Allied Telesis™

Release Note for Vista Manager EX Software Version 3.15.x

VISTA MANAGER™ EX

» 3.15.0

Acknowledgments

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/**

Content

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:

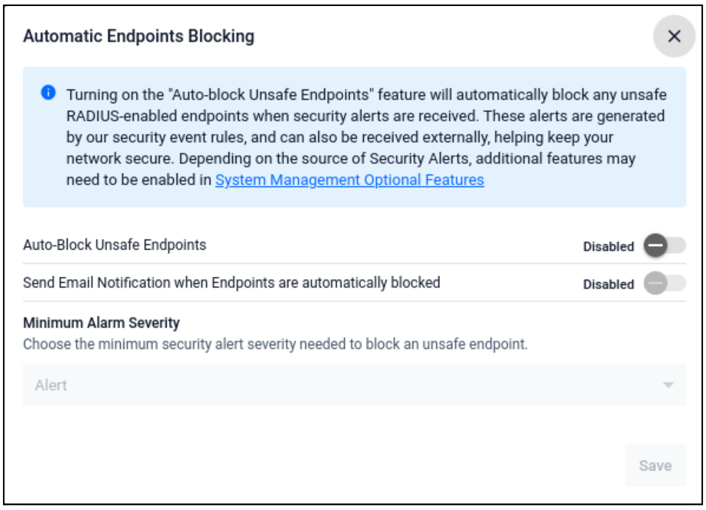
- “Support for SMTP OAuth Configuration” on page 6.
- “Using Experimental Features from Vista Labs” on page 15.
- “Vista Labs feature: Allie” on page 16.
- “Two-Factor Authentication support for login” on page 18.
- “Updates to link labels and bandwidth” on page 19.
- “Further Vista Manager EX API Support” on page 20.
- “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**.



Automatic Endpoints Blocking

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

Auto-Block Unsafe Endpoints: Disabled

Send Email Notification when Endpoints are automatically blocked: Disabled

Minimum Alarm Severity

Choose the minimum security alert severity needed to block an unsafe endpoint.

Alert

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.

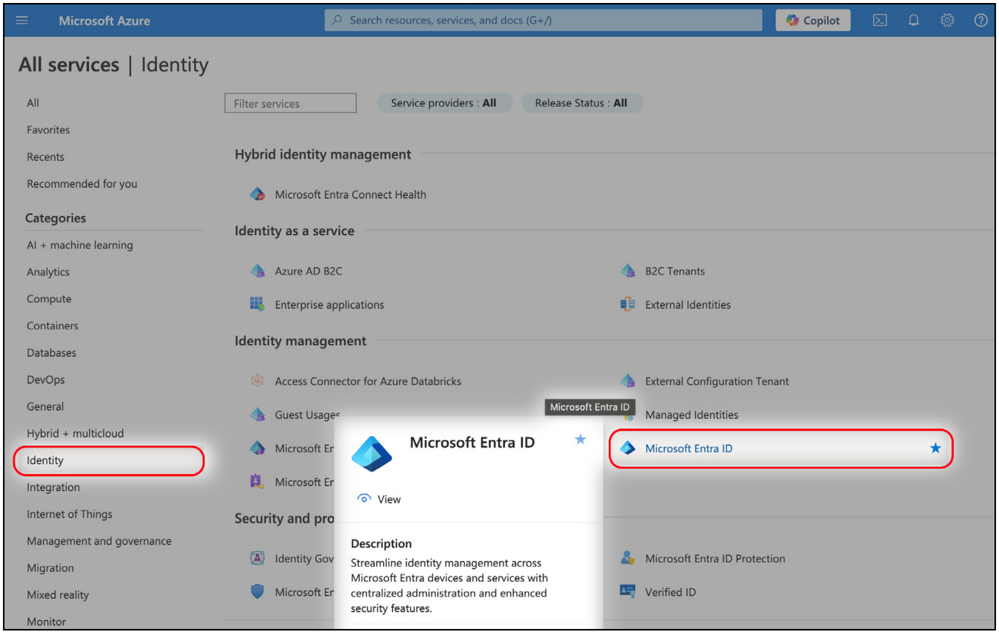
1. **Access the Azure Portal**

   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**.

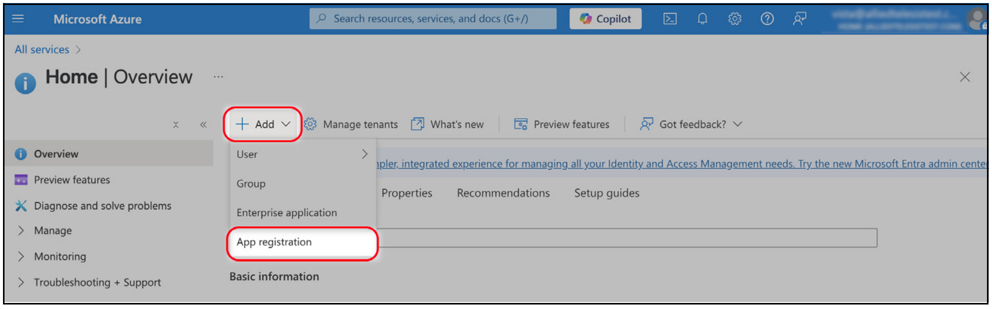
   - Alternatively search for Microsoft Entra ID and move to step 3.



Streamline identity management across Microsoft Entra devices and services with centralized administration and enhanced security features.

3. **Register a New Application**

   - Click **Add** > **App Registration**
   - Select **Single Page Application.**



...pler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin cente

4. Register an Application in Azure

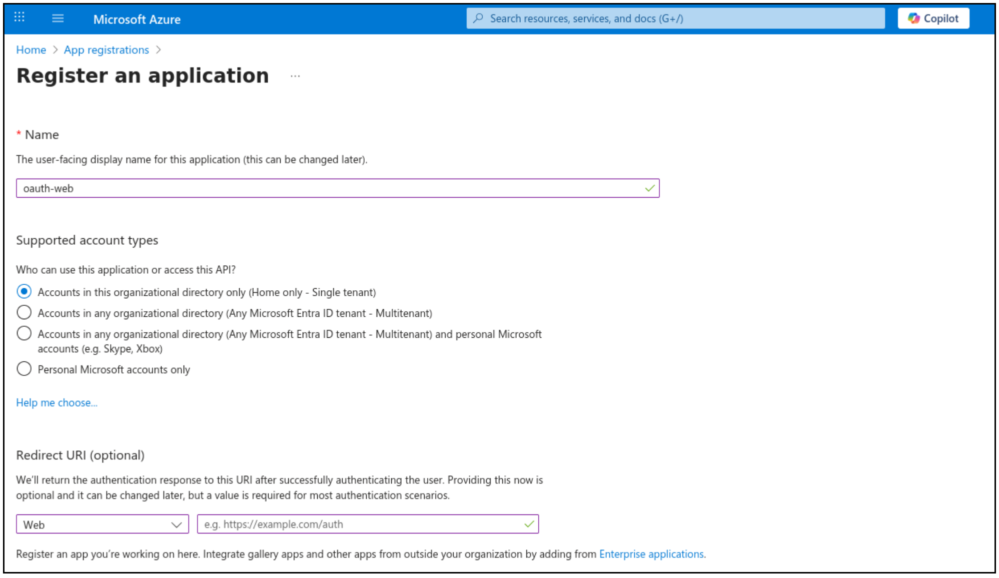
Fill out the Application registration form with the required details:

- 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.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

oauth-web ✓

Supported account types

Who can use this application or access this API?

● 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 only

Help me choose...

Redirect URI (optional)

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.

Web | e.g. https://example.com/auth ✓

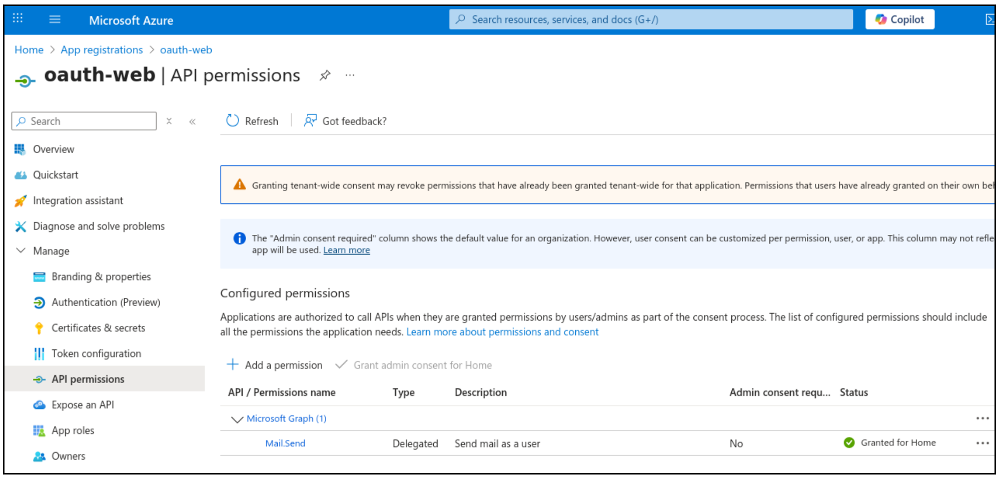
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

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**



Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own bel

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not refle app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

＋ Add a permission ✓ Grant admin consent for Home

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
Mail.Send	Delegated	Send mail as a user	No	✓ Granted for Home

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

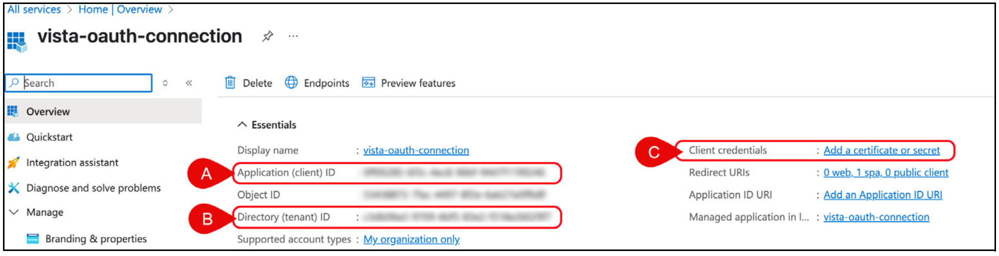
6. Complete Registration and Collect IDs from the Application Overview page

a. Copy the Client ID

b. Copy the Tenant ID

c. Click the 'Client Credentials' link and create a new Client Secret

- Copy the Client Secret



Display name : vista-oauth-connection

Application (client) ID : [redacted]

Object ID : [redacted]

Directory (tenant) ID : [redacted]

Supported account types : My organization only

Client credentials : Add a certificate or secret

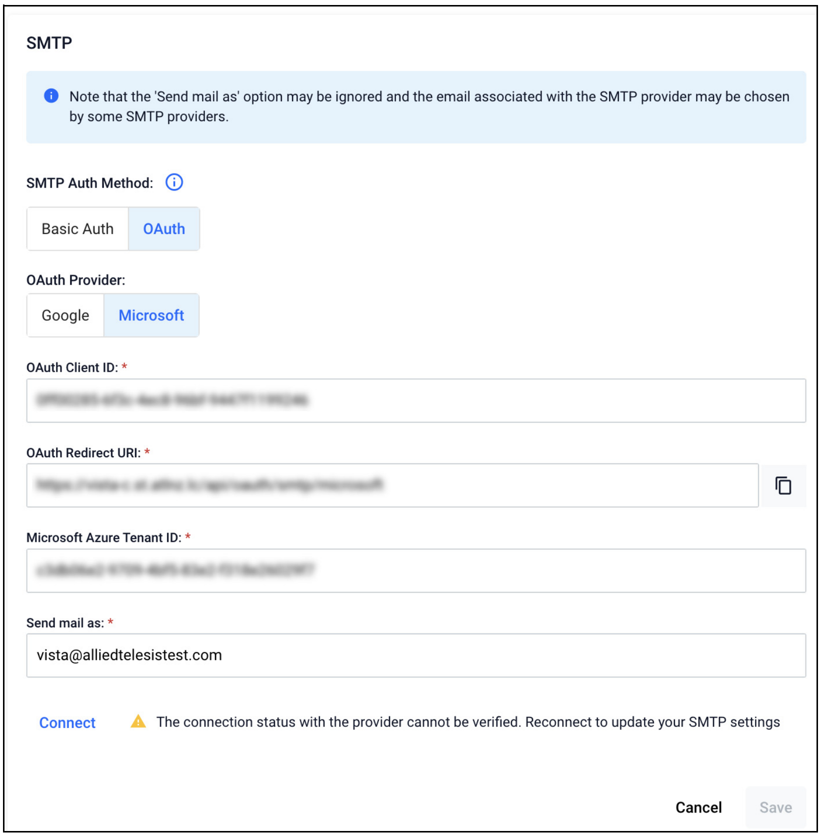
Redirect URIs : 0 web, 1 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in l... : vista-oauth-connection

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



SMTP

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.

SMTP Auth Method: Basic Auth [✓ OAuth]

OAuth Provider: Google [✓ Microsoft]

OAuth Client ID: * [redacted]

OAuth Redirect URI: * [redacted]

Microsoft Azure Tenant ID: * [redacted]

Send mail as: * vista@alliedtelesistest.com

Connect ⚠ The connection status with the provider cannot be verified. Reconnect to update your SMTP settings

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:

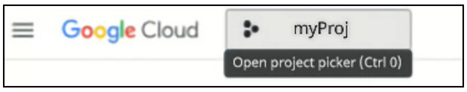
- a Google Workspace account
- access to the Google Cloud Platform

1. **Access the Google Cloud platform**

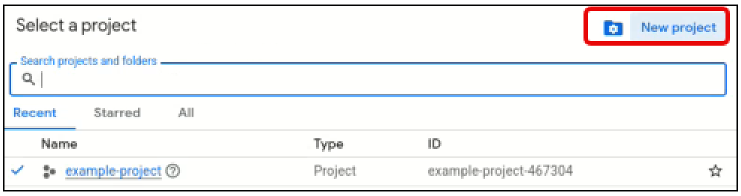
   Navigate to https://console.cloud.google.com/ and log in using your Google account credentials.

2. **Create a new OAuth project**

   - Click on the Project button in the top navigation bar

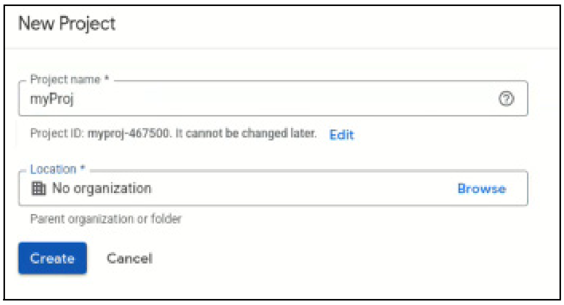


   - Select **New Project**



Name	Type	ID
✓ example-project	Project	example-project-467304

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



Project name *: myProj

Project ID: myproj-467500. It cannot be changed later. Edit

Location *: No organization

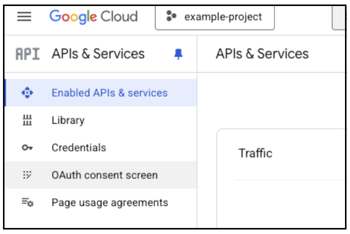
Parent organization or folder

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**

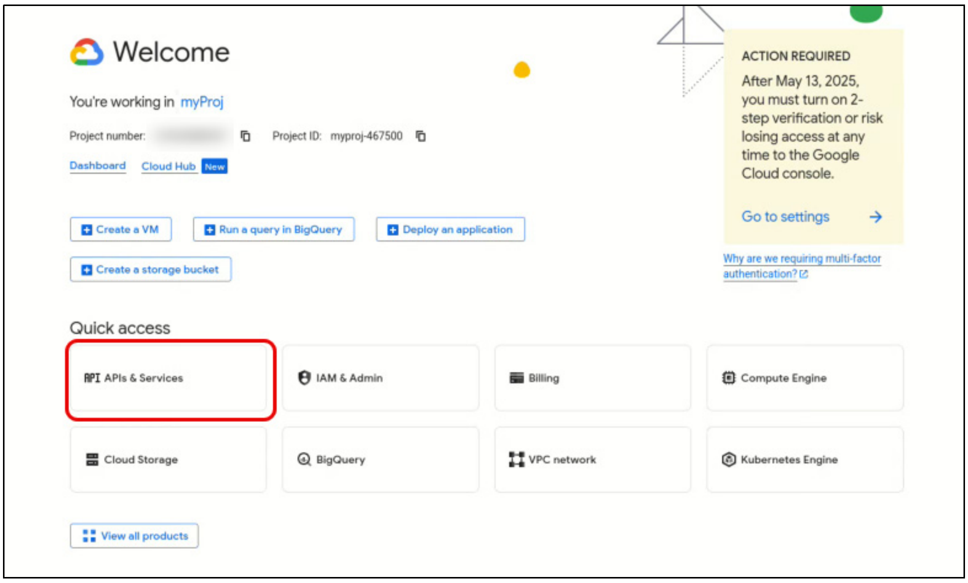
   - In the left menu, select OAuth consent screen.



   - 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



Welcome

You're working in myProj

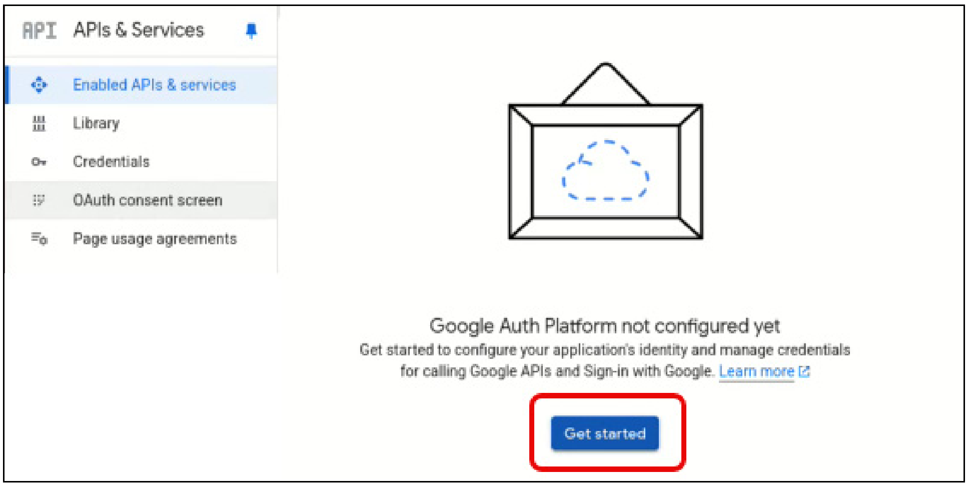
Project number: [redacted] Project ID: myproj-467500

ACTION REQUIRED

After May 13, 2025, you must turn on 2-step verification or risk losing access at any time to the Google Cloud console.

Why are we requiring multi-factor authentication?

- Click Get Started



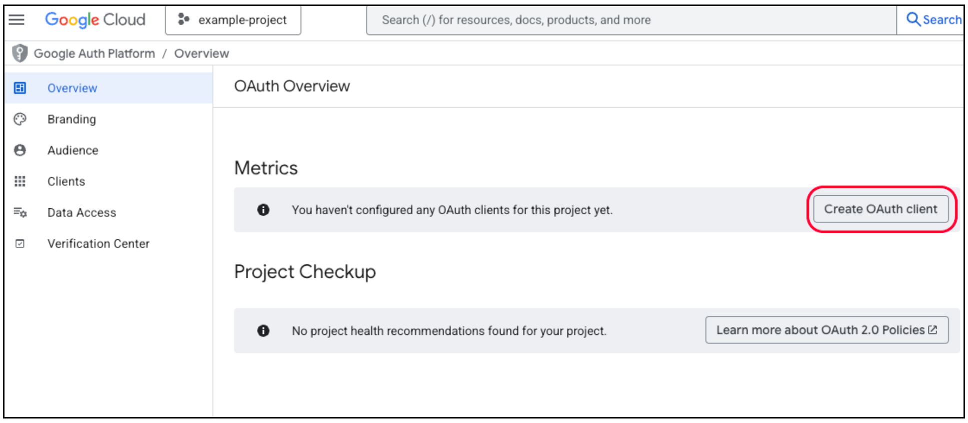
Google Auth Platform not configured yet

Get started to configure your application's identity and manage credentials for calling Google APIs and Sign-in with Google. Learn more

- 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

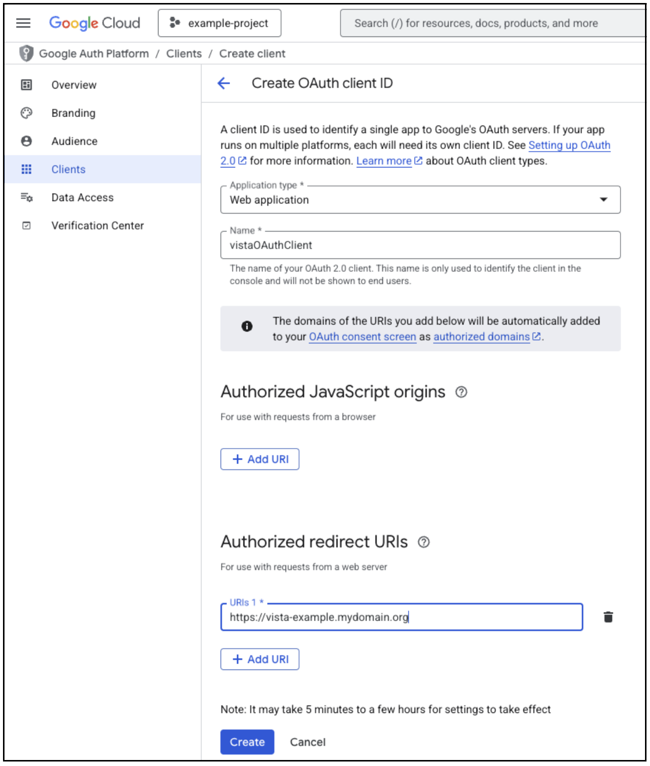
- From the OAuth Overview page, click **Create OAuth Client**



You haven't configured any OAuth clients for this project yet.

No project health recommendations found for your project.

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



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.

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

Authorized redirect URIs

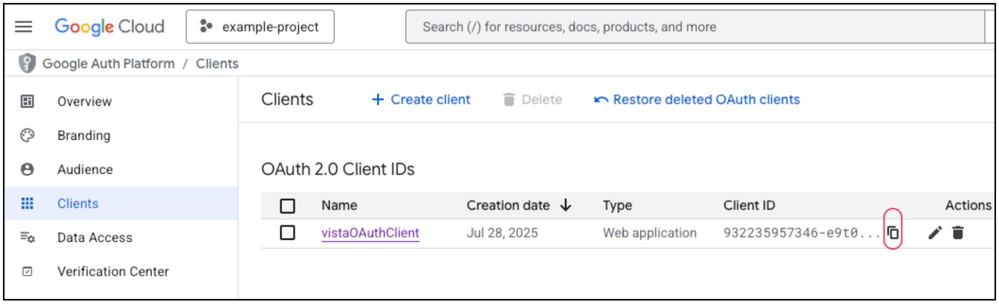
For use with requests from a web server

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

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

- Click **Create**

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

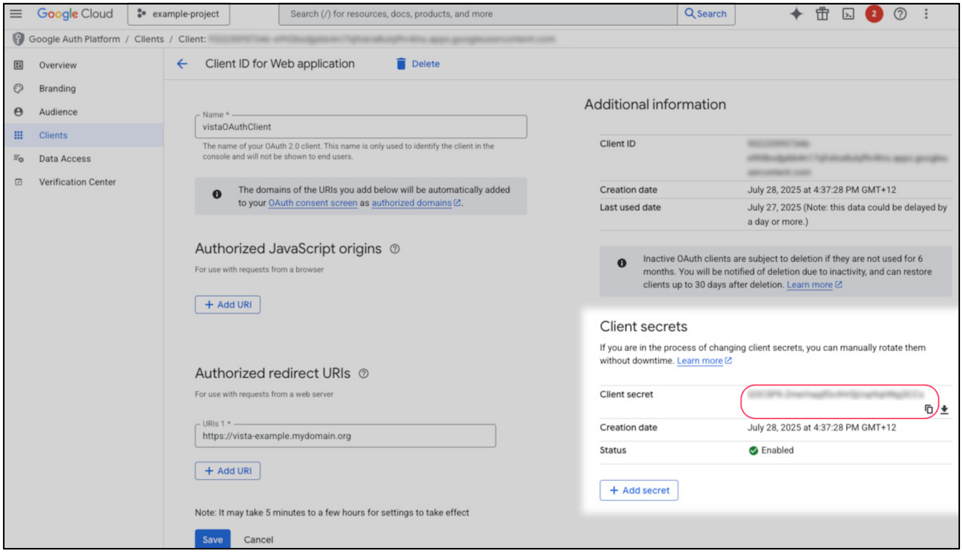


OAuth 2.0 Client IDs

□	Name	Creation date ↓	Type	Client ID	Actions
□	vistaOAuthClient	Jul 28, 2025	Web application	932235957346-e9t0...	

- 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.



Google Auth Platform / Clients / Client: [redacted]

Client ID for 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.

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

Authorized redirect URIs

For use with requests from a web server

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

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

Additional information

Client ID	[redacted]
Creation date	July 28, 2025 at 4:37:28 PM GMT+12
Last used date	July 27, 2025 (Note: this data could be delayed by a day or more.)

Inactive OAuth clients are subject to deletion if they are not used for 6 months. You will be notified of deletion due to inactivity, and can restore clients up to 30 days after deletion. Learn more

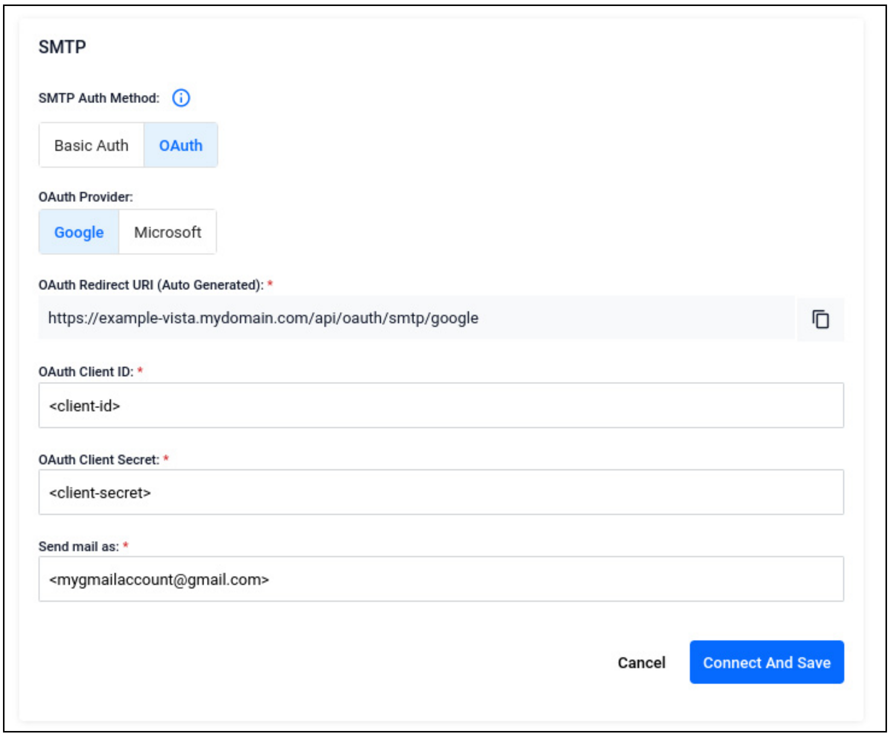
Client secrets

If you are in the process of changing client secrets, you can manually rotate them without downtime. Learn more

Client secret	[redacted]
Creation date	July 28, 2025 at 4:37:28 PM GMT+12
Status	Enabled

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



SMTP

SMTP Auth Method: OAuth

OAuth Provider: Google

OAuth Redirect URI (Auto Generated): * https://example-vista.mydomain.com/api/oauth/smtp/google

OAuth Client ID: * <client-id>

OAuth Client Secret: * <client-secret>

Send mail as: * <mygmailaccount@gmail.com>

- 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

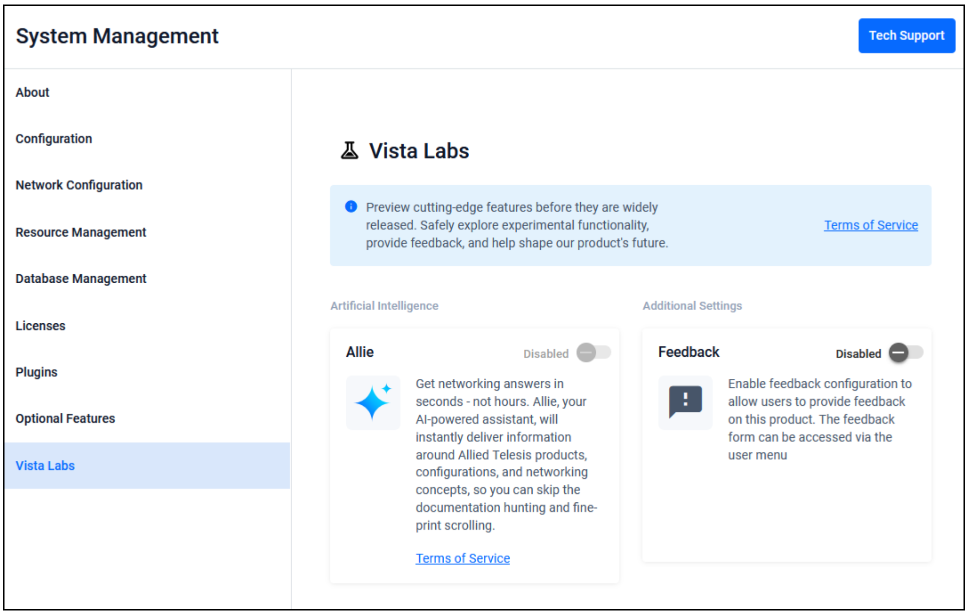
Applies to all Vista Manager EX installations

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.



Preview cutting-edge features before they are widely released. Safely explore experimental functionality, provide feedback, and help shape our product's future.

Get networking answers in seconds - not hours. Allie, your AI-powered assistant, will instantly deliver information around Allied Telesis products, configurations, and networking concepts, so you can skip the documentation hunting and fine-print scrolling.

Enable feedback configuration to allow users to provide feedback on this product. The feedback form can be accessed via the user menu

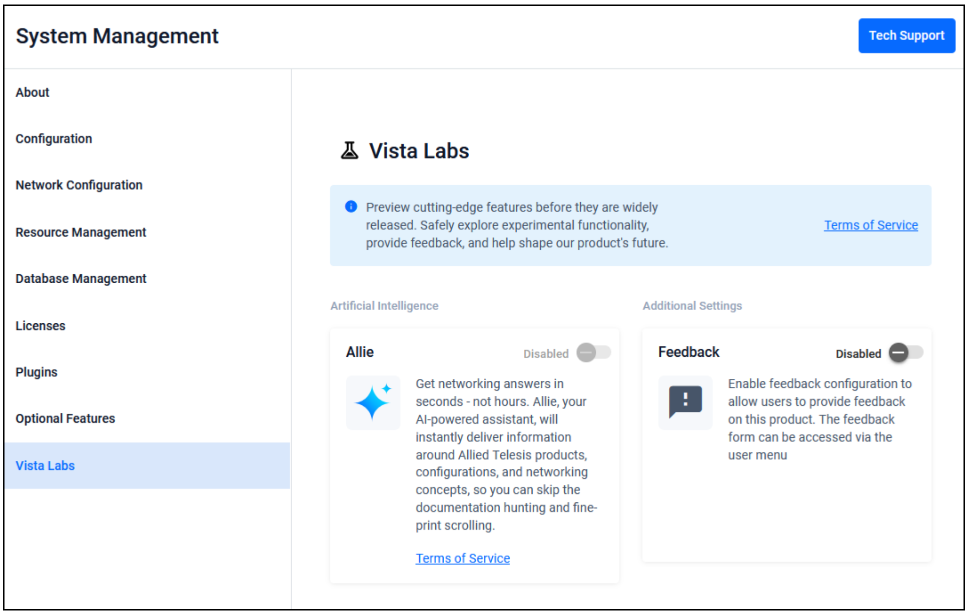
Toggle feedback to allow all users to provide feedback on Vista Manager. After toggling this, you can access the Feedback form from the User Management menu.

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.



System Management

Tech Support

About

Configuration

Network Configuration

Resource Management

Database Management

Licenses

Plugins

Optional Features

Vista Labs

Vista Labs

Preview cutting-edge features before they are widely released. Safely explore experimental functionality, provide feedback, and help shape our product's future.

Terms of Service

Artificial Intelligence

Allie — Disabled

Get networking answers in seconds - not hours. Allie, your AI-powered assistant, will instantly deliver information around Allied Telesis products, configurations, and networking concepts, so you can skip the documentation hunting and fine-print scrolling.

Terms of Service

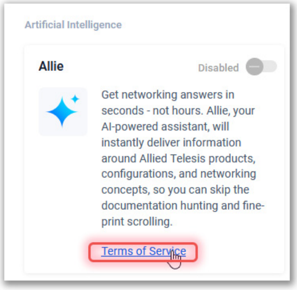
Additional Settings

Feedback — Disabled

Enable feedback configuration to allow users to provide feedback on this product. The feedback form can be accessed via the user menu

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.



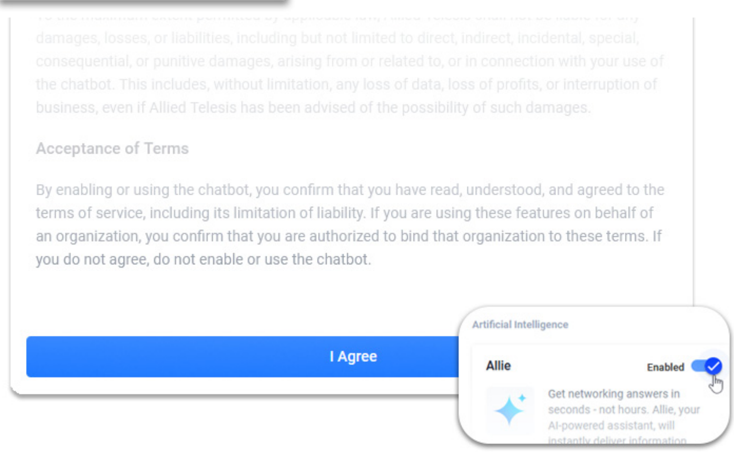
Artificial Intelligence

Allie — Disabled

Get networking answers in seconds - not hours. Allie, your AI-powered assistant, will instantly deliver information around Allied Telesis products, configurations, and networking concepts, so you can skip the documentation hunting and fine-print scrolling.

Terms of Service

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



damages, losses, or liabilities, including but not limited to direct, indirect, incidental, special, consequential, or punitive damages, arising from or related to, or in connection with your use of the chatbot. This includes, without limitation, any loss of data, loss of profits, or interruption of business, even if Allied Telesis has been advised of the possibility of such damages.

Acceptance of Terms

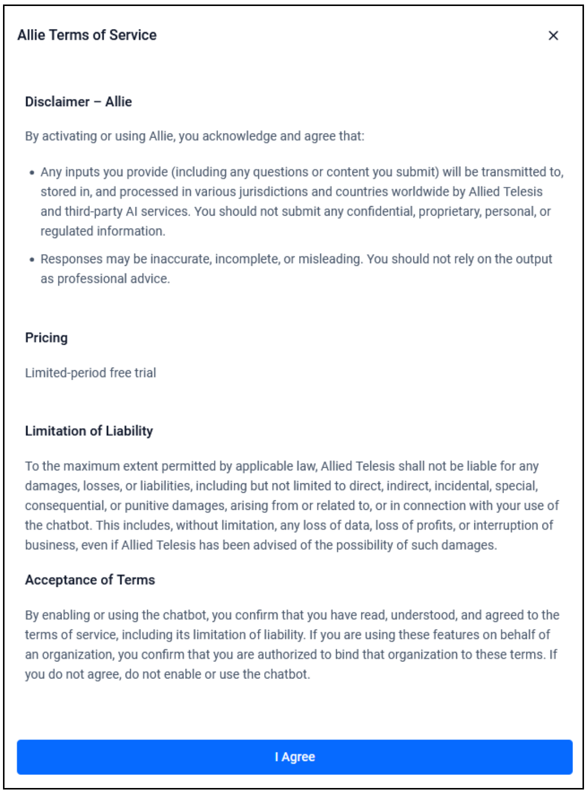
By enabling or using the chatbot, you confirm that you have read, understood, and agreed to the terms of service, including its limitation of liability. If you are using these features on behalf of an organization, you confirm that you are authorized to bind that organization to these terms. If you do not agree, do not enable or use the chatbot.

I Agree

Artificial Intelligence

Allie — Enabled

Get networking answers in seconds - not hours. Allie, your AI-powered assistant, will instantly deliver information



Allie Terms of Service ✕

Disclaimer – Allie

By activating or using Allie, you acknowledge and agree that:

- Any inputs you provide (including any questions or content you submit) will be transmitted to, stored in, and processed in various jurisdictions and countries worldwide by Allied Telesis and third-party AI services. You should not submit any confidential, proprietary, personal, or regulated information.
- Responses may be inaccurate, incomplete, or misleading. You should not rely on the output as professional advice.

Pricing

Limited-period free trial

Limitation of Liability

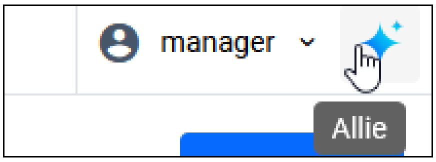
To the maximum extent permitted by applicable law, Allied Telesis shall not be liable for any damages, losses, or liabilities, including but not limited to direct, indirect, incidental, special, consequential, or punitive damages, arising from or related to, or in connection with your use of the chatbot. This includes, without limitation, any loss of data, loss of profits, or interruption of business, even if Allied Telesis has been advised of the possibility of such damages.

Acceptance of Terms

By enabling or using the chatbot, you confirm that you have read, understood, and agreed to the terms of service, including its limitation of liability. If you are using these features on behalf of an organization, you confirm that you are authorized to bind that organization to these terms. If you do not agree, do not enable or use the chatbot.

I Agree

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.

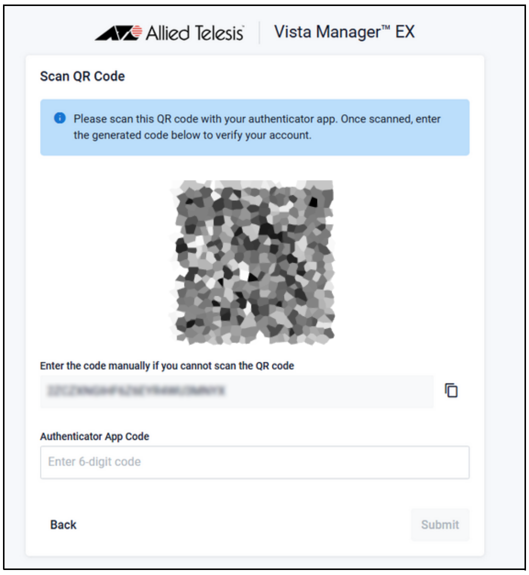
As an Admin user, you can enable 2FA for your own account, other admin accounts, or general users.

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).



Scan QR Code

Please scan this QR code with your authenticator app. Once scanned, enter the generated code below to verify your account.

Enter the code manually if you cannot scan the QR code

Authenticator App Code

Enter 6-digit code

- 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.

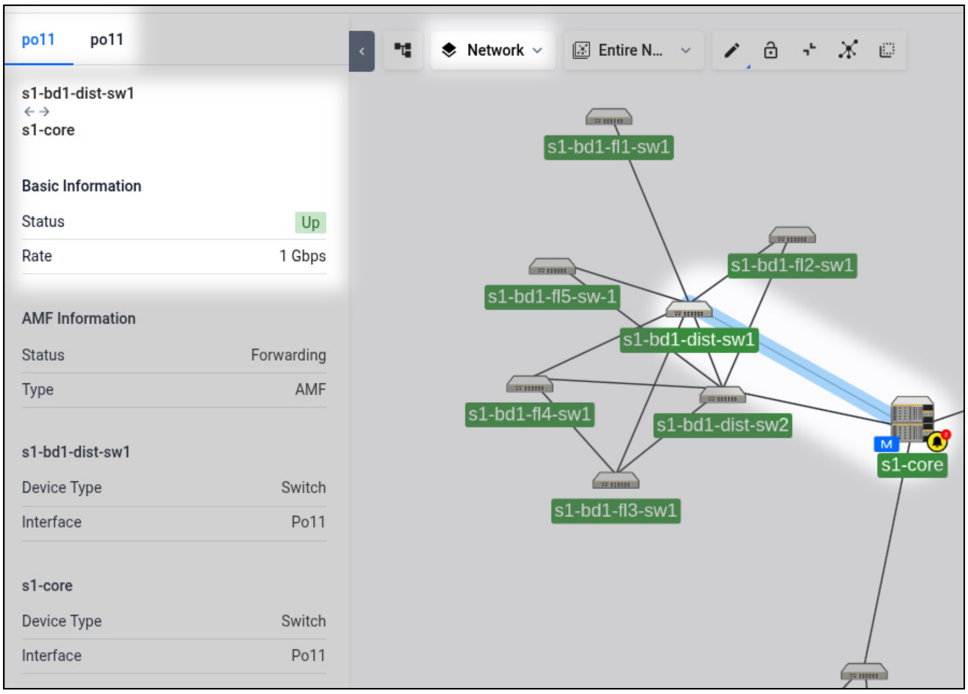
Updates to link labels and bandwidth

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.



po11 po11

s1-bd1-dist-sw1
↔
s1-core

Basic Information

Status	Up
Rate	1 Gbps

AMF Information

Status	Forwarding
Type	AMF

s1-bd1-dist-sw1

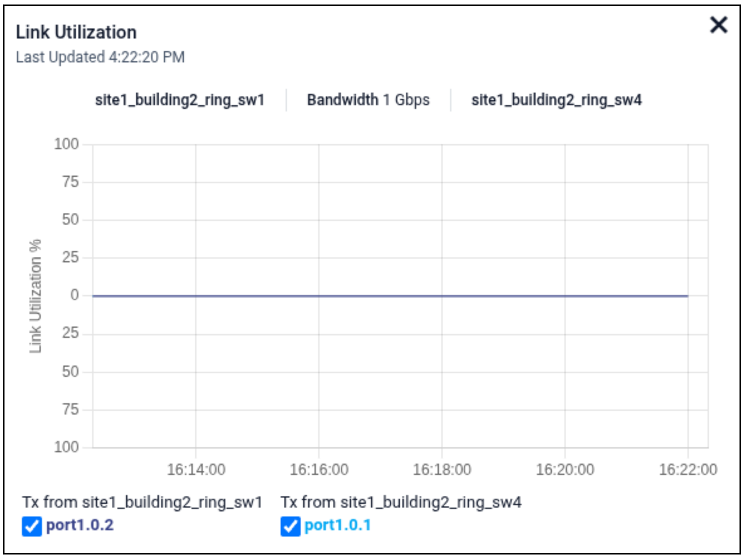
Device Type	Switch
Interface	Po11

s1-core

Device Type	Switch
Interface	Po11

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).



Link Utilization
Last Updated 4:22:20 PM

site1_building2_ring_sw1 | Bandwidth 1 Gbps | site1_building2_ring_sw4

Tx from site1_building2_ring_sw1
☑ port1.0.2

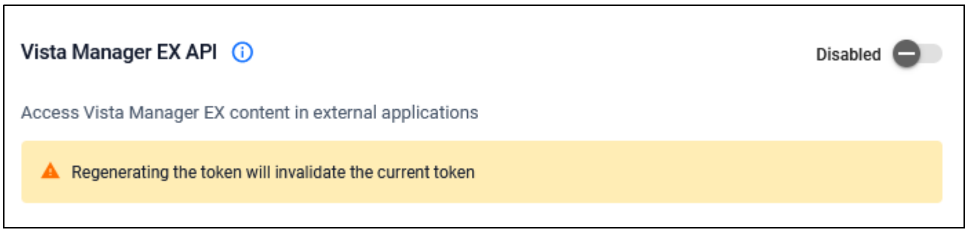
Tx from site1_building2_ring_sw4
☑ port1.0.1

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.



Vista Manager EX API ⓘ

Disabled

Access Vista Manager EX content in external applications

⚠ Regenerating the token will invalidate the current token

Click the ⓘ button to see instructions about how to use the API.

AWC enhancements

Ability to backup client history and logs for VST-VRT

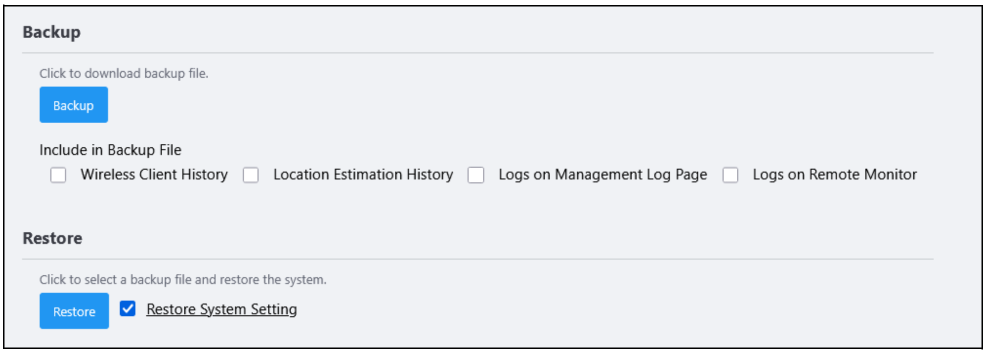
Applies to the AWC Plugin on Vista Manager VST-VRT installations.

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.



Backup

Click to download backup file.

Backup

Include in Backup File

□ Wireless Client History □ Location Estimation History □ Logs on Management Log Page □ Logs on Remote Monitor

Restore

Click to select a backup file and restore the system.

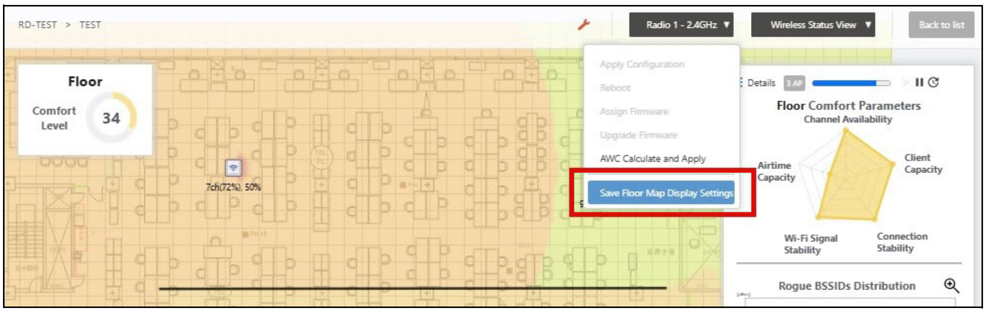
Restore ☑ Restore System Setting

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.

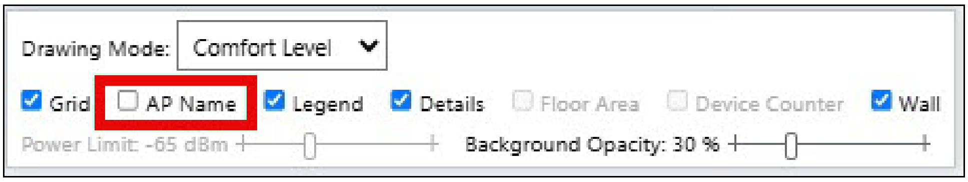


Option to display AP name above icons on floormap

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.



Drawing Mode: Comfort Level

☑ Grid ☐ AP Name ☑ Legend ☑ Details ☐ Floor Area ☐ Device Counter ☑ Wall

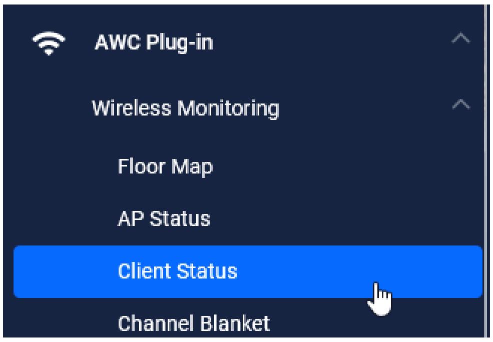
Power Limit: -65 dBm

Background Opacity: 30 %

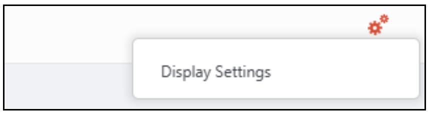
Client AP Status graphs

Applies to the AWC Plugin on Vista Manager EX installations.

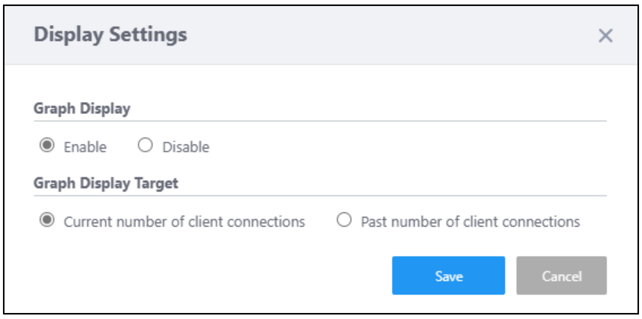
From version 3.15.0 onwards, you can view donut and stacked graphs of the current number of client connections on APs from the Client Status page.



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



Click the Display Settings, and Enable Graph Display.



Display Settings

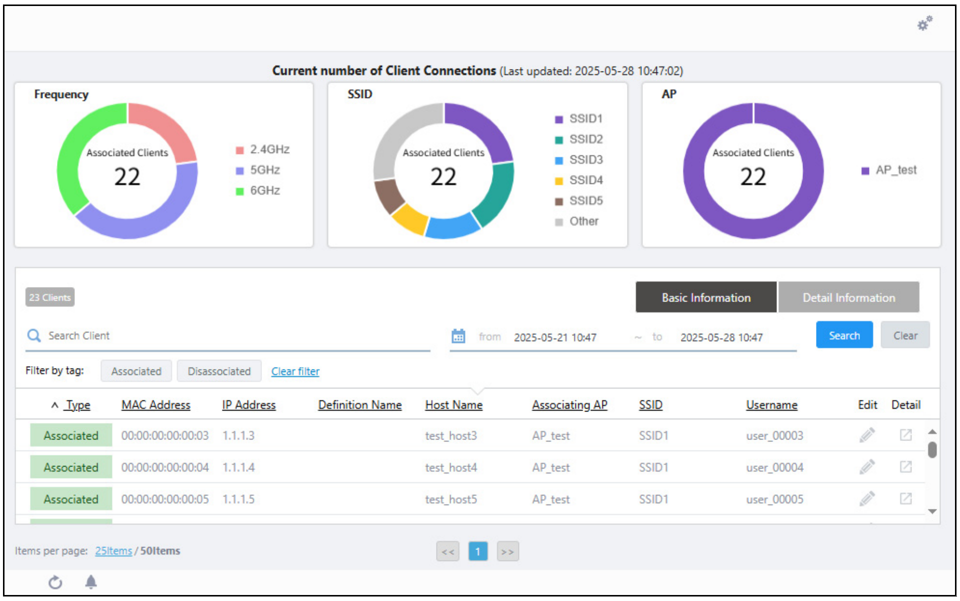
Graph Display

● Enable ○ Disable

Graph Display Target

● Current number of client connections ○ Past number of client connections

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



Current number of Client Connections (Last updated: 2025-05-28 10:47:02)

from 2025-05-21 10:47 ~ to 2025-05-28 10:47

Filter by tag: Associated Disassociated Clear filter

Type	MAC Address	IP Address	Definition Name	Host Name	Associating AP	SSID	Username	Edit	Detail
Associated	00:00:00:00:00:03	1.1.1.3		test_host3	AP_test	SSID1	user_00003	✎	↗
Associated	00:00:00:00:00:04	1.1.1.4		test_host4	AP_test	SSID1	user_00004	✎	↗
Associated	00:00:00:00:00:05	1.1.1.5		test_host5	AP_test	SSID1	user_00005	✎	↗

Items per page: 25Items / **50Items**

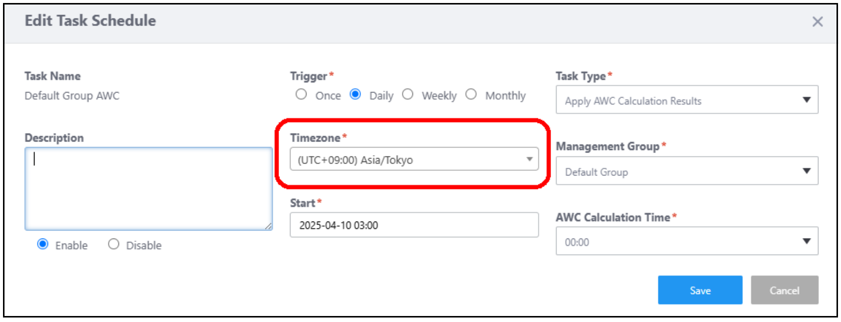
Timezone displayed based on your timezone

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.



Edit Task Schedule

Task Name: Default Group AWC

Trigger*: ○ Once ● Daily ○ Weekly ○ Monthly

Task Type*: Apply AWC Calculation Results

Description:

● Enable ○ Disable

Timezone*: (UTC+09:00) Asia/Tokyo

Start*: 2025-04-10 03:00

Management Group*: Default Group

AWC Calculation Time*: 00:00

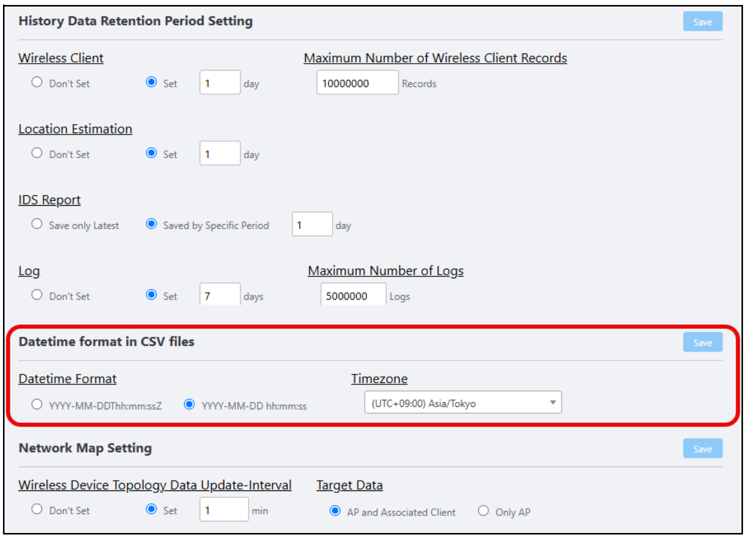
The default timezone is the timezone reported from your device running the AWC application.

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



History Data Retention Period Setting

Wireless Client: ○ Don't Set ● Set 1 day

Maximum Number of Wireless Client Records: 10000000 Records

Location Estimation: ○ Don't Set ● Set 1 day

IDS Report: ○ Save only Latest ● Saved by Specific Period 1 day

Log: ○ Don't Set ● Set 7 days

Maximum Number of Logs: 5000000 Logs

Datetime format in CSV files

Datetime Format: ○ YYYY-MM-DDThh:mm:ssZ ● YYYY-MM-DD hh:mm:ss

Timezone: (UTC+09:00) Asia/Tokyo

Network Map Setting

Wireless Device Topology Data Update-Interval: ○ Don't Set ● Set 1 min

Target Data: ● AP and Associated Client ○ Only AP

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.

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 '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'.

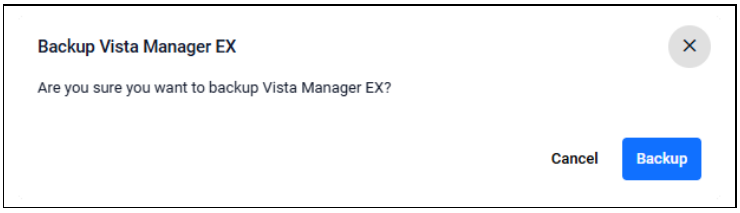
   Do not rename these files. The installation requires them to be in this format.

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.

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.



Backup Vista Manager EX

Are you sure you want to backup Vista Manager EX?

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\svrcmd.bat" 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\SMBackup.exe*"

   Follow the instructions on the screen.

Backup the AWC plug-in

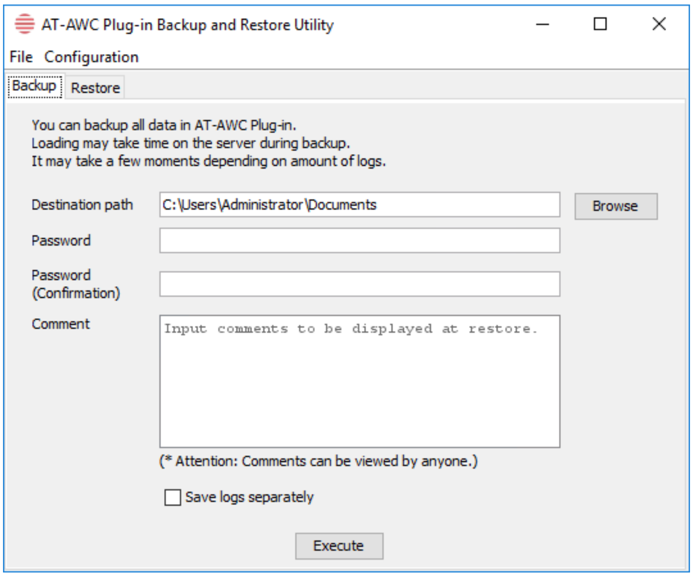
7. If you have the AWC plug-in installed then log on locally to the Vista Manager EX server.

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"



You can backup all data in AT-AWC Plug-in.
Loading may take time on the server during backup.
It may take a few moments depending on amount of logs.

Destination path: C:\Users\Administrator\Documents

Password

Password (Confirmation)

Comment: Input comments to be displayed at restore.

(* Attention: Comments can be viewed by anyone.)

□ Save logs separately

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

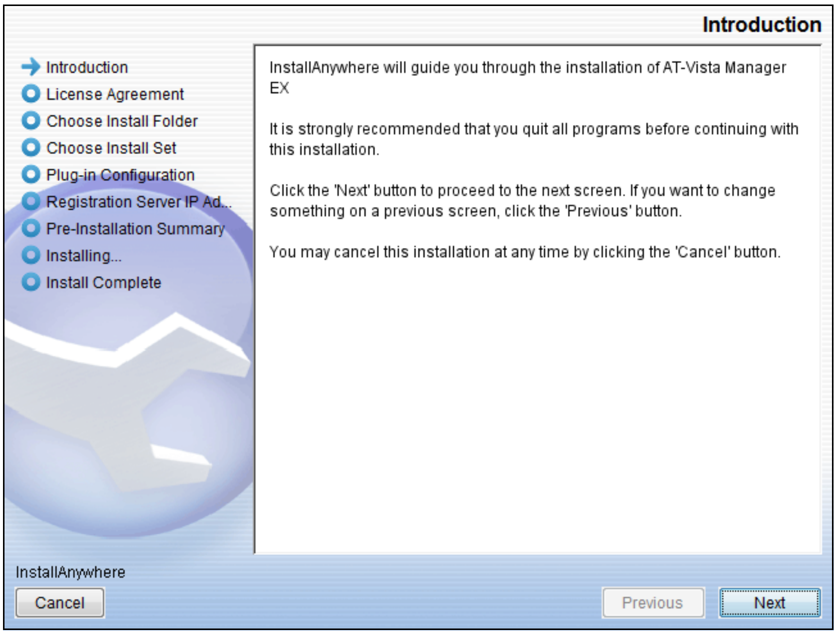
1. Log on to your Windows device as the same user as when installing.
2. Stop the server. Select ***AT-Vista Manager EX*** and then ***AT-Vista Manager EX - Stop Server*** from the Windows menu.
3. From the Windows menu, select ***AT-Vista Manager EX*** then ***AT-Vista Manager EX - Uninstall***.
4. 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 ‘atvmex***XXX***b***XX***w.exe’.

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

2. The ***Introduction*** dialog displays:



InstallAnywhere will guide you through the installation of AT-Vista Manager EX

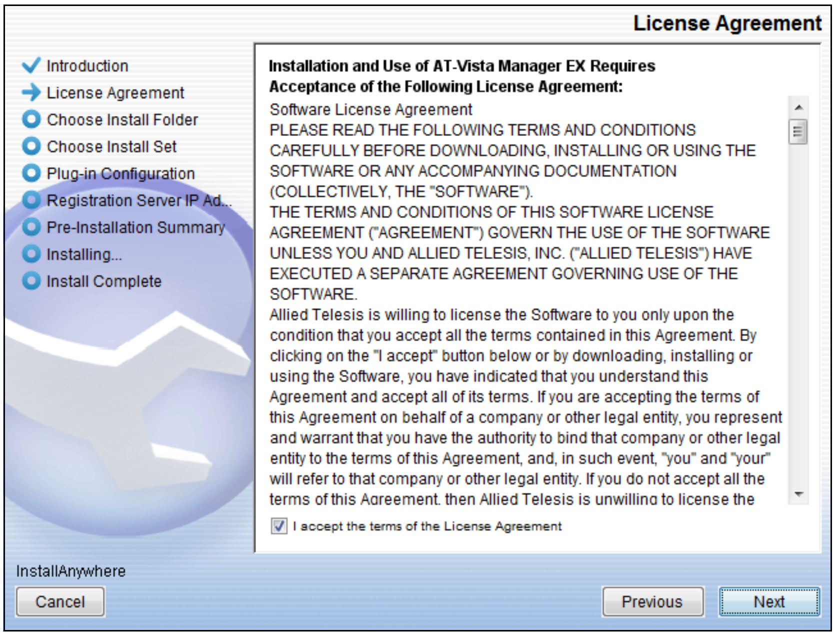
It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

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

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



Installation and Use of AT-Vista Manager EX Requires Acceptance of the Following License Agreement:

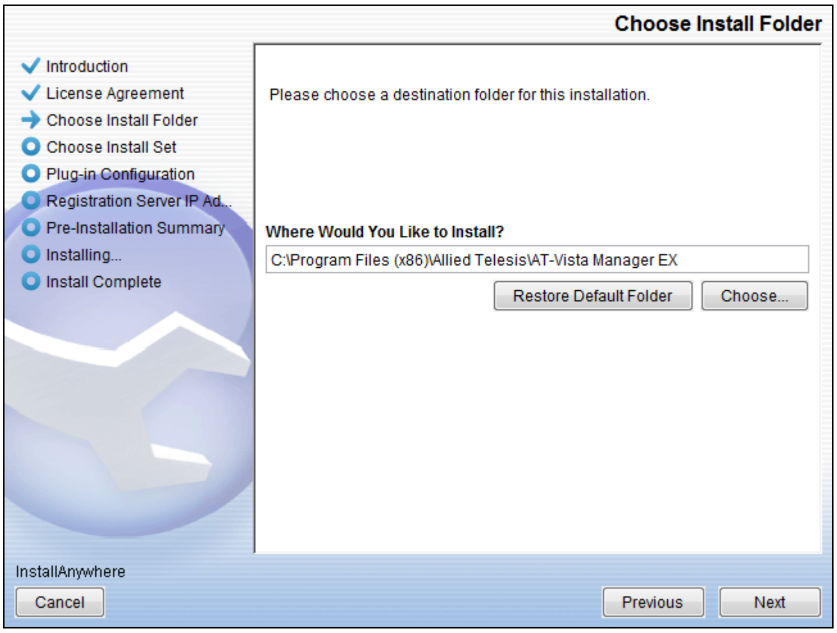
Software License Agreement
PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THE SOFTWARE OR ANY ACCOMPANYING DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE").
THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") GOVERN THE USE OF THE SOFTWARE UNLESS YOU AND ALLIED TELESIS, INC. ("ALLIED TELESIS") HAVE EXECUTED A SEPARATE AGREEMENT GOVERNING USE OF THE SOFTWARE.
Allied Telesis is willing to license the Software to you only upon the condition that you accept all the terms contained in this Agreement. By clicking on the "I accept" button below or by downloading, installing or using the Software, you have indicated that you understand this Agreement and accept all of its terms. If you are accepting the terms of this Agreement on behalf of a company or other legal entity, you represent and warrant that you have the authority to bind that company or other legal entity to the terms of this Agreement, and, in such event, "you" and "your" will refer to that company or other legal entity. If you do not accept all the terms of this Agreement, then Allied Telesis is unwilling to license the

☑ I accept the terms of the License Agreement

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:



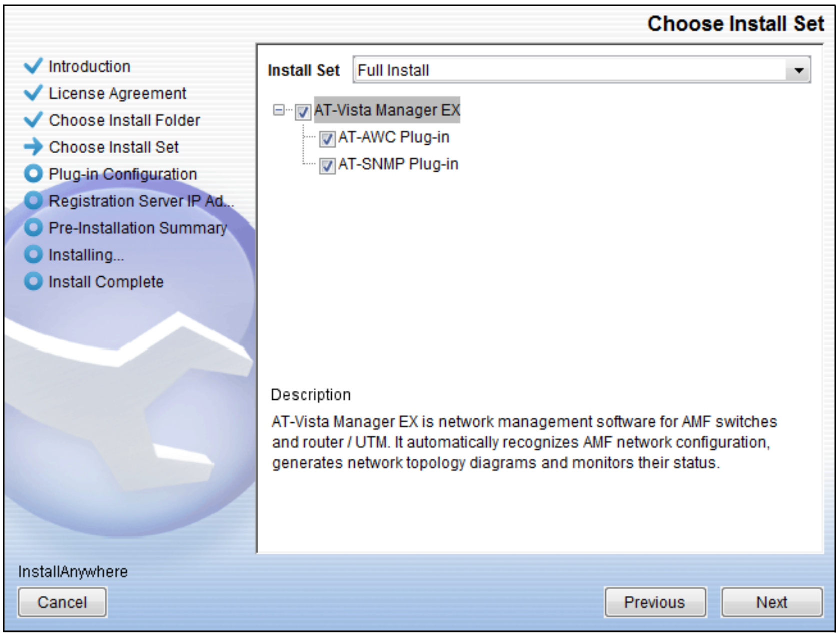
Please choose a destination folder for this installation.

Where Would You Like to Install?

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

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

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



Install Set: Full Install

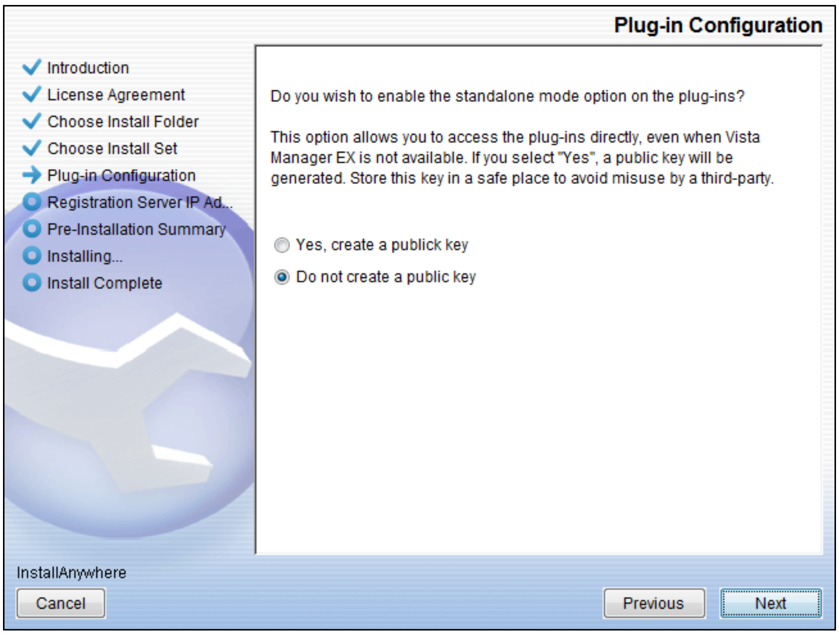
☑ AT-Vista Manager EX
☑ AT-AWC Plug-in
☑ AT-SNMP Plug-in

Description

AT-Vista Manager EX is network management software for AMF switches and router / UTM. It automatically recognizes AMF network configuration, generates network topology diagrams and monitors their status.

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:



Plug-in Configuration

Do you wish to enable the standalone mode option on the plug-ins?

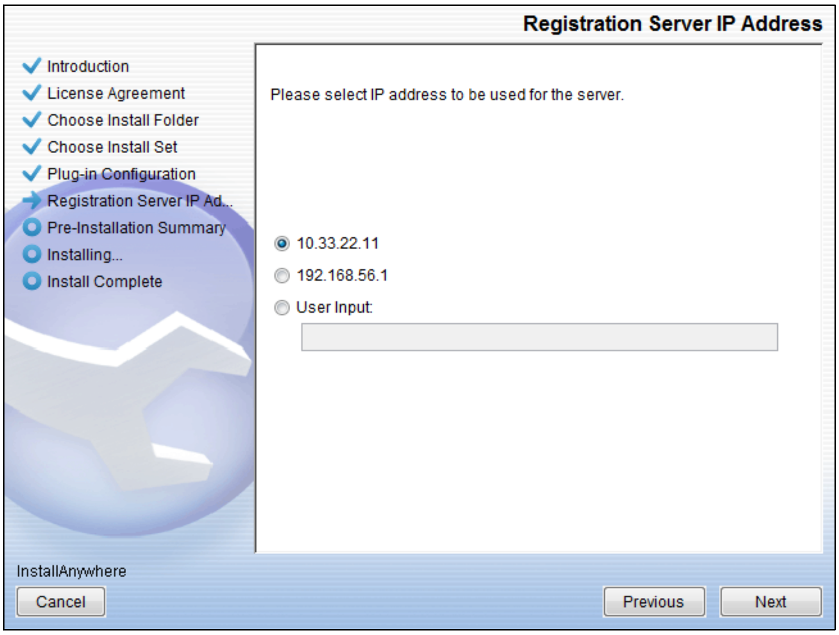
This option allows you to access the plug-ins directly, even when Vista Manager EX is not available. If you select "Yes", a public key will be generated. Store this key in a safe place to avoid misuse by a third-party.

○ Yes, create a publick key

● Do not create a public key

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:



Registration Server IP Address

Please select IP address to be used for the server.

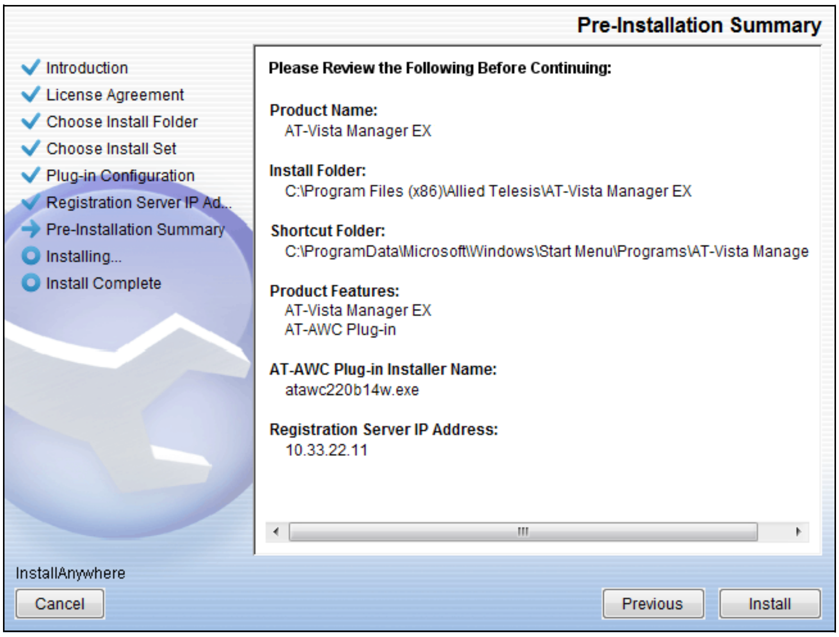
● 10.33.22.11

○ 192.168.56.1

○ User Input:

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:



Pre-Installation Summary

Please Review the Following Before Continuing:

Product Name:
AT-Vista Manager EX

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

Shortcut Folder:
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AT-Vista Manage

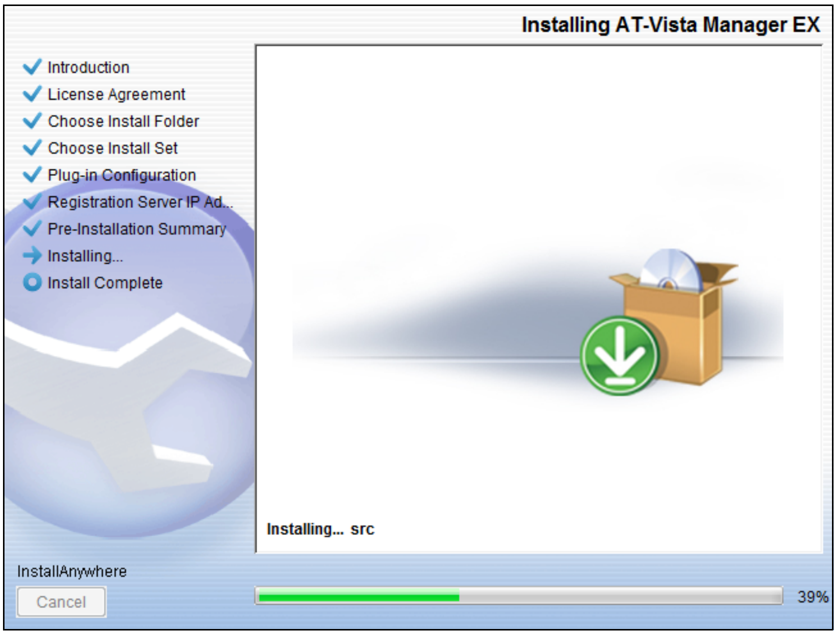
Product Features:
AT-Vista Manager EX
AT-AWC Plug-in

AT-AWC Plug-in Installer Name:
atawc220b14w.exe

Registration Server IP Address:
10.33.22.11

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**.

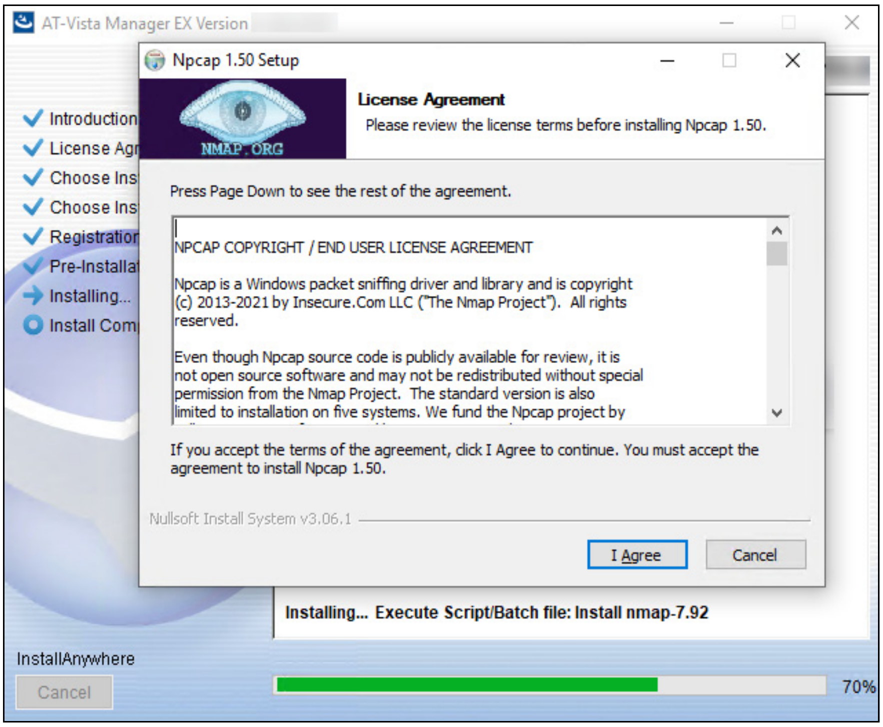
9. The ***Installing...*** dialog displays:



Installing AT-Vista Manager EX

Installing... src

10. The NPCAP installer dialog appears.



License Agreement

Please review the license terms before installing Npcap 1.50.

Press Page Down to see the rest of the agreement.

NPCAP COPYRIGHT / END USER LICENSE AGREEMENT

Npcap is a Windows packet sniffing driver and library and is copyright (c) 2013-2021 by Insecure.Com LLC ("The Nmap Project"). All rights reserved.

Even though Npcap source code is publicly available for review, it is not open source software and may not be redistributed without special permission from the Nmap Project. The standard version is also limited to installation on five systems. We fund the Npcap project by

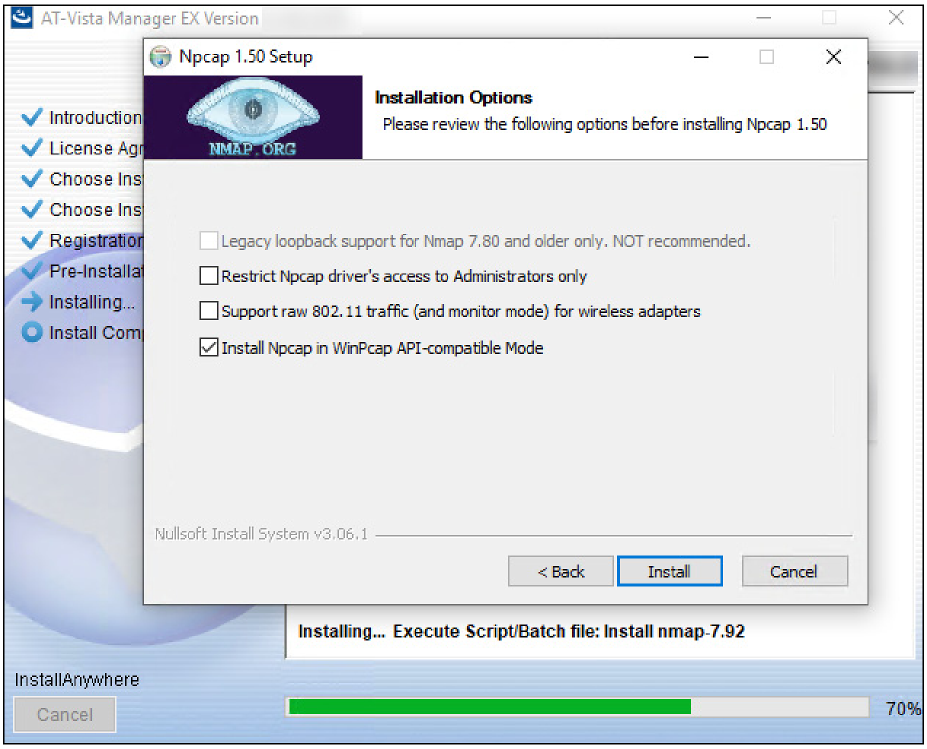
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 1.50.

Nullsoft Install System v3.06.1

Installing... Execute Script/Batch file: Install nmap-7.92

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

11. Click **Install**.



Installation Options

Please review the following options before installing Npcap 1.50

☐ Legacy loopback support for Nmap 7.80 and older only. NOT recommended.

☐ Restrict Npcap driver's access to Administrators only

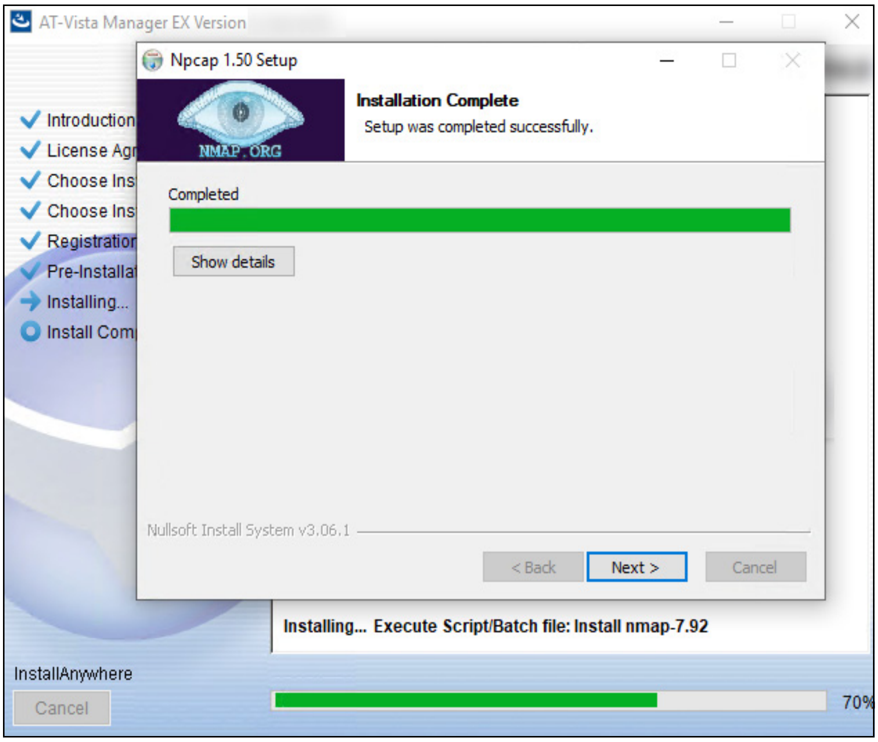
☐ Support raw 802.11 traffic (and monitor mode) for wireless adapters

☑ Install Npcap in WinPcap API-compatible Mode

Nullsoft Install System v3.06.1

Installing... Execute Script/Batch file: Install nmap-7.92

12. The Npcap install will install.



Installation Complete

Setup was completed successfully.

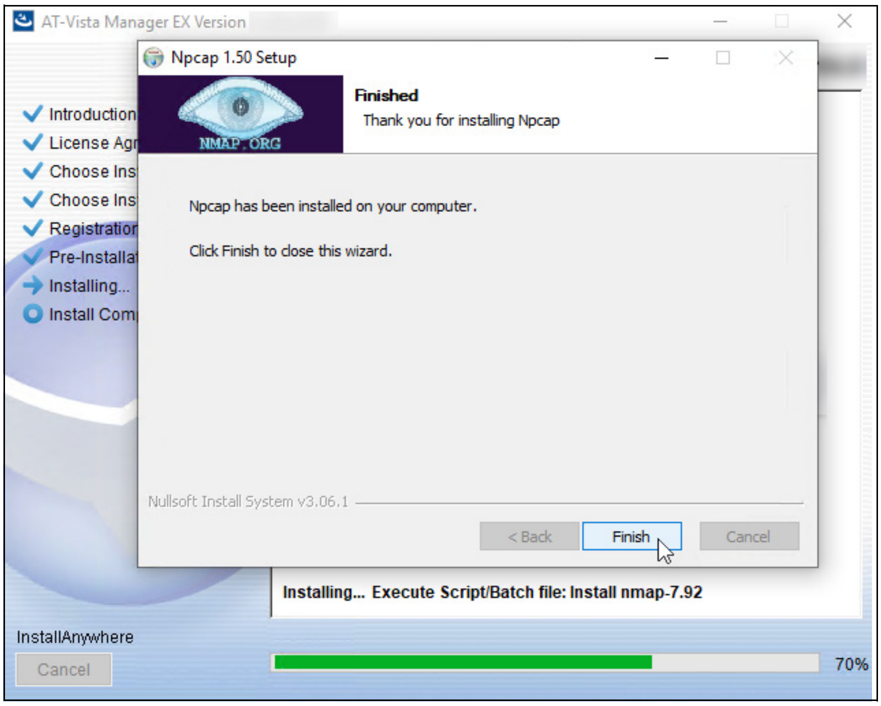
Completed

Installing... Execute Script/Batch file: Install nmap-7.92

70%

Click **Next**.

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



Finished

Thank you for installing Npcap

Npcap has been installed on your computer.

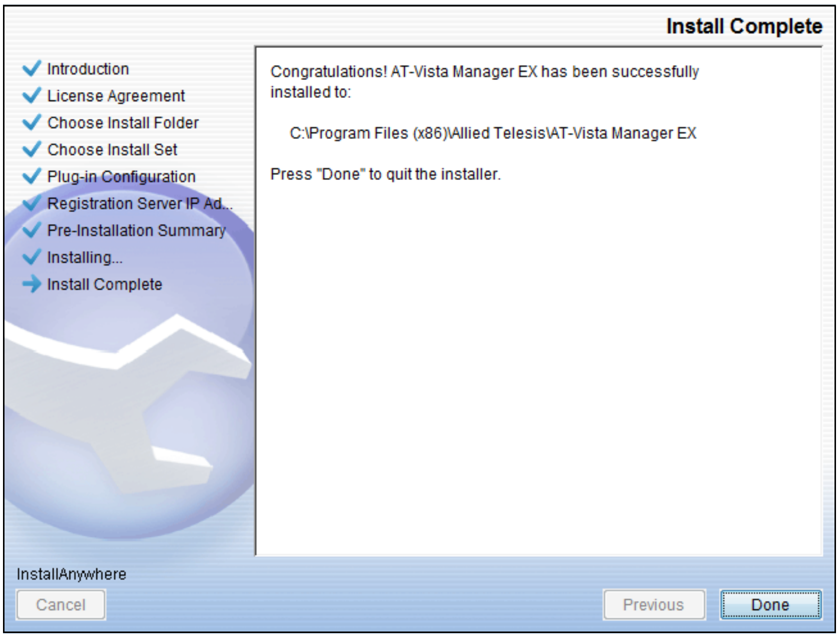
Click Finish to close this wizard.

Installing... Execute Script/Batch file: Install nmap-7.92

70%

Vista Manager will resume the rest of the download.

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



Congratulations! AT-Vista Manager EX has been successfully installed to:

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

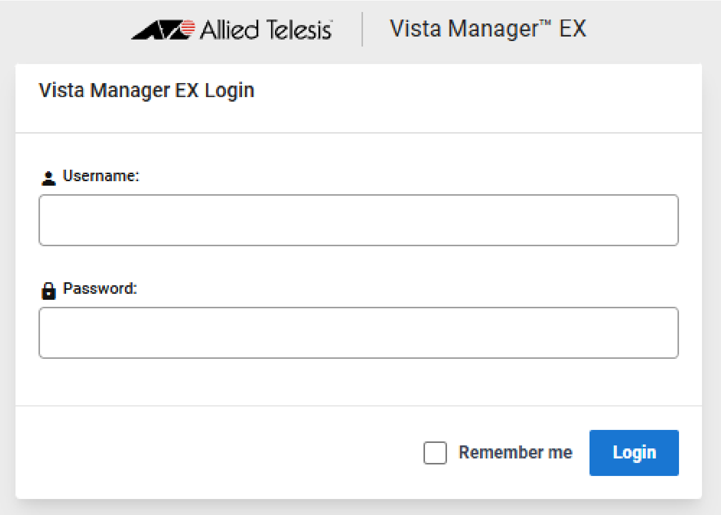
Press "Done" to quit the installer.

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

Restore the Vista Manager database

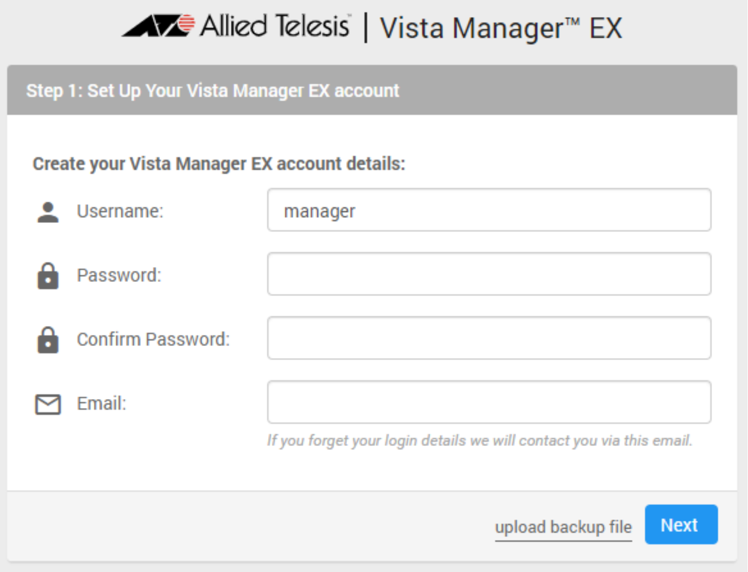
After the upgrade is complete, you need to restore the Vista Manager database. To do this, use the following procedure.

1. Login to Vista Manager.



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

2. Click on upload backup file.



Allied Telesis | Vista Manager™ EX

Step 1: Set Up Your Vista Manager EX account

Create your Vista Manager EX account details:

Username: manager

Password:

Confirm Password:

Email:

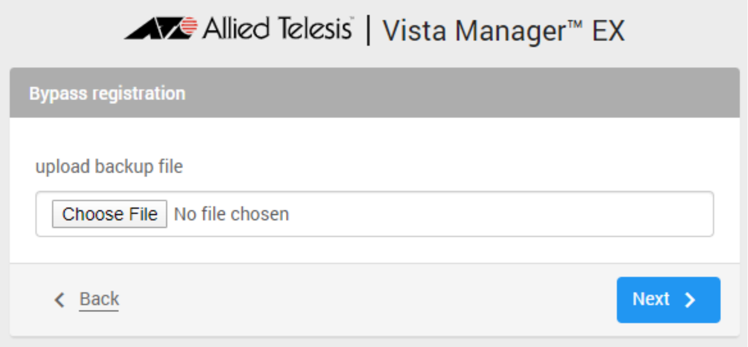
If you forget your login details we will contact you via this email.

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.



Allied Telesis | Vista Manager™ EX

Bypass registration

upload backup file

Choose File No file chosen

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.

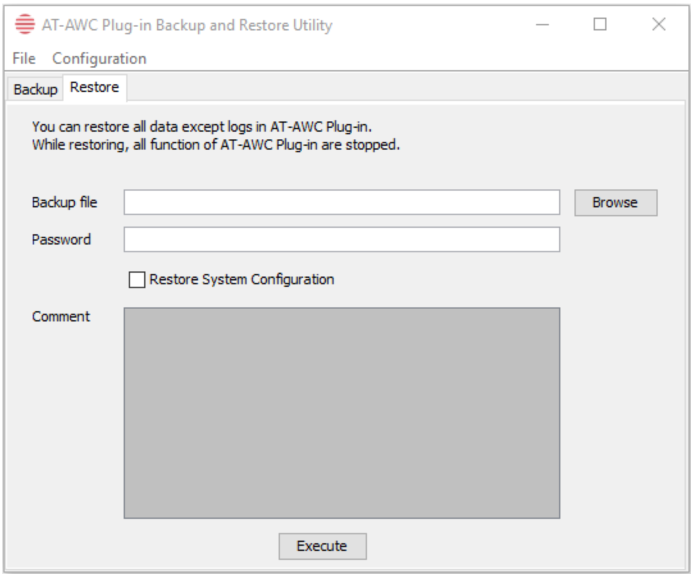
   “<*Vista Install Path*>\Plugins\AT-AWC\root\stopserver.bat"

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.



You can restore all data except logs in AT-AWC Plug-in.
While restoring, all function of AT-AWC Plug-in are stopped.

Backup file

Password

☐ Restore System Configuration

Comment

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.

Allied Telesis NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com