

IQUILA

SOFTWARE DEFINED NETWORKS

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 authentication

1813 UDP authentication

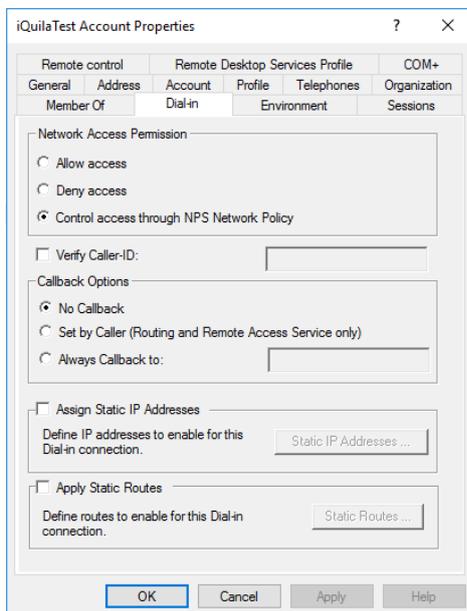
1645 UDP accounting (If you use the accounting feature within NPS.)

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

Step 1

Prepare Active Directory

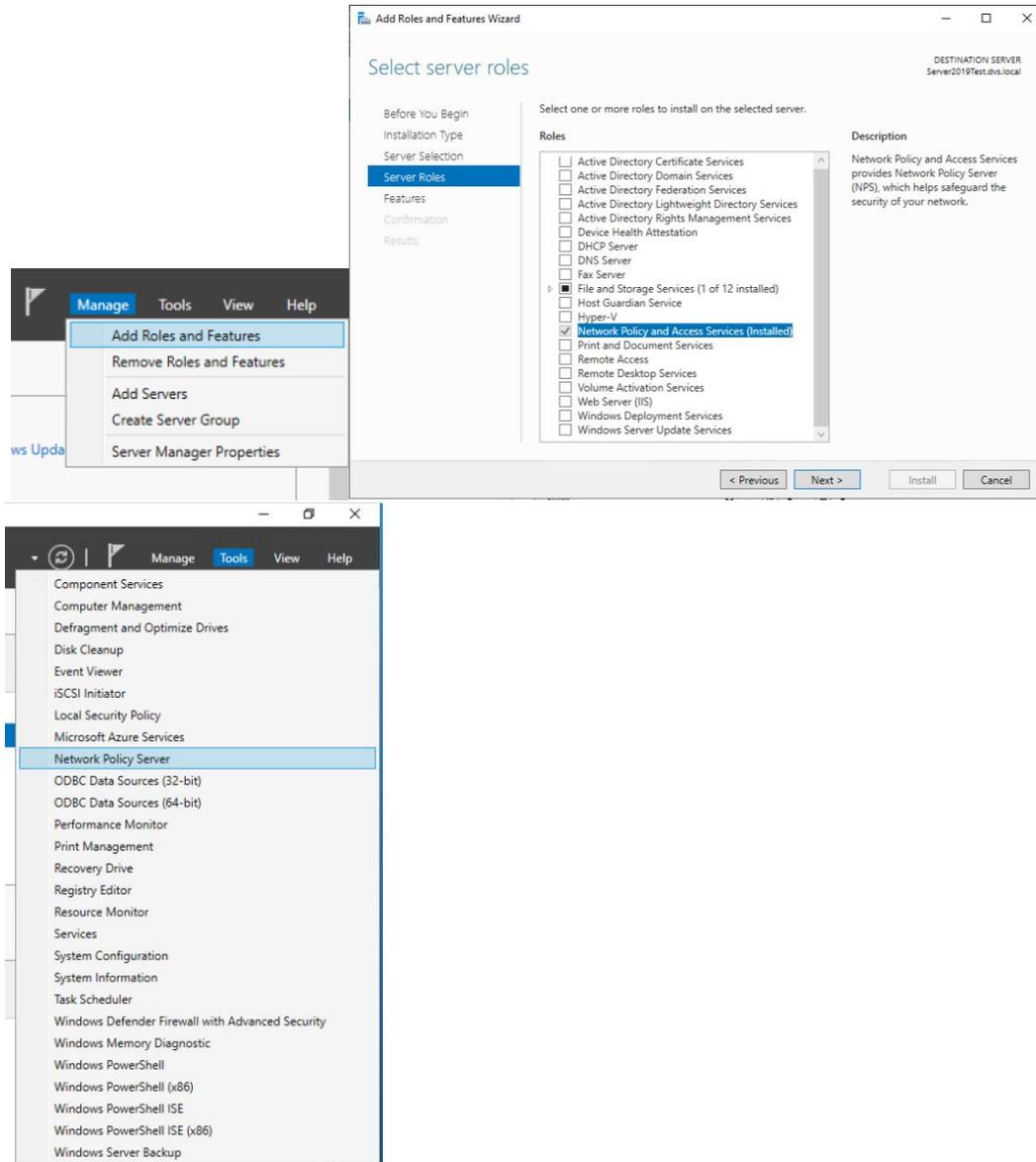
1. Create a RADIUS user group and put in AD user accounts that you want to use for RADIUS authentication.
2. Make sure that the user accounts properties have the option to be controlled through a NPS also.



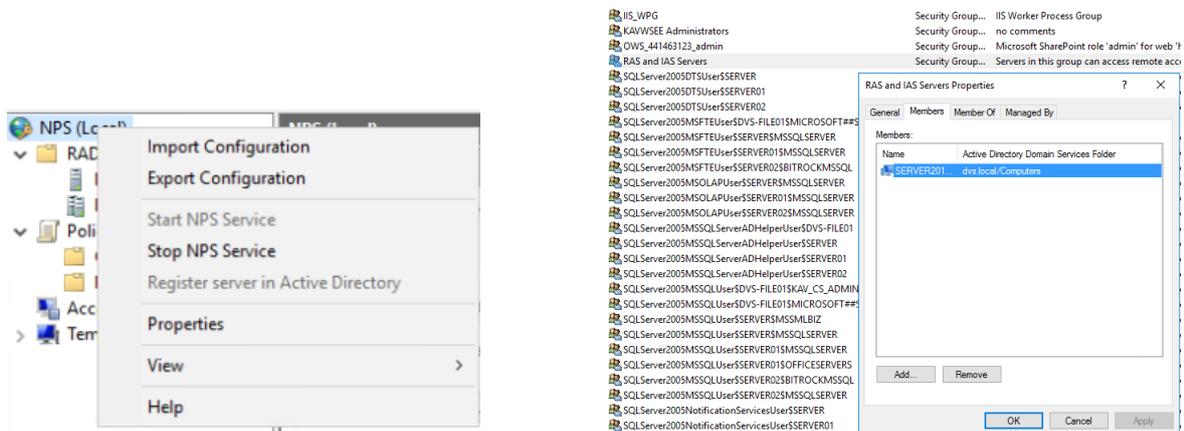
Step 2

Prepare the NPS role for RADIUS.

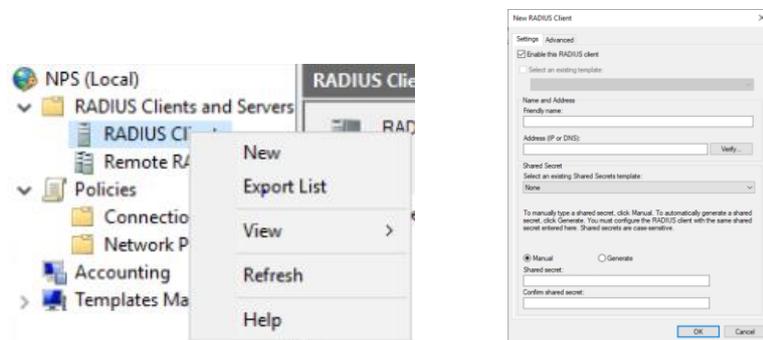
1. Install the NPS role through the add roles and features wizard. This can be done on a member server and doesn't require that the role is installed on a Domain Controller.



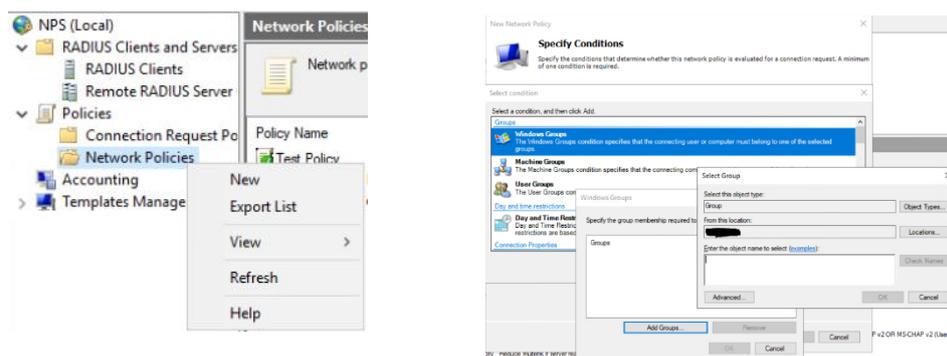
2. Once installed you need to register the NPS within AD so that it can read user accounts. Right click off NPS (Local) and choose "Register server in Active Directory". If you haven't got this option (Greyed out) it usually means you have in the past had a previous NPS within the domain. If this is 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.

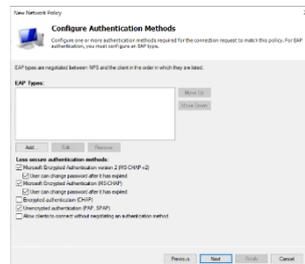


4. Right click off Policies – Network Policies and give your Policy a name. Leave the "Type of network access server" on Unspecified. Specify Conditions screen, Click Add and choose "Windows groups", Click the "Add groups button" and type the name of your AD group that you created before.

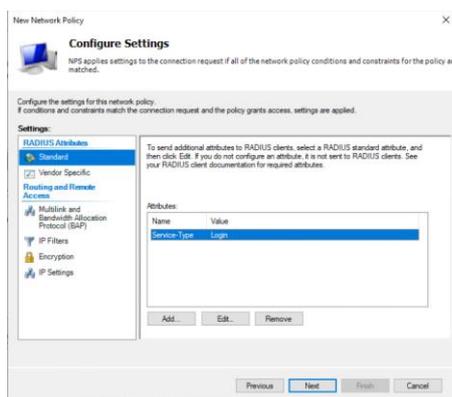


Choose "Access granted" and then on the next screen of the wizard tick "unencrypted authentication (PAP, SPAP)". Click "No" on the warning and leave the "Configure Constraints" section as it is.

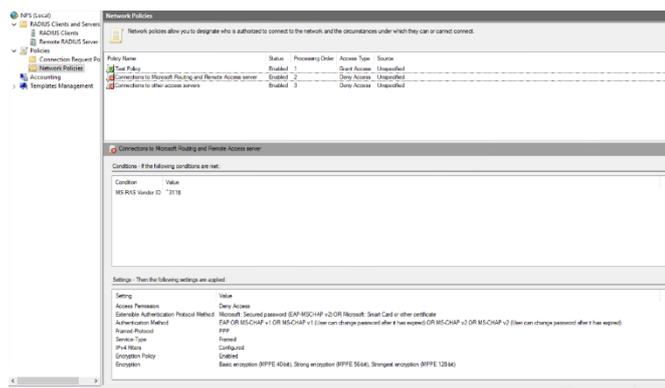
(Please note: Although PAP is used and you receive an unencrypted warning, all communications will pass through the encrypted iQuila Links, and at no time will your user details be broadcasted on an unencrypted link.)



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;



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.



Step 3

Set iQuila for RADIUS

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

The screenshot shows the 'Manage Virtual Switch' window in the iQuila VEN Server Manager. At the top, it indicates 'Licensed to: 0 days remaining'. The main area contains a table with columns for Virtual Switch Name, Status, Type, Users, Groups, Sessions, MAC Tables, IP Tables, Num Logins, Last Login, Last Communication, Transfer Bytes, and Transfer Packets. The 'RADIUSTest' vSwitch is highlighted in blue.

Virtual Switch Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables	Num Logins	Last Login	Last Communication	Transfer Bytes	Transfer Packets
[Redacted]	Online	Standalone	2	0	3	3	5	36	2021-10-08 16:34:05	2021-10-12 14:23:31	126,339,068,721	149,293,314
[Redacted]	Online	Standalone	31	1	31	34	37	8122	2021-10-12 14:15:04	2021-10-12 14:23:31	12,413,288,485.5	44,524,465,538
[Redacted]	Online	Standalone	1	0	0	0	0	0	2021-05-20 14:56:53	2021-07-20 14:59:10	0	0
[Redacted]	Online	Standalone	3	0	2	864	27	14	2021-09-19 03:39:13	2021-10-12 14:23:31	48,768,221,447.3	139,572,913,337
[Redacted]	Online	Standalone	0	0	0	0	0	0	2020-07-10 13:59:39	2020-07-10 13:59:39	0	0
[Redacted]	Online	Standalone	6	0	6	79	117	3399	2021-10-12 10:46:10	2021-10-12 14:23:31	11,804,464,581.0	35,947,172,177
[Redacted]	Online	Standalone	9	0	11	60	99	6323	2021-10-12 14:15:04	2021-10-12 14:23:31	15,111,535,532.4	68,178,077,060
[Redacted]	Online	Standalone	1	0	1	1	1	0	2021-06-29 07:09:19	2021-10-12 14:23:29	436,833,026	8476,202
[Redacted]	Online	Standalone	7	1	1	1	1	1904	2021-10-06 19:16:08	2021-10-12 14:23:31	64,476,691,343	493,870,165
RADIUSTest	Online	Standalone	1	0	1	1	4	7	2021-10-12 10:05:45	2021-10-12 14:23:29	9,338,175,941	7,282,263
[Redacted]	Online	Standalone	0	0	0	0	0	0	2021-07-28 12:48:21	2021-07-28 12:48:21	0	0
[Redacted]	Online	Standalone	0	0	0	0	0	0	2021-07-21 10:23:29	2021-07-21 10:23:29	0	0

2. Click the “Authentication Server Settings.”

The screenshot shows the 'Management of Virtual Switch - RADIUSTest' window. It features several configuration panels:

- Management of Security Database:** Includes 'Manage Users' and 'Manage Groups' buttons.
- Secure NAT Settings:** Contains a 'Virtual NAT and Virtual DHCP Server' button and a warning that 'Virtual NAT may conflict with your network, please check before enabling.'
- VEN Sessions Management:** Includes a 'Manage Sessions' button.
- VEN Certificates:** Contains 'Trusted CA Certificates' and 'Revoked Certs' buttons.
- VEN Sessions Management (bottom):** Includes a 'Manage Cascade Connections' button.
- Virtual Switch Settings:** Includes 'Switch Properties' and 'Authentication Server Setting' buttons.
- Current Status of this Virtual Switch:** A table showing various metrics like Sessions, MAC Tables, IP Tables, and Transfer Bytes.
- VEN Log Files:** Includes 'Log Save Setting' and 'Log File List' buttons.

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:
(use ',' or ';' to split multiple hostnames.)

Port: (UDP Port)

Shared Secret:

Confirm Shared Secret:

Retry Interval milliseconds (above 500, below 10000)

Note: The RADIUS server must accept requests from IP addresses of this VEN Server. Also, authentication by Password Authentication Protocol (PAP) must be enabled.

When using Windows AD Domain Controller or Windows Server Active Directory 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.

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.

Properties of User

User Name:
 Full Name:
 Note:

Auth Type:

- Anonymous Authentication
- Password Authentication
- Individual Certificate Authentication
- Signed Certificate Authentication
- RADIUS Authentication**
- AD Domain Authentication

Password Authentication Settings:

Password:
 Confirm Password:

RADIUS or AD Domain Authentication Settings:

Set the Expiration Date for This Account
 12/10/2021 000000

RADIUS or AD Domain Authentication Settings:

Note: Login attempts by password will be verified by the external RADIUS server, Windows AD domain controller, or Active Directory controller.

Specify User Name on Authentication Server
 User Name on Authentication Server:

Security Policy:

Set Security Policy

Group Name (Optional):

Individual Certificate Authentication Settings:

Note: The users using 'Individual Certificate Authentication' will be allowed or denied connection depending on whether the SSL client certificate completely matches the certificate that has been set for the user beforehand.

Signed Certificate Authentication Settings:

Note: Verification of whether the client certificate is signed is based on a certificate of a CA trusted by this Virtual Switch.

Limit Common Name (CN) Value

Limit Values of the Certificate Serial Number

Note: Enter hexadecimal values. (Example: 0155ABCDEFF)

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.

Setting Name:

Destination VPN Server:

Specify the host name or IP address, and the port number and the Virtual Hub on the destination VPN Server.

Host Name:

Port Number: Disable NAT-T

Virtual Hub Name:

Proxy Server as Relay:

You can connect to a VPN Server via a proxy server.

Proxy Type: Direct TCP/IP Connection (No Proxy)
 Connect via HTTP Proxy Server
 Connect via SOCKS Proxy Server

Server Certificate Verification Option:

Always Verify Server Certificate

Virtual Network Adapter to Use:

VPN Client Adapter - VPN

User Authentication Setting:

Set the user authentication information that is required when connecting to the VPN Server.

Auth Type:

User Name:

Password:

You can change the user's password on the VPN Server.

Advanced Setting of Communication:

Reconnects Automatically After Disconnected

Reconnect Count: times

Reconnect Interval: seconds

Infinite Reconnects (Keep VPN Always Online)

Use SSL 3.0 (1)

Hide Status and Errors Screens Hide IP Address Screens

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