



Alcatel-Lucent OmniAccess Stellar Access Point authentication and deployment Application Note

Release 2.1.1

Table of Contents

Hardware/Firmware requirements	3
Executive summary	3
Mac authentication	3
Introduction.....	3
Authentication against an external RADIUS server	3
Authentication policy on Windows server	3
OmniSwitch configuration through OmniVista	8
OmniSwitch configuration through CLI	11
Authentication using OmniVista UPAM RADIUS server	12
Create an Access Role Profile (ARP)	12
Create an authentication strategy	14
802.1x authentication	16
Introduction.....	16
Workflow	16
802.1x using OmniVista UPAM (Built-in certificates).....	16
Create an AAA Server Profile	16
Create an Access Role Profile and Deployment	17
Create an Access Auth Profile	18
Create an Authentication Strategy	19
Create an Access Policy	19
Create an AP group	20
802.1x using OmniVista UPAM (Custom Certificate)	20
Create a Certification Authority	20
Create an Access Point Certificate and assign to AP group	20
Import the access point certificate to OmniVista	20
Import the CA Certificate to OmniVista.....	22
Verification	22

802.1x using OmniVista (ADCS Certificates)22

- OmniAccess Stellar Access Point deployment23
- Scenario23
- Deployment Workflow23
- Import24
- Authentication24

Conclusion24

Hardware/Firmware requirements

OmniAccess Stellar: AWOS 4.0.4 or higher

Notice: OmniAccess Stellar AP1101 does not support supplicant option for 802.1x

OmniSwitch: AOS 8.8R01/AOS 6.7.2R02 MR build 160 or higher

OmniVista 2500 NMS: 4.6R2

OmniVista Cirrus: 4.6.2

Executive summary

The purpose of this document is to provision Alcatel-Lucent OmniAccess® Stellar Access Points (AP) securely, to avoid security breaches such as rogue APs. This document is intended as a guide. It will demonstrate how to implement security policies and protocols to protect your network's integrity. Also, this guide explains how easy it is to integrate complicated configurations with the Alcatel-Lucent OmniVista® 2500 Network Management System.

Mac authentication

Introduction

Media Access Control (MAC) is a simple authentication method that does not require certificates or Public Key Infrastructure (PKI). When using MAC authentication, a device's MAC address is verified against a list of allowed MAC addresses using the RADIUS protocol. MAC authentication is a weak form of authentication because MAC addresses can be easily spoofed. However, as we will see later in this document, MAC authentication can complement other more secure methods such as 802.1x.

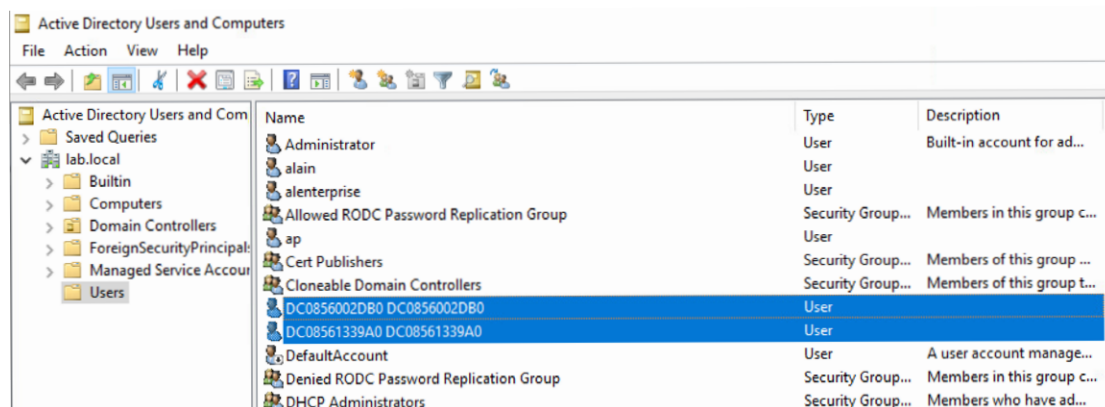
Authentication against an external RADIUS server

RADIUS is a standard protocol. Every RADIUS server will be able to authenticate an OmniAccess Stellar Access Point. Indeed, for this scenario, we will use a Network Policy Server (Windows). We're going to configure all the requirements to enable authentication on an OmniAccess Stellar Access Point based on the MAC address against an external RADIUS authentication server. For that we will use the following components:

- Windows Server: Active Directory, Network Policy Server (NPS)
- OmniSwitch: RADIUS client
- OmniAccess Stellar Access Point: End point
- OmniVista 2500 NMS: NAC configuration

Authentication policy on Windows server

In this section we will configure a policy to allow the OmniAccess Stellar Access Point to authenticate using NPS. The first step will be to create a username for each MAC address, as follows:



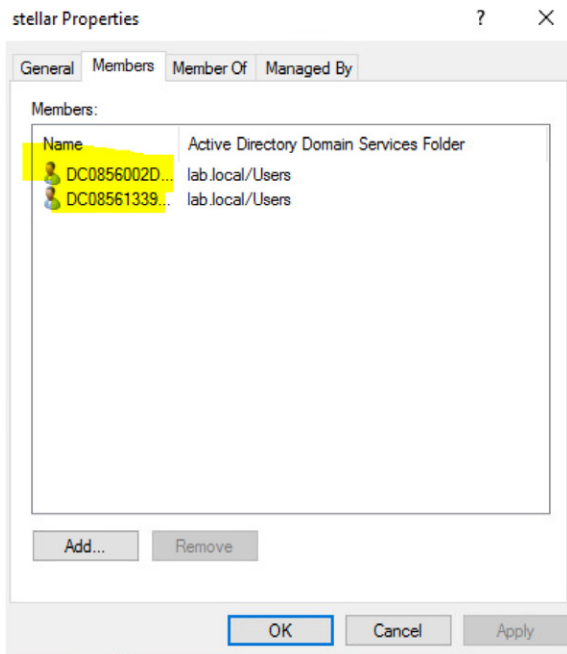
Application note

OmniAccess Stellar Access Point authentication and deployment application note

Powershell scripts can help you import a large number of MAC address from a .csv.

Notice: The password is the same string as the username.

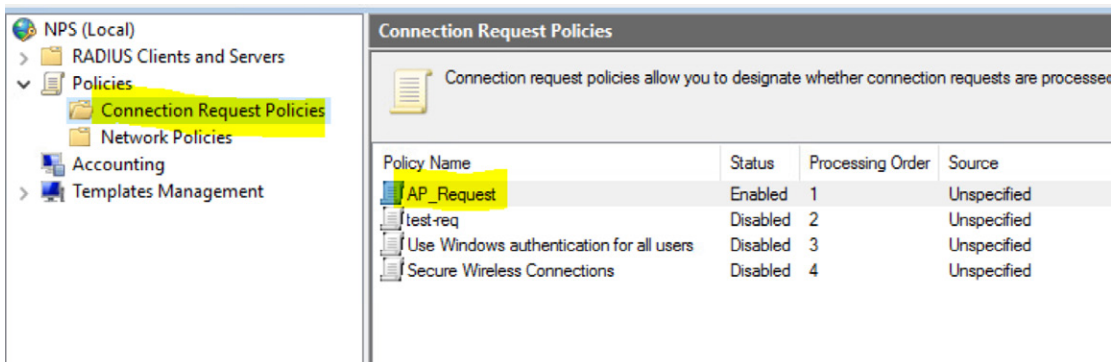
Once you've created the users, you should create a group to contain all of the users. In this example, we have created a group named stellar. Inside this group you can see our two previous users.



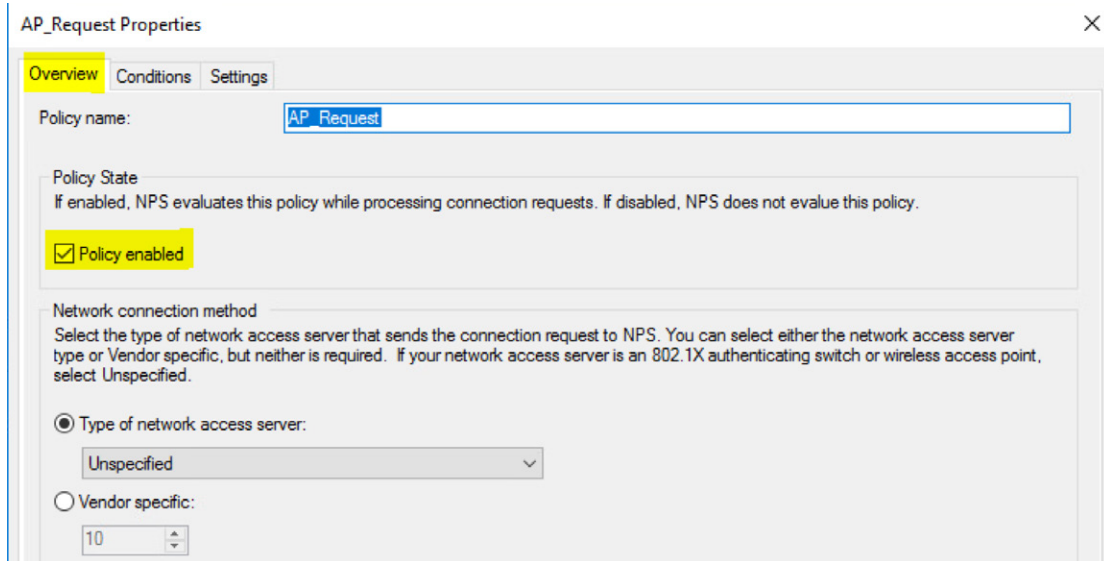
Now we can create the authentication rule for our access point. We will use **Network Policy Server (NPS)**.

Notice: Before you continue, you need to register your NPS server in the Active Directory. Also you will need to add a RADIUS client, which in our case is an Alcatel-Lucent OmniSwitch®.

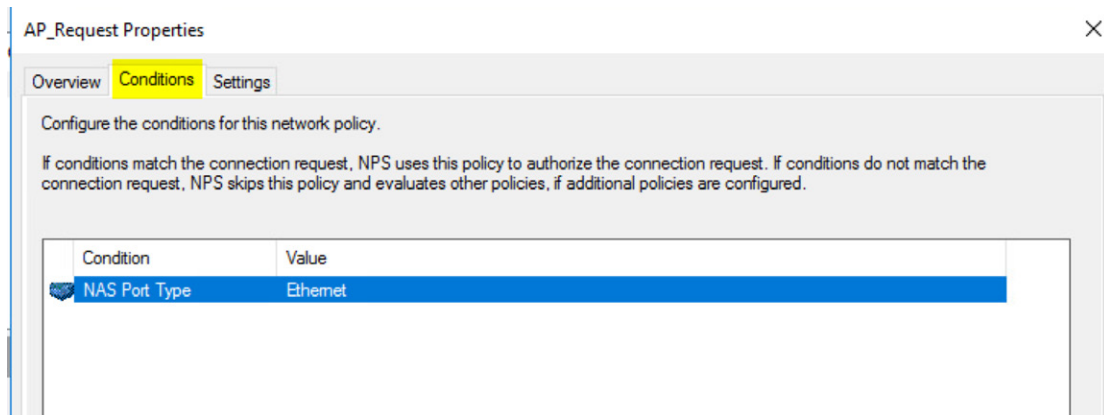
We will begin by creating a **Connection Request Policy**.



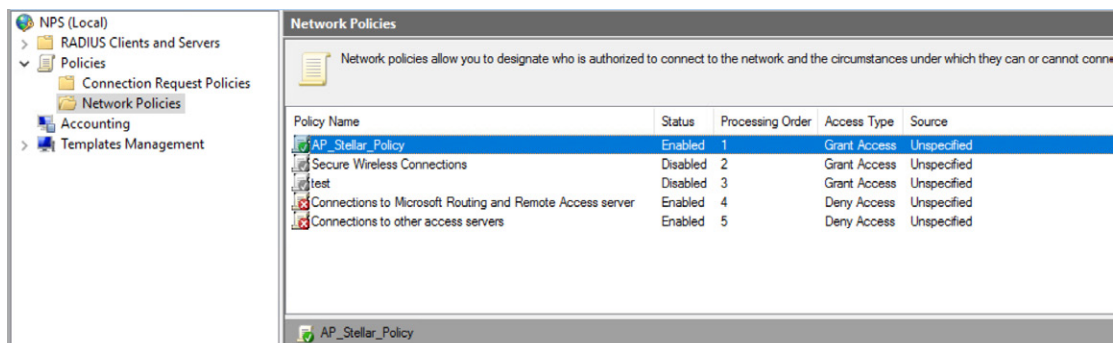
This policy will contain the parameters identified below. In the **Overview** panel select **Policy enabled**.



In the **Conditions** panel, choose **NAS Port Type**; under **Value** you should see **Ethernet**.



Click **OK**. You can now proceed to **Network Policies**. We have created a policy named **AP_Stellar_Policy**.



Application note

Following is the **Overview** of the policy.

The screenshot shows the 'AP_Stellar_Policy Properties' dialog box with the 'Overview' tab selected. The 'Policy name' field contains 'AP_Stellar_Policy'. The 'Policy State' section has 'Policy enabled' checked. The 'Access Permission' section has 'Grant access' selected. The 'Network connection method' section has 'Type of network access server' selected with 'Unspecified' in the dropdown menu.

AP_Stellar_Policy Properties

Overview Conditions Constraints Settings

Policy name: AP_Stellar_Policy

Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

Policy enabled

Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

Grant access. Grant access if the connection request matches this policy.
 Deny access. Deny access if the connection request matches this policy.
 Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:
Unspecified

Vendor specific:
10

The **Conditions** must match with the parameters below:

The screenshot shows the 'AP_Stellar_Policy Properties' dialog box with the 'Conditions' tab selected. It displays a table with two conditions: 'NAS Port Type' with value 'Ethernet' and 'User Groups' with value 'LAB\stellar'.

AP_Stellar_Policy Properties

Overview Conditions Constraints Settings

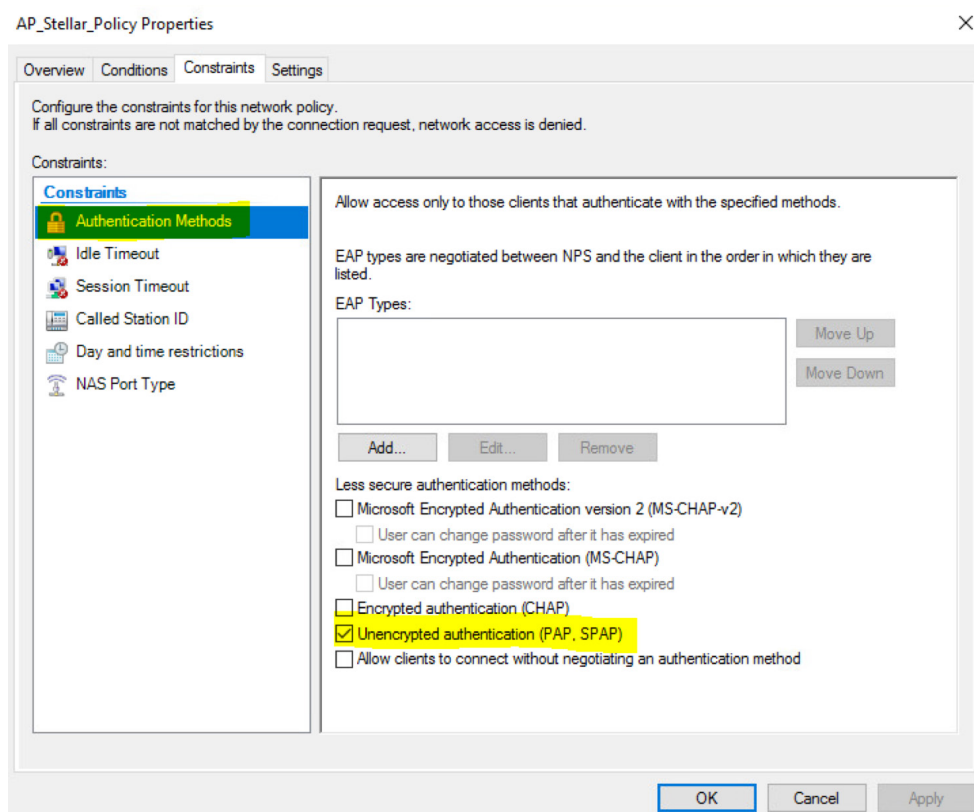
Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

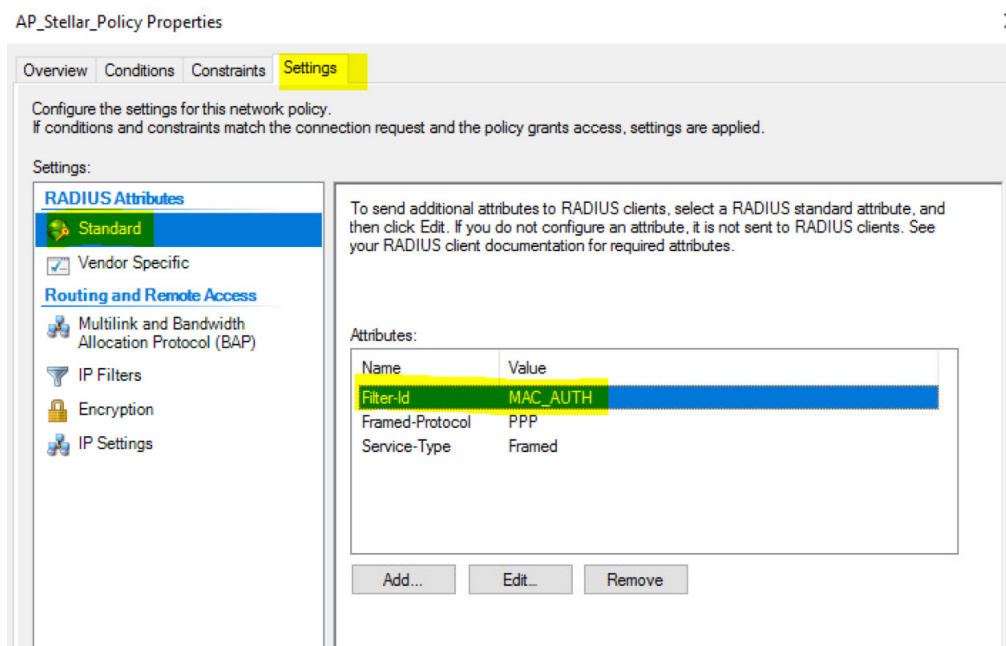
Condition	Value
NAS Port Type	Ethernet
User Groups	LAB\stellar

We can now return to the **stellar** group we created earlier.

The **Constraints** tab will enable you to choose the authentication protocol for the policy. To do this, you need to select **Unencrypted authentication (PAP, SPAP)**.



In the last tab labelled **Settings**, you will need to add a custom attribute which is the **Filter-Id**. The Filter-id must match with the UNP/ARP profile configured on your OmniSwitch. For this example, it's **MAC_AUTH**.



The authentication process on the authentication server is now complete. We can proceed to the OmniVista configuration.

Application note

OmniSwitch configuration through OmniVista

Following is the process to enable a secure port on an OmniSwitch through OmniVista:

- Add an authentication server
- Create an AAA profile
- Create an Access Auth Profile and Deployment
- Create an Access Role Profile and Deployment

Adding an authentication server

Home > Security > Authentication Servers > RADIUS > Create Server

RADIUS Server Management

Create RADIUS Server

* Server Name: RADIUS_Windows

* Host Name/IP Address: 172.20.1.1

Backup Host Name/IP Address: Enter Backup Host Name/IP Address (v4 | v6)

Retries: 3

Timeout: 2

* Shared Secret:

* Confirm Secret:

Authentication Port: 1812

Accounting Port: 1813

VRF Name: default

Create Cancel

Create an AAA profile

AAA Server Profile

Create AAA Server Profile

*Profile Name: RADIUS_Srv_Profile

Authentication Servers

802.1X	
MAC	
MAC Primary	RADIUS_Windows
Secondary	
Tertiary	
Quaternary	

Accounting Servers

Advanced Settings (Optional)

Create Cancel

Application note

OmniAccess Stellar Access Point authentication and deployment application note

Creating an Access Auth Profile and Deployment

Home > Unified Access > Unified Profile > Template > Access Auth Profile

Access Auth Profile

Create Access Auth Profile no Highlight

* Profile Name:

Default Settings

AAA Server Profile:

Port-Bounce:

MAC Auth: ENABLE

802.1X Auth:

Dynamic Service:

Customer Domain ID:

L2 Profile:

AP Mode: ENABLE

Secure:

Home > Unified Access > Unified Profile > Template > Access Auth Profile

Access Auth Profile

Apply to Devices: Clone + [F] [B] [M] [O] [R]

Search:

Profile Name	AAA Server Profile	Port-Bounce	MAC Auth
<input type="checkbox"/> ovBridgeDefaultPortTemplate		Disable	Enable
<input type="checkbox"/> ovWirelessDefaultPortTempl...		Disable	Enable
<input type="checkbox"/> ovAccessDefaultPortTemplate		Disable	Enable
<input checked="" type="checkbox"/> Radius_Auth_Profile	Radius_Srv_Profile	Disable	Enable

Show: All Showing All 4 rows

Default Settings

Profile Name	Radius_Auth_Profile
AAA Server Profile	Radius_Srv_Profile
Port-Bounce	Disable
MAC Auth	Enable
802.1X Auth	Disable
Dynamic Service	none
Customer Domain ID	0
L2 Profile	
AP Mode	Enable
Secure	Enable

No Auth/Failure/Alternate

Creating an Access Role Profile and Deployment

Home > Unified Access > Unified Profile > Template > Access Auth Profile

Access Role Profile

Edit Access Role Profile no Highlight

* Profile Name:

Access Role Profile Attributes

We now define the profile name. This name should match the Filter-Id you've set in the RADIUS server settings. If the authentication is successful, the Access Point will be mapped to the VLAN 115, which is the management VLAN .

Notice: If you wish to restrict more traffic you can add a policy list to only tolerate traffic toward the OmniVista IP address. To do this you will need to apply the policy list rules to your Access Role Profile.

Application note

OmniAccess Stellar Access Point authentication and deployment application note

Access Role Profile

☰ Access Role Profile Assignments

1. Select Devices
2. Configure the period policy
3. Configure the location policy
4. Review

Select Devices

Select the mapping method for access role profile(s) and devices to apply the configuration

Configure the mapping method for RadiusProfile

Mapping Method: Map To VLAN

VLAN(s): 115 +
(e.g. 5 or 10-20)

Select devices to apply the configuration

1 Device EDIT 0 AP Groups ADD

List of Selected Devices

Search all ...

Friendly Name	Type	Version	Status	Name
172.20.1.254	OS2360-P24	5.1.43.R02	Up	OS2360

Access Auth Profile Assignments

Access Auth Profile Radius_Auth_Profile

1. Select Devices

Select Devices

Select the mapping method for access role profile(s) and devices to apply the configuration

Configure the mapping method for RadiusProfile

Mapping Method: Map To VLAN

VLAN(s): 115 +
(e.g. 5 or 10-20)

Select devices to apply the configuration

1 Device EDIT 0 AP Groups ADD

List of Selected Devices

Search all ...

Friendly Name	Type	Version	Status	Name	Address	MAC Address	Location	DNS Name
172.20.1.254	OS2360-P24	5.1.43.R02	Up	OS2360	172.20.1.254	94-24-e155-8b-7d	Unknown	

Add Port
Port Type: VLAN Port
 UNP VLANs: Add UNP VLANs

ⓘ Add/Remove Ports

AVAILABLE 27

Search all ...

<input type="checkbox"/>	Port	Description	IF Index	Alias
<input type="checkbox"/>	1/1/1	Alcatel-Lucent Enterprise OS236...	1001	N/A
<input type="checkbox"/>	1/1/2	Alcatel-Lucent Enterprise OS236...	1002	N/A
<input type="checkbox"/>	1/1/3	Alcatel-Lucent Enterprise OS236...	1003	N/A
<input type="checkbox"/>	1/1/4	Alcatel-Lucent Enterprise OS236...	1004	N/A
<input type="checkbox"/>	1/1/5	Alcatel-Lucent Enterprise OS236...	1005	N/A
<input type="checkbox"/>	1/1/6	Alcatel-Lucent Enterprise OS236...	1006	N/A
<input type="checkbox"/>	1/1/8	Alcatel-Lucent Enterprise OS236...	1008	N/A
<input type="checkbox"/>	1/1/9	Alcatel-Lucent Enterprise OS236...	1009	N/A
<input type="checkbox"/>	1/1/10	Alcatel-Lucent Enterprise OS236...	1010	N/A
<input type="checkbox"/>	1/1/11	Alcatel-Lucent Enterprise OS236...	1011	N/A
<input type="checkbox"/>	1/1/12	Alcatel-Lucent Enterprise OS236...	1012	N/A
<input type="checkbox"/>	1/1/13	Alcatel-Lucent Enterprise OS236...	1013	N/A

Showing all 27 items Showing Page 1 of 3

SELECTED 1

Search all ...

<input checked="" type="checkbox"/>	Port	Description	IF Index	Alias
<input checked="" type="checkbox"/>	1/1/7	Alcatel-Lucent Enterprise OS236...	1007	N/A

Showing all 1 item Showing Page 1 of 1

OK
Cancel

Application note

OmniSwitch results

Once the configuration has been applied, we can see that the access point has been successfully authenticated.

```
→ sh unp user
Port      Username      Mac address      User IP      Vlan Profile      Type      Status
-----+-----+-----+-----+-----+-----+-----
1/1/7    dc:08:56:13:39:a0  dc:08:56:13:39:a0  -            115 RadiusProfile      Bridge      Active

Total users : 1

→ sh unp user details
Port: 1/1/7
MAC-Address: dc:08:56:13:39:a0
SAP = -,
Access Timestamp = 01/25/2023 10:25:40,
User Name = dc:08:56:13:39:a0,
IP-Address = 192.168.115.52,
Vlan = 115,
Authentication Type = Mac,
Authentication Status = Authenticated,
Authentication Failure Reason = -,
Authentication Retry Count = 0,
Authentication Server IP Used = 172.20.1.1,
Authentication Server Used = Radius Windows,
```

OmniSwitch configuration through CLI

Following is the process to enable a secure port on an OmniSwitch through CLI:

- Add a RADIUS server
- Create an AAA profile
- Create a UNP profile and template
- Apply an authentication method on the UNP port

Add a RADIUS server

```
aaa radius-server "DC1" host 172.20.1.1 auth-port 1812 key alcatel
```

Create an AAA Profile

```
aaa profile "MAC_AUTH_Profile"
aaa profile "MAC_AUTH_Profile" device-authentication mac "DC1"
```

Create a UNP profile and template

We define the profile name. This name should match with the Filter-Id you've set in the RADIUS server settings. If the authentication is successful, the access point will be mapped to the VLAN 115, which is the management VLAN .

Notice: If you wish to restrict more traffic you can add a policy list to only tolerate traffic toward the OmniVista IP address.

```
unp profile "MAC_AUTH"
unp profile "MAC_AUTH" map vlan 115

unp port-template MAC_AUTH direction both aaa-profile "MAC_AUTH_Profile"
classification ap-mode secure admin-state enable
unp port-template MAC_AUTH mac-authentication
```

Applying an authentication method on the UNP port

```
unp port 1/1/5 port-type bridge
unp port 1/1/5 port-template MAC_AUTH
```

Application note

OmniAccess Stellar Access Point authentication and deployment application note

Authentication using OmniVista UPAM RADIUS server

In this scenario we're going to configure all the requirements to enable authentication on the OmniAccess Stellar Access Point, based on the MAC Address UPAM which is the authentication module embedded in the OmniVista 2500 NMS . To do this we will use the following components:

- OmniSwitch: RADIUS client
- OmniAccess Stellar Access Point: End point
- OmniVista 2500 NMS: Authentication server, configuration

Create an Access Role Profile (ARP)

First, we are going to create a profile and map it to a VLAN. The management VLAN ID is 115.

Home > Unified Access > Unified Profile > Template > Access Role Profile

Access Role Profile

Create Access Role Profile

* Profile Name

Access Role Profile Attributes

Auth Flag DISABLE

Mobile Tag Status DISABLE

Redirect Status DISABLE

Once created, we must apply the **ARP** to the access switch to which the AP is connected.

Home > Unified Access > Unified Profile > Template > Access Role Profile

Access Role Profile

Access Role Profile

Search ...

<input type="checkbox"/>	Profile Name	Auth Flag	Mobile Tag Status	Redirect Status
<input type="checkbox"/>	defaultWLANProfile	Disable	Disable	Disable
<input type="checkbox"/>	RadiusProfile	Disable	Disable	Disable
<input checked="" type="checkbox"/>	UPAM_MAC	Disable	Disable	Disable

Access Role Profile Attributes

Profile Name UPAM_MAC

Auth Flag Disable

Mobile Tag Status Disable

Redirect Status Disable

Policy List

Location Policy Name

Period Policy Name

Inactivity Interval

We choose the VLAN we want to map to the **ARP** we've just created. To complete this process, select the access switch, then click on **Apply**.

Access Role Profile

☰ Access Role Profile Assignments

1. Select Devices
2. Configure the period policy
3. Configure the location policy
4. Review

Select Devices

Select the mapping method for access role profile(s) and devices to apply the configuration

Configure the mapping method for UPAM_MAC

Mapping Method:

VLAN(s): (e.g. 5 or 10-20)

Select devices to apply the configuration

1 Device EDIT 0 AP Groups ADD

List of Selected Devices

Search all ...

Friendly Name	Type	Version	Sta
172.20.1.254	OS2360-P24	5.1.43.R02	+

Importing the access point MAC address

For the first step, we will import the list of access point MAC addresses into the OmniVista local database. It will be used as a reference for authentication. It helps automate the identity creation.

Home > UPAM > Authentication > Company Property

Company Property

Print PSK Print QR Code Import +

Company Property Online Devices

Search ▼ Reset Export to .csv

Employee Account	Device Mac	Device Name	Device Category	Device Family	Device OS
No items to show					

Click this button more data.

Got It!

When you click on **Import** you can download a template to import identities.

Import File

Template

Browse

Note:

- Only support xls/csv/xlsx file.
- No more than 50,000 data per file.

Import
Cancel

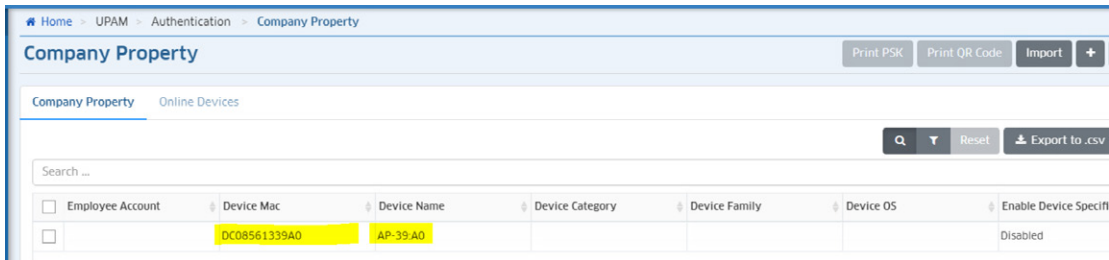
Application note

OmniAccess Stellar Access Point authentication and deployment application note

Notice: Be sure to specify the Access Role Profile name in the file you wish to import. Following is an example of the file .

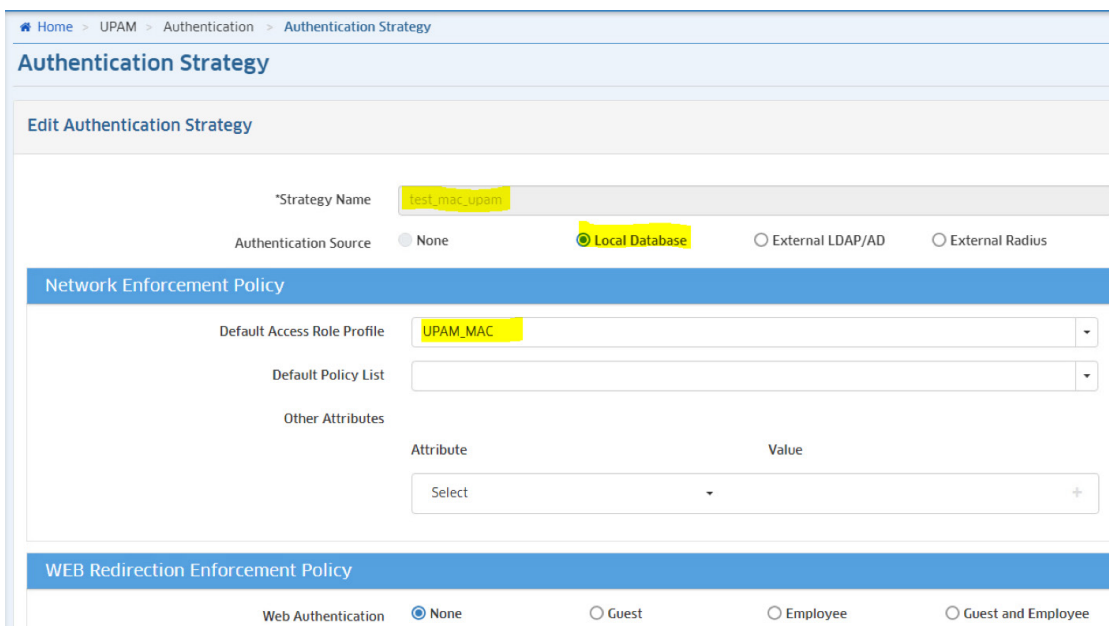
Device Mac(*)	Device Name	Employee Account	Device OS	Access Role Profile	Policy List
df:df:de:ee:ff:f2	AP-NAME1	AccessPoint	Unknown	UPAM_MAC	Policy1

Once the import process is complete you will be able to see all the access point identities on the **Company Property** tab.



Create an authentication strategy

We can now create an authentication strategy. Specify **Local Database**, as the authentication is verified with the OmniVista UPAM RADIUS server and the Access Role Profile previously defined.



Create an Access Policy

To complete the configuration, we create a Policy. First define a **Policy Name** and set a **Priority**. Next, specify the **Mapping Condition** for the authentication. Set the **Authentication Type** to **MAC** and the **Network Type** to **Wired**. These conditions will help to filter incoming requests. Last, select the Authentication Strategy you set up in the previous step.

Access Policy

Edit Access Policy

*Policy Name: test_mac_upam_ap

*Priority: 5

*Mapping Condition: Basic Attribute Advanced Attribute

Attribute	Operator	Value
Select		Add
Authentication Type	Equals	MAC
Network Type	Equals	Wired

*Authentication Strategy: test_mac_upam

OmniVista results

On the Authentication Record tab we can see the access point has been successfully authenticated with the configured parameters.

Authentication Record

Authentication Record List

Account Name	Client IPv4	Client IPv6	Device MAC
<input checked="" type="checkbox"/> DC08561339A0			DC08561339A0
<input type="checkbox"/> DC08561339A0			DC08561339A0
<input type="checkbox"/> DC08561339A0			DC08561339A0
<input type="checkbox"/> DC08561339A0			DC08561339A0
<input type="checkbox"/> DC08561339A0			DC08561339A0
<input type="checkbox"/> DC08561339A0			DC08561339A0

Showing All 7 rows

Basic

Account Name: DC08561339A0

Account Type: Employee

Client IPv4:

Client IPv6:

Device MAC: DC08561339A0

Authentication Type: MAC

Service Type: Call-Check

Auth Resource: Local Database

Access Policy: test_mac_upam_ap

Authentication Strategy: test_mac_upam

Web Access Strategy:

Authentication Result: Pass

Session Start: Jan 25, 2023 5:27:15 pm

Application note

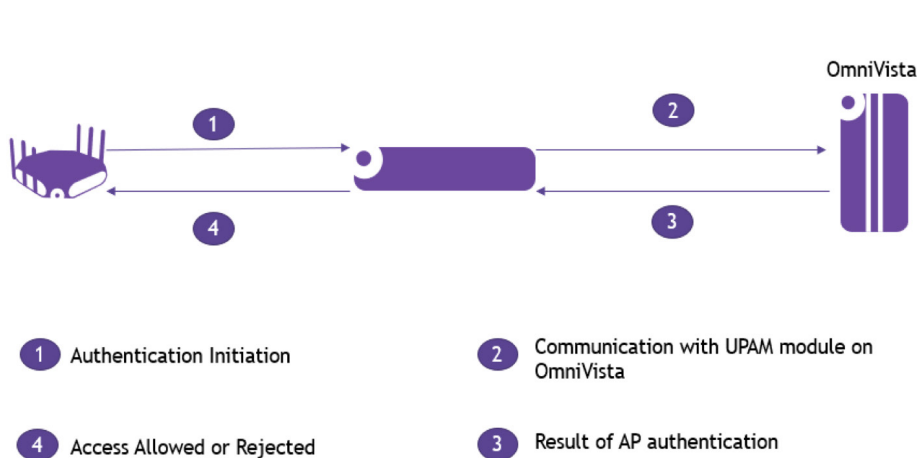
OmniAccess Stellar Access Point authentication and deployment application note

802.1x authentication

Introduction

EAP-TLS is considered the gold standard for network authentication security, however, despite being universally recognised as ultra-secure, it's still not widely implemented. That's largely because EAP-TLS was developed before the industry had the mature device onboarding solutions necessary for smooth device configuration at an enterprise-scale. Despite its reputation for being a complex protocol to implement, it is very simple to configure using OmniVista UPAM .

Workflow



802.1x using OmniVista UPAM (Built-in certificates)

Create an AAA Server Profile

We need to create a Profile to define the Server to which the access points will authenticate. For this scenario it will be the OmniVista UPAM authentication module.

The screenshot shows the configuration page for an AAA Server Profile. The breadcrumb navigation is: Home > Unified Access > Unified Profile > Template > AAA Server Profile. The page title is "AAA Server Profile". Below the title, there is a "Create AAA Server Profile" section. The "Profile Name" field is set to "UPAM_1x". Below this, there is a section for "Authentication Servers" with a sub-section for "802.1X". The "802.1X Primary" field is set to "UPAMRadiusServer". The "Secondary", "Tertiary", and "Quaternary" fields are empty.

Application note

OmniAccess Stellar Access Point authentication and deployment application note

Create an Access Role Profile and Deployment

For this scenario we're going to use another ARP name and another Management VLAN in order to create a clean configuration. First, we create an Access Role Profile and we map it to the Management VLAN.

Access Role Profile

Create Access Role Profile

* Profile Name

Access Role Profile Attributes

- Auth Flag
- Mobile Tag Status
- Redirect Status

Home > Unified Access > Unified Profile > Template > Access Role Profile

Access Role Profile

[Apply to Devices](#) [Clone](#)

Access Role Profile

Search ...

Profile Name	Auth Flag	Mobile Tag Status	Redirect Status
<input type="checkbox"/> defaultWLANProfile	Disable	Disable	Disable
<input type="checkbox"/> RadiusProfile	Disable	Disable	Disable
<input type="checkbox"/> UPAM_MAC	Disable	Disable	Disable
<input type="checkbox"/> _test	Disable	Disable	Disable
<input checked="" type="checkbox"/> UPAM_1X_ARP	Disable	Disable	Disable

Show: All Showing All 5 rows

Access Role Profile Attributes

Profile Name UPAM_1X_ARP

- Auth Flag Disable
- Mobile Tag Status Disable
- Redirect Status Disable

Policy List

- Location Policy Name
- Period Policy Name
- Inactivity Interval

Bandwidth Control Settings

- Upstream Bandwidth

Access Role Profile

Access Role Profile Assignments

- Select Devices
- Configure the period policy
- Configure the location policy
- Review

Select Devices

Select the mapping method for access role profile(s) and devices to apply the configuration

Configure the mapping method for UPAM_1X_ARP

Mapping Method

VLAN(s) (e.g. 5 or 10-20)

Select devices to apply the configuration

1 Device [EDIT](#) 0 AP Groups [ADD](#)

List of Selected Devices

Search all ...

Friendly Name	Type	Version	Status
172.20.1.254	OS2360-P24	5.1.43.R02	Up

Application note

OmniAccess Stellar Access Point authentication and deployment application note

Create an Access Auth Profile

Next, we create an Access Role Profile where we define the AAA profile to use and the authentication method that the destination port will support.

Home > Unified Access > Unified Profile > Template > Access Auth Profile

Access Auth Profile

Create Access Auth Profile

* Profile Name **UPAM_1x_AAP**

Default Settings

AAA Server Profile **UPAM_1x**

Port-Bounce DISABLE

MAC Auth DISABLE

802.1X Auth ENABLE

Dynamic Service

Customer Domain ID

L2 Profile

AP Mode ENABLE Secure

Then, we apply the configuration to the destination switch and ports.

Home > Unified Access > Unified Profile > Template > Access Auth Profile

Access Auth Profile

Apply to Devices Clone +

Access Auth Profile [Search] [Filter] [Reset] [Export to .csv] [Add to Report] [Print] [Share]

Search ...

Profile Name	AAA Server Profile	Port-Bounce	MAC Auth
<input type="checkbox"/> ovBridgeDefaultPortTemplate		Disable	Enable
<input type="checkbox"/> ovWirelessDefaultPortTemp...		Disable	Enable
<input type="checkbox"/> ovAccessDefaultPortTemplate		Disable	Enable
<input type="checkbox"/> Radius_Auth_Profile	Radius_Srv_Profile	Disable	Enable
<input type="checkbox"/> UPAM_MAC_AAP	UPAM_MAC	Disable	Disable
<input checked="" type="checkbox"/> UPAM_1x_AAP	UPAM_1x	Disable	Disable

Default Settings

Profile Name UPAM_1x_AAP

AAA Server Profile UPAM_1x

Port-Bounce Disable

MAC Auth Disable

802.1X Auth Enable

Dynamic Service none

Customer Domain ID 0

L2 Profile

Access Auth Profile

Access Auth Profile Assignments

Access Auth Profile **UPAM_1x_AAP**

Devices

1 Device **EDIT** 0 AP Groups **ADD**

List of Selected Devices

Search all ...

Friendly Name	Type	Version	Status
172.20.1.254	OS2360-P24	5.1.43.R02	Up

Add Port
Port Type: VLAN Port
UNP VLANs: Add UNP VLANs

Application note

OmniAccess Stellar Access Point authentication and deployment application note

Add/Remove Ports

AVAILABLE 27

Search all ...

<input type="checkbox"/>	Port	Description	IF Index	Alias
<input type="checkbox"/>	1/1/1	Alcatel-Lucent Enterprise OS236...	1001	N/A
<input type="checkbox"/>	1/1/2	Alcatel-Lucent Enterprise OS236...	1002	N/A
<input type="checkbox"/>	1/1/3	Alcatel-Lucent Enterprise OS236...	1003	N/A
<input type="checkbox"/>	1/1/4	Alcatel-Lucent Enterprise OS236...	1004	N/A
<input type="checkbox"/>	1/1/5	Alcatel-Lucent Enterprise OS236...	1005	N/A
<input type="checkbox"/>	1/1/6	Alcatel-Lucent Enterprise OS236...	1006	N/A
<input type="checkbox"/>	1/1/7	Alcatel-Lucent Enterprise OS236...	1007	N/A
<input type="checkbox"/>	1/1/9	Alcatel-Lucent Enterprise OS236...	1009	N/A
<input type="checkbox"/>	1/1/10	Alcatel-Lucent Enterprise OS236...	1010	N/A
<input type="checkbox"/>	1/1/11	Alcatel-Lucent Enterprise OS236...	1011	N/A
<input type="checkbox"/>	1/1/12	Alcatel-Lucent Enterprise OS236...	1012	N/A
<input type="checkbox"/>	1/1/13	Alcatel-Lucent Enterprise OS236...	1013	N/A

Showing all 27 items Showing Page 1 of 3

SELECTED 1

Search all ...

<input type="checkbox"/>	Port	Description	IF Index	Alias
<input checked="" type="checkbox"/>	1/1/8	Alcatel-Lucent Enterprise OS236...	1008	N/A

Showing all 1 item Showing Page 1 of 1

Create an Authentication Strategy

Home > UPAM > Authentication > Authentication Strategy

Authentication Strategy

Create Authentication Strategy

*Strategy Name:

Authentication Source: None Local Database External LDAP/AD External Radius

Network Enforcement Policy

Default Access Role Profile:

Default Policy List:

Other Attributes

Attribute	Value
Select	

WEB Redirection Enforcement Policy

Web Authentication: None Guest Employee Guest and Employee

Create an Access Policy

Home > UPAM > Authentication > Access Policy

Access Policy

Create Access Policy

*Policy Name:

*Priority:

*Mapping Condition: Basic Attribute Advanced Attribute

Attribute	Operator	Value
Select		
Authentication.Type	Equals	802.1X

*Authentication Strategy:

Application note

Create an AP group

Create New Group

General

*Group Name: Group1

Group Description: [Empty text area]

Auto-Group VLANs: [Empty text area]

*RF Profile: default profile

802.1X Suppliant on AP Management Port

802.1X Suppliant: ON

*Certificate for 802.1X: Select

Time

Timezone: Certs

802.1x using OmniVista UPAM (Custom Certificate)

In this section we will use openssl to create our own Certification Authority (CA) and generate a certificate for multiple access points among a single AP Group. Then we will import the certificates into OmniVista which will be responsible for authentication.

Create a Certification Authority

```
openssl genrsa -out rootCAKey.pem 2048
openssl req -x509 -sha256 -new -nodes -key rootCAKey.pem -days 3650 -out
rootCACert.pem
```

Create an Access Point Certificate and assign to AP group

```
openssl genrsa -des3 -out ap_server.key 2048
openssl req -new -key ap_server.key -out ap_server.csr -sha256
openssl x509 -req -in ap_server.csr -CA rootCACert.pem -CAkey rootCAKey.pem
-out ap_server_cert.pem -CAcreateserial -days 365 -sha256
```

Once complete you will have generated 4 files:

- The CA private key → rootCAKey.pem
- The CA public key → rootCACert.pem
- The AP public key → ap_server_cert.pem
- The AP private key → ap_server.key

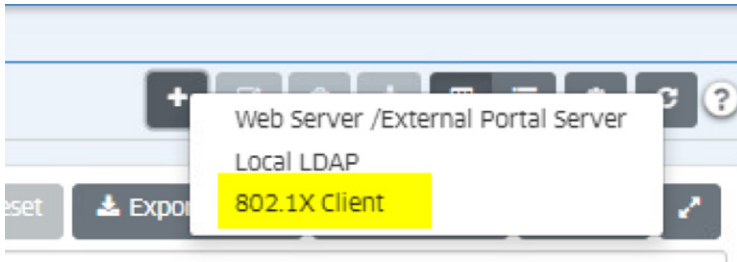
Import the access point certificate to OmniVista

This section is dedicated to importing certificates into OmniVista. First we need to import the certificate for the access point. To do this, you will use the previously generated key pair and add an 802.1x Client certificate.

Name	Type	Validity Start Time	Validity Stop Time
Certs	802.1X Client	Thu Jul 28 03:03:02 PDT 2022	Fri Jul 28 03:03:02 PDT 2023
APCert	802.1X Client	Fri Jan 27 08:56:34 PST 2023	Sat Jan 27 08:56:34 PST 2024

Application note

OmniAccess Stellar Access Point authentication and deployment application note



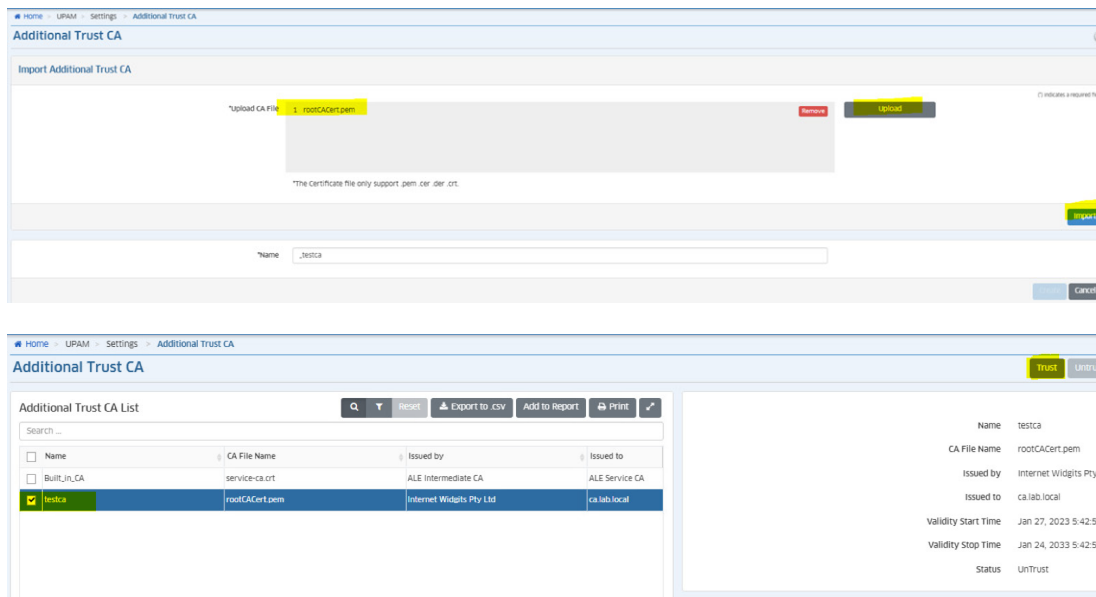
In the field **Upload AP certificate** browse for the access point certificate. In the **Upload Server Key File** field, select the private key of the certificate. Lastly, define a name and password used to decrypt the key.

To proceed you only need to change a few settings in the AP Group. First, enable the **802.1x Supplicant** feature and then select the certificate profile created in the previous step.

Application note

Import the CA Certificate to OmniVista

To complete the configuration, you must import the CA certificate that has been created. When the AP attempts to authenticate to OmniVista, the CA will validate if the client certificate comes from its signature.



Verification

On the OmniSwitch side, we can see that the OmniAccess Stellar Access Point has been successfully authenticated.

```
→ sh unp user details
Port: 1/1/8
MAC-Address: dc:08:56:13:39:a0
SAP = -,
Access Timestamp = 01/30/2023 15:08:32,
User Name = DC08561339A0,
IP-Address = 172.20.1.100,
Vlan = 172,
Authentication Type = 802.1x,
Authentication Status = Authenticated,
Authentication Failure Reason = -,
Authentication Retry Count = 0,
Authentication Server IP Used = 172.20.1.2,
Authentication Server Used = UPAMRadiusServer,
Server Reply-Message = -,
Profile = UPAM_1X_ARP,
Profile Source = Auth - Pass - Server UNP,
Profile From Auth Server = UPAM_1X_ARP,
```

802.1x using OmniVista (ADCS Certificates)

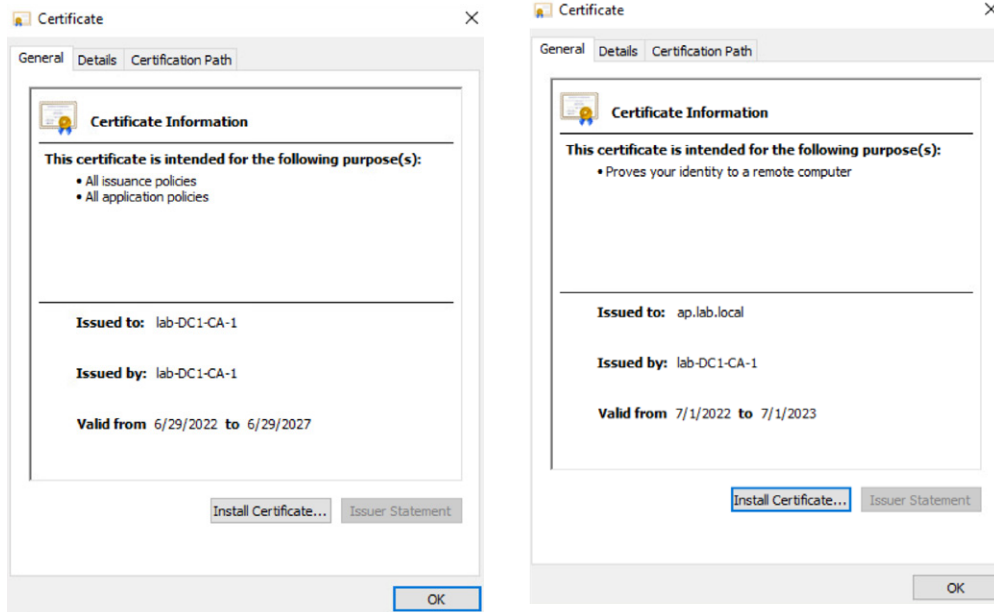
Suppose you have an existing Public Key Infrastructure (PKI) such as the Windows ecosystem, which includes Active Directory Certificate Services. You could import the PKI CA and generate a certificate which would be used for your OmniAccess Stellar Access Points.

Let's now review our certificates. On the left, are the CA certificates to import into OmniVista. (Refer to **Import CA Certificate to OmniVista**). On the right are the certificates to apply to the OmniAccess Stellar AP Group. (Refer to Import **Access Point certificate to OmniVista**).

Notice: When you generate the access point certificate, be sure to make the private key exportable. The public/private key pair is required.

Application note

OmniAccess Stellar Access Point authentication and deployment application note



OmniAccess Stellar Access Point deployment

Scenario

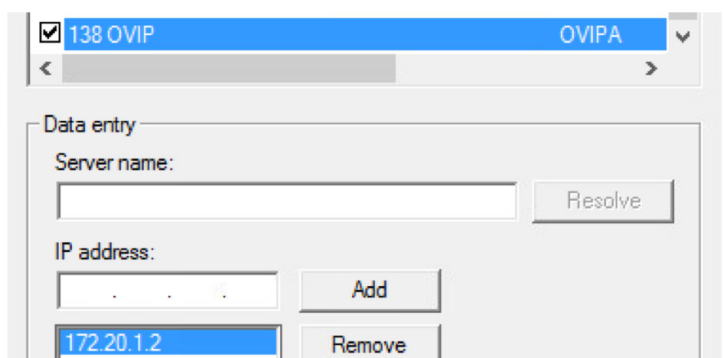
The goal of this section is to present a procedure to securely provision a large number of access points on your network. For this we will use a double authentication mechanism. The purpose is to authenticate the access points using two distinct methods. First, the access points will authenticate using the MAC address. If the access point belongs to the company's equipment, it will join its AP group in order to retrieve its configuration. The access point will download its certificate to be able to authenticate to the authentication server using the 802.1x protocol.

Deployment Workflow

Prerequisites

DHCP server:

- Option 138 enabled with the OmniVista IP address

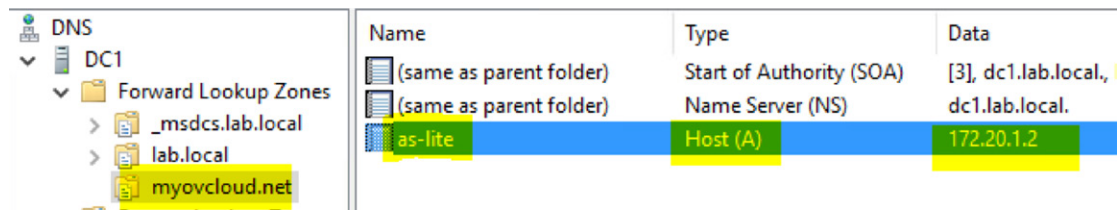


Application note

OmniAccess Stellar Access Point authentication and deployment application note

DNS server:

- Forward Zone myovcloud.net, and a type A registration to the OmniVista IP address.



Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[3], dc1.lab.local,
(same as parent folder)	Name Server (NS)	dc1.lab.local.
as-lite	Host (A)	172.20.1.2

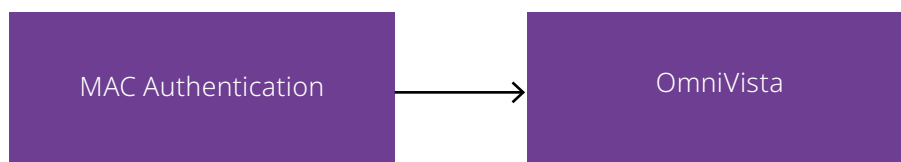
Import

In order to make the OmniAccess Stellar Access Point deployment simpler, you can import identities from a csv file, for example. Typically, you will be able to find all your access points MAC addresses in your purchase order. Refer to [Importing access point MAC address](#). You can also import access points into a pre-defined AP group once the OmniAccess Stellar Access Points have reached the OmniVista. It will automatically drag the access point to the identified AP Group.

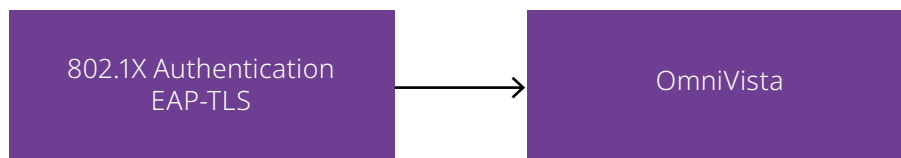
macAddress	groupName	apName	location	rfProfile
40:50:60::d0:e0:f0	default group	AP-40:50	floor	default profile
10:20:30::a0:b0:c0	default group	AP-10:20	floor	default profile

Authentication

For the authentication, here is an example of a workflow to ensure secure access. First, every defined access point will be MAC-authenticated using OmniVista UPAM. Once they have been successfully authenticated, they will download settings regarding to the AP Group they belong to and will be provisioned with a certificate. Refer to [MAC Authentication](#) to see how to implement.



Next, a different authentication method is used which is more secure (802.1x), please refer to [802.1x Authentication](#) to see how to implement.



Conclusion

In this document we have discussed the authentication protocols supported by OmniAccess Stellar Access Points and how to implement them in a large-scale network with a focus on automation and security while minimising the number of steps for configuration. We also covered how the OmniAccess Stellar Access Points and OmniSwitch interact with OmniVista's built-in authentication systems (UPAM) and third-party systems such as Windows Network Policy Server and Active Directory.