

IQUILA

SOFTWARE DEFINED NETWORKS

iQuila Cloud Windows Manager for Linux

IQ22064r3

This Document Applies to:

iQuila Cloud

www.iQuila.com

iQuila Bridge Cloud Setup for Windows

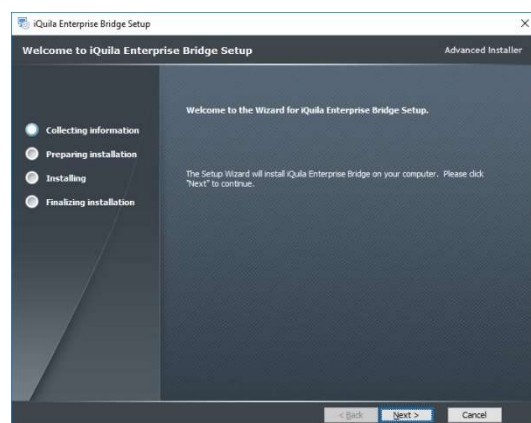
The iQuila Bridge Cloud software is an advanced AI-driven application that can bridge your entire network to the iQuila Cloud Layer2 virtual switch, this advanced software can be used in several different scenarios. This document will provide instructions on installing and setting up the Bridge software, you will be required to have a good understanding of Layer 2 networking.

Please use this software with great caution, incorrect use of this software could expose your network or cause your network to lock-up.

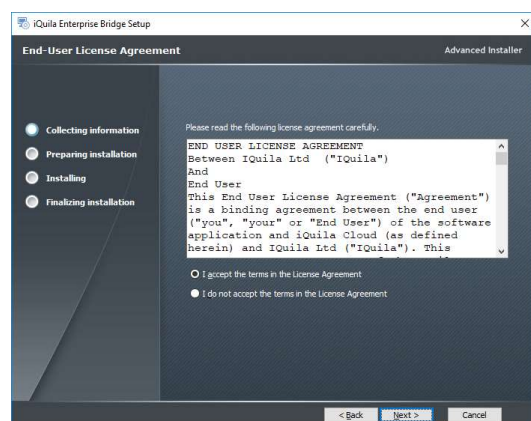
(Please take care not to cause a Layer 2 loop).

Once you have installed the Linux bridging software, please install the iQuila Windows manager as set out below.

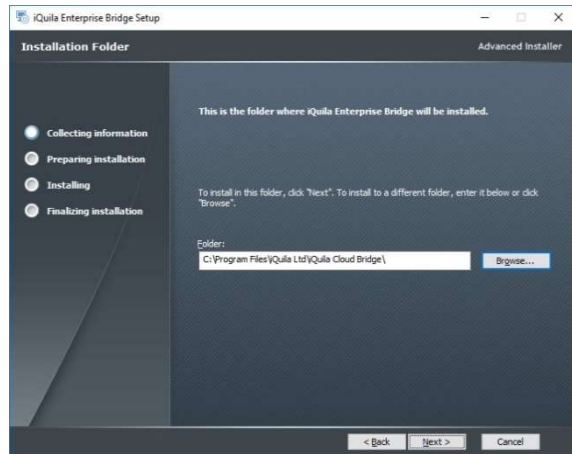
1. Install the iQuila Manager software by launching the application.



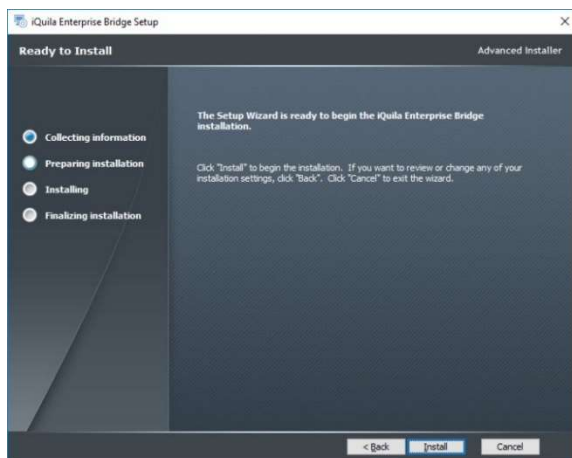
2. Accept the License Agreement.



- You may change the install path of the application, but we would recommend this is left to the default path.



- Once the wizard is ready, proceed with the install.



- When the install has finished, launch the iQuila Bridge application by clicking on the bridge icon placed on your desktop.

- This will launch the iQuila VEN Manager.

Select the Option Add Bridge



- You will now create and save a connection to your Linux server running iQuila Bridge.

Connection name = Enter a Name for your connection.

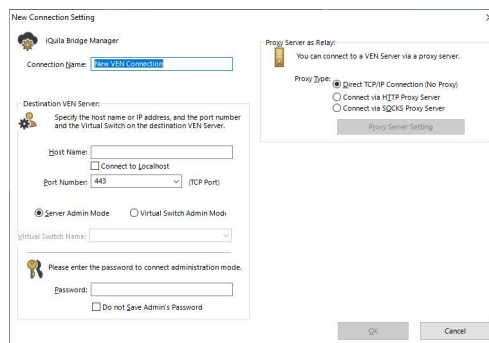
Under Host Name = Enter the Hostname or IP address of the Linux server you install the Linux bridging software.

Port Number = Enter the Port 5555 unless you have configured a different port.

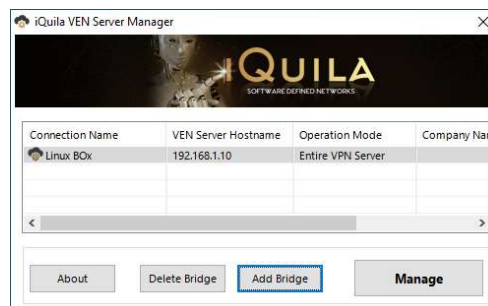
Password = if you have never logged on to this server please leave the password section blank.

If a Proxy server is between you and the iQuila Linux server then please Specify your proxy settings

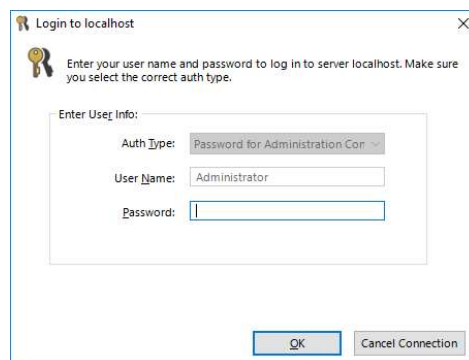
Select OK to Save and exit.



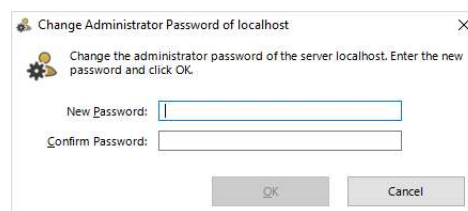
- You will now see your entry in the Connection Manager window, select the entry, and select Manage.



- Select the Manage button. A password window will appear, the default password is blank, so leave the password section blank and press OK.



10. The system will ask you to create a new password. Enter a new password in the password box and click OK.



11. You will be prompted with a statement asking you to confirm that you have had training and understand how Layer 2 networking works. If you understand Layer 2 networking, please proceed. Alternatively, please contact iQuila Support.
12. A confirmation box will show asking confirmation to start the network driver. To proceed, select YES. Once the network has been selected, and the driver started, the driver runs as a service under services. The network driver is a Kernel mode driver, so will automatically start as Windows is booting.
13. The next step is to enter your iQuila Cloud account details. Select Cloud Account setup and you will be prompted to fill in the following information.

Setting name = Enter your Cloud Device Name

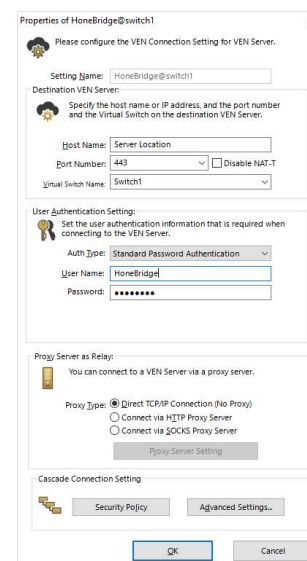
Host Name = This is the Hostname of the iQuila Cloud server you are connecting to. This will be shown in the email that was sent when you created your device on the iQuila Portal.

Port Number = Please leave this as 443 unless directed otherwise by iQuila support.

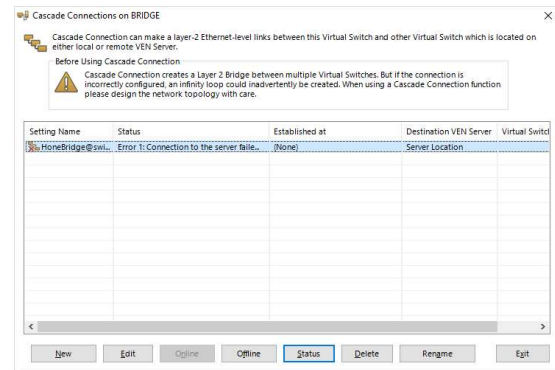
Username = Enter the iQuila Cloud device name you created.

Password = Enter the password you created for the Bridge device.

Proxy setting = If you are connecting via a Proxy server, please enter the correct Proxy information.

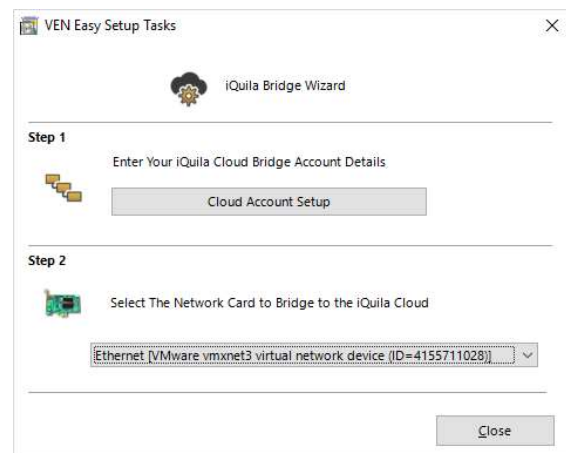


14. Click OK. A connection window will be displayed showing the status of the connection to the iQuila Cloud server. If the server is showing connected, click Exit. If the service is showing an error, please edit the connection details with the correct details and retry.

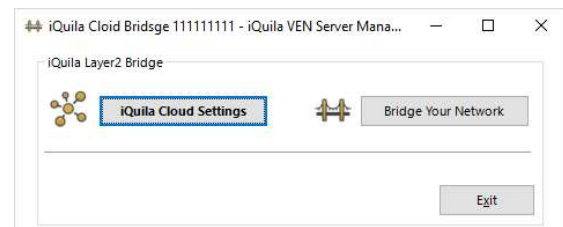


15. Select the dropdown and select the Network adaptor you would like to Bridge. (All traffic that is located on this network adaptor will be bridged.)

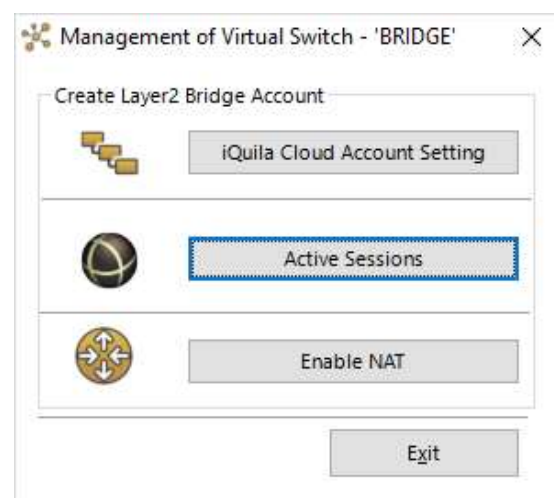
Once selected, click Close. This will now bridge your network to the iQuila Cloud switch.



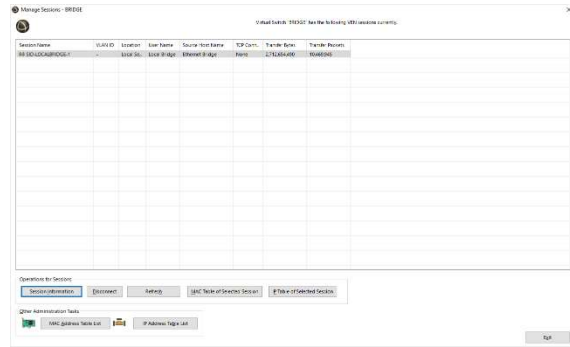
16. **Viewing Active Sessions on the network.** To view Active Sessions on the network, select the iQuila Cloud settings button.



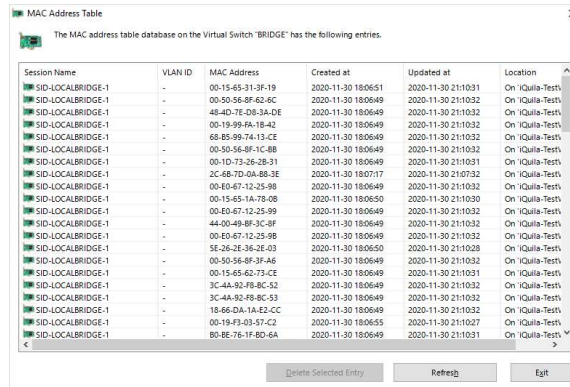
17. Click on the Active Sessions button.



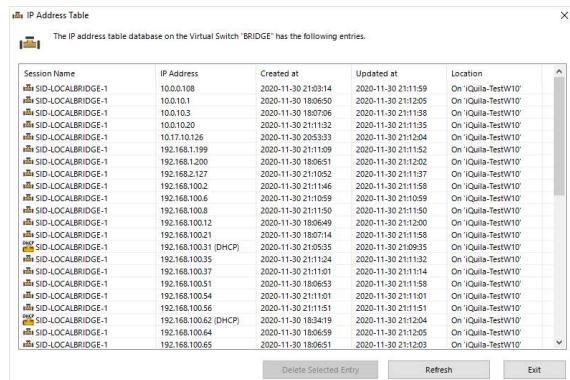
18. The Sessions Manager window will be displayed. This will show all active sessions on the remote network and local bridge.



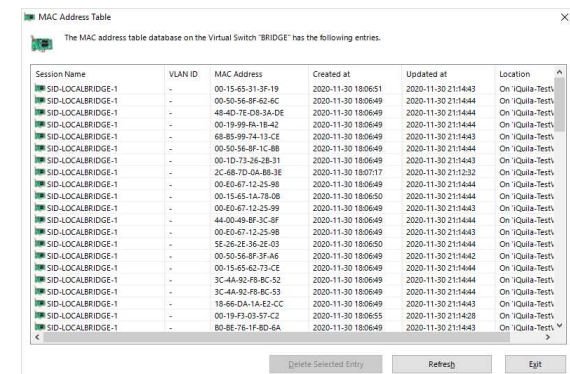
19. By selecting the Local Bridge entry, then selecting the MAC table of selected sessions, a display of all MAC addresses on the local bridge will be shown.



20. By selecting the IP Table of the selected session, a display of all IP addresses on the local bridge will be shown.



21. The MAC Address Table List will display all MAC accesses on the local database. This will be all the MAC addresses the iQuila Bridge software can see across the complete network.



22. The IP address Table List button will display all IP addresses the iQuila Bridge software can see across the complete network.

Session Name	IP Address	Created at	Updated at	Location
SID-LOCALBRIDGE-1	10.0.0.100	2020-11-30 21:03:14	2020-11-30 21:15:59	On iQuila-TestW10
SID-LOCALBRIDGE-1	10.0.10.1	2020-11-30 18:06:50	2020-11-30 21:16:10	On iQuila-TestW10
SID-LOCALBRIDGE-1	10.0.10.3	2020-11-30 18:07:06	2020-11-30 21:15:39	On iQuila-TestW10
SID-LOCALBRIDGE-1	10.0.10.20	2020-11-30 21:15:09	2020-11-30 21:15:35	On iQuila-TestW10
SID-LOCALBRIDGE-1	10.17.10.126	2020-11-30 20:53:33	2020-11-30 21:15:17	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.1.199	2020-11-30 21:15:09	2020-11-30 21:15:12	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.1.200	2020-11-30 18:06:51	2020-11-30 21:16:09	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.2	2020-11-30 21:11:46	2020-11-30 21:15:58	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.8	2020-11-30 21:14:39	2020-11-30 21:15:20	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.12	2020-11-30 18:06:49	2020-11-30 21:16:00	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.21	2020-11-30 18:07:14	2020-11-30 21:15:58	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.31 (DHCP)	2020-11-30 21:05:35	2020-11-30 21:15:35	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.51	2020-11-30 18:06:53	2020-11-30 21:16:09	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.62 (DHCP)	2020-11-30 18:34:19	2020-11-30 21:16:10	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.64	2020-11-30 18:06:59	2020-11-30 21:16:06	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.65	2020-11-30 18:06:51	2020-11-30 21:16:07	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.67	2020-11-30 21:16:01	2020-11-30 21:16:01	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.73	2020-11-30 21:14:30	2020-11-30 21:15:38	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.78	2020-11-30 18:06:49	2020-11-30 21:16:10	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.82	2020-11-30 20:53:33	2020-11-30 21:15:17	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.87	2020-11-30 21:16:08	2020-11-30 21:16:10	On iQuila-TestW10
SID-LOCALBRIDGE-1	192.168.100.104 (DHCP)	2020-11-30 20:42:56	2020-11-30 21:15:59	On iQuila-TestW10

NAT and DHCP Options

23. To enable NAT, enter the configuration window by selecting the iQuila Cloud setting option. Then select the Enable NAT option. The NAT configuration window will be displayed. To enable NAT, select the Enable NAT option. A confirmation window will ask you to confirm this selection. Click OK to enable NAT.

Caution = When enabling NAT, DHCP is Automatically enabled and will be broadcast down Bridge sessions or cloud sessions.

24. To configure NAT and DHCP, select the NAT Configuration option. The following configuration window will be displayed.

NAT Configuration
Set how NAT virtual host performs operation on the virtual network of Virtual Switch 'BRIDGE'.

Virtual Host's Network Interface Settings:
 MAC Address: FE-ED-CB-F8-FB-4C
 IP Address: 192.168.30.1
 Subnet Mask: 255.255.255.0

Virtual NAT Settings:
 Use Virtual NAT Function
 MTU Value: 1500 bytes
 TCP Session Timeout: 1800 seconds
 UDP Session Timeout: 60 seconds

Static routing table pushing function (for split tunneling):
 Push the static routing table to VEN clients.
 Edit the static routing table to push

Virtual DHCP Server Settings:
 Use Virtual DHCP Server Functions
 Distributes IP Address: 192.168.30.10 to 192.168.30.200
 Subnet Mask: 255.255.255.0
 Lease Limit: 7200 seconds

Options Applied to Clients (optional):
 Default Gateway Address: 192.168.30.1
 DNS Server Address 1: 192.168.30.1
 DNS Server Address 2: . . .
 Domain Name: dns.local

Save NAT or DHCP Server Operations to Log File

OK Cancel

Split Tunneling

25. To enable split tunneling on the remote clients, select the "Edit static routing table to push" option

Enter the routes you would like to push to the relevant clients. Press OK to save and push your configuration.

Edit the static routing table to push

This Virtual DHCP Server can push the classless static routes (RFC 3442) with DHCP reply messages to VEN clients.

Whether or not a VEN client can recognize the classless static routes (RFC 3442) depends on the target VEN client software. iQuila VEN Client and OpenVPN Client are supporting the classless static routes. On L2TP/IPsec and MS-SSTP protocols, the compatibility depends on the implementation of the client software.

You can realize the split tunneling if you clear the default gateway field on the Virtual DHCP Server options. On the client side, L2TP/IPsec and MS-SSTP clients need to be configured not to set up the default gateway for the split tunneling usage.

You can also push the classless static routes (RFC 3442) by your existing external DHCP server. In that case, disable the Virtual DHCP Server function on NAT, and you need not to set up the classless routes on this screen.

Edit the static routing table to push
 Example: 192.168.5.0/255.255.255.0/192.168.4.254, 10.0.0.0/255.0.0.0/192.168.4.253

Split multiple entries (maximum: 64 entries) by comma or space characters.
 Each entry must be specified in the "IP network address/subnet mask/gateway IP address" format.

See the RFC 3442 to understand the classless routes.

OK Cancel