iQuila Enterprise
Advanced Client Customization

IQ22090r4

This Document Applies to:

iQuila Enterprise 5.00

iQuila Enterprise Client is a powerful remote access application that Utilizers the iQuila VEN Layer 2 protocol, this guide will show you how to install the application and use the advanced features and customize the application for specific configurations for easy distribution.

1. Installing the iQuila Windows Enterprise Admin Application
2. iQuila Enterprise Overview
3. Managing Virtual Network Adaptors
4. Configuring multiple remote connections
5. Enabling Remote Management of the iQuila Client
6. Protecting configuration changes
7. Advanced Mode and Simple Mode
8. System Tray Menu
9. Exporting and importing configurations
10. Understanding the configuration file
11. Building a Custom Install with Easy Installer
12. MSI Silent Installs
13. Managing Split Tunnelling
14. iQuila Client Command Line Utility

1. Installing the iQuila Windows Enterprise Admin Application

When installing iQuila Enterprise service is installed called iQuila VNE Client, this service is linked to the iQuila engine that controls the VEN protocol, for iQuila to function this server is required to be running.

As default, the application is installed in C:\Program Files\iQuila Enterprise Client\ and consists of 3 main applications.

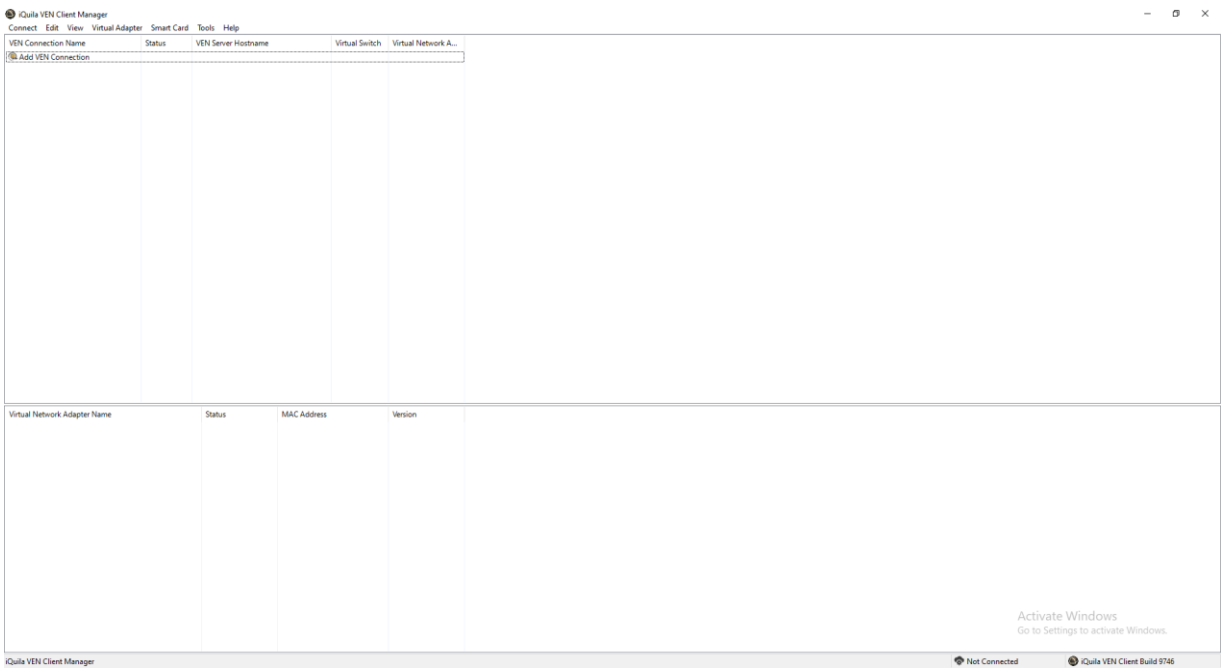
- iQuila Server.
- iQuila Manager.
- iQuila Command Line Utility.

Upon installation, two folders are created within the iQuila Client directory. ***backup.vpn_client.config*** and ***client_log***. The ***backup.vpn_client.config*** folder, stores backup configurations of any changes made to the config. The ***client_log*** folder holds all log files recorded by iQuila for debugging issues.

2. iQuila Enterprise Overview:

iQuila Enterprise has two interfaces, Simple and Advanced. The Advanced view gives you access to more complex configurations, whereas Simple mode, gives a simpler look, but making it less complex and easier for the client to manage. Custom installs can be created so that the application automatically launches into easier mode by default. The advanced mode can also be protected by a pre-set password, stopping users from changing the settings.

The iQuila Client Manager is set in two sections. The top section shows the configuration entries of connections and their status, the lower section shows the Virtual Network Adaptors that are installed.



You can add as many client configuration entries as you wish into the configuration window. If you require multiple connections to run at the same time, you will need to install multiple Virtual Network Adaptors, and then assign a different Virtual Network Adaptor to each of the different configurations that you require to run at the same time. You can add up to 127 Virtual Network Adaptors, giving you

the ability to have 127 different concurrent connections, running at the same time, connected to different iQuila Servers, Switches, or iQuila Cloud Servers. For more information on Virtual Network Adaptors Please see Section 3

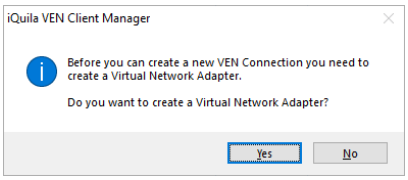
iQuila Enterprise Client Menus:

From the main iQuila Enterprise Client interface, there are several menu options as follows.

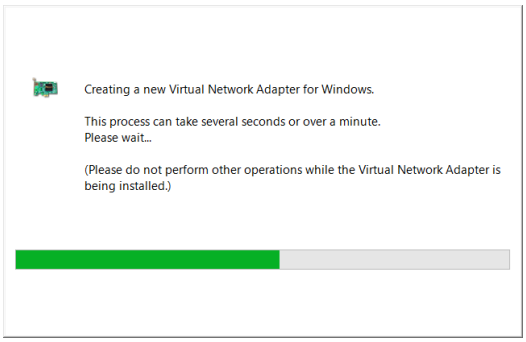
Menu Item	Details
Connect Menu	
Connect	Connects Selected Setting
View Status	View the Statis of the selected setting
Disconnect	Disconnect Selected Setting
Disconnect All	Disconnect all selected settings
Reset VEN Servers	Disconnect and Reconnect all connected Settings
New VEN Connection Settings	Create a New Setting Connection
Copy	Clone an Existing Setting
Create VEN Connection shortcut	Create a Shortcut for Selected Setting
Export VEN Connection Setting	Export Selected Setting
Import VEN Connection Setting	Import Selected Setting
Set as Startup Connection	Start Selected Setting in Kernel mode
Remove Startup Connection	Remove Kernel mode Startup for selected Setting
Rename	Rename selected Setting
Delete	Delete Selected Setting
Properties	Edit Selected Setting
Show Icons in Task Tray	Show Icon in Task Tray
Close Connection Manager	Close Connection Manager
Exit Connection Manager	Exit Connection Manager
Edit Menu	
Select All	Selects all Settings
Switch Selection	Switch Selected Setting with Unselected Settings
View Menu	
Show Status Bar	
Show Icon on Task Tray	Shows the current status on Connection Manager
Show Ports on Connection List	Displays the Icons on Task Tray
Show Windows 10 Stiles	Displays Windows 10 Look
Icon	Displays Manager View as Icons
Details	Displays Manager View as Details
Display Grid	Enables Grid View
Refresh	Refreshes View
Virtual Adaptors	
New Virtual Network Adaptor	Crates a New Virtual Network Adaptor
Enable Virtual Network Adaptor	Enables a Selected Disabled Network Adaptor
Disable Virtual Network Adaptor	Disables a Selected Enabled Network Adaptor
Delete Virtual Network Adaptor	Deletes a selected Virtual Network Adaptor
Reinstall Driver	Reinstall selected Virtual Network Adaptor Drivers
Open Windows Network Connections	Opens Windows Network Connections
USB Token	
USB Token Manager	Displays USB Token Manager
Select a USB Token to Use	Selects a USB Token for Use
Tools	
Set Password	Sets an Adman Password
Manage Trusted CA Certificates	Manage Trusted CA Certificates
Network Device Status	View Network Device Status
Optimize for Windows 10	Optimize TCP Buffers for Windows 10
Network Traffic Speed Test	Run Network Traffic Speed Test Tools
Switch Operation Mode	Switch to Simple Mode
Options	Displays Option
Help	
About	Info About iQuila Client Manager Version

Adding a New VEN Connection:

When adding a new VEN configuration, if you do not have a Virtual Network Adaptor installed, you will be asked to install one. A VEN Client connection requires a Virtual Network Adaptor to be able to connect.

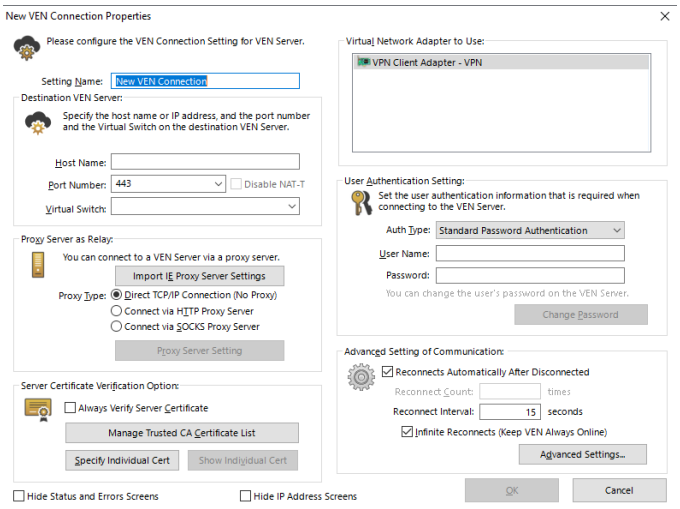


When adding a Virtual Network Adaptor, the iQuila VEN Kernel-mode Driver will also be installed. During install a window is displayed showing the progress of the Driver install.



Once the first Virtual Network Adaptor has been installed, you will be able to create your configuration. Click on **[Add VEN Connection]**. This will display the client configuration window.

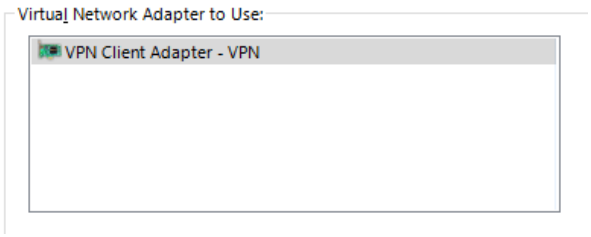
Enter the details required, please refer to the information set out in the table below.



Client Configuration Information	
Setting Name	This is the name displayed on the client for your reference
Host Name	Them the hostname or IP address of the iQuila Server you would like to connect to, if you are connecting to iQuila Cloud please enter the correct cloud address for the area you are connecting to, this address will be provided on the email sent when adding a Bridge device.
Port Number	Enter the port number you would like the connection to run on the default is 443
Virtual Switch	Enter the Name of the Virtual Switch you are connecting to

If you require a Proxy setting, please enter the correct configuration as listed below.

Proxy Server as Relay	
Import IE Proxy Settings	If you are using a Proxy Server, this button will allow you to import and Proxy setting listed in Internet Explorer or Edge for easy use.
Proxy Type	Select the Type of Proxy in use ❖ Direct TCP/IP Connection (no proxy) ❖ Connect via HTTP Proxy Server ❖ Connect via SCOKS Proxy
Proxy Server Settings	
Host Name	Host name of the Proxy Server
User Name	Proxy User name if required
Password	Proxy User password if required

Virtual Network Adaptors to Use	
Select the Virtual Network Adaptor to use for this connection, if you have multiple network adaptors created, they will be displayed in this box.	

User Authentication Settings	
Account Type	Select from the Option required ❖ Standard Password Authentication ❖ RADIUS or AD Authentication ❖ Client Certificates authentication ❖ USB Token Authentication
Standard Password Authentication	
User Name	Enter your user password or Cloud Device password
Password	Enter your user password or Cloud Device password
Change Password	The Change Password option only shows when Standard Password Authentication is selected, this gives the user the ability to reset their password.
RADIUS or AD Authentication	
User Name	Enter your RADIUS or AD user name
Password	Enter your RADIUS or AD Password
Client Certificates authentication	
User Name	Enter your Certificate account user name
Specify client certificate	Select your Client certificate
USB Token Authentication	
User Name	Enter your Account user name
Select USB Token	Select the USB Token with your certificate

Server Certificates Verification Options:

The Server Certificates Verification allows for an extra layer of Certificates Verification Security, to the iQuila Client / Server link. Totally stopping MTM (Man in The Middle attack), whilst giving a dual layer of security.

To use this section, you must first have installed a certificate in the certificate trusted CA certificates section, of the Virtual Switch, on the iQuila Enterprise Server.

The certificate trusted can be configured in two ways.

- **Install the Certificate in the iQuila Client:**

  This option allows you to install the Client certificate in the iQuila configuration.

  Select **[Specify individual Cert]**

  Select **[Load Certificate from File]** and click **[OK]**

  If you configured the certificate using a security phrase, you will be prompted for that phrase. Enter the phrase and click **[OK]**. The Certificate will then be installed.

  To View the Certificate, select **[Show Individual certificate]**

- **User a certificate on a USB Token:**

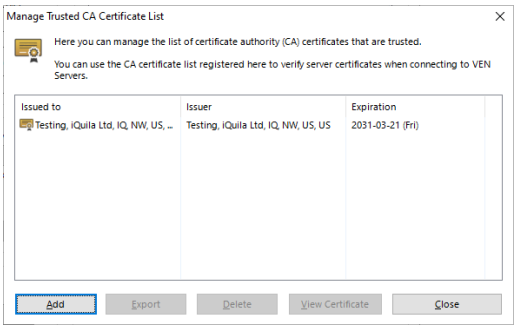
  Using Secure Tokens. This secures the connection and gives 2-factor Authentication to the iQuila client connecting to the iQuila Enterprise Server. Insert the USB Token with the pre-configured certificate into the client computer that is running the iQuila software client and select. **[Specify individual Cert]**

  Select **[Load Certificate from USB Token]** and click **[OK].**

  If you configured the certificate using a security pin, you will be prompted for that pin. Enter the pin and click **[OK].** The USB Token can now be used for Authentication.

  To View the Certificate, select **[Show Individual certificate].**

  If you have installed multiple different certificates, you can use the Manage Trusted CA certificate List to Manage these certificates. From this screen, you can select a certificate to use, export a certificate, delete a certificate or View a certificate.



For more information on certificates and USB Smart cards, please see the iQuila Enterprise Server Manuel v5.00.

Advanced Setting of Communications:

The Advanced Setting of Communications section allows you to configure the reconnection times, and intervals, between reconnection, attempts if a connection is lost to the iQuila Server or iQuila Cloud.

Reconnect Automatically after Disconnect	This option will set the connection to auto-reconnect if a connection is lost
Reconnect Count	The number of times the connection will attempt to reconnect (this option is not available if Infinite reconnects is set
Infinite reconnects (keep VEN always online)	This setting will attempt to reconnect the client until it reconnects.

Setting Account Status:

Account Status	
Hide Status and Error Screens	If this option is checked no error messages or status messages will be displayed to the user
Hide IP Address Status	If this option is checked the IP address assigned to the client will not be automatically displayed to the user on connection.

Advanced Settings:

The Advanced settings section is for the advanced configuration of the VEN Protocol. From this section, you can change the way the VEN Protocol connects and behaves.

Advanced Settings	
Number of TCP Connections	Changing this value sets the number of TCP connection the VEN protocol will use for the connection, for a full understanding of how the VEN protocol operates please see [Enterprise VEN Protocol with Embedded AI]
Establishing interval	Sets the Establishing interval in seconds.
Set Connection Lifetime of Each TCP Connection	Sets the time a TCP connection can stay active.
Use Half-Duplex Mode	Enables Half-Duplex mode (requires a minimum of 2 TCP Connection).
Disable VoIP / QoS	Disabled the Priority of VoIP Data
Encrypt VEN Session with SSL	This option is enabled as default and should only be disabled if Communications are made to localhost.
Use Data Compression	Enabled Data Compression on the connection.
Disable UDP Acceleration	For speed and performance, iQuila uses UDP Acceleration selecting this option will Disable UDP Acceleration.
Bridge / Router Mode	Enabling this option can enable the client to run in a Bridging / Routing mode (Bridging or Routing is required to be enabled on the user's account for this function).
Monitoring Mode	Enabled Monitoring Mode, used for Advanced Monitoring of a network, Monitoring is required to be enabled on the account for this function to work).
No Adjustments of the routing table	Enabled this option will restrict ant changes to the local routing table, this option is only available when Bridging is enabled on the account.

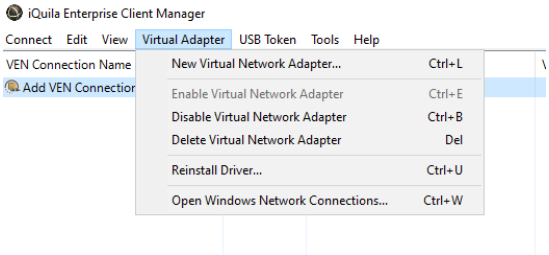
3. Managing Multiple Virtual Network Adaptors:

The iQuila Enterprise Client supports the use of multiple Virtual Network Adaptors. Each active iQuila Client connection requires a Virtual Network Adaptor. You can install up to 127 Virtual Network adaptors. Virtual Network adaptors can be installed via the iQuila Client Manager, or via the Command Line Utility. Virtual Network Adaptors are listed in the lower section of the iQuila Client Manager.

Virtual Network Adapter Name	Status	MAC Address	Version
VPN Client Adapter - VPN	Enabled	5E-65-E8-2B-D7-F8	4.25.0.9658

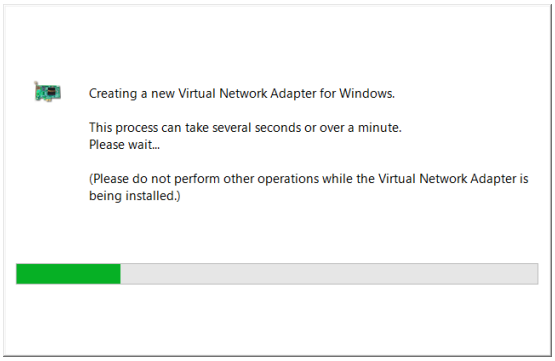
To Install a new Virtual Network Adaptor.

Select from the top Menu **[Virtual Adaptor]** and then **[New Virtual Network Adaptor]**.



The Create New Virtual Network Adaptor window will show. Enter a Name for the Virtual Network Adaptor. Enter the name as instructed and click **[OK]**. The install Driver wizard will be displayed as the driver is being installed.

Once the driver is installed it will appear in the lower section of the iQuila Client window.



To Delete a Virtual Network Adaptor. From the lower section of the main iQuila Client window, select the virtual network adaptor to be deleted, then from the main menu select **[Virtual Adaptor]**, then **[Delete Virtual Network Adaptor]**.

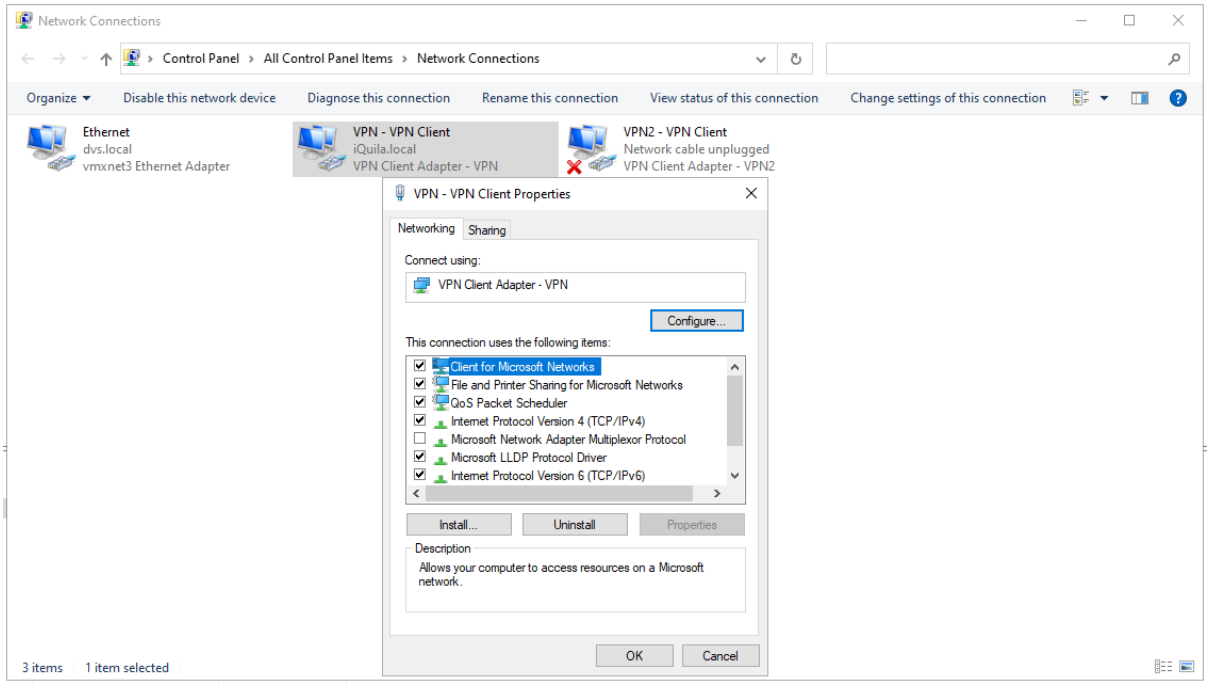
To Disable a Virtual Network Adaptor. From the lower section of the main iQuila Client window, select the virtual network adaptor to be disabled, then from the main menu select **[Virtual Adaptor]**, then **[Disable Virtual Network Adaptor]**.

To Enable a disabled Virtual Network Adaptor. From the lower section of the main iQuila Client window, select the virtual network adaptor to be enabled, then from the main menu select **[Virtual Adaptor]**, then **[Enable Virtual Network Adaptor]**.

If you are experiencing issues and need to reinstall the drivers for a selected Virtual Network Adaptor. Select the affected Virtual Network adaptor, from the lower section of the main iQuila Client window. Then from the main menu select **[Virtual Adaptor]**, then **[Reinstall Driver]**. A confirmation screen will be displayed click **[ok]** and the driver will be reinstalled.

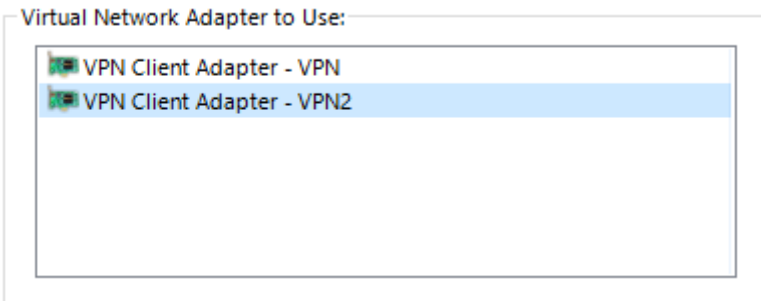
Virtual Network Adaptors in windows:

When a Virtual Network Adaptor is installed, it is also displayed in Windows Network Connections as a LAN Network Adaptor and carries all the same settings as a regular network adapter.



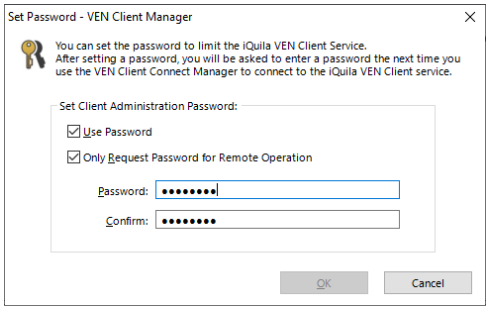
4. Configuring multiple connections:

The iQuila Enterprise Client can have multiple connections to different Servers, Switches, and Cloud Connections, all operating at the same time. Simply add multiple connections to the iQuila Manager. Only one connection can use a Virtual Network Adaptor at a time. If you require multiple concurrent connections to run at the same time, please configure multiple Virtual Network Adaptors. To set a specified Virtual Network Adaptor on the Client configuration window, under Virtual Network Adaptors. To use, select the required Virtual Network Adaptor.



6. Enabling remote Management of the iQuila Client:

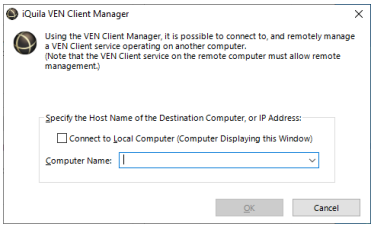
iQuila Enterprise Client support remote management. To enable remote management of the client, a remote access password must be configured. To set this password, select **[Tools]** from the main menu then **[Set Password].** Select the option **Use Password** and **Only require Password for remote Operation**. Checkboxes and click **[ok]**



Next, from the main menu select **[Tools],** then **[Options],** and select the option **Allow Remote Management of VEN Client Service** and click **[ok]**. The Remote management has now been enabled on the client.

To connect to a remote client, run the iQuila Remote Client Manager application, enter the Hostname or IP address of the remote client and select **[ok]** to connect.

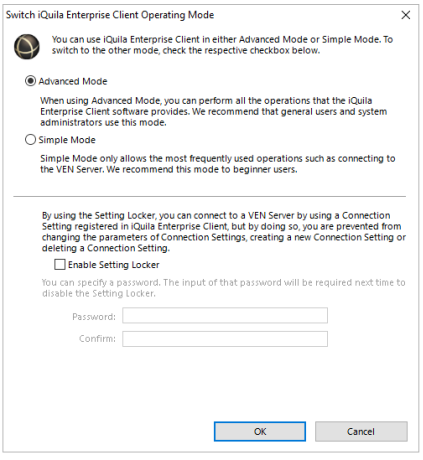
If the remote client is not on the same network as you, you can open port TCP 9930 on your firewall and create a NAT forward rule to gain access remotely to the client.



6. **Protecting configuration changes:**

iQuila supports a Password Protection function, to stop users from changing the settings or exporting the config files. To enable this function, from the main menu select **[Switch Operation Mode]**

Select **[Enable Setting Locker]** and enter a password, select **[OK]** to Save.



7. Advanced Mode and Simple Mode:

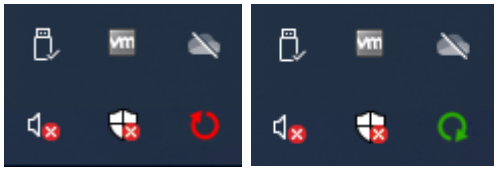
iQuila Enterprise client comes with two different views. Advanced Mode and Simple mode. The Advanced Mode gives you access to configure multiple clients but can be confusing to the standard user. Simple mode cuts down the functions available to the user and gives a simple look and feel to the application.

The mode can be set as default when building a custom install. Or switched from Advanced mode to Simple mode via the menu. Selecting **[Tools], [Switch Operation Mode],** select **[Simple mode]** and select **[ok].**

8. System Tray Menu:

iQuila Runs in the system tray. This can be enabled and disabled as suggested in section 2, from the Main Menu.

An iQuila status Icon is disapplied in the System tray, to indicate the connection status of iQuila.



System Tray Icon	
Non Rotating Red icon	Not connected
Fast Rotating Green icon	Attempting to Connect
Steady Rotating Green icon	Connected

When right-clicking on the Menu Icon the following menu Is displayed

iQuila Client System Tray Menu	
Close This Menu	Closes the System Tray Menu
Set VEN Connections	Display a Connection to connect to
Reset VEN Connection	Resets the select connection by disconnecting and reconnecting
Show Network Device Status	Displays the Status of Selected Network Adaptor
About VEN Client Manager	Displays Information about VEN Client Manager
Change Operation Mode	Change Operation Mode to Advanced
Show Icons on Task Tray	Removes the Icons and Menu from System Tray
Show / Close VEN Client Manager	Opens or closes the iQuila Client Manager
Exit VEN Client Manager Program	Closes the iQuila Client Manager and Tray Icon

When iQuila is installed, a Service is also installed in Windows Services.

6. Exporting and importing configurations:

The iQuila Client Manager allows you to Export and Import connection settings.

- **Exporting a Connection Setting:**
  To Export a connection Setting, select a previously created connection setting from the main client window. From the main menu, select **Connect** then **Export Connection Setting**, enter a name for the connection setting, and select a location, then click Save. You will be asked if you would like to remove Sensitive information from the connexion setting. Such as Username and Password. Select the desired option and the setting will be saved. (if saving Sensitive information with the connection setting, please keep this file secure).

- **Importing Connection Settings:**
  To Import a connection setting there are several ways.

  - From the Client Manager Menu, select **Connect**, then **[Import VEN connection Setting]**. The connection setting will be imported to the Client.

  - Double click on a previously exported connection setting file. You will be promoted, "would you like to import this VEN Connection file". Select **[yes]**. The connection file will be imported into the iQuila Client.

  - The iQuila Enterprise Client also support imputing setting via the Command Line Utility, please see section 14 iQuila Client Command Line Utility.

  - iQuila Enterprise Client has support for importing connection settings via network-scripts.

    These commands will create a Virtual Network Adaptor and import the connection file from a network location.

```
" C:\Program Files\iQuila Enterprise Client\vencmd_x64.exe" localhost /client /cmd:NicCreate VPN

" C:\Program Files\iQuila Enterprise Client\vencmd_x64.exe" localhost /client /cmd:AccountImport \\localhost\Users\admin\Documents\Company.vpn
```

10. Understanding the configuration file:

The iQuila Enterprise client runs using a configuring file called ***vpn.client.config*** The config file holds the configuration for the Client section of the iQuila Client application. Within this, the client setting for each connection configured is held.

Client Config:

Below is an empty client config without any connection settings inserted. You can manually edit the config file. To edit the config file, you will need to copy the file first to a different location, then edit the file before copying it back. You will also need to stop the iQuila Client Service from running in [Windows Services]. When building an install, using Easy Install, the contents of this config file will be used.

```
declare root
{
	bool DontSavePassword false
	byte EncryptedPassword +WzqGYrR3VYXrAhKPZLGEHcIwO8=
	bool PasswordRemoteOnly false
	string UserAgent Mozilla/5.0$20(Windows$20NT$206.3;$20WOW64;$20rv:29.0)$20Gecko/20100101$20Firefox/29.0
	uint UseSecureDeviceId 0

	declare AccountDatabase
	{
	}
	declare ClientManagerSetting
	{
		bool EasyMode false
		bool LockMode false
	}
	declare CommonProxySetting
	{
		string ProxyHostName $
		uint ProxyPort 0
		uint ProxyType 0
		string ProxyUsername $
	}
	declare Config
	{
		bool AllowRemoteConfig false
		uint64 AutoDeleteCheckDiskFreeSpaceMin 8589934592
		string KeepConnectHost keepalive.iquila.net
		uint KeepConnectInterval 50
		uint KeepConnectPort 80
		uint KeepConnectProtocol 1
		bool NoChangeWcmNetworkSettingOnWindows8 false
		bool UseKeepConnect false
	}
	declare RootCA
	{
	}
}
```

Config File explained	Value	Info
bool DontSavePassword	True / false	Sets if a User can Save Password
byte EncryptedPassword	Data	Encrypted Client software password
bool PasswordRemoteOnly	True / false	Enable to Disable Remote access to Client config
bool EasyMode	True / false	Sets client to boot on Simple or Normal mode
bool LockMode	True / false	Sets lock mode on client
string ProxyHostName	Data	Proxy Hostname
uint ProxyPort	Data	Proxy Port Number
uint ProxyType	Data	Proxy Type
string ProxyUsername	Data	Proxy User Name
bool AllowRemoteConfig	True / false	Enable to Disable remote access to client config
AutoDeleteCheckDiskFreeSpaceMin	Data	Define the amount of free space before logs over right
string KeepConnectHost	IP/ Hostname	IP Address or Hostname for Keepalive setting
uint KeepConnectInterval	Data	Keep alive Connect Interval in seconds
uint KeepConnectPort	Data	Keep alive connect Port
uint KeepConnectProtocol	Data	Keep alive Protocol type
bool NoChangeWcmNetworkSettingOnWindows8 false	0 TCP / 1 UDB	
bool UseKeepConnect	True / false	Enable or disable the Keepalive setting

Once an account to a remote server had been added to the client, it is automatically added to the running-config and inserted under-declare account followed by an automatically generated number to keep track of multiple accounts.

```
declare AccountDatabase
        {
                declare Account0
                {
                        bool CheckServerCert false
                        uint64 CreateDateTime 1616547781774
                        uint64 LastConnectDateTime 0
                        string ShortcutKey 38492E79E8E69FB052363D0EBB0E9FBC87331DD5
                        bool StartupAccount true
                        uint64 UpdateDateTime 1616547781774

                        declare ClientAuth
                        {
                                uint AuthType 1
                                byte HashedPassword AAAAAAAAAAAAAAAAAAAAAAAAAAA=
                                string Username $
                        }
                        declare ClientOption
                        {
                                string AccountName iQuila
                                uint AdditionalConnectionInterval 1
                                uint ConnectionDisconnectSpan 0
                                string DeviceName VPN
                                bool DisableQoS false
                                bool HalfConnection false
                                bool HideNicInfoWindow true
                                bool HideStatusWindow true
                                string Hostname iQuila$20Cluster$20server$20address
                                string HubName Switch$20Name
                                uint MaxConnection 1
                                bool NoRoutingTracking false
                                bool NoTls1 false
                                bool NoUdpAcceleration false
                                uint NumRetry 4294967295
                                uint Port 443
                                uint PortUDP 0
                                string ProxyName $
                                byte ProxyPassword $
                                uint ProxyPort 0
                                uint ProxyType 0
                                string ProxyUsername $
                                bool RequireBridgeRoutingMode false
                                bool RequireMonitorMode false
                                uint RetryInterval 15
                                bool UseCompress false
                                bool UseEncrypt true
                        }
                }
        }
```

Client Account config	Value	Info
declare Account0	Data	Auto-generated a number for each account added
bool CheckServerCert	True/ false	Enable to Disable Server Certificate checking
uint64 LastConnectDateTime	Value	
bool StartupAccount	True / false	Enable account to start with Kernel boot
uint64 UpdateDateTime	Data	The time and date account was last modified
uint AuthType 1	Value	Sets the Authentication type 0 = Anonymous 1=Password 2= RADIUS 3=CERT 4=USB token
byte HashedPassword	Date	Encrypted Users Password
string Username $	Data	User Name for server Account
string AccountName	Date	Account Display Name
string DeviceName	Value	Specifies the Virtual Adaptor Name to use for the connection
bool DisableQoS	True/ false	Enabled or disables QoS support
bool HalfConnection false	True / false	Enables or disables the half-duplex mode
bool HideNicInfoWindow true	True / false	Enables or disables Notifications to the client
bool HideStatusWindow true	True / false	Enables or disables Notifications to the client
string Hostname	Data	Hostname or IP address or the server connection to
string HubName	Data	Virtual Switch Name
bool NoRoutingTracking false	True / false	Enables or disables
bool NoTls1 false	True / false	Enables or disables Encryption
bool NoUdpAcceleration false	True / false	Enables or disables UDP Acceleration
uint NumRetry	Data	Sets the number of retries
uint Port 443	Data	Sets the port number to connect on
string ProxyName $	Data	Sets the Proxy Name
byte ProxyPassword $	Data	Sets the Proxy Password for the connection
uint ProxyPort 0	Data	Sets the Proxy Port for the connection
uint ProxyType 0	Data	Sets the Proxy Type of the connection
string ProxyUsername $	Data	Sets the Proxy user name of the connection

bool RequireBridgeRoutingMode false	True / false	Enables or disables
bool RequireMonitorMode false	True / false	Enables or disables
uint RetryInterval 15	Data	Sets the Retry Interval in seconds
bool UseCompress false	True / false	Enables or disables encryption on the connection
bool UseEncrypt true	True / false	Enables or disables encryption on the connection

10. Building a Custom Install with Easy Installer:

iQuila Enterprise has a built-in function, that allows a user to build a custom install, using your own configuration file. To access the Easy Installer Creator. Launch the application **[iQuila Enterprise Easy Install]** from the program's menu. (please note, you must have iQuila Admin Tools Installed. These can be downloaded from the iQuila Website).

Once you lunch the iQuila Easy Installer, the Easy Install wizard will start,

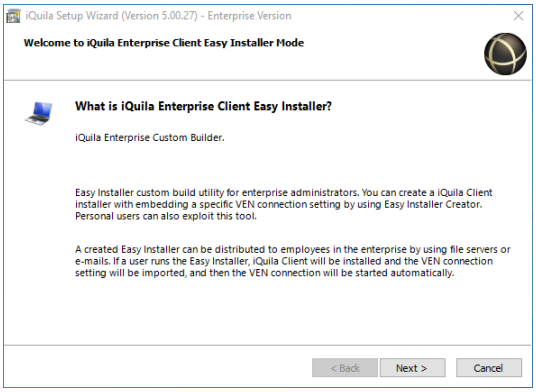
Select a previously created configuration setting that you would like built into the install.

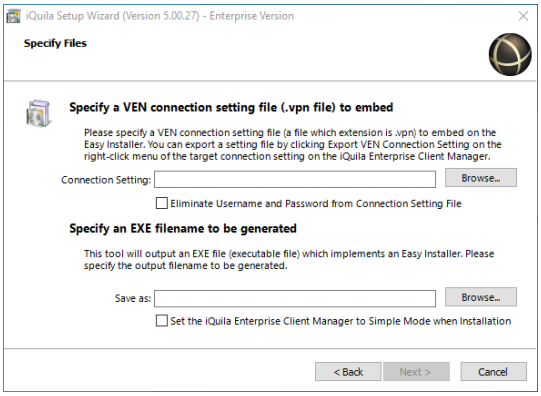
Select a Destination location and enter a file name you would like to call the execution (.exe) install file.

There is two other option you may like to set:

- **Set Client to Simple Mode:**
  This setting automatically sets the client to Simple mode on install.
- **Remove User Details:**
  This setting will remove any saved Credentials.

  Select **[Next]** and the easy install will create your custom install ready for distribution to your client.





12. MSI Silent Installs:

iQuila offers 4 silent install files that can be deployed over a network allowing you to automatically import connection settings as explained in section 9.

- ***iQuilaEnterpriseClient_Slient_Full.msi***
- ***iQuilaEnterpriseClient_Slient_Full.exe***

  This Install of iQuila enterprise will deploy in Simple mode with no connection settings, Connection setting import is required.

- ***iQuilaEnterpriseClient_Slient_NoIcons.msi***
- ***iQuilaEnterpriseClient_Slient_NoIcons.exe***

  This install of iQuila Enterprise will deploy in Simple mode, with no connection settings, and no icon shortcuts. Connection setting import is required.

  These files are available via the iQuila Website.

Connection setting can be imported into the application, please see section 9.

13. Managing Split Tunnelling:

The iQuila Client supports several ways of managing split tunneling.

- **Advanced Split Tunnelling per application.**

  If you are running iQuila Enterprise Server or your corporate DHCP server support RFC 3442, then routes can be pushed out over the network to the iQuila client. iQuila client v4.35 and above support static route, using the RFC 3442 Standard.

  In most cases, basic Split Tunnelling is sufficient and can be achieved in several ways.

- **Split Tunnelling with DHCP Gateway:**

  By Issuing a DHCP address to the iQuila client without a Gateway defined the iQuila client will automatically route all traffic locally and all traffic for the IP Address defined over the VEN link to the company network.

- **Split Tunnelling with Metrics:**

By changing the metric to a higher value on the Virtual Network adaptor, will route all internet traffic locally and all corporate traffic over the VEN link to the corporate network. For full details on changing Metrics, please refer to “Guide for Setting Gateway Metric” on our documentation website.

At https://iquila.com/Support/Documentation/

Metrics can be managed and changed via PowerShell using the following commands.

```
get-NetIPInterface -AddressFamily IPv4

These list the metric for individual NICs
Get-NetIPInterface -AddressFamily IPv4 -InterfaceAlias Ethernet
Get-NetIPInterface -AddressFamily IPv4 -InterfaceAlias "VPN - VPN Client"
Get-NetIPInterface -AddressFamily IPv4 -InterfaceAlias "VPN2 - VPN Client"
Get-NetIPInterface -AddressFamily IPv4 -InterfaceAlias "VPN3 - VPN Client"
Get-NetIPInterface -AddressFamily IPv4 -InterfaceAlias "VPN4 - VPN Client"


These changes the metric for individual NICs

Set-NetIPInterface -AddressFamily IPv4 -InterfaceAlias Ethernet -InterfaceMetric 10
Set-NetIPInterface -AddressFamily IPv4 -InterfaceAlias "VPN - VPN Client" -InterfaceMetric 20
Set-NetIPInterface -AddressFamily IPv4 -InterfaceAlias "VPN2 - VPN Client" -InterfaceMetric 30
Set-NetIPInterface -AddressFamily IPv4 -InterfaceAlias "VPN3 - VPN Client" -InterfaceMetric 50
Set-NetIPInterface -AddressFamily IPv4 -InterfaceAlias "VPN4 - VPN Client" -InterfaceMetric 50
```

15. iQuila Enterprise client comes with a full command-line interface, all aspects of the application can be configured via the command-line interface, please see the iQuila Client command Line Interface Document for full details.