SOFTWARE DEFINED NETWORKS

iQuila FAQ on RADIUS Integration

iQ22104r1

This Document Applies to:

iQuila Enterprise V5

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.

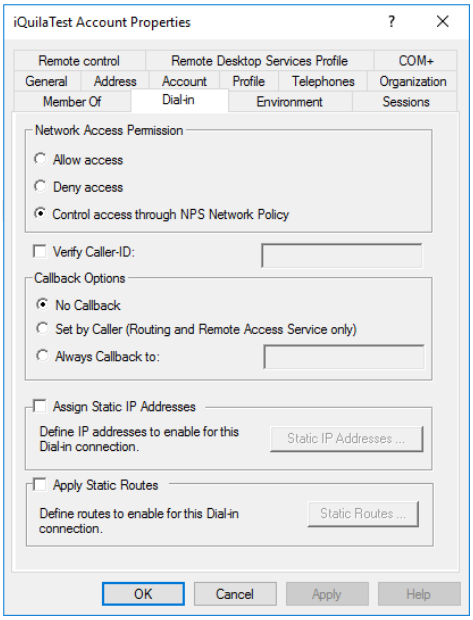
1812 UDP authentication
1813 UDP authentication
1645 UDP accounting (If you use the accounting feature within NPS.)
1646 UDP accounting (If you use the accounting feature within NPS.)

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.

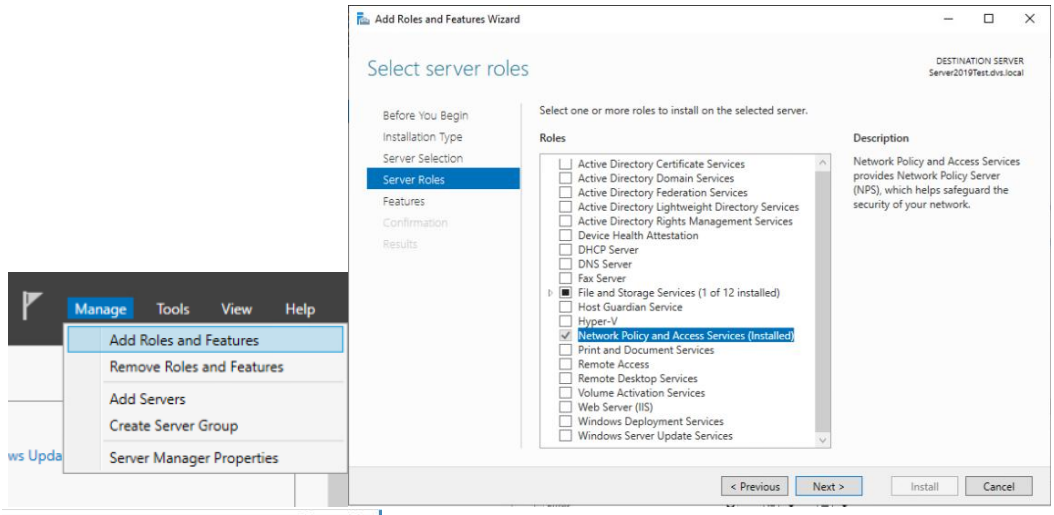
2. Make sure that the user accounts properties have the option to be controlled through a NPS also.

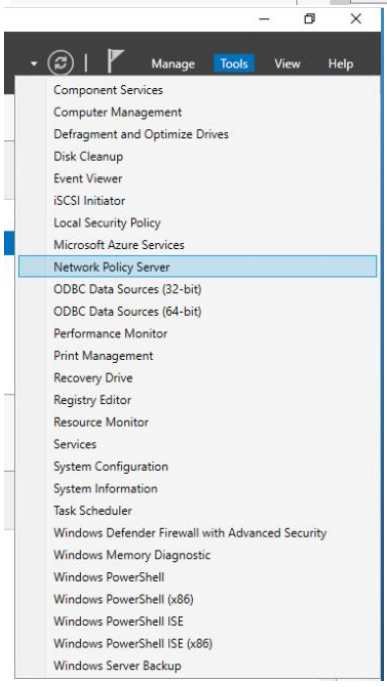


Step 2

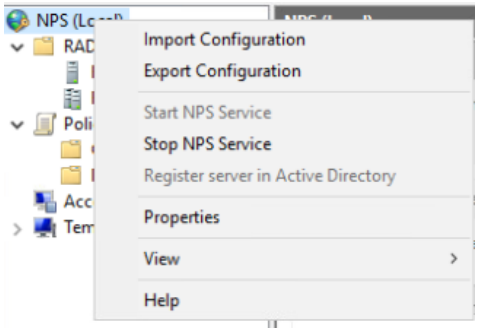
Prepare the NPS role for RADIUS.

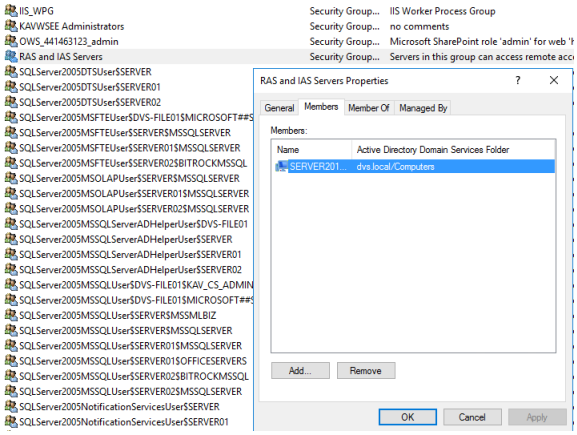
1. Install the NPS role through the add roles and features wizard. This can be done on a member server and doesn't require that the role is installed on a Domain Controller.



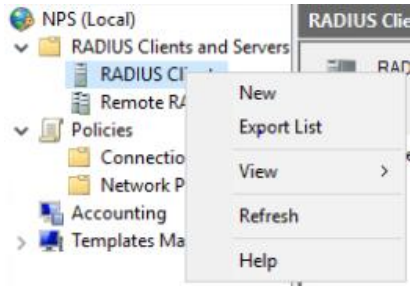


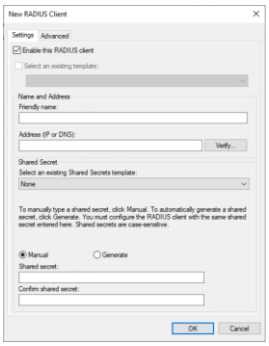
2. Once installed you need to register the NPS within AD so that it can read user accounts. Right click off NPS (Local) and choose "Register server in Active Directory". If you haven't got this option (Greyed out) it usually means you have in the past had a previous NPS within the domain. If this is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



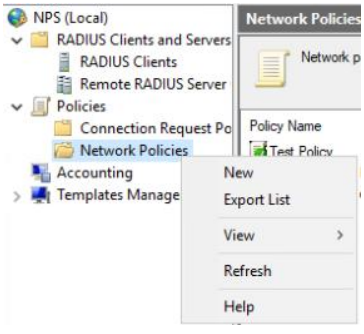


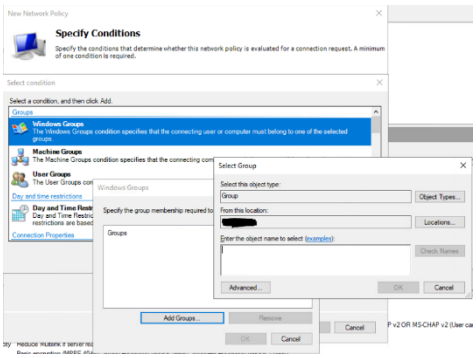
3. Right click of RADIUS Clients, click New - You will need to add the iQuila IP address of your iQuila Server. Give it a Share Secret that's used to connect iQuila vSwitch to NPS.





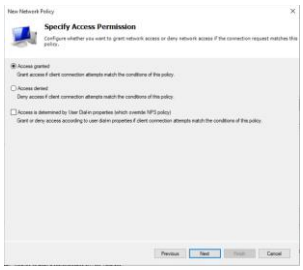
4. Right click off Policies – Network Policies and give your Policy a name. Leave the "Type of network access server" on Unspecified. Specify Conditions screen, Click Add and choose "Windows groups", Click the "Add groups button" and type the name of your AD group that you created before.

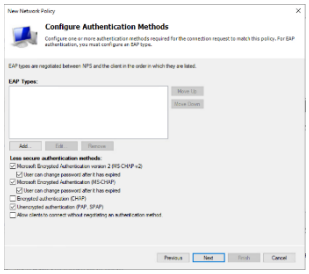




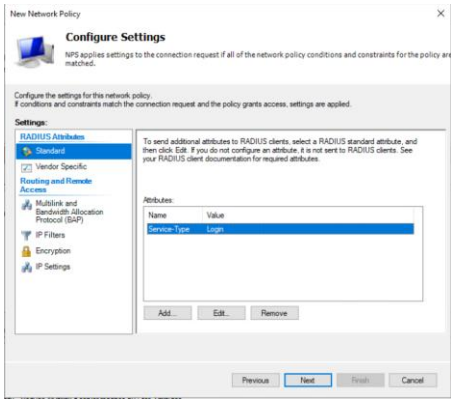
Choose ”Access granted” and then on the next screen of the wizard tick “unencrypted authentication (PAP, SPAP)”. Click “No” on the warning and leave the “Configure Constraints” section as it is.

(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.)

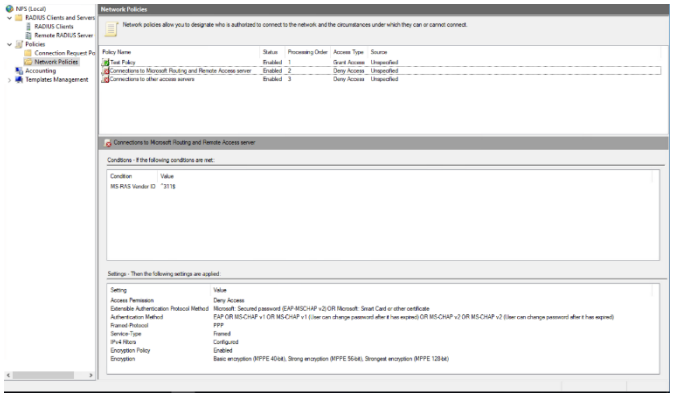




On the “Configure Settings” screen, remove “Framed-protocol PPP” and select (Service-Type) and click the “Edit” button and choose “Others” and select “Login.” So it looks like this;



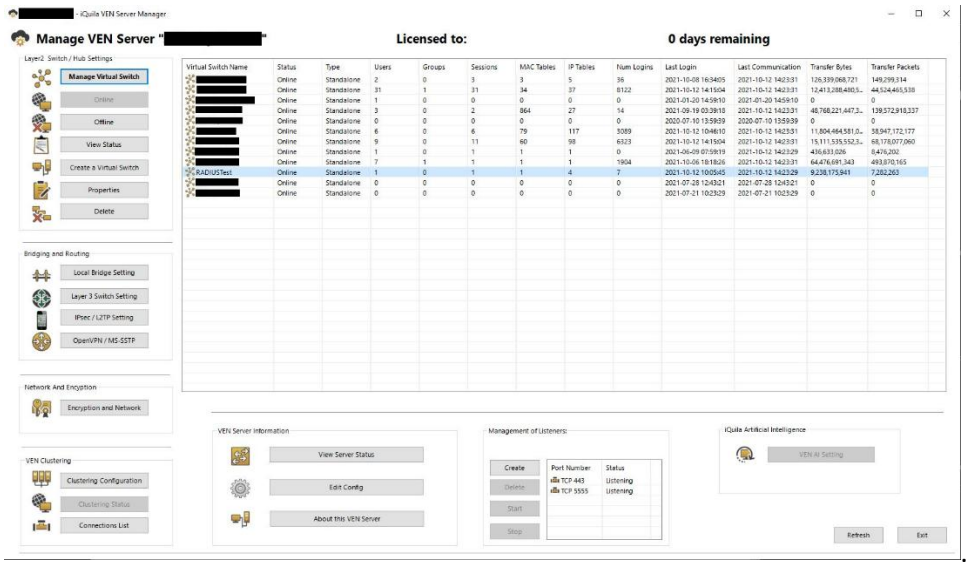
Click on Finish on the wizard on the “Completing new network policy.” If you have other policies then make sure your authentication policy is order 1 in the list as the policies get processed from top down starting with 1.



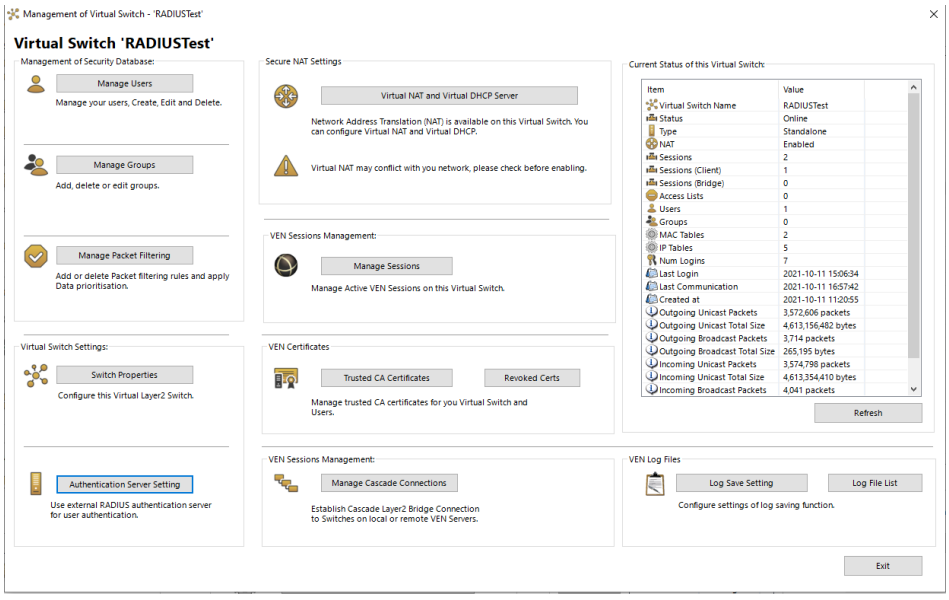
Step 3

Set iQuila for RADIUS

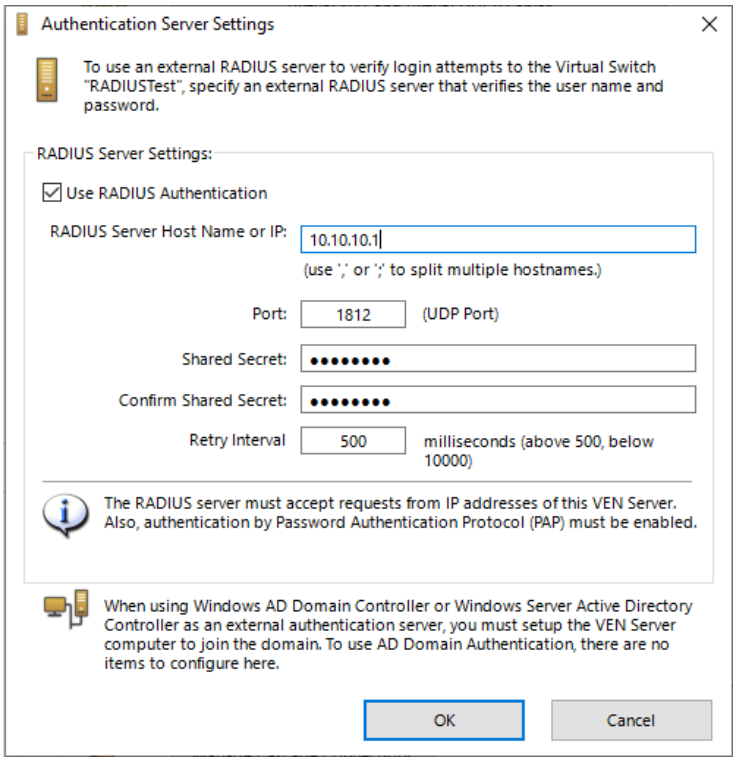
1. Login to your iQuila Enterprise Server and select your vSwitch and click “Manage Virtual Switch”.



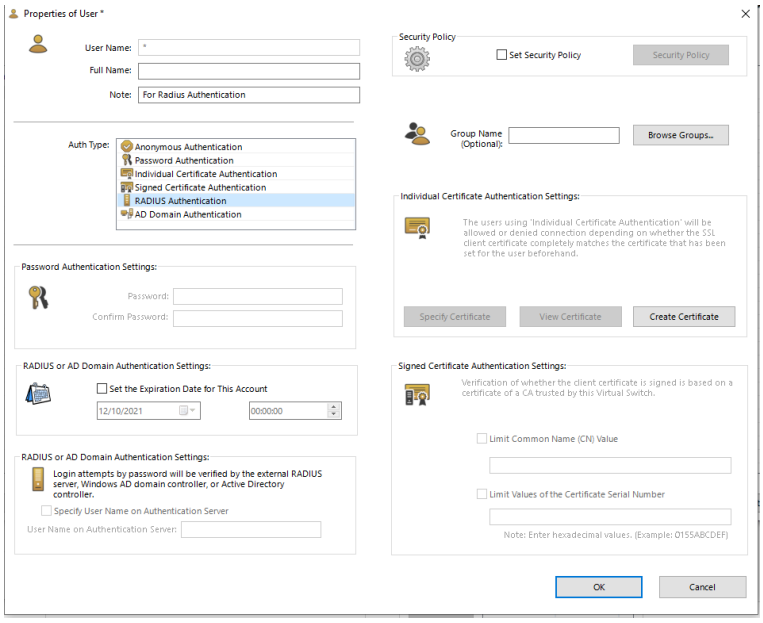
2. Click the “Authentication Server Settings.”



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

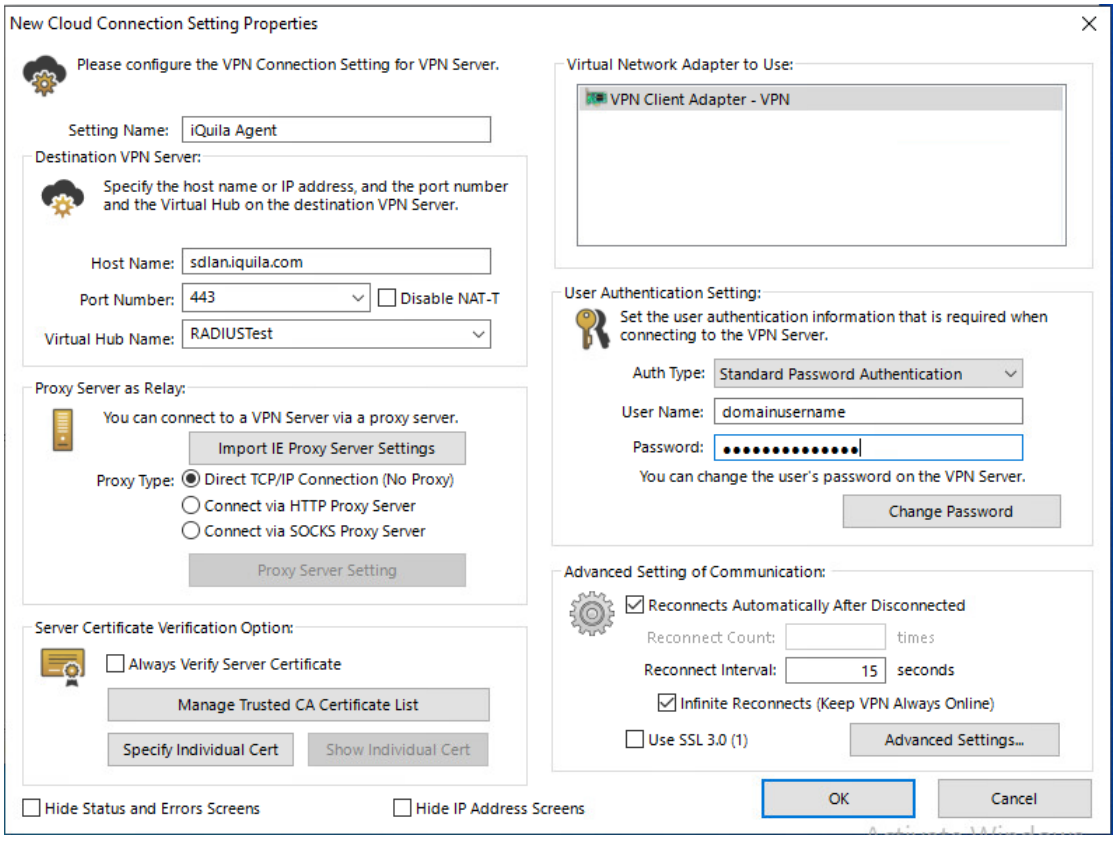


4. Click “Manage Users” button and create a new user account that will be used to forward credentials to the RADIUS NPS server for authentication. Enter a * for the username and choose RADIUS Authentication.



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.



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