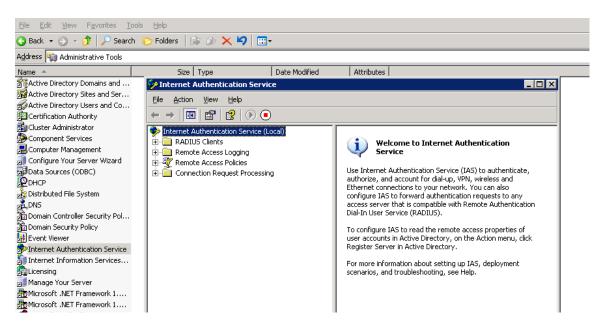
Management Authentication using Windows IAS as a Radius Server

OVERVIEW: In this we are using Radius server Windows IAS as a backend server for the management authentication for the controller. When the user try to login into the controller the request will first go to the external radius server to validate. If the user entry is present in the Windows AD(Active Directory) the success authentication will happen and the user can login into the controller with the admin rights. We are using this technique as to provide more security within the network, i.e. only valid users those have a privilege can access the network device.

Q: What are the settings I have to configure on the controller as well as on the radius server for successful management authentication and bypass the enable password?

First of all we have to configure an external radius server (IAS). Please do the below steps to configure the radius server.

Please navigate to Start -> Settings -> Control Panel -> Administrative Tools -> Internet Authentication Service ->click



Right click on the Internet Authentication Service(local) and check whether the service is start or not. If not please start the service.

🎐 Internet Authenticati	on Service		
<u>File A</u> ction <u>V</u> iew <u>H</u> el	р		
← → 🔃 😭 😫	0		
Internet Authentication ADIUS Clients Annuel Remote Access Log	Start Service Stop Service Register Server in Active Di	rectory	Welcome to Internet Authentication Service
Connection Request	⊻iew	•	rnet Authentication Service (IAS) to authenticate, e, and account for dial-up, VPN, wireless and connections to your network. You can also
	Properties Help		 IAS to forward authentication requests to any erver that is compatible with Remote Authentication ser Service (RADIUS).
		user acc Register	gure IAS to read the remote access properties of counts in Active Directory, on the Action menu, click Server in Active Directory.
			e information about setting up IAS, deployment is, and troubleshooting, see Help.

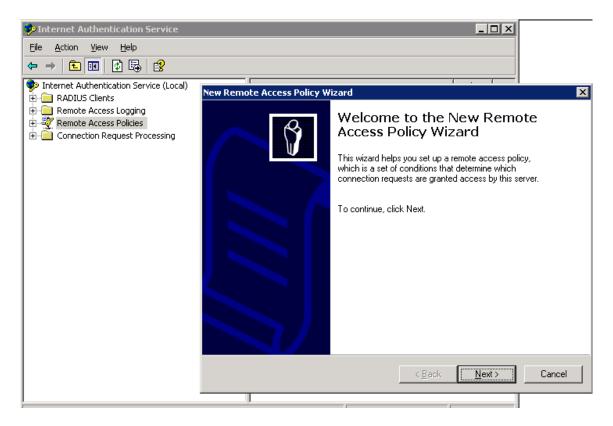
Right click on the "Radius Clients" and select New Radius Client. Specify any friendly name to the radius client and below mention the controller's IP address or Switch IP address. Click on next button.

🐤 Internet Authentication Service					
<u>File Action View H</u> elp					
	3				
Internet Authentication Service (Loca Additional Service (Loca Additional Service (Loca	al) New RADIUS CI Name and Ac Type a fr <u>F</u> riendly r	Idress iendly name and either an name: dress (IP or DNS):	Address IP Address or DNS name for Aruba	<u>V</u> erify	
			< <u>B</u> ack	<u>N</u> ext> (Cancel

Specify the Shared Secret key in the below screen (in my case its "aruba@123") and click the finish button.

👳 Internet Authentication Service					
<u>File Action View H</u> elp					
	?				
Internet Authentication Service (Local ADIUS Clients Remote Access Logging Remote Access Policies	ew RADIUS Client	ne Addre	ss 	Protocol	X
	Additional Information		on the client vendor a	attribute, specify the	
	RADIUS Standard Shared secret:	*****			_
	C <u>o</u> nfirm shared secret:	******			
	<u>Request must contain</u>	the Message Autho	enticator attribute		
			< <u>B</u> ack	Finish	Cancel

Now create the remote policy, right click on the "Remote Access Policies" and select "New Remote Access Policy" the below screen will appears. Lick on the next button



Select the first option "Use the wizard to set up" and give some name to the remote policy e.g. Remote-Policy. Click on the next button

New Remote Acces	s Policy Wizard			×
Policy Configu ra The wizard ca	ation Method an create a typical policy, or yo	u can create a (custom policy.	Ŷ
	ant to set up this policy?			
	wizard to set up a typical polic	y for a common	scenario	
◯ <u>S</u> et up a	a custom policy			
Type a name th <u>P</u> olicy name:	at describes this policy.			
<u>_</u> ,,,	1			
	Example: Authenticate all VPI	N connections.		
		< <u>B</u> ack	<u>N</u> ext >	Cancel

Select the options based on the method used to gain access to the network. In our case I am using Wireless. Click on next button

New Remote Access Policy Wizard	×
Access Method Policy conditions are based on the method used to gain access to the network.	
Select the method of access for which you want to create a policy.	
VPN Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.	
Dial-up Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.	
 Wireless Use for wireless LAN connections only. 	
C Ethernet Use for Ethernet connections, such as connections that use a switch.	
< <u>B</u> ack <u>N</u> ext > Cancel	

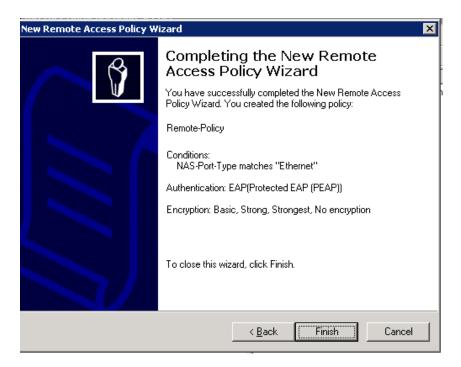
Select the user or group in the below screen. In my scenario I am using the user instead of group. Click on the next button.

w Remote Access Policy Wizard	
User or Group Access You can grant access to individual users, or you can grant access to se groups.	lected
Grant access based on the following: <u>User</u> User access permissions are specified in the user account.	
 Group Individual user permissions override group permissions. Group name: 	
	A <u>d</u> d <u>R</u> emove
J	
< <u>B</u> ack <u>N</u> ext >	Cancel

Select the Protected EAP (PEAP) from the drop down menu and click on the next button.

New Remote Access Policy Wizard		×
Authentication Methods EAP uses different types of security devices	s to authenticate users.	ŷ
<u>S</u> elect the EAP type for this policy. Type:		
Protected EAP (PEAP)	<u> </u>	Configure
MD5-Challenge Protected EAP (PEAP)		
Smart Card or other certificate		
	< <u>B</u> ack <u>N</u> ext >	Cancel

Click on the finish button to save the changes.



Right click on the Remote policy we have created just now and go to the properties.

🤣 Internet Authentication Service			
<u>File Action View H</u> elp			
 Internet Authentication Service (Local) RADIUS Clients Remote Access Logging Remote Access Policies Connection Request Processing 	Name Remote-Policy Connections to Microsoft Rou Connections to other access : -	Move Up Move D <u>o</u> wn Delete Rena <u>m</u> e P <u>roperties</u> Help	0 A

The below window will open. Choose the Grant remote access permission option and click on "Edit Profile"

Remote-Policy Properties ? 🗙
Settings
Specify the conditions that connection requests must match.
Policy <u>c</u> onditions:
NAS-Port-Type matches "Ethernet"
Add Edit <u>R</u> emove
If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.
Edit <u>P</u> rofile
Unless individual access permissions are specified in the user profile, this policy controls access to the network.
If a connection request matches the specified conditions: © Deny remote access permission
Grant remote access permission
OK Cancel Apply

Click on the Authentication tab and select the below authentication method that includes PAP and MSCHAP. Click on the Apply button to save the changes.

dit Dial-in Profile			? ×	
Dial-in Constraints Authentication	IP Encryption		Multilink dvanced	
Select the authentication me	ethods you want	to allow for this c	onnection.	
EAP Methods				
Microsoft Encrypted A	uthentication ve	rsion <u>2</u> (MS-CHA	P ∨2)	
User can change password after it has expired				
Microsoft Encrypted Authentication (MS-CHAP)				
🔲 U <u>s</u> er can chang	je password afte	r it has expired		
Encrypted authenticat	ion (CHAP)			
✓ Unencrypted authentication (PAP, SPAP)				
Unauthenticated access-				
Hlow clients to conner method.	ct without negoti	ating an authenti	cation	
	ОК	Cancel	Apply	

Click on the Advanced tab on the same window as above. Click on the add button

Edit I	Dial-in Profile		ĺ	? ×
	Dial-in Constraints Authentication	IP Encryption) Multilink Advanced	
A	pecify additional connection ccess server.	attributes to be return	ned to the Remote	
Π	ttri <u>b</u> utes: Name	Vendor	Value	-
	Service-Type	RADIUS Standard	Framed	
	1			
			<u></u>	<u>ו</u> צ
	A <u>d</u> d <u>E</u> dit	<u>R</u> emove		
	[ОК	Cancel Apply	,

Choose the Vendor-Specific option and click on Add button.

tribute:		
Name	Vendor	Description
Fermination-Action	RADIUS Standard	Specifies the action that the NAS should take when servic
Funnel-Assignment-ID	RADIUS Standard	Specifies the tunnel to which a session is assigned.
Funnel-Client-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel initiator during the a
Funnel-Client-Endpt	RADIUS Standard	Specifies the IP address of the initiator end of the tunnel.
Funnel-Medium-Type	RADIUS Standard	Specifies the transport medium used when creating a tunn
Funnel-Password	RADIUS Standard	Specifies the password used for authenticating to a remote
Funnel-Preference	RADIUS Standard	Specifies the relative preference assigned to each tunnel 🥡
Funnel-Pvt-Group-ID	RADIUS Standard	Specifies the Group ID for a tunneled session.
Funnel-Server-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel terminator during th
Funnel-Server-Endpt	RADIUS Standard	Specifies the IP address of the server end of the tunnel.
Funnel-Type	RADIUS Standard	Specifies the tunneling protocols used.
/endor-Specific	RADIUS Standard	Specifies the support of proprietary NAS features.
Cisco-AV-Pair	Cisco	Specifies the Cisco AV Pair VSA.
Allowed-Certificate-01D	Microsoft	Specifies the certificate purpose or usage object identifiers
Generate-Class-Attribute	Microsoft	Specifies whether IAS automatically generates the class al
Generate-Session-Timeout	Microsoft	Specifies whether IAS automatically generates the session
gnore-User-Dialin-Properties	Microsoft	Specifies that the user's dial-in properties are ignored.
MS-Quarantine-IPFilter	Microsoft	Specifies the IP traffic filter that is used by the Routing and

Click on the add button in the below window

Multivalued Attribut	e Information	? ×
Attribute name:		
Vendor-Specific		
Attribute number:		
26		
Attribute format:		
OctetString		
A <u>t</u> tribute values:		
Vendor	Value	Move <u>U</u> p
		Move <u>D</u> own
		<u>H</u> emove
		Edit
•		Þ
		ov l Canad l
		OK Cancel

Enter the vendor code as 14823(which is for Aruba) and choose the option Yes, It confirms. Click on Configure Attribute button

Vendor-Specific Attribute	Information	? ×
Attribute name:		
Vendor-Specific		
Specify network access serv	er vendor.	
Select from list:	RADIUS Standard	Ψ.
Enter Vendor Code:	14823	
Specify whether the attribute vendor specific attributes. Yes. It conforms No. It does not conform. Configure <u>A</u> ttribute	conforms to the RADIUS RFC spe	ecification for
	ОК	Cancel

Specify the Vendor-assigned attribute number as 3 and attribute value as 7 and click on Ok button to save the changes.

Configure VSA (RFC compliant)		? ×
Vendor-assigned attribute number: 3		
Attribute format:		•
Attri <u>b</u> ute value:		
	ОК Са	incel
		incei

Click on Ok and apply buttons in all the windows as to save the changes. Also create a user entry in the active directory. After creating the user entry on the Windows Active directory, right click on the user and go to the properties. Select the Dial-in tab and choose the "Allow access" for the user and click on Ok button.

ram Properties ?
Remote control Terminal Services Profile COM+ General Address Account Profile Telephones Organization Member Of Dial-in Environment Sessions
Remote Access Permission (Dial-in or VPN) Image: Allow access Image: Deny access Image: Deny access Image: Deny access through Remote Access Policy
✓ erify Caller-ID: Callback Options Image: No Callback Image: Set by Caller (Routing and Remote Access Service only) Image: Always Callback to:
Assign a Static IP Address Apply Static Routes Define routes to enable for this Dial-in Connection. Static Routes
OK Cancel Apply

The setting we have to configure on the Aruba controller or Switch.

FROM WEBUI:

Please navigate to Configuration tab-> Under Security click on Authentication -> Select the Servers tab -> Click on RADIUS Server -> Specify any name e.g. Aruba -> add -> Apply

n e tworks Con	figuration	C Decoroproprove	
Monitoring Configuration	Diagnostics Maintenance	Plan Events Reports Licenses will expire in 2	7 days Save Configuration Logout ad
Network Controller	Security > Authentica	tion > Servers	
VLANs	Servers AAA Profiles	L2 Authentication L3 Authentication User Ru	les Advanced
Ports	Г		
IP	 Server Group 	RADIUS Server	
Security Authentication		Instance	Actions
Authentication Access Control	 RADIUS Server 	Aruba Add	
Wireless AP Configuration	LDAP Server		
AP Installation	Internal DB		
Management General Administration	● Tacacs Accounting Server		
Certificates	TACACS Server		
Logging			
Clock			
Advanced Services Redundancy			Apply

Click on the Radius server you just created and specify the details like radius client ip address and the shared secret key -> Apply

Conf	figuration		epseuseuse		
Monitoring Configuration	Diagnostics Maintenance Pl	an Events Reports	Licenses will expire in 27 d	ays Save Con	ifiguration Logout adr
Network Controller	Security > Authenticat	ion > Servers			
VLANs Ports	Servers AAA Profiles L2	Authentication L3 Auth	nentication User Rules	Advanced	
IP Security	Server Group	RADIUS Server > Aruba		Show Reference	e Save As Re:
Authentication Access Control	RADIUS Server Aruba	Host	10.130.226.10		•••••
AP Configuration AP Installation	LDAP Server	Host	10.130.226.10	Key	Retype:
Management General	● Internal DB	Auth Port Retransmits	3	Acct Port Timeout	1813 5 sec
Administration Certificates	Tacacs Accounting Server	NAS ID		NAS IP	
SNMP Logging	TACACS Server	Use MD5		Mode	
Clock Advanced Services		•			Þ
Redundancy IP Mobility					Apply

Click on the Server Group under the same window and create a new server group e.g. Test-Server -> Add -> Apply

n e t w o r k s Conf	iguration	·		
Monitoring Configuration	Diagnostics Maintenance	Plan Events Reports Licens	es will expire in 27 days Save Configuration Logou	ut admin
Network Controller	Security > Authenti	cation > Servers		
VLANs	Servers AAA Profiles	L2 Authentication L3 Authenticati	on User Rules Advanced	
Ports				
IP	 Server Group 	Server Group		
Security		Instance	Actions	
Authentication	default	default	Show Reference Delete	
Access Control	internal	internal	Show Reference Delete	
Wireless AP Configuration	sq-auth-vpn	sg-auth-vpn	Show Reference Delete	
AP Installation			Show Reference Delete	
Management	 RADIUS Server 	Test-Server Add		
General	Aruba			
Administration				
Certificates	LDAP Server			
SNMP				
Logging	Internal DB			
Clock				
Advanced Services				
Redundancy			Appl	lv
TP Mobility				.,

Choose the Server Group you created above -> on the RHS click on new button choose the radius server from the drop down menu -> Add Server -> Apply

networks	Config	juration					10010010					
Monitoring Configura	ation	Diagnos	tics Mainten	ance f	Plan Events	Reports	Licenses w	rill expire in 2	7 days	Save Config	uration	Logout admi
Network Controller	S	Gecuri	ty > Autho	entica	tion > Serv	ers						
VLANs		Server	s AAA Prof	iles I	2 Authentication	L3 Authe	ntication	User Ru	les Advand	ed		
Ports												
IP		🗏 Se	rver Group	-						-1 - 6		
Security					Server Group >	Test-Serve				Show Ref	erence	Save A
Authentication			default									
Access Control			internal		Fail Through							
Wireless AP Configuration			sg-auth-vpn		Servers		_					
AP Installation			Test-Server		Aruba	Radius	rver-Type	No	im-FQDN	Match-Rule	- 0	Actions
Management General		E RA	DIUS Server		New			110			Edit	Delete
Administration			Aruba		Server Rules							
Certificates			Aroba		Priority	Attribu	te C	peration	Operand	Action	Valu	e
SNMP		₽ ID	AP Server		New							
Logging		•	AP Server		1							
Clock		4			1						1	F
Advanced Services Redundancy												
IP Mobility		Configur	ation Updated suc	cessfully.								Apply

As to check whether the communication is happens between Aruba Controller and radius server. Go to Diagnostics tab -> AAA test server -> From the drop down menu select the radius server e.g. Aruba -> choose any authentication method PAP or MSCHAPv2-> Specify the username -> type the password -> Begin test

If you will see the Authentication successful means communication happens between Aruba controller and Radius server.

networks Diag	gnostics	
Monitoring Configuration	Diagnostics Maintenance Plan	Events Reports Licenses will expire in 27 days Logout admin
Network Ping	Network > AAA Test Serve	er
Traceroute	Server Name	Aruba (IP Address: 10.130.226.10 - Radius) 💌
AAA Test Server	Authentication method	© MSCHAPV2 O PAP
Debug Config		
General Technical Support	Username	ram
Technical Support SSH Terminal	Password	••••••
Access Point Received Configuration	Authentication successful	Begin Test
Software Status		
Debug Log		
Technical Support		
Detailed Statistics		
Web Diagnostics		

Please navigate to Configuration tab-> Under Management click on Administration -> On the RHS select the server group under Management Authentication Servers from the drop-down menu e.g. Test-Server-> Apply

networks	Confi	guration			010010010010010				7300	
Monitoring Cor	nfiguration	Diagnostics	Maintenance	Plan Events Repo	rts Licenses	will expire in 2	7 days	Save	Configuration	Logout adm
Network Controller		Managen	nent > Admi	inistration						
VLANs										
Ports										
IP		Manageme Name	WebUI CA Certifica	ate Client Certificat	a Cavial No	CCU Dublic V	ev Certificate	Role	Action	
Security		admin	Webbi CA Certifica		e Serial No	55H PUDIIC K	ley certificate	root	Edit Delete	_
Authentication								1000	Eur Belea	2
Access Control		Add								
Wireless										
AP Configuration		Manageme	nt Authentication	n Servers						
AP Installation					-					
Management		Default Ro	e	root	•	1ode				
General										
Administration										
Certificates		Server Gro	oup > default	•			Show R	eference	Save As	Reset
SNMP			default							
Logging		Fail Throug	h sg-auth-vpr		1					
Clock			Test-Server							
Advanced Servic	es	Servers	NEW							
Redundancy			Name	Server-Type	trim-F(2DN	Match-Rul	e	Actions	
IP Mobility		New								
Stateful Firewall		Server R	ules							

Try to login into the controller with the user entry present on the Windows Active Directory e.g. in my case ram is the username.

	2				ARUBA 80	100					
Mon	itoring						1777	-19		AR	
onitoring Configuration	Diagnostics Maintena	ince	Plan	Ev	ents	oorts					
etwork Netwo Monitoring	Network Summa	ary				Securi	ity Summ	ary			
All WLAN Controllers	WI AN Network Status						tack Summa				
All Access Points	WLAN NELWORK Status	Total	Total	TREEC	IPSEC	WLAN AL	LIACK SUMMA	•	t 5 Min I	nat Haur	
All Air Monitors		Up	Down		Down	Desidefo	Service Attacks	0	Lomin L		
II Wired Access Points	WI AN Controllers	Up	0	Up	Down		ation Attacks	-		-	0
lobal Events	Access Points	1		0				<u>0</u>	2	-	0
ntroller		0	4	0	1	-	Pattern Matches	_	<u>(</u>	-	0
ontroller Summary	Air Monitors	0	0	0	0	Policy Viola		<u>0</u>	<u>0</u>	-	0
ccess Points	Wired Access Points	0	0	<u>0</u>	<u>0</u>	Unauthoriz	zed Devices Dete	ected <u>0</u>	9	2	1
Vired Access Points	Unprovisioned Access Points										
	Duplicate AP Name	0				Rogue A	P Classificati	on Sumn	nary		
Wired Mux Ports	RADIUS Servers	2	0					Last 5 Min	Last Ho	ur All	
Air Monitors	LDAP Servers	0	0			Rogue APs	s Detected	<u>o</u>	<u>0</u>	<u>0</u>	
Clients						Rogue APs	s Disabled	<u>0</u>	0	0	
Blacklist Clients	WLAN Performance Sur	nmary	1			Suspected	Rogue APs	<u>0</u>	0	<u>0</u>	
Firewall Hits	L	ast 5 M	lin Last	Hour	All	Interfering	APs Detected	<u>0</u>	0	<u>0</u>	
Futernal Convince Interface	Load Balancing Events		0		0	Known Inte	erfering APs	0	0	0	

FROM CLI:

(Aruba) #configure t

Enter Configuration commands, one per line. End with CNTL/Z

(Aruba) (config) #aaa authentication-server radius **Aruba** (Aruba) (RADIUS Server "Aruba") #enable (Aruba) (RADIUS Server "Aruba") #host **10.130.226.10** (Aruba) (RADIUS Server "Aruba") #key **aruba@123** (Aruba) (RADIUS Server "Aruba") #exit (Aruba) (config) #exit (Aruba) #aaa test-server pap Aruba ram aruba@123

Authentication successful

(Aruba) #show aaa authentication-server all

Auth Server Table

Name	Туре	IP addr	AuthPort	Status	Inservice	Requests
		10.130.226.4 10.130.226.1				-

(Aruba) #

User: ram

Password: ******** NOTICE NOTICE -- This switch has active licenses that will expire in 21 days NOTICE NOTICE -- See 'show license' for details. NOTICE

(Aruba) #