MAB lists are used for devices that can't use certificates to authenticate using wired 802.1x via Cisco ISE.

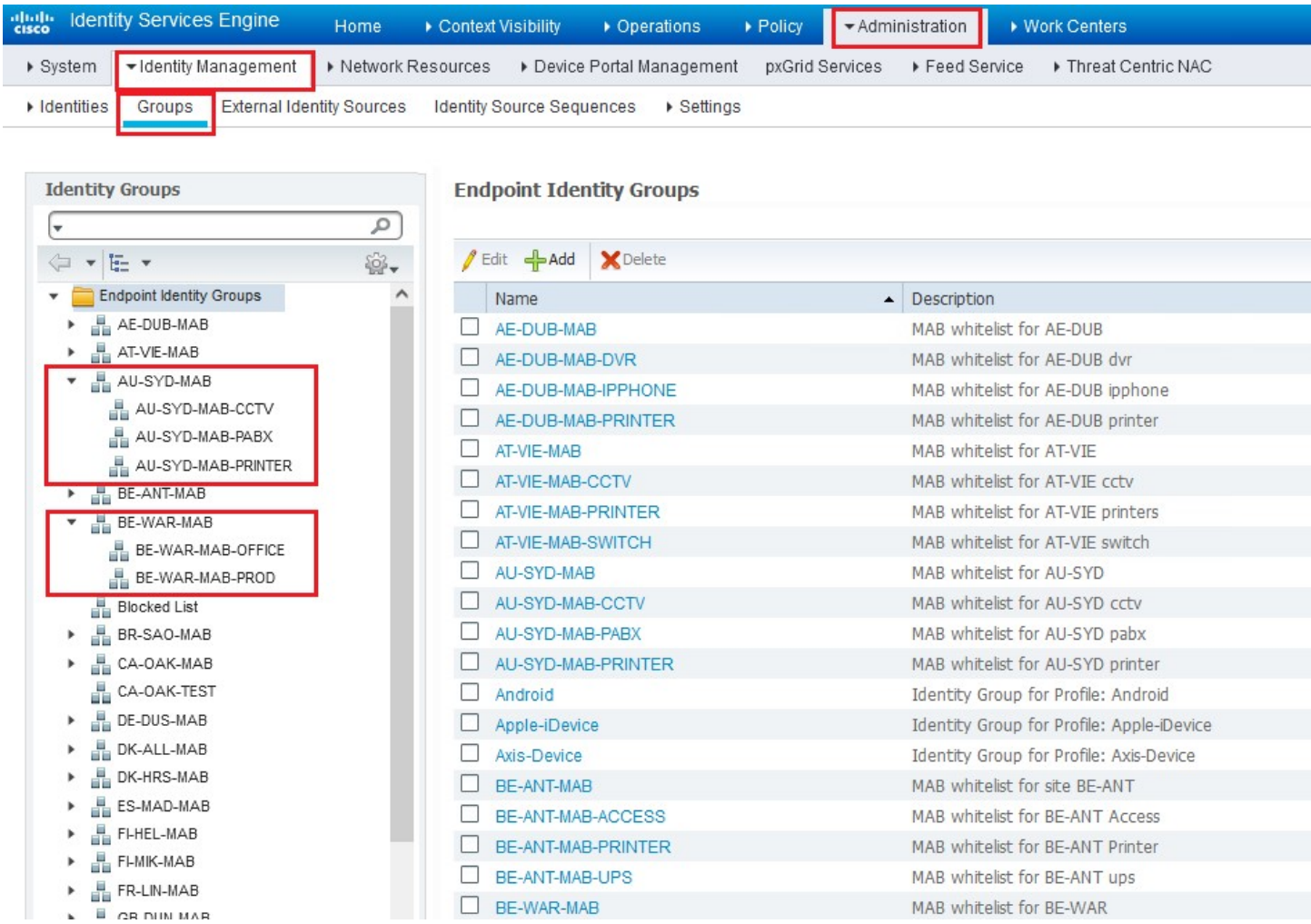
The MAB lists have a standard that needs to be followed. If a device do not fit in any group or if MHC requests a new group, this should be sent in to us as a separate ticket to change.

The standards at the time of writing are:
Global: #SITECODE#-MAB
Printers: #SITECODE#-MAB-PRINTER
Phones: #SITECODE#-MAB-IPPHONE
CCTV: #SITECODE#-MAB-CCTV
Other IoT: #SITECODE#-MAB-IOT
UPS: #SITECODE#-MAB-UPS
Factory sites:
Office: #SITECODE#-MAB-OFFICE
Production: #SITECODE#-MAB-PROD

Where #SITECODE# is to be replaced with each site. (example: MY-KUL-MAB-OFFICE.)

NOTE: At the time of writing, production equipment will not be added to MAB. So if a ticket is sent in with production equipment being blocked by 802.1x, the 802.1x should be removed from the switchport and a description added to the port describing what is connected. (Example: Prod. PLC)

The MAB lists are located in Cisco ISE, at **Administration > Identity Management > Groups**



Here are all the MAB groups that are used. The structure is first **Site**, and then what **type of device**. (As seen on the expanded AU-SYD and BE-WAR)
Currently the groups are only used for granting access, and it does not do any difference on site. But this is for future use.

mac addresses can be added in two ways. Either manually on each group, or imported as a CSV file. importing a CSV is the recommended way, as it can be somewhat cumbersome to add manually. Also ISE needs to know about the mac address in that case.

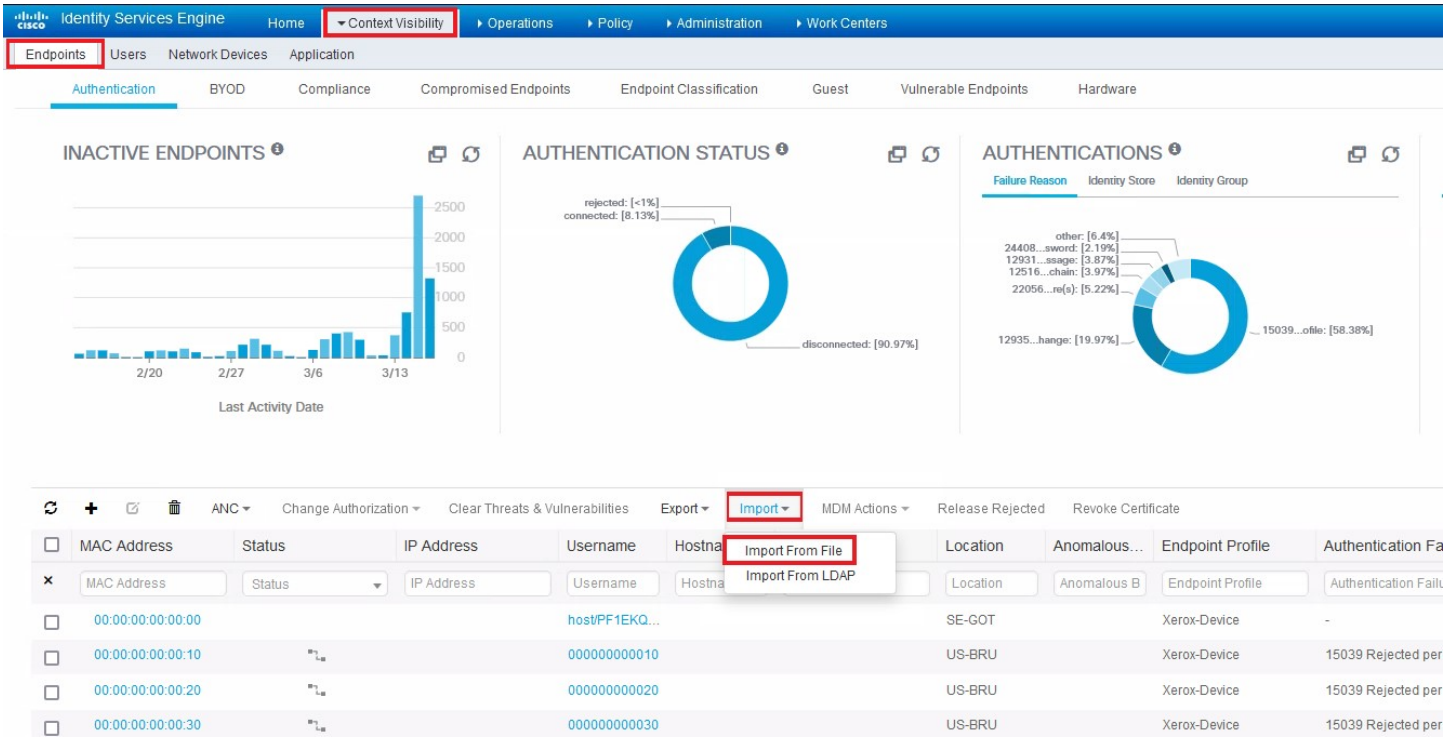
When importing an CSV, there is a template to be used.
NOTE: ISE can display errors with CSVs edited in Excel, so edit them in a text editor to make sure they are clean.
The template looks the following:
MACAddress,EndPointPolicy,IdentityGroup,Description,Location

So in a text editor, add all the fields with commas to separate and one row per device.
For example:
MACAddress,EndPointPolicy,IdentityGroup,Description,Location
00:D0:24:13:BF:82,Unknown,BE-WAR-MAB-OFFICE,,BE-WAR

5C:62:5A:25:F0:DB,Canon-Device,BE-WAR-MAB-OFFICE,BE-WAR,Canon TM-305
34:9F:7B:57:96:0D,Canon-Device,BE-WAR-MAB-OFFICE,BE-WAR,Printer: Canon iR-ADV C5840
00:0E:C4:D1:2E:7C,Unknown,BE-WAR-MAB-PROD,BE-WAR,Screensoft mini PC - communication screen

Mac address = The mac address of the device.
EndPointPolicy = This is ISEs identification of the device. If it is unknown, type unknown or leave blank. (just type two commas ,, to leave it blank.)
IdentityGroup = MAB group.
Description = A short description of the device, this should MHC provide.
Location = Site where it is connected.

To import, go to **Context Visibility > Endpoints.**



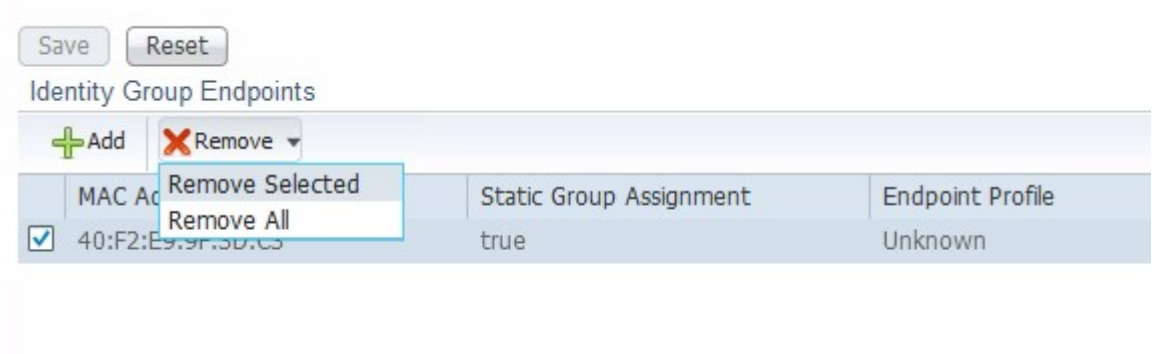
This is where ISE stores all endpoints and also shows the status of the endpoint, if it is associated to a MAB group etc.
If the device is listed here, it can be manually added to the group.
But to add using a CSV, click on **Import** and then **Import From File.**
Upload the CSV and click **Submit.** A template can also be generated from here.
ISE will display an error if there was something wrong with the file. Otherwise you should see a success message and the device can now be viewed in the MAB group.

Edit a mac address

To edit a mac address, use the CSV template import. There is no option to change details in the mab group.

Remove a mac address

Navigate to the mab group (under **Administration > Identity Management > Groups)** where you want to delete a mac address.



NOTE! If more mac addreses are to be removed, refer to SOP8631.

Remove 802.1x on a switchport

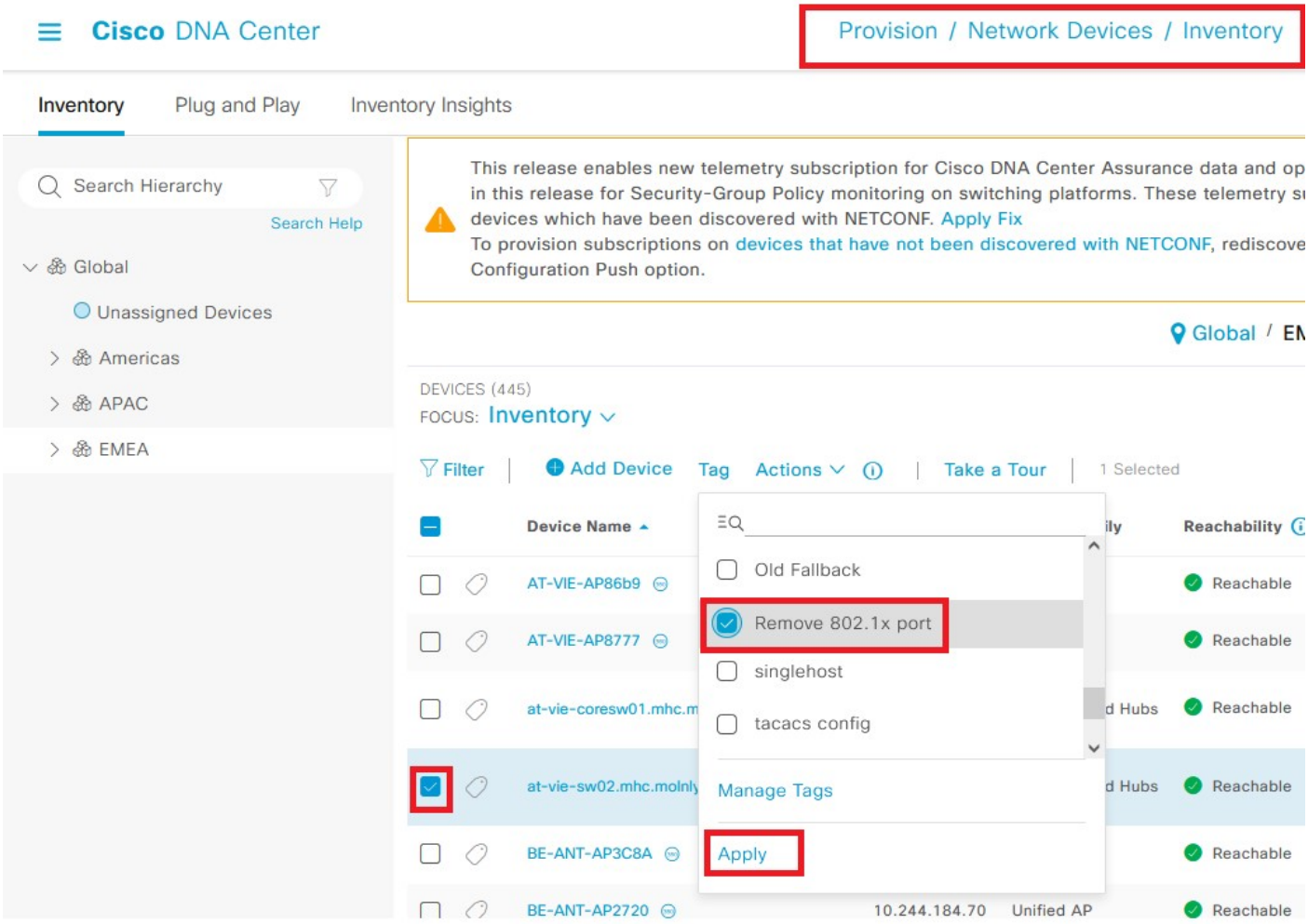
If 802.1x configuration is to be removed from a switchport, for example if a production device is getting denied access on a 802.1x port, there is a template in DNA-Center that does this.
The configuration that will be removed are:

authentication open
authentication order
authentication priority
authentication port-control
authentication periodic
authentication timer reauthenticate
access-session control-direction
access-session host-mode
access-session port-control
mab
dot1x pae
dot1x timeout tx-period
dot1x max-reauth-req
service-policy type control subscriber
ip access-group MONITOR-ALLOW-ALL in

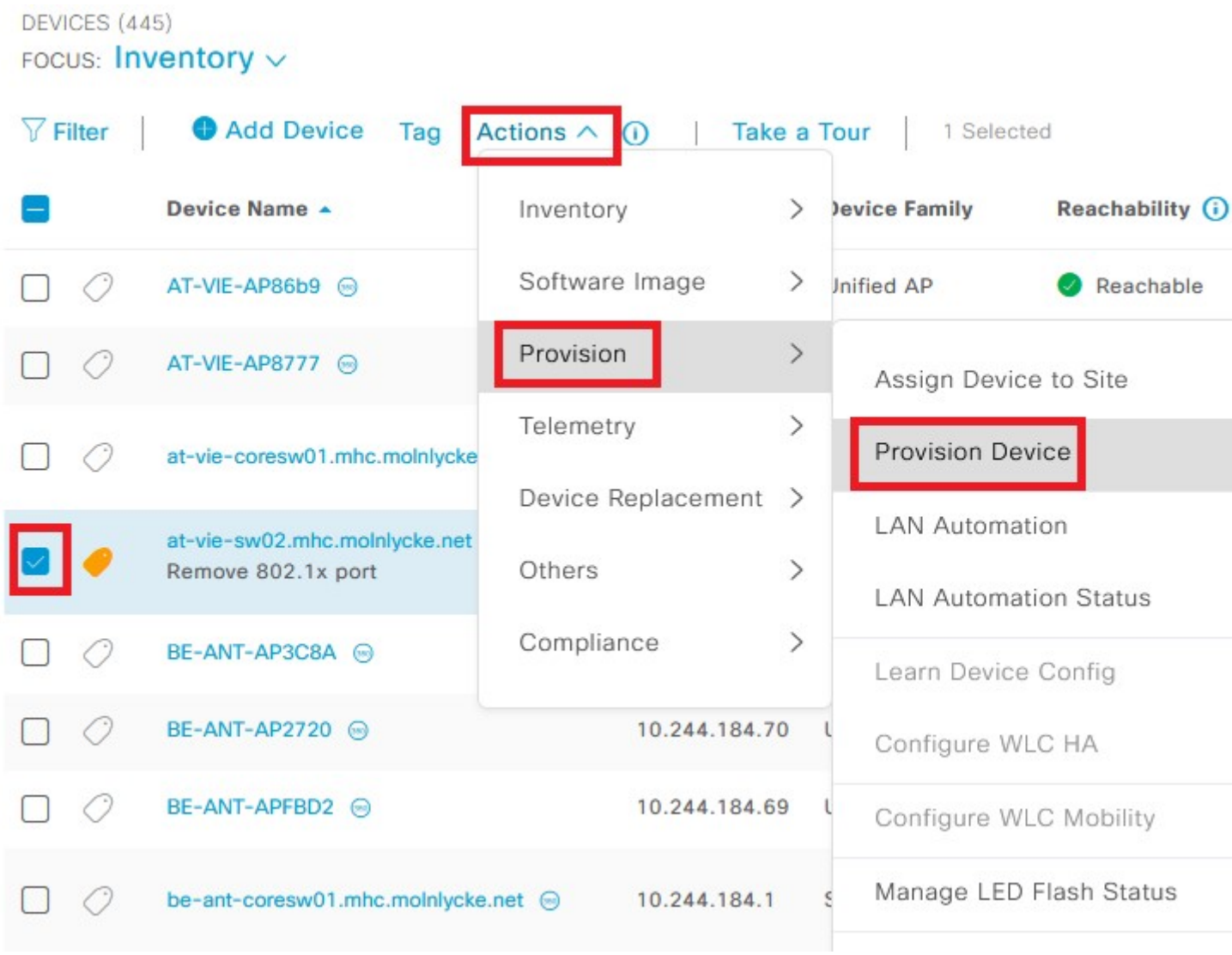
All new config is using ibns 2.0 (access-session) and not ibns 1.0 (authentication), but we have both in the config in case there is an old switch with ibns 1.0

Login to dnacenter.mhc.molnlycke.net with candi credentials.

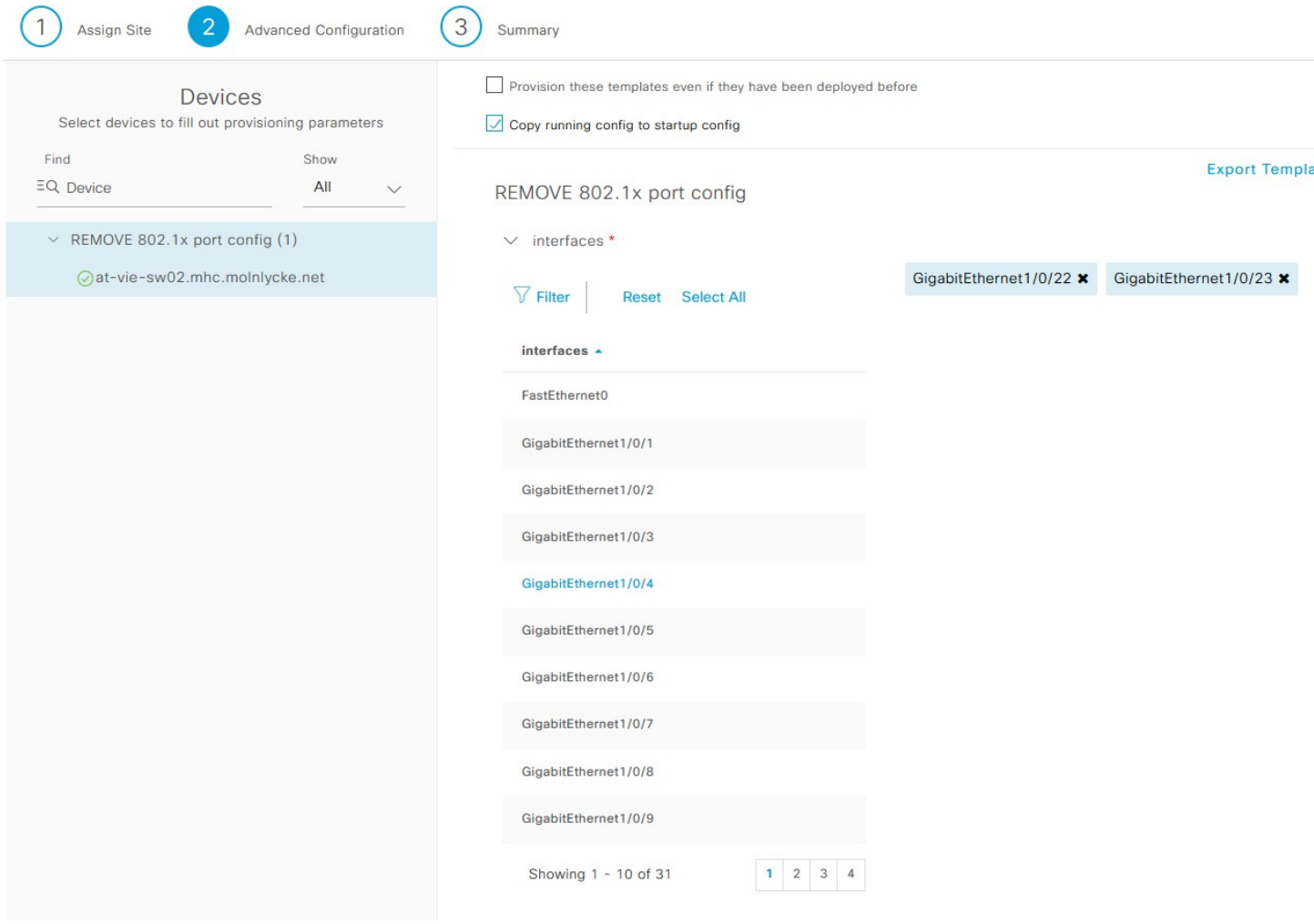
Navigate to **Provision > Inventory** and select the switch you are going to remove the port on.
Click on **Tag**, and select **"Remove 802.1x port"** and click **Apply.**



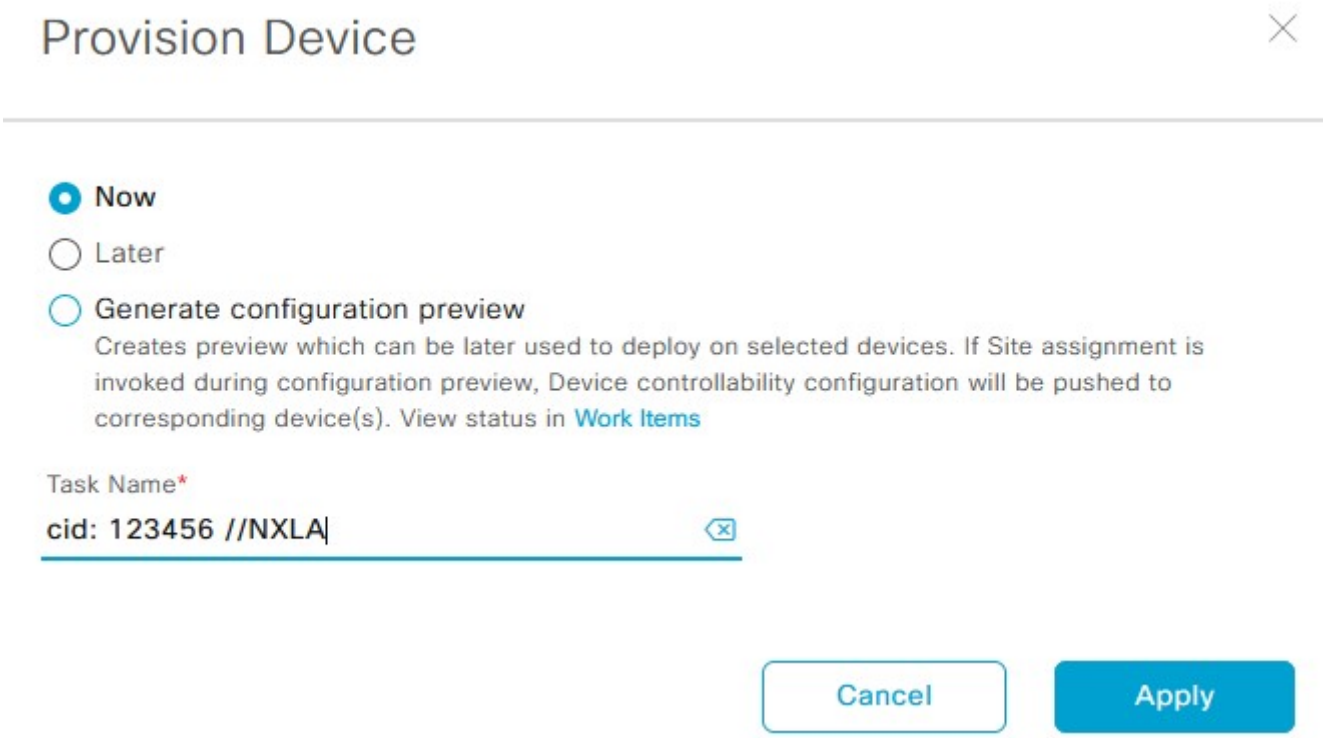
Select the switch once more, and click on **Actions > Provision > Provision device.**



Expand the **REMOVE 802.1x port config** to the left, select the switch and then select the port(s) that should not have 802.1x.



Click **Next,** and then **Deploy.**
Leave it at **Now** if you want to push it out immediately, otherwise click on **Later** to schedule.
In the task name, write in the ticket ID along with a signature. See below for example.



Click **Apply** to push out the configuration.
To view status, go to **Activities > Tasks.** If it is still In Progress you might need to refresh.
Wait for it to be either **Success** or **Failed**, if it is Failed verify what went wrong by clicking on the task name and **See Details.**

Also verify in the switchconfig by connecting with ssh to the switch or run a show command via DNA-Center to make sure the config is removed.