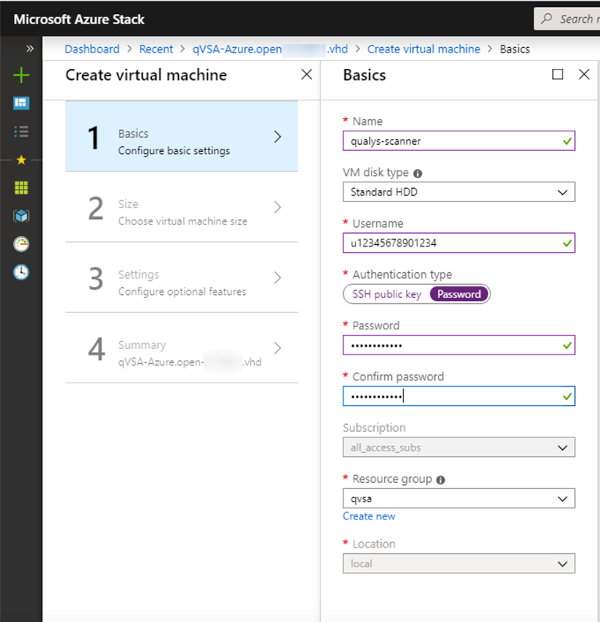
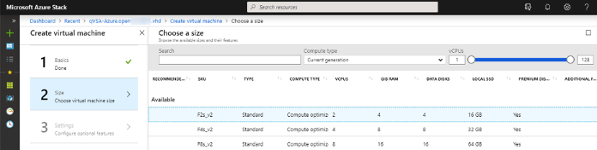
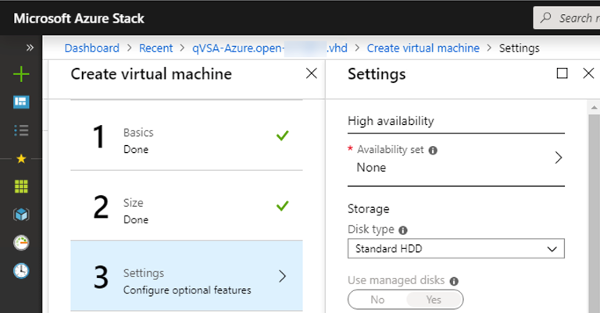
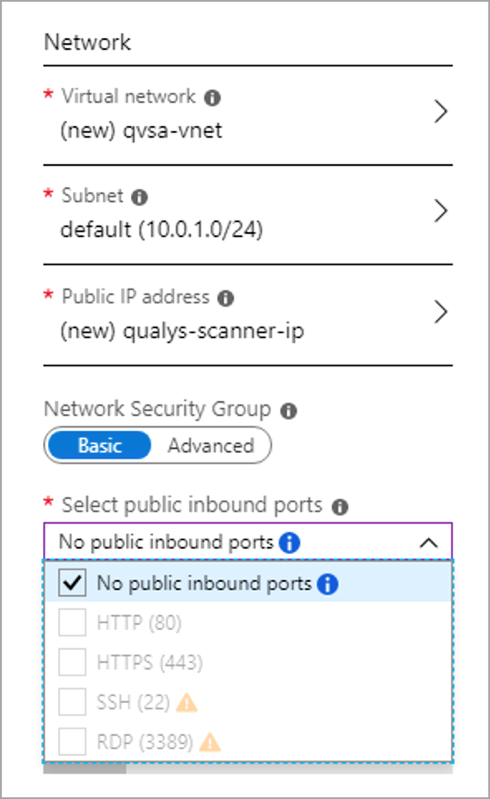
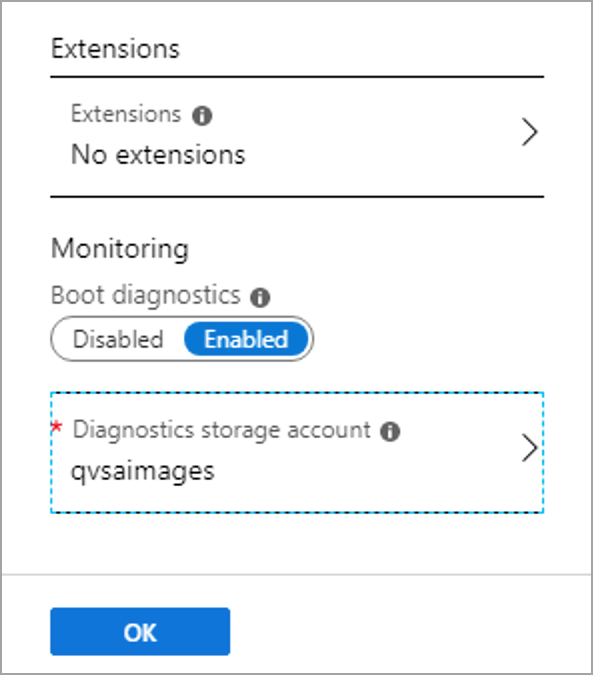
**Deploy Qualys Virtual Scanner Appliance from custom image**

**Note 1**: Please only use the Qualys Virtual Scanner Appliance image available on the Azure Marketplace or the Signed URL provided by Qualys. Using images downloaded from the Qualys UI will not work on Azure Stack, even with disk format conversions.  
**Note 2**: Tested on Azure Stack build 1.1910.0.58 with Wire Protocol version 2015-04-05 only.  
  
Here are the steps:  
1) Log into your Azure Stack account. From the main menu choose Dashboard > Images and select the qVSA image you obtained from Qualys.  
2) Click on ‘New VM’. Fill out the following fields and then click OK:  
  
**Name** – This is the name of your Qualys scanner. Scanner VM name must be between 1 and 64 characters long and may contain alpha-numeric characters, dots '.' and hyphens '-' only. It must start and end with alpha-numeric character.  
  
**VM Disk type** – You can choose a disk that best meets your requirements.  
  
**Username** – The Username is your personalization code, retrieved from the Qualys platform, with a 'u' prepended: “u2009XXXXXXXXXX”  
  
**Authentication type** – Choose “Password”. Since Qualys Virtual Scanner is a locked-down Linux appliance, managed completely from the Qualys Cloud Platform, Azure Stack username, password and SSH public key are not used for any kind of authentication but rather as a mechanism to pass configuration information from Azure Stack to the appliance.  
  
If you consider using of SSL Proxy on your scanner, you can pass proxy configuration through this field.

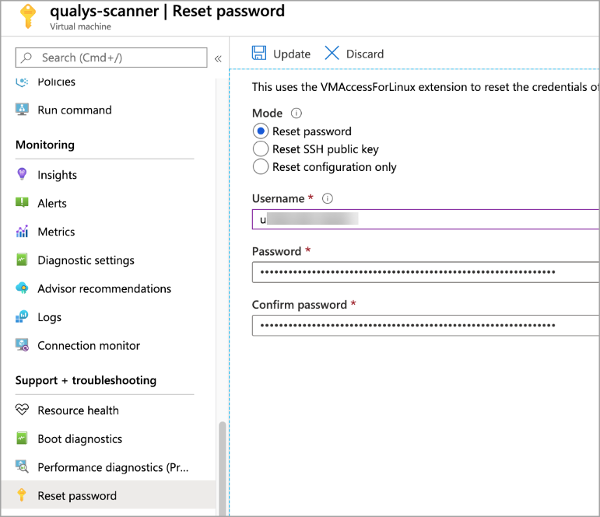
**Proxy server configuration:**

You can configure the Qualys Scanner to use SSL proxy for all outbound communication with the Qualys Cloud Platform. We support both IP and FQDN for the proxy server configuration. You'll specify the proxy server URL in the Password field using this format: proxy://username:password@proxyhost:port  
  
Formatting:  
If you have a domain user, the format is proxy://domain\username:password@proxyhost:port  
If authentication is not used, the format is proxy://proxyhost:port  
where proxyhost is the IPv4 address or the FQDN of the proxy server, port is the port the proxy server is running on  
  
Examples:  
proxy://jdoe:[abc12345@10.40.1.123](mailto:abc12345@10.40.1.123):3128  
proxy://jdoe:abc12345@myproxy.qualys.com:3128  
  
**Resource Group** – You can either use an existing Resource group or create a new one.  
To learn more about resource group, please visit Azure documentation: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal>.  
  
**Location** – local  
  
[](https://qualys--c.na90.content.force.com/sfc/dist/version/download/?oid=00D20000000m0ae&ids=0682L000007bYbE&d=%2Fa%2F2L0000009NjT%2FUNeSaKqneOQ15JbaZiErIW8zJc9ffBrsV.5lFYGV1m4&asPdf=false)  
  
3) On the next screen you need to choose a size for your virtual scanner. Qualys scanner supports **up to 16 cores and no more than 16 GB ram**. We recommend a ratio of 3-4 GB of memory per core.  
  
[](https://qualys--c.na90.content.force.com/sfc/dist/version/download/?oid=00D20000000m0ae&ids=0682L000007bYbF&d=%2Fa%2F2L0000009Njg%2FDqY3RDzl_jXKgTBu6LyXnIhx5U.crg6eJCIBV_EouVg&asPdf=false)  
  
4) On this screen you have to configure:  
  
**High Availability** – Choose “None”.  
  
**Storage** – Choose Disk type for your Qualys scanner.  
  
[](https://qualys--c.na90.content.force.com/sfc/dist/version/download/?oid=00D20000000m0ae&ids=0682L000007bYbG&d=%2Fa%2F2L0000009Njd%2Fc3bDeALzngK6FZ26_0gsY0b1hxtOvCoCtI6k0a5yd38&asPdf=false)  
  
**Network** – You should configure Virtual Network, Subnet and Public IP address for your VM. To learn more about Virtual Network, please visit Azure documentation: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>  
  
[](https://qualys--c.na90.content.force.com/sfc/dist/version/download/?oid=00D20000000m0ae&ids=0682L000007bYbH&d=%2Fa%2F2L0000009Nj2%2F8O05NiOQ67TSQY.pMJ52oLusCp7VF.cT.69bSSGNayE&asPdf=false)  
  
**Extensions** – No extension.  
  
**Monitoring** – We recommend Monitoring to be “Enabled”. Choose Diagnostics storage account and press OK button.  
  
[](https://qualys--c.na90.content.force.com/sfc/dist/version/download/?oid=00D20000000m0ae&ids=0682L000007bYbI&d=%2Fa%2F2L0000009NjG%2FgoiBupjubButkz5g8tH_z5PkGwBxwk5Z6ixMNhcWH04&asPdf=false)  
  
5) Review Summary of your VM. If everything looks good, click OK to start the deployment of the scanner.  
  
6) Once Azure completes the deployment, click on ‘Go to Resource’ to access the scanner deployment in your resource group.  
  
Your scanner will update and connect to the Qualys Cloud Platform. This process may take some time, depending on location. Once connected, you'll be able to use your Azure scanner from the Qualys Cloud Platform as you would any virtual scanner appliance.

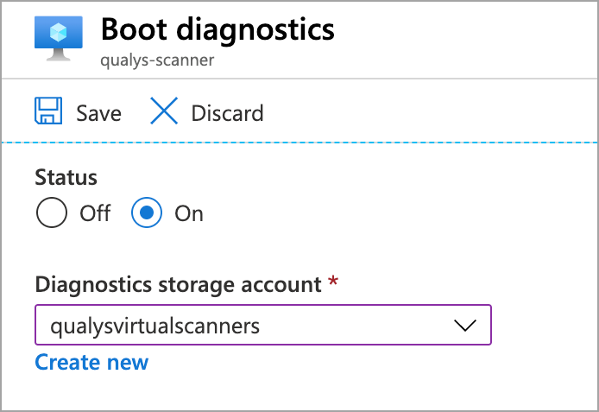
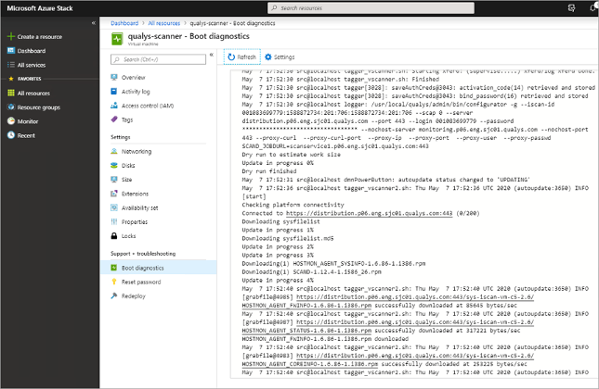
**How do I know my scanner is ready to use?**

Check your virtual scanner status in the Qualys UI. Go to Scans > Appliances and find your scanner in the list.  
  
Note: It can take several minutes for the Qualys user interface to get updated after you add a new appliance. Please refresh your browser periodically to ensure that you are seeing the most up to date details.  
  
[](https://qualys--c.na90.content.force.com/sfc/dist/version/download/?oid=00D20000000m0ae&ids=0682L000007bYbJ&d=%2Fa%2F2L0000009NjB%2FqQCNyjYuPBEDyZj3BAGnS0.bGF7A5N6NTUaVbhSb8N8&asPdf=false)  
  
[Active icon](https://qualys--c.na90.content.force.com/sfc/dist/version/download/?oid=00D20000000m0ae&ids=0682L000007bYbK&d=%2Fa%2F2L0000009Nje%2F8dp.wJfQixPLXjoSfd93H4DA.JMtueqLlKzuFFPnqjw&asPdf=false) tells you your virtual scanner is ready. Now you can start internal scans! (Next to this, you’ll see the busy icon which is grayed out until you launch a scan using this scanner.)

**Updating proxy settings upon deployment**

User can update their scanner with new proxy settings or disable the proxy upon deployment. To do so, locate your scanner virtual machine and click on ‘Reset password’.  
  
To update with new proxy settings, enter the new proxy configuration value in ‘Password’ and ‘Confirm Password’ fields and click on the ‘Update’ button.  
  
Note: Password fields should be prefixed with proxy://. This is because Azure cloud does not have mutable user metadata and the scanner interprets password value as an SSL proxy URL token, prefixed with proxy://.  
  
Username: u<Perscode>, e.g. u99999999999999  
Password: proxy://<new proxy value>  
Confirm Password: proxy://<new proxy value>  
  
[](https://qualys--c.na90.content.force.com/sfc/dist/version/download/?oid=00D20000000m0ae&ids=0682L000007bYbL&d=%2Fa%2F2L0000009Njn%2FQRgLFHGb4cV9dIwdT2zKGf8S40U_4OXoa.Y20Ksc8L0&asPdf=false)  
  
To disable proxy, click on ‘Reset password’, enter the exact value, ‘\*Rem0ve\_Pr0xy\*’, for Password and Confirm Password fields and click on ‘Update’ button.

**Troubleshooting**

If boot diagnostics was not enabled during scanner deployment and you would like to troubleshoot issues with your scanner, you can still enable Boot diagnostics. Diagnostics will include log output from the scanner. From the virtual machine details, click on ‘Boot diagnostics’, Set Status to On and select the storage account created for your Qualys scanners. Click ‘Save’ and reboot the virtual machine, if needed.  
  
[](https://qualys--c.na90.content.force.com/sfc/dist/version/download/?oid=00D20000000m0ae&ids=0682L000007bYbM&d=%2Fa%2F2L0000009NjJ%2FfNoyujT0XSsl3_lgnNI.U7lBmW6Q9oacEuNYDmiEfpY&asPdf=false)  
  
Click on Boot diagnostics to view the serial log.  
  
[](https://qualys--c.na90.content.force.com/sfc/dist/version/download/?oid=00D20000000m0ae&ids=0682L000007bYbN&d=%2Fa%2F2L0000009Njo%2FVvHe1oMuDAcplDjAN.yZfYnNKTYE2KmqM4NtA05A7.0&asPdf=false)

**For Customers on Private Cloud Platforms**

It could take hours to download the latest qVSA image from Qualys cloud storage account to your machine and then upload it to your Azure storage account using the Azure GUI. Save time by copying the image directly from Qualys cloud storage to your Azure account with Azure CLI tools.  
  
Here are the steps:  
1) Qualys Operations will provide you with a link to the qVSA image.  
2) Set up [Azure CLI tools](https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest) and log in to your Azure subscription using the Azure CLI "azure login" command.  
3) Copy the qVSA image from Qualys to your Azure subscription using this format:  
  
azure storage blob copy start [sourceUri] [options] [destContainer]  
  
where:  
[sourceUri] is the qVSA image link provided by Qualys Operations  
[options] are:  
-a, --account-name <accountName> the storage account name  
-k, --account-key <accountKey> the storage account key  
[destContainer] is the destination container in the "storage" specified with option "-a"  
  
Example:  
azure storage blob copy start "https://NNNimages.blob.core.windows.net/images/qVSA-Azure--X.X.x-x.vhd?st=YYYY-MM-DDT01%3A20%3A01Z&se=YYYY-MM-DDT01%3A20%3A01Z&sp=rl&sv=YYYY-MM-DD&sr=c&sig=signaturesamplexxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxD" -a "storageNNNN" -k "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx==" images  
  
Once you have Qualys qVSA image in Azure Cloud storage account you could send it to Azure Stack’s Storage account by using azcopy. We tested azcopy v7 with Azure Stack.  
  
Example:  
AzCopy.exe /Source:"https://qvsaimages.blob.core.windows.net/images" /Pattern:"qVSA-Azure.open-2.7.29-1.vhd"  
/Dest:"https://qvsaimages.blob.local.azurestack.external/images"  
/SourceKey:"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"  
/DestKey:"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx" /S /SyncCopy /V