

Autonomous Integrated Network Management

Centralized Control, with Automated Backup,
Upgrade, Expansion, and Recovery



A
u
t
o
n
o
m
o
u
s

M
a
n
a
g
e
m
e
n
t

F
r
a
m
e
w
o
r
k



Widespread Adoption of IoT and DX

AMF

Challenge

Growing complexity of management due to increasing scale and capacity of IT infrastructure

Solution

Centralize, simplify and automate operation and management to achieve integrated management

Is the management and operation of your

Modern IT infrastructure faces issues caused by recent social transformation. With the widespread adoption of IoT and efforts to drive digital transformation (DX), distributed locations and integrated management have become essential. On top of this, there is growing demand for IT infrastructure and effective responses to incidents - key factors in increasing the burden placed on administrators.



Increasingly Elaborate Cyber Attacks

AMF-SEC

Challenge

Increase in incidents caused by vulnerable IT infrastructure

Solution

Enhancing security and greatly reducing operational burden and operating costs

Driving Workstyle Reforms

AMF-WAN



Challenge
Solution

Growing demand for more flexible and stable IT infrastructure

Improve WAN performance with powerful features including centralized management, dynamic bandwidth use, and automated application optimization

"network" becoming complex and cumbersome?

In response, Allied Telesis autonomous integrated network management solutions enable easy and secure centralized operation and management, without administrators needing a deep understanding of wired or wireless LANs, or WANs.

FUTURE PLANS

AMF will evolve into an Artificial Intelligence Management Framework which will enable a new form of network management and operation called intent-based network management. Network infrastructure will learn, analyze and adapt simply from administrators entering their intent.

Impacts of Population Decrease and Aging

Vista Manager Series



Challenge
Solution

An aging population leading to shortages in skilled IT infrastructure administrators.

Improving the efficiency of management and operation simply, intuitively and visually

Centralized management of complex networks



The widespread adoption of IoT and digital transformation makes management complex, as the scale and capacity of IT infrastructure increases

As the number and types of devices capable of connecting to networks grows, IT infrastructure has diversified and its management and operation is increasingly complex.

- Client needs have diversified, networks take more time and effort to build
- Network management hours have increased as more devices are being used
- Operators are unable to respond to faults due to the absence of network specialists



Solved by Allied Telesis

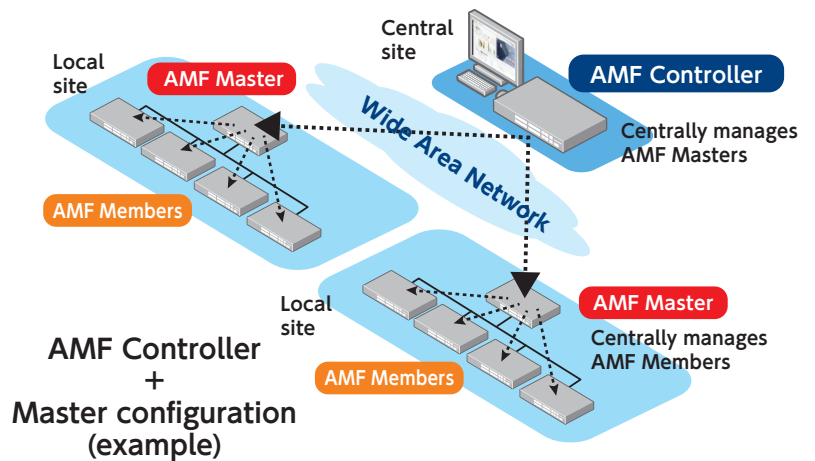
AMF enables integrated network management by centralizing, simplifying and automating

By centralizing, simplifying and automating network management and operation, AMF enables integrated network management, significantly reducing costs, time and technical skills required to operate and manage networks.

● What is AMF?

AMF is an autonomous integrated network management technology developed by Allied Telesis. In addition to centralized management and automated network expansion, AMF removes network problems through simpler, more highly convenient integrated management functionality, including automated recovery.

The devices (AMF nodes) that make up an AMF network can be divided into three types: AMF Controller, AMF Master, and AMF Member. AMF Controllers manage AMF Masters, which in turn manage AMF Members. Through this functionality, it is possible to achieve centralized management of AMF Members and AMF Masters, even when they are distributed across multiple locations.



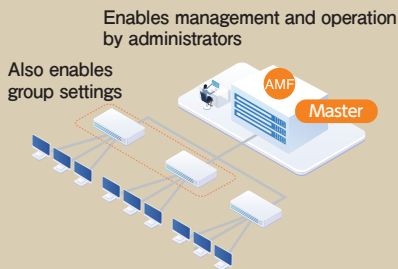
- Removes unnecessary costs due to duplication and distribution of personnel and hardware
- Resolves increases in man-hours due to complex structure and cumbersome procedures

For example, where 80 nodes are being managed:

Benefit	Conventional network work-hours / costs	AMF	Reduction	Additional Info
Centralize	Management work-hours	AMF	$\frac{1}{80}$	<ul style="list-style-type: none"> ● In a conventional network, 80 nodes are managed individually ● AMF batch-manages management IPs, firmware and configurations
Simplify	Operation work-hours	AMF	$\frac{1}{6}$	<ul style="list-style-type: none"> ● With a conventional network, a large amount of advance preparation is required (approx. 120 minutes until recovery) ● AMF enables automated recovery by re-connection to factory-default devices (approx. 20 minutes until recovery)
Automate	Cost of changes	AMF	$\frac{1}{20}$	<ul style="list-style-type: none"> ● Conventional network: USD1,600 (USD80 × 20 hours (80 nodes × 15 minutes)) ● AMF: USD80 (USD80 × 1 hour for the batch process; in reality takes approx. 15 to 20 minutes)

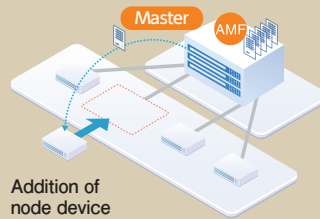
● Centralized management

AMF enables centralized management of one, many, or all devices at once. This reduces the burden of network administration."



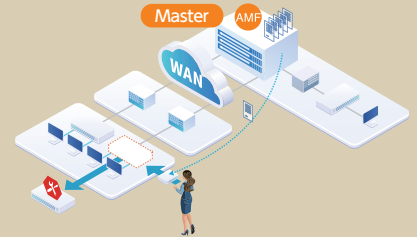
● Automated network expansion

Firmware and setting files registered on the master device in advance are automatically applied to all devices under the control of the master at the time of addition, simply by connecting them.



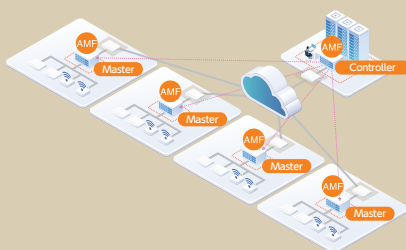
● Automated recovery

Because tasks such as firmware updates and restoration of settings are performed automatically, network settings are recovered automatically simply by replacing malfunctioning devices with factory-new devices.



● Scalable management

A controller can manage multiple master nodes. This enables scalable management of very large networks, as each master manages a specified number of nodes.



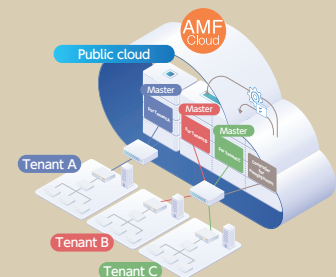
● Network device management

AMF can display details of and manage IoT devices in your network, such as surveillance cameras, medical devices and IP (VoIP) phones. Even where networks use non-AMF products (such as thirdparty devices), you can obtain information about these devices and manage them with AMF. This includes ONVIF Profile Q devices.



● Cloud support

It is possible to deploy AMF management services in the cloud, to reduce CAPEX. AMF also supports multi-tenant configurations, enabling you to support multiple customers while keeping each customer's network management separate.



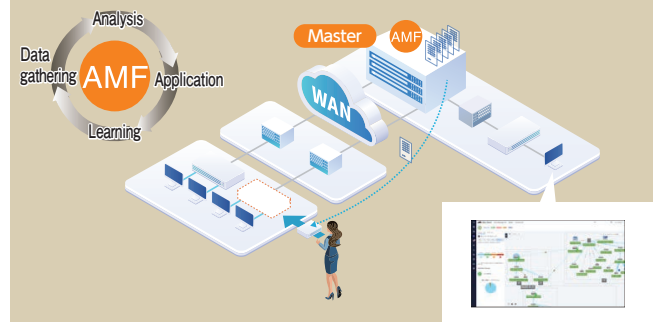
● Network visualization

Because graphical maps for networks configured with AMF are automatically created, administrators can check the state of the network configuration visually. (Uses AT-Vista Manager EX, our feature-rich single pane of glass GUI)



● Autonomous network optimization

Integration of AMF with the Vista Manager Series provides high-end features such as predictive analysis of data traffic and device status for autonomous network optimization. Visibility is also provided of any devices suspected of carrying malware, which have been discovered by AMF-Security (AMF-Sec) and automatically quarantined.



FUTURE PLANS

It will be possible to display a custom icon for any individual device connected to your network. This feature will increase the visibility of devices and further facilitate intuitive management of the network as a whole.

Autonomously respond to incidents - before it's too late



Difficulties

Cyber attacks - Increase in incidents caused by vulnerable IT infrastructure

By the time an administrator realizes a malware breach has occurred, the infection has already spread throughout the entire network.

- Operators want to minimize damage and spread of cyber attacks
- Companies must protect themselves from the leakage of sensitive business information
- Network operation and management takes time and effort and incurs costs



Solved by Allied Telesis

In addition to enhancing security, AMF-Sec also greatly reduces the burden and costs of network operation

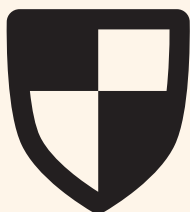
AMF-Sec automatically isolates infected devices from the network, and prevents the spread of malware.

● What is AMF-Sec?

AMF-Sec is a groundbreaking technology that enables flexible and agile changes to network configurations and settings using SDN (Software-Defined Networking), which enables a programmable network.

By integrating technology partner solutions (such as IT asset management and measures against targeted cyber attacks) with the network itself, AMF-Sec enhances security and reduces the costs and burden associated with network operation.

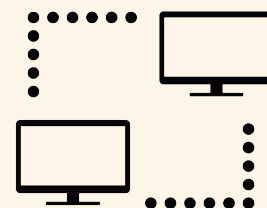
Cyber Security



● Improves and enhances Cyber security

- Acts against targeted attacks and malware
- Provides monitoring, analysis and control
- Prevents unauthorized operation and rehabilitates vulnerable devices

Provisioning

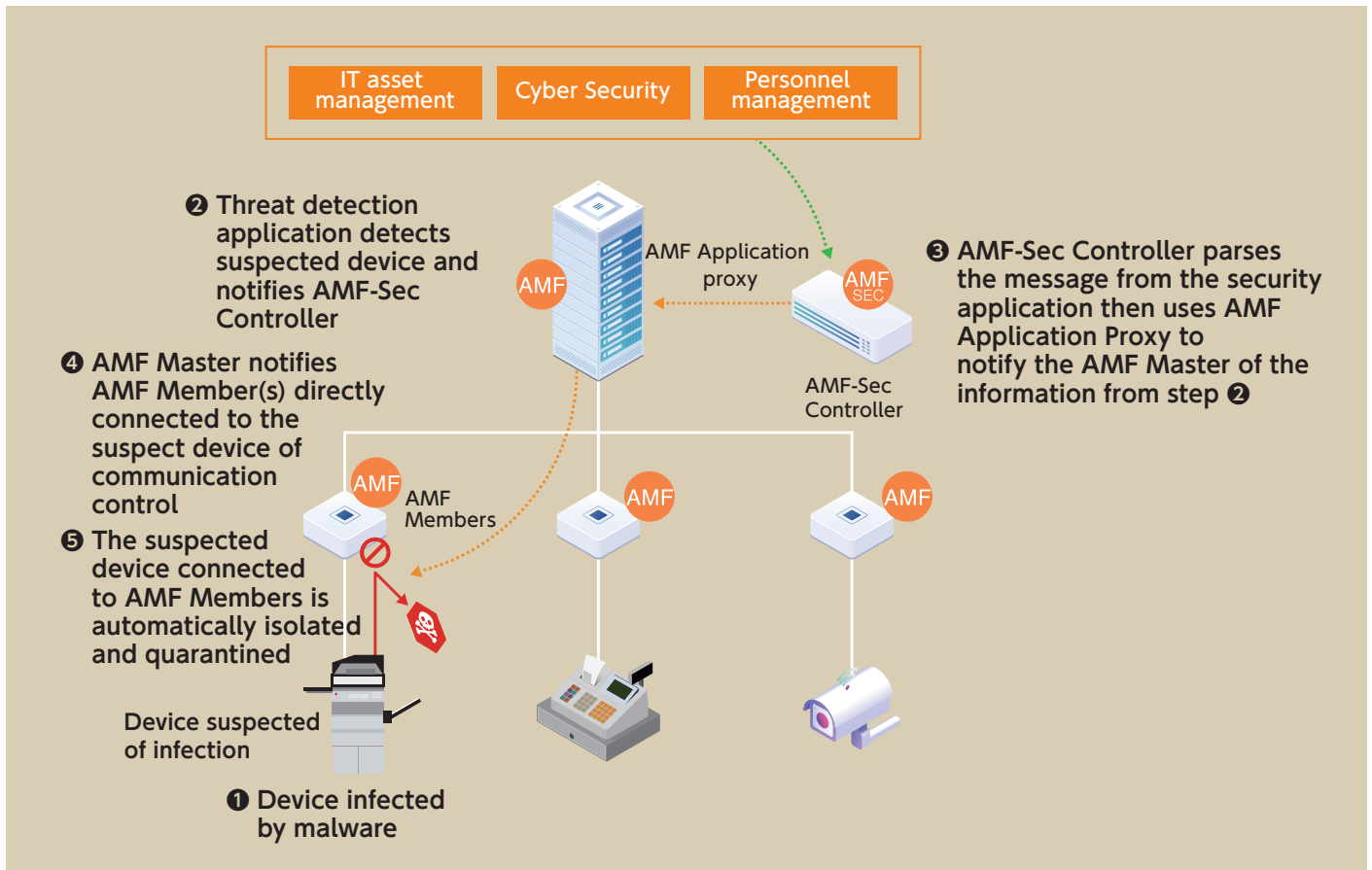


● Authentication Database integration

- IT asset management
- Personnel management
- Certification / authentication

AMF-Sec System Outline Diagram

How AMF-Sec works with security applications to prevent malware infection



AMF-Sec deployment options

The functionality explained above (i.e. the automated isolation and quarantine of suspected devices) is enabled by introducing AMF-Sec. For different environments, Allied Telesis offers AMF-Sec Controller and AMF-Sec Controller mini.

AMF-Sec Controller

The AMF-Sec Controller is a software appliance that can run in a range of virtual environments. In networks that already use AMF, adding AMF-Sec enhances cyber security with minimal investment.

AMF-Sec Controller mini

The AMF-Sec controller is available integrated into some routers, and some switch models (coming soon), and the Vista Manager Network Appliance (coming soon). This enables networks to achieve integrated management and enhance cyber security with minimal cost.

*In order to use AMF-Sec Controller, the AMF Master must support AMF Application Proxy feature. Please see page 13 for a list of devices that support AMF Application Proxy feature.



FUTURE PLANS

Moving forward, in addition to application integration, we will continue to drive the evolution of comprehensive Secure infrastructure, such as by enhancing Captive Portal, and Authentication functionality for supporting PassPoint, to securely onboard customers to the network.

Creating stress-free networks with AMF-WAN



Workstyle reforms - Growing demand for more flexible, more stable IT infrastructure

With use of IP (VoIP) phones becoming commonplace and growing dependency on WAN networks, the range of devices (including PCs, smartphones and tablets) connecting to networks is diversifying, and the shift towards IoT is progressing.

- Changing network settings every time the number of locations changes is bothersome
- Network load becomes heavy at certain times, such as during Windows updates, which interferes with day to day work processes
- Operators want to increase lines availability but also suppress costs
- Internet response speed has fallen due to the introduction of Office 365 and other SaaS services, etc.



AMF-WAN optimizes WAN networks with diverse functionality

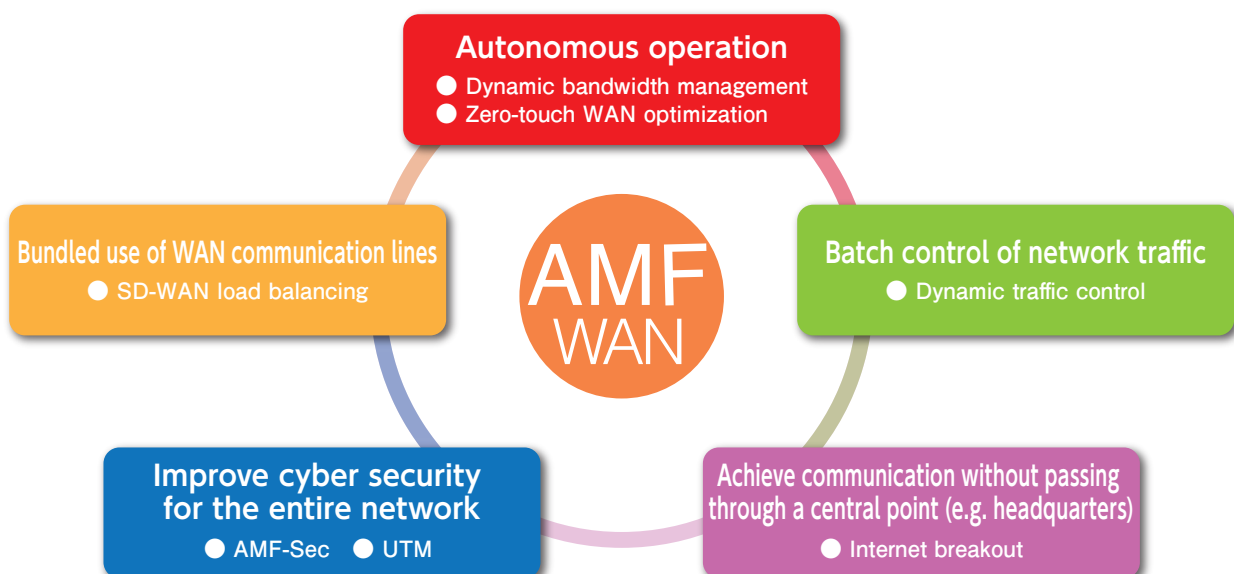
AMF-WAN, our Software-Defined WAN (SD-WAN) solution, optimizes inter-branch traffic, by prioritizing critical applications, load-balancing traffic, and securing business data transfer. AMF-WAN reduces the complexity and cost of WAN infrastructure.

● What is AMF-WAN?

AMF-WAN is an application of SDN—a technology which enables operation and management of networks through software control—for WAN (Wide Area Networks). Utilizing AMF-WAN, it is possible to optimize network performance and simplify WAN management.

Using AMF-WAN enables operators to create stress-free networks, by performing load balancing of bandwidth that has become crowded due to cloud-type applications and Internet connections, and reducing network costs. AMF-WAN improves network operation performance by monitoring and managing network quality and the causes of network faults, and prioritizing control of data volumes for specific applications.

Through integration with AMF (which improves network availability), AMF-SEC (which ensures network Cyber security), and AT-Vista Manager EX (which seeks to increase operational efficiency), AMF-WAN enables more stable network operation.



Key Features

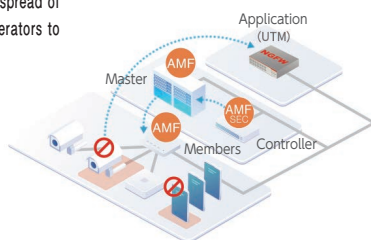
Key Features of AMF-WAN

In addition to network load balancing, bandwidth control and application control, through its integration with AMF, AT-Vista Manager EX and AMF-SEC, AMF-WAN solves various challenges such as improving network availability, increasing operating efficiency and ensuring security.

Enhancing overall network security, including terminal and IoT devices

● AMF-Sec Network Cyber Security

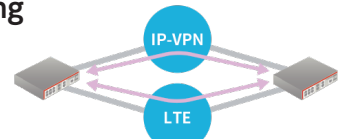
When integrated with an AMF-Sec Controller, based on threat data detected by AT-AR3050S / AT-AR4050S, AMF-WAN automatically isolates and quarantines any wired or wireless device suspected of introducing malware. This prevents the spread of threats within the LAN and enables operators to increase the safety of the entire network.



Load balancing of WAN connections on an individual application basis

● SD-WAN Load Balancing

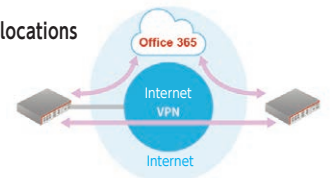
SD-WAN load balancing enables active-active operation of multiple WAN connections, facilitating the construction of efficient intranet architectures. In addition to IP address and port-based load balancing, it also enables assignment on an individual application basis.



Direct access to specific apps from remote locations

● Internet Breakout

Internet breakout enables cloud-based applications (e.g. Office 365) to be accessed directly from branch offices, without the traffic having to pass through a central head-office. This improves performance and reduces traffic volume on head-office WAN connections"



Visualizing the state of WAN usage

● WAN Topology Map

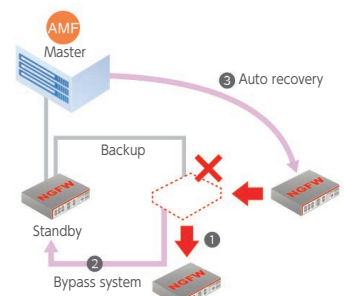
WAN Topology Map using AT-Vista Manager EX visualizes the state of WAN usage. AMF-WAN enables administrators to see the current state of operation of IPsec VPNs, a popular form of encrypted communication for enterprises. Colors indicate the connection status of each tunnel, providing information at a glance. Vista Manager EX also makes it easy to see application usage.



Offering uninterrupted communication over a single WAN connection, and automated recovery

● Bypass System / Auto-Recovery

Bypass ports enable device redundancy even with a single WAN network connection. In the event of faults such as active-side device malfunctions (including device power source malfunctions) and LAN-side port link down failures, bypass system functionality limits downtime by replacing the faulty device with a standby device. This saves on network connection costs and increases the availability of the overall system, while at the same time achieving swift recovery simply by replacing devices with AMF functionality, improving network maintainability. When using auto recovery, the task of replacing faulty devices is carried out automatically.

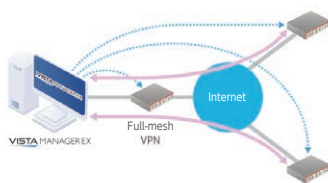


Coming soon

Easy creation and management of VPNs

● Dynamic VPN

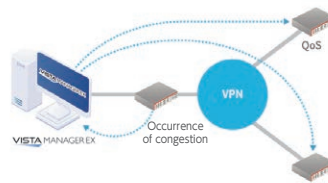
Dynamic VPN enables easy and secure creation of private networks using reasonably priced Internet connections. By constructing a full-mesh VPN, it is also possible to distribute traffic on the central side.



Batch control of network traffic

● Dynamic Traffic Control

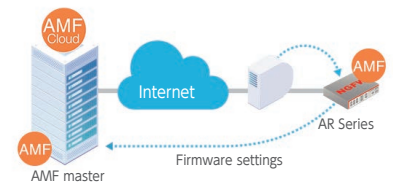
Dynamic traffic control monitors connection traffic and implements bandwidth control for the entire network according to traffic volume. This enables congestion control for WAN connections at all locations and assignment of bandwidth to match the usage rate of each connection, thereby facilitating the effective use of WAN connections.



Automated setup simply by connecting to the WAN

● Zero-touch Configuration

Zero-touch configuration enables setup tasks to be completed automatically simply by connecting devices to the WAN network in their factory-default state. This makes it possible to complete setup tasks easily, without the need to dispatch engineers with an in-depth knowledge of network devices.



FUTURE PLANS

In the future, it will become possible to visualize usage, status, and performance of WAN networks. AMF will enable the creation of intent-based networks, which optimize network traffic automatically based on the intent of administrators, and make it possible for users to enjoy optimized use of limited WAN bandwidth at any time.

Achieving easy and simple network management



Decline in the number of IT infrastructure administrators and engineers

In the USA, there are concerns over the decrease in the number of network administrators and engineers.

- Networks are complex and difficult to grasp
- Administrators want to manage both wired and wireless, and both LAN and WAN networks



Solved by Allied Telesis

Vista Manager Series improves the efficiency

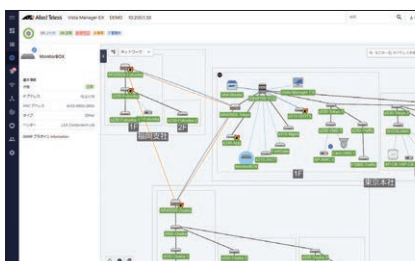
of network management through simple, intuitive and visualized operation

By using the Vista Manager Series, administrators can visualize entire networks spanning LAN, WAN, wired and wireless, enabling integration of operation and management for complex networks. This makes it possible to create stable, high-quality networks even with limited numbers of administrators.

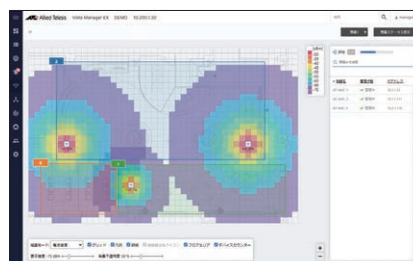
● What is Vista Manager Series?

Vista Manager Series is a network management solution that enables batch management of both on-premises and cloud environments, including not only Allied Telesis switches, routers and wireless LAN access points, but also third-party network devices. Through visualization, it enables easy and simple network management through intuitive on-screen operation. It allows instant checking of network status and issues, and timely resolution of problems and events.

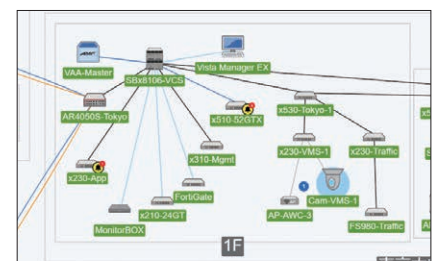
Key Features and Management Screens of Vista Manager Series



Network Map



Wireless LAN Management



SNMP Management

Asset Management

Performs batch management of IoT devices as well as conventional network devices

VLAN Map

Enables creation, display and editing of VLANs via the GUI

Traffic Monitoring

Visualizes the state and content of LAN/WAN communications

Service Monitoring

Monitors the state of services on nodes

Tracepath

Show network connectivity between any two selected devices on the map

Syslog Server

Problem alerts, and network change information is easily accessible from logs

*Supported devices differ between AT-Vista Manager EX, Vista Manager APL and Vista Manager mini.

For details, see www.alliedtelesis.com/products/software/VistaManager



● For details of key features, see:

www.alliedtelesis.com/software/VistaManager/datasheet

AT-Vista Manager EX, Vista Manager APL and Vista Manager mini offer integrated network management to match network scale and management needs.

AT-Vista Manager EX: Visualization and integrated management for large-scale networks

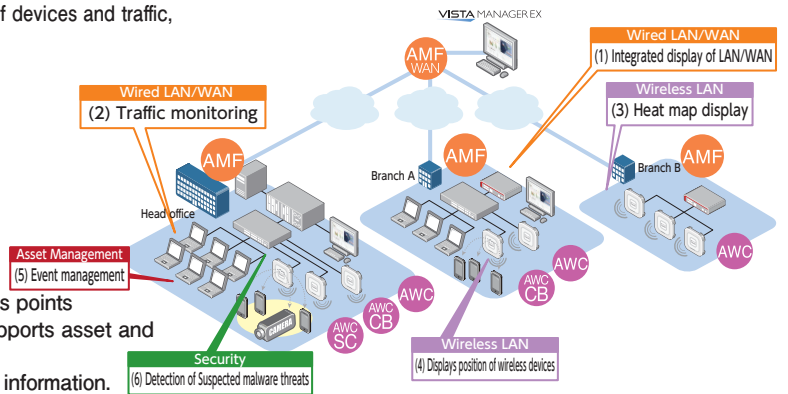
AT-Vista Manager EX offers high extensibility and enables visualization of devices and traffic, to flexibly manage small to large-sized networks.

Key Features

- Integrated management of WAN, LAN, wired and wireless networks
- Manage third party devices with SNMP
- Expansion of wireless area is possible simply by adding licenses

Use Case

- (1) Batch management for head office and branch locations
- (2) Visualize bandwidth utilization and protocol use.
- (3) Ascertaining signal strength and status for wireless access points
- (4) Monitor the location history of mobile devices, which supports asset and network planning.
- (5) Notifies the administrator of events, based on device trap information.
- (6) Automatically blocks malware anywhere in the network.



Vista Manager APL: LAN/WAN integration and all-in-one network management

Vista Manager APL retains the extensive functionality of Vista Manager EX, but offers an optimal range of features to support small to medium-sized network environments, as well as integrated framework and security features.

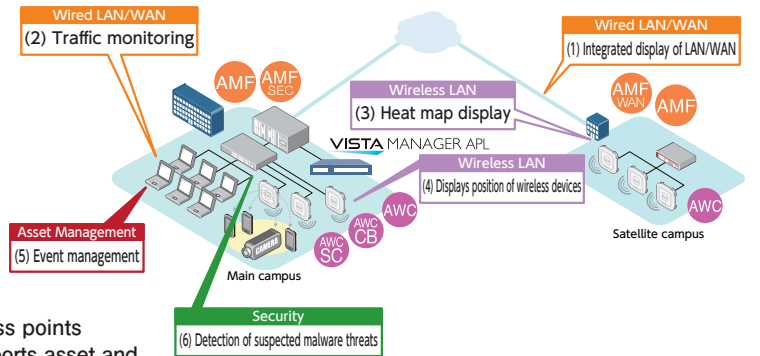
Key Features

- Ideal for management of small to medium-sized LAN/WAN networks
- All automation and management applications come pre-installed for convenience



Use Case

- (1) Batch management for head office and branch locations
- (2) Visualize bandwidth utilization and protocol use.
- (3) Ascertaining signal strength and status for wireless access points
- (4) Monitor the location history of mobile devices, which supports asset and network planning.
- (5) Notifies the administrator of events, based on device trap information.
- (6) Automatically blocks malware anywhere in the network.



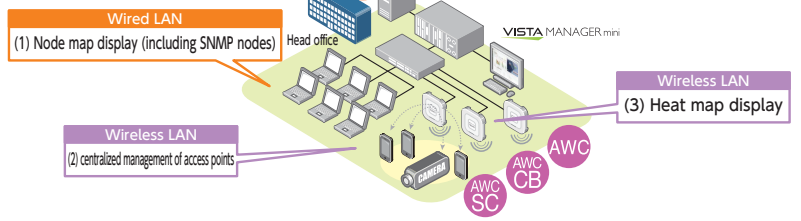
Vista Manager mini: Enables casual and easy introduction to match small-scale networks

Enables intuitive network management, tailored toward LAN networks.

Enables all-in-one management of small to medium-sized wired and wireless networks.

Key Features

- Ideal for LAN network management
- Built into some switch and router models
- Expansion of wireless area is possible simply by adding licenses



Use Case

- (1) Centralized management of wired LAN networks and display of node status
- (2) Centralized management of wireless access points inside buildings
- (3) Visualization of signal strength for wireless access points inside buildings using heat mapping

- A separate license is required when using AT-Vista Manager EX. Supported devices are required when using Vista Manager APL and Vista Manager mini respectively. Please see page 13.

License Table for AMF, AMF-Sec, AMF-WAN and Vista

AMF & AMF-Sec License Selection Guide

- AMF is recommended for its integrated management functionality, achieving centralization, simplification and autonomization of network operation and management while reducing deployment, maintenance and operation costs.
- You can also choose to introduce AMF-Sec functionality, which utilizes the AMF framework to enhance security and increase efficiency of network operation and management, by automatically isolating infected devices from the network and preventing the spread of malware threats.
- Select the necessary devices for AMF and AMF-Sec, using the following guide.

For small-scale networks

Choose conditions for configuring your AMF network

For large-scale networks

(1) You want to operate infrastructure that integrates both network and management functionality, using assets kept on premises.

Achieve integrated management with switches and routers

● Required licenses and devices

AMF Master license	e.g. AT-FL-GEN2-AM20/40/80
AMF Master device	e.g. AT-SBx908GEN2, AT-x950

(2) You want to operate infrastructure with independent network and management functionality, using assets kept on premises.

Integrated management is provided through an appliance. Also caters to changes in network configuration policy

● Required licenses and devices

AMF Master license	e.g. AT-FL-AMFCLOUD-BASE-1YR
Integrated management appliance	AT-VST-APL

(3) You do not want to own any hardware.

AMF networks are configured using software. Start with annual payments

● Required license

AMF Cloud license	e.g. AT-FL-AMFCLOUD-BASE-1YR/5YR
-------------------	----------------------------------

Enhance security by adding AMF-Sec!

Uses AMF-Sec Controller in the same hardware as AMF Master. Enables customers who have already introduced AMF to further increase the benefits of their investment.

● Additional license

e.g. AMF-Sec Mini License

Uses AMF-Sec Controller functionality built into the VST-APL appliance to offer security measures at optimal cost.

● Additional license

AT-FL-SESC-BaseST-(1YR/5YR)

Achieves integrated management and access control without the need to own hardware assets, through a software-based AMF-Sec Controller.

● Additional license

AT-FL-SESC-BaseST-(1YR/5YR)

Option (1) Use customer assets (switches and firewalls) kept on premises

*With this pattern, AMF-Sec can only be added when devices that support AMF-Sec Controller mini (shown in blue) have been deployed.

Solution	Licenses and devices	Product used	Summary	Explanation
AMF	e.g. AT-FL-GEN2-AM20/40/80/120/180/300-1YR/5YR AT-FL-AR4-AM20 ■ Switches SBx8100 Series ■ UTM Firewalls AR4050S ■ SBx908 GEN2 ■ x950 Series ■ x930 Series ■ x550 Series ■ x530 Series ■ x510 Series	SBx8100 Series SBx908 GEN2 x950 Series x930 Series x550 Series x530 Series x510 Series AR4050S	AMF Master license Device that supports AMF-Sec Controller mini	Provides AMF-Sec Controller functionality, and achieves access control for AMF members in conjunction with an AMF-Sec Controller in the same hardware. Introducing the above license for these products enables provision of the AMF-Sec Controller functionality (required for AMF-Sec access control) and AMF Master functionality from these products.
When adding AMF-Sec	AT-FL-AR4-ASEC-1YR/5YR Coming soon on SBx908Gen2, x950 Series	SBx908 GEN2* x950 Series* AR4050S	AMF-Sec Controller mini license	Application of this license enables activation of the AMF-Sec Controller functionality built into the devices, and enables access control for AMF Members in conjunction with AMF-Sec Master(s) in the same hardware.

*Adding this license will enable the use of AMF-Sec with the AT-SBx908 GEN2 and x950 Series.

Option (2) Use customer assets (VST-APL) kept on premises

Solution	Licenses and devices	Product used	Summary	Explanation
AMF	e.g. AT-FL-AMFCLOUD-BASE-1YR/5YR	AT-VST-APL-06 AT-VST-APL-10	Software (virtual appliance)	Provides AMF Master and/or AMF Controller functionality through software (virtual appliances).
When adding AMF-Sec	AT-FL-SESC-BASE-1YR/5YR		Integrated management appliance	Introducing the license shown on the left for these products enables provision of the AMF-Sec Controller functionality (required for AMF-Sec access control) and AMF Master functionality by AT-VST-APL in one hardware appliance.

Option (3) Use software without owning any hardware assets

Solution	License	Product used	Summary	Explanation
AMF	e.g. AT-FL-AMFCLOUD-BASE-1YR/5YR	AMF Cloud	Software (virtual appliance)*	Provides AMF Master and/or AMF Controller functionality through software (virtual appliances).
When adding AMF-Sec	AT-FL-SESC-BASE-1YR/5YR	AMF-Sec Controller		Enables access control for AMF Members based on device information from an AMF-Sec Controller by notifying AMF Cloud of information on devices that are subject to access control.

*The software includes a license.

- Allied Telesis can customize ideal network environments to match your wishes and needs. For more information, please contact us at www.alliedtelesis.com/contact



● Names of licenses listed on this page omit the license period (1Y, etc.) and edition (2020, etc.) Please be aware that actual licensed product names include the period and edition.

AMF & AMF-Sec License Lineup

AMF & AMF-Sec functionality can be used by introducing an annual license to devices or software.

What is an annual license?

- An annual license is a subscription-type license that enables use of features or functionality for a specified period.
- All functions offer a Basic License with a license period of 1 or 5 years, enabling an investment to match your desired period of use.
- Some functions can also be used with an Additional License to manage extra nodes, enabling a flexible response as your network expands.

Points for attention when using licenses

- A Basic License is required in order to use the functionality. Please note that functionality cannot be supported without a Basic License.
- The start date for each license will be applied from the date specified by the customer. When adding additional nodes for management, start dates are applied as of the date specified for each additional license.

● AMF Controller / AMF Master

Function	Supported product type	Product name	Number of manageable nodes	Feature License
Controller	For AMF Cloud		Up to 60 Masters.	AT-FL-AMFCLLOUD-CTRL-(1YR/5YR)
	Switch products	AT-SBx81CFC960	Up to 60 Masters.	AT-FL-CF9-AC10/30/60-(1YR/5YR)
AT-SBx908 GEN2		AT-FL-GEN2-AC10/30/60-(1YR/5YR)		
Master	For AMF Cloud		1 member	AT-FL-AMFCLLOUD-EX1-(1YR/5YR)
			10 members	AT-FL-AMFCLLOUD-EX10-(1YR/5YR)
	For switches		Up to 300 Members	e.g. AT-FL-GEN2-AM20/40/80/120/180/300-1YR/5YR
	For firewalls		20 members	AT-FL-AR4-AM20-(1YR/5YR)

1) The AMF Cloud Controller license AT-AMFCLLOUD-CTRL supports the addition of management nodes with the Basic License.

● AMF-Sec Controller

Supported product type	Basic License
AMF-Sec Controller	AT-FL-SESC-BASE-(1YR/5YR)
AMF-Sec Controller for AT-VST-APL	AT-FL-SESC-BASE-(1YR/5YR)
AMF-Sec Controller mini for switches	Coming soon on SBx908Gen2, x950 Series
AMF-Sec Controller mini for routers	AT-FL-AR4-ASEC-(1YR/5YR)

Vista Manager Series

We recommend the Vista Manager Series, which enables customers to improve the efficiency of their network management and operation simply, intuitively and visually, through network visualization. Vista Manager mini can be used as a standard feature simply by introducing supporting devices*1. AT-VST-APL-06 and AT-VST-APL-10 support AT-Vista Manager EX as a standard feature.

*1 Vista Manager mini can be used with all devices in the following table that support AMF Master functionality, except AMF Cloud and SBx8100 Series devices.

● AT-Vista Manager EX Basic License

Basic License	
AT-FL-VISTA-BASE-(1YR/5YR)	AT-Vista Manager EX basic package (AMF node management)

For details of Vista Manager mini and Vista Manager APL licenses, please see our website at www.alliedtelesis.com/products/software/VistaManager

List of Devices that Support AMF and AMF-WAN (by Product)

Please select devices according to your required AMF / AMF-WAN functionality and products.

Category	Product name	Supported functionality					
		AMF				AMF-Sec/Mini	AMF-WAN
		Controller	Master	Member	Application proxy		
Appliance	AT-VST-APL	○*1	○*1	-	○	○*4	-
Software	AMF Cloud	○	○	-	○	-	-
Routers	AT-AR4050S	-	○	○	-	○*2	○
	AT-AR3050S	-	-	○	-	-	○
	AT-AR2050V	-	-	○	-	-	○
	AT-AR2010V	-	-	○	-	-	○
	AT-AR1050V	-	-	○	-	-	○
Core switches	AT-SBx81CFC960	○	○	○	○	-	-
	AT-SBx908 GEN2	○	○	○	○	○*2	-
	x950 Series	-	○	○	○*4	○*2	-
Distribution switches	x930 Series	-	○	○	○*4	-	-
	x550 Series	-	○	○	-	-	-
	x530 Series	-	○	○	-	-	-
	x510 Series	-	○	○	-	-	-

Category	Product name	Supported functionality					
		AMF				AMF-Sec/Mini	AMF-WAN
		Controller	Master	Member	Application proxy		
Edge switches	x530L Series	-	○	○	-	-	-
	x320 Series	-	-	○	-	-	-
	XS900MX Series	-	-	○*3	-	-	-
	GS900MX Series	-	-	○*3	-	-	-
	GS980EM Series	-	-	○*3	-	-	-
	x230/x230L Series	-	-	○	-	-	-
	x220 Series	-	-	○	-	-	-
	GS980M Series	-	-	○*3	-	-	-
Industrial switches	FS980M Series	-	-	○*3	-	-	-
	IE340/IE340L Series	-	-	○	-	-	-
	IE210L Series	-	-	○	-	-	-
	IE200 Series	-	-	○	-	-	-

*1 The Vista Network Appliance requires connection to an AMF-Master to use. *2 Require Mini License (Coming soon on SBx908GEN2 and x950). *3 Supported only as an AMF edge node. *4 License required.

● Table of Maximum Node Numbers

Addition of AMF Master and/or AMF Controller licenses enables management up to the following maximum numbers of nodes.

	AT-AR4050S	x530 Series/x550 Series	x930 Series	x950 Series	AT-SBx908 GEN2/AT-SBx81CFC960	AMF Cloud (single mode*1)	AMF Cloud (multi-tenant mode)
AMF Controller (no. of AMF Masters)	-	-	-	-	60	60	300
AMF Master (no. of AMF Members)	20	40	120	180	300	300	300

*1 A single AMF Controller or AMF Master can be used on a single virtual machine or AT-VST-APL. Both functions cannot be used at the same time.

AMF, AMF-SEC and AT-Vista Manager EX Customer Success Stories

Healthcare	 <p>Toranomon Hospital (Federation of National Public Service Personnel Mutual Aid Associations)</p>	 <p>Juntendo University Hospital (Juntendo University Medical Department)</p>	 <p>Meiseikai healthcare foundation</p>
Local Government	 <p>Ichikawa Town Hall, Hyogo Prefecture</p>	 <p>Itami City Hall, Hyogo Prefecture</p>	 <p>Tamba City Hall, Hyogo Prefecture</p>
Culture and Education	 <p>The University of Electro-Communications</p>	 <p>Shujitsu High School and Junior High School (Shujitsu Gakuen)</p>	 <p>Toyohashi University of Technology</p>
Manufacturing and Enterprise	 <p>S&B Foods Inc.</p>	 <p>AGC Inc. Sagami Plant</p>	 <p>ZTV Co., Ltd.</p>

Go here for more information. >>> <https://www.alliedtelesis.com/success-stories> 

 **For safety**
Please be sure to read the attached manual and use the product correctly.

● CentreCOM, SwitchBlade, Secure EnterpriseSDN, AMFframework, AMFPlus, VCStack, EPSRing, LoopGuard, AlliedView, AT-Vista Manager, AT-VA, AT-AWC, AT-UWC, Allied Telesis Unified Wireless Controller, EtherGRID, Envigilant, Net.Service, Net.Cover, Net.Monitor, Net.Assist, Allied Hikari, Net.CyberSecurity, and Net.Campus are registered trademarks of Allied Telesis Holdings K.K. ● Other company names and product names are either trademarks or registered trademarks of each company. ● Product specifications, appearances, standard prices, and other information listed are subject to change without notice. ● If Allied Telesis products are taken outside of Japan or provided to a non-resident, as described in the Foreign Exchange and Foreign Trade Act, it is assumed that the customer agrees to comply fully with the export-related legislation of the government of Japan, including the Foreign Exchange and Foreign Trade Act, as well as that of foreign governments, and that all necessary procedures will be carried out at the responsibility and cost burden of the customer. ● These products are intended for use in Japan and, if taken outside of Japan, will not be covered by any product warranty or quality assurance guarantee, nor any kind of support or repair services. ● Photographs may differ from actual product colors due to printing. ● Listed details are as of September 2020. ● Unauthorized use, duplication, copying, modification, processing, reprinting, etc., of the materials herein is prohibited.



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