

# iQuila FAQ on RADIUS Integration

iQ22104r1

This Document Applies to: iQuila Enterprise V5

www.iQuila.com

# **Configuring RADIUS & NPS for iQuila**

This guide applies to Microsoft Server 2016 / 2019

Note: If there is a firewall between the NPS server and Domain Controller you will need to allow the following Ports to be open for RADIUS to work.

1812 UDP authentication1813 UDP authentication1645 UDP accounting (If you use the accounting feature within NPS.)1646 UDP accounting (If you use the accounting feature within NPS.)

#### Step 1

**Prepare Active Directory** 

**1.** Create a RADIUS user group and put in AD user accounts that you want to use for RADIUS authentication.

2. Make sure that the user accounts properties have the option to be controlled through a NPS also.



## Step 2

Prepare the NPS role for RADIUS.

1. Install the NPS role through the add roles and features wizard. This can be done on a member server and doesn't require that the role is installed on a Domain Controller.



2. Once installed you need to register the NPS within AD so that it can read user accounts. Right click off NPS (Local) and choose "Register server in Active Directory". If you haven't got this option (Greyed out) it usually means you have in the past had a previous NPS within the domain. If this is the case you can manually add the name of your NPS server in the "RAS and IAS Servers group" within the Users AD folder to achieve this and remove any old servers that may have had the NPS role installed.



**3.** Right click of RADIUS Clients, click New - You will need to add the iQuila IP address of your iQuila Server. Give it a Share Secret that's used to connect iQuila vSwitch to NPS.

		New PADIOS CITER
		Settings Advanced
		Enable this RADIUS client
NPS (Local)	RADIUS Clie	Select an existing template:
RADIUS Clients ar	d Servers	Name and Address
RADIUS CI		Address (IP or DNS):
ET D DI	New	Verfy
Remote RA		Shared Secret
El a na	Even et Lint	Select an existing Shared Secrets template:
Connectio	View >	To manually type a shared secret, click Manual. To extornatically generate a shared secret, click Generate. Touinual configure the RADUIS dient with the same shared secret entered here. Shared secrets are case senative.
Accounting	Refresh	Manual     O Generate     Shared secret:
🚽 Templates Ma	Help	OK Canon

**4.** Right click off Policies – Network Policies and give your Policy a name. Leave the "Type of network access server" on Unspecified. Specify Conditions screen, Click Add and choose "Windows groups", Click the "Add groups button" and type the name of your AD group that you created before.

<ul> <li>NPS (Local)</li> <li>RADIUS Clients and Set</li> <li>RADIUS Clients</li> </ul>	Network Policies	New NoticeN Palloy X  Sector Conditions  Sector Conditions  Provide a condition of the According to the Acco	
Remote RADIUS Se     Policies     Connection Reques     Network Policies	st Po Policy Name	Solut condition X Seed a condition with the olds Add. Context Output Description Descripti	
Accounting	New Export List View > Refresh	Monitoria Construction     Monitoria Construction     Monitoria Construction     Monitoria Construction     Monitoria Construction     Monitoria Construction     Monitoria     Mon	X Cliect Types Locators. Oreck Names Cancel
	rieip	Add Groups. Proceeding and Proceeding Procee	2 OR MS-CHAP v2 (User of

Choose "Access granted" and then on the next screen of the wizard tick "unencrypted authentication (PAP, SPAP)". Click "No" on the warning and leave the "Configure Constraints" section as it is.

(Please note: Although PAP is used and you receive an unencrypted warning, all communications will pass through the encrypted iQuila Links, and at no time will your user details be broadcasted on an unencrypted link.)

and Palicy ×	New Network Policy
Specify Access Permission Configure whether you want to grant relevant access or dery relevant access if the connection registert matches this printy.	Configure Authentication Methods
unit) on if their connection allow to condition of the policy.	EAP types are regarded between NPS and the client in the order in which they are lated.
ened en 6 clerk convectore alterativo match files andigene al films policy; alternized by: Stare Date programme (which surveys) in 1975 policy;	Now the
ting access according to user dates properties if client connection attempts waith the conditions of the policy	M M Remain
	Less secure auflicerication methods: Discussed Burgards Addresidation works 2 (05 OKP 4.2) El loss can cancer generated and in the secure Discussed Burgards Adventidation (15 COVP) El loss can change generated and in the secured
	Compare an example of (n) (1) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2
Previous New Treat	Period Net Troph 1

On the "Configure Settings" screen, remove "Framed-protocol PPP" and select (Service-Type) and click the "Edit" button and choose "Others" and select "Login." So it looks like this;

matched.	sk policy.
ttings:	a a construction of the second s
ADIUS Attributes	To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click. Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See
Vendor Specific	your RADIUS client documentation for required attributes.
Routing and Remote	
A. Multilink and	Attrbutes:
Bandwidth Allocation Protocol (BAP)	Name Value
P Filters	Service-Type Logn
Encryption	
P Settings	
	AddEdt Remove

Click on Finish on the wizard on the "Completing new network policy." If you have other policies then make sure your authentication policy is order 1 in the list as the policies get processed from top down starting with 1.

NES (Lecol)	Naturck Policias		_	_						
V E RADIUS Clients and Servers										
RADIUS Clients	ADUS Clients									
Remote RADIUS Server										
✓ J										
Connection Request Po	Policy Name	Status	Processing Order	Access Type	Source					
Network Policies	Test Folcy	Frabled	1	Grant Access	Unspecified					
Accounting	Connections to Microsoft Routing and Remo	te Access server Enabled	2	Deny Access	Unspecified					
> A Templates Management	Connections to other access servers	brabled	3	Deny Access	Unspecified					
	- Connections to Monacet Boution and Bas	onte àccess secur						-		
	0 contraction of the second of the second									
	Conditions - If the following conditions are met									
	Condition Value									
	MS RAS Vender ID 2118									
	Setting - Then the following settings are avoided									
								_		
	Setting	Value								
	Access Pemission	Deny Access								
	Extensible Authentication Protocol Method	Mcrosoft: Secured password	EAP-MSCHAP v210	R Monsoft: Sr	art Card or other certificate					
	Authentication Method	EAP OR MS-CHAP v1 OR MS	CHAP v1 (User car	change passes	ord after it has expired) OR MS-	CHAP v2 OR MS-CHAP v2 (liter can	change password after it has expired)			
	Framed-Photocol	PPP								
	Service-Type	Framed								
	Pv4 Ros	Configured								
	Encryption Policy	Enabled								
	Encryption	Basic encryption (MPPE 40bit	), Strong encryption	(MPPE 56-bit), 1	trongest encryption (MPPE 12	Bèx)				
								_		
< >										

#### Step 3

Set iQuila for RADIUS

1. Login to your iQuila Enterprise Server and select your vSwitch and click "Manage Virtual Switch".

Mai	nage VEN Server '				Li	censed t	<b>o</b> :				0 days rem	aining		
r2 Swi	tch / Hub Settings	Virtual Switch Name	Status	Tipe	Users	Groups	Sessions	MAC Tables	IP Tables	Num Logins	Last Login	Last Communication	Transfer Bytes	Transfer Packets
30	Manage Virtual Switch	-92	Celline	Standalone	2	0	4	3	5	36	2021-10-08 16:34:05	2021-10-12 142331	126 339 068 721	149 299 314
	-	20	Online	Standalone	31	1	31	34	37	6122	2021-10-12 14:15:04	2021-10-12 1423:31	12,413,288,480,5	44,524,465,538
1	Online	10	Online	Standalone	1	0	0	0	0	0	2021-01-20 14:59:10	2021-01-20 1459:10	0	0
-	17	26	Online	Standalone	3	0	2	864	27	54	2021-09-19 03:39:18	2021-10-12 142331	48,768,221,447,3	139,572,918,337
	Offine	*	Online	Standalone	0	0	0	0	0	0	2020-07-10 13:59:39	2020-07-10 1359:39	0	0
S	12/244	2	Online	Standalone	6	0	6	79	117	3089	2021-10-12 10:46:10	2021-10-12 142331	11,804,464,581,0	38,947,172,177
<b>1</b>	View Status	×	Online	Standalone	9	0	11	60	98	6323	2021-10-12 14:15:04	2021-10-12 14:23:31	15,111,535,552,3.	68,178,077,060
1		1	Online	Standalone	1	0	1	1	1	0	2021-05-09 07:59:19	2021-10-12 1423:29	436,633,026	8,476,202
-	Country of Michael Country	1	Online	Standalone	7	1	1	1	1	1904	2021-10-06 18:18:26	2021-10-12 14:23:31	64,476,691,343	493,870,165
12	Create of Vision Strifts	RADIUSTest	Online	Standalone	1	0	1	1	4	7	2021-10-12 10:05:45	2021-10-12 14:23:29	9,238,175,941	7,282,263
=1.	Annual Providence	100 M	Online	Standalone	0	0	0	0	0	0	2021-07-28 12:43:21	2021-07-28 12:43:21	0	0
1	Properties		Online	Standalone	0	0	0	0	0	0	2021-07-21 10:23:29	2021-07-21 10:23:29	0	0
-	Delete													
ging ar	nd Routing													
++	Local Bridge Setting													
۲	Layer 3 Switch Setting	-												
<b>1</b>	IPsec / LZTP Setting													
<b>3</b>	OpenVPN / MS-SSTP													
nork Ar	nd Encyption													
2	Encryption and Network													
		VEN Server int	ormation				Manaj	pement of Listen	H2:		ic.	ula Artificial Intelligence		
( Cluste	aring	00 00		View Server Stat	tus		_					( <b>Q</b> )	EN Al Setting	
199	Clustering Configuration	-	-	Tela Canta				reste Po	rt Number TCP 443	Ustening				
	Clustering Status	19: 1	h	concornig				Start	TCP 5555	Ustening				
-				About this VEN S	in an						1			
ALC: NO	Connections List				115			the second se						

### 2. Click the "Authentication Server Settings."



**3.** Enable "Use RADIUS Authentication." Enter your NPS servers IP and enter your shared secret, confirm, and click OK.

Authentication Server Settings	×
To use an external RADIUS server to verify login attempts to the Virtual Switch "RADIUSTest", specify an external RADIUS server that verifies the user name and password.	
RADIUS Server Settings:	
Use RADIUS Authentication	
RADIUS Server Host Name or IP: 10.10.10.1	1
(use ',' or ',' to split multiple hostnames.)	-
Port: 1812 (UDP Port)	
Shared Secret:	
Confirm Shared Secret: ••••••	
Retry Interval 500 milliseconds (above 500, below 10000)	
The RADIUS server must accept requests from IP addresses of this VEN Server. Also, authentication by Password Authentication Protocol (PAP) must be enabled	- J.
When using Windows AD Domain Controller or Windows Server Active Director Controller as an external authentication server, you must setup the VEN Server computer to join the domain. To use AD Domain Authentication, there are no items to configure here.	/
OK Cancel	

**4.** Click "Manage Users" button and create a new user account that will be used to forward credentials to the RADIUS NPS server for authentication. Enter a \* for the username and choose RADIUS Authentication.

S User Name:	*	Security Policy	Security Policy
Full Name:			Security roney
Note:	For Radius Authentication		
Auth Type: 👩 🖉	nonymous Authentication assword Authentication	Group Name (Optional):	Browse Groups
100 III 100 III 100 III	dividual Certificate Authentication gned Certificate Authentication ADIUS Authentication	Individual Certificate Authentication Settings:	
<b>₽</b> ₿ <b>₽</b>	D Domain Authentication	The users using 'Individual Certificate Authen allowed or denied connection depending or client certificate completely matches the certi set for the user beforehand.	ntication' will be h whether the SSL ficate that has been
ADIUS or AD Domain Authe	titication Settings: Expiration Date for This Account	Signed Certificate Authentication Settings: Verification of whether the client certificate is certificate of a CA trusted by this Virtual Swite	s signed is based on : ch.
		Limit Common Name (CN) Value	
DIUS or AD Domain Auther	tication Settings:		
DIUS or AD Domain Auther Login attempts by pa server, Windows AD d controller.	tication Settings: sword will be verified by the external RADIUS omain controller, or Active Directory Authentication Server	Limit Values of the Certificate Serial Nu	mber
ADIUS or AD Domain Authen	lication Settings: sword will be verified by the external RADIUS smain controller, or Active Directory Authentication Server n Server	Limit Values of the Certificate Serial Nu Note: Enter hexadecimal values. (Ex	mber ample: 0155ABCDEF)

Then at the device end, for all devices that you want to use AD authentication, give the connection a name, add your iQuila host name and then your Virtual Hub Name (vSwitch) name. On the "User Authentication Settings" section choose "RADIUS or NT Domain Authentication" and type your AD domain username and password. Click OK and then connect within the iQuila Client.

If your AD user account resides within group you created for RADIUS access in AD then your user will be allowed to login to the domain.

New Cloud Connection Setting Properties	×
Please configure the VPN Connection Setting for VPN Server.	Virtual Network Adapter to Use:
Setting Name:       iQuila Agent         Destination VPN Server:	
Host Name: sdlan.iquila.com Port Number: 443  Virtual Hub Name: RADIUSTest  V	User Authentication Setting: Set the user authentication information that is required when connecting to the VPN Server.
Proxy Server as Relay: You can connect to a VPN Server via a proxy server. Import IE Proxy Server Settings Proxy Type:  Direct TCP/IP Connection (No Proxy) Connect via HTTP Proxy Server Connect via SOCKS Proxy Server	Auth Type:       Standard Password Authentication         User Name:       domainusername         Password:       ••••••••••••         You can change the user's password on the VPN Server.         Change Password
Proxy Server Setting	Advanced Setting of Communication:
Server Certificate Verification Option:	Reconnect Count: times Reconnect Interval: 15 seconds
Manage Trusted CA Certificate List Specify Individual Cert Show Individual Cert	✓ Infinite Reconnects (Keep VPN Always Online)         □ Use SSL 3.0 (1)         Advanced Settings
Hide Status and Errors Screens Hide IP Address Scr	reens OK Cancel

It will then login to iQuila using your domain credentials using the RADIUS protocol via the NPS role.