**Compass ZTP Configuration Guide**

The Zero Touch Provisioning tool allows you to deploy switches remotely through a centrally maintained and configured system. For ZTP to function a DHCP server is required that has the capability of providing DHCP option 66 (TFTP server) and 144 (configuration file) to a switch.

The tool supports the following mechanisms:

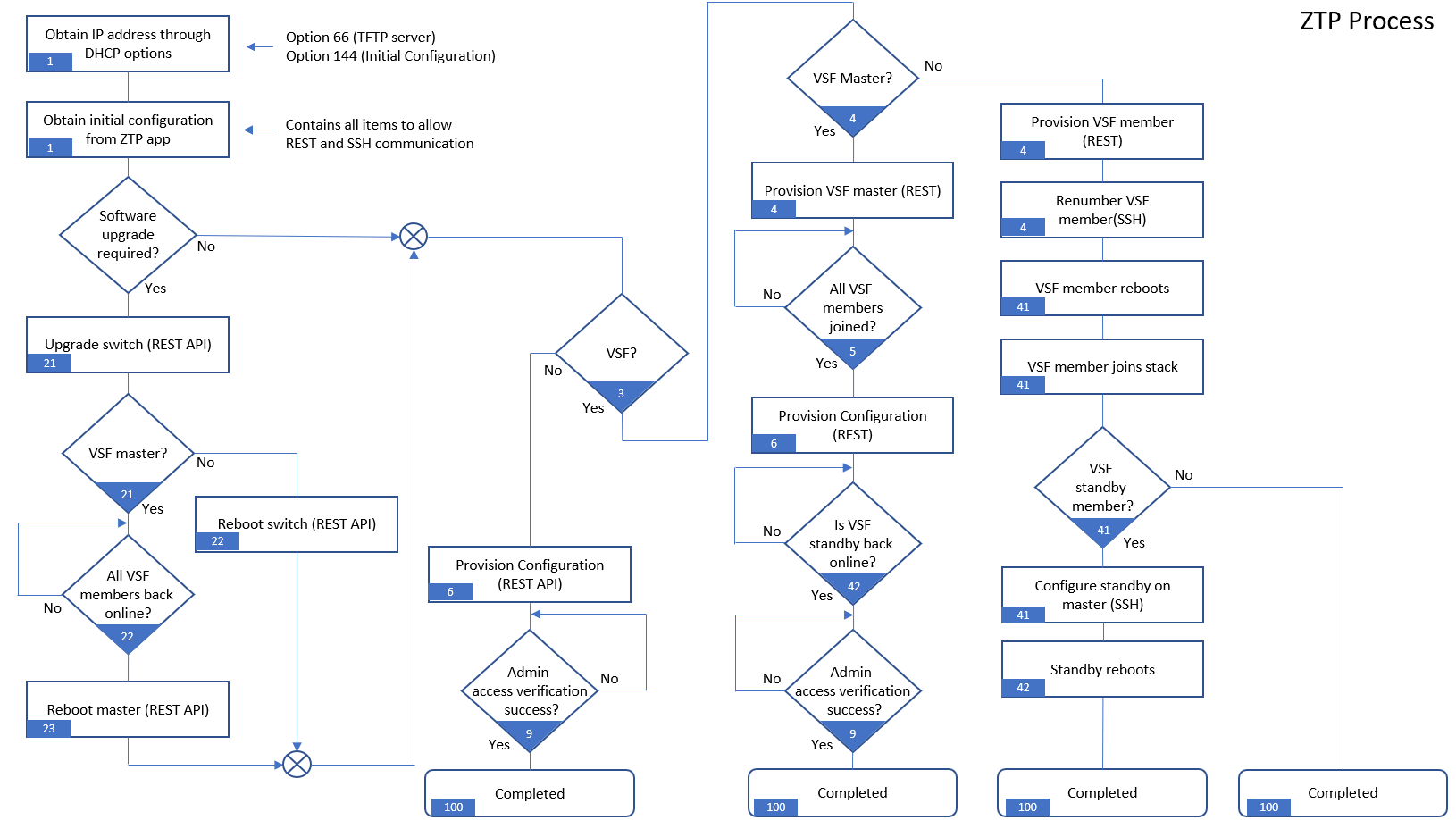
* DHCP based ZTP (requires DHCP mirroring)
* Static IP address based ZTP
* IPAM support for Infoblox and PHPIPAM

The tool supports the following devices:

* Aruba 6300 (stand alone and VSF, through default and mgmt. VRF)
* Aruba 8320 (through the mgmt VRF)
* Aruba 8325 (through the mgmt. VRF)
* Halon OVA

**ZTP Process**

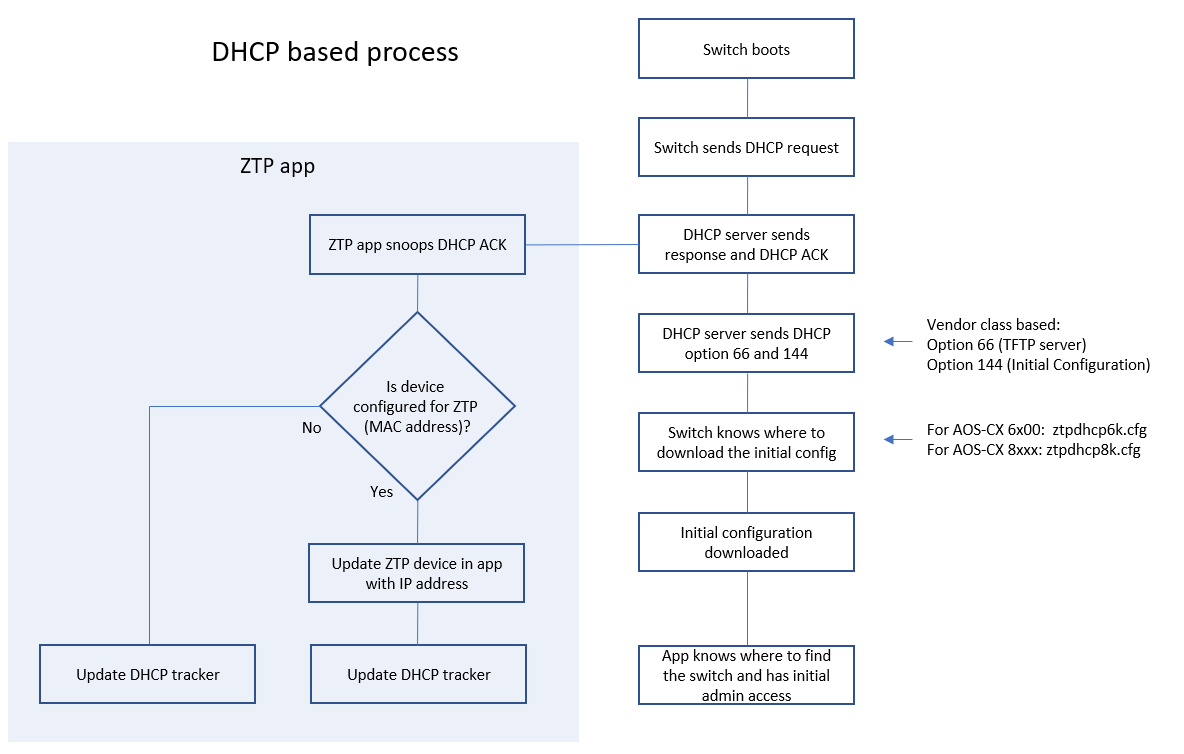
The diagram below shows the ZTP process that is executed by the ZTP daemon of the app.



The blue tags in the diagram identify the stage in the ZTP process.

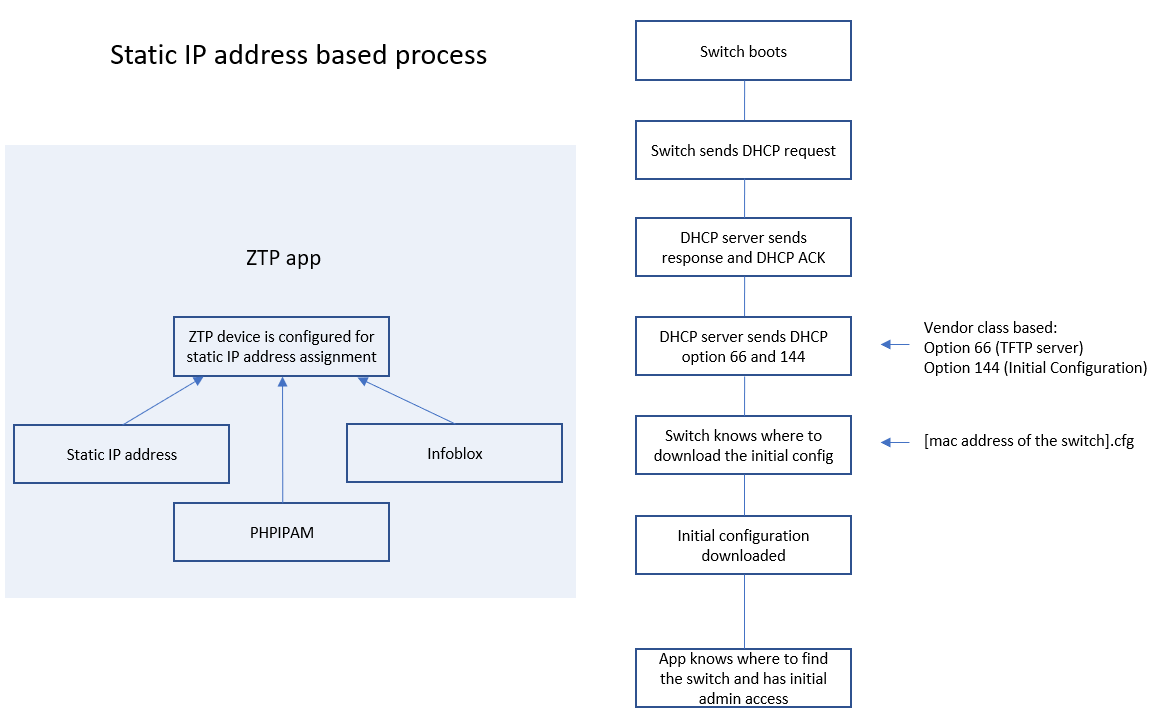
The ZTP app works with static assigned IP addresses or DHCP. When using DHCP for IP address assignment to the ZTP devices, it is required for the app to snoop the DHCP traffic of the DHCP server. This is necessary so that the app will know which IP address is assigned to the ZTP device. If the Compass application is running on the same VLAN as the DHCP server, there is no additional networking configuration required.  
If the Compass application is running on a different subnet, it cannot snoop the DHCP broadcast responses from the DHCP server. In those cases, it is required to configure a mirror port, either local or remote.

The flowchart below describes the process:



If it is not possible to snoop the DHCP traffic, ZTP through static IP address assignment is also supported.  
This will require the configuration of DHCP policies on the DHCP server. In a DHCP policy the configuration file for the switch to download from the TFTP server is manually defined per switch.

The diagram below shows the process for static IP address assignment.



The configuration process of the DHCP server is described in the next chapter.

**DHCP server preparation**

This document covers the DHCP server preparation, based on Windows DHCP server.

For the Compass ZTP tool to access the switches, the switch will require an initial configuration file that is pushed by the tool through TFTP. In order for the switch to know the location and configuration, DHCP options have to be configured on the DHCP server.

On Microsoft DHCP server, the first step is to configure the Vendor Classes for the Aruba Switches.

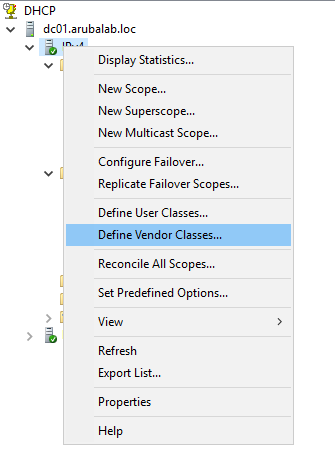
Before defining the vendor class, issue the following command on the switch that you would like to add the vendor class for:

*show dhcp client vendor-class-identifier*

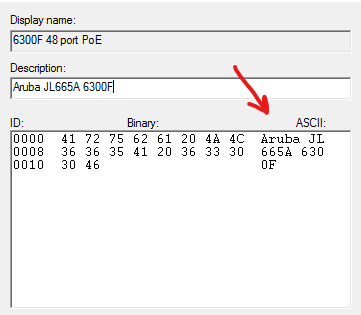
The switch will return the Vendor Class Identifier that you require for the configuration of the vendor class on the DHCP server.

For example, the VCI of a 48 port PoE switch 6300 is:

Vendor Class Identifier: ***Aruba JL665A 6300F***



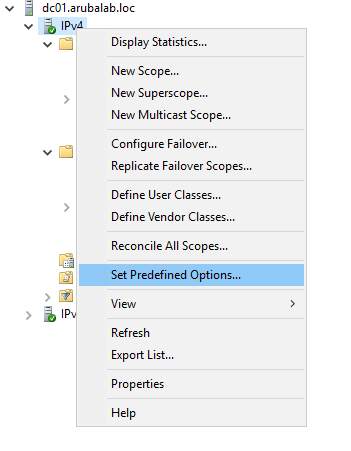
On the DHCP server, right click on the IPv4 item and select “Define Vendor Classes”.



Click on “Add” and enter the information in the required fields. In the ASCII section of the form, you have to enter the Vendor Class Identifier (example shown below).

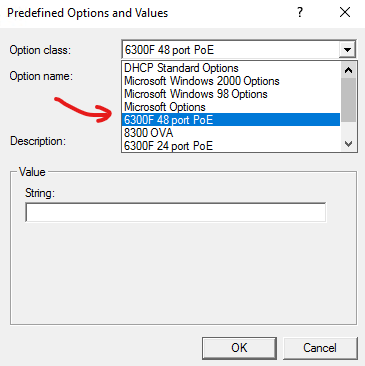
Click “Add” to add the Vendor Class.

Next is to define the predefined options for the Vendor Class. This is option 66 (for the TFTP server) and option 144 (for defining the configuration file).

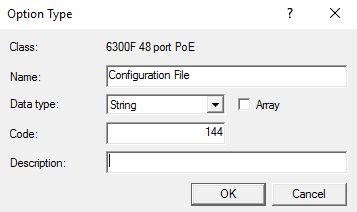


On the DHCP server, right click on the IPv4 item and select “Set Predefined Options”.

Option 66 is a default option that exists on the DHCP server, so this does not have to be configured, only option 144 has to be configured. When using DHCP address assigned ZTP, the default ZTP configuration file can be assigned to this option.



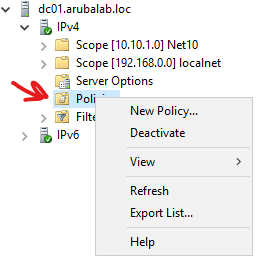
From the Option class select field, select the Vendor class, that you have created, and click “Add”.



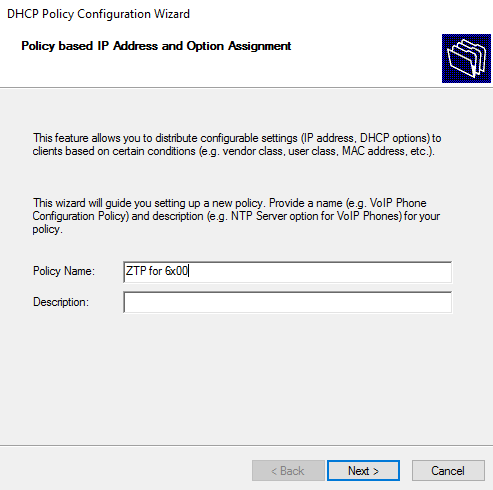
Add option code 144 (a string data type), provide a name/description, click “OK” and confirm the predefined options.

As said, there are two options for IP address assignment with ZTP, either through DHCP or static IP address assignment.

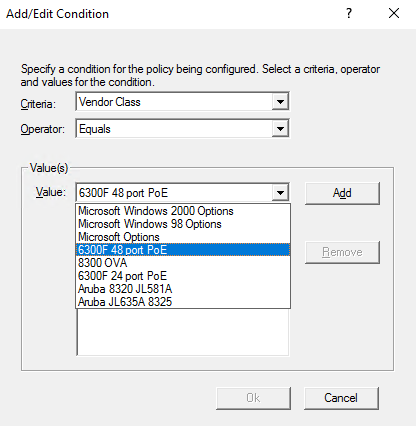
For DHCP assigned ZTP, the easiest way to configure the scope options is through a global policy. This policy is assigned to all the scopes.



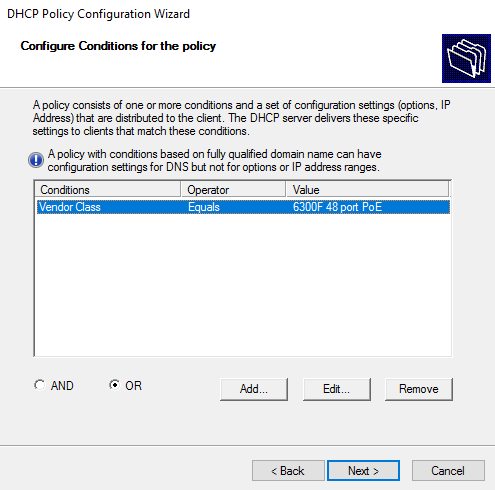
In the DHCP management tool, right click on the “Policies” item in the “IPv4 scope and select “New Policy”.



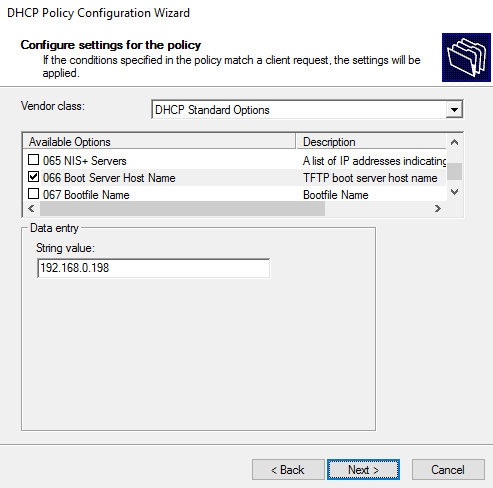
Provide a name (and optionally a description), and click “Next”.



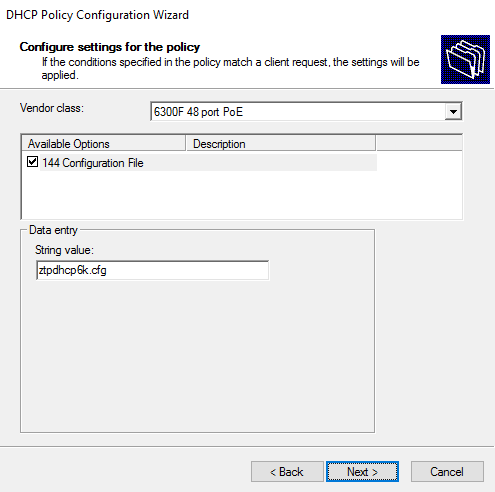
Add a condition, this is the Vendor Class Identifier condition. Click “Add”, and from the Vendor Class criterium, select the Vendor Class that you have created and click “Add”. Click “OK” to confirm.



The condition is now in the list. Click “Next”.



From the DHCP Standard Options, select option 66, and enter the IP address of the TFTP server. This is the IP address of the Compass app.

From the Vendor class list, select the VCI that you have just created, select option 144, and enter the name of the configuration file. For the 6x00 series switches, the default configuration file name for ZTP through DHCP is **ztpdhcp6k.cfg**.

For the 83x0 series switches, the default configuration file name for ZTP through DHCP is **ztpdhcp8k.cfg**.

Click “Next”.



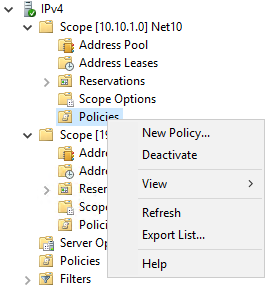
You now get an overview of the configured policy. Because this is a global policy, this will be active in all the DHCP scopes. Click “Finish” to add the policy.

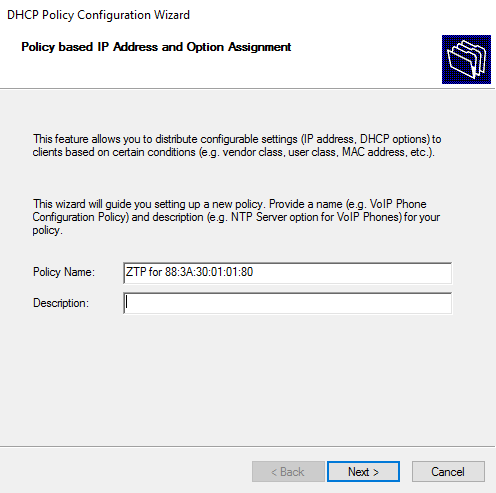
You can repeat this process for other switches, first create the Vendor Class, then define the predefined options, and then configure a global policy.

If you are planning to use ZTP with static IP address assignment, you have to configure a policy for each device. This is because the DHCP server needs to know which initial configuration file to push to the switch. You can either configure a global policy, or define a policy in the scope where the switch resides. The process for defining a policy for a static IP address ZTP device is very similar to defining a policy for a DHCP ZTP device, the main differences are that you have to set an additional condition, defining the MAC address of the switch, and assign a different configuration file.

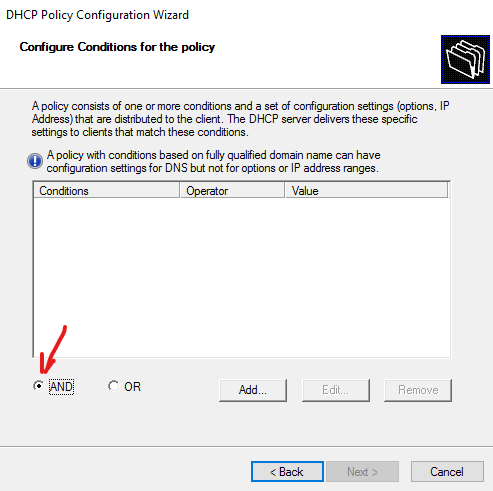
Before configuration of the policy, you have to obtain the MAC address of the switch that you want to zero touch provision. You can find the MAC address of the system (which is typically assigned to VLAN 1), on the box of the device and also on the orange retractable tag on the switch. The management interface MAC address is the system MAC address + 1. For example, if the system MAC address (on the cardboard box) is 88:3A:30:01:01:**80**, this is the MAC address when you ZTP through one of the data ports. If you ZTP on the Management interface the MAC address will be 88:3a:30:01:01:**81**

This is important for the assignment of the configuration file on the DHCP server.

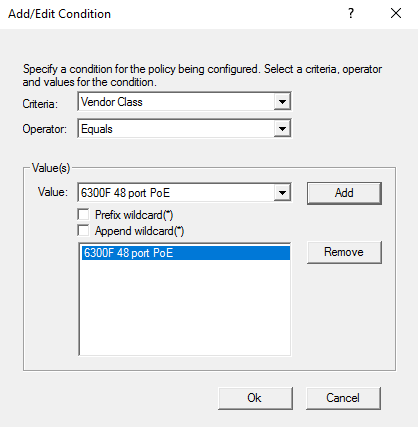
As said, you can configure a global policy, or configure a policy in the DHCP scope. Right click on “Policies” and select “New Policy”.



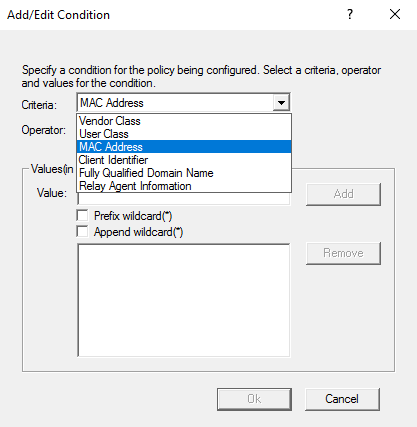
Provide a descriptive name for the policy and click “Next”.

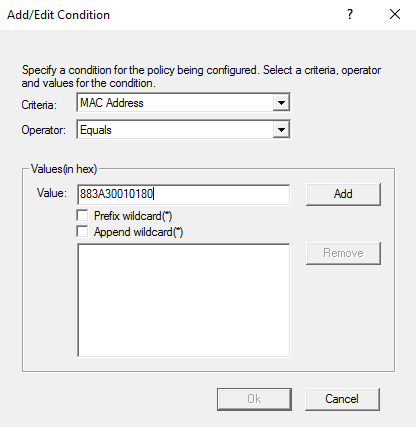


In the policy conditions, you are now checking on MAC address and Vendor Class, so you have to select the “AND” operand.

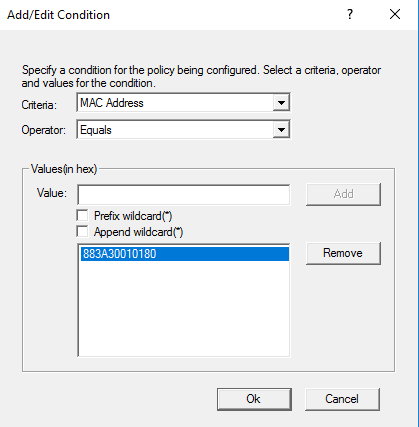


Add the conditions for the Vendor Class.

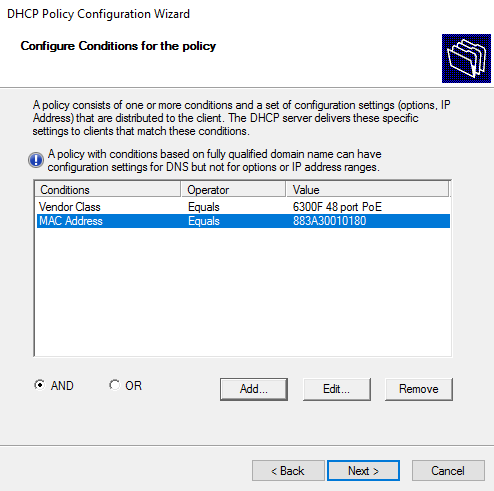
And add another condition for the MAC address of the switch by selecting “MAC Address” from the criteria field



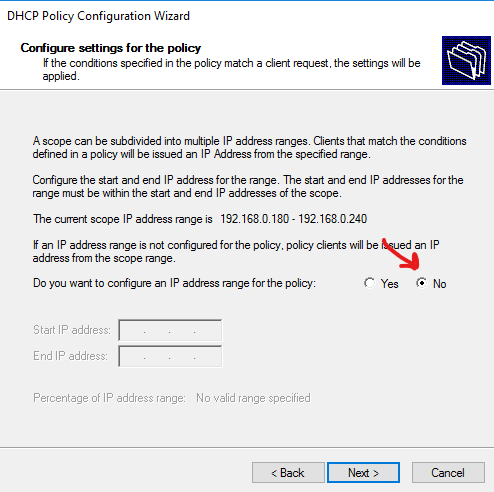
In the Value field, enter the MAC address without separators (only the hex value), and click “Add”.



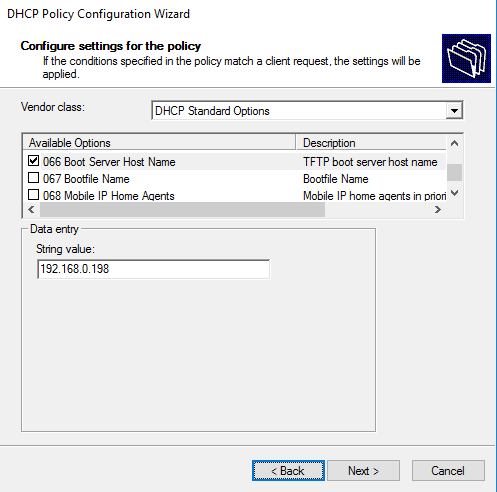
Click “Ok” to add the MAC address condition.



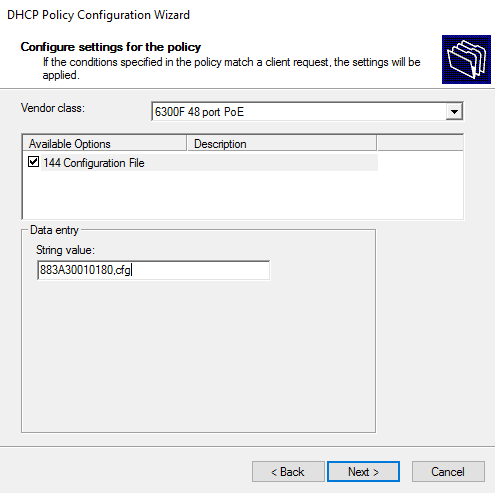
Click “Next”.



Skip the scope address options, by selecting “No”, and click “Next”.



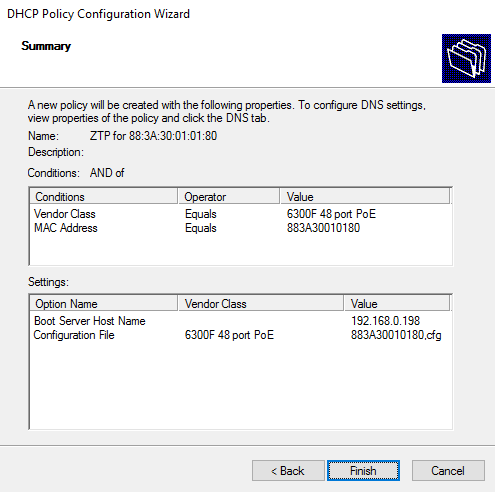
Next is to configure the scope options, 66 and 144. For option 66, select that option from the DHCP Standard Options Vendor class, and enter the IP address of the TFTP server.



For option 144, instead of assigning the default ztpdhcp\*\*.cfg, you have to provide the [macaddress].cfg as shown in the screenshot.

This is the configuration file that will be generated by the app, when ZTP is enabled for the selected device. This configuration file will contain the static IP address that will allow the app to communicate with the device.

Click “Next”.



You will get an overview of the policy. Click “Finish”.

This concludes the configuration of the DHCP server.

**Port mirroring configuration examples**

This chapter provides configuration examples for the setup of port mirroring that allows for the snooping of DHCP packets. The configuration examples are:

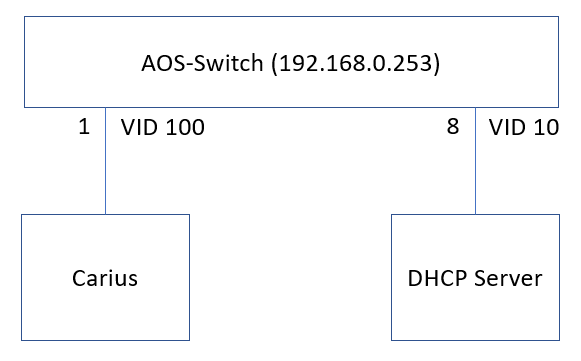
* Local mirroring on AOS-Switch
* Remote mirroring on AOS-Switch
* Local mirroring on AOS-CX
* Remote mirroring on AOS-CX

The configuration of a mirroring port is required if the Compass server is located on a different subnet because the DHCP server packets boundaries are within a VLAN.

In addition, if DHCP helper or DHCP relay is used, the DHCP server will respond to DHCP request with a unicast response instead of a broadcast. This is because the client for that request is located on a different subnet. If this is the case, mirroring also has to be configured.

**Local mirroring on AOS-Switch**

The diagram below shows an example setup where port 1 is connected to the Compass application server, and port 8 is connected to the DHCP server. The goal is to mirror DHCP traffic that comes in and goes out on port 8, is mirrored to port 1 so that the Compass application server can snoop the DHCP traffic. Note that the Compass host is on a different VLAN than the DHCP server. If the Compass host is on the same VLAN, there is no requirement for configuring port mirroring on the single switch.



The switch configuration looks like this:

*class ipv4 "dhcp-mirror"*

*10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 67 68*

*exit*

*policy mirror "dhcp-mirror"*

*10 class ipv4 "dhcp-mirror" action mirror 1*

*exit*

*mirror 1 port 1*

*interface 8*

*monitor all both mirror 1*

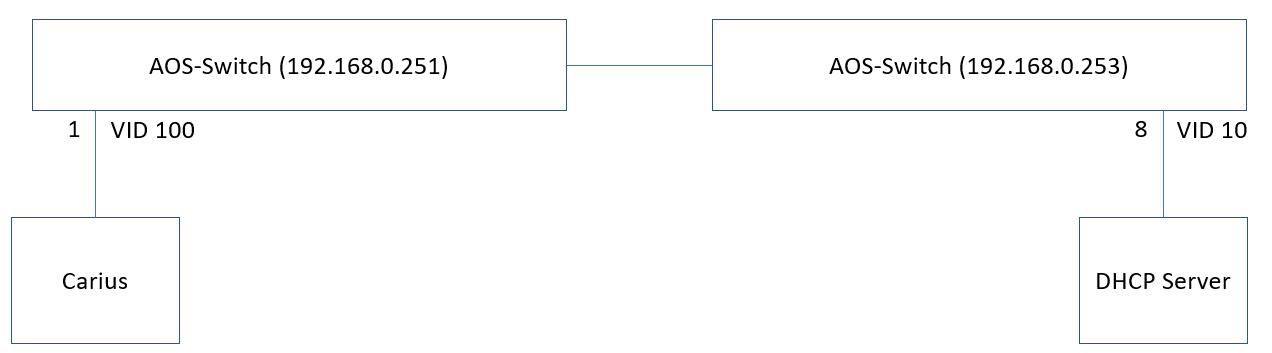
*exit*

The first step is to create a class that classifies the DHCP traffic (class ipv4). Next is to create a mirror policy where the class is assigned to the mirror port. This will actually filter all traffic, except for DHCP traffic. And finally, the mirror port is created and the DHCP server port is assigned to the mirror instance.

**Remote mirroring on AOS-Switch**

The diagram below shows an example setup where the Compass application server is connected to port 1 of a switch, and the DHCP server is connected to port 8 of another switch. In this example, the link is not traversing a router, but this is also supported, as long as the switches can reach each other.

The remote mirror is based on a GRE tunnel that is created between the switches, this tunnel will carry the monitored traffic.



Configuration on the mirroring switch (Compass):

*mirror endpoint ip 192.168.0.253 9000 192.168.0.251 port 1*

The above command creates the GRE tunnel to destination switch 192.168.0.253 on UDP port 9000, and the traffic that comes from this tunnel is mirrored to port 1.

Configuration on the DHCP server switch:

*class ipv4 "dhcp-mirror"*

*10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 range 67 68*

*exit*

*policy mirror "dhcp-mirror"*

*10 class ipv4 "dhcp-mirror" action mirror 1*

*exit*

*mirror 1 remote ip 192.168.0.253 9000 192.168.0.251*

*interface 8*

*service-policy "dhcp-mirror" in*

*exit*

The configuration looks very similar to configuring local mirroring, there are two differences. The “mirror 1 remote” command creates the tunnel to the destination switch (destination port 9000).

On the port to which the DHCP server is connected, a service policy is assigned, this policy makes sure that only the traffic that is defined in the “dhcp-mirror” policy is handled.

**Local mirroring on AOS-CX**

The diagram below shows an example setup where port 1 is connected to the Compass application server, and port 48 is connected to the DHCP server. The goal is to mirror DHCP traffic that comes in and goes out on port 48, is mirrored to port 1 so that the Compass application server can snoop the DHCP traffic. Note that the Compass host is on a different VLAN than the DHCP server. If the Compass host is on the same VLAN, there is no requirement for configuring port mirroring on the single switch.



The switch configuration looks like this:

*class ip dhcp-mirror*

*10 match udp any any range 67 68*

*policy dhcp-mirror*

*10 class ip dhcp-mirror action mirror 1*

*mirror session 1*

*destination interface 1/1/1*

*enable*

*interface 1/1/48*

*apply policy dhcp-mirror out*

*apply policy dhcp-mirror in*

The class is created for classifying the DHCP traffic and in the policy the action for this class is to mirror the DHCP traffic to mirror session 1. Because a policy is used, in the mirror session, you don’t configure the source, if you would do that, this will forward all traffic again. Finally, on the interface that connects to the DHCP server, apply the policy for outbound traffic.

**Remote mirroring on AOS-CX**

At this moment, there is no support for RSPAN on AOS-CX, only ERSPAN (10.04). It is recommended to have an RSPAN configuration because typically with ERSPAN traffic is encapsulated in GRE which makes it more difficult to analyze DHCP packets on Compass.

**IPAM Integration**

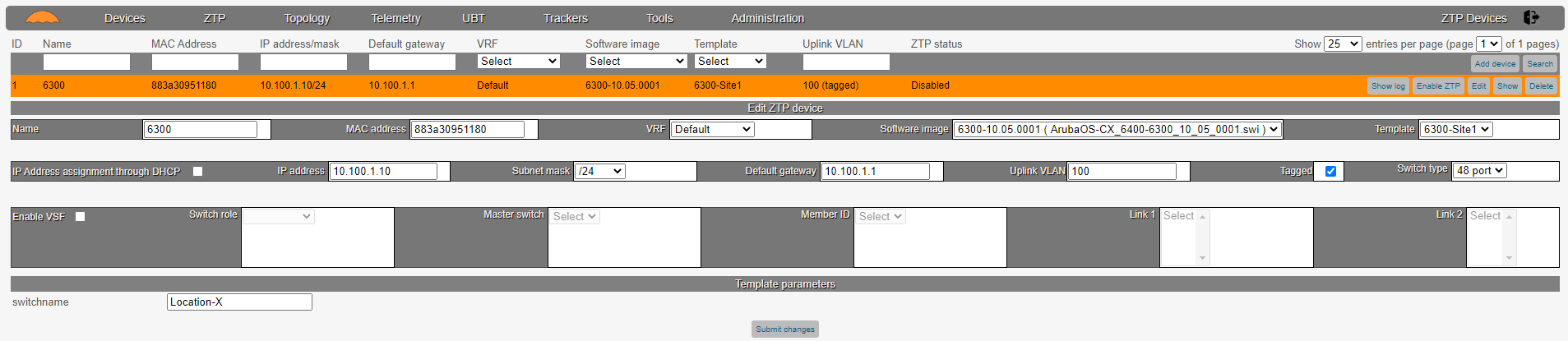
When ZTP with static IP address assignment is deployed, there are three options:

* Static IP address assignment with the ZTP app
* Static IP address assignment with PHPIPAM
* Static IP address assignment with Infoblox

When using IPAM integration options, the app retrieves the available subnets and IP address ranges from the IPAM, from which you can select an IP address.

**Static IP address assignment with the ZTP app**

This feature is very straight forward. You assign an IP address to the device in the Devices form. This IP address will be used as communication IP address with the initial communication between ZTP app and the switch.



For static IP address assignment, it is also possible to specify an uplink VLAN, and whether this VLAN should be tagged or untagged. The purpose of this feature is that in some cases, it is not desired to perform the ZTP process on the default untagged VLAN. When an uplink VLAN is specified, the configuration for the initial configuration contains that VLAN configuration, whereas the VLAN is created in the initial configuration and assigned as tagged or untagged (depending on the setting in this form) to the high speed uplink ports and the two highest data ports. For the 48 port switch this is interface 47 and 48, for the 24 port switch this is interface 23 and 24.

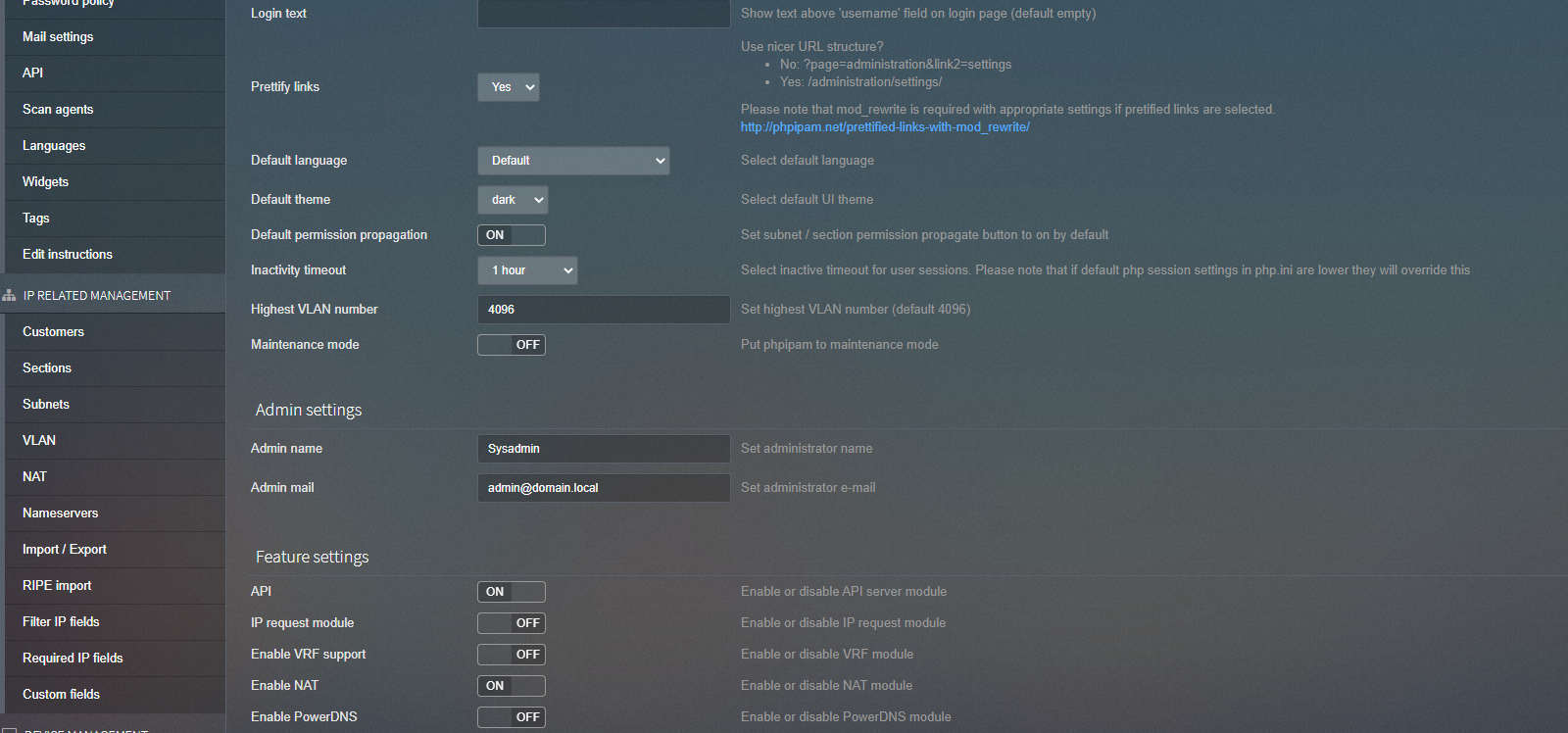
**Static IP address assignment with PHPIPAM**

First step for setting up integration with PHPIPAM is the configuration of PHPIPAM.

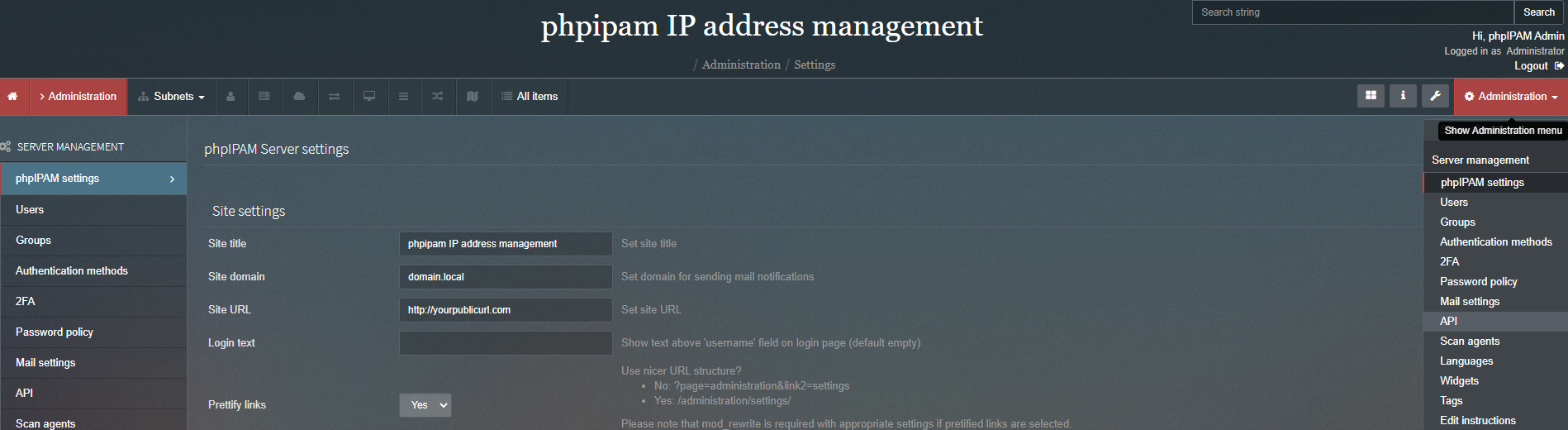
Login to PHPIPAM with administrative rights, and from the “Administration” pull down menu, select “phpIPAM settings”.



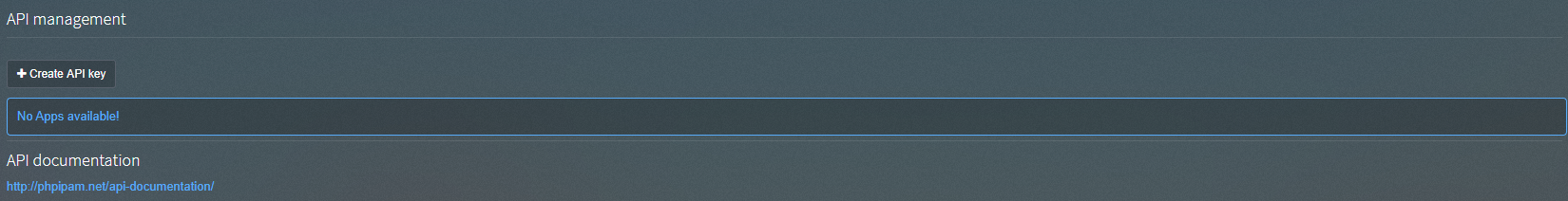
Scroll down and verify whether the API switch has been set to “On”.



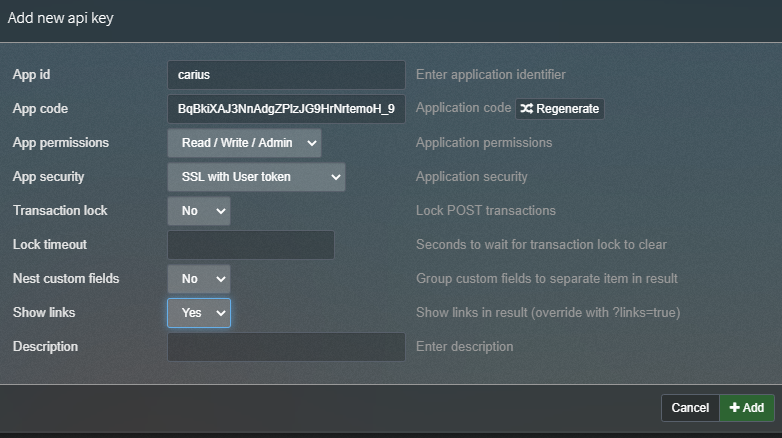
Next step is to create an API user. From the “Administration” pull down menu, select “API”.



Click on “+ Create API key”.

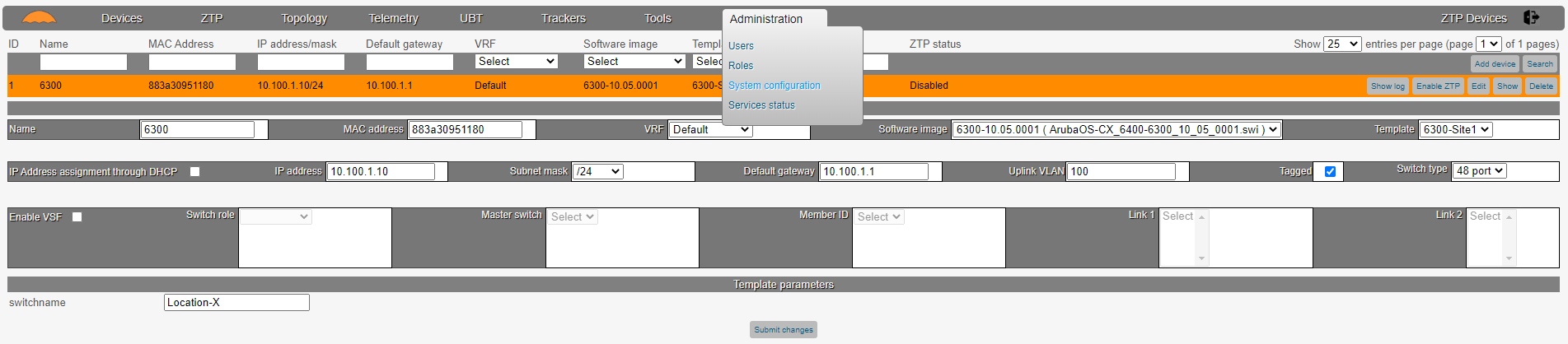


Provide the information as shown in the example screenshot below. In the Compass app, you will need the App id, App code and App security information. Set the app security to “SSL with User token”.  
Click on “Add” to create the API key.

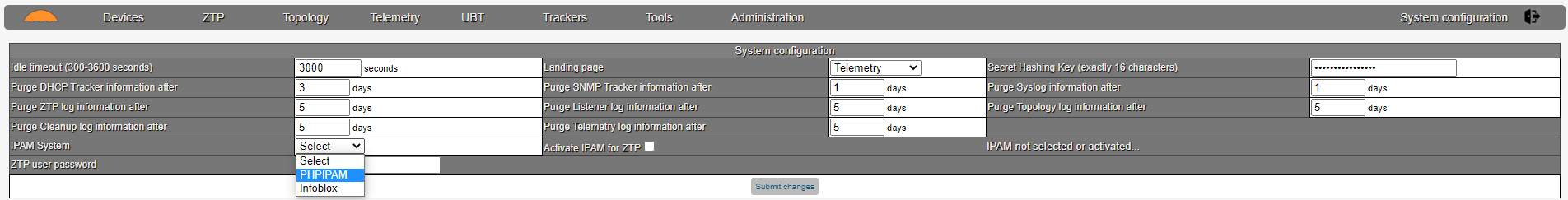


In this example, you will use the PHPIPAM admin user account for logging into the system. Of course, it is better practice to create a specific API user in PHPIPAM, this is something that you can do as well, but it is beyond the scope of this document.

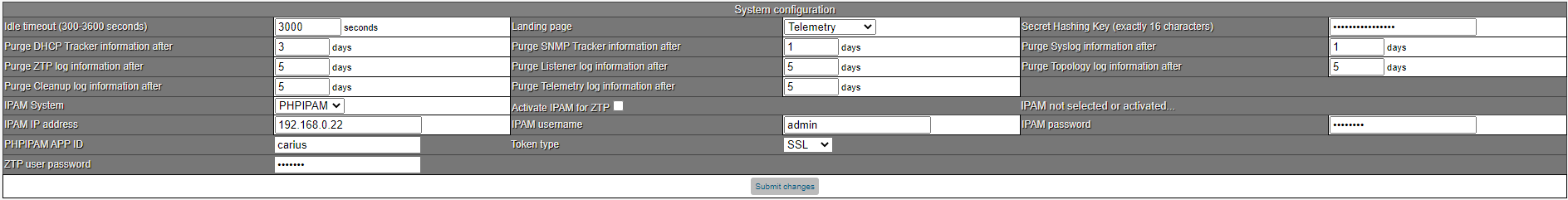
In the Compass app, navigate to “System configuration” in the “Administration” section.



From the IPAM System pull down menu, select “PHPIPAM”.

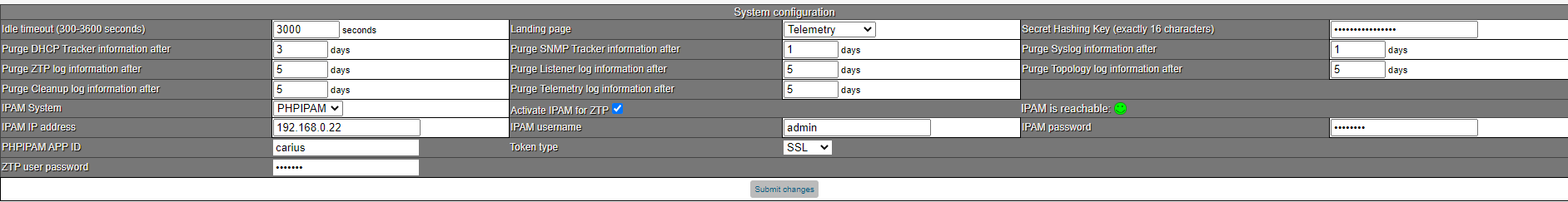


Once selected, you will see a couple of new options that you need to configure. Enter the information as shown in the screenshot below, don’t submit the form at this moment.



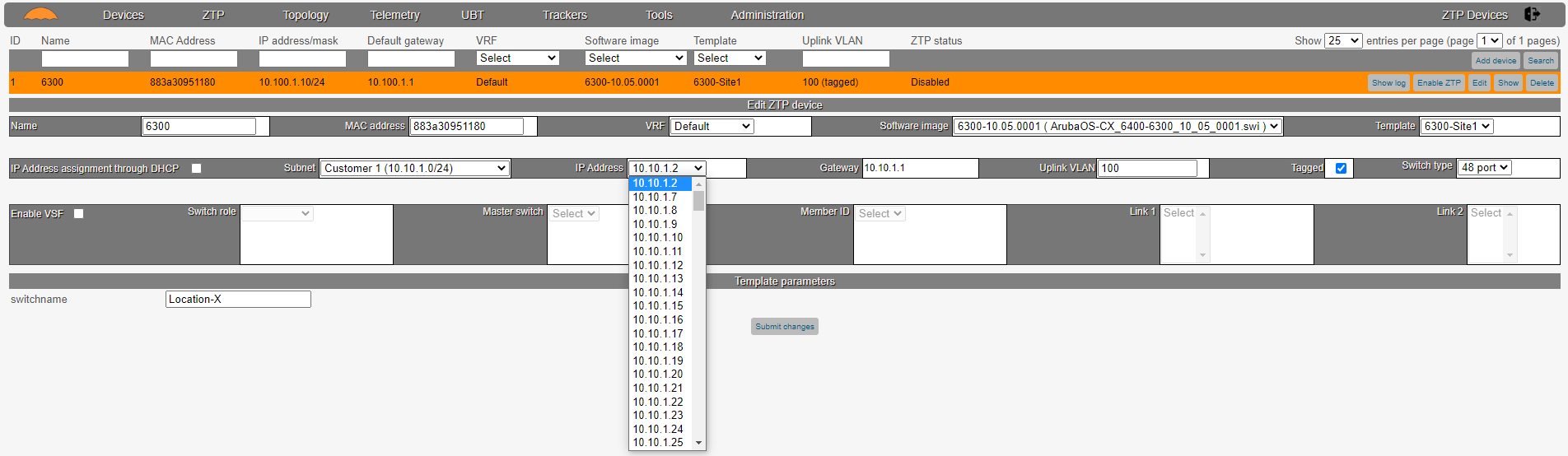
Now, click the “Activate IPAM for ZTP” checkbox. The app now tries to establish a connection with PHPIPAM.

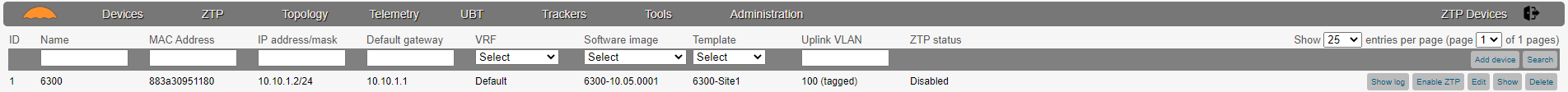
Once the checkbox is clicked, you can see in the status that the IPAM is reachable. This is proof that you can use PHPIPAM for IP address assignment in the ZTP app. Now, you can click “Submit” to store the settings.



If you now navigate to the ZTP devices again, and add/edit one of the devices, you will get a list of the subnets that have been configured in PHPIPAM and you can select the relevant subnet and IP address for that device.





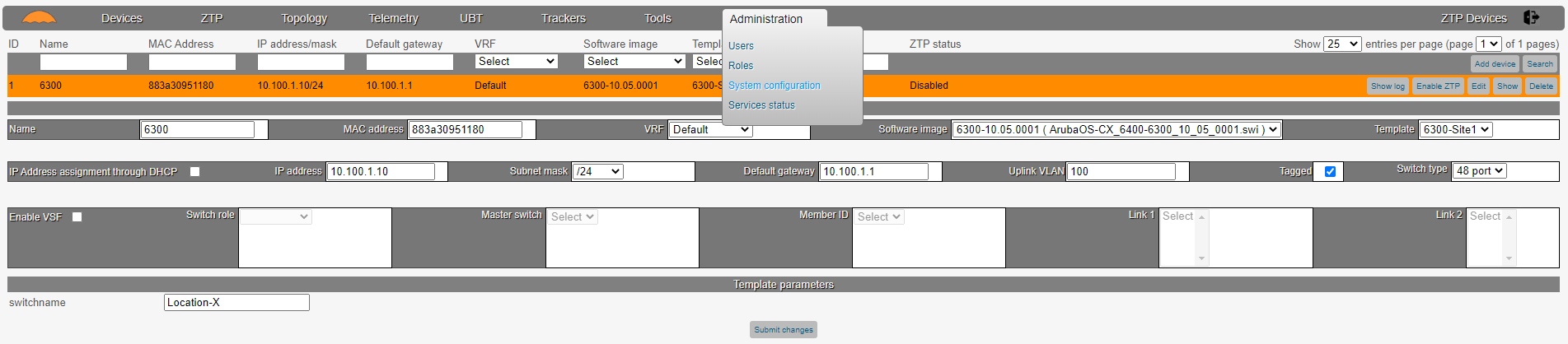


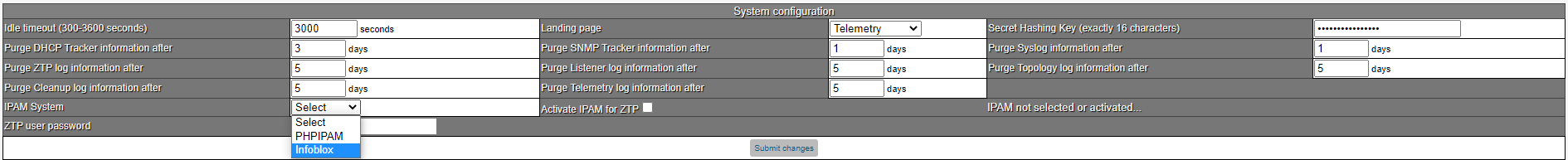
For the configuration of subnets in PHPIPAM, please refer to the documentation of PHPIPAM.

**Static IP address assignment with Infoblox**

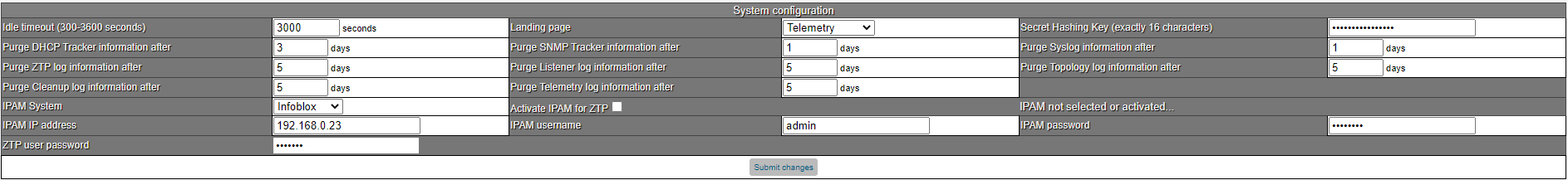
The setup of IP address assignment through Infoblox is very easy. For integration, we will also use the administrative user account of Infoblox, for the configuration of restricted user accounts (API) in Infoblox, please refer to the Infoblox documentation.

In the “Administration” section, select “System configuration”.

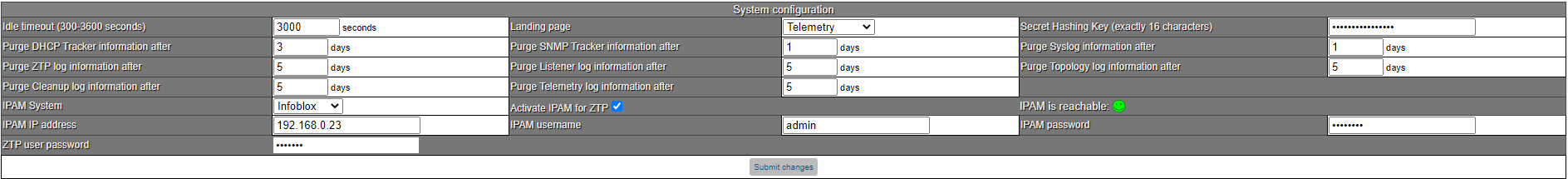


From the “IPAM System” pull down menu, select “Infoblox”. You will see some new fields in the form. 

Enter the IP address of the Infoblox system and the username/password account that you want to use to access the Infoblox API.

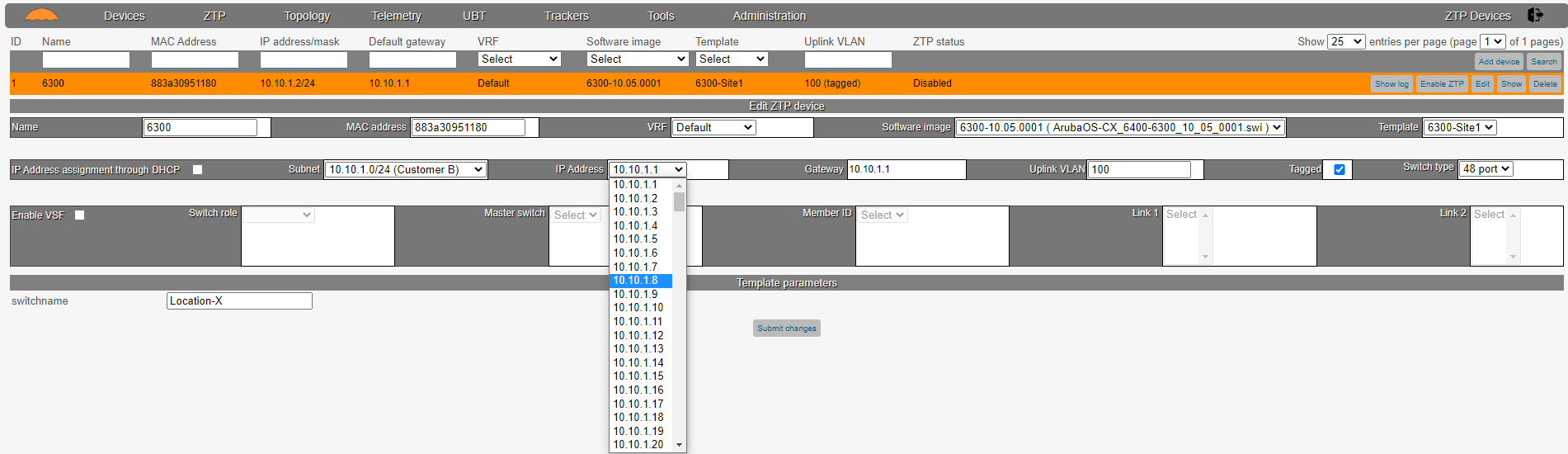


Same as with the PHPIPAM integration, don’t submit the form but click on “Activate IPAM for ZTP”. You should see the smiley face when the connection with Infoblox is successful.



Navigate to the ZTP devices and you can now make a selection from the subnets that are available in Infoblox.







For the configuration of subnets in Infoblox, please refer to the documentation of Infoblox.

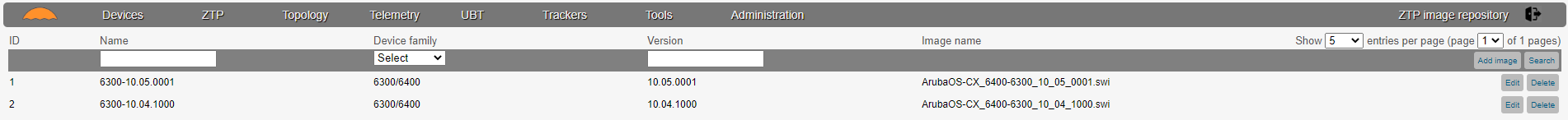
**ZTP workflow**

The goal of the ZTP functionality is to make it as intuitive as possible. The configuration flow consists of up to three steps:

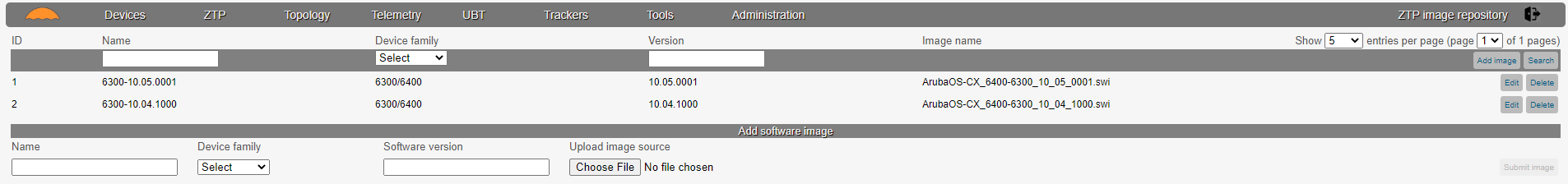
* Software image repository
* Configuration templates
* The ZTP device configuration

**Software image repository**

If you want to perform a software upgrade during the ZTP process, this is supported by the app.



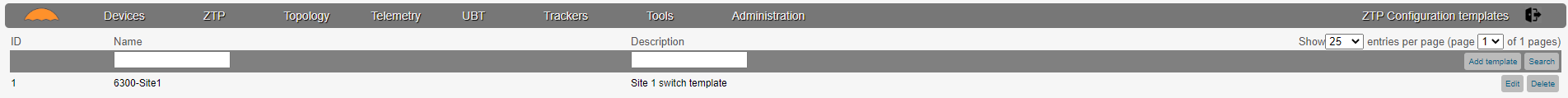
You can upload the software images to the server, and in the ZTP device configuration, you can then assign the software image to the device.



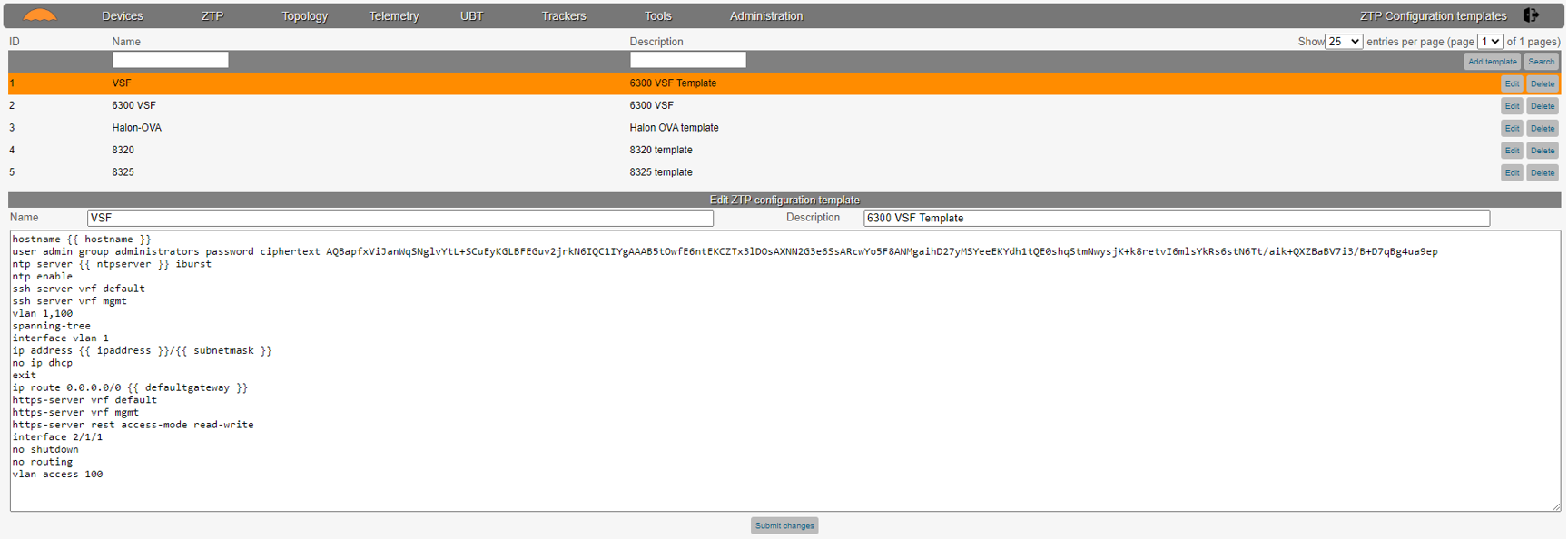
This is a very straight forward and easy process.

**Configuration templates**

In the templates section, you can create configuration templates for each device, or even use template parameters.

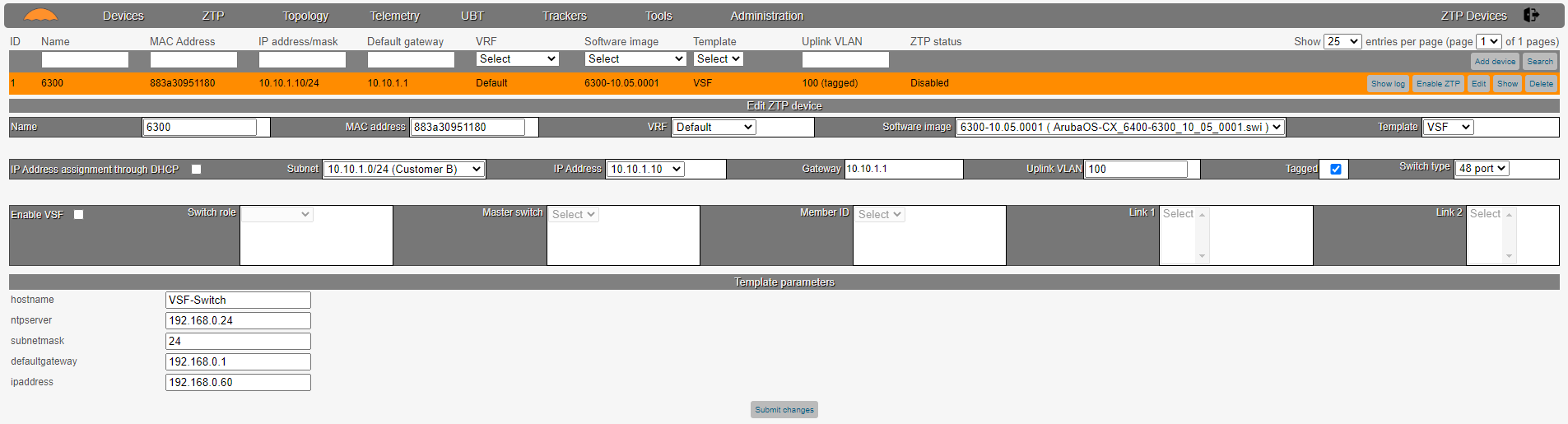


In the example below, you can see a configuration template for a 6300 VSF.



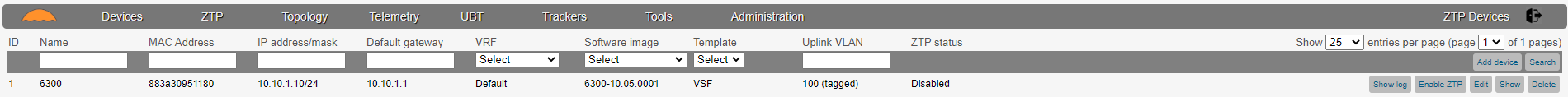
In the configuration you can see {{ … }} items. These are Jinja2 type variables, the app can convert this Jinja formatted variables in the ZTP device configuration.   
For example, in the configuration above, you can see the {{ hostname }} and {{ ntpserver }} variable. When you configure the ZTP device and assign this configuration template to the device, the form will allow you to configure these variables.

Let’s have a look.

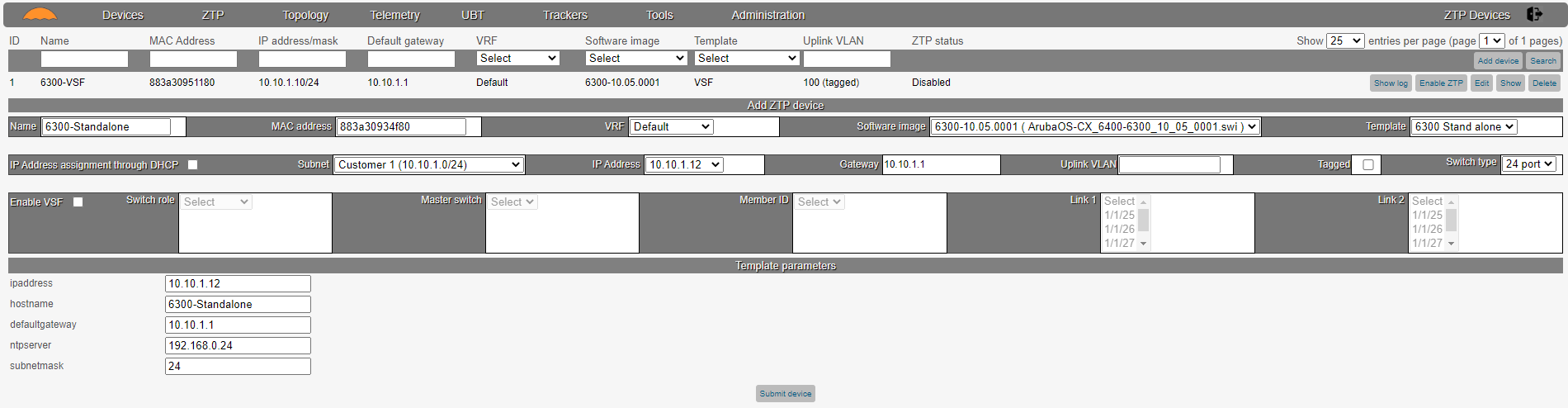


**Devices**

The ZTP device context allows you to configure and monitor ZTP devices. Let’s begin with the configuration of a device by clicking the “Add device” button.



The configuration is very intuitive and easy to understand, here is a short explanation of the fields. The below example is for a stand alone device (6300).



The MAC address field is very important. This is the MAC address of the device that connects to the network. You can find the MAC address of the switch on the box, and on the orange label of the switch. The MAC address that you find on the box and orange label is the system MAC address. If you choose to perform ZTP from the management interface you need to add 1 to that address, so for example if the system MAC address is 00291C123456, then the Management interface MAC address is 00291C123457.

You can choose whether you want to use DHCP or static IP address assignment. Remember that when you use DHCP as ZTP method, the app requires the snooping of DHCP ACK packets (setup port mirroring). If you choose to use static IP address assignment, you need to configure DHCP policies on the DHCP server (this has been explained earlier in this document).

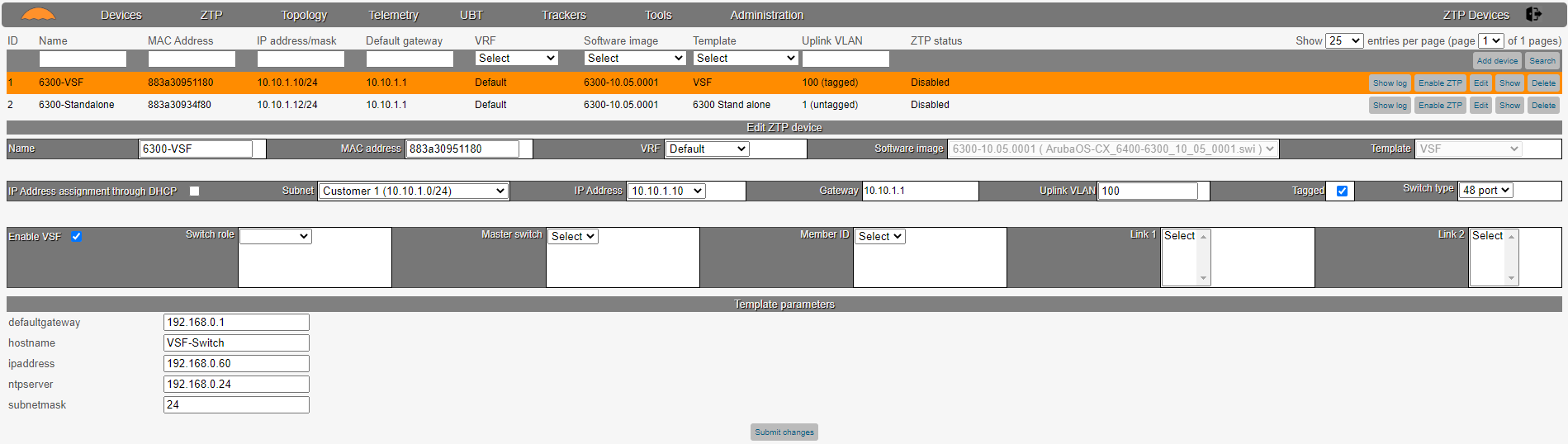
The “VRF” field allows you to set the VRF from which to perform the ZTP, “Default” is when using one of the data ports (only supported on 6x00), “Management” is for ZTP through the management interface (supported on all CX platforms, from release 10.04.0010).

In the “Software image” field you can select the software image that you want to use for upgrading the switch during ZTP. This is an optional field, if you don’t want to upgrade during ZTP, you can leave this field empty. In addition, when you select a software image, and the switch is already running on that software image, the software update is not necessary and will therefore not take place.

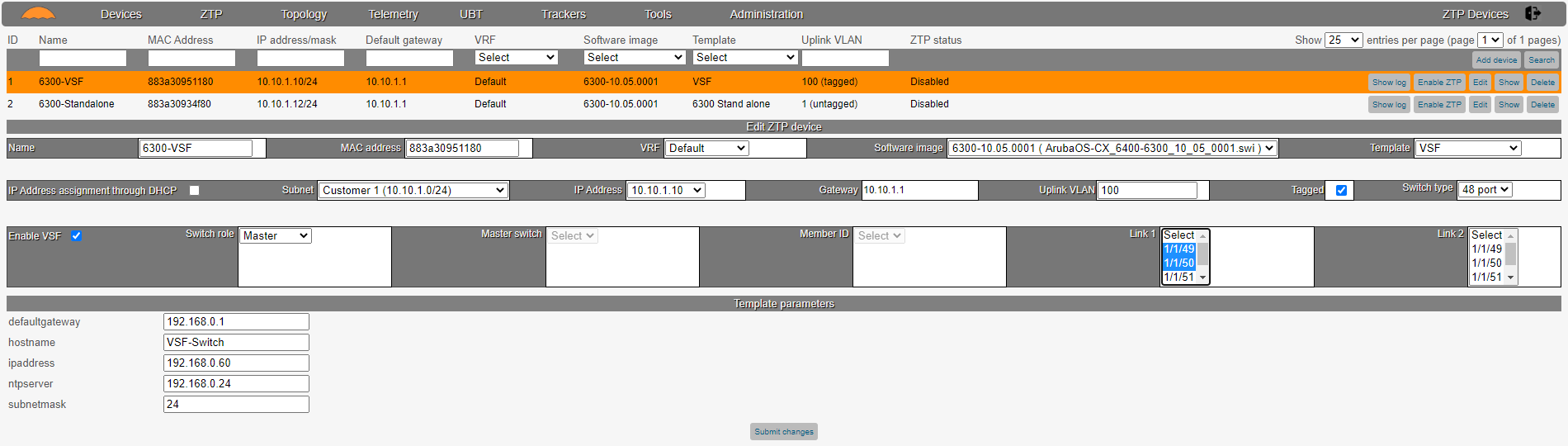
The “Template” field allows you to assign a configuration template. In the example above you can see that the template contains some template parameters, that you need to fill in (requirement).

And that’s really it for configuring a stand-alone switch.

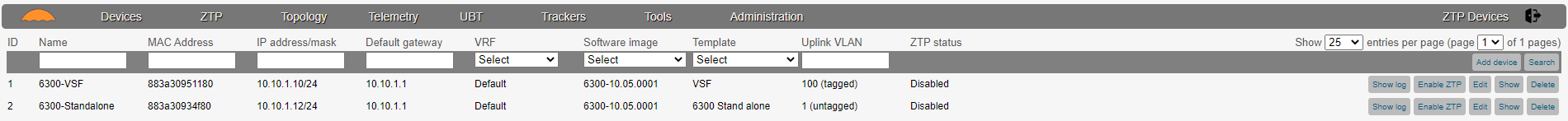
In the Device form, you can also see a VSF section, let’s have a look at that section.



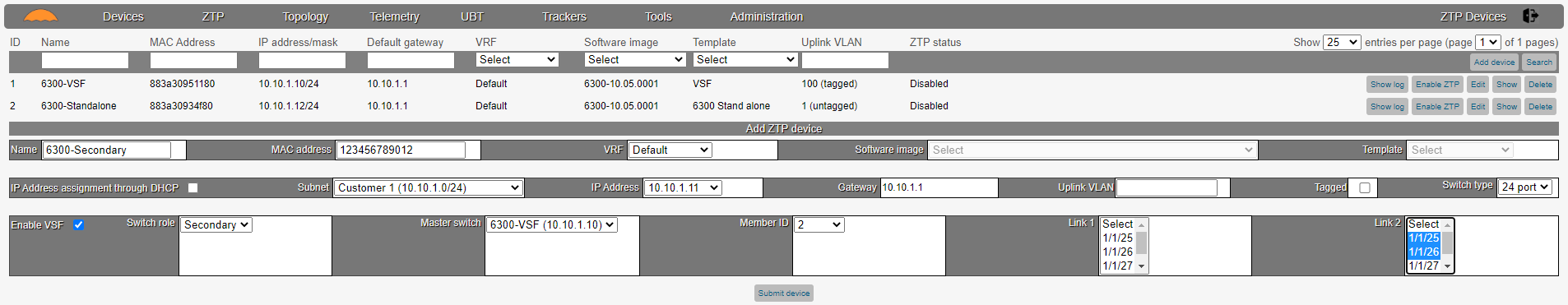
Once you click the “Enable VSF” checkbox, the VSF section is enabled for configuration. The “Switch role” select allows you to set the role of the switch (Master, Secondary or member). If you set the role type to secondary or member, you have to assign this switch to a master switch (which is the next select field). The member ID is only required for secondary or member switches, and in the “Switch type” select field, you have to select whether this is a 24 port or 48 port switch. This is needed because the app needs to know the port numbers for the VSF links. Let’s configure this switch as master switch, it is a 48 port switch, and port 49 and 50 are the VSF ports (link 1) to a second switch.



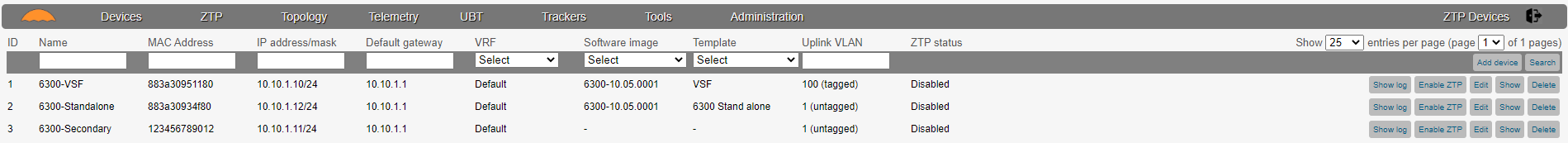
Now, let’s submit the changes and you can see this switch in the list.



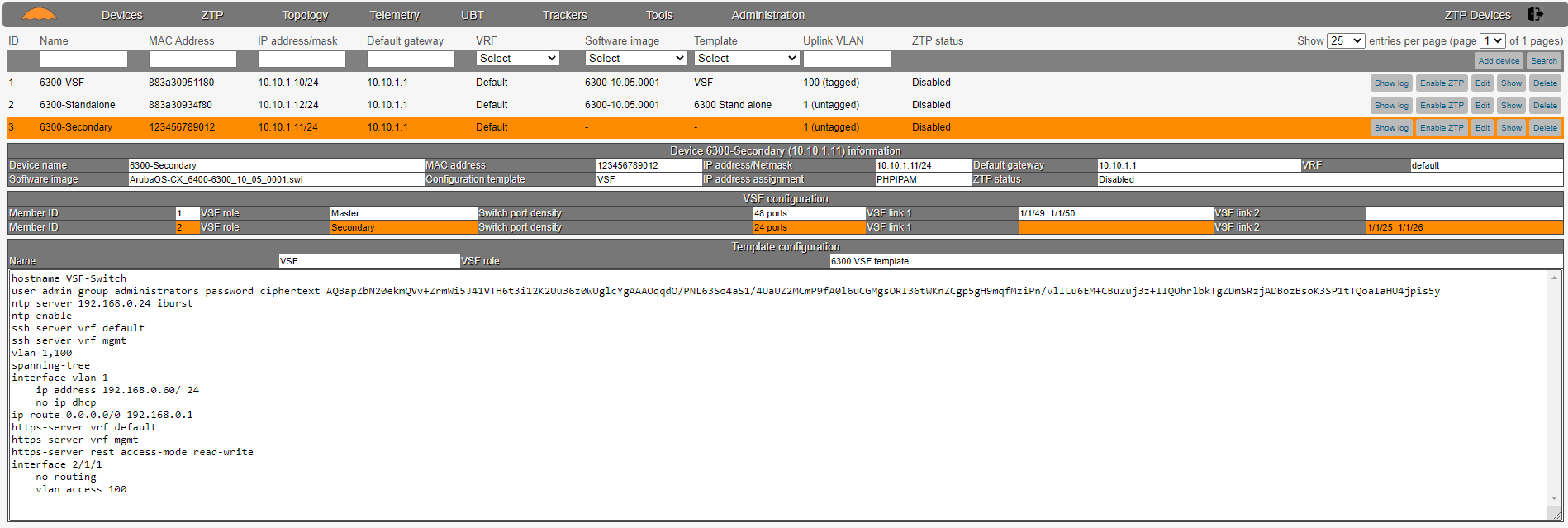
Now, let’s add a second switch and configure this switch as secondary member of switch 123456789012. Notice what happens when you enable VSF and set the switch role to secondary. The “Software image” and “Template” select fields are now disabled. In the “Master switch” select field, you can now select the master switch.



Select the “Member ID”, “Switch type” and assign the interfaces to the VSF link (Link 2). Submit the device.

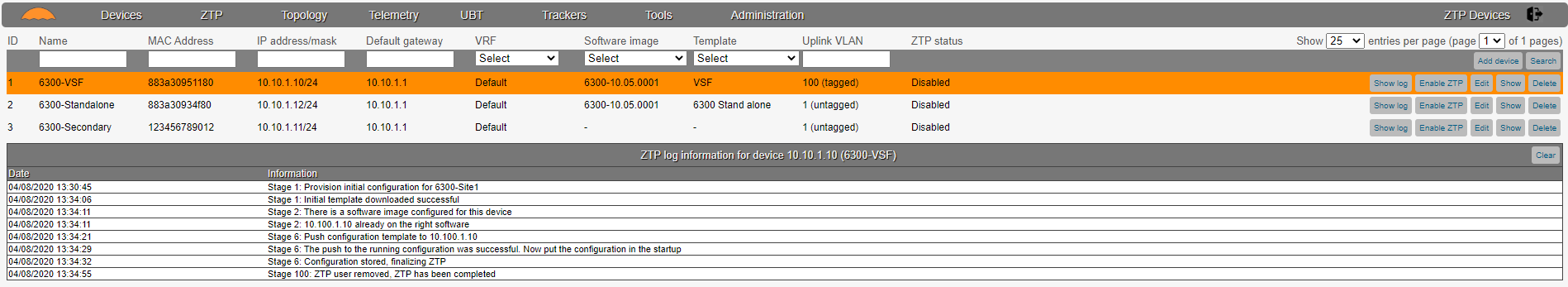


The “Show” button shows you the configuration of the ZTP device, if you click on one of the VSF devices, you will also see the full VSF configuration.



When you enable ZTP on one or more devices you will get a live update of the status in the “ZTP Status” column.

In addition, when you click on the “Show log” button, you can also see the history and live status of the ZTP process.



**Final note, but very important**

For ZTP on a VSF it is required that all member switches have one of their data ports (not the VSF ports) or the management interface (depending whether ZTP takes place from the default or mgmt. VRF) connected to the master switch. Once the VSF ports are configured on the master, this will disable all data communication on these ports. The VSF members require a data connection, hence this requirement. Once the ZTP process has been completed, the data cables can be removed and normal VSF operation is accomplished.

