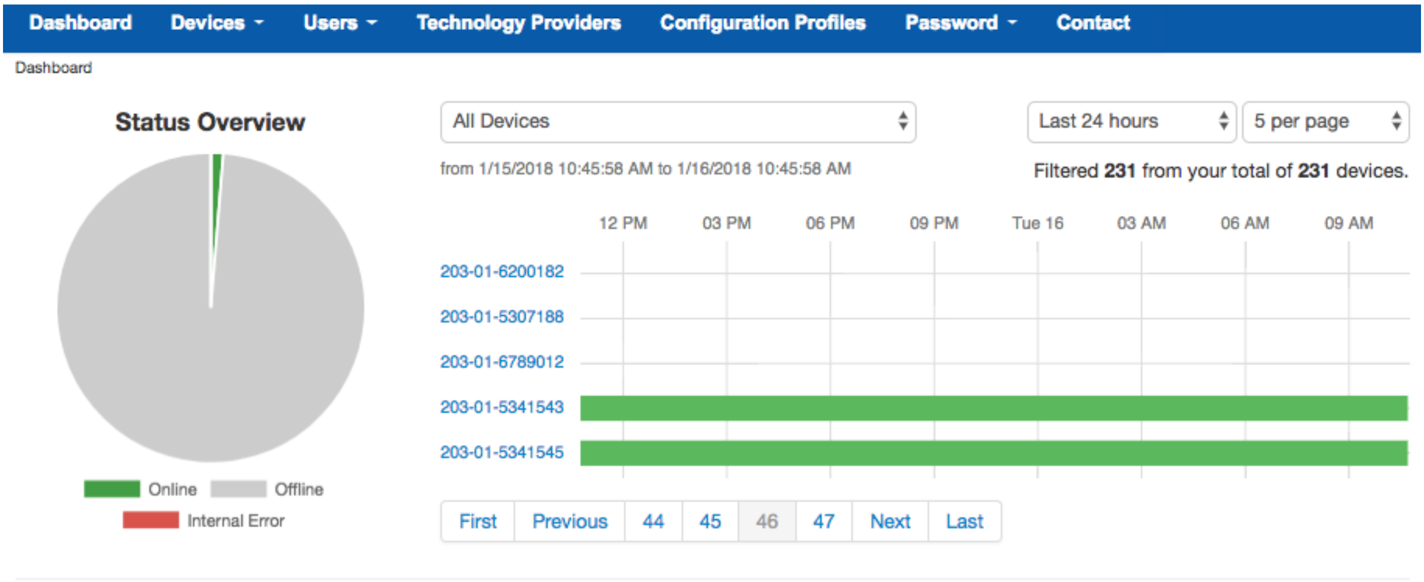
Filter 2 options:

- Last 24 hours
- Last 7 days
- Last 30 days

Filter 3 options:

- 5 per page
- 10 per page
- 25 per page

You may leave this dashboard open: it will auto-update every 15 minutes.



All Devices

Last 24 hours

5 per page

from 1/15/2018 10:45:58 AM to 1/16/2018 10:45:58 AM

Filtered **231** from your total of **231** devices.

203-01-6200182
203-01-5307188
203-01-6789012
203-01-5341543
203-01-5341545

Figure 2 Device Status Dashboard

5.2 Geo-Location

This is a map-view of the physical location of your remote assets.

***NOTE**: By default, WebAccess/DMP will not know the physical geo-location of your remote assets, and therefore it cannot automatically map them!*

To populate this location on the map on WebAccess/DMP, you will have to configure your assets to provide this information, or you may add meta-data into DMP (with the “drop a pin” feature).
i.e.
Add location meta-data on DMP by “Dropping a Pin” for each of your remote assets.
Enable the remote asset to report actual location, using GPS and location user-modules (or apps)
Enable the remote asset to report actual location, using SNMP configuration
See section 4.

If WebAccess/DMP has location-information from your organisation’s remote assets, it will plot them on the Geo-Location map on the dashboard.

Individual devices will appear as a pin on the map: clusters of devices will appear as a blue-circle with a count inside, which indicates the number of devices in the cluster. You may zoom in on these clusters.

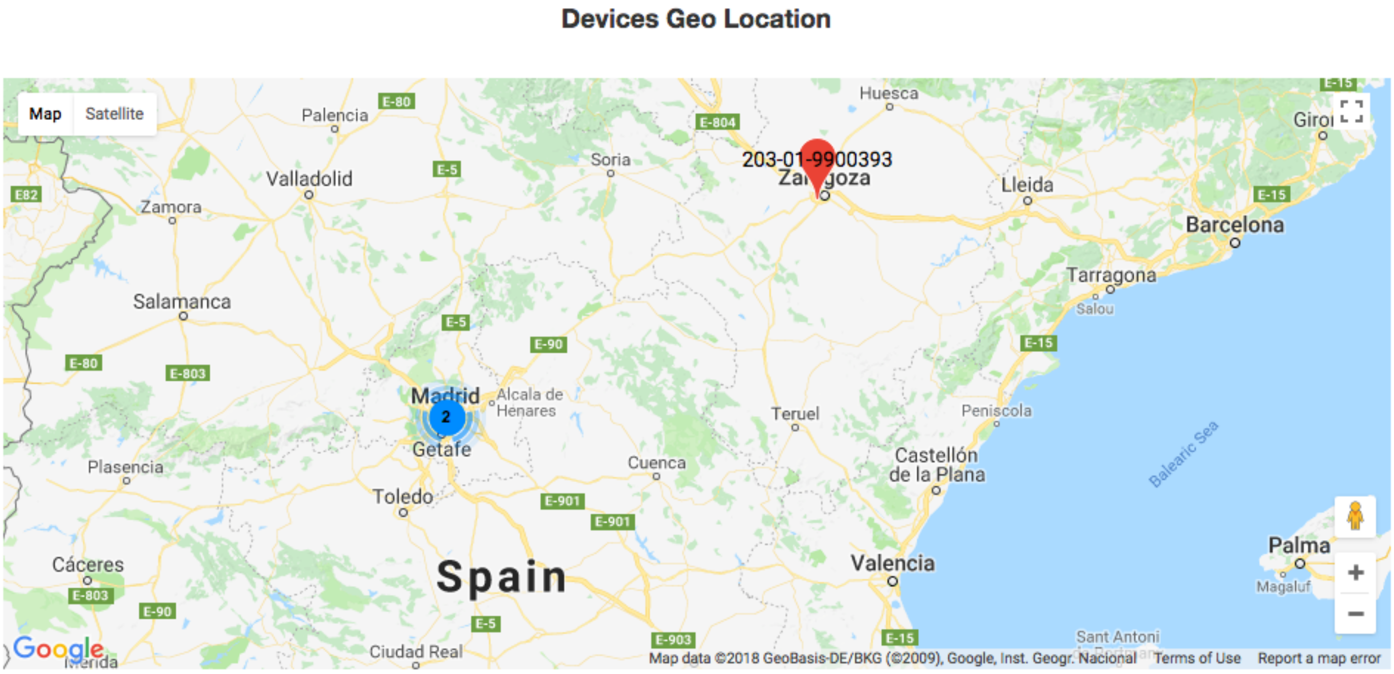
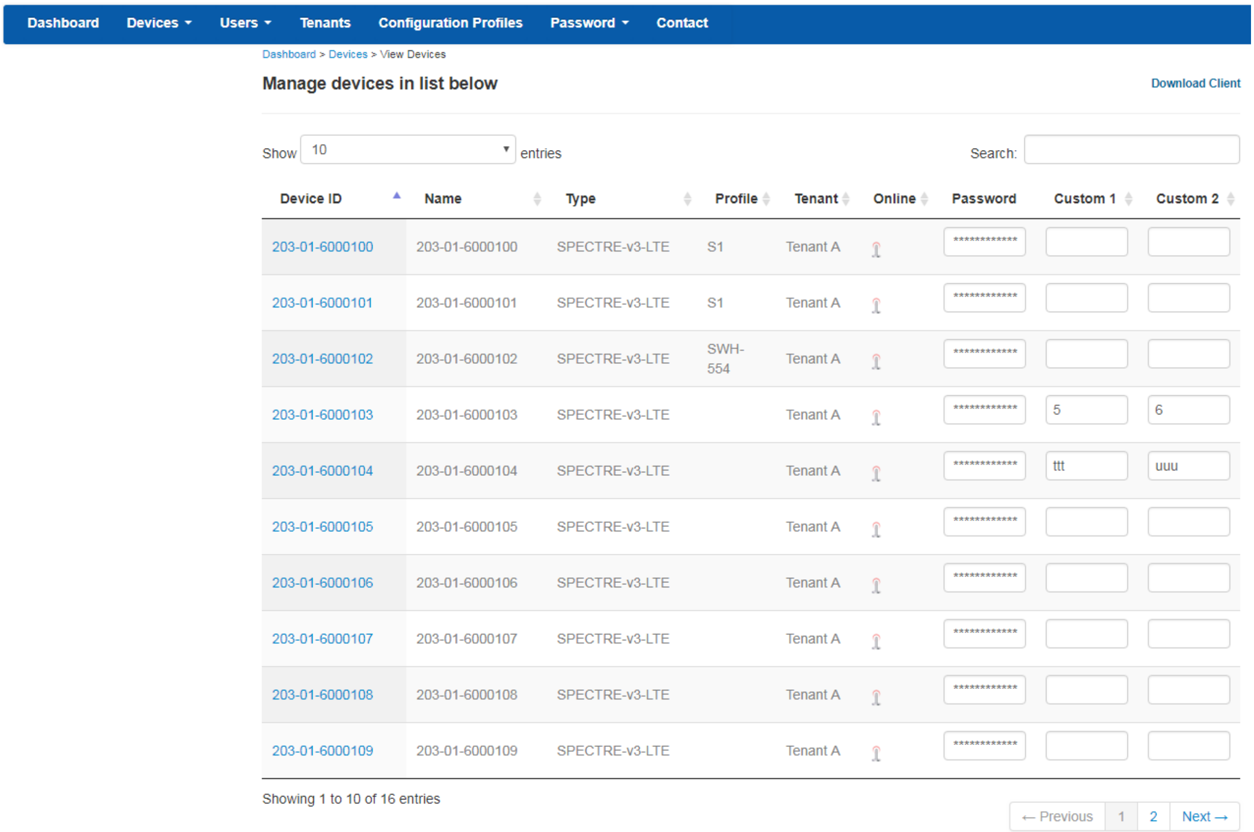


Figure 3 Devices Geo Location

5.3 View Devices

The View Devices screen provides a listing of important summary information of the devices relevant to that user account. The view will differ depending on account type. For example, the admin and TPadmin accounts can see the password field while the TPUser cannot.

Users can see at a glance if their device is online or offline or if their device is in a profile. Where device is in a profile the profile name will be displayed in the grid.



Manage devices in list below

Device ID	Name	Type	Profile	Tenant	Online	Password	Custom 1	Custom 2
203-01-6000100	203-01-6000100	SPECTRE-v3-LTE	S1	Tenant A	⚲	************		
203-01-6000101	203-01-6000101	SPECTRE-v3-LTE	S1	Tenant A	⚲	************		
203-01-6000102	203-01-6000102	SPECTRE-v3-LTE	SWH-554	Tenant A	⚲	************		
203-01-6000103	203-01-6000103	SPECTRE-v3-LTE		Tenant A	⚲	************	5	6
203-01-6000104	203-01-6000104	SPECTRE-v3-LTE		Tenant A	⚲	************	ttt	uuu
203-01-6000105	203-01-6000105	SPECTRE-v3-LTE		Tenant A	⚲	************		
203-01-6000106	203-01-6000106	SPECTRE-v3-LTE		Tenant A	⚲	************		
203-01-6000107	203-01-6000107	SPECTRE-v3-LTE		Tenant A	⚲	************		
203-01-6000108	203-01-6000108	SPECTRE-v3-LTE		Tenant A	⚲	************		
203-01-6000109	203-01-6000109	SPECTRE-v3-LTE		Tenant A	⚲	************		

Showing 1 to 10 of 16 entries

Figure 4 View Devices Page

There are 2 Custom fields provide for each asset: You may enter custom text in these fields, and they will be stored as meta-data for that asset (provided you "Save" them). It is important to remember that these custom fields are used for descriptive purposes only. The data in these fields is not propagated to the device. A password management feature has been introduced into DMP in 1.7. The password field is visible in the view devices screen though the password is obfuscated.

Paging, sorting and searching is implemented on the grid. The page size of the grid can be defined using predefined amounts in the show entries drop down at the top left of the page. Paging is implemented on the client side only. This means that the initial load of the page will load all the devices. This will be reviewed in future releases. The search feature will operate on all the columns in the grid with the exception of the password and online columns. Searching is not case sensitive.

Clicking on an individual Device ID field will take you to the 'Manage Device' screen which provides the detailed device status and settings menu for that device.

***NOTE**: Click on the "Download Client" link if you do not have the client installed on your router. This file needs to be installed on your router via the router's local web browser.*

***NOTE**: The client will have a filename like "hmpclient.tgz". We have recently become aware that some browsers on some Operating Systems treat this filetype as a "known type" - which can cause confusion because the browser will make it look like you're downloading a file that you don't want.*

for example:

- *the Safari browser on MAC OS may treat this file as a "TextEdit.app" document.*
- *the MS Edge browser on Windows 10 with Solitaire Extensions installed treats this file as a ".solitairetheme8" document.*

In all cases, it is safe to download the file, and to use it as intended.

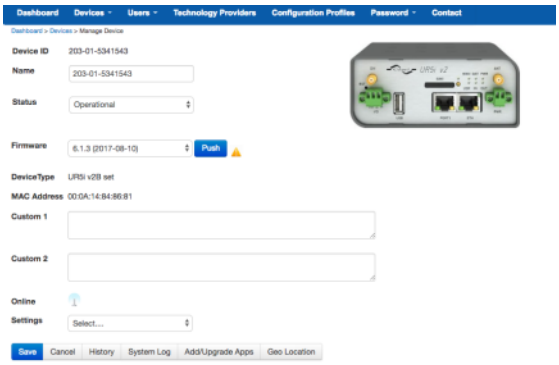
5.4 Manage Devices (Individually)

Upon selecting a device and moving to the manage devices screen, you will be presented with one of two screens, depending upon whether the device is individually managed, or is part of a Configuration Profile.

5.4.1 Individually Managed Devices

The main Manage Device screen shows summary information for the device, plus links to more detailed information as follows:

Device ID: The unique ID of the device.



Device ID 203-01-5341543

Name 203-01-5341543

Status Operational

Firmware 6.1.3 (2017-08-10)

DeviceType UR5i v2B set

MAC Address 00:0A:14:84:86:81

Custom 1

Custom 2

Online

Settings Select....

Name: A free text field into which you can enter a device name that has relevance to you. This name will appear on other screens to help confirm you are dealing with the expected device, and so should be unique. Remember that searches by name are not case sensitive, so do not rely on character case to define uniqueness. For the new name to be stored, the 'Save' button needs to be clicked

Status: These have no relevance within WebAccess/DMP, but are included to allow users to distinguish between devices that are in service (operational), Idle (for example in stock in a warehouse waiting to be deployed) or Decommissioned (for example retired due to upgrade).

Firmware: This is the firmware version last deployed in the unit. A dropdown menu provides options for alternative firmware versions that could be downloaded to the device. Selecting an alternative version and pressing 'Push' will cause that firmware to be queued for download to the device and, upon receipt, will overwrite the previously installed firmware.

Device Type: The part number corresponding to the deployed device. The picture of the device shown in the top right of the screen should also match that deployed.

Custom 1 and Custom 2: These are free-text fields. Any information entered here will be stored as meta data for this device. The text entered here also appears on, and can be edited through, the "View Devices" screen.

MAC Address: The MAC Address of ETH0.

Online: The current communications status of the device, indicated by the same Icons defined in previous sections.

Settings: This is a drop-down list that enables you to manage the configuration settings for this device. You may select "All" settings, or you may select a specific group of settings. When you make your selection, you will be guided to the "Settings editor".

5.4.2 The Settings Editor

The main settings available are accessed via a navigation pane on the left of this screen. These parameters vary according to the type of device involved, and essentially mirror the options available via the devices local web browser. Please refer to your device manual for the specific relevance of these settings.

There is some global action buttons found at the top of each screen as follows:

Back: Revert any changes to their original settings and exit to the main Manage Device screen.

Apply Changes: Send this configuration to the remote device, now.

NOTE*: this causes only the configuration data from the section currently on display to be sent to the device.*

In addition, there is a global '**Advanced Settings'** menu bar at the bottom of each screen.

NOTE*: we do not recommend that you use the Advanced Settings options, unless you are sure you know what will happen in the system, and on your remote device.*

Expanding this section offers the following options:

Reboot: Remotely reboot this device, now.

Complete Command: Complete a pending command from the DMP queue. Typically, you would use this if there are pending commands on the DMP queue that are not automatically completing, and that are therefore blocking all subsequent commands to the remote device.

Sync: Uploads the current configuration from the remote device into WebAccess/DMP. Typically, you would use this to ensure that the configuration items on DMP match with the configuration items on the remote device. This can be useful if configuration changes have been made for this device, both from DMP and on the local embedded web-server of the remote device.

Import Config: Takes a previously saved configuration (.cfg) file (for example, one that was backed up from a router), load it into WebAccess/DMP, and use it to configure this device.

5.4.3 Manage Device: Buttons

5.4.3.1 Push

Push the Selected Firmware version to the device.

5.4.3.2 Save

Saves changes made to any of the Meta Data on the Manage Device page.

5.4.3.3 Cancel

Ignore all changes and move back to the Device selection screen.

5.4.3.4 History

Display an audit-log of all actions that have been queued for this device. This log shows the command; user name, timestamp action was queued, timestamp action was completed, success/fail, response (if any).

5.4.3.5 Add/Upgrade Apps

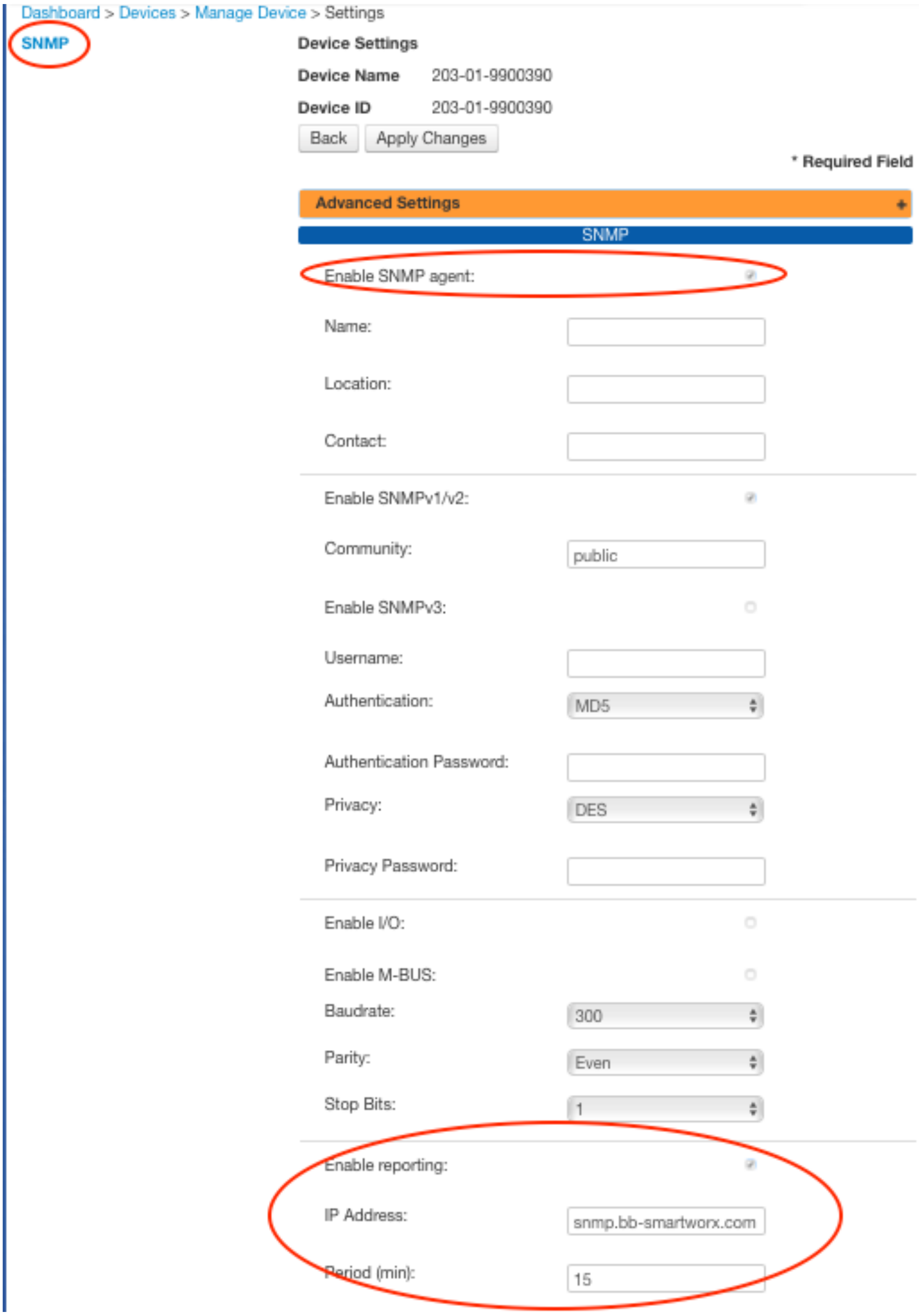
This takes you to a screen which presents all of the available User Modules and Applications (Apps) which may be downloaded to this device. Apps are selected via the checkbox, and deployed by pressing the 'Add Selected Apps' button. The 'Tag' field is a free format text field which may be used to provide a site specific comment against the app. It has no relevance within WebAccess/DMP, but does appear on various other screens as an 'aide-memoir'. If the App you require is not listed, please contact your Advantech representative.

Once added, Apps will appear in the 'Manage Apps' section of the main device screen. Clicking on the name of the App will take you to the App specific configuration pages, where these exist. Navigation through the App configuration pages follows the same principles as for other settings pages outlined above. Refer to the App documentation for details of the significance of individual fields on this screen. Apps may also be removed from the device from this section by selecting with the tick boxes and clicking on 'Remove Selected Apps'.

***NOTE**: A star icon ☆ indicates that a newer version of an App is available.*

5.4.3.6 Reports

***NOTE**: This button will only be available if your remote device has been configured to report SNMP data to the DMP server (snmp.bb-smartworx.com). If you have an on-premises installation of WebAccess/DMP, please contact your system administrator to get details of the correct snmp address to configure.*



Dashboard > Devices > Manage Device > Settings

SNMP

Device Settings

Device Name	203-01-9900390
Device ID	203-01-9900390

* Required Field

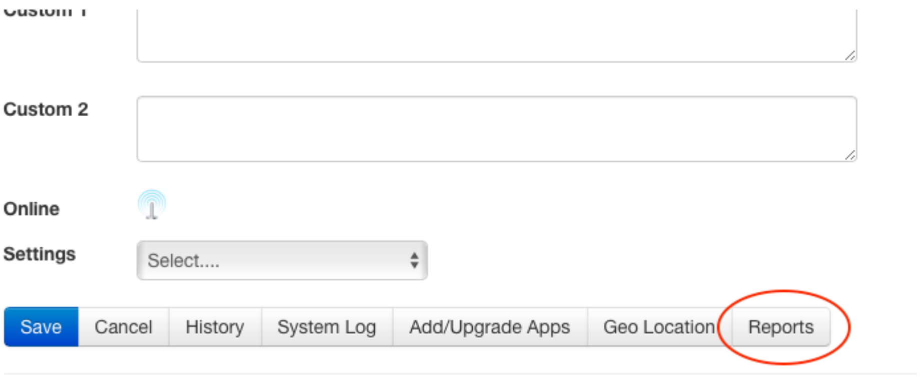
Advanced Settings

SNMP

Enable SNMP agent:	☑
Name:	
Location:	
Contact:	
Enable SNMPv1/v2:	☑
Community:	public
Enable SNMPv3:	□
Username:	
Authentication:	MD5
Authentication Password:	
Privacy:	DES
Privacy Password:	
Enable I/O:	□
Enable M-BUS:	□
Baudrate:	300
Parity:	Even
Stop Bits:	1
Enable reporting:	☑
IP Address:	snmp.bb-smartworx.com
Period (min):	15

Figure 5 SNMP Settings Page

For each Device on which you have SNMP Reports enabled, and for which there has been SNMP data received and stored, you will see the “Reports” button appear on the Manage Device page.



Custom 1

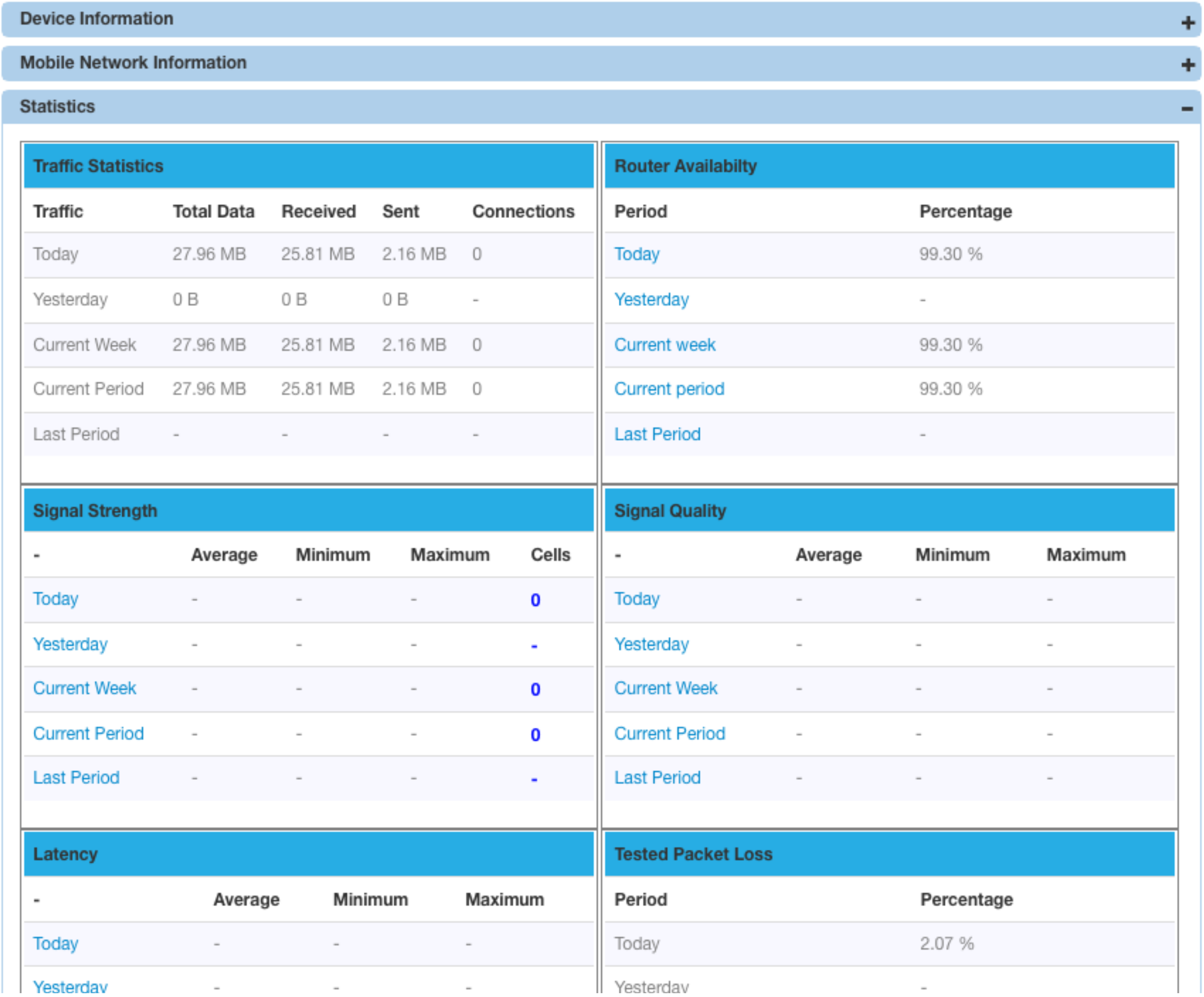
Custom 2

Online

Settings: Select....

Figure 6 Launch Device Report

The Reports button takes you to a screen which shows snmp based diagnostics data and statistics for this device.



Traffic Statistics

Traffic	Total Data	Received	Sent	Connections
Today	27.96 MB	25.81 MB	2.16 MB	0
Yesterday	0 B	0 B	0 B	-
Current Week	27.96 MB	25.81 MB	2.16 MB	0
Current Period	27.96 MB	25.81 MB	2.16 MB	0
Last Period	-	-	-	-

Router Availabilty

Period	Percentage
Today	99.30 %
Yesterday	-
Current week	99.30 %
Current period	99.30 %
Last Period	-

Signal Strength

-	Average	Minimum	Maximum	Cells
Today	-	-	-	0
Yesterday	-	-	-	-
Current Week	-	-	-	0
Current Period	-	-	-	0
Last Period	-	-	-	-

Signal Quality

-	Average	Minimum	Maximum
Today	-	-	-
Yesterday	-	-	-
Current Week	-	-	-
Current Period	-	-	-
Last Period	-	-	-

Latency

-	Average	Minimum	Maximum
Today	-	-	-
Yesterday	-	-	-

Tested Packet Loss

Period	Percentage
Today	2.07 %
Yesterday	-

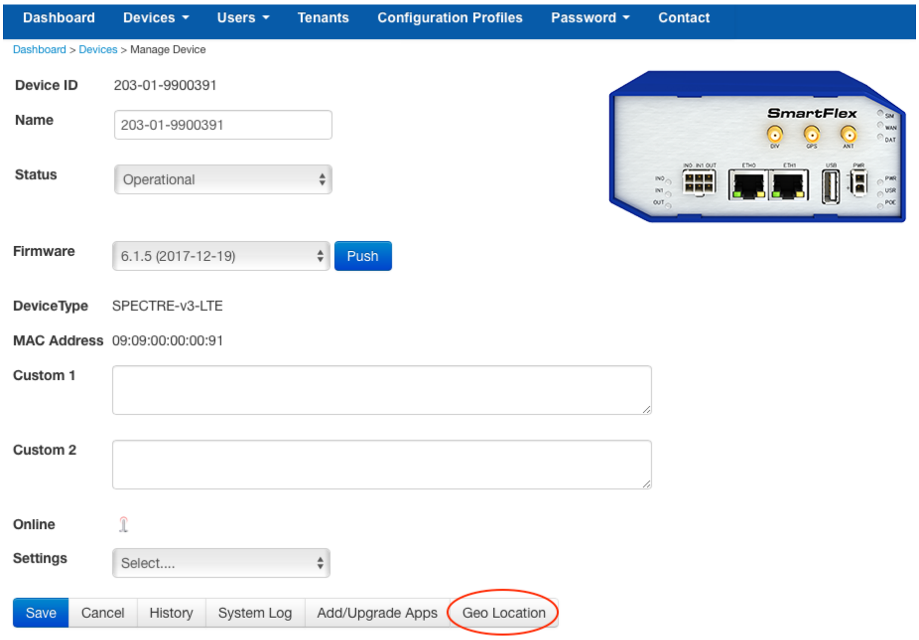
Figure 7 SNMP Report

In the statistics section, where a statistic is described in blue text, clicking on the text will take you through to a screen showing a graph of the value over the selected time period.

5.4.3.7 Geo Location

You may “drop a pin” on a map, or enter latitude and longitude location details, in order to provide specific, static geo-location information for this device.

This information will be used to populate the “Geo Location” map in your Dashboard.
Select your Device, then click on the “Geo Location”



Device ID 203-01-9900391
Name 203-01-9900391
Status Operational
Firmware 6.1.5 (2017-12-19)
DeviceType SPECTRE-v3-LTE
MAC Address 09:09:00:00:00:91
Custom 1
Custom 2
Online
Settings Select....

Figure 8 Launch Geo Location Page

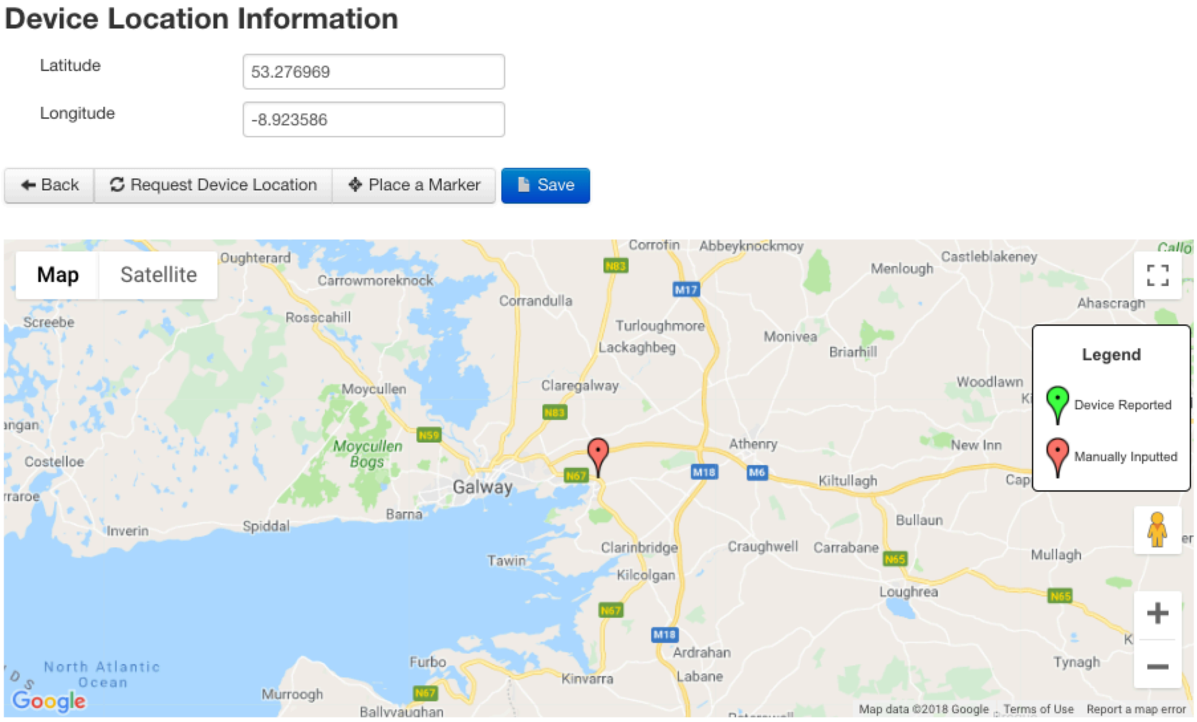
There are 3 ways to get (or set) the geo-loation of the device.

Manually Enter Latitude and Longitude:
If you know the coordinates, you may enter the latitude and longitude, and the pin will appear on the map in-location.

Place a Marker:
Select the button “place a marker”: a pin will appear on the map, and you may drag it into position. As you drag it into position, the latitude and longitude coordinates will auto-populate.

Request Device Location:
You may request location direct from the device. If your device is GPS enabled, it will report-back the coordinates, and the pin will be automatically placed onto the map.

***NOTE**: there are 2 colours used: a red pin will be used in the case of manually entering the coordinates, or dropping the pin on the map. A green pin will be used if the location automatically populated from the device.*



Device Location Information

Latitude: 53.276969

Longitude: -8.923586

Figure 9 Set and Save Device Coordinates

Click on “Save Coordinates”.

5.4.3.8 System Log

This button makes a real-time request to your devices, to get the System Log from it.

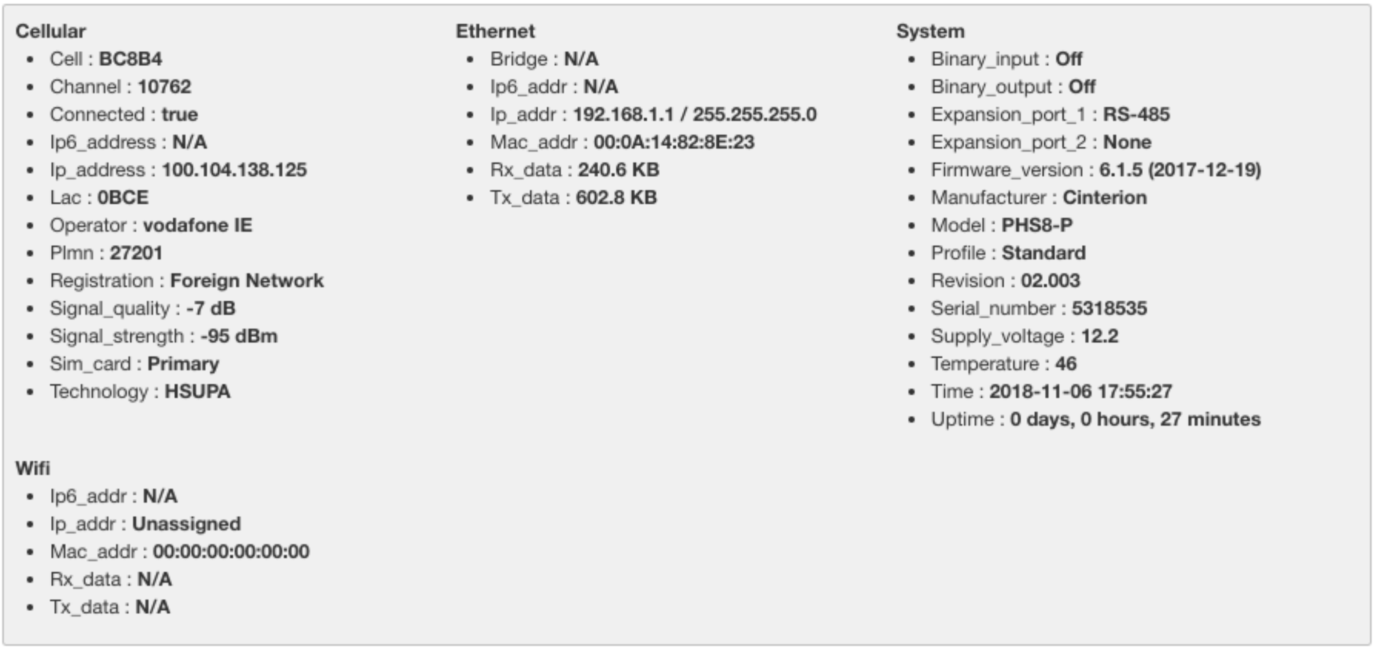
When the page loads, it will display the last known System Log for this device: if the requested information is received from the device while the page is still open, then the latest System Log information will be displayed immediately.

5.4.3.9 Device Status

Use this button to request real-time device-status from your device.

This request will fetch specific information from the device, including Cellular status and statistics, Wifi status and statistics, Ethernet status and statistics, and general System status.

When the page loads, it will display the last know status for ths device: if the requested information is received from the device while the page is still open, then the latest Status information will be displayed immediately.



Cellular

- Cell : **BC8B4**
- Channel : **10762**
- Connected : **true**
- Ip6_address : **N/A**
- Ip_address : **100.104.138.125**
- Lac : **0BCE**
- Operator : **vodafone IE**
- Plmn : **27201**
- Registration : **Foreign Network**
- Signal_quality : **-7 dB**
- Signal_strength : **-95 dBm**
- Sim_card : **Primary**
- Technology : **HSUPA**

Wifi

- Ip6_addr : **N/A**
- Ip_addr : **Unassigned**
- Mac_addr : **00:00:00:00:00:00**
- Rx_data : **N/A**
- Tx_data : **N/A**

Ethernet

- Bridge : **N/A**
- Ip6_addr : **N/A**
- Ip_addr : **192.168.1.1 / 255.255.255.0**
- Mac_addr : **00:0A:14:82:8E:23**
- Rx_data : **240.6 KB**
- Tx_data : **602.8 KB**

System

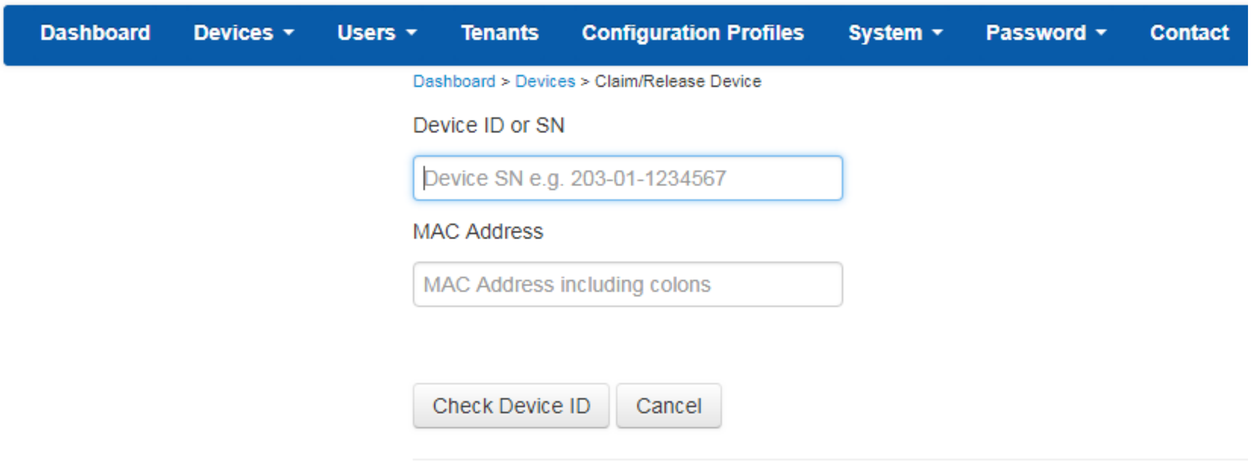
- Binary_input : **Off**
- Binary_output : **Off**
- Expansion_port_1 : **RS-485**
- Expansion_port_2 : **None**
- Firmware_version : **6.1.5 (2017-12-19)**
- Manufacturer : **Cinterion**
- Model : **PHS8-P**
- Profile : **Standard**
- Revision : **02.003**
- Serial_number : **5318535**
- Supply_voltage : **12.2**
- Temperature : **46**
- Time : **2018-11-06 17:55:27**
- Uptime : **0 days, 0 hours, 27 minutes**

Figure 10 Example Device Status

5.5 Manage Devices (in Groups - Configuration Profiles)

If a device is part of a Configuration Profile, then clicking on the Device ID field will take you to the configuration pages for the appropriate Configuration Profile. See later section on Configuration Profiles for further information.

5.6 Claim/ Release Devices



Device ID or SN

Device SN e.g. 203-01-1234567

MAC Address

MAC Address including colons

Figure 11 Claim Device

The Claim/Release Devices screen is the mechanism used to allocate devices to your account.
Every device has a unique Device ID, which is based on the Serial Number of the device.
At the time of manufacture, every device is registered with hub.bb-smartworx.com.
The combination of the Device ID and the MAC Address of the 1st Ethernet port provides a unique combination.

When you receive your device, or batch of devices, you need to “Claim” it into your organisation’s Account: This step makes sure that these devices are yours, and that they cannot be seen by, or claimed by, any other entities.

To Claim each device, you need to enter the full Device ID or Serial Number, and the full MAC Address. Click on ‘Check Device ID’ to confirm that it is available to be claimed by you: then click on ‘Claim Device’ in order to claim it into your account.

The procedure is the same for Releasing a Device: If you have claimed a Device, and you want to move it into a different organisation or account, then you will need to Release it before it can be Claimed by the other account.

Every Device may only be Claimed by one account.

5.6.1 Auto-Claim Process

Importing and claiming large quantities of devices is possible in two ways.
First, you may use the API.
Please see section 7.

Second, you may use the UI (on the Emu Edition), under the System menu item.
To see how you may import and claim large quantities of Devices using the UI, please see section 9.

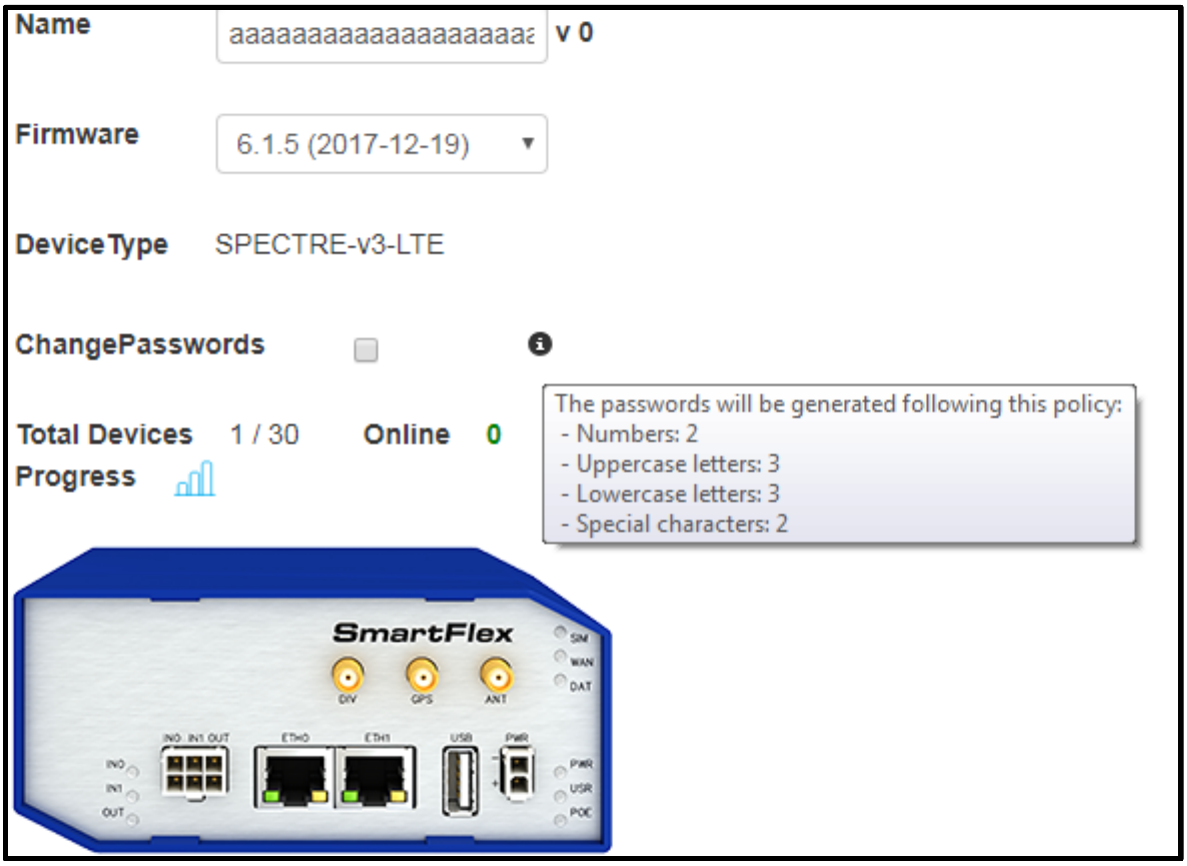
5.7 Device Password Management

5.7.1 Introduction

This feature was added to DMP in release version 1.7.

This feature enables DMP to automatically generate a unique and random password, and then to apply that password automatically to the remote assets (devices).

In this way, the remote-assets can be effectively secured from unwanted, local in-field re-configuration.



Name aaaaaaaaaaaaaaaaaaaa v 0

Firmware 6.1.5 (2017-12-19) ▾

Device Type SPECTRE-v3-LTE

ChangePasswords ☐

The passwords will be generated following this policy:
- Numbers: 2
- Uppercase letters: 3
- Lowercase letters: 3
- Special characters: 2

Total Devices 1 / 30 Online 0

Progress

Figure 12 Password Restriction

5.7.2 Password Criteria

The criteria that specifies a valid password is fixed (cannot be configured by the user).
These criteria are:

- Must have 2 numbers
- Must have 2 uppercase letters
- Must have 2 lower case letters
- Must have 2 special characters

These rules are displayed on the UI in the edit config profile screen shown above.

5.7.3 Resetting remote device Passwords

The passwords are automatically generated by DMP based on the password criteria.
Users can request that a reset-password action is sent to individual remote devices. Assuming the device is online, and the action is successful, users can then view an individual device password on the UI.

The password cannot be viewed by default, or by accident. The user is required to select the password field. The password will be displayed for 5 seconds.

This facilitates local in-field re-confiuration where that is necessary.

NOTE*: if the Local users of the device knows the device-password, s/he can log into that device and change the password again, locally. If this occurs DMP will not be notified of the change. DMP will keep, and display on-request, the “last known password” from DMP’s point of view. If this is no longer accurate, please use DMP to re-set the password once more. The device is not rebooted after the password has been reset.*

5.7.4 Resetting remtote device Passwrods via Configuration Profile

If the password management logic is enabled for the configuration profile, then all devices in the profile are treated as a single unit. This means committing any changes on a profile will trigger a unique and random password reset for each individual device in the profile.

The Configuration Profile must opt-in to the password management feature by selecting the checkbox on the Edit Configuration Profile screen. Once the commit has finished the checkbox will default to unchecked. If this checkbox is unchecked and alterations are subsequently made to the profile, then no change password commands will be sent to the devices.

There is no time limit applied to the password on the device. Users will have to perform save + edit + commit on the profile with password management enabled to trigger the change password actions.

5.7.5 Password Storage

The password for the device is stored in the devices table in the back-end server database. It is not encrypted: we expect that the server itself is secure.

5.7.6 Viewing Passwords

The password for a device can be viewed on the view devices page. By default, on the page view, the password will is obfuscated (i.e. you cannot read it).
Clicking on the obfuscated password trigger a password-fetch from the backend database.
The password will be visible for 5 seconds after which it will disappear.
The password is never cached and is not part of the view devices page DOM.

Not all users of the system can see the passwords in DMP. Only Admin and TPAdmin users can see the passwords.
TPUsers may request the system to reset passwords: but they can’t view the password field.

Viewing the password may show “unknown”.
The reason for this is the root password for that particular device is not currently known by DMP: In other words, DMP has never initiated a Reset Password action to that remote device.

***NOTE**: DMP will only display the “last known password” that DMP itself has sent to the remote Device. If DMP has never sent a password the field will be “unknown”. If DMP has sent a password, it will be displayed. If the local device-password was changed by a local user, unknown to DMP, then the password displayed by DMP will be incorrect. In this case, use DMP to reset that device’s password again.*

6 Users and Roles

The Users option on the main toolbar allows the creation of new users, together with the allocation of roles to those users.
All users created here will belong to the same organisation Account.
By default, the account-creation user will be a “TechnologyProviderAdmin” role.

6.1 Create User

Upon clicking the Create User button, a screen appears into which the relevant details are placed, followed by pressing the ‘Create’ or ‘Cancel’ (revert back to main Users screen without adding user).

Two User Roles are available in the Eagle edition (cloud):

TechnologyProviderAdmin: There must be at least one TPAdmin user-role for every Account. There is no upper limit. By default, the account-creation user will be a TPAdmin.

TechnologyProviderUser: The TPUser role carries most of the same permissions as the TPAdmin role: one big difference however, is that the TPUser role does not provide permission to create new users.

There are additional User Roles available in the Emu edition (on-premises) :

Administrator: The Administrator role is the super-user role. The Administrator has full permissions on all features of the software. Furthermore, the Administrator may oversee Tenancies. An Administrator may create other “Administrator” users. The reserved user “admin” is an Administrator role. We recommend that you do not use the “admin” user, but instead create at least one user on your environment with the Administrator role.

Manufacturer: The Manufacturer role is only useful for Creating / Importing devices into the system. We recommend that you do not use this role.

Permissions	Administrator	TPAdmin	TPUser	Manufacturer
Oversee all Tenants	Yes	No	No	No
Oversee all Devices for all Tenants	Yes	No	No	No
Dashboard: Status Overview Dashboard: Geo Location	Yes Yes	Yes Yes	Yes Yes	No No
Device: View	Yes	Yes	Yes	No
Device: Manage	Yes	Yes	Yes	No
Device: Claim / Release	Yes	Yes	Yes	No
Configuration Profiles: Create New	Yes	Yes	Yes	No
Configuration Profiles: Edit	Yes	Yes	Yes	No
Configuration Profiles: Commit	Yes	Yes	Yes	No
Configuration Profiles: Delete	Yes	Yes	No	No
Users: Create Administrators	Yes	No	No	No
Users: Create TPAdmin users	Yes	Yes	No	No
Users: Create TPUser users	Yes	Yes	Np	No
Users: Lock/Unlock Users	Yes	Yes	No	No
Users: Delete Users	Yes	Yes	No	No
Tenant: Edit	Yes	Yes	No	No
Tenant: Configure Account Profile	Yes	Yes	No	No
System: Import Devices	Yes	No	No	Yes
System: De-Register Devices	Yes	No	No	No
System: Create Sites	Yes	No	No	No
System: Licence Management	Yes	No	No	No
Reset Password of Remote Device	Yes	Yes	Yes	No
View Password of Remote Device	Yes	Yes	No	No

When a user has been created, WebAccess/DMP will automatically send an email-invitation to that user's email address. That invitation includes a link to a "password creation" page. The user will create their own password, and thereafter they will have access to the system.

NOTE*: This is a cloud, or hosted-server, remote-asset management platform. We recommend that you only create users that you trust, and that you enforce a strong password policy.*

6.2 Search

Search through any of the fields. The search function is not case-sensitive.

6.3 Lock/Unlock

From time to time user accounts will get locked out. This happens, for example, when a user has forgotten his password, and he has attempted to login 3 (or more) times using an incorrect password.
Any TPAdmin can un-lock a user-account.
Any TPAdmin can also lock a user-account (for example, if that user is not currently active in the organisation).

Do this by clicking on the padlock image.

6.4 Delete User

The "administrator" cannot be deleted.

The “administrator”, or any “admin” user, can delete all other users.

A “TPAdmin” user can delete any “TPUser” that exists in his Tenant Account.

A “TPUser” cannot delete any users.

A user cannot delete his own account.

6.5 Edit User

Every user can edit his own account.

The “administrator” can edit every user account.
Any “admin” user can edit every user account.

A “TPAdmin” user can edit every user account in his own Tenant account (including other TPAdmin users).

A “TPUser” can only edit his own account.

6.6 History

Click on History to see the audit-log of this user’s activity on the system.

6.7 Email

Click on the email link to edit the user details.

7 Tenant

7.1 Introduction

A Tenant (previously known as “Technology Provider”) is the label that WebAccess/DMP uses for an Organisation Account.
The Tenant is the Organisation that this Account has been created for.

All TPAdmin users can edit the information associated with the Tenant Account.

7.2 Account Details

There are a number of details that you can enter that describes your Organisation Account
(e.g. Organisation Name, Address, Phone number and Mobile number of the main account-holder).

7.3 Account Profile Settings

The Account Profile Settings are configurable settings that describe how you want your Profile to behave.

7.3.1 Enable Daily Syslog

Each device keeps a “syslog”.
On DMP, if you check the “enable daily syslog” checkbox, then DMP will request that syslog, from every device in the Tenancy, every day.
This aggregate of all syslogs will be kept on DMP, for the last 30 days.

7.3.1.1 Syslog File

The SystemLog or “syslog” is a log of actions and events that occur on the remote devices. The amount of data held in the syslog varies and is heavily dependent on how busy the device is. When then log file reaches its size limitation the data in the file is overwritten with the most recent actions and events. Typically the syslog file ranges in size between 10k and 70k. These log files sit on the device.

7.3.1.2 Syslog Enabled

If syslog is enabled on your Account, then the system will automatically request a syslog from all of the routers associated with your account (and “online” at the time of the request) on a daily basis. This will happen at midnight, UTC. The schedule is not configurable.

The data from the syslog file is stored in the ErrorMessage column of QueuedCommand table in the backend database. Up to 2GB may be stored. The obtained syslog for each router will be retained on the system, in the database, for 7 days. The most recent syslog for each individual router may be viewed by clicking the “System Log” button on the Manage Device screen.

To view previous logs, click on the router you want to see and click the History button, then use the search bar to search for “SystemLog”.

If you wish to keep an audit of activity on your devices then this field should always remain checked.

8 API

WebAccess/DMP has a Server-to-Server API service available.
The API feature has been available since release number 1.2.1

The API may be accessed through the link on the top-right of the WebAccess/DMP UI (available from release version 1.8) or via the URL: hub.bb-smartworx.com/API/v2/

NOTE: As new API versions are released, they will be available under the specified API version number at the end of the WebAccess/DMP URL.

This API offers RESTful services.

8.1 API Pre-Requisites and Constraints

API v1 only works with routers.
API v2 works with all routers and SmartSwarm IoT gateways.

The API works with routers that are in a Configuration Profile: but it is more limited. It only allows the read-only requests to complete.

The routers must have Firmware Version 6.0.0 or above
The gateways must have Firmware Version 2.2.0 or above.

The routers must have the “API Manager” user module installed… OR
The routers must have “hmpclient” version 1.6 or higher

8.2 API Endpoints

API endpoints evolve over time: at the time of print, the API is at version 2.
The best source of up-to-date documentation is in the software itself (e.g. http://hub.bb-smartworx.com/api/v2/).

As a rule of thumb, when the API up-revs by a full version (e.g. v1 to v2; or v2 to v3), the up-revved version is NOT backward compatible with the previous version.

However, the previous version will still be supported as documented (e.g. http://hub.bb-smartworx.com/api/v1/).

The available endpoints, in version 2, were:

REST Service	String	Description
POST	/user-tokens	Returns a token after authenticating the user. This is the token that should be used in all other endpoints. This token is revoked after 24 hours of inactivity.
POST	/device-tokens	Returns a device token if the ID and MAC provided are correct. This token can later be used to claim the device and call the other endpoints.
GET	/devices	If logged as administrator, requests all devices. The request can contain a filter. As this endpoint returns all devices, it's advisable to filter it to avoid unnecessary stress on the system

POST	/devices	If logged as administrator, creates a new device on the system. The Type property is not required when creating a device and will be ignored if set. After creation a Technology Provider Admin or User can claim the device.
DELETE	/devices/{deviceToken}	Completely removes a device from WebAccess/DMP, including all history. This endpoint will return error if the device belongs to a Configuration Profile
GET	/my-devices	Returns properties for all devices claimed by the user. Some identify the device and are read-only while others are mutable, like the connection status.
PATCH	/my-devices{deviceToken}	Allows modification of some device properties, the claimed status and some text properties. The device's token can be obtained through the /device-tokens endpoint.
GET	/my-devices/{deviceToken}/configurations	Requests the full configuration to the device. "config" and "section" parameters allow to get a subset of the config but are useful only for Gateways. Routers return text/plain as a set of key=value pairs, equivalent to backup the configuration from the device web interface. Gateways return a JSON array with each section as an object
PATCH	/my-devices/{deviceToken}/configurations	Writes a full or partial configuration to the device
GET	/my-devices/{deviceToken}/files	It requests all Gateway files that WebAccess/DMP knows of, openvpn certificates and keys. The optional file parameter acts as a filter and must contain a valid path of one of the known files. The extension of the file is optional. Routers are not able to answer this request, so this endpoint will return an error message when querying them.
PUT	/my-devices/{deviceToken}/files	Overwrites a list of files on the Gateway. The objects in the array must have the same format of the one received on the GET endpoint or an error will be returned. The allowed files to write are also the ones returned by the GET endpoint. The extension of the file is optional. The array of files is processed one by one. If an error occurs the process will be stopped and the error returned
POST	/my-devices/{deviceToken}/reboot	Commands a device to reboot and returns immediately. The device will not send any warning or confirmation to users connected through other interfaces, like http or ssh. It may take up to 5 minutes for the device to be responsive again. This is the only endpoint that represents a "request for command". The response is 202 Accepted and the device will apply it in its own time.
GET	/my-devices/{deviceToken}/status	Returns the status information of the device. The contents of the object vary depending on the device, although the general structure of the example will always be present.

NOTE*: The latest API documentation will be available on the live environment: e.g. http://hub.bb-smartworx.com/api/v2/*

9 Configuration Profiles

Sometimes, you will want to manage your remote assets in groups, rather than individually.
When this is the case, you should consider using Configuration Profiles.

9.1 Introduction

A Device may be configured in many ways:

1. A device may be configured as an individual device, via the WebAccess/DMP UI.
2. A device may be configured as an individual device, via the WebAccess/DMP API for Devices.
3. A device may be configured as an individual device, via the device's local web-server.
4. A device may be configured as part of a Configuration Profile, via the WebAccess/DMP UI.

When using Configuration Profiles to configure an estate of remote-devices, the assumption is that this is the only method being used for remote-device configuration.

- **1 and 4 are mutually exclusive**: a Device cannot be configured as an individual device via the UI, if it is in a Configuration Profile.
- **2 and 4 are mutually exclusive**: a Device cannot be configured as an individual device via the API, if it is in a Configuration Profile.
- **3 and 4 are NOT mutually exclusive**: but we STRONGLY RECOMMEND that the device is NOT configured as an individual device, via the local device's web-server. Doing so will result in un-defined WebAccess/DMP system behaviour.

***NOTE**: When using Configuration Profiles to manage groups of devices, you should not use any other method to configure those devices.*

9.2 What is a Configuration Profile?

This is feature that enables you to create a group or groups (aka. profiles) of Devices that you want to configure in the same or similar ways.

The TPAdmin and TPUser roles can create and Edit Configuration Profiles that belong to their organisation Account: the TPUser cannot delete a Configuration Profile.

The number of Devices that may be in a Configuration Profile is limited: it will be limited to either 200 or 500 devices, depending on your licence.

Every Configuration Profile may be created for only one Device Type.

A Device Type is defined by the unique Order Code for the Device.

Using the Configuration Profiles feature, you will be able to:

- Define which Settings should be configured as the "Profile" level, and which should be configured on an Individual Device level
  - Settings that are "Profile" level will be configured once, then written to all Devices in the Profile
  - Settings that are "Device" level will be configured individually on a per-Device basis
    - "Device" level settings may be configured using an excel spreadsheet
- Define the FW version you want on all of the Devices on your Profile.
- Manage Profile Settings
  - For "Profile" level settings, set any, or all, of the device settings to what you want them to be

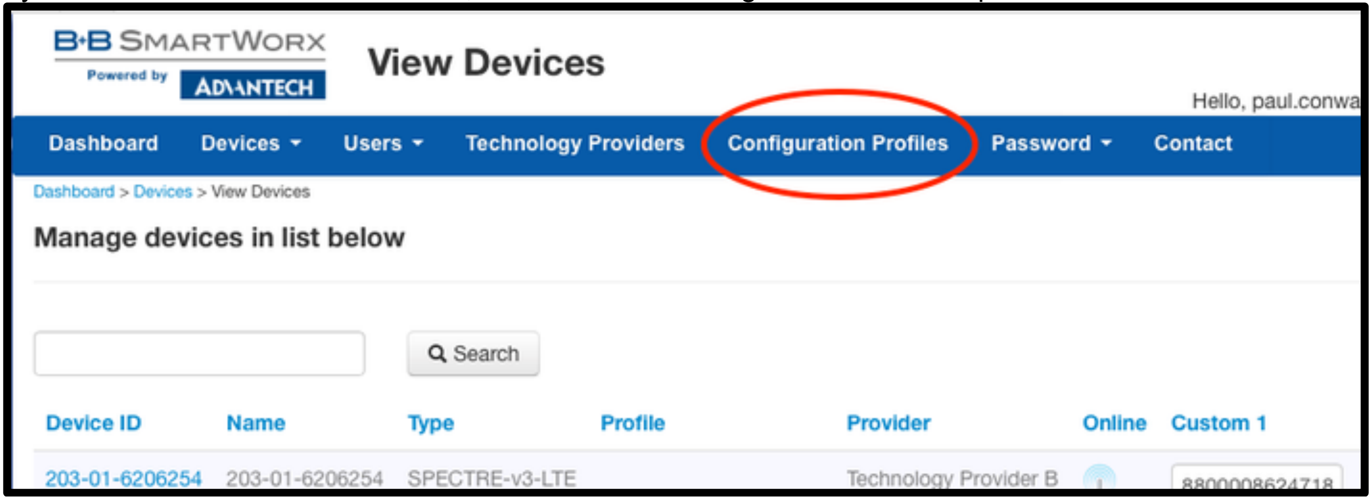
    - For "Device" level settings, export to an excel-sheet, set the individual settings to what you want them to be, then import your settings back into the Profile
- Manage Apps
    - Select the Apps (User Modules) that you want on all of your Devices
    - Define which of the Apps settings should be "Profile" level, and which should be "Device" level
        - For "Profile" level App Settings, set any, or all, of the device settings to what you want them to be
        - For "Device" level App settings, export to an excel-sheet, set the individual settings to what you want them to be, then import your settings back into the Profile
- Manage Devices
    - Select the Devices that you want to have in this Profile
        - The Devices can be placed into a Profile, before you turn them on
    - Add Devices to the Profile later
    - Remove Devices from the Profile
    - Reboot Devices in the Profile

9.2.1 Examples of when this feature is useful

- Zero-touch configuration of field-devices
- One or more configuration-change is required for a pre-defined Group of remote devices
- Firmware Update is required for a pre-defined Group of remote devices
- New Apps are required for a pre-defined Group of remote devices

9.2.2 How do I use it?

Login to your account on WebAccess/DMP, and select the Configuration Profiles option from the menu bar.



View Devices

Hello, paul.conwa

Dashboard > Devices > View Devices

Manage devices in list below

Device ID	Name	Type	Profile	Provider	Online	Custom 1
203-01-6206254	203-01-6206254	SPECTRE-v3-LTE		Technology Provider B		8800008624718

Figure 13 Configuration Profile Menu

9.3 The Configuration Profiles Workflow: Overview

9.3.1 The General Workflow: Context Diagram

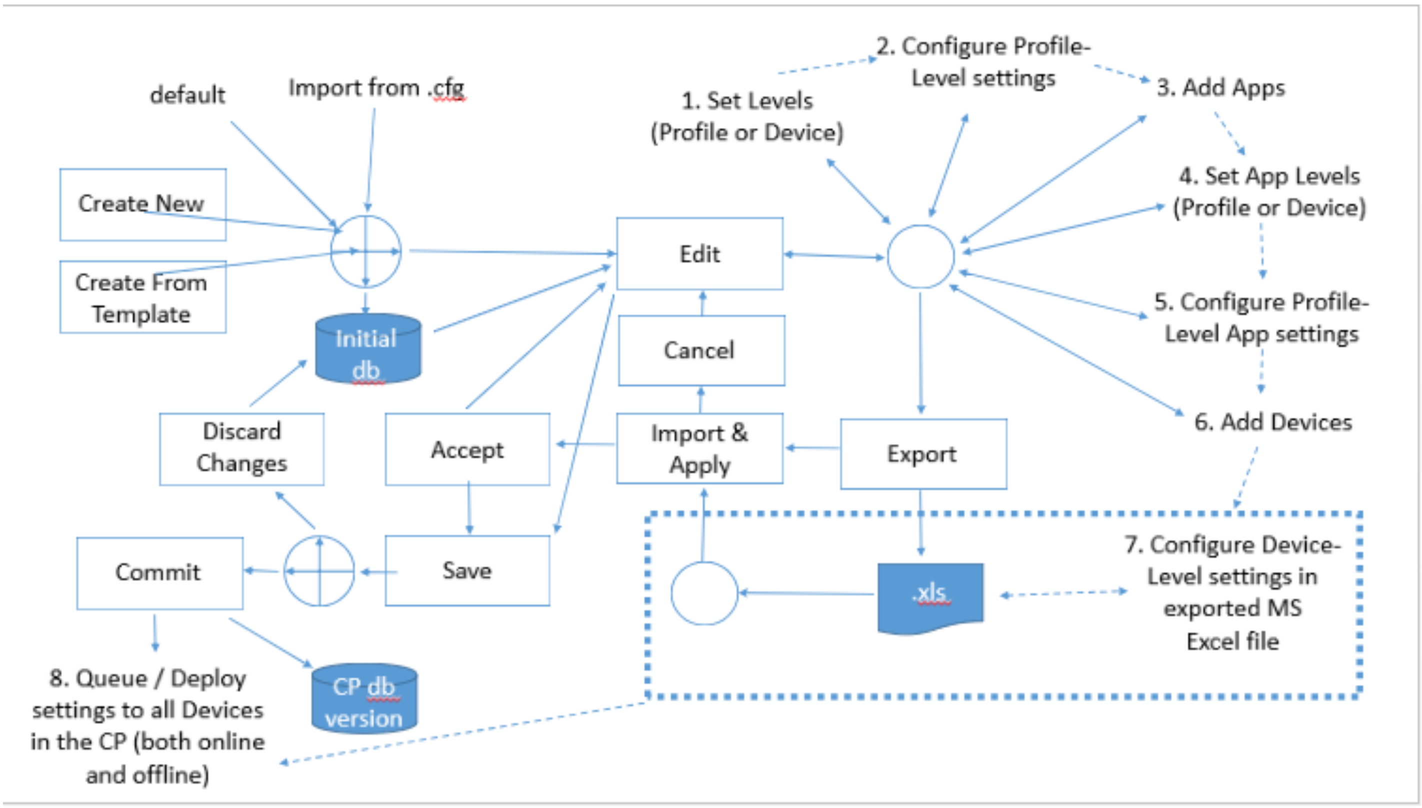

default
Import from .cfg
Create New
Create From Template
Initial db
Edit
Cancel
Import & Apply
Export
Discard Changes
Accept
Save
Commit
CP db version
1. Set Levels (Profile or Device)
2. Configure Profile-Level settings
3. Add Apps
4. Set App Levels (Profile or Device)
5. Configure Profile-Level App settings
6. Add Devices
7. Configure Device-Level settings in exported MS Excel file
.xls
8. Queue / Deploy settings to all Devices in the CP (both online and offline)

Figure 14 Configuration Profile Workflow

We will refer to this diagram for contextual purposes during our discussion of Configuration Profiles.

9.3.2 The Simple Workflow

This workflow is appropriate when you are pre-configuring your device-estate so that every device will receive the exact same configuration. It is recommended that users configure the properties of the profile first before adding apps and devices. The steps would therefore be

1. Create the profile with specific device type and firmware
2. Edit the profile and change settings (ssh, vvrp, mobile wan, NAT ...etc.) followed by save + commit.
3. Edit the profile and add the apps. save + commit
4. Edit the profile and add the devices. Save + commit

In the initial versions of DMP adding devices was a mandatory step in the creation of a profile. This is no longer the case. If there are no devices in the profile then the profile is redundant as no commands will be queued.

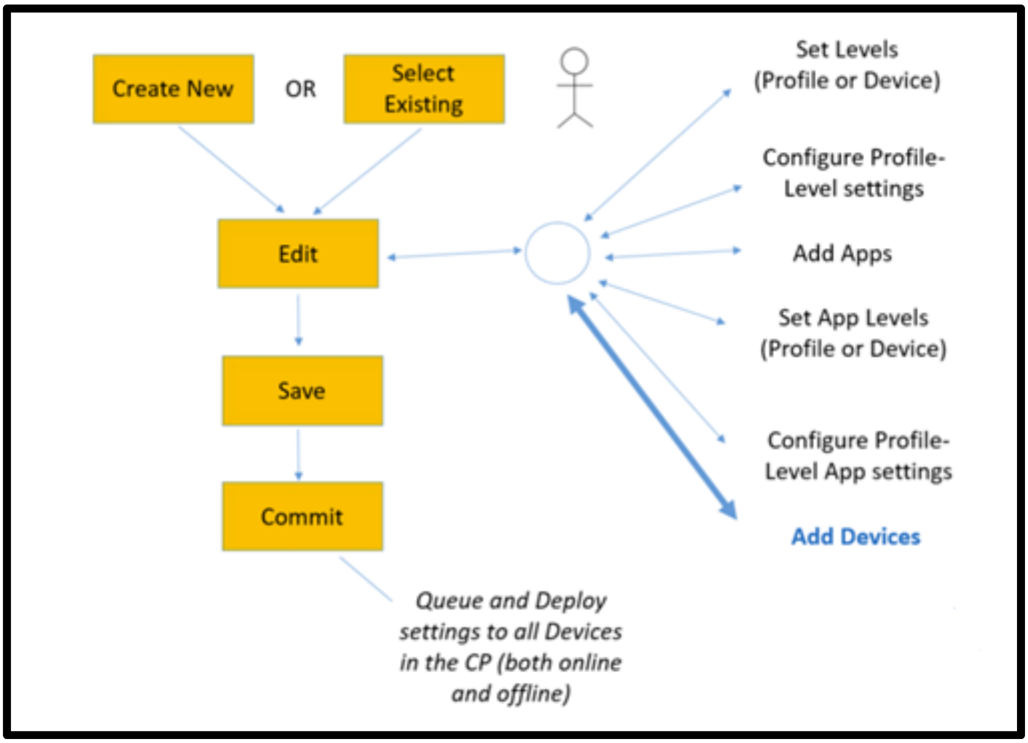

Create New
OR
Select Existing
Edit
Save
Commit
Set Levels (Profile or Device)
Configure Profile-Level settings
Add Apps
Set App Levels (Profile or Device)
Configure Profile-Level App settings
Add Devices
Queue and Deploy settings to all Devices in the CP (both online and offline)

Figure 15 Configuration Profile Simple Workflow

9.3.3 The Simple Workflow: Context Diagram

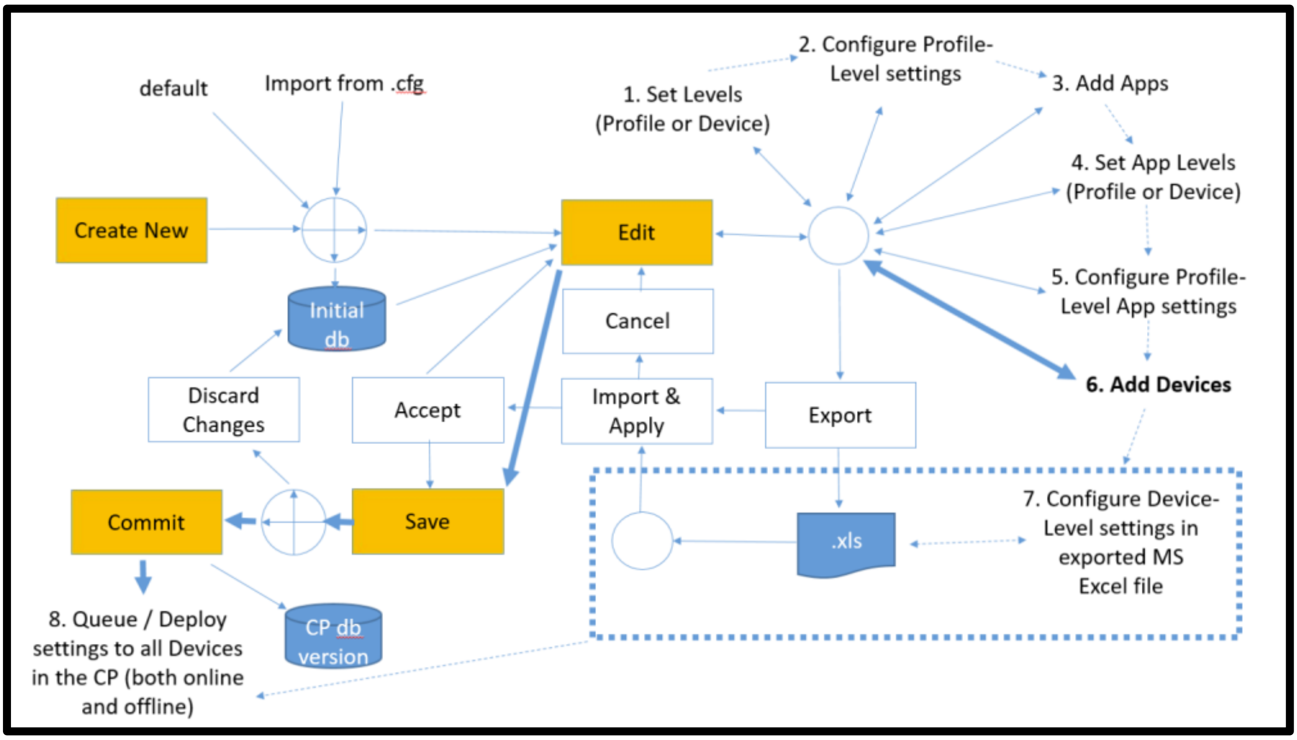

default
Import from .cfg
Create New
Initial db
Edit
Cancel
Discard Changes
Accept
Import & Apply
Export
Commit
Save
8. Queue / Deploy settings to all Devices in the CP (both online and offline)
CP db version
1. Set Levels (Profile or Device)
2. Configure Profile-Level settings
3. Add Apps
4. Set App Levels (Profile or Device)
5. Configure Profile-Level App settings
6. Add Devices
7. Configure Device-Level settings in exported MS Excel file
.xls

Figure 16 Simple Workflow Context

9.3.4 The Full Workflow

This workflow is appropriate when:

- You are pre-configuring your device-estate...
  - so that every device will receive the exact same settings for some (profile level) configuration-items
  - so that every device will receive specific individual settings for some (device level) configuration-items

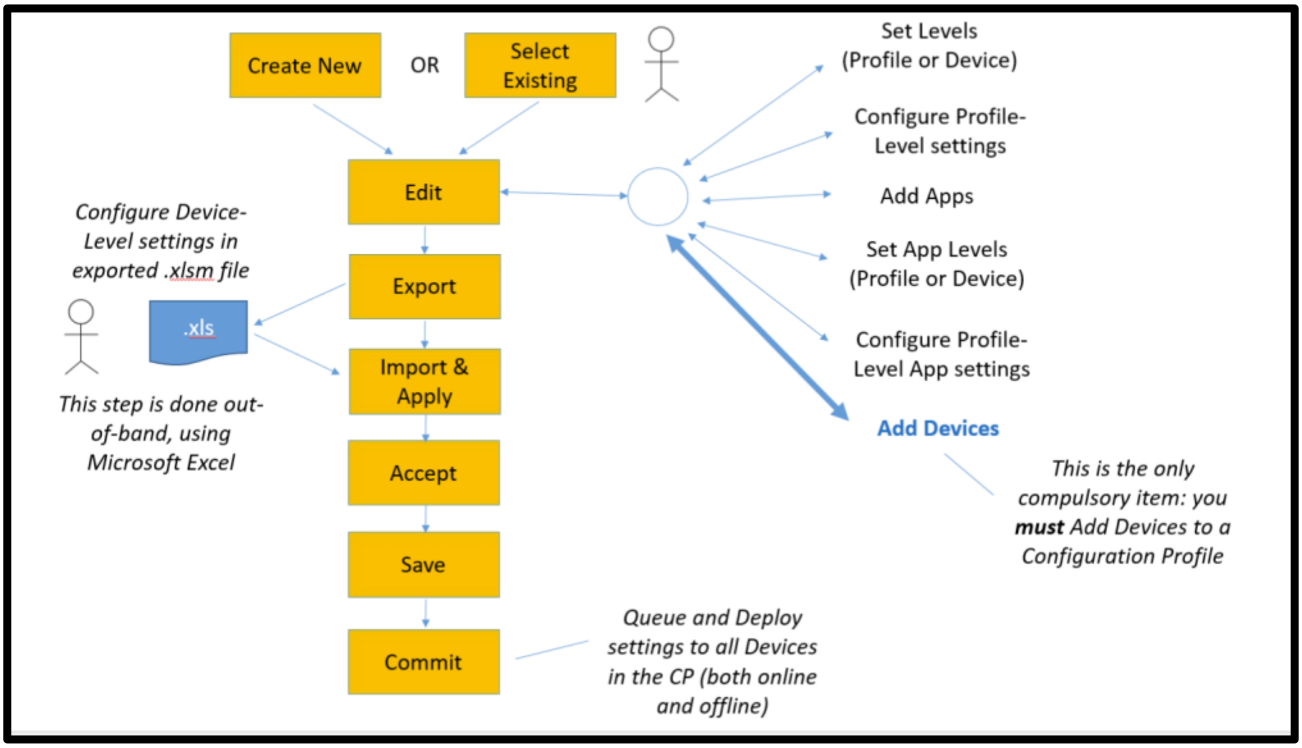
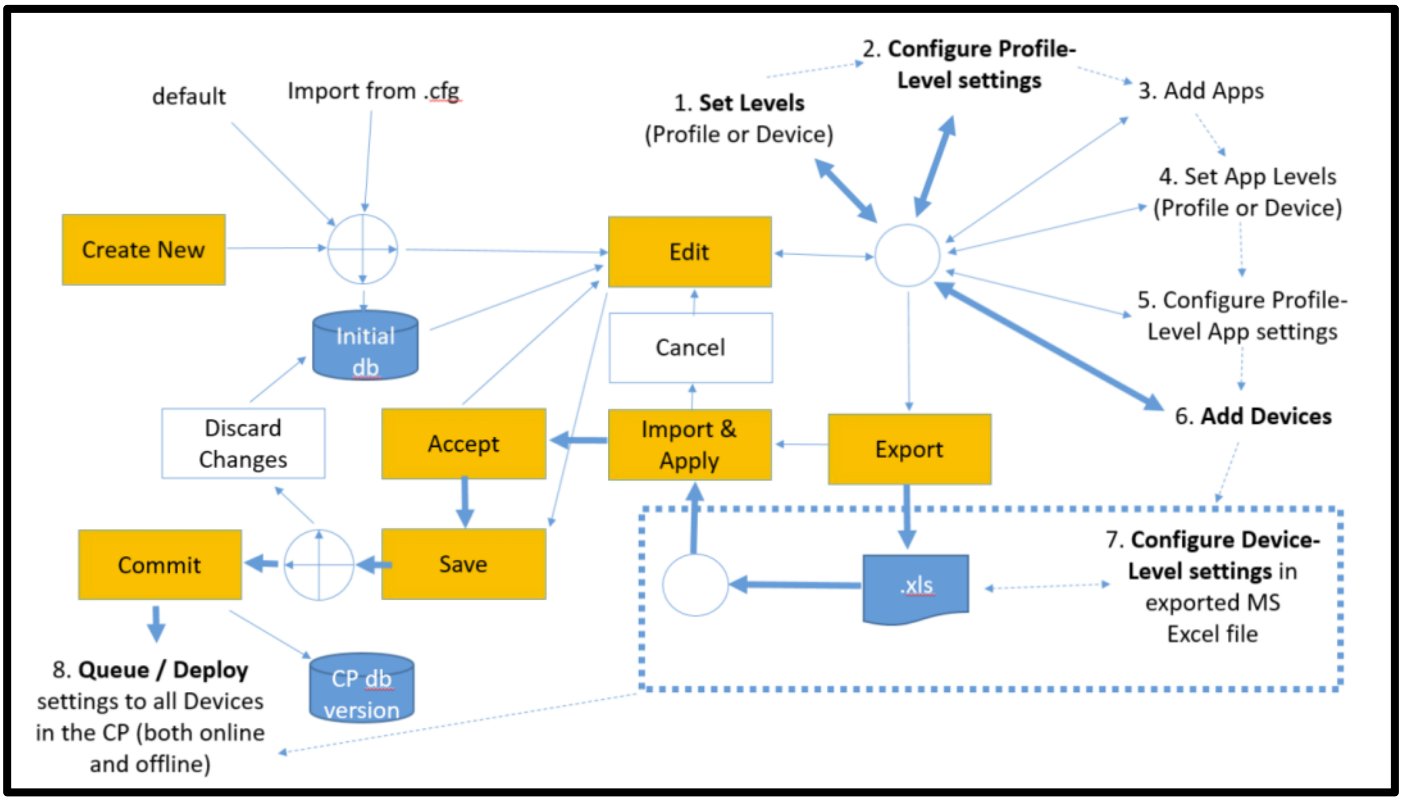

Create New
OR
Select Existing
Edit
Export
Import & Apply
Accept
Save
Commit
Configure Device-Level settings in exported .xlsm file
.xls
This step is done out-of-band, using Microsoft Excel
Set Levels (Profile or Device)
Configure Profile-Level settings
Add Apps
Set App Levels (Profile or Device)
Configure Profile-Level App settings
Add Devices
This is the only compulsory item: you must Add Devices to a Configuration Profile
Queue and Deploy settings to all Devices in the CP (both online and offline)

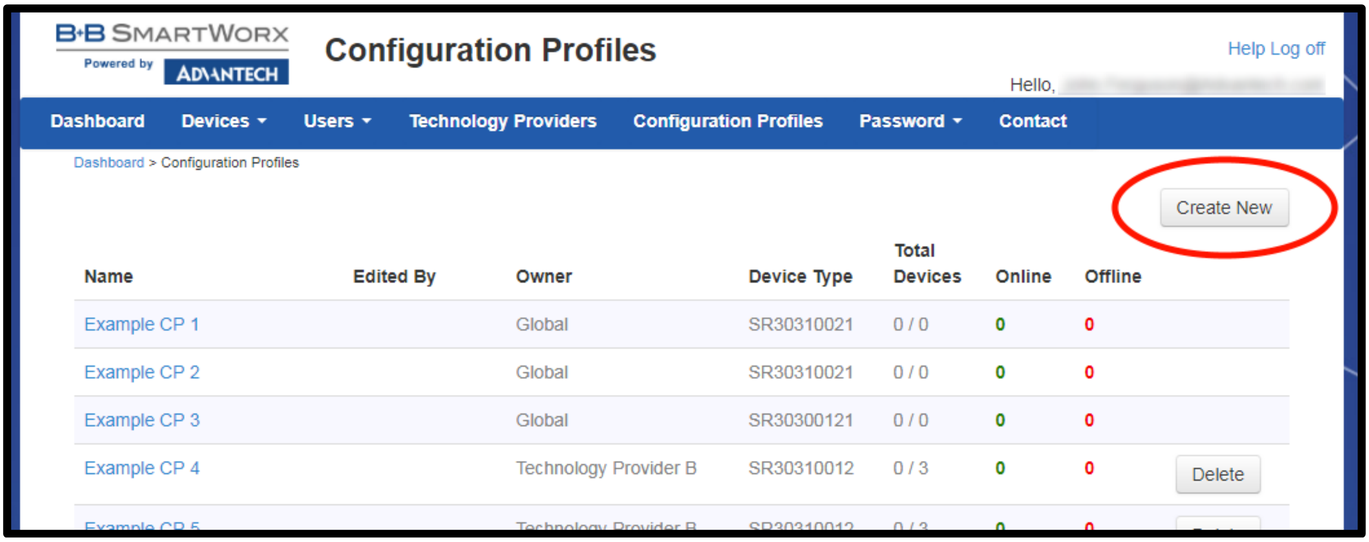
Figure 17 Full Workflow

9.3.5 The Full Workflow: Context Diagram


default
Import from .cfg
Create New
Initial db
Discard Changes
Commit
8. Queue / Deploy settings to all Devices in the CP (both online and offline)
CP db version
Accept
Save
Edit
Cancel
Import & Apply
Export
.xls
1. Set Levels (Profile or Device)
2. Configure Profile-Level settings
3. Add Apps
4. Set App Levels (Profile or Device)
5. Configure Profile-Level App settings
6. Add Devices
7. Configure Device-Level settings in exported MS Excel file

9.4 Create a New Configuration Profile

Click on the "Create New" button.



Configuration Profiles

Help Log off

Hello, [redacted]

Dashboard | Devices ▾ | Users ▾ | Technology Providers | Configuration Profiles | Password ▾ | Contact

Dashboard > Configuration Profiles

Create New

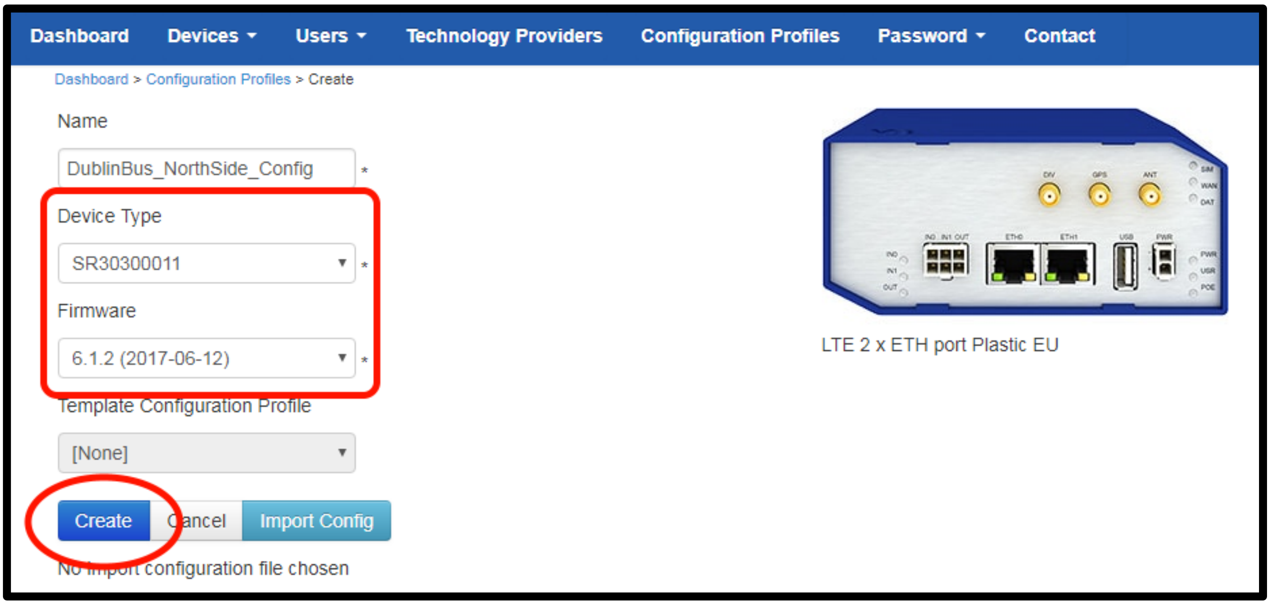
Name	Edited By	Owner	Device Type	Total Devices	Online	Offline	
Example CP 1		Global	SR30310021	0 / 0	0	0	
Example CP 2		Global	SR30310021	0 / 0	0	0	
Example CP 3		Global	SR30300121	0 / 0	0	0	
Example CP 4		Technology Provider B	SR30310012	0 / 3	0	0	Delete
Example CP 5		Technology Provider B	SR30310012	0 / 3	0	0	

Figure 18 Launch Create Profile Page

From here, you have two options.

9.4.1 Use Defaults

Create a Configuration Profile (CP) from the WebAccess/DMP (DMP) default settings.
Select the Device Type and FW version for this CP.
You must also give it a unique name.
Then select "create".



Dashboard | Devices ▾ | Users ▾ | Technology Providers | Configuration Profiles | Password ▾ | Contact

Dashboard > Configuration Profiles > Create

Name: DublinBus_NorthSide_Config *

Device Type: SR30300011 ▾ *

Firmware: 6.1.2 (2017-06-12) ▾ *

Template Configuration Profile: [None] ▾

Create | Cancel | Import Config

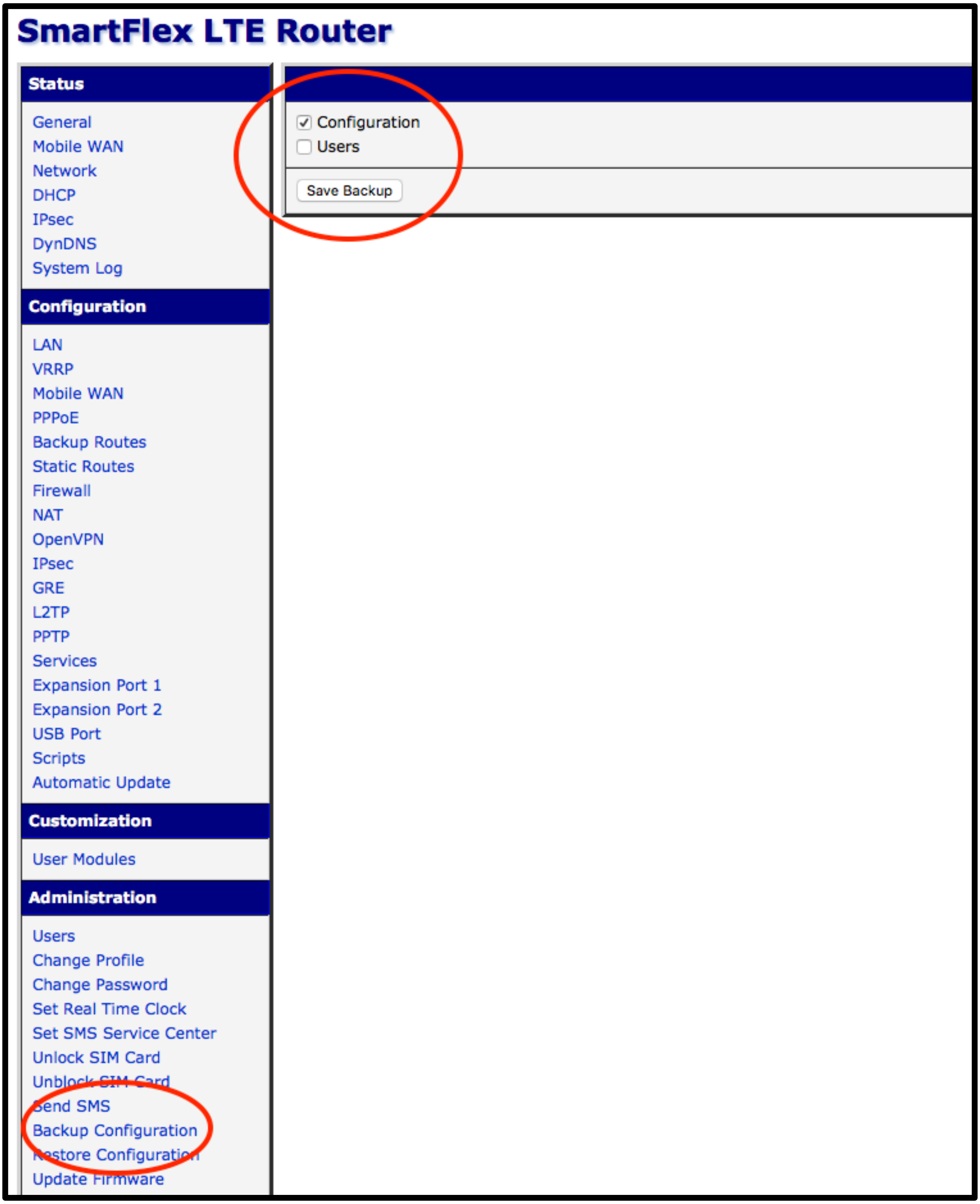
No import configuration file chosen

LTE 2 x ETH port Plastic EU

Figure 19 Create Profile

9.4.2 Import a Router's .cfg file

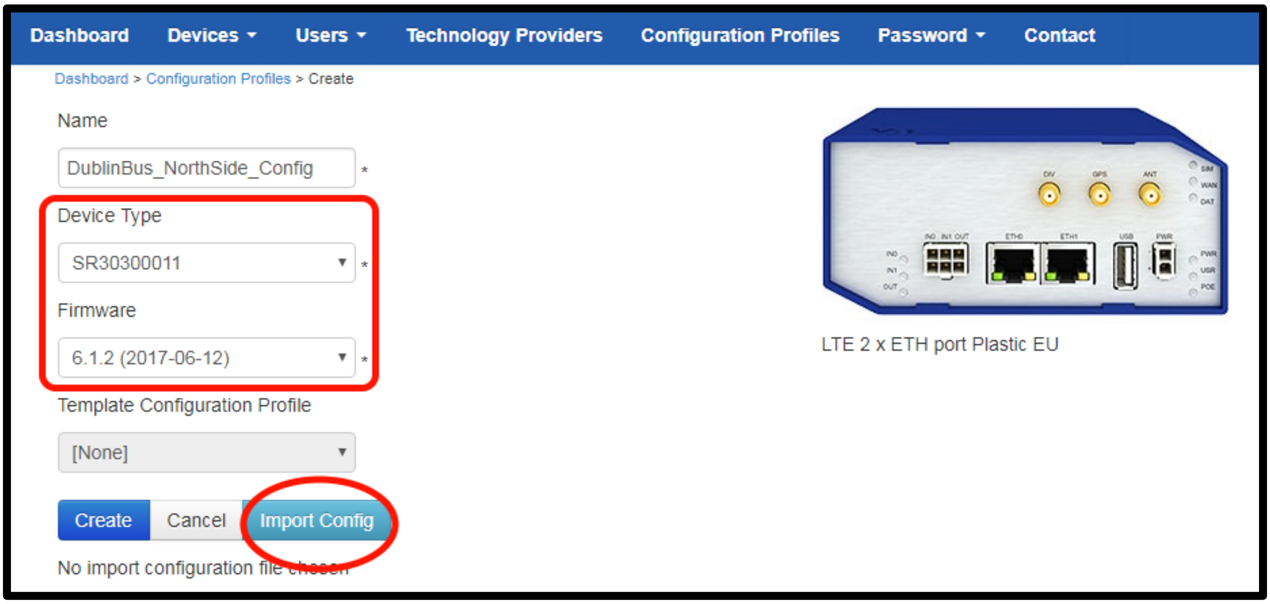
Create a Configuration Profile from a "configuration backup" file that you exported from a router.
First, configure your device the way you would like the CP to be configured. Then export this configuration to a file, using the router's "Backup Configuration" option.



☑ Configuration
☐ Users

Figure 20 Device Configuration File Generation

Next, import this configuration into the DMP CP by selecting the "Import Config" option.



Dashboard > Configuration Profiles > Create

Name: DublinBus_NorthSide_Config *

Device Type: SR30300011 *

Firmware: 6.1.2 (2017-06-12) *

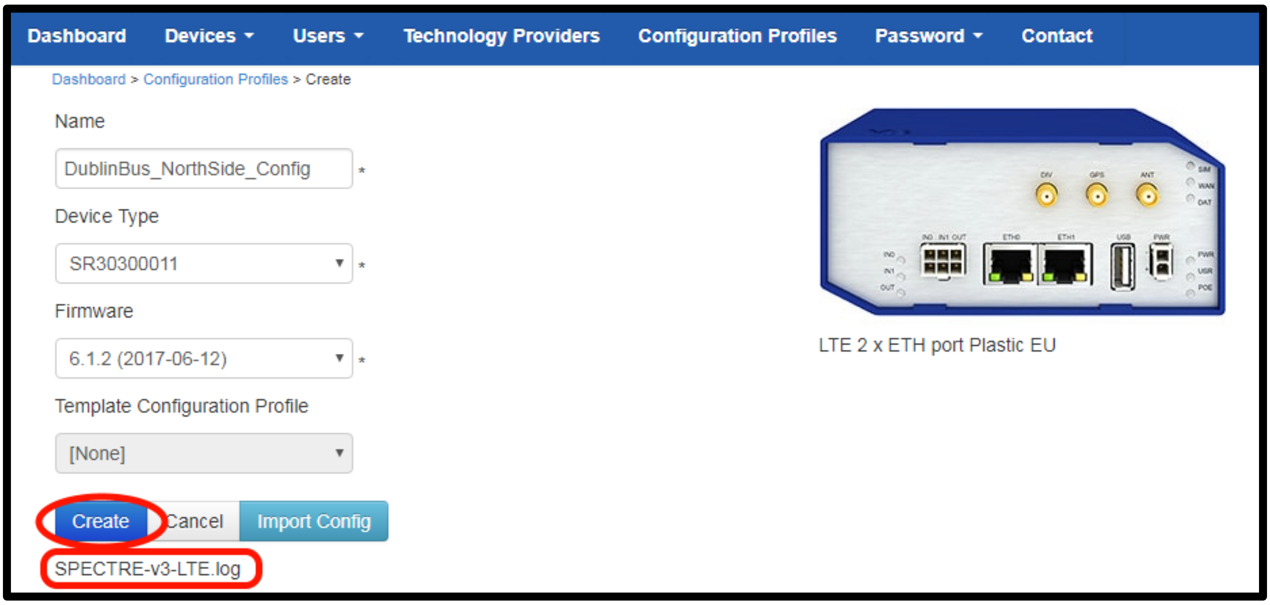
Template Configuration Profile: [None]

No import configuration file chosen

LTE 2 x ETH port Plastic EU

Figure 21 Create Configuration Profile From Config

The name of the import file will appear in the UI.
Now, select "Create".



Dashboard > Configuration Profiles > Create

Name: DublinBus_NorthSide_Config *

Device Type: SR30300011 *

Firmware: 6.1.2 (2017-06-12) *

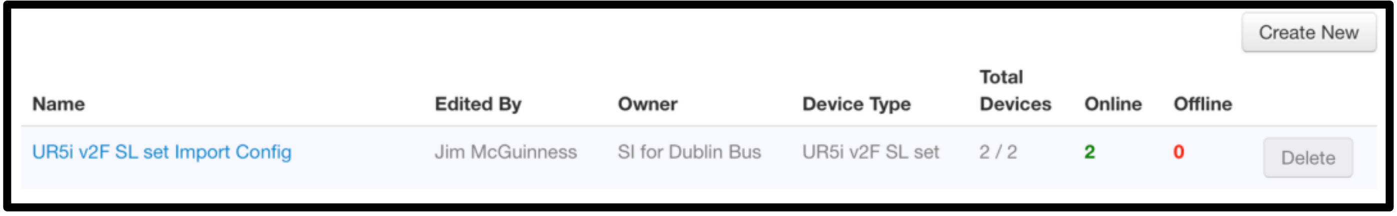
Template Configuration Profile: [None]

SPECTRE-v3-LTE.log

LTE 2 x ETH port Plastic EU

Figure 22 Create Configuration Profile

Select an Existing Configuration Profile
On the CP View, you will see information regarding the CPs that have been created on the Platform.
To Select a Configuration Profile, simply click on the name of that CP.



Name	Edited By	Owner	Device Type	Total Devices	Online	Offline	
UR5i v2F SL set Import Config	Jim McGuinness	SI for Dublin Bus	UR5i v2F SL set	2 / 2	2	0	Delete

Column	Description

Name	This is the name of the Configuration Profile (CP). The one you created will be listed here.
Edited By	This is the name of the last person who edited the CP. If there's no name, then it has not been edited since it has been created.
Owner	This is the name of the organisation account that "owns" (created) this CP. A "Global" owner means that this CP was created by the Site Administrator. Only Site Administrators can edit or delete a "Global" CP.
Device Type	The device-type that each CP was created for. There's a one-to-one relationship between a Device Type and a CP.
Total Devices	This shows 2 numbers, in this format " n / m " "n" represents the number of devices, of this device-type, that are currently included in this CP. "m" represents the total number of devices, of this Device Type, on the system. NOTE that, if some of these devices are already in another CP, then they will not be available for use in this one.
Online	This is the number of devices that are included in this CP, that are currently Online. This will be a number between 0 and "n".
Offline	This is the number of devices that are included in this CP, that are currently Offline. This will be a number between 0 and "n".

Button	Function
DELETE	Remove this CP from the system. It is only possible to Delete a CP if: there are no Devices in the CP you have permission to Delete the CP the CP is not currently in Editor Mode
Create New	Create a New Configuration Profile

9.4.3 Creating from templates

Profiles can also be created from existing profiles in the system. This is useful in scenarios where a profile may be tested in a lab setting prior to been published to the release pipeline. There are some key points to remember when using the templates:

- The profile created from the template will inherit the settings and apps of the template but **NOT** the devices.
- A profile can only be created from template if the intended device type of the profile is the same as the template.
- Once the profile is persisted to the database the relationship between the template and profile is lost. Users could possibly adopt a naming convention for the profiles that will retain this relationship.
- The firmware of the profile is set from the template.
- Any user that can create a profile can create a template.
- Admin uses are the only users that can create Global templates. They are also the only users of the system that can delete the Global templates.
- There is no restriction on the nesting of templates. In other words, a template can inherit from another template and so on.
- Changes to the parent template will **NOT** be inherited by the profiles that have already been created from the template.

9.5 Configuration Profile Modes

There are 4 possible modes that the Configuration Profile may be in.

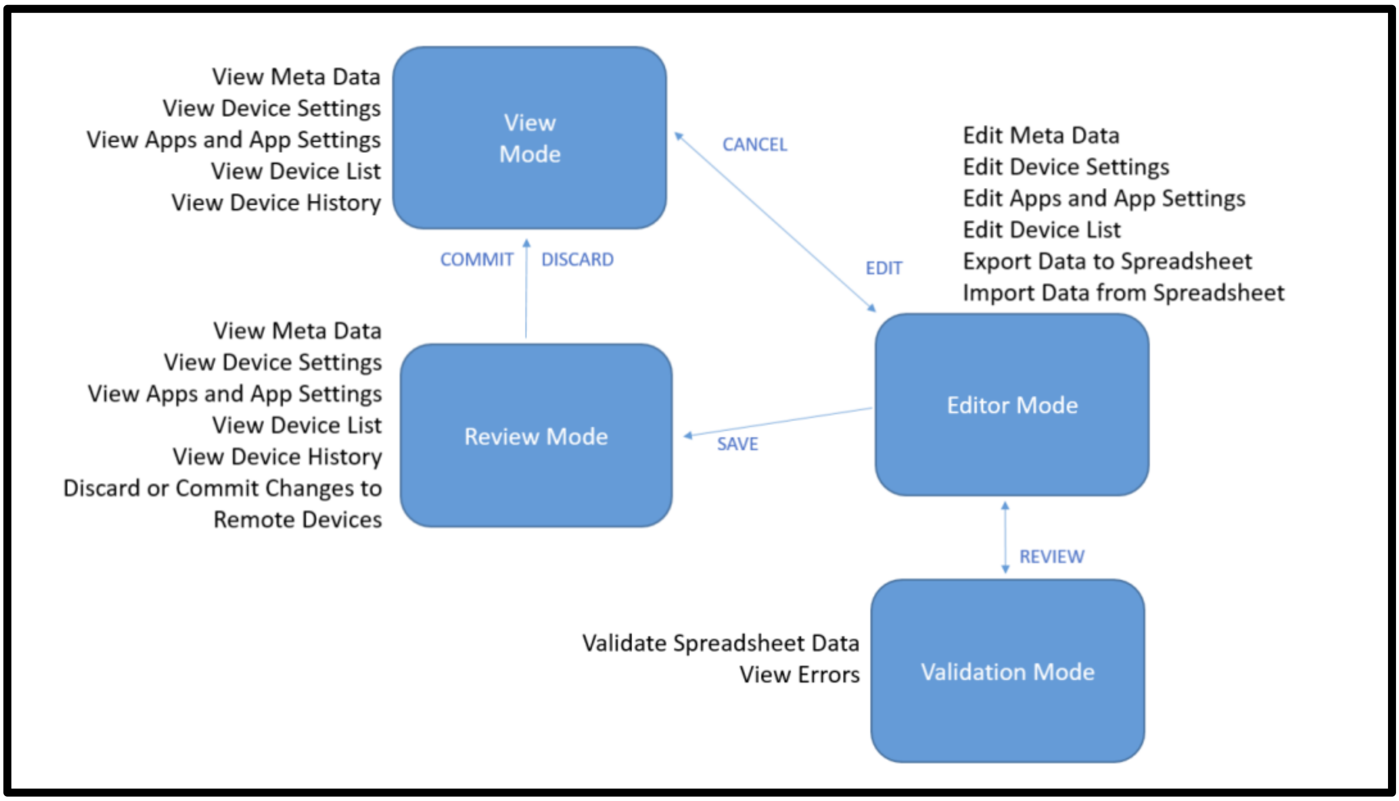


Figure 23 Profile Modes

9.5.1 View Mode

View Mode is the default mode of all configuration profiles irrespective of the creator. After creation, the profile will be in view mode. Users have a limited set of actions they can perform on the profile in view mode.

In View Mode, it is not possible to make any changes.
You can Export Data to Spreadsheet only if there is at least one Device in the CP.

In order to make changes to the CP, you must select the Edit button in order to enter the Editor Mode.
You will be able to enter Editor Mode if:

- You have permissions to Edit this CP
- This CP is not held in Editor Mode by another user

9.5.1.1 Functions available

View Meta Data	Configuration Profile Name Firmware version Device Type Total Devices Online/Offline Devices
View Device Setting	(“Manage Profile Settings”)
View Profile Apps and App Settings	(“Manage Apps”)
View Device List	(“Manage Devices”)

9.5.1.2 *Buttons Available*

Export	Export the CP to a Spreadsheet This button only works if there is at least one Device in the CP.
Edit	Transition into Editor Mode

9.5.2 Editor Mode

9.5.2.1 *Functions available*

Edit Meta Data	CP name Firmware Version
Edit Device Settings	("Manage Profile Settings")
Edit Apps and App Settings	("Manage Apps")
Edit Device List	("Manage Devices")
Export Data to Spreadsheet	
Import Data from Spreadsheet	

9.5.2.2 *NOTEs*

A CP may be edited by only one user at a time.
A user may be editing more than one CP at a time.
There are over 1000 possible configuration-items.

For both "**Manage Profile Settings**" and "**Manage Apps**":

Every available configuration-item can be designated as a Profile Level configuration-item, or a Device Level configuration-item (see next section).

When you create a new CP, the majority of the configuration-items will default to "Profile Level".
Please take the time to go through the configuration-items, and configure the Level Value appropriately for your use-case.

- **Profile-Level** configuration items **cannot** be edited in the exported spreadsheet.
- **Device-Level** configuration items **can** be edited in the exported spreadsheet.

Under the "**Manage Devices**" tab, you will see all available devices listed.
A device is available for this CP if:

- It is the correct Device Type
- It is not in another CP
- It has been claimed by a member of the User Account that you belong to

Online/Offline status does not affect a Devices' availability.

9.5.2.3 *Buttons Available*

Export	Export the CP to a Spreadsheet. This button only works if there is at least one Device in the CP. Device Settings in an exported CP may be edited out-of-band.
Import & Apply	Import a spreadsheet that has been edited out-of-band. Transition into Validation Mode If the data is not valid

Identify the ERRORS and write them to a spreadsheet
Transition back into Editor Mode
If the data is valid, you will get the option to ACCEPT or CANCEL
ACCEPT:
Save all changes into the Editor Mode of the CP
Transition back into Editor Mode
CANCEL:
Do not import any data
Transition back into Editor Mode

Save

Save all changes you have made to the CP.
This has the effect of SAVING your changes to the CP in Editor Mode.
This DOES NOT deploy any changes to the remote Devices.
Transition into Review Mode

Discard Changes

Abort Editor Mode.
Return the CP to that state that existed prior to entering Editor Mode.
All changes, EVEN THE SAVED CHANGES, will be aborted.
Transition into View Mode

9.5.3 Validation Mode

9.5.3.1 Functions available

There are no user-functions available in this mode.

9.5.3.2 NOTEs

The internal state-machine will transition into **Validation** Mode to ensure that all settings are valid including those:

- Exported to the spreadsheet
- Imported from the spreadsheet
- Deployed to devices

9.5.3.3 Buttons Available

There are no buttons available in this mode.

9.5.4 Review Mode

9.5.4.1 Functions available

Commit
Discard Changes
View Meta Data

Configuration Profile Name
Firmware version
Device Type
Total Devices
Online/Offline Devices

View Device Settings

("Manage Profile Settings")

View Profile Apps and App Settings

("Manage Apps")

View Device List ("Manage Devices")

9.5.4.2 NOTEs

After configurations are made and the Save button is clicked, the CP will be in **Review** Mode.
In Review Mode, it is not possible to make any changes.

The purpose is to provide a last reviewable state where no changes can be made.
Any changes will be highlighted in RED.
No commands will be queued until the Commit button is clicked.

9.5.4.3 Buttons Available

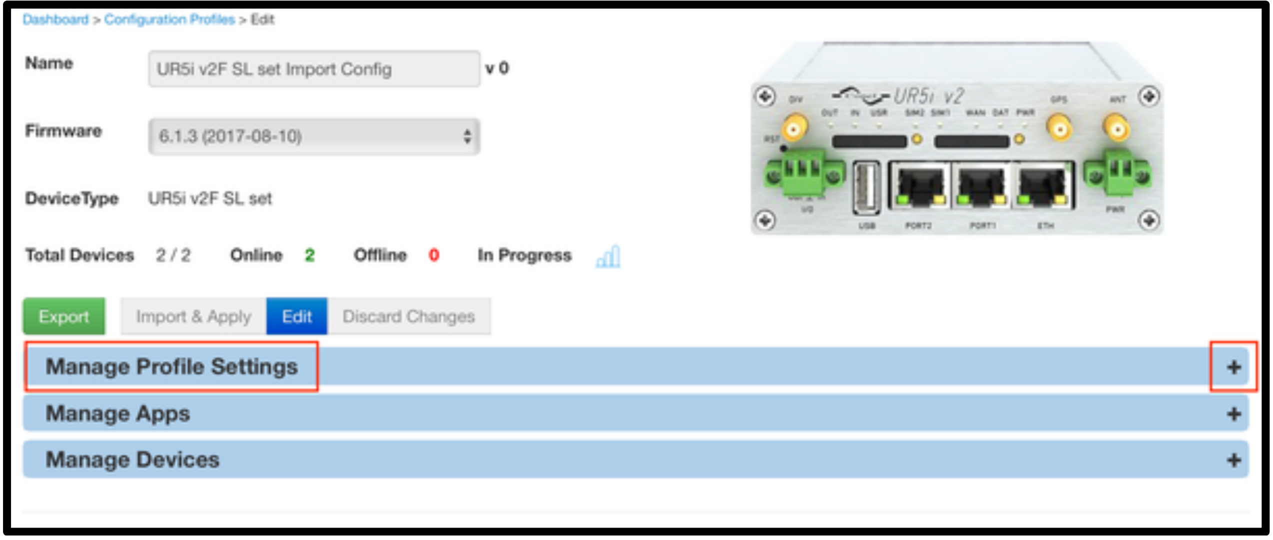
Commit
The Commit button is only available after you Save changes to the CP in Editor Mode.
DEPLOY all changes to all devices in the CP
Transition into View Mode

Discard Changes
Abort Editor Mode.
Return the CP to that state that existed prior to entering Editor Mode.
All changes, EVEN THE SAVED CHANGES, will be aborted.
Transition into View Mode

9.6 Configuring the Configuration Profile (in Editor Mode)

9.6.1 Set Levels (Profile or Device)

Select the Configuration Profiles view; select "Manage Profile Settings".



Dashboard > Configuration Profiles > Edit

Name: UR5i v2F SL set Import Config v 0

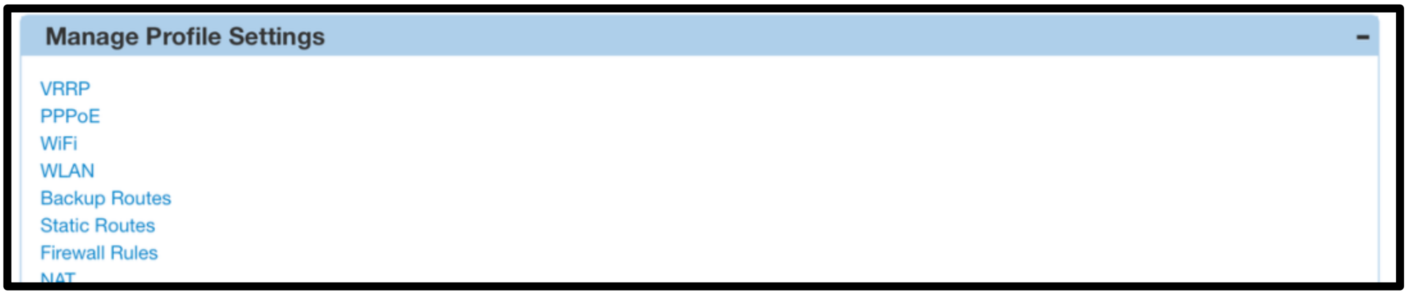
Firmware: 6.1.3 (2017-08-10)

DeviceType: UR5i v2F SL set

Total Devices 2 / 2 Online 2 Offline 0 In Progress

Figure 24 Expand Profile Settings

Then select the "Configuration Item" group that you wish to configure.



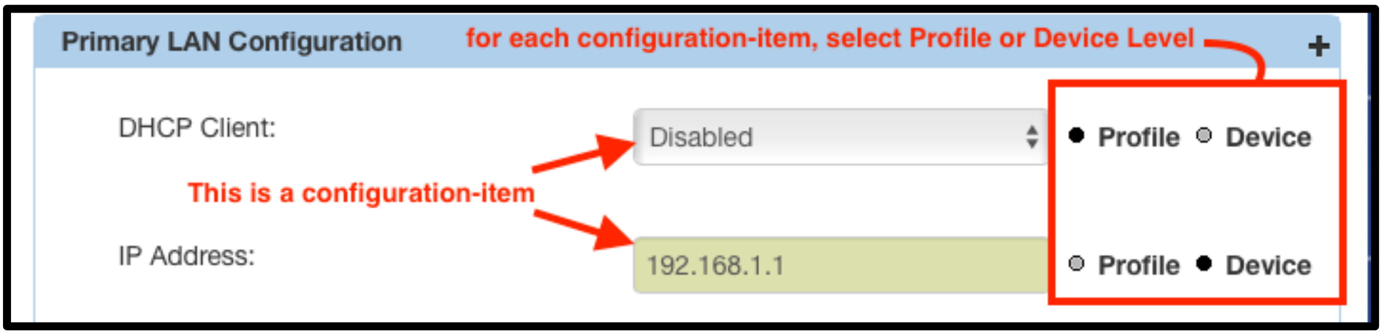
Manage Profile Settings

VRRP
PPPoE
WiFi
WLAN
Backup Routes
Static Routes
Firewall Rules
NAT

Figure 25 Configuration Item Groups

Every configuration-item (aka "setting") may be a Profile Level setting, or a Device Level setting.

NOTE*: It is very important that you decide, and configure, the Level Value for each configuration-item.*



Primary LAN Configuration

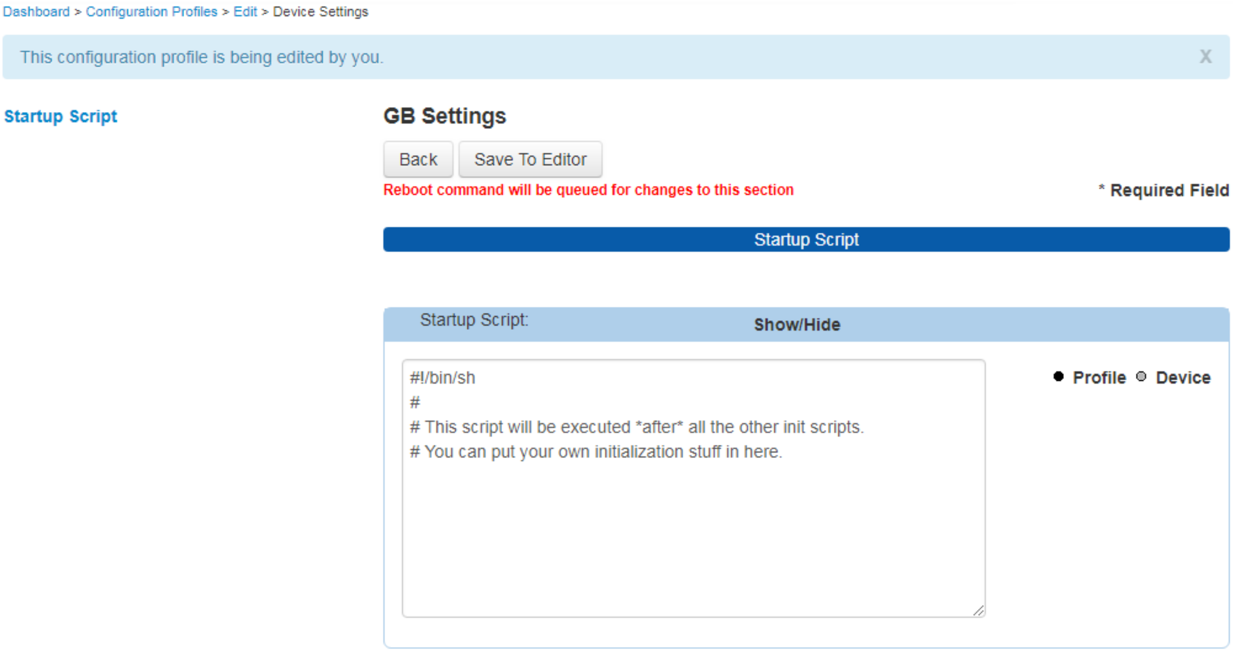
for each configuration-item, select Profile or Device Level

DHCP Client: Disabled ● Profile ○ Device

This is a configuration-item

IP Address: 192.168.1.1 ○ Profile ● Device

Figure 26 Device v Configuration Level Setting



Dashboard > Configuration Profiles > Edit > Device Settings

This configuration profile is being edited by you.

Startup Script

GB Settings

Back | Save To Editor

Reboot command will be queued for changes to this section

* Required Field

Startup Script

Startup Script: Show/Hide

```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here.
```

● Profile ○ Device

Some settings require the device to be rebooted in order for the changes to take effect. A message indicating a Reboot command will be applied is displayed for these setting.

Reboot will automatically be queued when changes are made to the following configuration settings

- NTP
- Startup Script
- Up Script
- Down Script

***NOTE**: A single Reboot command will be applied to a profile when the changes committed require a reboot. This command will be applied after all changes have been completed.*

9.6.2 Option 1: Profile Level

If you want to apply the exact same value to a setting in ALL of the devices in your CP, then that setting should be configured as a Profile Level setting.

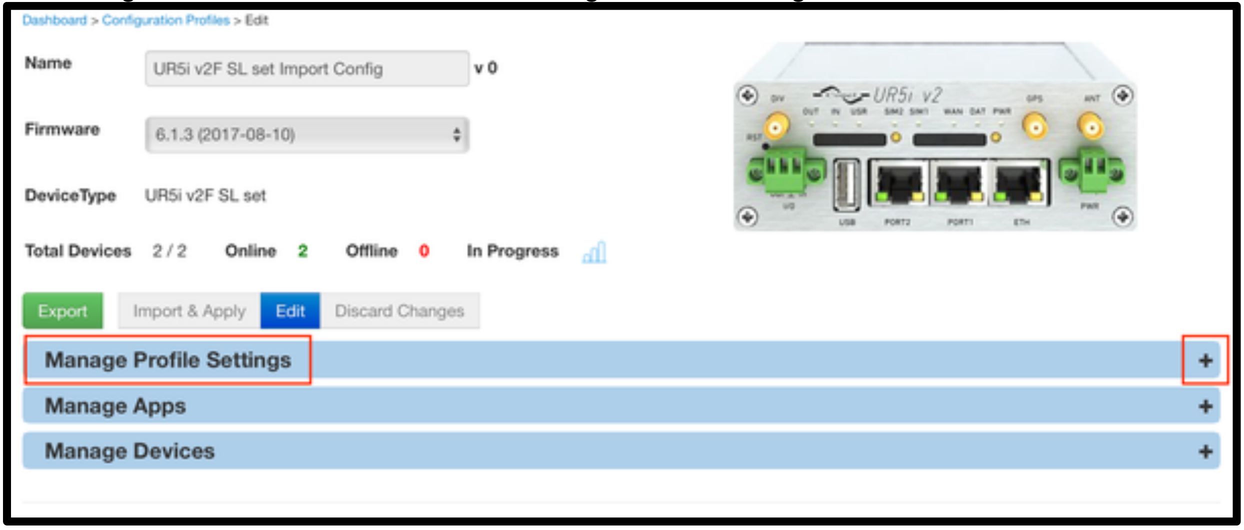
Profile-Level configuration items cannot be edited in the exported spreadsheet.

9.6.3 Option 2: Device Level

If you want to apply a unique value to a setting in SOME or ALL of the devices in your CP, then that setting should be configured as a Device Level setting.
Device-Level configuration items can be edited in the exported spreadsheet.

9.6.4 Configure Profile-Level settings

Select the Configuration Profiles view; select "Manage Profile Settings".



Dashboard > Configuration Profiles > Edit

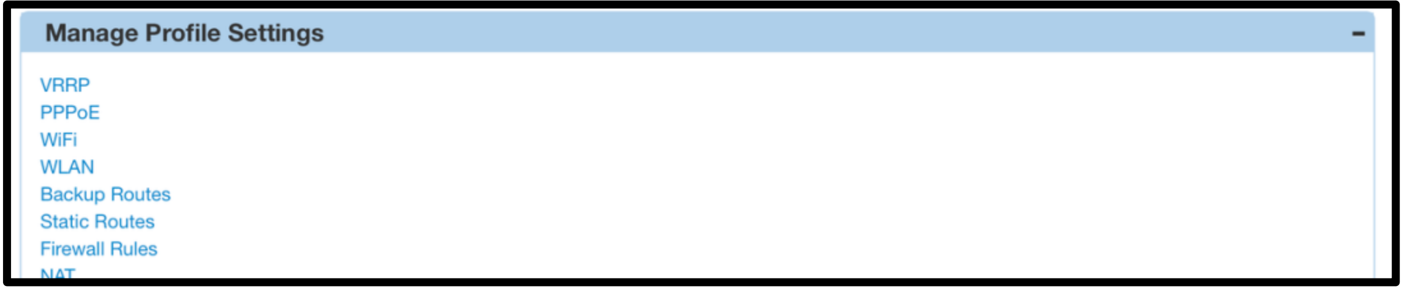
Name: UR5i v2F SL set Import Config v 0

Firmware: 6.1.3 (2017-08-10)

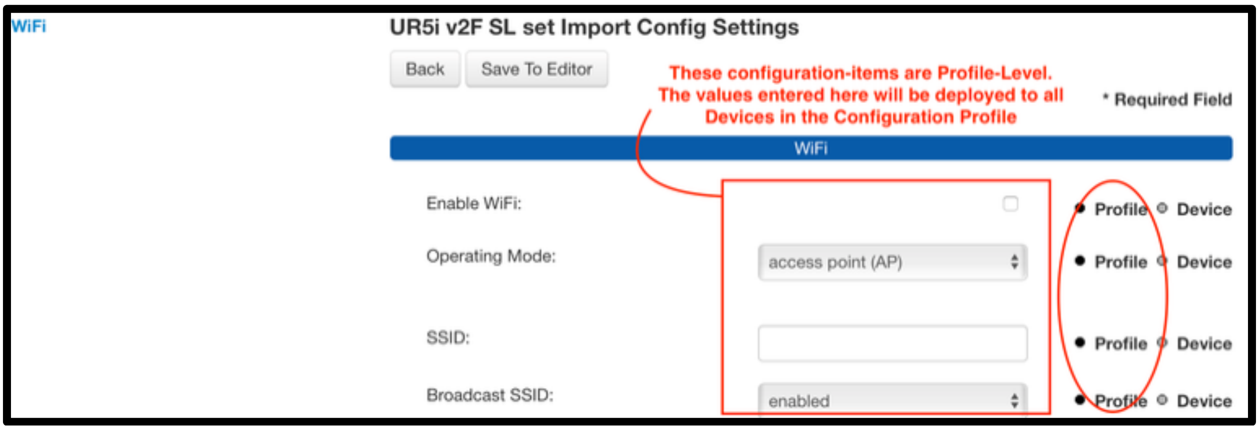
DeviceType: UR5i v2F SL set

Total Devices 2 / 2 Online 2 Offline 0 In Progress

Then select the "Configuration Item" group that you wish to configure.



NOTE*: For every configuration-item that you have configured as Profile Level, it is very important that you enter the desired value for that setting.The values entered into Profile-Level configuration-items will be sent to every device in the CP.*



WiFi

UR5i v2F SL set Import Config Settings

These configuration-items are Profile-Level. The values entered here will be deployed to all Devices in the Configuration Profile

* Required Field

Enable WiFi: □ ● Profile ○ Device

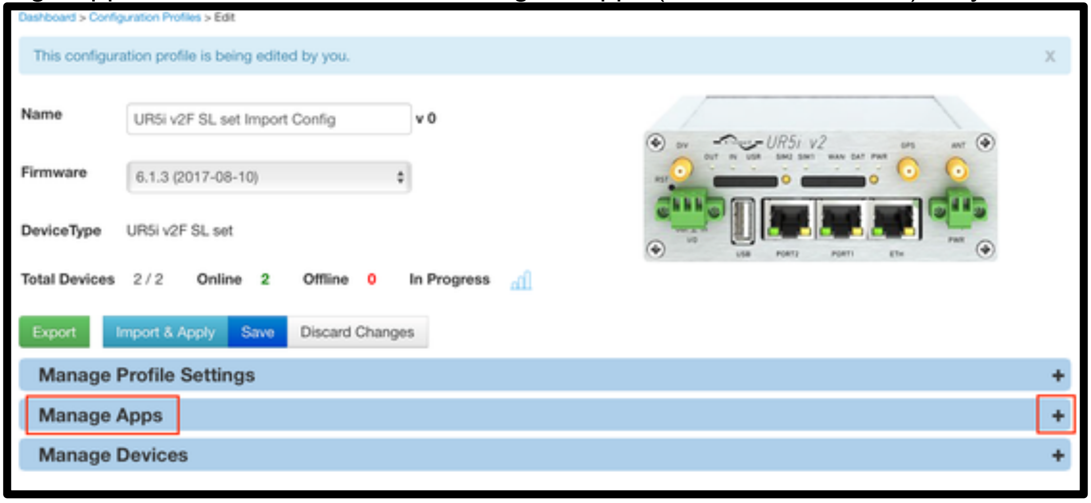
Operating Mode: access point (AP) ● Profile ○ Device

SSID: ● Profile ○ Device

Broadcast SSID: enabled ● Profile ○ Device

9.6.5 Add Apps

Use the "Manage Apps" area add, remove and configure Apps (aka. User Modules) for your Devices.



Dashboard > Configuration Profiles > Edit

This configuration profile is being edited by you.

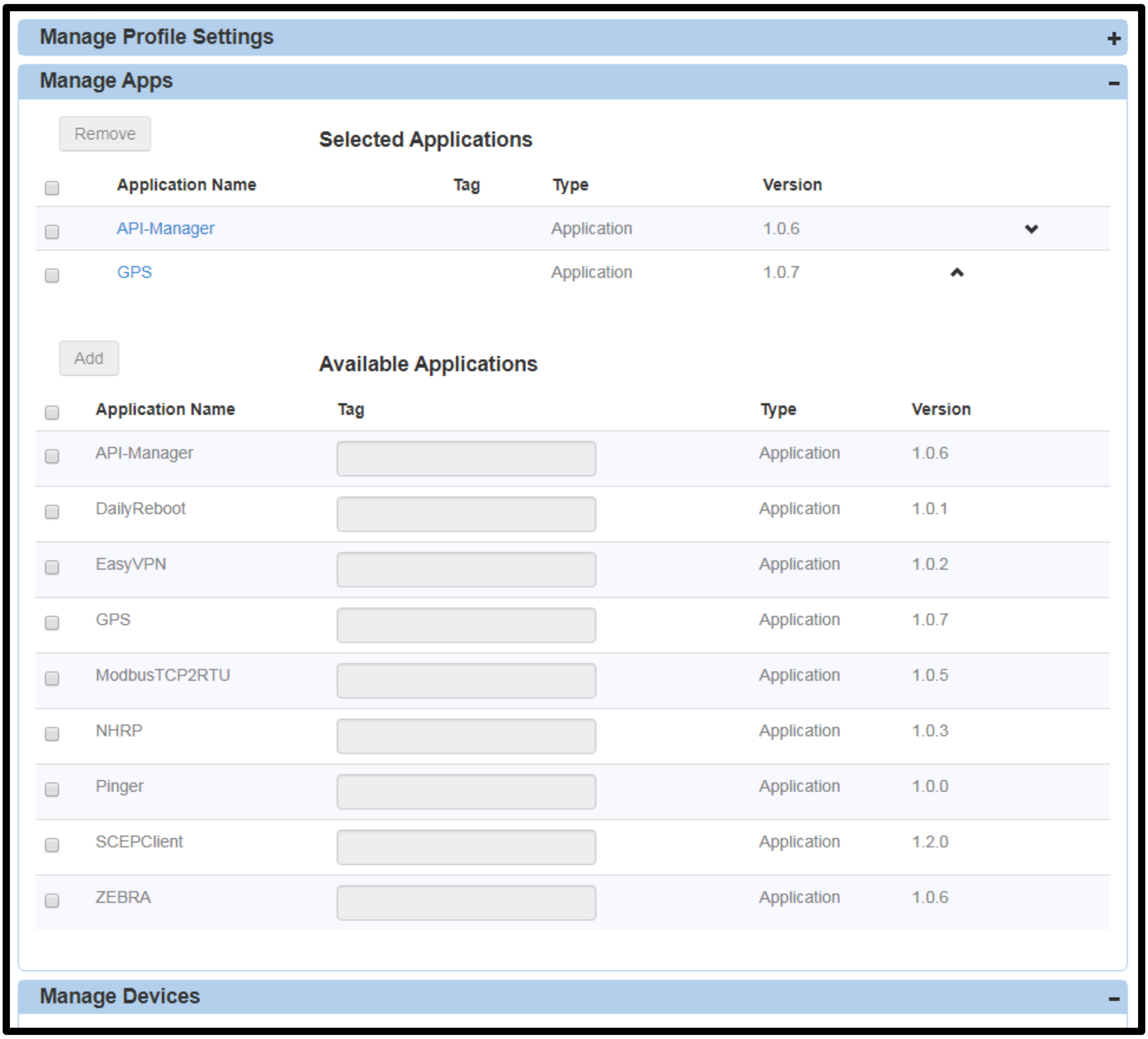
Name: UR5i v2F SL set Import Config v 0

Firmware: 6.1.3 (2017-08-10)

DeviceType: UR5i v2F SL set

Total Devices 2 / 2 Online 2 Offline 0 In Progress

Figure 27 Manage App Panel Expander



Manage Profile Settings +

Manage Apps –

Remove

Selected Applications

□	Application Name	Tag	Type	Version	
□	API-Manager		Application	1.0.6	⌄
□	GPS		Application	1.0.7	⌃

Add

Available Applications

□	Application Name	Tag	Type	Version
□	API-Manager		Application	1.0.6
□	DailyReboot		Application	1.0.1
□	EasyVPN		Application	1.0.2
□	GPS		Application	1.0.7
□	ModbusTCP2RTU		Application	1.0.5
□	NHRP		Application	1.0.3
□	Pinger		Application	1.0.0
□	SCEPClient		Application	1.2.0
□	ZEBRA		Application	1.0.6

Manage Devices –

Figure 28 List Applications

Within the "Manage Apps" tab, there are 2 sections:

9.6.5.1 Section 1: Selected Applications

This shows a list of the Applications / User Modules that have are currently included in this CP.

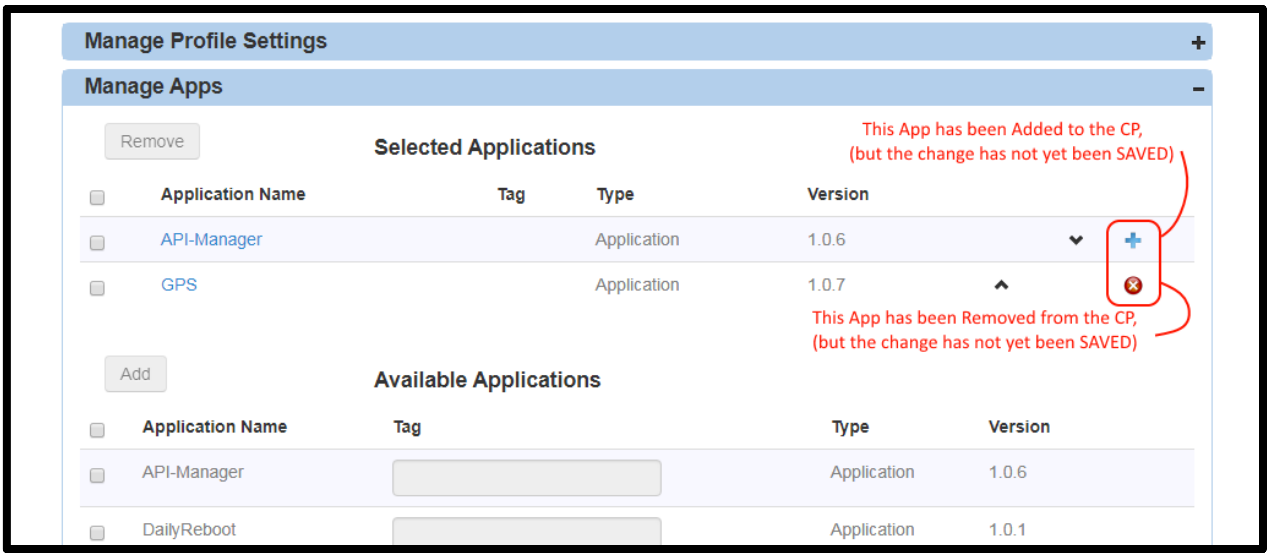
Column	Meaning
Selection (checkbox)	At the top level, if you check this checkbox it will select ALL applications in the list.
Application Name	This is the name of the Application / user-module. In order to modify configuration-item settings that are specific to an Application, click on the Application name.
Tag	A unique meta data tag for your Application.
Type	This is the Type of Application.
Version	This is the Version of the application.

Position arrows	These arrows allow you to position the Application in the list, for easier navigation.
Button	**Function**
Remove	Remove the selected Applications / User Modules from this CP. When you Remove an Application, it will not disappear from the "Removed Applications" list immediately. Instead, an X symbol will appear, which indicates that this Application has been Removed from the CP, but this change has not yet been SAVED.

9.6.5.2 Section 2: Available Applications

This shows a list of the Applications / User Modules that are currently available to be included in this CP.

Column	Meaning
Selection (checkbox)	At the top level, if you check this checkbox it will select ALL applications in the list.
Application Name	This is the name of the Application / user-module. In order to modify configuration-item settings that are specific to an Application, click on the Application name.
Tag	A unique meta data tag for your Application.
Type	This is the Type of Application.
Version	This is the Version of the application.
Button	**Function**
Add	Add the selected Applications / User Modules into this CP. When you Add an Application, it will immediately appear in the "Selected Applications" list, with a + symbol that indicates that this Application has been Added to the CP, but this change has not yet been SAVED.



Manage Profile Settings +

Manage Apps –

Remove

Selected Applications

This App has been Added to the CP, (but the change has not yet been SAVED)

☐	Application Name	Tag	Type	Version		
☐	API-Manager		Application	1.0.6	⌄	+
☐	GPS		Application	1.0.7	^	⊗

This App has been Removed from the CP, (but the change has not yet been SAVED)

Add

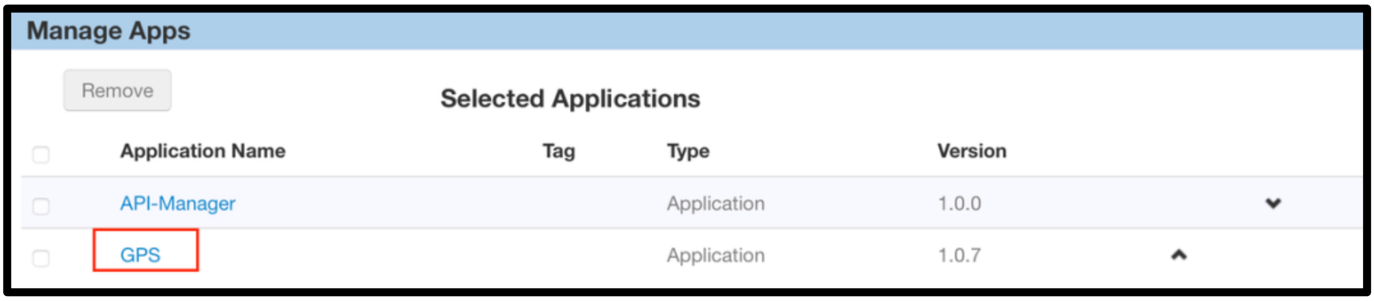
Available Applications

☐	Application Name	Tag	Type	Version
☐	API-Manager		Application	1.0.6
☐	DailyReboot		Application	1.0.1

Figure 29 Application Added / Removed

9.6.5.3 Set App Levels

Apps have the same options as standard Device Configuration Items.
You must decide which configuration-items for each App should be Profile level, and which should be Device level.
Some Apps have lots of Configuration Items: Some Apps have few or none.
To configure an App, click on the name of the App.



Manage Apps

Remove

Selected Applications

□	Application Name	Tag	Type	Version
□	API-Manager		Application	1.0.0
□	GPS		Application	1.0.7

Figure 30 Managed Apps

9.6.5.4 Profile Level

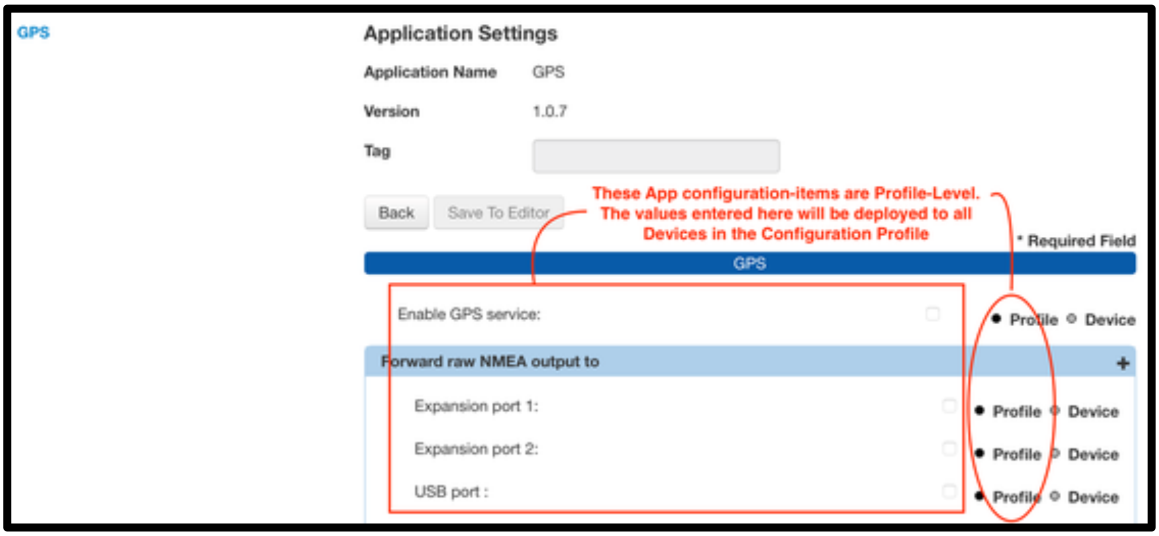
If you want to apply the exact same value to an App setting in ALL of the devices in your CP, then that setting should be configured as a Profile Level setting.
Profile-Level configuration items **cannot** be edited in the exported spreadsheet.

9.6.5.5 Device Level

If you want to apply a unique value to an App setting in SOME or ALL of the devices in your CP, then that setting should be configured as a Device Level setting.
Device-Level configuration items can be edited in the exported spreadsheet.

9.6.5.6 Configure Profile Level App settings

Select the name of the App, and then set the Profile Level configuration-items.



GPS

Application Settings

Application Name GPS

Version 1.0.7

Tag

Back | Save To Editor

These App configuration-items are Profile-Level. The values entered here will be deployed to all Devices in the Configuration Profile

* Required Field

GPS

Enable GPS service: □ ● Profile ○ Device

Forward raw NMEA output to +

Expansion port 1: □ ● Profile ○ Device

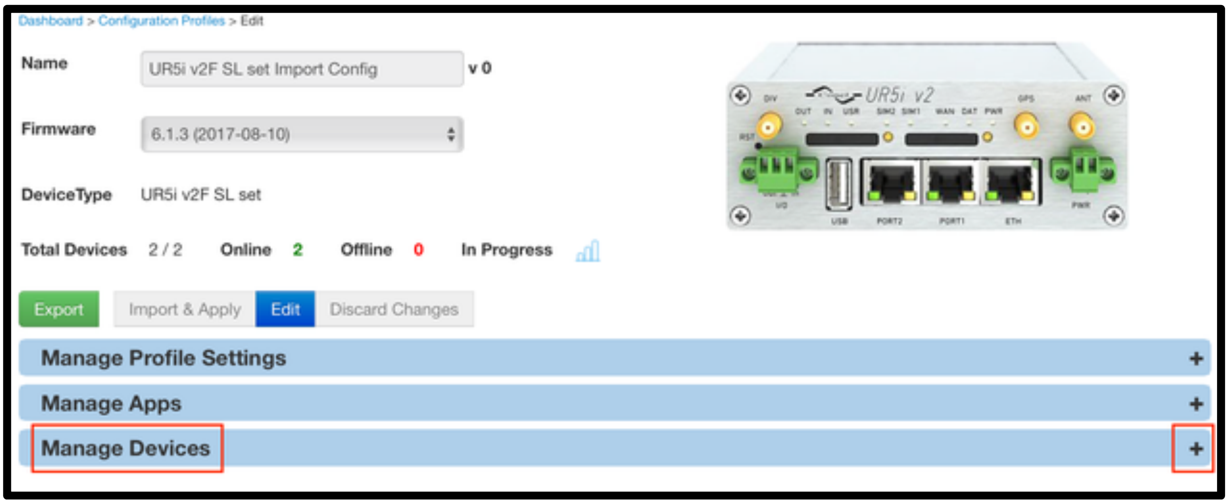
Expansion port 2: □ ● Profile ○ Device

USB port : □ ● Profile ○ Device

Figure 31 GPS Setting Screen

9.6.6 Add Devices

A Configuration Profile must have Devices added to it: you will not be able to export or deploy a Configuration Profile without at least one Device.



Dashboard > Configuration Profiles > Edit

Name: UR5i v2F SL set Import Config v 0

Firmware: 6.1.3 (2017-08-10)

DeviceType: UR5i v2F SL set

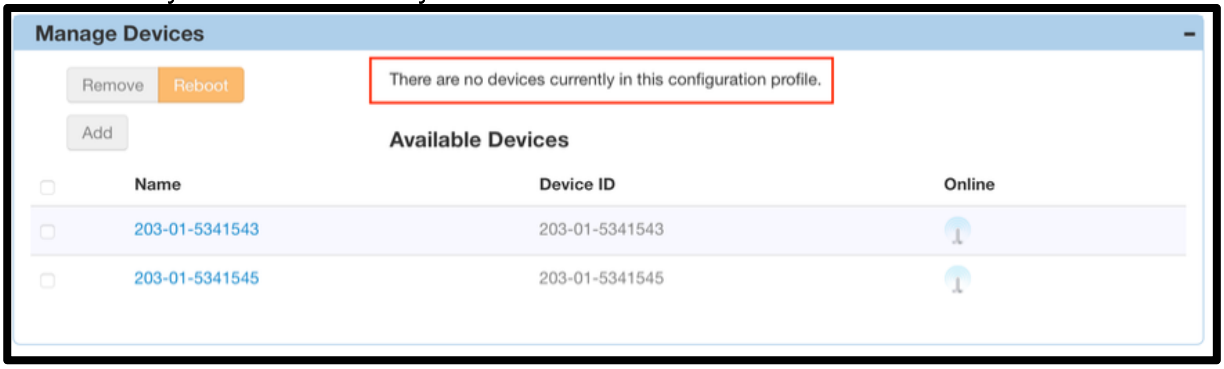
Total Devices 2 / 2 Online 2 Offline 0 In Progress

Figure 32 Contracted Configuration Profile Screen

From the overview view, we can see that there are 2 devices of this type, and they are both available to this profile.
Both of these devices are currently Online.
When you enter for the first time, you will see the list of Available Devices.

A Device is Available if:

- It has been Claimed into your Account
- It is the same Device Type as the CP
- It is not in any other CP on the system



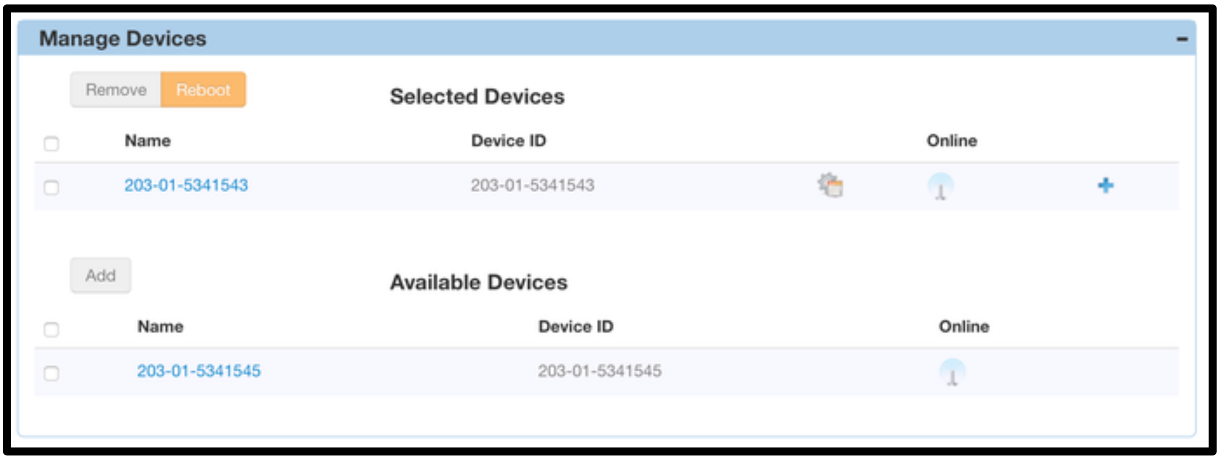
There are no devices currently in this configuration profile.

Available Devices

□	Name	Device ID	Online
□	203-01-5341543	203-01-5341543	
□	203-01-5341545	203-01-5341545	

Figure 33 No Device Present Notification

You can use the selection checkbox, in the left-hand-column, to select a Device, and then use the Add button to add it into your CP.



Manage Devices

Selected Devices

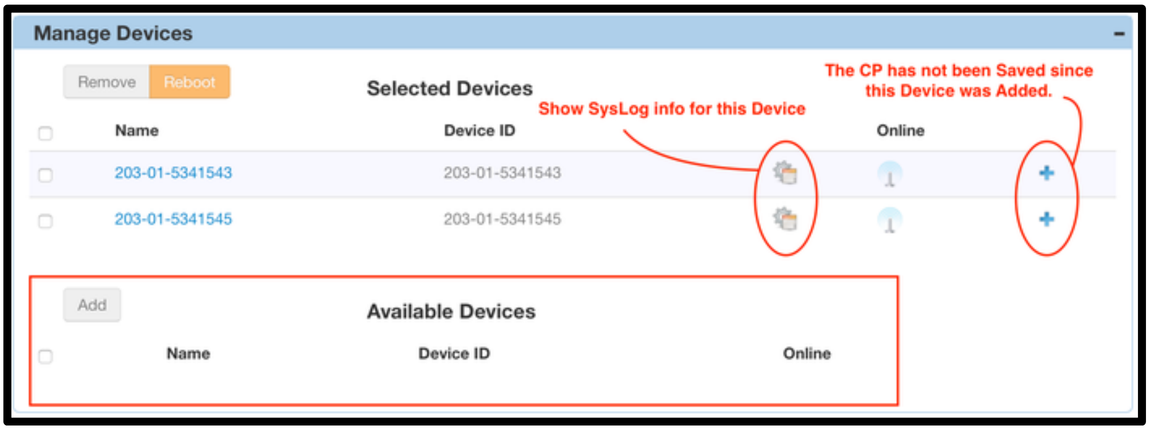
□	Name	Device ID	Online
□	203-01-5341543	203-01-5341543	+

Available Devices

□	Name	Device ID	Online
□	203-01-5341545	203-01-5341545	

Figure 34 Add Device To Configuration Profile View

There will now be a new list: Selected Devices.
A Device can only appear on one list: If has been Added to the CP, it will appear in the Selected Devices list.
If it has not been added to the CP, but it satisfies the "availability" criteria, it will appear in the Available Devices list.
When there are no more Available Devices, the Available Devices list will be empty.



Manage Devices

Remove
Reboot
Add
The CP has not been Saved since this Device was Added.
Show SysLog info for this Device

Selected Devices

□	Name	Device ID	Online
□	203-01-5341543	203-01-5341543	+
□	203-01-5341545	203-01-5341545	+

Available Devices

□	Name	Device ID	Online

9.6.6.1 *Configure Device-Level settings in the exported excel file*

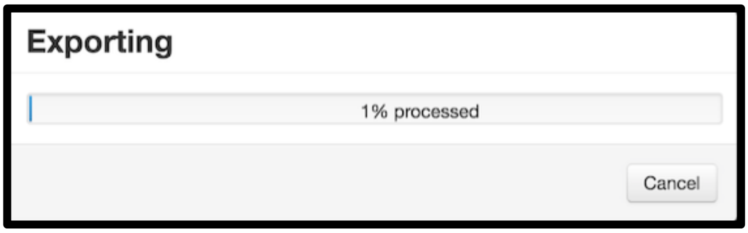
If you want to apply the exact same value to a setting in ALL of the devices in your CP, and all of your settings are configured as a Profile Level setting, then you do not need to take this step.
If you want to apply a unique value to a setting in SOME or ALL of the devices in your CP, and those settings have been configured as a Device Level setting, then you are ready to proceed with this step.
Export the Configuration Profile to a Microsoft Excel workbook
Hit the Export button to export the CP into an editable Spreadsheet

***NOTE**: only Microsoft Excel is currently supported.*

This export process can take some time, depending on:

- how many Devices you have in your CP
- how many Profile Level configuration-items there are
- how many Device Level configuration-items there are

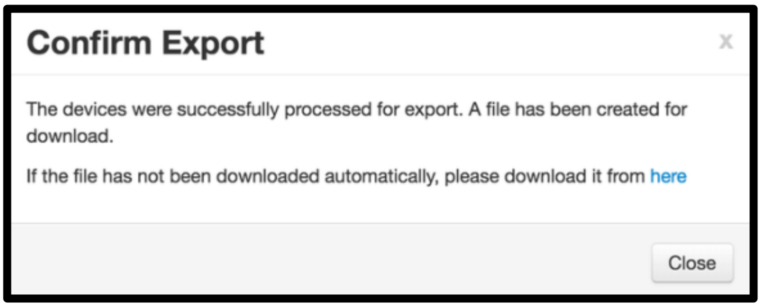
As a rule-of-thumb: more Profile level, and less Device-Level, configuration-items will result in a faster export; fewer Devices will result in a faster export.



Exporting

1% processed

When the export has completed, the Excel File will be available in the Downloads folder of your browser.



Confirm Export

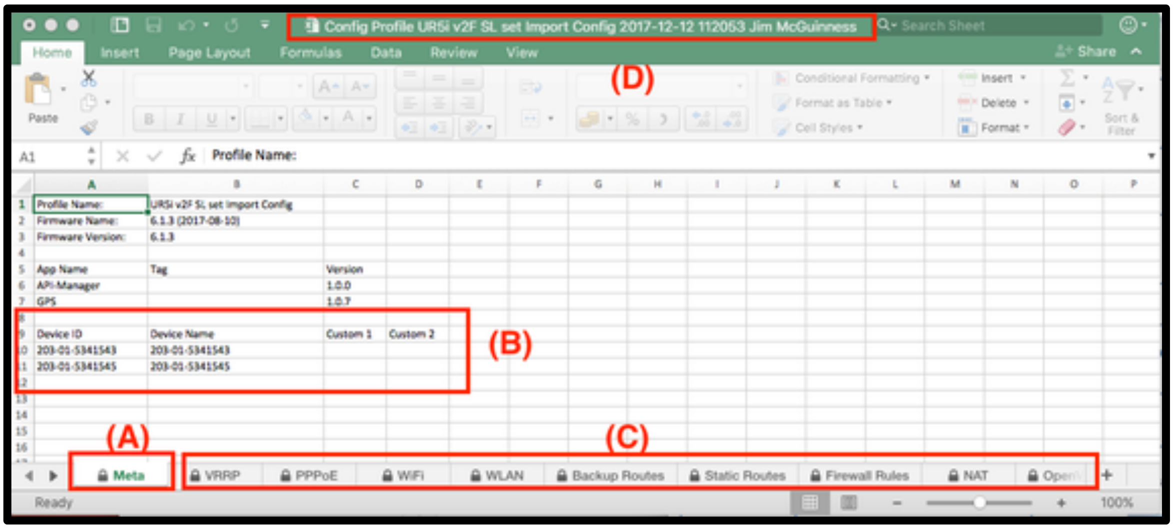
The devices were successfully processed for export. A file has been created for download.

If the file has not been downloaded automatically, please download it from here

9.6.6.2 *Working with the Excel Workbook*

The exported Excel workbook will take a standard format.

Warning: *It is very important that you do NOT edit the TAB names (A), (C), or change the order of the Columns*



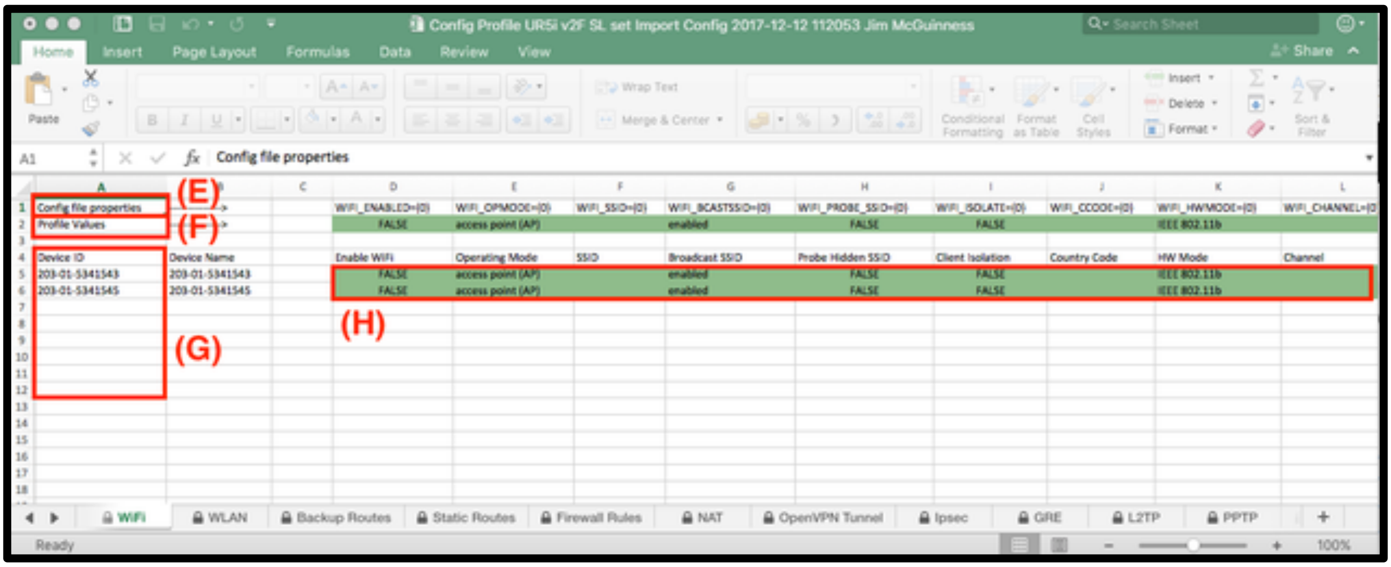
Config Profile URSi v2F SL set Import Config 2017-12-12 112053 Jim McGuinness

A1 Profile Name:

	A	B	C	D
1	Profile Name:	URSi v2F SL set Import Config		
2	Firmware Name:	6.1.3 (2017-08-10)		
3	Firmware Version:	6.1.3		
4				
5	App Name	Tag	Version	
6	API-Manager		1.0.0	
7	GPS		1.0.7	
8				
9	Device ID	Device Name	Custom 1	Custom 2
10	203-01-5341543	203-01-5341543		
11	203-01-5341545	203-01-5341545		

Notation	Description
(A)	This is the Meta Tab. The Meta Tab contains the Meta-Data for the Configuration Profile. The data in this Tab does not get sent to the Devices as configuration settings: The data that's in this tab is stored on WebAccess/DMP.
(B)	The list of Devices, by Device ID and Name, will be shown in column A. There are 2 Custom fields for each Device. You can edit the Custom fields for each device, using this spreadsheet. Remember that the data on this tab is not sent to the Devices: it will be stored on WebAccess/DMP.

(C)	For each Configuration Group that's available on WebAccess/DMP, under "Manage Profile Settings", there will be a Tab in the Workbook. All of the Tabs represent groups of configuration-items. The values in these Tabs will be the settings that will be deployed to, and stored as settings on, each Device.
(D)	The name of the Workbook is made from : "Config Profile" + Name of the Config Profile + Date and Time of creation + User Name

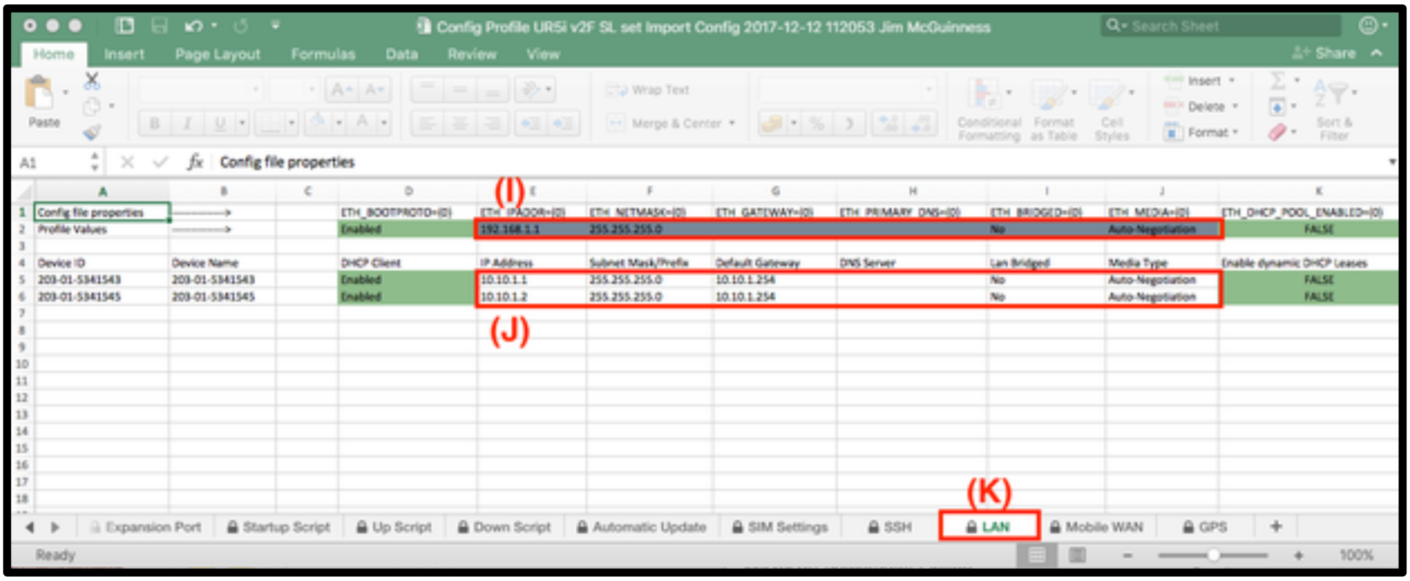


Config Profile UR5i v2F SL set Import Config 2017-12-12 112053 Jim McGuinness

A1 Config file properties

	A	B	C	D	E	F	G	H	I	J	K	L
1	Config file properties			WIFI_ENABLED=(0)	WIFI_OPMODE=(0)	WIFI_SSID=(0)	WIFI_BCASTSSID=(0)	WIFI_PROBE_SSID=(0)	WIFI_ISOLATE=(0)	WIFI_CCODE=(0)	WIFI_HWMODE=(0)	WIFI_CHANNEL=(0
2	Profile Values			FALSE	access point (AP)		enabled	FALSE	FALSE		IEEE 802.11b	
3												
4	Device ID	Device Name		Enable WiFi	Operating Mode	SSID	Broadcast SSID	Probe Hidden SSID	Client Isolation	Country Code	HW Mode	Channel
5	203-01-5341543	203-01-5341543		FALSE	access point (AP)		enabled	FALSE	FALSE		IEEE 802.11b	
6	203-01-5341545	203-01-5341545		FALSE	access point (AP)		enabled	FALSE	FALSE		IEEE 802.11b	

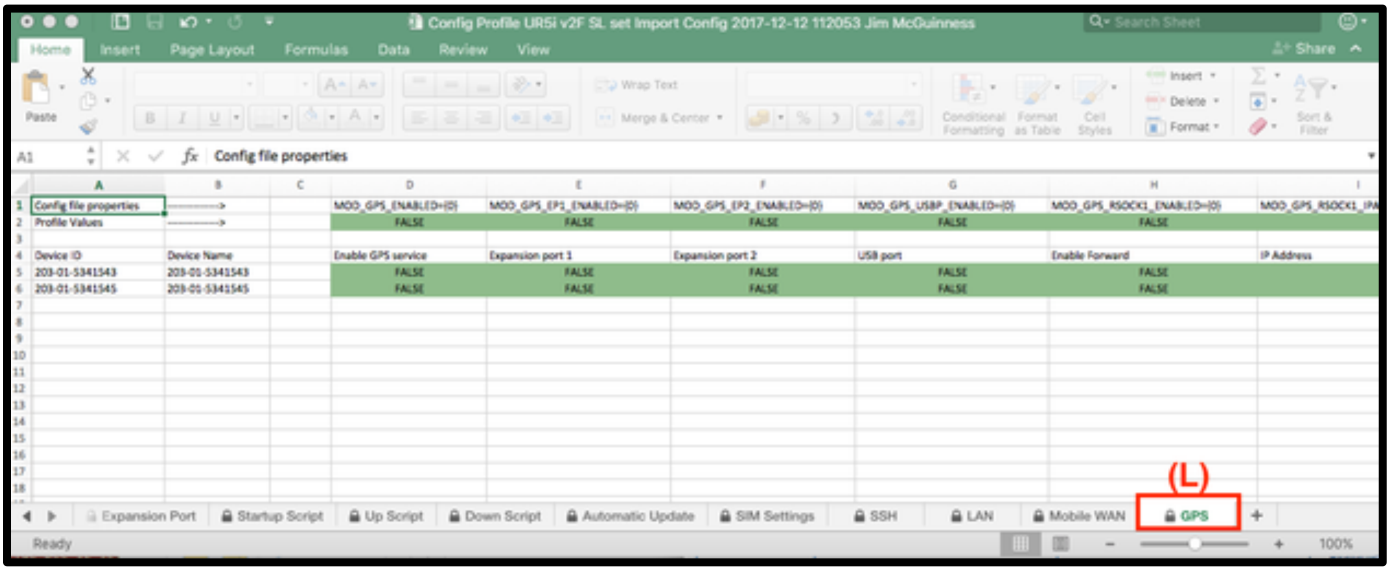
Notation	Description
(E)	Row 1 represents the actual configuration-item setting that's written into the router's configuration file (.cfg file). DO NOT EDIT OR REMOVE THIS ROW.
(F)	Row 2 represents the default-value for every configuration-item setting in the Configuration Profile. If the cell is GREEN (like the cells in this example), this configuration-item is a Profile Level setting. DO NOT EDIT OR REMOVE THIS ROW.
(G)	Column A will always contain the list of Devices that are Selected in the Configuration Profile. Column B will always contain the names of those Devices. DO NOT EDIT OR REMOVE THESE COLUMNS. DO NOT ADD DEVICE IDS TO THE END OF THE COLUMN. DO NOT EDIT OR REMOVE THESE COLUMNS.
(H)	For every configuration-item, for every Device, the actual value that will be deployed to it is shown in these cells. IF the cell is GREEN (like the cells in this example), then you CAN NOT EDIT IT. This is what a Profile-Level setting looks like in the spreadsheet.



Config file properties

	A	B	C	D	E	F	G	H	I	J	K
1	Config file properties	----------->		ETH_BOOTPROTO=(0)	ETH_IPADDR=(0)	ETH_NETMASK=(0)	ETH_GATEWAY=(0)	ETH_PRIMARY_DNS=(0)	ETH_BRIDGED=(0)	ETH_MEDIA=(0)	ETH_DHCP_POOL_ENABLED=(0)
2	Profile Values	----------->		Enabled	192.168.1.1	255.255.255.0			No	Auto-Negotiation	FALSE
3											
4	Device ID	Device Name		DHCP Client	IP Address	Subnet Mask/Prefix	Default Gateway	DNS Server	Lan Bridged	Media Type	Enable dynamic DHCP Leases
5	203-01-5341543	203-01-5341543		Enabled	10.10.1.1	255.255.255.0	10.10.1.254		No	Auto-Negotiation	FALSE
6	203-01-5341545	203-01-5341545		Enabled	10.10.1.2	255.255.255.0	10.10.1.254		No	Auto-Negotiation	FALSE

Notation	Description
(I)	Row 2 represents the default-value for every configuration-item setting in the Configuration Profile. If the cell is BLUE (like the cells in this example), this configuration-item is a Device Level setting. DO NOT EDIT OR REMOVE THIS ROW.
(J)	For every configuration-item, for every Device, the actual value that will be deployed to it is shown in these cells. IF the cell is CLEAR (like the cells in this example), then you CAN EDIT IT because it is a Device Level cell. You can see in this example that we have put different values, for 2 devices, into cells E5 and E6. This is what a Device-Level setting looks like in the spreadsheet. Note that, if you do not enter a value into the cell, and there's a Default Value shown in row 1, then the Default Value will be written into this setting for every Device.
(K)	These examples are shown for the LAN configuration group.



Config file properties

	A	B	C	D	E	F	G	H	I
1	Config file properties	----------->		MOD_GPS_ENABLED=(0)	MOD_GPS_EP1_ENABLED=(0)	MOD_GPS_EP2_ENABLED=(0)	MOD_GPS_USBP_ENABLED=(0)	MOD_GPS_RSOCK1_ENABLED=(0)	MOD_GPS_RSOCK1_IPA
2	Profile Values	----------->		FALSE	FALSE	FALSE	FALSE	FALSE	
3									
4	Device ID	Device Name		Enable GPS service	Expansion port 1	Expansion port 2	USB port	Enable Forward	IP Address
5	203-01-5341543	203-01-5341543		FALSE	FALSE	FALSE	FALSE	FALSE	
6	203-01-5341545	203-01-5341545		FALSE	FALSE	FALSE	FALSE	FALSE	

Notation	Description
(L)	If you have added Apps (User Modules), and those Apps have configuration-items associated with them, then each App will appear as a Tab on the Excel workbook. In this example, the GPS App is shown as a Tab. The configuration items for the GPS App are shown in the worksheet. Apps follow the same rules as the rest of the Configuration Groups in the workbook.

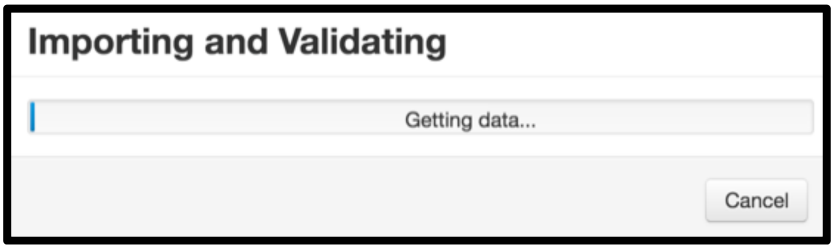
9.6.6.3 Activate your Configuration Profile and Deploy to Devices

After you have modified the Device Level settings in the spreadsheet, it's time to import it back into WebAccess/DMP.

Click on the "Import and Apply" button.
Select the excel file from the file-system.
The system will begin to import the file: During the import, it will validate the data in each cell.
This import process can take some time, depending on:

- how many Devices you have in your CP
- how many Profile Level configuration-items there are
- how many Device Level configuration-items there are

As a rule-of-thumb: more Profile level, and less Device-Level, configuration-items will result in a faster import; fewer Devices will result in a faster import.

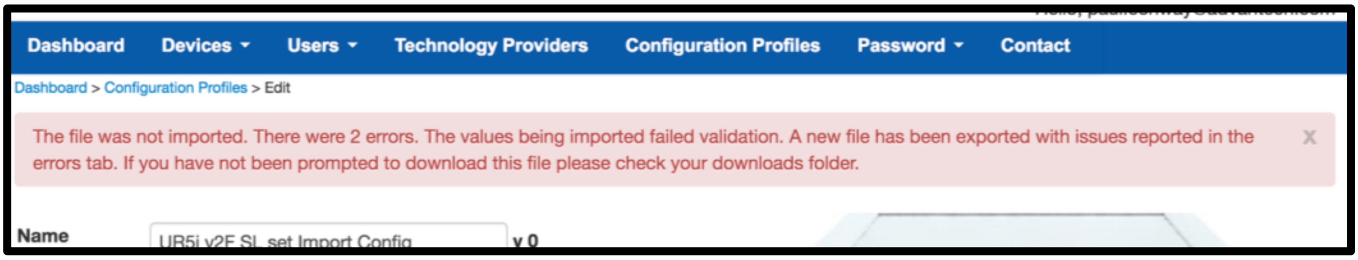


Importing and Validating

Getting data...

9.6.7 If the Import Validation Fails

2 things will happen if Validation Fails.
First: WebAccess/DMP will publish a warning, on-screen, that tells you that the import-validation failed.

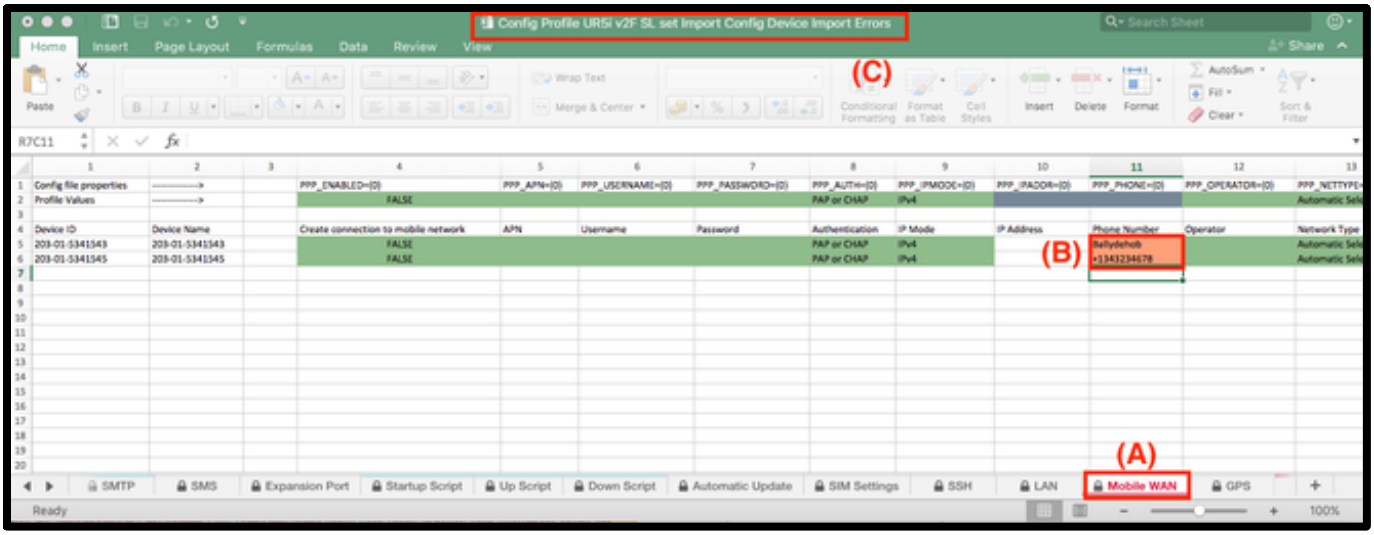


The file was not imported. There were 2 errors. The values being imported failed validation. A new file has been exported with issues reported in the errors tab. If you have not been prompted to download this file please check your downloads folder.

Figure 35 Import Failed Notification

Second: WebAccess/DMP will create another excel file, and it will export it to the Downloads area of your Browser.
This excel file will contain the details of the Validation Errors.

Open the "errors" excel file.



	1	2	3	4	5	6	7	8	9	10	11	12	13
1	Config file properties	------------>		PPP_ENABLED=(0)	PPP_APN=(0)	PPP_USERNAME=(0)	PPP_PASSWORD=(0)	PPP_AUTH=(0)	PPP_IPMODE=(0)	PPP_IPADDR=(0)	PPP_PHONE=(0)	PPP_OPERATOR=(0)	PPP_NETTYPE=
2	Profile Values	------------>		FALSE				PAP or CHAP	IPv4				Automatic Sel
3													
4	Device ID	Device Name		Create connection to mobile network	APN	Username	Password	Authentication	IP Mode	IP Address	Phone Number	Operator	Network Type
5	203-01-5341543	203-01-5341543		FALSE				PAP or CHAP	IPv4		Ballydehob		Automatic Sel
6	203-01-5341545	203-01-5341545		FALSE				PAP or CHAP	IPv4		+1343234678		Automatic Sel

Figure 36 Spreadsheet Error Notification

Notation	Description
(A)	For every Tab that there's a Validation Error on, the Tab Name will be written in RED.
(B)	For every Cell that there's a Validation Error on, the Cell will be coloured in RED.
(C)	The excel filename will have the word "Errors" appended onto the end.

10 System (Emu Edition only)

***NOTE**: The Emu Edition is the on-premises installed instance of the software. The System options are not available on the cloud instance.*

The System Menu option will only be available to users with the “admin” role, and it provides additional features required by on-prem installations of WebAccess/DMP (i.e. the Emu Edition)

Using this menu-option, you may:

- Import Devices into you on-premises instance.
- Claim Devices into a Tenant account, during the initial import and creation of those devices
- Purchase or Renew your run-time licence

10.1 System-Devices

10.1.1 Adding Devices to your Platform

Devices may be Created into the platform via the System menu. This menu is only available to “admin” and “manufacturer” roles.

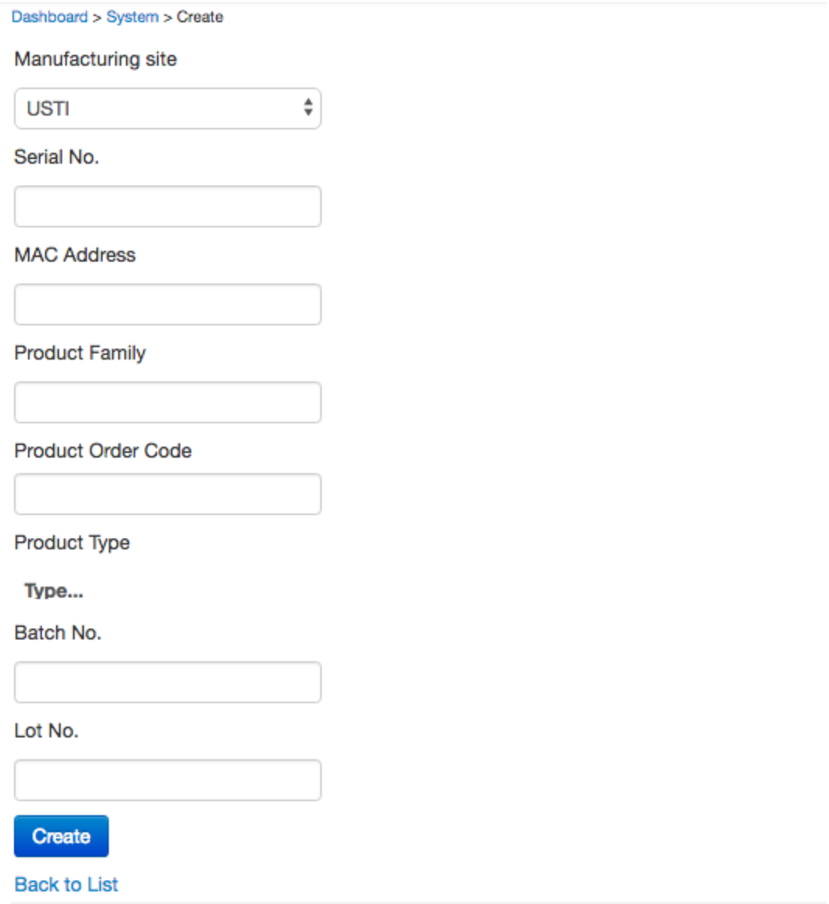
Devices may be created one-at-a-time, using the “Create New” button, or many-at-a-time using the “Import Devices” button.

To use the Import Devices option, a list of Devices must be entered into an ASCII formatted csv or text file.

10.1.2 Using the “Create Device” option

Using the Create Device method, you may:

- Create a single Device into the database (i.e. this device will become a Created Device in the database, which counts as one of your Licenced Devices)



Dashboard > System > Create

Manufacturing site

USTI

Serial No.

MAC Address

Product Family

Product Order Code

Product Type

Type...

Batch No.

Lot No.

Figure 37 Create Device Screen

10.1.3 Using the "Import Devices" option

Using the Import Devices method, you may:

- Import a list of devices (up to the number of Devices allowed by your licence)
- Create these Devices in the database (i.e. these devices become Created Devices, which are now Licenced Devices on your platform)
- Claim these devices to a specified Tenant

10.1.4 Import file format

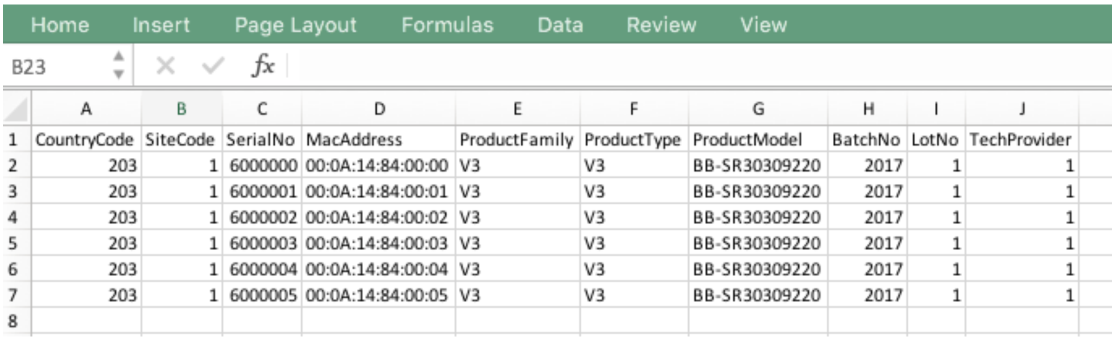
Users can import a batch of devices into the system and claim them using a csv file. The table below lists the columns in the file. There are a couple of important points to consider when using the file which should be understood.

The headers must be included in the file. These headers allow the import mechanism to map the correct column in the file to the correct column in the database table. In order to claim and the import the devices the file must contain the technology provide id. If the file doesn't contain this number then the devices will be imported but will remain unclaimed. The devices will then need to be reclaimed. Users should also restrain from adding spaces between the commas in the file as this interferes with the matching process in the system. Ideally the file should be created with application like notepad and save as ASCII with .csv extension.

Field	Example	Type	Rqrd?	Description
CountryCode	203	string(3)	Y	Always 203 or BB-203
SiteCode	01 or 1	string(2)	Y	Usually 01 or 1. Can be 2, 02, 3, 03.
SerialNo	6000000	string(20)	Y	SN as it appears on the label
MacAddress	00:0A:14:84:00:00	string(16)	Y	Full MAC Address with colons
ProductFamily	V3	string(100)	N	Useful for filtering
ProductType	SmartFlex	string(100)	N	Useful for filtering
ProductModel	BB-SR30300011	string(255)	Y	Order code as it appears on the label
BatchNo	6	integer	N	Useful for filtering
LotNo	2017	integer	N	Useful for filtering
TechProvider	1	integer	N	Use this field if you want to automatically **claim** devices into a specific Tenant account during the Device Import process. LEAVE THIS FIELD EMPTY IF YOU DO NOT WANT TO CLAIM THE DEVICES TO A TENANT.

NOTE:
The "TechProvider" ID may be obtained from WebAccess/DMP.

You will need to login to DMP as the "admin" user, then select the "Tenants" menu-option.
Select the Tenant that you wish to Claim devices for.
The required ID number is the number which appears at the end of the URL in the address bar e.g. 1
<SERVER_NAME>/TechnologyProvider/Edit/1



	A	B	C	D	E	F	G	H	I	J
1	CountryCode	SiteCode	SerialNo	MacAddress	ProductFamily	ProductType	ProductModel	BatchNo	LotNo	TechProvider
2	203	1	6000000	00:0A:14:84:00:00	V3	V3	BB-SR30309220	2017	1	1
3	203	1	6000001	00:0A:14:84:00:01	V3	V3	BB-SR30309220	2017	1	1
4	203	1	6000002	00:0A:14:84:00:02	V3	V3	BB-SR30309220	2017	1	1
5	203	1	6000003	00:0A:14:84:00:03	V3	V3	BB-SR30309220	2017	1	1
6	203	1	6000004	00:0A:14:84:00:04	V3	V3	BB-SR30309220	2017	1	1
7	203	1	6000005	00:0A:14:84:00:05	V3	V3	BB-SR30309220	2017	1	1
8										

Figure 38 Example Import file

10.1.5 Import sample file

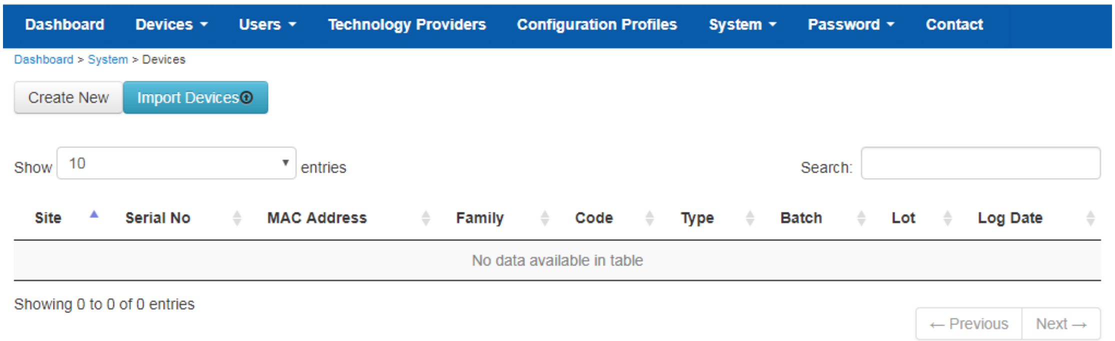
Attached is a sample file used to import devices

ImportSampleFile.csv

10.1.6 Importing the file

As the “admin” user:

- Login to WebAccess/DMP Emu Edition
- Click System – Devices



Site	Serial No	MAC Address	Family	Code	Type	Batch	Lot	Log Date
No data available in table								

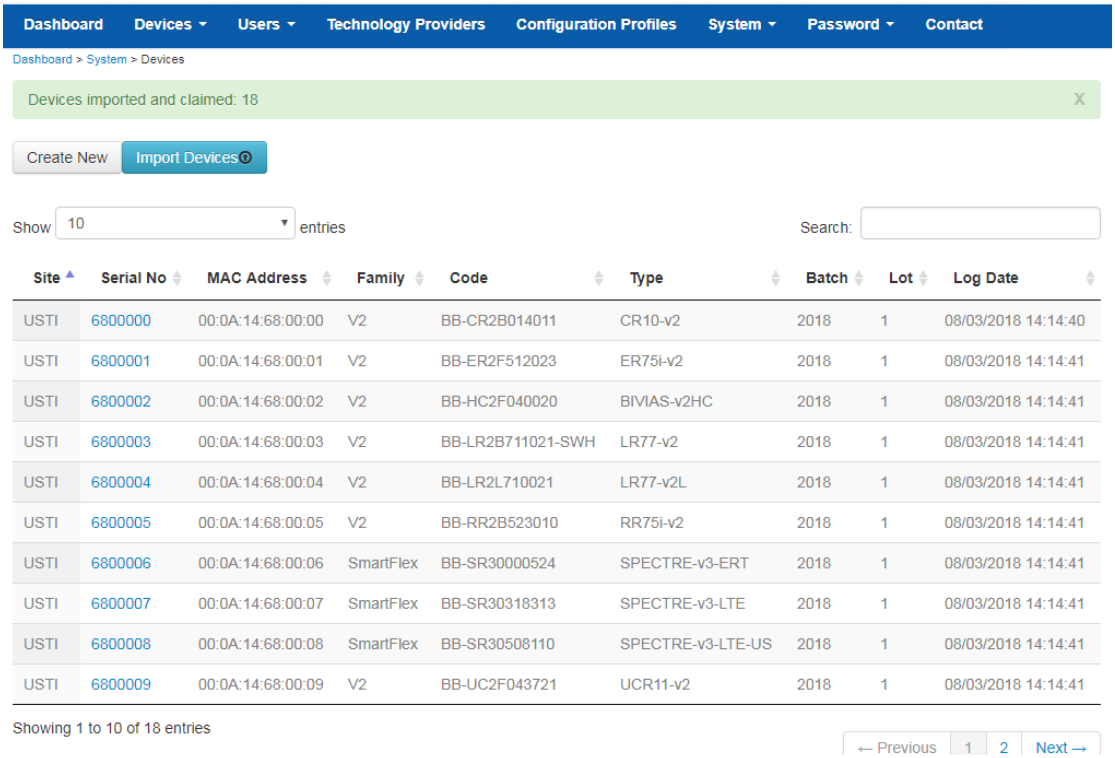
Showing 0 to 0 of 0 entries

Figure 39 Import Devices File

- Click Import Devices
- Browse to the location of the import file
- Click Open

Devices will now be imported and Created on your Platform

***NOTE**: If you did not leave the TechProvider field empty, these devices will also be CLAIMED into the Tenant Account you specified.*



Dashboard > System > Devices

Devices imported and claimed: 18

Show 10 entries Search:

Site	Serial No	MAC Address	Family	Code	Type	Batch	Lot	Log Date
USTI	6800000	00:0A:14:68:00:00	V2	BB-CR2B014011	CR10-v2	2018	1	08/03/2018 14:14:40
USTI	6800001	00:0A:14:68:00:01	V2	BB-ER2F512023	ER75i-v2	2018	1	08/03/2018 14:14:41
USTI	6800002	00:0A:14:68:00:02	V2	BB-HC2F040020	BIVIAS-v2HC	2018	1	08/03/2018 14:14:41
USTI	6800003	00:0A:14:68:00:03	V2	BB-LR2B711021-SWH	LR77-v2	2018	1	08/03/2018 14:14:41
USTI	6800004	00:0A:14:68:00:04	V2	BB-LR2L710021	LR77-v2L	2018	1	08/03/2018 14:14:41
USTI	6800005	00:0A:14:68:00:05	V2	BB-RR2B523010	RR75i-v2	2018	1	08/03/2018 14:14:41
USTI	6800006	00:0A:14:68:00:06	SmartFlex	BB-SR30000524	SPECTRE-v3-ERT	2018	1	08/03/2018 14:14:41
USTI	6800007	00:0A:14:68:00:07	SmartFlex	BB-SR30318313	SPECTRE-v3-LTE	2018	1	08/03/2018 14:14:41
USTI	6800008	00:0A:14:68:00:08	SmartFlex	BB-SR30508110	SPECTRE-v3-LTE-US	2018	1	08/03/2018 14:14:41
USTI	6800009	00:0A:14:68:00:09	V2	BB-UC2F043721	UCR11-v2	2018	1	08/03/2018 14:14:41

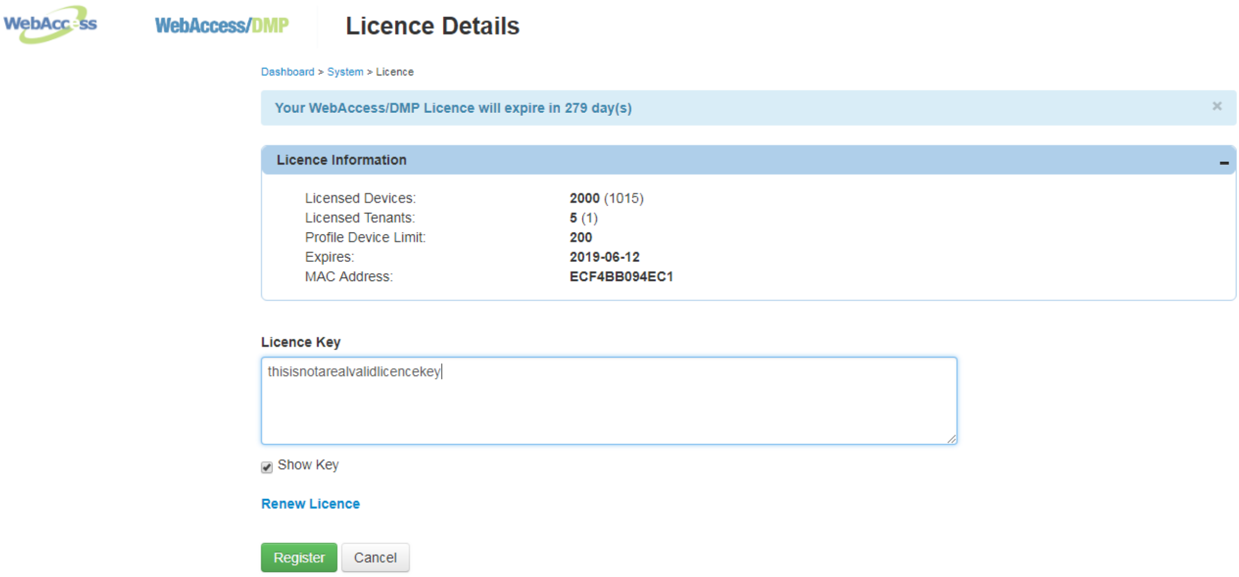
Showing 1 to 10 of 18 entries

Figure 40 Devices Imported Successfully

10.2 System-Licence

This item lets you see the status of the licence-type you currently have.

From here, you may also enter the details of any new licence you have purchased, or you may renew your existing licence.



Licence Details

Dashboard > System > Licence

Your WebAccess/DMP Licence will expire in 279 day(s)

Licence Information

Licensed Devices:	**2000** (1015)
Licensed Tenants:	**5** (1)
Profile Device Limit:	**200**
Expires:	**2019-06-12**
MAC Address:	**ECF4BB094EC1**

Licence Key

thisisnotarealvalidlicencekey

☑ Show Key

Renew Licence

Figure 41 Licence Information

11 Password

The Password screen allows a user to change their individual password. Good practice suggests passwords should be at least 8 characters long, and contain a mix of uppercase and lowercase alphabet letters, plus numbers and special characters.

Password policy is not currently enforced within WebAccess/DMP.

12 Contact

This page provides a freeform text box into which you can provide feedback, suggestions or bug reports directly into Advantech's WebAccess/DMP team. Just write your comments and click on 'Submit'.

13 Supplementary Information

13.1 Browser Compatibility

Google Chrome is the officially supported browser for DMP. The platform has been extensively tested and developed with Google Chrome version 66. Testing has been performed using Firefox versions 55-60. There are some known issues with Microsoft Edge and Safari.

13.2 System Procedures

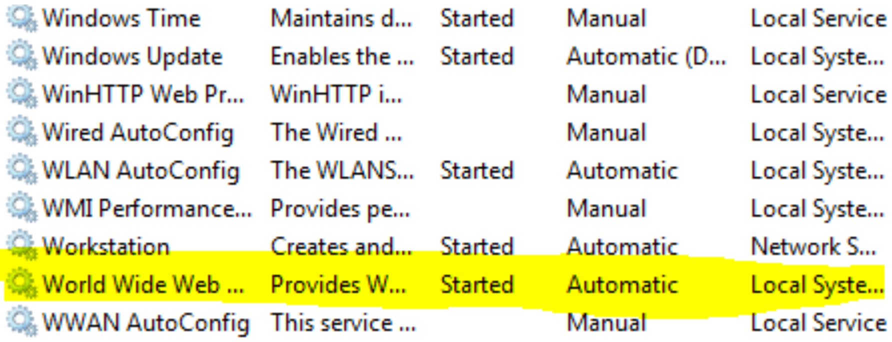
13.2.1 Introduction

DMP is a client server application. The server component is built using Microsoft ASP.NET webforms and hosted using IIS. In order to run the code in IIS the server will need .Net framework installed. The database is MS SQL Server.

13.2.2 DMP Web Application Offline / Online

Taking DMP offline when DMP is the only site on the server involves a series of steps that ideally should be performed in following order:

- Log in to the server hosting the web application
- Open the command console with admin privileges
- Stop IIS by typing net stop wssvc and hitting return. The command should report success
- If in doubt confirm the WWW service has stopped on the server. This can be done by going to Run -> services.msc. At the bottom of the service dialog the service prefixed with world wide web should have blank status indicating that it’s no longer running. The image below shows this service running.
- At this point the web site is offline and the server can now be restarted.



Windows Time	Maintains d...	Started	Manual	Local Service
Windows Update	Enables the ...	Started	Automatic (D...	Local Syste...
WinHTTP Web Pr...	WinHTTP i...		Manual	Local Service
Wired AutoConfig	The Wired ...		Manual	Local Syste...
WLAN AutoConfig	The WLANS...	Started	Automatic	Local Syste...
WMI Performance...	Provides pe...		Manual	Local Syste...
Workstation	Creates and...	Started	Automatic	Network S...
World Wide Web ...	Provides W...	Started	Automatic	Local Syste...
WWAN AutoConfig	This service ...		Manual	Local Service

Figure 42 IIS Service in Services Console

There may be situations where DMP isn’t the only web application on the server. If the requirement is to stop the DMP application only then use the IIS Manager to stop the web application. Once this is complete the site can no longer be contacted via public URL.

Restarting DMP depends on how the site was disabled above. If the site was stopped using the IIS Manager then the site can be started again by clicking Start under Manage Web Site in the IIS Manager tool. This assumes that IIS has not been stopped. If the site was disabled by disabling IIS then IIS must be re-enabled on the server. This is accomplished by following the steps outlined below:

- Log in to the DMP web application server
- Open the command console with admin privileges
- Start IIS by typing `net start w3svc` or `iisreset /start`. The command if successful will report success. Users can confirm IIS is running by checking the World Wide Web service listed previously. It should be reporting status of started.
- Once the above command is successful open the IIS Manager (Run -> inetmgr) and check to ensure the website is running. Start should be greyed out which indicates that the site is running. If this is not greyed out then click on start under Manage Web Site in IIS Manager
- Browse to the url and ensure that the login screen is presented.

13.2.3 DMP Database Offline/Online

From time to time the database may have to be taken offline. This may be for a variety of reasons. In a release scenario there is no reason to take the database offline. In this situation disabling the web application as specified above will prevent the public from using the site. Effectively the database is in pseudo single user mode. Then the release scripts can be executed against the database and the web application returned to normal functioning status.

In some circumstances the database has to be taken offline. This may be due to the application moving to new server. In these situations use the following steps

- Take the web application offline by stopping the web site using IIS Manager
- Stop IIS outline in the processes above.
- Backup the database using SQL Management Studio. There are numerous examples online regarding steps to do this.
- If there are multiple databases in the same instance as DMP then use SQL Management Studio to set the database to offline by following these steps:
    - Open SQL Management Studio right click on the AggregatorDB
    - Select Tasks -> take offline
    - Once offline the database icon will change with red arrow pointing downwards and the name of the database followed by “(Offline)”
    - The database is now offline.
- If DMP is the only database on the instance users can disable the SQL server agent and indirectly take the database offline. Again there are numerous examples online around how this operation can be performed.

The database should be backed up nightly. A database backup should precede any operation on the database requiring the web application to be taken offline.

13.3 Schedule Jobs

13.3.1 SQL Agent

13.3.1.1 Check-in History

Every x number of minutes a device (router, gateway) calls home and records the fact that it has checked in. This information is used on the dashboard screen to indicate period when devices have gone offline. The dashboard will display 30 days of data. keeping large amounts of checkin history will cause the database size to increase and the performance to degrade. It is vital this job is executed on a daily basis.

13.3.1.2 Queued Commands

After a period of time, historic queued commands will build up in the queued command table. If disc space is not an issue, then this shouldn’t be a problem. If on the other hand space is an issue, then this table will need to be archived at regular intervals. A sql job is create that performs such action. The job is called Maintenance_DeleteQueuedCommandHistory. Users should schedule this job at a time that is convenient. Ideally this should be schedule in the middle of the night when the system is not busy.