

# Vista Manager EX

## Virtual Appliance Installation Guide

### Introduction

#### Vista Manager EX

Vista Manager EX™ is a graphical network monitoring and management tool for Allied Telesis Autonomous Management Framework™ (AMF) networks. Vista Manager EX automatically creates a complete topology map from an AMF network of switches, firewalls and wireless access points (APs), showing areas and multiple levels of connected devices. Vista Manager EX facilitates simple management of many, or all, network devices from a dashboard that gives you a central overview of your network. From the dashboard you can monitor up-to-date network status, and take action to resolve any network problems.

AMF operations can be performed directly by navigating from the following tools available from the central dashboard:

- **Dashboard**  
Displays your network details and network map including all devices connected to each area. Also shows a 24-hour event history at a glance and a list of color-coded recent events.
- **Asset Management**  
Displays a complete list of all devices on the network and allows you to search for specific devices. This list can be filtered by categories or exported. To manage devices, you can create groups, assign icons, or view licenses.
- **Network Map**  
Displays a graphical topology map of your AMF network. From here you can view pop up details of an area that displays the number of AMF devices, guest devices, device name and IP address. Actions such as backup master, SSH to master, and backup device can be carried out directly from the network map.

- **Event Log**  
Displays a list of events that are color coded red for critical, orange for abnormal and green for normal. Events can be filtered by status.
- **Service Monitoring**  
Allows an administrator to learn the status of services running on devices on the network. Configure a monitoring task to run periodically, or to monitor services on demand.
- **Allied Intent-based Orchestrator**  
Provides network optimization, automation, management, and visualization. Also offers automation of branch security and WAN bandwidth management.
- **SD-WAN**  
Enables you to set acceptable performance metrics for any application, and load-balance traffic to meet requirements. By monitoring VPN link quality, time-sensitive or critical traffic is automatically switched over to the optimal link as required.
- **User Management**  
Administrator access allows you to add, change or delete Vista Manager EX users.
- **System Management**  
Displays various system details such as the current version, serial number, and license information. It also allows you to manage the system configuration, such as SMTP settings.

## Vista Manager plugins

Vista Manager plugins are only available on Windows-based Vista Manager installations. Plugins are not available on Vista Manager virtual appliances.

## Audience for this guide

This guide is intended for computer system administrators and network engineers. It describes how to install a Vista Manager EX **virtual appliance**. For information on how to install **Windows-based** Vista Manager EX, with optional plugins, see the [Vista Manager EX Windows-based Installation Guide](#).

Planning an AMF network is beyond the scope of this installation guide. For further documentation of AMF configuration, including examples and command references, please see the links provided in the [“Related documents”](#) section below.

## Related documents

For information on how to use Vista Manager, see the [Vista Manager EX User Guide](#). The following documents give more information about Vista Manager EX:

- [Vista Manager EX Datasheet](#)

The following documents give more information about AMF:

- [AMF Feature Overview and Configuration Guide](#)
- [AMF Solutions and more information](#)

These documents are available from the links above or on our website at [alliedtelesis.com](http://alliedtelesis.com)

# Contents

Introduction .....	1
Vista Manager EX.....	1
Vista Manager plugins .....	2
Audience for this guide .....	2
Related documents.....	3
Contents.....	4
System Specifications.....	6
AMF software version compatibility.....	6
Server requirements.....	6
Hardware requirements .....	6
Supported browsers .....	6
Supported virtualization environments .....	7
AMF network support .....	7
x930 Expansion Module .....	7
Vista Manager and RMON .....	7
Syslog generation for AMF guest devices .....	8
Syslog forwarding .....	8
AMF Security (AMF-Sec) support .....	8
Licensing .....	9
Managing your licenses .....	10
Plugins .....	11
90 day trial license .....	11
Preparing your AMF Network for Vista Manager EX .....	12
Enable the HTTP service on your devices .....	12
Allow Vista Manager EX to discover the AMF network.....	12
Configure the AMF log event host .....	12
Configure certificate for device authentication .....	13
Connection timeout on masters and controllers .....	14
Installing the Vista Manager EX Virtual Appliance.....	15
Install on Windows Server 2012 R2 Hyper-V.....	15
Install on VMware vSphere Hypervisor (ESXi) 6.0/6.5/6.7 .....	19
Additional Installation Tasks.....	24
Assign a static network configuration.....	24
Ports used by Vista.....	25
Initial login .....	26
Login to Vista Manager EX .....	26

Troubleshooting .....	29
Ports and URLs used by Vista Manager EX .....	29
Allow Vista Manager EX to discover the AMF network.....	30
Reboot AMF master/controller after configuring certificates.....	30
Clear browser cache.....	30
Unexpected Communication Error during installation.....	30
Supported Devices.....	31

# System Specifications

## AMF software version compatibility

- All AMF devices must run version 5.5.0-2.x or later.
- If any of your Controller or Master devices are running 5.5.0-2.x, then all other devices must run 5.5.0-1.1 or later.
- If your AMF Master device is running 5.5.0-0.x, then all other devices must also run 5.5.0-0.x (not 5.5.0-1.x or 5.5.0-2.x).
- If your AMF Master device is running 5.5.0-2.x, then member devices can run 5.5.0-0.x or 5.5.0-1.x.
- Vista Manager 3.11.0 does not support the Virtual Appliance installation.

## Server requirements

Vista Manager EX needs to be installed on a server that has:

- Connectivity to your AMF master or controller

## Hardware requirements

We recommend the following hardware specifications or higher:

- CPU - Intel Core i5, 4 core processor, 2.5 GHz or higher
- Memory - 8GB RAM or larger (16GB or larger when using SNMP plugin)
- Hard Disk Drive - 200GB or larger (300 GB or larger when using SNMP plugin)

## Supported browsers

- Google Chrome
- Mozilla Firefox
- Internet Explorer 11
- Microsoft Edge
- Safari for iPad

## Supported virtualization environments

- Windows Server 2012 R2 Hyper-V
- Windows Server 2016 Hyper-V
- VMware vSphere Hypervisor (ESXi) 6.0/6.5/6.7

## AMF network support

Vista Manager EX supports a single AMF network with up to 60 AMF areas. It identifies the AMF network by registering the IP address of the AMF controller, or one of the AMF masters if no controller exists. When using an AMF master, you can only have one area.

Each area can have a maximum of 300 devices, with an overall network size of 3000 devices (including AMF and guest devices). Vista Manager EX only supports a single AMF controller in a network, or a single AMF master if there is no AMF controller.

## x930 Expansion Module

**Caution:** The x930 expansion module is not recognized by Vista Manager. This means that it cannot configure VLANs on those ports.

## Vista Manager and RMON

When Vista Manager connects to an AlliedWare Plus network, it automatically enables the RMON (Remote Network Monitoring) commands on each AMF interface port that it finds. This is done for the purpose of collecting traffic statistics.

It does this by modifying the running config on all switchports that interconnect AMF devices (including LAGs). No notification is shown that these changes are being made.

**Caution:** If the **copy run start** or **wr** commands are run on one of these devices, these config changes will be made permanent.

## Syslog generation for AMF guest devices

When a guest device joins or leaves an AMF network, syslog messages will be generated containing these fields:

- Network name
- Area name
- Port number
- Model type
- MAC address
- IP address

Information from these log messages are intended to help facilitate easy deployment and replacement of APs.

## Syslog forwarding

As an administrator, you will have the option to configure syslog forwarding to an external server. This functionality forwards all received syslog messages to a specified syslog server, regardless of any rules configured. Only one external syslog server is supported.

**Note:** The source address of a syslog cannot be retained to its external server.

## AMF Security (AMF-Sec) support

The existing alarm notification supports both AlliedWare Plus devices and wireless devices by leveraging on syslog messages from the AMF-Sec server. Vista Manager EX shows alarms on the integrated map for both blacklist and whitelist security events on AlliedWare Plus devices.

Configure all your AMF-Sec servers to send syslog messages to Vista Manager EX. All syslog messages from the AMF-Sec servers will then appear on the Event > Syslog page.

For more information on this feature, see the [Vista Manager EX User Guide](#).

## Licensing

Vista Manager EX licensing is subscription based. Download the license file from the [Allied Telesis download center](#). The base license file is applied during the Vista Manager software installation procedure. Subscription licenses are tied to the Vista Manager database and are maintained across backups and restores. If, however, you reinitialize the database you will need to get a new license file.

The base license and optional plugin licenses have separate license periods. If the base license expires, the optional features will not be available, even if they are still licensed.

You can install multiple plugin licenses (for the same feature) each with their own license period. This allows you to manage a total number of devices equal to the sum of the devices of the active licenses. For example, if you have two SNMP plugin licenses installed, each for 10 devices, you will be able to manage a total of 20 devices through the SNMP plugin.

## Managing your licenses

1. To add a new license to Vista Manager EX, or view existing licenses, select **System Management**.

The screenshot shows the 'System Management' interface. The 'Licenses' tab is selected in the top navigation bar. The main content area is divided into two columns. The left column contains 'Vista Manager EX' and 'Device GUI' sections, each with version and build information. The right column contains an 'About SMTP' section with various configuration fields. A red circle highlights the gear icon in the left sidebar.

2. To display your current licenses, go to the **Licenses** tab.
3. To add a new license click the **Update Licenses** button and select the required license file to upload.

The screenshot shows the 'Licenses' page. The 'Licenses' tab is highlighted in the navigation bar. The main content area displays a table of licenses. A red circle highlights the 'Update Licenses' button in the top right corner. Another red circle highlights the gear icon in the left sidebar.

	17	2018	2019	2020	2021	2022	2023	2024	2025
Vista Manager EX	Vista Manager EX Base License								
Allied Intent-based Orchestrator					Allied Intent-based Orchestrator License				
AWC Plugin	AWC Plugin - Access Points Licensed: 10								
AWC Smart Connect			AWC Smart Connect - Access Points Licensed: 90						
AWC Channel Blanket				AWC Channel Blanket - Access Points Licensed: 10					
SNMP Plugin		SNMP Plugin License							

## Plugins

The Licenses tab also shows any licenses you may have for Vista Manager EX plugins.

**Note:** Vista Manager EX plugins are only available on **Windows-based** Vista Manager EX installations. Plugins are not available on Vista Manager EX installations supplied as virtual appliances.

For more information on licensing options and plugins see the [Vista Manager EX Datasheet](#).

## 90 day trial license

As long as you are using Vista for the first time you can use a 90 day trial license. A trial license is only available on new installations. It is not available on systems that have been previously licensed, or systems restored from backups that have been previously licensed.

This license gives full access to Vista Manager EX, the Allied Intent-based Orchestrator, and the plugins. There is no grace period after the license expires, but you will receive expiry notifications at 28, 21, 14, 7, and 1 day/s before expiry. You can add a purchased license on the license management page at any time before the trial has finished.

# Preparing your AMF Network for Vista Manager EX

## Enable the HTTP service on your devices

To use Vista Manager EX, you must enable the HTTP service on all AMF devices, including all AMF masters and controllers. On AlliedWare Plus UTM firewalls, VPN routers, and virtual AMF appliances (VAAs), the HTTP service is disabled by default, while on AlliedWare Plus switches the HTTP service is enabled by default.

To enable the HTTP service, use the commands:

```
awplus# configure terminal
awplus(config)# service http
```

You can use an AMF working set command to configure this option on all your devices:

```
awplus# atmf working-set group all
AMF[10]# configure terminal
AMF[10](config)# service http
```

## Allow Vista Manager EX to discover the AMF network

Run the following commands on your AMF controller (if you have one in your network) and all AMF masters to allow Vista Manager EX to discovery your AMF network:

```
awplus# configure terminal
awplus(config)# atmf topology-gui enable
```

## Configure the AMF log event host

If the AMF controller or AMF master you intend to register with Vista Manager EX is configured to send event notifications to Vista Manager EX, then Vista Manager EX will display them on its dashboard and event log page.

This command need only be run on the AMF controller/master registered with Vista Manager EX:

```
awplus# configure terminal
awplus(config)# log event-host <ip-address> atmf-topology-event
```

**Note:** The IP address is the address of the server that Vista Manager EX is running on.

**Note:** The AMF controller/master you intend to register with Vista Manager EX must have layer 3 connectivity to the Vista Manager EX server.

## Configure certificate for device authentication

Vista Manager is able to be configured to use a certificate to authenticate communication within your AMF network. Once the AMF controller/master has been configured, this process is automatic, and allows the controller/master to authenticate and connect to any device in the network without requiring a username and password.

**Note:** The use of this feature is optional, but highly recommended. If you do not configure this option, you will need to ensure that all devices in the AMF network to be managed by Vista Manager have the same username and password as the AMF controller/master.

To configure your AMF network to use certificate authentication, enter the following commands on your AMF controller/master:

```
awplus# configure terminal
awplus(config)# crypto pki trustpoint <trustpoint-name>
awplus(ca-trustpoint)# enrollment selfsigned
awplus(ca-trustpoint)# rsakeypair <key-name>
awplus(ca-trustpoint)# exit
awplus(config)# exit
awplus# crypto pki authenticate <trustpoint-name>
awplus# crypto pki enroll <trustpoint-name>
awplus# configure terminal
awplus(config)# atm trustpoint <trustpoint-name>
```

**Note:** Save this configuration and reboot your AMF controller/master after running the **atmf trustpoint** command for this change to take affect.

**Note:** In an AMF network with multiple areas, this process only needs to be carried out on the controller/master. It does not need to be repeated on each individual area's master.

This functionality is disabled by default, but it is recommended that it is enabled. If you need to turn this feature on or off, this can be done from Vista Manager configuration settings:

---

Use certificates (recommended):

---

Use password if certificate fails:

---

The **Use password if certificate fails** option can also be enabled. When it is turned **On**, if the certificate authentication fails, it will revert to using the username and password to authenticate. This will only work if all devices have been configured with the same username and password as the controller/master, as mentioned above.

## Connection timeout on masters and controllers

We recommend not changing the session timeout on your AMF master or controller using the **line vty exec-timeout** command. If you do decide to change it, it should not be set to **0**, as this may result in sessions that can't be reached and never time out.

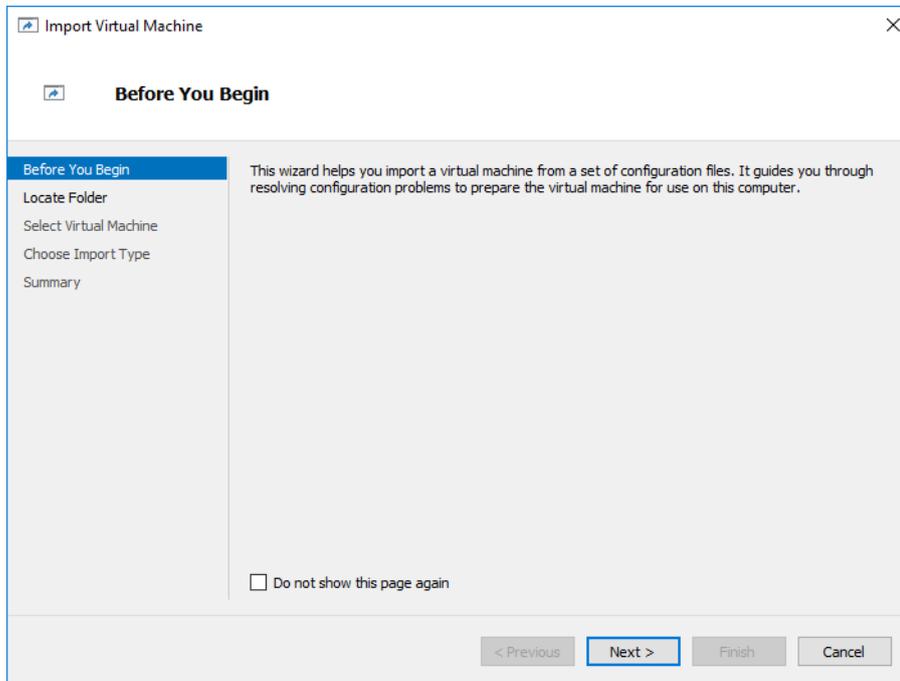
# Installing the Vista Manager EX Virtual Appliance

## Install on Windows Server 2012 R2 Hyper-V

The following instructions describe how to install and configure Vista Manager EX on Hyper-V:

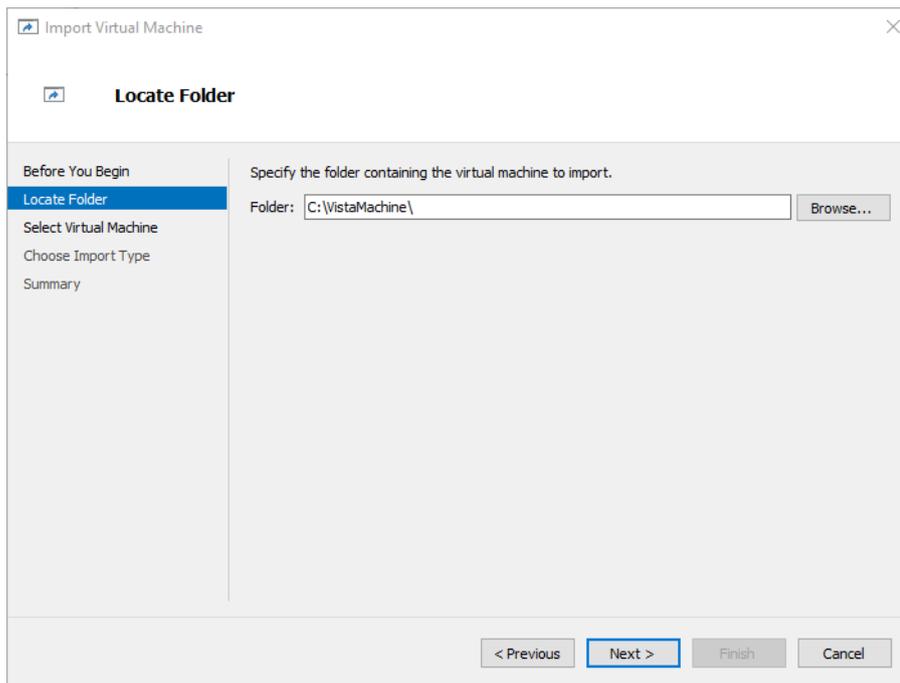
- You can download Hyper-V from the Microsoft website <https://www.microsoft.com/en-us/cloud-platform/windows-server>. Follow the wizard setup instructions.
- You can download Vista Manager EX from the [Allied Telesis download center](#). The Hyper-V image is supplied as an archive file called 'Vista Manager.zip'.
- Extract the contents of this archive to a suitable location.
- Import this virtual machine to Hyper-V from the menu **Action > Import Virtual Machine**. Browse to the virtual machine folder and import it.

The **Import Virtual Machine** wizard displays:



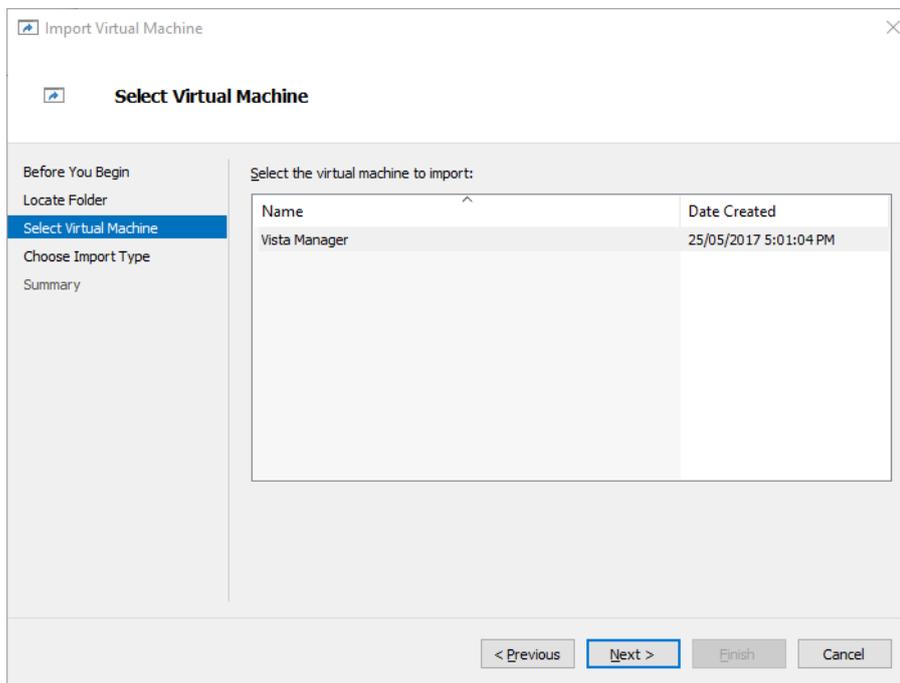
Click **Next**.

The **Locate Folder** dialog displays as follows:



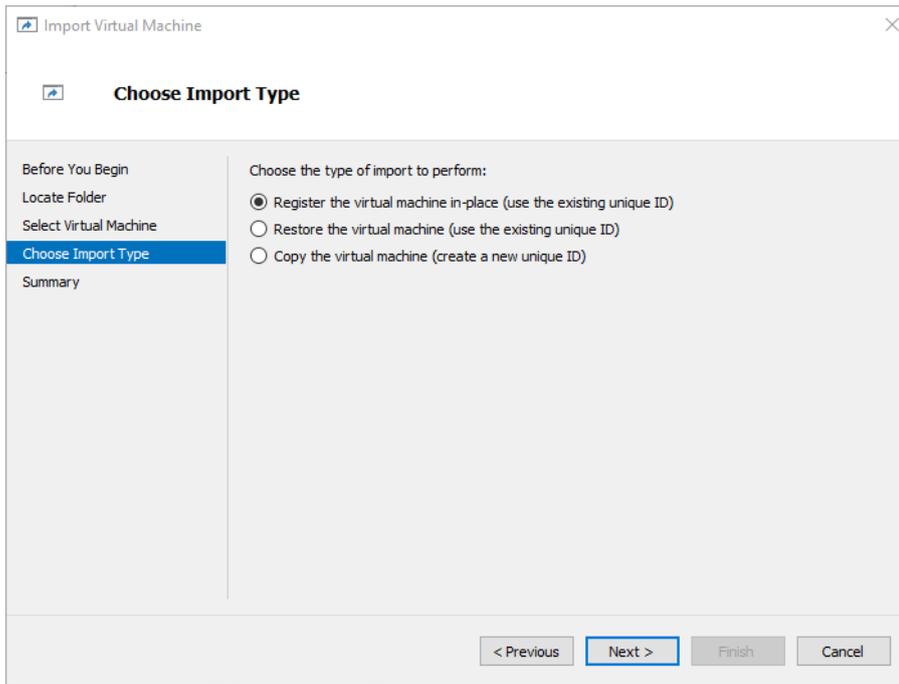
Locate the virtual machine you extracted earlier and click **Next**.

The **Select Virtual Machine** dialog displays:



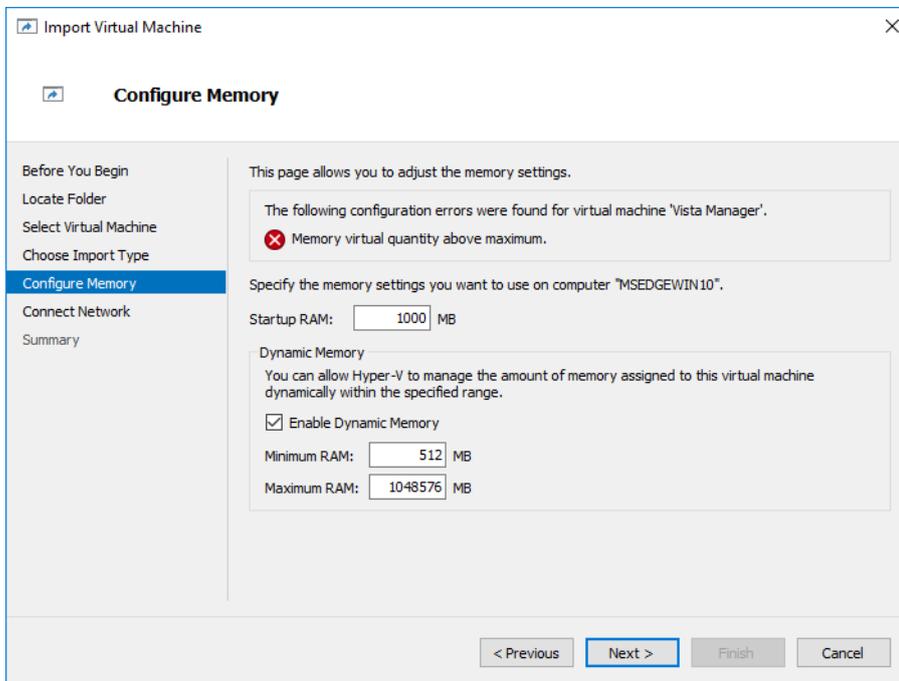
Select the **Vista Manager** virtual machine and click **Next**.

Set the **Import Type** as follows:



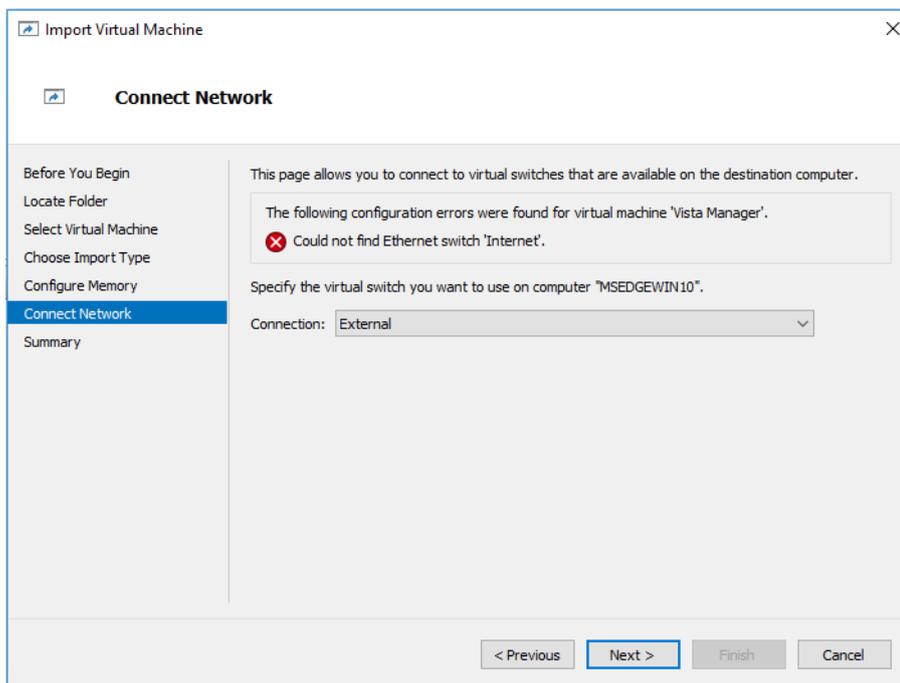
Click **Next**.

The Vista Manager EX virtual machine is configured to run with 1000 MB of memory. If an error message is displayed then select a value appropriate for your hypervisor server.



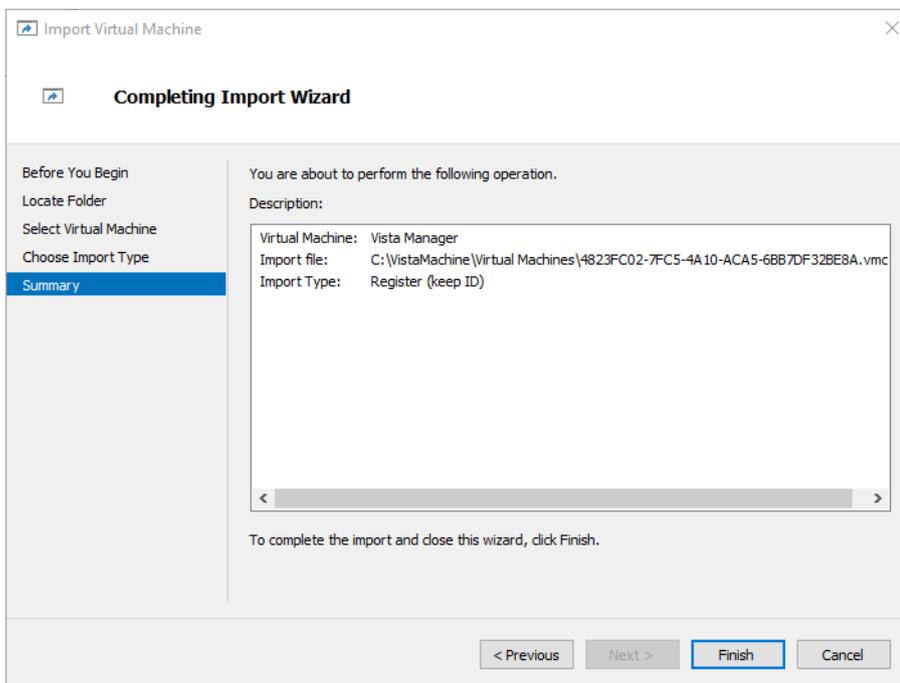
Click **Next**.

The Vista Manager EX virtual machine is configured to run on an external virtual switch named “Internet”. An error message is displayed if there is no switch named “Internet”. Use the **Connection:** drop down list to select an appropriate external switch.

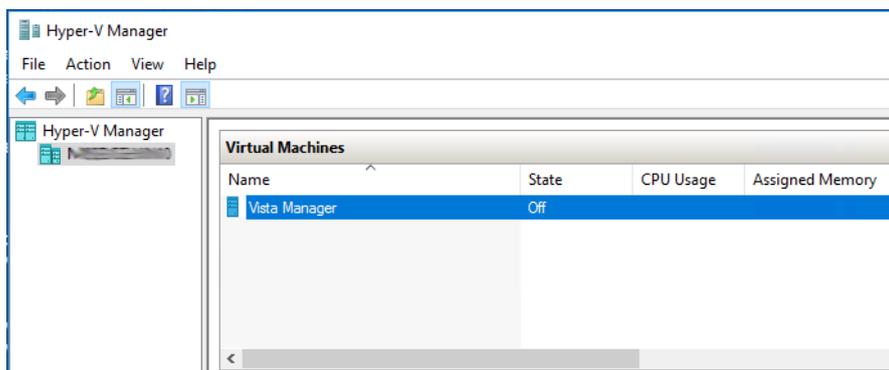


Click **Next**.

On the **Completing Import Wizard** dialog click **Finish**.



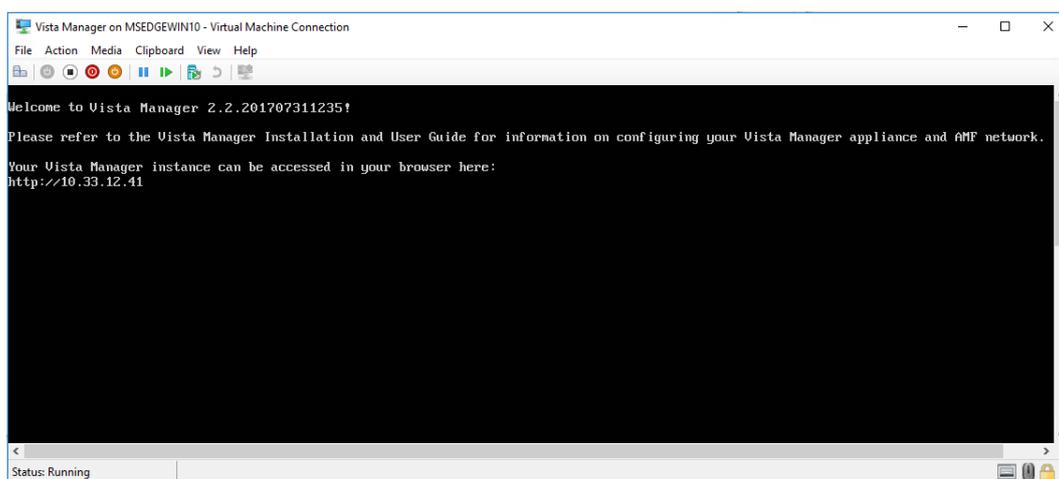
Connect to the Vista Manager EX virtual machine by selecting **Action > Connect** from the Hyper-V Manager menu.



Then select **Action > Start** to start the virtual machine.

During boot up, the Virtual machine will obtain an IP Address from a DHCP server. If no DHCP server is available, or you would prefer to assign a static IP address, then follow the procedure **“Assign a static network configuration” on page 24.**

Once the virtual machine has booted the following window displays:



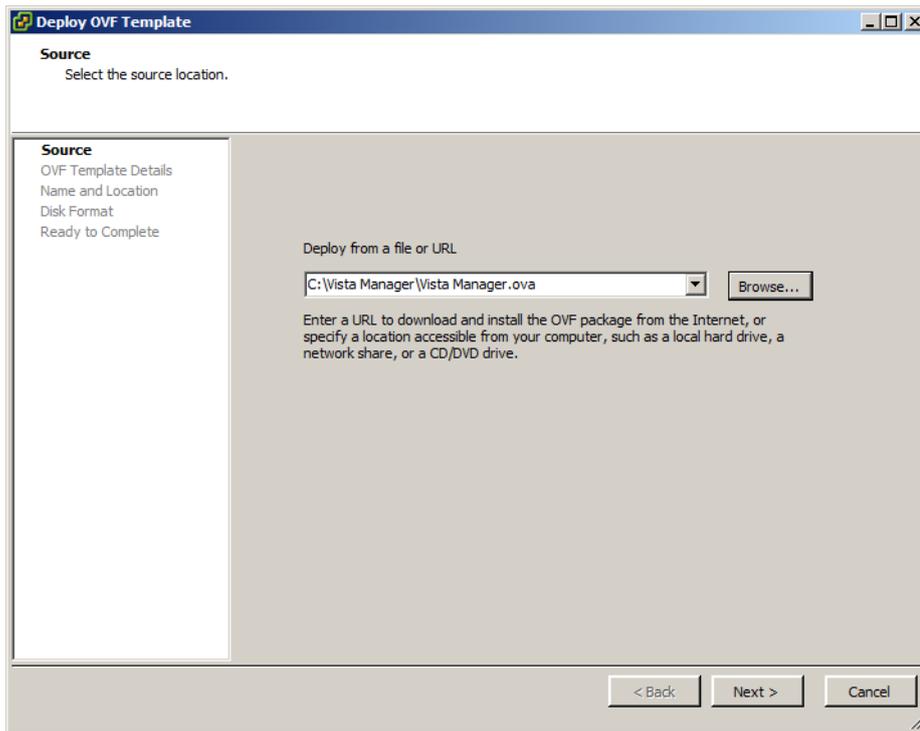
Make a note of the IP address given in this window. You can use it to access Vista Manager EX via a web browser.

## Install on VMware vSphere Hypervisor (ESXi) 6.0/6.5/6.7

The following instructions describe how to install and configure Vista Manager EX on VMware:

- You can download VMware from <https://www.vmware.com>. Follow the wizard setup instructions.
- You can download Vista Manager EX from the [Allied Telesis download center](#). The executable file is called 'Vista Manager.ova'.
- Deploy the 'Vista Manager.ova' file to VMware from the menu **File > Deploy OVF Template**. Browse to the '.ova' file and deploy it.

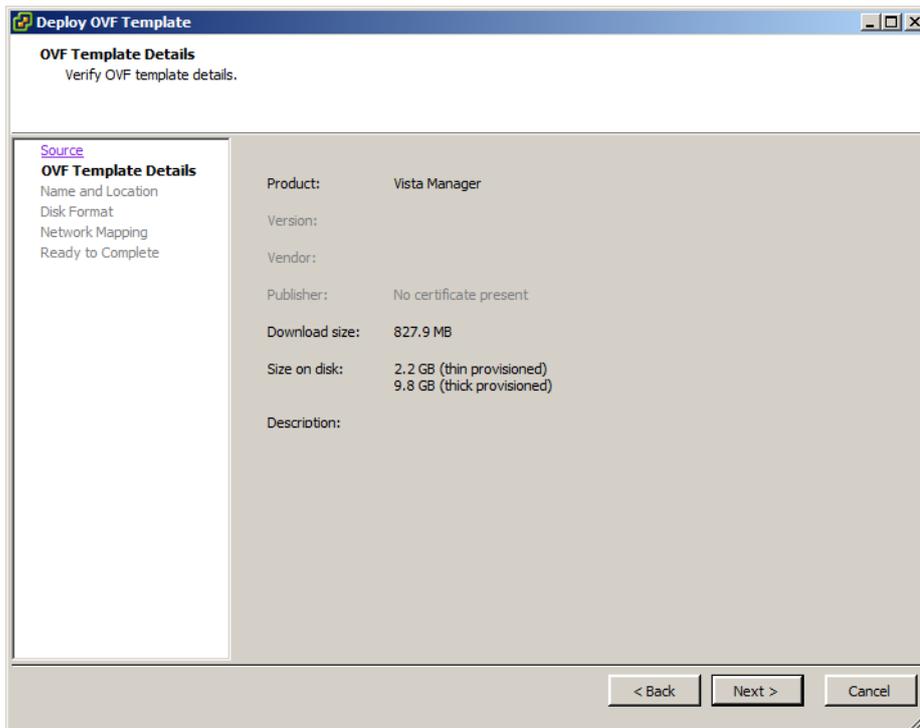
The **Deploy OVF Template** dialog displays:



Browse to the downloaded “.ova” file location, select it, and click **Next**.

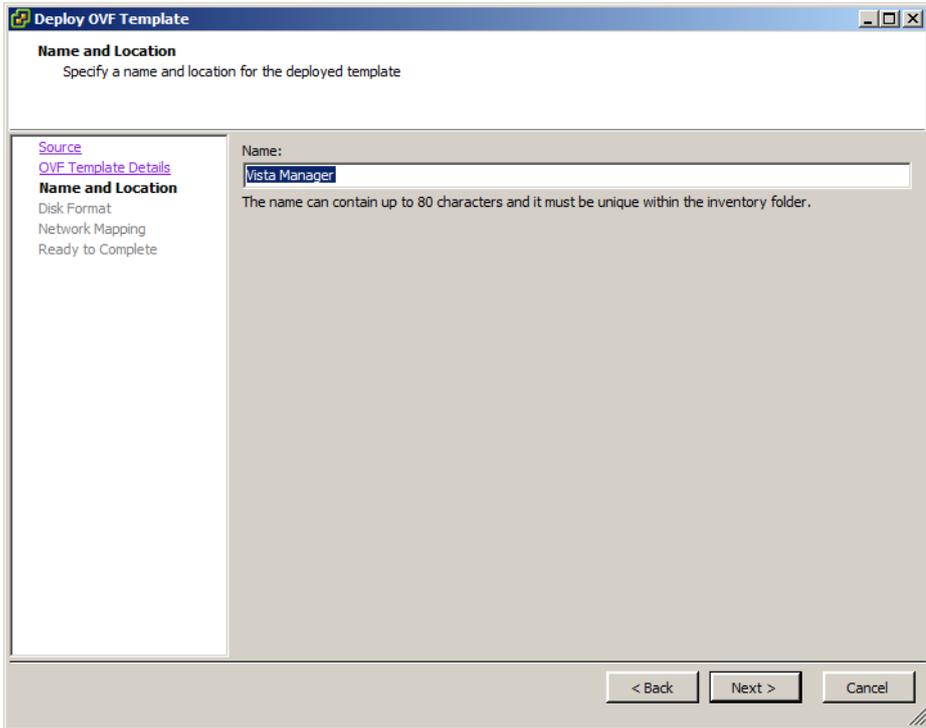
**Note:** If you are using a version earlier than VMware vSphere Hypervisor (ESXi) 6.7, you may receive a warning about the OVF package. If you do receive this warning, click Yes to continue.

The **OVF Template Details** dialog displays:



Click **Next** to proceed.

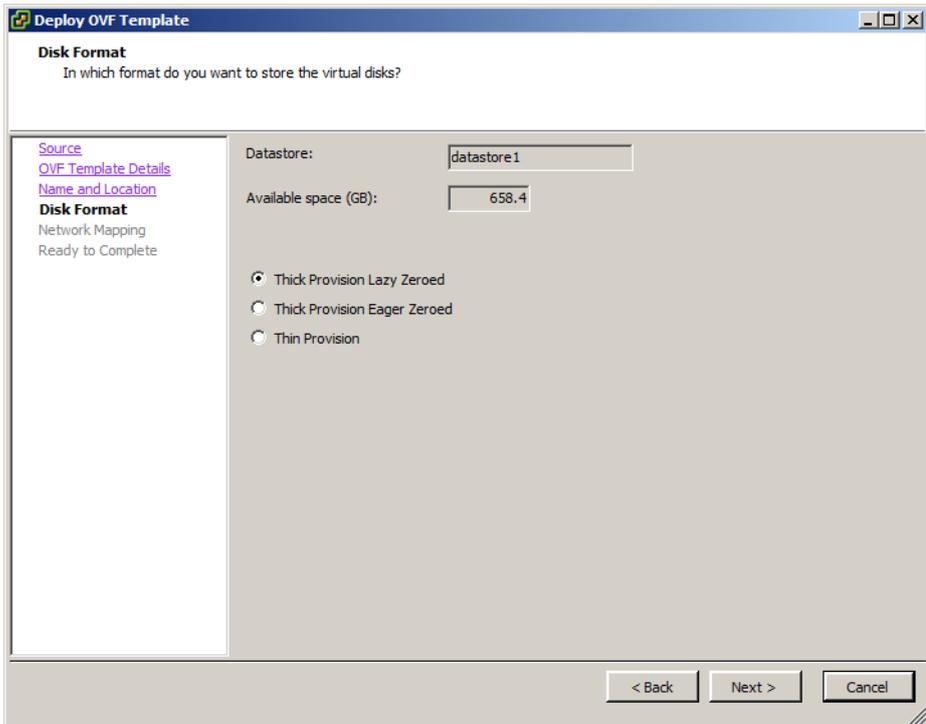
The **Name and Location** dialog displays:



Enter an appropriate name for your virtual machine and click **Next**.

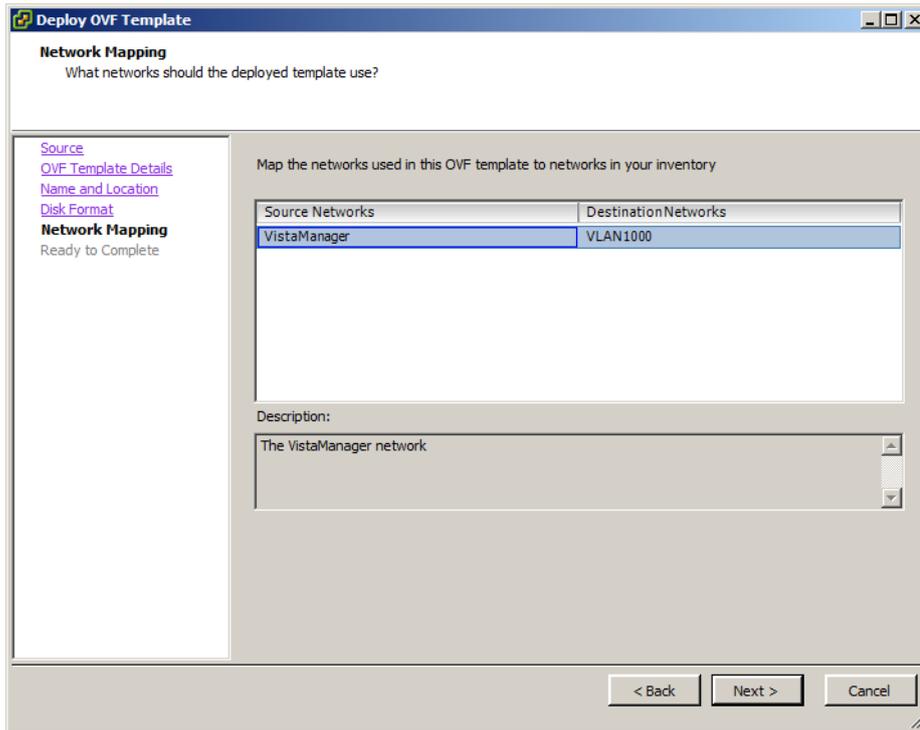
If you have Resource Pools and Network Storage configured you will be prompted to choose an appropriate Resource Pool and Network Storage to host the virtual machine.

The **Disk Format** dialog displays:



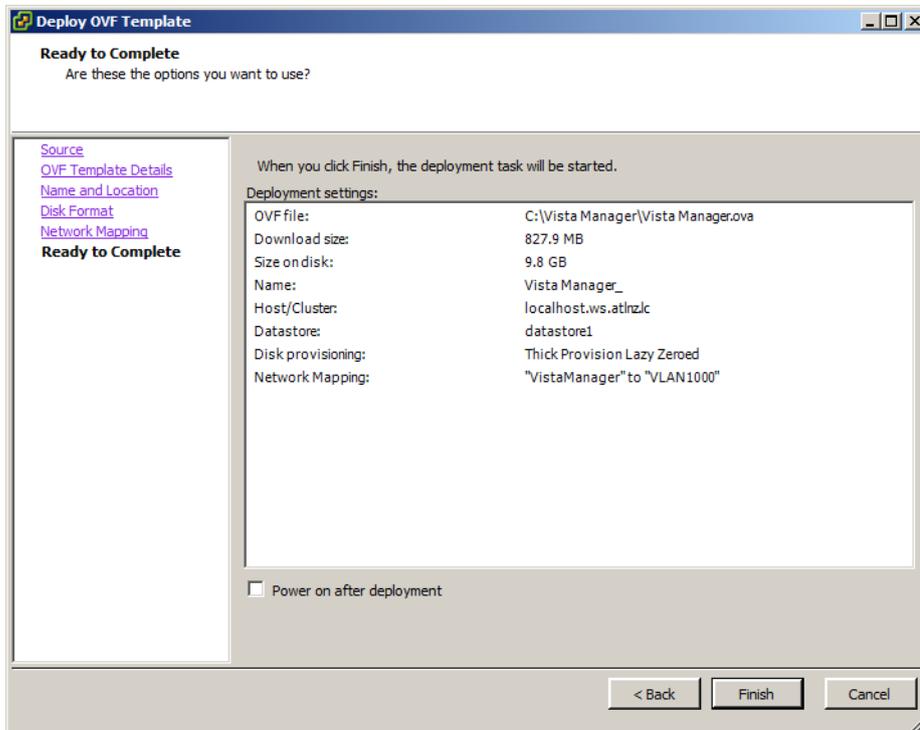
Pick a suitable provision method and click **Next**.

The **Network Mapping** dialog displays:

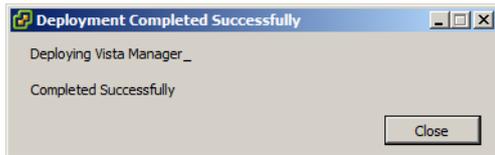


Select an appropriate bridged network, one that has access to the devices you wish to manage using Vista Manager EX, and click **Next**.

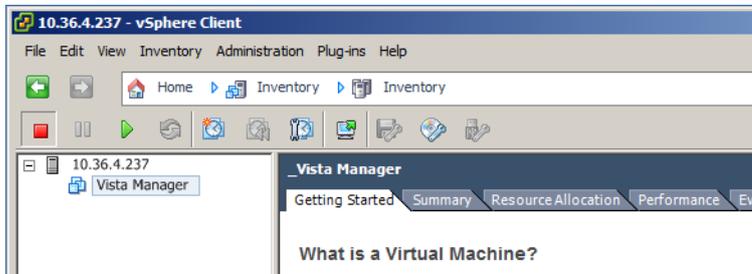
On the **Ready to Complete** dialog click **Finish**:



Once the deployment is complete you will see the **Deployment Completed Successfully** dialog.

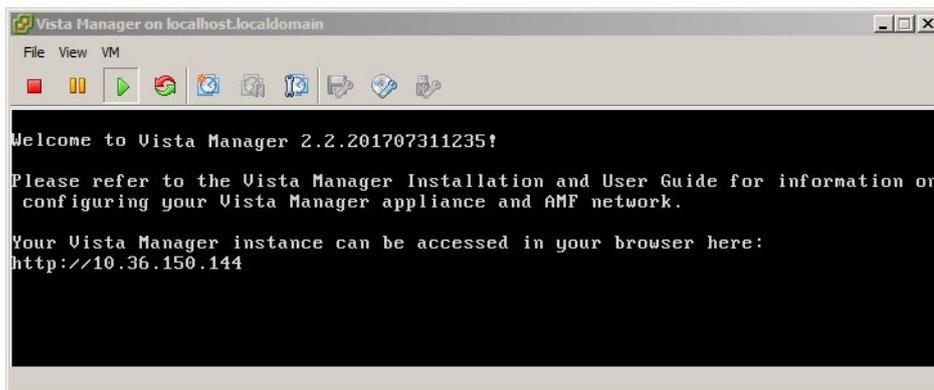


Use the toolbar to power on the Vista Manager virtual machine and open the console



During boot up, the Virtual machine will obtain an IP Address from a DHCP server. If no DHCP server is available, or you would prefer to assign a static IP address, then follow the procedure from **[“Assign a static network configuration” on page 24.](#)**

Once the virtual machine has booted the following window displays:



Make a note of the IP address given in this window. You will use it to access Vista Manager EX via a web browser.

# Additional Installation Tasks

## Assign a static network configuration

Assigning a static network configuration is optional and only required if there is no DHCP server to automatically configure the Vista Manager EX virtual machine's network settings.

**Note:** This option is only available on virtual machine installations.

Vista Manager EX uses **Netplan** to configure the network. (For more information see <https://netplan.io>.)

### Step 1: Create a Netplan configuration file

Create a netplan configuration file (.yaml) on your system in a text editor of your choice. We recommend you name this file **01-netcfg.yaml** to fit Netplan naming conventions.

### Step 2: Format the '01-netcfg.yaml' file with the following contents

Below is a sample configuration. Use settings appropriate for your network and hypervisor configuration.

**Note:** The formatting of this file is very specific. The text indentation is required, and all indentation must be done with spaces, not with tabs (e.g: The 'search:' key is indented by 8 spaces, not 1 tab). For more information on YAML files, see <https://yaml.org/spec/1.2/spec.html>.

```
network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      addresses:
        - 192.168.1.100/24
      gateway4: 192.168.1.254
      nameservers:
        search: [mydomain, otherdomain]
        addresses: [192.168.100.1, 1.1.1.1]
```

### Step 3: Create an ISO image containing this single file on your system.

Use the terminal on the host system you are deploying your virtual machine on, and create an ISO image containing the YAML file created in the previous step.

The command using the Linux 'genisoimage' utility to create an ISO image called 'netplanconfig.iso' is:

```
genisoimage -output netplanconfig.iso -volid cidata -joliet -rock 01-netcfg.yaml
```

The command using the Windows 'mkisofs' utility to create an ISO image on Windows is:

```
mkisofs -output netplanconfig.iso -volid cidata -joliet -rock 01-netcfg.yaml
```

### Step 4: Mount the "netplanconfig.iso" as the CD/DVD image of the virtual machine and reboot to apply.

If you want to change the static IP address, you need to reboot the virtual machine with a new ISO image in the CD/DVD drive. Leave the ISO image inserted in the CD/DVD drive for all reboots.

## Ports used by Vista

Vista Manager EX makes use of the following ports. These ports may need to be configured on your firewall:

- UDP port 514 (syslog), used by the AMF master/controller to send logs to Vista Manager EX.
- TCP port 443 (HTTPS), used if the HTTPS mode of Vista Manager EX is enabled.
- TCP ports 443 and 12943, used if you are not using certificates for device authentication.
- TCP ports 12945 and 12946, used if you are using certificates for device authentication (recommended).

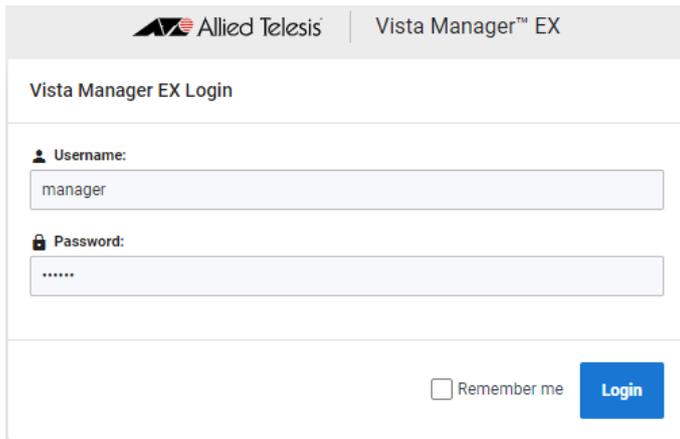
# Initial login

## Login to Vista Manager EX

To connect to Vista Manager EX from a remote machine use the URL <http://<ip address>>, where **<ip address>** is the address displayed on the Vista Manager EX appliance console screen after it boots.

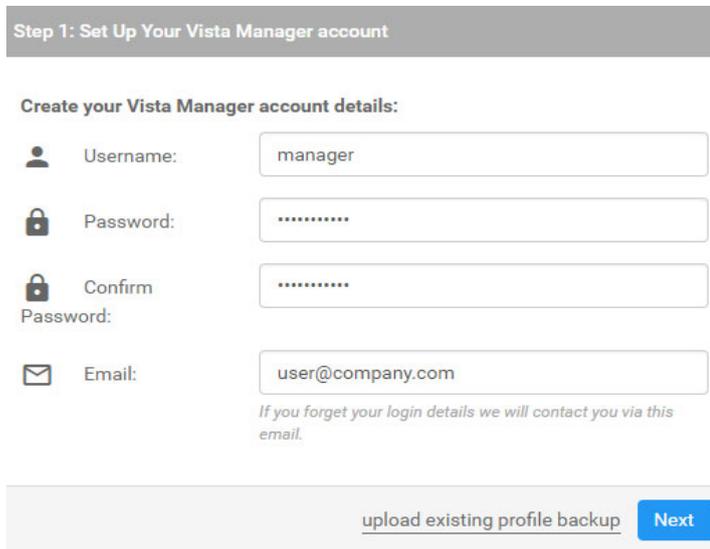
**Note:** Vista Manager requires JavaScript to be enabled in your web browser.

From the **Vista Manager Login** dialog:



- Enter the **Username** manager
- Enter the **Password** friend
- Click **Login**

The **Set Up Your Vista Manager account** dialog displays:



- Enter your **Username**
- Enter your **Password**
- Re-enter your Password to **Confirm**
- Enter your **Email**
- Click **Next**.

If you want to use a backup to restore a previous database, click **upload existing profile backup**.

The **Upload License File** dialog displays:

Step 2: Upload License File

Please upload your Vista Manager EX licenses file.

The licenses file you provided should be associated with the following Vista Manager EX serial number.

Serial Number: 610b416b-1d86-4f68-a30c-29cd130dc567

Select License File:  No file chosen

If you do not have a license file, please contact Allied Telesis.

[Use 90 day trial license](#) [upload backup file](#) [Next >](#)

- Click **Choose File** to upload your Vista Manager EX license file
- Click **Next**.

**Note:** If your licenses file is not associated with the Serial Number listed in your dialog or you do not have a license file, then contact your authorized Allied Telesis support center to obtain a license.

**Note:** If this is the first time you are using Vista you have the option to apply the 90 day trial license. This gives you full access to Vista Manager EX for 90 days.

The **Set Up Your Network** dialog displays:

Step 3: Set Up Your Network

Enter AMF Network Master or Controller IPv4 or IPv6 Address or Domain Name:

10.37.223.34

Enter AMF Network Master or Controller Username and Password:

Username: manager

Password: .....

[upload existing profile backup](#) [Next >](#)

- Enter the **IP Address** for the AMF Master or Controller
- Enter the AMF Controller or Master **Username**
- Enter the AMF Controller or Master **Password**

**Note:** The Master (or Controller) username and password must be for a user with level 15 (full access) privileges.

The **Set Up Your SMTP settings** dialog displays:

Step 4: Set Up Your SMTP settings

Enter the IP address of your SMTP server, which will be used to email Vista Manager users to verify account details, and for password retrieval.

Enter your internal network's SMTP server:

xxx.xxx.xxx.xxx

Enter your SMTP server's username and password:

Username: manager

Password: .....

[do this later](#) [Proceed >](#)

- Enter the **IP Address** of your SMTP server
- Enter the SMTP Server **Username**
- Enter the SMTP Server **Password**

You will receive a message saying that the set up is successful.

# Troubleshooting

## Ports and URLs used by Vista Manager EX

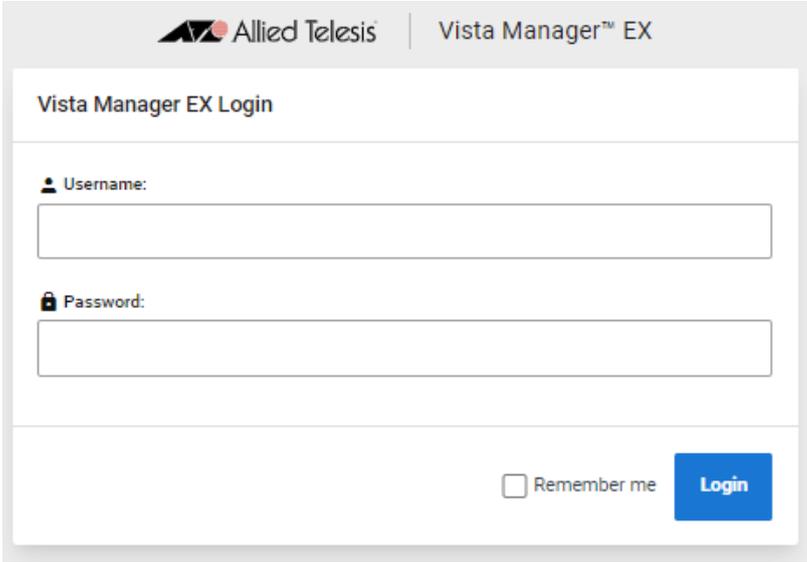
You can use these settings to check that Vista Manager and the plugins are installed correctly.

1. After installation, Vista Manager EX, and the plugins, will be installed on the following ports.

Vista Manager	Port 5000
AT-AWC	Port 5443
AT-SNMP	Port 6443

2. You can test that Vista Manager is working correctly by using the following URL:

- <http://localhost:5000>



3. You can test whether the plugin APIs are active using the following URLs:

- [https://localhost:5443/wireless\\_plugin/api/plugin\\_registration](https://localhost:5443/wireless_plugin/api/plugin_registration)

```
{"version":"100","baseUrl":"http://localhost:8080/wireless_plugin/api","product":{"name":"AT-Vista Manager plugin","type":"awc","version":{"major":"1","minor":"2","revision":"0","build":"B06"},"capabilities":["node"]}
```

- [https://localhost:6443/NetManager/api/plugin\\_registration](https://localhost:6443/NetManager/api/plugin_registration)

```
{"version":"1.0.0","baseUrl":"http://10.33.24.38/NetManager/api","product":{"name":"SNMP Plugin","type":"anr","version":{"major":"1","minor":"0","revision":"0","build":"B04"},"capabilities":["menu","event"]}}
```

**Note:** These URLs can only be used locally on the Vista Manager server using “localhost”.

## Allow Vista Manager EX to discover the AMF network

If, after installation, there are no devices on the AMF network/area map check that the following command has been run on your AMF controller (if present) and all AMF masters.

```
awplus# configure terminal
awplus(config)# atmf topology-gui enable
```

## Reboot AMF master/controller after configuring certificates

If you receive the following error message:

```
Error during polling - Error: Device did not accept a certificate request
and basic auth fallback is disabled. Details: Error: connect ECONNREFUSED
xxx.xxx.xxx.xxx:12946
```

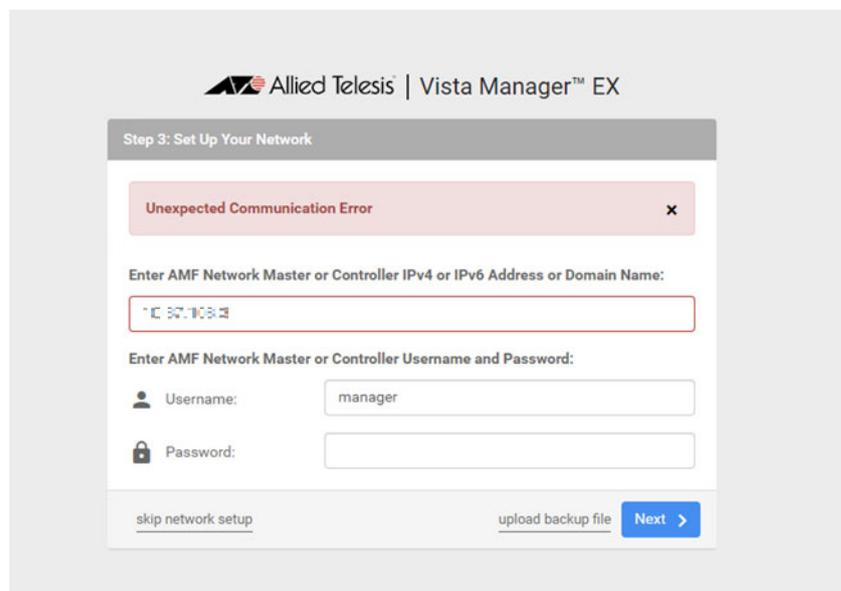
Check that you have correctly configured your AMF master/controller for certificate authentication and that you saved your configuration and rebooted your master/controller after running the **atmf trustpoint** command (see "[Configure certificate for device authentication](#)" on page 13).

## Clear browser cache

Clear your browser's cache after upgrading your Vista Manager EX installation. Incomplete dialog boxes, incorrectly populated drop-down lists, and truncated forms are all symptoms of a caching problem.

## Unexpected Communication Error during installation

During Step 3: Set Up Your Network in the installation process, you may receive the following error:



This is due to the **atmf topology-gui enable** command not having been run on the master. You can resolve this by running the command on the master, then clicking the Next button.

For further information, refer to "[Allow Vista Manager EX to discover the AMF network](#)".

# Supported Devices

Vista Manager EX supports all current AlliedWare Plus products. For more information, see your products datasheet:

- [Vista Manager EX Datasheet](#)

C613-04081-00 REV M



NETWORK SMARTER

**North America Headquarters** | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895

**Asia-Pacific Headquarters** | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830

**EMEA & CSA Operations** | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

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

© 2024 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.