SOFTWARE DEFINED NETWORKS

iQuila Deployment Guide for iQuila Bridge in Microsoft Azure

iQ22059r3

This Document Applies to:

iQuila Enterprise

Microsoft Azure

Bridge Deployment Guide

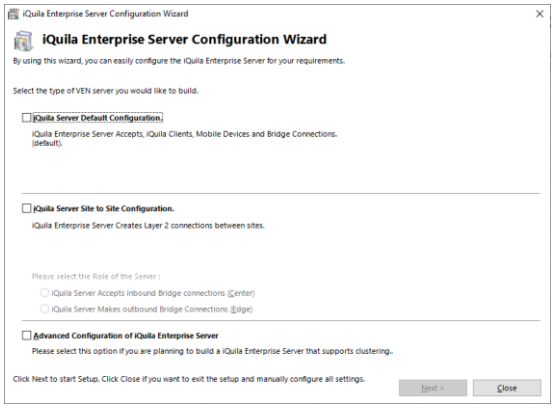
Overview

iQuila Enterprise is a powerful tunnelling platform allowing you to extend your corporate network across multiple locations while keeping the tightest of security across your network, using iQuila enterprise bridges you can easily link in remote branch offices around the world and home workers at ease. The advance AI manages the multicast traffic over your network, and the security policy centre allows you to control what data can travel to what destination you select over your network.

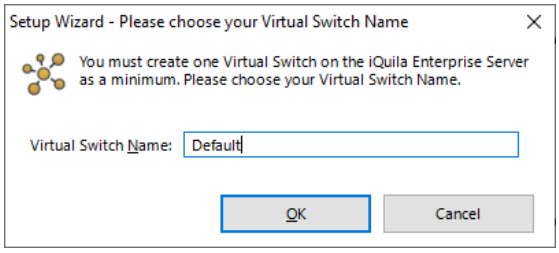
This Deployment Guide will guide you through setting up the iQuila Enterprise Bridge Appliances along with the iQuila Enterprise windows client software.

Deploying the Enterprise Server / Bridge

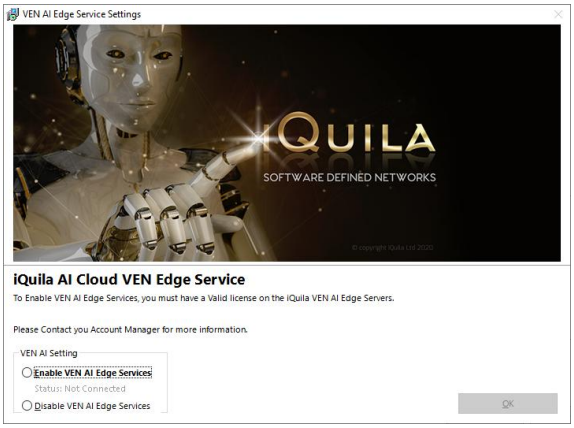
From the iQuila Manager login to the iQuila server you have just deployed, the first time you login you will be prompted with a wizard, select the 1st option iQuila Server Default and click next.



You will then be asked to create a default Virtual Switch. Enter a name of choice then select ok.



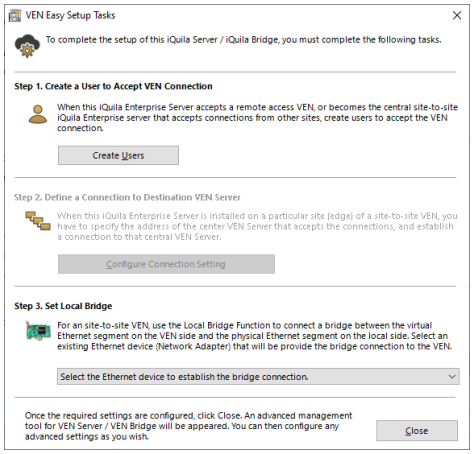
If your service includes the VEN AI Edge Processing, you can enable it here. If your subscription does not include this feature, please select Disable VEN AI Edge Processing and click ok.



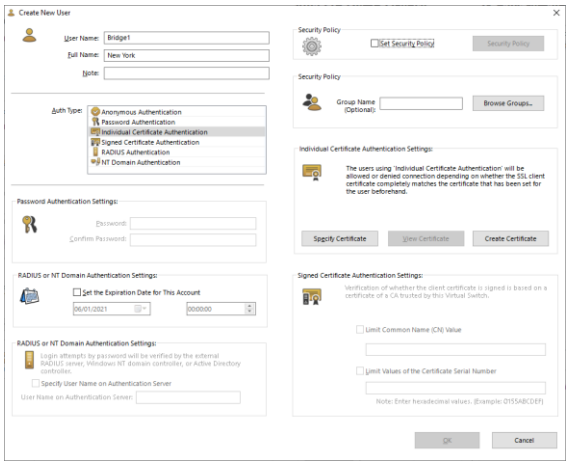
The wizard will now ask you to create user accounts.

User accounts are used for Authenticating Server, Bridge devices along with client software connections.

To create your users select create users.



The Auth type is defined, by Security Permissions from the dropdown list.



First, we will go through setting up a bridge user account.

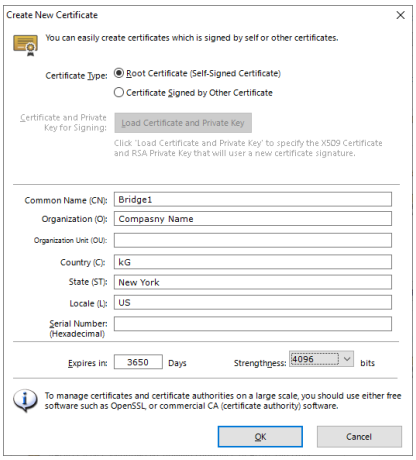
Under username enter the name of your choice, for this bridge device in this scenario we will choose the username Bridge1. In the full name section enter the name of the location of the bridge that will be located. In this scenario we chose New York.

Now select the authentication type you would like, there are 6 different types of authentications in this scenario. We will use Individual certificate authentication.

Next, select the create certificate button.

The ***create new certificate*** window will show

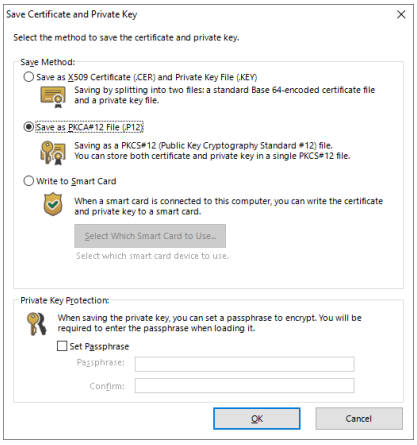
Fill out the relevant information and ***select the strengthens bits from the dropdown field.***
then ***select OK.***



You will now be asked to select the format, and protection for your certificate, in this scenario we will select Save as PKCA#12

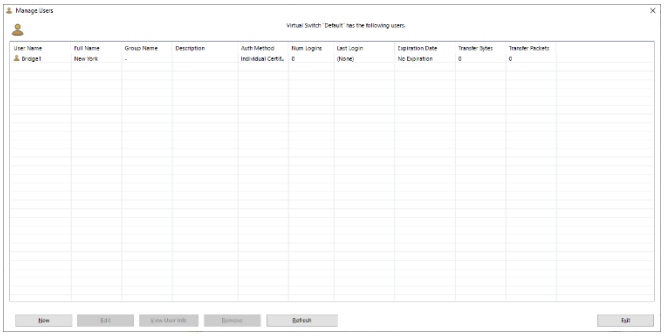
Then, select ***set passphrase*** and enter a strong passphrase to protect the certificate.

Click save and save the certificate with a name that will identify it later e.g. Bridge1 New York.



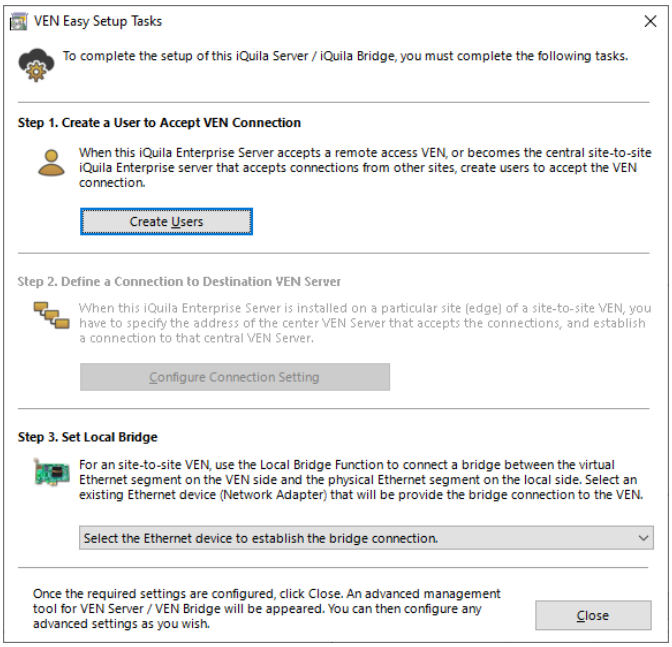
Once the certificate has been saved, the user window will be displayed, you can add further users accounts now or they can be added later.

Once you have finished adding users click **Exit**



This will return you back to the easy setup wizard.

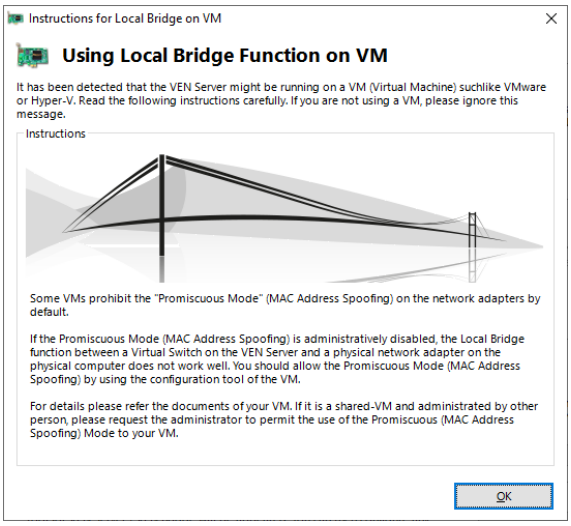
Under Step 3 ***select the dropdown*** and ***select the network adaptor*** you would like to bridge, normally this will be a different adaptor to the adaptor used for management, once selected ***select Close.***



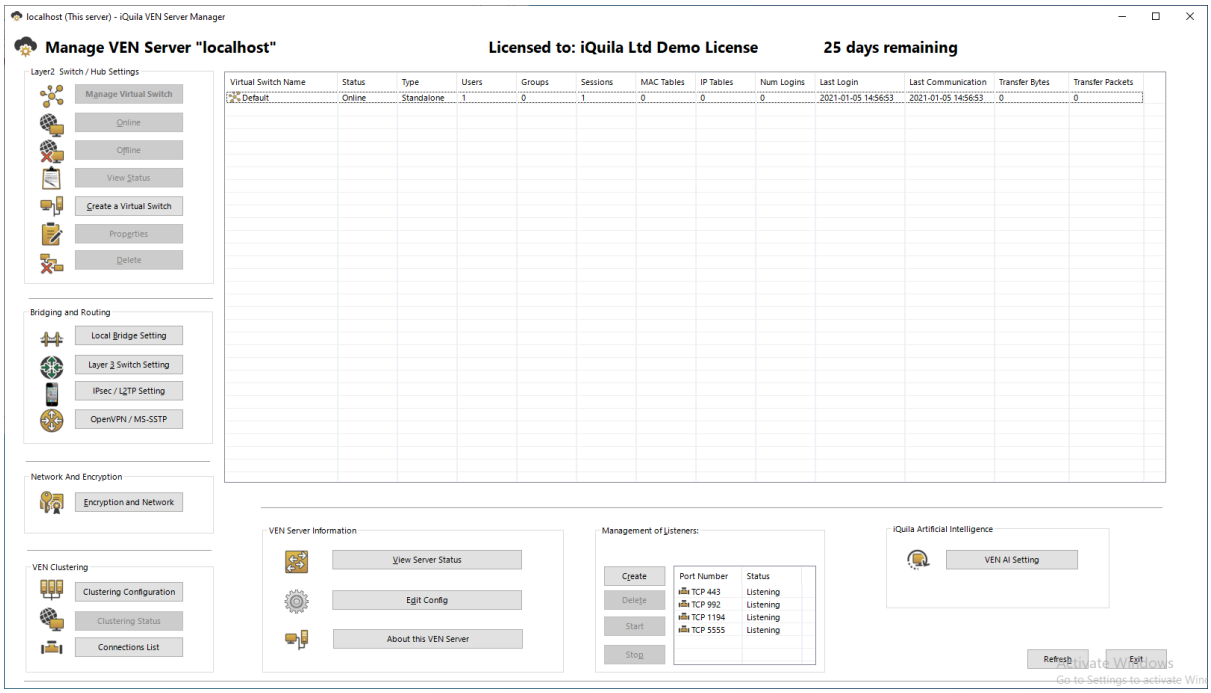
If you are using a Virtual Environment, a Notification window will be displayed.

It is important for iQuila to function correctly promiscuous mode is set to accept on virtual infrastructure.

Please make the necessary changes and ***click ok.***

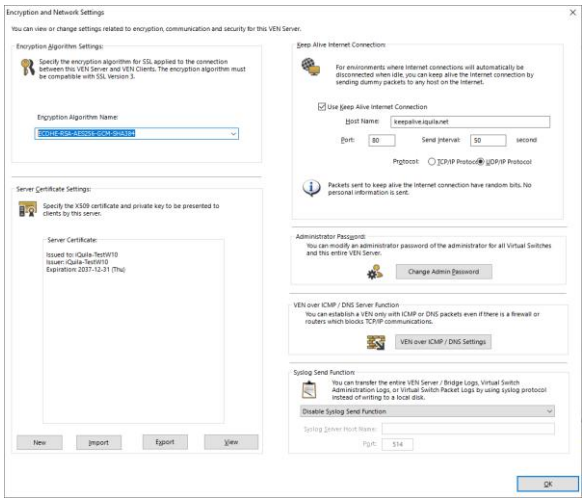


You will now be displayed the main iQuila Management window.



Encryption Setup

Select Encryption and Network button, this will display the Encryption and Network settings window.

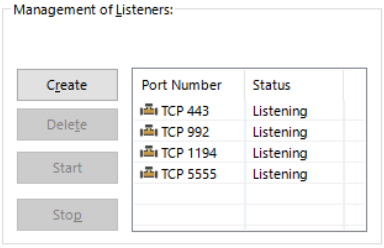


Under Encryption and Algorithm ***select the Appropriate encryption algorithm***, in this case for strong encryption we will select the algorithm.

ECDHE-RSA-AES256-GCM-SHA384

Once selected ***click OK***

From the main management window under Management of Listeners, ***select any additional ports*** you may like the server to listen on and communicate with. The default port for communication from clients and bridges is TCP port 443.

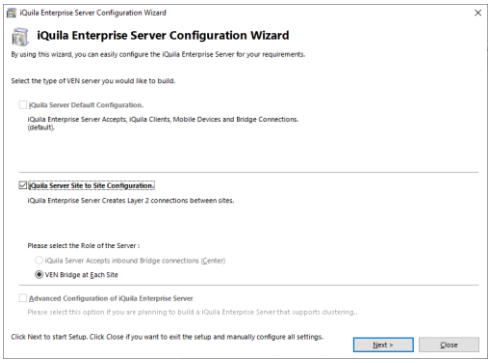


If you are locating the iQuila Enterprise Device behind a firewall. **Please read the iQuila Enterprise Firewall pdf**

Configuring a Bridge Device

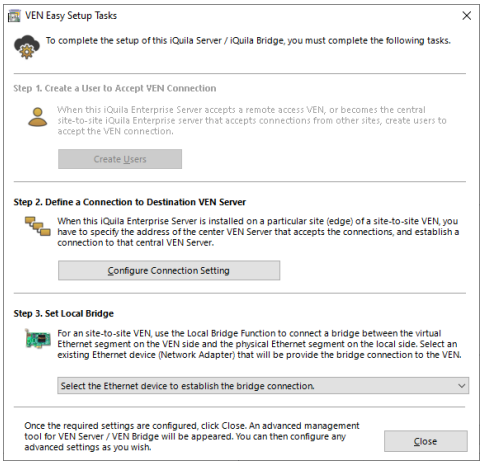
Bridge Device Management is configured on TCP Port 5555, configure your iQuila enterprise manager to the IP of the bridge device and connect, when you first connect to an iQuila Device it will ask you to create a password.

When you connect to the iQuila Bridge for the first time you will be presented with the iQuila Bridge configuration window.



Click Next.

As Bridge devices do not require users this section is not avaliable, so please ***proceed to step 2*** configure connection setting

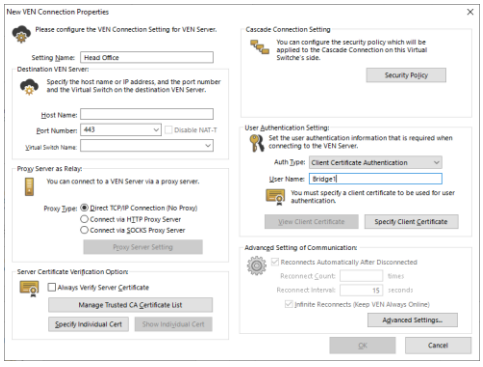


The Connection setting window will show

Under Setting name, ***enter a name of the connection setting*** e.g., Head Office

Host Name: ***enter the host name or IP address*** of the iQuila Enterprise server.

Port Number: unless you have configured different port numbers on the iQuila Enterprise server the port number can be left as default Port 443.



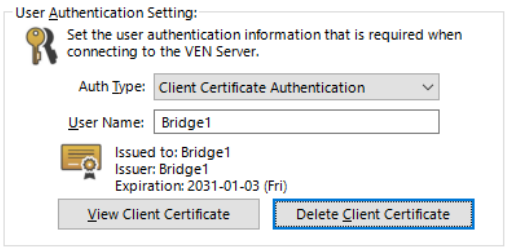
The virtual Switch name should be auto populated (unless you have disabled this function on the iQuila Server) if this function is **disabled** then manually ***enter the Virtual Switch name***.

Under the section User and authentication setting***, change the Auth Type to Client Certificate authentication*** and ***enter the username created with the certificate***, in this scenario we will use Bridge1.

Select the Option, ***specify client certificate***, select the ***Certificate we made previously Bridge1 New York***, you will be prompted for the Security Phrase, once entered ***press Ok.***

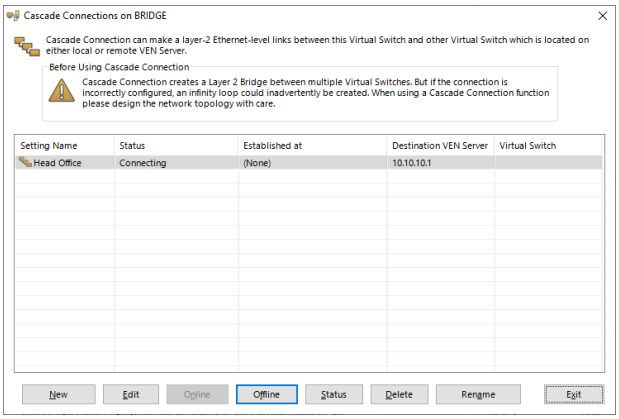
The certificates name an expiry date will be displayed.

Click ok

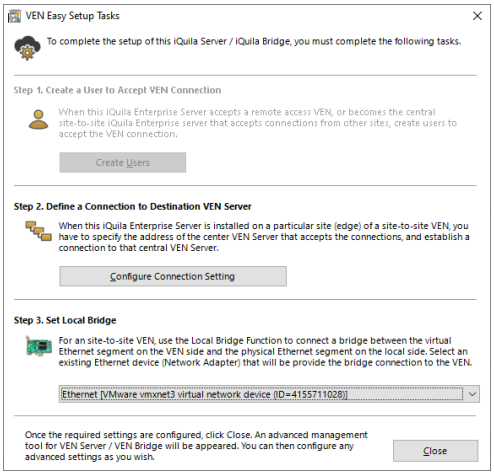


The cascade connection window is displayed the status of the connection to the server.

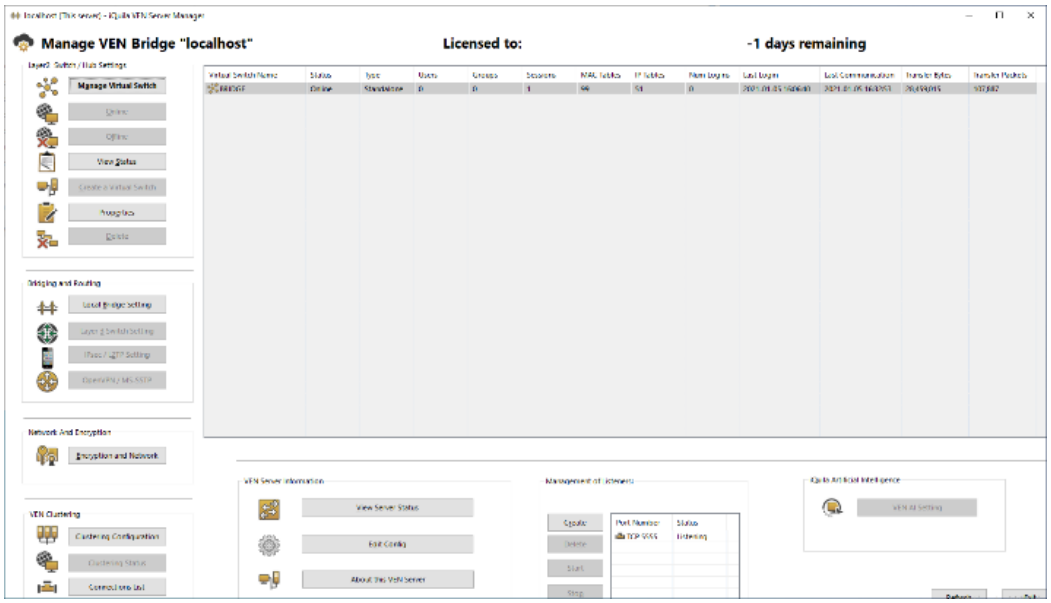
Select Exit



On Step 3 of the wizard ***select the drop down*** and ***select the network adaptor*** you would like to bridge and ***select close***.



You will now be presented with the main management windows for Bridges.



Packet Filtering & Data Prioritisation

iQuila Enterprise Packet Filtering and Data Prioritisation enables you to secure your network whilst prioritising your important data, depending on your Licensing, up to 4,096 entries can be defined in a Virtual Switch. Packet Filtering is a function which either passes or discards IP packets passing through network devices according to designated rules commonly referred to as packet filtering rules, rules are processed on the priority number assigned to each rule, the lower the priority number set the more important the rule. Multiple rules can be created for both IPv4 and IPv6

Data which can be Defined by Packet Filtering Entries.

The following data can be defined by the access list registered in the Virtual Switch. Data which can be Defined by Packet Filtering Entries

Basic Setting

Access List Memo.

Enter a description of the access list entry. This entry enables the setting of an arbitrary character string to clarify the entry for the Virtual Switch Administrator, and its contents has no effect on packet filtering operation.

Action.

Designates how an IP packet is treated when a matching entry definition is found in the access list. Sets to [Pass] or [Discard].

Priority.

Designates the priority of an entry within the access list as an integer. The lower the integer, the higher the priority the packet has over the VEN connection. If there are access list entries with the same priority, it is undefined as to which is applied first.

Filtering Option for IP Headers

Source IP address.

Designates the sending IP address as the packet's matching criteria. It is also possible to designate a subnet range including multiple IP addresses by designating the network address and subnet mask. All, sending IP addresses match when no range is designated.

Destination IP address.

Designates the destination IP address as the packet's matching criteria. It is also possible to designate a subnet range including multiple IP addresses by designating the network address and subnet mask. All destination IP addresses match when no range is designated.

Protocol Type.

Designates the protocol number of that IP packet as the packet's matching criteria. It is possible to match all IP protocols. The numbers which can be designated can be entered as integers although 6 (TCP/IP), 17 (UDP/IP) and 1 (ICMP) are already defined.

Source / destination port number range.

The minimum or maximum source port and destination port numbers can be designated as the packet's matching criteria when TCP/IP or UDP/IP is selected as the protocol type. All port numbers are regarded as matching when no values are designated.

Filtering Options for User and Groups

Source username.

A username can be designated as the packet's matching criteria when wishing to match only those packets sent by a specific user (strictly speaking, it is the packet sent by the VEN session of a specific username). Sending usernames are not checked when no name is designated.

Destination username.

A username can be designated as the packet's matching criteria when wishing to match only those packets to be received by a specific user (strictly speaking, it is the packet intended to be received by the VEN session of a specific username). Destination usernames are not checked when no name is designated.

Access List Entries Match

When none of the Access List Entries Match.

When multiple access lists are registered on a Virtual Switch and the IP packet does not match any of the entries contained therein, a [Pass] action is decided by default.

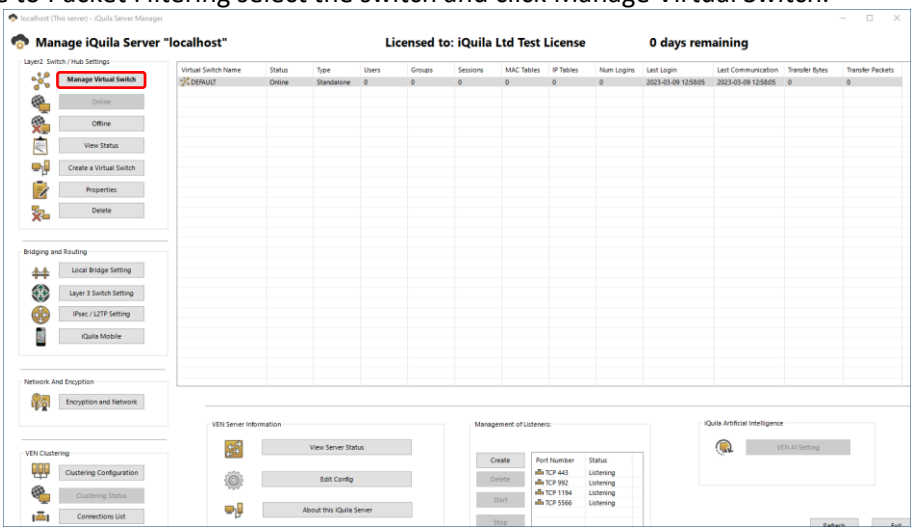
Adding, Deleting & Editing Access List Entries.

To add, delete or edit entries in the access list, click on the [Manage Access lists] button in the iQuila Server Manager. Next click on the [Add], [Delete] or [Edit] buttons. Be sure to click the [Save] button after completing any changes to the access list, as changes are not applied to the Virtual Switch unless saved. Furthermore, the access list is enabled from the instant it is set (also applies to iQuila VEN sessions which are already connected.

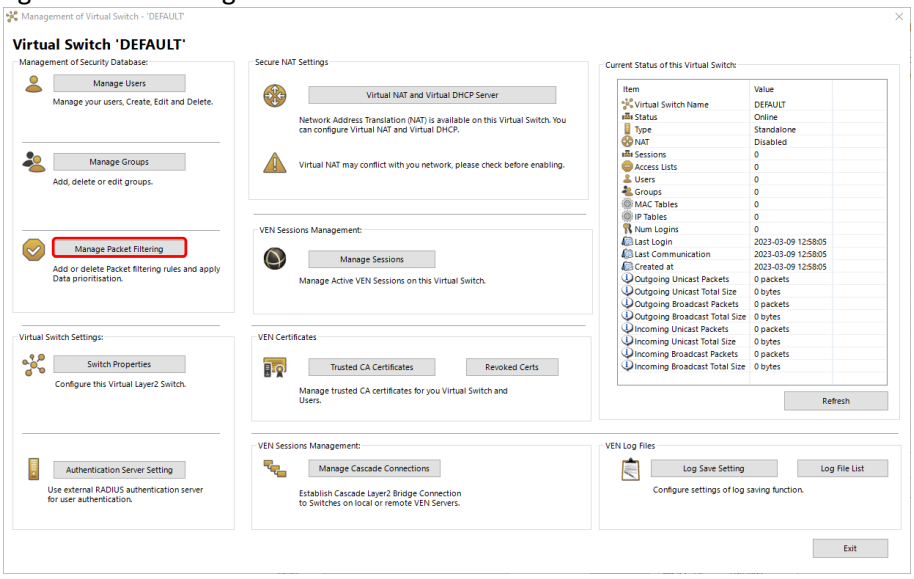
To modify the access list with the command line utility, use the [AccessAdd], [AccessList], [AccessDelete], [AccessEnable] and [AccessDisable] commands.

The following section is a brief insight to adding Packet Filtering Rules.

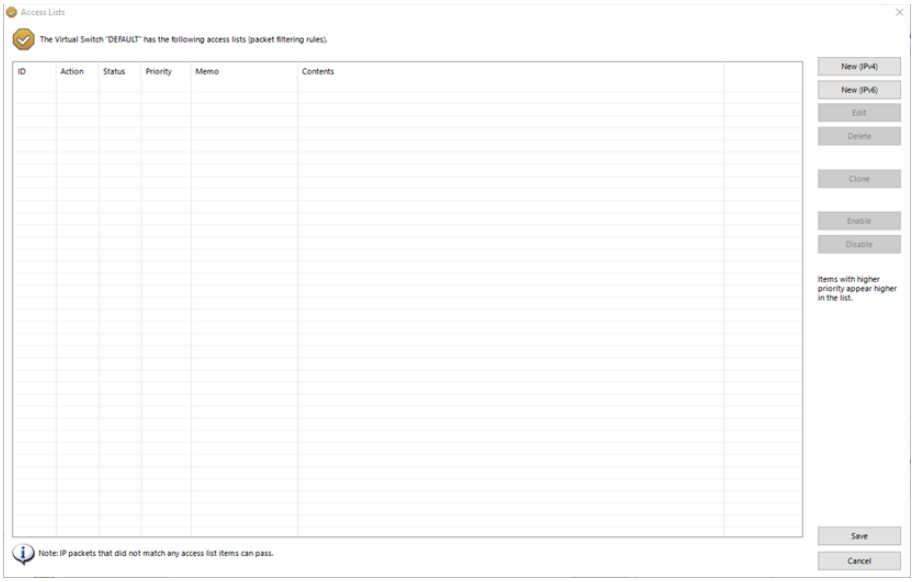
To navigate to Packet Filtering select the switch and click Manage Virtual Switch.



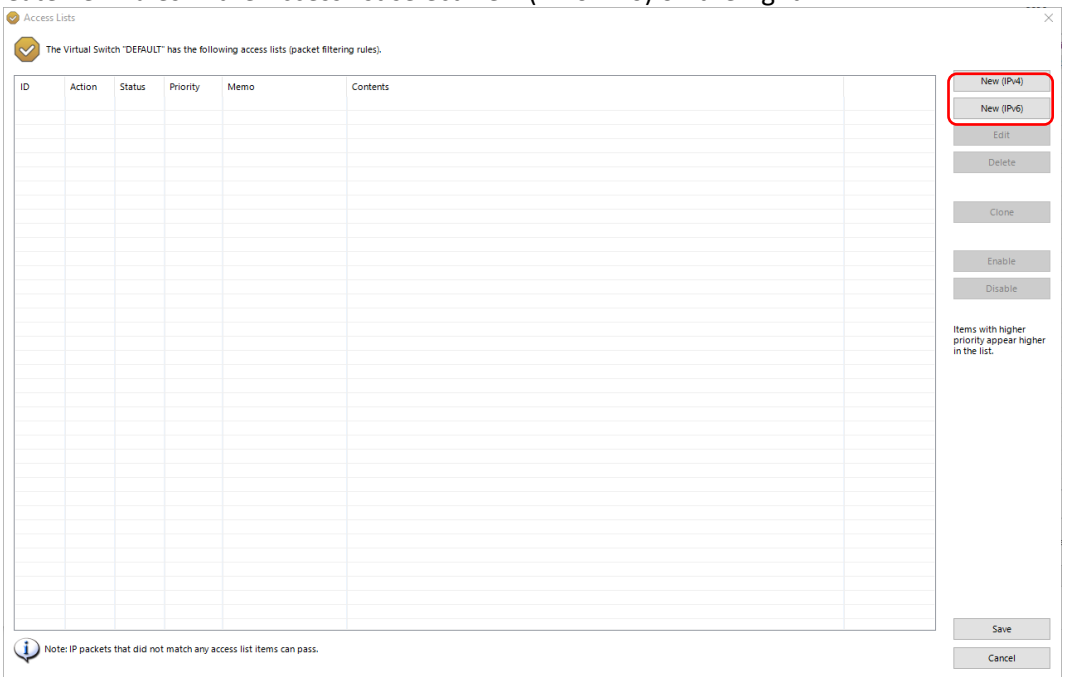
Select Manage Packet Filtering.



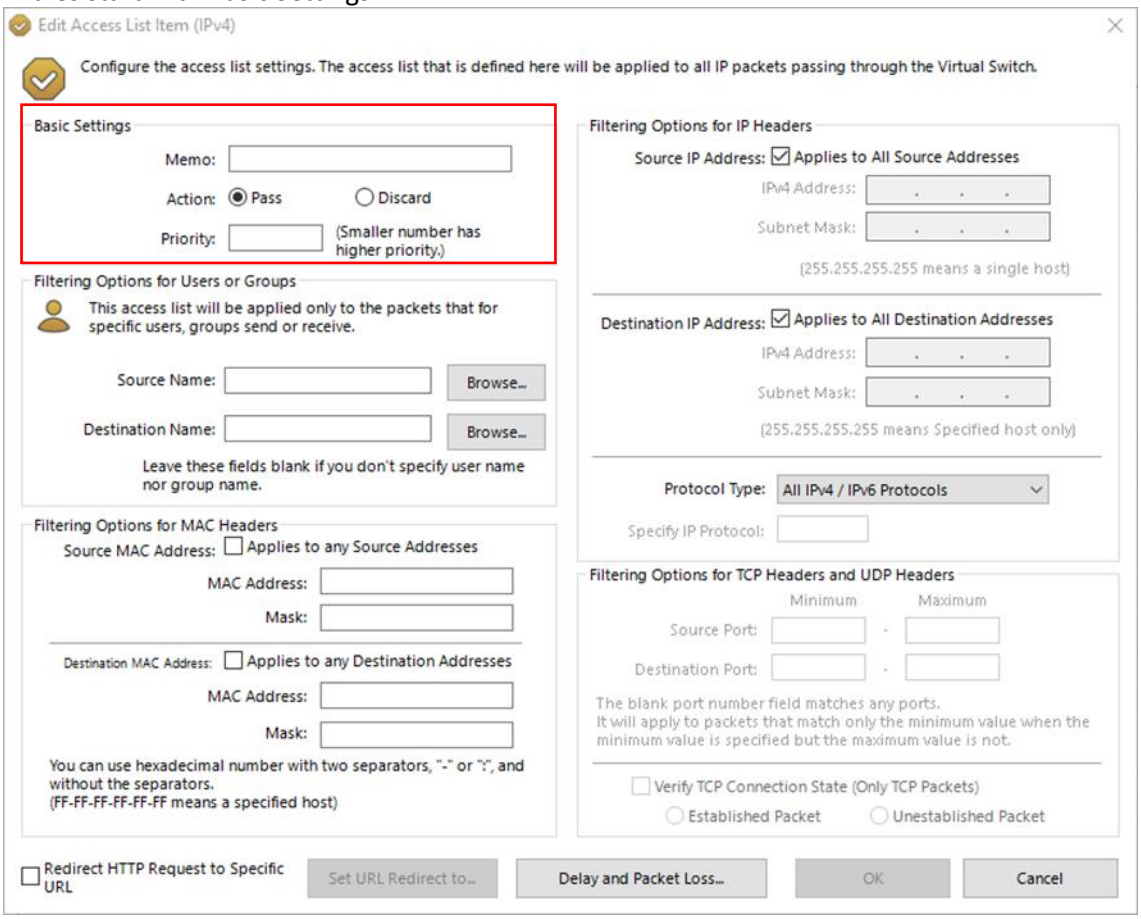
The Action List for rule creation.



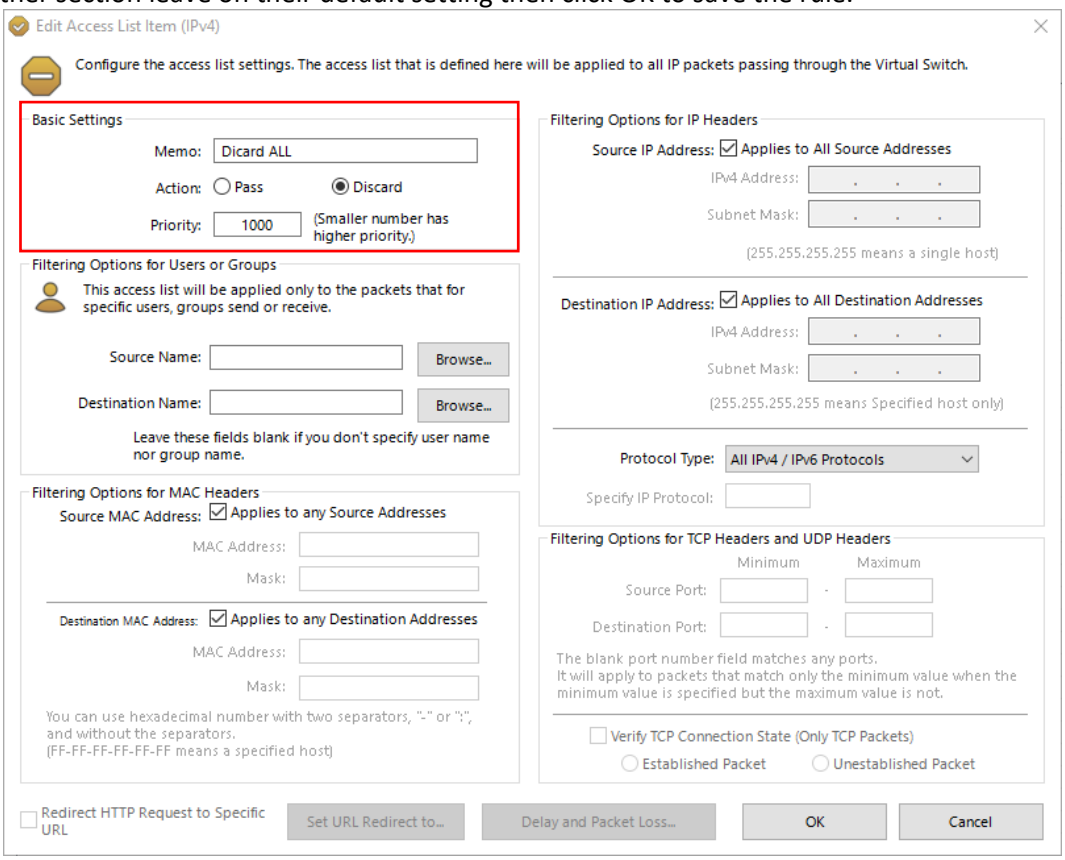
To create new rules in the Access list select New (IP4or IP6) on the right.



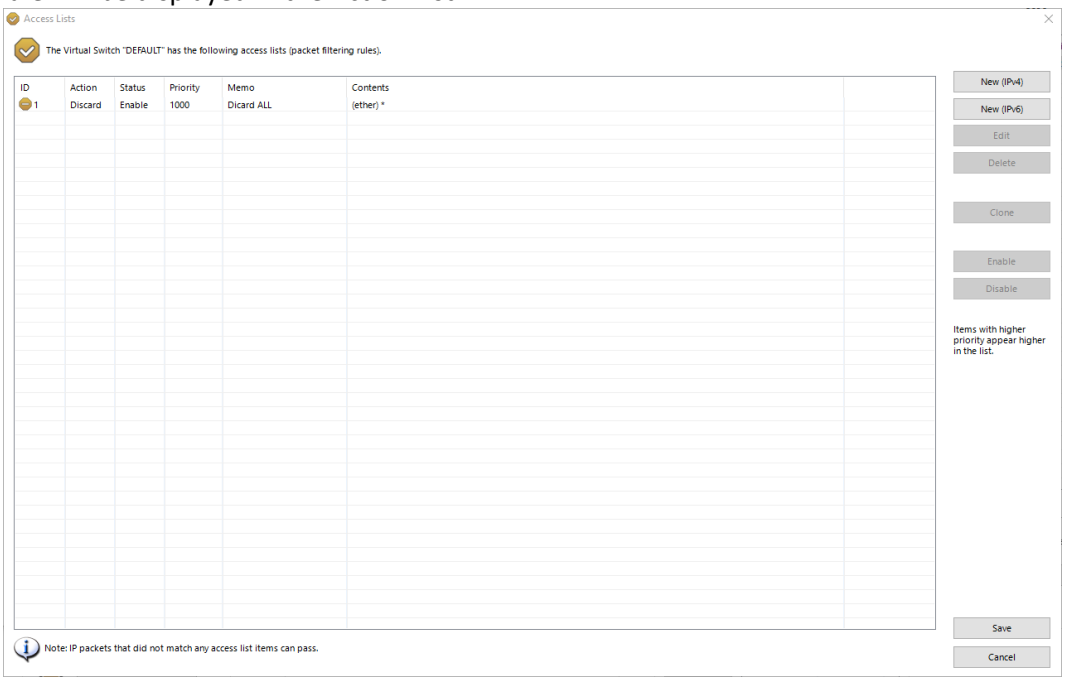
All rules start with Basic Settings.



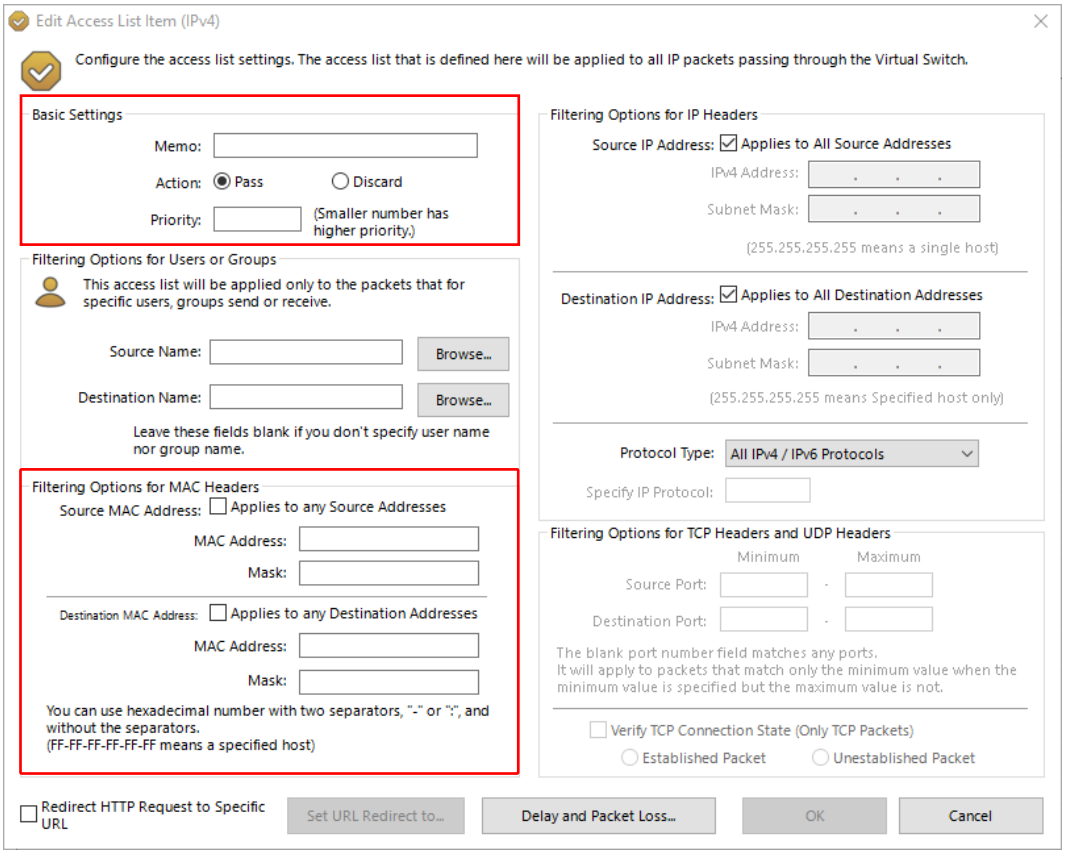
The first recommended rule to be applied a Discard ALL rule. This will drop all packets to the switch and should be set for IP4 and IP6.
In this example.
Set the Memo (Rule frendly name) to Discard ALL.
Set Action to Discard. Discard drops the packet.
Set Priority to 1000. Sets the priority position of the rule.
All other section leave on their default setting then click OK to save the rule.



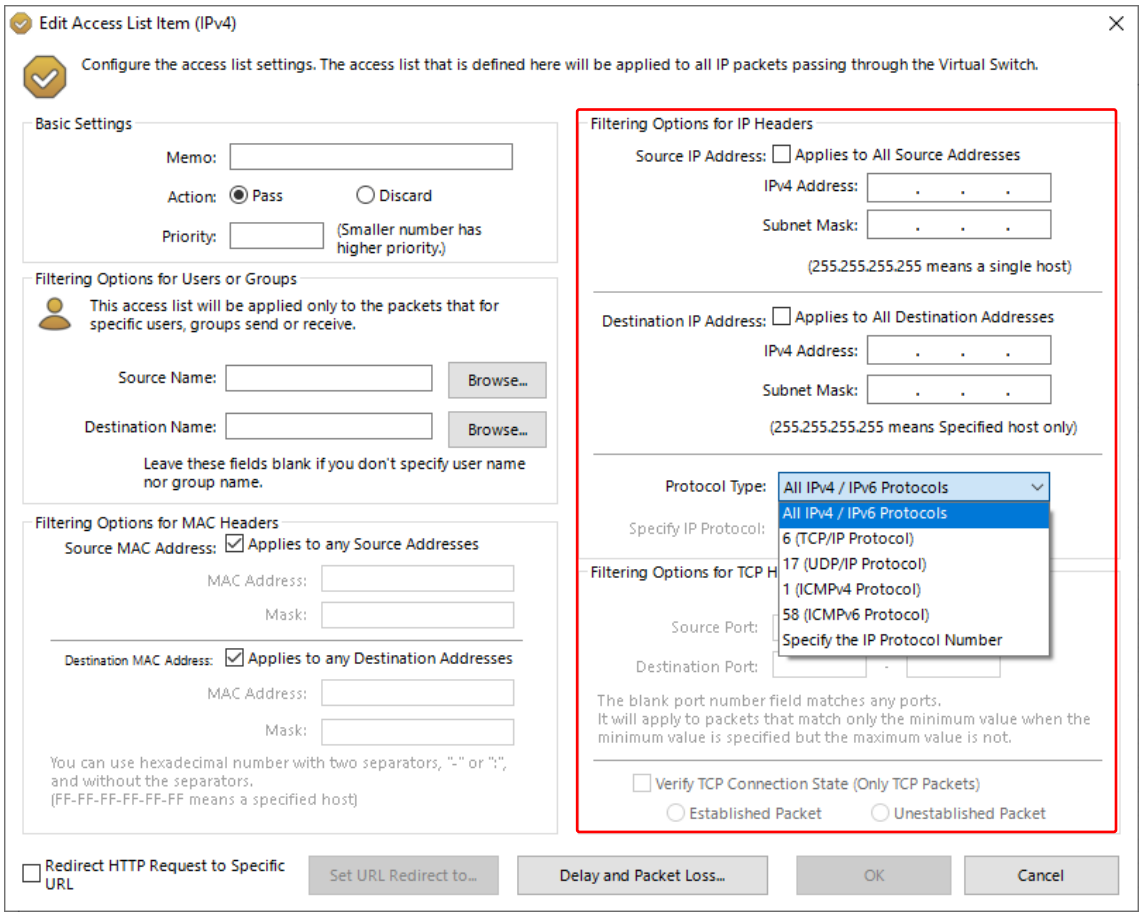
The rule will be displayed in the Action List



Filtering by MAC address.
Set the Basic Settings first.
The default setting for MAC filtering is set to Apply to any source address. Untick the source/destination box to enter a specific MAC address.
Select OK to add the rule.



Filter Option for IP Headers is the main rules to set based on source/destination address and protocal type. Default setting allows any source or destination IP address and All IP4/IP6 protocol types



Protocal Type allows you to select a custom protocol by selecting the Specify the IP Protocal number option from the list. The dropdown list contains the standard 4 protocol types by default. The Filtering options for TCP/UDP headers are the same as as used in all firewalls for traffic routing.