

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

Release 2.1.1



Application note OmniAccess Stellar Access Point authentication and deployment application note

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 deployment	23
Scenario	23
Deployment Workflow	23
Import	24
Authentication	24
Conclusion	24

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 adress 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:

Active Directory Users and Computers							
File Action View Help							
⊨ ⇒ 2 📷 4 X 🖫 🕞 🛛 🗊 3 8 11 7 2 8							
Active Directory Users and Com > Saved Queries	Name & Administrator	Type User	Description Built-in account for ad				
 ✓ pill lab.local > □ Builtin > □ Computers > □ Domain Controllers > □ ForeignSecurityPrincipal: > □ Managed Service Account □ Users 	alain alaint Alenterprise Allowed RODC Password Replication Group	User User Security Group	Members in this group c				
	🐮 ap 🕸 Cert Publishers 🕰 Cloneable Domain Controllers	User Security Group Security Group	Members of this group Members of this group t				
	C0856002DB0 DC0856002DB0	User User					
	 DefaultAccount Denied RODC Password Replication Group DHCP Administrators 	User Security Group Security Group	A user account manage Members in this group c Members who have ad				

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.

stellar Pro	operties				?	×
General	Members	Member Of	Managed By			
Member	rs:					
Name	20856002D. 208561339.	Active Dir lab.local/1 . lab.local/1	ectory Domain Users Users	Services Folder		
Ad	d	Remove				
			ОК	Cancel	Арр	ly

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**.

	ons Settings
olicy name:	AP_Request
Policy State	
If enabled, NP	evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy.
Policy enab	ed _
Network conne	ction method
Select the type	of network access server that sends the connection request to NPS. You can select either the network access server
hina ar Vandai	specific, but neutrents required. If your network access server is an ouz. IX authenticating switch or wreless access point,
type or Vendor select Unspec	ea.
select Unspec	ea.
type or Vendor select Unspec	ea. vork access server:

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

AP_Request Properties		×
Overview Conditions Settings		
Configure the conditions for this	network policy.	
If conditions match the connecti connection request, NPS skips t	on request, NPS uses this policy to authorize the connection request. If conditions do not match the his policy and evaluates other policies, if additional policies are configured.	
Condition	Value	
MAS Port Type	Ethernet	

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

NPS (Local) RADIUS Clients and Servers	Network Policies						
 Policies Connection Request Policies Network Policies 	Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect						
National Accounting	Policy Name	Status	Processing Order	Access Type	Source		
> 💐 Templates Management	AP_Stellar_Policy	Enabled	1	Grant Access	Unspecified		
	Secure Wireless Connections	Disabled	2	Grant Access	Unspecified		
	test	Disabled	3	Grant Access	Unspecified		
	Connections to Microsoft Routing and Remote Access server	Enabled	4	Deny Access	Unspecified		
	Connections to other access servers	Enabled	5	Deny Access	Unspecified		
	AP_Stellar_Policy						

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

eview Conditions Constraints Settings olicy name: IPStellar_Policy Policy State If enabled. NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. Image: Policy enabled Image: Policy enabled Image: 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? Image: Policy access. Grant access if the connection request matches this policy. Deny access. Grant access if the connection request matches this policy. Image: Policy access. Deny access if the connection request matches this policy. Image: Policy access. Deny access if the connection request matches this policy. Image: Policy access. Deny access if the connection request matches this policy. Image: Policy access. Deny access if the connection request matches this policy. Image: Policy access. Deny access if the connection request matches this policy. Image: Policy access. Image: Policy access. Deny access if the connection request matches the 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 releveed. If your network access server	_Stellar_Policy Pr	operties	
olicy name: NPStellar_Policy Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. Policy enabled 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? If 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 confliction request to 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. If type of network access server: Unspecified Vendor specifie: Vendor specifie:	rerview Condition	s Constraints Settings	
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 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 point, select Unspecified. Type of network access server: Unspecified. Vendor specific: 10 2	olicy name:	AP_Stellar_Policy	
It enabled, NPS evaluates this policy while performing authorization. It disabled, NPS does not evaluate this policy. Policy enabled Access Pemission 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? 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? If decrements of 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 point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10 2	Policy State		
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 point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10	It enabled, NPS e	valuates this policy while performing authorization. If disabled, NPS does not evaluate this policy.	
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 point, select Unspecified. Type of network access server: Unspecified Vendor specific:	Policy enable	i i i i i i i i i i i i i i i i i i i	
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 point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10	Access Permissio	n	
Clearst 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 specified. Type of network access server: Unspecified Vendor specific: 10	If conditions and	constraints of the network policy match the connection request, the policy can either grant access or de	ny
 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 			
 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 point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10			
 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 specified. Type of network access server: Unspecified Vendor specific: 10	Grant access.	Grant access if the connection request matches this policy.	
O 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 point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10			
□ 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	 Deny access. 	Deny access if the connection request matches this policy.	
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. Image: Type of network access server: Description Vendor specific: Description Vendor specific: Description Vendor specific: Select the type of network access server: Description Vendor specific: Description Vendor specific: Description Ve	Ignore user ac	count dial-in properties	
It 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. Inspecified Vendor specific:			
Autholization 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. Inspecified Vendor specific: 10	If the connection	In request matches the conditions and constraints of this network policy and the policy grants access, perform	
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 •	autriorization w	an network policy only, do not evaluate the dial-in properties of user accounts .	
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	Network connect	ion method	
Type of network access server: Unspecified Vendor specific: 10	Select the type of or Vendor specific select Unspecific	network access server that sends the connection request to NPS. You can select either the network access , but neither is required. If your network access server is an 802.1X authenticating switch or wireless access d.	server type point,
Unspecified Vendor specific:	Type of netwo	irk access server:	
O Vendor specific: 10 ♀	Unspecified	~	
10	O Vendor specif	ic:	
	10		
	10		

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

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 connection request, NPS skips this policy and evaluates other policies, if additional policies are configured. Condition Value	Ins Constraints Settings itions for this network policy. Itions for this network policy. the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request. If connection request and the connection request	_Stellar_	Policy Prop	erties		
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 connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.	Itions for this network policy. the connection request. NPS uses this policy to authorize the connection request. If conditions do not match the t, NPS skips this policy and evaluates other policies, if additional policies are configured. Value Value Ethemet LAB\stellar	verview	Conditions	Constraints	Settings	
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.	the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the t, NPS skips this policy and evaluates other policies, if additional policies are configured.	Configure	the conditior	ns for this net	work policy	
Condition Value	t, NPS skips this policy and evaluates other policies, if additional policies are configured. Value tethemet LAB\stellar	f conditio	ns match the	connection r	equest, NF	2S uses this policy to authorize the connection request. If conditions do not match the
Condition Value	Value Ethemet LAB\stellar	connectio	n request, N	PS skips this (policy and	evaluates other policies, if additional policies are configured.
Condition Value	Value Ethemet LAB\stellar					
	be Ethemet LAB∖stellar	Con	dition	V	alue	
VAS Port Type Ethemet	LAB\stellar		Port Type	E	themet	
🏭 User Groups LAB\stellar		📇 Use	r Groups	L	AB∖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)**.

AP_Stellar_Policy Properties	×
Overview Conditions Constraints Settings	
Configure the constraints for this network policy. If all constraints are not matched by the connection request, network access is denied. Constraints:	
Authentication Methods Allow access only to those clients that authen Allow access only to those clients that authen EAP types are negotiated between NPS and t isted.	tucate with the specified methods.
Called Station ID Called Stati	Move Up Move Down
Add Edit Remov Less secure authentication methods: Microsoft Encrypted Authentication version User can change password after it has Microsoft Encrypted Authentication (MS-C	n 2 (MS-CHAP-v2) expired :HAP) expired
Encrypted authentication (CHAP) Unencrypted authentication (PAP, SPAP) Allow clients to connect without negotiatin	g an authentication method
	OK Cancel Apply

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**.

verview Conditions Constraints Sett	ings	
Configure the settings for this network poli f conditions and constraints match the co	icy. onnection request and the	policy grants access, settings are applied.
ettings:		
RADIUS Attributes	To send additional a	ttributes to RADIUS clients, select a RADIUS standard attribute, and
Standard	your RADIUS client	u do not configure an attribute, it is not sent to RADIUS clients. See documentation for required attributes.
Vendor Specific		-
Routing and Remote Access		
Multilink and Bandwidth Allocation Protocol (BAP)	Attributes:	
TP Filters	Name	Value
Encryption	Filter-Id	MAC_AUTH
IP Settings	Framed-Protocol	Framed
33		handa
	Add	Edit Remove

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

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 > RADIU	S >> Create Server		
RADIUS Server Management			?
Create RADIUS Server			
* Server Name	Radius_Windows		(*) indicates a required field
* 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	~ ^	
(i) VRF Name	default		
			Create Cancel

Create an AAA profile

AAA Server Profile			¢
Create AAA Server Profile			
			(7) indicates a required field
	*Profile Name	Radius_Srv_Profile	
Authentication Servers			
802.1X			

MAC		
MAC Primary	Radius_Windows -	
Secondary		
Tertiary		
Quaternary		
Accounting Servers		~
Advanced Settings (Optional)		~
		Create

Creating an Access Auth Profile and Deployment

ccess Auth Profile				
Create Access Auth Profile			no Highlight	
* Profile Name	Radius Arth Profile			indicates a require
Default Settings				
AAA Server Profile	Radius_Srv_Profile	•		
Port-Bounce	O DISABLE			
MAC Auth	FNARE O			
802.1X Auth	O DISABLE			
Dynamic Service		•		
Customer Domain ID	<u>0</u>	•		
L2 Profile		*		
AP Mode				

Devices Clone +	Apply to				cess Auth Profile
		d to Report 🛛 🖶 Print 🖌 🖍	≜ Export to .csv Ade	Q T Reset	ccess Auth Profile
Radius_Auth_Profile	Profile Name				Search
	Default Settings	MAC Auth	Port-Bounce	AAA Server Profile	Profile Name
Padiur Sty Profile	AAA Server Profile	Enable	Disable	e	ovBridgeDefaultPortTemplate
Radius_Srv_Prome	ANA Server Prome	Enable	Disable		ovWirelessDefaultPortTempl.
Disable	Port-Bounce	Enable	Disable	ie -	ovAccessDefaultPortTemplate
Enable	MAC Auth	Enable	Disable	Radius_Srv_Profile	Radius_Auth_Profile
Disable	802.1X Auth	,)	
none	Dynamic Service				
0	Customer Domain ID				
	L2 Profile				
Enable	AP Mode				
Foable	Secure	All 4 rows < < > >	Showing		Show: All 🗸

Creating an Access Role Profile and Deployment

	Access Role Profile		
ľ	Edit Access Role Profile		no Highlight
	* Profile Name	RedusProfile	
L	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.

Access Role Profile

1. Select Devices	Select Devices	thad for accordingly	refile(c) and dovises to apply the	configuration				
2. Configure the period policy	beleet the mapping me	thou for accessione p	tome(s) and devices to apply the					
3. Configure the location policy	Configure the mapping method for RadiusProfile							
4. Review		Mapping Method	Map To VLAN	•				
		i VLAN(s)	(e.g. 5 or 10-20)	+				
	(i) Select devices to	apply the config	uration					
	1 Device EDIT	0 AP Groups	ADD					
	List of Selected De	evices						
	Q Search all							
	Friendly Name	Туре	Version	Status	Name			
	• 172.20.1.254	052360-P24	5.1.43.R02	Up	052360			

Access Auth Profile Assignments

	Access Auth Profile Ra	adius_Auth_Profile						
evices								
1 Device EDIT •	0 AP Groups ADD							
List of Selected Dev	ices							
Q Search all								
Friendly Name	Туре	Version	Status	Name	Address	MAC Address	Location	DNS Name
172.20.1.254 Add_Port Port Type: VLAN Port UNP VLANs: Add UNP VL	OS2360-P24	5.1.43.R02	Up	052360	172.20.1.254	94:24:e1:55:8b:7d	Unknown	

Add/Remove Ports

AVAILABLE 27					SELECTED 1			
Q Search all	• ·				Q Search all			
↓ la Port	Description	IF Index	Alias		 Port 	Description	IF Index	Alias
1/1/1	Alcatel-Lucent Enterprise OS236	1001	N/A	Add s	✓ 1/1/7	Alcatel-Lucent Enterprise 0S236	1007	N/A
1/1/2	Alcatel-Lucent Enterprise 05236	1002	N/A	Aug 2				
1/1/3	Alcatel-Lucent Enterprise 05236	1003	N/A	Add All »				
1/1/4	Alcatel-Lucent Enterprise 05236	1004	N/A	< Remove				
1/1/5	Alcatel-Lucent Enterprise 05236	1005	N/A	« Remove All				
1/1/6	Alcatel-Lucent Enterprise 05236	1006	N/A					
1/1/8	Alcatel-Lucent Enterprise 05236	1008	N/A					
1/1/9	Alcatel-Lucent Enterprise 05236	1009	N/A					
1/1/10	Alcatel-Lucent Enterprise 05236	1010	N/A					
1/1/11	Alcatel-Lucent Enterprise 05236	1011	N/A					
1/1/12	Alcatel-Lucent Enterprise 05236	1012	N/A					
1/1/13	Alcatel-Lucent Enterprise 05236	1013	N/A					
Showing all 27 i	items Showing Page 1	of 3 «	< 1 > »		Showing all 1 item	Showing Page 1	of 1 🤍 <	1 >

OK Cancel

OmniSwitch results

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

\rightarrow sh	unp user							
Port	Username	Mac addr	ess	User IP	Vlan	Profile	Туре	Status
1/1/7	dc:08:56:13:39:a0	dc:08:56	:13:39:a0	-	115	RadiusProfile	Bridge	Active
Total	users : 1							
→ sh Port: M	unp user details 1/1/7 AC-Address: dc:08:56:13 SAP	:39:a0	= -,	2022 10.25.40				
	User Name IP-Address Vlan		= dc:08: = 192.16 = 115,	56:13:39:a0, 8.115.52,				
	Authentication Type Authentication Status Authentication Failure	Reason	= Mac, = Authen = -,	ticated,				
	Authentication Retry C Authentication Server Authentication Server	ount IP Used Used	= 0, = 172.20 = Radius	.1.1, _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
```

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	UPAM_MAC					
Access Role Profile Attributes						
(i) Auth Flag	DISABLE					
(i) Mobile Tag Status	DISABLE					
(i) Redirect Status	DISABLE					

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

ome > Unified Access	> Unified Profile > Temp	plate > Access Role Profile				
Access Role Profile Apply to De						
Access Role Profile	Q T Rese	t 🛓 Export to .csv 🛛 Add	d to Report 🔒 Print 🖨			
Search						
Profile Name	🔶 Auth Flag	Mobile Tag Status	Redirect Status			
defaultWLANProfile	Disable	Disable	Disable			
RadiusProfile	Disable	Disable	Disable			
✓ UPAM_MAC	Disable	Disable	Disable			
			J			

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	Select Devices	thad for access role r	profile(s) and devices to apply th	e configuration			
2. Configure the period policy			some(s) and devices to apply th	e comportation			
3. Configure the location policy	Configure the mapping method for UPAM_MAC						
4. Review		Mapping Method	Map To VLAN				
		i VLAN(s)	115 8				
	(i) Select devices to	apply the confi	(e.g. 5 or 10-20)				
	1 Device EDIT	0 AP Groups	ADD				
	List of Selected D	evices					
	Q Search all						
	Friendly Name	Туре	Version	Sta			
	• 172.20.1.254	OS2360-P24	5.1.43.R02	U			

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 Prin	t QR Co <mark>de 🛛 Import 🛛 🛨</mark>
Company Property Online Devices				
			Q T	Reset 🕹 Export to .csv
Search				Click this button
Employee Account	Device Category	Device Family	Device OS	💠 🛛 more data.
				Got It!
	No ite	ems to show		

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

🛓 Import	File		
	≛ Template	Choose File	Browse
		Note: -Only support xls/csv/xlsx file. -No more than 50,000 data per file.	
			Import Cancel

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.

# Home > UPAM > Authentic	ation > Company Prop	erty				
Company Property					Print PSK Prin	it QR Code Import +
Company Property Online D	levices				_	
Search					Q Y	Reset £ Export to .csv
Employee Account	Device Mac	Device Name	Device Category	Device Family	Device OS	Enable Device Specifi
	DC08561339A0	AP-39:A0				Disabled

Create an authentication strategy

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

# Home > UPAM > Authentication > Authentication Strategy						
Authentication Strategy						
Edit Authentication Strategy						
*Strategy Name	test_mac_upam					
Authentication Source	None	Local Database	O External LDAP/AD	O External Radius		
Network Enforcement Policy						
Default Access Role Profile	UPAM_MAC			•		
Default Policy List				•		
Other Attributes						
	Attribute		Value			
	Select	.		+		
WEB Redirection Enforcement Policy						
Web Authentication	None	O Guest	O Employee	O Guest and Employee		

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			
(i) *Priority	5			× ^
(i)*Mapping Condition	Basic Attribute	C	Advanced Attribute	
	Attribute	Operator	Value	
	Select	•		
	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 R	ecord				Generati
Authentication Recor	d List Q T Rese	et 🛃 Export to .csv 🛛 Ad	d to Report 🛛 🖨 Print 🖉		
Search				Basic	
Account Name	Client IPv4	Client IPv6	Device MAC	Account Name	DC0956122040
✓ DC08561339A0			DC08561339A0	Account Name	00000100000
DC08561339A0			DC08561339A0	Account Type	Employee
DC08561339A0			DC08561339A0	Client IPv4	
DC08561339A0			DC08561339A0	Client IPv6	
DC08561339A0			DC08561339A0	Device MAC	DC08561339A0
DC08561339A0			DC08561339A0	Authentication Type	MAC
DC08561339A0			DC08561339A0	Service Type	Call-Check
				Auth Resource	Local Database
				Access Policy	test_mac_upam_ap
				Authentication Strategy	test_mac_upam
<			*	Web Access Strategy	
Show: All 🗸		Showing	All 7 rows	Authentication Result	Pass
				Session Start	Jan 25, 2023 5:27:15 p

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 procotol 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.

# Home > Unified Access > Unified Profile > Template > .	AAA Server Profile	
AAA Server Profile		(
Create AAA Server Profile		
		(*) indicates a required field
*Profile Name	UPAM_1x	
Authentication Servers		
802.1X		
802.1X Primary	UPAMRadiusServer 🔹	
Secondary	•	
Tertiary	· ·	
Quaternary		

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 Profi	le				
	* Profile Name	UPAM_1X_ARP			
Access Role Profile A	ttributes				
	Auth Flag Mobile Tag Status Arctice Status	DISABLE DISABLE DISABLE			
Home > Unified Access > Un	nified Profile > Template =	Access Role Profile		- Annive th	Devices Clone
Access Note Frome					Clone
Access Role Profile	Q T Reset	Export to .csv 📗 Add 🗄	to Report 🛛 🖨 Print 🖉	Profile Name	UPAM_1X_ARP
Profile Name	Auth Flag	Mobile Tag Status	Redirect Status	Access Role Profile Attributes	
defaultWLANProfile	Disable	Disable	Disable	Auth Flag	Disable
RadiusProfile	Disable	Disable	Disable	Autor Tag	Disobie
UPAM_MAC	Disable	Disable	Disable	Mobile Tag Status	Disable
test	Disable	Disable	Disable	Redirect Status	Disable

Disab	Redirect Status	Disable	Disable	Disable	test	
	Policy List	Disable	Disable	Disable	UPAM_1X_ARP	~
	Location Policy Name					
	Period Policy Name					
	Inactivity Interval					
	Bandwidth Control Settings	÷				
	Upstream Bandwidth	ws « < > »	Showing A		now: All 🗸	Sho

Access Role Profile

1. Select Devices	Select Devices	had for access role r	profile(s) and devices to apply the	configuration	
2. Configure the period policy	Select the mapping met		prometal and devices to apply the	comporation	
3. Configure the location policy	Configure the mapping method for UPAM_1X_ARP				
4. Review		Mapping Method	Map To VLAN	•	
	④VLAN(s) 172 0				
	Select devices to Device EDIT	apply the config	guration		
	List of Selected De	vices			
	Q Search all				
	Friendly Name	Туре	Version	Status	
	• 172.20.1.254	OS2360-P24	5.1.43.R02	Up	

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	# 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					
Dynamic Service					
Customer Domain ID	0				
L2 Profile					
AP Mode					

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

				- 1 (
ess Auth Profile	Q T Reset	🛓 Export to .csv 📗 A	dd to Report 🛛 🖨 Print 🖌 🖍			
arch					Profile Name	UPAM_1x_AAP
Profile Name	AAA Server Profile	Port-Bounce	eq MAC Auth	Default Sett	ings	
ovBridgeDefaultPortTemplate		Disable	Enable		AAA Server Profile	LIPAM 1x
ovWirelessDefaultPortTempl		Disable	Enable		Devt Devee	Disable
ovAccessDefaultPortTemplate		Disable	Enable		Port-Boonce	Disable
Radius_Auth_Profile	Radius_Srv_Profile	Disable	Enable		MAC Auth	Disable
UPAM_MAC_AAP	UPAM_MAC	Disable	Disable		802.1X Auth	Enable
UPAM_1x_AAP	UPAM_1x	Disable	Disable		Dynamic Service	none
					Customer Domain ID	0
cess Auth Profi	le				Customer Domain ID	0
cess Auth Profi	le ssignments				Customer Domain ID	0
cess Auth Profi	le ssignments Access Auth	n Profile	, ДАР		Customer Domain ID	0
cess Auth Profi ccess Auth Profile As evices	le ssignments Access Auth	Profile UPAM_1;	(_AAP		Customer Domain ID L2 Profile	0
cess Auth Profile As evices 1 Device EDIT	ile ssignments Access Auth 0 AP Groups	ADD	(AAP		Customer Domain ID L2 Profile	0
cess Auth Profile As ccess Auth Profile As evices 1 Device EDIT * List of Selected Device	ile ssignments Access Auth 0 AP Groups Vices	ADD	(AAP		Customer Domain ID	0
cess Auth Profi ccess Auth Profile As evices 1 Device EDIT • List of Selected Dev Q Search all	le ssignments Access Auth 0 AP Groups /ices	n Profile UPAM_1: ADD	(AAP		Customer Domain ID L2 Profile	0
cess Auth Profile As evices 1 Device EDIT • List of Selected Dev G Search all Friendly Name	Ie ssignments Access Auth 0 AP Groups //ices	n Profile UPAM_1: ADD	<u>с_</u> ААР Version	Status	Customer Domain ID L2 Profile	0

Application note

OmniAccess Stellar Access Point authentication and deployment application note

AILABLE Z/					SELECTED 1			
Search all					Q Search all			
↓2 Port	Description	IF Index	Alias		✓ Port	Description	IF Index	Ali
1/1/1	Alcatel-Lucent Enterprise OS236	1001	N/A	Add >	✓ 1/1/8	Alcatel-Lucent Enterprise 0S236	1008	N/
1/1/2	Alcatel-Lucent Enterprise OS236	1002	N/A	Aug				
1/1/3	Alcatel-Lucent Enterprise OS236	1003	N/A	Add All »				
1/1/4	Alcatel-Lucent Enterprise OS236	1004	N/A	< Remove				
1/1/5	Alcatel-Lucent Enterprise OS236	1005	N/A	« Remove All				
1/1/6	Alcatel-Lucent Enterprise OS236	1006	N/A					
1/1/7	Alcatel-Lucent Enterprise OS236	1007	N/A					
1/1/9	Alcatel-Lucent Enterprise OS236	1009	N/A					
1/1/10	Alcatel-Lucent Enterprise OS236	1010	N/A					
1/1/11	Alcatel-Lucent Enterprise OS236	1011	N/A					
1/1/12	Alcatel-Lucent Enterprise OS236	1012	N/A					
1/1/13	Alcatel-Lucent Enterprise OS236	1013	N/A					

Create an Authentication Strategy

Home > UPAM > Authentication > Authentication Str	# Home > UPAM > Authentication > Authentication Strategy					
Authentication Strategy						
Create Authentication Strategy						
"Strategy Name	1x_UPAM_Auth					
Authentication Source	None	Local Database	O External LDAP/AD	O External Radius		
Network Enforcement Policy						
Default Access Role Profile	UPAM_1X_ARP			•		
Default Policy List						
Other Attributes						
	Attribute		Value			
	Select	•		+		
WEB Redirection Enforcement Policy						
Web Authentication	None	○ Guest	○ Employee	O Guest and Employee		

Create an Access Policy

Home > UPAM > Authentication > Access Policy				
Access Policy				
Create Access Policy				
*Policy Name (1) *Priority (1)*Mapping Condition	1x_UPAM_Policy 5		O Advanced Attribute	× ^
	Attribute	Operator	Value	
	Authentication Type	- Equals	802.1X	×
*Authentication Strategy	1x_UPAM_Auth			•

Create an AP group

Create New Group		
General		
"Group Name	Group1	
Group Description		
Auto-Group VLANs		
"RF Profile	default profile -	
802.1X Supplicant on AP Management Port		
802.1X Suppliant		
*Certificate for 802.1X	Select •	
	Q Fearch +	
Time	Built-in Certificate	
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 \rightarrow 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.

Alcatel·Lucent		NETWORK -	CONFIGURATION - UNIFIED ACCESS -	SECURITY + ADMINISTRATION + UPAM + WLAN +	
AP REGISTRATION 🖈	Home > Network > AP Registration > Certificate				
Access Points AP Group	Certificate				•
Certificate External Captive Portal Config File	Certificate List				Q T Reset 🛓 Expor
IOT/Location/Advanced Analytics Server Data VPN Servers Export WLAN Support	Name Corts Corts	Type 802.1X Client		Validity Start Time Thu Jul 28 03:03:02 PDT 2022	Valicity Stop Time Fri Jul 28 03:03:02 PDT 2023
INTO	APCert	802.1X Client		Fri Jan 27 08:56:34 PST 2023	Sat Jan 27 08:56:34 PST 2024



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.

# Home > Network > AP Registration > Certificate			
Certificate			3
Create 802.1X Client Certificate			
"Upload AP Certificate	1 aplanvariant part	Upload	() indicates a required field
	"The certificate file only supports PEM or DER encoded certificates (e.g., pem.cer. der.ort)		
			Import
"Upload Server Key File	1 ардичения	Upload	() indicates a required field
	"The Certificate file only supports key.		
			Import
*Name	APorts		
Private Key Password			
Repeat Private Key Password			

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.

Edit Group Edit Group Description		
Edit Group		
General		
*Group Name	Group1	
Group Description		
Auto Couro 10 Abir		
*RF Profile	default profile	•
802.1X Supplicant on AP Management Port		
802.1X Suppliant		
Certificate for 802.1X	APCert	•
Time	Q Bearch Built-in Certificate	•
Timezone	Certs	
Daylight Saving Time	APCet	

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.

in norme of settings - Papartorial in	TO ALCH						
Additional Trust CA							٢
Import Additional Trust CA							
	"Upioad CA Fil <mark>e</mark>	1 rootCACert pem			Remove	Upload	C) indicates a required field
		"The Certificate file only sup	aport .pem .cer .der .crt.				
							Import
	"Name	_testca					
							Gancel
							Grade
							Cancel
₩ Home > UPAM > Settings > Addi	itional Trust CA						Cancel
W Home > UPAM > Settings > Addi Additional Trust CA	itional Trust CA						Trust Untrust
Home > UPAM > Settings > Add Additional Trust CA Additional Trust CA List	itional Trust CA	٩	Reset 🛓 Diport to .csv 🖌	Xi to Report 🔒 Print 🖌			Trust Untrust
W Home - UPAM - Settings - Addi Additional Trust CA Additional Trust CA List Setton -	itional Trust CA	٩	Reset & Deport to .csv A	3d to Report 🔒 Print 🖉		Name	Trust Untrust testca
w Home UPAM Settings Add Additional Trust CA Additional Trust CA List Search Name	Itional Trust CA	٩	Rest: Depart to .cv A	as to Report A Print Z		Name CA File Name	Trust Untrust Testca rootCACert.pem
W Home UPAM settings Add Additional Trust CA Additional Trust CA List Search - Name BuiltyingCA	Itional Trust CA	٩	Reset Deport to .csv A	50 to Report 🔑 Print 📝		Name CA File Name Issued by	Trust Untrust testca rootCACert.pem internet Widgits Pty Lt
Home UPAM settings Addi Additional Trust CA Additional Trust CA List Search _ Batt_In_CA gradue Instead	itional Trust CA CA File Name service-ca of rootCACert perm	٩٣	Rest: Depart to .csv A Issued by ALE Intermediate CA Intermediate CA	di to Report 🔒 Print 📝		Name CA File Name Issued by Issued 10	testca rootCACert.pem internet Widgits Pty Lt ca.lab.local
Home UPAM - Settings - Addi Additional Trust CA Additional Trust CA List Search _ Ball, n, CA pade pade pade pade	itional Trust CA CA File Name service-ca.oft postCACert.pem	٩	Reset Loport to .cv A Issued by ALE intermediate CA Intermediate SA	d to Report A Print Print Print ALE Service CA callablocal		Name CA File Name Issued by Issued to Validity Start Time	testca rootCACert pem internet Wildgits Pty Lt calab.local Jan 27, 2023 5:42:55 p
Home UPAM Settings Addi Additional Trust CA Additional Trust CA List Search _ Name Belt Jn CA getate texter	CA File Name service-ca.ort rosticACert.pem	٩	Best Loport to cov A Sued by ALE Intermediate CA Intermet Widgits Phy Ltd	Ad to Report Ap Print I		Name CA File Name Issued by Validity Start Time Validity Start Time	testca rootCACert.pem internet.Widgits Pty Lt ca.lab.local Jan 27, 2023 5:4255 [2] Jan 24, 2033 5:4255 [2]
W Home · UPAM · Settings · Addi Additional Trust CA Additional Trust CA List Settin_ Name Pathun,cA V Wate	CA File Name Service-ca.ort rootCACert.pem	Q 7	Beset Deport to rsv A Issued by ALE intermediate CA Internet Widgits Pty Ltd	Ad to Report A Print A		Name CA File Name Issued by Sseed 10 Validity Start Time Validity Start Time Validity Start Time Validity Start Starts Starts	testca rootCACert pem internet Widgits Pry Lt calabiocai Jan 27, 2023 5:42:55 p Jan 24, 2033 5:42:55 p Unitrust

Verification

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



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.

Certificate	Certificate General Details Certification Path
Certificate Information This certificate is intended for the following purpose(s): • All issuance policies • All application policies	Certificate Information This certificate is intended for the following purpose(s): • Proves your identity to a remote computer
Issued to: lab-DC1-CA-1	Issued to: ap.lab.local Issued by: lab-DC1-CA-1
Issued by: lab-DC1-CA-1 Valid from 6/29/2022 to 6/29/2027	Valid from 7/1/2022 to 7/1/2023
Install Certificate Issuer Staten	Install Certificate Issuer Statement
	ок

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 configration. 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

✓ 138 OVIP		OVIPA 🗸
c _g		>
Data entry		
Server name:		
		Resolve
IP address:		
	ا بيہ	
· · · ·	Add	
172 20 1 2	Remove	

DNS server:

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



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 <u>Importing access point MAC address</u>. 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	<u>apName</u>	location	<u>rfProfile</u>
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 <u>MAC Authentication</u> to see how to implement.



Next, a different authentication method is used which is more secure (802.1x), please refer to $\frac{802.1x}{\text{Authentication}}$ 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.

www.al-enterprise.com The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: www.al-enterprise.com/en/ legal/trademarks-copyright. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. © Copyright 2023 ALE International, ALE USA Inc. All rights reserved in all countries. DID23042701EN (May 2023)

