Meraki & Freeradius for Lab testing

Guide to setup Freeradius on Raspberry for using as a AAA server for Meraki.
Because Raspberry is running a Debian based OS, this guide should work on all Debian based systems.

Content

Testmatrix:

	MR55 (27.5)	MS350 (14.4)	MS390 (14.5)	MX65 (15.38)
MAB	√	√	√	√
MAB + VLAN	√	√	√	na
MAB + GroupPolicy	√	na	na	na
MAB + GroupPolicyACL	na	√	na	na
MAB + VLAN + GroupPolicyACL	na	√	na	na
MAB + SGT (AdaptivePolicy)	√	na	√	na
802.1X	√	√	√	√
802.1X + VLAN	√	√	√	na
802.1X + GroupPolicy	√	na	na	na
802.1X + GroupPolicyACL	na	√	na	na
802.1X + VLAN + GrouPolicyACL	na	√	na	na
802.1X + SGT (AdaptivePolicy)	√	na	√	na
				na
iPSK	√	na	na	na
iPSK + VLAN	√	na	na	na
iPSK + GroupPolicy	√	na	na	na
iPSK + SGT (AdaptivePolicy)	√	na	na	na

na = not available , not tested

Raspberry Pi Setup

For setting up your Raspberry Pi without mouse and keyboard have a look @:
https://github.com/thomas-sterber/Setup_Raspberry_without_mouse_and_keyboard

Install Freeradius

```
#sudo apt-get update
#sudo apt-get dist-upgrade
#sudo apt-get install freeradius
#sudo apt-get install freeradius-utils
```

Freeradius start/stop/autostart , Debug mode

Check Freeradius service

```
#sudo service freeradius status
#pgrep freeradius
```

Stop service also disable autostart after boot

```
#sudo service freeradius stop
```

Start service also enable autostart after reboot

```
#sudo service freeradius start
```

Start in Debug Mode

```
# sudo service freeradius stop
# sudo freeradius -X
```

Basic Freeradius Configuration

ssh to the Raspberry and login. (pi/meraki123)

>> Backup/move/clear orgiginal configs files

```
#mkdir freeradius_backup
#cd freeradius_backup
#sudo su
#cp /etc/freeradius/3.0/users .
#> /etc/freeradius/3.0/users
#cp /etc/freeradius/3.0/clients.conf .
#> /etc/freeradius/3.0/clients.conf
#cp /etc/freeradius/3.0/radiusd.conf .
#cp /etc/freeradius/3.0/mods-available/eap .
#exit
```

>> modify config-files

```
#sudo vim /etc/freeradius/3.0/mods-available/eap
```

change two time 'use_tunneled_reply' to 'yes'
(EAP-TTLS section and EAP-PEAP section)
This allows to configure the radius attributes direct in 'users'

```
use_tunneled_reply = yes
```

```
#sudo vim /etc/freeradius/3.0/radiusd.conf
```

change 'name = freeradius' to 'name = meraki-freeradius'

Test your Freeradius Server

```
#sudo vim /etc/freeradius/3.0/clients.conf

        client localhost {
             ipaddr = 127.0.0.1
             secret  = secret123
             }

#sudo vim /etc/freeradius/3.0/users

        thomas                 Cleartext-Password := "sterber"



#sudo freeradius -X      (terminal 1)
#radtest thomas sterber 127.0.0.1 0 secret123      (terminal 2)
        (user) (pwd) (server ip) (NAS Port) (secret)
```

Freeradius and Dashboard Configs

Configure Freeradius 'clients.conf'

```
#sudo vim /etc/freeradius/3.0/clients.conf
```

Trust all incoming requests (best practice for Lab environments)

```
client all {
        ipaddr          = 0.0.0.0/0
        secret          = secret123
}
```

Localhost

```
client localhost {
        ipaddr          = 127.0.0.1
        secret          = secret123
        }
```

Dedicated device

```
client mr56 {
        ipaddr          = 172.16.1.4
        secret          = secret123
        }
```

Network

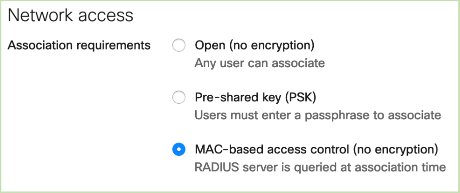
```
client net_172.16 {
        ipaddr          = 172.16.0.0/16
        secret          = secret123
        }
```

Configure MAB

>>Freeradius 'users' Config for MR, MS and MX

```
a45046d55355                    Cleartext-Password := "a45046d55355"
...
```

>>Meraki Dashboard Wifi Config



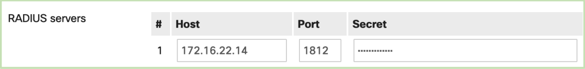
Network access

Association requirements

○ Open (no encryption)
Any user can associate

○ Pre-shared key (PSK)
Users must enter a passphrase to associate

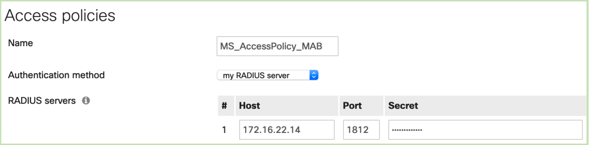
● MAC-based access control (no encryption)
RADIUS server is queried at association time



RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	············

>>Meraki Dashboard Switching Config



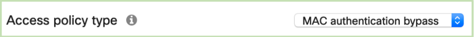
Access policies

Name: MS_AccessPolicy_MAB

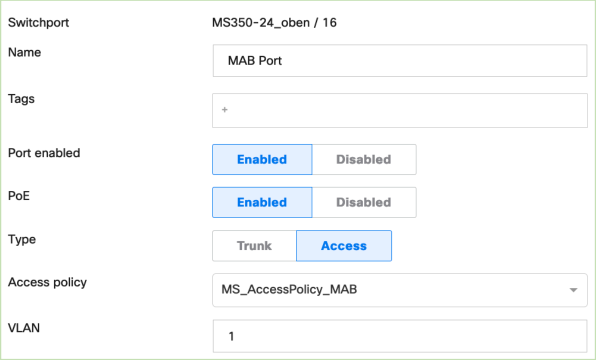
Authentication method: my RADIUS server

RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	············

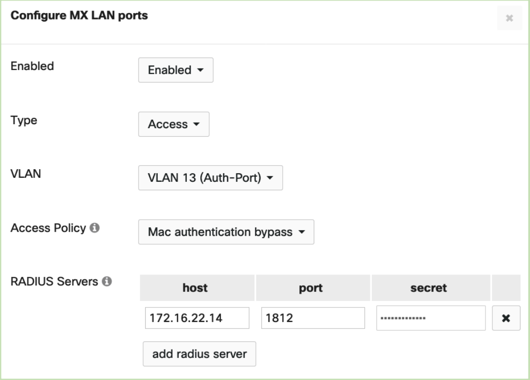


Access policy type: MAC authentication bypass



Switchport	MS350-24_oben / 16
Name	MAB Port
Tags	+
Port enabled	[✓ Enabled] Disabled
PoE	[✓ Enabled] Disabled
Type	Trunk [✓ Access]
Access policy	MS_AccessPolicy_MAB
VLAN	1

>>Meraki Dashboard MX Config



Configure MX LAN ports

Enabled	Enabled
Type	Access
VLAN	VLAN 13 (Auth-Port)
Access Policy	Mac authentication bypass

RADIUS Servers

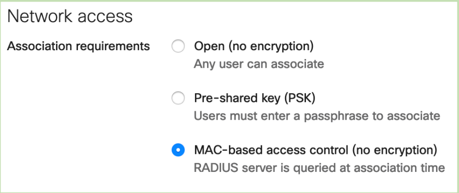
host	port	secret
172.16.22.14	1812	·············

Configure MAB + VLAN assignment

>>Freeradius 'users' Config for MR and MS for VLAN 10

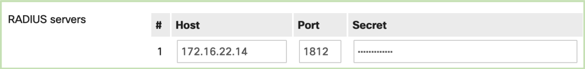
```
9829a642667c            Cleartext-Password := "9829a642667c"
                        Tunnel-Medium-Type = 6,
                        Tunnel-Private-Group-ID = 10,
                        Tunnel-Type = VLAN
```

>>Meraki Dashboard Wifi Config



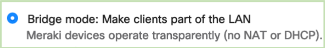
Network access

Association requirements
- ○ Open (no encryption)
  Any user can associate
- ○ Pre-shared key (PSK)
  Users must enter a passphrase to associate
- ● MAC-based access control (no encryption)
  RADIUS server is queried at association time

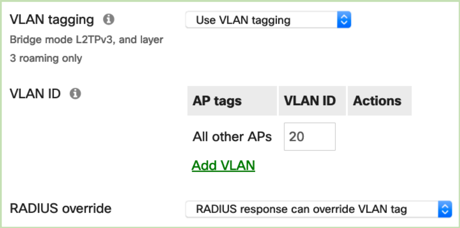


RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	············



● Bridge mode: Make clients part of the LAN
Meraki devices operate transparently (no NAT or DHCP).



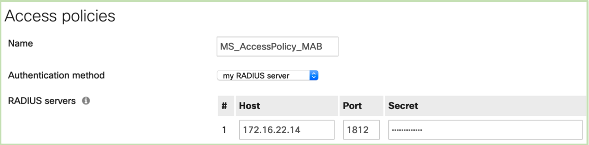
VLAN tagging: Use VLAN tagging
Bridge mode L2TPv3, and layer 3 roaming only

VLAN ID

AP tags	VLAN ID	Actions
All other APs	20	

RADIUS override: RADIUS response can override VLAN tag

>>Meraki Dashboard Switch Config



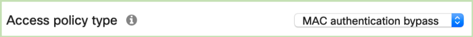
Access policies

Name: MS_AccessPolicy_MAB

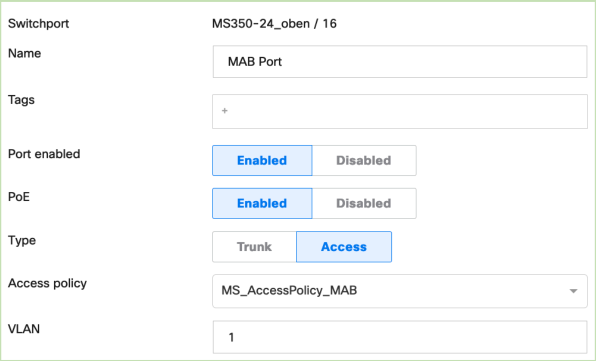
Authentication method: my RADIUS server

RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	············



Access policy type: MAC authentication bypass



Switchport: MS350-24_oben / 16

Name: MAB Port

Tags: +

Port enabled: [✓ Enabled] Disabled

PoE: [✓ Enabled] Disabled

Type: Trunk [✓ Access]

Access policy: MS_AccessPolicy_MAB

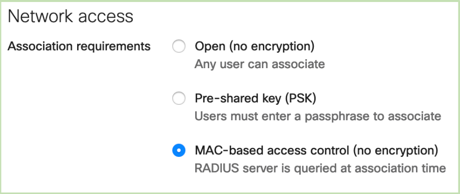
VLAN: 1

Configure MAB + GroupPolicy assignment

>>Freeradius 'users' Config for MR

```
e82a44a133c1                    Cleartext-Password := "e82a44a133c1"
                                Filter-ID := GroupPolicy_01
```

>>Meraki Dashboard Wifi Config



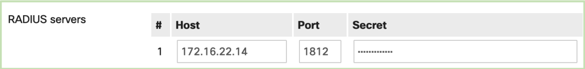
Network access

Association requirements

○ Open (no encryption)
Any user can associate

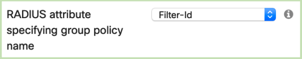
○ Pre-shared key (PSK)
Users must enter a passphrase to associate

● MAC-based access control (no encryption)
RADIUS server is queried at association time

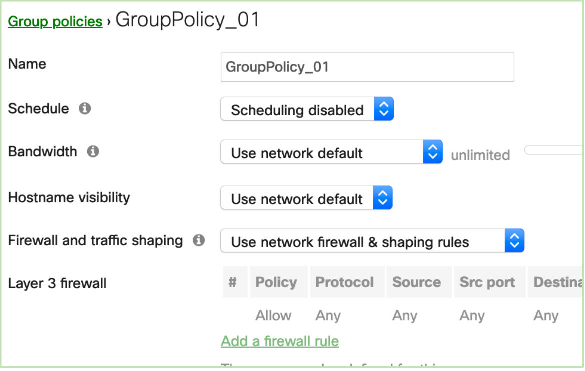


RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	············



RADIUS attribute specifying group policy name: Filter-Id



Group policies › GroupPolicy_01

Name: GroupPolicy_01

Schedule: Scheduling disabled

Bandwidth: Use network default — unlimited

Hostname visibility: Use network default

Firewall and traffic shaping: Use network firewall & shaping rules

Layer 3 firewall

#	Policy	Protocol	Source	Src port	Destina
	Allow	Any	Any	Any	Any

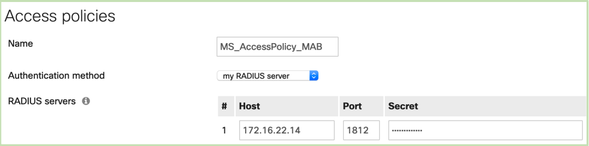
Add a firewall rule

Configure MAB + GroupPolicyACL assignment

>>Freeradius 'users' Config for MS

```
9829a642667c            Cleartext-Password := "9829a642667c"
                        Filter-ID := MSGroupPolicyACL_01
```

>>Meraki Dashboard Switch Config



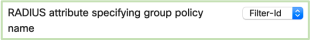
Access policies

Name: MS_AccessPolicy_MAB

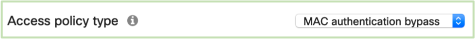
Authentication method: my RADIUS server

RADIUS servers

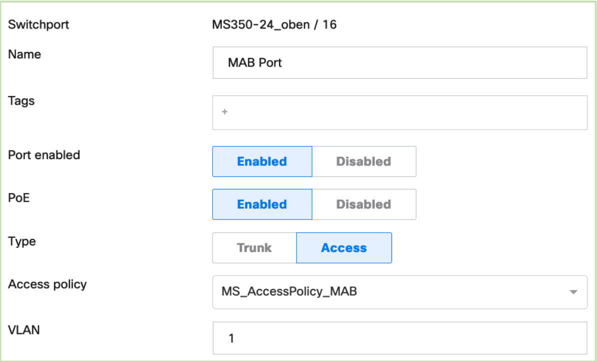
#	Host	Port	Secret
1	172.16.22.14	1812	············



RADIUS attribute specifying group policy name: Filter-Id



Access policy type: MAC authentication bypass



Switchport: MS350-24_oben / 16

Name: MAB Port

Tags: +

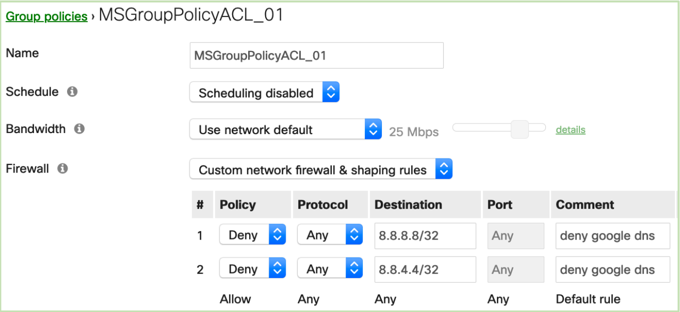
Port enabled: **Enabled** Disabled

PoE: **Enabled** Disabled

Type: Trunk **Access**

Access policy: MS_AccessPolicy_MAB

VLAN: 1



Group policies › MSGroupPolicyACL_01

Name: MSGroupPolicyACL_01

Schedule: Scheduling disabled

Bandwidth: Use network default 25 Mbps details

Firewall: Custom network firewall & shaping rules

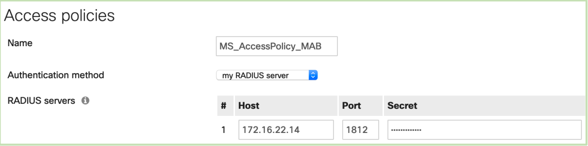
#	Policy	Protocol	Destination	Port	Comment
1	Deny	Any	8.8.8.8/32	Any	deny google dns
2	Deny	Any	8.8.4.4/32	Any	deny google dns
	Allow	Any	Any	Any	Default rule

Configure MAB + VLAN + GroupPolicyACL assignment

>>Freeradius 'users' Config for MS

```
9829a642667c            Cleartext-Password := "9829a642667c"
                        Filter-ID := MSGroupPolicyACL_01,
                        Tunnel-Medium-Type = 6,
                        Tunnel-Private-Group-ID = 10,
                        Tunnel-Type = VLAN
```

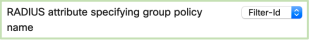
>>Meraki Dashboard Switch Config



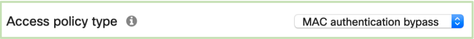
Access policies

Name	MS_AccessPolicy_MAB
Authentication method	my RADIUS server
RADIUS servers	

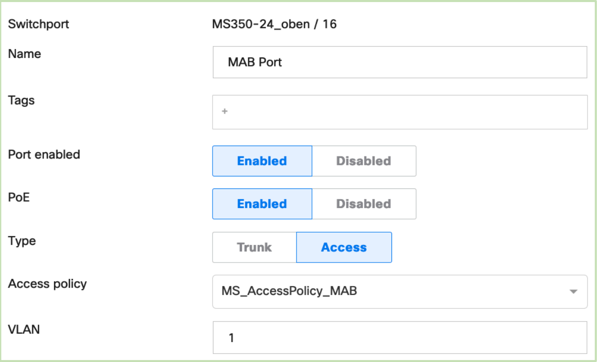
#	Host	Port	Secret
1	172.16.22.14	1812	···········



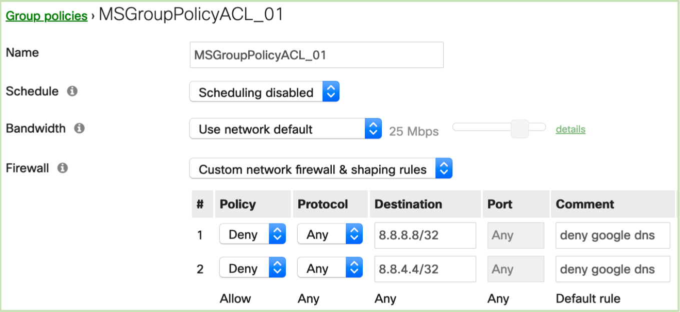
RADIUS attribute specifying group policy name: Filter-Id



Access policy type: MAC authentication bypass



Switchport	MS350-24_oben / 16
Name	MAB Port
Tags	+
Port enabled	[✓ Enabled] Disabled
PoE	[✓ Enabled] Disabled
Type	Trunk [✓ Access]
Access policy	MS_AccessPolicy_MAB
VLAN	1



Group policies › MSGroupPolicyACL_01

Name	MSGroupPolicyACL_01
Schedule	Scheduling disabled
Bandwidth	Use network default 25 Mbps
Firewall	Custom network firewall & shaping rules

#	Policy	Protocol	Destination	Port	Comment
1	Deny	Any	8.8.8.8/32	Any	deny google dns
2	Deny	Any	8.8.4.4/32	Any	deny google dns
	Allow	Any	Any	Any	Default rule

Configure MAB + SGT 100 assignment

For more detail informations regarding SGT , Adaptive Policy, please have a look @

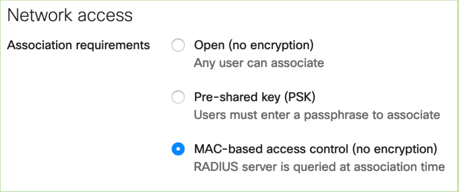
Adaptive Policy MR Config

Adaptive Policy MS Config

>>Freeradius 'users' Config for MS390 and MR Wifi6
(SGT 100 = hex 0064)

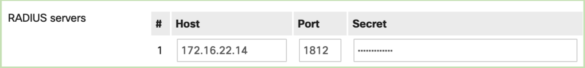
```
9829a642667c            Cleartext-Password := "9829a642667c"
                        Cisco-AVPair = "cts:security-group-tag=0064-00"
```

>>Meraki Dashboard Wifi Config



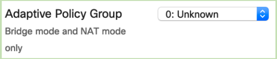
Network access

Association requirements
○ Open (no encryption)
Any user can associate
○ Pre-shared key (PSK)
Users must enter a passphrase to associate
● MAC-based access control (no encryption)
RADIUS server is queried at association time



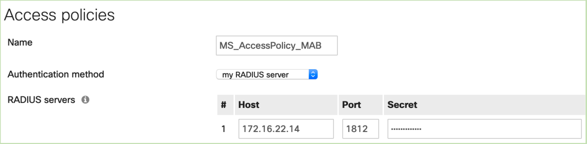
RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	....



Adaptive Policy Group: 0: Unknown
Bridge mode and NAT mode only

>>Meraki Dashboard Switching Config



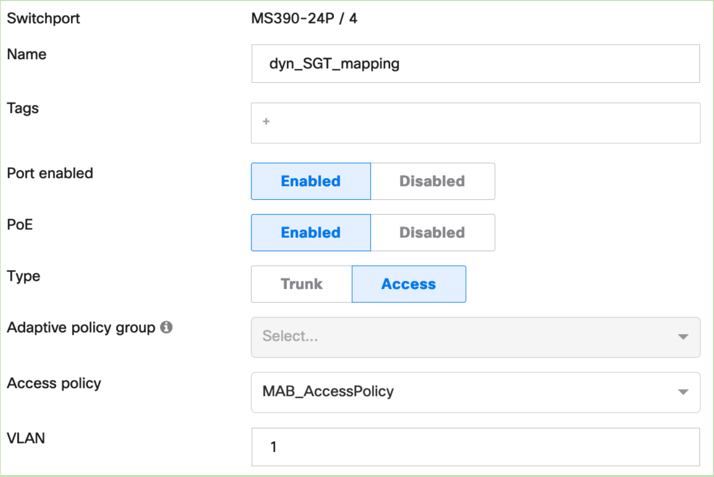
Access policies

Name: MS_AccessPolicy_MAB

Authentication method: my RADIUS server

RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	....



Switchport: MS390-24P / 4

Name: dyn_SGT_mapping

Tags: +

Port enabled: [✓ Enabled] Disabled

PoE: [✓ Enabled] Disabled

Type: Trunk [✓ Access]

Adaptive policy group: Select...

Access policy: MAB_AccessPolicy

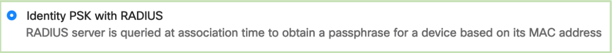
VLAN: 1

Configure iPSK

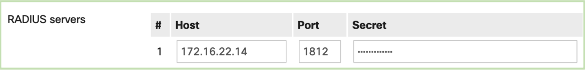
>>Freeradius 'users' Config for MR
(Tunnel-password == pre-shared password , 8 characters min)

```
a45046d55355            Cleartext-Password := "a45046d55355"
                        Tunnel-password = psk12345
```

>>Meraki Dashboard Wifi Config



● Identity PSK with RADIUS
RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address



RADIUS servers

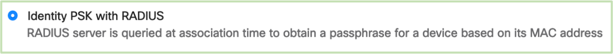
#	Host	Port	Secret
1	172.16.22.14	1812	············

Configure iPSK + VLAN assignment

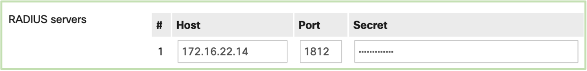
>>Freeradius 'users' Config for MR

```
a45046d55355            Cleartext-Password := "a45046d55355"
                        Tunnel-password = psk12345,
                        Tunnel-Medium-Type = 6,
                        Tunnel-Private-Group-ID = 10,
                        Tunnel-Type = VLAN
```

>>Meraki Dashboard Wifi Config

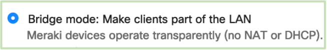


● Identity PSK with RADIUS
RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address

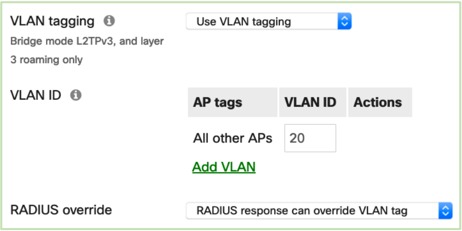


RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	············



● Bridge mode: Make clients part of the LAN
Meraki devices operate transparently (no NAT or DHCP).



VLAN tagging: Use VLAN tagging
Bridge mode L2TPv3, and layer 3 roaming only

VLAN ID

AP tags	VLAN ID	Actions
All other APs	20	

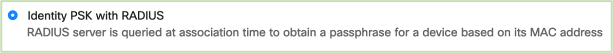
RADIUS override: RADIUS response can override VLAN tag

Configure iPSK + GroupPolicy assignment

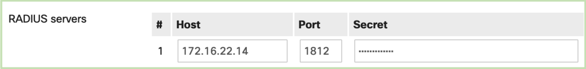
>>Freeradius Config for MR

```
a45046d55355        Cleartext-Password := "a45046d55355"
                            Tunnel-password = psk12345,
                            Filter-ID := GPolicy_A
```

>>Meraki Dashboard Wifi Config

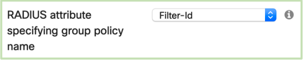


● Identity PSK with RADIUS
RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address

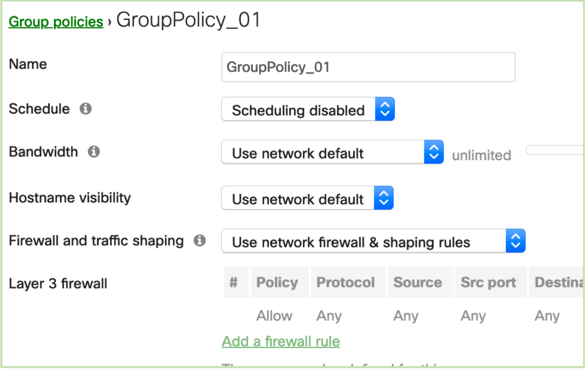


RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	············



RADIUS attribute specifying group policy name: Filter-Id



Group policies › GroupPolicy_01

Name: GroupPolicy_01

Schedule: Scheduling disabled

Bandwidth: Use network default unlimited

Hostname visibility: Use network default

Firewall and traffic shaping: Use network firewall & shaping rules

Layer 3 firewall

#	Policy	Protocol	Source	Src port	Destina
	Allow	Any	Any	Any	Any

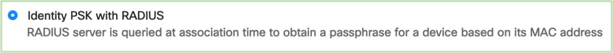
Add a firewall rule

Configure iPSK + SGT (100) assignment

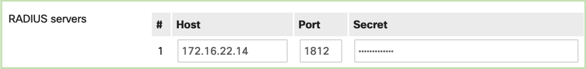
>>Freeradius Config for MR

```
a45046d55355        Cleartext-Password := "a45046d55355"
                            Tunnel-password = psk12345,
                            Cisco-AVPair = "cts:security-group-tag=0064-00"
```

>>Meraki Wifi Config

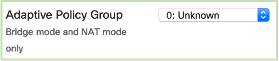


● Identity PSK with RADIUS
RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address



RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	•••••••••••••



Adaptive Policy Group
Bridge mode and NAT mode only

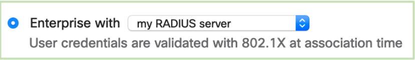
0: Unknown

Configure 802.1X

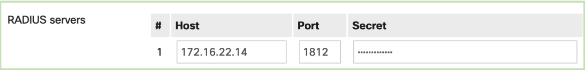
>>Freeradius Config for MR, MS and MX

```
thomas                              Cleartext-Password := "sterber"
```

>>Meraki Dashboard Wifi Config



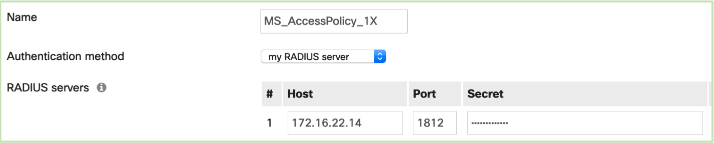
● Enterprise with my RADIUS server
User credentials are validated with 802.1X at association time



RADIUS servers

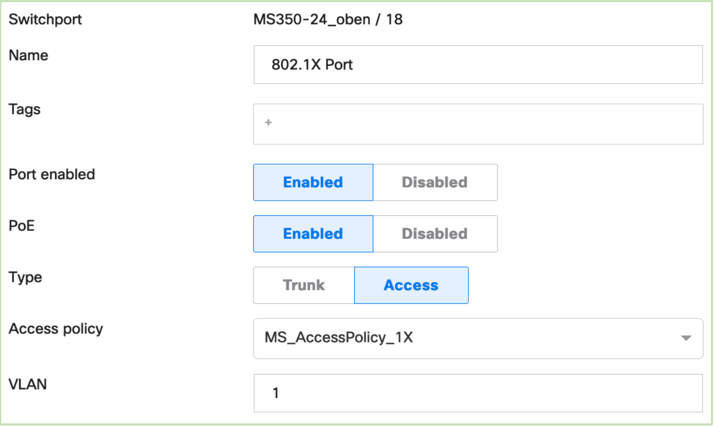
#	Host	Port	Secret
1	172.16.22.14	1812	············

>>Meraki Dashboard Switching Config



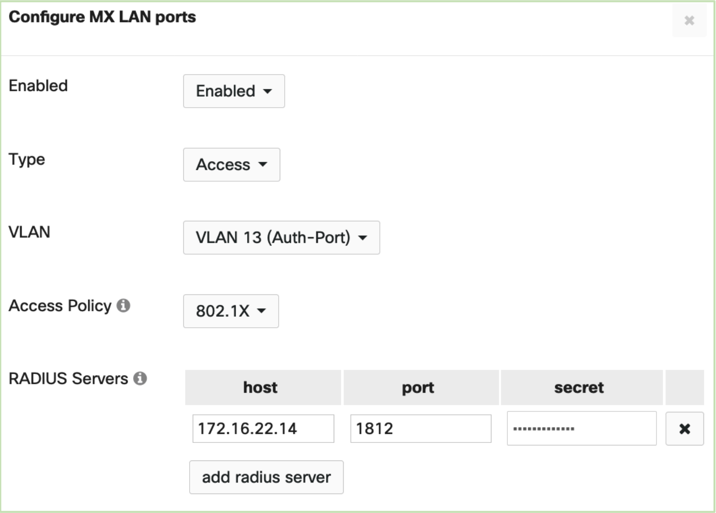
Name	MS_AccessPolicy_1X
Authentication method	my RADIUS server
RADIUS servers	

#	Host	Port	Secret
1	172.16.22.14	1812	············



Switchport	MS350-24_oben / 18
Name	802.1X Port
Tags	+
Port enabled	[✓ Enabled] Disabled
PoE	[✓ Enabled] Disabled
Type	Trunk [✓ Access]
Access policy	MS_AccessPolicy_1X
VLAN	1

>>Meraki Dashboard MX Config



Configure MX LAN ports

Enabled	Enabled
Type	Access
VLAN	VLAN 13 (Auth-Port)
Access Policy	802.1X
RADIUS Servers	

host	port	secret	
172.16.22.14	1812	··············	✖

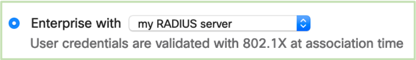
add radius server

Configure 802.1X + VLAN assignment

>>Freeradius Config for MR and MS

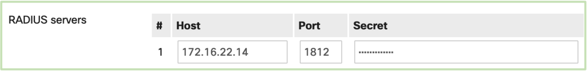
```
thomas          Cleartext-Password := "sterber"
                Tunnel-Medium-Type = 6,
                Tunnel-Private-Group-ID = 10,
                Tunnel-Type = VLAN
```

>>Meraki Dashboard Wifi Config



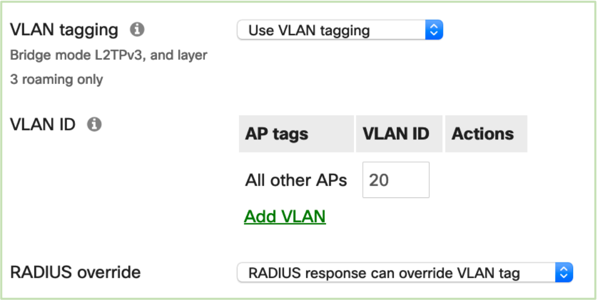
● Enterprise with my RADIUS server

User credentials are validated with 802.1X at association time



RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	············



VLAN tagging: Use VLAN tagging

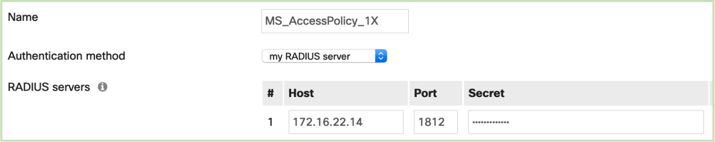
Bridge mode L2TPv3, and layer 3 roaming only

VLAN ID

AP tags	VLAN ID	Actions
All other APs	20	

RADIUS override: RADIUS response can override VLAN tag

>>Meraki Dashboard Switch Config

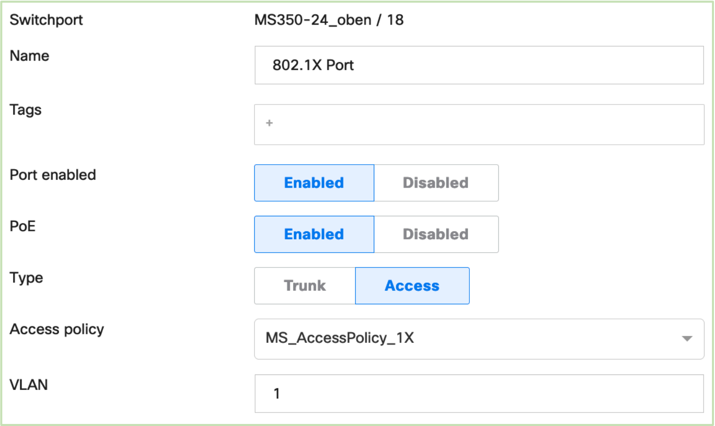


Name: MS_AccessPolicy_1X

Authentication method: my RADIUS server

RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	············



Switchport: MS350-24_oben / 18

Name: 802.1X Port

Tags: +

Port enabled: [✓ Enabled] Disabled

PoE: [✓ Enabled] Disabled

Type: Trunk [✓ Access]

Access policy: MS_AccessPolicy_1X

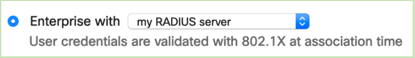
VLAN: 1

Configure 802.1X + GroupPolicy assignment

>>Freeradius Config for MR

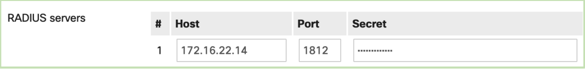
```
thomas                  Cleartext-Password := "sterber"
                        Filter-ID := GroupPolicy_01
```

>>Meraki Dashboard Wifi Config



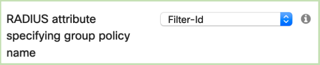
● Enterprise with my RADIUS server

User credentials are validated with 802.1X at association time

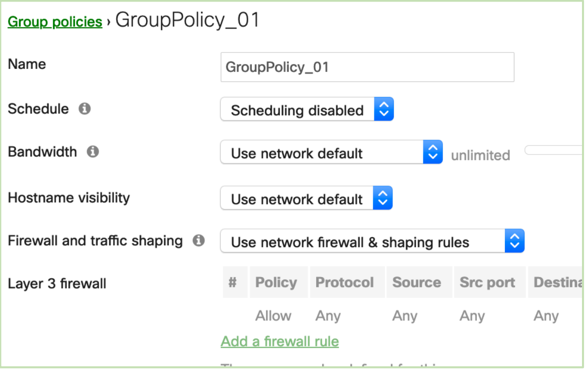


RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	············



RADIUS attribute specifying group policy name: Filter-Id



Group policies › GroupPolicy_01

Name: GroupPolicy_01

Schedule: Scheduling disabled

Bandwidth: Use network default unlimited

Hostname visibility: Use network default

Firewall and traffic shaping: Use network firewall & shaping rules

Layer 3 firewall

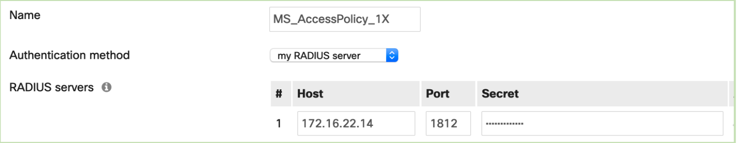
#	Policy	Protocol	Source	Src port	Destina
	Allow	Any	Any	Any	Any

Configure 802.1X + GroupPolicyACL assignment

>>Freeradius Config for MS

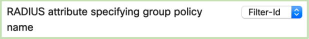
```
        thomas                Cleartext-Password := "sterber"
                                     Filter-ID := MSGroupPolicyACL_01
```

>>Meraki Dashboard Switch Config

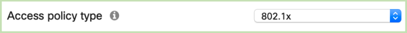


Name	MS_AccessPolicy_1X
Authentication method	my RADIUS server
RADIUS servers	

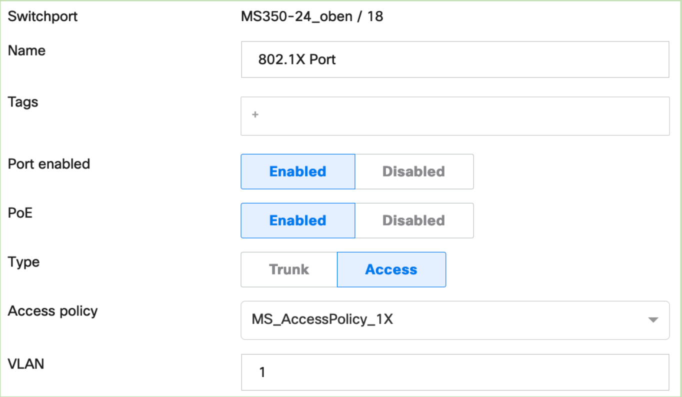
#	Host	Port	Secret
1	172.16.22.14	1812	············



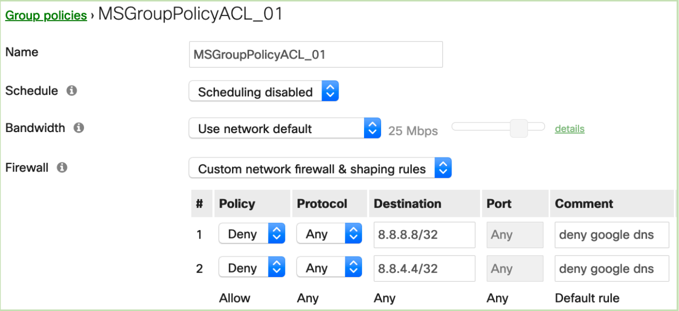
RADIUS attribute specifying group policy name: Filter-Id



Access policy type: 802.1x



Switchport	MS350-24_oben / 18
Name	802.1X Port
Tags	+
Port enabled	Enabled / Disabled (Enabled)
PoE	Enabled / Disabled (Enabled)
Type	Trunk / Access (Access)
Access policy	MS_AccessPolicy_1X
VLAN	1



Group policies › MSGroupPolicyACL_01

Name	MSGroupPolicyACL_01
Schedule	Scheduling disabled
Bandwidth	Use network default 25 Mbps details
Firewall	Custom network firewall & shaping rules

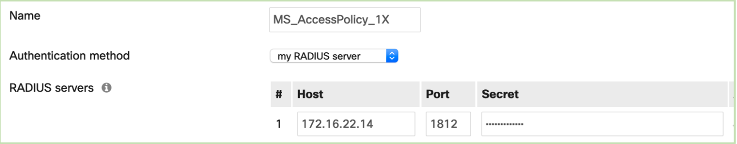
#	Policy	Protocol	Destination	Port	Comment
1	Deny	Any	8.8.8.8/32	Any	deny google dns
2	Deny	Any	8.8.4.4/32	Any	deny google dns
	Allow	Any	Any	Any	Default rule

Configure 802.1X + VLAN + GroupPolicyACL assignment

>>Freeradius Config for MS

```
thomas              Cleartext-Password := "sterber"
                            Filter-ID := MSGroupPolicyACL_01,
                            Tunnel-Medium-Type = 6,
                            Tunnel-Private-Group-ID = 10,
                            Tunnel-Type = VLAN
```

>>Meraki Switch Config

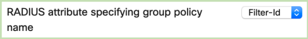


Name: MS_AccessPolicy_1X

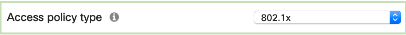
Authentication method: my RADIUS server

RADIUS servers

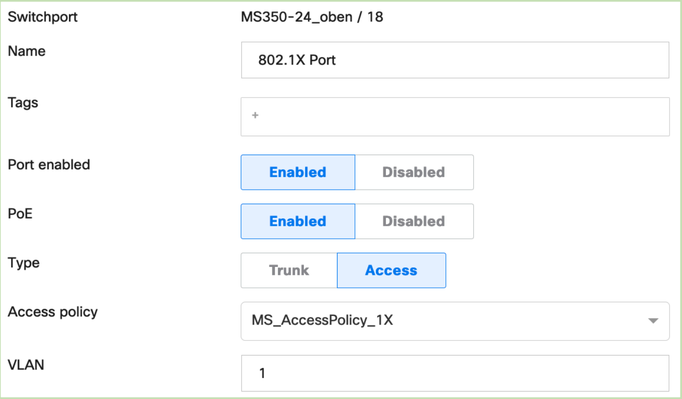
#	Host	Port	Secret
1	172.16.22.14	1812	············



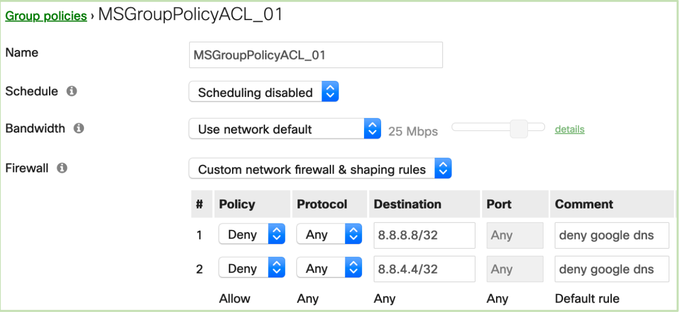
RADIUS attribute specifying group policy name: Filter-Id



Access policy type: 802.1x



Switchport	MS350-24_oben / 18
Name	802.1X Port
Tags	+
Port enabled	[✓ Enabled] Disabled
PoE	[✓ Enabled] Disabled
Type	Trunk [✓ Access]
Access policy	MS_AccessPolicy_1X
VLAN	1



Group policies › MSGroupPolicyACL_01

Name: MSGroupPolicyACL_01

Schedule: Scheduling disabled

Bandwidth: Use network default 25 Mbps details

Firewall: Custom network firewall & shaping rules

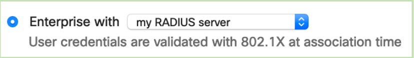
#	Policy	Protocol	Destination	Port	Comment
1	Deny	Any	8.8.8.8/32	Any	deny google dns
2	Deny	Any	8.8.4.4/32	Any	deny google dns
	Allow	Any	Any	Any	Default rule

Configure 802.1X + SGT 100 assignment

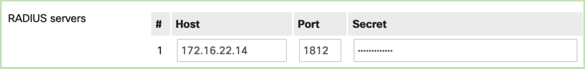
>>Freeradius Config for MS390 and MR Wifi6
(SGT 100 = hex 0064)

```
thomas                    Cleartext-Password := "sterber"
                          Cisco-AVPair = "cts:security-group-tag=0064-00"
```

>>Meraki Dashboard Wifi Config

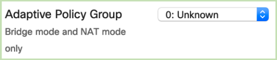


● Enterprise with my RADIUS server
User credentials are validated with 802.1X at association time



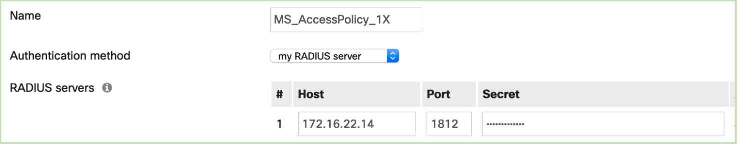
RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	············



Adaptive Policy Group: 0: Unknown
Bridge mode and NAT mode only

>>Meraki Dashboard Switching Config

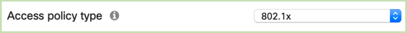


Name: MS_AccessPolicy_1X

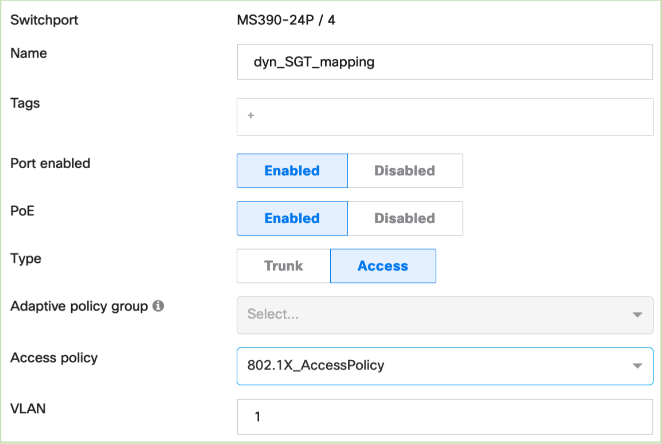
Authentication method: my RADIUS server

RADIUS servers

#	Host	Port	Secret
1	172.16.22.14	1812	············



Access policy type: 802.1x



Switchport	MS390-24P / 4
Name	dyn_SGT_mapping
Tags	+
Port enabled	[✓ Enabled] Disabled
PoE	[✓ Enabled] Disabled
Type	Trunk [✓ Access]
Adaptive policy group	Select...
Access policy	802.1X_AccessPolicy
VLAN	1