JUNIPER NETWORKS | Engineering Simplicity

Network Configuration Example

Microsegmentation with GBP Using Mist Wired Assurance 3rd Edition

Published

2024-07-18

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Microsegmentation with GBP Using Mist Wired Assurance 3rd Edition

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

Table of Contents

Chapter 1 VXLAN Group Based Policies Overview

About this Configuration Example

Scope

Use this Network Configuration Example (NCE) of Microsegmentation with GBP Using Mist Wired Assurance 3rd Edition. You will learn how VXLAN Group Based Policies work and how you can make use of them via examples.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation.
Send your comments to design-center-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Solution Benefits

Enterprise networks are undergoing massive transitions to accommodate the growing demand for cloud-ready, scalable, and efficient network. There's also demand for the plethora of Internet of Things (IoT) and mobile devices. As the number of devices grows, so does network complexity with an ever-greater need for microsegmentation and security. To meet these challenges, you need a network with Automation and Artificial Intelligence (AI) for operational simplification. A Juniper Networks Campus Fabric IP Clos supporting microsegmentation with Group Based Policies is a highly scalable, standards-based architecture (https://www.rfc-editor.org/rfc/rfc8365). This architecture delivers consistent and optimized Enterprise security requirements managed through the Juniper Mist UI.

Solution Overview

With group-based policy (GBP), you can enable microsegmentation at the access layer within a Campus Fabric IP Clos and leverage EVPN VXLAN to provide traffic isolation within and between broadcast domains as well as simplify security policies across a Campus Fabric. See Figure 1.

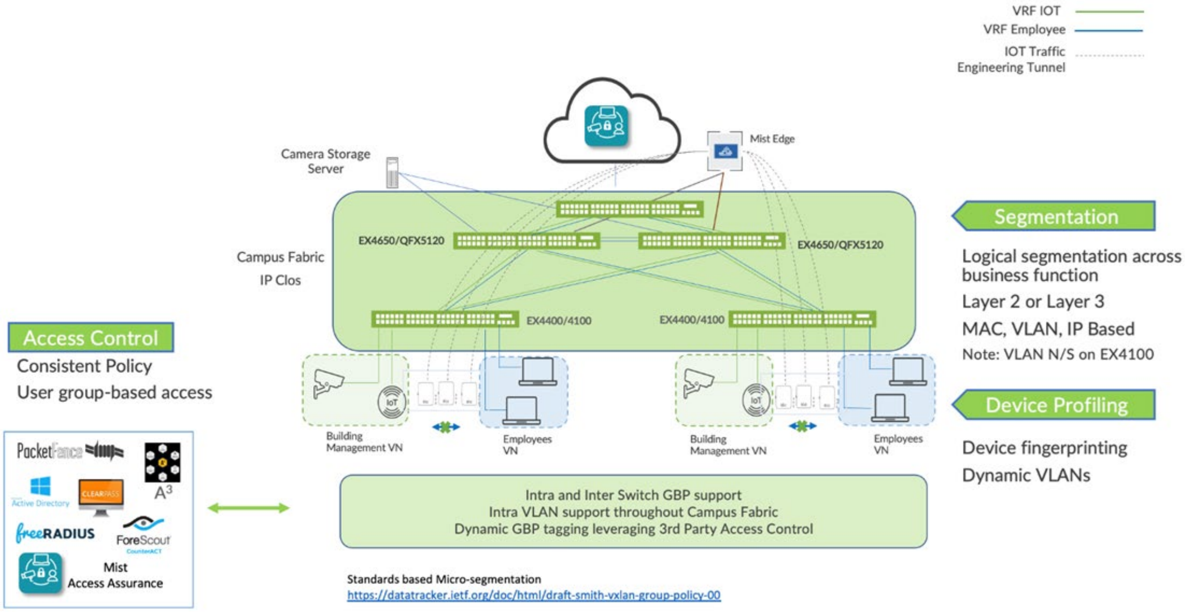
There are several benefits of Group Based Policy microsegmentation:

Standards based — https://datatracker.ietf.org/doc/html/draft-smith-vxlan-group-policy-05

- Simplified Workflow—Group Based Policy is administered through the Mist UI and provides a simple and well-understood workflow for Network Wide Policy control and enforcement. GBP also simplifies network configuration by avoiding the need for large numbers of firewall filters on all devices to ensure lateral threat protection.

- Consistency—GBP provides consistent, customer-managed security policies across the Enterprise through the Mist UI.
- Location-agnostic connectivity—GBP leverages underlying VXLAN technology to provide location-agnostic endpoint access control.
- More granular control—Because GBP can be enforced as a Layer 2 method, it provides tighter control than with traditional ACL-based methods. With VXLAN Group-Based Policies you can block traffic to and from clients inside the same VLAN.
- Network access Control—GBP allows for dynamic or static tagging of wired clients.
    - Dynamic GBP tagging works with industry standards-based RADIUS and Network access Control platforms, including Juniper Mist cloud-based Access Assurance.
    - Static GBP tagging allows you to assign GBP tags by IP prefix, MAC address, VLAN, and port on all access ports in the fabric.

Figure 1



Chapter 2 Use Case and Reference Architecture

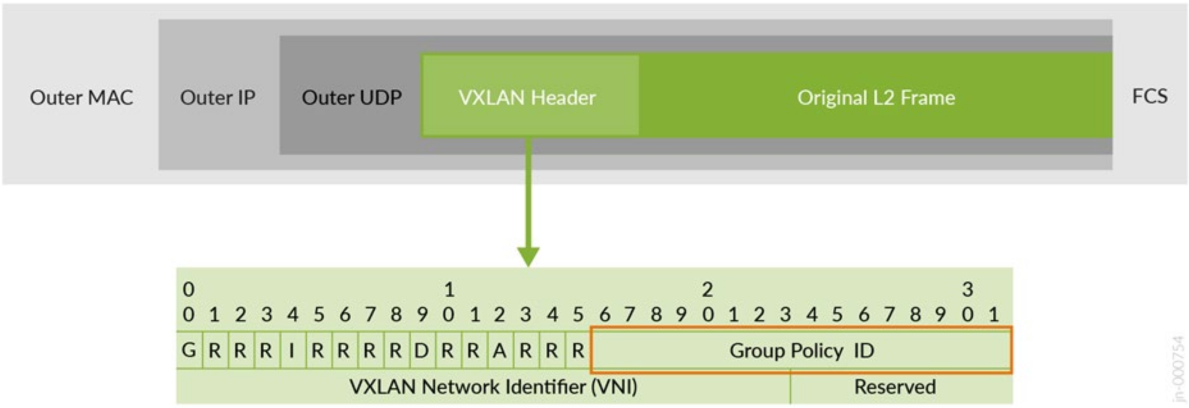
Overview

You can achieve micro and macro segmentation, for example to secure data and assets, in a VXLAN architecture using Group Based Policy (GBP). GBP leverages underlying VXLAN technology to provide location-agnostic endpoint access control. GBP allows you to implement consistent security policies across your enterprise network domains. You can simplify your network configuration by using GBP, avoiding the need to configure large numbers of firewall filters on all your switches. GBP blocks lateral threats by ensuring consistent application of security group policies throughout the network, regardless of the location of endpoints or users. VXLAN-GBP works by leveraging a reserved field in the VXLAN header for use as a Scalable Group Tag (SGT). You can use the SGTs as match conditions in firewall filter rules. Using an SGT is more robust than using port or MAC addresses to achieve similar results. SGTs can be assigned statically (by configuring the switch on a per port or per MAC basis), or they can be configured on the RADIUS server and pushed to the switch through 802.1X when the user is authenticated.

The segmentation enabled by VXLAN-GBP is especially useful in campus VXLAN environments because it gives you a practical way to create network access policies that are independent of the underlying network topology. It simplifies the design and implementation phases of developing network application and endpoint-device security policies.

You can find more detailed information on the VXLAN-GBP standard in the IEEE RFC, I-D.draft-smith-vxlan-group-policy. For the purposes of this example architecture, VXLAN-GBP leverages a reserved field in the VXLAN header as an SGT, as shown in Figure 2.

Figure 2



Starting with Junos 22.4R1 Juniper switches support VXLAN-GBP in egress and ingress enforcing mode as below:

- GBP egress enforcement:
  - This is the IETF standards-based approach.

    - The GBP-tag is part of the VXLAN data plane and needs to be set as the Group Policy ID in the VXLAN Header.
    - As the destination GBP-tag from a remote switch, the packet must be sent to the remote switch every time. The remote switch can then act as an enforcement point for traffic egressing the fabric to the next wired client and can, based on SGT Policy, block the traffic, and discard the packet.

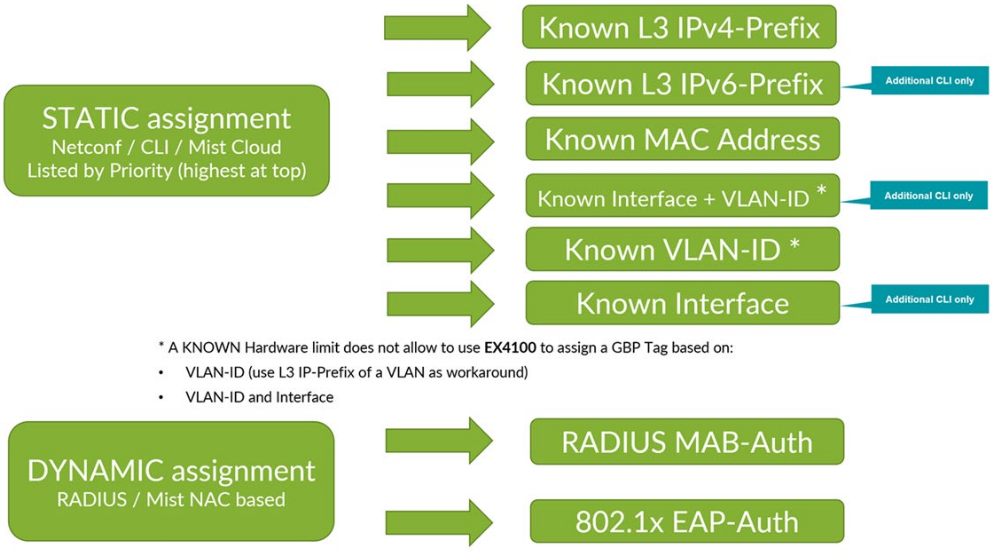
- GBP ingress enforcement

    - This is a Juniper proprietary enhancement to the Junos GBP and SGT implementations.
    - This enhancement is available starting with Junos release version 22.4R1.
    - Here the GBP-tag is an extension of the control plane (BGP-MP extension).
    - The GBP-tag information is added through a vendor-specific attribute to the EVPN Type-2 MAC and IP address information that the fabric shares among its nodes. In this case, the Group Policy ID in the VXLAN header is always left Zero as it is not used for enforcement.
    - The huge advantage is that the destination GBP-tag of a wired client present on a remote switch is already known because it's learned through the control plane. With this enhancement the SGT on the local switch where the source wired client is attached can preemptively block traffic that is not allowed to be sent to a destination client on a remote switch. The enforcement of SGT's always happens at the ingress wired client switch. The need to send all traffic through the fabric even though it may get discarded by the SGT, as in the standards-based approach, does not happen with this solution.
    - This extension makes it easier for administrators to debug GBP-based traffic forwarding decisions. You can review a local switch to know if traffic would be allowed or blocked by a remote switch. Junos commands like "show ethernet-switching table" display GBP-tag information of local and remote wired clients.

NOTE: Mist-managed campus fabrics automatically activate ingress GBP enforcement.

There are different ways you can apply a GBP-tag to a wired client to be used by the SGT's to allow or block traffic. See Figure 3.

Figure 3



You can assign GBP-tags as follows:

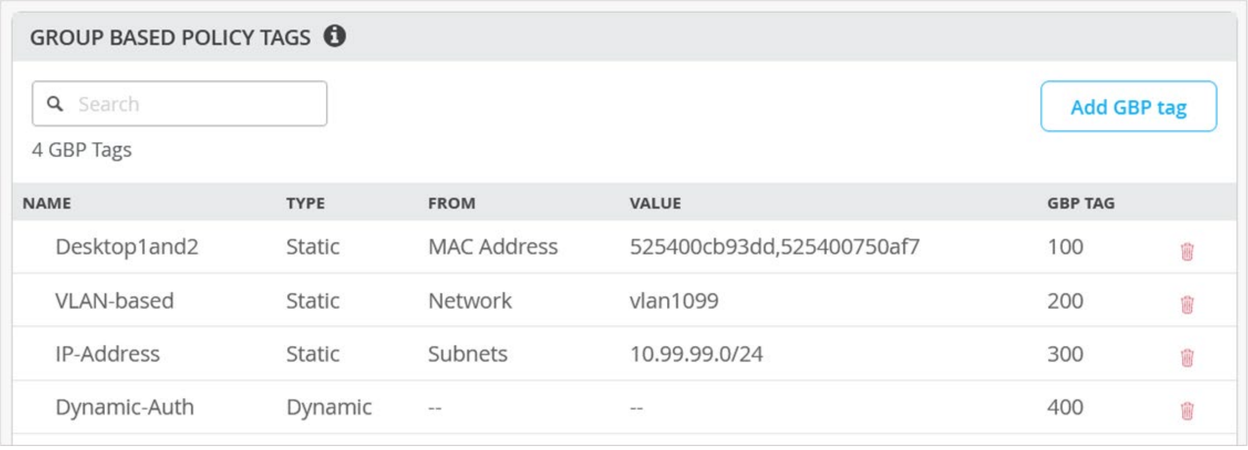
- Static GBP-tag assignment:
  - You must configure static to identify a wired client and assign the GBP-tag to it.
  - Match criteria (depending on Junos OS Release version) can be:
    - 1.) Layer 3 IPv4 prefixes and hosts
    - 2.) Layer 3 IPv6 prefixes and hosts
    - 3.) Layer 2 MAC-Address
    - 4.) switch Interface/Port and VLAN-ID (not supported on EX4100 switches).
    - 5.) Layer2 VLAN-ID (not supported on EX4100 switches).
    - 6.) switch Interface/Port

- For dynamic GBP-tag assignment:
  - The wired client needs to be authenticated at switch port entering the fabric.
  - Is based on RADIUS server authorization information which is part of the RADIUS access accept message.
  - The wired client authentication can be:
    - IEEE 802.1X EAP based.
    - MAC address based (MAB).

NOTE: There is no prioritization between any static GBP-tag and dynamic GBP-tag assignment. A port can only be used for one of the two assignment methods at any time. Currently, there is no support for cascading these methods.

The Mist Cloud GUI simplifies this process and abstracts the switch configuration needed as shown in Figure 4.

Figure 4



GROUP BASED POLICY TAGS

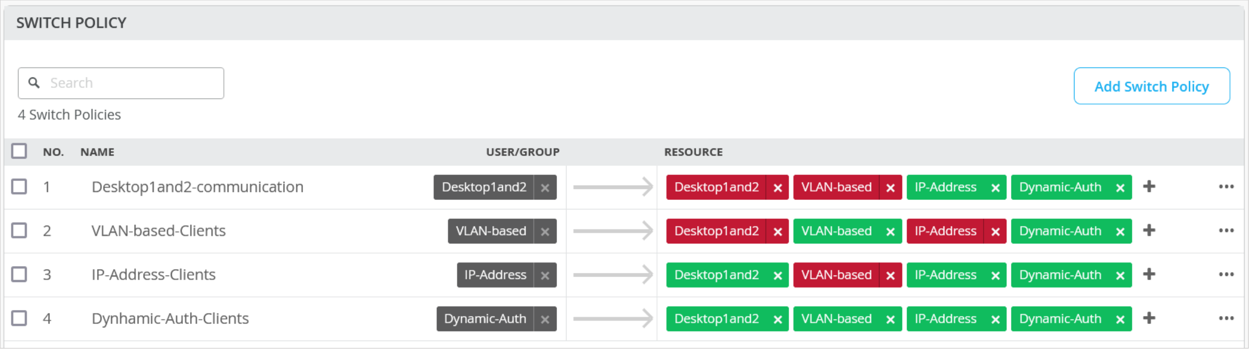
Search

Add GBP tag

4 GBP Tags

NAME	TYPE	FROM	VALUE	GBP TAG
Desktop1and2	Static	MAC Address	525400cb93dd,525400750af7	100
VLAN-based	Static	Network	vlan1099	200
IP-Address	Static	Subnets	10.99.99.0/24	300
Dynamic-Auth	Dynamic	--	--	400

After defining the GBP-tag assignment you need to specify the SGTs as switch policies. Again, the Mist Cloud simplifies and abstracts this process in its GUI, allowing you to build an intuitive communication matrix.



SWITCH POLICY

Search

Add Switch Policy

4 Switch Policies

□	NO.	NAME	USER/GROUP		RESOURCE
□	1	Desktop1and2-communication	Desktop1and2 ×	→	🟥 Desktop1and2 × 🟥 VLAN-based × 🟩 IP-Address × 🟩 Dynamic-Auth × +
□	2	VLAN-based-Clients	VLAN-based ×	→	🟥 Desktop1and2 × 🟩 VLAN-based × 🟥 IP-Address × 🟩 Dynamic-Auth × +
□	3	IP-Address-Clients	IP-Address ×	→	🟩 Desktop1and2 × 🟥 VLAN-based × 🟩 IP-Address × 🟩 Dynamic-Auth × +
□	4	Dynhamic-Auth-Clients	Dynamic-Auth ×	→	🟩 Desktop1and2 × 🟩 VLAN-based × 🟩 IP-Address × 🟩 Dynamic-Auth × +

NOTE: We strongly recommend using a switch template to configure static or dynamic GBP-tag assignments and SGT policies since the templates ease the task of distributing this information across all access switches of an IP-Clos fabric.

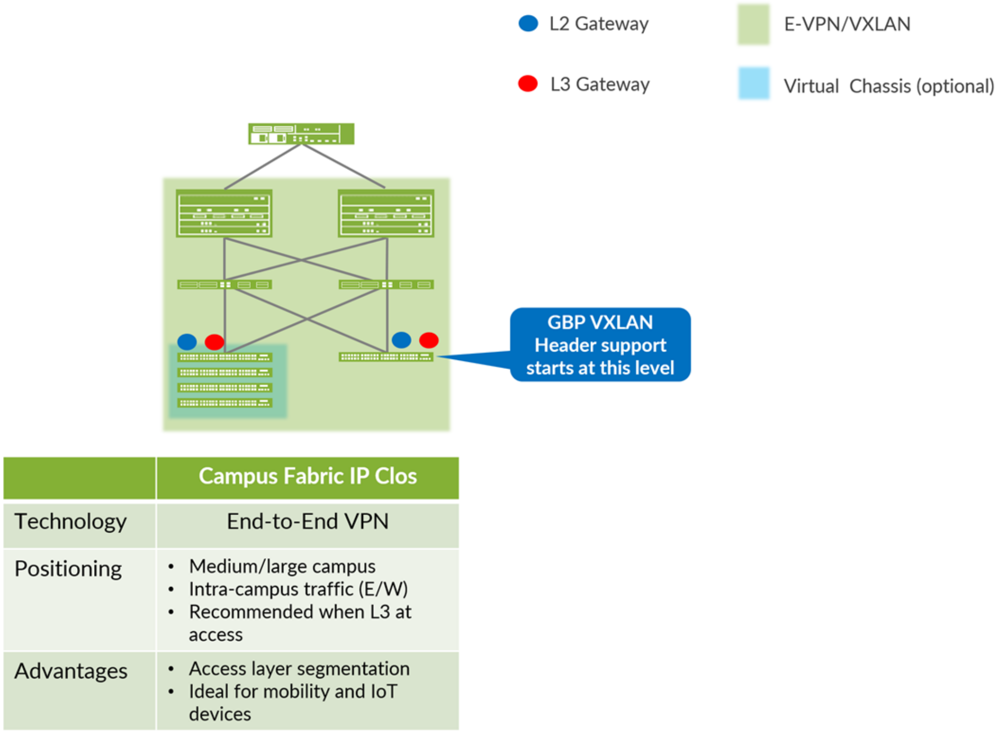
Chapter 3 Known Limitations of VXLAN GBP Testing and support

There are a few areas to consider when testing VXLAN GBP support as covered in this document.

VXLAN GBP Works Only with IP-Clos Fabrics

The technology only supports VXLAN GBP in an IP-Clos fabric because this is the only design where the VXLAN Layer 2 VTEP is supported at the access switch layer.

Figure 5


● L2 Gateway
● L3 Gateway
🟩 E-VPN/VXLAN
▨ Virtual Chassis (optional)
GBP VXLAN Header support starts at this level

	Campus Fabric IP Clos
Technology	End-to-End VPN
Positioning	• Medium/large campus • Intra-campus traffic (E/W) • Recommended when L3 at access
Advantages	• Access layer segmentation • Ideal for mobility and IoT devices

Until a better solution is found, all other fabric types like EVPN Multihoming, CRB, or ERB do not allow GBP-tag management of wired clients because:

- The VXLAN Layer starts at the distribution or collapsed core layer hence, wired clients can communicate uncontrolled to each other locally from port-to-port within the same access switch. Private VLANs do not help in this case because they are created through static Junos OS configuration and won’t follow a dynamically assigned GBP-tag.
- Between the access switch and upper switches such as distribution or collapsed core there is only normal LAG established. Hence, between these stages of the fabric-only VLANs and MAC addresses play a role, and the GBP-tag gets lost in transit. You must start with VXLAN at the lowest stage of the fabric.

- For wired clients performing dynamic RADIUS-based authentication, the wired client gets a GBP-tag assigned as part of the authorization process on the access switch it is attached to. Again, there is no additional protocol to pass this information to the upper fabric stage, so this information is unseen by the fabric and cannot be reconstructed by it.

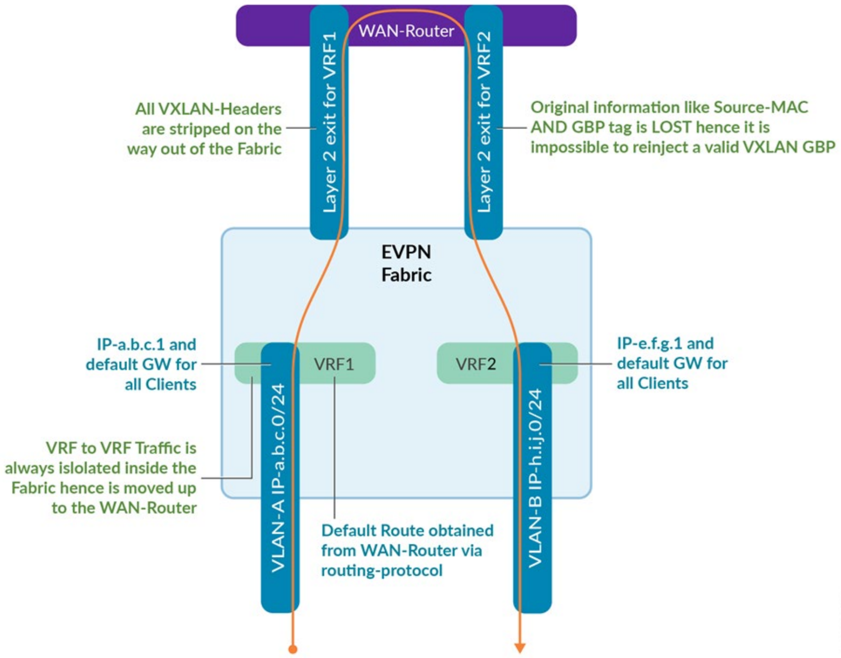
NOTE: You can attach a desktop switch to the fabric's access switch to manage, for example, a VoIP phone and a PC on a Campus Fabric IP-Clos. If you want to perform dynamic authentication, you must perform a second, MAC-based, authentication on the fabric's access switch to get synchronized information about which GBP-tag to assign. This is because the attached desktop switch does not share its RADIUS-based authorization information with the access switch

No Support for VRF to VRF GBP-Tag Distribution

If your network has a fabric with more than a single virtual routing and forwarding (VRF), the GBP-tag distribution is limited to the VLANs inside the same VRF. As shown in Figure 6, VRF-to-VRF GBP-tag distribution does not work because of the following technical reasons:

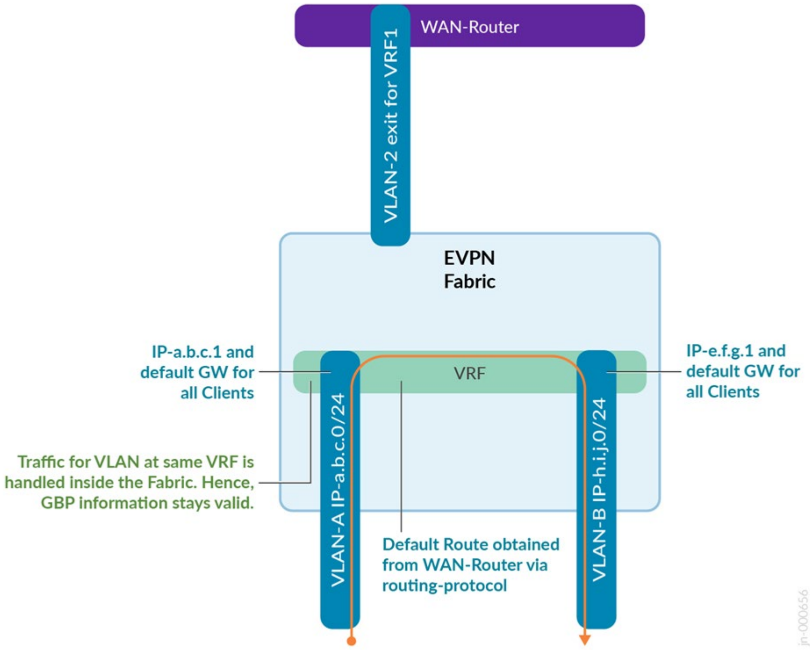
- All Mist-managed campus fabrics have isolation inside the fabric when traffic is passing between two VRF's. There is no route leaking between VRF's allowed inside the fabric itself for security reasons. Traffic between VRFs must always go South-to-North to the WAN router. The WAN router can then permit or forward the traffic between the VRF's and allow the traffic to flow back through the fabric to the destination VRF and VLAN.
- WAN routers are usually not part of the VXLAN layer of a fabric. They use either a:
    - Layer 2 configuration with VLAN's and trunk ports and static routes between the fabric and the WAN router.
    - Layer 3 configuration with P2P links and a routing protocol such as OSPF or eBGP between the fabric and the WAN router.
- You encounter a similar situation as in EVPN multihoming of CRB and ERB fabrics mentioned above where traffic between stages uses a different environment and the on-hook information of the VXLAN tunnel gets lost between these stages. It is almost impossible to reconstruct the original information because when the packet gets back into the fabric towards the destination VRF, the original MAC address is lost.

Figure 6


WAN-Router
Layer 2 exit for VRF1
Layer 2 exit for VRF2
All VXLAN-Headers are stripped on the way out of the Fabric
Original information like Source-MAC AND GBP tag is LOST hence it is impossible to reinject a valid VXLAN GBP
EVPN Fabric
IP-a.b.c.1 and default GW for all Clients
VRF1
VRF2
IP-e.f.g.1 and default GW for all Clients
VRF to VRF Traffic is always islolated inside the Fabric hence is moved up to the WAN-Router
VLAN-A IP-a.b.c.0/24
VLAN-B IP-h.i.j.0/24
Default Route obtained from WAN-Router via routing-protocol
jn-000755

It’s better to consider moving the VLAN’s towards the same VRF of the fabric as such traffic will remain inside the fabric as East-West traffic not utilizing the WAN router. In such a case GBP-based management remains valid. See Figure 7.

Figure 7


WAN-Router
VLAN-2 exit for VRF1
EVPN Fabric
IP-a.b.c.1 and default GW for all Clients
VRF
IP-e.f.g.1 and default GW for all Clients
Traffic for VLAN at same VRF is handled inside the Fabric. Hence, GBP information stays valid.
VLAN-A IP-a.b.c.0/24
VLAN-B IP-h.i.j.0/24
Default Route obtained from WAN-Router via routing-protocol
jn-000656

NOTE: A single global VRF is recommended to be used in this case. The usage of GBP then mitigates the need for multiple VRF’s for security needs.

Known Junos Switch-Firmware Limitations

When **configuring GBP usage for the first time** on an Access-Switch one needs to schedule a maintenance window before they get activated and used. Junos requires a restart of the control plane to include this change:

- On a standalone Switch one could re-start the Packet-Forwarding-Engine (PFE) to archive the needed control plane restart for GBP inclusion.
- On a Virtual Chassis one needs to issue a complete reboot of the entire Virtual Chassis to archive the needed control plane restart for GBP inclusion.

Known Hardware Limitations

Juniper EX4100 series switches have the following documented limitations:

- Static Interface/Port and VLAN-ID based GBP-tag assignments are not possible on EX4100 Platform.
- Static VLAN-ID based GBP-tag assignments are not possible on EX4100 Platform. We suggest you use the IPv4 Prefix of the VLAN to achieve similar functionality.

Known Mist GUI Limitations

In the current Beta version, the Mist GUI only supports the following static GBP-tag assignments:

- IPv4 prefix-based static GBP-tag assignments called **Subnets**.
- MAC address host-based static GBP-tag assignments called **MAC Address**.
- VLAN-ID based static GBP-tag assignments called **Network**.

Currently you must use additional Junos OS CLI if you want to make use of:

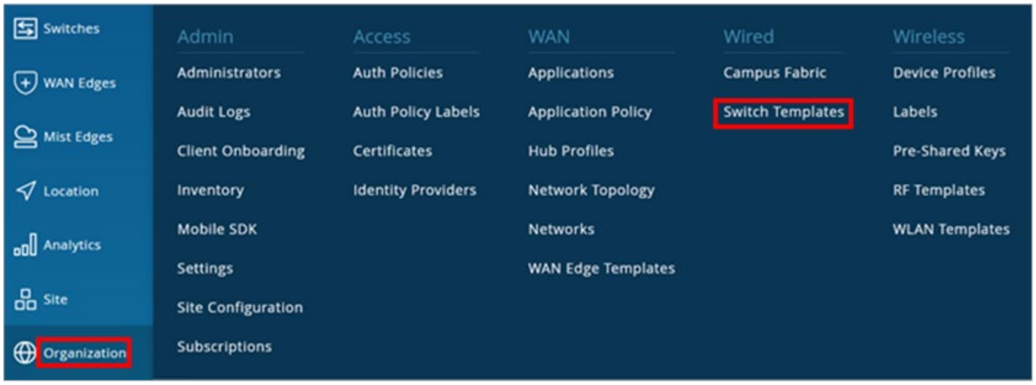
- Switch port-based (interface-based) static GBP-tag assignments
- Switch port-based (interface-based) and VLAN ID-based static GBP-tag assignments

Wireless and Wired Client Segmentation Policies Use Different Sections in Mist GUI

Currently the microsegmentation of Mist-managed Fabrics is archived for wired and wireless clients in different sections of the Mist GUI:

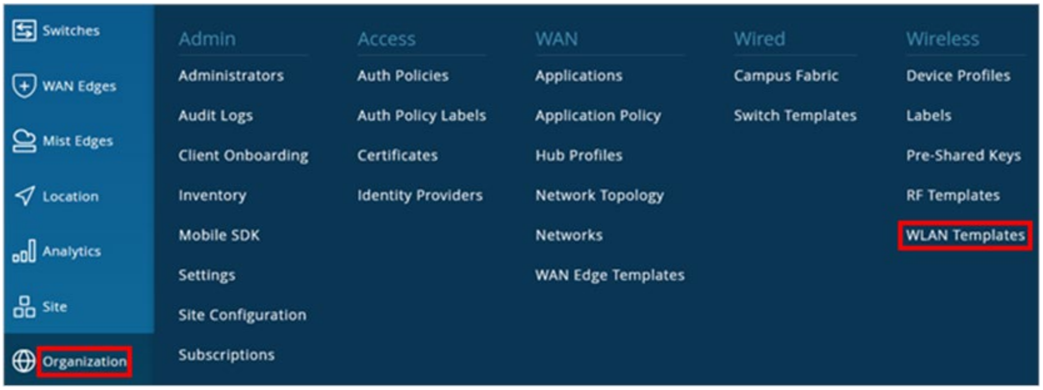
- GBP/SGT-based microsegmentation of wired clients should be configured on the Organization > Switch Templates page. See Figure 8.

Figure 8

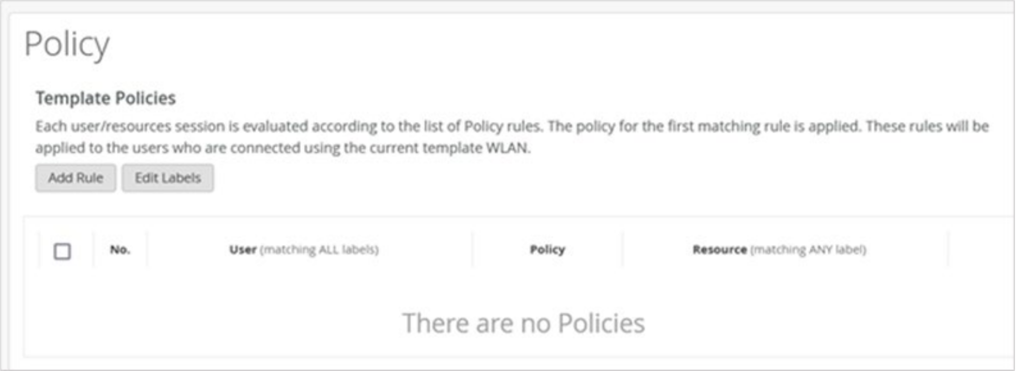


- Policy configuration of microsegmentation for wireless clients should be configured on the Organization > WLAN Templates page. See Figure 9.

Figure 9



After you create a new WLAN Template, you can start to manage and configure the policies for wireless clients.



Policy

Template Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied. These rules will be applied to the users who are connected using the current template WLAN.

□	No.	User (matching ALL labels)	Policy	Resource (matching ANY label)

There are no Policies

NOTE: As of the publish date of this NCE, GBP-tag management is not extended to APs.

Chapter 4 Recommendations

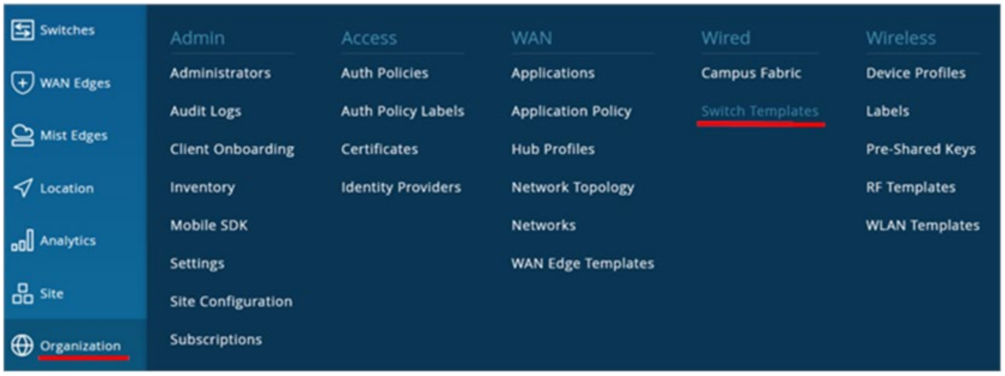
The following simple guidelines will help you to successfully implement a Campus Fabric using VXLAN-based Group-based Policies in your network:

- Consider building and managing the fabric using the Mist portal as part of what is shown in this NCE.
- The only supported fabric type for VXLAN-based Group-based policies is IP-Clos.
- The only supported switch types for access switches are the Juniper EX4400-Series and EX4100-Series switches.
- When you intend to do static GBP-tag assignments via VLAN-ID it is better to use the IP prefix of a VLAN since the IP prefix would also be recognized by Juniper EX4100-Series switches.
- Dynamic assignments via third-party RADIUS servers should be easy to implement once you have configured the RADIUS Dictionaries to support the Vendor Attribute “Juniper-switching-Filter” with the right string value.
- If your wired clients are in different VRFs of the same fabric, consider configuring the segmentation in the WAN router for controlling the forwarding between the two VRFs.
- If you attach a desktop switch at the access switch then you may need to do a second authentication at the access switch before entering the Fabric.
- Microsegmentation of wired and wireless clients is managed using the Mist GUI but in different sections of the GUI.
- Always use a switch template for all switches in the fabric to sync all changes you do regarding GBP-tag assignments and SGT Policies. Do not configure each switch individually.
- When configuring GBP for the first time you need to schedule a maintenance window for your Access-Switches to restart the PFE for a standalone Switch or a reboot of a Virtual Chassis before your GBP configuration gets activated.
- **All deployments must be done with Junos version 24.2R1 or higher** as only those guarantees sync between Layer 2 and Layer 3 GBP Tags internal tables. Also check that the Mist Fabric pushes the following Junos to each Switch activating this sync “set forwarding-options evpn-vxlan gbp mac-ip-inter-tagging” . If this is missing, please add as additional CLI to your Access Switch Template.

Chapter 5 EXAMPLES: Switch Template Configuration

NOTE: All examples were executed with Junos 24.2R1 and an additional CLI on each access switch “set forwarding-options evpn-vxlan gbp mac-ip-inter-tagging.” For production grade environments it is expected using Junos 24.2R2 or later.

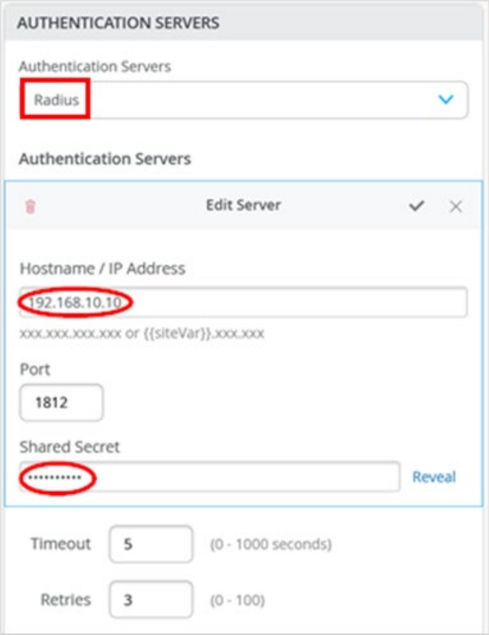
All configuration examples of this section are made in a switch Template that is assigned to all switches. Switch templates can be configured via **Organization > Switch Templates** tab of the Mist GUI



Third-Party RADIUS Server configuration

At the beginning of the switch Template one can configure third-party RADIUS Servers. The minimum items that must be configured are:

- Select as Authentication Servers=”RADIUS”
- Add at least one new Authentication Server:
  - Configure the hostname or IP address through which this RADIUS server responds to requests.
  - Set a shared secret between the switch and the server to allow communication.



AUTHENTICATION SERVERS

Authentication Servers: Radius

Authentication Servers

Edit Server

Hostname / IP Address: 192.168.10.10

xxx.xxx.xxx.xxx or {{siteVar}}.xxx.xxx

Port: 1812

Shared Secret: ••••••••••

Timeout: 5 (0 - 1000 seconds)

Retries: 3 (0 - 100)

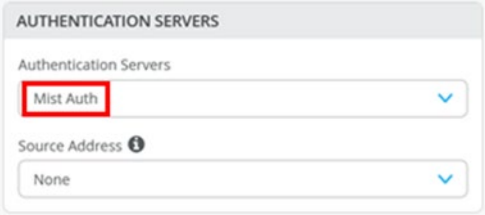
You must perform a similar process on the RADIUS server for each client. Configure in the RADIUS server, the IP address of the client and shared secret. Ensure you define the vendor-specific dictionary for the switch that acts as the RADIUS client.

Mist Authentication Configuration

There is not much to configure if you intend using Mist Access Assurance:

- Select as Authentication Servers=”Mist Auth”

Figure 10



AUTHENTICATION SERVERS

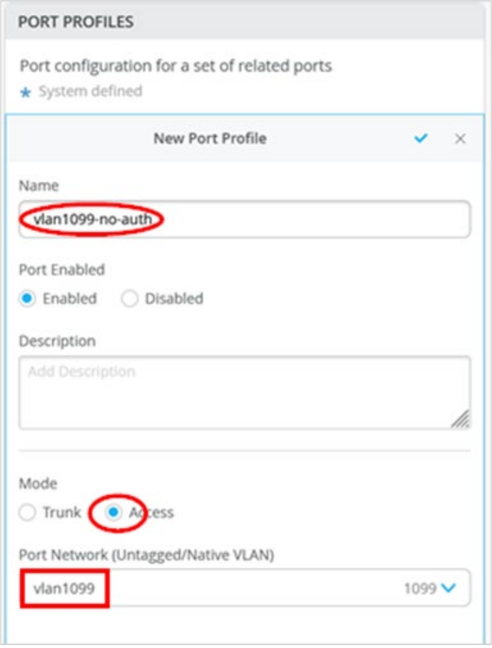
Authentication Servers: Mist Auth

Source Address: None

Port Profiles Used for Testing

The following port profiles were used during testing:

- All static GBP-tag assignments used one without any special authentication:
    - Port Profile Name=”vlan1099-no-auth”
    - Mode=”access”
    - Port Network=”vlan1099”



PORT PROFILES

Port configuration for a set of related ports

★ System defined

New Port Profile

Name: vlan1099-no-auth

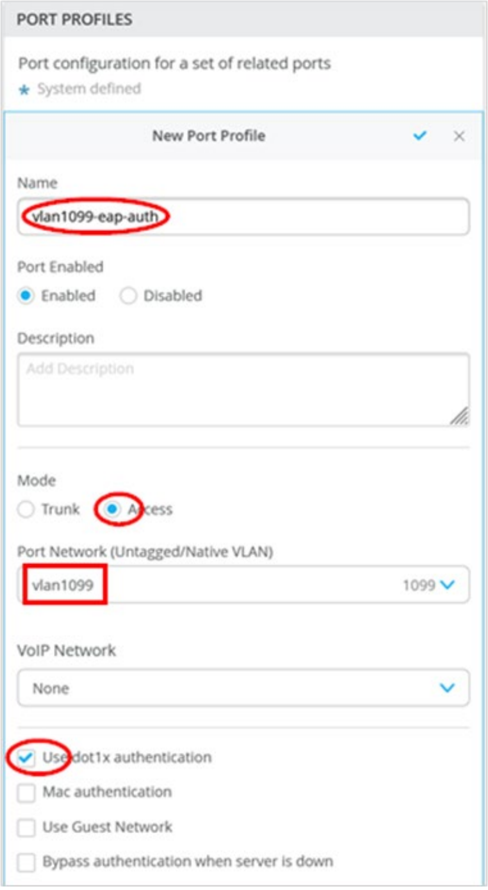
Port Enabled: ● Enabled ○ Disabled

Description: Add Description

Mode: ○ Trunk ● Access

Port Network (Untagged/Native VLAN): vlan1099 1099

- All dynamic GBP-tag assignments with 802.1X supplicants used:
    - Port Profile Name=”vlan1099-eap-auth”
    - Mode=”access”
    - Port Network=”vlan1099”
    - Use dot1x authentication=”Checked/Enabled”



PORT PROFILES

Port configuration for a set of related ports

★ System defined

New Port Profile ✓ ×

Name

vlan1099-eap-auth

Port Enabled

● Enabled ○ Disabled

Description

Add Description

Mode

○ Trunk ● Access

Port Network (Untagged/Native VLAN)

vlan1099 1099

VoIP Network

None

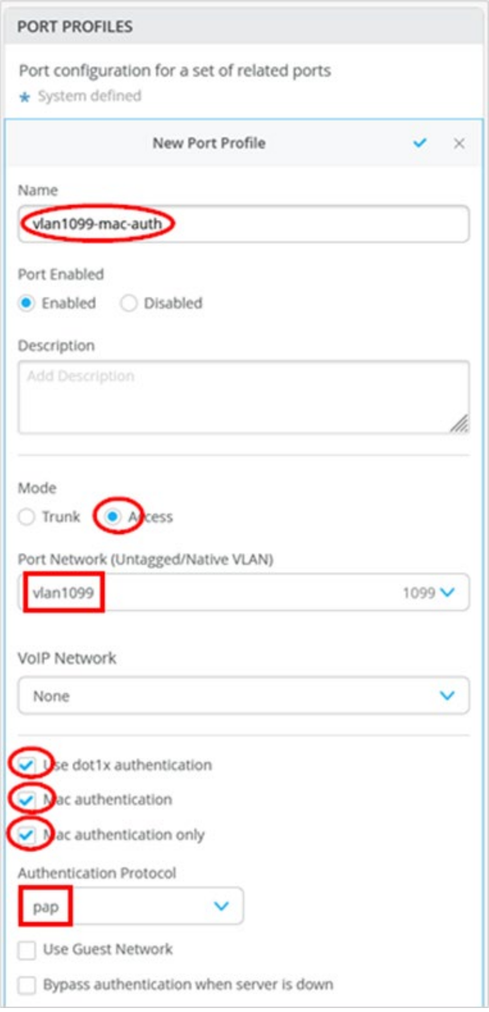
☑ Use dot1x authentication

☐ Mac authentication

☐ Use Guest Network

☐ Bypass authentication when server is down

- All dynamic GBP-tag assignments with via MAC-Address used:
  - Port Profile Name=”vlan1099-mac-auth”
  - Mode=”access”
  - Port Network=”vlan1099”
  - Use dot1x authentication=”Checked/Enabled”
  - Mac authentication=”Checked/Enabled”
  - Mac authentication only=”Checked/Enabled.” Note: This prevents the switch from attempting an EAP-based authentication which would fail and cause 60 seconds of delay.
  - Authentication Protocol=”pap.” This was easier to configure on the RADIUS server side.



PORT PROFILES

Port configuration for a set of related ports

★ System defined

New Port Profile ✓ ×

Name

vlan1099-mac-auth

Port Enabled

● Enabled ○ Disabled

Description

Add Description

Mode

○ Trunk ● Access

Port Network (Untagged/Native VLAN)

vlan1099 1099

VoIP Network

None

☑ Use dot1x authentication

☑ Mac authentication

☑ Mac authentication only

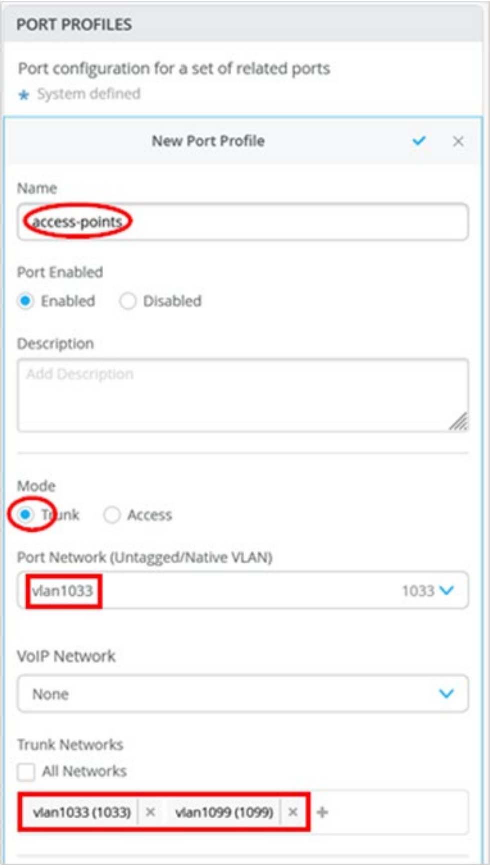
Authentication Protocol

pap

□ Use Guest Network

□ Bypass authentication when server is down

- Finally for the access Point we used the following Port Profile:
  - Port Profile Name=”access-points”
  - Mode=”Trunk”
  - Port Network=”vlan1033”
  - Trunk Networks=”vlan1033” + ”vlan1099”



PORT PROFILES

Port configuration for a set of related ports

★ System defined

New Port Profile

Name

access-points

Port Enabled

● Enabled ○ Disabled

Description

Add Description

Mode

● Trunk ○ Access

Port Network (Untagged/Native VLAN)

vlan1033 1033

VoIP Network

None

Trunk Networks

□ All Networks

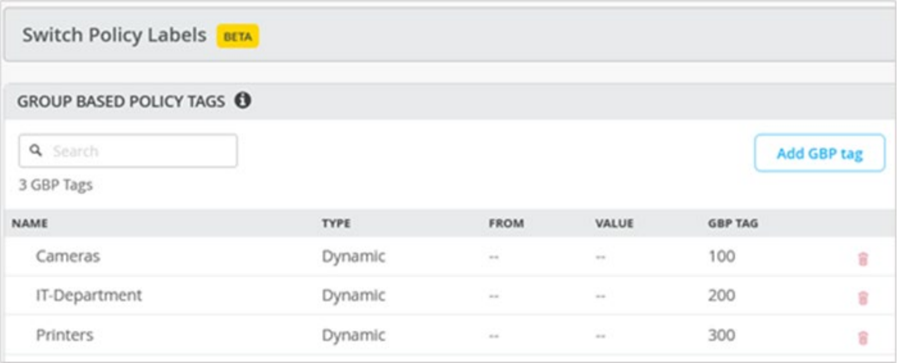
vlan1033 (1033) × vlan1099 (1099) × +

GBP-Tag Assignments

We've used different GBP-tag assignments configurations depending on the test cases.

Figure 11 shows a list of GBP-tag assignments that were used for testing the RADIUS servers with MAB and 802.1X clients.

Figure 11



Switch Policy Labels BETA

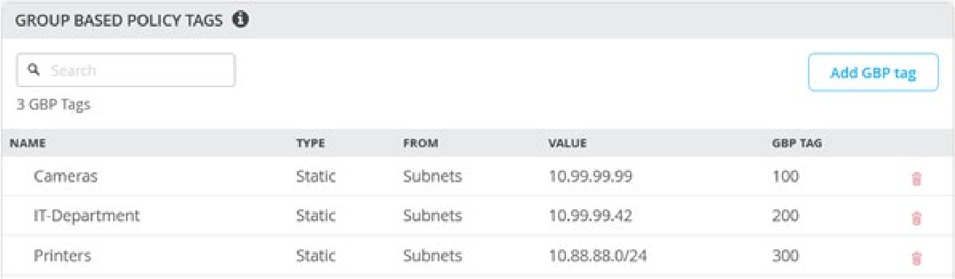
GROUP BASED POLICY TAGS

3 GBP Tags

NAME	TYPE	FROM	VALUE	GBP TAG
Cameras	Dynamic	--	--	100
IT-Department	Dynamic	--	--	200
Printers	Dynamic	--	--	300

Figure 12 shows a list of GBP-tag assignments that were used for testing static, IP address-based assignments.

Figure 12



GROUP BASED POLICY TAGS

Search

Add GBP tag

3 GBP Tags

NAME	TYPE	FROM	VALUE	GBP TAG
Cameras	Static	Subnets	10.99.99.99	100
IT-Department	Static	Subnets	10.99.99.42	200
Printers	Static	Subnets	10.88.88.0/24	300

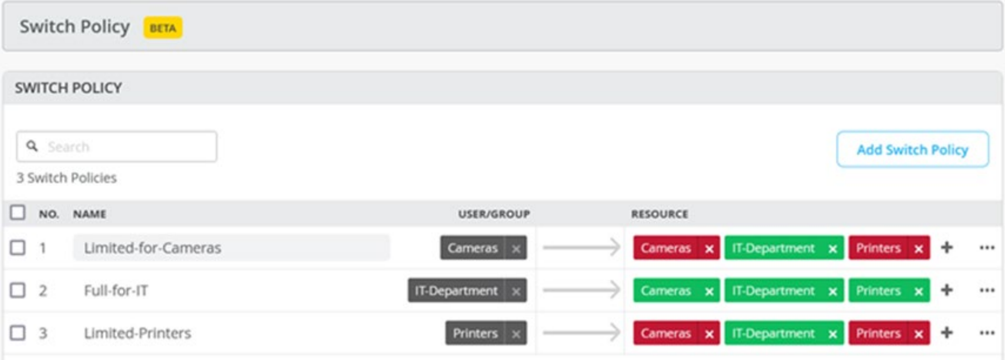
- For the entire GBP-tag assignment testing more permutations of static assignments were used but we do not list them here.

NOTE: If you use VLAN ID-based (network-based) assignments and the access switch is a Juniper EX4100-Series switch which cannot utilize those features, the Mist management cloud will automatically filter out those invalid Junos OS commands, so they are not pushed to the switch. The remaining configuration stays intact as intended.

GBP Policy Assignments

Most of the time, the following matrix of SGT policy enforcements to block or allow traffic between GBP-tags were used.

Figure 13



Switch Policy BETA

SWITCH POLICY

Search

Add Switch Policy

3 Switch Policies

□ NO.	NAME	USER/GROUP	RESOURCE
□ 1	Limited-for-Cameras	Cameras ×	🟥 Cameras × 🟩 IT-Department × 🟥 Printers ×
□ 2	Full-for-IT	IT-Department ×	🟩 Cameras × 🟩 IT-Department × 🟩 Printers ×
□ 3	Limited-Printers	Printers ×	🟥 Cameras × 🟩 IT-Department × 🟥 Printers ×

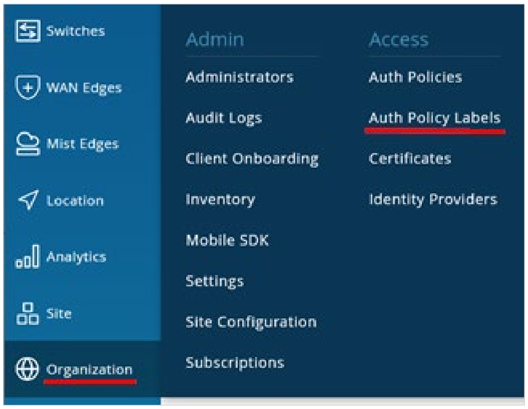
Chapter 6 EXAMPLES: Dynamic Client Authentication using the Mist Authentication Cloud

In this section we provide examples on how to authenticate wired clients using Mist Access Assurance and how you can repeat the testing performed in this NCE. First, ensure that your switch template uses “Mist Auth” in the authentication servers field as shown in Figure 10.

Client Label creation

Then, you must create the RADIUS **Authorization Policy Labels** on the **Organization > Auth Policy Labels** page.

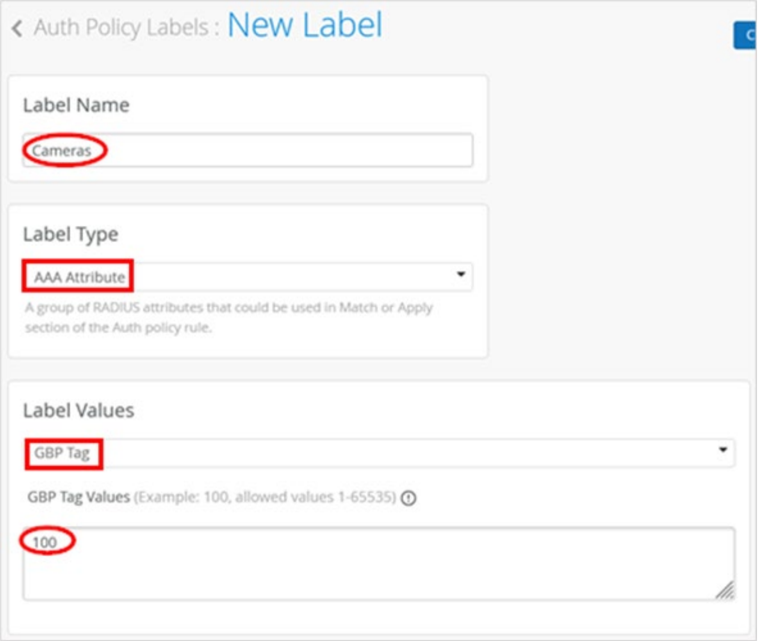
Figure 14



Create labels for at least three GBP-tags you want to assign:

- First create the new auth policy label
    - Label Name=”Cameras”
    - Label Type=”AAA Attribute.” Note: This is used to indicate it’s used as a RADIUS message.
    - Port Network=”GBP Tag”
    - GBP Tag Values=”100”

Figure 15



< Auth Policy Labels : New Label

Label Name

Cameras

Label Type

AAA Attribute

A group of RADIUS attributes that could be used in Match or Apply section of the Auth policy rule.

Label Values

GBP Tag

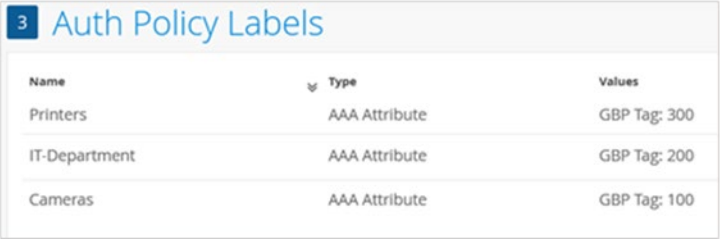
GBP Tag Values (Example: 100, allowed values 1-65535)

100

- Second create this new auth policy label:
  - Label Name=”IT-Department”
  - Label Type=”AAA Attribute”
  - Port Network=”GBP Tag”
  - GBP Tag Values=”200”
- Third create this new auth policy label:
  - Label Name=”Printers”
  - Label Type=”AAA Attribute”
  - Port Network=”GBP Tag”
  - GBP Tag Values=”300”

The resulting configuration of all three Labels should look like the list shown in Figure 16.

Figure 16



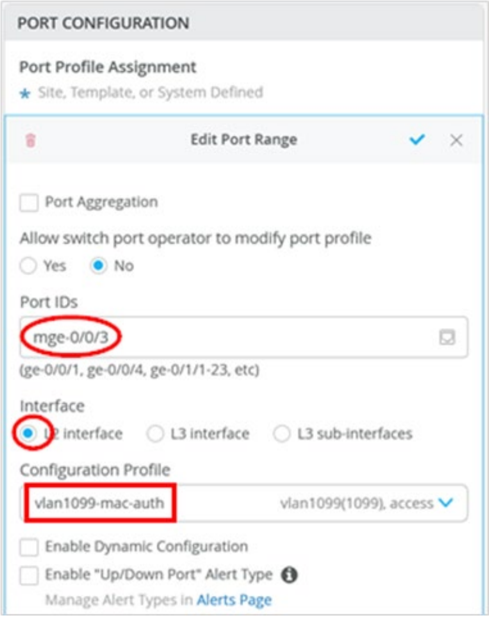
3 Auth Policy Labels

Name	Type	Values
Printers	AAA Attribute	GBP Tag: 300
IT-Department	AAA Attribute	GBP Tag: 200
Cameras	AAA Attribute	GBP Tag: 100

MAC Address-Based Client Authentication

When you intend to use MAC address-based client authentication, ensure that the switch ports where your clients are attached use the right port profile. In our case we used the port profile=”vlan1099-mac-auth” and configured the switch ports as shown in Figure 17. Use port IDs appropriate for your environment.

Figure 17



PORT CONFIGURATION

Port Profile Assignment

★ Site, Template, or System Defined

Edit Port Range ✓ ×

□ Port Aggregation

Allow switch port operator to modify port profile

○ Yes ● No

Port IDs

mge-0/0/3

(ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)

Interface

● L2 interface ○ L3 interface ○ L3 sub-interfaces

Configuration Profile

vlan1099-mac-auth vlan1099(1099), access

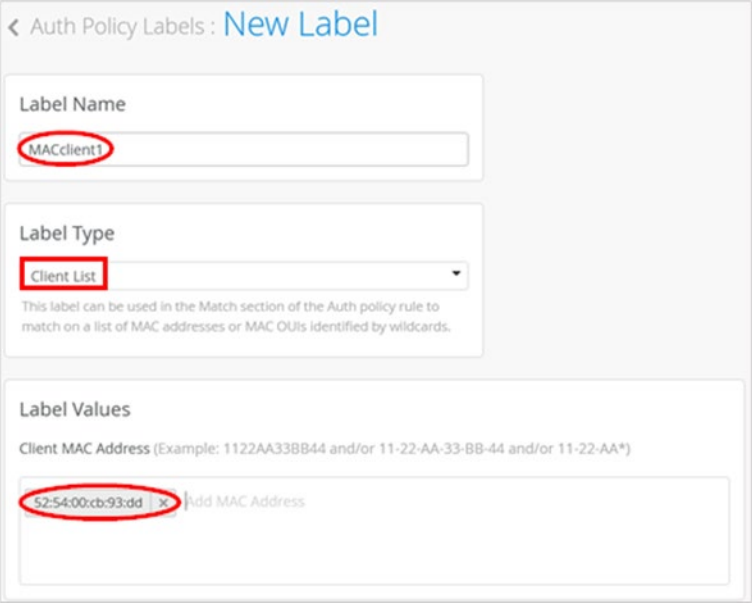
□ Enable Dynamic Configuration

□ Enable "Up/Down Port" Alert Type

Manage Alert Types in Alerts Page

Next, create auth labels to identify the MAC addresses of your wired clients as shown in the following example.

- Create a new auth label:
    - Label Name=”MACclient1”
    - Label Type=”Client List” as this is used to validate MAC-Addresses.
    - Label Values=”<client1-MAC-Address>”



‹ Auth Policy Labels : New Label

Label Name

MACclient1

Label Type

Client List

This label can be used in the Match section of the Auth policy rule to match on a list of MAC addresses or MAC OUIs identified by wildcards.

Label Values

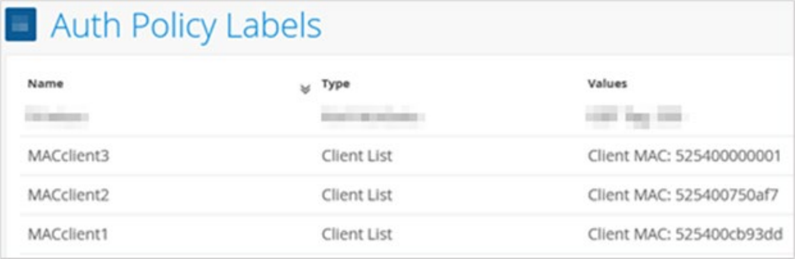
Client MAC Address (Example: 1122AA33BB44 and/or 11-22-AA-33-BB-44 and/or 11-22-AA*)

52:54:00:cb:93:dd ×

Add MAC Address

Create other auth labels based on the above example for at least 3 MAC address-based clients. An example of the results is shown in Figure 18.

Figure 18

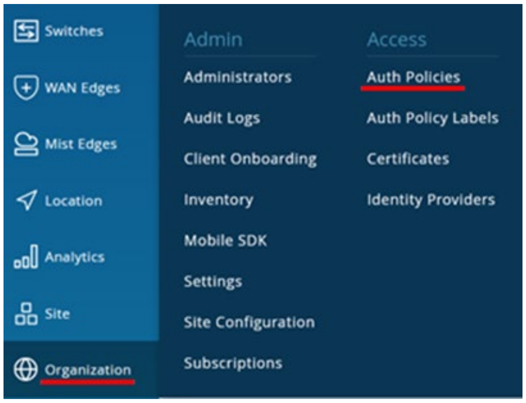


Auth Policy Labels

Name	Type	Values
[redacted]	[redacted]	[redacted]
MACclient3	Client List	Client MAC: 525400000001
MACclient2	Client List	Client MAC: 525400750af7
MACclient1	Client List	Client MAC: 525400cb93dd

Next you must create various authentication policies on the **Organization > Auth Policies** page.

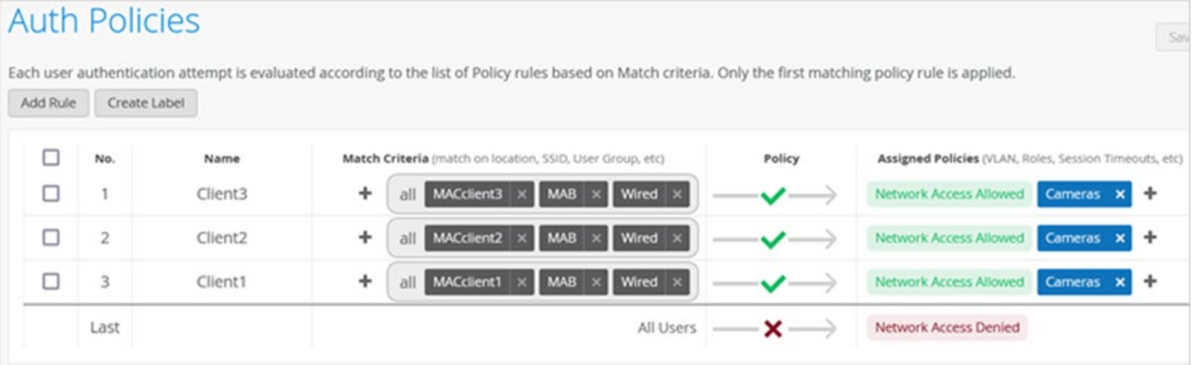
Figure 19



In the example below we want every client to get GBP-tag1 (our “Printers”) assigned. Hence, the configuration looks like:

- Auth Policy for first client:
  - Name=”Client1”
  - Match Criteria=”MACclient1” + “MAB” + “Wired”
  - Policy=”Pass”
  - Assigned Policies=”Network Access Allowed” + “Cameras”
- Auth Policy for second client:
  - Name=”Client2”
  - Match Criteria=”MACclient2” + “MAB” + “Wired”
  - Policy=”Pass”
  - Assigned Policies=”Network Access Allowed” + “Cameras”
- Auth Policy for third client:
  - Name=”Client3”
  - Match Criteria=”MACclient3” + “MAB” + “Wired”
  - Policy=”Pass”
  - Assigned Policies=”Network Access Allowed” + “Cameras”

Figure 20



Auth Policies

Each user authentication attempt is evaluated according to the list of Policy rules based on Match criteria. Only the first matching policy rule is applied.

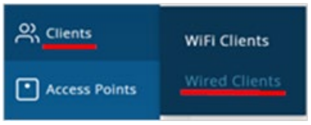
□	No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)
□	1	Client3	+ all MACclient3 × MAB × Wired ×	✓	Network Access Allowed Cameras × +
□	2	Client2	+ all MACclient2 × MAB × Wired ×	✓	Network Access Allowed Cameras × +
□	3	Client1	+ all MACclient1 × MAB × Wired ×	✓	Network Access Allowed Cameras × +
	Last		All Users	✗	Network Access Denied

We have chosen to define one authentication policy per client because then you can change the assigned policy for each client individually to assign and test with a different GBP-tag.

NOTE: When testing dynamic, MAC address-based authentication, there is a default of 10 minutes before a re-authentication happens.
When you change labels to test other combinations, 10 minutes might too long to wait. In a lab situation, you can use the additional Junos OS CLI feature to shorten the reauthentication period.
For example, to set a 60 second reauthentication period, use the following additional Junos OS CLI:
“set protocols dot1x authenticator interface vlan1099-mac-auth reauthentication 60”.

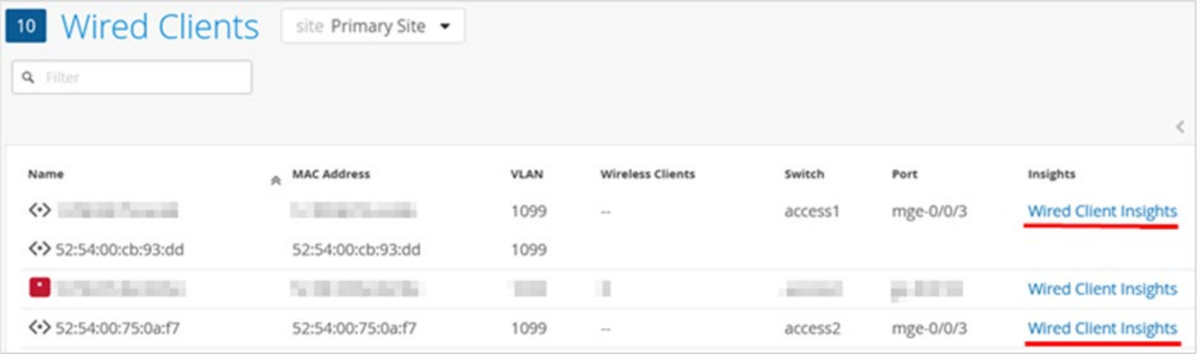
After your clients are authenticated by Mist Access Assurance, you can check the GBP-tag assignment. To do so, navigate to **Clients > Wired Clients** in the Mist GUI.

Figure 21



Identify the wired clients you have configured and click on **Wired Client Insights**.

Figure 22



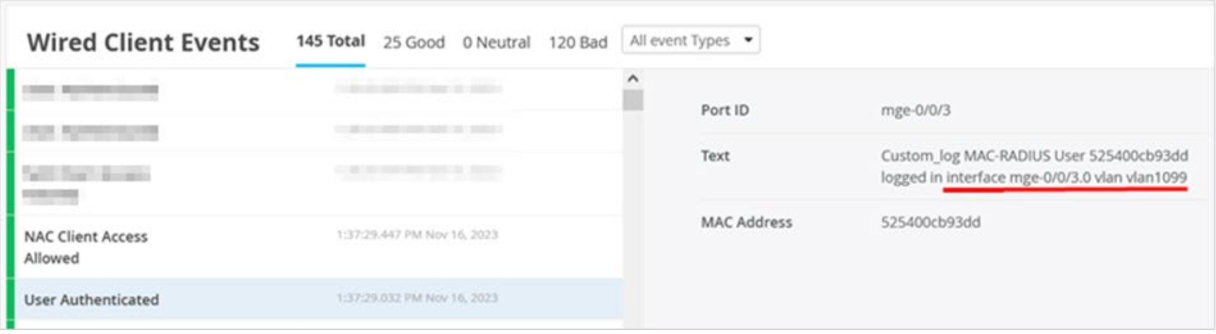
10 Wired Clients site Primary Site

Filter

Name	MAC Address	VLAN	Wireless Clients	Switch	Port	Insights
[redacted]	[redacted]	1099	--	access1	mge-0/0/3	Wired Client Insights
52:54:00:cb:93:dd	52:54:00:cb:93:dd	1099				
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Wired Client Insights
52:54:00:75:0a:f7	52:54:00:75:0a:f7	1099	--	access2	mge-0/0/3	Wired Client Insights

Below is an example of the first client events report. You can see which interface the new client connected through.

Figure 23



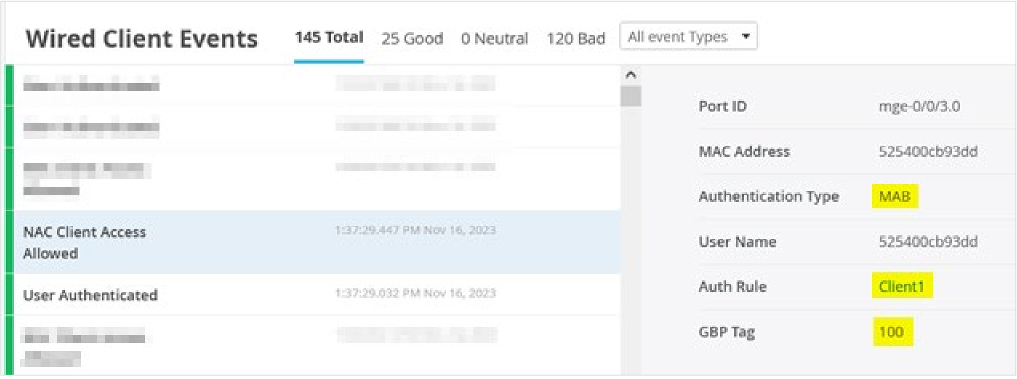
Wired Client Events 145 Total 25 Good 0 Neutral 120 Bad All event Types

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
NAC Client Access Allowed	1:37:29.447 PM Nov 16, 2023
User Authenticated	1:37:29.032 PM Nov 16, 2023

Port ID	mge-0/0/3
Text	Custom_log MAC-RADIUS User 525400cb93dd logged in interface mge-0/0/3.0 vlan vlan1099
MAC Address	525400cb93dd

The second Event you would typically see is the NAC authentication itself. Below, you can see the authentication type, the Auth Rule that was found valid to be used and final the GBP-tag that was applied as part of the dynamic authentication.

Figure 24



Wired Client Events

145 Total | 25 Good | 0 Neutral | 120 Bad | All event Types

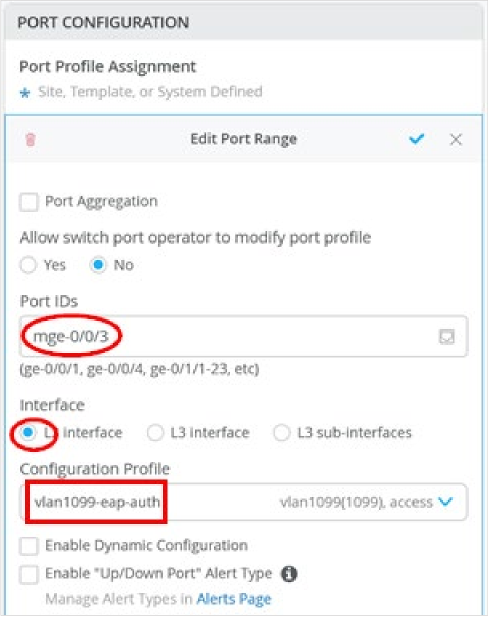
Event	Time
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
NAC Client Access Allowed	1:37:29.447 PM Nov 16, 2023
User Authenticated	1:37:29.032 PM Nov 16, 2023
[redacted]	[redacted]

Port ID	mge-0/0/3.0
MAC Address	525400cb93dd
Authentication Type	MAB
User Name	525400cb93dd
Auth Rule	Client1
GBP Tag	100

IEEE 802.1X-based Client Authentication

When you intend to use IEEE 802.1X-based client authentication ensure that the switch ports where your clients are attached use the right port profile. In our case, we used the port profile, ”vlan1099-eap-auth” and configured the switch ports as shown in the example below. Use port IDs appropriate for your environment.

Figure 25



PORT CONFIGURATION

Port Profile Assignment

* Site, Template, or System Defined

Edit Port Range

□ Port Aggregation

Allow switch port operator to modify port profile

○ Yes ● No

Port IDs: mge-0/0/3

(ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)

Interface

● L2 interface ○ L3 interface ○ L3 sub-interfaces

Configuration Profile: vlan1099-eap-auth — vlan1099(1099), access

□ Enable Dynamic Configuration

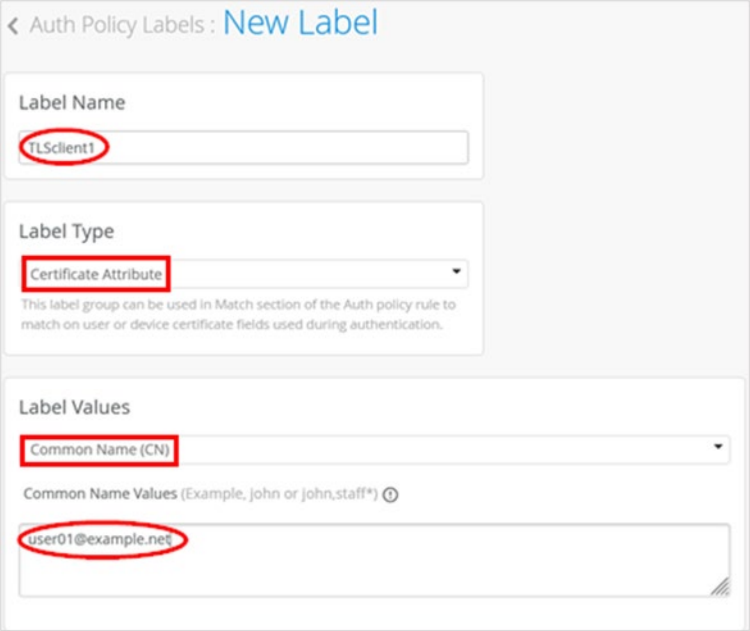
□ Enable "Up/Down Port" Alert Type

Manage Alert Types in Alerts Page

When testing, we wanted to be able to identify a minimum of three clients individually to be able to assign them different GBP-tags dynamically. The approach chosen was to use EAP-TLS and determine the individual client by attributes of their client certificates stored on each supplicant. Which values you choose depends on the enterprise PKI you intend to use. In our case, we knew that each client has a different name in the Common Name attribute of the supplicant certificate. Hence, we used this field to create three client labels as shown in the example below.

- Create a new authentication policy label by navigating to **Organization > Auth Label** and configuring the fields as shown in the following list.
  - Label Name=”TLSclient1”
  - Label Type=”Certificate Attribute”
  - Label Values=”Common Name (CN)”
  - Common Names Values=”user01@example.net”

Figure 26



Auth Policy Labels : New Label

Label Name

TLSclient1

Label Type

Certificate Attribute

This label group can be used in Match section of the Auth policy rule to match on user or device certificate fields used during authentication.

Label Values

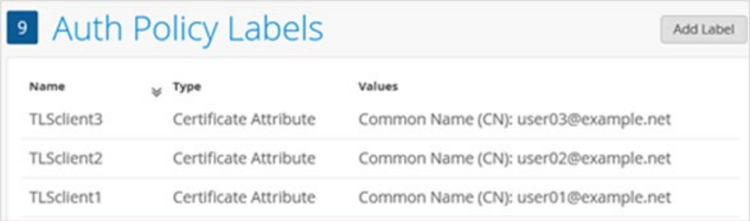
Common Name (CN)

Common Name Values (Example, john or john,staff*)

user01@example.net

- Create other labels based on the example above for at least three TLS clients as shown in Figure 27.

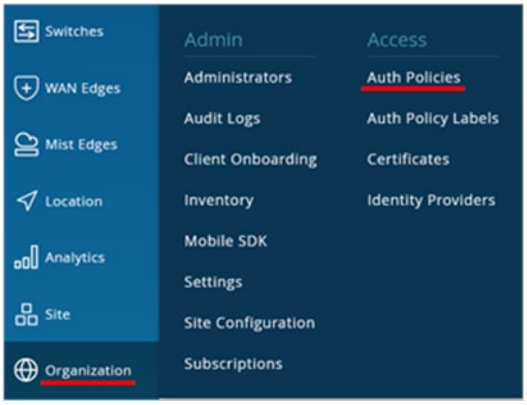
Figure 27



9 Auth Policy Labels

Name	Type	Values
TLSclient3	Certificate Attribute	Common Name (CN): user03@example.net
TLSclient2	Certificate Attribute	Common Name (CN): user02@example.net
TLSclient1	Certificate Attribute	Common Name (CN): user01@example.net

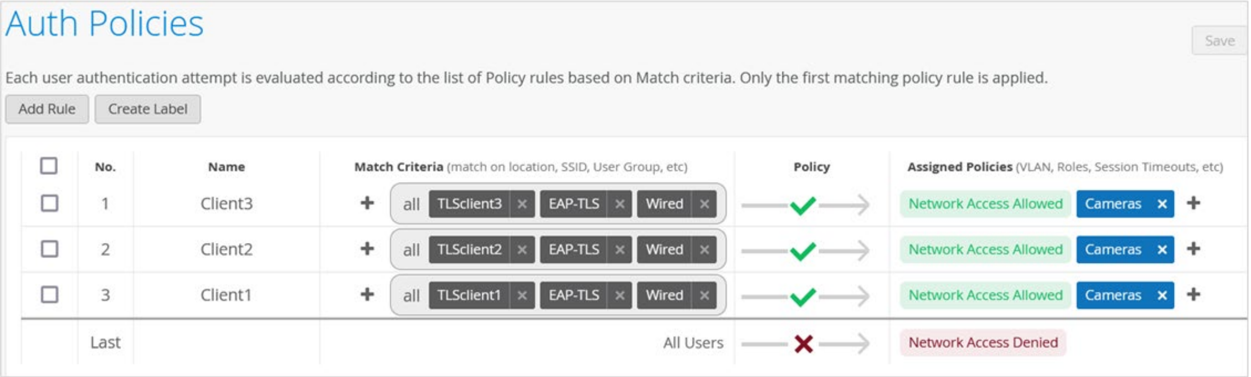
Next, create various authentication policies on the **Organization > Auth Policies** page.



In the example below we want every client to have the GBP-tag1 (our "Printers") assigned. Hence, the configuration looks like:

- Auth Policy for first client:
  - Name="Client1"
  - Match Criteria="TLSclient1" + "EAP-TLS" + "Wired"
  - Policy="Pass"
  - Assigned Policies="Network Access Allowed" + "Cameras"
- Auth Policy for second client:
  - Name="Client2"
  - Match Criteria="TLSclient2" + "EAP-TLS" + "Wired"
  - Policy="Pass"
  - Assigned Policies="Network Access Allowed" + "Cameras"
- Auth Policy for third client:
  - Name="Client3"
  - Match Criteria="TLSclient3" + "EAP-TLS" + "Wired"
  - Policy="Pass"
  - Assigned Policies="Network Access Allowed" + "Cameras"

Figure 28



Auth Policies

Save

Each user authentication attempt is evaluated according to the list of Policy rules based on Match criteria. Only the first matching policy rule is applied.

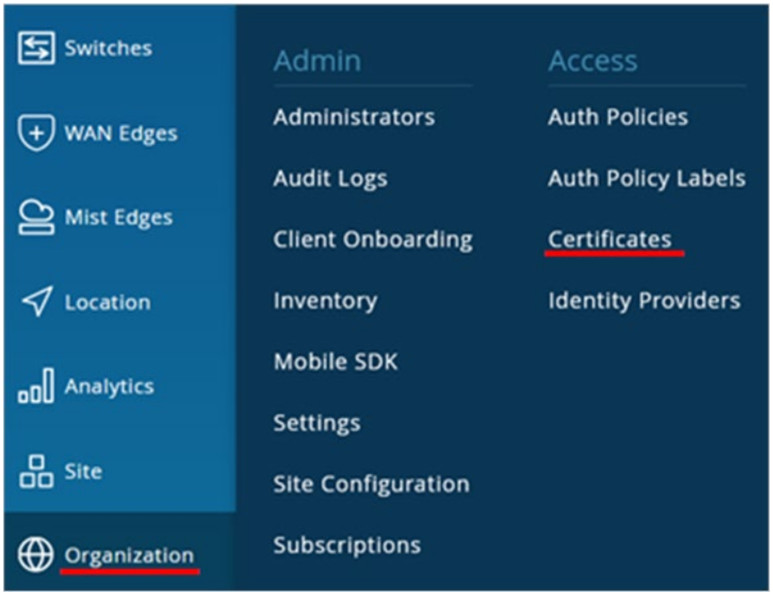
Add Rule | Create Label

□	No.	Name	Match Criteria (match on location, SSID, User Group, etc)	Policy	Assigned Policies (VLAN, Roles, Session Timeouts, etc)
□	1	Client3	+ all TLSclient3 × EAP-TLS × Wired ×	✓	Network Access Allowed Cameras × +
□	2	Client2	+ all TLSclient2 × EAP-TLS × Wired ×	✓	Network Access Allowed Cameras × +
□	3	Client1	+ all TLSclient1 × EAP-TLS × Wired ×	✓	Network Access Allowed Cameras × +
	Last		All Users	✗	Network Access Denied

At this point, if not already done, you must configure your enterprise PKI for the Mist Authentication Cloud:

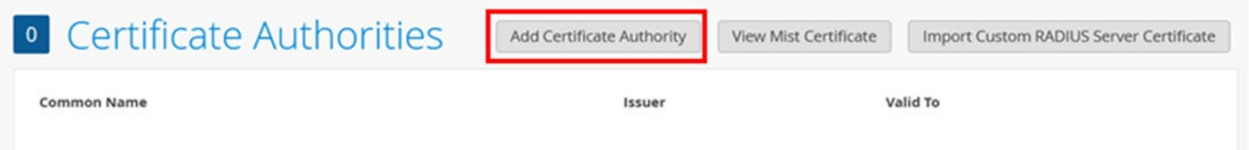
- Navigate to **Organization > Certificates**

Figure 29



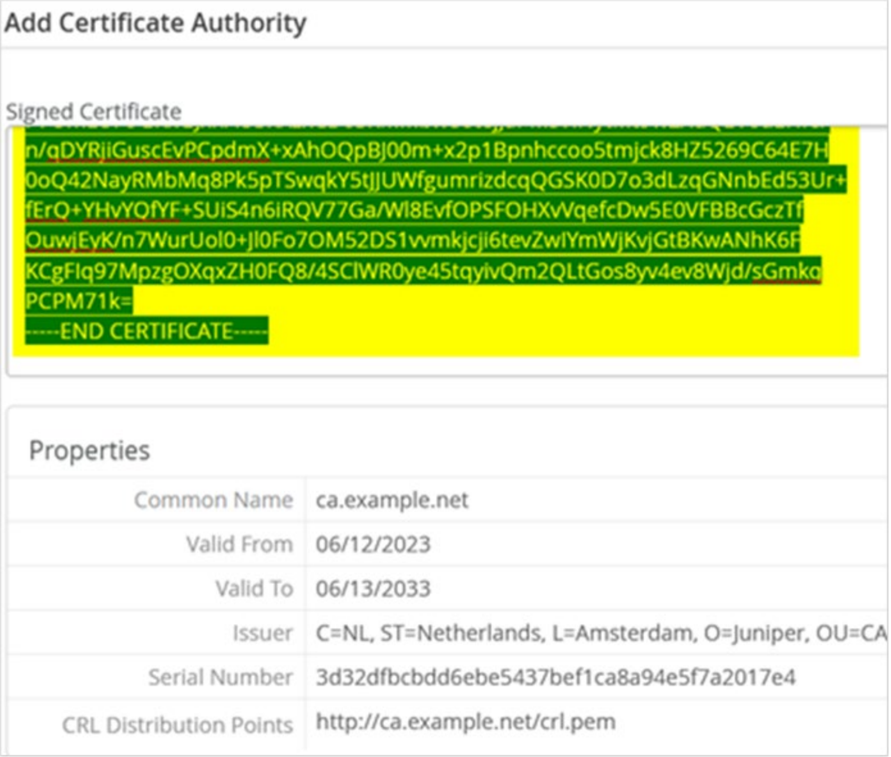
- Click on the “Add Certificate Authority” button as shown in Figure 30.

Figure 30



- Paste the base64-encoded part of your Enterprise PKI Root-CA in the “Signed Certificate” window.

Figure 31



Add Certificate Authority

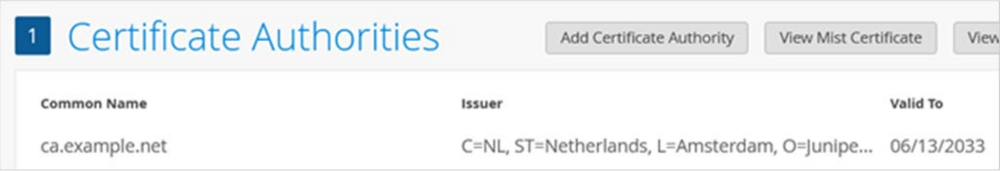
Signed Certificate

```
n/qDYRjiGuscEvPCpdmX+xAhOQpBJ00m+x2p1Bpnhccoo5tmjck8HZ5269C64E7H
0oQ42NayRMbMq8Pk5pTSwqkY5tJJUWfgumrizdcqQGSK0D7o3dLzqGNnbEd53Ur+
fErQ+YHvYQfYF+SUiS4n6iRQV77Ga/Wl8EvfOPSFOHXvVqefcDw5E0VFBBcGczTf
OuwjEyK/n7WurUol0+Jl0Fo7OM52DS1vvmkjcji6tevZwlYmWjKvjGtBKwANhK6F
KCgFlq97MpzgOXqxZH0FQ8/4SClWR0ye45tqyivQm2QLtGos8yv4ev8Wjd/sGmkq
PCPM71k=
-----END CERTIFICATE-----
```

Properties

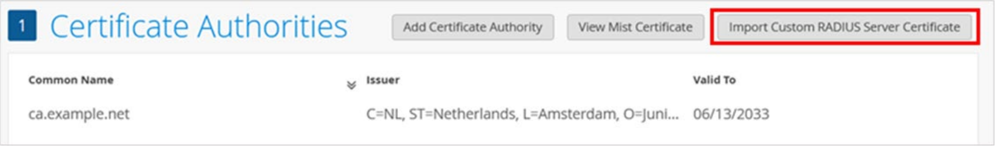
Common Name	ca.example.net
Valid From	06/12/2023
Valid To	06/13/2033
Issuer	C=NL, ST=Netherlands, L=Amsterdam, O=Juniper, OU=CA
Serial Number	3d32dfbcbdd6ebe5437bef1ca8a94e5f7a2017e4
CRL Distribution Points	http://ca.example.net/crl.pem

The result should look like this:



Common Name	Issuer	Valid To
ca.example.net	C=NL, ST=Netherlands, L=Amsterdam, O=Junipe...	06/13/2033

- Now click on “Import Custom RADIUS Server Certificate”



1
Certificate Authorities
Add Certificate Authority
View Mist Certificate
Import Custom RADIUS Server Certificate

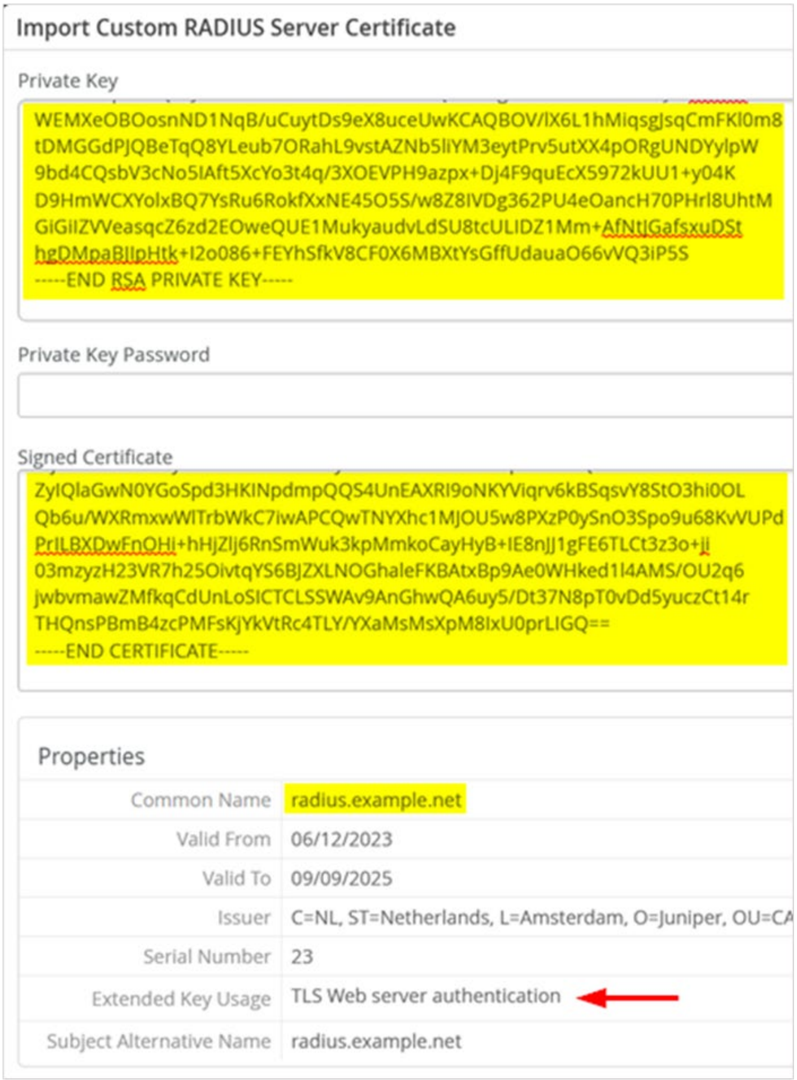
Common Name	Issuer	Valid To
ca.example.net	C=NL, ST=Netherlands, L=Amsterdam, O=Juni...	06/13/2033

- Apply the following configuration:
    - Paste the content of the base64-encoded part of your Enterprise PKI RADIUS Server Certificate-Key into the “Private Key” field.
    - Depending on your Enterprise PKI, your RADIUS Server Certificate may need a password to open the encrypted key. If that is the case, provide this information here.

    - Paste the content of the base64-encoded part of your Enterprise PKI RADIUS Server Certificate-Public into the “Signed Certificate” field.

- Confirm the information in the populated property fields:
    - The common name should be a DNS-FQDN.
    - Extended Key Usage=**TLS Web server authentication**

Figure 32



Import Custom RADIUS Server Certificate

Private Key

```
WEMXeOBOosnND1NqB/uCuytDs9eX8uceUwKCAQBOV/lX6L1hMiqsgJsqCmFKl0m8
tDMGGdPJQBeTqQ8YLeub7ORahL9vstAZNb5liYM3eytPrv5utXX4pORgUNDYylpW
9bd4CQsbV3cNo5lAft5XcYo3t4q/3XOEVPH9azpx+Dj4F9quEcX5972kUU1+y04K
D9HmWCXYolxBQ7YsRu6RokfXxNE45O5S/w8Z8lVDg362PU4eOancH70PHrl8UhtM
GIGiIZVVeasqcZ6zd2EOweQUE1MukyaudvLdSU8tcULIDZ1Mm+AfNtIGafsxuDSt
hgDMpaBJlpHtk+I2o086+FEYhSfkV8CF0X6MBXtYsGffUdauaO66vVQ3iP5S
-----END RSA PRIVATE KEY-----
```

Private Key Password

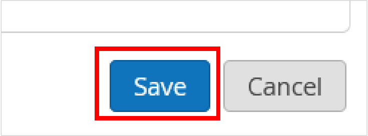
Signed Certificate

```
ZyIQlaGwN0YGoSpd3HKINpdmpQQS4UnEAXRI9oNKYViqrv6kBSqsvY8StO3hi0OL
Qb6u/WXRmxwWlTrbWkC7iwAPCQwTNYXhc1MJOU5w8PXzP0ySnO3Spo9u68KvVUPd
PrILBXDwFnOHi+hHJZlj6RnSmWuk3kpMmkoCayHyB+IE8nJJ1gFE6TLCt3z3o+Ji
03mzyzH23VR7h25OivtqYS6BJZXLNOGhaleFKBAtxBp9Ae0WHked1l4AMS/OU2q6
jwbvmawZMfkqCdUnLoSICTCLSSWAv9AnGhwQA6uy5/Dt37N8pT0vDd5yuczCt14r
THQnsPBmB4zcPMFsKjYkVtRc4TLY/YXaMsMsXpM8IxU0prLIGQ==
-----END CERTIFICATE-----
```

Properties

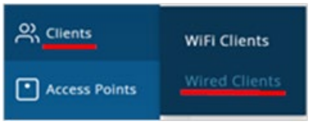
Common Name	radius.example.net
Valid From	06/12/2023
Valid To	09/09/2025
Issuer	C=NL, ST=Netherlands, L=Amsterdam, O=Juniper, OU=CA
Serial Number	23
Extended Key Usage	TLS Web server authentication
Subject Alternative Name	radius.example.net

- Click **Save**.

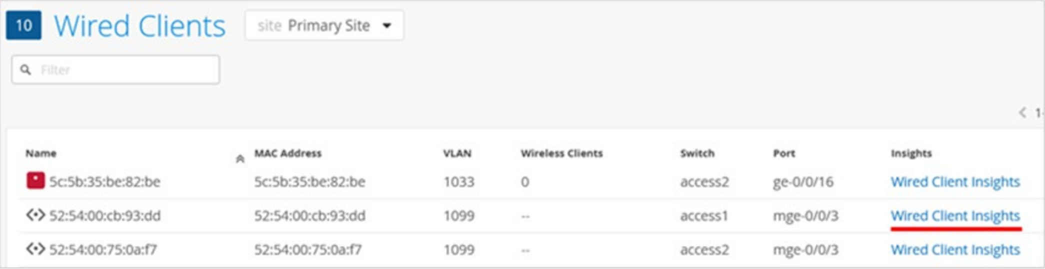


Now you can start to authenticate your EAP-TLS clients.

After your clients are authenticated by Mist Access Assurance you can check the GBP-tag assignment. To do this, navigate to **Clients > Wired Clients**.



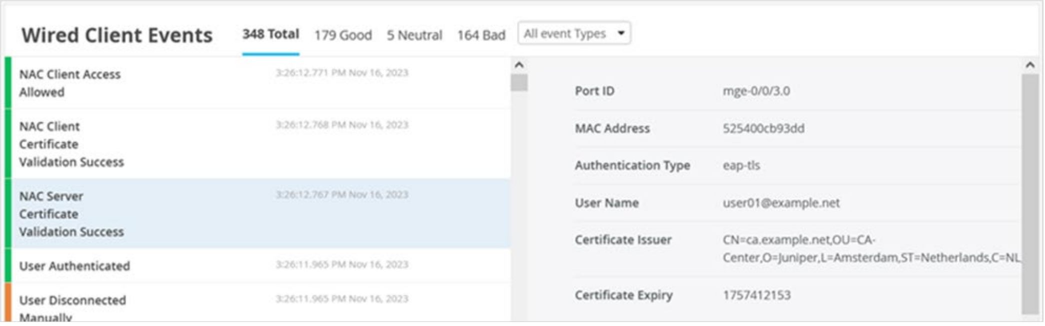
Identify the wired client you have configured and click on **Wired Client Insights**.



10 Wired Clients — site Primary Site

Name	MAC Address	VLAN	Wireless Clients	Switch	Port	Insights
5c:5b:35:be:82:be	5c:5b:35:be:82:be	1033	0	access2	ge-0/0/16	Wired Client Insights
52:54:00:cb:93:dd	52:54:00:cb:93:dd	1099	--	access1	mge-0/0/3	Wired Client Insights
52:54:00:75:0a:f7	52:54:00:75:0a:f7	1099	--	access2	mge-0/0/3	Wired Client Insights

The first check is the Certificate of the RADIUS server.

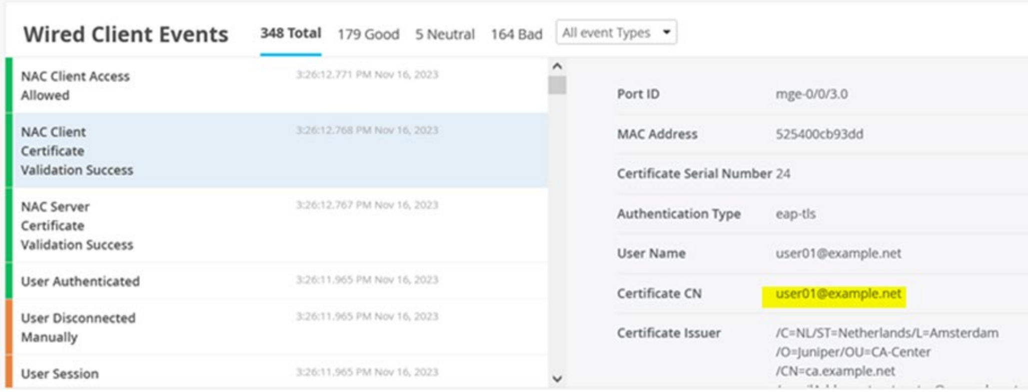


Wired Client Events — 348 Total 179 Good 5 Neutral 164 Bad — All event Types

Event	Time
NAC Client Access Allowed	3:26:12.771 PM Nov 16, 2023
NAC Client Certificate Validation Success	3:26:12.768 PM Nov 16, 2023
NAC Server Certificate Validation Success	3:26:12.767 PM Nov 16, 2023
User Authenticated	3:26:11.965 PM Nov 16, 2023
User Disconnected Manually	3:26:11.965 PM Nov 16, 2023

Port ID	mge-0/0/3.0
MAC Address	525400cb93dd
Authentication Type	eap-tls
User Name	user01@example.net
Certificate Issuer	CN=ca.example.net,OU=CA-Center,O=Juniper,L=Amsterdam,ST=Netherlands,C=NL
Certificate Expiry	1757412153

Next, you see the information about the client certificate from the supplicant that the RADIUS server checked for validation. Here it is important to review the certificate attributes because we use them to identify a single client.



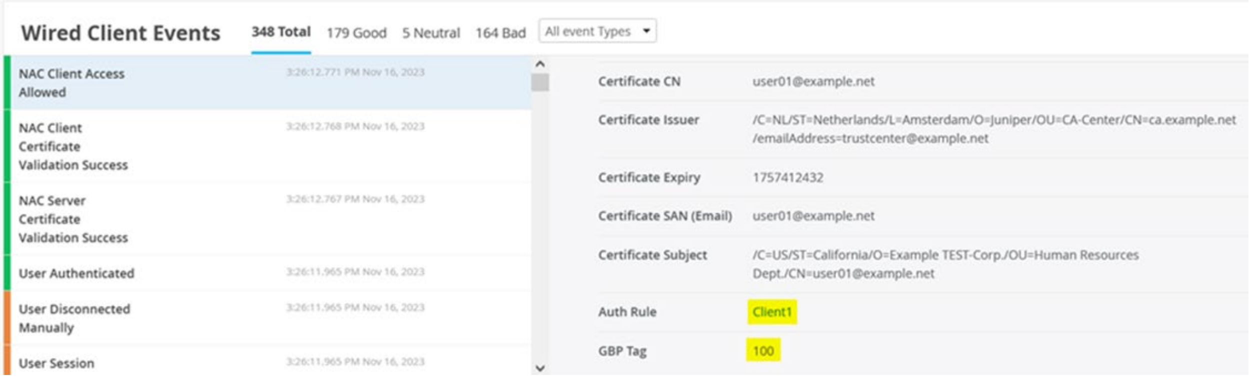
Wired Client Events

348 Total 179 Good 5 Neutral 164 Bad

NAC Client Access Allowed	3:26:12.771 PM Nov 16, 2023
NAC Client Certificate Validation Success	3:26:12.768 PM Nov 16, 2023
NAC Server Certificate Validation Success	3:26:12.767 PM Nov 16, 2023
User Authenticated	3:26:11.965 PM Nov 16, 2023
User Disconnected Manually	3:26:11.965 PM Nov 16, 2023
User Session	3:26:11.965 PM Nov 16, 2023

Port ID	mge-0/0/3.0
MAC Address	525400cb93dd
Certificate Serial Number	24
Authentication Type	eap-tls
User Name	user01@example.net
Certificate CN	user01@example.net
Certificate Issuer	/C=NL/ST=Netherlands/L=Amsterdam /O=Juniper/OU=CA-Center /CN=ca.example.net

Then you see the decision of the NAC system to allow network access for this client and which rule decided it. The GBP-tag assigned can also be reviewed.



Wired Client Events

348 Total 179 Good 5 Neutral 164 Bad

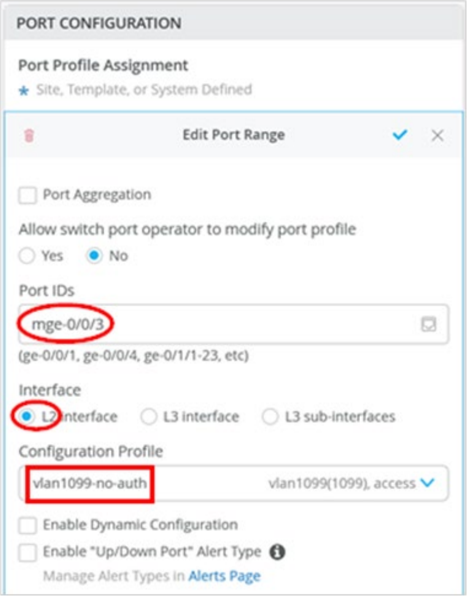
NAC Client Access Allowed	3:26:12.771 PM Nov 16, 2023
NAC Client Certificate Validation Success	3:26:12.768 PM Nov 16, 2023
NAC Server Certificate Validation Success	3:26:12.767 PM Nov 16, 2023
User Authenticated	3:26:11.965 PM Nov 16, 2023
User Disconnected Manually	3:26:11.965 PM Nov 16, 2023
User Session	3:26:11.965 PM Nov 16, 2023

Certificate CN	user01@example.net
Certificate Issuer	/C=NL/ST=Netherlands/L=Amsterdam/O=Juniper/OU=CA-Center/CN=ca.example.net /emailAddress=trustcenter@example.net
Certificate Expiry	1757412432
Certificate SAN (Email)	user01@example.net
Certificate Subject	/C=US/ST=California/O=Example TEST-Corp./OU=Human Resources Dept./CN=user01@example.net
Auth Rule	Client1
GBP Tag	100

Chapter 7 EXAMPLES: Static Client Assignments

When you intend to use static GBP-tag assignments, ensure that the switch ports where your clients are attached use the right port profile. In our case, we used the port profile=”vlan1099-no-auth” (because we do not want any dynamic RADIUS assignment) and configured the switch ports as shown in the example below. Use port IDs appropriate for your environment.

Figure 33



PORT CONFIGURATION

Port Profile Assignment

★ Site, Template, or System Defined

Edit Port Range

□ Port Aggregation

Allow switch port operator to modify port profile

○ Yes ● No

Port IDs

mge-0/0/3

(ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)

Interface

● L2 interface ○ L3 interface ○ L3 sub-interfaces

Configuration Profile

vlan1099-no-auth vlan1099(1099), access

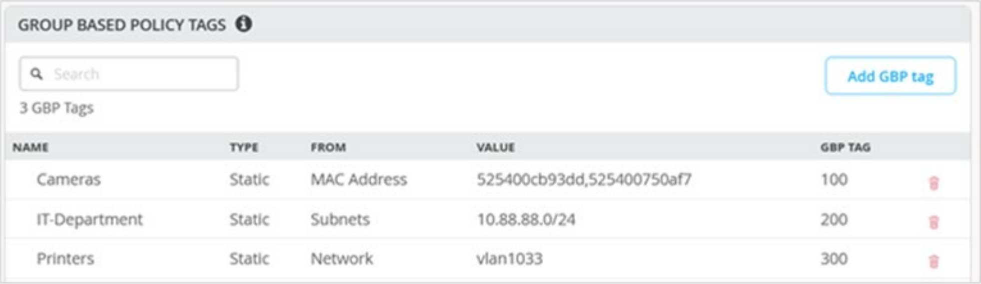
□ Enable Dynamic Configuration

□ Enable "Up/Down Port" Alert Type

Manage Alert Types in Alerts Page

Instead of a dynamic GBP-tag assignment you must now modify the switch template to use static assignments. Here is an example of the configuration used during testing.

Figure 34



GROUP BASED POLICY TAGS

3 GBP Tags

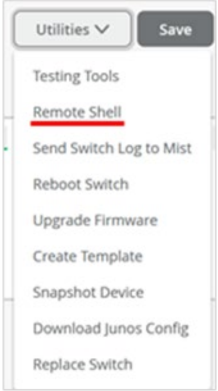
NAME	TYPE	FROM	VALUE	GBP TAG
Cameras	Static	MAC Address	525400cb93dd,525400750af7	100
IT-Department	Static	Subnets	10.88.88.0/24	200
Printers	Static	Network	vlan1033	300

NOTE: Ensure your wireless clients really produce some traffic on the network. For example, Linux clients tend to be rather quiet, meaning you won’t be able to see the GBP-tag appear.

Chapter 8 EXAMPLES: Debugging Examples Using the Junos OS CLI

If you understand Junos CLI, you can utilize the commands shown below when checking something locally on a switch. The Mist GUI can open a remote shell to each switch it manages as shown in Figure 35 .

Figure 35



Below is an example of a successful dynamic authentication using a MAB Auth-capable RADIUS server. You can see the Dynamic Filter attribute set the GBP-tag to 300.

```
root@access1> show dot1x interface mge-0/0/3
802.1X Information:
Interface     Role           State           MAC address          User
mge-0/0/3.0   Authenticator  Authenticated   52:54:00:CB:93:DD
525400cb93dd

root@access1> show dot1x interface mge-0/0/3 detail
mge-0/0/3.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Enabled
  Mac Radius Authentication Protocol: PAP
  Reauthentication: Enabled
  Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: not configured
  Number of connected supplicants: 1
    Supplicant: 525400cb93dd, 52:54:00:CB:93:DD
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Mac Radius
      Authenticated VLAN: vlan1099
      Dynamic Filter: apply action gbp-tag 300
      Session Reauth interval: 3600 seconds
      Reauthentication due in 2595 seconds
      Session Accounting Interim  Interval: 36000 seconds
      Accounting Update  due in 34995 seconds
      Eapol-Block: Not In Effect
      Domain: Data
```

Next is a review of the MAC table of a local switch where in this example:

- The MAC address 52:54:00:75:0a:f7 is reported as reachable remotely via VXLAN-vtep having GBP-tag 300 assigned.
- MAC-Address 52:54:00:cb:93:dd is reported as reachable locally on interface mge-0/0/3.0 with GBP-tag 300 assigned.

```
root@access1> show ethernet-switching table

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P -
Persistent static
           SE - statistics enabled, NM - non configured MAC, R - remote
PE MAC, O - ovsdb MAC)


Ethernet switching table : 4 entries, 4 learned
Routing instance : default-switch
   Vlan                MAC                 MAC       GBP    Logical
SVLBNH/      Active
   name                address             flags     tag    interface
VENH Index   source
   vlan1033            5c:5b:35:be:82:be   DR               vtep.32771
172.16.254.5
   vlan1033            d4:20:b0:01:46:09   D                ge-0/0/16.0
   vlan1099            52:54:00:75:0a:f7   DR         300   vtep.32771
172.16.254.5
   vlan1099            52:54:00:cb:93:dd   D          300   mge-0/0/3.0
```

Below is an example of the Junos OS configuration for dynamically authenticated clients we used while testing.

```
set groups top firewall family any filter gbp_Limited-for-Cameras term 01
from gbp-src-tag 100
set groups top firewall family any filter gbp_Limited-for-Cameras term 01
from gbp-dst-tag 100
set groups top firewall family any filter gbp_Limited-for-Cameras term 01
then discard
set groups top firewall family any filter gbp_Limited-for-Cameras term 02
from gbp-src-tag 100
set groups top firewall family any filter gbp_Limited-for-Cameras term 02
from gbp-dst-tag 200
set groups top firewall family any filter gbp_Limited-for-Cameras term 02
then accept
set groups top firewall family any filter gbp_Limited-for-Cameras term 03
from gbp-src-tag 100
set groups top firewall family any filter gbp_Limited-for-Cameras term 03
from gbp-dst-tag 300
set groups top firewall family any filter gbp_Limited-for-Cameras term 03
then discard
set groups top firewall family any filter gbp_Full-for-IT term 01 from
gbp-src-tag 200
set groups top firewall family any filter gbp_Full-for-IT term 01 from
gbp-dst-tag 100
set groups top firewall family any filter gbp_Full-for-IT term 01 then
accept
set groups top firewall family any filter gbp_Full-for-IT term 02 from
```

```
gbp-src-tag 200
set groups top firewall family any filter gbp_Full-for-IT term 02 from
gbp-dst-tag 200
set groups top firewall family any filter gbp_Full-for-IT term 02 then
accept
set groups top firewall family any filter gbp_Full-for-IT term 03 from
gbp-src-tag 200
set groups top firewall family any filter gbp_Full-for-IT term 03 from
gbp-dst-tag 300
set groups top firewall family any filter gbp_Full-for-IT term 03 then
accept
set groups top firewall family any filter gbp_Limited-Printers term 01
from gbp-src-tag 300
set groups top firewall family any filter gbp_Limited-Printers term 01
from gbp-dst-tag 100
set groups top firewall family any filter gbp_Limited-Printers term 01
then discard
set groups top firewall family any filter gbp_Limited-Printers term 02
from gbp-src-tag 300
set groups top firewall family any filter gbp_Limited-Printers term 02
from gbp-dst-tag 200
set groups top firewall family any filter gbp_Limited-Printers term 02
then accept
set groups top firewall family any filter gbp_Limited-Printers term 03
from gbp-src-tag 300
set groups top firewall family any filter gbp_Limited-Printers term 03
from gbp-dst-tag 300
set groups top firewall family any filter gbp_Limited-Printers term 03
then discard
set groups top chassis forwarding-options vxlan-gbp-profile
set forwarding-options evpn-vxlan gbp mac-ip-inter-tagging
```