

# Release Note for Vista Manager EX Software Version 3.15.x



## VISTA MANAGER™ EX

» 3.15.0

---

## Acknowledgments

©2026 Allied Telesis Inc. All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Allied Telesis, AlliedWare Plus, Allied Telesis Management Framework, EPSRing, SwitchBlade, VCStack and VCStack Plus are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc. Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Additional brands, names and products mentioned herein may be trademarks of their respective companies.

## Getting the most from this Release Note

To get the best from this release note, we recommend using Adobe Acrobat Reader version 8 or later. You can download Acrobat free from [www.adobe.com/](http://www.adobe.com/)

---

# Content

<b>What's New in Vista Manager EX v3.15.0 .....</b>	<b>4</b>
<b>Important Considerations Before Upgrading .....</b>	<b>25</b>
<b>Obtaining User Documentation .....</b>	<b>26</b>
<b>Upgrading Vista Manager as a Windows-based installation .....</b>	<b>27</b>
<b>Upgrading Vista Manager on VST-APL .....</b>	<b>39</b>
<b>Upgrading Vista Manager on VST-VRT .....</b>	<b>39</b>
<b>Troubleshooting .....</b>	<b>39</b>

# What's New in Vista Manager EX v3.15.0

## Introduction

This release note describes the new features in Vista Manager EX™ v3.15.0. It covers changes to Vista Manager EX plus the optional Autonomous Wave Controller (AWC) plugin.

Further information is included for other supported plugins, and AMF Plus supported menu items, highlighted with a badge in the Vista Manager EX UI.

You can obtain the software files from the [Software Download area of the Allied Telesis website](#). Log in using your assigned email address and password.

Contact your authorized Allied Telesis support center to obtain licenses.

---

**Caution:** Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc.



While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

---

## New Features and Enhancements

This section summarizes the new features and enhancements added to Vista Manager EX version 3.15.0.

It includes:

- [“Support for SMTP OAuth Configuration” on page 6.](#)
- [“Using Experimental Features from Vista Labs” on page 15.](#)
- [“Vista Labs feature: Allie” on page 16.](#)
- [“Two-Factor Authentication support for login” on page 18.](#)
- [“Updates to link labels and bandwidth” on page 19.](#)
- [“Further Vista Manager EX API Support” on page 20.](#)
- [“Classing Oversize packets as errors” on page 20.](#)
- [“AWC enhancements” on page 21.](#)

---

## Change to the text on Automatic Endpoints Blocking feature

*Applies to all Vista Manager EX installations*

From version 3.15.0 onwards, text has been changed on the Automatic Endpoints Blocking popup to reflect the broader range of security alert sources.

Depending on the source of Security Alerts, additional features may need to be enabled in **System Management > Optional Features**.

The screenshot shows a configuration window titled "Automatic Endpoints Blocking" with a close button (X) in the top right corner. Inside the window, there is a blue information box with a blue 'i' icon containing the following text: "Turning on the 'Auto-block Unsafe Endpoints' feature will automatically block any unsafe RADIUS-enabled endpoints when security alerts are received. These alerts are generated by our security event rules, and can also be received externally, helping keep your network secure. Depending on the source of Security Alerts, additional features may need to be enabled in [System Management Optional Features](#)". Below this box are two toggle switches, both currently set to "Disabled": "Auto-Block Unsafe Endpoints" and "Send Email Notification when Endpoints are automatically blocked". Underneath is a section titled "Minimum Alarm Severity" with the instruction "Choose the minimum security alert severity needed to block an unsafe endpoint." and a dropdown menu currently showing "Alert". A "Save" button is located in the bottom right corner of the window.

---

## Support for SMTP OAuth Configuration

*Applies to all Vista Manager EX installations*

From version 3.15.0 onwards, you can use OAuth as an SMTP authorization method by configuring OAuth for SMTP.

OAuth allows Vista Manager to securely request permission to send emails on your behalf without storing your password.

Support for SMTP OAuth is supported with the following email providers:

- Google
- Microsoft

**Note:** You must access Vista Manager from the same hostname as specified in your redirect URI for security reasons. We recommend using the most public hostname of your Vista Manager EX server or a DNS-allocated host address. Your redirect URI must use HTTPS.

### How to configure OAuth with Microsoft

You will need the following prior to setup:

- an Azure subscription,
- a Microsoft Entra Subscription,
- and an Outlook Online subscription with at least 1 user set up. Vista Manager will send emails from this account.

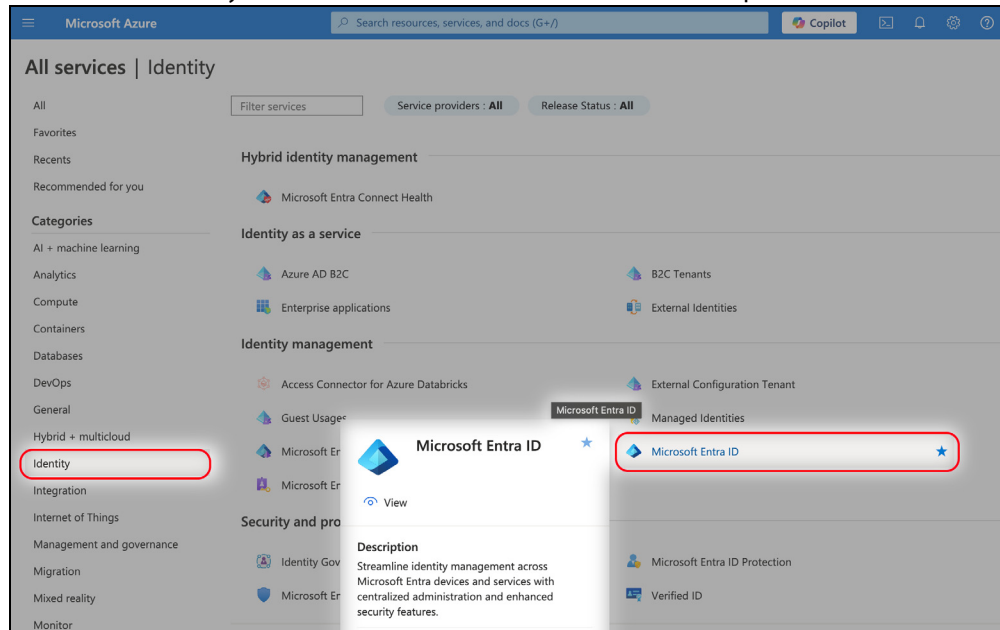
### 1. Access the Azure Portal

Access the Azure Portal from <https://portal.azure.com/#home> and log in using your Microsoft Azure credentials.

### 2. Navigate to Microsoft Entra ID

Go to **All Services > Identity > Microsoft Entra ID**.

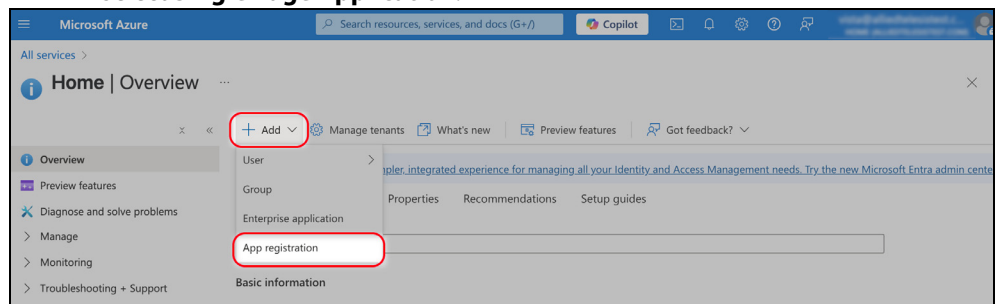
- Alternatively search for Microsoft Entra ID and move to step 3.



### 3. Register a New Application

- Click **Add > App Registration**

- Select **Single Page Application**.



#### 4. Register an Application in Azure

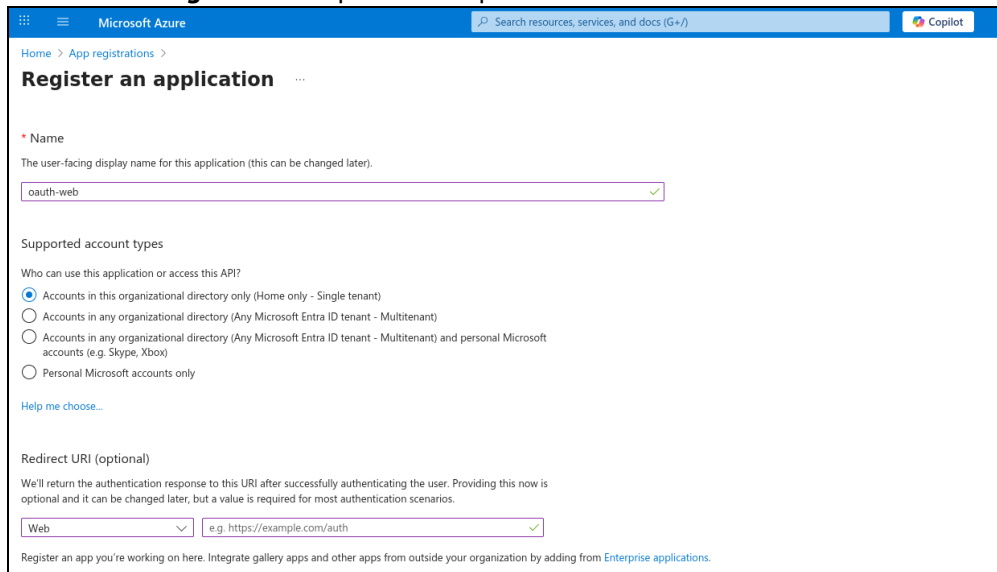
Fill out the Application registration form with the required details:

- For Web Application Type select **Single Tenant**
- **Paste** the redirect URI from **Vista Manager**

This is auto-generated by Vista Manager in the "Redirect URI" form field.

Copy this from Vista Manager and paste it into the Redirect URI field in the Azure App Registration form. You can see how to get the Redirect URI from ["Support for SMTP OAuth Configuration"](#) on page 6.

- Click **Register** to complete this step.



The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The page title is 'Register an application' and the breadcrumb is 'Home > App registrations >'. The form includes the following fields and options:

- Name:** A text input field containing 'oauth-web' with a green checkmark on the right. Below the field is the text: 'The user-facing display name for this application (this can be changed later).'
- Supported account types:** A section titled 'Who can use this application or access this API?' with four radio button options:
  - Accounts in this organizational directory only (Home only - Single tenant)
  - Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
  - Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
  - Personal Microsoft accounts onlyA link 'Help me choose...' is located below these options.
- Redirect URI (optional):** A section with the text: 'We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.' It contains two input fields: a dropdown menu set to 'Web' and a text input field containing 'e.g. https://example.com/auth' with a green checkmark on the right.

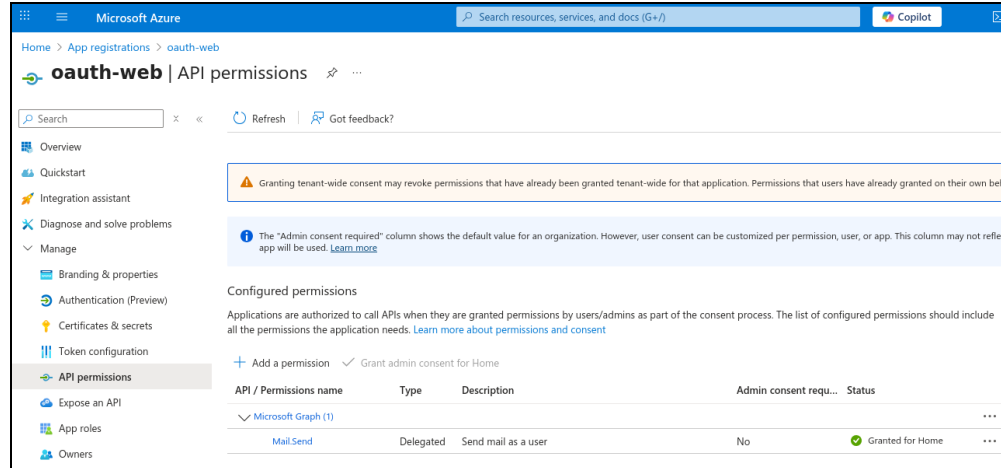
At the bottom of the form, there is a note: 'Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.'

## 5. Assign Email-Sending Permissions to Azure for Vista Manager

In the Azure Portal, go to the App Registration for Vista Manager.

Under API Permissions, add a new permission for Microsoft Graph:

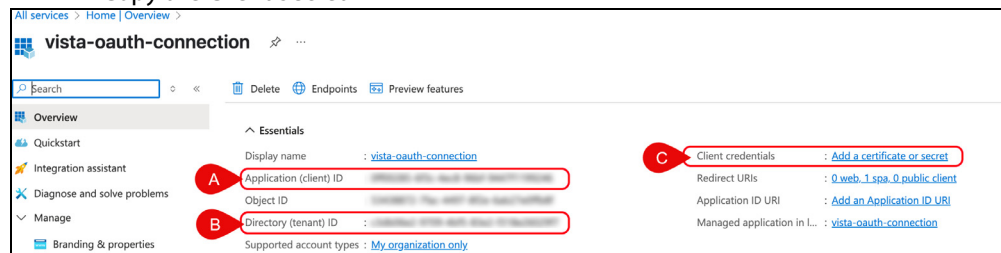
- Type - **Delegated**
- Permission - **Mail.Send**



- Click **Register**
- The Application Overview page will open where you can find the Tenant ID and Client ID

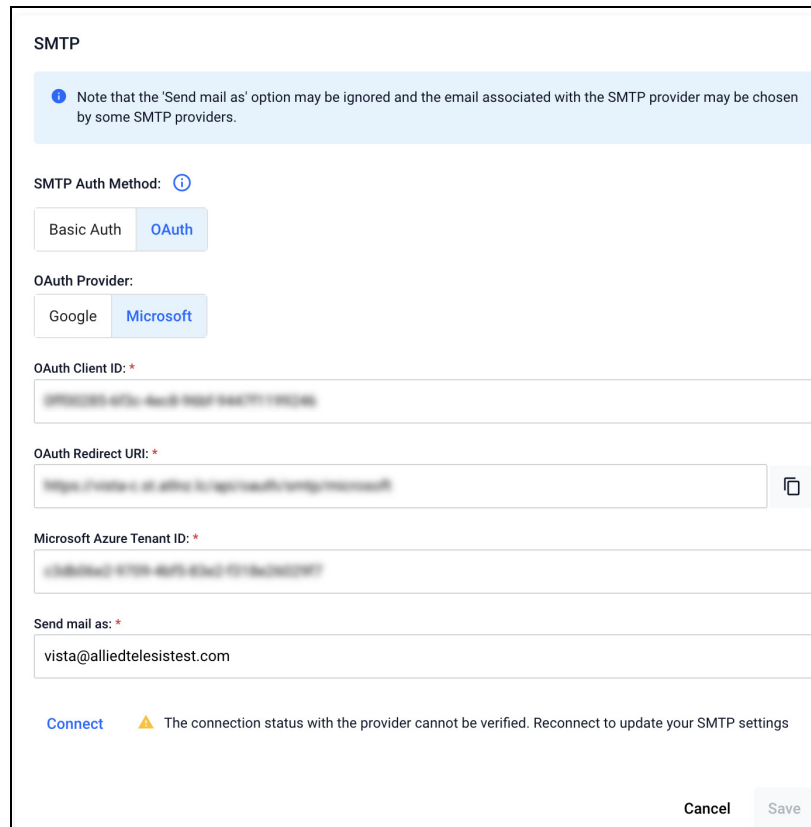
## 6. Complete Registration and Collect IDs from the Application Overview page

- Copy the Client ID
  - Copy the Tenant ID
  - Click the 'Client Credentials' link and create a new Client Secret
- Copy the Client Secret



## 7. Set up the OAuth in Vista Manager

- Go to the **System Management > Configuration** page.
- Scroll down to the SMTP settings and click **Edit**.
- Under the SMTP Auth Method, select the OAuth tab.
- Select from Microsoft as a provider and enter the previously copied Client ID, Tenant ID, and Client Secret



The screenshot shows the SMTP configuration interface. At the top, there is a note: "Note that the 'Send mail as' option may be ignored and the email associated with the SMTP provider may be chosen by some SMTP providers." Below this, the "SMTP Auth Method" is set to "OAuth". The "OAuth Provider" is set to "Microsoft". The "OAuth Client ID" field contains a masked value. The "OAuth Redirect URI" field contains a URL with a copy icon. The "Microsoft Azure Tenant ID" field contains a masked value. The "Send mail as" field contains the email address "vista@alliedtelesistest.com". At the bottom, there is a "Connect" button, a warning message: "The connection status with the provider cannot be verified. Reconnect to update your SMTP settings", and "Cancel" and "Save" buttons.

## 8. Connect your Microsoft Entra account with Vista Manager

- Click **Connect and Save** to go to the Microsoft landing page.
- Sign in with your Microsoft Entra credentials, and you will be sent back to Vista Manager.
- You will see a **Green Tick** when the connection is successful.
- If verification takes longer than 30 seconds a warning message is shown.

## Configuration of an Application with Google

You will need the following prior to setup:

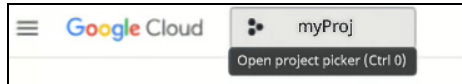
- a Google Workspace account
- access to the Google Cloud Platform

### 1. Access the Google Cloud platform

Navigate to <https://console.cloud.google.com/> and log in using your Google account credentials.

### 2. Create a new OAuth project

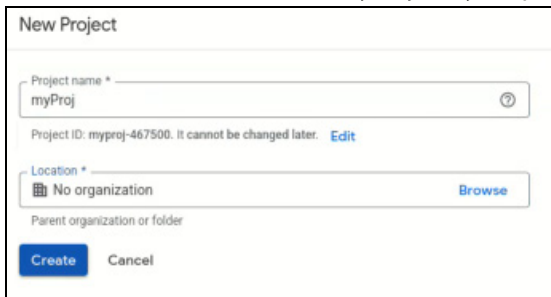
- Click on the Project button in the top navigation bar



- Select **New Project**



- Enter a name (such as myProj) for your project and click **Create**.

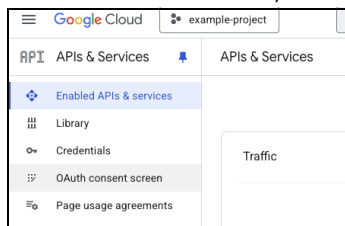


### 3. Create a new OAuth Client

- Click on the name of the existing project to go to the Overview screen.
- On the Overview page, click the **Create OAuth client**
- Enter Application information for your project

### 4. Configure OAuth Consent Screen

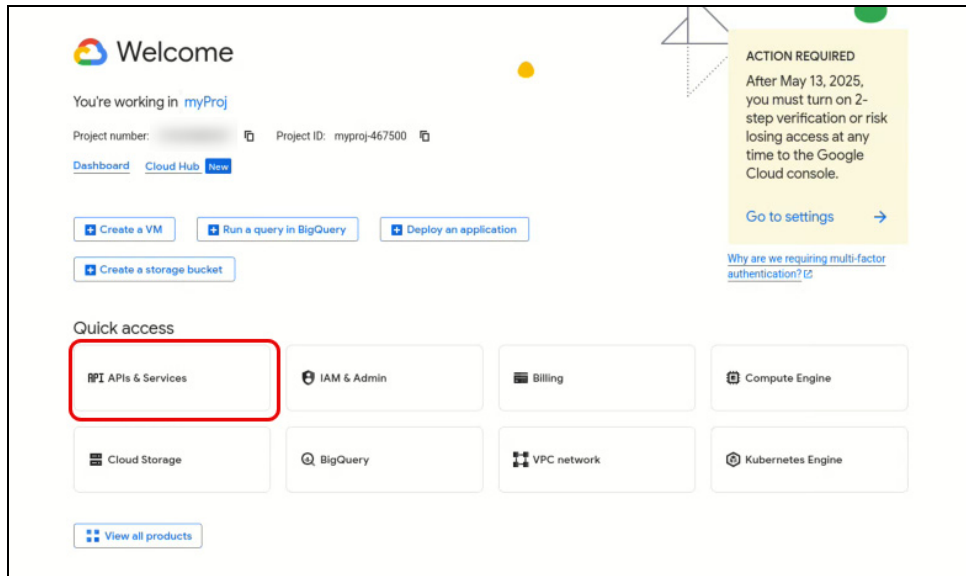
- In the left menu, select OAuth consent screen.



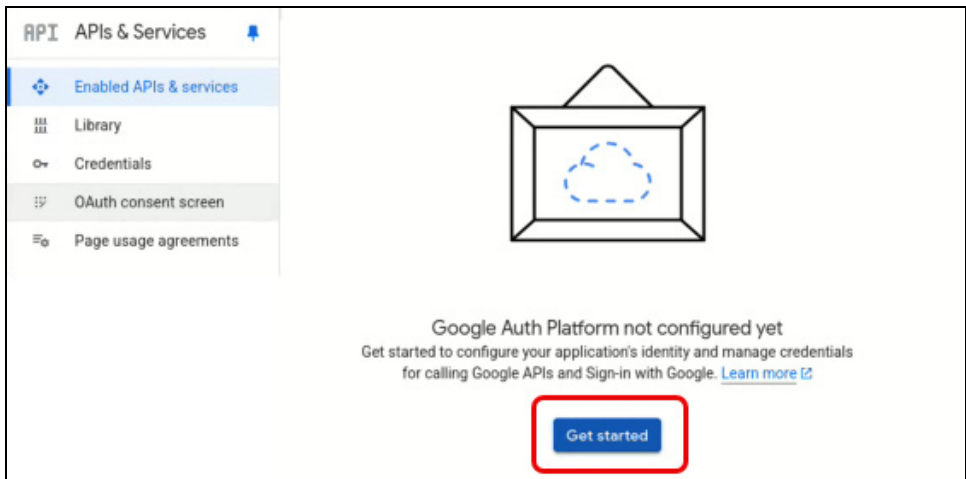
- We recommend selecting **Internal** as Google Workspaces will restrict access to 'send emails as' to emails within your organization.
- Fill in the required fields (App name, User support email, Developer contact information)
- Save and continue

### 5. Configure the Google Auth Platform

- On your newly created project's dashboard click APIs & Services button



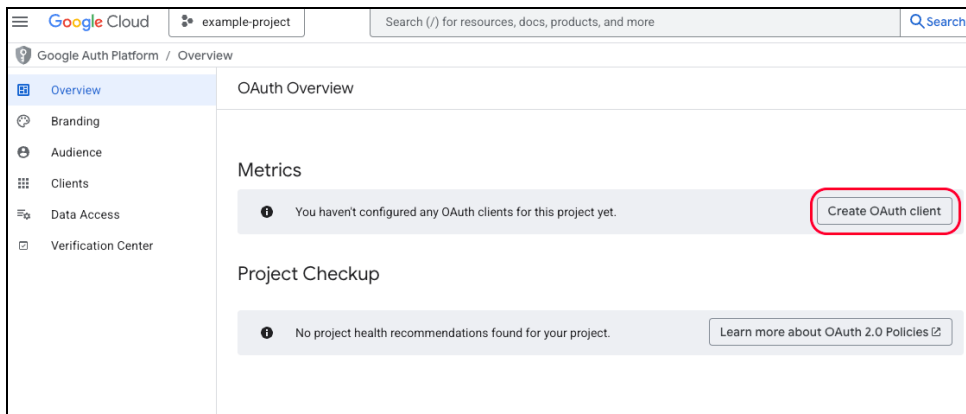
- Click Get Started



- Enter the project configuration information, and click Create when done.
- This will take you to the OAuth Overview page.

## 6. Create OAuth Client ID Credentials

- From the OAuth Overview page, click **Create OAuth Client**



- In the **Authorized redirect URIs** section, add the redirect URI provided by Vista Manager.

Google Cloud example-project Search (/) for resources, docs, products, and more

Google Auth Platform / Clients / Create client

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type \*  
Web application

Name \*  
vistaOAuthClient

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

**i** The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins ⓘ  
For use with requests from a browser

+ Add URI

Authorized redirect URIs ⓘ  
For use with requests from a web server

URIs 1 \*  
https://vista-example.mydomain.org

+ Add URI

Note: It may take 5 minutes to a few hours for settings to take effect

Create Cancel

- Click **Create**

- After creating the credentials, **copy the Client ID** by clicking the copy icon

Google Cloud example-project Search (/) for resources, docs, products, and more

Google Auth Platform / Clients

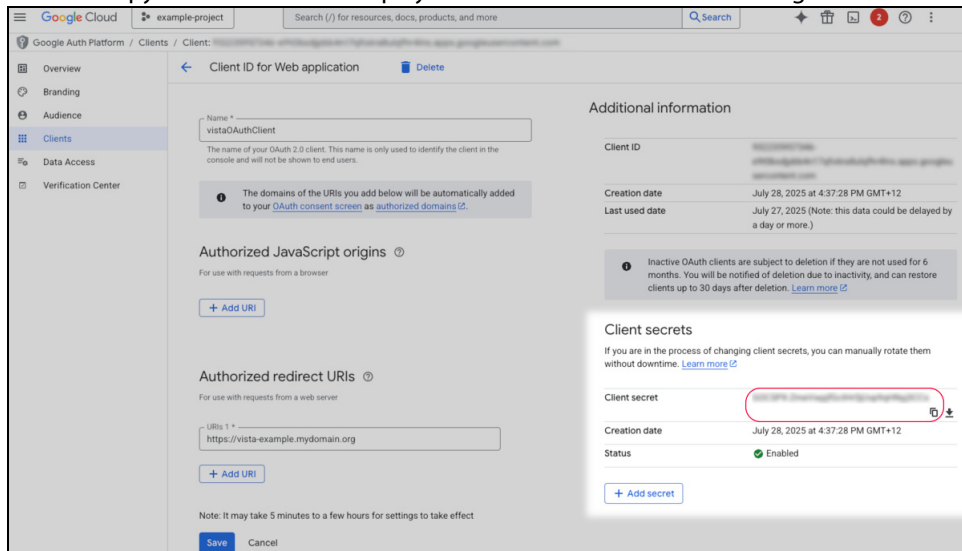
Clients + Create client Delete Restore deleted OAuth clients

OAuth 2.0 Client IDs

<input type="checkbox"/>	Name	Creation date ↓	Type	Client ID	Actions
<input type="checkbox"/>	<a href="#">vistaOAuthClient</a>	Jul 28, 2025	Web application	932235957346-e9t0...	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

- Click on the **name of the new Client ID** to go to the Client ID for Web application page.

- Copy the Client Secret displayed on the screen in the bottom right.



## 7. Set up the OAuth in Vista Manager

- Go to the **System Management > Configuration** page.
- Scroll down to the SMTP settings and click **Edit**.
- Under the SMTP Auth Method, select the OAuth tab.
- Select from Google as a provider and enter the previously copied OAuth Client ID and OAuth Client Secret
- Enter the email account you would like to send emails as
- Click Connect and Save

The screenshot shows the SMTP configuration page in Vista Manager. The 'SMTP Auth Method' is set to 'OAuth'. The 'OAuth Provider' is set to 'Google'. The 'OAuth Redirect URI (Auto Generated)' is 'https://example-vista.mydomain.com/api/oauth/smtp/google'. The 'OAuth Client ID' field contains '<client-id>'. The 'OAuth Client Secret' field contains '<client-secret>'. The 'Send mail as' field contains '<mygmailaccount@gmail.com>'. There are 'Cancel' and 'Connect And Save' buttons at the bottom right.

- If verification takes longer than 30 seconds a warning message is shown.

## 8. Connect your Google account with Vista Manager

- Click **Connect and Save** to go to the Google landing page.
- Sign in with your Google account, and you will be sent back to Vista Manager.
- You will see a **Green Tick** when the connection is successful.

## Using Experimental Features from Vista Labs

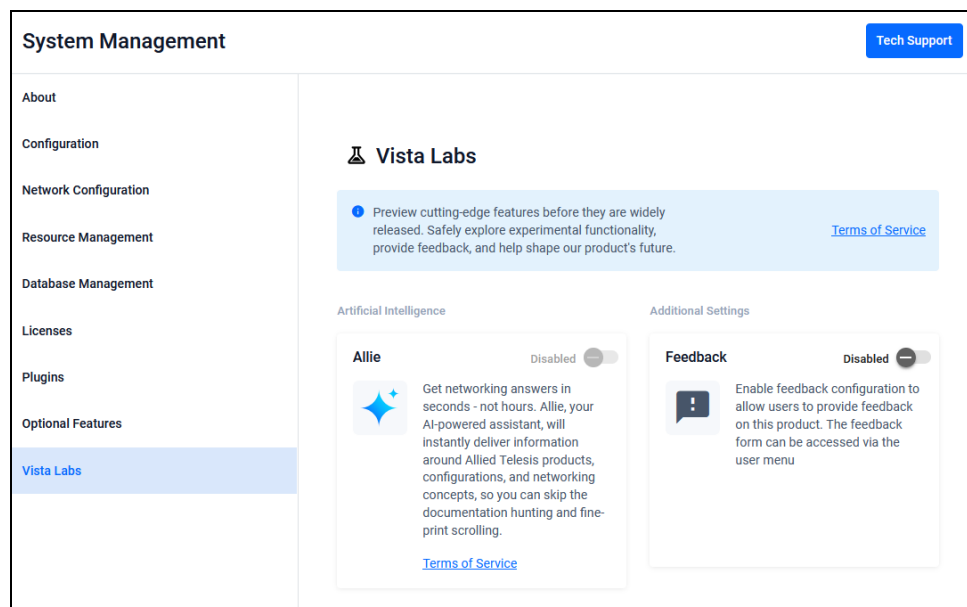
*Applies to all Vista Manager EX installations*

From version 3.15.0 onwards, you can trial new or experimental features from the new Vista Labs menu.

A Terms of Service popup will appear when you click on the Vista Labs tab. Please read it prior to agreeing to use Vista Labs features. It can be viewed again from the Terms of Service link on the info-card above the features.

You will then have access to the Vista Labs features, and you can toggle on features you would like to use.

Currently, these new features include Allie, our AI assistant, and feedback for Vista Manager.



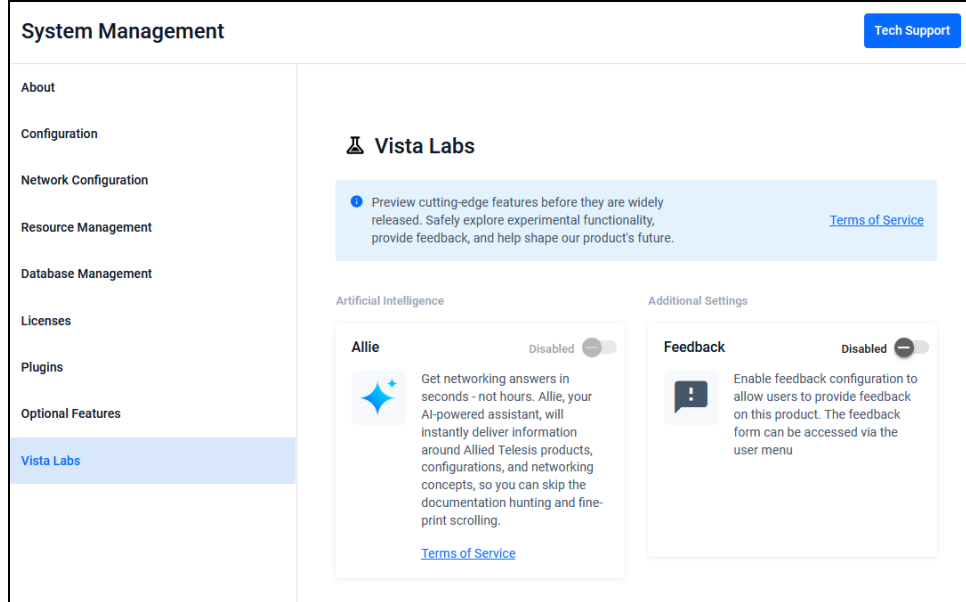
Toggle feedback to allow all users to provide feedback on Vista Manager. After toggling this, you can access the Feedback form from the User Management menu.

If you have any feedback for the Vista Labs features, use the Feedback section of the Vista Labs page.

# Vista Labs feature: Allie

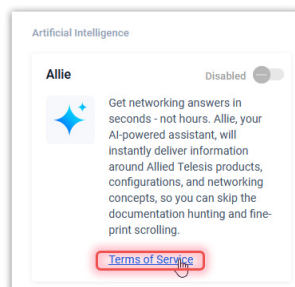
Applies to all Vista Manager EX installations

From version 3.15.0 onwards, you can access our AI assistant, Allie, within Vista Manager to receive assistance.

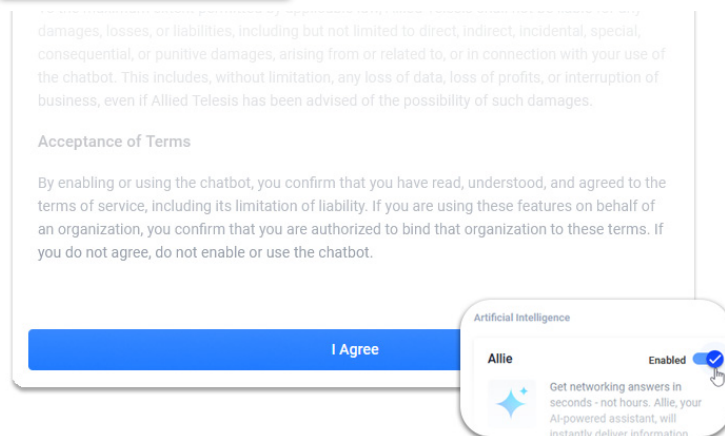


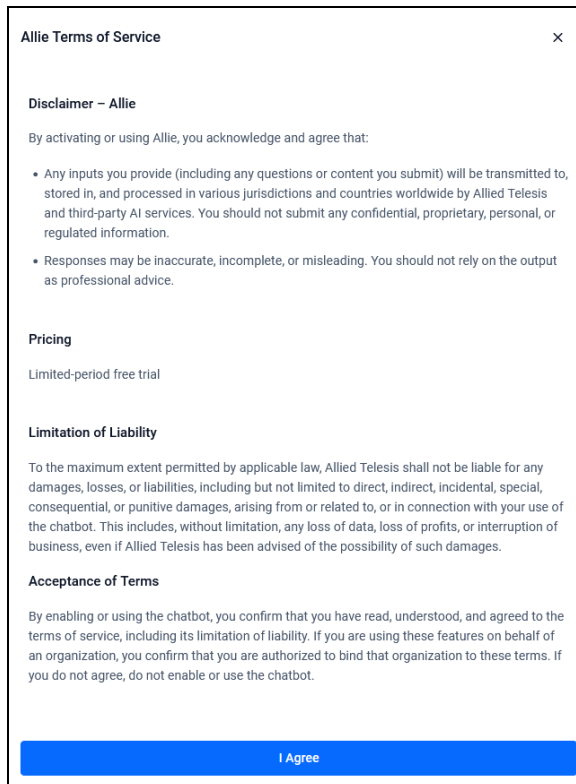
Allie can give you guidance on network configurations and features, networking concepts, and information on Allied Telesis products.

When you first see the widget, the Enable/Disable toggle will be greyed out.

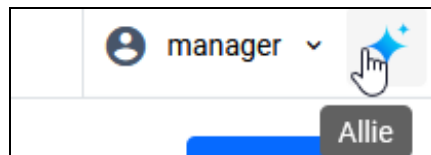


To enable Allie, you must first read Allie's Terms of Service under the widget before you can Enable the feature.





After you enable Allie, click the new icon in the top right corner to start a chat.



---

# Two-Factor Authentication support for login

*Applies to all Vista Manager EX installations*

From version 3.15.0 onwards, support for Two-Factor Authentication (2FA) has been added to Vista Manager.

As an Admin user, you can enable 2FA for your own account, other admin accounts, or general users.

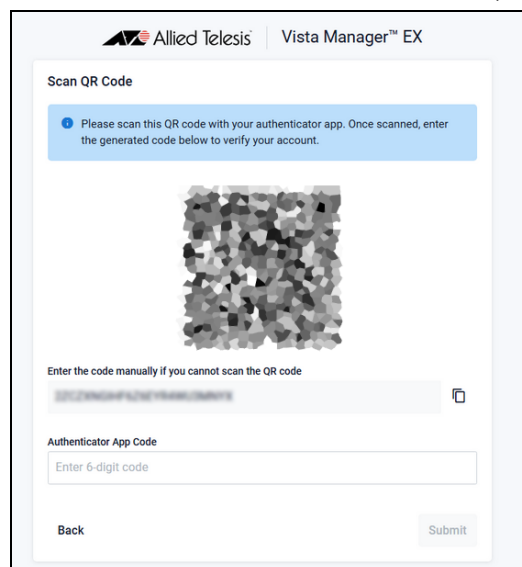
1. To enable 2FA, click the toggle on the User Management page.

**Note:** 2FA requires SMTP to be configured before it can be enabled.

If you are using a VST-APL device, 2FA requires an NTP server to be set up for accurate time service.

2. After enabling 2FA from Vista Manager, when you next log in you will be shown a QR code to scan on your authentication app of choice.

2FA is supported with any mobile authenticator that supports TOTP (such as Google Authenticator, Microsoft Authenticator, Authy, LastPass Authenticator, and many more).



The screenshot shows the Vista Manager EX login interface. At the top, it says "Allied Telesis Vista Manager™ EX". Below that, the heading is "Scan QR Code". A blue instruction box says: "Please scan this QR code with your authenticator app. Once scanned, enter the generated code below to verify your account." In the center is a large QR code. Below the QR code, there is a text input field with the placeholder "Enter the code manually if you cannot scan the QR code" and a copy icon. Underneath that is another text input field labeled "Authenticator App Code" with the placeholder "Enter 6-digit code". At the bottom left is a "Back" link, and at the bottom right is a "Submit" button.

- User level accounts cannot enable or disable 2FA.
- Authenticator codes appear under the title 'VistaManager: Your Username'
- Enter a valid code from your authenticator app into the Authenticator App Code field. Click **Submit** and you will log in as normal.
- After 5 incorrect code attempts, you must wait 5 minutes before you can try again
- Clicking **Remember me** on the login screen skips 2FA, even if it is enabled. **Remember me** lasts for 14 days.

## Reissuing the QR code

You can re-issue the 2FA QR in different ways, depending on the status of your account.

- As a normal user, click the reset link sent to your registered email.
- Admin users can enable and disable 2FA for that specific account.

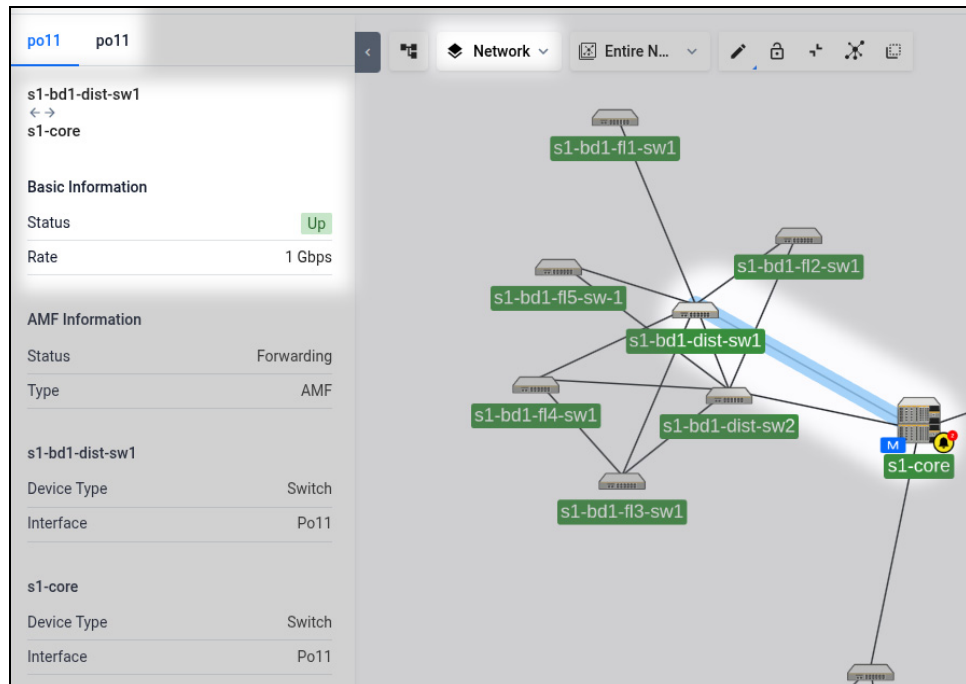
# Updates to link labels and bandwidth

Applies to all Vista Manager EX installations

From version 3.15.0 onwards, the link side panel has been updated.

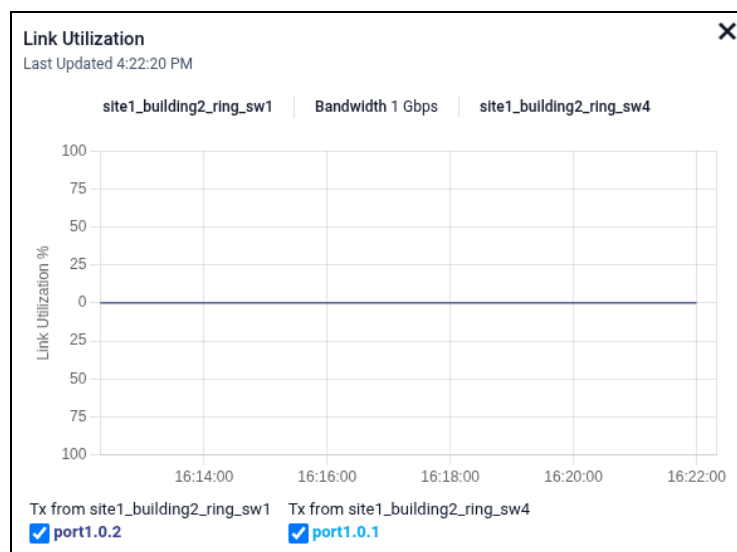
When you click on a link between two devices on the Network Map, two tabs that represent the two directions of the link have been added.

You can see the speed rate of the link in gigabits per second (Gbps) under the status column. This speed will scale based on the speed of the link.



Note that both tunnel links and STOAT links where one link is a non-STOAT device, and is not learned via any other plugin will not display two tabs.

The Link Utilization graph also shows the link Bandwidth. This label will change depending on the speed of the link (such as Kbps, Mbps, or Gbps).



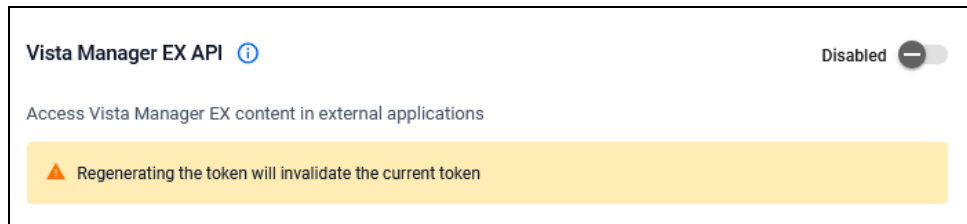
---

## Further Vista Manager EX API Support

*Applies to all Vista Manager EX installations*

From version 3.15.0 onwards, support for extra API categories for Health Monitoring and Endpoints have been added.

You can create a token for access to the API from the System Management > Configuration page.



Click the [i](#) button to see instructions about how to use the API.

## Classing Oversize packets as errors

*Applies to all Vista Manager EX installations*

From version 3.15.0 onwards, oversize packets are not classified as errors by default, however you can turn on the function to classify them as errors by toggling them on.

You can do this by opening the Health Monitoring Settings > Size section from the Health Monitoring dashboard.

## AWC enhancements

### Ability to backup client history and logs for VST-VRT

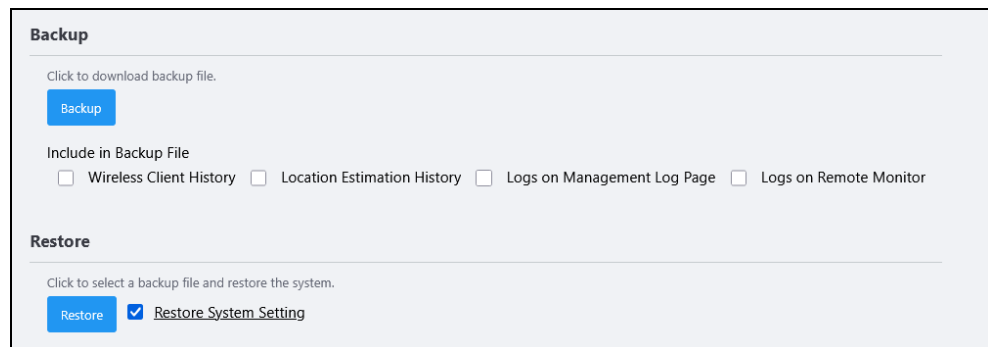
*Applies to the AWC Plugin on Vista Manager VST-VRT installations.*

From version 3.15.0 onwards, support has been added for client history and logs for VST-VRT installations. You can take a backup of your existing data from the Windows version of the AWC plugin, and restore it on the VST-VRT version.

To do this, navigate to the **AWC Plugin > System Setting** menu and scroll down to Backup.

You can then restore the downloaded backup from Vista Manager's AWC Plugin > System Setting menu by selecting it in the Restore section.

Select any optional features you want to back up (such as Location Estimation History or Logs on Remote Monitor) and they will be included in the export.



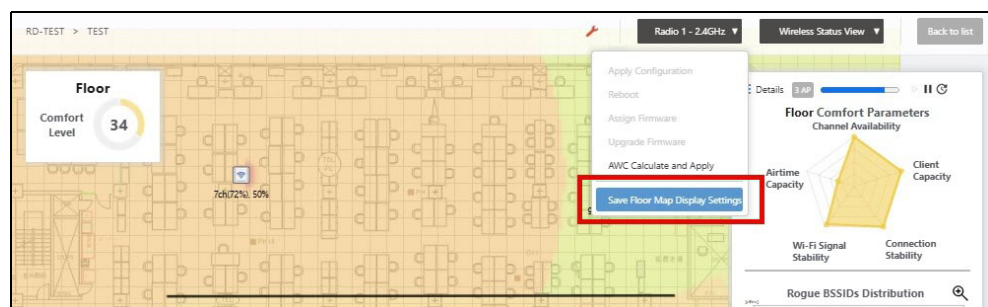
The screenshot shows a 'Backup' section with a 'Backup' button and a 'Restore' section with a 'Restore' button and a checked 'Restore System Setting' option. The 'Include in Backup File' section has four unchecked checkboxes: 'Wireless Client History', 'Location Estimation History', 'Logs on Management Log Page', and 'Logs on Remote Monitor'.

### Option to save current floormap settings

*Applies to the AWC Plugin on Vista Manager EX installations.*

From version 3.15.0 onwards, you can save the current floormap view settings.

You can save the current view by clicking the spanner icon when in the AWC Floormap view, then selecting the 'Save Floor Map Display Settings' option.



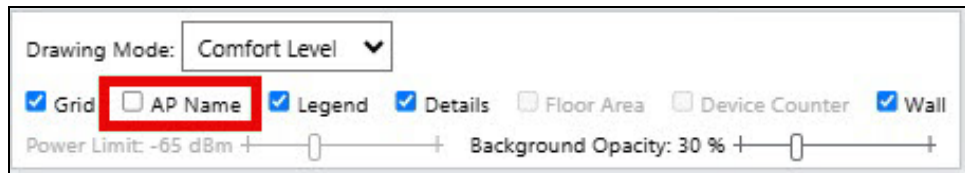
---

## Option to display AP name above icons on floormap

*Applies to the AWC Plugin on Vista Manager EX installations.*

From version 3.15.0 onwards, you can select to always display an AP's name above its floormap icon.

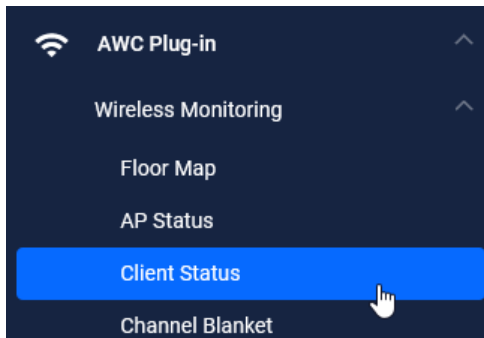
To display AP names above icons, click the 'AP Name' checkbox from the floormap settings overlay.



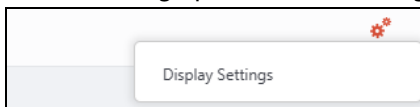
## Client AP Status graphs

*Applies to the AWC Plugin on Vista Manager EX installations.*

From version 3.15.0 onwards, you can view donut and stacked graphs of the current number of client connections on APs from the Client Status page.

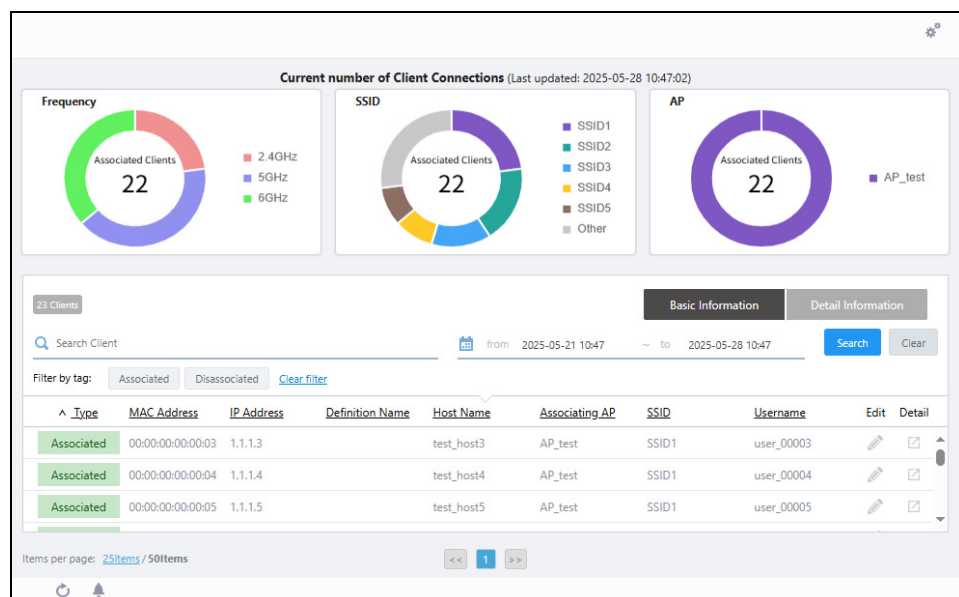


To enable the graphs, hover over the gear icon to open the drop-down menu.



Click the Display Settings, and Enable Graph Display.

- The donut graph shows the number of client connections by frequency, SSID, and AP.
- The stacked graph shows the history of client connections.



## Timezone displayed based on your timezone

Applies to the AWC Plugin on Vista Manager EX installations.

From version 3.15.0 onwards, support for timezones have been added. Time-based outputs will now display in your local PC's timezone.

## Selecting different timezones for specific task

You can set a specific timezone for tasks when scheduling a task from the Task Scheduling page.

The default timezone is the timezone reported from your device running the AWC application.

**Note:** When daylight savings time and standard time is switched, some tasks will be skipped or pass through twice. We recommend you do not set 'Start' or 'AWC Calculation Time' tasks during daylight savings time.

## Selecting a timezone exported on a CSV file

The time shown when exporting a CSV file defaults to Coordinated Universal Time (UTC), however you can set a custom timezone in the AWC settings. You can export CSV files in the following formats:

- YYYY-MM-DDThh:mm:ssZ with Coordinated Universal Time (UTC) Time as the timezone
- YYYY-MM-DD hh:mm:ss with your custom selected timezone

The screenshot shows the 'History Data Retention Period Setting' interface. The 'Datetime format in CSV files' section is highlighted with a red border. It contains two fields: 'Datetime Format' and 'Timezone'. The 'Datetime Format' field has two radio button options: 'YYYY-MM-DDThh:mm:ssZ' (unselected) and 'YYYY-MM-DD hh:mm:ss' (selected). The 'Timezone' field is a dropdown menu currently showing '(UTC+09:00) Asia/Tokyo'. Other sections visible include 'Wireless Client', 'Location Estimation', 'IDS Report', 'Log', and 'Network Map Setting', each with its own set of configuration options and 'Save' buttons.

---

# Important Considerations Before Upgrading

This section describes changes that may affect Vista Manager EX or your network's behavior if you upgrade. Please read it carefully before upgrading.

## Manual polling recommended if upgrading

*Applies to all Vista Manager EX installations*

From version 3.11.0 onwards, we recommend that you poll the network manually after upgrading Vista Manager EX.

This makes sure that Vista Manager EX acquires functionality that has been added in the new release, including functionality that depends on information from devices. Otherwise, features may fail to detect devices and will not work as intended.

To poll manually, use the **Refresh Topology** button on the Network Map:



## Traffic map data not restored

When you upgrade Vista Manager EX, traffic map data from earlier versions will not be imported.

## Upgrading versions earlier than 3.9.0

If you create a backup on a version earlier than 3.9.0, and you want to upgrade to a new version, you must first install your backup on version 3.9.0 and export the backup again. Then you can upload the new backup to a later version of Vista Manager (such as v3.14.0).

If you upgrade directly to 3.14.0 instead (for example, from 3.7.0 to 3.14.0 without upgrading to 3.9.0 first), you may encounter data corruption or incompatibility issues.

Alternatively, you can choose to perform a fresh install of the newer version and configure it from new.

## Health Monitoring sensor widgets are empty after upgrading from 3.13.x

After upgrading from 3.13.x, sensor gauge widgets will be empty on the Health Monitoring page's flexible dashboard. If you have created any latest or historical temperature widgets for specific devices, you need to re-create these widgets again after upgrading.

---

## Internet Explorer 11 compatibility

When using the Vista Manager EX integrated map with Internet Explorer 11, you may find performance to be slower, particularly with large maps. Therefore, we recommend using a different browser, especially if you have a large network.

## Virtualization support

The Vista Manager EX virtual appliance is not supported on VMware vSphere Hypervisor (ESXi) 5.5. Please upgrade to VMware vSphere Hypervisor (ESXi) 6.0, 6.5, 6.7, 7, or 8 if you wish to use this version of Vista Manager EX.

## Vista Manager plugins

Do **not** delete a plugin from Vista Manager during a version upgrade. No de-registering or re-registering of plugins is required during this stage.

## Fibre monitoring feature permissions

Note that on a **new** installation of Vista Manager EX, you will need to enable **Active Fibre Monitoring** permissions for users. This can be done on the **User Management** page.

## Disabling Internet Breakout disables all PBR rules

Internet Breakout uses policy-based routing (PBR) rules. When you use Vista Manager EX to disable Internet Breakout, it disables all PBR rules, including:

- rules created by SDWAN, and
- rules created by Internet Breakout, and
- rules created manually through the CLI.

# Obtaining User Documentation

### Vista Manager documentation

Installation Guides, User Guides and Release Notes for Vista Manager EX are available on our [website, alliedtelesis.com](http://www.alliedtelesis.com).

### AMF Plus documentation

For full AlliedWare Plus documentation, see our online documentation library. For AMF Plus, the library includes the following documents:

- the [AMF Plus Feature Overview and Configuration Guide](#)
- the [AMF Plus Datasheet](#)
- the [AMF Plus Cloud Installation Guide](#).

---

# Upgrading Vista Manager as a Windows-based installation

Windows-based Vista Manager has two optional plug-ins. These can be upgraded at the same time as Vista Manager EX.

## Obtain the executable files

1. Download Vista Manager EX from the [Allied Telesis Support Portal](#). 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 'atvmexXXXbXXw.exe', with the Xs denoting the version and build numbers.
  - The AWC plug-in is called 'atawcXXXbXXw.exe'.
  - The SNMP plug-in is called 'atsnmpXXXbXXw.exe'.

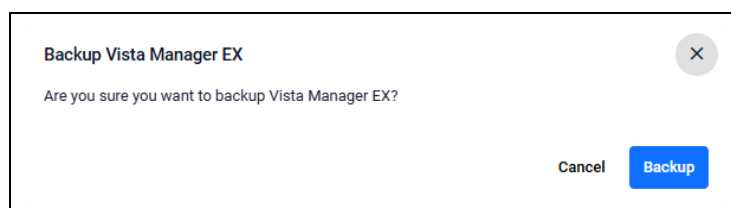
*Do not rename these files. The installation requires them to be in this format.*

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.

## Backup Vista Manager EX and the plug-ins

### Backup Vista Manager EX

1. Log in to Vista Manager and select the **System Management** page.
2. In the **Database Management** page, click on the **Backup** button next to the Backup tab.
3. Click **Backup** again to confirm you wish to make a backup.



This automatically downloads a **tar** file backup to your default download location.

### Backup the SNMP plug-in

4. If you have the SNMP plug-in installed, log on locally to the **Vista Manager EX Server** on your Windows device.
5. **Stop** the SNMP server services using the shortcut or by running the following command line:

```
"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\svrstop
```

6. Run the backup utility by using the shortcut or by running the following command line.

```
"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\SMBBackup.exe"
```

Follow the instructions on the screen.

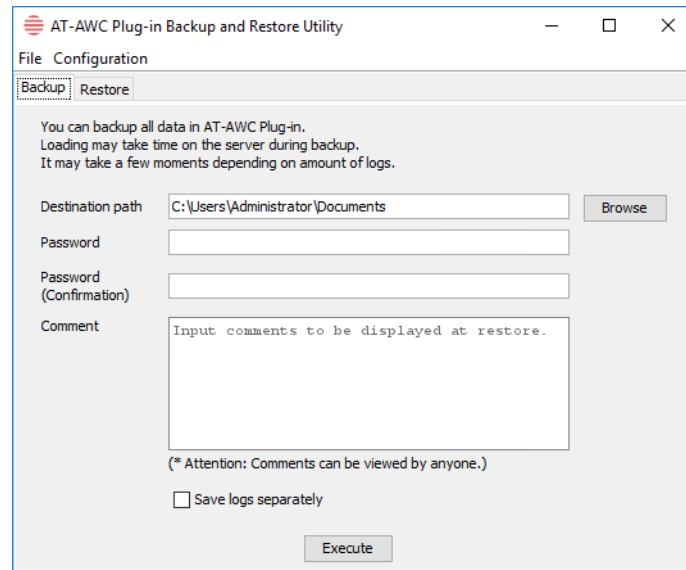
## Backup the AWC plug-in

7. If you have the AWC plug-in installed then log on locally to the Vista Manager EX server.
8. Stop the AWC server services using the shortcut or by running the following command line.

**"<Vista Install Path>\Plugins\AT-AWC\root\stopserver.bat"**

9. Run the backup/restore utility by using the shortcut or running the following command line.

**"<Vista Install Path>\Plugins\AT-AWC\tools\maintenance\maintenance.bat"**



10. Select the backup tab and follow the instructions on the screen.

**Note:** The default location of <Vista Install Path> is **C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX**

## Uninstall the existing version

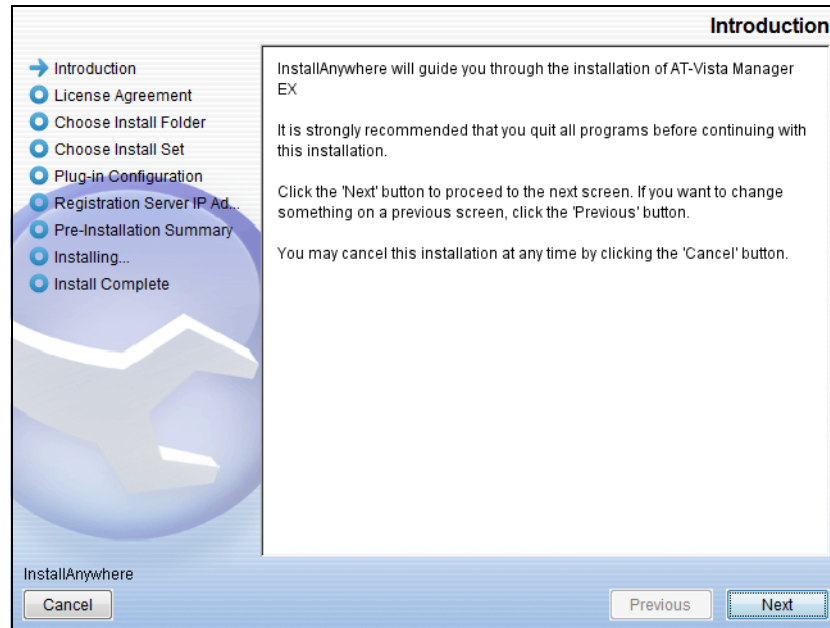
1. Log on to your Windows device as the same user as when installing.
2. Stop the server. Select **AT-Vista Manager EX** and then **AT-Vista Manager EX - Stop Server** from the Windows menu.
3. From the Windows menu, select **AT-Vista Manager EX** then **AT-Vista Manager EX - Uninstall**.
4. The AT-Vista Manager EX uninstaller starts.
5. Click the **Uninstall** button to uninstall.
6. If a dialogue box prompting you to restart the system is displayed, select **Restart the system** or **Restart later** and click the **Finish** button.
7. Delete the installation folder. The default installation folder is:  
**C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX**
8. Reboot the system.

## Install the new version

1. From your Windows device, execute the Vista Manager EX installation program 'atvmexXXXbXXw.exe'.

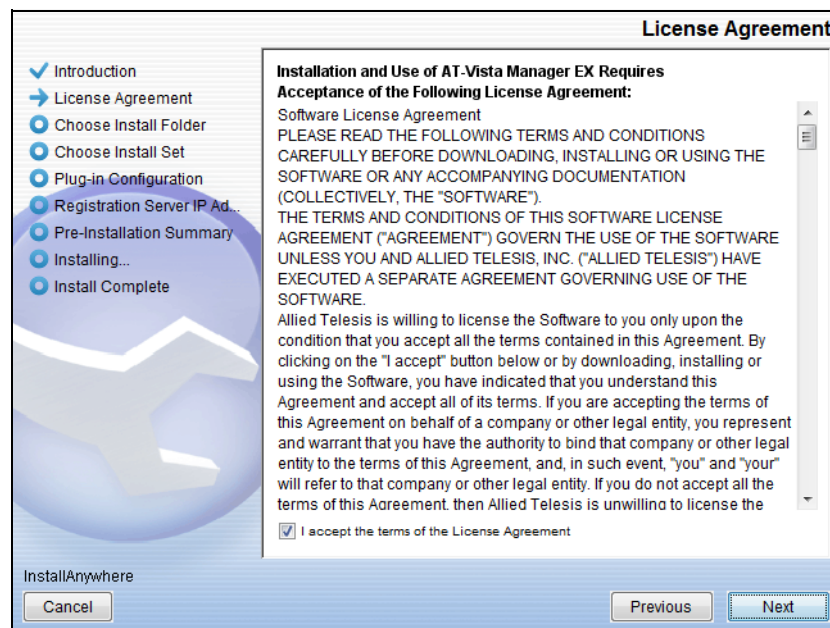
**Note:** You must have administrator privileges to run the installer.

2. The **Introduction** dialog displays:



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

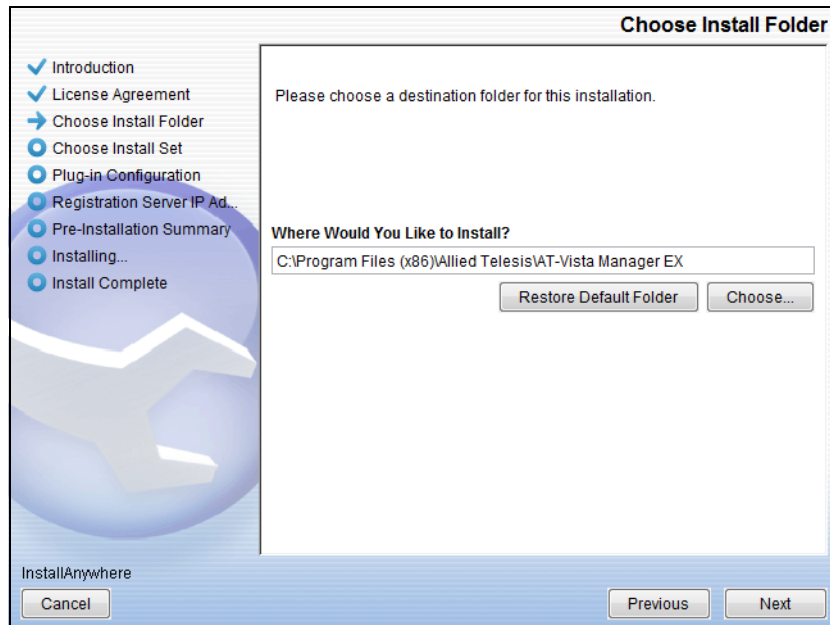
3. The **License Agreement** dialog displays:



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

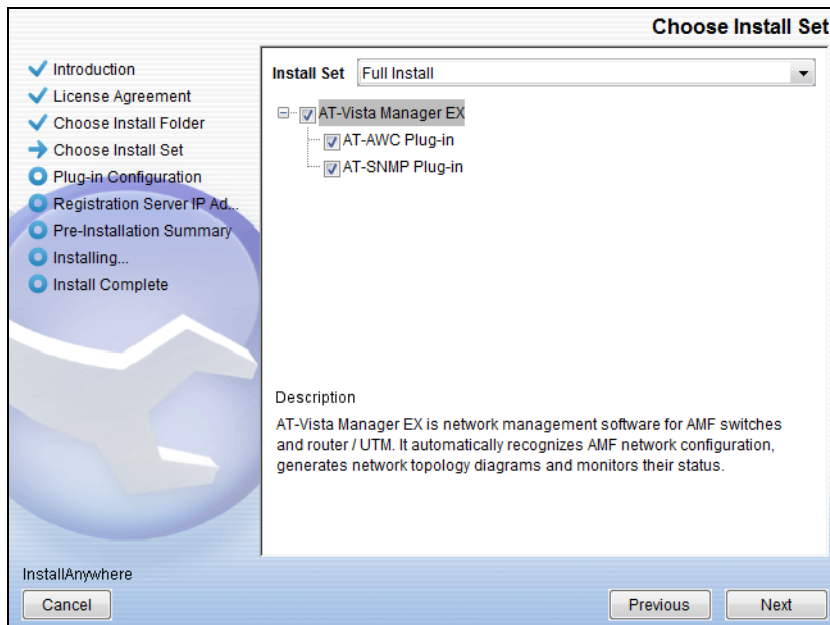
- Click **I accept the terms of the License Agreement**
- Click **Next**

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



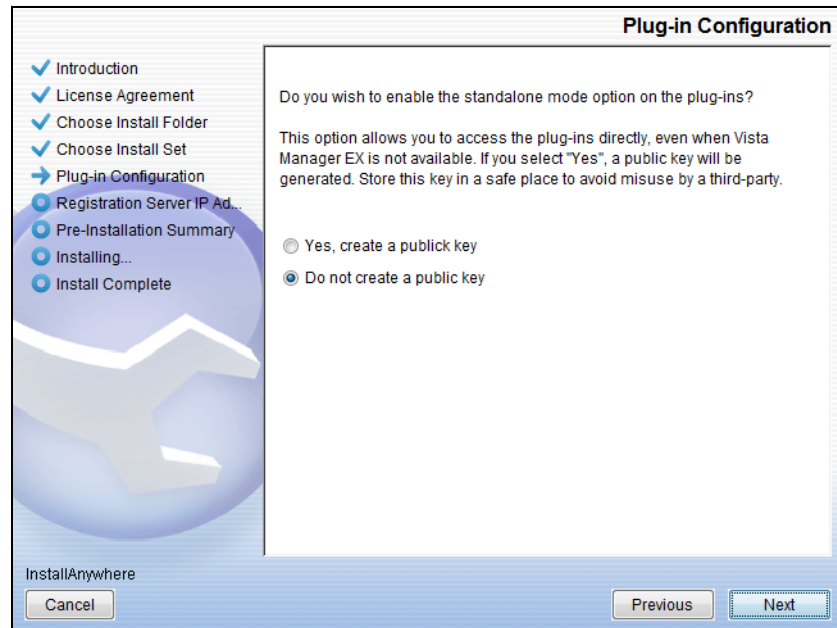
Select a destination location and click **Next**.

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



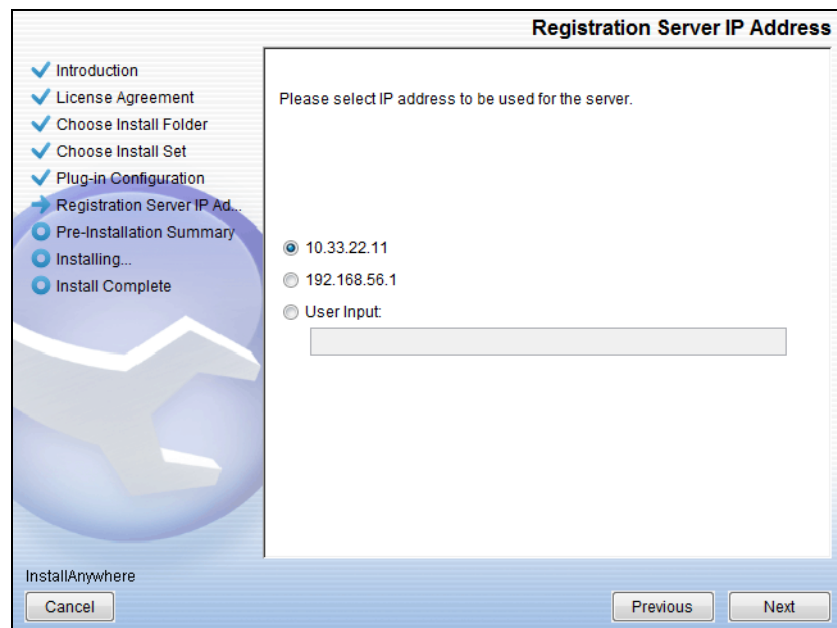
Select **Full Install** from the drop down list. By default all plug-ins are selected. Clear the check box for any plug-ins you do not wish to install. Click **Next**.

6. The **Plug-In Configuration** dialog displays:



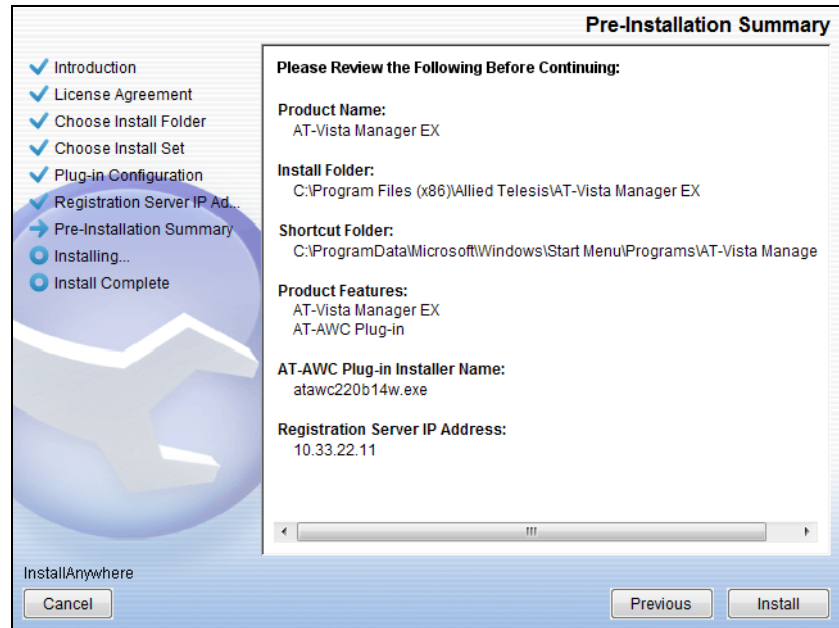
Select **Do not create a public key** unless you are intending to use the plug-ins in standalone mode. For more information on standalone mode, refer to the Installation Guide. Click **Next**.

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



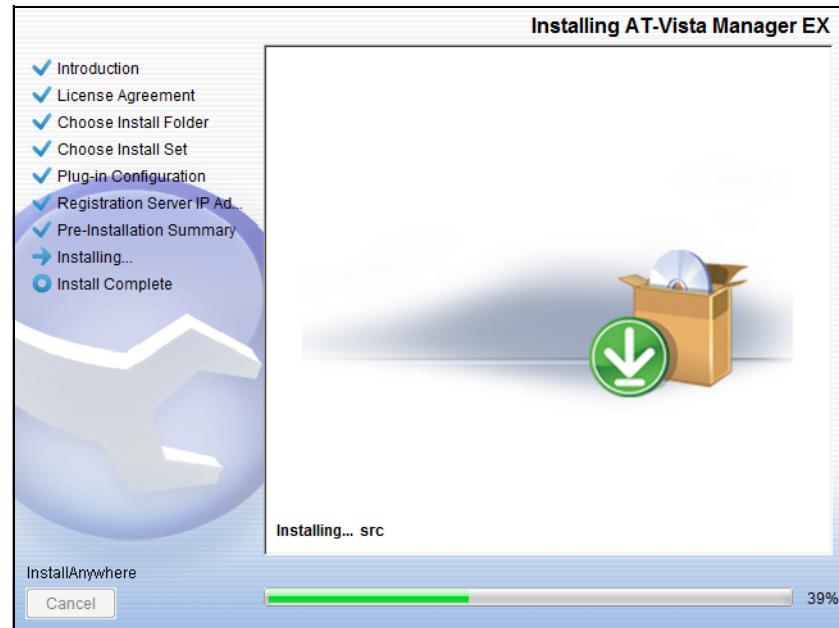
Either select from the list of IP addresses already configured on the Windows machine, or input a valid IP address. Click **Next**.

8. The **Pre-Installation Summary** dialog displays:

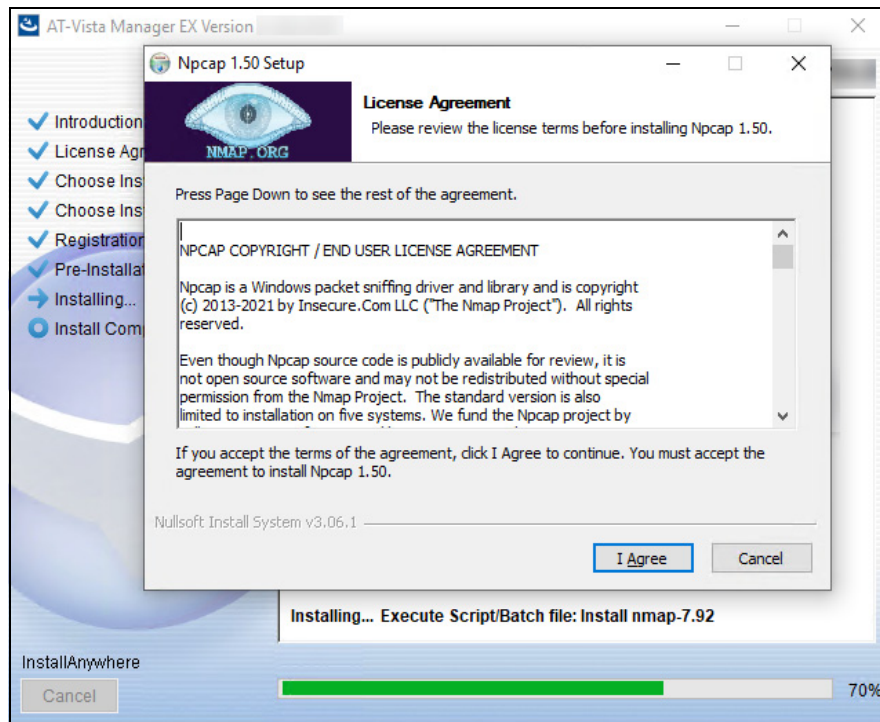


Check that your Product Name, Install Folder, Shortcut Folder, Product Features, Plug-in Installer Name and Registration IP Address are correct, and then click **Install**.

9. The **Installing...** dialog displays:

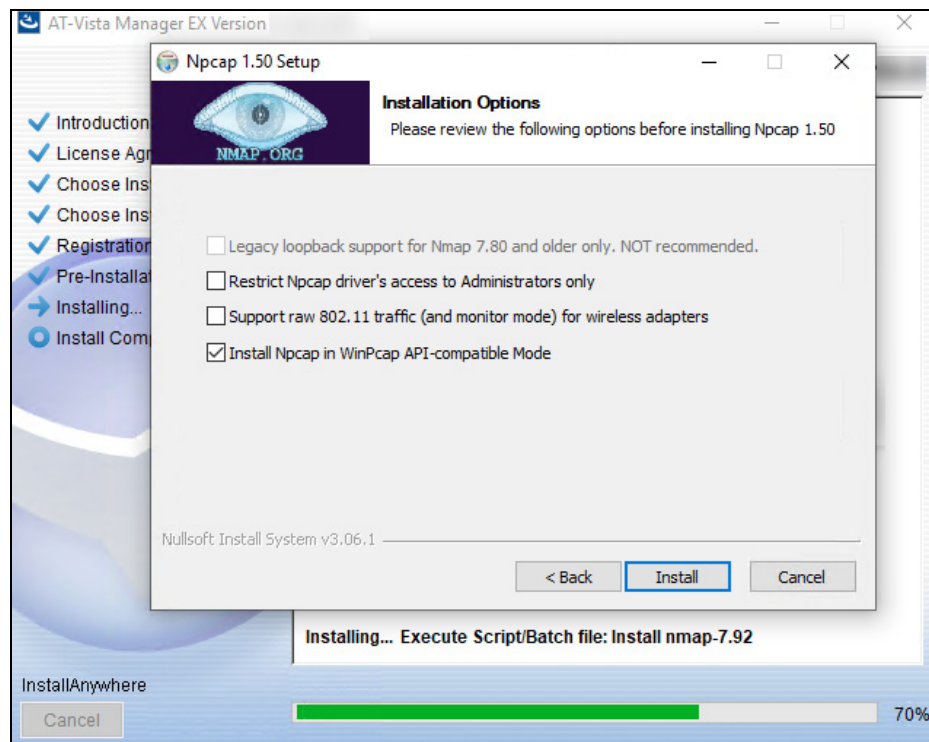


10. The NPCAP installer dialog appears.

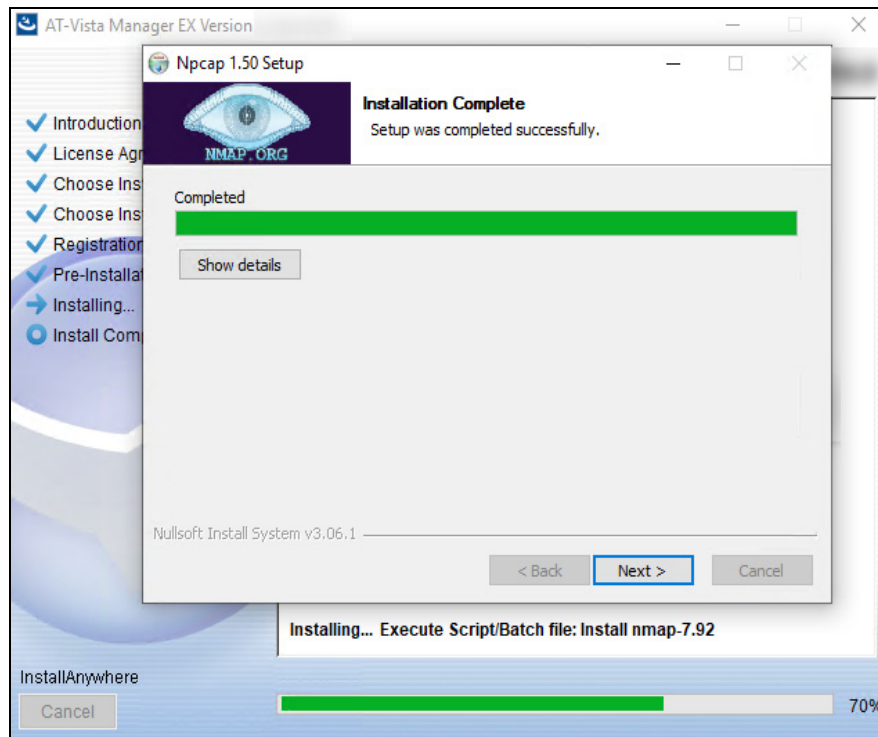


Click **I Agree** to proceed with the install.

11. Click **Install**.

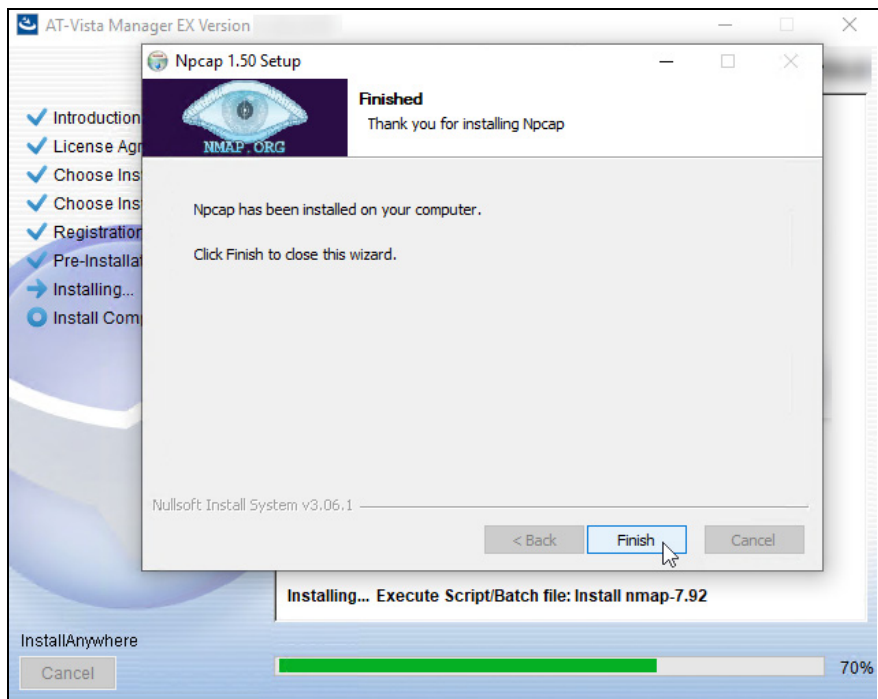


12. The Npcap install will install.



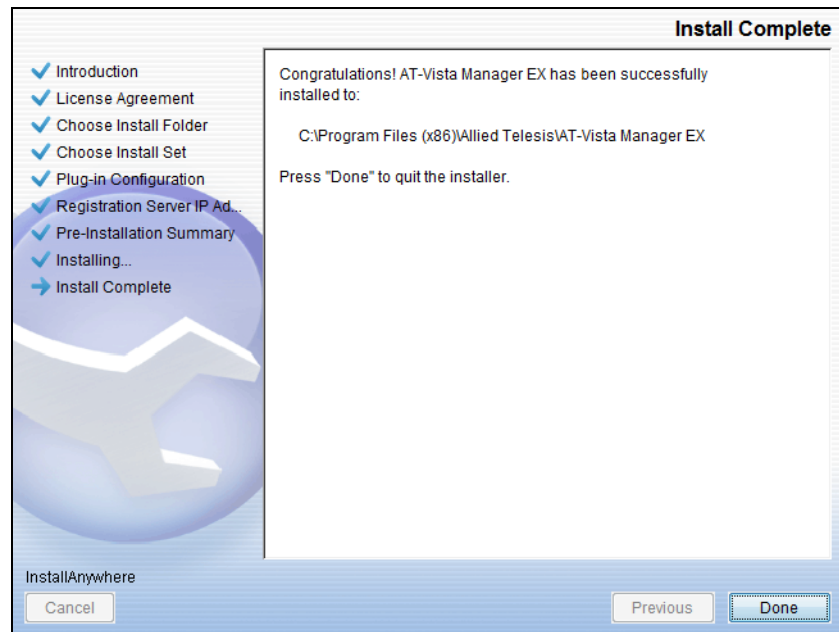
Click **Next**.

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



Vista Manager will resume the rest of the download.

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



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

### Restore the Vista Manager database

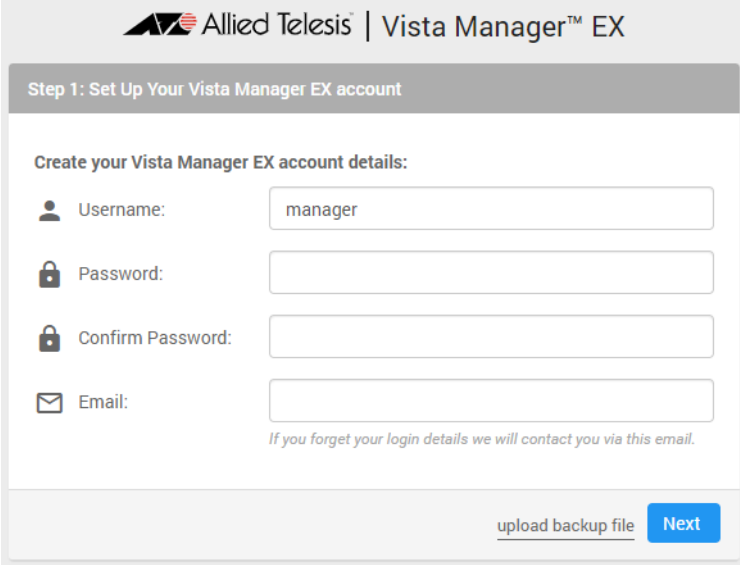
After the upgrade is complete, you need to restore the Vista Manager database. To do this, use the following procedure.

1. Login to Vista Manager.

The image shows a web browser window displaying the "Vista Manager EX Login" page. The page header includes the Allied Telesis logo and the text "Vista Manager™ EX". The main content area is titled "Vista Manager EX Login" and contains two input fields: "Username:" and "Password:". Below the password field, there is a checkbox labeled "Remember me" and a blue "Login" button.

Enter the **Username** manager and the **Password** friend. Click Login.

2. Click on upload backup file.

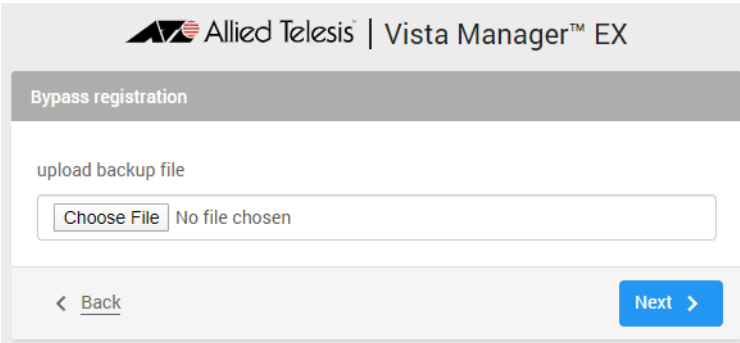


**Caution** Your serial number and license information are part of your database backup. If you upload the backup file when upgrading, you will keep the same serial number, and your licensing will continue to work without interruption.

However, if you configure a new instance of Vista Manager EX, without uploading your backup, a new serial number will be generated, and your existing licensing will no longer work. You will need to contact Allied Telesis support to generate a new license.

Therefore, it is **STRONGLY** recommended that you upload your database backup to ensure your licensing keeps working.

3. Select the database backup to upload. Click on Choose File, and browse to your Vista Manager database backup. Click Next. The Vista Manager database will be restored.



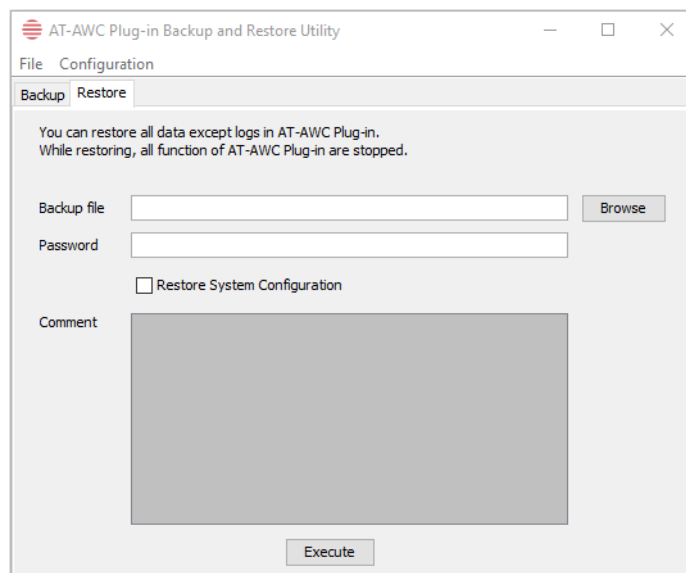
## Restore the SNMP plug-in

4. If you have the SNMP plug-in installed then log on locally to the Vista Manager EX server.
5. Stop the SNMP server services using the shortcut or by running the following command line.  
**"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\svrcmd.bat" svrstop**
6. Run the restore utility by using the shortcut or by running the following command line.  
**"<Vista Install Path>\Plugins\AT-SNMP\NetManager\bin\SMRestore.exe"**  
Follow the instructions on the screen.

## Restore the AWC plug-in

7. If you have the AWC plug-in installed then log on locally to the Vista Manager EX server.
8. Stop the AWC server services using the shortcut or by running the following command line.  
**"<Vista Install Path>\Plugins\AT-AWC\root\stopserver.bat"**
9. Run the backup/restore utility by using the shortcut or running the following command line.  
**"<Vista Install Path>\Plugins\AT-AWC\tools\maintenance\maintenance.bat"**
10. Select the restore tab on the dialog and follow the instructions on the screen.

**Note:** By default, restoring the AWC database will not restore the system configuration. You can restore the system configuration by checking the Restore System Configuration checkbox in the backup/restore utility.



We recommend that you check the Restore System Configuration checkbox, as it will allow you to restore the following system configuration settings:

- Database Settings
  - « Maximum Memory Usage
- Data Retention Period Settings
  - « Associated Client History

- 
- « Client Location Estimation History
  - « IDS Report History
  - Network Map Settings
    - « Wireless Client Update-Interval
  - Client Location Estimation History data

The system configuration contains settings that are tailored to the machine that created the backup. If you are restoring the backup on a different machine, particularly if that machine has a lower specification, it is recommended not to restore the system configuration.

**Note:** The default location of <Vista Install Path> is **C:\Program Files (x86)\Allied Telesis\AT-Vista Manager EX**

# Upgrading Vista Manager on VST-APL

See the [Vista Manager Network Appliance \(VST-APL\) Release Note](#).

# Upgrading Vista Manager on VST-VRT

See the [Vista Manager Virtual \(VST-VRT\) Release Note](#).

# Troubleshooting

See the Troubleshooting chapter in the [Vista Manager EX User Guide](#).