

iQuila Deployment Guide for

iQuila Enterprise Server and Bridge

iQ22055r3

This Document Applies to:

iQuila Enterprise

www.iQuila.com

iQuila Enterprise Server / 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 are able to 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.

🥡 iQuila Enterprise Server Configuration Wizard	
we using this wizard, you can easily configure the iQuila Enterprise Server for your requirements.	
lect the type of VEN server you would like to build.	
Quila Server Default Configuration.	
Quila Enterprise Server Accepts, iQuila Clients, Mobile Devices and Bridge Connections.	
fermion de	
Quila Server Site to Site Configuration.	
iQuila Enterprise Server Creates Layer 2 connections between sites.	
Please select the Role of the Server :	
 IQuila Server Accepts inbound Bridge connections (Center) 	
 IQuila Server Makes outbound Bridge Connections (Edge) 	
Advanced Conferentian of Ordin Enterplan Ferrary	
Diago calest this antion if you are placed to build a Chila Saterorise Course that supports during	
rease select this option in you are planning to ound a IQUIII Enterprise Server that supports clustering.	
ck Next to start Setup. Click Close if you want to exit the setup and manually configure all settings.	

You must create one Virtual Switch on the iQuila Enterprise Server

<u>O</u>K

as a minimum. Please choose your Virtual Switch Name.

Setup Wizard - Please choose your Virtual Switch Name

Virtual Switch Name: Default

👼 iQuila Entermira Seniar Configurat

ď

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.



 \times

Cancel

User types are defined by Security Permissions

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 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 authentication in this scenario. We will use Individual certificate authentication.

	Dident		Security Policy		
-	Name: brigger			Set Security Policy	Security Policy
Eul	Name: New York		.050.		
	Note:		Security Policy		
<u>A</u> uth Typ	e: OAnonymous Authentica R Password Authenticati	ation	4 •	roup Name (Optional):	Browse Groups
	Individual Certificate A	Authentication (Contraction)			
	RADIUS Authentication	a	Individual Cert	tificate Authentication Settings:	
	♥ NT Domain Authentical	stion		The users using 'Individual Certificate allowed or denied connection depend certificate completely matches the certificate completely matches the certificat	Authentication' will be ding on whether the SSL clie tificate that has been set fo
Password Authentica	tion Settings:			the user beforehand.	
R	Eassword:				
50	nfirm Password:		Specify Ce	ertificate View Certificate	Create Certificate
RADIUS or NT Doma	ain Authentication Settings:		Signed Certific	ate Authentication Settings:	
	Set the Expiration Date for Tr	This Account	20	Verification of whether the client cert	ificate is signed is based o
And D	6/01/2021	000000	8.8.		
				Limit Common Name (CN) Valu	e
RADIUS or NT Doma	in Authentication Settings:	ed by the external			
RADIUS or NT Doma RADIUS or NT Doma RADIUS serv RADIUS serv	in Authentication Settings: sts by password will be verifie er, Windows NT domain conte	ed by the external roller, or Active Directory		Limit Values of the Certificate S	arial Number
RADIUS or NT Doma RADIUS or NT Doma RADIUS serve controller.	in Authentication Settings sts by password will be verifie tr, Windows NT domain contr Name on Authentication Serve	ed by the external roller, or Active Directory		Limit Values of the Certificate S	erial Number
RADIUS or NT Doma RADIUS or NT Doma RADIUS serve controller. Specity User User Name on Aut	in Authentication Settings: sts by passwood will be verifie rr, Windows NT domain contr Name on Authentication Serve verification Server:	ed by the esternal roller, or Active Directory er		Limit Values of the Certificate S	erial Number
RADIUS or NT Doma RADIUS or NT Doma RADIUS serve controller. Specity User User Name on Auth	in Authentication Settings: pts by password will be wriffie rr, Vilindows NT domain conte Name on Authentication Serve werdication Servers	ed by the external solier, or Active Directory er		Umit Values of the Certificate S	erial Number lues. (Example: 015SABCD8

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.*

Create New Certificate		Х
You can easily cre	eate certificates which is signed by self or other certificates.	
Certificate Type:	<u>R</u> oot Certificate (Self-Signed Certificate)	
	Certificate Signed by Other Certificate	
<u>Certificate</u> and Private Key for Signing:	Load Certificate and Private Key	
	Click 'Load Certificate and Private Key' to specify the XSD9 Certificate and RSA Private Key that will user a new certificate signature.	
		_
Common Name (CN):	Bridge1	
Organization (O):	Compasny Name	
Organization Unit (OU):		
Country (C):	kG	
State (ST):	New York	
Locale (L):	US	
Serial Number: (Hexadecimal)		
<u>E</u> xpires in:	3650 Days Strengthness: 4096 V bits	
To manage certif software such as	icates and certificate authorities on a large scale, you should use either OpenSSL or commercial CA (certificate authority) software.	free
	QK Cancel	

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.

Save Certificate	e and Private Key	×
Select the me	thod to save the certificate and private key.	
Sa <u>v</u> e Metho	d:	
⊖ Save as	<u>X</u> 509 Certificate (.CER) and Private Key File (.KEY) Saving by splitting into two files: a standard Base 64-encoded certificate file and a private key file.	
Save as	PKCA#12 File (P12)	
Ra	Saving as a PKCS#12 (Public Key Cryptography Standard #12) file. You can store both certificate and private key in a single PKCS#12 file.	
O Write to	5 Smart Card	
e	When a smart card is connected to this computer, you can write the certificate and private key to a smart card.	
	Select Which Smart Card to Use	
	Select which smart card device to use.	
Private Key F	Protection	
R w	hen saving the private key, you can set a passphrase to encrypt. You will be quired to enter the passphrase when loading it.	
	Set Passphrase	
	Pagsphrase:	
	Confirm:	
R wr	hen saving the private key, you can set a passphrase to encrypt. You will be quired to enter the passphrase when loading it. Set Passphrase: Passphrase: Confirm: QK Cancel	

Once you have finished adding users click Exit

This will return you back to the easy setup wizard.

Under Step3 *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*.



tep 1. (Create a User to Accept VEN Connection
	When this iQuila Enterprise Server accepts a remote access VEN, or becomes the central site-to iQuila Enterprise server that accepts connections from other sites, create users to accept the VE connection.
	Create Users
tep 2. I	Define a Connection to Destination VEN Server
۰ <u>ر</u>	When this iQuila Enterprise Server is installed on a particular site (edge) of a site-to-site VEN have to specify the address of the center VEN Server that accepts the connections, and estab a connection to that central VEN Server.
	<u>C</u> onfigure Connection Setting
tep 3. !	Set Local Bridge
)	For an site-to-site VEN, use the Local Bridge Function to connect a bridge between the virtual Ethernet segment on the VEN side and the physical Ethernet segment on the local side. Select existing Ethernet device (Network Adapter) that will be provide the bridge connection to the V

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.*

Instr	uctions for Local Bridge on VM
	Using Local Bridge Function on VM
lt has b or Hype messag	een detected that the VEN Server might be running on a VM (Virtual Machine) suchlike VMware r-V. Read the following instructions carefully. If you are not using a VM, please ignore this le.
Instru	ctions
Som	e VMs prohibit the "Promiscuous Mode" (MAC Address Spoofing) on the network adapters by
defa	ult.
If the funct phys Spoo	Promiscuous Mode (MAC Address Spoofing) is administratively disabled, the Local Bridge ion between a Virtual Switch on the VEN Server and a physical network adapter on the ical computer does not work well. You should allow the Promiscuous Mode (MAC Address fing) by using the configuration tool of the VM.
For o	letails please refer the documents of your VM. If it is a shared-VM and administrated by other on, please request the administrator to permit the use of the Promiscuous (MAC Address sting) Mode to your VM.

anage VEN Server	"localhost"			Li	icensed t	o: iQuila	Ltd Den	no Licen	se	25 days re	emaining		
Switch / Hub Settings	Virtual Switch Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables	Num Logins	Last Login	Last Communication	Transfer Bytes	Transfer Packets
Manage Virtual Switch	Default	Online	Standalone	1	0	1	0	0	0	2021-01-05 14:56:53	3 2021-01-05 14:56:53	0	0
0.1													
Online													
Offline													
View <u>S</u> tatus													
Create a Virtual Switch													
Propgrties													
Delete													
and Routing													
Local <u>B</u> ridge Setting													
Layer <u>3</u> Switch Setting													
IPsec / L2TP Setting													
OpenVPN / MS-SSTP													
And Free allow													
Encryption and Network													
	VEN Server Int	ormation				Manag	gement of Lister	ners:			iQuila Artificial Intelligence		
stering	¢⊅ ¢⊅		⊻iew Server Sta	tus							(v	EN AI Setting	
Clustering Configuration			Table Country			0	igeate P	ort Number In TCP 443	Status Listening				
Clustering Status	iQ:		Egit Config				vere <u>t</u> e d	TCP 992	Listening Listening				
			About this VEN S	erver			Start	TCP 5555	Listening				

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

lanagement of	Listeners:	
C <u>r</u> eate	Port Number	Status
	🖷 TCP 443	Listening
Dele <u>t</u> e	🛋 TCP 992	Listening
	🛋 TCP 1194	Listening
Start	1 TCP 5555	Listening
Sto <u>p</u>		

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.

Ruila Enterprise Server Configuration Wizard	
🔃 iQuila Enterprise Server Configuration Wizard	
by using this wizard, you can easily configure the iQuila Enterprise Server for your requirements.	
elect the type of VEN server you would like to build.	
Quila Server Default Configuration.	
Quila Enterprise Server Accepts, iQuila Clients, Mobile Devices and Bridge Connections. (default).	
Quila Server Site to Site Configuration.	
IQuila Enterprise Server Creates Layer 2 connections between sites.	
Please select the Role of the Server :	
IQuila Server Accepts inbound Bridge connections (Center)	
VEN Bridge at Each Site	
Advanced Configuration of iQuila Enterprise Server	
Please select this option if you are planning to build a iQuila Enterprise Server that supports dustering.	
Click Next to start Setup. Click Close if you want to exit the setup and manually configure all settings.	Close
Bext >	Glose

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

ate a User to Accept VEN Connection
When this iQuila Enterprise Server accepts a remote access VEN, or becomes the central ite-to-like iQuila Enterprise server that accepts connections from other sites, create users to coept the VEN connection.
Create <u>U</u> sers
Configure Connection Setting
Local Bridge
themet segment on the VEN side and the physical Ethernet segment on the local side. Select an xisting Ethernet device (Network Adapter) that will be provide the bridge connection to the VEN

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 addres*s 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

Cascade Connecti	ons on BRIDGE	hernet-level links hetween this Virtu	al Switch and other Virtual Sw	itch which is located or
either local o	remote VEN Server.			
Gase Case Incomplea	Cascade Connection ade Connection creates a Lay rectly configured, an infinity l se design the network topolo	ver 2 Bridge between multiple Virtua loop could inadvertently be created. gg with care.	I Switches. But if the connectic When using a Cascade Conne	n is ction function
ting Name	Status	Established at	Destination VEN Server	Virtual Switch
Head Office	Connecting	(None)	10.10.10.1	

On Step3 of the wizard *select the drop down* and *select the network adaptor* you would like to bridge and *select close*.

🐢 '	o complete the setup of this iQuila Server / iQuila Bridge, you must complete the following tasks
tep 1. C	reate a User to Accept VEN Connection
2	When this IQuila Enterprise Server accepts a remote access VEN, or becomes the central site-to-site IQuila Enterprise server that accepts connections from other sites, create users to accept the VEN connection.
	Create <u>U</u> sers
itep 2. D	Define a Connection to Destination VEN Server When this (Quila Enterprise Server is installed on a particular site (edge) of a site-to-gite VEN y I have to specify the address of the center VEN Server that accepts the connections, and establis connection to that central VEN Server.
itep 2. D	Vefine a Connection to Destination VEN Server When this Quila Enterprise Server is installed on a particular site (edge) of a site-to-site VEN y have to specify the address of the center VEN Server that accepts the connections, and establis connection to that central VEN Server. Qonfigure Connection Setting
tep 3. S	efine a Connection to Destination VEN Server When this (Quila Enterprise Server is installed on a particular site (edge) of a site-to-site VEN y have to append; the address of the center VEN Server that accepts the connections, and establis connection to that central VEN Server Configure Connection Setting et Local Bridge For an site-to-site VEN use the Local Bridge Function to connect a bridge between the virtual
tep 2. D	When this Quila Enterprise Server is installed on a particular site (edge) of a site-to-site VEN y have to specify the address of the center VEN Server that accepts the connections, and establis connection to that central VEN Server. Qonfigure Connection Setting et Local Bridge For an iste-to-site VEN use the local Bridge Function to connect a bridge between the virtual Ethemed segment on the VEN side and the physical Ethernet segment on the local side.



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

Manage VEN Bridge "localhost"				Licensed to:						-1 days remaining					
er2 Sut	tch / Hub Settings	Virtual Switch Name	Status	her	Users	Groups	Septem	MAC lables	Pictos	New Logins	Last been	Last Communication	hansler Byles	Translat Pash	
×.	Manage Virtual Switch	Station .	Diffice	Standalone	0	0	1	99	\$1	0	2021-01-05 1606-00	2021-01-05 163253	20,459,015	107,687	
8	Quine														
2	Office														
	Wew Status														
-	Create a Virtual Switch														
1	Propplace														
ç.	Delete														
	Layer give following Theory Latter Setting Deenvery MS-SSTP														
tvork Ar	ad Encryption														
វៃត្	Encryption and Network														
		VEN Server Information					- Management of Listeners					- Kai la Artificial Intelligence			
EN Clustering		<i>:</i> *	View Server Status				Create Port Number Status				1		EN AI Setting		
-	Castering Configuration	۲		Eait Cardig			D	elete	TCP 5555	listening					
÷	Clustering Status						3	lart							