

Sehen Steuern Schützen

Marco Katzenmayer



1. Bestandsaufnahme
2. Lieschen Müller
3. Vista Manager EX
4. Dynamic Asset Management
5. Intelligent Edge Security
6. RADgate

Agenda



Bestandsaufnahme An was haben wir gedacht?

Sicherheit in meinem Netzwerk

1. Physische Sicherheit

- **Rechenzentrums-/Serverraum-Sicherung:**
- Zaunanlagen (Physischer Perimeter)
- Zutrittskontrollsysteme
- Überwachungskameras
- Alarmanlagen
- Brandschutz
- Löschanlage
- Unterbrechungsfreie Stromversorgung (USV)



2. Perimeter-Schutz

- **Firewall & Next-Generation Firewalls (NGFW)**
 - Der Türsteher am Tor ins Haus
- **Intrusion Detection/Prevention Systems (IDS/IPS)**
 - Einbruchserkennung und Verhinderung
- **VPN (Virtual Private Network)**
 - Verbindung meiner Niederlassungen und Mitarbeiter (Unterwegs/zur Hause)
- **Netzwerksegmentierung**
 - Bereiche im Netzwerk voneinander trennen



3. Endpunktsicherheit (Schutz der Geräte)

- **Endpoint Detection and Responds (EDR / Antivirus)**
 - Anti-Virensoftware auf den Endgeräten

- **Mobile Device Management (MDM)**
 - Welche Apps darf ich installieren und welche nicht.

- **Patch-Management**
 - Die Geräte sollen auf dem aktuellen Stand gehalten werden



4. Identitäts- und Zugriffsmanagement (IAM)

- **Zwei-Faktor-Authentifizierung (2FA/MFA)**
- Ein zweiter Faktor Ubikey, Smartphone, OTP wird benötigt für die Anmeldung.

- **Single Sign-On (SSO)**
- Erleichterung der Anmeldung an verschiedenen Systemen.

- **Rechte und Rollenkonzept**
- Die Rechte und Rollen sollen nur die nötigen Berechtigungen erhalten.



5. Datensicherheit und Resilienz

- **Backup:**
- **Regelmäßige, automatisierte Datensicherungen**
- **(idealerweise nach der 3-2-1-Regel.**
- 3 Kopien, 2 verschiedene Medien, 1 Kopie extern/offline

- **Verschlüsselung:**
- Einsatz von Verschlüsselung für Daten auf Datenträgern (at rest) und bei Übertragung (in transit)



6. Organisatorische Sicherheit & Awareness

- **Security Awareness Trainings:**
 - Sensibilisierung der Mitarbeiter um Phishing-Mails und Social Engineering zu verhindern (menschliches Versagen ist oft Ursache für Sicherheitsverletzungen)
- **IT-Sicherheitsrichtlinien**
 - Klare Regeln zur Nutzung von IT-Systemen
- **Penetration Testing**
 - Regelmäßige, simulierte Angriffe zur Identifikation von Schwachstellen



Lieschen Müller vom Sicherheitsdienst

- Lieschen Müller ist eine der zuverlässigsten Mitarbeiterinnen im Unternehmen. Seit Jahren arbeitete sie im Sicherheitsteam – ironischerweise zuständig für Zutrittskontrollen und Besucherverwaltung. IT-Sicherheit war dabei nie wirklich ihr Thema. „Dafür gibt’s doch die Kollegen aus der IT“.
- An diesem Morgen war alles ein bisschen anders. Ihr Dienstlaptop war am Wochenende kaputtgegangen, und da sie kurzfristig einspringen musste, griff sie kurzerhand zu ihrem privaten Notebook von zu Hause.
- Am Empfang angekommen, verband sie ihr Gerät direkt mit dem internen Netzwerk. Es funktionierte sofort...



Was sie nicht wusste:

- Ihr privates Gerät war bereits seit Tagen kompromittiert. Beim Herunterladen eines vermeintlich harmlosen PDF-Tools hatte sie unbemerkt Schadsoftware installiert. Diese wartete nur darauf, in ein größeres Netzwerk zu gelangen.
- Kaum war Lieschens Laptop verbunden, begann im Hintergrund ein stilles Schauspiel. Die Schadsoftware scannte das Netzwerk, suchte nach offenen Ports und schlecht gesicherten Systemen. Innerhalb weniger Minuten hatte sie erste Verbindungen zum Zutrittskontrollserver aufgebaut.
- Währenddessen saß Lieschen entspannt an ihrem Platz, trank Kaffee und lächelte Besucher an. „Alles ganz normal“, dachte sie.
- Doch im Netzwerk begann es zu rumoren. Ungewöhnlicher Traffic, merkwürdige Anfragen, steigende Last auf einzelnen Systemen. Die IT-Abteilung wurde nervös.
- „Wir sehen verdächtige Aktivitäten aus dem internen Netz“, sagte einer der Administratoren. „Das kommt nicht von außen.“



Die Spur führte schnell zurück zum Empfang.

Als die IT schließlich bei Lieschen stand und sie baten, ihr Gerät sofort vom Netzwerk zu trennen, war sie völlig überrascht. „Ich habe doch gar nichts gemacht!“

Lieschen hatte nichts aktiv falsch gemacht – aber sie hatte auch nichts hinterfragt. Kein sicheres Gerät, keine Überprüfung, keine Einschränkungen im Netzwerk. Ihr gut gemeinter Einsatz hatte eine Sicherheitslücke geöffnet, die das gesamte Unternehmen gefährdete.

Am Ende konnte der Vorfall zwar eingedämmt werden, aber der Schaden war schon da. Systeme mussten neu aufgesetzt, Daten überprüft und Sicherheitsmaßnahmen verschärft werden.

Für Lieschen war es eine harte Lektion. Für das Unternehmen auch.

Denn sie hatten gelernt:

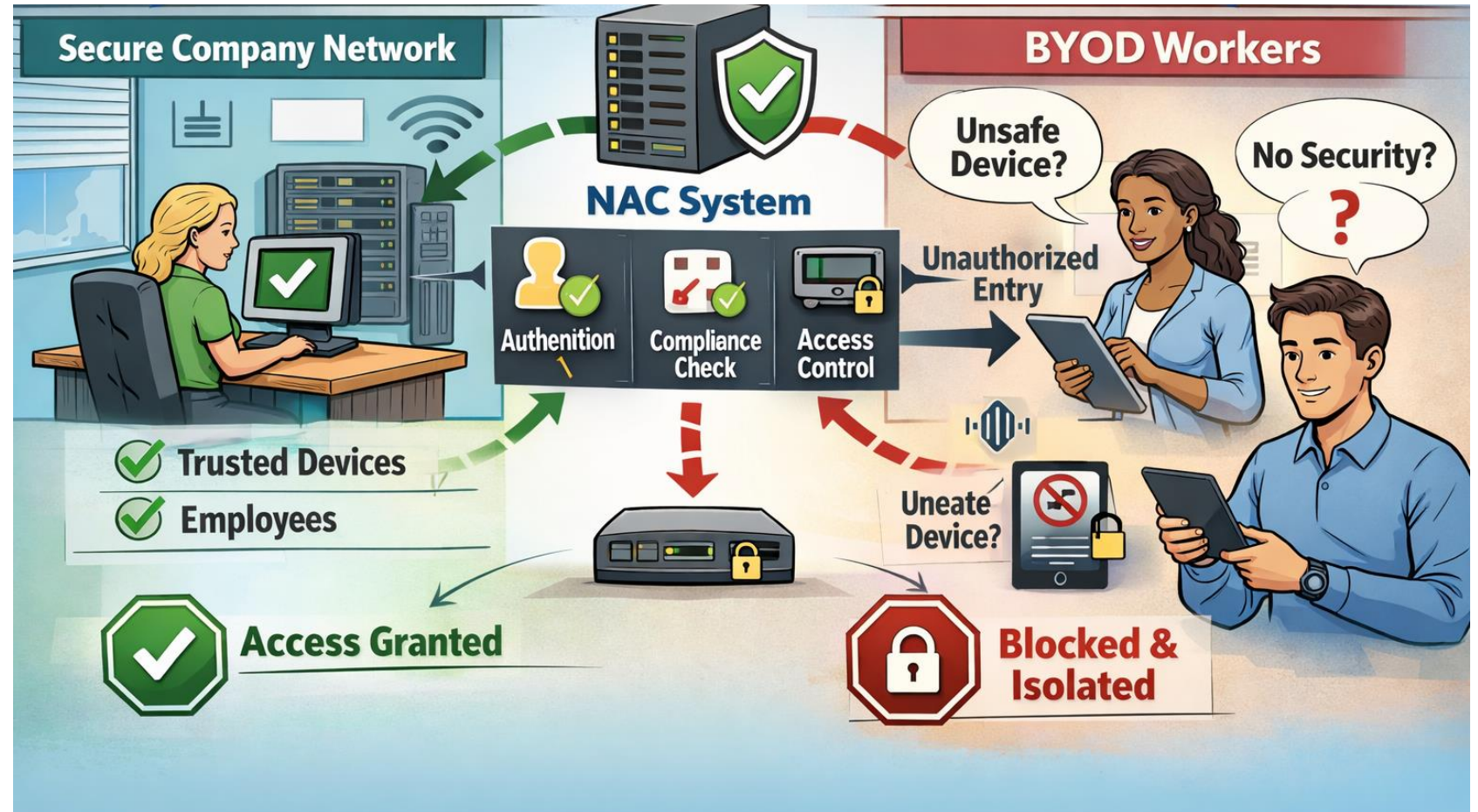
Nicht nur Angreifer von außen sind ein Risiko – manchmal reicht ein einziger unbedarfter Moment im Inneren.



BYOD

Private Hardware:

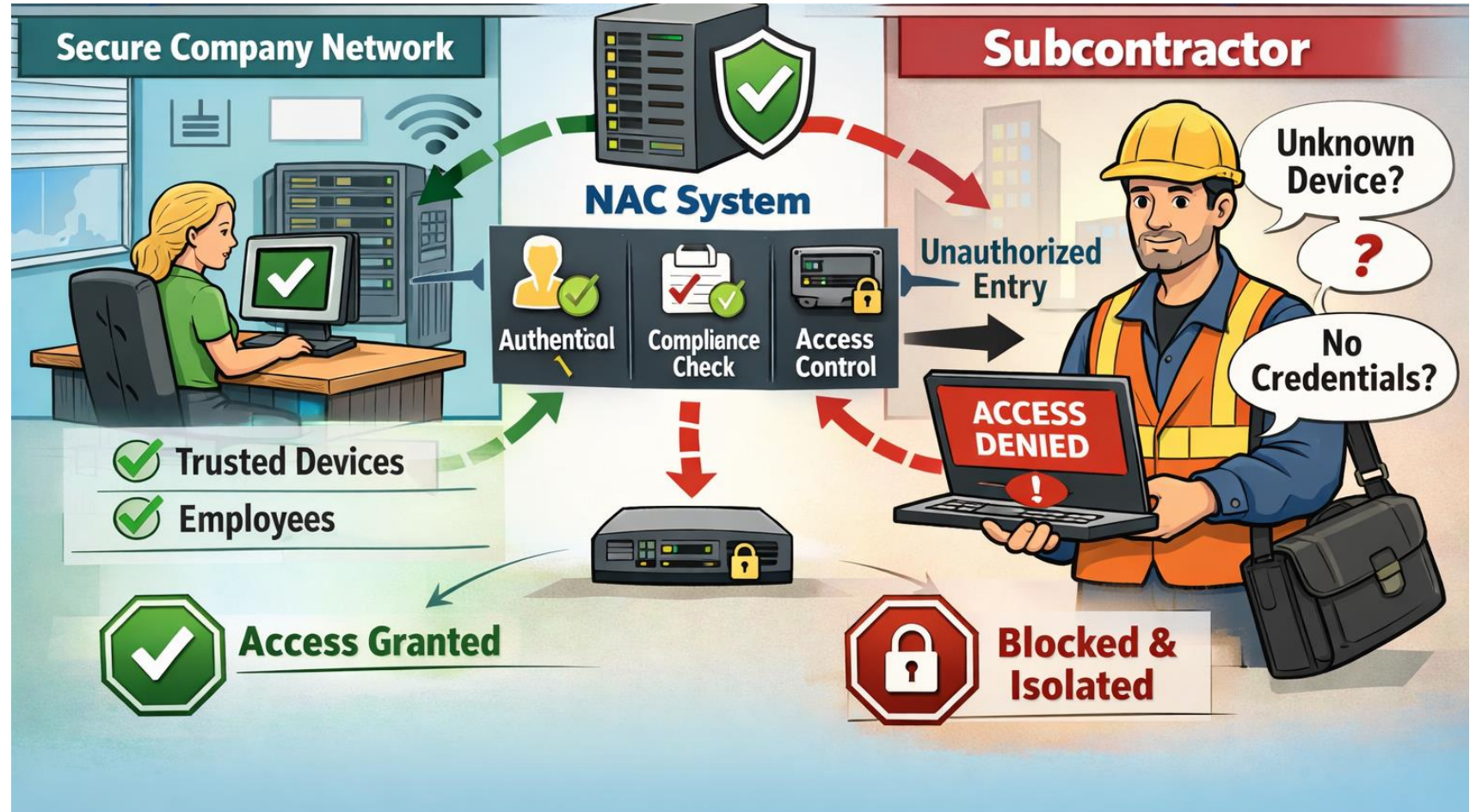
- Notebooks, Tablets,
- Router mit WLAN
- IoT-Geräte,
- Spielekonsolen
- Internet-Radios
- Smart-Home-Hubs
- Sprachassistenten
- Smart-TV



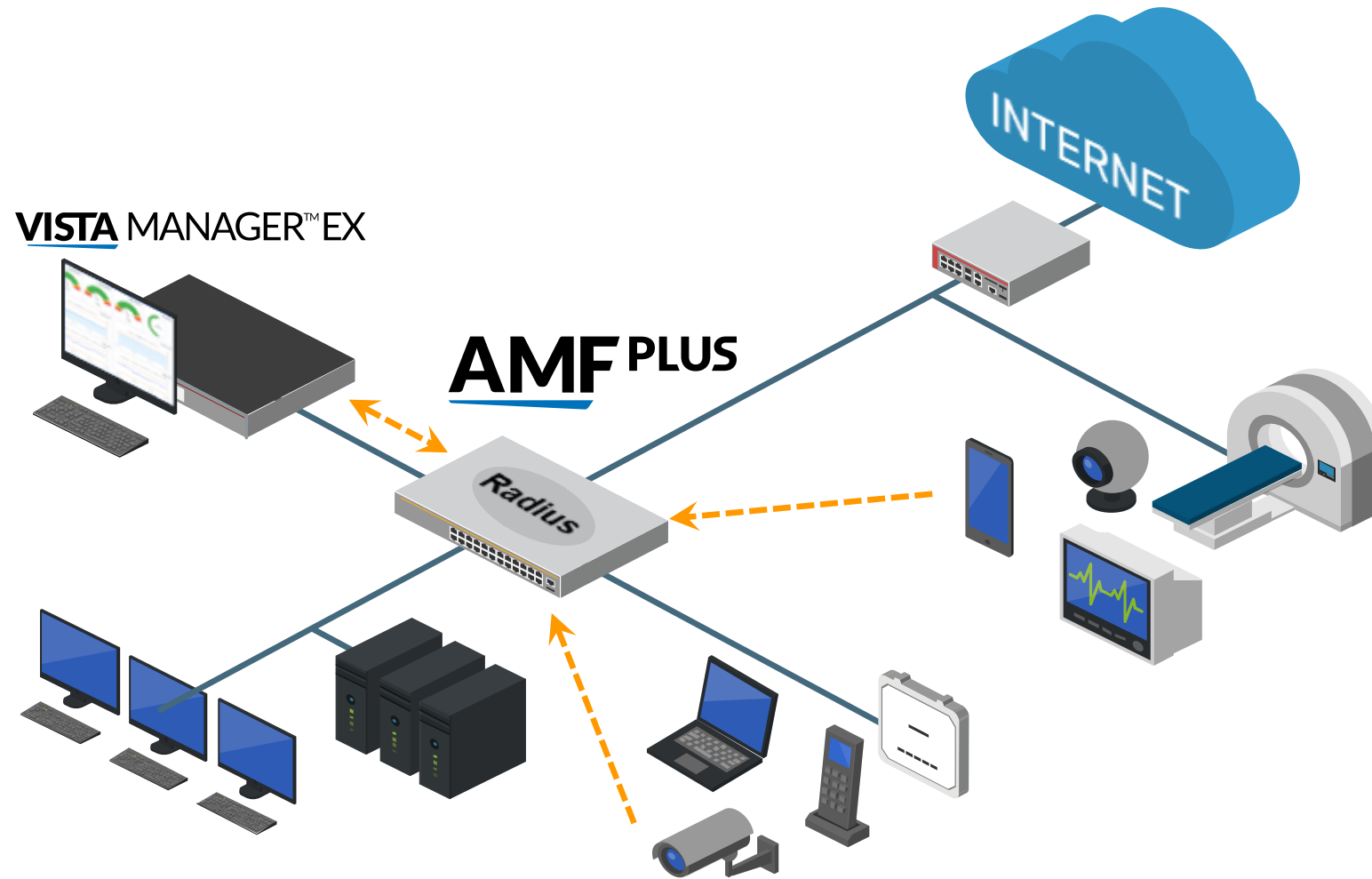
“Gast oder Fremdfirmen”

Gäste

- Wartung
- Montage
- Reinigung
- Sicherheitsdienst
- Logistik
- Entsorgung
- Catering



Wir können mehr...



A decorative background on the left side of the slide featuring a network diagram. It consists of numerous small grey dots (nodes) connected by thin grey lines, forming a complex, interconnected web that tapers off towards the right.

Vista Manager EX

Network Access Control



Vista Manager EX and RADIUS Server

Enable RADIUS Server

Allied Telesis | Vista Manager EX | amf | 192.168.1.11

14 Devices | 13 Up | 1 Down

Search network

manager

Search name or IP address

The diagram illustrates a network configuration. A RADIUS server (radgate) is connected to Vista Manager EX. Vista Manager EX is connected to a switch (swi01), which is highlighted with a blue box. A context menu is open over swi01, showing options: Sites, Groups, Manage Device, Backup Device, SSH to Device, Loop Protection, Enable RADIUS Server (highlighted in red), and Undo Merge Device. Other devices in the network include TQ6702gen2-R, TQ7403-R, AMF-CLOUD, and rtr01. The network is labeled 'Demo'.



Vista Manager EX and RADIUS Server

Manage RADIUS Server

Vista Manager EX | amf | 192.168.1.11

manager ▾

- Dashboard
- Network Map
- Health Monitoring AMF+
- Events
- Asset Management
- Network Services
 - Access Control
 - Service Monitoring
 - RADIUS
- Intent Networks
- WAN
- AWC Plug-in
 - Wireless Monitoring
 - Wireless Configuration
 - Wireless Maintenance
- Device Search
- System Setting
- SNMP Plug-in
- User Management
- System Management

RADIUS Server ?

Shared Secret
+ Add External Server

Devices

radgate
swi01

swi01
Users Groups NAS

All Time (No filter applied)
All Groups ▾

Assign User(s) To Group
Delete Selected Users

<input type="checkbox"/>	User [▲]	Successful Logins	Failed Login Attempts	Group	Conflict	Reject Status	Last Interaction Time	Action
<input type="checkbox"/>	00-04-7d-40-d9-0d	577	0	Group-VLAN6			11:24:04 2026-04-17	⋮
<input type="checkbox"/>	00-40-84-f2-94-6a	138	0	Group-VLAN6			10:29:31 2026-04-17	⋮
<input type="checkbox"/>	00-40-8c-ca-5f-1d	81	0	Group-VLAN7			10:29:27 2026-04-17	⋮
<input type="checkbox"/>	0c-37-96-14-f4-b2	562	0	Group-VLAN1			18:13:55 2026-04-16	⋮
<input type="checkbox"/>	10-98-19-a3-89-b8	2514	0	Group-VLAN1			11:23:55 2026-04-17	⋮
<input type="checkbox"/>	user1	0	0	Group-VLAN2			14:51:50 2026-04-07	⋮

1 to 6 of 6
⏪ <
Page 1 of 1
> ⏩

©2025 Allied Telesis, Inc. All rights reserved.

18

Innovation und Sicherheit in Einklang bringen

- **Geräteerkennung**

- Zentrale Verwaltungsliste
 - Gerätebestand
- Unterstützung verschiedener Hersteller
 - Auditberichte

- **Selbstschutz**

- Umfassende Zugriffskontrolle
- Verhinderung von Abhör- und Manipulationsversuchen
 - Agentloser Schutz

- **Optimieren und automatisieren**

- Intelligente Zugriffskontrolle (ACLs) zur Erhöhung der Sicherheit
- QOS zur Verbesserung der Leistung
- Echtzeitüberwachung des Netzwerkzustands



**Dynamic
Asset Management**



**Intelligent
Edge Security**



**Network
Visibility & Control**

A decorative background on the left side of the slide featuring a network diagram. It consists of numerous small grey dots (nodes) connected by thin grey lines, forming a complex, interconnected web that tapers off towards the right.

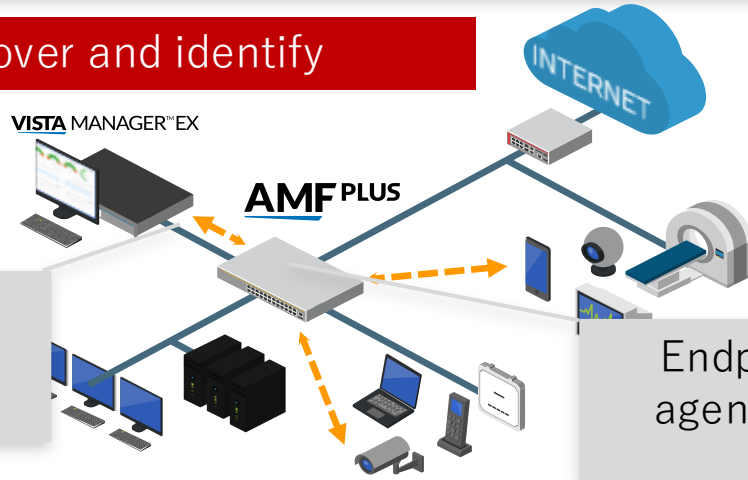
Dynamic Asset Management

Network Access Control



AMF Plus – DAM (Dynamic Asset Management)

Discover and identify



Options of discovery
SNMP, API

Endpoint without agent : LLDP, DHCP, DOT1X

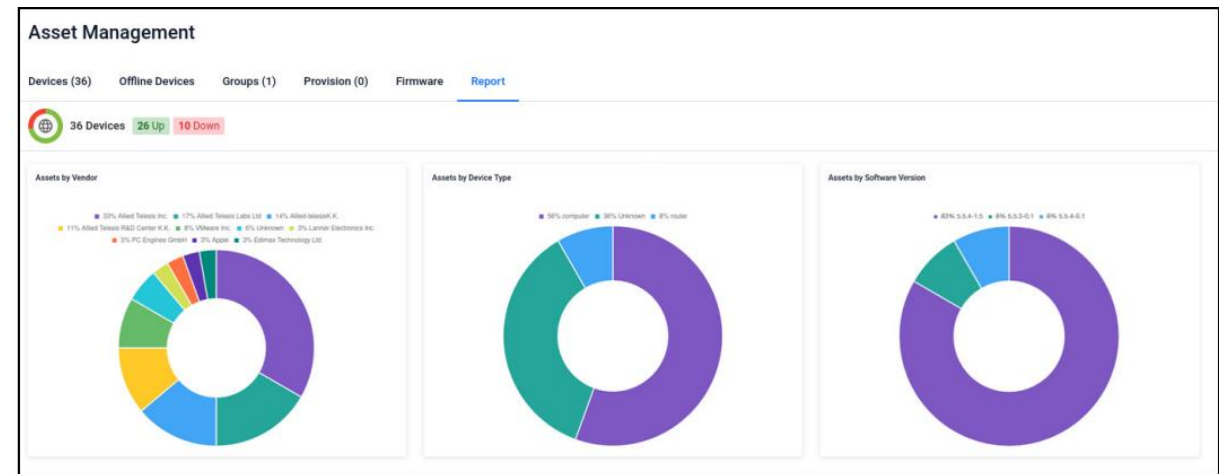
STOAT (Standardized Topology Organizer & Transport)

The screenshot shows the AMF Plus interface with a network map on the right and device details on the left. The network map displays a central switch connected to various devices like an Environmental-Sensor, Security-Camera, IP-Phone, Printer, and Windows-Server. The device details panel on the left shows information for a Windows-Server, including its status, management address, MAC address, and vendors.

Dynamic inventory

Device Name	IP Addresses	Status	Device Type	MAC Addresses	License Stat.	Icon	Action
Windows-Server	169.254.72.202	Normal	-	0015.5d11.3e11	-		⋮
TQR-AMFPLUS-DEMO	172.16.206.100	Normal	AT-T06702 GEN2-R	0003.7fba.cb4d	Active		⋮
sta-c8-94-02-10-60-13	169.254.221.99	Normal	-	c894.021d.6013	-		⋮
Security-Camera	172.16.207.151	Normal	-	000a.4427.d9e5	-		⋮
ROUTER-AMFPLUS-DEMO	10.36.150.33	Normal	AR4050S	0000.cd38.ecea	Active		⋮
Printer	172.16.207.150	Normal	-	000a.cd37.0003	-		⋮
Office-5	10.38.117.12	Normal	-	e01a.ea70.8563	-		⋮
Management-Switch	10.38.117.23	Normal	-	e01a.ea67.336a	-		⋮
linuxclient2	172.16.201.57	Normal	-	0015.5d11.3e0e	-		⋮
linuxclient1	172.16.201.56	Normal	-	0015.5d11.3e0d	-		⋮

Details of terminals using third-party systems



A background graphic on the left side of the slide, consisting of a complex network of interconnected nodes and lines, resembling a mesh or a web structure, rendered in a light gray color.

Intelligent Edge Security

Network Access Control



AMF Plus – IES (Intelligent Edge Security)

VISTA MANAGER™ EX Control Radius

Allied Telesis | Vista Manager EX | EMEA_Demo | 192.168.185.2 | manager

Local RADIUS Server Shared Secret

Stack-x550-28XSQ Export Certificate

Users Groups NAS

All Groups + Add User

Assign user(s) to group Delete Selected Users

<input type="checkbox"/>	User	Group	Reject Status	Action
<input type="checkbox"/>	4c-d7-17-73-f3-9c	Video		⋮
<input type="checkbox"/>	d4-be-d9-6b-3c-86	Video		⋮

Group
For dynamic VLAN

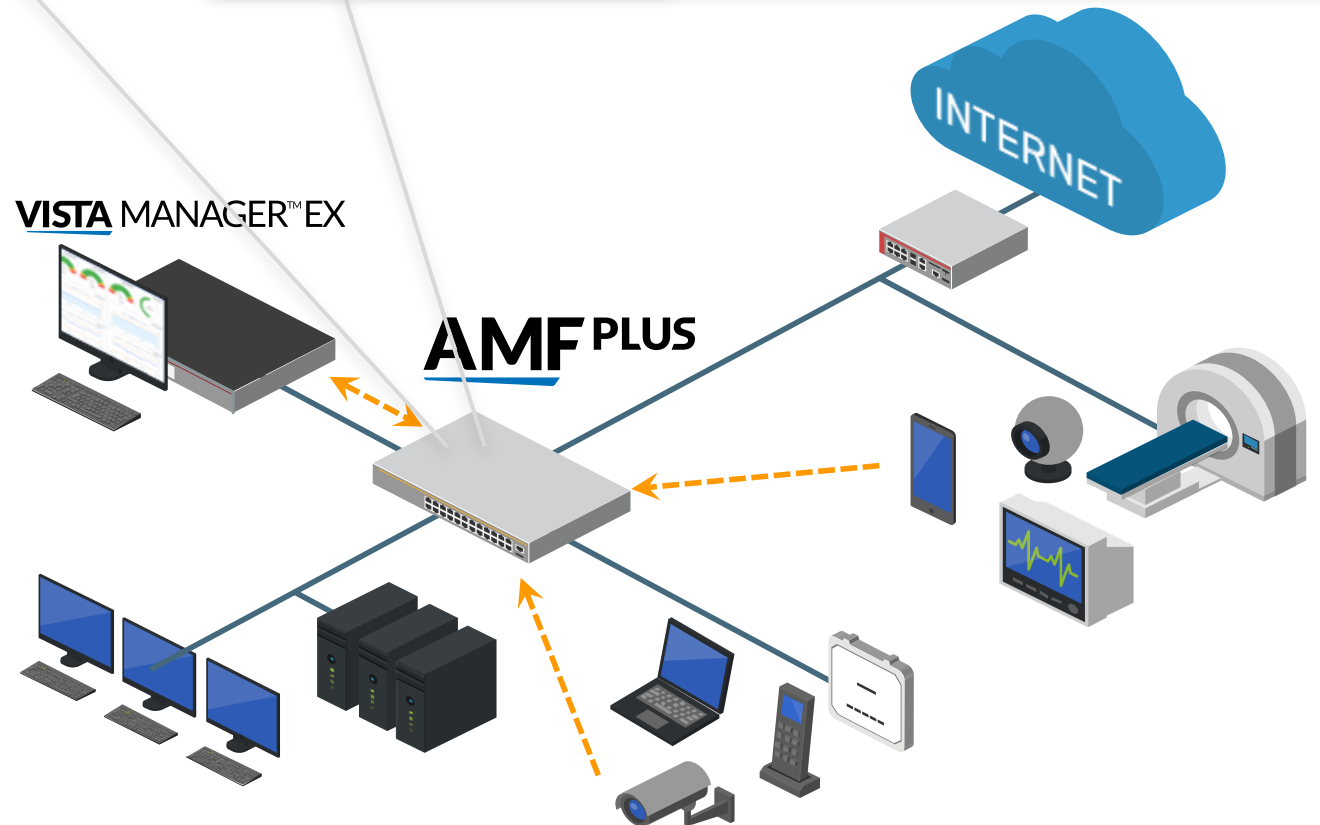
Add a Group ×

Name *

VLAN

Switch Radius Local
Authentication of devices

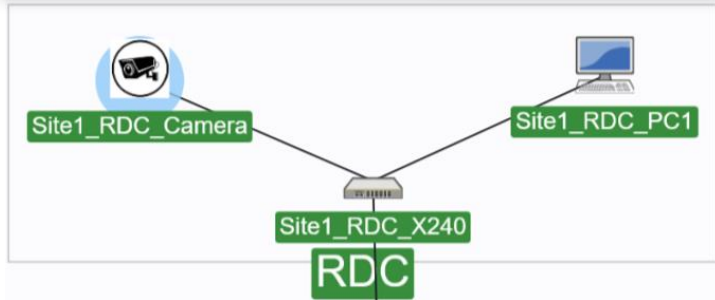
xSeries
Standard 100 Users
Premium License 5000 Users



AMF Plus – IES

VISTA MANAGER™ EX

Topology MAP



VISTA MANAGER™ EX

Endpoint management

Asset Management

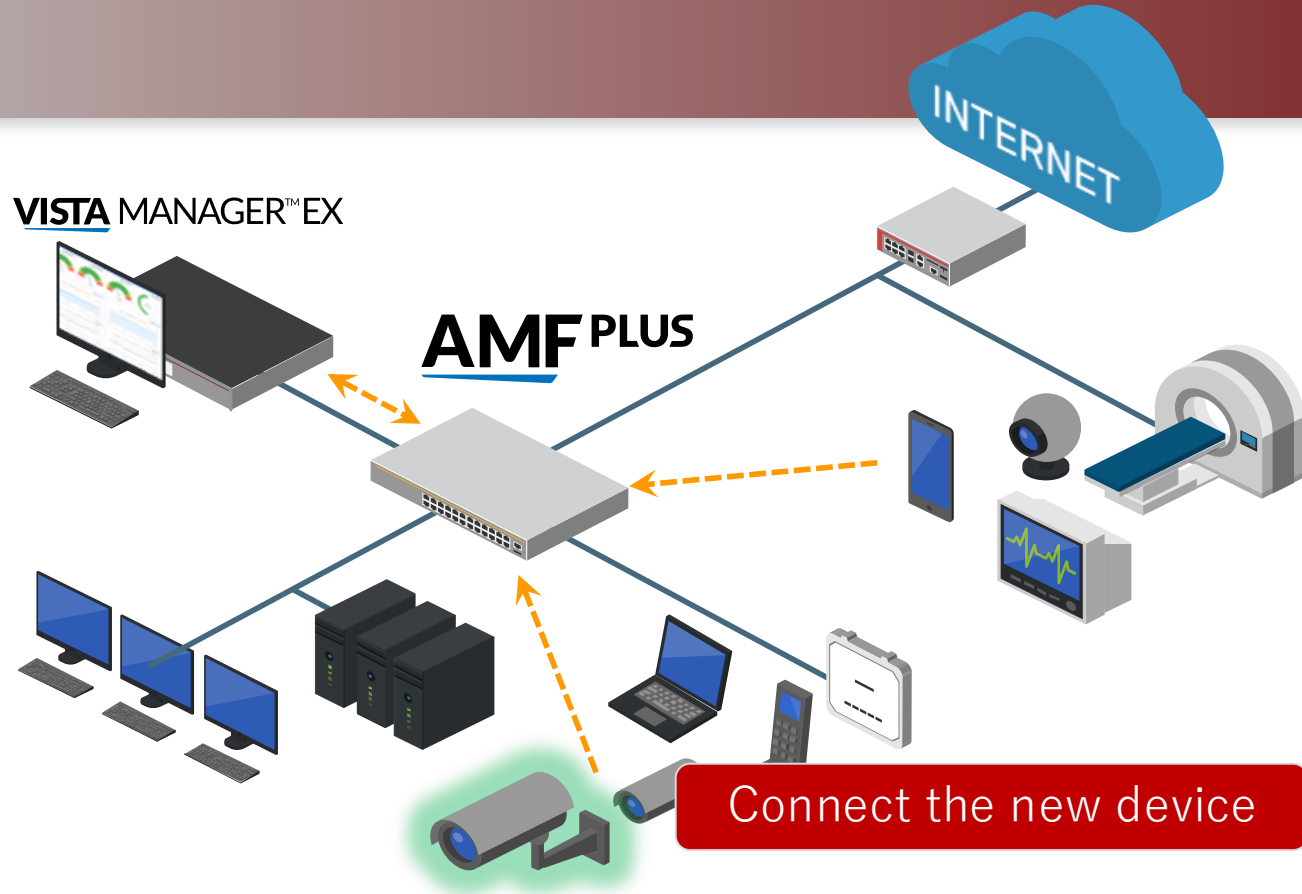
Devices (16) Endpoints (6) Offline Devices (0) Groups (5) Provision (0) Firmware Report

Block Selected Allow Selected Search by keyword

<input type="checkbox"/>	MAC Address	RADIUS Username	RADIUS Server Hostname	NAS Hostname	Status	Authentication	Vendor	Icon	Action
<input type="checkbox"/>	98e7.4389.abb6	98-e7-43-89-ab-b6	Site1_S1_X550	Site1_RDC_X240	Allowed	Authenticated	Dell Inc.		<input type="button" value="Block device"/> <input type="button" value="Allow device"/>

VISTA MANAGER™ EX

AMF PLUS



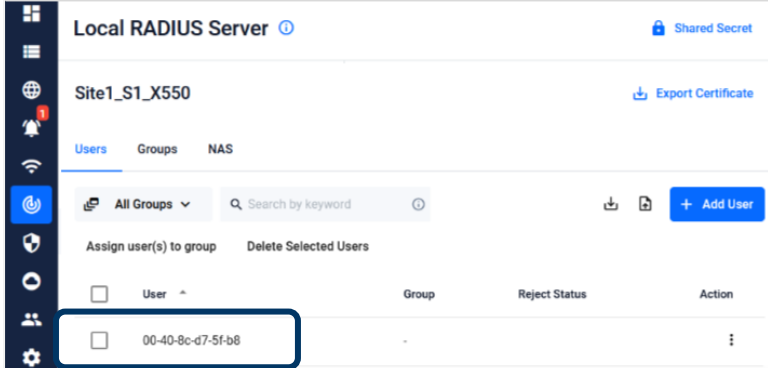
Connect the new device

What should I do?



AMF Plus – IES

Automatic new entry
in the Radius server



VISTA MANAGER™ EX

Endpoint management

Asset Management

Devices (16) Endpoints (6) Offline Devices (0) Groups (5) Provision (0) Firmware Report

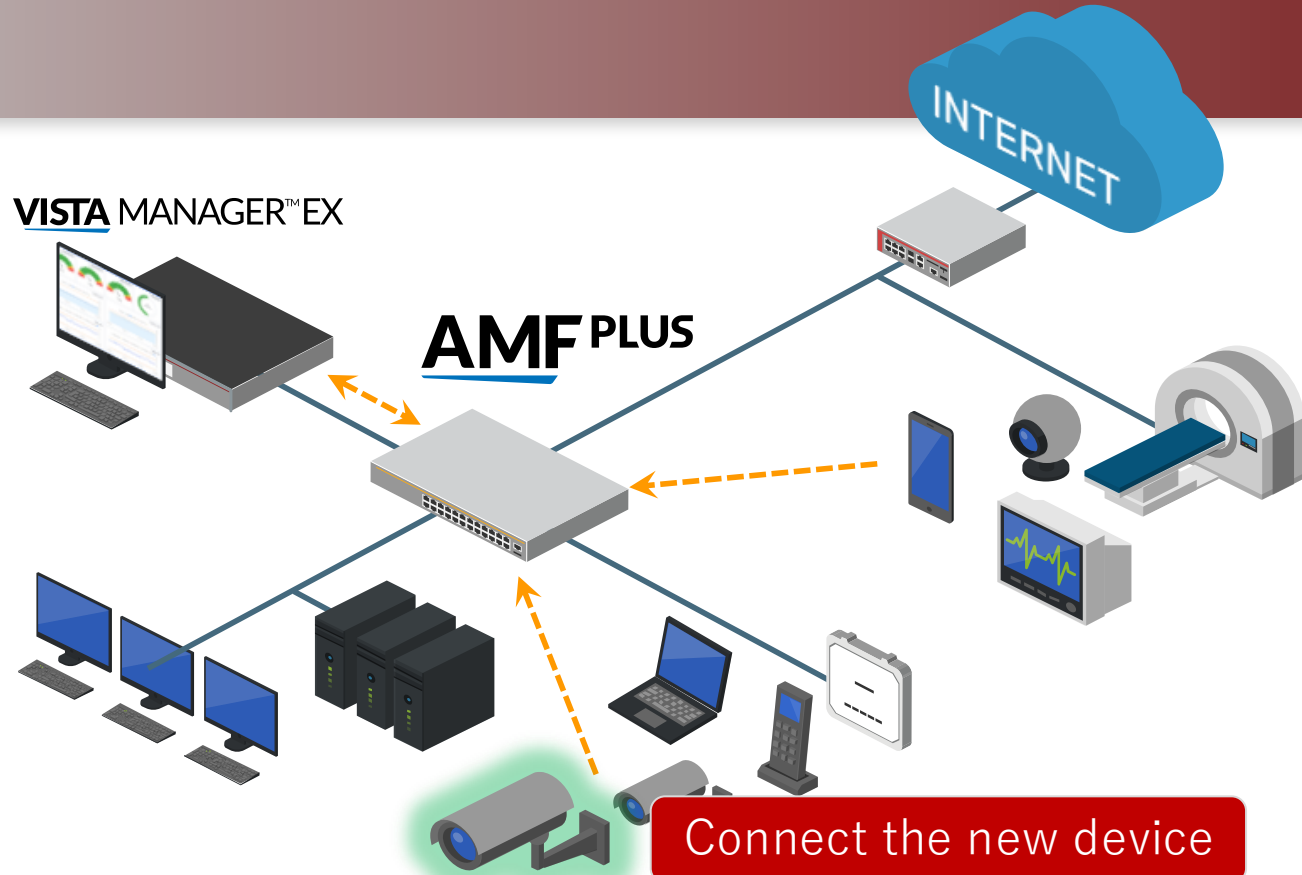
Block Selected Allow Selected Search by keyword

MAC Address	RADIUS Username	RADIUS Server Hostname	NAS Hostname	Status	Authentication	Vendor	Icon	Action
98e7.4389.abb6	98-e7-43-89-ab-b6	Site1_S1_X550	Site1_RDC_X240	Allowed	Authenticated	Dell Inc.		
0040.8cd7.5fb8	0040.8cd7.5fb8	Site1_S1_X550	Site1_RDC_X240	Allowed	Authenticated	Axis Communications AB		Block device Allow device

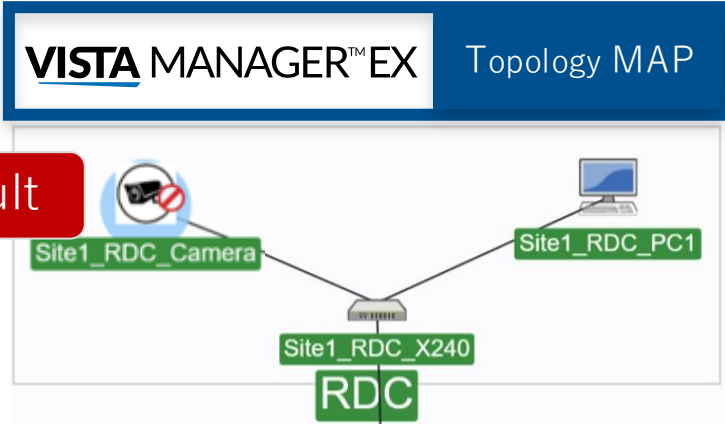
It's a new camera

VISTA MANAGER™ EX

AMF PLUS



AMF Plus – IES – Block a Device



VISTA MANAGER™ EX Endpoint Management

Asset Management

Devices (13) **Endpoints (8)** Offline Devices (0) Groups (5) Provision (1) Firmware Report

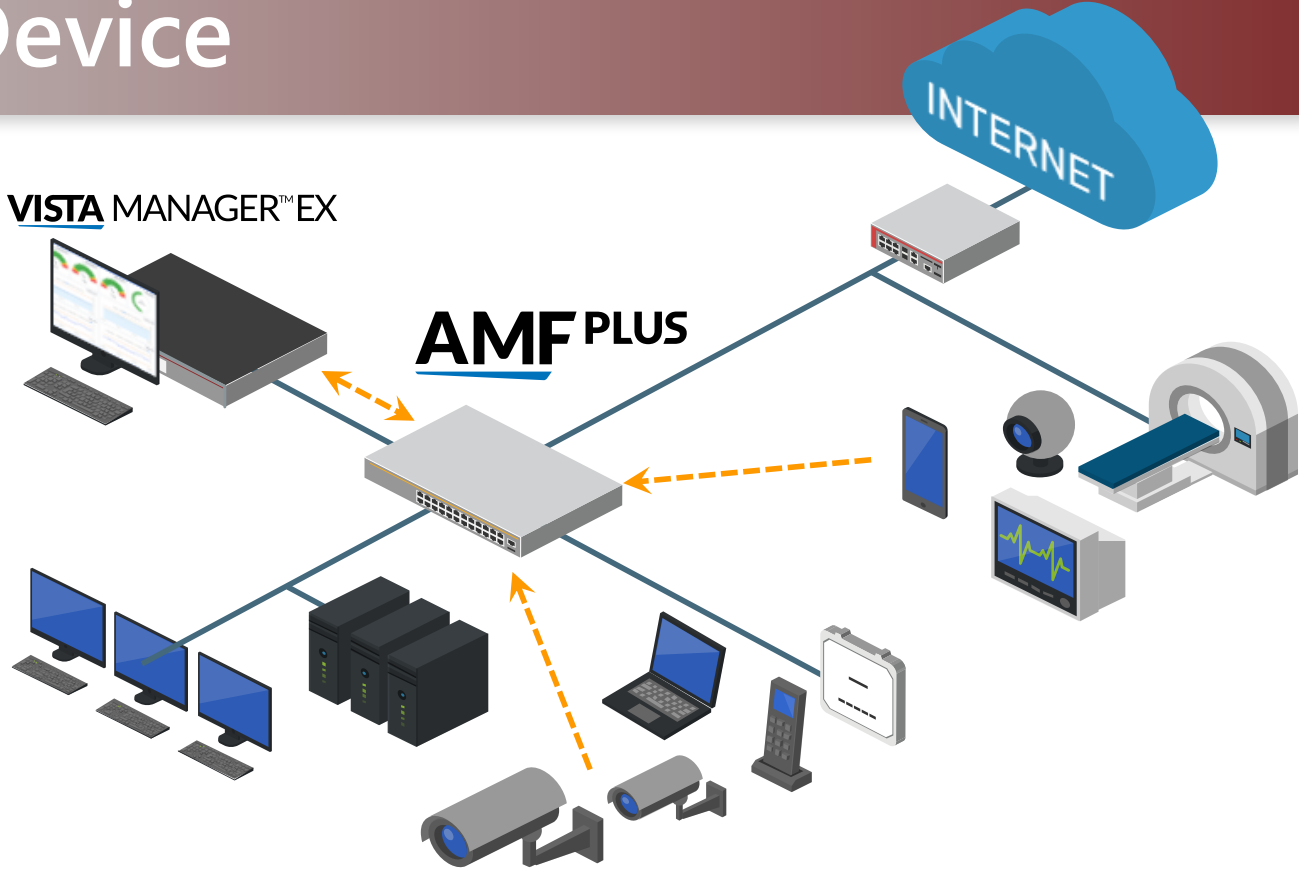
Block Selected Allow Selected Search by keyword

<input type="checkbox"/>	MAC Address	RADIUS Username	RADIUS Server Hostn...	NAS Hostname	NAS Interface	Status	Authenticat...	Icon	Action
<input type="checkbox"/>	e0db.55e7.d6d2	e0-db-55-e7-d6-d2	Site1_S1_X550	Site1_RDC_X240	port1.0.17	Allowed	Authenticated		⋮
<input type="checkbox"/>	0040.8cd7.5fb8	00-40-8c-d7-5f-b8	Site1_S1_X550	Site1_RDC_X240	port1.0.18	Blocked			⋮

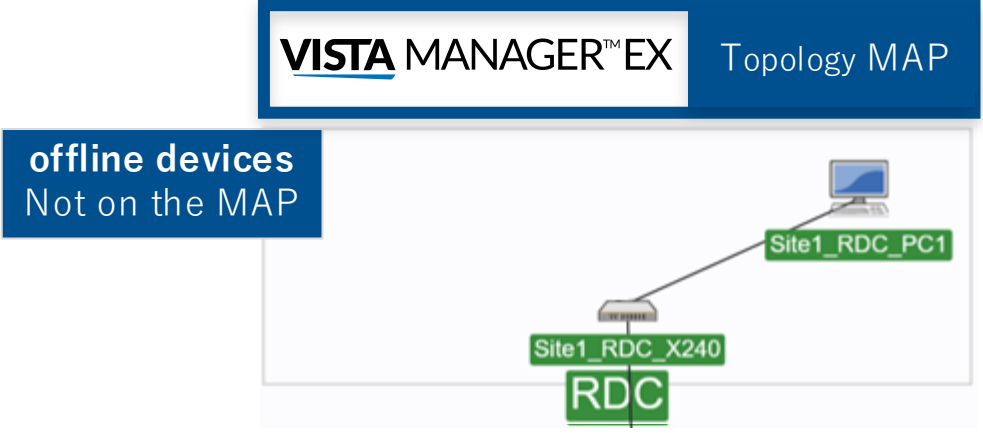
Result

Block device
Allow device

Action on the device



AMF Plus – IES – Identification of offline devices



VISTA MANAGER™ EX Offline devices Management

Asset Management

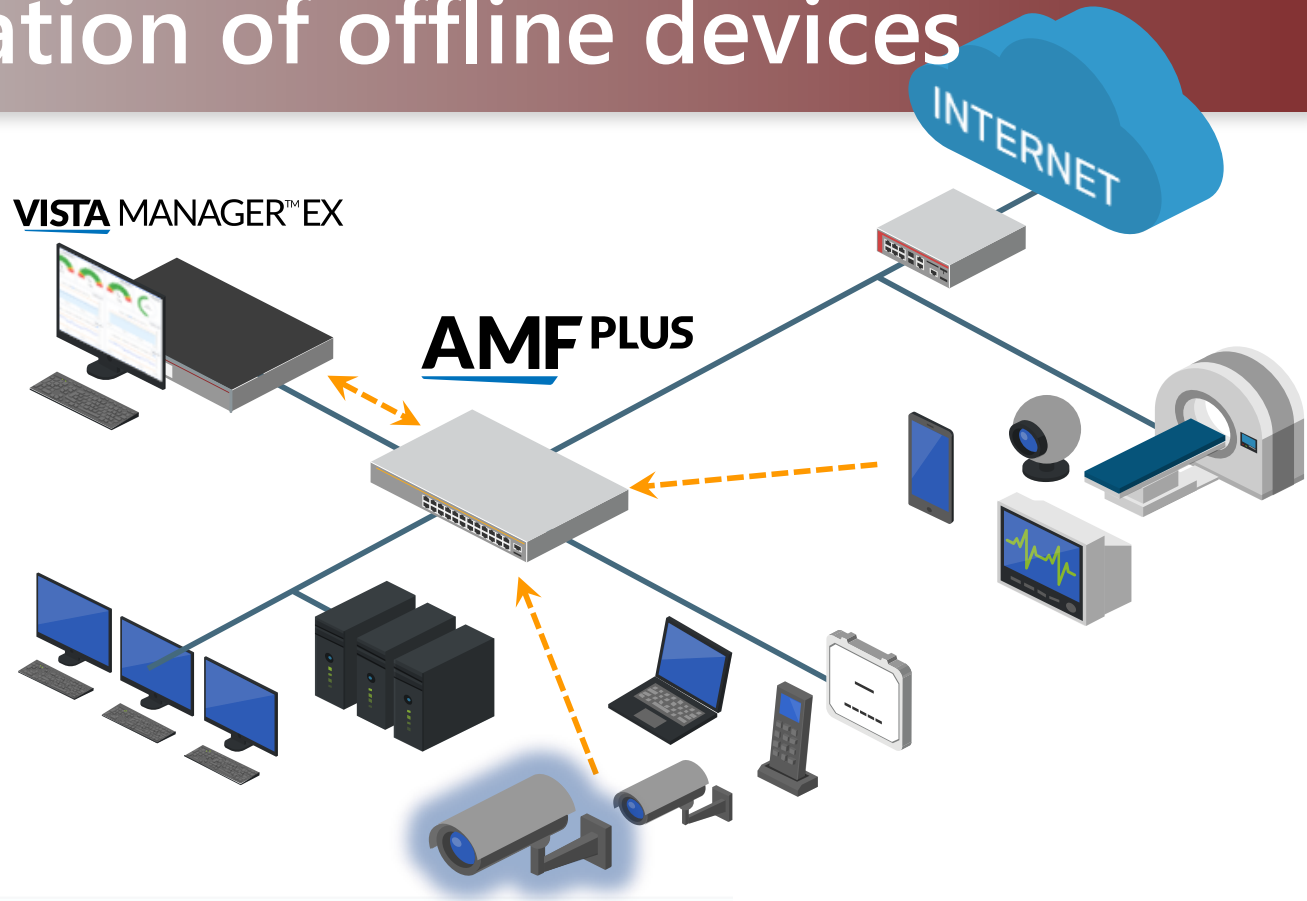
Devices (15) Endpoints (9) **Offline Devices (1)** Groups (5) Provision (0) Firmware Report

Search by keyword

Delete Selected Delete All

<input type="checkbox"/>	MAC Address	Device Name	Vendor	Last Disconnect Time	Action
<input type="checkbox"/>	0040.8cd7.5fb8	0040.8cd7.5fb8	Axis Communications AB	01:51:02 2025-02-18	⋮

Enabled





RADgate

Network Access Control



RADgate

- Die RADIUS-Server-Anwendung von Allied Telesis (AT-RADgate) ermöglicht die Benutzerauthentifizierung und die Netzwerkzugangskontrolle.
- Als Plug-in für Vista Manager werden Benutzer- und Endgeräteinformationen nahtlos integriert, um eine zentralisierte Verwaltung im Einklang mit den Sicherheitsrichtlinien des Unternehmens zu ermöglichen.



Self
Defending
Network

VISTA MANAGER™ EX

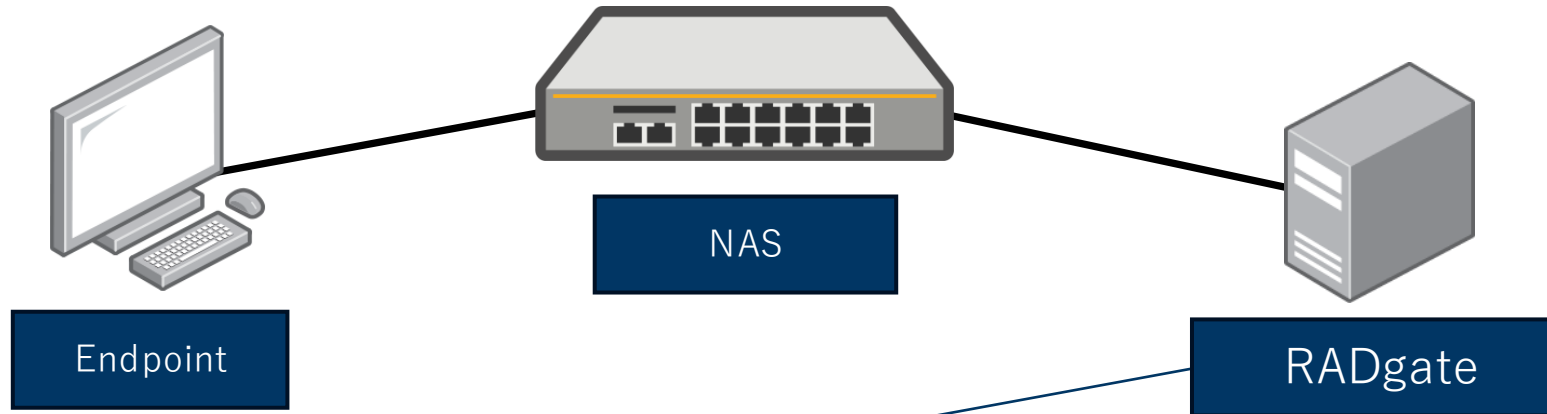


RADIUS Server plug-in

- **Authentifizierungsserver**
- **Zentrale Verwaltung:**
 - Benutzer, Endgeräte und NAS
 - Zwei-Faktor-Authentifizierung
 - Netzwerkzugriffsregeln
- Lokal oder mit Active Directory



Endpoint Authentifizierung



The screenshot shows the 'Policy Management' section of the web interface. The left sidebar contains a menu with items: Policy Management, Status Monitor, Event Management, Account Management, RADIUS Management, and System Management. The main content area has tabs for 'User', 'Endpoint', 'NAS / RADIUS Proxy', 'NAS Profile', 'Supplicant Profile', and 'Global'. The 'Endpoint' tab is selected. Below the tabs is a search bar and a table with columns: MAC Address, Device Name, Access Level, Tag, and Note.

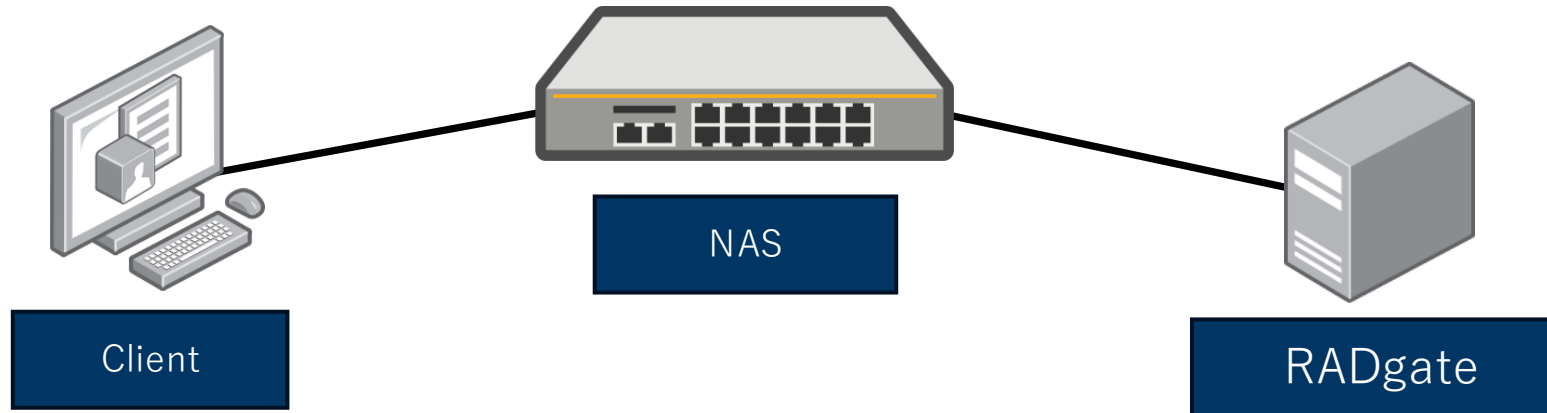
MAC Address	Device Name	Access Level	Tag	Note
0040.8cd7.5fb8	Video			
d4be.d96b.3c86	DESKTOP-NVAKUKO			

The screenshot shows the 'Policy Management' section of the web interface. The left sidebar contains a menu with items: Policy Management, Status Monitor, Event Management, Account Management, RADIUS Management, and System Management. The main content area has tabs for 'User', 'Endpoint', 'NAS / RADIUS Proxy', 'NAS Profile', 'Supplicant Profile', and 'Global'. The 'Supplicant Profile' tab is selected. Below the tabs is a search bar and a table with columns: Name, Priority, Action, and Reason.

Name	Priority	Action	Reason
Supplicant_Pass	7	Pass	Pass devices that I know
Supplicant_Undecide	7	Undecide	Undecide devices that I don't know



Benutzer Authentifizierung



The screenshot shows the web interface for AT-RADgate. The left sidebar contains navigation options: Policy Management (selected), Status Monitor, Event Management, Account Management, RADIUS Management, and System Management. The main content area is titled 'Policy Management' and includes a search bar and a table of users.

User	Endpoint	NAS / RADIUS Proxy	NAS Profile	Supplicant Profile	Global
Search by keyword					
Login Name	Full Name	Access Level	Tag	Note	
matthieu	matthieu mirabel				
suzanne	suzanne airiau				



Globale parameter



- Benutzer



- Endpunkte



- NAS /
- RADIUS Proxy



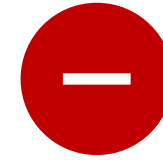
- NAS Profile



Default Regeln



- Endpunkt **ist** in der lokalen Datenbank



- Endpunkt **ist nicht** in der lokalen Datenbank

The screenshot displays the AT-RADgate web interface. The left sidebar contains navigation options: Policy Management (selected), Status Monitor, Event Management, Account Management, RADIUS Management, and System Management. The main content area is titled 'Policy Management' and includes tabs for User, Endpoint, NAS / RADIUS Proxy, NAS Profile, Supplicant Profile (selected), and Global. A search bar labeled 'Search by keyword' is present. Below the search bar is a table with columns: Name, Priority, Action, Reason, and Note. A '+ Add' button is located in the top right corner of the table area. The user 'manager' is logged in.



Supplicant Profile

Add Supplicant Profile

Name* [Max 63 characters]

Priority* [1-15]

Condition

Device

- All endpoints
- Registered devices
- Unregistered devices
- Specified by MAC address
- Specified by name

Settings

Action*

Filter ID [Max 255 characters]

Filter Rule [Max 1024 characters]

Additional Information

Reason [Max 63 characters]

Cancel

Add Supplicant Profile

Priority* [1-15]

Condition

Device

Access Level

Tag [Max 255 characters]

Settings

Action*

- Pass
- Drop
- Isolate
- Undecide
- Notice

Additional Information

Reason [Max 63 characters]

Note [Max 63 characters]

Cancel



RADIUS Management

• Proxy Settings

- RADIUS Proxy function
- Proxying CoA/Disconnect packets is not supported
- Creation of Proxy rules to forward packets to different servers

• Active Directory

- User authentication with AD information
- AD and LDAP Servers authentication cannot be used together

• LDAP Server

- User authentication with LDAP information
- Authentication protocol PAP or EAP-TTLS
- Only Windows Active Directory servers



Certification Authority Management

- Locale CA mit SSL Zertifikatsmanagement

CA Management

Certificate Certificate profile User Cert Issue Tool

<input type="checkbox"/>	Status	Common Name (CN)	Effective ...	Expiry Da...	
<input type="checkbox"/>	Valid	suzanne	2025-12-22	2035-12-20	⋮

Revoke



Vista Manager EX

Enable AT-RADgate in Vista Manager EX

The screenshot shows the 'System Management' page in Vista Manager EX. The left sidebar contains navigation options: Dashboard, Network Map, Health Monitoring (AMF), Events, Asset Management, Network Services, Intent Networks, WAN, AWC Plug-in, SNMP Plug-in, User Management, and System Management (selected). The main content area is titled 'System Management' and includes a 'Tech Support' button. Under 'Optional Features', several features are listed with their status and descriptions:

- Record Randomized MAC Addresses:** Enabled. Description: Display devices with randomized MAC addresses such as mobile phones in Network Map and Asset Management. Warning: This feature will increase the number of visible devices in the Network Map and may reduce performance.
- Convert Syslog Security Messages:** Disabled. Description: Convert syslog security messages from third party applications into dismissable alarms/events on the event log.
- AT-RADgate:** Enabled. Description: AT-RADgate provides Authentication Services that comply with the IETF RADIUS standard. It is deployed on a container instance of the ACP system. You can add external AT-RADgate servers from the Radius feature page. Warning: This feature may impact system performance. Disabling the feature will stop Vista Manager from communicating with any added AT-RADgate servers while the servers will continue to operate.
- Advanced Monitoring:** Disabled. Description: Visualize data sourced from third-party monitoring agents in Health Monitoring dashboards. Warning: This feature may impact system performance. Each device with Advanced Monitoring enabled will increase the system's storage requirements and the time required for data retrieval.
- Bookmarks:** Disabled. Description: Display external links in the main menu.
- Vista Manager EX API:** Disabled. Description: Access Vista Manager EX content in external applications. Warning: Regenerating the token will invalidate the current token.

Add AT-RADgate

The screenshot shows the 'RADIUS Server' configuration page in Vista Manager EX. The left sidebar is the same as in the previous screenshot. The main content area is titled 'RADIUS Server' and shows a table of configured RADIUS servers:

Device	Users	Groups	NAS
radgate			

Below the table, there is a search bar and a table of users:

Assign User(s) To Group	Delete Selected Users
<input type="checkbox"/> User	
<input type="checkbox"/> 00-0a-c6-09-07-ec	
<input type="checkbox"/> 34-6c-77-c6-2c-61	
<input type="checkbox"/> 56-6c-8f-a2-0a-bc	
<input type="checkbox"/> 64-bc-09-6b-3c-85	
<input type="checkbox"/> 6b-7e-b3-88-45-58	
<input type="checkbox"/> etc	
<input type="checkbox"/> suzanne	

Manage AT-RADgate

The screenshot shows the 'Network Map' page in Vista Manager EX. The left sidebar is the same as in the previous screenshots. The main content area is titled 'Network Map' and shows a network diagram. The diagram is a hierarchical tree structure representing a datacenter network:

- Backbone:** DC_BACKBONE_Back1, DC_BACKBONE_Back2
- Servers-Pr:** Proxmox-1, Proxmox-2, Proxmox-3
- Leaf:** DC_LEAF_Leaf1, DC_LEAF_Leaf2, DC_LEAF_Leaf3, DC_LEAF_Leaf4
- Spine:** DC_SPINE_Spine1, DC_SPINE_Spine2
- Border:** DC_BORDER_Border1, DC_BORDER_Border2
- OOB:** DC_OOB_Mgmt

The diagram shows connections between these components. A sidebar on the right provides options for managing the device: Sites, Groups, Manage Device, and Undo Merge Device. The main content area also shows basic information for the selected device (radgate):

- Discovery Source: SNMP Plug-in
- Status: Normal
- Management Addresses: 10.90.107.221
- Version: 1.1.1+1





Vielen Dank

Marco Katzenmayer
Sales Engineer