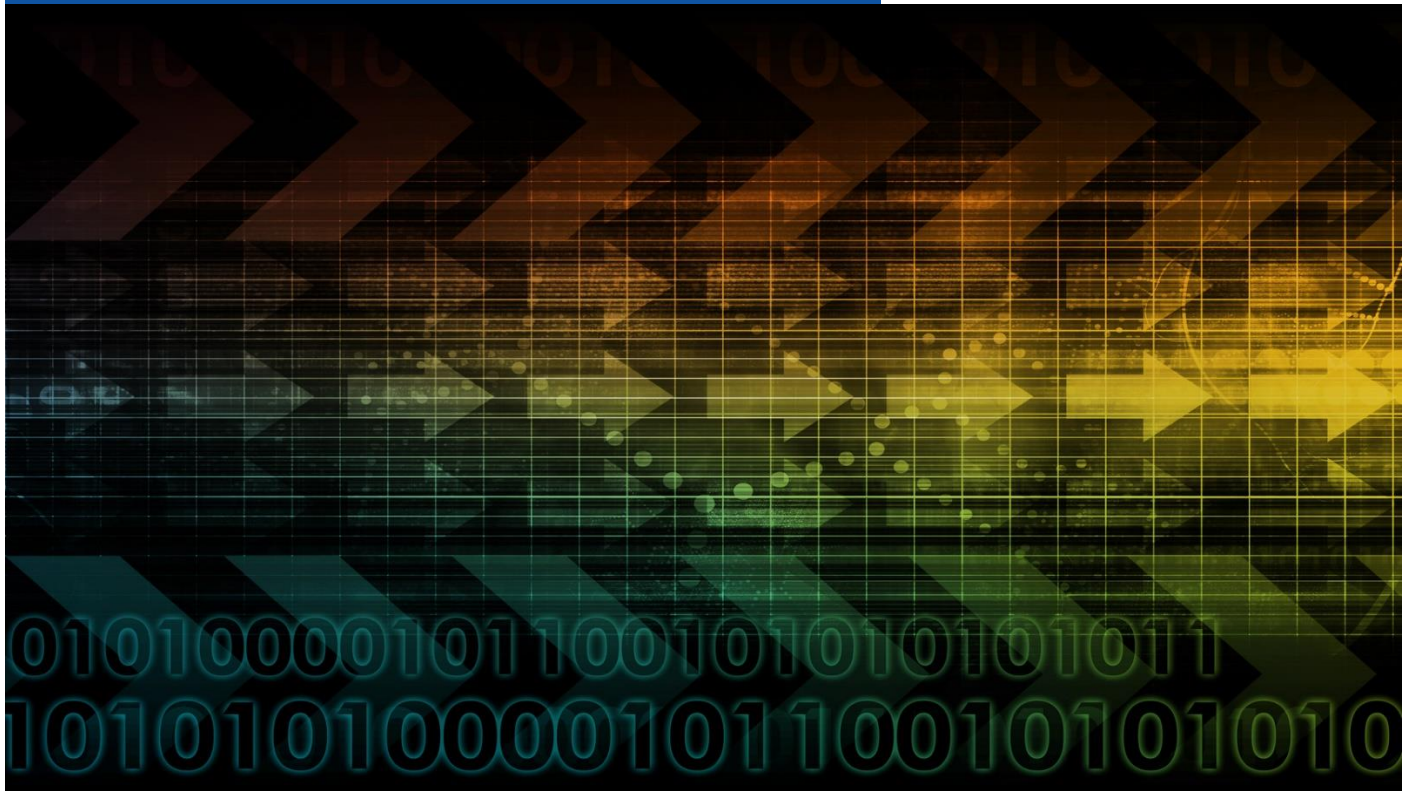




Clone Guard  
Security Scanning



# Clone Systems Internal Scanner

## Setup Manual

May 2024



# TABLE OF CONTENTS

WELCOME.....4

    Getting Started .....4

    Installation Steps.....4

DOWNLOAD THE INTERNAL SCANNER .....5

    Overview.....5

    Access the Internal Scanner.....5

ORACLE VIRTUALBOX .....6

    Overview.....6

    Import and Configure the Internal Scanner .....6

KVM .....10

    Overview.....10

    Import and Configure the Internal Scanner with Virt-manager .....10

VMWARE ESXI .....15

    Overview.....15

    Import and Configure the Internal Scanner .....15

VMWARE VSPHERE .....19

    Overview.....19

    Import and Configure the Internal Scanner .....19

VMWARE WORKSTATION .....25

    Overview.....25

    Import and Configure the Internal Scanner .....25

CITRIX XENSERVER .....27

    Overview.....27

    Import and Configure the Internal Scanner .....27

MICROSOFT HYPER-V .....32

    Overview.....32

    Import and Configure the Internal Scanner .....32

AWS MARKETPLACE .....37

    Overview.....37

    Import the AWS Security Scanner .....37

    Configure the AWS Security Scanner.....40

AZURE MARKETPLACE .....47

    Overview.....47

    Import the AZURE Security Scanner .....47

    Configure the AZURE Security Scanner .....54

INITIALIZE INTERNAL SCANNER .....59

    Overview.....59

    Default Settings .....59

    Initialize the Internal Scanner .....60

# WELCOME

The Clone Systems suite of Security Scanning solutions provides a capability of scanning your corporation's internal private network to help identify and remediate vulnerabilities. In order to conduct these internal scans, you must configure an internal scanner on your corporation's virtual environment and register it with your Clone Systems Security Scanning solution.

## Getting Started

This setup manual provides you with instructions on how to configure an internal scanner for use with your Clone Systems Security Scanning Solution. The Internal Scanner is available for the following Virtual Environments:

Internal Scanner Supported on the Following Virtual Environments
Oracle VirtualBox
KVM
VMWare ESXi / vSphere / Workstation
Citrix XenServer
Microsoft Hyper-V
Microsoft AZURE Cloud
Amazon AWS Cloud

## Installation Steps

The following details the steps involved with configuring the internal scanner.

Installation Steps
1. <a href="#">Download the Internal Scanner</a>
2. <a href="#">Configure the Internal Scanner within your Virtual Environment</a>
3. <a href="#">Initialize the Internal Scanner</a>

# DOWNLOAD THE INTERNAL SCANNER

## Overview

The following will provide an overview of how to access and download the Internal Scanner that is supported by your corporation’s virtual environment.

## Access the Internal Scanner

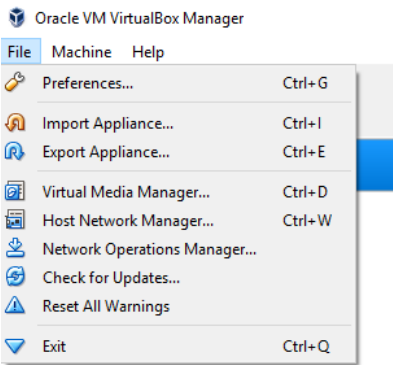
Steps for Downloading the Internal Scanner	
<b>Step 1</b>  <b>Download the Virtual Scanner Image</b>	Navigate your browser to the hyperlink below and download the image that matches your environment.  <a href="https://www.clone-systems.com/virtual-scanner-downloads/">https://www.clone-systems.com/virtual-scanner-downloads/</a>

# ORACLE VIRTUALBOX

## Overview

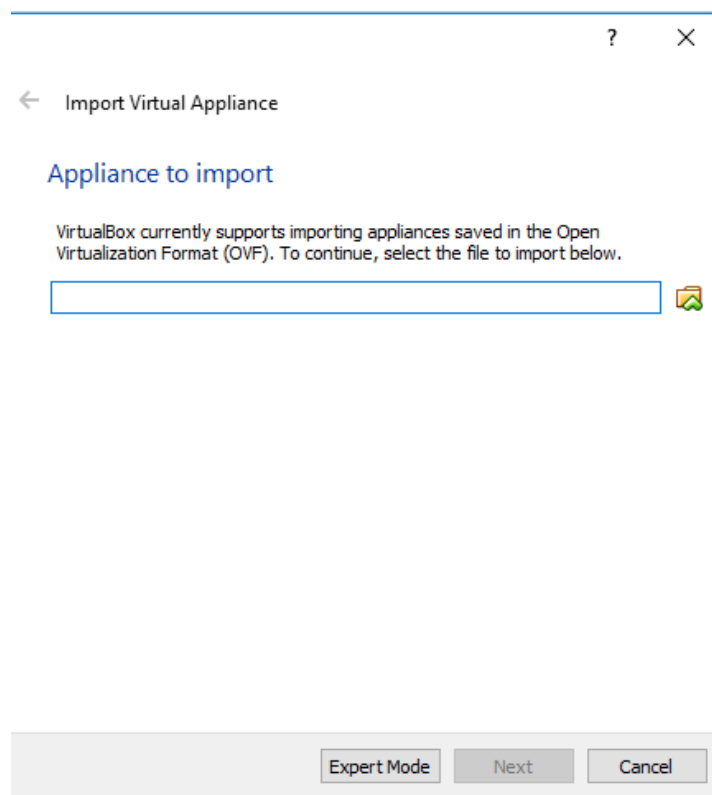
The following will provide an overview of how to configure the Clone Systems Internal Scanner on Oracle VirtualBox.

## Import and Configure the Internal Scanner

Steps for Importing the Internal Scanner into VirtualBox	
<div>Step 1</div> <div>Begin the Import Wizard</div>	<div>From the VirtualBox <b>File</b> menu select <b>Import Appliance</b>.</div> <div></div>

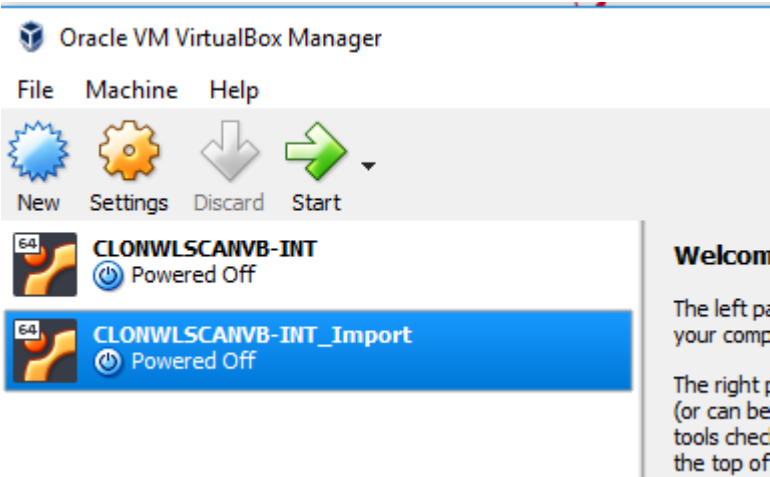
**Step 2****Select the ova file for  
the Internal Scanner**

This will begin the **Import Wizard**. Select the **ova** file for the Internal Scanner that you extracted from the Tarball and then click **Next**.



<p><b>Step 3</b></p> <p><b>Setup the import for the Internal Scanner</b></p>	<p>Depending on your environment you may want to reinitialize the MAC addresses by selecting the checkbox in front of <b>Reinitialize the MAC address of all network cards</b>, but it is not required. Click <b>Import</b>.</p> <div data-bbox="423 388 1232 1278"><div><div>?</div><div>×</div></div><div>← Import Virtual Appliance</div><div>Appliance settings</div><div>These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.</div><div><div>Virtual System 1</div><div><div><div><div></div><div>Name</div></div><div>CLONWLSCANVB-INT_1</div></div><div><div><div></div><div>Product</div></div><div>Clone System Internal Scanner</div></div><div><div><div></div><div>Vendor</div></div><div>Clone Systems Inc</div></div><div><div><div></div><div>Vendor-URL</div></div><div>https://www.clone-systems.com</div></div><div><div><div></div><div>Version</div></div><div>0.40</div></div><div><div><div></div><div>Description</div></div><div>Clone System Internal Scanner (Vi...</div></div><div><div><div></div><div>Guest OS Type</div></div><div><div><div></div><div>Ubuntu (64-bit)</div></div></div></div></div><div><div><input type="checkbox"/> Reinitialize the MAC address of all network cards</div><div>Appliance is not signed</div></div><div><div>Restore Defaults</div><div>Import</div><div>Cancel</div></div></div></div>
<p><b>Step 4</b></p> <p><b>Import the Internal Scanner</b></p>	<p>The import process will begin and may take a few minutes depending on the hardware that comprises your Corporation's virtual environment.</p> <div data-bbox="423 1444 1395 1728"><div>Importing Appliance ...: Importing appliance 'D:\VMS\CLONWLSCANVB-Scanne...</div><div><div><div></div></div><div><div>Importing virtual disk image 'CLONWLSCANVB-Scanner-disk001.vmdk' ... (2/3)</div><div><div></div><div>3%</div><div>×</div></div><div>2 minutes, 53 seconds remaining</div></div></div></div>



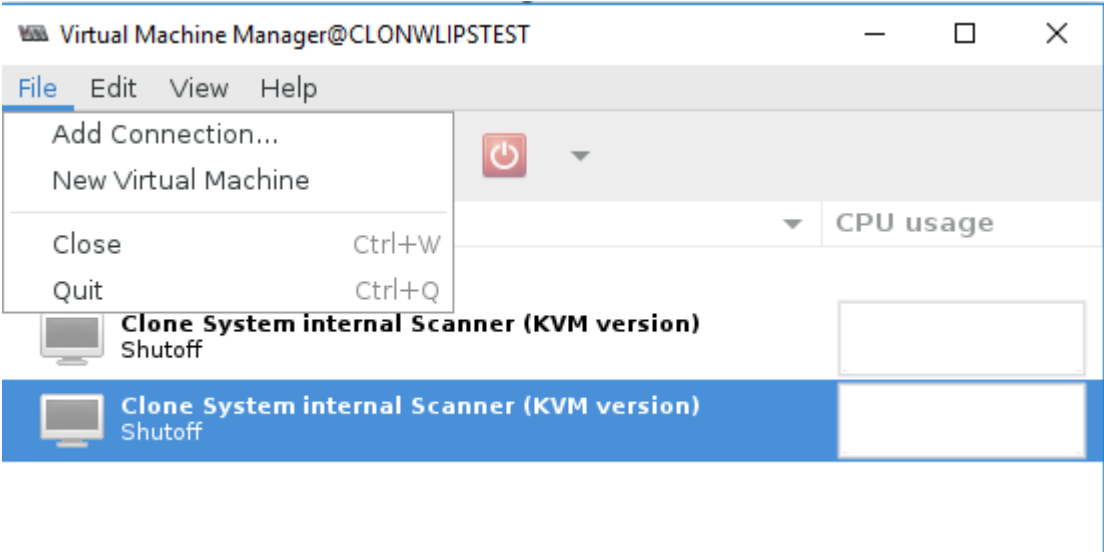
<p><b>Step 5</b></p> <p><b>Configure network settings and start the Internal Scanner</b></p>	<p>When the import of the Internal Scanner is completed you will see the new Virtual Machine in your VM inventory.</p> <p>Before you start the Internal Scanner, please edit the <b>Settings</b> and modify the <b>networking</b> options for your corporate network.</p> <p><b>Note:</b> Confirm your network settings for the Internal Scanner before powering it on.</p> <div data-bbox="431 537 1196 1010">The screenshot shows the Oracle VM VirtualBox Manager interface. At the top, there's a title bar and a menu bar with 'File', 'Machine', and 'Help'. Below the menu bar is a toolbar with icons for 'New' (a blue star), 'Settings' (a yellow gear), 'Discard' (a grey arrow pointing down), and 'Start' (a green arrow pointing right). The main area displays a list of virtual machines. The first VM is 'CLONWLSCANVB-INT' with a status of 'Powered Off'. The second VM is 'CLONWLSCANVB-INT_Import', which is highlighted with a blue background and also has a status of 'Powered Off'. On the right side of the window, a 'Welcome' message is partially visible, starting with 'The left pa...' and 'your comp...'.<p>Oracle VM VirtualBox Manager</p><p>File Machine Help</p><p>New Settings Discard Start</p><p>CLONWLSCANVB-INT Powered Off</p><p>CLONWLSCANVB-INT_Import Powered Off</p><p>Welcome</p><p>The left pa your comp</p><p>The right p (or can be tools chec the top of</p></div>
--	---

KVM

Overview

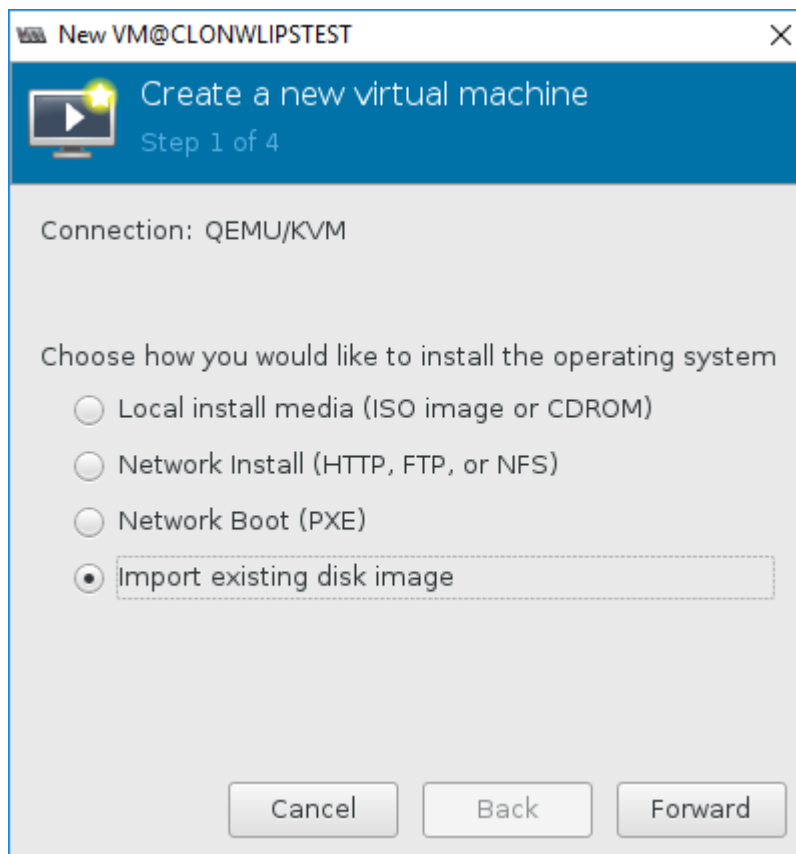
The following will provide an overview of how to configure the Clone Systems Internal Scanner on KVM.

Import and Configure the Internal Scanner with Virt-manager

Steps for Importing the Internal Scanner into KVM with Virt-manager	
Step 1  Create New Virtual Machine with Virt-manager	<p>From the Virt-manager <b>File</b> menu select <b>New Virtual Machine</b>.</p> 

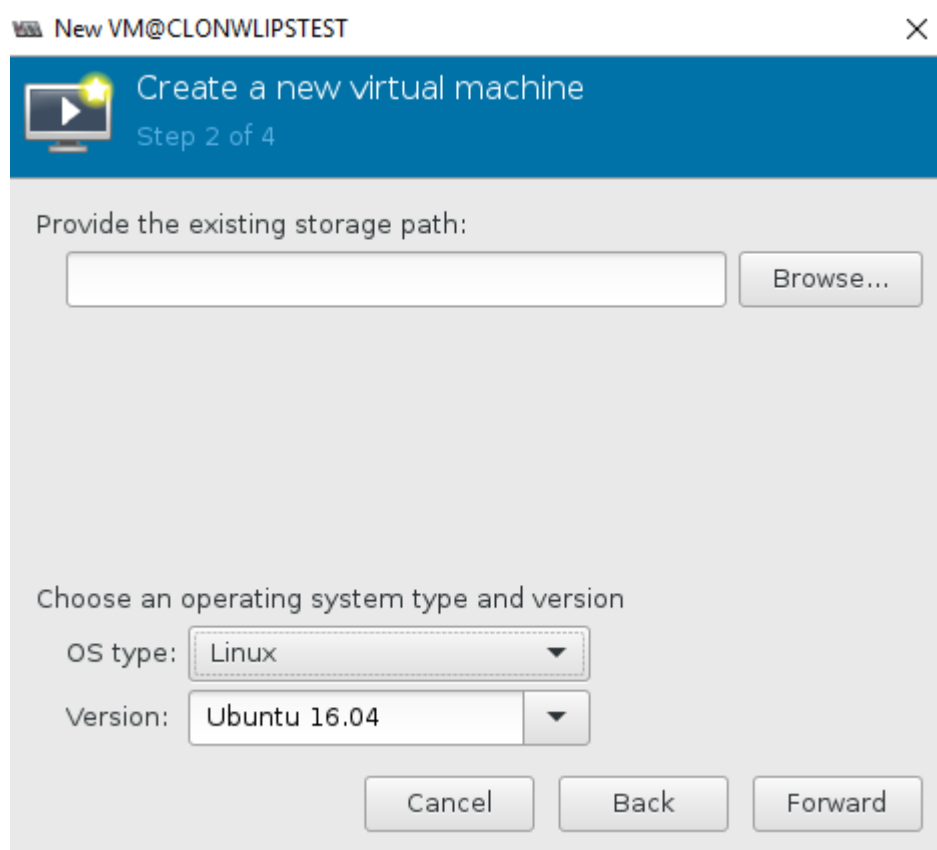
**Step 2****Import the Internal  
Scanner disk image**

This will begin the **New Virtual Machine Wizard**. Select **Import existing disk image** and then click **Forward**.



**Step 3****Setup the Disk Image  
and OS Type**

Select the **disk image** file for the Internal Scanner that you extracted from the Tarball and then select **Linux** for the **OS type** and **Ubuntu 16.04** for the **Version** and then click **Forward**.



New VM@CLONWLIPSTEST

Create a new virtual machine  
Step 2 of 4

Provide the existing storage path:

Choose an operating system type and version

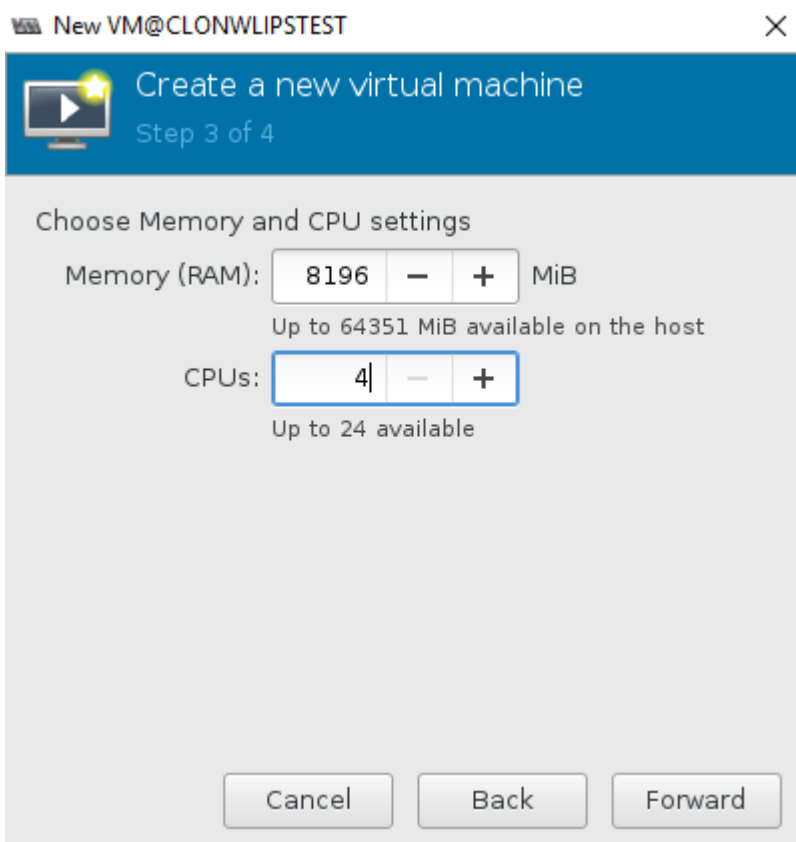
OS type:

Version:

**Step 4****Set the RAM and CPU settings**

Set the Memory and CPU values to the configuration recommended by Clone Systems. Set the **Memory to 8196** and set the **CPUs to 4**.

**Note:** Setting the Memory and CPU to values lower than the recommended settings will impact the scanning performance.



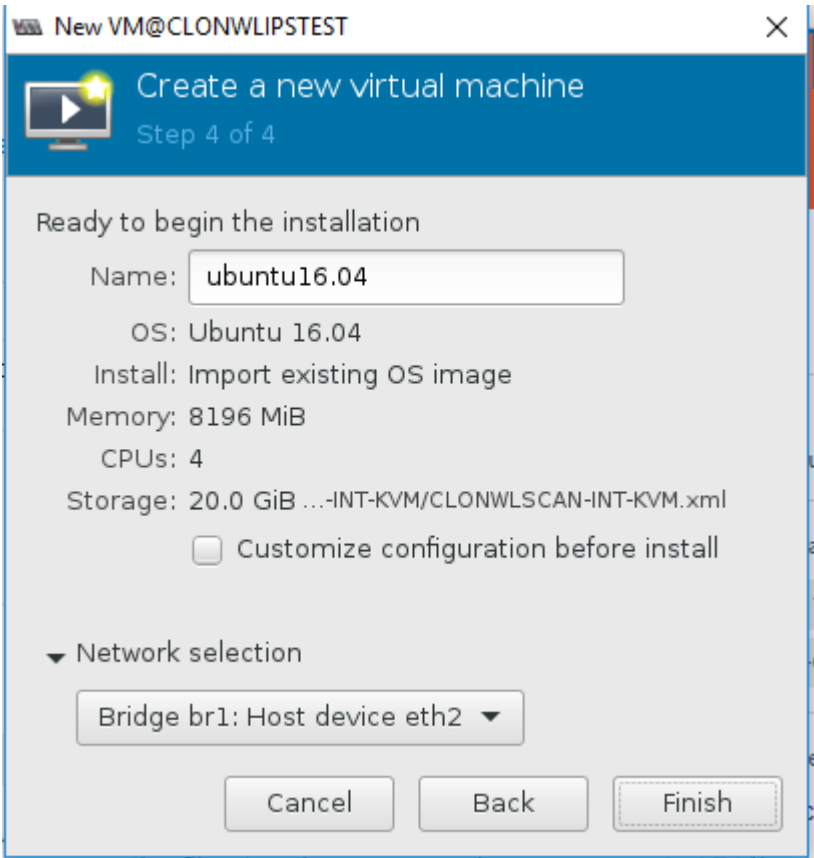
Step 5

Configure network settings and start the Internal Scanner

When the import of the Internal Scanner is completed you will see the new Virtual Machine in your VM inventory.

Change the Virtual Machine **Name** according to your naming convention and modify the **networking** options for your corporate network than click **Finish**

**Note:** Confirm your network settings for the Internal Scanner before powering it on.

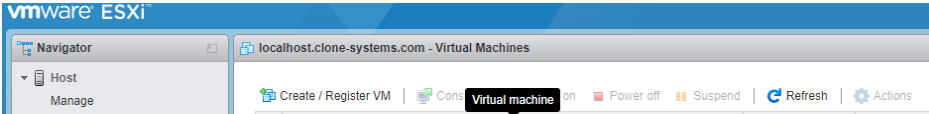
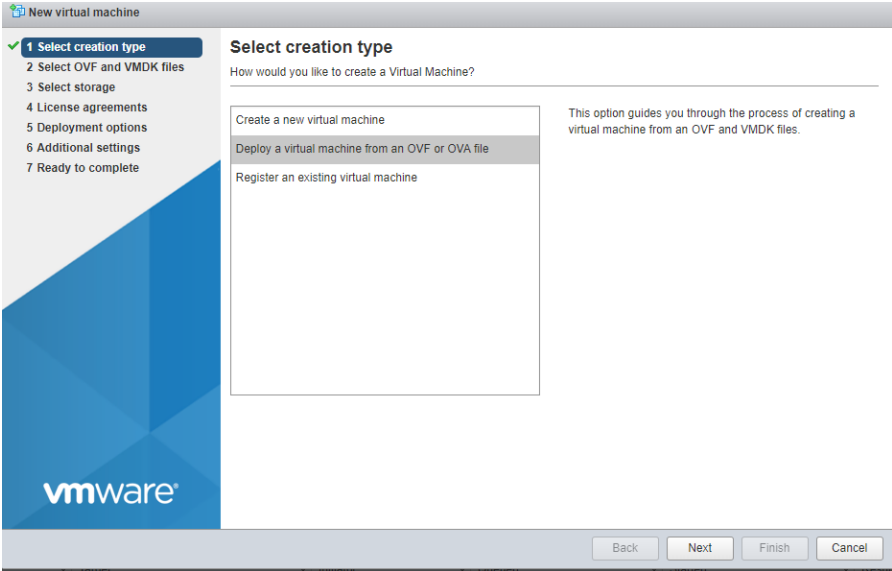


# VMWARE ESXI

## Overview

The following will provide an overview of how to configure the Clone Systems Internal Scanner on VMware ESXi.

## Import and Configure the Internal Scanner

Steps for Importing the Internal Scanner into VMware ESXi	
<div>Step 1</div> <div>Begin the New Virtual Machine Wizard</div>	<div>From the <b>Virtual Machine</b> tab select <b>Create/Register VM</b>.</div> <div></div>
<div>Step 2</div> <div>Select Creation Type</div>	<div>On the <b>Select creation type</b> step select <b>Deploy a virtual machine from an OVF or OVA file</b>.</div> <div></div>

Step 3

Select OVF and VMDK Files for Internal Scanner

On the **Select OVF and VMDK files** step select a Virtual Machine name and select both the **vmdk** and **ovf** file for the Internal Scanner that you extracted from the Tarball and click **Next**.

The screenshot shows the 'New virtual machine - Clone-Internal-Scanner' wizard. On the left, a progress bar indicates the steps: 1. Select creation type, 2. Select OVF and VMDK files (current step), 3. Select storage, 4. License agreements, 5. Deployment options, 6. Additional settings, and 7. Ready to complete. The main area is titled 'Select OVF and VMDK files' and contains the instruction 'Select the OVF and VMDK files or OVA for the VM you would like to deploy'. Below this, there is a text field 'Enter a name for the virtual machine.' with the value 'Clone-Internal-Scanner'. A note states: 'Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.' A list of selected files is shown: 'CLONWLSCANX-vmworkstation.ovf' and 'CLONWLSCANX-vmworkstation-disk1.vmdk'. At the bottom right, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

Step 4

Select the Storage

On the **Select storage** step select the storage for your environment and click **Next**.

The screenshot shows the 'New virtual machine - Clone-Internal-Scanner' wizard. On the left, a progress bar indicates the steps: 1. Select creation type, 2. Select OVF and VMDK files, 3. Select storage (current step), 4. License agreements, 5. Deployment options, 6. Additional settings, and 7. Ready to complete. The main area is titled 'Select storage' and contains the instruction 'Select the storage type and datastore'. Below this, there are two buttons: 'Standard' (selected) and 'Persistent Memory'. A note states: 'Select a datastore for the virtual machine's configuration files and all of its' virtual disks.' A table lists available datastores:

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	1.81 TB	1.5 TB	VMFS5	Supported	Single

At the bottom right, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.



**Step 5****Configure Networking**

On the **Deployment options** step select the correct network mappings for your corporate network and click **Next**.

The screenshot shows the 'New virtual machine - Clone-Internal-Scanner' wizard in VMware Workstation. The left sidebar lists five steps: 1 Select creation type, 2 Select OVF and VMDK files, 3 Select storage, 4 Deployment options (highlighted), and 5 Ready to complete. The main area is titled 'Deployment options' with the subtitle 'Select deployment options'. It contains three sections: 'Network mappings' with a dropdown menu set to 'bridged' and 'VM Network'; 'Disk provisioning' with radio buttons for 'Thin' (selected) and 'Thick'; and 'Power on automatically' with a checked checkbox. At the bottom right are buttons for 'Back', 'Next', 'Finish', and 'Cancel'. The VMware logo is visible in the bottom left corner of the window.

Deployment options	
Select deployment options	
Network mappings	bridged VM Network
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick
Power on automatically	<input checked="" type="checkbox"/>

**Step 6****Complete configuration**

On the **Ready to complete** step click **Finish**.

**Note:** Once the Import has completed confirm your network settings for the Internal Scanner before powering it on.

The screenshot shows the 'New virtual machine - Clone-Internal-Scanner' wizard in VMware Workstation. The left sidebar lists five steps: 1 Select creation type, 2 Select OVF and VMDK files, 3 Select storage, 4 Deployment options, and 5 Ready to complete (highlighted). The main area is titled 'Ready to complete' and includes the instruction 'Review your settings selection before finishing the wizard'. Below this is a table of settings:

Product	CLONWLSCANX
VM Name	Clone-Internal-Scanner
Disks	CLONWLSCANX-vmworkstation-disk1.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	bridged: VM Network
Guest OS Name	Unknown

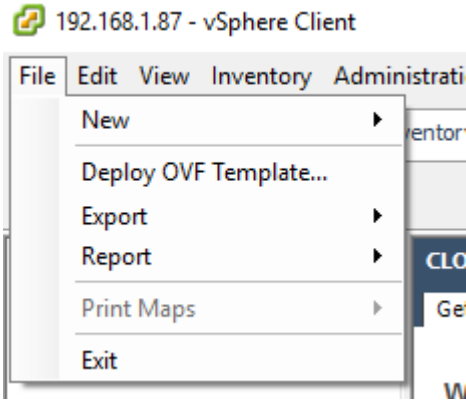
Below the table is a yellow warning icon and the text: 'Do not refresh your browser while this VM is being deployed.' At the bottom right are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

# VMWARE VSPHERE

## Overview

The following will provide an overview of how to configure the Clone Systems Internal Scanner on VMware vSphere.

## Import and Configure the Internal Scanner

Steps for Importing the Internal Scanner into VMware vSphere	
Step 1  Begin the Deploy OVF template Wizard	<p>From the vSphere <b>File</b> menu select <b>Deploy OVF template</b>.</p>  <p>The screenshot shows the VMware vSphere Client interface with the 'File' menu open. The menu options are: New, Deploy OVF Template..., Export, Report, Print Maps, and Exit. The 'Deploy OVF Template...' option is highlighted. The background shows the vSphere Client window title '192.168.1.87 - vSphere Client' and other menu items like 'Edit', 'View', 'Inventory', and 'Administration'.</p>


**Step 2****Select Source for  
Internal Scanner**

On the **Source** step select the **ovf/ova** file for the Internal Scanner that you extracted from the Tarball and click **Next**.

The screenshot shows a window titled "Deploy OVF Template" with standard window controls (minimize, maximize, close). Below the title bar, the "Source" step is selected, with the instruction "Select the source location." Below this is a list of steps: "Source" (selected), "OVF Template Details", "Name and Location", "Disk Format", and "Ready to Complete". The main area of the window is titled "Deploy from a file or URL" and contains a text input field with a dropdown arrow and a "Browse..." button. Below the input field, there is a paragraph of text: "Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive." At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

**Step 3****Verify OVF Template**

On the **OVF Template Details** verify the template details and click **Next**.

 Deploy OVF Template

— □ ×

**OVF Template Details**

Verify OVF template details.

[Source](#)**OVF Template Details**

Name and Location

Disk Format

Ready to Complete

Product: CLONWLSKANX-

Version:

Vendor:

Publisher: No certificate present

Download size: Less than 1 MB

Size on disk: Unknown (thin provisioned)  
60.0 GB (thick provisioned)Description: Clone Systems Scanning VM  
Configured for 172.16.1.26  
netmask 255.255.0.0  
gateway 172.16.1.250Issues or questions please contact:  
esupport@clone-systems.com

&lt; Back

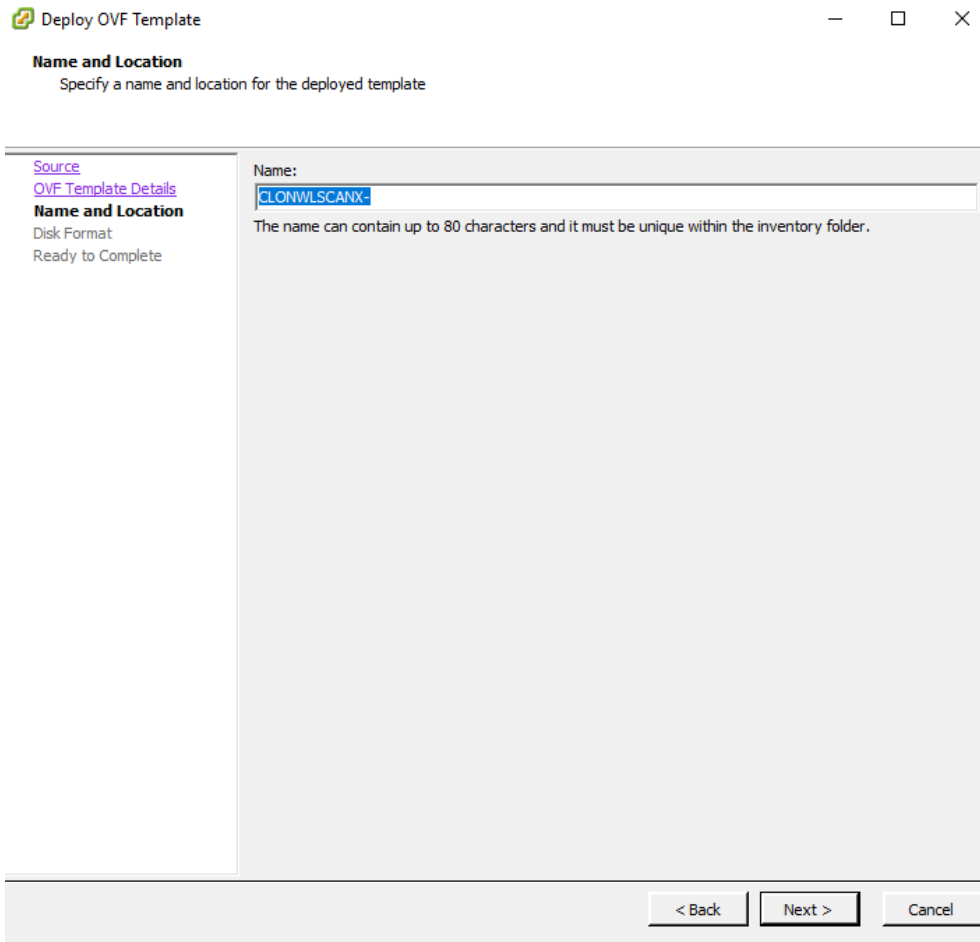
Next &gt;

Cancel

### Step 4

## Set Name and Location

On the **Name and Location** step enter a name for the Internal Scanner and click **Next**.



**Step 5****Select the Datastore**

On the **Disk Format** step select the Datastore information for your corporate network and click **Next**.

The screenshot shows the 'Deploy OVF Template' wizard window. The title bar says 'Deploy OVF Template' with standard window controls. The main content area is titled 'Disk Format' with the subtitle 'In which format do you want to store the virtual disks?'. On the left, there is a sidebar with links: 'Source', 'OVF Template Details', 'Name and Location', and 'Disk Format' (which is highlighted). Below the links, it says 'Ready to Complete'. The main area contains the following fields and options:

- Datastore:** A text box containing 'datastore1'.
- Available space (GB):** A text box containing '91.6'.
- Provisioning Options:** Three radio buttons are listed:
  - ☒ Thick Provision Lazy Zeroed
  - ☐ Thick Provision Eager Zeroed
  - ☐ Thin Provision

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**Step 6****Complete configuration**

On the **Ready to complete** step click **Finish**.

**Note:** Once the Import has completed confirm your network settings for the Internal Scanner before powering it on.

The screenshot shows a window titled "Deploy OVF Template" with standard window controls (minimize, maximize, close). Below the title bar, the text "Ready to Complete" is displayed, followed by the question "Are these the options you want to use?".

On the left side of the window, there is a vertical list of links: "Source", "OVF Template Details", "Name and Location", "Disk Format", and "Ready to Complete" (which is highlighted in bold). Below these links is a section titled "When you click Finish, the deployment task will be started." followed by a "Deployment settings:" label.

The deployment settings are listed in a table-like format:

OVF file:	D:\CLONWLSCANXv5\CLONWLSCANX.ovf
Download size:	Less than 1 MB
Size on disk:	60.0 GB
Name:	CLONWLSCANX-
Host/Cluster:	CLONVMMWARE-ESX.clone-systems.com
Datastore:	datastore1
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"VM Network" to "VM Network"

Below the settings table, there is a checkbox labeled "Power on after deployment" which is currently unchecked.

At the bottom right of the window, there are three buttons: "< Back", "Finish" (which is highlighted with a darker border), and "Cancel".

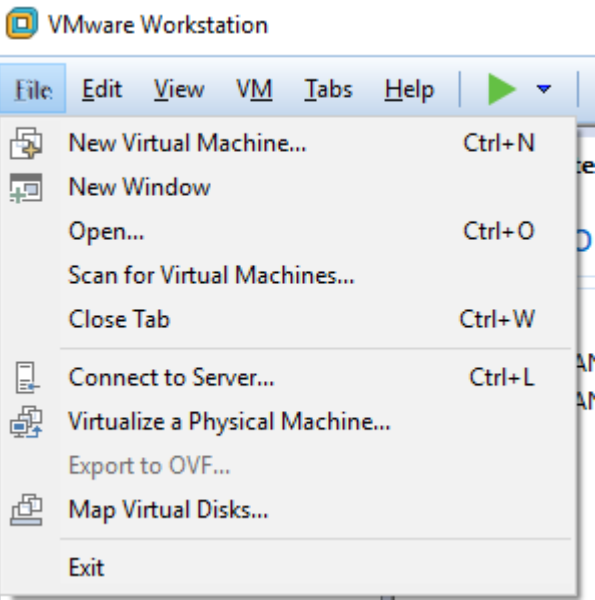


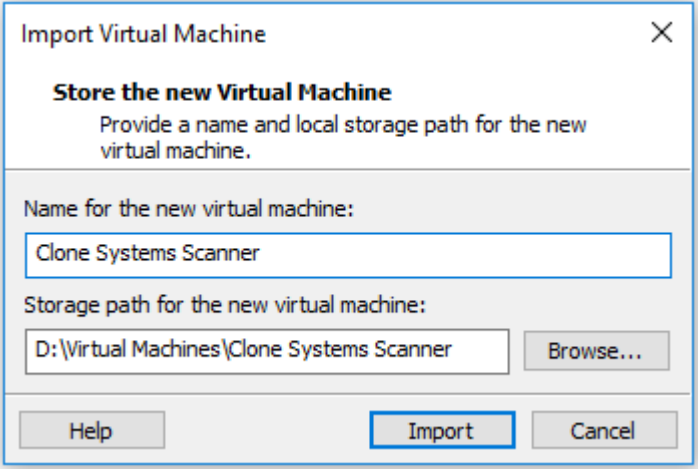
# VMWARE WORKSTATION

## Overview

The following will provide an overview of how to configure the Clone Systems Internal Scanner on VMware Workstation.

## Import and Configure the Internal Scanner

Steps for Importing the Internal Scanner into VMware Workstation	
<div>Step 1</div> <div>Open Source for Internal Scanner</div>	<div>From the Workstation <b>File</b> menu click Open and select the <b>ovf/ova</b> file for the Internal Scanner that you extracted from the Tarball</div> <div>A screenshot of the VMware Workstation application window. The 'File' menu is open, showing options: New Virtual Machine... (Ctrl+N), New Window, Open... (Ctrl+O), Scan for Virtual Machines..., Close Tab (Ctrl+W), Connect to Server... (Ctrl+L), Virtualize a Physical Machine..., Export to OVF..., Map Virtual Disks..., and Exit. The 'Open...' option is highlighted.</div>

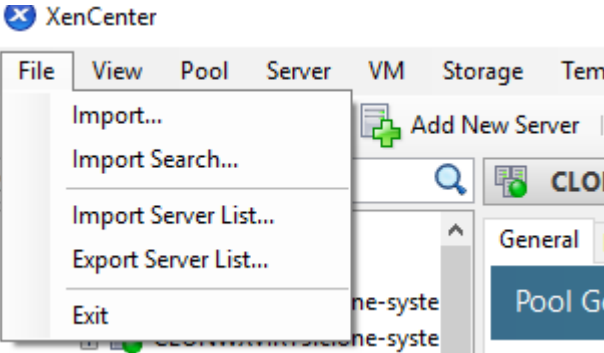
<div>Step 2</div> <div>Set Name and Storage Path</div>	<div>The <b>Import Virtual Machine</b> Wizard will begin. Select a <b>Name</b> for the Internal Scanner and click <b>Import</b>.</div> <div></div>
<div>Step 3</div> <div>Configure Networking</div>	<div>After the Internal Scanner is imported, change the network adaptor for your corporate network.</div> <div><b>Note:</b> Confirm your network settings for the Internal Scanner before powering it on.</div>

# CITRIX XENSERVER

## Overview

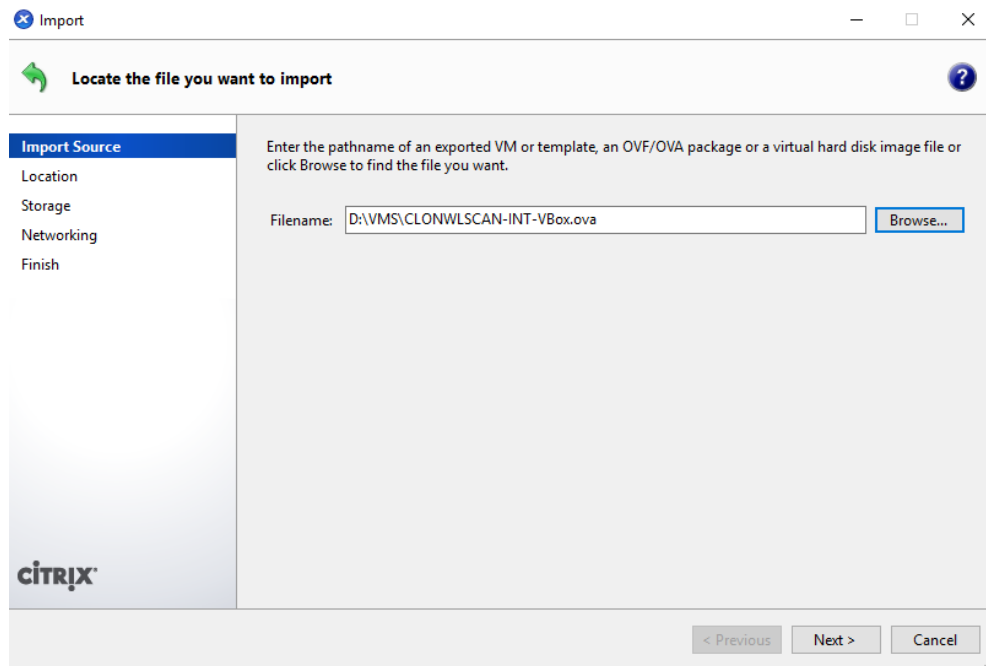
The following will provide an overview of how to configure the Clone Systems Internal Scanner on Citrix Xenserver.

## Import and Configure the Internal Scanner

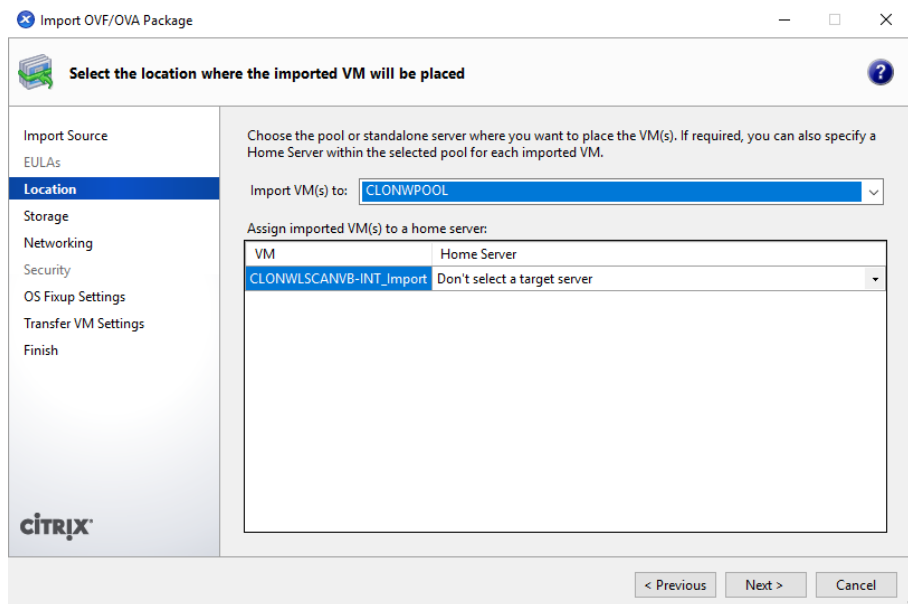
Steps for Importing the Internal Scanner into Citrix Xenserver	
Step 1  Start the Import Wizard	<p>From the XenCenter <b>File</b> menu click <b>Import</b> to begin the Import Wizard.</p>  <p>The screenshot shows the XenCenter application window. The 'File' menu is open, displaying options: 'Import...', 'Import Search...', 'Import Server List...', 'Export Server List...', and 'Exit'. The 'Import...' option is highlighted. In the background, other menu items like 'View', 'Pool', 'Server', 'VM', 'Storage', and 'Template' are visible. On the right side of the interface, there are buttons for 'Add New Server', 'CLO...', and a 'General' tab for a 'Pool G...'.</p>

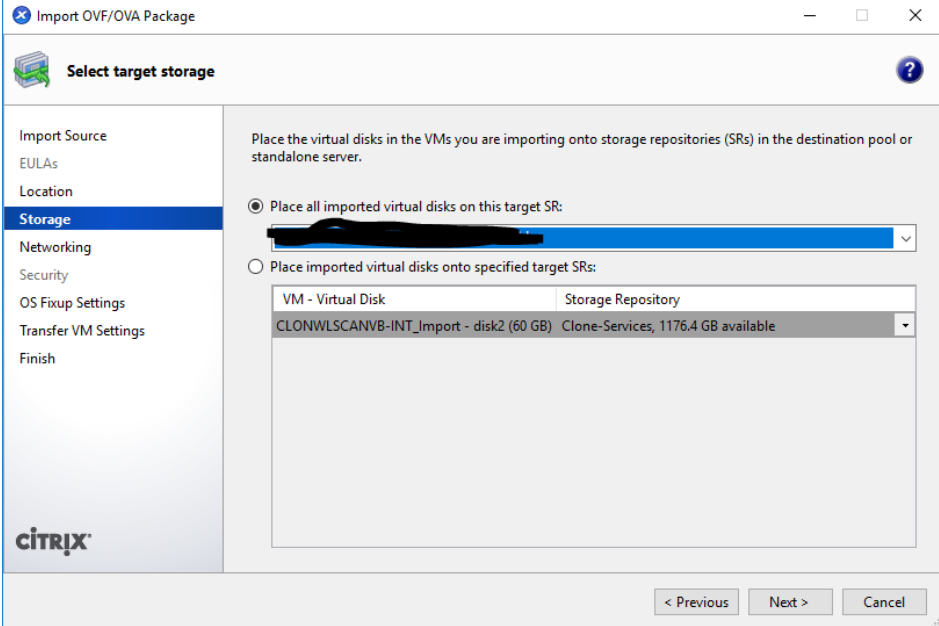
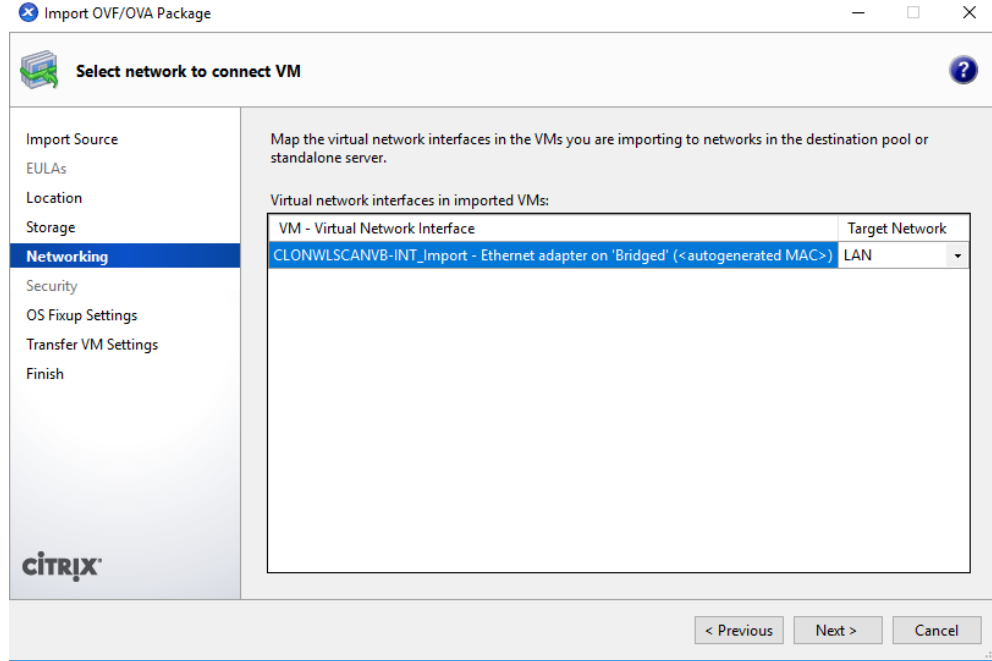
**Step 2****Select Source for  
Internal Scanner**

On the **Import Source** step select the **ovf/ova** file for the Internal Scanner that you extracted from the Tarball and click **Next**.

**Step 3****Select Location**

On the **Location** step select your Pool or Server that you want to configure the Internal Scanner on and click **Next**.



<div>Step 4</div> <div>Select Storage Location</div>	<div>On the <b>Storage</b> step select the storage location and click <b>Next</b>.</div> <div></div>
<div>Step 5</div> <div>Configure Interface Adapters</div>	<div>On the <b>Networking</b> step select the network interfaces for the Internal Scanner and click <b>Next</b>.</div> <div></div>

**Step 6****Configure OS Settings**

On the **OS Fixup Settings** select **Don't user Operating System Fixup** and click **Next**.

The screenshot shows the 'Import OVF/OVA Package' window with the 'OS Fixup Settings' step selected in the left sidebar. The main area is titled 'Use Operating System Fixup to ensure hypervisor interoperability'. It contains a description of Operating System Fixup and two radio button options: 'Don't use Operating System Fixup' (selected) and 'Use Operating System Fixup'. Below the options is a dropdown menu for 'Location of OS Fixup ISO' set to 'ISO-TempNew (1492.7 GB)'. The Citrix logo is in the bottom left, and navigation buttons '< Previous', 'Next >', and 'Cancel' are in the bottom right.

**Step 7****Configure Networking**

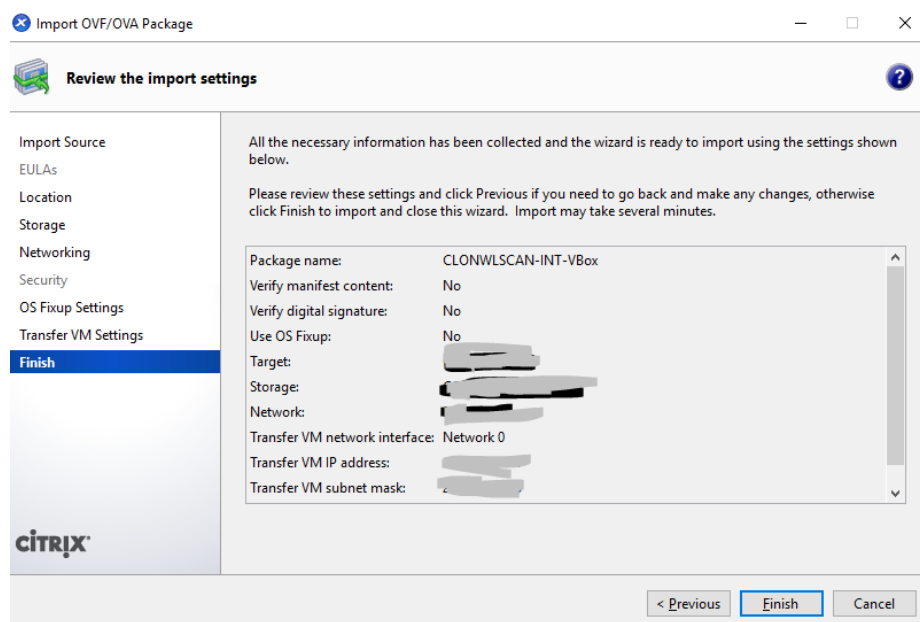
On the **Transfer VM Settings** step configure your corporate network information for the Internal Scanner and click **Next**.

The screenshot shows the 'Import OVF/OVA Package' window with the 'Transfer VM Settings' step selected in the left sidebar. The main area is titled 'Configure networking options for the Transfer VM'. It contains a dropdown menu for 'Network' set to 'Network 0 (management)'. Below this is a 'Network Settings' section with two radio button options: 'Automatically obtain network settings using DHCP' (selected) and 'Use these network settings:'. The latter option has input fields for 'IP address', 'Subnet mask', and 'Gateway'. The Citrix logo is in the bottom left, and navigation buttons '< Previous', 'Next >', and 'Cancel' are in the bottom right.

**Step 8****Review Import Settings  
and Import the Internal  
Scanner**

On the **Finish** step review the configuration settings and click **Finish** to begin the import process.

**Note:** Once the Import has completed confirm your network settings for the Internal Scanner before powering it on.



# MICROSOFT HYPER-V

## Overview

The following will provide an overview of how to configure the Clone Systems Internal Scanner on Microsoft Hyper-V.

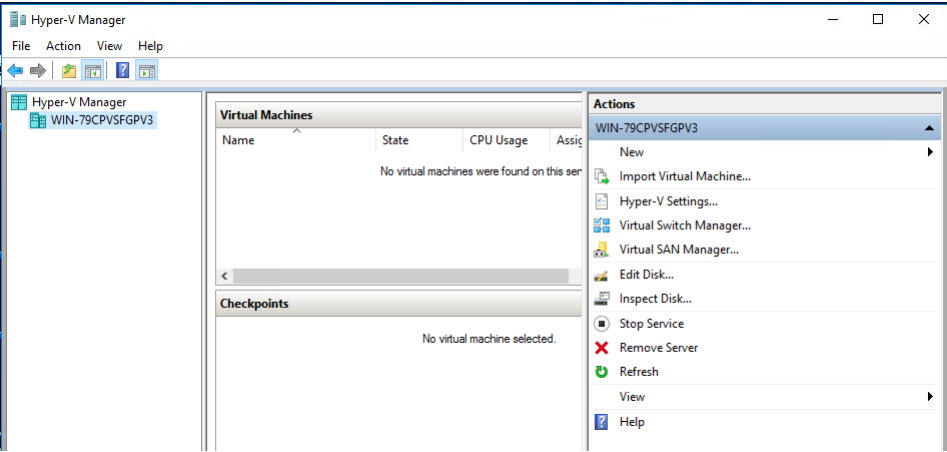
## Import and Configure the Internal Scanner

Steps for Importing the Internal Scanner into Microsoft Hyper-V

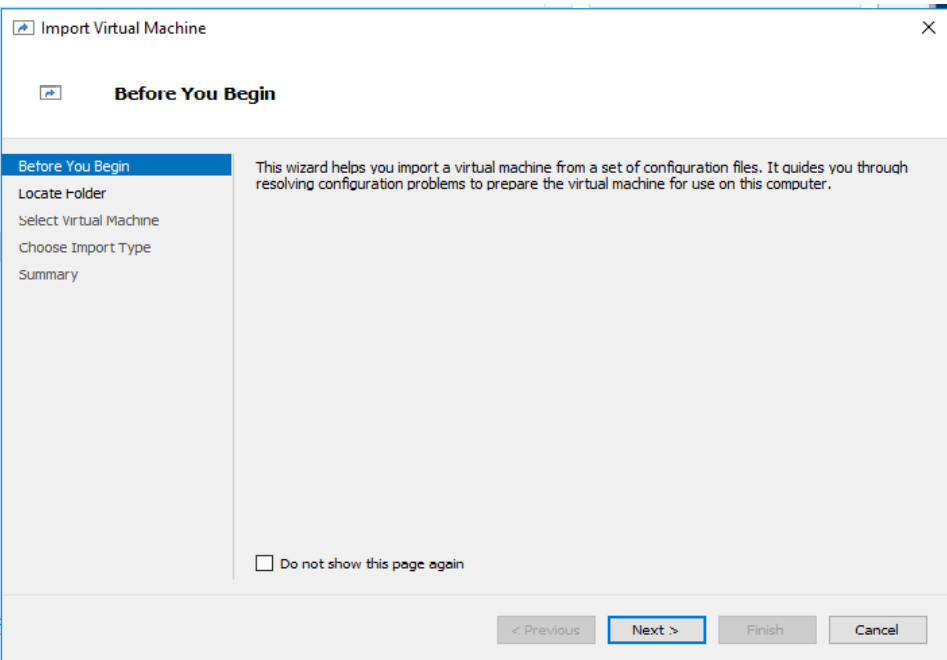
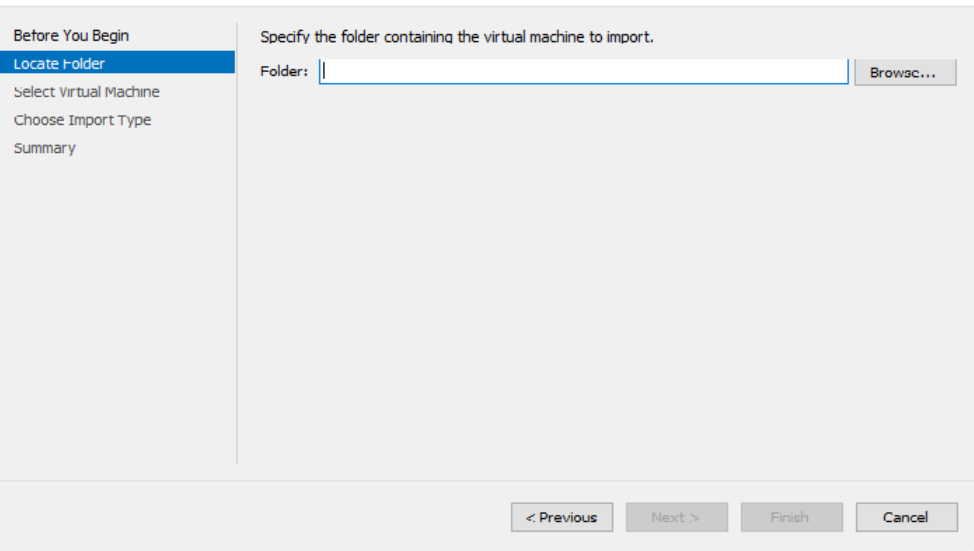
Step 1

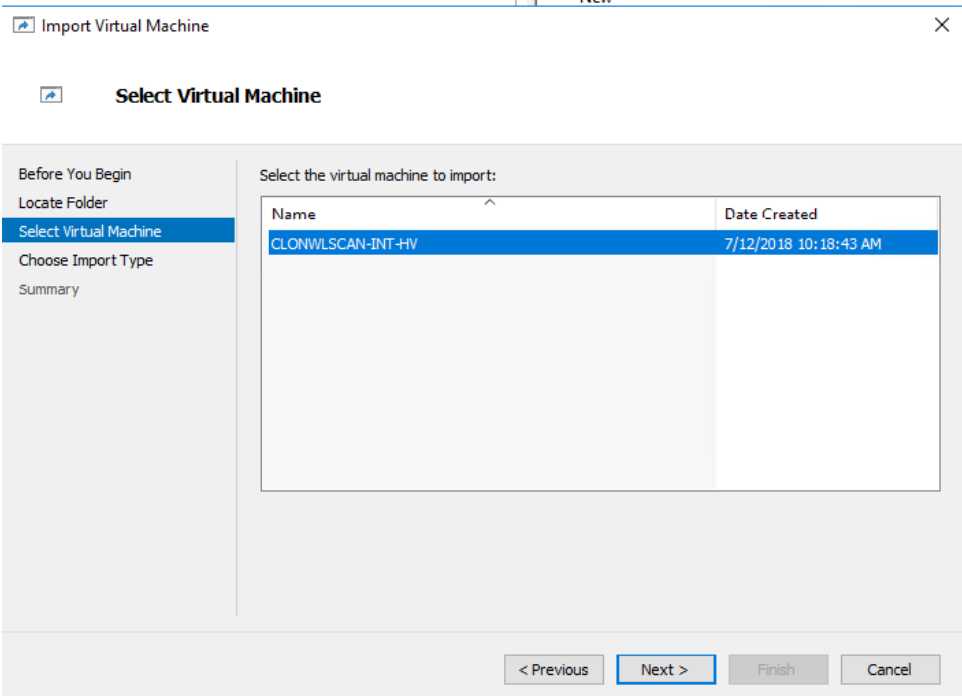
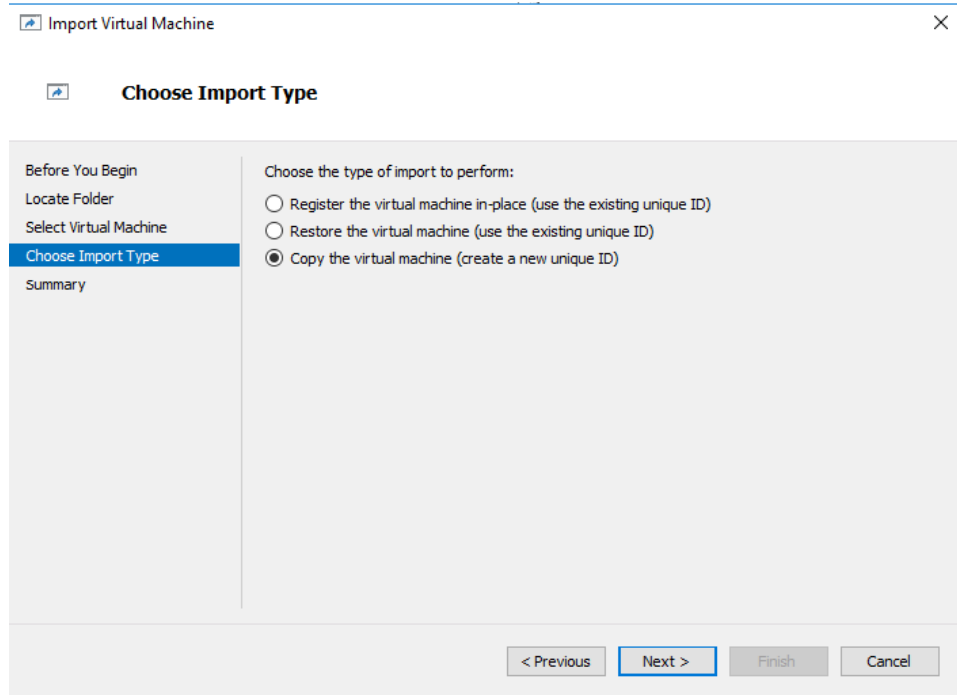
Start the Import Wizard

From the Hyper-V manager click **Import Virtual Machine** to begin the Import Wizard.





<p><b>Step 2</b></p> <p><b>Begin the Import Wizard</b></p>	<p>On the <b>Before You Begin</b> step click <b>Next</b>.</p> 
<p><b>Step 3</b></p> <p><b>Select Source for Internal Scanner</b></p>	<p>On the <b>Locate Folder</b> step select the <b>VM image</b> file for the Internal Scanner that you extracted from the Tarball and click <b>Next</b>.</p> 

<div>Step 4</div> <div>Select Internal Scanner</div>	<div>On the <b>Select Virtual Machine</b> step select the Internal Scanner and click <b>Next</b>.</div> <div></div>
<div>Step 5</div> <div>Choose Import Type</div>	<div>On the <b>Choose Import Type</b> select <b>Copy the virtual machine (create a new unique ID)</b> and then click <b>Next</b>.</div> <div></div>

**Step 6****Choose Destination for Internal Scanner**

On the **Choose Destination** step select the storage location for your environment and click **Next**.

The screenshot shows a window titled "Import Virtual Machine" with a close button (X) in the top right corner. Below the title bar is a section titled "Choose Folders for Virtual Machine Files". On the left is a sidebar with a list of steps: "Before You Begin", "Locate Folder", "Select Virtual Machine", "Choose Import Type", "Choose Destination" (highlighted in blue), "Choose Storage Folders", and "Summary". The main area contains the following text: "You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration." Below this is a checkbox labeled "Store the virtual machine in a different location" which is checked. There are three input fields, each with a "Browse..." button: "Virtual machine configuration folder:" (containing "C:\ProgramData\Microsoft\Windows\Hyper-V\"), "Checkpoint store:" (containing "C:\ProgramData\Microsoft\Windows\Hyper-V\"), and "Smart Paging folder:" (containing "C:\ProgramData\Microsoft\Windows\Hyper-V\"). At the bottom are four buttons: "< Previous", "Next >" (highlighted in blue), "Finish", and "Cancel".

**Step 7****Choose Destination for virtual hard disks**

On the **Choose Storage Folders** step select the destination for the virtual hard disks used by the Internal Scanner then click **Next**.

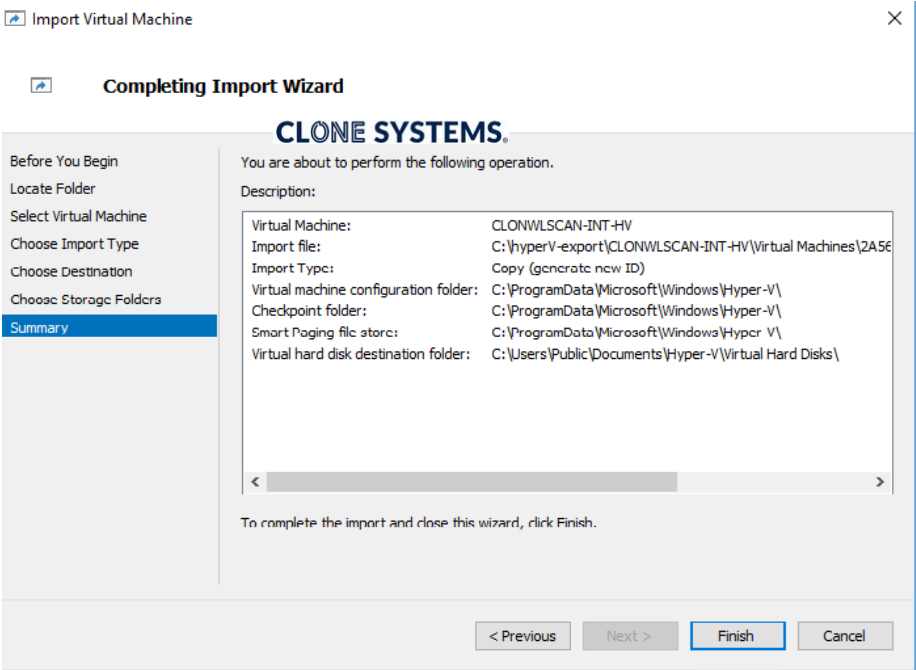
The screenshot shows a window titled "Import Virtual Machine" with a close button (X) in the top right corner. Below the title bar is a section titled "Choose Folders to Store Virtual Hard Disks". On the left is a sidebar with a list of steps: "Before You Begin", "Locate Folder", "Select Virtual Machine", "Choose Import Type", "Choose Destination", "Choose Storage Folders" (highlighted in blue), and "Summary". The main area contains the text: "Where do you want to store the imported virtual hard disks for this virtual machine?" Below this is a "Location:" label followed by an input field containing "C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\" and a "Browse..." button. At the bottom are four buttons: "< Previous", "Next >" (highlighted in blue), "Finish", and "Cancel".

Step 8

Review Import Settings  
and Import the Internal  
Scanner

On the **Summary** step review the configuration settings and click **Finish** to begin the import process.

**Note:** Once the Import has completed confirm your network settings for the Internal Scanner before powering it on.



# AWS MARKETPLACE

## Overview

The following will provide an overview of how to configure the Clone Systems Internal Scanner on AWS Marketplace.

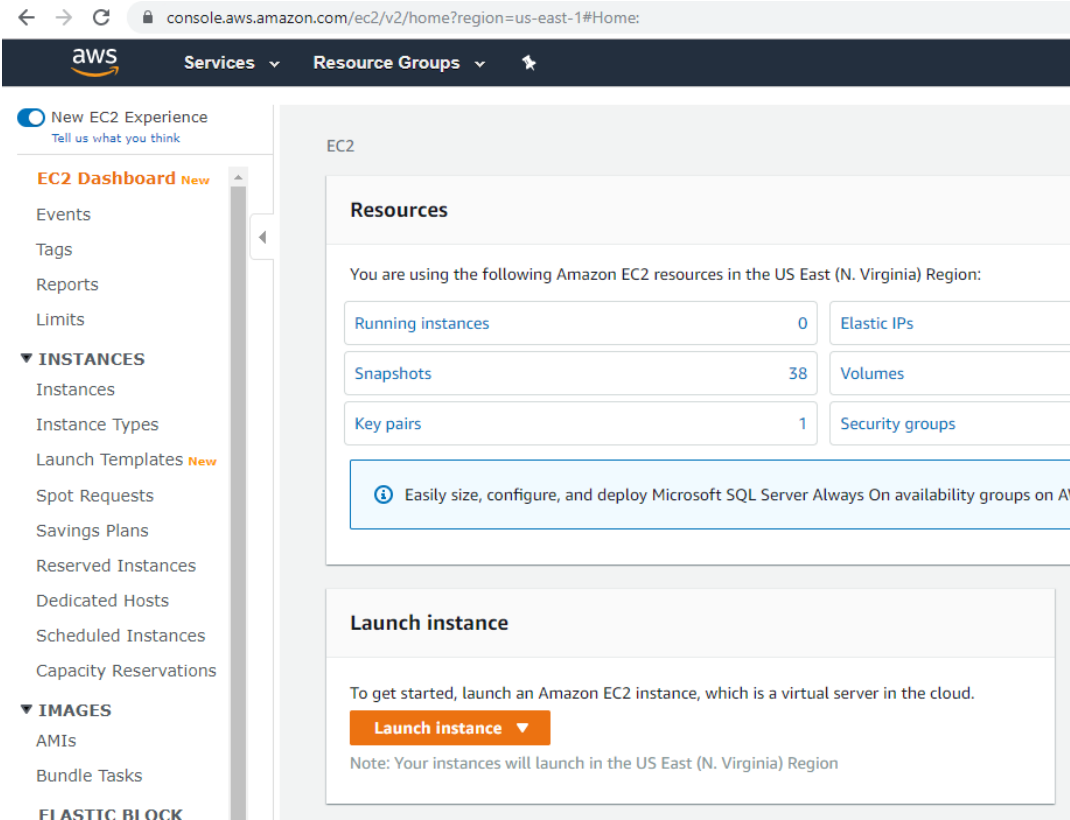
## Import the AWS Security Scanner

Steps for Importing the Security Scanner from AWS Marketplace

Step 1

Open Console

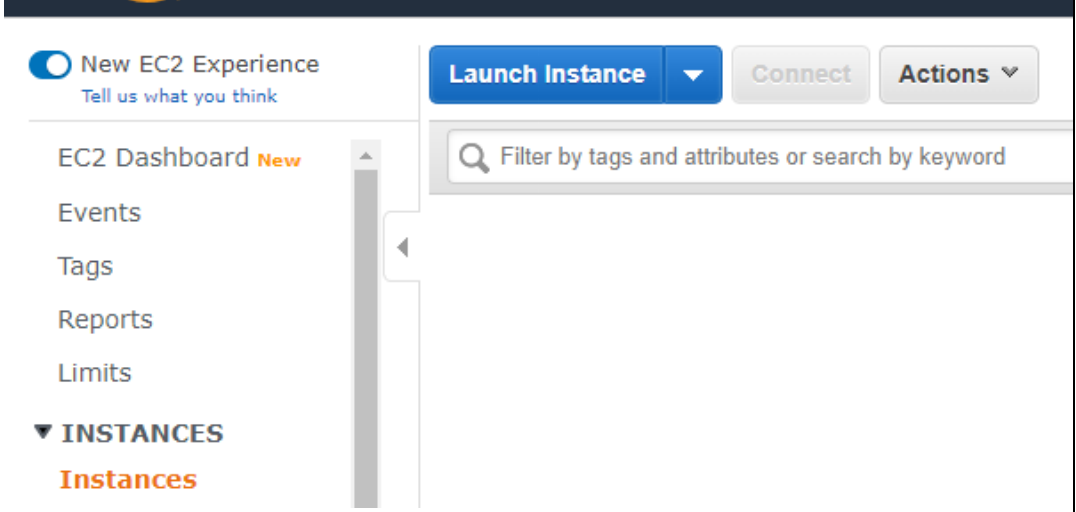
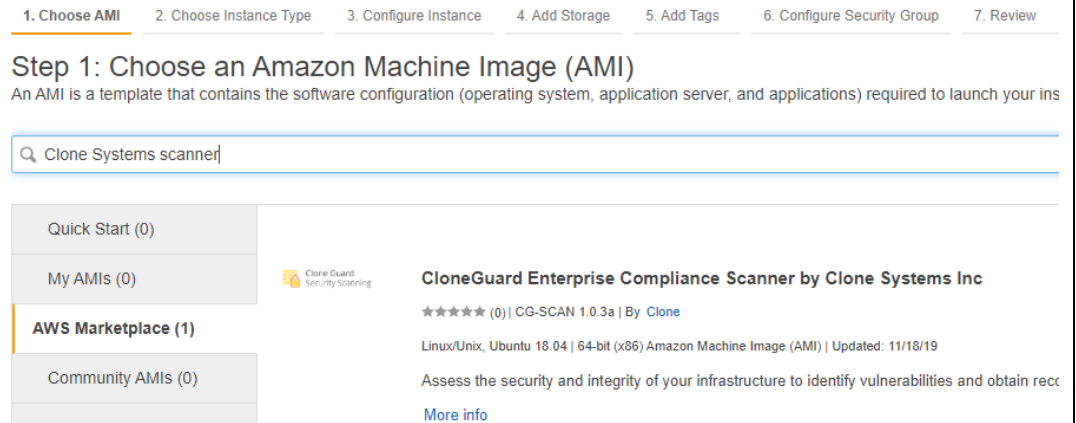
Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>



© 1998 – 2024 Clone Systems, Inc.

Properly Secure Your Business Network

CLONE SYSTEMS.

<p><b>Step 2</b></p> <p><b>Launch Instance</b></p>	<p>From the Amazon EC2 dashboard, choose <b>Instance</b> and then <b>Launch Instance</b>.</p>  <p>The screenshot shows the Amazon EC2 dashboard. On the left, there is a navigation menu with options: EC2 Dashboard (marked as 'New'), Events, Tags, Reports, Limits, and INSTANCES (expanded to show 'Instances'). On the right, there is a 'Launch Instance' button, a 'Connect' button, and an 'Actions' dropdown menu. Below these buttons is a search bar with the text 'Filter by tags and attributes or search by keyword'.</p>
<p><b>Step 3</b></p> <p><b>Choose AMI</b></p>	<p>On the <b>Choose an Amazon Machine Image (AMI)</b> page, choose the <b>AWS Marketplace</b> category on the left and search for <b>Clone Systems Scanner</b> and click on <b>Select</b></p>  <p>The screenshot shows the 'Choose an Amazon Machine Image (AMI)' page. At the top, there is a progress bar with seven steps: 1. Choose AMI (selected), 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. Below the progress bar, the title 'Step 1: Choose an Amazon Machine Image (AMI)' is displayed, followed by a description: 'An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your ins'. A search bar contains the text 'Clone Systems scanner'. On the left, there is a list of categories: Quick Start (0), My AMIs (0), AWS Marketplace (1), and Community AMIs (0). The 'AWS Marketplace (1)' category is selected. On the right, the search results for 'CloneGuard Enterprise Compliance Scanner by Clone Systems Inc' are shown, including a star rating, version number (CG-SCAN 1.0.3a), and a 'More info' link.</p>
<p><b>Step 4</b></p> <p><b>Continue</b></p>	<p>A dialog displays an overview of the product you've selected. You can view the pricing information, as well as any other information that the vendor has provided. When you're ready, choose <b>Continue</b>.</p>

Step 5  
Choose Instance Type

On the **Choose an Instance Type** page, select the hardware configuration and size of the instance to launch. When you're done, choose **Next: Configure Instance Details**. The t2.large should work for most environments. You can always the instance at a later date. Click on **Review and Launch**

Currently selected: t2.large (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 8 GiB memory, EBS only)  
Note: The vendor recommends using a t2.large instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)
<input type="radio"/>	General purpose	t2.nano	1	0.5	EBS only
<input type="radio"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only
<input type="radio"/>	General purpose	t2.small	1	2	EBS only
<input type="radio"/>	General purpose	t2.medium	2	4	EBS only
<input checked="" type="radio"/>	General purpose	t2.large	2	8	EBS only
<input type="radio"/>	General purpose	t2.xlarge	4	16	EBS only
<input type="radio"/>	General purpose	t2.2xlarge	8	32	EBS only

Step 6  
Launch Instance

Choose **Launch** to select or create a key pair, and launch your instance

Step 7: Review Instance Launch  
Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

CloneGuard Enterprise Compliance Scanner by Clone Systems Inc

Root Device Type: ebs    Virtualization type: hvm

Hourly Software Fees: \$0.00 per hour on t2.large instance. Additional taxes or fees may apply. Software charges will begin once you launch this AMI and continue until you terminate the instance.

By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.large	Variable	2	8	EBS only	-	Low to Moderate

Security Groups

Security group name    CloneGuard Enterprise Compliance Scanner by Clone Systems Inc-CG-SCAN 1-0-3a-AutogenByAWSMP-

Cancel    Previous    Launch

<div><div>Step 6</div><div>Create Key Pair and Download</div></div>	<div>Create the key pair and download it so you can use it in the next section. Select <b>Launch Instances</b> once you’ve download the key pair</div> <div><div><div>Select an existing key pair or create a new key pair</div><div><p>A key pair consists of a <b>public key</b> that AWS stores, and a <b>private key file</b> that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.</p><p>Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about <a href="#">removing existing key pairs from a public AMI</a>.</p><div><div>Create a new key pair</div><div><div>Key pair name</div><div>security scanner key pair</div></div><div>Download Key Pair</div></div><div><div><div>You have to download the <b>private key file</b> (*.pem file) before you can continue. <b>Store it in a secure and accessible location.</b> You will not be able to download the file again after it's created.</div></div></div><div><div>Cancel</div><div>Launch Instances</div></div></div></div></div>
---	--

Configure the AWS Security Scanner

Steps for Importing the Internal Scanner into AWS Marketplace	
<div><div>Step 1</div><div>Connect to the instance</div></div>	<div>After deployment, you will need the <b>key pair</b>, created above during the EC2 setup, and the Elastic IP of the instance, to connect the instance.</div> <div>The box is Ubuntu-based, so you will need to use SSH to access the box.</div> <div><b>Note:</b> if you are using putty, please follow the instructions in the link below on converting the keypair, for putty compatibility.</div> <div><a href="https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html">https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html</a></div>



	<p>The username is <b>ubuntu</b>.</p> <p>The example below is using the default OpenSSH client that comes with Windows 10 (1809 and above).</p> <pre>C:\aws&gt;ssh -l ubuntu -i linuxtest.pem 34.234.93.101</pre> <p>After logging you will be presented with a menu similar to the below menu:</p> <pre>Clone Systems - Appliance Setup Menu 1.0.3 1. Configure Network (LAN) Interface 2. Configure Connectivity to the Manager 3. Reboot Appliance 4. Shutdown Appliance 5. Change Password 6. Troubleshooting Tools 7. Setup Clone SOC Access 8. Exit Menu Enter choice [1 - 8]:</pre>
<p><b>Step 2</b></p> <p><b>Configure Network Settings</b></p>	<p>The first step is to configure your network settings (IP/subnet/gateway/DNS). To configure the network settings, select 1 from the text menu and press <b>Enter</b>. The settings default to DHCP, which the AWS default.</p> <p>This new menu will also display your current configuration. If you need to update this, you can choose option 1 for DHCP (which is selected by default), option 2 will allow you to set a static IP, or option 3 to return to the main menu.</p> <pre>Current IP address configuration: Address type: DHCP IP address: 172.31.14.88 Subnet mask: 255.255.240.0 Gateway: 172.31.0.1 Broadcast: 172.31.15.255 Nameservers: 127.0.0.53  1. Configure Interface for DHCP 2. Configure Interface with Static IP 3. Return to Main Menu Please choose an option [1 - 3]:</pre> <p>Setting a Static IP address</p> <p>To set a static IP address select option The IP Address must be in dotted decimal format (Example: 192.168.1.20) and then press <b>Enter</b>.</p>

```
=====
Current IP address configuration:

```

```
IP address: 192.168.1.20
Subnet mask: 255.255.255.0
Gateway: 192.168.1.1
Network: 192.168.1.0
Broadcast: 192.168.1.255
Nameservers: 192.168.1.1 4.2.2.2
=====
```

```
Please enter the IP address you would like to configure, (Format 192.168.1.2):
```

The second prompt will ask you to enter your subnet mask which must be in dotted decimal format (Example: 255.255.255.0) and then press **Enter**.

```
Please enter the subnet mask you would like to configure, (Format 255.255.255.0): 255.255.255.128
```

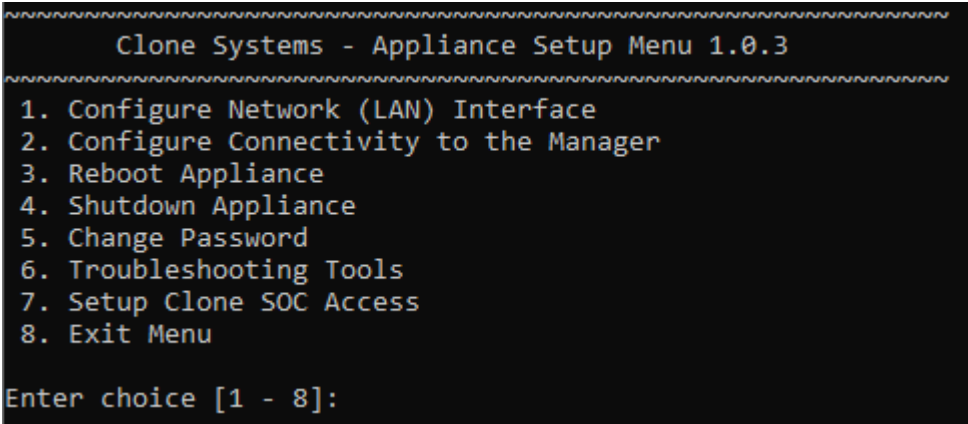
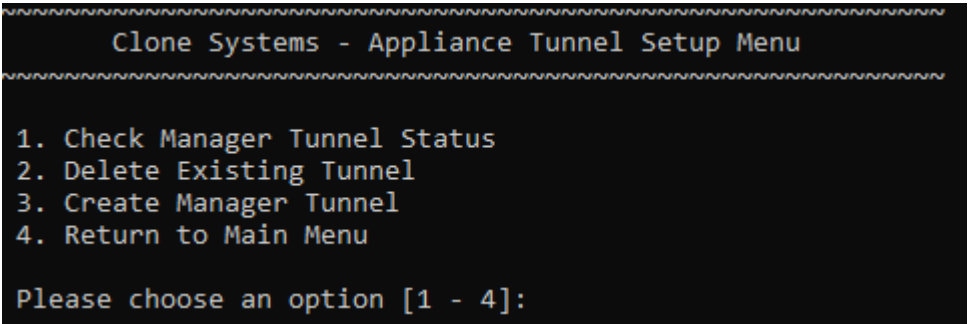
The third prompt will ask you to enter your gateway address which must be in dotted decimal format (Example: 192.168.1.1) and then press **Enter**.

```
Please enter the gateway you would like to configure, (Format 192.168.1.1): 192.168.0.1_
```

The fourth prompt will ask you to enter your DNS servers. Typically, you will configure your internal DNS servers that exist within your infrastructure. If you do not have a DNS server you can use the free open DNS servers 8.8.8.8 and 4.2.2.2. Note: The DNS IP address need to be in dotted decimal format and the DNS servers need to be separated by a space (Example: 8.8.8.8 4.2.2.2) and then press **Enter**.

```
Please enter the dns servers you would like to configure, (Format 4.2.2.2 8.8.8.8): 8.8.8.8 4.2.2.2
```

The last prompt will display the new Network configuration and ask you to confirm the changes. Enter **y** for Yes after which the Internal Scanner will be rebooted within one minute or **n** for No. After applying the new configuration, you may need to exit out of the current session and re-establish the connect with the newly configured IP address.

<p><b>Step 3</b></p> <p><b>Configure Clone Access Keys</b></p>	<p>The next step is to configure the clone access keys need for the secure tunnel to be establish between the scanning front end and the virtual scanner. From the main menu select option 7, this will take about a minute to complete and exit to the main menu</p> 
<p><b>Step 4</b></p> <p><b>Configure Connectivity to the Manager (scanning front-end)</b></p>	<p>Before you begin this step, you will need to make sure your instance access SSH access (TCP port 22) to the scanning front end (the address will vary between on your front end, it will be in the (38.126.154.0/24 or 38.123.140.0/25 IP blocks). You will also need the setup email from the front end, in this email it will provide you with URL for the manager, username, key (aka password), mgmt. port, and scanner port. If you do not have this email you will need to complete the New scanner setup in the front end.</p> <p>To begin select option 2 Configure connectivity to the manager, it will clear the screen and present you will the new menu. Option 1 will display the current tunnel status, option 2 will delete the tunnel, and option 3 will create the tunnel and option 4 will return you to the main menu. Select option 3 and press <b>Enter</b> to continue.</p>  <p>You will be prompted for the information from the email, first it will ask for the URL you can put the address in as either a dns name (if you have dns configured) or by IP address for example pciscan.clone-systems.com or 38.123.140.80, then press <b>Enter</b>. It will now prompt you for a username enter the username and press <b>Enter</b>. It will now prompt you for the key please note that the key will not be displayed on the screen, you will now be asked for the management port and scanner port, press <b>Enter</b> after entering each. **Please note the below screenshot is an example</p>

only do not use these values.

```
Please enter the Scanning Portal URI: pciscan.clone-systems.com
Please enter the user name:csadmin-oRg
Please enter the key (you will not see any characters):
Please enter the Managment Port: 29377
Please enter the Scanner Port: 29376
```

This will take a few minutes to complete the tunnel setup, when it is finish you will be presented with the screen with a lot of information, what you want to look for the tunnel\_alive : true, this means that the tunnel is connected and activity, \*\*Please note the values on the screenshot are for example only

```
{
  "data": {
    "bind_address": null,
    "uuid": "013462a0-6fa7-4593-a95f-c0695b6de259",
    "tunnel_pid": "12385",
    "stdout_find_pids": [
      "cg_foun+ 12373  0.0  0.0  4528  1092 ?        Ss   13:54   0:00 /usr/lib/autossh/autossh -M 0 -N -o ExitOnFo
wardFailure yes -o ServerAliveInterval 30 -o ServerAliveCountMax 2 -o StrictHostKeyChecking=no -A csadmin-oRgy@pciscan.
clone-systems.com -R 29376:localhost:9390 -R 29377:localhost:22",
      "cg_foun+ 12385  0.0  0.0  174248  5932 ?        S    13:54   0:00 /usr/bin/ssh -N -o ExitOnForwardFailure yes -
o ServerAliveInterval 30 -o ServerAliveCountMax 2 -o StrictHostKeyChecking=no -A -R 29376:localhost:9390 -R 29377:localh
ost:22 csadmin-oRgy@pciscan.clone-systems.com"
    ],
    "autossh_pid": "12373",
    "tunnel_alive": true,
    "running": true,
    "name": "Tunnel-2pciscan.clone-systems.com"
  }
}
Press [Enter] key to continue...
```

Press **Enter** this will take you to the main menu, if you want to double check the tunnel status, you can return the main, by selecting option 2, then option 1 Check Manger Tunnel Status. \*\* Please note that the screenshot below is for an example only and your output may different and may not be in color.

```
~~~~~
Clone Systems - Appliance Tunnel Setup Menu
~~~~~

1. Check Manager Tunnel Status
2. Delete Existing Tunnel
3. Create Manager Tunnel
4. Return to Main Menu

Please choose an option [1 - 4]: 1

Current Tunnel Listing:
Tunnel Number 1 ):
{
  "name": "Tunnel-2pciscan.clone-systems.com",
  "uuid": "013462a0-6fa7-4593-a95f-c0695b6de259",
  "running": true
}

Press [Enter] key to continue...
```

You are now ready to start your scanning; this is done on the front-end. If you have issues or questions please let us know at [esupport@clone-systems.com](mailto:esupport@clone-systems.com).

(Optional)

Step 6

Deleting the Tunnel

If you are finished and want to delete the tunnel to the manger, you will select option 2, then select option 2 to delete the tunnel. It will prompt you for which tunnel you will like to delete (typically there will only be one tunnel, tunnel 1, but there could be multiple tunnels depending on the configurations). Select the tunnel number you want to delete (typically it is 1), from the display the press **Enter**, it will prompt you to make sure you want to delete the tunnel, when the tunnel is deleted you will not be able to use this scanner to do scanning, press **Y** for yes or **N** or No.

```
Clone Systems - Appliance Tunnel Setup Menu

1. Check Manager Tunnel Status
2. Delete Existing Tunnel
3. Create Manager Tunnel
4. Return to Main Menu

Please choose an option [1 - 4]: 2

Current Tunnel Listing:
Tunnel Number 1 ):
{
  "name": "Tunnel-2pciscan.clone-systems.com",
  "uuid": "013462a0-6fa7-4593-a95f-c0695b6de259",
  "running": true
}

Which tunnel do you want to delete? (Select 1-1): 1

You are about to delete the tunnel with uuid: 013462a0-6fa7-4593-a95f-c0695b6de259.
are you sure (y/n) ?
```

The command will take a minute or two to complete, you will then give you a status, a status of true mean the tunnel was torn down and delete, a status of false mean something went wrong, if this happen please try again, and if it persist please contact support at [esupport@clone-systems.com](mailto:esupport@clone-systems.com).

```
You are about to delete the tunnel with uuid: 013462a0-6fa7-4593-a95f-c0695b6de259.
are you sure (y/n) ?y
yes
{
  "status" : true
}
```


You will be returned to the main menu, after a few seconds.

# AZURE MARKETPLACE

## Overview

The following will provide an overview of how to configure the Clone Systems Internal Scanner on AWS Marketplace.

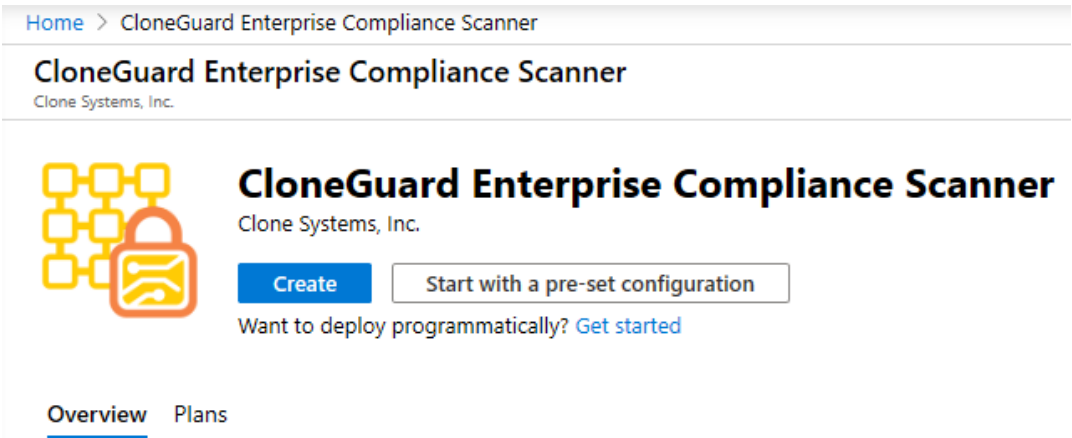
## Import the AZURE Security Scanner

Steps for Importing the Security Scanner from AZURE Marketplace	
<div>Step 1</div> <div>Open Console</div>	<div>Login to your Microsoft Azure account, and go to the marketplace using the following link: <a href="https://azuremarketplace.microsoft.com/en-us/marketplace/apps/clone-systems.cg-entscan1?tab=Overview">https://azuremarketplace.microsoft.com/en-us/marketplace/apps/clone-systems.cg-entscan1?tab=Overview</a></div> <div>You will see the Clone Enterprise Compliance Scanner</div> <div><div></div><div><div>CloneGuard Enterprise Compliance Scanner</div><div>Clone Systems, Inc.</div><div>★★★★★ (0) <a href="#">Write a review</a></div><div><div>Overview</div><div>Plans + Pricing</div><div>Reviews</div></div><div><div>GET IT NOW</div></div><div><div>Pricing information</div><div><a href="#">Bring your own license</a></div><div>+ Azure infrastructure costs</div></div></div><div><div>Enterprise Compliance Scanner for Clone Systems CloneGuard</div><div>With the CloneGuard Enterprise Compliance scanner you can perform network scanning and compliance scanning scanner supports PCI Compliance scanning, Vulnerability scanning and Pentest scanning</div></div></div>

Step 2

Deploy the AZURE Scanner

Click the Get it Now button, and it will bring up the Create Screen



Once you click Create, the Create a virtual Machine wizard will appear. Assign the VM to a resource group or create a new resource group. In the Instance Details section fill out the virtual machine name and select the region and availability option that your organization uses, leave the image as CloneGuard Enterprise Compliance Scanner, and the default size is



the minimum recommended.

[Home](#) > [CloneGuard Enterprise Compliance Scanner](#) > [Create a virtual machine](#)

### Create a virtual machine

**Basics**   Disks   Networking   Management   Advanced   Tags   Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own image.  
Complete the Basics tab then Review + create to provision a virtual machine with default parameters and customization.

#### Project details

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

Subscription \* ⓘ

Resource group \* ⓘ

Micro[REDACTED]

main[REDACTED]

[Create new](#)

#### Instance details

Virtual machine name \* ⓘ

Region \* ⓘ

Availability options ⓘ

Image \* ⓘ

Azure Spot instance ⓘ

Size \* ⓘ

cgent-scanner

(US) East US

No infrastructure redundancy required

CloneGuard Enterprise Compliance Scanner

[Browse all public and private images](#)

☐ Yes

☒ No

**Standard D2s v3**

2 vcpus, 8 GiB memory (\$70.08/month)

[Change size](#)

Administrator account

Authentication type ⓘ

☐ SSH public key

☒ Password

Under the Administrator Account section, select Password as the Authentication type, then enter the username and password for management of the box. Click Next to move to Disk selection.

<div>Step 3</div> <div>Finish VM Deployment</div>	<p>The Disk Section is next, we do not require any changes to this section, please click next and move to the networking section.</p> <p>In the networking section of the Create VM wizard, you can select your network options, the scanner requires SSH access (TCP/22) out bound to your scanning web interface (such as <a href="https://pciscan.clone-systems.com">pciscan.clone-systems.com</a>).</p>
---	---

[Home](#) > [CloneGuard Enterprise Compliance Scanner](#) > [Create a virtual machine](#)

## Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Define network connectivity for your virtual machine by configuring network interface card (NIC) ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \*

Default

Create new

Subnet \*

default

Manage subnet configuration

Public IP

(new) cgent-scanner-ip

Create new

NIC network security group

☐ None

☐ Basic

☒ Advanced

**i** This VM image has preconfigured NSG rules

Configure network security group \*

(new) cgent-scanner-nsg

Create new

Accelerated networking

☐ On

☒ Off

The selected image does not support accelerated networking.

### Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution.

Place this virtual machine behind an existing load balancing solution?

☐ Yes

☒ No

[Review + create](#)

[< Previous](#)

[Next : Management >](#)

Click Next to move to the Management section, it is setup to allow default SSH in bound for management, keep the default settings, if you require an advanced or tag setting you can continue to those sections, they are not required for this image, after you have your settings click Review + Create.

AZURE VM wizard will now validate the image and configuration setting, this may take several minutes, when this is complete you will receive the validation passed screen, you can now click create

[Home](#) / [Clonerguard Enterprise Compliance Scanner](#) / [Create a virtual machine](#)

## Create a virtual machine

✓ Validation passed

Basics Disks **Networking** Management Advanced Tags Re

## PRODUCT DETAILS

## CloneGuard Enterprise Compliance Scanner

by Clone Systems, Inc.

[Terms of use](#) | [Privacy policy](#)

Not covered by credits ⓘ

0.0000 USD/hr

Standard D2s v3

by Microsoft

[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ

0.0960 USD/hr

### Pricing for other VM sizes

**TEDMAC**

Your Deployment is now in queue and you will receive updates on it progress, the time will vary.

- ■ ■ Your deployment is underway



Deployment name: CreateVm-clone-systems.cg-entscan1-entsc1-2...




Subscription: [REDACTED]

Resource group: [REDACTED]

Start time: 3/24/2020, 2:41:42 PM

Correlation ID: [REDACTED]

Deployment details (Download)

Resource	Type	Status	Operation details
 <a href="#">cgent-scanner604</a>	Microsoft.Network/networkInterfaces	Created	<a href="#">Operation details</a>
 <a href="#">cgent-scanner-nsg</a>	Microsoft.Network/networkSecurityGrou...	OK	<a href="#">Operation details</a>
 <a href="#">cgent-scanner-ip</a>	Microsoft.Network/publicIpAddresses	OK	<a href="#">Operation details</a>

When the deployment is complete you can select the Go to resource button to go directly to the overview page for the newly created VM.

✓

Your deployment is complete

Deployment name: CreateVm-clone-systems.cg-entscan1-entsc1-2...

Subscription: [REDACTED]

Resource group: [REDACTED]

Start time: 3/24/2020, 2:41:42 PM

Correlation ID: [REDACTED]

Deployment details (Download)

Next steps

Setup auto-shutdown Recommended

Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

Go to resource

From the overview page you will see the status of the VM, and current IP address information. You will need the public address to initialize the new VM.

Connect

Start

Restart

Stop

Capture

Delete

Refresh

Resource group (change) : [REDACTED]

Status : Running

Location : East US

Subscription (change) : [REDACTED]

Subscription ID : [REDACTED]

Computer name : cgent-scanner

Operating system : Linux (ubuntu 18.04)

Size : Standard D2s v3 (2 vcpus, 8 GiB memory)

Azure Spot : N/A

Public IP address : [REDACTED]

Private IP address : 10.[REDACTED]

Public IP address (IPv6) : -

Private IP address (IPv6) : -

Virtual network/subnet : Default/default

DNS name : Configure

© 1998 – 2024 Clone Systems, Inc.

Properly Secure Your Business Network

CLONE SYSTEMS.

Configure the AZURE Security Scanner

Steps for Initializing AZURE Security Scanner	
<div>Step 1</div> <div>Connect to the instance</div>	<p>After deployment, you will need the public IP address, created above during the deployment.</p> <p>The box is Ubuntu-based, so you will need to use SSH to access the box.</p> <p>You will need to use the username and password you entered during deployment.</p> <p>After logging you will be presented with a menu similar to the below menu:</p> <div><pre> Clone Systems - Appliance Setup Menu 1.0.3 1. Configure Network (LAN) Interface 2. Configure Connectivity to the Manager 3. Reboot Appliance 4. Shutdown Appliance 5. Change Password 6. Troubleshooting Tools 7. Setup Clone SOC Access 8. Exit Menu Enter choice [1 - 8]: </pre></div>
<div>Step 2</div> <div>Configure Network Settings</div>	<p>The first step is to configure your network settings (IP/subnet/gateway/DNS). To configure the network settings, select 1 from the text menu and press <b>Enter</b>. The settings default to DHCP, which is the AZURE default.</p> <p>This new menu will also display your current configuration. If you need to update this, you can choose option 1 for DHCP (which is selected by default), option 2 will allow you to set a static IP, or option 3 to return to the main menu.</p> <div><pre> Current IP address configuration: Address type: DHCP IP address: 172.31.14.88 Subnet mask: 255.255.240.0 Gateway: 172.31.0.1 Broadcast: 172.31.15.255 Nameservers: 127.0.0.53 1. Configure Interface for DHCP 2. Configure Interface with Static IP 3. Return to Main Menu Please choose an option [1 - 3]: </pre></div>

### Setting a Static IP address

To set a static IP address select option The IP Address must be in dotted decimal format (Example: 192.168.1.20) and then press **Enter**.

```
=====
Current IP address configuration:
```

```
IP address: 192.168.1.20
Subnet mask: 255.255.255.0
Gateway: 192.168.1.1
Network: 192.168.1.0
Broadcast: 192.168.1.255
Nameservers: 192.168.1.1 4.2.2.2
=====
```

```
Please enter the IP address you would like to configure, (Format 192.168.1.2):
```

The second prompt will ask you to enter your subnet mask which must be in dotted decimal format (Example: 255.255.255.0) and then press **Enter**.

```
Please enter the subnet mask you would like to configure, (Format 255.255.255.0): 255.255.255.128
```

The third prompt will ask you to enter your gateway address which must be in dotted decimal format (Example: 192.168.1.1) and then press **Enter**.

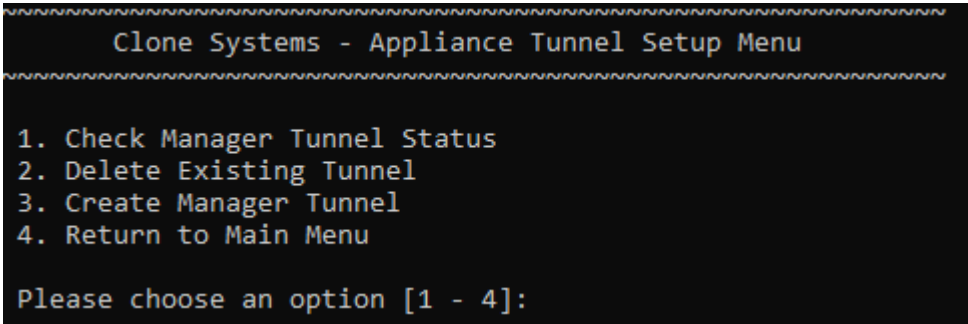
```
Please enter the gateway you would like to configure, (Format 192.168.1.1): 192.168.0.1_
```

The fourth prompt will ask you to enter your DNS servers. Typically, you will configure your internal DNS servers that exist within your infrastructure. If you do not have a DNS server you can use the free open DNS servers 8.8.8.8 and 4.2.2.2. Note: The DNS IP address need to be in dotted decimal format and the DNS servers need to be separated by a space (Example: 8.8.8.8 4.2.2.2) and then press **Enter**.

```
Please enter the dns servers you would like to configure, (Format 4.2.2.2 8.8.8.8): 8.8.8.8 4.2.2.2
```

The last prompt will display the new Network configuration and ask you to confirm the changes.

Enter **y** for Yes after which the Internal Scanner will be rebooted within one minute or **n** for No. After applying the new configuration, you may need to exit out of the current session and re-establish the connect with the newly configured IP address.

<p><b>Step 3</b></p> <p><b>Configure Connectivity to the Manager (scanning front-end)</b></p>	<p>Before you begin this step, you will need to make sure your instance access SSH access (TCP port 22) to the scanning front end (the address will vary between on your front end, it will be in the (38.126.154.0/24 or 38.123.140.0/25 IP blocks). You will also need the setup email from the front end, in this email it will provide you with URL for the manager, username, key (aka password), mgmt. port, and scanner port. If you do not have this email you will need to complete the New scanner setup in the front end.</p> <p>To begin select option 2 Configure connectivity to the manager, it will clear the screen and present you will the new menu. Option 1 will display the current tunnel status, option 2 will delete the tunnel, and option 3 will create the tunnel and option 4 will return you to the main menu. Select option 3 and press <b>Enter</b> to continue.</p>  <p>You will be prompted for the information from the email, first it will ask for the URL you can put the address in as either a dns name (if you have dns configured) or by IP address for example pciscan.clone-systems.com or 38.123.140.80, then press <b>Enter</b>. It will now prompt you for a username enter the username and press <b>Enter</b>. It will now prompt you for the key please note that the key will not be displayed on the screen, you will now be asked for the management port and scanner port, press <b>Enter</b> after entering each. **Please note the below screenshot is an example only do not use these values.</p>  <p>This will take a few minutes to complete the tunnel setup, when it is finish you will be presented with the screen with a lot of information, what you want to look for the tunnel_alive : true, this means that the tunnel is connected and activity, **Please note the values on the screenshot are for example</p>
---	---



only

```

{
  "data": {
    "bind_address": null,
    "uuid": "013462a0-6fa7-4593-a95f-c0695b6de259",
    "tunnel_pid": "12385",
    "stdout_find_pids": [
      "cg_fount+ 12373  0.0  0.0  4528  1092 ?          Ss   13:54   0:00 /usr/lib/autossh/autossh -M 0 -N -o ExitOnFo
wardFailure yes -o ServerAliveInterval 30 -o ServerAliveCountMax 2 -o StrictHostKeyChecking=no -A csadmin-oRgy@pciscan.
clone-systems.com -R 29376:localhost:9390 -R 29377:localhost:22",
      "cg_fount+ 12385  0.0  0.0  174248  5932 ?        S    13:54   0:00 /usr/bin/ssh -N -o ExitOnForwardFailure yes -
o ServerAliveInterval 30 -o ServerAliveCountMax 2 -o StrictHostKeyChecking=no -A -R 29376:localhost:9390 -R 29377:localh
ost:22 csadmin-oRgy@pciscan.clone-systems.com"
    ],
    "autossh_pid": "12373",
    "tunnel_alive": true,
    "running": true,
    "name": "Tunnel-2pciscan.clone-systems.com"
  }
}
Press [Enter] key to continue...

```

Press **Enter** this will take you to the main menu, if you want to double check the tunnel status, you can return the main, by selecting option 2, then option 1 Check Manger Tunnel Status. \*\* Please note that the screenshot below is for an example only and your output may different and may not be in color.

```

~~~~~
Clone Systems - Appliance Tunnel Setup Menu
~~~~~

1. Check Manager Tunnel Status
2. Delete Existing Tunnel
3. Create Manager Tunnel
4. Return to Main Menu

Please choose an option [1 - 4]: 1

Current Tunnel Listing:
Tunnel Number 1 ):
{
  "name": "Tunnel-2pciscan.clone-systems.com",
  "uuid": "013462a0-6fa7-4593-a95f-c0695b6de259",
  "running": true
}

Press [Enter] key to continue...

```

You are now ready to start your scanning; this is done on the front-end. If you have issues or questions please let us know at [esupport@clone-systems.com](mailto:esupport@clone-systems.com).

(Optional)

Step 4

Deleting the Tunnel

If you are finished and want to delete the tunnel to the manger, you will select option 2, then select option 2 to delete the tunnel. It will prompt you for which tunnel you will like to delete (typically there will only be one tunnel, tunnel 1, but there could be multiple tunnels depending on the configurations). Select the tunnel number you want to delete (typically it is 1), from the display the press **Enter**, it will prompt you to make sure you want to delete the tunnel, when the tunnel is deleted you will not be able to use this scanner to do scanning, press **Y** for yes or **N** or No.

```
Clone Systems - Appliance Tunnel Setup Menu

1. Check Manager Tunnel Status
2. Delete Existing Tunnel
3. Create Manager Tunnel
4. Return to Main Menu

Please choose an option [1 - 4]: 2

Current Tunnel Listing:
Tunnel Number 1 ):
{
  "name": "Tunnel-2pciscan.clone-systems.com",
  "uuid": "013462a0-6fa7-4593-a95f-c0695b6de259",
  "running": true
}

Which tunnel do you want to delete? (Select 1-1): 1

You are about to delete the tunnel with uuid: 013462a0-6fa7-4593-a95f-c0695b6de259.
are you sure (y/n) ?
```

The command will take a minute or two to complete, you will then give you a status, a status of true mean the tunnel was torn down and delete, a status of false mean something went wrong, if this happen please try again, and if it persist please contact support at [esupport@clone-systems.com](mailto:esupport@clone-systems.com).

```
You are about to delete the tunnel with uuid: 013462a0-6fa7-4593-a95f-c0695b6de259.
are you sure (y/n) ?y
yes
{
  "status" : true
}
```

You will be returned to the main menu, after a few seconds.

# INITIALIZE INTERNAL SCANNER

## Overview

The following will provide an overview of how to initialize the Internal Scanner for use with your Clone Systems Security Scanning solution.

**Note:** Please review the default settings detailed below before powering up the Internal Scanner as they may conflict with your existing Network environment. You can place the Internal Scanner in an isolated network / host only network connection which will provide you an opportunity to update the Network Settings that work best for your environment.




## Default Settings

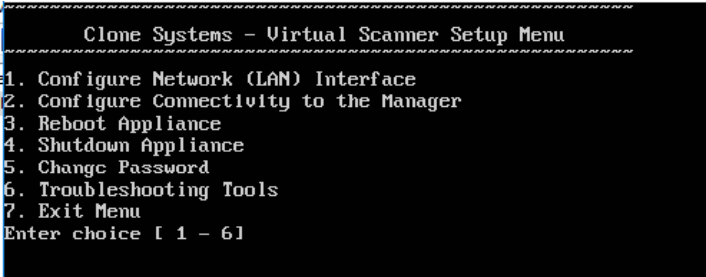
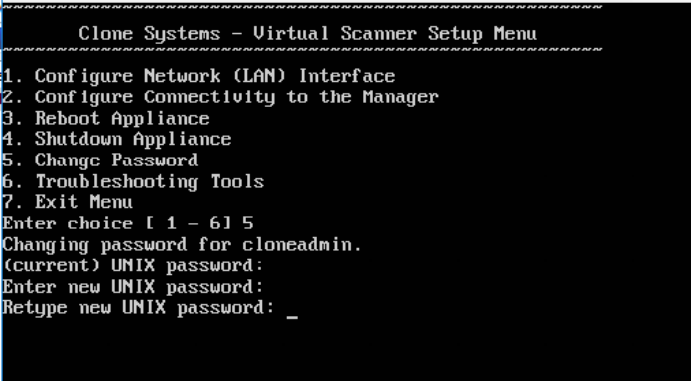
This Clone Systems Internal Scanner is shipped with default credentials and network settings. You should review this information and will likely need to change these settings so that you can use the Internal Scanner in your environment.

Internal Scanner Default Settings	
Default IP Address	192.168.1.20/24
Default Gateway	192.168.1.1
Default DNS	192.168.1.1 & 4.2.2.2
Default Username	cloneadmin
Default Password (This password is case sensitive)	CloneSy\$t3msScanner


Initialize the Internal Scanner


In order to complete the changes, you will need console access to the Internal Scanner.

Steps for Initializing the Internal Scanner	
<div>Step 1</div> <div>Adding the Scanner to the Front-End Portal</div>	<div><div>Log into your Clone Systems Partner Portal and navigate to the Scanners page.</div><div><div>Options ▾Admin ▾</div><div><div>Targets</div><div>Schedules</div><div>Notifications</div><div>Exceptions</div><div>Credentials</div><div>Port Lists</div><div>Scanners</div></div></div><div><div>Note:</div> If you do not see this button, please verify that you are using the correct service.</div><div><div><div><div></div><div></div><div></div></div></div><div><div>If you still do not see it, then your account has not been given permission to scan internally. Please contact the Clone Systems Security Operation Center at <a href="mailto:esupport@clone-systems.com">esupport@clone-systems.com</a> or <b>1.800.414.0321</b> to update your account.</div><div>When on the Scanners page: click <b>New Scanner</b>, then select a <b>Name</b> for the Internal Scanner, and click <b>Create Scanner</b> (<b>comment</b> optional).</div><div><div>Note:</div> Once the Scanner has been created, Scanner Setup Info will be sent to your account’s email address.</div></div></div></div>

<div>Step 2</div> <div>Login to the Internal Scanner from the Console</div>	<p>After configuring the Network settings within your Virtual Infrastructure, start the Internal Scanner.</p> <p>Access the Internal Scanner via a console session and at the Ubuntu login prompt login with the default username <b>cloneadmin</b> and password <b>CloneSy\$t3msScanner</b></p>
<div>Step 3</div> <div>Change the Default Password</div>	<p>Upon logging into the Internal Scanner, you will be presented with a text-based menu system to complete the initialization of the Internal Scanner.</p> <div></div> <p>Enter choice 5 to change the default password. You will be prompted to enter the current password which is the default password <b>CloneSy\$t3msScanner</b> and then prompted to enter a new password twice.</p> <div></div> <p>Upon successfully changing the default password you will be returned to the main menu.</p> <p><b>Note:</b> There are no password recovery options. If you lose or forget the password you will need to reimport the Internal Scanner.</p>
<div>Step 3</div> <div>Configure your Network Interface</div>	<p>Choose Option 1 from the menu.</p> <p>This will clear the screen and present you with the current Network configuration and prompt you for a new IP address. The IP Address must be in dotted decimal format (Example: 192.168.1.20) and then press <b>Enter</b>.</p>

	<div><pre>===== Current IP address configuration: IP address: 192.168.1.20 Subnet mask: 255.255.255.0 Gateway: 192.168.1.1 Network: 192.168.1.0 Broadcast: 192.168.1.255 Nameservers: 192.168.1.1 4.2.2.2 =====  Please enter the IP address you would like to configure, (Format 192.168.1.2):</pre></div> <p>The second prompt will ask you to enter your subnet mask which must be in dotted decimal format (Example: 255.255.255.0) and then press <b>Enter</b>.</p> <div><pre>Please enter the subnet mask you would like to configure, (Format 255.255.255.0): 255.255.255.128</pre></div> <p>The third prompt will ask you to enter your gateway address which must be in dotted decimal format (Example: 192.168.1.1) and then press <b>Enter</b>.</p> <div><pre>Please enter the gateway you would like to configure, (Format 192.168.1.1): 192.168.0.1_</pre></div> <p>The fourth prompt will ask you to enter your DNS servers. Typically, you will configure your internal DNS servers that exist within your infrastructure. If you do not have a DNS server you can use the free open DNS servers 8.8.8.8 and 4.2.2.2. Note: The DNS IP address need to be in dotted decimal format and the DNS servers need to be separated by a space (Example: 8.8.8.8 4.2.2.2) and then press <b>Enter</b>.</p> <div><pre>Please enter the dns servers you would like to configure, (Format 4.2.2.2 8.8.8.8): 8.8.8.8 4.2.2.2</pre></div> <p>The last prompt will display the new Network configuration and ask you to confirm the changes. Enter <b>y</b> for Yes after which the Internal Scanner will be rebooted within one minute or <b>n</b> for No.</p> <div><pre>The following will be applied to the interface and the appliance will be rebooted IP Address: 192.168.0.12 Subnet Address: 255.255.255.128 Gateway Address: 192.168.0.1 Broadcast Address: 192.168.0.127 Network Address: 192.168.0.0 DNS servers: 8.8.8.8 4.2.2.2  Are you sure? (y/n)</pre></div>
Step 4	<p><b>Note:</b> Before executing this step, confirm that you have received the following information from Step 1:</p>

<p><b>Connect the Internal Scanner to your Clone Systems Security Scanning solution</b></p>	<ol style="list-style-type: none"> <li>1. The Clone Systems Security Scanning <b>Manager IP address</b> or <b>DNS name</b></li> <li>2. The <b>Password (Key)</b> for connecting the Clone Systems Security Scanning Manager</li> <li>3. The Clone Systems Security Scanning <b>Scanner Port</b></li> <li>4. The Clone Systems Security Scanning <b>Management Port</b></li> </ol> <p>Choose Option <b>2</b> will open up a menu for configuring the Internal Scanners Tunnel back to your Clone Systems Security Scanning solution.</p>  <p><b>1 – Check Manager Tunnel Status:</b> If selected will check the status of the tunnel. If no tunnel is configured it will return and error. When finished you can press <b>Enter</b> to return to the main menu.</p> <p><b>2 – Delete Existing Tunnel:</b> If selected will prompt you to confirm that you want to delete the tunnel. Enter <b>y</b> to delete the tunnel or <b>n</b> to cancel and return to the main menu.</p> <p><b>3 – Create Manager Tunnel:</b> If selected will prompt you for the information provided by the Clone Systems Security Operations Center. Start by selecting the type of appliance you are setting up which is the <b>Internal Scanner Appliance</b> so choose Option <b>1</b>. Next, you will be prompted for the Clone Systems Security Scanning <b>Manager IP address</b> or <b>DNS name</b>. Upon entering the Manager IP address or DNS name you will be prompted for the <b>Password (Key)</b>. Upon entering the Password, you will be prompted for the <b>Scanner Port</b> and then the <b>Management Port</b> for connecting the Clone Systems Security Scanning Manager.</p> <p>If the settings are correct the tunnel will be created and you will be returned to the main text-based menu system.</p> <p>At this point you should contact the Clone Systems Security Operation Center at <a href="mailto:esupport@clone-systems.com">esupport@clone-systems.com</a> or <b>1.800.414.0321</b> to verify the tunnel.</p> <p>Once the tunnel is verified by the Clone Systems Security Operation Center, you can use the Internal Scanner in your Clone Systems Security Scanning Solution.</p>
<p><b>Step 5</b></p>	<p>Choosing Option <b>7</b> will exit you from the text-based menu system and return you to the Ubuntu login prompt.</p>

Exit the text-based menu system	
(Optional)  Step 6  Troubleshooting	<p>Choosing Option <b>6</b> will open up a menu with troubleshooting tools. You will have the option to:</p> <p><b>1 – Auto Test:</b> If selected will run ping to the configured Gateway and NSLookup to cnn.com. When finished you can press <b>Enter</b> to return to the main menu.</p> <p><b>2 – Custom Ping:</b> If selected will prompt you for an IP address or DNS name to ping (Example: 192.168.0.12 or <a href="http://www.google.com">www.google.com</a>). It will execute a Ping test and output the results to the screen. When finished you can press <b>Enter</b> to return to the main menu.</p> <p><b>3 – Custom NSLookup:</b> If selected will prompt you for a DNS name to lookup and then attempt to return the IP address from NSLookup for the DNS name entered. When finished you can press <b>Enter</b> to return to the main menu.</p> <p><b>4 – Exit:</b> If selected this will exit you from the troubleshooting menu and return you to the main text-based menu system.</p> 



<div>(Optional)</div> <div>Step 7</div> <div>Rebooting and Shutting Down the Internal Scanner</div>	<p>Choosing Option <b>3</b> will ask you to confirm that you want to reboot the Internal Scanner.</p> <p>Choosing Option <b>4</b> will ask you to confirm that you want to shutdown the Internal Scanner.</p> <p>Enter <b>y</b> for yes or <b>n</b> for no and then press <b>Enter</b>.</p> <p><b>Note:</b> If you click <b>y</b> for yes, the Internal Scanner will reboot or shutdown within one minute depending on which menu option you selected.</p> <div></div>
<div>(Optional)</div> <div>Step 8</div> <div>Allowing users to use the internal scanner</div>	<p>If you want to allow your customer to use the scanner, you will have to set the necessary permissions by editing their organization. You will need to enable VRMS and/or Penetration Testing, then enable Internal VRMS and/or Internal Penetration respectively (example below).</p> <div><div>Exclude this Organization from the License Count (Unlimited Licenses)</div><div>Enabled</div></div> <div><div>Enable PCI for this Organization</div><div>Disabled</div></div> <div><div>Enable VRMS for this Organization</div><div>Enabled</div></div> <div><div>Enable Penetration Testing for this Organization</div><div>Disabled</div></div> <div><div>Settings</div><div>Internal VRMS</div><div>Enabled</div></div> <div><div>Internal Penetration</div><div>Disabled</div></div> <p><b>Note:</b> If they did not have permission to VRMS and/or Penetration Testing previously, you will have to add a license for each new service.</p>