

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**

Identity Services Engine Home Context Visibility Operations Policy **Administration** Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

Endpoint Identity Groups

- AE-DUB-MAB
- AT-VIE-MAB
- AU-SYD-MAB**
 - AU-SYD-MAB-CCTV
 - AU-SYD-MAB-PABX
 - AU-SYD-MAB-PRINTER
- BE-ANT-MAB
- BE-WAR-MAB**
 - BE-WAR-MAB-OFFICE
 - BE-WAR-MAB-PROD
- Blocked List
- BR-SAO-MAB
- CA-OAK-MAB
- CA-OAK-TEST
- DE-DUS-MAB
- DK-ALL-MAB
- DK-HRS-MAB
- ES-MAD-MAB
- FI-HEL-MAB
- FI-MIK-MAB
- FR-LIN-MAB
- GR-DUM-MAB

Endpoint Identity Groups

Edit Add Delete

Name	Description
<input type="checkbox"/> AE-DUB-MAB	MAB whitelist for AE-DUB
<input type="checkbox"/> AE-DUB-MAB-DVR	MAB whitelist for AE-DUB dvr
<input type="checkbox"/> AE-DUB-MAB-IPPHONE	MAB whitelist for AE-DUB iphone
<input type="checkbox"/> AE-DUB-MAB-PRINTER	MAB whitelist for AE-DUB printer
<input type="checkbox"/> AT-VIE-MAB	MAB whitelist for AT-VIE
<input type="checkbox"/> AT-VIE-MAB-CCTV	MAB whitelist for AT-VIE cctv
<input type="checkbox"/> AT-VIE-MAB-PRINTER	MAB whitelist for AT-VIE printers
<input type="checkbox"/> AT-VIE-MAB-SWITCH	MAB whitelist for AT-VIE switch
<input type="checkbox"/> AU-SYD-MAB	MAB whitelist for AU-SYD
<input type="checkbox"/> AU-SYD-MAB-CCTV	MAB whitelist for AU-SYD cctv
<input type="checkbox"/> AU-SYD-MAB-PABX	MAB whitelist for AU-SYD pabx
<input type="checkbox"/> AU-SYD-MAB-PRINTER	MAB whitelist for AU-SYD printer
<input type="checkbox"/> Android	Identity Group for Profile: Android
<input type="checkbox"/> Apple-iDevice	Identity Group for Profile: Apple-iDevice
<input type="checkbox"/> Axis-Device	Identity Group for Profile: Axis-Device
<input type="checkbox"/> BE-ANT-MAB	MAB whitelist for site BE-ANT
<input type="checkbox"/> BE-ANT-MAB-ACCESS	MAB whitelist for BE-ANT Access
<input type="checkbox"/> BE-ANT-MAB-PRINTER	MAB whitelist for BE-ANT Printer
<input type="checkbox"/> BE-ANT-MAB-UPS	MAB whitelist for BE-ANT ups
<input type="checkbox"/> BE-WAR-MAB	MAB whitelist for BE-WAR

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.

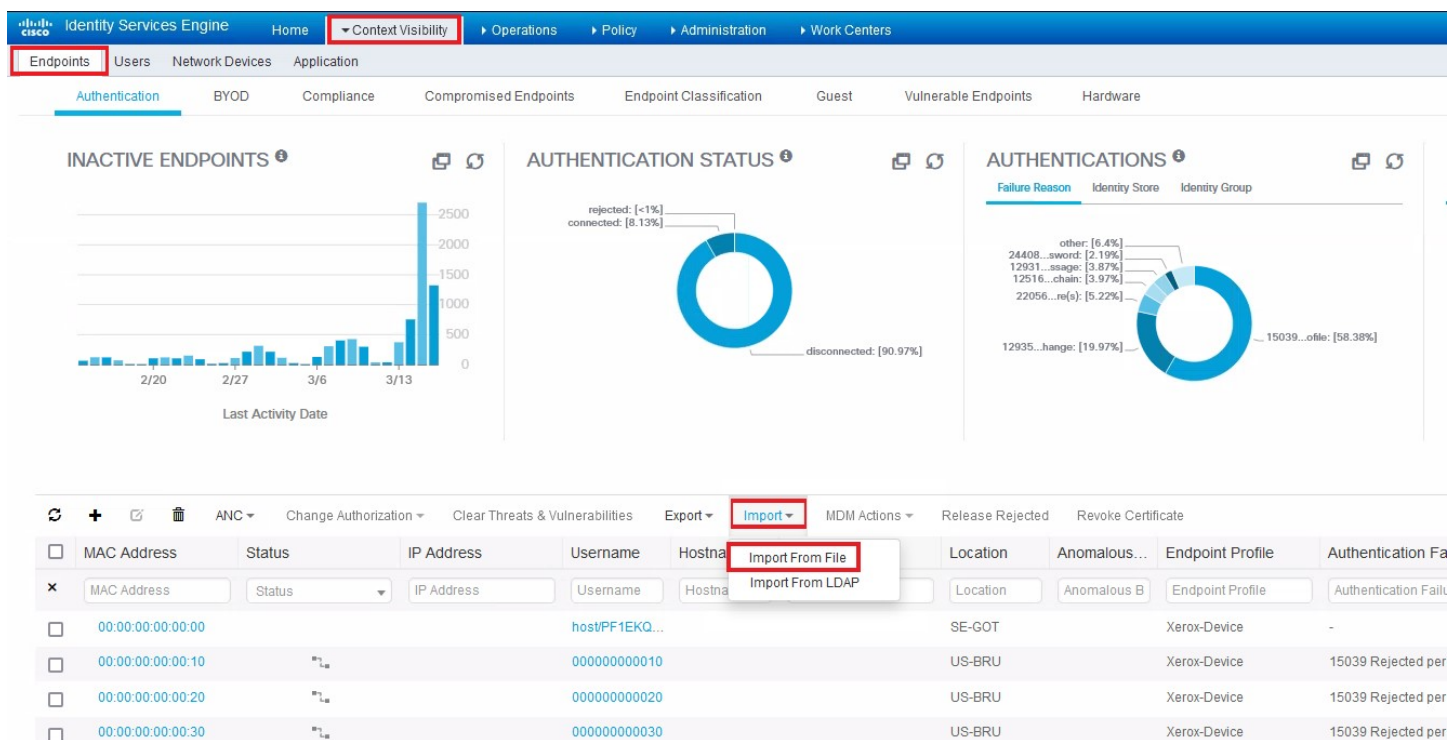
EndPointPolicy = This is ISEs identification of the device. If it is unknown, type unknown or leave blank.
(just type two commas ,, to leave it blank.)

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.

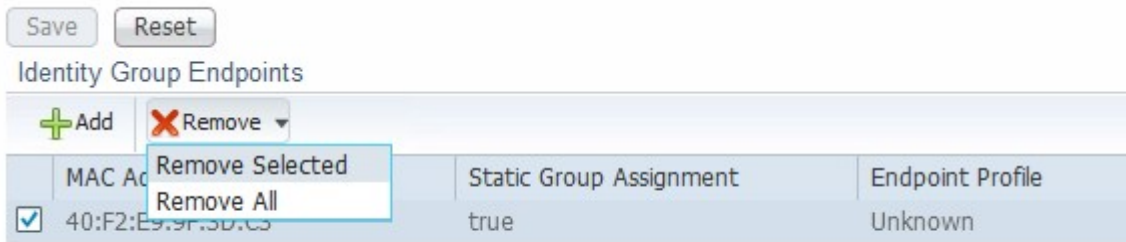
ISE will display an error if there was something wrong with the file. Otherwise you should see a success message and the device can now be viewed in the MAB group.

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 addresses 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**.

Inventory Plug and Play Inventory Insights

Search Hierarchy

Search Help

Global

Unassigned Devices

> Americas

> APAC

> EMEA



This release enables new telemetry subscription for Cisco DNA Center Assurance data and op in this release for Security-Group Policy monitoring on switching platforms. These telemetry s devices which have been discovered with NETCONF. [Apply Fix](#)
To provision subscriptions on [devices that have not been discovered with NETCONF](#), rediscover Configuration Push option.

Global / EN

DEVICES (445)

FOCUS: Inventory

Filter

Add Device

Tag

Actions

i

Take a Tour

1 Selected

	Device Name		Reachability
<input type="checkbox"/>	AT-VIE-AP86b9	<input type="checkbox"/> Old Fallback	Reachable
<input type="checkbox"/>	AT-VIE-AP8777	<input checked="" type="checkbox"/> Remove 802.1x port	Reachable
<input type="checkbox"/>	at-vie-coresw01.mhc.m	<input type="checkbox"/> singlehost	Reachable
<input type="checkbox"/>	at-vie-sw02.mhc.moln	<input type="checkbox"/> tacacs config	Reachable
<input checked="" type="checkbox"/>	BE-ANT-AP3C8A	Manage Tags	Reachable
<input type="checkbox"/>	BE-ANT-AP2720	Apply	Reachable

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

DEVICES (445)

FOCUS: **Inventory** ▾

Filter | Add Device Tag **Actions** ^ ⓘ | Take a Tour | 1 Selected

	Device Name ▴		Device Family	Reachability ⓘ
<input type="checkbox"/>	AT-VIE-AP86b9 ⓘ		Unified AP	✓ Reachable
<input type="checkbox"/>	AT-VIE-AP8777 ⓘ			
<input type="checkbox"/>	at-vie-coresw01.mhc.molnlycke			
<input checked="" type="checkbox"/>	at-vie-sw02.mhc.molnlycke.net Remove 802.1x port			
<input type="checkbox"/>	BE-ANT-AP3C8A ⓘ			
<input type="checkbox"/>	BE-ANT-AP2720 ⓘ	10.244.184.70		
<input type="checkbox"/>	BE-ANT-APFBD2 ⓘ	10.244.184.69		
<input type="checkbox"/>	be-ant-coresw01.mhc.molnlycke.net ⓘ	10.244.184.1		

Inventory >

Software Image >

Provision >

Telemetry >

Device Replacement >

Others >

Compliance >

Assign Device to Site

Provision Device

LAN Automation

LAN Automation Status

Learn Device Config

Configure WLC HA

Configure WLC Mobility

Manage LED Flash Status

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.

Devices

Select devices to fill out provisioning parameters

Find
Show

Device
All

REMOVE 802.1x port config (1)

at-vie-sw02.mhc.molnlycke.net

☐ Provision these templates even if they have been deployed before
☒ Copy running config to startup config

REMOVE 802.1x port config

interfaces *

Filter
Reset
Select All

interfaces

FastEthernet0

GigabitEthernet1/0/1

GigabitEthernet1/0/2

GigabitEthernet1/0/3

GigabitEthernet1/0/4

GigabitEthernet1/0/5

GigabitEthernet1/0/6

GigabitEthernet1/0/7

GigabitEthernet1/0/8

GigabitEthernet1/0/9

Showing 1 - 10 of 31

1
2
3
4

GigabitEthernet1/0/22 ✕

GigabitEthernet1/0/23 ✕

Export Template

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.

Provision Device



☒ **Now**

☐ Later

☐ **Generate configuration preview**

Creates preview which can be later used to deploy on selected devices. If Site assignment is invoked during configuration preview, Device controllability configuration will be pushed to corresponding device(s). View status in [Work Items](#)

Task Name*

cid: 123456 //NXLA|



Cancel

Apply

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.