



# VULSCAN

by RapidFire Tools



## INSTALLATION GUIDE

### VulScan Virtual Appliance

1/17/2024 2:53 PM



+1-678-323-1300



[rapidfiretools.com](http://rapidfiretools.com)



[support@rapidfiretools.com](mailto:support@rapidfiretools.com)

# Contents

---

<b>Purpose of this Guide</b> .....	<b>4</b>
<u>Important: VulScan and the Virtual Appliance</u> .....	4
<b>Virtual Appliance System Requirements</b> .....	<b>5</b>
<u>Hyper-V Installation System Requirements</u> .....	5
<u>VMware Installation System Requirements</u> .....	6
<u>Virtual Appliance Operational System Requirements</u> .....	6
<u>RapidFire Tools Server and Virtual Appliance Firewall Requirements</u> .....	6
<b>VulScan Installation Procedure for Hyper-V</b> .....	<b>8</b>
<u>Step 1 — Download and Run the Virtual Appliance Installer</u> .....	8
<u>Step 2 — Select Target</u> .....	10
<u>Step 3 — Verify that Installation Requirements are Met</u> .....	11
Overriding Disk Space Requirements .....	12
<u>Step 4 — Select Scanner Type</u> .....	14
<u>Step 5 — Enter the Network Detective Account Credentials</u> .....	15
Virtual Appliance ID Requirements .....	15
<u>Step 6 — Select Appliance ID Screen</u> .....	16
Record the Appliance ID for the Virtual Appliance Installation .....	17
<u>Step 7 — Download VMs</u> .....	18
<u>Step 8 — Select Folder to Install Virtual Appliance</u> .....	20
<u>Step 9 — Configure Required Virtual Switches</u> .....	21
Using an Existing External Virtual Switch .....	21
Creating and Selecting a new External Virtual Switch .....	22
<u>Step 10 — Define Network Settings</u> .....	23
Network Settings using DHCP .....	23
Network Settings using a Static IP Address .....	23
<u>Step 11 — Proxy Settings</u> .....	25

<u>Step 12 — Verify Settings Prior to Installation</u> .....	27
<u>Step 13 — Monitor Installation Progress Status</u> .....	28
<u>Step 14 — Confirm that Appliance Meets Operational Requirements</u> .....	30
<b>VulScan Installation Procedure for VMware</b> .....	<b>31</b>
<u>Step 1 — Download and Run the Virtual Appliance Installer</u> .....	31
<u>Step 2 — Select Target</u> .....	33
<u>Step 3 — Verification that Installation Requirements are Met</u> .....	34
<u>Step 4 — Select Scanner Type</u> .....	35
<u>Step 5 — Enter the Network Detective Account Credentials</u> .....	36
Virtual Appliance ID Requirements .....	36
<u>Step 6 — Select Appliance ID Screen</u> .....	36
Record the Appliance ID for the Virtual Appliance Installation .....	37
<u>Step 7 — Set VMware Server Credentials</u> .....	38
<u>Step 8 — Set VMware Server Settings</u> .....	39
<u>Step 9 — Set VMware Network Settings</u> .....	40
<u>Step 10 — Initiate the Download VM Process</u> .....	41
<u>Step 11 — View VM Download Progress and Install Package Status</u> .....	42
<u>Step 12 — Define Network Settings</u> .....	44
<u>Step 13 — Proxy Settings</u> .....	44
<u>Step 14 — Verify Settings Prior to Installation</u> .....	46
<u>Step 15 — Monitor Installation Progress Status</u> .....	47
<u>Step 16 — Confirm that Appliance Meets Operational Requirements</u> .....	48
<b>Discovery Agent Installation Procedure</b> .....	<b>49</b>
<u>Silent Install for Discovery Agent</u> .....	49
Uninstall Script for Discovery Agent .....	50

## Purpose of this Guide

This guide is intended for users of the RapidFire Tools Software Appliance for VulScan by RapidFire Tools. The appliance must be installed within a Microsoft Hyper-V or VMware environment to operate one or more of the Software Appliances.

The instructions here will guide you through: "[VulScan Installation Procedure for Hyper-V](#)" on page 8 and "[VulScan Installation Procedure for VMware](#)" on page 31.

Additional guides are available for Reporter and Inspector. This guide is designed to be used in conjunction with other supplementary guides available at <https://www.rapidfiretools.com/vs-downloads>.

## Important: VulScan and the Virtual Appliance

The **VulScan** product is ONLY compatible with the **Virtual Appliance**. You cannot use VulScan with the RapidFire Tools Server. VulScan performs internal vulnerability scans on the target network using the Virtual Appliance.

# Virtual Appliance System Requirements

The following is a list of computer and software system requirements that are necessary to INSTALL the **Virtual Appliance**:

## Hyper-V Installation System Requirements

### 1. Microsoft Hyper-V Enabled Server or Workstation Requirements:

- a. Microsoft Hyper-V enabled Windows Server 2012 or higher server operating system

OR

- b. Microsoft Hyper-V enabled Windows 8.1 Pro or higher server operating system

**Note:** Hyper-V Management Tools must be included when installing Hyper-V using the Windows Programs and Features option, or via the PowerShell on a Hyper-V Server Core installation.

2. **Recommended Virtual Memory Availability Requirement:** 8 GB of free and available Virtual Memory in the Hyper-V environment

3. **Recommended Disk Space Requirement:** 40 GB of free disk space

### 4. Recommended Processor for Dedicated and Non-Dedicated Systems Hyper-V Installations

- a. *Dedicated Microsoft Hyper-V System to run the Virtual Appliance*

**Recommendation:** Intel i5 or faster processor for dedicated deployments

- b. *Non-Dedicated Microsoft Hyper-V System used to run other guest instances and run the Virtual Appliance*

**Recommendation:** Intel Xeon class server processors capable for hosts running multiple instances

**Note:** These memory requirements are over and above the host machine's current memory requirements for Windows, Hyper-V, and any other application memory requirements that must be met by the host

machine.

## 5. Access to the Internet.

# VMware Installation System Requirements

## VMware System Requirements

The following is a list of system requirements that are necessary to INSTALL the Virtual Appliance on VMware:

**VMware Version:** ESXi 5.5 or higher

**Virtual Machine Memory:** 8 GB available

**Virtual Disk Size:** 40 GB

**Additional requirements include:** PowerCLI 6.3 and access to the Internet.

In order to be able to use the Virtual Appliance, the appliance must be licensed from RapidFire Tools for installation and use.

# Virtual Appliance Operational System Requirements

The following is a list of system requirements that are necessary to OPERATE the Virtual Appliance on Hyper-V or VMware.

Operational System Requirements:

- 16 GB Available RAM
- 40 GB Hard Drive Space

# RapidFire Tools Server and Virtual Appliance Firewall Requirements

MSP Partners and end customers using RapidFire Tools appliances (Server or Virtual Appliance) should configure the firewall rules on their networks to enable access to the following RapidFire Tools URLs. This list applies to all Servers and Virtual Appliances (Compliance Manager, Cyber Hawk, Reporter, and Inspector).

- [gatekeeper.rapidfiretools.com](http://gatekeeper.rapidfiretools.com)
- [go.rapidfiretools.com](http://go.rapidfiretools.com)

- [au.rapidfiretools.com](https://au.rapidfiretools.com)
- [go-eu.rapidfiretools.com](https://go-eu.rapidfiretools.com)
- [go-au.rapidfiretools.com](https://go-au.rapidfiretools.com)
- [wcflb.rapidfiretools.com](https://wcflb.rapidfiretools.com)
- [wcflb-eu.rapidfiretools.com](https://wcflb-eu.rapidfiretools.com)
- [wcflb-au.rapidfiretools.com](https://wcflb-au.rapidfiretools.com)
- [api.ndglue.com](https://api.ndglue.com)
- [networkdetective.s3.amazonaws.com](https://networkdetective.s3.amazonaws.com)
- [download.rapidfiretools.com](https://download.rapidfiretools.com)

The RapidFire Tools Server and Discovery Agent requires access to **port 443**.

The Virtual Appliance requires access to the Greenbone Community Feed at [feed.community.greenbone.net](https://feed.community.greenbone.net) using **port 873**.

# VulScan Installation Procedure for Hyper-V

To perform the installation of the **Virtual Appliance for Hyper-V**, follow the instructions below.

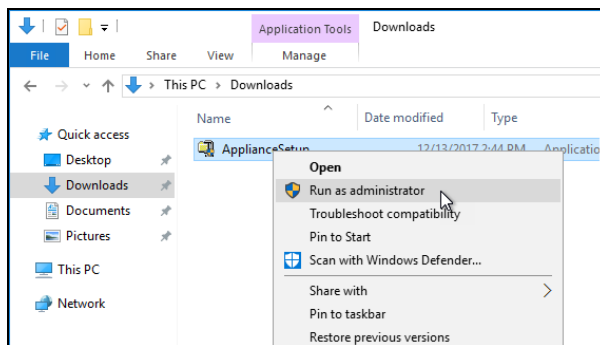
## Step 1 — Download and Run the Virtual Appliance Installer

The **Installer** file is a self-extracting ZIP file that is used to initiate the installation of the **Virtual Appliance** on the host system. To begin the installation procedure:

1. Download and run the **VulScan Virtual Appliance Installer** file at <https://www.rapidfiretools.com/vs-downloads>. The Installer file is named **VulnerabilityScannerSetup.exe**.

**Important:** Be sure to download the "Virtual Appliance Installer", and NOT the RapidFire Tools Server installer.

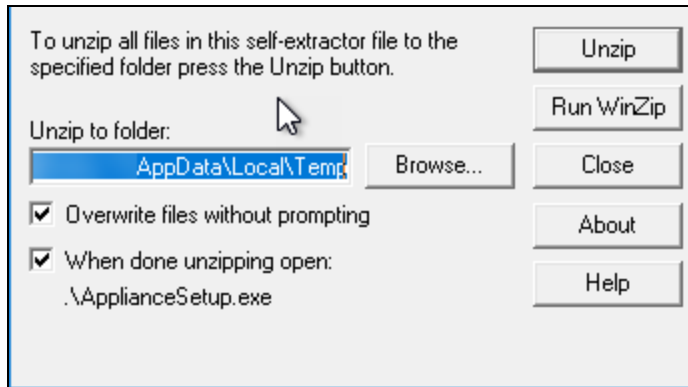
2. After downloading the installer, right click on **VulnerabilityScannerSetup.exe** and click **Run as Administrator**.



3. Use the **Unzip** option to unzip the files into a folder location of your choice and start



the installation program.



**Important:** You must have Administrator privileges and access rights in order to complete the installation process successfully.

## Step 2 — Select Target

1. Select the **Microsoft Hyper-V** option to install on a Hyper-V enabled system.

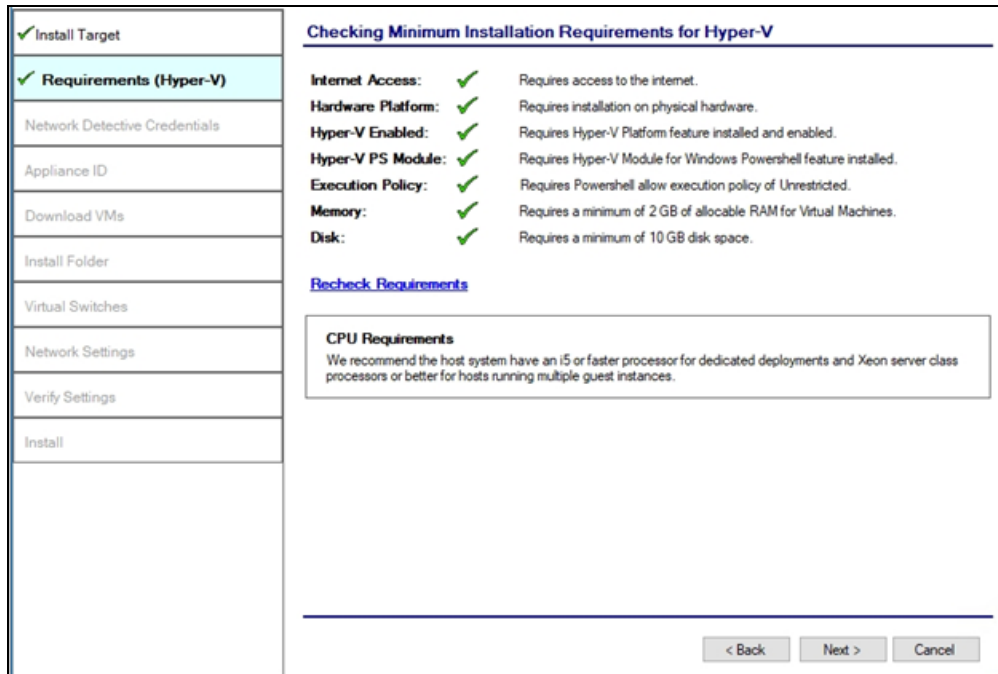
The screenshot displays the 'Install Target' configuration window. On the left, a vertical sidebar lists the installation steps, with 'Install Target' marked as complete. The main content area shows three radio button options for the installation target: 'Microsoft Hyper-V' (selected), 'vmware', and 'Manual Configuration (Advanced)'. The 'Microsoft Hyper-V' option is accompanied by the Windows logo and the text 'Microsoft Hyper-V'. The 'vmware' option is accompanied by the VMware logo. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

2. Click **Next**.

### Step 3 — Verify that Installation Requirements are Met

In this step, the installer checks to see if the host system meets the system requirements. These requirements include:

- Hyper-V enablement status
- minimum memory requirements necessary for installation
- amount of available disk space



If a particular requirement is not met, the installer will present an error status:

Requirement	Status	Description
Internet Access	✓	Requires access to the internet.
Hardware Platform	✓	Requires installation on physical hardware.
Hyper-V Enabled	✓	Requires Hyper-V Platform feature installed and enabled.
Hyper-V PS Module	✓	Requires Hyper-V Module for Windows Powershell feature installed.
Execution Policy	✓	Requires Powershell allow execution policy of Unrestricted.
Memory	✓	Requires a minimum of 2 GB of allocable RAM for Virtual Machines.
Disk	✗	Requires a minimum of 10 GB disk space.

[Recheck Requirements](#)

**CPU Requirements**  
We recommend the host system have an i5 or faster processor for dedicated deployments and Xeon server class processors or better for hosts running multiple guest instances.

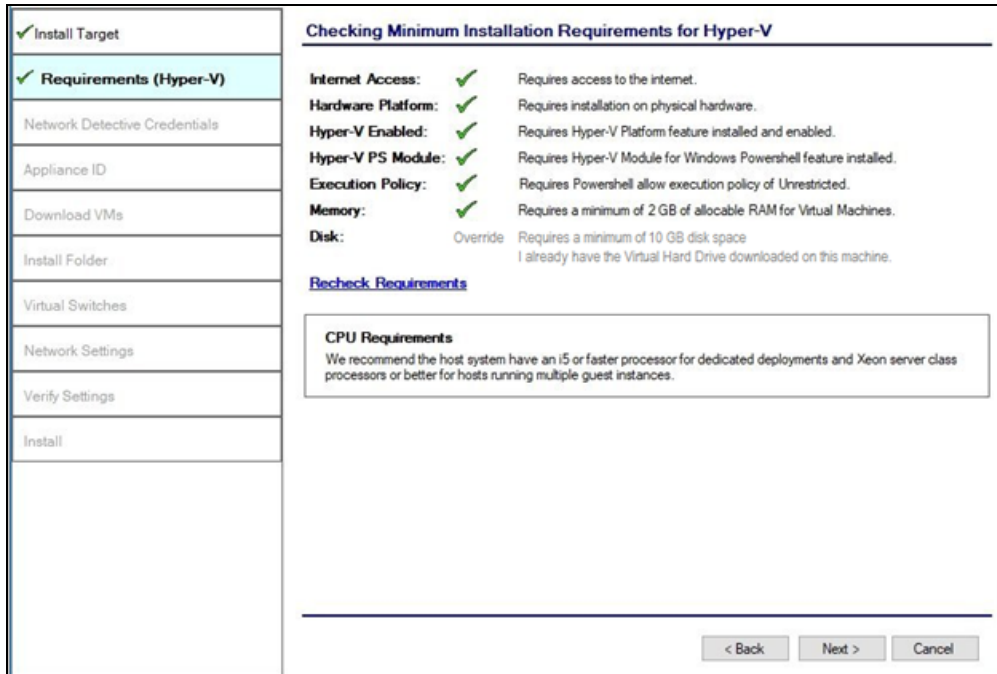
< Back   Next >   Cancel

When all requirements are checked successfully, click **Next**.

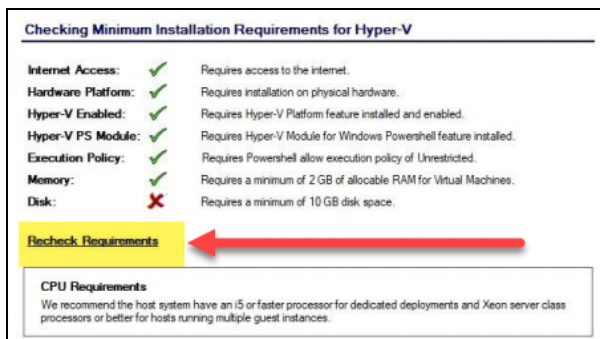
## Overriding Disk Space Requirements

If the installer detects that there is not enough disk space to meet the minimum installation requirements, a red **X** will appear next to the disk space requirement.

The Installer will present an option for you “**override**” the disk space requirement. Click **I already have the Virtual Hard Drives downloaded on this machine** to override the requirement.



Alternatively, if you choose to free up some disk space, click **Recheck Requirements** to attempt to continue the installation process.

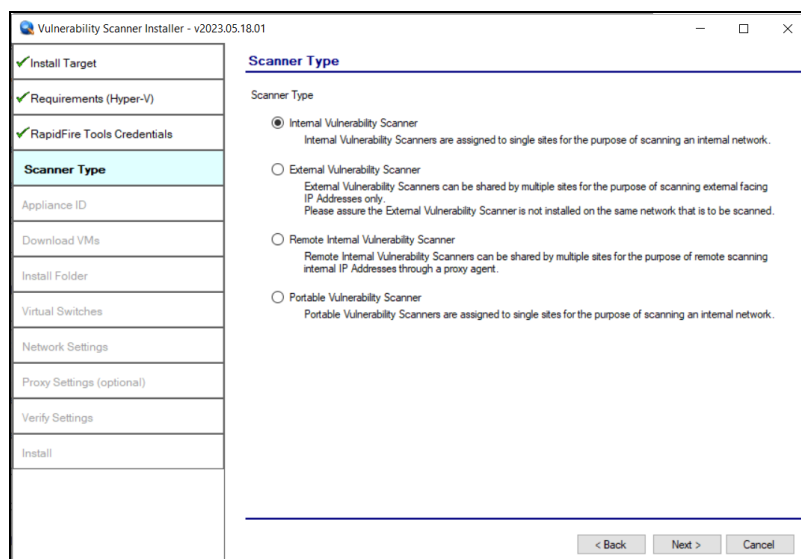


Once the system has been configured to meet the disk space requirement, or the disk space requirement has been overridden, click **Next**.

## Step 4 — Select Scanner Type

In this step, select whether to install an **internal** or **external** vulnerability scanner and click **Next**.

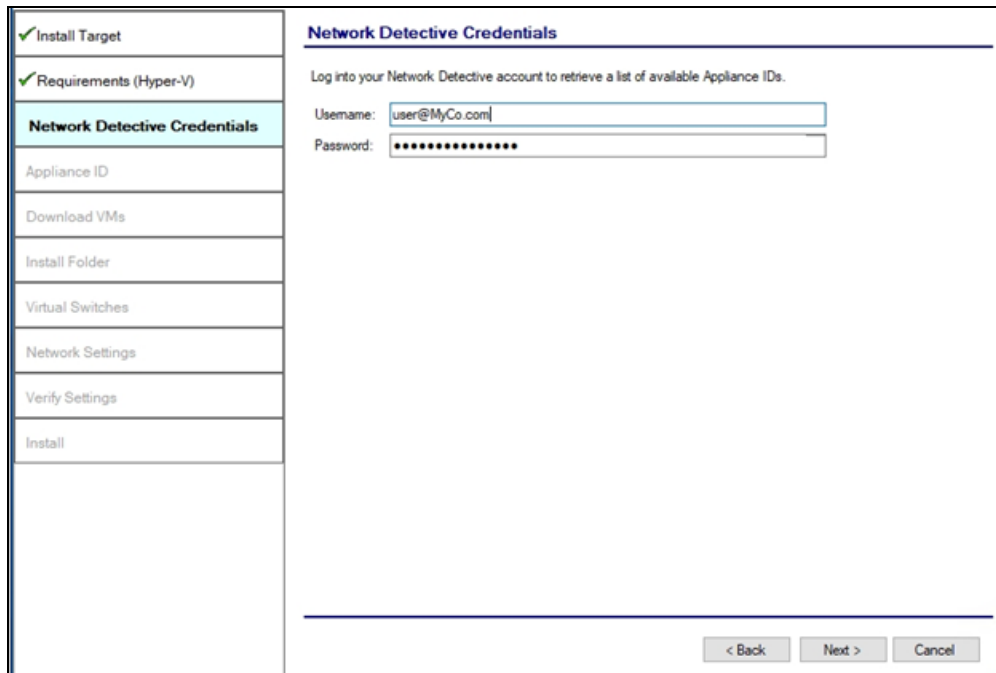
- In order to **perform an internal vulnerability scan**, you will need to **install an internal appliance**. Install the internal appliance directly on the target network to be assessed. The internal scan appliance is marked with the prefix "**IVS**."
- In order to **perform an external vulnerability scan**, you will need to **install an external appliance**. Install the external appliance on a **SEPARATE** network from the target network to be assessed. We recommend you install the external scan appliance your MSP network. The external scan appliance is marked with the prefix "**EVS**."
- The **Portable VulScan appliance (PVS)** can be installed on a physical device that you move from site to site. Otherwise, it functions in the same way as the internal scan appliance.
- The **Remote Internal Vulnerability Scanner (RIVS)** can be shared my multiple sites for the purpose of scanning internal IP Addresses through a proxy agent. It is installed on the MSP network and accesses the customer network through a VPN connection.
- See the VulScan User Guide at <https://www.rapidfiretools.com/vs-downloads> for complete documentation.



## Step 5 — Enter the Network Detective Account Credentials

In this step, enter your Network Detective account credentials in order to retrieve the list of Appliance IDs available for your account. To do this:

1. Enter valid **Network Detective** account login credentials.
2. Click **Next**.



The screenshot shows a software installation wizard window. On the left is a vertical sidebar with a list of steps: 'Install Target' (checked), 'Requirements (Hyper-V)' (checked), 'Network Detective Credentials' (highlighted in light blue), 'Appliance ID', 'Download VMs', 'Install Folder', 'Virtual Switches', 'Network Settings', 'Verify Settings', and 'Install'. The main area of the window is titled 'Network Detective Credentials' and contains the instruction: 'Log into your Network Detective account to retrieve a list of available Appliance IDs.' Below this are two input fields: 'Username:' with the text 'user@MyCo.com' and 'Password:' with a masked password of ten asterisks. At the bottom right of the main area are three buttons: '< Back', 'Next >', and 'Cancel'.

## Virtual Appliance ID Requirements

If during the login process you receive the “No available Appliance IDs are associated with this account” message, contact the Technical Support Team at RapidFire Tools to verify that at least one valid Virtual Appliance ID has been assigned to the user’s Network Detective account.

✓ Install Target	<h3>Network Detective Credentials</h3> <p>Log into your Network Detective account to retrieve a list of available Appliance IDs.</p> <p>Username: <input type="text" value="user@MyCo.com"/></p> <p>Password: <input type="password" value="*****"/></p> <p><b>Invalid login and password</b></p> <hr/> <p>&lt; Back    Next &gt;    Cancel</p>
✓ Requirements (Hyper-V)	
<b>Network Detective Credentials</b>	
Appliance ID	
Download VMs	
Install Folder	
Virtual Switches	
Network Settings	
Verify Settings	
Install	

## Step 6 — Select Appliance ID Screen

After the Network Detective login credentials have been authenticated, you must assign an available Appliance ID that has been allocated to the user's Network Detective account to the Virtual Appliance that is being installed.

The Appliance ID Window will display all of the Appliance IDs assigned to the user's account.

To the right of each Appliance ID value is a list of the Software Appliances (i.e. Cyber Hawk, Reporter, and/or Inspector) that are provisioned to operate with each Appliance ID.



The screenshot shows the 'Appliance ID' step of the installation wizard. On the left is a vertical sidebar with a list of steps: 'Install Target', 'Requirements (Hyper-V)', 'Network Detective Credentials', 'Appliance ID' (highlighted in light blue), 'Download VMs', 'Install Folder', 'Virtual Switches', 'Network Settings', 'Verify Settings', and 'Install'. The main area is titled 'Appliance ID' and contains the following text: 'Select the Appliance ID you wish to associate with the Virtual Appliance. Ensure that the selected appliance is properly provisioned for the desired features.' Below this is a list of 'Available Appliance IDs' with 'NDA1-24' selected. The list includes: NDA1-24, NDA1-31, NDA1-36, NDA1-37, NDA1-38, NDA1-45, NDA1-47, NDA1-52, NDA1-54, NDA1-69, NDA1-79, NDA1-83, NDA1-86, and NDA1-94. At the bottom of the main area is a checkbox labeled 'Enable automatic updates for the Virtual Appliance.' which is checked. At the very bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Select the Appliance ID that is to be assigned to the Virtual Appliance that is being installed.

## Record the Appliance ID for the Virtual Appliance Installation

Upon selection of the Appliance ID, the Appliance ID should be recorded so that the user knows which Appliance ID has been associated with the Virtual Appliance's installation.

After selecting and recording the Appliance ID to be assigned to the Virtual Appliance installation, select the Next button to proceed to the next step of downloading the Virtual Machines that are required to complete the Virtual Appliance's installation.

## Step 7 — Download VMs


In this step, download the VM image required to install the virtual appliance:

1. Click **Browse** and select a Download Folder for the VM image.

**Note:** If you have already downloaded the VM, select its folder.

The screenshot shows the 'Download VMs' step in the installation wizard. On the left is a vertical sidebar with a list of steps: 'Install Target', 'Requirements (Hyper-V)', 'Network Detective Credentials', 'Appliance ID', 'Download VMs' (highlighted in light blue), 'Install Folder', 'Virtual Switches', 'Network Settings', 'Verify Settings', and 'Install'. The main area is titled 'Download VMs' and contains the following text: 'Select the folder to download the VM images. If you have previously downloaded the images, select the folder where they reside. Press Next to begin the download (if needed)'. Below this is a 'Download Folder:' label followed by a text box containing the path 'C:\Users\admin\Downloads\NDA' and a 'Browse' button. Underneath, the 'Install Package Status' is shown in red text: 'The install image does not exist. Clicking Next will download the latest image.' At the bottom right of the main area are three buttons: '< Back', 'Next >', and 'Cancel'.

2. Click **Next** button to initiate the download process. A window will be displayed to present the progress of the VM download process. The Install Package Status bar will display the progress of the VM download.

✓ Install Target	<h3>Download VMs</h3> <p>Select the folder to download the VM images. If you have previously downloaded the images, select the folder where they reside. Press Next to begin the download (if needed).</p> <p>Download Folder: <input type="text" value="C:\Users\admin\Downloads\NDA\"/> <input type="button" value="Browse"/></p> <p>Install Package Status:  284879373 of 1589437443 bytes transferred (17.9% complete).</p>
✓ Requirements (Hyper-V)	
✓ Network Detective Credentials	
✓ Appliance ID	
<b>✓ Download VMs</b>	
Install Folder	
Virtual Switches	
Network Settings	
Verify Settings	
Install	
<input type="button" value=" &lt; Back"/> <input type="button" value=" Next &gt;"/> <input type="button" value=" Cancel"/>	

Once the VM has been downloaded (or you select a folder with a previously downloaded VM), the **Install Package Status** will be updated.

✓ Install Target	<h3>Download VMs</h3> <p>Select the folder to download the VM images. If you have previously downloaded the images, select the folder where they reside. Press Next to begin the download (if needed).</p> <p>Download Folder: <input type="text" value="C:\Users\admin\Downloads\NDA\"/> <input type="button" value="Browse"/></p> <p>Install Package Status: <b>Downloaded</b></p>
✓ Requirements (Hyper-V)	
✓ Network Detective Credentials	
✓ Appliance ID	
<b>✓ Download VMs</b>	
Install Folder	
Virtual Switches	
Network Settings	
Verify Settings	
Install	
<input type="button" value=" &lt; Back"/> <input type="button" value=" Next &gt;"/> <input type="button" value=" Cancel"/>	

3. Once the VMs have been downloaded or made available for installation, click **Next**.

## Step 8 — Select Folder to Install Virtual Appliance

1. Click **Browse** and select an install folder for the appliance program files.

**Note:** The default installation folder is the system's Hyper-V location folder.

The screenshot shows the 'Install Folder' step of the VulScan installation wizard. On the left is a vertical navigation pane with the following steps: 'Install Target' (checked), 'Requirements (Hyper-V)' (checked), 'Network Detective Credentials' (checked), 'Appliance ID' (checked), 'Download VMs' (checked), 'Install Folder' (checked and highlighted in light blue), 'Virtual Switches', 'Network Settings', 'Verify Settings', and 'Install'. The main area is titled 'Install Folder' and contains the instruction: 'Select the folder to install the Virtual Machines. This is the folder the virtual hard drives (.vhdx) will reside.' Below this is a text box labeled 'Install Folder:' containing the path 'C:\ProgramData\Microsoft\Windows\Hyper-V' and a 'Browse' button. At the bottom right of the main area are three buttons: '< Back', 'Next >', and 'Cancel'.

2. Click **Next** to continue the installation process and configure the required Virtual Switches.

## Step 9 — Configure Required Virtual Switches

**Important:** The appliance requires an **External Virtual Switch** to be configured within the Hyper-V instance. The switch is necessary for the appliance to be installed and function.

In this step, you can either:

- Use an existing external Virtual Switch
- Create a new Virtual Switch on an existing network interface

### Using an Existing External Virtual Switch

1. Select the **Use an existing external Virtual Switch** option.

The screenshot shows the 'Virtual Switches' configuration window. On the left is a navigation pane with the following items: 'Install Target', 'Requirements (Hyper-V)', 'Network Detective Credentials', 'Appliance ID', 'Download VMs', 'Install Folder', 'Virtual Switches' (highlighted), 'Network Settings', 'Verify Settings', and 'Install'. The main content area is titled 'Virtual Switches' and contains the following text: 'External Virtual Switch' and 'The External Virtual Switch is used by the Virtual Appliance to communicate with the corporate network and the Internet. Please select which Network Adapter the External Virtual Switch should use.' There are two radio button options: 'Use an existing external Virtual Switch' (which is selected) and 'Create a new Virtual Switch on an existing network interface'. Below the first option is a dropdown menu for 'External Virtual Switches' with the value 'NDA-External-VS [Realtek PCIe GBE Family Controller]'. Below the second option is a note: '\* Only network interfaces that are not currently configured in an existing Virtual Switch will be shown.' This is followed by a 'Network Interface' dropdown menu with the value 'Intel(R) Dual Band Wireless-AC 3165' and a 'Virtual Switch Name' text box with the value 'NDA-External-VS'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

2. Use the drop-down menu to select a switch from a list of those available on the Hyper-V system.
3. Click **Next** button to continue the installation process.

## Creating and Selecting a new External Virtual Switch

If the system being used is a new Hyper-V system and no External Virtual Switches are set-up and available, or if you wish to create an External Virtual Switch to use with the appliance:

1. Select the **Create a new Virtual Switch on an existing Network Interface** option.

The screenshot shows the 'Virtual Switches' configuration window. On the left is a sidebar with a list of steps: 'Install Target', 'Requirements (Hyper-V)', 'Network Detective Credentials', 'Appliance ID', 'Download VMs', 'Install Folder', 'Virtual Switches' (highlighted), 'Network Settings', 'Verify Settings', and 'Install'. The main content area is titled 'Virtual Switches' and contains the 'External Virtual Switch' section. It explains that the External Virtual Switch is used for network communication. Two options are presented: 'Use an existing external Virtual Switch' (unselected) and 'Create a new Virtual Switch on an existing network interface' (selected). Below the second option, a note states: '\*Only network interfaces that are not currently configured in an existing Virtual Switch will be shown.' The 'Network Interface' dropdown menu is set to 'Intel(R) Ethernet Connection I217-LM'. The 'Virtual Switch Name' text box contains 'NDA-External-VS'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

2. Next, select the **Network Interface**.

**Note:** Do not use a Wireless NIC as the Network Interface for the External Virtual Switch.

3. Type in the name of the new **External Virtual Switch**.
4. Click **Next**.

## Step 10 — Define Network Settings

In this step, the Appliance can use an IP Address assigned by DHCP or a static IP address that you define.

### Network Settings using DHCP

To set up the Appliance to obtain an IP address and DNS server information automatically:

1. Select the “**Obtain an IP address and DNS servers automatically (DHCP)**” option.

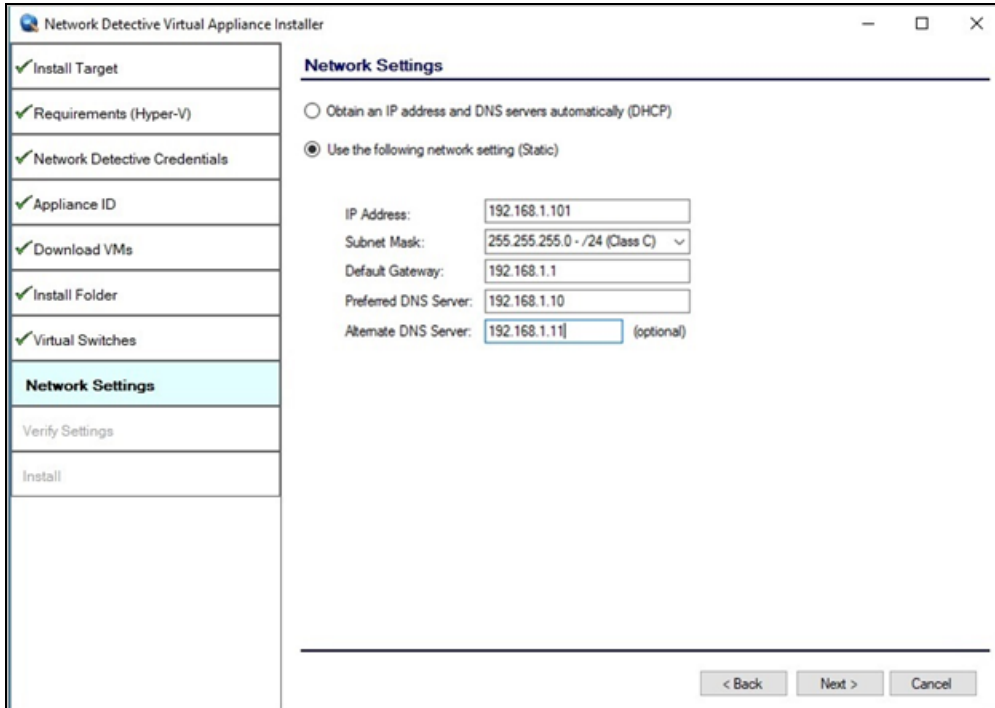
The screenshot shows the 'Network Settings' configuration window. On the left is a vertical list of steps, with 'Network Settings' highlighted in light blue. The main content area is titled 'Network Settings' and contains two radio button options. The first option, 'Obtain an IP address and DNS servers automatically (DHCP)', is selected. The second option is 'Use the following network setting (Static)'. Below the static option are input fields for IP Address, Subnet Mask (set to 255.255.255.0 - /24 (Class C)), Default Gateway, Preferred DNS Server, and Alternate DNS Server (optional). At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

2. Click **Next**.

### Network Settings using a Static IP Address

To define a static IP address for use by the Appliance:

1. Select the **“Use the following network settings (Static)”** option.
2. Next, define the **IP Address**, **Subnet Mask**, **Default Gateway**, **Preferred DNS Server**, and the **Alternate DNS Server**. The **Alternate DNS Server** setting is optional.



The screenshot shows the 'Network Detective Virtual Appliance Installer' window. On the left is a navigation pane with the following items: 'Install Target', 'Requirements (Hyper-V)', 'Network Detective Credentials', 'Appliance ID', 'Download VMs', 'Install Folder', 'Virtual Switches', 'Network Settings' (highlighted), 'Verify Settings', and 'Install'. The main area is titled 'Network Settings' and contains two radio button options: 'Obtain an IP address and DNS servers automatically (DHCP)' (unselected) and 'Use the following network setting (Static)' (selected). Below these are five input fields: 'IP Address' (192.168.1.101), 'Subnet Mask' (255.255.255.0 - /24 (Class C) with a dropdown arrow), 'Default Gateway' (192.168.1.1), 'Preferred DNS Server' (192.168.1.10), and 'Alternate DNS Server' (192.168.1.11) with '(optional)' text to its right. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.



**Note:** For **Inspector**, you will need to enter the IP address of the Inspector VM under **Scanner IP**.

3. Click **Next**.

## Step 11 — Proxy Settings

When installing any RapidFire Tools Virtual Appliance (Cyber Hawk, VulScan, Reporter, and Compliance Manager), you can specify a proxy server.

You will need:

- Server name or IP address
- Port
- Username
- Password

**Tip:** Click **Test Proxy Settings** to be sure you can connect successfully.

## Step 12 — Verify Settings Prior to Installation

Prior to completion of the installation process, the **Installer** will present the **Verify Settings** window.

Check and, if necessary, modify the **Appliance ID**, **Install Folder**, the **Virtual Switches** configuration, and the **Virtual Hard Drive** locations.

Step	Configuration
✓ Install Target	<b>Verify Settings</b>
✓ Requirements (Hyper-V)	<b>Configuration</b>
✓ Network Detective Credentials	<b>Appliance ID:</b> NDA1-69 (Detector)
✓ Appliance ID	<b>Install Folder:</b> C:\ProgramData\Microsoft\Windows\Hyper-V
✓ Download VMs	<b>Virtual Machine</b>
✓ Install Folder	<b>Hard Drive:</b> C:\ProgramData\Microsoft\Windows\Hyper-V\NDA1-69.vhdx
✓ Virtual Switches	<b>Switch:</b> NDA-External-VS [Intel(R) Ethernet Connection I2-LM]
✓ Network Settings	<b>Network Settings</b>
✓ <b>Verify Settings</b>	<b>IP Address:</b> (use DHCP)
Install	< Back   Install >   Cancel

After verifying the settings are correct, click the **Install** button.

This action will start the **Virtual Appliance's** installation on the Hyper-V based system.

## Step 13 — Monitor Installation Progress Status

In this step, the installer details the status of the tasks performed during the installation.

Task	Notes
✓ Extract Virtual Machine	Completed
⚙️ Create External Virtual Switch	Creating external virtual switch...
Create Virtual Machine	
Configure Network Settings	
Obtain IP Address	
Check VM Configuration Status	
Configure Virtual Appliance Settings	
Appliance Services Running	
Update Virtual Appliance to Latest Version (via Internet)	

If any installation task fails to complete, you can read a description of the issue in the Notes column.

When a **Task** during the installation process fails to complete, the appliance installation process is terminated. Click **Retry Install Now** to attempt the installation again.

When the installation process is successfully completed, a confirmation window will appear.

**Install**

Installing the Network Detective appliance. This process typically takes between 10-20 minutes.  
Appliance ID: NDA1-69 (Detector)

Task	Notes
✓ Extract Virtual Machine	Completed
✓ Create External Virtual Switch	Completed
✓ Create Virtual Machine	Operational
✓ Configure Network Settings	DHCP enabled
✓ Obtain IP Address	
✓ Check VM Configuration Status	Ready to be configured.
✓ Configure Virtual Appliance Settings	Completed
✓ Appliance Services Running	Running
✓ Update Virtual Appliance to Latest Version (via Internet)	Completed

[View Install Log](#)

Installation Complete

Congratulations! The Network Detective Appliance has been installed and is ready for use.

[Close](#)

[< Back](#)   [Finish](#)   [Cancel](#)

**Tip:** After installing the appliance, be sure to double check that it meets the [Virtual Appliance Operational System Requirements](#).

**Note:** During the user’s Remote Access to the Hyper-V system used to perform the Virtual Appliance installation, the user may experience a temporary loss of Remote Access connectivity.

In cases where the user that is remotely accessing the Hyper-V system in order to perform the installation of the Virtual Appliance, and the user creates a new External Virtual Switch for the Virtual Appliance’s use, the established remote access network connection will be momentarily terminated by the Hyper-V system.

The remote access software used to access the system should issue one or more retries to re-establish the remote access connection to the Hyper-V system to enable the user to complete the Virtual Appliance installation process.

## Step 14 — Confirm that Appliance Meets Operational Requirements

Once you install the appliance, be sure that it meets the Operational Requirements:

- 16 GB Available RAM
- 40 GB Hard Drive Space

# VulScan Installation Procedure for VMware

To perform the installation of the **Virtual Appliance for VMware**, please follow the instructions below.

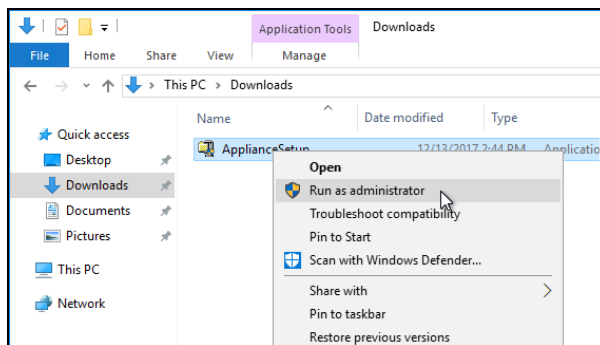
## Step 1 — Download and Run the Virtual Appliance Installer

The **Installer** file is a self-extracting ZIP file that is used to initiate the installation of the **Virtual Appliance** on the host system. To begin the installation procedure:

1. Download and run the **VulScan Virtual Appliance Installer** file at <https://www.rapidfiretools.com/vs-downloads>. The Installer file is named **VulnerabilityScannerSetup.exe**.

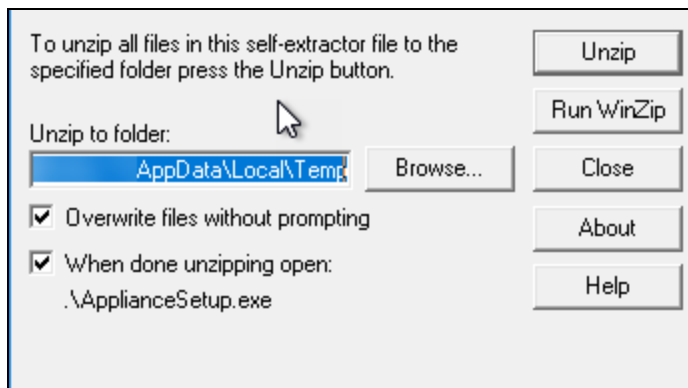
**Important:** Be sure to download the "Virtual Appliance Installer", and NOT the RapidFire Tools Server installer.

2. After downloading the installer, right click on **VulnerabilityScannerSetup.exe** and click **Run as Administrator**.



3. Use the **Unzip** option to unzip the files into a folder location of your choice and start

the installation program.



**Important:** You must have Administrator privileges and access rights in order to complete the installation process successfully.



## Step 2 — Select Target

1. Select the **VMware** option to install on a VMware enabled system.

The screenshot shows the 'Install Target' configuration window. The left sidebar contains a list of steps: 'Install Target' (checked), 'Requirements (Hyper-V)', 'Network Detective Credentials', 'Appliance ID', 'Download VMs', 'Install Folder', 'Virtual Switches', 'Network Settings', 'Proxy Settings (optional)', 'Verify Settings', and 'Install'. The main area displays three radio button options: 'Microsoft Hyper-V' (selected), 'vmware' (highlighted in yellow), and 'Manual Configuration (Advanced)'. At the bottom right, there are buttons for '< Back', 'Next >', and 'Cancel'.

2. Select the **Next** button to proceed with the installation.

## Step 3 — Verification that Installation Requirements are Met

In this step, the installer checks to see if the host system meets the system requirements. These requirements include:

- Internet access
- VMware vSphere PowerCLI 6.3 or higher installed

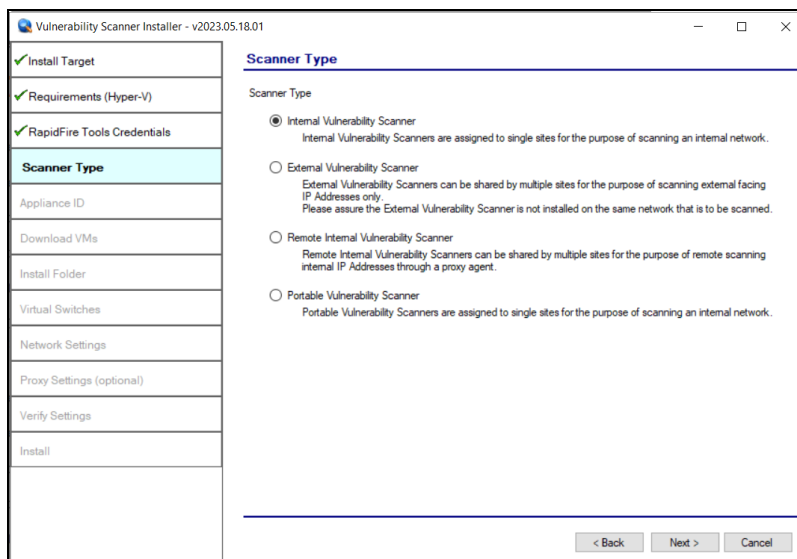
✓ Install Target	<b>Checking Minimum Installation Requirements for VMware</b>	
✓ Requirements (VMware)	<b>Internet Access:</b> ✓	Requires access to the internet.
Network Detective Credentials	<b>PowerCLI 6.3:</b> ✓	Requires VMware vSphere PowerCLI 6.3 or higher installed.
Appliance ID	<a href="#">Recheck Requirements</a>	
VMware Server		
VMware VM Settings		
VMware Network Settings		
Download VMs		
Network Settings		
Verify Settings		
Install		
	<input data-bbox="971 1115 1052 1140" type="button" value=" &lt; Back "/> <input data-bbox="1068 1115 1149 1140" type="button" value=" Next &gt; "/> <input data-bbox="1166 1115 1247 1140" type="button" value=" Cancel "/>	

When all requirements are checked successfully, click **Next**.

## Step 4 — Select Scanner Type

In this step, select whether to install an **internal** or **external** vulnerability scanner and click **Next**.

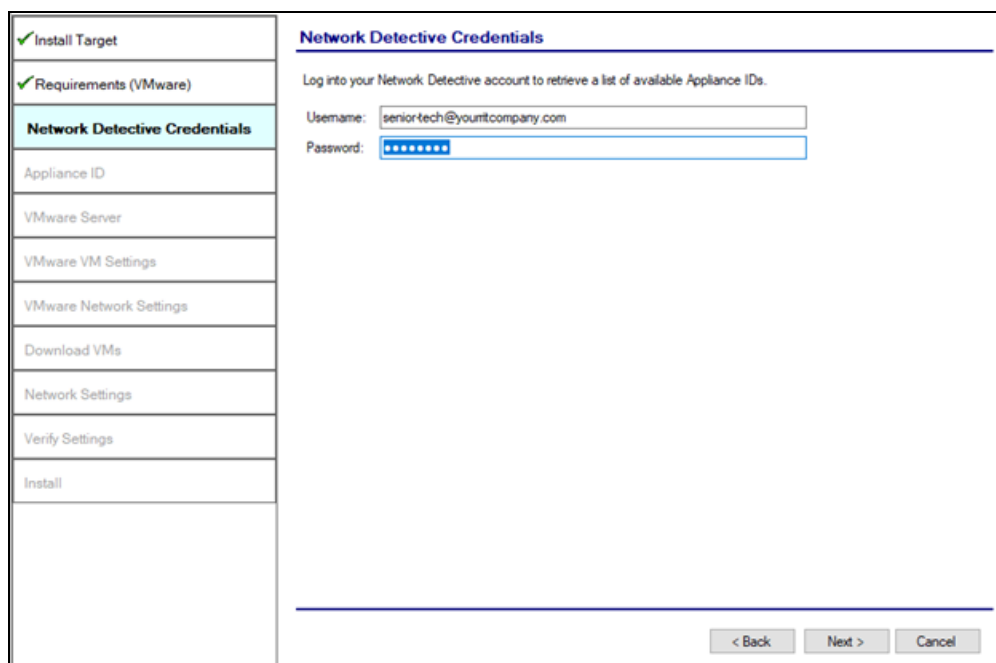
- In order to **perform an internal vulnerability scan**, you will need to **install an internal appliance**. Install the internal appliance directly on the target network to be assessed. The internal scan appliance is marked with the prefix "**IVS**."
- In order to **perform an external vulnerability scan**, you will need to **install an external appliance**. Install the external appliance on a **SEPARATE** network from the target network to be assessed. We recommend you install the external scan appliance your MSP network. The external scan appliance is marked with the prefix "**EVS**."
- The **Portable VulScan appliance (PVS)** can be installed on a physical device that you move from site to site. Otherwise, it functions in the same way as the internal scan appliance.
- The **Remote Internal Vulnerability Scanner (RIVS)** can be shared my multiple sites for the purpose of scanning internal IP Addresses through a proxy agent. It is installed on the MSP network and accesses the customer network through a VPN connection.
- See the VulScan User Guide at <https://www.rapidfiretools.com/vs-downloads> for complete documentation.



## Step 5 — Enter the Network Detective Account Credentials

In this step, enter your Network Detective account credentials in order to retrieve the list of Appliance IDs available for your account. To do this:

1. Enter valid **Network Detective** account login credentials.
2. Click **Next**.



The screenshot shows a software installation wizard window. On the left is a vertical sidebar with a list of steps: 'Install Target' (checked), 'Requirements (VMware)' (checked), 'Network Detective Credentials' (highlighted in light blue), 'Appliance ID', 'VMware Server', 'VMware VM Settings', 'VMware Network Settings', 'Download VMs', 'Network Settings', 'Verify Settings', and 'Install'. The main area of the window is titled 'Network Detective Credentials' and contains the instruction: 'Log into your Network Detective account to retrieve a list of available Appliance IDs.' Below this are two input fields: 'Username:' with the text 'senior-tech@youritcompany.com' and 'Password:' with a masked password of eight dots. At the bottom right of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

## Virtual Appliance ID Requirements

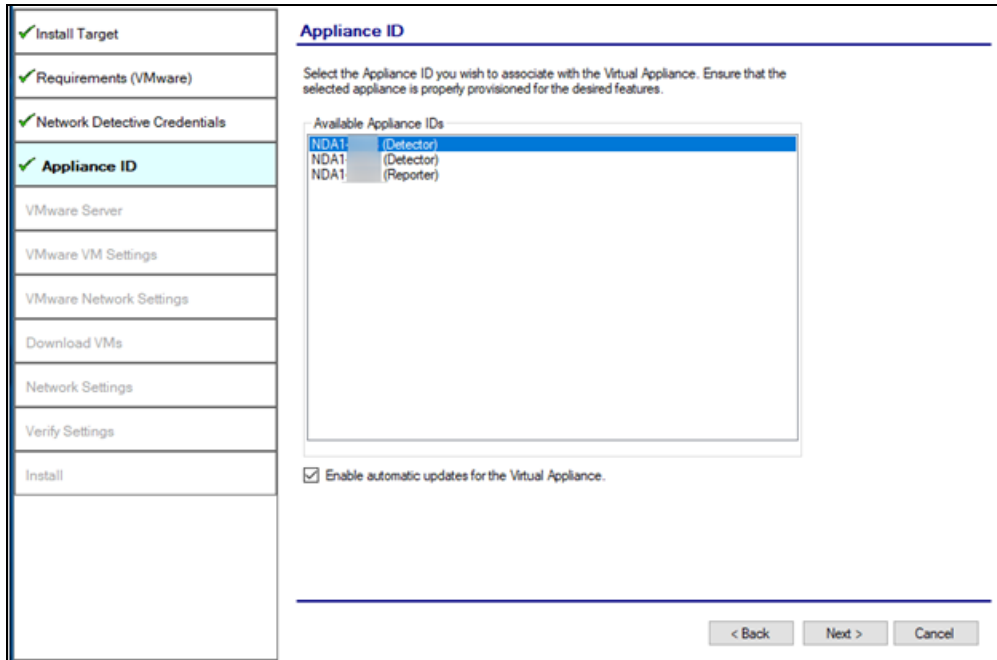
If during the login process you receive the “No available Appliance IDs are associated with this account” message, contact the Technical Support Team at RapidFire Tools to verify that at least one valid Virtual Appliance ID has been assigned to the user’s Network Detective account.

## Step 6 — Select Appliance ID Screen

After the Network Detective login credentials have been authenticated, you must assign an available Appliance ID that has been allocated to the user’s Network Detective account to the Virtual Appliance that is being installed.

The Appliance ID Window will display all of the Appliance IDs assigned to the user’s account.

To the right of each Appliance ID value is a list of the Software Appliances (i.e. Cyber Hawk, Reporter, and/or Inspector) that are provisioned to operate with each Appliance ID.



Select the Appliance ID that is to be assigned to the Virtual Appliance that is being installed.

## Record the Appliance ID for the Virtual Appliance Installation

Upon selection of the Appliance ID, the Appliance ID should be recorded so that the user knows which Appliance ID has been associated with the Virtual Appliance’s installation.

After selecting and recording the Appliance ID to be assigned to the Virtual Appliance installation, select the Next button to proceed to the next step of downloading the Virtual Machines that are required to complete the Virtual Appliance’s installation.

## Step 7 — Set VMware Server Credentials

In the VMware Server window, enter the **VMware Server** account **IP Address/Name** and login **credentials** used to access your **VMware Server** that will be used to operate the **Virtual Appliance**.

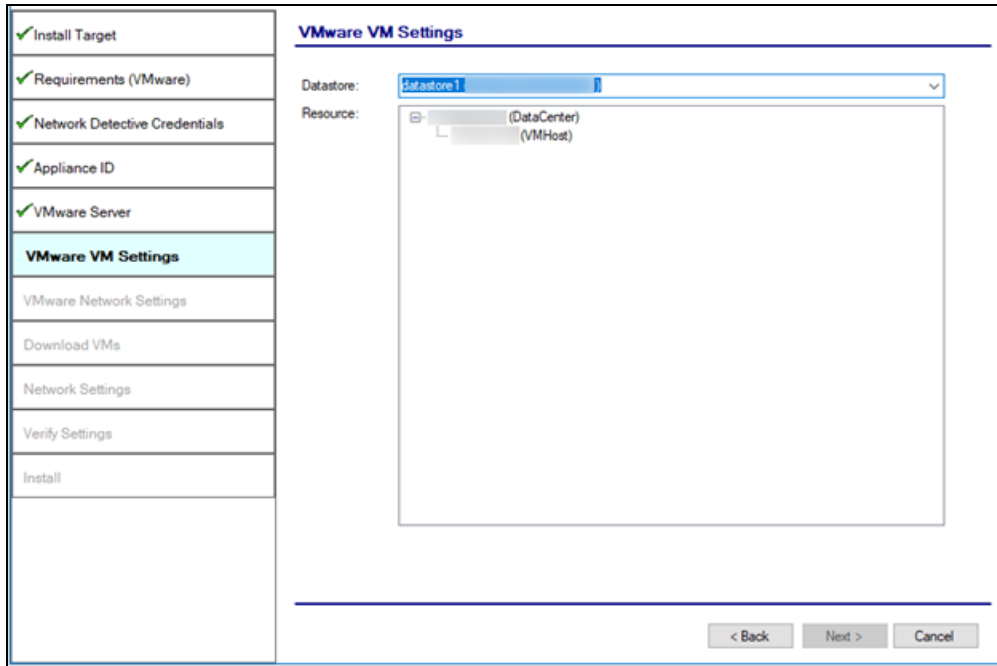
This should be the same information used in the VMware vSphere Client program used in your environment to access the **VMware Server**.

✓ Install Target	<h3>VMware Server</h3> <p>Please enter the setting to connect to the remote VMware Server. This should be the same information entered in the VMware vSphere Client program.</p> <p>IP address / Name: <input type="text"/></p> <p>User name: <input type="text" value="root"/></p> <p>Password: <input type="password" value="*****"/></p> <p>&lt; Back   Next &gt;   Cancel</p>
✓ Requirements (VMware)	
✓ Network Detective Credentials	
✓ Appliance ID	
<b>VMware Server</b>	
VMware VM Settings	
VMware Network Settings	
Download VMs	
Network Settings	
Verify Settings	
Install	

Select the **Next** button to proceed with the installation.

## Step 8 — Set VMware Server Settings

Select and enter in the VMware Server’s **Datastore** and **Resource Pool** settings information in the fields presented in the VMware VM Settings window.



Select the **Next** button to proceed with the installation.

## Step 9 — Set VMware Network Settings

Select the **External Port Group** that will be used by the **Virtual Appliance** to communicate with your network.

**Note:** If there are no existing switches or **External Port Groups** available, then use vSphere to create one, and select the Refresh link in the **VMware Network Settings** window to make the **External Port Group** you created available for selection.

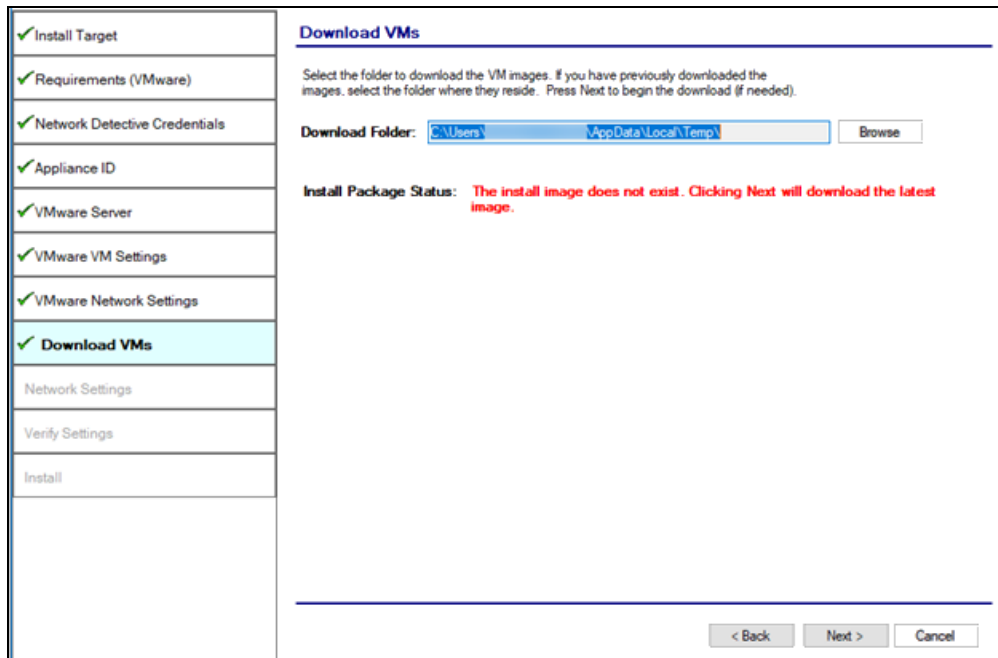
The screenshot shows the 'VMware Network Settings' window. On the left is a vertical navigation pane with the following items: 'Install Target', 'Requirements (VMware)', 'Network Detective Credentials', 'Appliance ID', 'VMware Server', 'VMware VM Settings', 'VMware Network Settings' (highlighted in light blue), 'Download VMs', 'Network Settings', 'Verify Settings', and 'Install'. The main content area is titled 'VMware Network Settings' and contains the following text: 'External Port Group', 'The External Virtual Switch is used by the Virtual Appliance to communicate with the corporate network and the Internet. Please select which Network Adapter the External Virtual Switch should use.', and 'If there are no existing switches or port groups, please use the vSphere client to create one. Use the Refresh button to update the dropdown list.' Below this text is a dropdown menu labeled 'External Port Groups:' with 'VM Network' selected and a 'Refresh' link to its right. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Select the **Next** button to proceed with the installation.



## Step 10 — Initiate the Download VM Process

In this step of the **Virtual Appliance's** installation process, the window below will be displayed to indicate that the VM required to install the **Virtual Appliance** have not been downloaded at this point of the installation process.

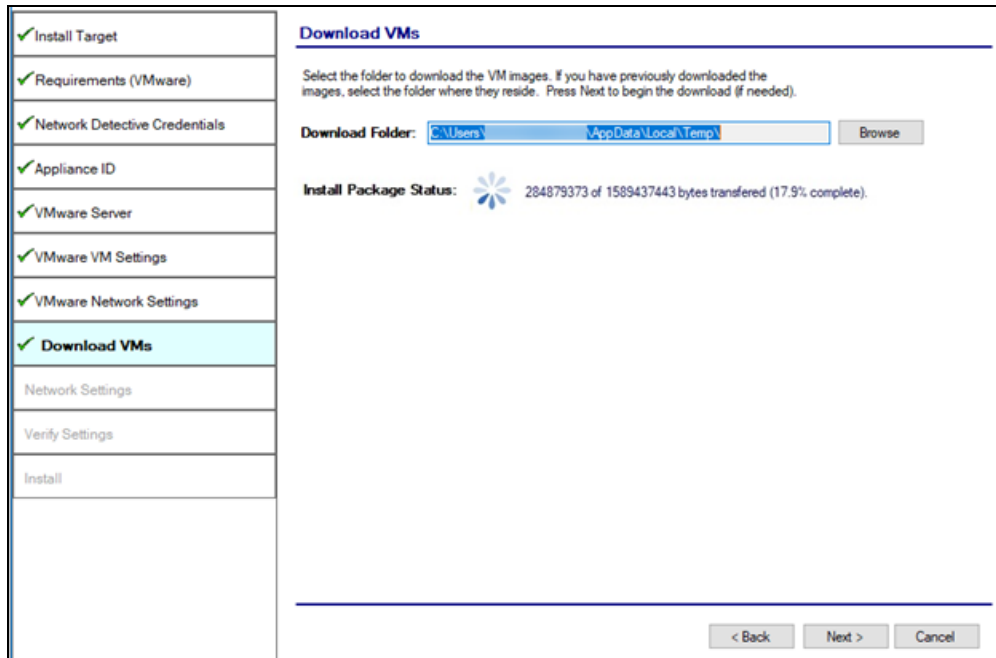


To proceed with downloading the required VM, the user must select the folder that is to be used to store the VM that are about to be downloaded.

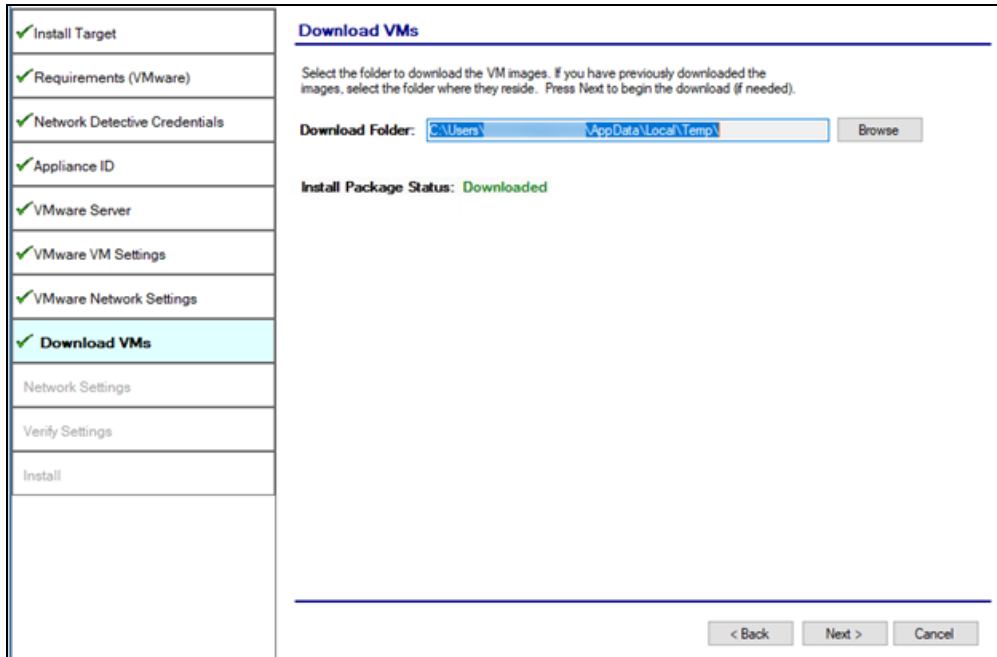
Then select the **Next** button to initiate the download process. A window will be displayed to present the progress of the VM download process.

## Step 11 — View VM Download Progress and Install Package Status

During the VM download process, the Install Package Status bar will display the progress of the VM download.



Once the VM have been downloaded, or when the user selects a folder where the VM bundle has already been downloaded, the **Install Package Status** in the **Download VM** window will be updated to indicate that the VM have been “**downloaded**” as displayed below.



Once the VM have been downloaded or available for installation, proceed with **Virtual Appliance** installation process by selecting the **Next** button.

The next window displayed enables the user to select the folder to be used for the **Virtual Appliance's** installation

## Step 12 — Define Network Settings

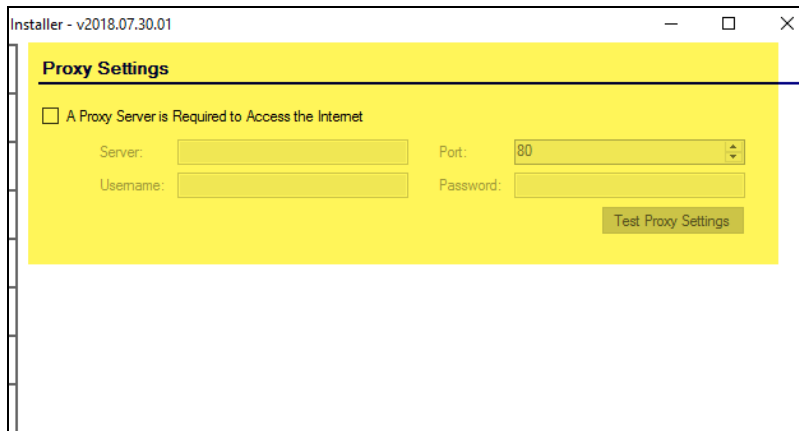
In this step of the **Virtual Appliance's** installation process, the window below will be displayed to enable you to assign the Network Settings for the installation.

The screenshot shows a software installation window titled "Network Settings". On the left is a vertical progress bar with the following steps: "Install Target", "Requirements (VMware)", "Network Detective Credentials", "Appliance ID", "VMware Server", "VMware VM Settings", "VMware Network Settings", "Download VMs", "Network Settings" (highlighted in light blue), "Verify Settings", and "Install". The main area of the window is titled "Network Settings" and contains two radio button options: "Obtain an IP address and DNS servers automatically (DHCP)" (which is selected) and "Use the following network setting (Static)". Below these options are input fields for "IP Address:", "Subnet Mask:" (with a dropdown menu showing "255.255.255.0 - /24 (Class C)"), "Default Gateway:", "Preferred DNS Server:", and "Alternate DNS Server:" (with "(optional)" text next to it). At the bottom right of the window are three buttons: "< Back", "Next >", and "Cancel".

Once you have defined the **Network Settings** for the **Virtual Appliance**, proceed with **Virtual Appliance** installation process by selecting the **Next** button.

## Step 13 — Proxy Settings

When installing any RapidFire Tools Virtual Appliance (Cyber Hawk, VulScan, Reporter, and Compliance Manager), you can specify a proxy server.



You will need:

- Server name or IP address
- Port
- Username
- Password

**Tip:** Click **Test Proxy Settings** to be sure you can connect successfully.

## Step 14 — Verify Settings Prior to Installation

Prior to the completion of the installation process, the **Installer** will present the **Verify Settings** window.

This step in the installation process provides the user with the opportunity to check, and if necessary, modify the **Appliance ID** section, **VMware Server Settings**, **VMware VM Settings**, and the **VMware Network Settings** configuration.

✓ Install Target	<b>Verify Settings</b>
✓ Requirements (VMware)	<b>Network Detective Configuration</b>
✓ Network Detective Credentials	Appliance ID: NDA1 (Detector)
✓ Appliance ID	<b>VMware Settings</b>
✓ VMware Server	Datastore: (123.727 free out of 231)
✓ VMware VM Settings	Resource: (VMHost)
✓ VMware Network Settings	Network: VM Network
✓ Download VMs	<b>Network Settings</b>
✓ Network Settings	IP Address: (use DHCP)
✓ <b>Verify Settings</b>	
Install	

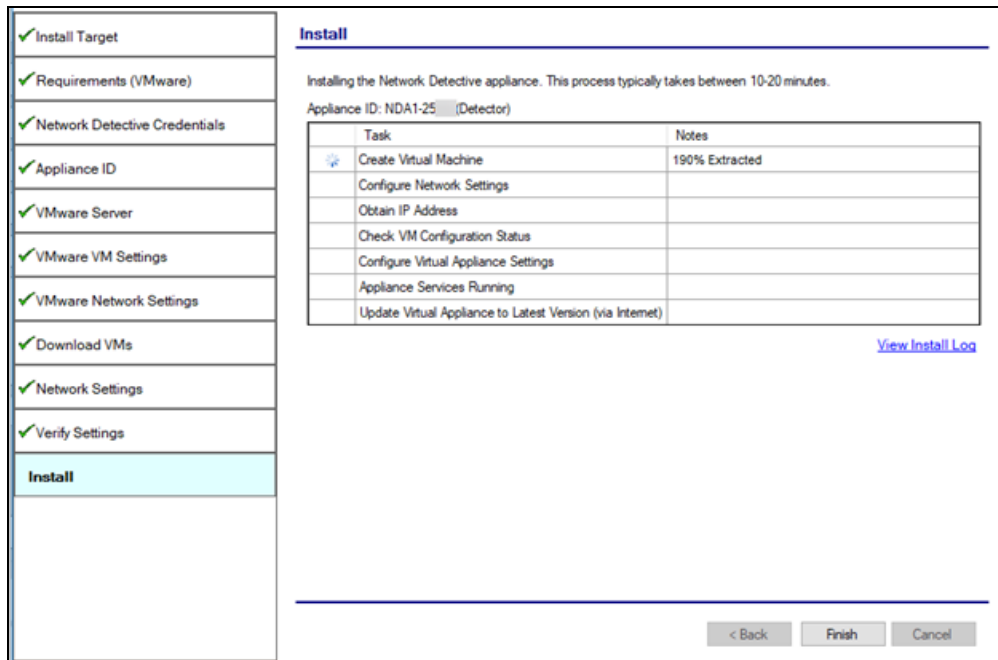
< Back   Install >   Cancel

After verifying the settings are correct, select the **Install** button.

This action will start the **Virtual Appliance's** installation on the VMware based system.

## Step 15 — Monitor Installation Progress Status

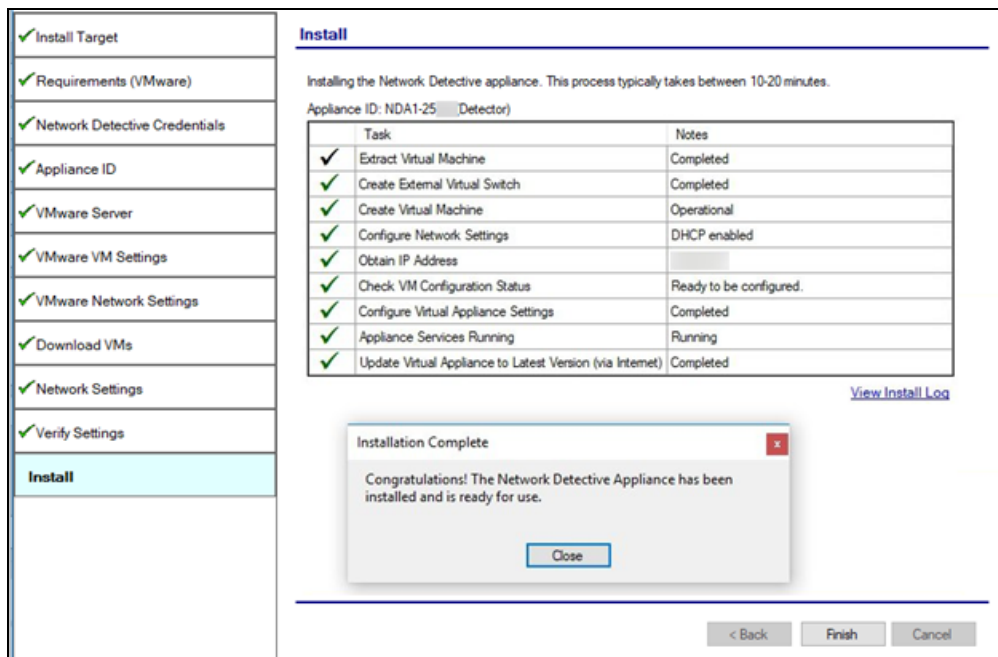
During this final step in the installation process, the **Installer** program’s window presents the installation tasks and their statuses as the **Installer** program installs and configures the **Virtual Appliance**.



In the case that any installation **Task** fails to complete, the user will be presented with a description of the issue within the **Notes** column of this window.

When a **Task** during the installation process fails to complete, the **Virtual Appliance** installation process is terminated. A “**Retry Install Now**” link will appear to enable the user to attempt to retry the installation.

When the installation process is successfully completed, the **Installer** will notify the user that the **Virtual Appliance** installation process is complete as displayed below.



**Install**

Installing the Network Detective appliance. This process typically takes between 10-20 minutes.

Appliance ID: NDA1-25 (Detector)

Task	Notes
✓ Extract Virtual Machine	Completed
✓ Create External Virtual Switch	Completed
✓ Create Virtual Machine	Operational
✓ Configure Network Settings	DHCP enabled
✓ Obtain IP Address	
✓ Check VM Configuration Status	Ready to be configured.
✓ Configure Virtual Appliance Settings	Completed
✓ Appliance Services Running	Running
✓ Update Virtual Appliance to Latest Version (via Internet)	Completed

[View Install Log](#)

Installation Complete

Congratulations! The Network Detective Appliance has been installed and is ready for use.

Close

< Back Finish Cancel

**Tip:** After installing the appliance, be sure to double check that it meets the [Virtual Appliance Operational System Requirements](#).

## Step 16 — Confirm that Appliance Meets Operational Requirements

Once you install the appliance, be sure that it meets the Operational Requirements:

- 16 GB Available RAM
- 40 GB Hard Drive Space

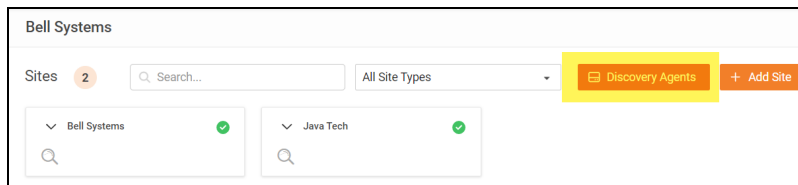


# Discovery Agent Installation Procedure

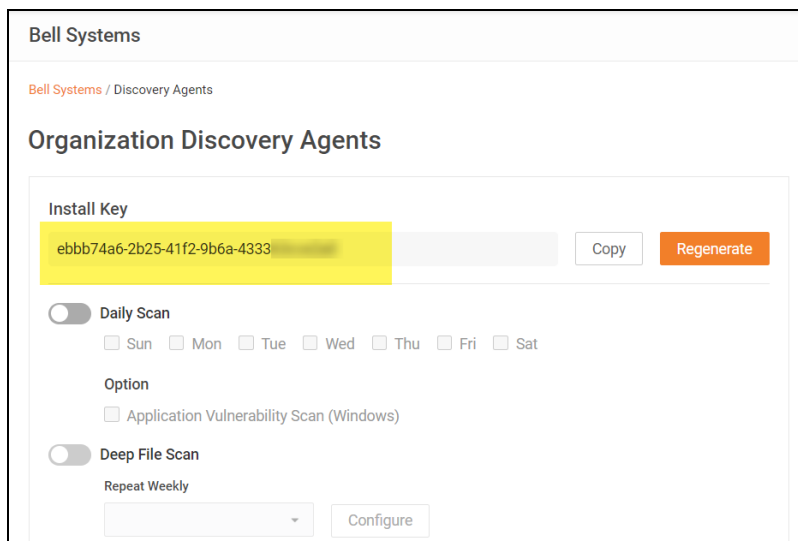
## Silent Install for Discovery Agent

Use the commands below in a batch file, Powershell Script, or similar, to perform a silent install for the Discovery Agent. You can combine these commands with others you may use for your agent deployments.

1. First, find and copy the **Install Key**. From the Organization where you wish to deploy the agent, click **Discovery Agents**.



2. **Generate** and **copy** the Install Key.



3. Next, download the agent on the target endpoint. You can use this URL: <https://download.rapidfiretools.com/download/DiscoveryAgent.msi>
4. Save the agent installer in the same location where you will run the batch file.
5. Next, use the following two commands. Replace `<your key>` with the value for the Install Key that you copied earlier.

To install the agent:

```
msiexec /qn /i DiscoveryAgent.msi /L*V install-silent.log
```

To bind the agent to your site:

```
"C:\Program Files (x86)\DiscoveryAgent\Agent\bin\register-device.exe" -installkey <your key> (without the < >)
```

You can also append a **label** and **comment** to the command above. Example:

```
"C:\Program Files (x86)\DiscoveryAgent\Agent\bin\register-device.exe" -installkey <your key> -label "Your Label" -comment "Your Comment" (without the < >)
```

## Uninstall Script for Discovery Agent

Use the command below to uninstall Discovery Agents:

**Important:** This command will not remove the Agent from appearing in the RapidFire Tools Portal. If you wish to uninstall an Agent, we recommend that you first remove it from the Portal. While the Agent is online, use the **Remove Agents** option from **[Your Organization] > Discovery Agents**, then run the command below on the endpoint that hosts the agent. See the "Enable Discovery Agents" topic for a complete walk-through.

```
msiexec /x DiscoveryAgent.msi /L*V uninstall-silent.log
```