Technical Guide

Vista Manager EX

Windows-based Installation Guide

Introduction

Vista Manager EX

Vista Manager EX™ is a visual network monitoring and management tool for your network. With the use of additional Allied Telesis Autonomous Management Framework™ (AMF) Plus tools, you can further monitor the health of devices and network areas, and use a variety of Intent Network features.

Vista Manager EX automatically creates a complete topology map from your network of various switches, firewalls and wireless access points and routers. 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.

Vista Manager EX includes the following tools from the sidebar to monitor your network:

- Dashboard
  Displays your network details and a small 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.
- Network Map
  Displays a graphical topology map of your network. From here you can view pop up details of an area that displays the number of devices, device names, and IP addresses. Actions such as backing up the AMF master, connecting to the master with SSH, and backing up a device can be carried out directly from the network map.
- Health Monitoring
  Displays a customisable dashboard to monitor the health of devices in your network.
- Events
  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.

- 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 Services
  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.
- Intent Networks
  Provides network optimization, automation, management, and visualization.
- WAN
  Offers automation of branch security and WAN bandwidth management.
  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.

AWC plug-in

Applicable to Windows-based Vista Manager installations with the AWC plug-in.

Allied Telesis Autonomous Wave Control (AWC) is an advanced network technology that utilizes game theory to deliver significant improvements in wireless network connectivity and performance. AWC can automatically minimize coverage gaps and reduce Access Point (AP) interference and respond to network configuration changes and bandwidth demands from user devices.

AWC is closely integrated with Allied Telesis Autonomous Management Framework (AMF) and is managed by Allied Telesis Vista Manager EX. AWC is available as an optional plug-in to Vista Manager.

SNMP plug-in

Applicable to Windows-based Vista Manager installations with the SNMP plug-in.

Note: From Vista Manager version 3.11.0 onwards, the SNMP plug-in is enabled by default in an AMF Plus environment. This means that if you have a current active and enabled AMF Plus license on your AMF masters and controllers, then the functionality of the SNMP plug-in is available to you. There is no setup required for you to use this.

The Vista Manager SNMP plug-in can acquire detailed information and statistics from a broad range of networking devices. Different views enable users to manage devices the way they prefer. It supports management of up to 2000 devices, and in large networks it automatically searches for

SNMP agents and displays each device found in tree form, for an easy view of the overall network topology. The SNMP plug-in is a powerful addition to Vista Manager EX, adding management flexibility by supporting non-AMF devices.

The SNMP plug-in also offers a MIB compiler, and generates a chart based on MIB values. It offers support for iMG devices and basic SNMP management, like alive monitoring and access to the iMG GUI. You can also backup and restore your settings.

The SNMP plug-in is closely managed by Allied Telesis Vista Manager EX and is available as an optional plug-in to Vista Manager.

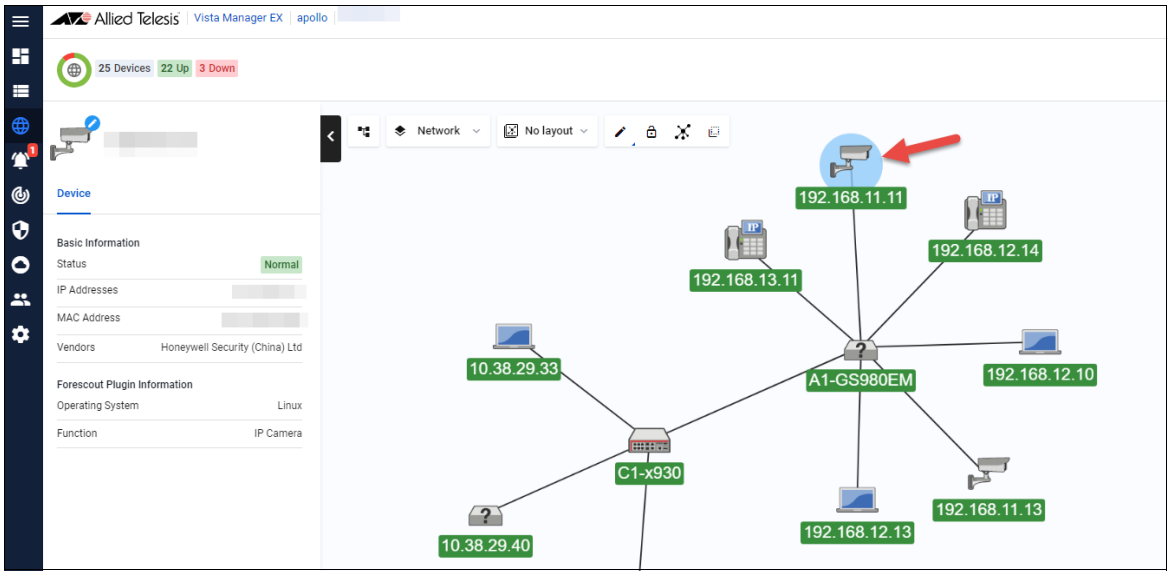
Forescout

Applicable to Windows-based Vista Manager installations with the Forescout plug-in.

The Forescout plugin automatically discovers non–Allied Telesis devices and displays them as dynamic icons on the network map. It also displays information about those devices in the side panel summary. Vista Manager polls Forescout every 5 minutes to retrieve the latest information.

Additionally, Forescout classifies each device by device type. Vista Manager then uses this information to automatically select an appropriate icon specific to each discovered device. Examples of such devices could be printers, phones, cameras or personal computers connected to your network. As a result, you see a more complete view of your network.

For example, the following figure shows a Honeywell IP camera that has been discovered through the Forescout plugin.



You can also:

- create a group of Forescout-discovered devices from the map or Asset Management page. For example, you can make a group of all your printers.
- change the default icon for different discovered devices.
- manually add custom links between a discovered device and an Allied Telesis device via the Edit layer of the map.

Note that Vista Manager EX only displays the information that Forescout has discovered. Forescout only finds links to edge devices, so the complete topology with links may not display. To resolve this, you can manually add custom links to the Vista Manager EX map.

Nozomi Plugin

Applicable to Windows-based Vista Manager installations with the Nozomi plug-in.

From version 3.12.0 onwards, Vista Manager supports the Nozomi plugin.

You must first configure the Nozomi Guardian sensor prior to registering it in Vista Manager EX.

To see information about the configuration of Nozomi, see the following documentation:

- Nozomi Plugin User Guide.
- Vista Manager EX User Guide.

Audience for this guide

This guide is intended for computer system administrators and network engineers. It describes how to install **Windows-based** Vista Manager EX, with optional plug-ins. For information on how to install a Vista Manager EX **virtual appliance**, see the Vista Manager EX Virtual Appliance 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 and AMF Plus:

- AMF Plus and AMF Feature Overview and Configuration Guide
- AMF Feature Overview and Configuration Guide (for earlier software versions)
- AMF Introduction and videos

These documents are available from the links above or on our website at alliedtelesis.com

Contents

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.

Upgrading requirements

In order to upgrade and install the latest version of Vista Manager EX, you must first uninstall the previous version. To see how to uninstall Vista Manager EX, see "Uninstalling Vista Manager EX" on page 32.

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 Windows OS versions

- Windows 10 Pro (64bit)
- Windows Server 2016 (Standard, Datacenter edition
- Windows Server 2019 (Essential, Standard, Datacenter edition)

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.

Wireless AP network support

Vista Manager EX with the AWC plug-in supports up to 3000 wireless APs. The following limits apply to wireless AP setups:

- Maximum number of AP management groups: 100
- Maximum number of AP profiles: 300
- Maximum number of concurrent AP operations: 350
- A maximum of 120 APs can be added to a single floor map.

MAC address list

The maximum number of APs that can be registered in the MAC address list is 2048. Supported AP models are TQ5k and TQ1k series only.

For other models, the maximum number of registered APs is 1024.

Station location and channel blanket

If Station Location is enabled, the maximum number of APs that can have a channel blanket profile applied is 500.

SNMP network support

Vista Manager EX with the SNMP plug-in supports up to 2000 SNMP devices.

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.

Auto recovery

The AWC plug-in auto-recovery feature requires that the APs are running AlliedWare Plus version 5.4.8-1.x or later.

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

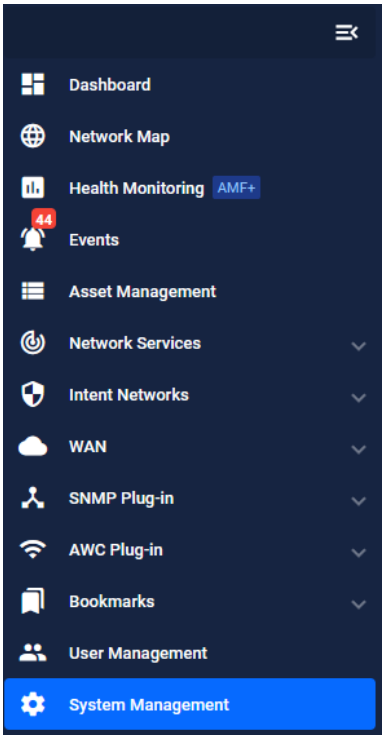
Vista Manager EX licensing is subscription based. Download the license file from the Allied Telesis download center. The base license file is applied during the Vista Manager software installation procedure. Subscription licenses are tied to the Vista Manager database and are maintained across backups 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.

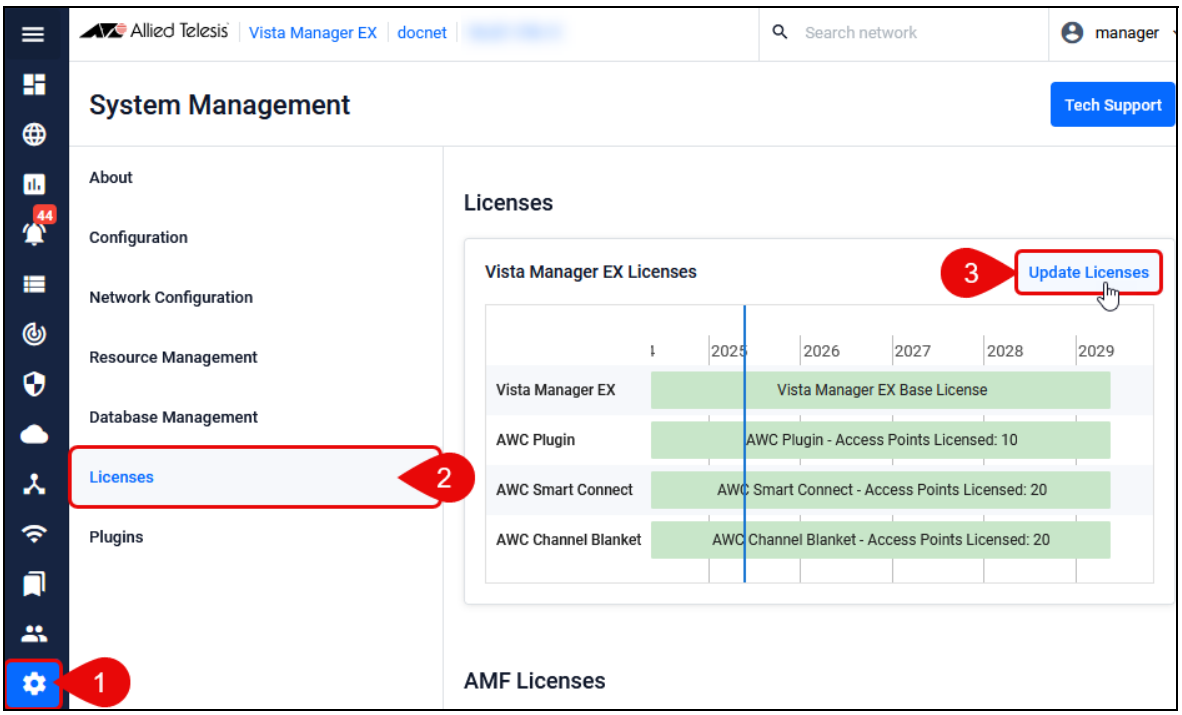
Managing your licenses

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



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.



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.

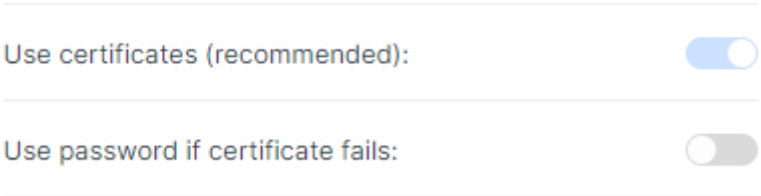
To configure your AMF network to use certificate authentication, enter the following commands on your AMF controller/master:

```
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)# atmf 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:



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.

Install Vista Manager EX on Windows

We recommend that you start with a fresh Microsoft Windows OS installation. While it is possible to make use of an existing installation, the setup process is influenced by security settings, patches, upgrades, etc. You will need more experience with running web-based applications on Windows to install on an existing installation.

Microsoft Windows requirements

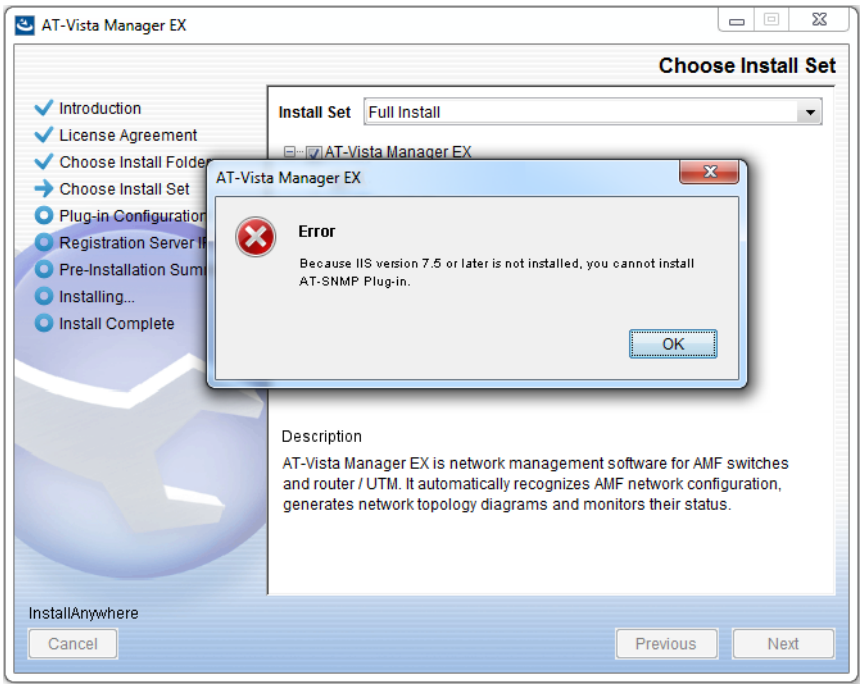
Note: These requirements are only necessary if you are installing the SNMP plug-in, as it runs on Windows Internet Information Services (IIS).

The SNMP plug-in requires the following to be installed/configured on Microsoft Windows **before** installation:

- IIS version 7.5 or later (this is shipped with Windows)
- .NET Framework version 4.8 or later
- ASP.NET
- .NET Extensibility

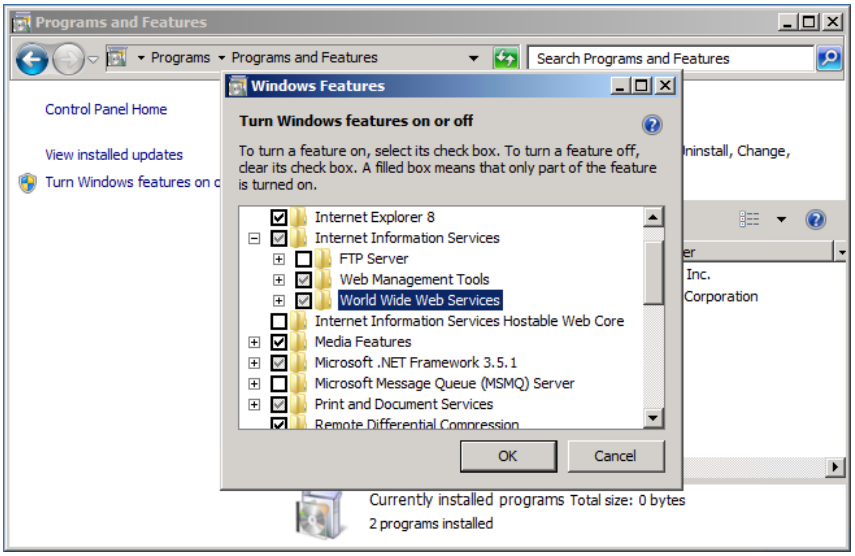
Internet Information Services (IIS)

IIS 7.5, or later, is shipped pre-installed on all supported versions of Windows. It needs to be enabled for the SNMP plug-in to operate. If you receive the following error message during installation please enable IIS.



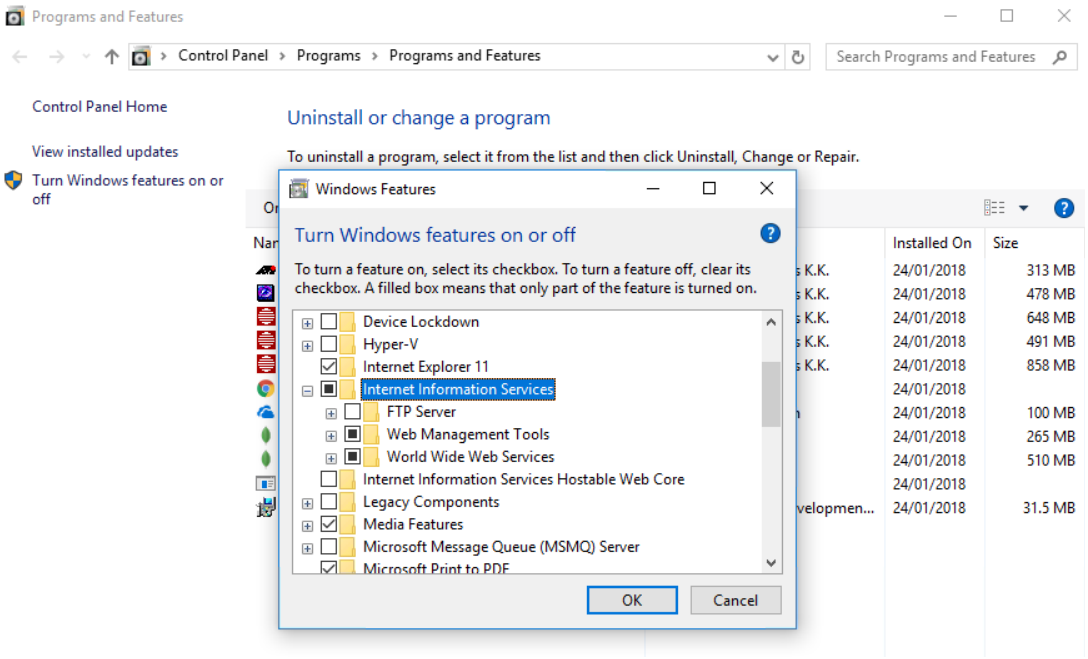
Windows 7

1. On Windows 7select the **Programs and Features** dialog.
2. Click **Turn Windows features on or off**.
3. Open up the **Internet Information Services** feature and ensure that **World Wide Web Services** and **Web Management Tools** are selected.

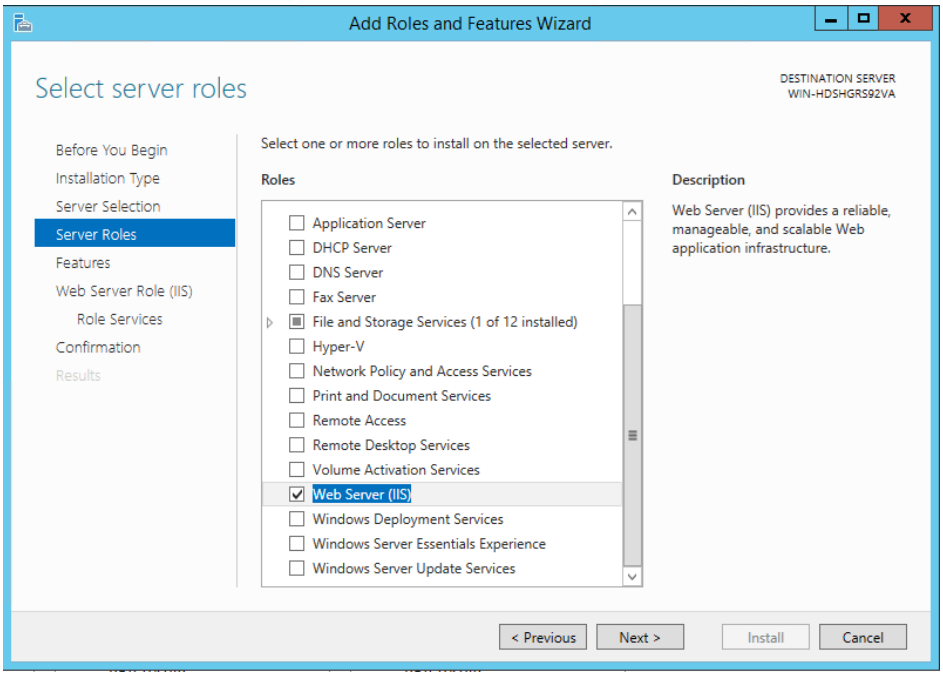


Windows 10

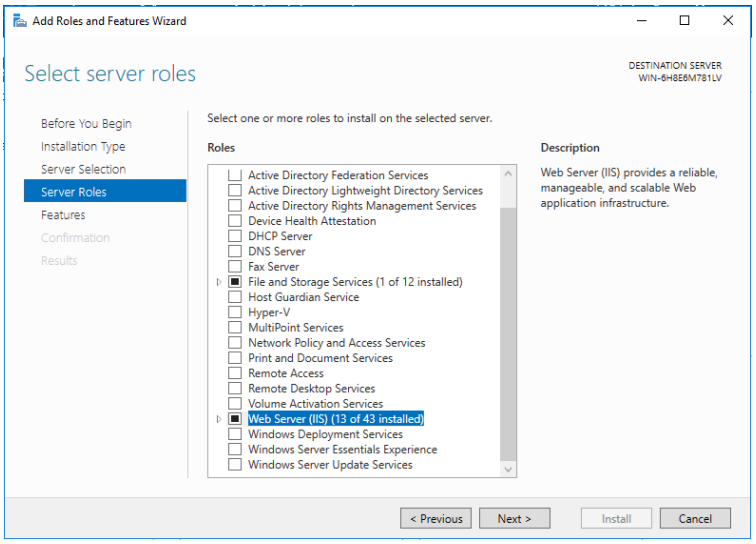
1. On Windows 10 select the **Programs and Features** dialog.
2. Click **Turn Windows features on or off**.
3. Open up the **Internet Information Services** feature and ensure that **World Wide Web Services** and **Web Management Tools** are selected.



Windows Server 2012 On Windows Server 2012 R2 use the **Add Roles and Features Wizard** to add the **Web Server (IIS)** role.

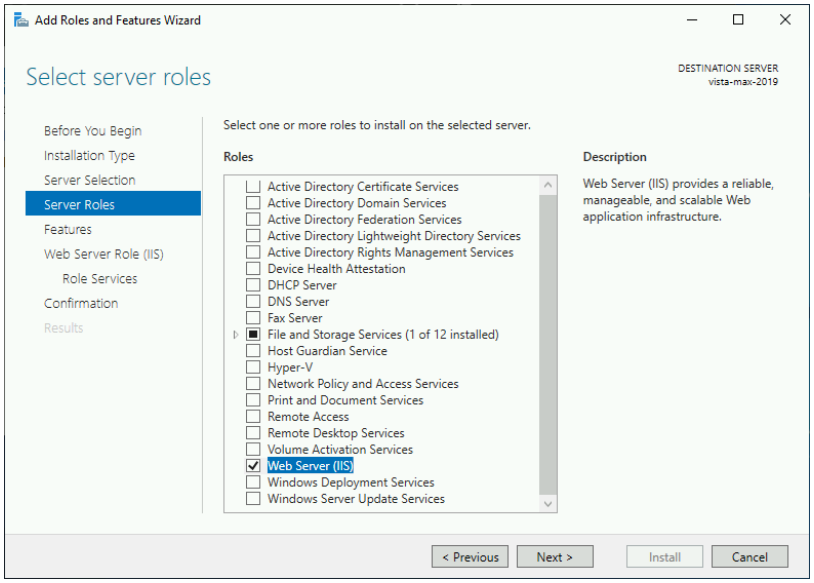


Windows Server 2016 On Windows Server 2016 use the **Add Roles and Features Wizard** to add the **Web Server (IIS)** role.



Windows Server 2019

On Windows Server 2019 use the **Add Roles and Features Wizard** to add the **Web Server (IIS)** role.



.NET Framework version 4.8 or later

This can be downloaded from the Microsoft .Net Framework Download page. Alternatively, you can use **Windows Update** to get the latest version of the .Net Framework. If you are installing on Windows Server, you can also install it from the **Add Roles and Features Wizard**.

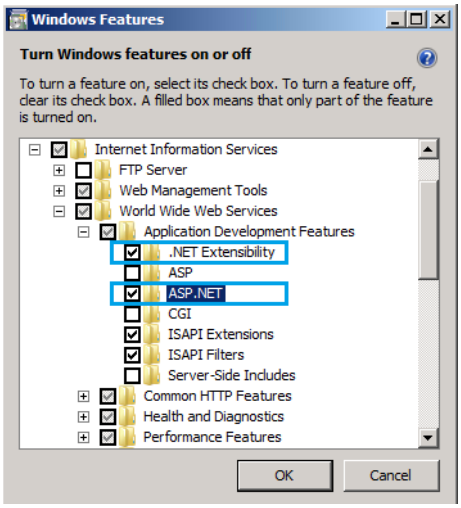
If you are unsure of which version of .Net Framework is installed on your system, see the Microsoft article, How to: Determine Which .NET Framework Versions Are Installed.

ASP.NET and .NET Extensibility

Once IIS is installed and the .Net Framework updated to at least 4.8, add the following ASP.NET and .Net Extensibility Features.

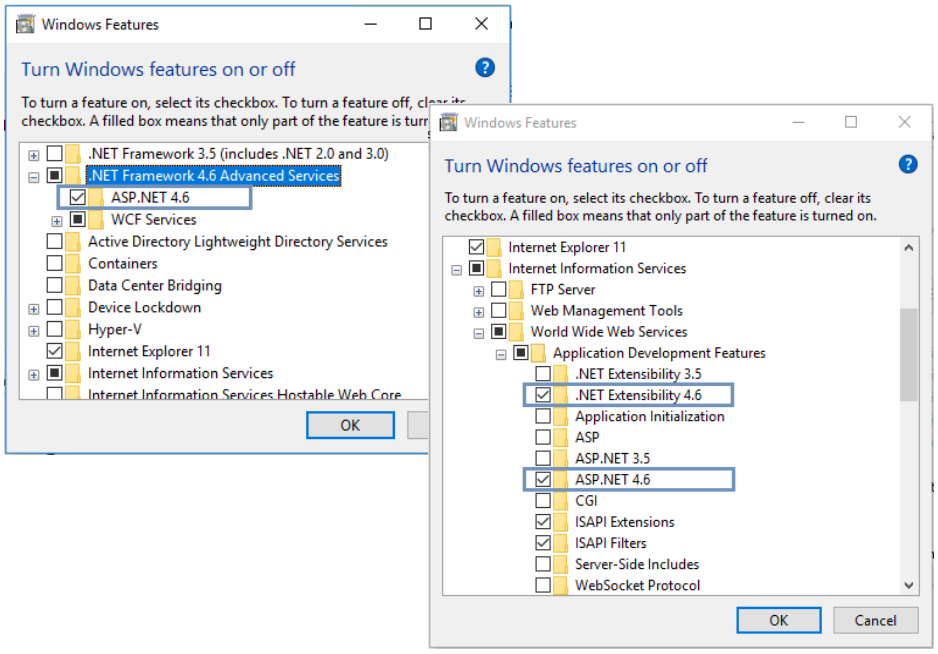
Windows 7

1. On Windows 7 select the **Programs and Features** dialog.
2. Click **Turn Windows features on or off**.
3. Select the features highlighted in the following screenshot.

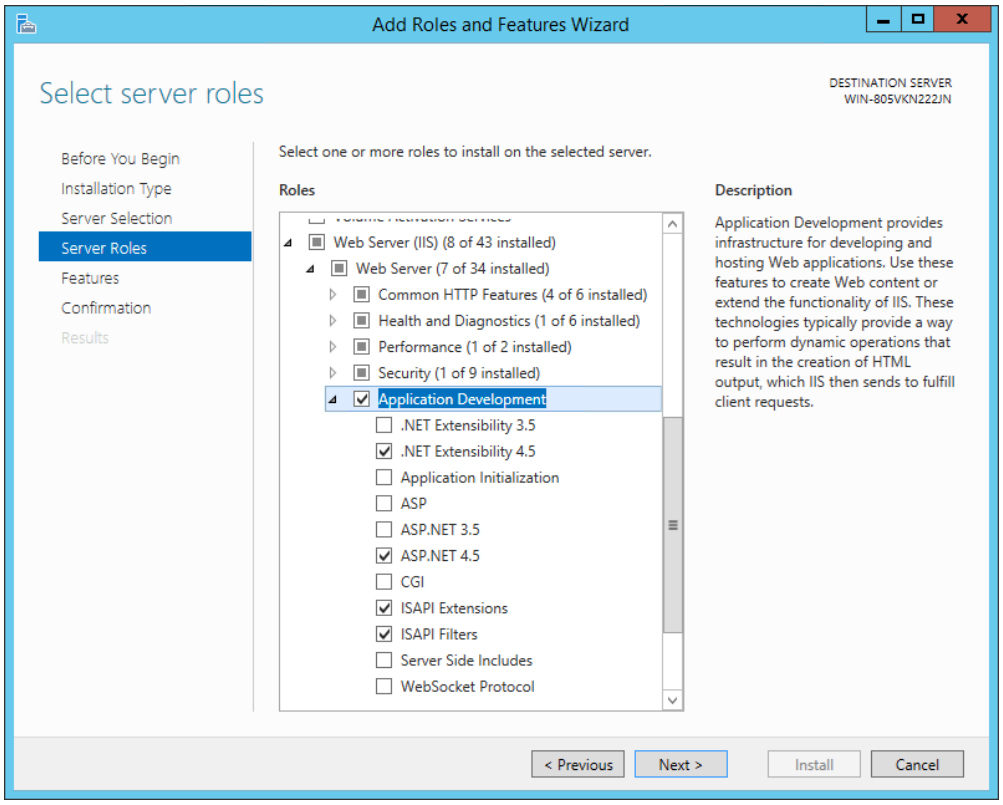


Windows 10

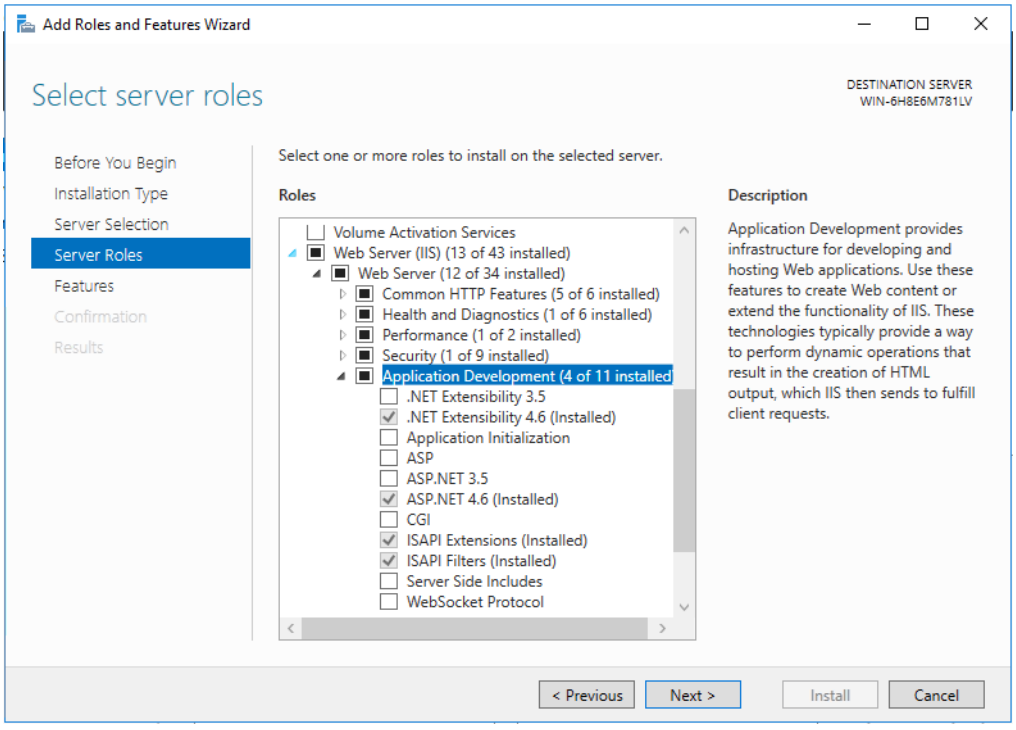
1. On Windows 10 select the **Programs and Features** dialog.
2. Click **Turn Windows features on or off**.
3. Select the features highlighted in the following two screenshots.



Windows Server 2012 On Windows Server 2012 R2 use the **Add Roles and Features Wizard** to add the **.Net Extensibility 4.x** and **ASP.NET 4.x** roles. The selection should look like the following screenshot.

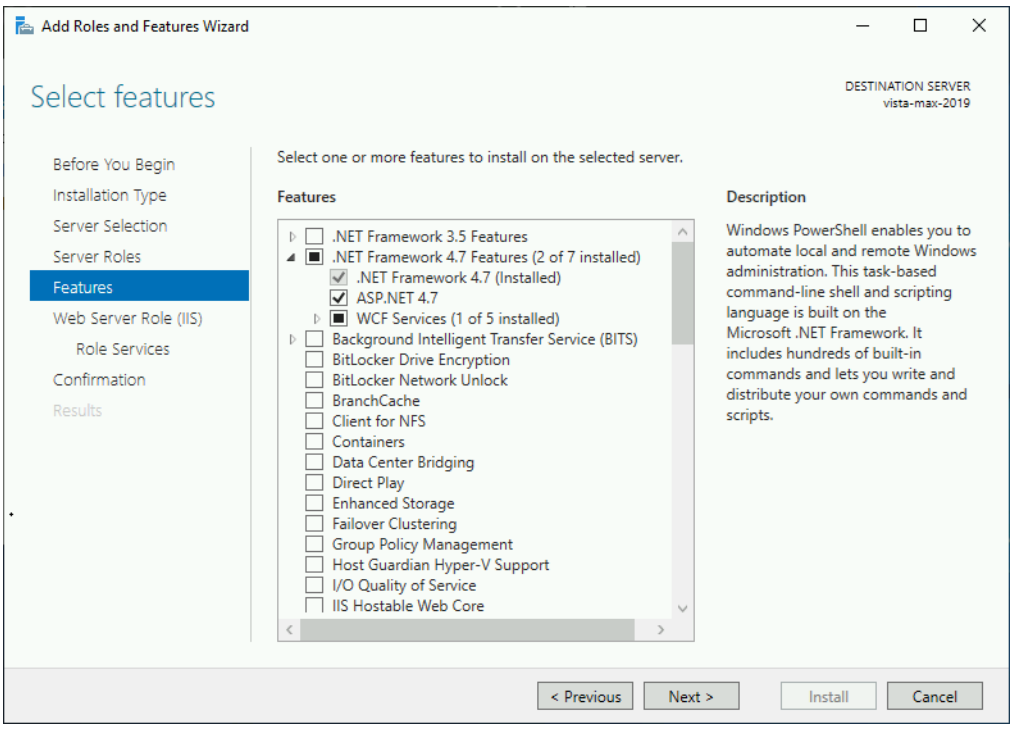


Windows Server 2016 On Windows Server 2016 use the **Add Roles and Features Wizard** to add the **.Net Extensibility 4.x** and **ASP.NET 4.x** roles. The selection should look like the following screenshot.

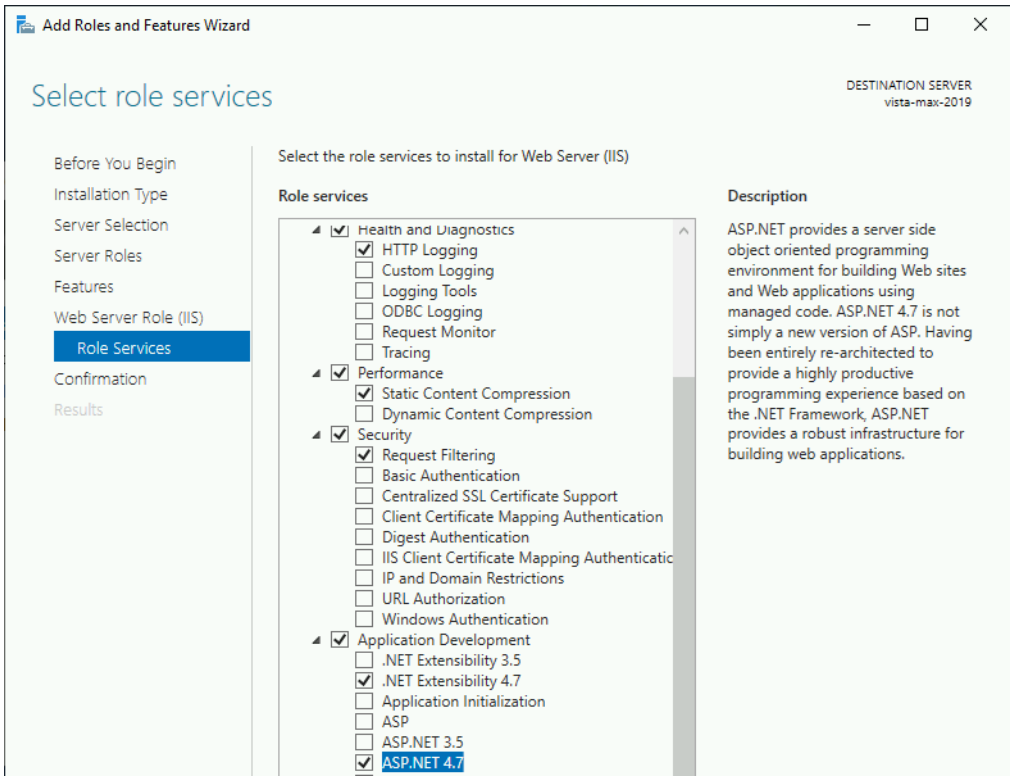


Windows Server 2019

1. On Windows Server 2019 use the **Features** section of the **Add Roles and Features Wizard** to add the **ASP.NET 4.x** role. The selection should look like the following screenshot.



2. In the **Role Services** section of the **Add Roles and Features Wizard** add the **.NET Extensibility 4.x** role. The selection should look like the following screenshot.



Note: Windows does not always display the correct ASP.NET version in this dialog. It may show .Net 4.5 when .Net 4.6 or 4.7 has already been installed.

Install Vista Manager EX on Windows

The following instructions describe how to install and configure **Vista Manager EX** and optionally the **Vista Manager AWC** and SNMP plug-ins on Microsoft Windows:

Note: To install a new update of Vista Manager EX, you must first uninstall the old version. To see how to uninstall Vista Manager EX, see "Uninstalling Vista Manager EX" on page 32.

1. Download Vista Manager EX from the Allied Telesis download center. If you are going to install the AWC and/or SNMP plug-ins then download these files from the same location.
   - The Vista Manager EX installation executable is named 'atvmex***XXX***b***XX***w.exe', with the ***Xs*** denoting the version and build numbers.
   - The AWC plug-in is called 'atawc***XXX***b***XX***w.exe'.
   - The SNMP plug-in is called 'atsnmp***XXX***b***XX***w.exe'.

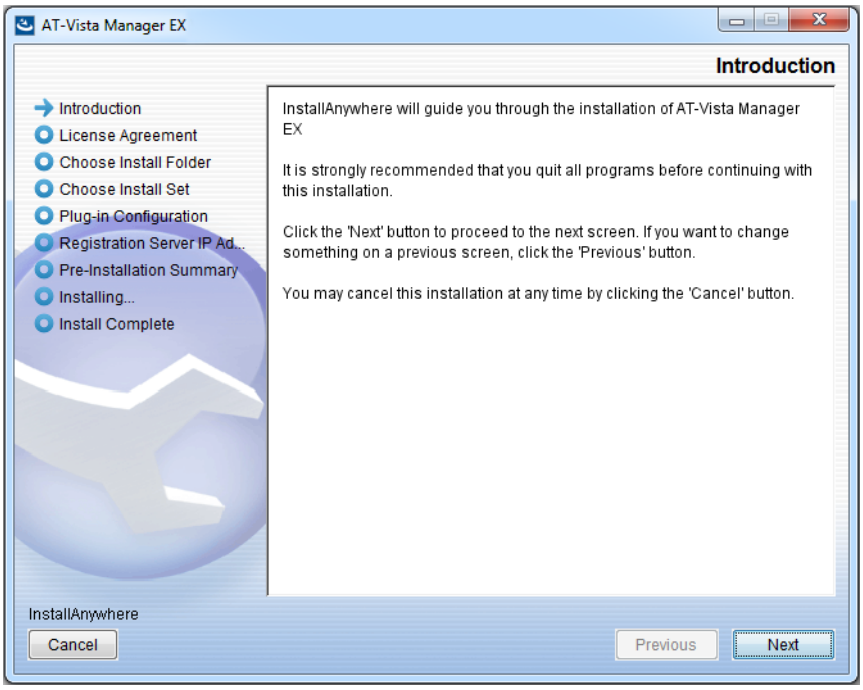
   Do not rename these files. The installation requires them to be in this format.

2. Put the executables for Vista Manager and any plug-ins you wish to install in a single folder. This folder must be accessible from the machine you wish to install Vista Manager on.

- Execute the Vista Manager EX installation program 'atvmex***XXX***b***XX***w.exe'.

Note: You must have administrator privileges to run the installer.

3. The **Introduction** dialog displays:



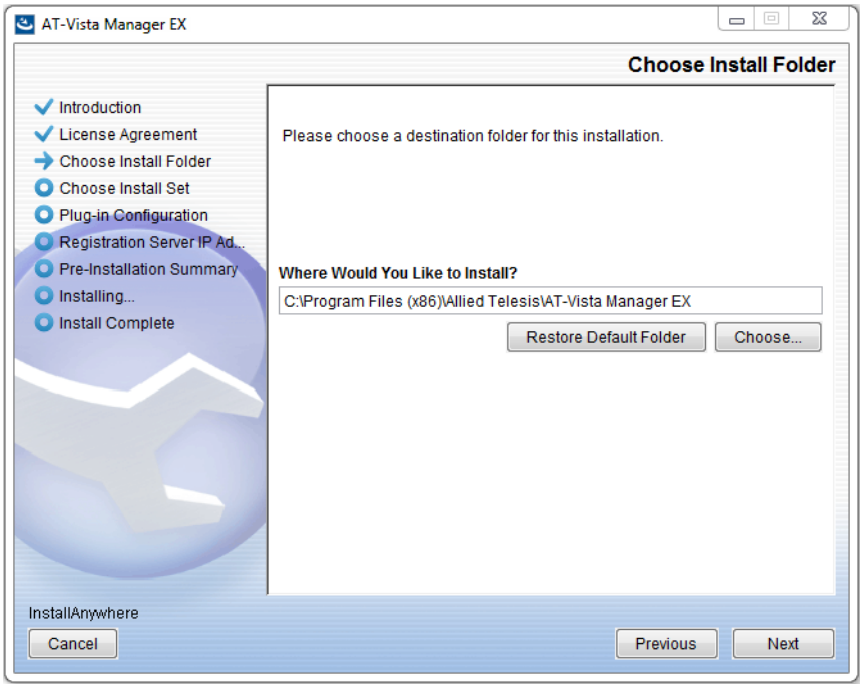
This wizard will guide you through the installation of the latest version of Vista Manager EX. Click **Next**.

4. The **License Agreement** dialog displays:

Read the software license agreement terms and conditions. If you agree to accept the terms of the license agreement:

- Click **I accept the terms of the License Agreement**
- Click **Next**

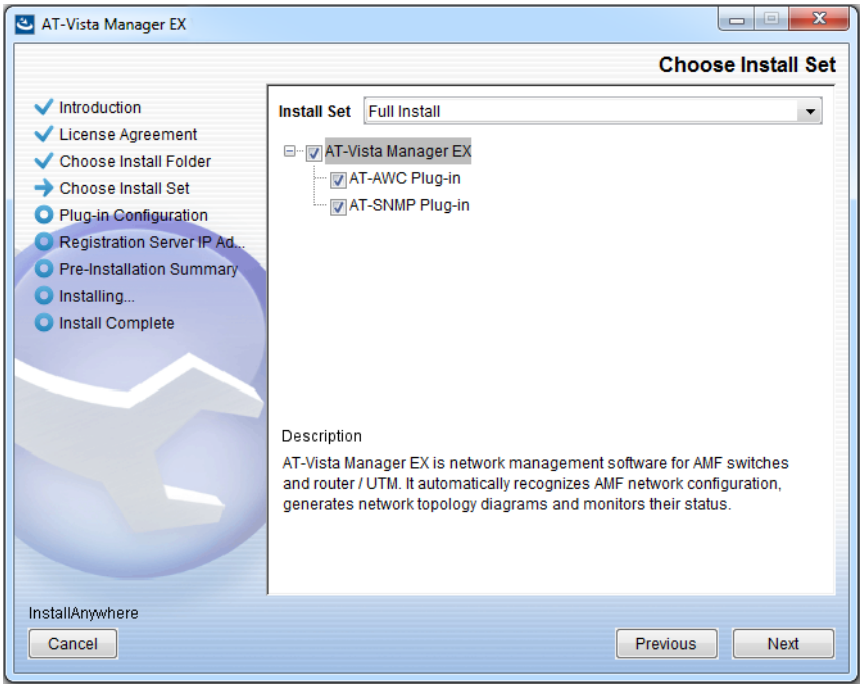
5. The **Choose Install Folder** dialog displays:



Select a destination location and click **Next**.

Caution: If you are installing the SNMP plug-in, you must use the default location.

6. The **Choose Install Set** dialog displays:



Select **Full Install** from the drop down list. By default all plug-ins will be selected. Clear the check box for any plug-ins you do not wish to install.

7. The **Plug-in Configuration** dialog displays:

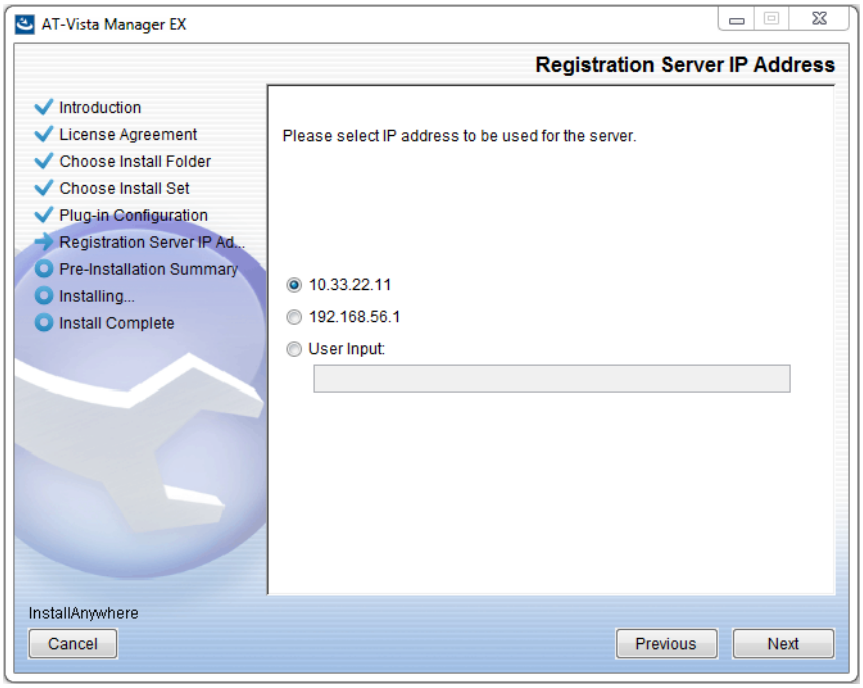
Unless you need direct access to the web management screen of the plug-ins, select **Do not create a public key**.

To enable direct access to the web management screen of the plug-ins, for example if Vista Manager is not working, select **Create a public key**.

When you select **Create a public key**, a file named "public-key.pem" is created in the following folder after installation:
C:\Users\[user name]\Documents\Allied Telesis\AT-Vista Manager EX\certificates\public-key.pem

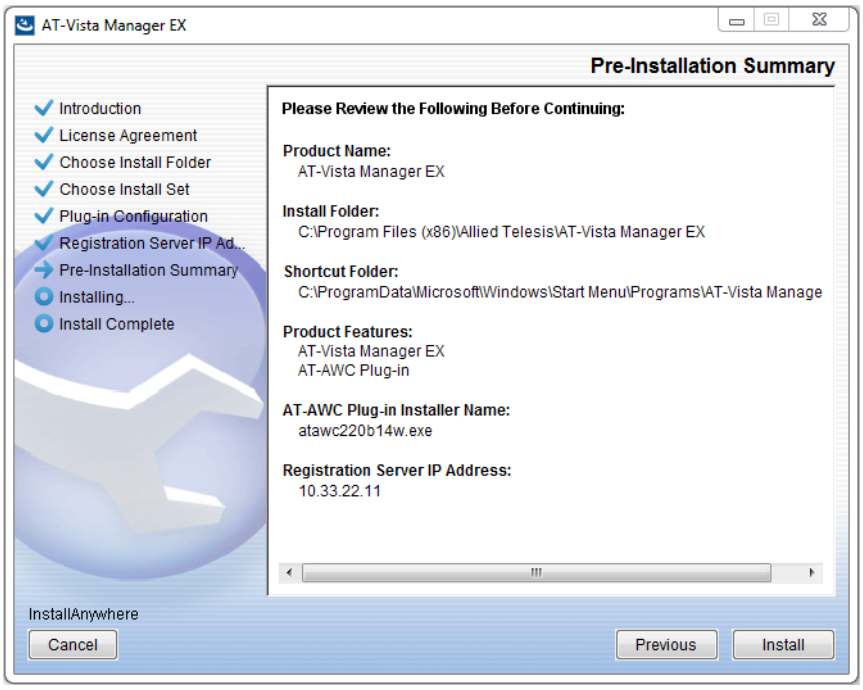
This public key file allows you to access the AWC and SNMP plug-ins without access to Vista Manager authentication. Keep the public key file securely in a place where access authority is restricted.

8. The **Registration Server IP Address** dialog displays:



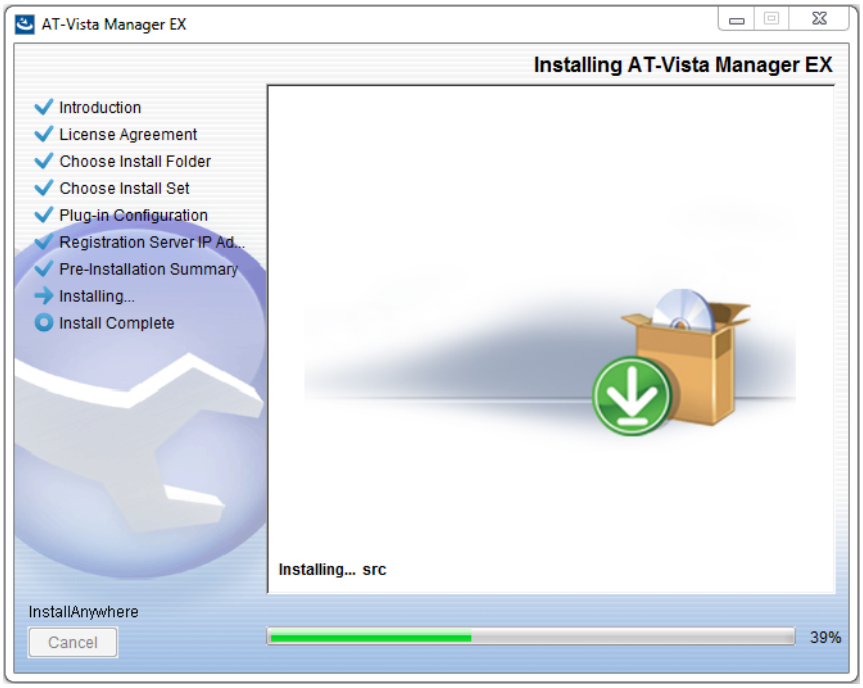
Either select from the list of IP addresses already configured on the Windows machine, or input a valid IP address. Make a note of this address; it is used by APs to connect to the Vista Manager EX AWC plug-in. Click **Next**.

9. From the **Pre-Installation Summary** dialog:

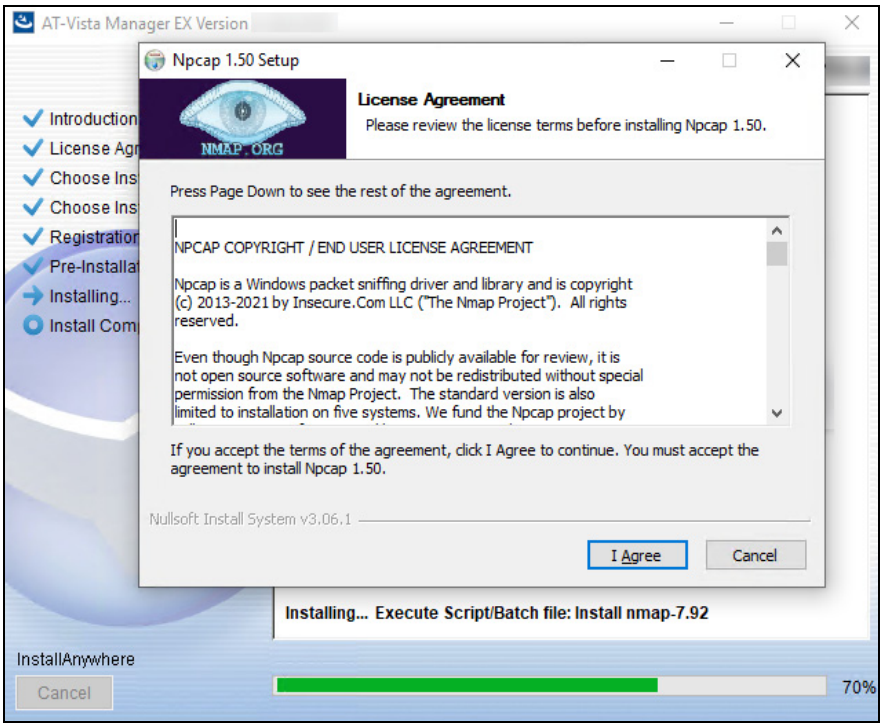


Check that your Product Name, Install Folder, Shortcut Folder, Product Features, Plug-in Installer Name and Registration IP Address are correct, and then click **Install**.

10. The **Installing...** dialog displays:

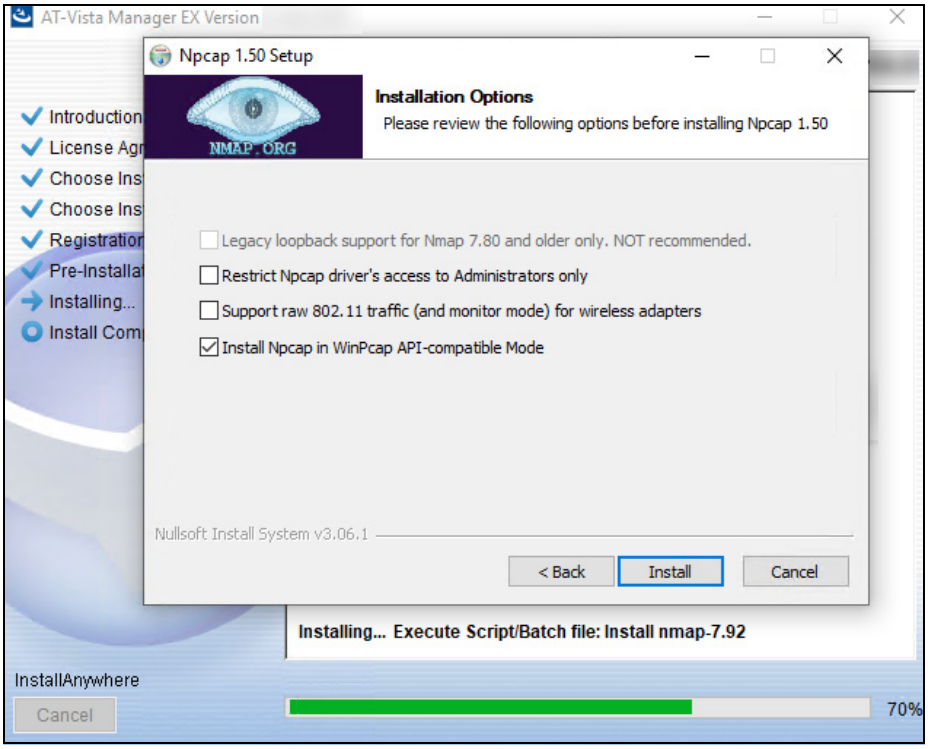


11. The Npcap installer dialog appears.

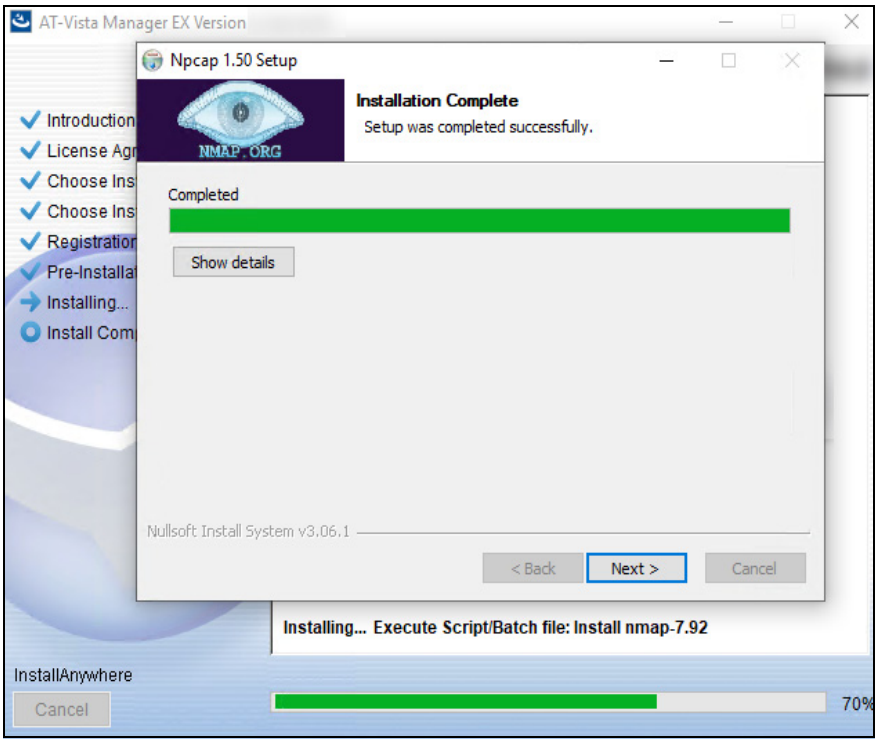


Click **I Agree** to proceed with the install.

12. Click **Install**.

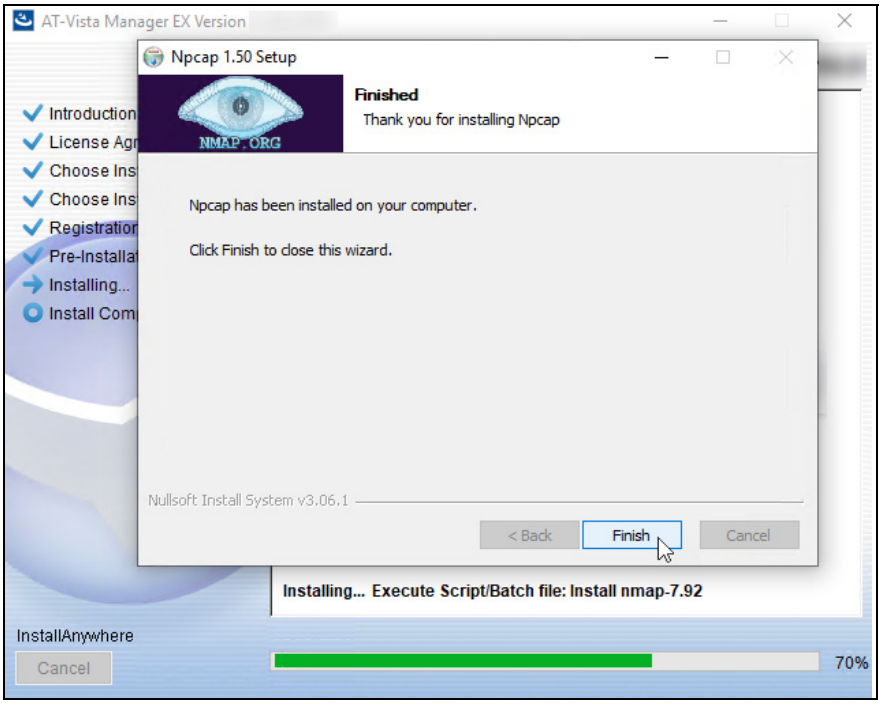


13. The Npcap install will install.



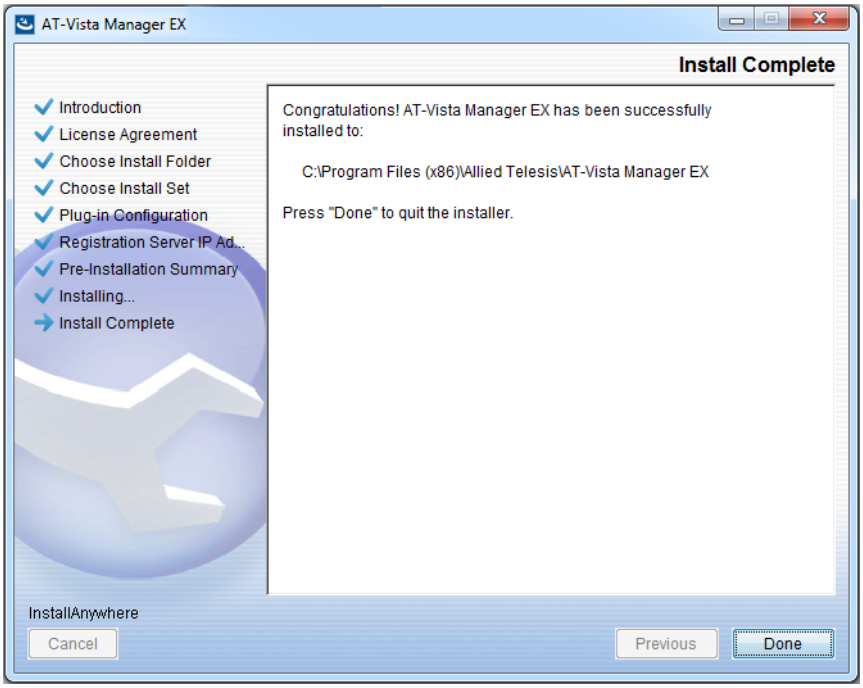
Click **Next**.

14. Click **Finish** to close the Npcap installer.



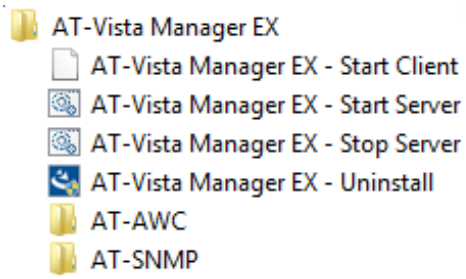
Vista Manager will resume the rest of the download.

15. Once the installation is complete you will see the **Install Complete** dialog:



Check that the installation has completed successfully and click **Done**.

16. The installation creates a program group with shortcuts to Start/Stop Vista Manager and the plug-in services. There are also shortcuts to backup and restore the SNMP and AWC plug-ins.



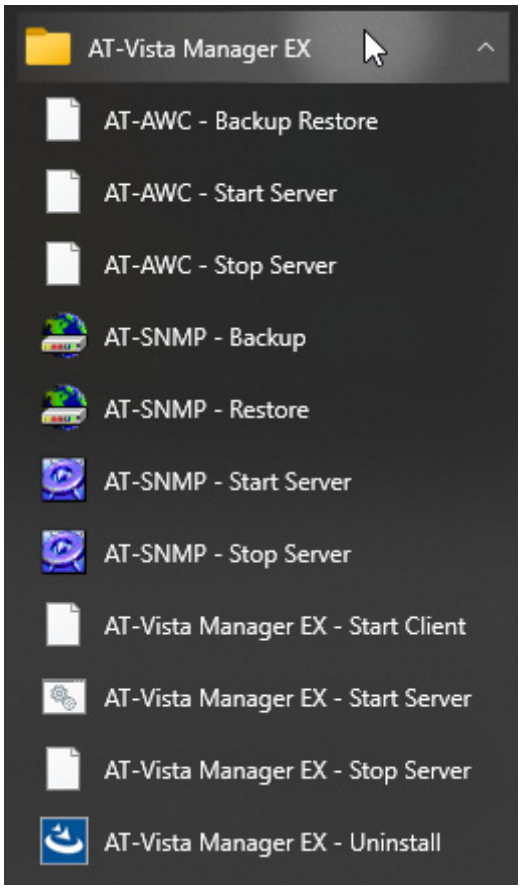
All the necessary services are automatically started after installation, and whenever the Windows host is rebooted.

17. Reboot your system at this point to ensure all services have started correctly.

Uninstalling Vista Manager EX

To uninstall Vista Manager EX, follow the procedure below.

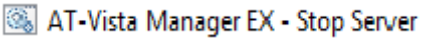
The uninstall process requires you to run several executables. You can find these in the AT-Vista Manager EX Start menu directory.



If you can't locate the Start menu items, or want to run them directly, you can find them in the Vista Manager EX installation directory.

The default installation folder (when installed on the C drive) is:
C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX.

Step 1. **First, stop the server**



Run the **AT-Vista Manager EX - Stop Server** executable.

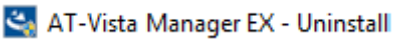
Step 2. **If you have the SNMP plug-in installed, stop the SNMP server.**

Run the **AT-SNMP - Stop Server** executable.

Note: If you uninstall without stopping the SNMP plug-in server, a message such as "The file that needs to be updated is currently in use" may be displayed.

In this case, select **Automatically close and attempt to restart the application** and click the **OK** button.

Step 3. **Uninstall Vista Manager EX**



Run the **AT-Vista Manager EX - Uninstall** executable.

Step 4. **Click the Uninstall button to uninstall.**

Step 5. If a dialog box to restart the system is displayed, select **Restart system** or **Restart later** and click the **Finish** button.

Note: If you select Restart system, it is advised that you close anything you have open beforehand, as unsaved data may not be preserved.

Step 6. **Delete the installation folder**

After restarting the system, delete the installation folder.

The default installation folder (when installed on the C drive) is:
C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX

Additional Installation Tasks

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 162 (SNMP trap), used by SNMP devices to send traps to the SNMP plug-in.
- UDP port 514 (syslog), used by the AMF master/controller to send logs to Vista Manager EX.
- TCP port 5000, which gives access to the Vista Manager web interface.
- TCP port 5443, which gives access to the AWC plug-in web interface. (This depends on which port you configured the AWC plug-in to run on during installation.)
- TCP port 6443, which gives access to the SNMP plug-in web interface.
- 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).TCP port 65437-65439, which the wireless APs use to communicate with the AWC plug-in.

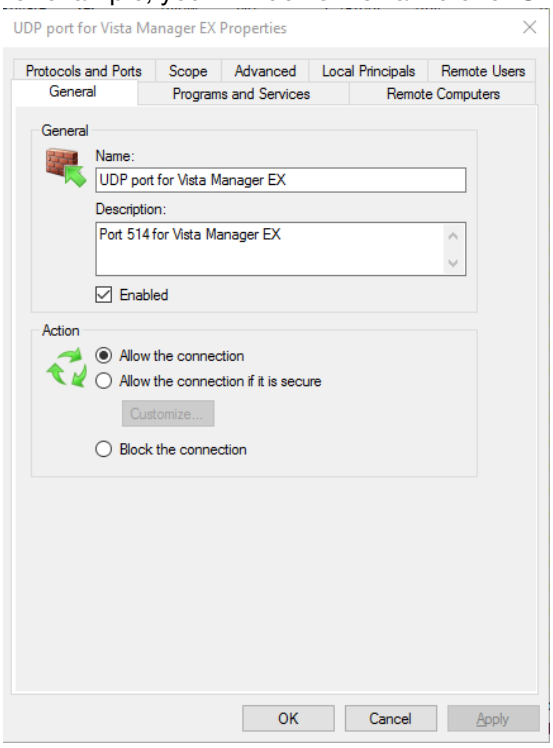
Create Windows inbound firewall rules

For remote access to Vista Manager EX, and the AWC and SNMP plug-ins, it is necessary to allow external network access. A UDP rule is required for ports 162 and 514 and a TCP rule is required for ports 443, 5000, 5443, and 65437-65439.

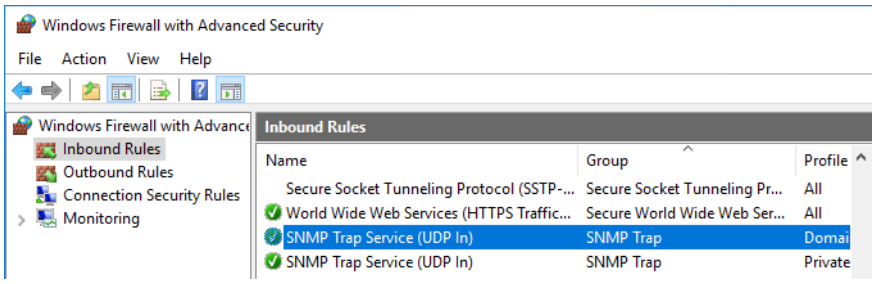
Note: 5443 is the port number used for the AWC plug-in in this guide. Please adjust according to your installation.

1. From the Windows **Control Panel**, select **System and Security > Windows Firewall**
2. Select **Advanced Settings**
3. Select **Inbound Rules > New Rule**
4. Follow the **New Inbound Rule Wizard** as follows:
   - Select **Port** and click **Next**
   - Select **TCP,** then select **Specific local ports** and enter port numbers **443, 5000, 5443, 65437-65439** and click **Next**
   - Select **Allow the connection** and click **Next**
   - Select **Domain**, **Private** and **Public** and click **Next**
   - Enter a name for the new inbound rule, for example **Vista Manager EX** and also a description if required and click **Next**.
5. Set up two new inbound rules for the **UDP** ports **162** and **514**.

For example, your Windows firewall rule for UDP port 514 should look like this:



6. Ensure the SNMP Trap Service firewall rules are enabled.



Create Windows firewall rules for SNMP plug-in

If a firewall is enabled on the Vista Manager EX server, trap reception by the SNMP plug-in and automatic subnet search using the direct broadcast address are not possible. To enable them:

1. From the Windows **Control Panel**, select **System and Security > Windows Firewall**
2. From the left side of the dialog, click **Allow an app or feature through Windows Firewall**.
3. Click **Change Settings** at the top of the **Allowed apps** dialog. In the list of items in the dialog, locate **SNMP Trap**.
4. Check the **Private** and **Public** checkboxes.
5. Click **OK** at the bottom of the **Allowed Apps** dialog.
6. Select **Advanced Settings**.
7. Select **Inbound Rules > New Rule**.
8. In the **New Inbound Rule Wizard** dialog, select **Custom** as the rule type and click **Next**.

9. Select **All Programs**.
10. Click on **Customize**. Select **Apply to this service**, and select **ATKK Network Monitor AutoDiscovery Manager Service** from the list. Click **OK** and then click **Next**.
11. On the **Protocol and Ports** dialog, select **ICMPv4** for **Protocol Type** and click **Customize**.
12. In the **Customize ICMP Settings** dialog box, select **Specific ICMP types**. For the **This ICMP type** fields, select **0** for **Type** and **Any** for **Code**, then click **Add**. Check that the newly-added type is checked, click **OK**, return to the **Protocol and Port** dialog, and click **Next**.
13. On the **Scope** dialog, click **Next**.
14. On the **Action** dialog, select **Allow the connection** and click **Next**.
15. On the **Profile** dialog, select the required destination. If you do not need to use anything other than the SNMP plug-in, select **Domain** or **Private** only. Click **Next**.

Note: If the **Network Location** is set to **Public Network**, communication is not possible unless **Public** is selected.

16. On the **Name** dialog, enter a name of your choice (for example **ICMP automatic search**). Click **Finish** to complete the **New Inbound Rule Wizard**.
17. Back in the **Windows Firewall with Advanced Security** screen, select **Inbound Rules > New Rule**.
18. On the **New Inbound Rule Wizard** dialog, select **Port** as the rule type and click **Next**.
19. On the **Protocol and Ports** dialog, select **UDP** for the option, and select the **Specific local ports** radio button. In the text field, enter **6343** as the port number, and click **Next**.
20. On the **Action** dialog, select **Allow the connection** and click **Next**.
21. On the **Profile** dialog, select the required destination. If you do not need to use anything other than the SNMP plug-in, select **Domain** or **Private** only. Click **Next**.

Note: If the **Network Location** is set to **Public Network**, communication is not possible unless **Public** is selected.

- On the **Name** dialog, enter a name of your choice (for example **sFlow packet**). Click **Finish** to complete the **New Inbound Rule Wizard**.

Configuring the Forescout API

Vista manager polls Forescout's Enterprise manager API to get a list of endpoints along with information about these end points that a CounterACT device has collected from the device. If the customer has multiple CounterACT devices, they need to be registered with the Forescout's Enterprise manager.

The Enterprise Manager is the controller that manages CounterACT appliance activity, policies, and collects information about endpoint activity. You can see the information retrieved from the Enterprise Manager from the Forescout Console program.

In order to run the Forescout plug-in, you need to configure three things in the Forescout console application:

Step 1. **Install eyeExtend Connect**

Step 2. **Start the web API module**

Step 3. **Configure the web API module**

Note that this guide does not cover step 1, and instead covers the web API that connects with Vista Manager. When using this guide, we assume that you have all of your CounterACT devices registered with the Forescout console. For information about installing eyeExtend Connect, as well as documentation for the full installation of Forescout CounterACT, refer to the official Forescout documentation portal.

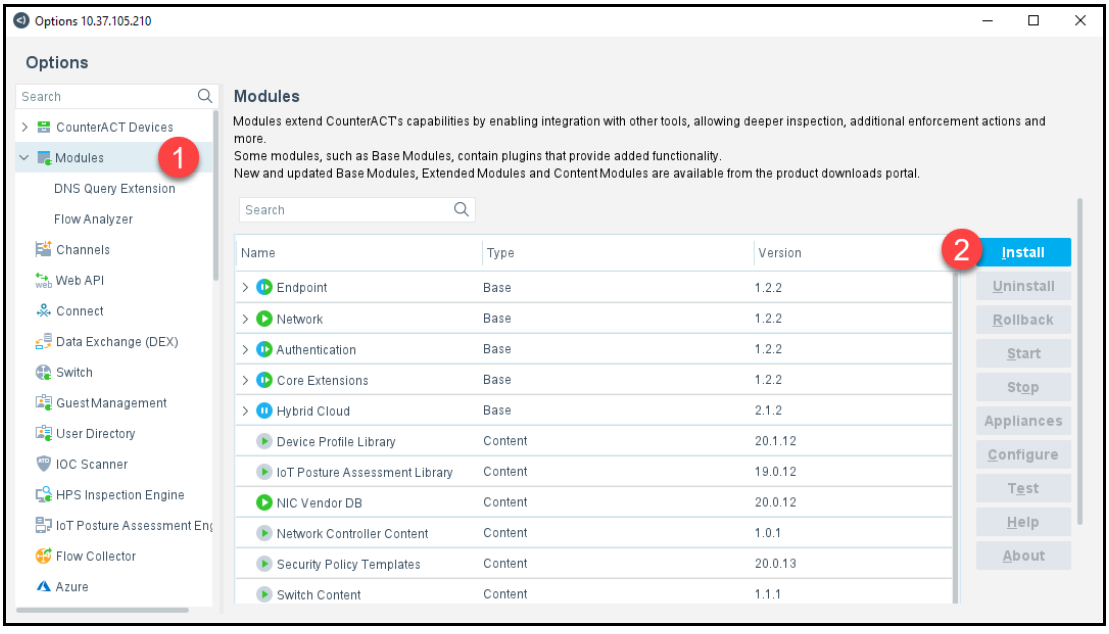
First, install eyeExtend Connect. Once eyeExtend is installed, proceed with installing the Connect web API from the Forescout Console.

Step 1. In the Forescout Console, go to **Options** > **Modules.**

Step 2. Click on the **Install** button, which will open your file browser.

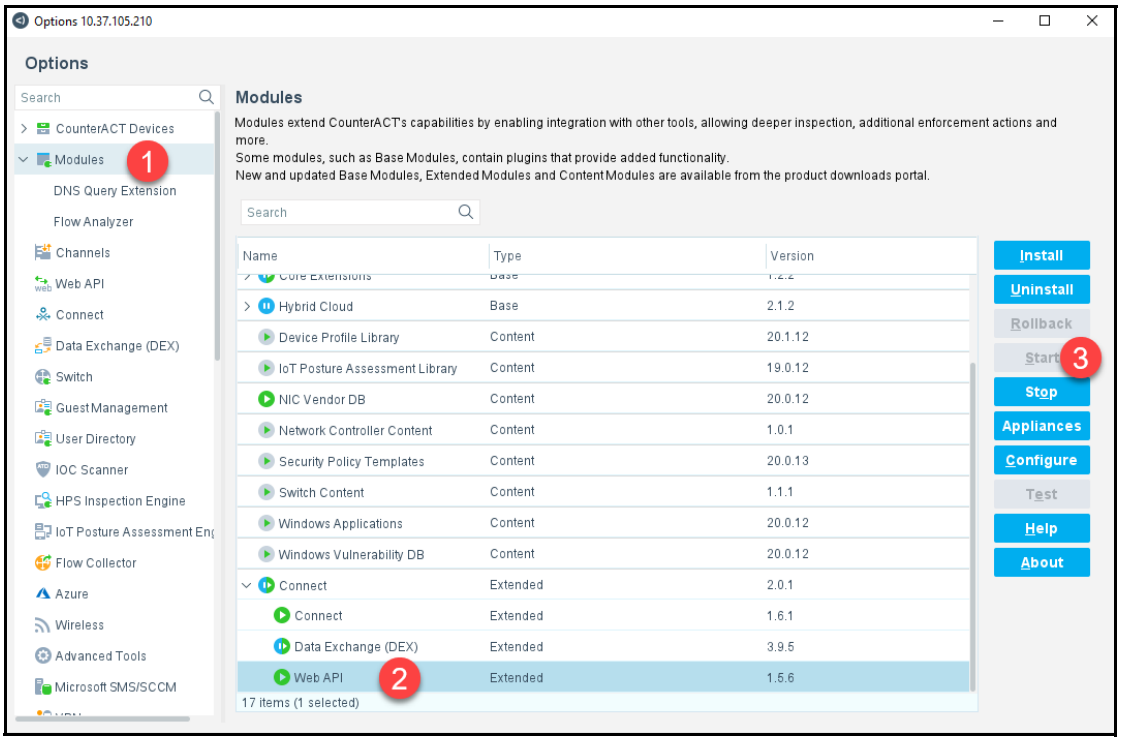
Step 3. Select the **Forescout Connect FPI File** to install the web API.

The web API will now appear in the Modules list under the **Connect** heading.



Note that the web API may need to be started after installing. If it is already active, the Start button will be grayed-out.

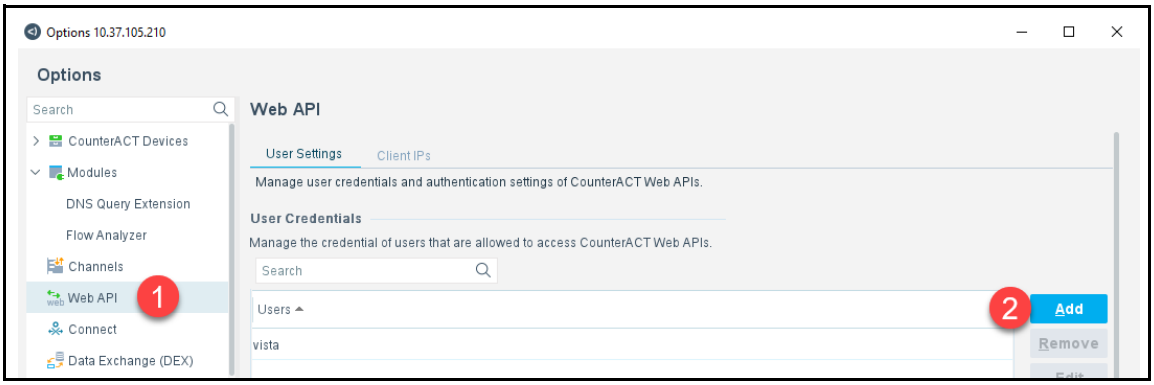
1. To start the module, go to **Options > Modules** in the Forescout console and scroll down to the **Connect** module.
2. Expand the connect module accordion menu and select **Web API.**
3. Click the **Start** button on the right side of the window to start the web API



Creating a Web API User

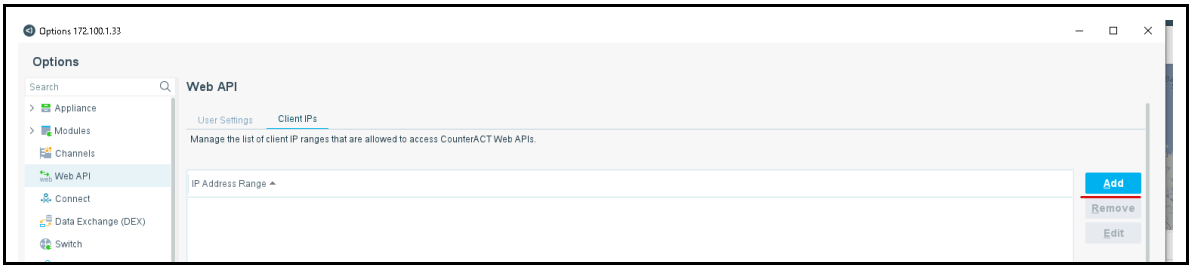
For Vista Manager to access CounterACT devices for polling, we will create a web API user.

- In the Options menu, select **Web API**
- On the Web API module click the **User Settings** tab
- Then, click **Add** to add a User.



Next, we will allow all IP addresses to access the Web API:

- On the web API module click the **client IPs** tab
- Then, click **Add**



To register the Forescout plugin with Vista Manager, see "Registering the plug-ins" on page 43.

Virus scanning software exclusions

To prevent false detection, quarantine, and deletion of necessary files by virus scanning software, you should exclude the following directories used by Vista Manager EX from being detected.

Refer to your virus scanning software manual for detailed instructions.

- AVM EX installation directory

C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX

- Npcap

C:\Program Files\Npcap

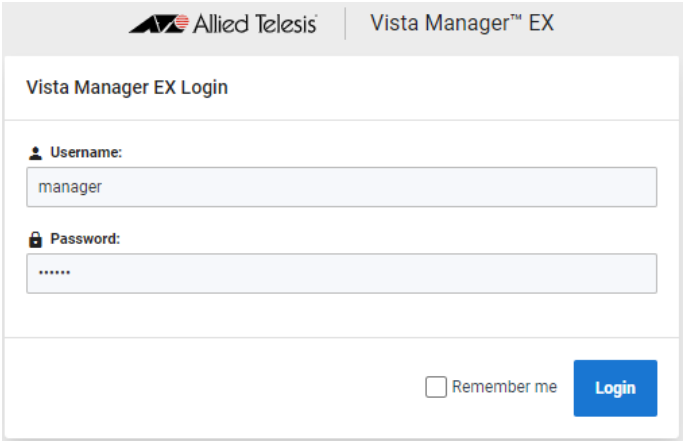
Initial login

Login to Vista Manager EX

To connect to Vista Manager EX from a remote machine use the URL http://<***ip address***>:5000, where ***<ip address>*** is the address you selected on the **Registration Server IP Address** dialog. You can also do this locally on the Vista Manager host machine using the URL http://localhost:5000.

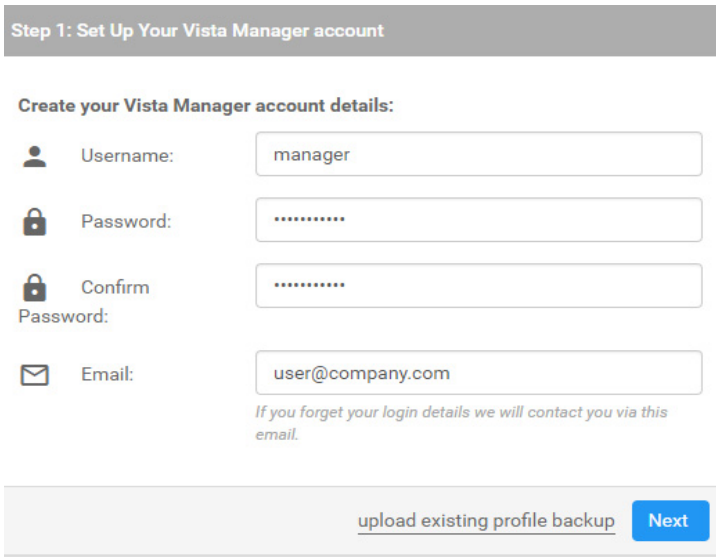
Note: Vista Manager requires JavaScript to be enabled in your web browser.

From the **Vista Manager Login** dialog:



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

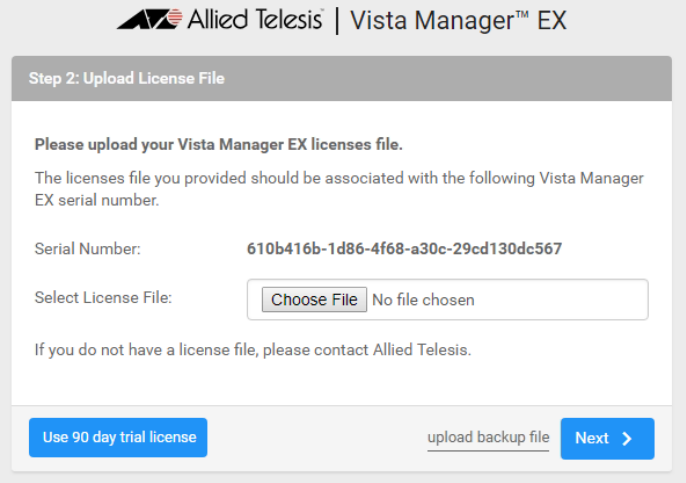
The **Set Up Your Vista Manager account** dialog displays:



- 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:

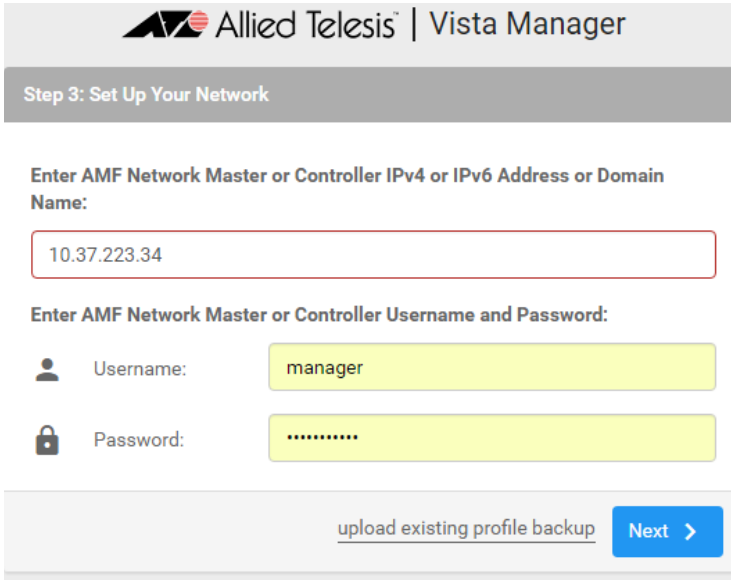


- Click **Choose File** to upload your Vista Manager EX license file
- Click **Next**.

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, and any plug-ins you have installed, for 90 days.

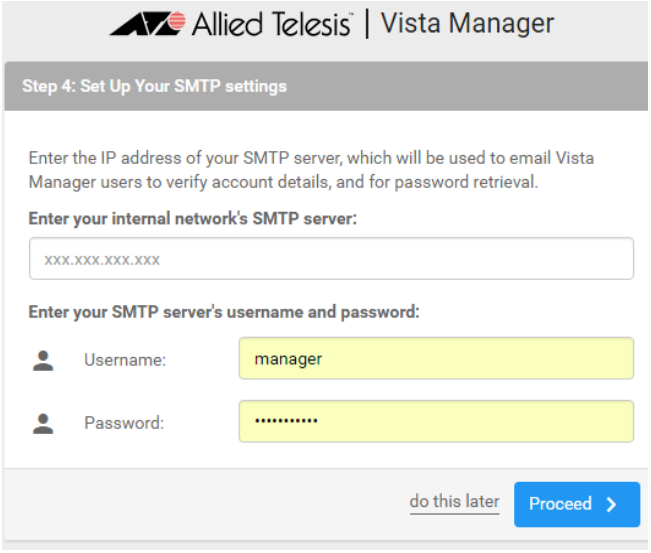
The **Set Up Your Network** dialog displays:



- 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:



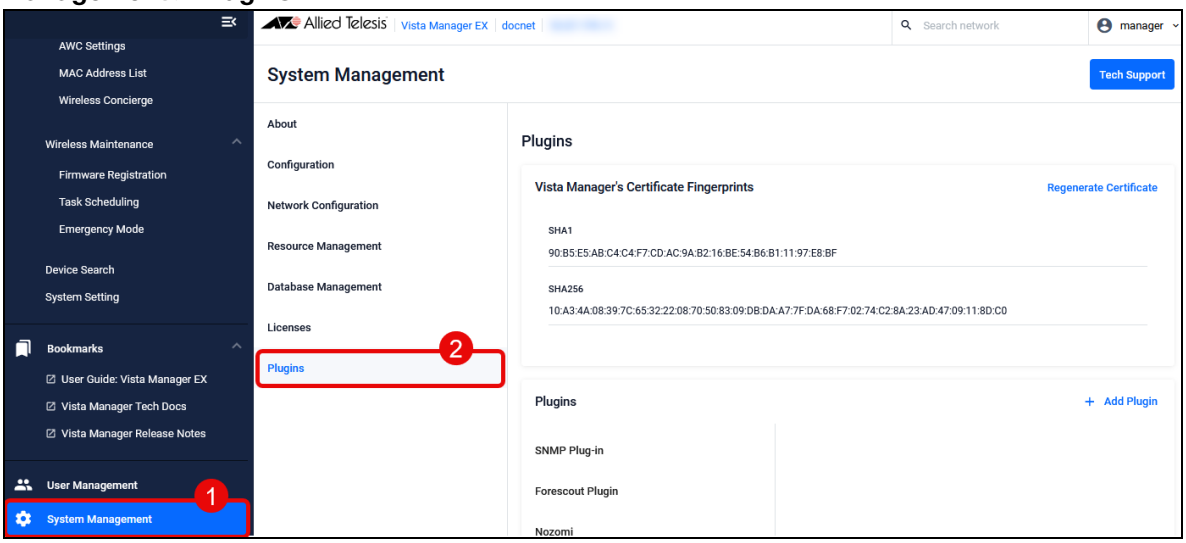
- Enter the **IP Address** of your SMTP server
- Enter the SMTP Server **Username**
- Enter the SMTP Server **Password**

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

Registering the plug-ins

The AWC and SNMP plug-ins require separate subscription licenses from Vista Manager. See "Licensing" on page 11 for details.

After you have successfully logged in to Vista Manager EX, to set up the plug-ins, go to **System Management** > **Plugins**.



AWC plug-in

1. Click **Add Plug-in** and enter the following details for the AWC plug-in:

- **Server URL:** https://localhost:5443/wireless_plugin

2. Click **Verify Connection**
3. To check the plug-in fingerprint for the AWC plug-in:

   a. Locate the directory that Vista Manager was installed to.

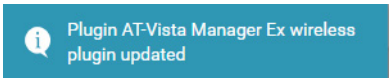
   b. Open the following sub-directory:

   - ***<Vista Install Path>*\Plugins\AT-AWC\apache\key**

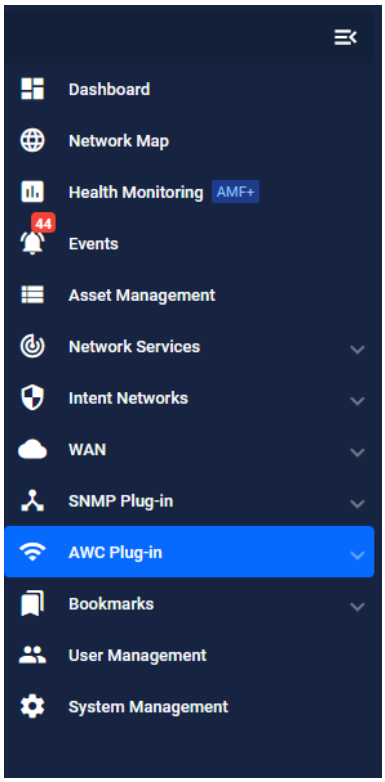
   c. Open the file fingerprint.txt.

4. Once you have confirmed that the fingerprints match, click **Save**.

The following information message is displayed showing that the plug-in has been updated:



You can now access the **AWC** plug-in from the **Vista Manager EX** menu as follows:



SNMP plug-in

1. Click **Add Plug-in** and enter the following details for the SNMP plug-in:

- **Server URL:** https://localhost:6443/NetManager

2. Click **Verify Connection**
3. To check the plug-in fingerprint for the SNMP plug-in:

   a. Right-click the Windows start menu, and select Computer Management.

   b. Select Services and Applications > Internet Information Service (IIS) Manager.

   c. Select Server Certificates.

   d. Select **netman**, then click on the View action.

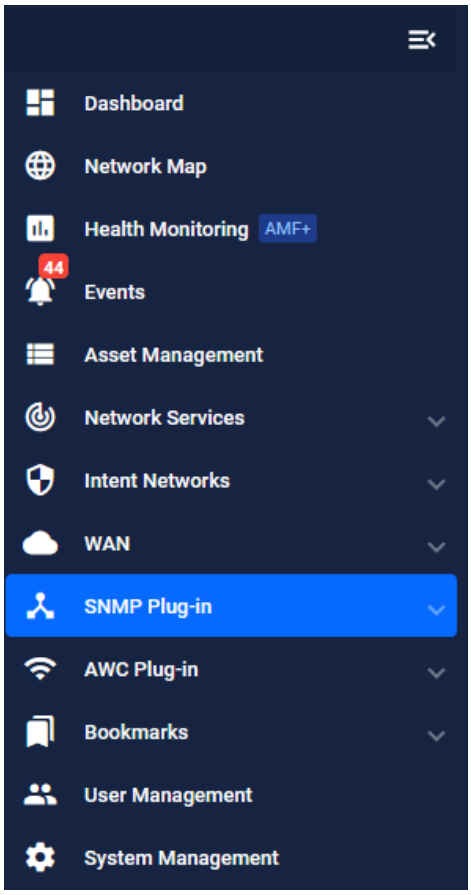
   e. Click the Details tab.

   f. The value will be displayed in the Thumbprint field.

4. Once you have confirmed that the fingerprints match, click **Save**.

The following information message is displayed showing that the plug-in has been updated:

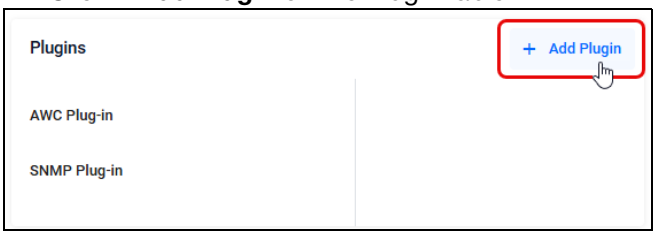
You can now access the **SNMP** plug-in from the **Vista Manager EX** menu as follows:



Forescout You must configure the Forescout API first before enabling the Forescout plugin in Vista Manager's GUI. For information about how to configure the Forescout API, see "Configuring the Forescout API" on page 36.

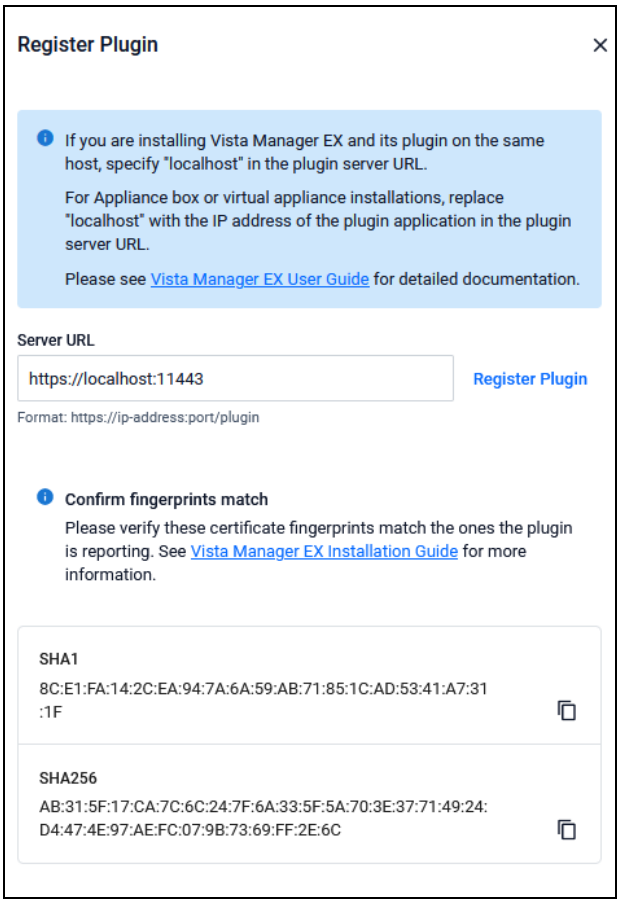
After upgrading to version 3.9.1 or later, you need to register the plugin. To do this:

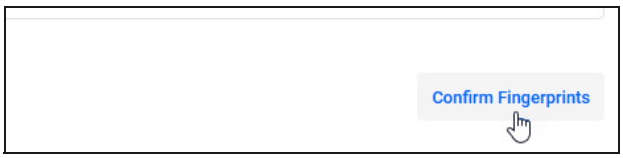
1. Go to **System Management** > **Plugins.**
2. Click **+ Add Plugin** on the Plugin table.



3. Register the plugin in the textbox with the server URL of **https://localhost:11443**
4. Click **Register Plugin** and Vista Manager will generate the certificate's fingerprints.

5. Confirm that the fingerprints match the Forescout program, then click **Confirm Fingerprints**.





6. Scroll down and enter the additional Forescout setup settings:
   - Username
   - Password
   - IP address

7. Click **Save.**
   The Plugin will be added to your plugin list.

Changing the AWC plug-in port

By default, the AWC plug-in and SNMP plug-in web server HTTPS port numbers are set to 5443 for the AWC plug-in, and 6443 for the SNMP plug-in. If you need to change the HTTPS port number of the AWC plug-in, you can do so with the following procedure.

Note: The Vista Manager EX server port number (5000/443) and the SNMP plug-in HTTPS port number (6443) cannot be changed.

Note: HTTP connection to the AWC plug-in and SNMP plug-in management screen is not possible.

Note: Do not duplicate the AWC plug-in server port number with other services running on the Vista Manager EX server, SNMP plug-in server, or the server on which Vista Manager EX is installed.

1. Browse to the Vista Manager EX installation directory, and then open the Plugins\AT-AWC\tools\change_port\ directory.
2. Right click on **change_port.bat** and click **Run as administrator**.
3. You will be asked “Please input the port number:”. Enter the new port number.
4. When batch processing is complete, the port number has been updated.

To check that the port has been updated, browse to the login screen using the new port number. For example, if you changed the port to “8443”, try accessing https://localhost:8443/ with your web browser.

If the settings have been changed correctly, the AWC plug-in login screen is displayed.

Import plug-in server certificate

The AWC plug-in and SNMP plug-in web management screens are accessed via HTTPS.

To connect to the AWC plug-in and SNMP plug-in HTTPS server from a remote browsing environment, it is necessary to import the server certificate in the remote browsing environment.

Note: HTTP connection to the AWC plug-in and SNMP plug-in management screen is not possible.

Note: The following instructions and screenshots are taken from Internet Explorer 11. Different versions may have slightly different appearance or text.

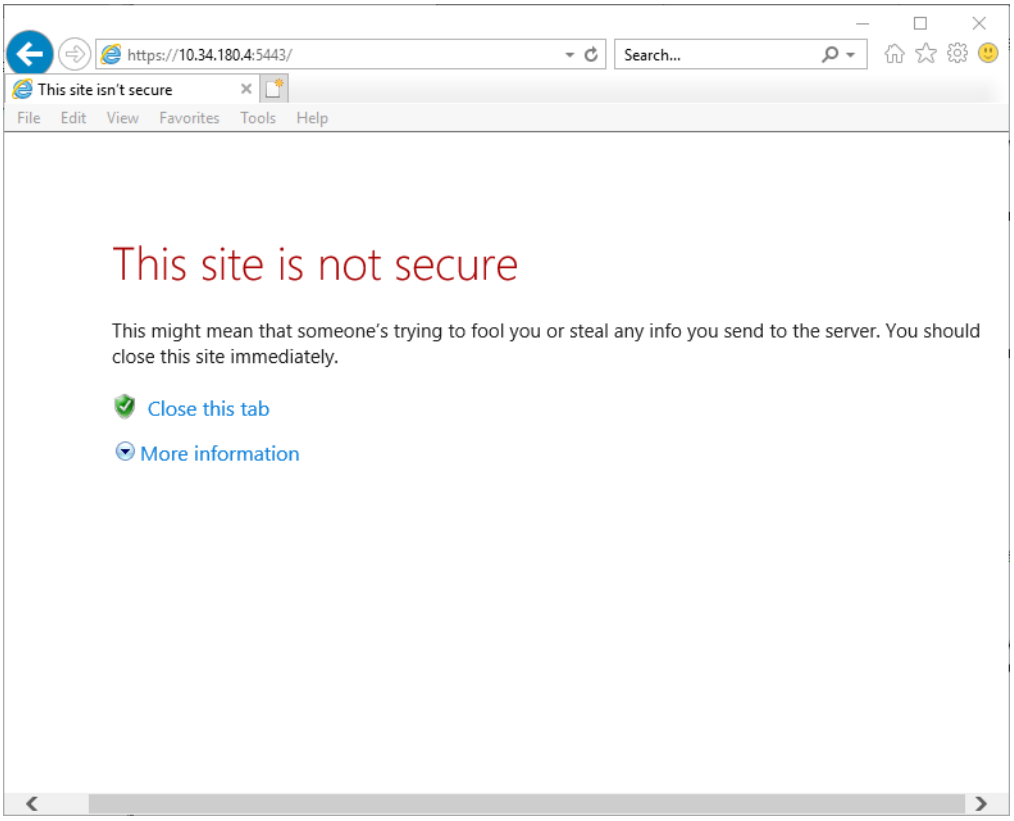
1. Log in to the PC as a user with administrator privileges.
2. Start the web browser as an administrator. You can do this by right clicking and selecting **Run as administrator**.

3. Enter the URL corresponding to the plug-in into the address field of the web browser and press the Enter key.

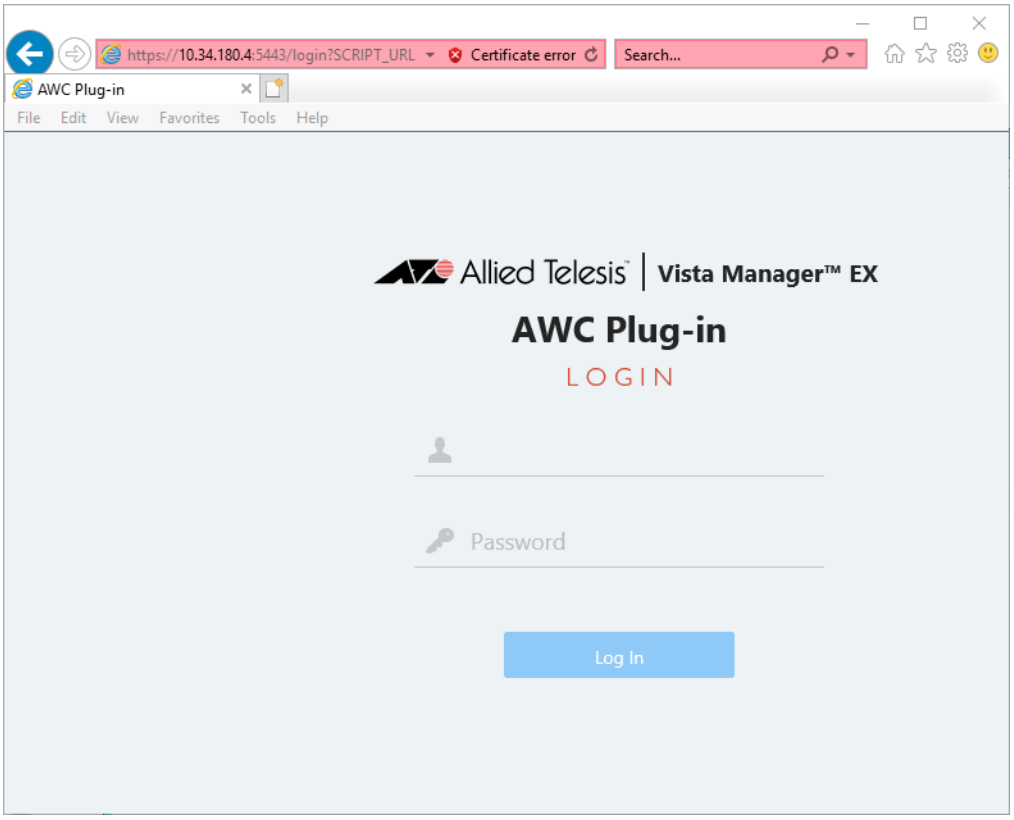
   a. AWC plug-in:
   https://(IP address of the Vista Manager EX server):5443

   b. SNMP plug-in:
   https://(IP address of Vista Manager EX server):6443/NetManager/web2/

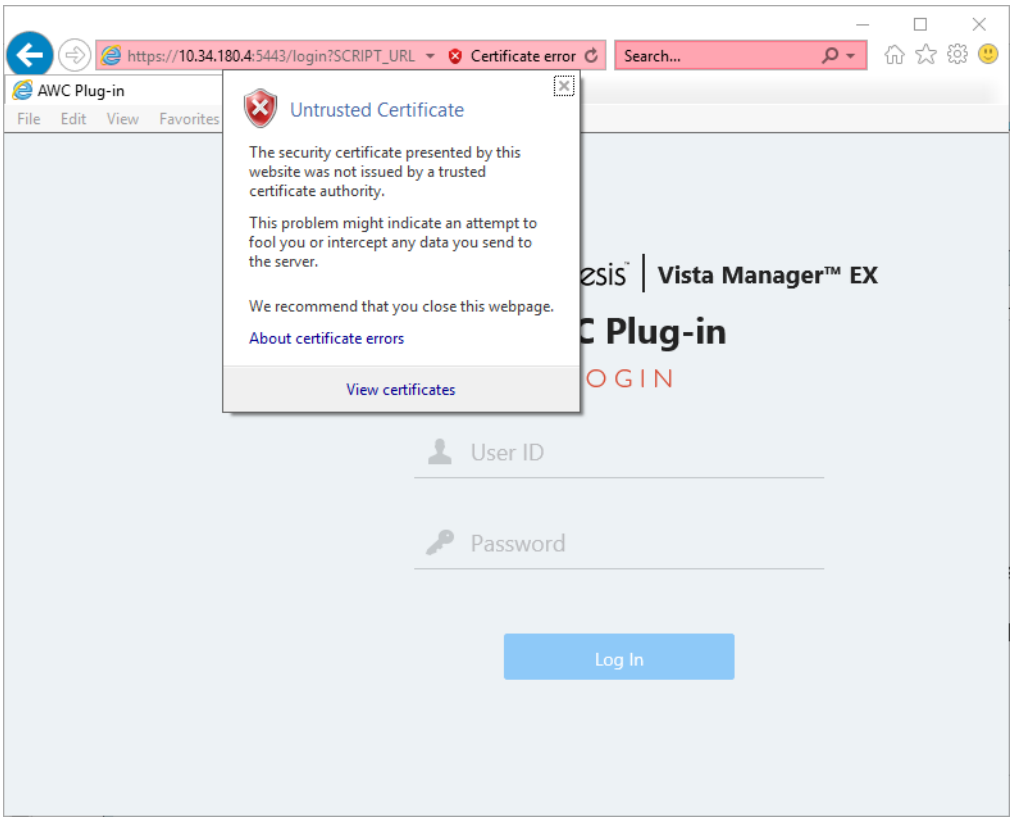
A warning page will appear stating “This site is not secure”.



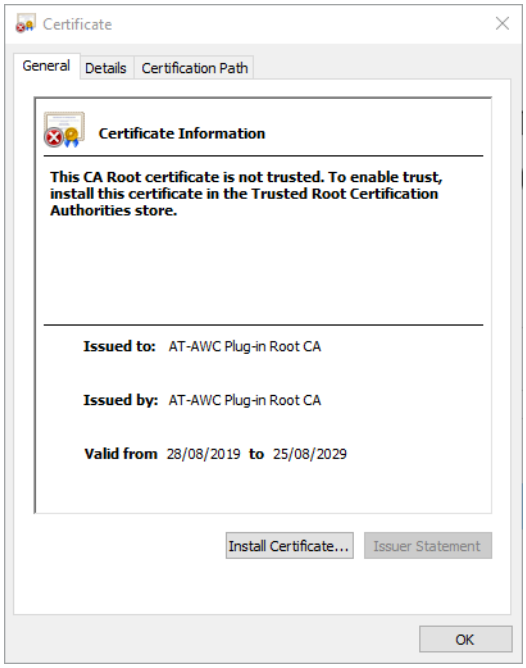
4. Click **More information** then **Go on to the webpage (not recommended)** at the bottom of the screen. The AWC plug-in login screen is displayed. At this time, the address bar of the web browser turns red and **Certificate error** is displayed.



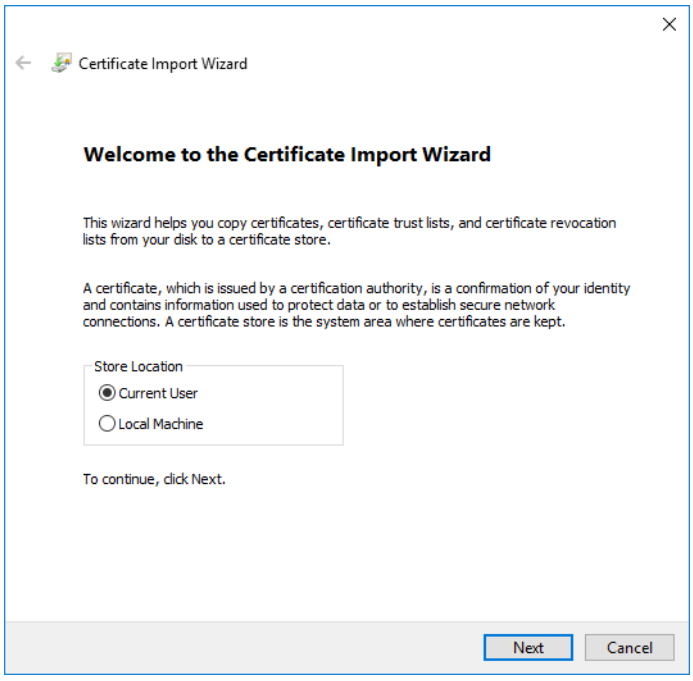
5. Click the **Certificate Error** display. The message “Untrusted certificate” appears.



6. Click **View Certificates** at the bottom of the message. The **Certificate** dialog opens.

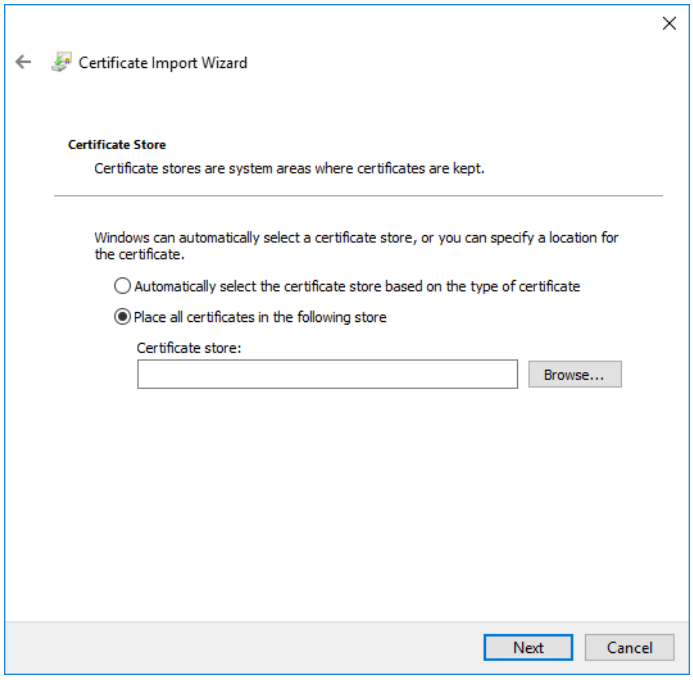


7. In the **Certificate** dialog, click the **Install Certificate** button. The **Certificate Import Wizard** dialog box appears.



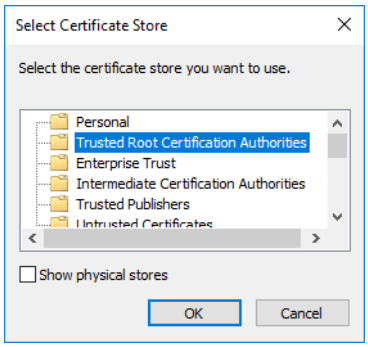
8. On the **Welcome to the Certificate Import Wizard** screen, select **Local Machine** from **Store Location** and click the **Next** button.

9. On the **Certificate Store** screen, select **Place all certificates in the following store**.



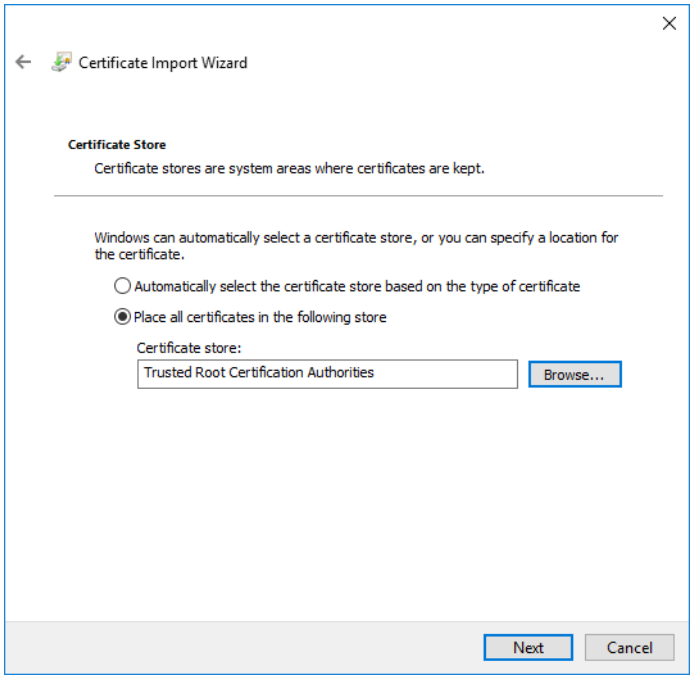
The **Browse** button is enabled.

10. Click the **Browse** button. The **Select Certificate Store** dialog is displayed.

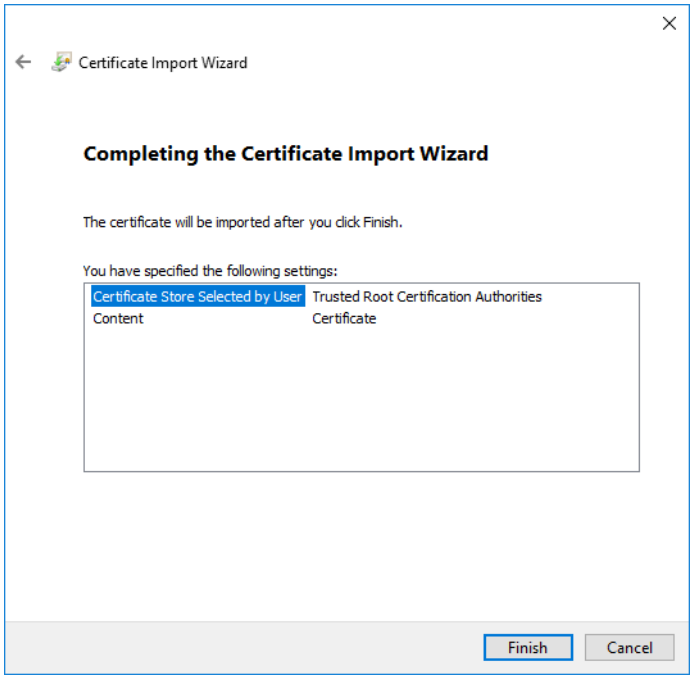


11. In the **Certificate Store Selection** dialog, select **Trusted Root Certification Authorities** and click the **OK** button. The **Certificate Selection** dialog box closes, and **Trusted Root**

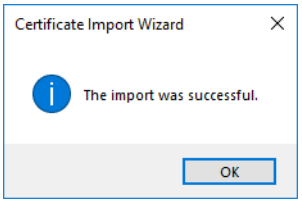
Certification Authorities is displayed in the **Certificate Store** column of the **Certificate Import Wizard** dialog box.



12. Click the **Next** button. The **Completing the Certificate Import Wizard** screen appears.



13. Click the **Finish** button. The **Certificate Import Wizard** dialog displays the message **Imported successfully**.



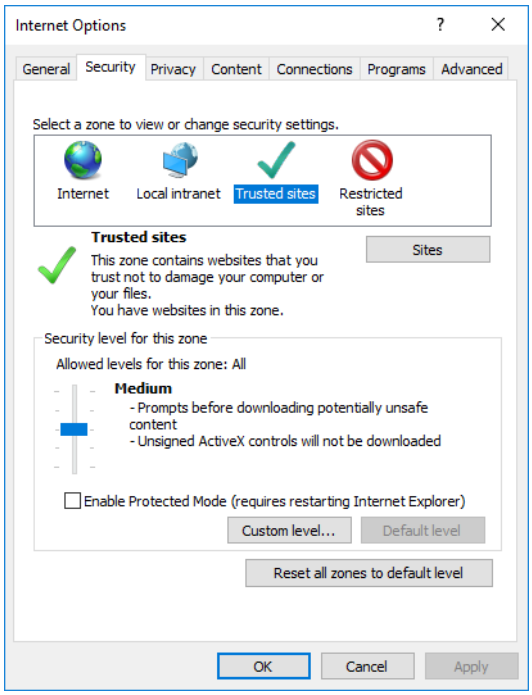
14. Click **OK** to close the **Certificate Import Wizard** dialog.

Add Vista Manager EX to trusted sites

When using Windows Server as the host operating system, and Internet Explorer 11 for the web browser from a remote browsing environment, you need to add the URL to access Vista Manager EX as a trusted site.

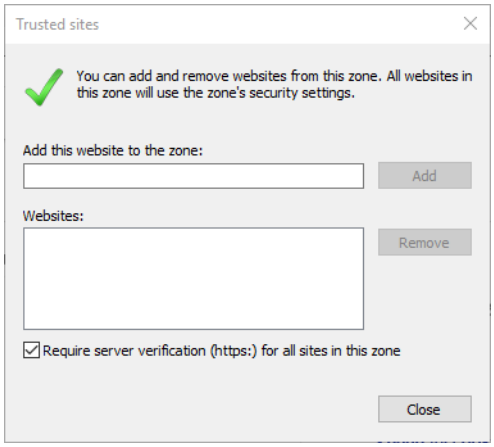
To add items to the trusted sites:

1. Open **Internet Options**, and select the **Security** tab. Select **Trusted sites** from the list of zones.



   Click the **Sites** button.

2. For each of the sites listed below, enter them in the **Add this website to the zone** text box, and click **Add**.



Note: If you are adding HTTP sites (as opposed to HTTPS), you must un-check the **Require server verification (https:) for all sites in this zone** checkbox.

3. Click **Close** on the **Trusted sites** dialog. Click **OK** on the **Internet Options** dialog.

Depending on how you are remotely accessing Vista Manager EX, refer to the list below to determine which sites to add to the Trusted Sites list.

1. “http://localhost:5000” or “https://localhost”
   OR
   “http://127.0.0.1:5000” or “https://127.0.0.1”
   - http://localhost
   - http://127.0.0.1
   - https://localhost
   - https://127.0.0.1
2. “http://<Windows host name>” or “https://<Windows host name>”
   OR
   “http://<Vista Manager server IP address>5000” or “https://<Vista Manager server IP address>”
   - http://<Windows host name>
   - http://<Vista Manager server IP address>
   - https://<Windows host name>
   - https://<Vista Manager server IP address>
3. “http://<DNS host name>:5000” or “https://<DNS host name>”
   - http://<DNS host name>
   - http://<Vista Manager server IP address>
   - https://<DNS host name>
   - https://<Vista Manager server IP address>

Exception settings when using Web proxy

If the AWC plug-in is installed on a Vista Manager EX server that is configured to use a proxy server, when accessing the AWC plug-in page from the server, add the IP address of the AWC plug-in to the exceptions for the proxy.

1. Open the **Internet Options** dialog. Select the **Connections** tab.
2. Under **Local Area Network (LAN) settings**, Click the **LAN settings** button. The **Local Area Network (LAN) Settings** dialog is displayed.
3. Click the **Advanced** button for **Proxy server**. The **Proxy Settings** dialog box appears.
4. Add the IP address of the AWC plug-in to **Exceptions**.
5. Click the **OK** button to close the **Proxy Settings** dialog. Then click the **OK** button to close the **Local Area Network (LAN) Settings** dialog. Then click the **OK** button to close the **Internet Properties** dialog.

Troubleshooting

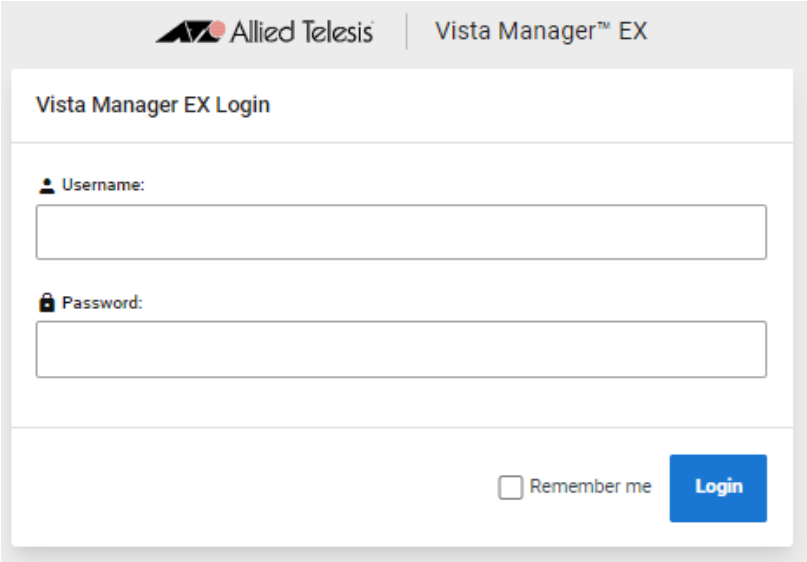
Ports and URLs used by Vista Manager EX

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

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

   - https://localhost:6443/NetManager/api/plugin_registration

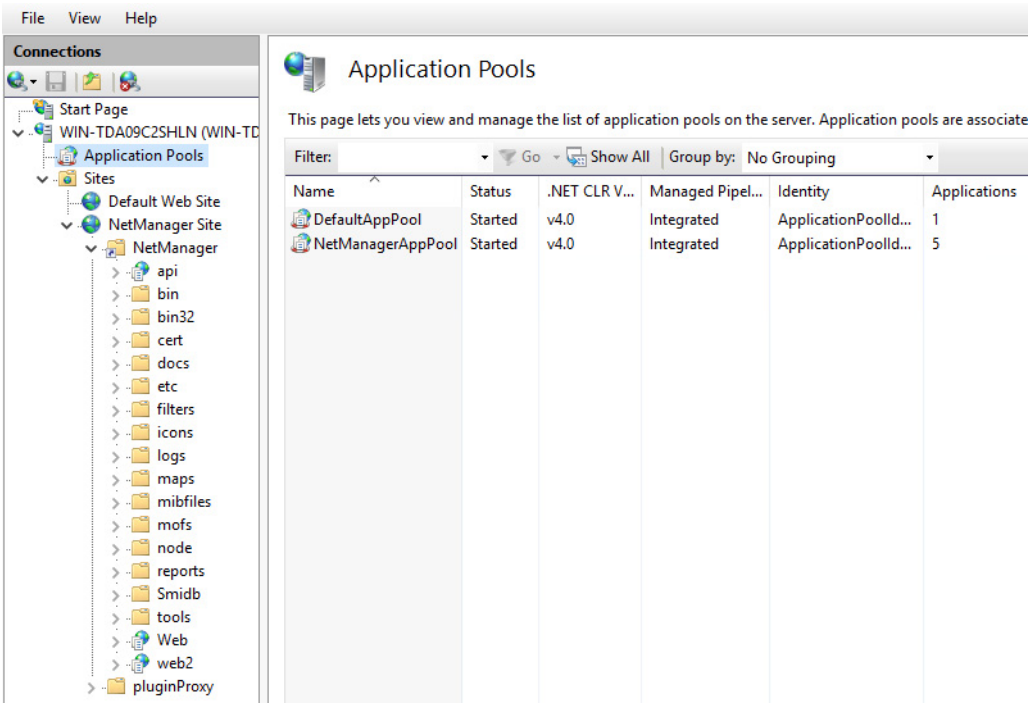
{"version":"1.0.0","baseUrl":"http://10.33.24.38/NetManager/api","product":{"name":"SNMP Plugin","type":"ann
{"major":1,"minor":0,"revision":0,"build":"B04"},"capabilities":["menu","event"]}}

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

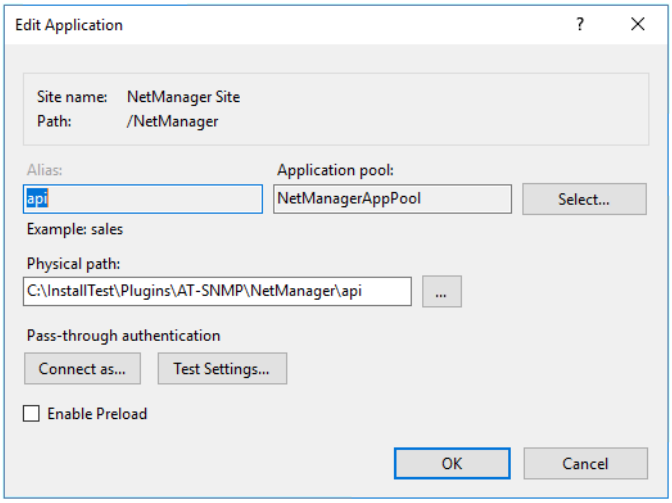
SNMP plug-in application pool settings

If you are having issues with the SNMP plug-in, you can check the IIS settings are correct.

1. Launch **Internet Information Services (IIS) Manager** on the Vista Manager EX server.
2. Expand out the following items in the Connections pane tree on the left-hand side:
   Computer name -> Sites -> NetManager Site -> NetManager
3. Make sure that the **api** and **web2** applications are available, and configured, as per the following screenshots.

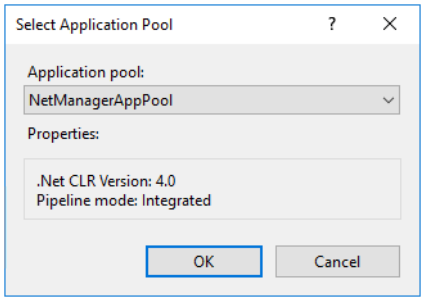


4. Select **api** in the Connections pane and then select Basic Settings in the Actions pane.

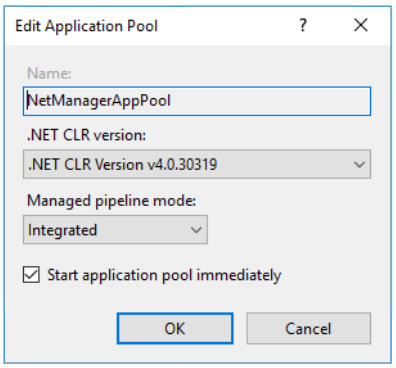


5. Click the select button and check that the Select Application Pool settings have the following properties:

   - .Net CLR version: 4.0
   - Pipeline mode: integration



6. Repeat for the **web** application.
7. If the **NetManagerAppPool** does not have the required properties, then select Application Pool in the Connections pane.
8. Select **NetManagerAppPool** from the Application Pools screen and select Basic Settings from the Edit Application Pool pane.
9. The application pool settings should look like the following:



Note: The “xxxxx” portion of the **.Net CLR Version v4.0.xxxxx** version will vary depending on the Windows OS installed.

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 15).

Clear browser cache

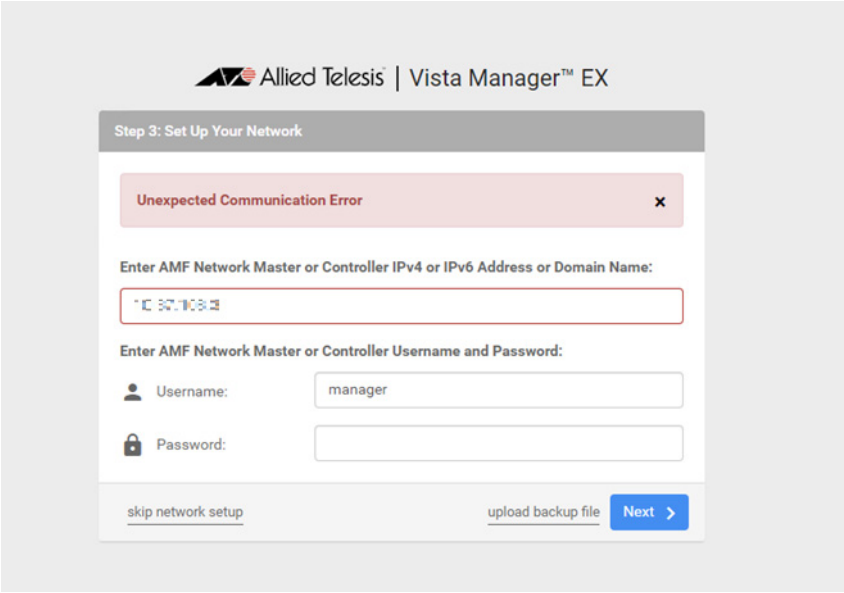
Clear your browser's cache after upgrading your Vista Manager EX installation. Incomplete dialog boxes, incorrectly populated drop-down lists, and truncated forms are all symptoms of a caching problem.

De-register the AWC plug-in on large wireless networks

Individual APs may disappear from the AWC plug-in if the plug-in is managing a large wireless network (approximately 600 APs or more). If this occurs, de-register the AWC plug-in from the Vista Manager's **System Management -> Plug-in Management** page. Features such as licensing, auto-recovery, and importing an AP from a guest device will still work, even if the plug-in is not registered.

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".

Problems adding plug-ins

If you are having difficulty adding the plug-ins in Vista Manager EX, make sure that you have done the following:

- Check that you have the correct URL for each plug-in as described in "Registering the plug-ins", and click on Verify Connection.
- Make sure that you have the certificates installed as described in "Import plug-in server certificate".
- Add the server address to your trusted sites as described in "Add Vista Manager EX to trusted sites".
- Add an exception for the server to your web proxy as described in "Exception settings when using Web proxy".

Supported Devices

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

- Vista Manager EX Datasheet

We recommend you run the most recent AlliedWare Plus version available for your device.

C613-04081-00 REV N