SAPPHIRE™

Sapphire Connect

Initial Client Setup

Document Version : 1.0

Document Information

Document Title :	**Connect Customer Documentation 2.8**
Creation Date :	19/04/21

Document History

Version	Date	Description
1.0	9/4/2020	Initial Version
2.0	23/7/2020	Update documentation for ‘Connect’ branding
2.1	27/7/2020	Add Azure installation note
2.2	14/8/2020	Add AWS installation notes
2.3	14/12/2020	Add overview, troubleshooting and minor corrections.
2.4	11/01/2021	Fix typing error in the OpenVPN port number
2.5	5/2/2021	Add detail introduction and Installation clarifications.
2.6	19/04/21	Now available in Azure Marketplace
2.7	02/07/21	Change of gateway IP address
2.8	11/07/24	Add Azure serial console information

Glossary of Terms

Term	Description
OpenVPN	A standard VPN protocol, used by the Sapphire Connect system.
AWS	Amazon Web Services – Amazon’s cloud computing service
Azure	Microsoft’s cloud computing service

Table of Contents

1 Introduction

1.1 Rationale

Due to the global outbreak of the COVID-19 virus, to ensure the safety and health of Sapphire and customer staff, it is now important to be able to carry out testing operations without having to travel to a customer's site.

Such a system will require the following characteristics :-

- Provide service delivery across the Internet operated by a tester working from home.
- Require no physical interaction between the customer and Sapphire staff.
- Testing speed should be as independent on the tester's home Internet speed as possible (the average domestic Internet connection has an upload rate of 7.2Mbps [1])
- Be able to access the customer's internal networks and network segments directly in a similar manner to a traditional test.
- Where there is network segregation as per a traditional test, where access is granted and moved, the new solution would require this also.
- Protect the customer's network from unauthorised access from the Sapphire infrastructure.
- Protect the customer's network from unauthorised access from the Internet.
- Protect the Sapphire infrastructure from unauthorised access from the customer's infrastructure.
- Be easy to use for both the customer and the tester.

1.2 Outline

Testing activity will be carried out via a Virtual Machine (The Connect VM) that will be installed within the customer's infrastructure. The VM is based on the 'Kali' Linux operating system. Kali is a distribution specifically tailored for performing security testing and therefore has a suite of specialist testing tools and applications installed. This VM should be seen as an equivalent of the tester's laptop in a traditional on-site test.

A private, virtualised network has been created with a connection to the Internet with a VPN gateway (the Connect VPN Gateway).

The Sapphire testing team already have access to a virtualised environment known as 'VET'. Access to VET is via a strongly authenticated secure 'client to site' VPN link establishing a connection directly from the tester's assigned Sapphire laptop. Both the Connect network and the VET environment reside in a data-centre within the UK.

During set-up, a copy of the Connect VM will be delivered to the customer along with a configuration package containing a set of authentication keys unique to the customer and the secure shell 'public key' authentication details belonging to the tester(s) assigned to the customer. The customer can upload this package to the Connect VM via a simple web user interface. The Connect VM will then connect to the Connect VPN using the customer-specific authentication keys.

The secure shell (ssh) service on the Connect VM will be made accessible to the tester via their connection to VET. Each tester has a unique public/private authentication key-pair for secure shell. Therefore only the tester(s) assigned to the customer will be able to gain access to the Connect VM. Once connected, testing can be carried out from the Connect VM in a similar manner to how testing is carried out from a tester's laptop in a traditional internal test.

[1] https://www.ispreview.co.uk/index.php/2019/05/ofcom-2019-report-avg-home-broadband-isp-speeds-hit-54mbps.html

1.3 Inherent Security Segregation

This architecture does not require the customer to permit access to any services from the Internet, and no services or systems on the customer network will be directly reachable from an untrusted network. Only the Connect VM will be reachable from a tightly controlled subset of the Sapphire infrastructure.

Other than a single ‘outbound’ firewall rule to permit the Connect VM to connect to the Connect VPN, there should need be no changes to the customer’s security infrastructure to permit operation.

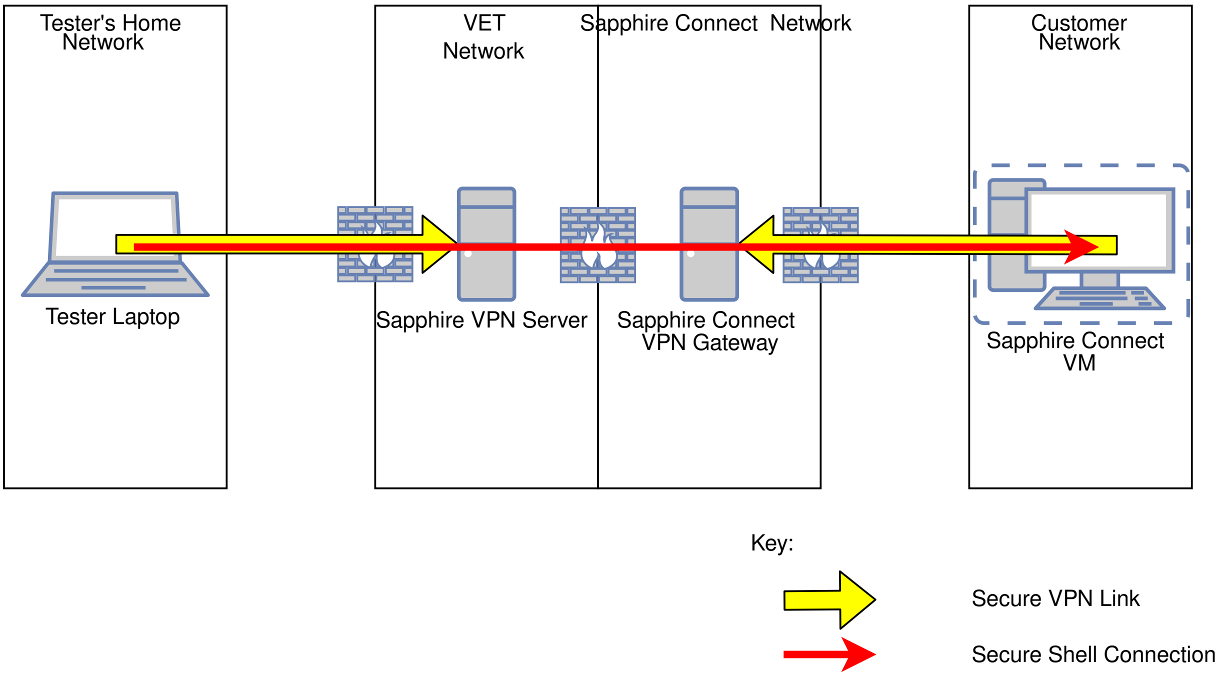
The customer’s network will not be ‘aware’ of any aspect of the Sapphire infrastructure (other than the Connect VM).

Due to segregation between VET and the Connect network, the Connect VM is only ‘aware’ of the Connect VPN gateway. The Connect VPN tunnel is created as a ‘link-local’ only network. No IP routes are created on the VM.

Other than the Connect VM, no Sapphire infrastructure is aware of any internal customer architecture. The Connect VPN system will be aware of the ‘external’ Internet IP address of the customer. Source and Destination NAT and firewall rules exist on the VPN server to permit a tester’s access to the secure shell service on the Connect VM without needing to route IP addresses related to the ‘link-local’ or customer networks.

This design permits reliable operation even if a portion of the customer’s network or test targets has IP address ranges that match or overlap with the address ranges used within the Sapphire infrastructure.

1.4 High Level Connectivity Diagram



2 Installation

2.1 Overview

Sapphire Connect operates as a virtual machine (VM) running on many common virtualised environments (see section 2.2 for more details).

Each VM requires approximately 70GB of disk space, a minimum of 2 virtual CPUs and a minimum of 8 GB RAM. We recommend to allocate 4vCPUs and 16GB RAM if available.

You may need to modify firewall rules on your network. The system needs the following traffic flows permitted :

Source	Destination	Protocol	Reason
Your Workstation	VM	TCP / 5477	To access the web based configuration interface.
VM	Sapphire Connect Gateway (195.97.212.62)	UDP / 1194	Sapphire Connect VPN Connectivity.

There are no firewall rules to be configured on the VM itself.

2.2 Virtual Machine

The virtual machine is packaged in various formats to suit differing virtualisation environments. Currently, three variants exist.

URL	Supported Hypervisors
https://connect.sapphire.net/vmware-image	VMWare and Virtualbox
https://connect.sapphire.net/hyperv-image	Hyper-V
Azure Marketplace. Search for “Sapphire Connect”	Azure
Community AMI search for “sapphire connect”	AWS

You should import the VM into the hypervisor in accordance with the standard instructions for that hypervisor.

As these images are large (approximately 6GB to download and take more space when uncompressed – approximately 20GB for the Hyper-V image and 65GB for the Azure image), it is recommended that the images are downloaded directly to a network connected to the target environment via a fast link. If you are working remotely it will likely be faster to log in to a system on your internal network and download the files to there.

Advice on installing to the Azure cloud environment can be found in section 3 of this document.

Advice on installing to the Amazon AWS cloud environment can be found in section 4 of this document.

2.3 Networking

The VM should be placed so that it’s network interface can access the systems to be tested.

2.3.1 VmWare and VirtualBox

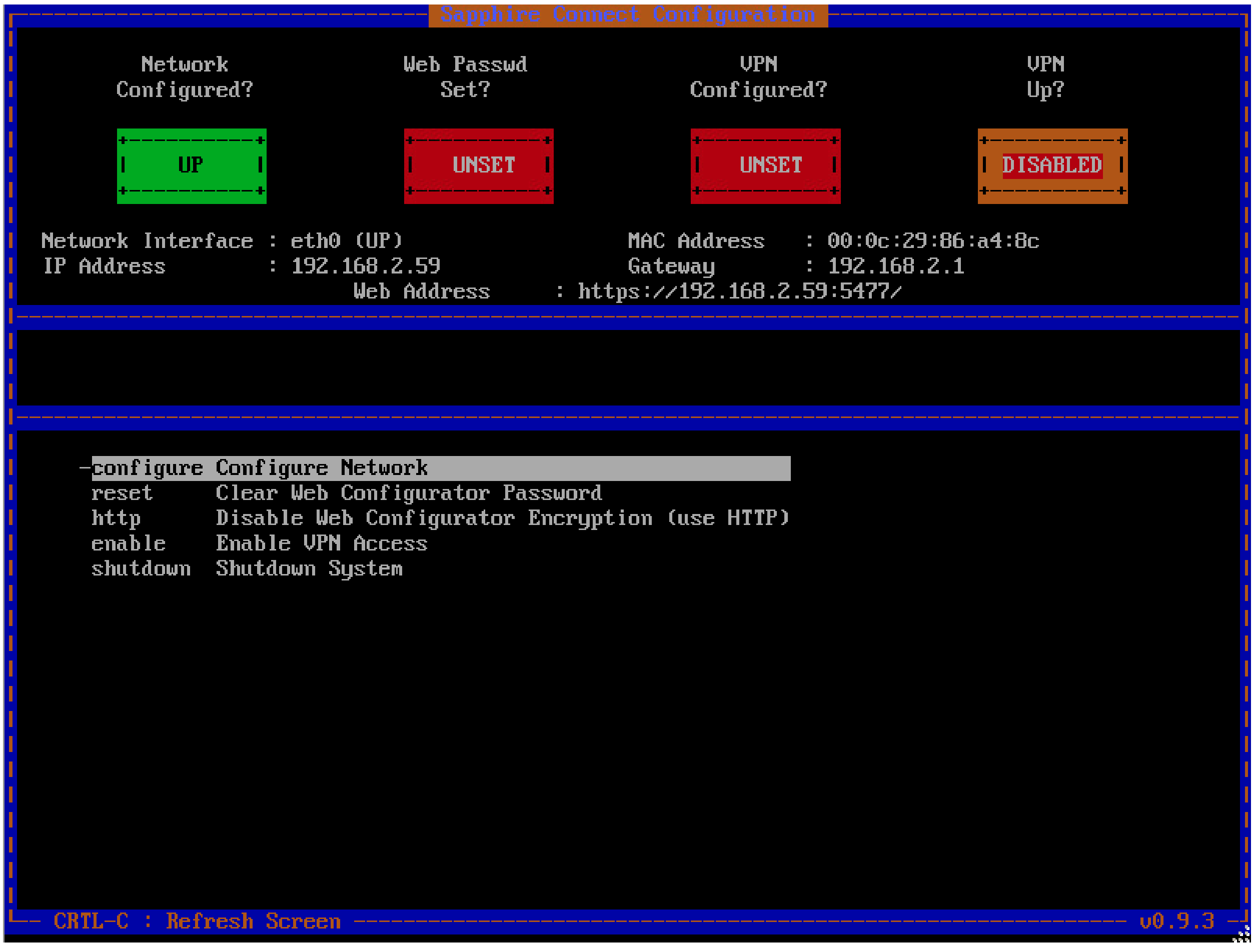
The VM for VmWare and Virtual box has a virtual network adapter already defined. It should be modified so that it is connected to a suitable network.

2.3.2 Hyper-V

The Hyper-V VM will attempt to connect to a virtual switch called ‘LAN’. If such a switch does not exist, the import procedure will prompt to ask what switch to connect to. The virtual switch connection can be changed after import.

2.4 Initial Setup

Once booted, the VM console should appear similar to the following

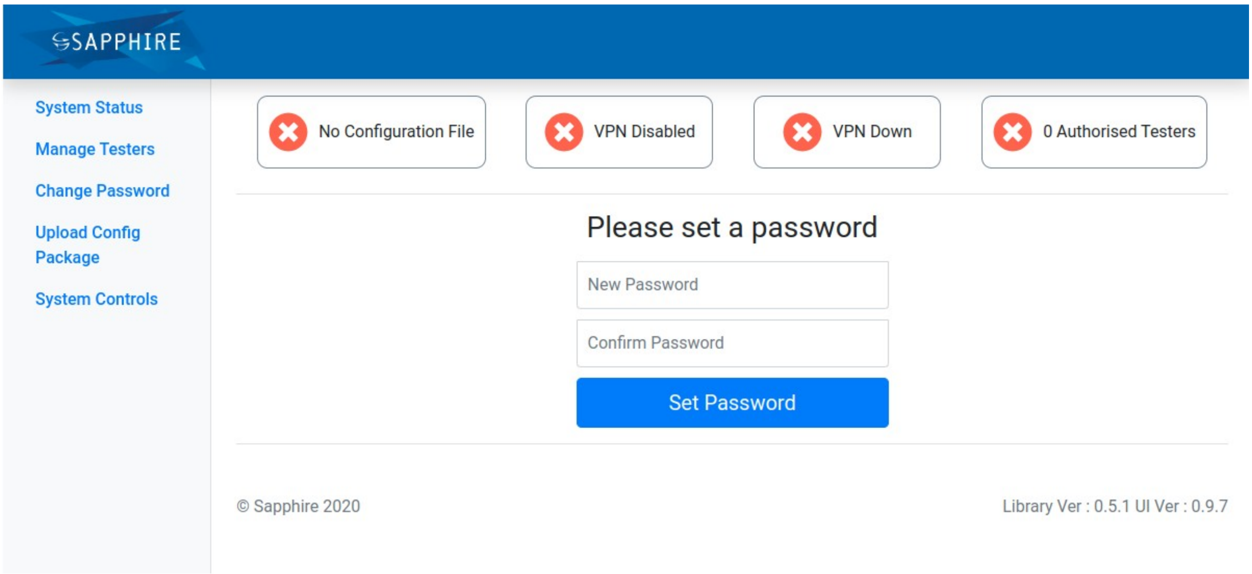


```
                              Sapphire Connect Configuration

      Network              Web Passwd              VPN                  VPN
    Configured?               Set?              Configured?              Up?

        UP                   UNSET                UNSET               DISABLED

 Network Interface : eth0 (UP)                    MAC Address    : 00:0c:29:86:a4:8c
 IP Address        : 192.168.2.59                 Gateway        : 192.168.2.1
                          Web Address      : https://192.168.2.59:5477/



     -configure Configure Network
      reset     Clear Web Configurator Password
      http      Disable Web Configurator Encryption (use HTTP)
      enable    Enable VPN Access
      shutdown  Shutdown System

 CRTL-C : Refresh Screen                                                          v0.9.3
```

2.5 *Web Interface*

If it has managed to configure itself an IP, it will bring up a web interface. This is an HTTPS service on port 5477. Connect to this web interface using a web browser from your computer.

The web interface is password protected to prevent unauthorised users from changing settings. The first time you access the web interface it will prompt you to set a password.

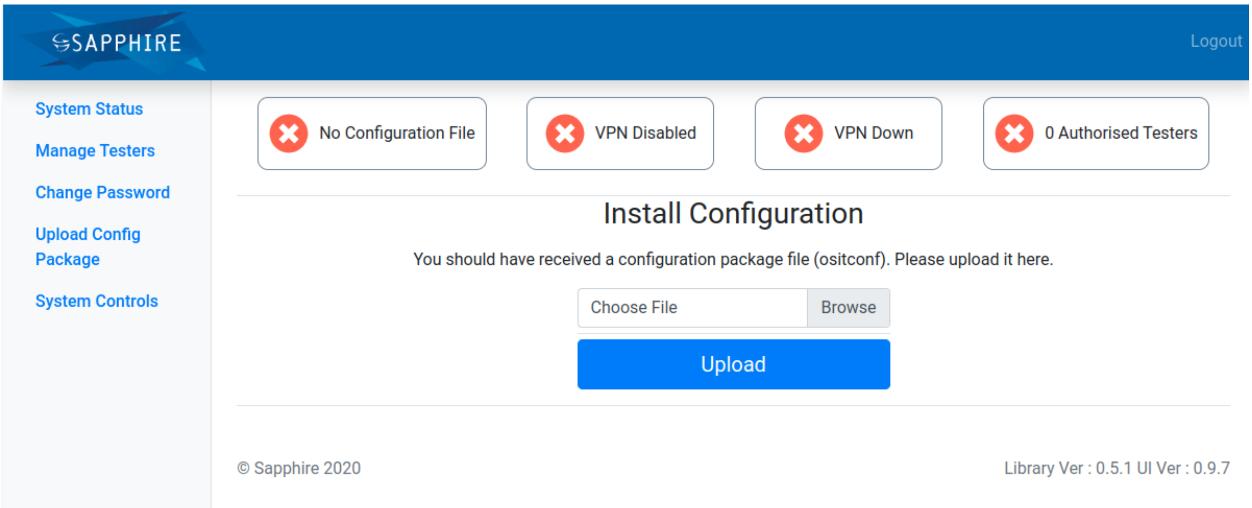


The password is needed if you wish to access the web interface in future to change the configuration package, permitted testers or to shutdown the VM.

The password for the web interface should be kept secret and does not need to be shared with the tester or any other Sapphire personnel.

2.5.1 Configuration Package

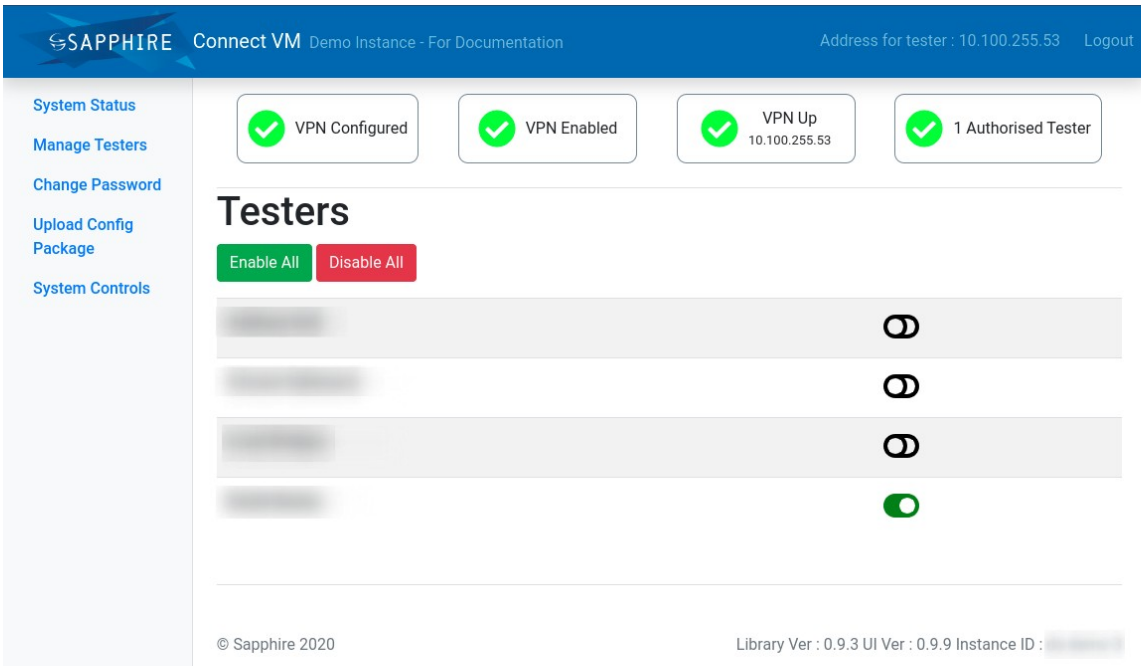
You will have been provided with a configuration file (ositconf). The next screen prompts you to upload it.



You should have received a configuration package file (ositconf). Please upload it here.

2.5.2 VPN Connection

After upload, the Connect VM will automatically attempt to make an outbound connection to the Connect VPN server and will prompt you to authorise the tester(s) to connect.



If the VPN does not connect after a few seconds, ensure that firewall rules permit the VM to connect to 195.97.212.62 on UDP port 1194 (OpenVPN)

2.5.3 Enabling Testers

Once connected, select to enable the tester(s) access.

At this point, the tester will be able to access the system and begin a test of your network.

2.6 Internal Firewalls

To facilitate infrastructure testing, it is important that any internal firewalls or network security groups are configured to allow the VM's internal IP address to access all services on all target hosts.

If the test is of a particular service or web application, please ensure that firewalls permit access to the services to be tested.

2.7 Complex Environments

Larger environments or networks spanning multiple sites or security boundaries may make testing from a single network location infeasible. In such cases, it is possible to assign extra network interfaces to the Connect VM or it may be best to perform testing from multiple, separate VMS. Such situations are easily accommodated. The choice between using multiple interfaces or multiple VMS will be affected by the network topology and your security requirements. Please inform Sapphire of any such complications so we can advise and adjust appropriately.

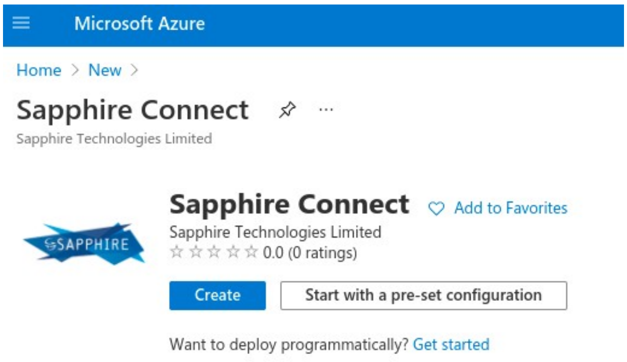
If you are using multiple Connect VMs, we will provide a different configuration file for each VM. The same file cannot be used to activate multiple Connect VMs simultaneously. Attempting to do so will result in unreliable communications for those VMs.

3 Azure Installation

The Connect VM is available within the Azure Marketplace.

3.1 Create an Instance

In the Azure Portal, select 'Create a Resource' then search for 'Sapphire Connect' in the search box.



Microsoft Azure

Home > New >

Sapphire Connect

Sapphire Technologies Limited

Sapphire Connect ♡ Add to Favorites

Sapphire Technologies Limited

☆☆☆☆☆ 0.0 (0 ratings)

Create | Start with a pre-set configuration

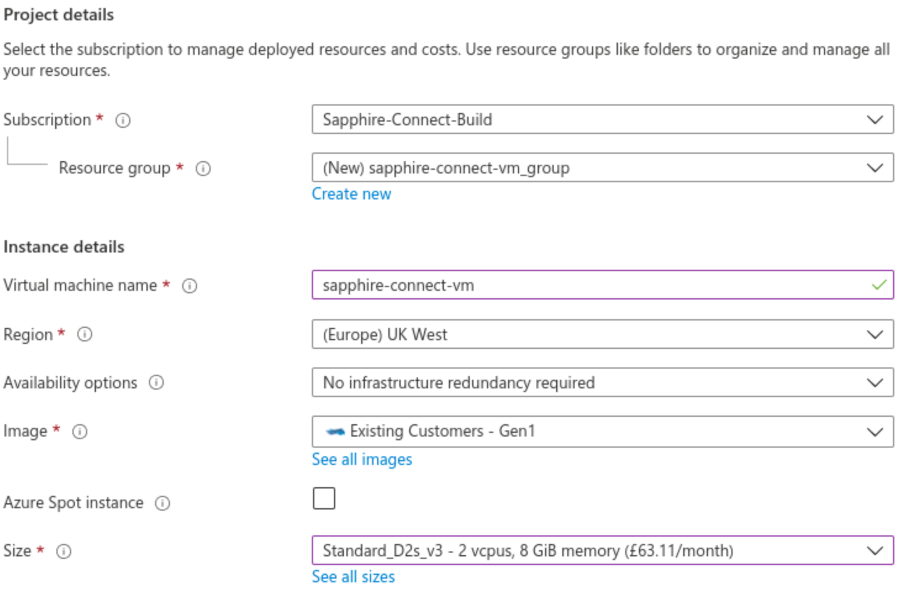
Want to deploy programmatically? Get started

Select 'Create' to start the process to create a new VM.

3.1.1 Basic Settings

Set the resource group, name and region as suitable for your Azure tenancy. The VM does not require any infrastructure redundancy . The Image type should remain as 'Existing Customers – Gen 1'

The default VM size is 'Standard_D2s_v3'. This has 2 vcpus and 8GB RAM. This will suffice for many tests, but large or complex networks may require more resources - the tester will inform you if a larger VM is required. You should not use a spot instance for this VM.



Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Sapphire-Connect-Build

Resource group * : (New) sapphire-connect-vm_group

Create new

Instance details

Virtual machine name * : sapphire-connect-vm ✓

Region * : (Europe) UK West

Availability options : No infrastructure redundancy required

Image * : Existing Customers - Gen1

See all images

Azure Spot instance : □

Size * : Standard_D2s_v3 - 2 vcpus, 8 GiB memory (£63.11/month)

See all sizes

You can leave the 'Administrator Account' section at the default values, this is not currently used by the Sapphire Connect VM.

3.1.2 Disks

The VM does not require a separate data disk to be created, the default settings will work without modification. This will result in a 64GB OS disk being created for the VM.

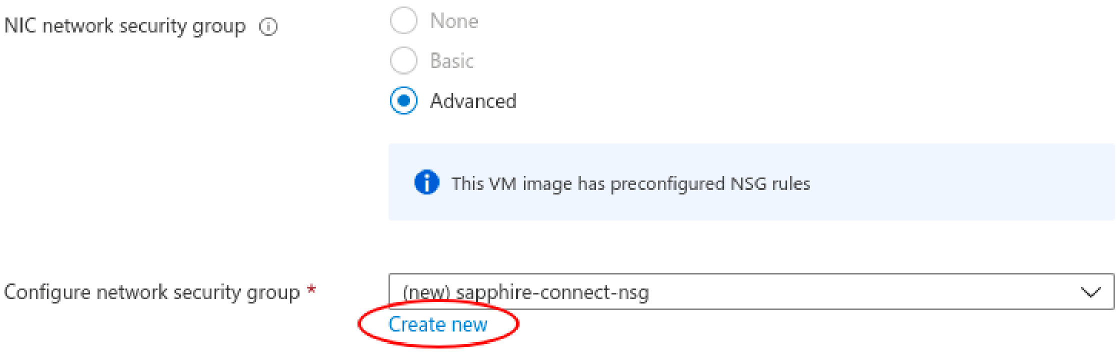
3.1.3 Networking

Place the VM into a suitable network and subnet to be able to access the target systems.

The VM will need to be able to communicate to the Connect VPN gateway server and you will need to be able to access the web interface on the VM. If your Azure network infrastructure will facilitate this without allocating a 'Public IP' address then one should not be assigned.

You need to configure a Security Group that will allow you to connect to the VM on port 5477/tcp (Custom TCP Service). This service will let you manage the Connect VM and does not affect the tester's ability to use the system. The security group should be configured so that this service is only accessible from trusted IP addresses. If the VM has a public IP address, the default network security group (nsg) settings will expose the Sapphire Connect Web UI to the Internet. We recommend that the nsg is modified to permit access only from trusted locations.

Select 'Create new' under the Configure network security group drop-down..



NIC network security group ⓘ

○ None

○ Basic

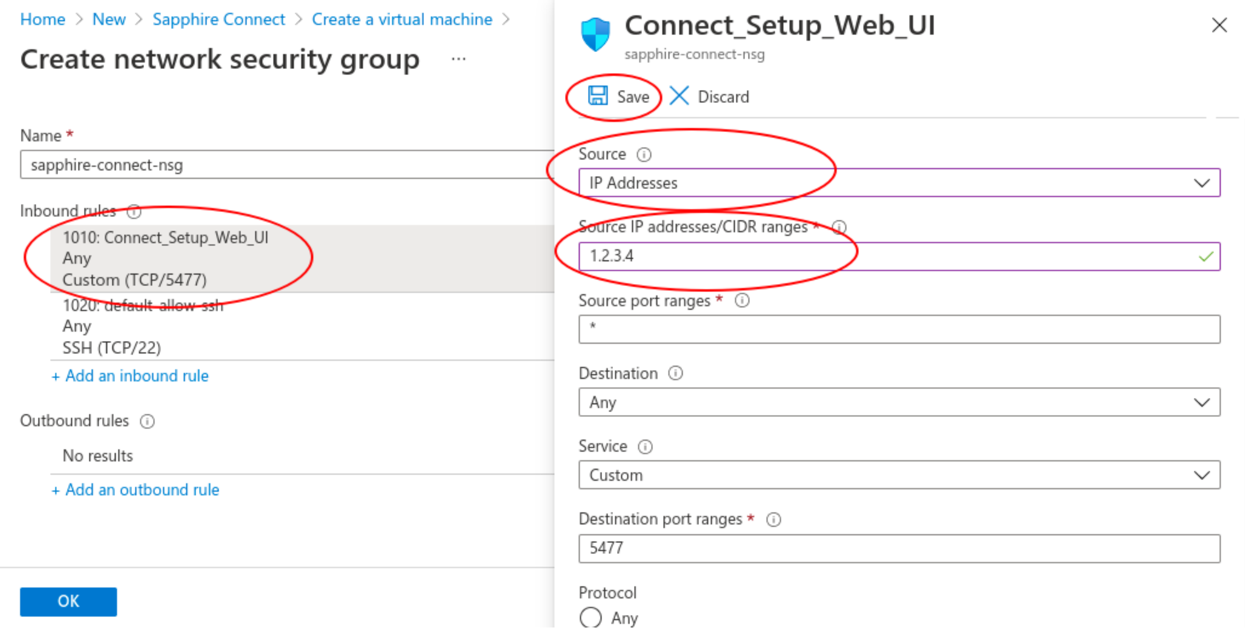
● Advanced

This VM image has preconfigured NSG rules

Configure network security group *: (new) sapphire-connect-nsg

Create new

Click on the 'Connect_Setup_Web_UI' rule and set the source type to 'IP Address' and set the source address range to your trusted network, then save the rule. Sometimes Azure will require you to modify the 'Priority' of the rule in order to save it. This can be set yo any value.



Home > New > Sapphire Connect > Create a virtual machine >

Create network security group ...

Name *: sapphire-connect-nsg

Inbound rules ⓘ

1010: Connect_Setup_Web_UI
Any
Custom (TCP/5477)

1020: default-allow-ssh
Any
SSH (TCP/22)

+ Add an inbound rule

Outbound rules ⓘ

No results

+ Add an outbound rule

OK

Connect_Setup_Web_UI
sapphire-connect-nsg

Save Discard

Source ⓘ: IP Addresses

Source IP addresses/CIDR ranges * ⓘ: 1.2.3.4

Source port ranges * ⓘ: *

Destination ⓘ: Any

Service ⓘ: Custom

Destination port ranges * ⓘ: 5477

Protocol
○ Any

3.1.4 Management

Boot diagnostics should be enabled for the VM. This will allow access to the system console if needed. No other management options are used.

3.1.5 Advanced

No options on the 'Advanced' pane are required to be set.

3.1.6 Tags

Sapphire Connect does not require any specific tags. You should set any tags as appropriate for your organisation.

3.1.7 Review + Create

The 'Review + Create' pane will perform some basic validation of your configuration and display the pricing for the VM. There is no charge for the Sapphire Connect VM software though the cost of the Azure instance will be charged by Microsoft.

Review the configuration and click 'Create' to create the VM. You may be prompted to create and download a ssh key. This is fine to do though the generated key is not used.

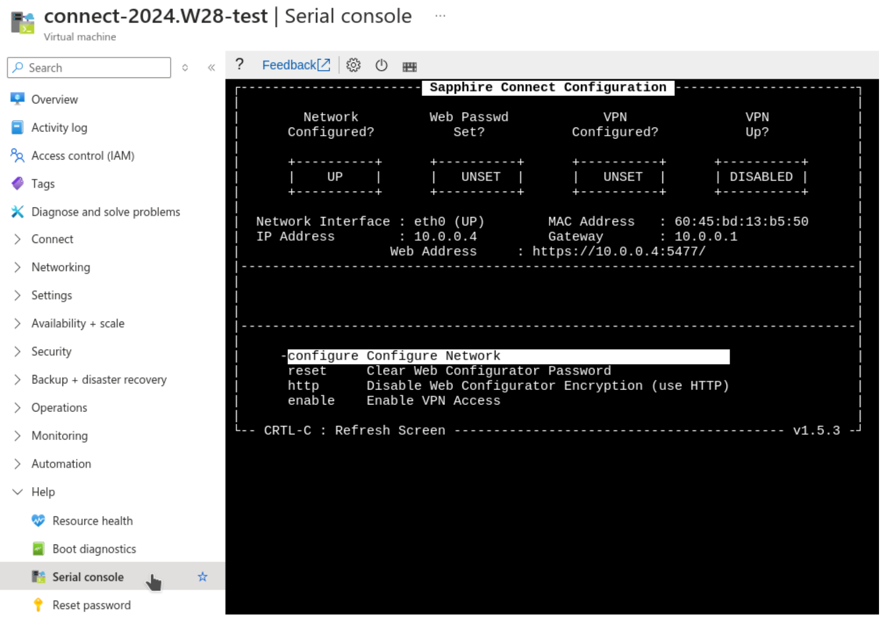
3.2 Launch

After a couple of minutes, you should receive confirmation that the deployment is complete, the HTTPS web interface will be accessible on TCP port 5477. If this is inaccessible, please review your network settings and security groups.

Continue to set up the system as described in section 2.5.

3.3 Console Access

The console interface is accessible via the Azure 'Serial Console'. This can be reached via the 'Help' section then viewing the virtual machine in the Azure portal.



```
┌---------------------- Sapphire Connect Configuration -----------------------┐
|                                                                               |
|      Network         Web Passwd          VPN               VPN              |
|    Configured?          Set?          Configured?           Up?             |
|                                                                               |
|    +----------+     +----------+     +----------+     +----------+          |
|    |    UP    |     |   UNSET  |     |   UNSET  |     | DISABLED |          |
|    +----------+     +----------+     +----------+     +----------+          |
|                                                                               |
|  Network Interface : eth0 (UP)         MAC Address    : 60:45:bd:13:b5:50    |
|  IP Address        : 10.0.0.4          Gateway        : 10.0.0.1             |
|                  Web Address     : https://10.0.0.4:5477/                     |
|-------------------------------------------------------------------------------|
|                                                                               |
|                                                                               |
|                                                                               |
|-------------------------------------------------------------------------------|
|                                                                               |
|      -configure Configure Network                                            |
|       reset     Clear Web Configurator Password                               |
|       http      Disable Web Configurator Encryption (use HTTP)                |
|       enable    Enable VPN Access                                             |
|                                                                               |
└-- CRTL-C : Refresh Screen ------------------------------------------- v1.5.3 -┘
```

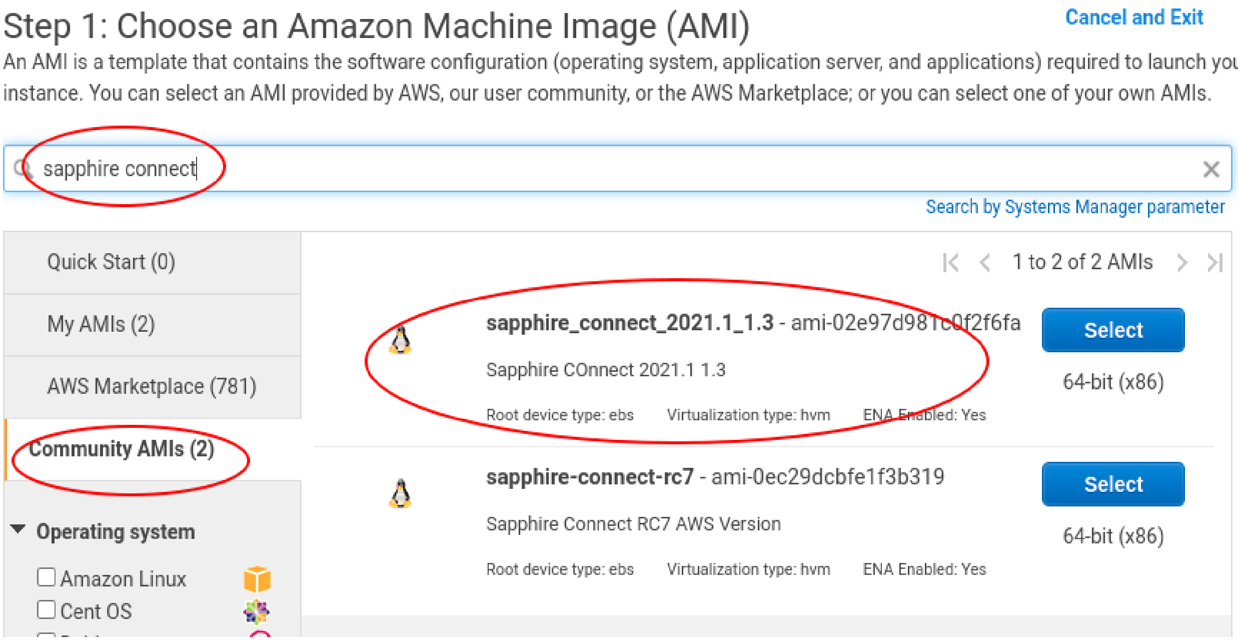
4 AWS Installation

The Connect VM for AWS is provided as a 'Community AMI' within the AWS system.

It is currently only available within the 'eu-west-2' (London) region. It can be made available in other regions, please contact Sapphire if your network(s) exist in other regions so a copy can be provisioned for you.

4.1 *Create an Instance*

In the AWS console, start to create a VM instance as usual. One of the first screens will prompt you to select an instance image. Ordinarily, you would select an image from the AWS Marketplace or an existing image in your tenancy. In this case, select 'Community AMIs' in the left-hand menu and search for 'sapphire connect'. You should see a result similar to the following.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch you instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

sapphire connect

1 to 2 of 2 AMIs

sapphire_connect_2021.1_1.3 - ami-02e97d981c0f2f6fa
Sapphire COnnect 2021.1 1.3
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit (x86)

sapphire-connect-rc7 - ami-0ec29dcbfe1f3b319
Sapphire Connect RC7 AWS Version
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit (x86)

Click the 'Select' button to install the latest available version of the Sapphire Connect AMI.

4.1.1 Instance Type

The software used to perform most testing will require at least two virtual CPUs and 8GB RAM. As such, we would recommend selecting the 't3.large' instance type. This should suffice for most tests.

Large or more complex target systems may require more resources on the Connect VM. Your tester will let you know if the test would benefit from more RAM or CPU cores.

When selected, click on 'Next: Configure Instance Details'

4.1.2 Instance Details

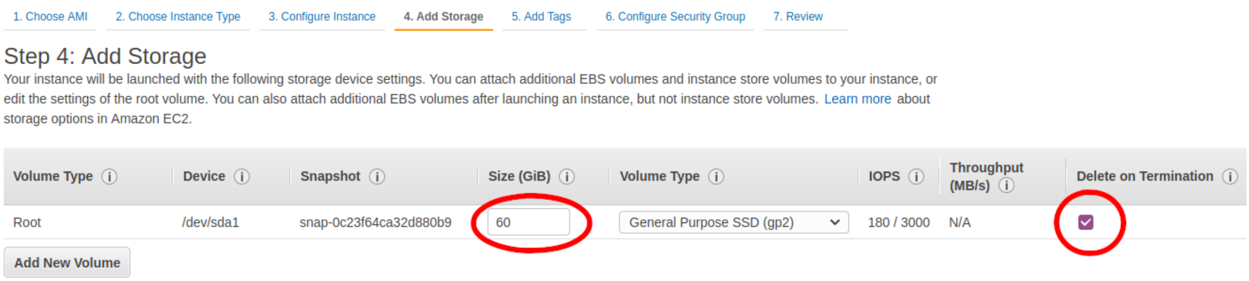
Place the VM into a suitable network and subnet to be able to access the target systems.

The VM will need to be able to communicate to the Connect VPN gateway server and you will need to be able to access the web interface on the VM. If your AWS network infrastructure will facilitate this without allocating a 'Public IP' address then one should not be assigned.

Select 'Next: Add Storage'

4.1.3 Storage

The image disk size covers the bare minimum for the operating system. We will need more space for this for the usage of testing tools and accumulation of test data. 60 GB of space should be adequate for most tests (this can be expanded later if more space is required), you should also select for the storage volume to be automatically deleted when the VM is terminated, as shown in the image below.



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination
Root	/dev/sda1	snap-0c23f64ca32d880b9	60	General Purpose SSD (gp2)	180 / 3000	N/A	☑

Then click 'Next : Add Tags'

4.1.4 Tags

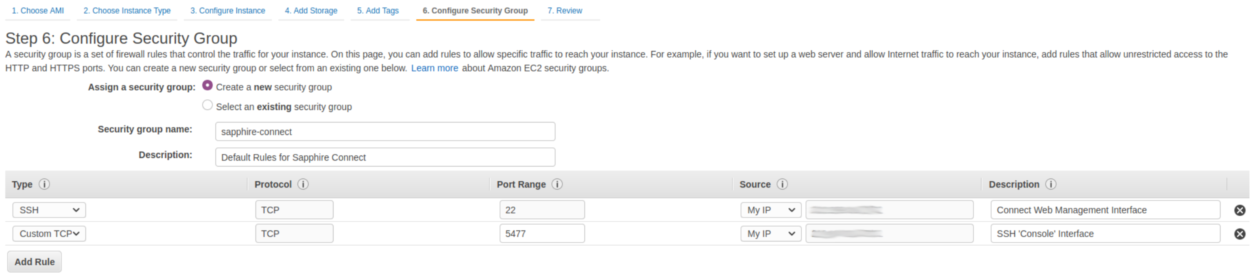
Sapphire Connect does not require any specific tags. You should set any tags as appropriate for your organisation.

Click 'Next : Configure Security Group'

4.1.5 Security Group

You need to configure a Security Group that will allow you to connect to the VM on port 5477/tcp (Custom TCP Service) and port 22/tcp (SSH). These services will let you manage the Connect VM and do not affect the tester's ability to use the system. The security group should be configured so that these services are only accessible from trusted IP addresses.

The following shows the most basic example for a simple installation where the Connect VM has been allocated a public IP address. It is unlikely that this will be suitable for more complex AWS environments.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: sapphire-connect

Description: Default Rules for Sapphire Connect

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	My IP [redacted]	Connect Web Management Interface
Custom TCP	TCP	5477	My IP [redacted]	SSH 'Console' Interface

Click to 'Review and Launch' the VM

4.1.6 Authentication Keypair

You will be prompted to select or generate an authentication keypair for the VM.

This keypair will allow you to use secure shell to gain access to the 'console' interface (shown in section 2.4). This will usually only be needed if you forget the web interface password and want to reconfigure the system.

4.2 Launch

Once the instance is launched, the HTTPS web interface will be accessible on TCP port 5477. If this is inaccessible, please review your network settings and security groups.

Continue to set up the system as described in section 2.5.

4.3 Console Access

Should you need to access the console interface, use a secure shell client to authenticate with the username ‘connect’ and the keypair you generated in the final step of creating the instance.

5 Troubleshooting

5.1 Web Browser Encryption

If when connecting to port 5477 on the VM, your web browser returns an error indicating that it cannot negotiate an encrypted connection, it may be that your browser cannot support TLS v1.2.

Try using a different browser. All modern, current browsers should be able to connect (though it may be possible that support for TLS v1.2 has been disabled by an administrative setting such as ‘Group Policy’)

If changing the browser is not possible then HTTPS can be disabled by accessing the VM console (or secure shell in AWS) and selecting the ‘http’ menu option. Note that this will result in the password and security keys being transmitted without encryption. This should only be enabled on a secure, trusted network.

SAPPHIRE™

The information in this document is subject to change without notice and must not be construed, as a commitment on the part of Sapphire Technologies Ltd. Sapphire Technologies assumes no responsibility for any errors that may appear in this document.