



Network Security Guidelines

Best practices and recommendations

About This Document

Purpose

The purpose of this document is to describe practical secure design and implementation of Alcatel-Lucent Enterprise switching, wireless, and network management system products using best practice recommendations.

Audience

The intended audience for this document includes customer and business partner networking professionals involved in the design and deployment of enterprise networks.

Scope

This document provides suggestions and best practices for adding and maintaining security of an OmniSwitch, Stellar WLAN, and OmniVista NMS network with secure configurations. Its scope is to provide general recommendations and best practices to be followed to support network administrators to securely design and configure their network, and will not cover every aspect of network and/or information security due to the diversity of information systems.

The functionality and features described in this document corresponds to the following releases:

- OmniSwitch AOS Release 8.10R2
- Stellar AWOS 5.0.1
- OmniVista 2500/Cirrus R4.9.1 / OmniVista Cirrus R10.4.3

For more details on the described functionalities, please refer to the configuration guides referenced in the [Related Documents](#) section.

Table of Contents

About This Document.....	2
Purpose	2
Audience	2
Scope	2
Introduction	5
Security at Alcatel-Lucent Enterprise	5
In-Depth Security Multi-Layered Approach	5
Secure By Design	6
Product Security Incident Response Team	7
General Security Recommendations	7
Updating Software Regularly	7
Control Physical Access.....	8
Training and Awareness	8
Switching Network Security.....	9
Management Plane	9
U-boot Access and Authentication	9
ONIE Authentication	9
Verify Image Integrity	9
Out-Of-Band Management	10
In-band Management (Management VRF)	10
Restrict Management Access	11
Changing the Default Admin Accounts Passwords.....	11
Securing the Console Port	11
Disable Insecure Management Ports	12
Securing SSH	12
Configuring Login Parameters and Session Timers.....	14
Securing WebView	15
Multi-Factor Authentication.....	16
AAA - Authentication and Authorization	16
Auditing and Compliance	19
Certificate Management	22
Secure Modes	26
Banner	30
Passwords	30
Control Plane.....	31
Securing Routing Protocols	32
Securing Label Distribution Protocols.....	34
Securing Link Management Protocols	34
Securing Discovery Protocols.....	35
Securing Network Management Protocols	38
Control Plane Protection Protocols	45
Other Control Plane Security Features	46

Data Plane	47
MACsec.....	47
IPv4 and IPv6	49
Learned Port Security	50
Wireless Network Security	51
Management Plane	51
Stellar WiFi Express - Change Default Passwords	51
Certificate Management	52
Stellar WiFi Express - Account Management.....	56
Stellar WiFi Express - Banner	57
Time Synchronization	57
Logging	58
SNMP	60
Control Plane.....	61
Certificate Management	61
Wireless Intrusion Protection System (wIPS).....	67
Data Plane	73
WPA3 Encryption	73
WiFi Enhanced Open - OWE	74
Client Isolation	75
Encrypting Roaming Client Context.....	75
Network Management System Security	76
Management Plane	76
Firewall Requirements	76
Change Default Passwords.....	76
Two-Factor Authentication Login.....	77
Disable Unused Services	78
Time Synchronization	78
Certificate Management	79
Securely Onboarding Network Devices	80
Provisioning Management Roles, Groups, and Users.....	82
Logging and Analytics	82
Control Plane.....	85
Certificate Management	85
Quarantine Manager	88
REST API Security Recommendations	89
Switching - Web Services Security	90
Conclusion	90
Related Documents	90

Introduction

In the contemporary digital era, as networks and technologies undergo continuous evolution, it has become paramount for businesses to safeguard their sensitive data and critical infrastructure from potential exploits perpetrated by malicious actors. Over the course of the last few years, almost every enterprise and government organization has changed the way its employees communicate, collaborate, and share information. While the rapid shift to support employees working from home was crucial to maintain business continuity during the pandemic, it came with a price: The network perimeter now extends well beyond traditional office boundaries, significantly increasing the organization's attack surface. Implementing a comprehensive and multifaceted security strategy is indispensable to fortify your business against such threats.

Today, a company's information system must be secure, encompassing its infrastructure, servers, and applications. Security is not a tangible product or feature that can be purchased but rather a process that involves the organization's methods for protecting information systems against unauthorized access.

Security is not an option in the architectures of global solutions, even if there is an endless balance to strike between the value of the data that needs protection and the cost of this protection. This clearly implies that the "sensitive" data to be protected has been previously evaluated and deemed valuable. From an end-user perspective, security must be provided transparently to avoid adding complexity.

As cyber threats continue to evolve and become more sophisticated, organizations must remain vigilant to safeguard sensitive information and maintain business continuity. Regularly reviewing certifications and ensuring compliance is paramount for data security, mitigating risks, and avoiding potential penalties. Implementing robust compliance measures not only protects your data but also enhances your company's reputation and fosters trust among stakeholders.

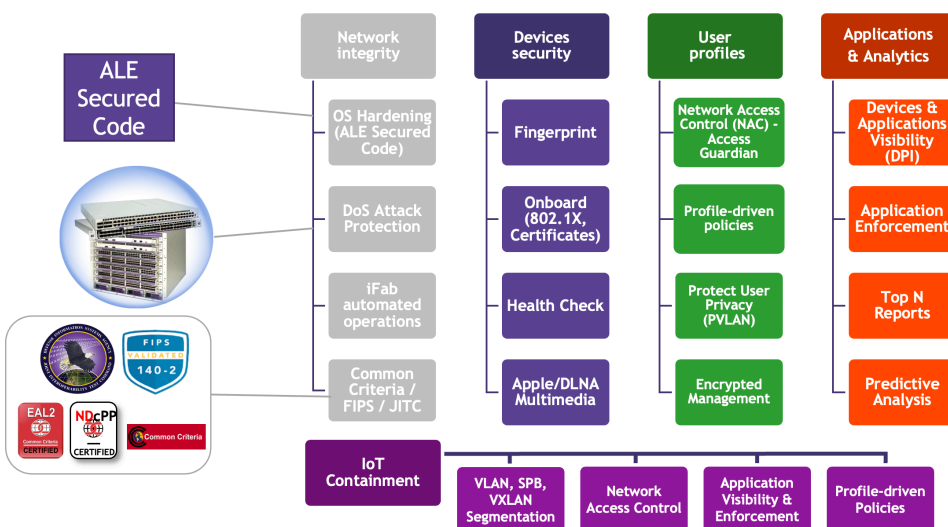
Several factors must be taken into consideration when configuring networking equipment in campus networks. Depending on the location, networking equipment may have a diverse range of functions. Implementing robust network security necessitates a comprehensive strategy employing multiple layers of defense. Alcatel-Lucent Enterprise OmniSwitch and OmniAccess Stellar WLAN are inherently "security ready" from the outset.

Security at Alcatel-Lucent Enterprise

In-Depth Security Multi-Layered Approach

Security is a fundamental component of the enterprise network architecture, particularly in the context of the increasing adoption of Bring Your Own Device (BYOD), Internet of Things (IoT), and exploration of cloud-based applications. A comprehensive security framework must be established from the ground up and applied universally across all network access methods, whether wired or wireless.

At Alcatel-Lucent Enterprise, we recommend an integrated security approach that begins with network integrity, device security, user profiles, application analytics, and subsequently progresses to the levels of IoT containment, operating system security, and code validation.



ALE layered security includes:

- At the user level, verifying that users are always authenticated and authorized with the correct access rights (using policies and profiles).
- At the device level, checking that devices are authenticated and compliant with IT-established security rules. This can be achieved with agents installed on devices that perform a quick security scan before devices connect to the network. For instance, the scan can ensure that the devices joining the network have up-to-date anti-virus software, and the latest version of their operating system.
- At the application level, setting rules associated with specific applications (including blocking, limiting bandwidth or identifying who can use them).
- At the network level, ALE switches and access points offer smart analytics capabilities that provide visibility and detailed information about the network, users, devices and applications being used on the network.
- ALE's smart analytics also provides deep packet inspection (DPI) capabilities, which detect the type of data and applications moving through the network, making it possible to identify unusual network traffic patterns and unauthorized activity and network intrusion.
- At the IoT level, devices are placed in virtual containers using network virtualization techniques that allow multiple devices and networks to use the same physical infrastructure, while remaining isolated from the rest of the network. By segregating the network with virtual containers, if a breach does occur in one part of the virtual network, it does not affect other applications.

Secure By Design

Alcatel-Lucent Enterprise products follow a secure by design approach. Below are examples of features which are enabled by default on OmniSwitch products out-of-the-box:

- **DoS Filtering:** By default, the switch filters denial of service (DoS) attacks, which are security attacks aimed at devices that are available on a private network or the Internet
- **Security Certifications:** ALE products received the highest levels of certification from major governmental agencies, including:
 - JITC Certification
 - NATO Certification
 - Common Criteria EAL2 and NDcPP Certification
 - FIPS 140-2 Certification
- **Signed AOS Image:** This provides verification of software integrity by providing the ability to determine if the AOS software comes from a trusted source and to detect if it has been tampered with after signing. Using RSA-4096 and SHA-256, AOS images are signed with a private key allowing AOS to verify the signature with a corresponding public key during reload and flash synchronization. The required public key and the intermediate CA bundle will automatically be setup on the switch for signature verification. U-boot version 8.9.70.R04 and above supports AOS signed images only (8.9R4 and above). Please verify the signed image support with your hardware/software platform from the AOS Release Notes.
- **Secure Diversified Code:** This employs multiple techniques to identify vulnerabilities, such as software architecture reviews, source code analysis (using both manual techniques and automated tools), vulnerability scanning tools and techniques, as well as analysis of known vulnerabilities in third-party code. ALE employs a set of technologies to ensure switch software integrity including:
 - Independent third-party verification and validation (IV&V): source code analysis, white box, and black box testing searching for vulnerabilities in external interfaces.
 - Software diversification: ALE software implements address space layout randomization (ASLR). Each switch boot generates unique memory layout
 - Secure software delivery: Dedicated USA based server for US Government downloads
 - TAA Compliance: ALE USA supply chain process enables designation of OmniSwitch models as TAA Country of Origin (CoO) USA

Product Security Incident Response Team

At Alcatel-Lucent Enterprise, it is our goal to ensure that our products are developed with all appropriate security principles as basis. We follow a comprehensive security program that combines:

- Secure software development best practices, processes, and tools
- Rigorous product security requirements
- Periodic validation and quality of security testing before release

Despite these security principles and related actions, vulnerabilities can be discovered in the software components of our products which, when exploited, can have an impact on the security level of these products once deployed in customer's networks.

ALE has a dedicated Product Security Incident Response Team (PSIRT) managing requests, investigations and reporting vulnerabilities or technical issues impacting ALE product. We report vulnerabilities to our Business Partners (BPs) and customers, with detailed description of criticality and publish public vulnerability advisories with available upgrades and fixes and relevant software version.

ALE PSIRT works with third-party coordination centers such as CERT-IST, NVD and US-CERT to manage vulnerabilities notices. The reports are referred to with a unique Common Vulnerabilities and Exposures (CVE) number.

Recommendation: Subscribe to ALE security advisory alerts on this link: [ALE Security Advisory Alerts](#).

Individuals or organizations that are experiencing technical security issue with an ALE product or solution are strongly encouraged to contact the ALE PSIRT by following these steps:

1. (Optional) Obtain the ALE PSIRT PGP public key, which can be found on <https://keyserver.pgp.com>. This will ensure the confidentiality of the communication which is a key point at this step to protect the security of our customers in regards with our responsible disclosure policy.
2. Complete the vulnerability summary report that can be downloaded from <https://www.al-enterprise.com/en/support/security-advisories>
3. Send the completed report to the email address: psirt@al-enterprise.com
4. (Optional) Consider sending the report email with the reporting organization's public PGP key and by encrypting the message with the ALE PSIRT PGP public key.

For more details about the Product Security incident response process, we encourage you to visit: <https://www.al-enterprise.com/en/support/security-advisories>

General Security Recommendations

Updating Software Regularly

Unfortunately, even mature, secure code, such as the openSSH and openssl used in AOS, have security updates. It is important to apply the updates to your network as soon as it is available. When vulnerabilities are analyzed and if any impacts are confirmed, and when there is a remediation, the ALE PSIRT will coordinate a fix and impact assessment, and define, together with the product line team, the resolution delivery timeframe, notification plans and disclosure to public organisations such as mitre.org and CERT organisations. When there is sufficient information to communicate, the Security Advisories Committee will request the creation or update of a Security Advisory (SA), which will be published and shared with the relevant stakeholders.

Since vulnerabilities are publically disclosed they are also known by malicious attackers who will exploit these vulnerabilities, which is why it is critical to apply these patches as soon as they are available. If a workaround or mitigation is available, it will be published as part of the security advisory.

Regularly check for ALE security advisories through its dedicated public page at [ALE Security Advisories](#) support site or you can also [sign up](#) to automatically receive security advisories for both OmniSwitch and Stellar wireless.

Control Physical Access

Physical access to switches, APs, and wiring closets allows a malicious actor to power cycle a switch, remove or replace critical components, or to alter cable wiring. Physical access to network jacks allows a malicious actor to enter the network inside the firewall. It is recommended that critical switches be housed in locked rooms with limited access. The OmniSwitch's coldStart and warmStart traps should be monitored to detect cycling of critical switches. It is recommended that the APs be managed through the OmniVista 2500 NMS or OmniVista® Cirrus.

Training and Awareness

Organizations work hard to select honest employees, however, without information security awareness training the employees may inadvertently leave network elements vulnerable to misuse. We have to understand that information systems are dynamic and are very susceptible to change. As corporate security policies evolve and threat actors innovate new way to maliciously harm victims, organizations have to adapt to these changes and educate employees on maintaining a good cybersecurity hygiene.

ALE offers training classes to enhance the network personnel's skills. In addition, ALE provides a number of user manuals including; the OmniSwitch User Guides for detailed CLI syntax and other security configuration options. Following is a listing of the user guides referenced in the [Related Documents](#) section:

- **AOS Switch Management Guide:** This guide will help users understand the switch's directory structure, the command line interface (CLI), configuration files, basic security features, and basic administrative functions. The features and procedures in this guide will help form a foundation that will allow you to configure more advanced switching features later in the network provisioning process.
- **AOS Network Configuration Guide:** Read this guide when your switch is up and running and you are ready to familiarize yourself with the software functions. When you are ready to connect your switch to the network, you will need to learn how the OmniSwitch implements fundamental software features, such as 802.1Q, VLANs, Spanning Tree, and network routing protocols. The OmniSwitch AOS Network Configuration Guide contains overview information, procedures, and examples on how standard networking technologies are configured on the OmniSwitch.
- **AOS CLI Guide:** Details the CLI syntax and usage including examples.
- **AOS Advanced Routing Guide:** This configuration guide includes information about configuring the following Layer 3 features
 - Open Shortest Path First (OSPF) protocol
 - Border Gateway Protocol (BGP)
 - Multicast routing boundaries
 - Distance Vector Multicast Routing Protocol (DVMRP)
 - Protocol-Independent Multicast (PIM)—Sparse Mode, Dense Mode, and Source-Specific Multicast (SSM)
- **AOS Specification Guide:** This guide lists all verified features and tested specification tables for the specified AOS release version.
- **OmniSwitch AOS Release Notes:** These release notes accompany the OmniSwitch AOS Releases software. These release notes provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.
- **OmniVista Online User Guide:** OmniVista help user guide can be found in the context-sensitive on-line help within the network management applications. The on-line help user guide can be accessed while configuring OmniVista features by simply clicking on the help "?" on the upper right-hand corner of the OmniVista browser window, or by clicking on the "Support Center" button to access the documentation.
- **OmniAccess Stellar AP User Guide:** This guide describes all features supported by the Stellar AP and provides instructions and examples for configuring ALE OmniAccess Stellar Access Point.

- **OmniAccess Stellar AWOS Release Notes:** These release notes accompany the OmniAccess Stellar Operating System (AWOS) Releases software for the Stellar APs. It provides important information on individual software and hardware features. Since much of the information in the release notes is not included in the hardware and software user manuals, it is important to read all sections of this document before installing new hardware or loading new software.

The network administrator will reference a combination of those user guides to configure the OmniSwitch features through CLI or Stellar WLAN via OmniVista. Each guide serves its purpose as summarized above. Other user guides for the hardware, fiber optic transceivers, and Data Center specific features are also available to support those functions.

We also invite you to visit our [Spacewalkers](#) website, which is a technical network community website and a dedicated space for users, customers and partners to connect and share about Alcatel-Lucent Enterprise network products and solutions. At the heart of Spacewalkers sits the forum where members can ask and answer questions. A vast array of technical resources, such as datasheets, Microsoft Visio stencils (diagrams), demo videos, solution guides and much more, is also available on the platform, as is ALE's latest network news and blog posts written by technical subject matter experts. Access to Spacewalkers is free (login required).

Switching Network Security

Management Plane

The management plane is responsible for handling traffic or services destined to the network device that is intended to configure, manage, or monitor the network device. It is a crucial for the management plane to be secure. Examples of management plane services include: administrative device access (Telnet, SSH, HTTP, and HTTPS), SNMP, and security protocols like RADIUS and TACACS+.

U-boot Access and Authentication

Depending on the OmniSwitch hardware platform, it may use the ONIE or the U-boot bootloader.

The U-boot provides access to system parameters, with which boot images and system variables can be manipulated by any user having physical or console access to the switch, which can cause security related issues.

Disabling U-boot access is not recommended since if the AOS image is corrupted or invalid, U-boot will not be able to start AOS and recovery if not possible. In this case, the switch must be returned to the factory for repair as it cannot be recovered by the admin user.

OmniSwitch allows to configure U-boot password authentication. This can only be configured with the “admin” account.

```
-> uboot authentication enable password abcd1234
```

Keep in mind that if the flash is corrupted and U-boot fails to start the AOS with the password enabled and the password is forgotten, the switch must be returned to the factory for repair.

ONIE Authentication

Depending on the OmniSwitch hardware platform, it may use the ONIE or the U-boot bootloader.

OmniSwitch allows to configure ONIE password authentication. This can only be configured with the “admin” account.

```
-> onie authentication enable password abcd1234
```

Please note that if the password is forgotten there is no other mechanism to perform disaster recovery and the switch needs to undergo RMA.

Recommendation: Secure U-boot/ONIE access with password authentication

Verify Image Integrity

To verify whether the SHA256 hash key of an image file located in the specified directory matches the SHA256 hash key in the specified key file, use the image integrity-check command with the name of the directory in “/flash” or include the full path (for example, “working” or “/flash/working”), and the name of the key file or include the full path (for example, “hash.txt” or “/flash/hash.txt”).

If the name of the key file is specified without the directory path, the switch will look for the key file in the same directory specified for the image file.

The following format is used to store the hash key values in the key file:

Uos.img: f0ff173eff38e43e0598663da2185a363fcb5bd407201d7537d0a6b9f58670e

For example,

```
-> image integrity check /flash/working key-file /flash/hash.txt
This operation may take several minutes...
Success: Key matched.
```

Recommendation: Signed images feature automatically verifies the integrity of the AOS image. Verifying the integrity of the image manually can be performed if you are using an unsupported version for signed images and is recommended to be done before upgrading your software.

Out-Of-Band Management

Recommendation: Setup a dedicated physical Out-Of-Band (OOB) management network separate from the data network used by business services. If this is not possible, then in-band management can be configured using a dedicated network segment (VLAN/VRF) but will not provide the same level of security.

OmniSwitch products provide a dedicated Ethernet Management Port (EMP) which allows you to bypass the Network Interface (NI) modules and remotely manage the switch directly through the Chassis Management Modules (CMM). In case the OmniSwitch product lacks an EMP port, you can use the USB-to-Ethernet interface which allows the interface to be treated just like an EMP interface.

The EMP IP address is stored in the vcboot.cfg file. To configure the EMP IP address, which is shared between CMMs:

```
-> ip interface emp address 198.51.100.100 mask 255.255.0.0
```

In case you require to set the EMP IP address for each CMM (in case of Virtual Chassis setup), although not required for remote access, this can be done by modifying the boot parameters. This can be useful for troubleshooting purposes.

Please refer to the AOS Switch Management Guide referenced in the [Related Documents](#) section for more details.

In-band Management (Management VRF)

In case it is not possible to use a dedicated physical OOB management network, you should configure a dedicated management VRF network. The Management VRF feature gives the user the ability to control which VRF is used for the various switch management protocols (Telnet, RADIUS, and so on.) It is recommended that the user specify a single VRF that all management services can be configured in. For example, both RADIUS and LDAP can use vrf-1.

You can disable management access for a specific VRF using the below commands as an example:

```
-> vrf data ssh admin-state disable
-> vrf data telnet admin-state disable
-> vrf data webview server disable
```

Recommendation: If you are using in-band management, use a separate VRF for management access, and another VRF for data. If your OmniSwitch product allows it, in the data VRF, disable all management access and the relevant TCP/UDP ports.

You should also disable the TCP/UDP service ports for the well-known services that will not be used in the data VRF using the below command:

```
-> vrf data ip service ftp admin-state disable
-> vrf data ip service ssh admin-state disable
-> vrf data ip service all admin-state disable
```

Restrict Management Access

You should restrict management connections only from a predefined list of IP addresses. The IP management station feature can be used for this purpose. When the management station is enabled, the switch access is allowed only from those IP addresses configured as management station IP, and only if they are not in the banned list.

Recommendation: Restrict management access to management stations IP addresses

Please note that this feature is applicable only when ASA enhanced mode is enabled. Please refer to [Secure Modes](#) section for more details about ASA enhanced mode.

To enable the IP management station feature in a switch:

```
-> aaa switch-access management stations admin-state enable
```

Enable the management station from the console to avoid termination of any session.

To configure the IP addresses for the management station to be allowed remote access:

```
-> aaa switch-access management stations 100.15.5.9
```

A maximum of 64 management stations can be configured.

Changing the Default Admin Accounts Passwords

By default, two user management accounts are available at the first bootup of the switch. They are “**admin**” and “**secureadmin**” user account, both having the default password of “**switch**”. The access privilege is applied based on the account selected.

Recommendation: Change the “admin” account password at first boot-up and keep it safe.

```
-> user admin password c0mPl3Xp@$w0rD
```

The “**secureadmin**” user must change the default password during first login to the switch. The “**secureadmin**” is a privileged user account with much secured access to the switch, with features including:

- Check integrity of image.
- Check integrity of vcboot.cfg.
- Process self-test functions (hardware and software).

Securing the Console Port

By default, switch management users may be authenticated through the console port via the local user database. If external servers are configured for other management interfaces (such as Telnet, or HTTP), but the servers become unavailable, the switch will poll the local user database for login information.

Access to the console port provides secure failover in case of misconfiguration or if external authentication servers become unavailable. The **admin** user is always authorized through the console port via the local database (provided the correct password is supplied), even if access to the console port is disabled.

The database includes information about whether a user is able to log into the switch and which kinds of privileges or rights the user has for managing the switch. The database may be set up by the “**admin**” user or any user with write privileges to the AAA commands.

Recommendation: Secure and restrict console access.

The below command can be used to restrict all users except the user “**admin**” from accessing the switch through the secure console session:

```
-> aaa console admin-only enable
```

In some security cases, console access can be disabled. With console access to the switch, the malicious actor can easily reset the admin password. That is why restricting physical access to your networking equipment is also critical.

To disable switch access through the console port of the switch:

```
-> aaa session console disable
```

It is recommended to create a backup of the configuration file before using this command. If the console access is disabled through configuration (on both working and certified directory) and the telnet/SSH/WebView session is also not available to the switch, contact customer support to recover the switch.

Disable Insecure Management Ports

When a switch initially boots up, all supported TCP/UDP well-known service ports are enabled (open). Although these ports provide access for essential switch management services, such as telnet, FTP, SNMP, they also are vulnerable to DoS attacks. It is possible to scan open service ports and launch such attacks based on well-known port information.

The “ip service” command allows you to disable (close) TCP/UDP well-known service ports selectively and enable them when necessary. This command only operates on TCP/UDP ports that are opened by default. It has no impact on ports that are opened by loading applications, such as RIP and BGP.

Insecure protocols are provided by AOS to support legacy systems. They are not recommended. Secure protocols are available which provide the same type of functionality. All service which are not used should be disabled to further reduce exposure. You can use the commands below to disable all IP services and selectively enable the required secure services:

```
-> ip service all admin-state disable
-> ip service ssh https snmp radius ntp admin-state enable
```

You can force using SSL for WebView access to the switch as mentioned in the [Using WebView](#) section.

Recommendation: Disable all IP services and selectively enable required secure protocols.

Below is a list of insecure protocols and their replacements (if applicable):

Insecure Protocol	Secure Replacement	Reason
Telnet	SSH	telnet does not use encryption nor certificates
FTP	SFTP SCP	FTP does not use encryption nor certificates
TFTP	SFTP SCP	TFTP does not use encryption nor certificates
SNMPv1	SNMPv3	SNMPv1 does not provide for user authentication nor encryption. SNMPv3 provides both user authentication and privacy.
SNMPv2/2c	SNMPv3	SNMPv2/2c uses only community strings for authentication. SNMPv3 provides both user authentication and privacy.
HTTP	HTTPS	HTTP is insecure protocol. Use HTTPS instead.
NTP	N/A	Disable unless NTP is used. If used, enable authentication.
RADIUS	N/A	Disable unless RADIUS is used.

Securing SSH

To start using and authenticating to the switch using Secure Shell (SSH), the management interface should be configured to specify the authentication server as mentioned in the [Management Interfaces Configuration](#) section.

Enforce Strong SSH Ciphers

The SSH feature provides a secure mechanism that allows you to log in to a remote switch, to execute commands on a remote device, and to move files from one device to another. SSH provides secure, encrypted communications even when your transmission is between two untrusted hosts or over an unsecure network. SSH protects against a variety of security risks including the following:

- IP spoofing
- IP source routing

- DNS spoofing
- Interception of clear-text passwords and other data by intermediate hosts
- Manipulation of data by users on intermediate hosts

The OmniSwitch SSH server is identified by one or several host-specific keys. Both the client and server process the key exchange to choose a common algorithm for encryption, signature, and compression. This key exchange is included in the SSH transport layer protocol. It uses a key agreement to produce a shared secret that cannot be determined by either the client or the server alone.

The key exchange is combined with a signature and the host key to provide host authentication. Once the exchange is completed, the client and the server turn encryption on using the selected algorithm and key.

When the client tries to authenticate, the server determines the process used by telling the client which authentication methods can be used. The client has the freedom to attempt several methods listed by the server. The server will disconnect itself from the client if a certain number of failed authentications are attempted or if a time-out period expires. Authentication is performed independent of whether the SSH interface or the SFTP file transfer protocol will be implemented.

The following elements are supported:

Host Key Type	DSA/RSA
Cipher Algorithms	AES, Blowfish, Cast, 3DES, Arcfour, Rijndael
Signature Algorithms	MD5, SHA1
Compression Algorithms	None Supported
Key Exchange Algorithms	diffie-hellman-group-exchange-sha1 diffie-hellman-group1-sha1
Key Location	/flash/system
Key File Names	Public: - ssh_host_key.pub, ssh_host_dsa_key.pub, ssh_host_rsa_key.pub Private: - ssh_host_key, ssh_host_dsa_key, ssh_host_rsa_key

To enable the enforcement of strong SSH ciphers, you can configure the command below:

```
-> ssh strong-ciphers enable
```

You can also enable enforcement of strong SSH Hash-based Message Authentication Codes (HMAC) configuration which will enforce the use of “*hmac-sha2-256*, *hmac-sha2-512*” in the SSH server. This can be configured using the command below:

```
-> ssh strong-hmacs enable
```

Recommendation: Enforce strong SSH Cipher algorithms and HMAC configuration.

Using SSH Public Key Authentication

You can also set up SSH Public Key Authentication (PKA) between an OmniSwitch and a client device.

A comment must be provided when generating the public key (*remote_ssh_user@device*) and the key must be in the following format:

```
<ssh-rsa | ssh-dsa> <encrypted key> <remote_ssh_user@device>
```

Example Key:

```
ssh-rsa
AAAAB3NzaClyc2EAAKjgnivubn9872435nsdg8dfsgfd8dfgfd7Rah1sqeyh6v3v6Hji4sOXwn+jdhAHJTM2Iq1R
jwccObEdYc67VM9+2ZwEipJI5HY11qbYKTA0em0kwKHNa+naIkWsTSwNj81HaAkaL21LMhcHnRytBfTeyySLgNHx
y6VFX1ipMN3pdtQbJn0cfRIevyxroMs7S+nMvht1lhrRzNaC3iW90IskS9zNjKUD2Becj5+Bt1JHmlqu3Is9H67
kySdHeF1XTMVWHDo30n9msAlvB7Bqolw26qzV3S97vbhrApQtYJAn0bIilVIAEasIYIbqrkTQ/kmDO4uMpCDgZKt
a7bP+P3CjBrGmK1w98 remote_ssh_user@device
```

The steps below use a *userid* of “*new_ssh_user*” on the OmniSwitch as an example:

1. Use the ssh-keygen utility of the OpenSSH software suite to generate a private and public key pair as shown below:

```
#ssh-keygen -t rsa -C remote_ssh_user@device
```

2. Save the private key on the client device.
3. Copy the the public key to the switch in the preferred directory. Including the userid as part of the filename can help identify the different keys:

```
#scp ~/.ssh/new_ssh_user_rsa.pub admin@192.168.2.1:/flash/system
```

4. Verify that the *userid* that will use SSH is a valid user name on the OmniSwitch. If the username does not already exist on the switch create the user name with the appropriate privileges.
5. Install the public key on the OmniSwitch for the specified user.

```
-> installsshkey new_ssh_user /flash/system/new_ssh_user_rsa.pub
```

6. Connect to the OmniSwitch using SSH with PKA.

```
#ssh -o PreferredAuthentications=publickey new_ssh_user@192.168.2.1 -v
```

7. (Optional) To enforce Secure Shell PKA on a switch and not prompt for a password, use the below command:

```
-> ssh enforce-pubkey-auth
```

Please refer to the AOS Switch Management Guide referenced in the [Related Documents](#) section for more details.

Recommendation: Use PKA for SSH connections between your OmniSwitch and client devices. This significantly enhances security by eliminating password risk and protects against brute-force attacks. It also provides benefits of automation and improving the network administrator experience by simplifying access management.

Configuring Login Parameters and Session Timers

You can set the number of times a user may attempt to unsuccessfully log in to the switch's CLI by using the **session login-attempt** command as follows:

```
-> session login-attempt 5
```

In this example, the user may attempt to log in to the CLI five (5) times unsuccessfully. If the user attempts to log in the sixth time, the switch will break the TCP connection. The default login attempts is set to 3 times.

Recommendation: Minimize the number of login attempts to prevent brute-force attacks

You may also set the length of time allowed for a successful login by using the **session login-timeout** command as follows:

```
-> session login-timeout 20
```

In this example, the user must complete the login process within 20 seconds. This means that the time between a user entering a login name and the switch processing a valid password must not exceed 20 seconds. If the time-out period exceeds, the switch will break the TCP connection. The default login timeout is 55 seconds.

You can configure the session time-out for incomplete or broken SSH session using the **ssh login-grace-time** command as follows:

```
-> ssh login-grace-time 200
```

In this example, the incomplete or broken SSH session will time-out after 200 seconds. This means the user must establish a SSH session within 200 seconds. The default login grace time period is set to 120 seconds.

Recommendation: Minimize SSH login grace timeout and session timeout to protect against resource abuse and unauthorized access

You can set the amount of time that a user must be inactive before the session times out. To change the setting, enter the **session timeout** command with the type of session and the desired number of minutes. The default session timeout is set to 4 minutes.

For example:

```
-> session cli timeout 8
-> session ftp timeout 5
-> session http timeout 10
```

Recommendation: Minimize session timeout timers and session limits to protect against resource abuse

You can configure as well the concurrent session limit for FTP, SSH, Telnet and HTTP or HTTPS. The access is denied when the number of sessions exceed the configured session-limit. The default setting is different depending on the type of session. For SSH connection, the default is 8 concurrent sessions. This can be set using the command below:

```
-> session ftp session-limit 2
-> session ssh session-limit 4
-> session telnet session-limit 3
-> session http session-limit 20
```

IP Lockout Threshold

The lockout threshold number specifies the number of failed login attempts from an IP address after which the IP address will be banned from switch access. By default, the lockout threshold value is set to 6. To configure:

```
-> aaa switch-access ip-lockout-threshold 2
```

IP address is permanently blocked/banned if the number of authentication failures from a particular IP reaches the IP lockout threshold within the window, which is two times of the user lockout window.

A maximum of 128 IPs will be added to the banned list. When the maximum limit has reached, oldest entry from the list is removed to accommodate the new entries.

Recommendation: Configure IP Lockout Threshold to protect switch access from brute-force attacks

To release the banned IP addresses that are blocked due to failed login attempts:

```
-> aaa switch-access banned-ip all release
-> aaa switch-access banned-ip 100.2.45.56 release
```

Please note that the IP lockout feature is applicable only if ASA enhanced mode is enabled. Please refer to the [Secure Modes](#) section for more details about Enhanced mode.

Securing WebView

The switch can be monitored and configured using WebView, Alcatel-Lucent Enterprise's web-based device management tool. The WebView application is embedded in the switch and is accessible via a web browser.

By default, WebView server is enabled, access is enabled, and strong cipher algorithm SSL is forced and used. For this reason, the following algorithms will not be supported: RC4-SHA, RC4-MD5, ECDHE-RSA-RC4-SHA, IDEA-CBC-SHA, DES-CBC3-SHA, EDH-RSA-DES-CBC3-SHA, ECDHE-RSA-DES-CBC3-SHA, aNULL, eNULL, EXPORT, DES, MD5, PSK, RC4.

However, to authenticate to WebView, the management interface should be configured to specify the authentication server as mentioned in the [ASA Management Interfaces Configuration](#) section.

Recommendation: Disable the webview server from the switch and the relevant TCP/UDP ports if it is not needed to reduce the attack surface and mitigate security risks.

To disable the WebView server, the below command can be issued:

```
-> webview server disable
```

You should also disable the relevant TCP/UDP ports as highlighted in the [Disable Insecure Management Ports](#) section.

For details about certificate management of the WebView management interface, please refer to the [WebView Certificate](#) section.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a security process designed to provide multiple layers of protection by requiring users to verify their identity using more than one method of authentication. However, while being ubiquitous and easy to implement, password-based authentication presents several security weaknesses, including: predictability, re-use, issues with complexity, sharing and phishing, brute force attacks, and longevity.

There are many use cases to implement MFA, including using Google Authenticator or Duo. These are covered in great detail in the “Multi-Factor Authentication with Google Authenticator or Duo” application note referenced in the [Related Documents](#) section.

Recommendation: Use MFA since it provides a significantly higher level of security than traditional single-factor authentication methods

AAA - Authentication and Authorization

The local authentication, authorization and accounting (AAA) configuration enforces device access control, provides a mechanism for tracking configuration changes, and enforces security policy.

Login information and privileges may be stored on the switch and/or an external server, depending on the type of external server you are using and how you configure switch access. An external RADIUS or LDAP server can supply both user login and authorization information. External servers may also be used for accounting, which includes logging statistics about user sessions. If an external server is not available or is not configured, user login information and user authorization may be provided through the local user database on the switch. Logging may also be accomplished directly on the switch.

Recommendation: Centralize access control through external servers to improve the consistency of access control, allow network-wide control of accounts, simplify and reduce administrative costs of account provisioning and deprovisioning, and provide accounting and audit trails for user and admin sessions.

Authenticated Switch Access (ASA) is a way of authenticating users who want to manage the switch. With authenticated access, all switch login attempts require authentication via the local user database or via a third-party server. There are two modes for ASA: default and enhanced. We will cover enhanced mode in a [Secure Modes](#) section.

Setting up ASA involves the following general steps:

1. Set Up the Authentication Servers.
2. Set Up the Local User Database: Set up user information on the switch if user login or privilege information will be pulled from the switch. The privileges and profiles are sometimes referred to as authorization.
3. Set Up the Management Interfaces.
4. Set Up Accounting: This step is optional but recommended.

These procedures will be described briefly in this section.

Management Interfaces Configuration

Use the “aaa authentication” command to specify the management interface through which switch access is permitted (such as console, telnet, ftp, http, or ssh). Specify the server and backup servers to be used for checking user login and privilege information. Multiple servers of different types may be specified. For example:

```
-> aaa authentication ssh rad1 ldap2 local
```

The order of the server names is important. The switch uses the first available server in the list. In this example, the switch would use rad1 to authenticate Telnet users. If rad1 becomes unavailable, the switch will use ldap2. If ldap2 then becomes unavailable, the switch will use the local user database to authenticate users.

Repeat the above command for each management interface to which you want to configure access; or use the “default” keyword to specify access for all interfaces for which access is not specifically denied. For example, if you want to configure access for all management interfaces except HTTP, you would enter:

```
-> no aaa authentication http
-> aaa authentication default rad1 local
```

Please note that if you want to use WebView to manage the switch, make sure HTTP/S is enabled.

Authentication and Authorization with External Servers

If an external RADIUS, LDAP, and/or TACACS+ servers are used for user login information, use the “aaa radius-server”, “aaa ldap-server”, or “aaa tacacs+-server” commands to configure the switch to communicate with these servers. For example, to configure an external RADIUS authentication server:

```
-> aaa radius-server rad1 host 10.10.1.2 key amadeus
```

After configuring the remote servers, you can specify the server type in the management interface as mentioned in the previous section.

RADIUS over TLS

It is recommended to use RADIUS over TLS. This provides secured communication between RADIUS and TCP peers using TLS. RADIUS uses MD5 algorithm for secured communication, implementation of TLS further reduces the risk of attack on MD5 encrypted RADIUS packets. There by all RADIUS requests and RADIUS responses are encrypted and transferred between OmniSwitch and RADIUS server.

To configure TLS for RADIUS server, SSL must be enabled for the RADIUS server:

```
-> aaa radius-server radsrv1 host rad1_ipaddr key rad1_secret vrf-name rad_vrf ssl
```

Recommendation: Configure RADIUS over TLS for enhanced security.

Please refer to the [PKI](#) section which explains the PKI feature. This allows to select common certificate and public key security mode and configure the TLS version for the applications (RADIUS, LDAP, Captive Portal, Syslog and SNMP) using OpenSSL.

For more information, see the “Managing Authentication Servers” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* referenced in the [Related Documents](#) section.

Authentication and Authorization with Local User Database

For local authentication, we will be required to configure the local user database. To set up a user account, use the **user** command, which specifies the following:

- **Password**
- **Privileges:** The user’s read and write access to command domains and families. This is the same as authorization.
- **SNMP access:** Whether or not the user is permitted to manage the switch via SNMP.

Typically, options for the user are configured at the same time the user is created. An example of creating a user and setting access privileges for the account is given here:

```
-> user thomas password techpubs read-write domain-policy
```

In addition, another account, “**default**”, is available on the switch for default settings only; this account cannot be used to log into the switch. It is used to store and modify default settings for new users.

Authorization (User Privileges)

To configure privileges for a user, enter the user command with the read-only or read-write option and the desired CLI command domain names or command family names. The read-only option provides access to show commands; the read-write option provides access to configuration commands and show commands. Command families are subsets of command domains.

Recommendation: Implement role-based access control by setting up custom authorization per user

If you create a user without specifying any privileges, the user’s account will be configured with the privileges specified for the default user account.

Command domains and families are listed here:

Domain	Corresponding Families
domain-admin	file ssh scp-sftp telnet ntp dshell debug tftp-client dhcp-server dhcpv6-server dhcp-message-service dhcp-active-lease service
domain-system	system lldp snmp rmon webmgt config license-manager storage-locking alarm-manager pkgmgr remote-config
domain-physical	chassis module interface uddl pmm port-mapping health multi-chassis capability vfc loopback-detection lanpower pppoe-ia port-manager
domain-network	ip rip ospf isis bgp vrrp ip-routing ipmr ipms ripng ospf3 bfd vrf grm openflow isis-vc
domain-layer2	vlan bridge stp 802.1q linkagg ip-dhcp ha-vlan spb-isis evb app-fingerprint vm-snooping mrp
domain-service	dns svcmgr link-fault-propagation
domain-policy	qos slb tcam-mgr
domain-security	session ipsec mvrp aaa netsec da-unp sec-km macsec
domain-mpls	mpls
domain-vc	virtual-chassis
domain-datacenter	dc-apps auto-fabric
domain-afn	sip-snooping dpi app-monitoring device-profile

In addition to command families, the keywords “all” or “none” may be used to set privileges for all command families or no command families respectively. You can also use the keyword “all-except” to disable the function privileges for a specific family or domain for a user.

An example of setting up user privileges:

```
-> user thomas read-write domain-network ip-helper telnet
```

User thomas will have write access to all the configuration commands and show commands in the network domain, as well as Telnet and IP helper (DHCP relay) commands. The user will not be able to execute any other commands on the switch.

This configuration is described in detail in the “Managing Switch User Accounts” chapter of the *OmniSwitch AOS Release 8 Switch Management Guide* referenced in the [Related Documents](#) section.

Please note that if you want to use WebView to manage the switch, make sure HTTP is enabled.

Auditing and Compliance

AAA - Accounting with Local User Database or External Servers

Accounting servers track network resources such as time, packets, bytes, etc., and user activity (when a user logs in and out, how many login attempts were made, session length, etc.). The accounting servers may be located anywhere in the network.

To enable accounting (logging a user session) for ASA, use the “**aaa accounting session**” command with the relevant server name(s). In this example, the RADIUS and LDAP servers have already been configured through the “**aaa radius-server**” and “**aaa ldap-server**” commands.

```
-> aaa accounting session rad1 ldap2 local
```

Recommendation: Enable accounting for auditing and compliance purposes to a centralized location.

After this command is entered, accounting will be performed through the “**rad1**” RADIUS server. If that server is unavailable, the LDAP server, “**ldap2**”, will be used for accounting. If that server is unavailable, logging will be done locally on the switch through the Switch Logging feature.

Command Logging

Command logging is a feature which, when enabled, automatically creates a “command.log” file which stores a comprehensive CLI command history for all active sessions since the function was first enabled.

To enable command logging:

```
-> command-log enable
```

Recommendation: Enable command logging to keep an audit trail of all commands entered through the CLI.

SNMP

SNMP provides an industry standard communications model used by network administrators to manage and monitor their network devices. The SNMP agent in the switch can communicate with multiple managers. You can configure the switch to communicate with different management stations by using different versions of SNMP. The switch supports three versions of SNMP—v1, v2, and v3, however it is recommended to only use SNMPv3.

Recommendation: SNMPv1/2/2c should be avoided entirely as they are insecure. SNMPv3 is significantly more secure with added encryption, robust authentication, message integrity, and role-based access control.

SNMPv3 supports three models:

- View-Based Access Control Model (VACM)
- User-Based Security Model (USM)
- Transport Security Model (TSM)

These security models are supported along with these added security features:

- Message integrity—Ensuring that a packet has not been tampered with in transit.
- Time Frame Protection—Limiting requests to specified time frames. The user can specify a time frame so that any PDU bearing an out of date timestamp will be ignored.
- Encryption—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.
- Authentication—Determining that the message is from a valid source holding the correct privileges.

In this section, we will cover the USM. TSM will be covered in the [SNMP over TLS](#) section.

SNMP authentication types SHA and MD5 are available with DES and AES encryption. The **sha**, **md5**, **sha+des**, **md5+des**, **sha+aes** keywords may be used in the command syntax when configuring the user account as mentioned in the next section.

By default, the switch is set to “privacy all”, which means the switch accepts only authenticated and encrypted v3 Sets, Gets, and Get-Nexts.

SNMP Management Station

An SNMP management station is a workstation configured to receive SNMP traps from the switch. You must identify this station to the switch by using the **snmp station** CLI command.

The following information is needed to define an SNMP management station.

- The IP address of the SNMP management station device.
- The UDP destination port number on the management station. This identifies the port to which the switch will send traps.
- The SNMP version used by the switch to send traps.
- A user account name that the management station will recognize.

Recommendation: Use a separate user account for SNMP management access. Disable SSH and other management features for this user using the command: “user snmpuser allow-ssh disable”.

For example, to set up an SNMP NMS by using the switch's CLI, proceed as follows:

1. Specify the user account name and the authentication type for that user. For example:

```
-> user NMSuserV3MD5DES md5+des password *****
```

2. Specify the UDP destination port number (in this case 8010), the IP address of the management station (199.199.100.200), a user account name (NMSuserV3MD5DES), and the SNMP version number (v3). For example:

```
-> snmp station 199.199.100.200 8010 NMSuserV3MD5DES v3 enable
```

Use the same command as above for specifying the IPv6 address of the management station. For example:

```
-> snmp station 300::1 enable
```

SNMP Authentication Traps

Recommendation: Enable SNMP authentication traps.

The authentication trap is sent when an SNMP authentication failure is detected. This trap is a signal to the management station that the switch received a message from an unauthorized protocol entity. This normally means that a network entity attempted an operation on the switch for which it had insufficient authorization. When the SNMP authentication trap is enabled, the switch will forward a trap to the management station. The following command will enable the authentication trap:

```
-> snmp authentication trap enable
```

The trap will be suppressed if the SNMP authentication trap is disabled.

SNMP over TLS

For enhanced security, you should enable TLS encryption by enabling the TSM security model for SNMP. TSM is a framework that allows TLS or DTLS to provide a secure communication channel for securing SNMP messages.

TSM can be enabled using the “**snmp security tsm**” command. For example:

```
-> snmp security tsm enable
```

When the TSM security model is enabled, all the v1/v2/v3 USM request and traps are discarded. The SNMP requests are supported only over IPv4 transport.

The TSM mode requires the users local and remote identity to be configured.

The user account must be mapped to the remote certificate in TSM mode. To map the remote identity to a user, use the “**snmp tsm-map**” command. For example:

```
-> snmp tsm-map remote-identity manager.crt user NMSuserV3MD5DES
```

Recommendation: Use TSM SNMP model when you already have PKI infrastructure available, otherwise use USM SNMP model.

To send SNMP traps over TLS connection, the SNMP station needs to be configured with TSM user along with certificate identities. These configurations are supported only for SNMP version 3.

Use the **snmp station** command to configure the TSM security mode. For example:

```
-> snmp station 168.22.1.1 NMSuserV3MD5DES v3 tsm local-identity aluSubagent.crt  
remote-identity manager.crt enable
```

Please refer to the [PKI](#) section which explains the PKI feature. This allows to select common certificate and public key security mode and configure the TLS version for the applications (RADIUS, LDAP, Captive Portal, Syslog and SNMP) using OpenSSL.

Switch Logging

Switch logging is an event logging utility that is useful in maintaining and servicing the switch. Switch logging uses a formatted string mechanism to either record or discard event data from switch applications.

The log records are copied to the output devices configured for the switch. Log records can be sent to a text file and written into the flash file system. The log records can also be scrolled to the console of the switch or to a remote IP address.

Switch logging information can be customized and configured through CLI commands, WebView, and SNMP. Log information can be helpful in resolving configuration or authentication issues, as well as general switch errors.

Switch logging is enabled by default with info (6) severity level. The output is sent to the console and to the flash memory with a default logging file size of 1250 Kbytes.

You can also assign severity levels to the switch applications that cause some of the events to be filtered out of your display. The `swlog appid` command is used to assign the severity levels to the applications.

The syntax for the `swlog appid` command requires that you identify a switch application and assign it a severity level. The severity level controls the kinds of error-type events that are recorded by the switch logging function. If an application experiences an event equal to or greater than the severity level assigned to the application, the event is recorded and forwarded to the configured output devices. You can specify the application either by the application ID CLI keyword or by its numeric equivalent.

The `level` keyword is used with the `swlog appid` command to assign the error-type severity level to the specified application IDs. Values range from 1 (highest severity) to 8 (lowest severity). For example:

```
-> swlog appid bridge level warning
```

To enable the host to send its log to the remote syslog server, enter the following command:

```
-> swlog host output socket enable
```

To configure syslog over TLS, use the `swlog output` command. For example:

```
-> swlog output socket 192.168.120.140 tls
```

Recommendation: Centralize syslog logging using TLS encryption and add a second syslog server for redundancy.

This enables syslog over TLS for the configured IP address.

Please refer to the [PKI](#) section which explains the PKI feature. This allows to select common certificate and public key security mode and configure the TLS version for the applications (RADIUS, LDAP, Captive Portal, Syslog and SNMP) using OpenSSL.

Certificate Management

Configuring Public Key Infrastructure

Applications using OpenSSL can select the public key to communicate with external servers when servers require to verify client certificate. Likewise, clients can also validate the server certificate. This prevents the spoofing attacks.

The following three public key security modes can be configured for TLS client to communicate with external servers:

- **No Validation:** This is the default mode, in this mode the client applications do not provide certificate and not validate server certificate.
- **Server Certificate Validation:** In this mode, the client application is required to provide clients certificate but the client will validate the server certificate using the pre-installed CA certificate.
- **Mutual Authentication:** In this mode, the client application must load their certificates and key files and provide clients certificate to server.

The applications can also limit the TLS version it uses.

The PKI feature allows to select common certificate and public key security mode and configure the TLS version for the applications (RADIUS, LDAP, Captive Portal, Syslog and SNMP) using OpenSSL.

To configure server certificate validation:

```
-> ssl pki client validate-certificate admin-state enable
```

When the feature is enabled or disabled the switch must be rebooted for the changes to be applied.

When the server validation is enabled, the TLS client (LDAP, RADIUS, SYSLOG) applications validate server certificate.

To configure mutual authentication for client and server:

```
-> ssl pki < client | server > mutual-authentication admin-state enable
```

When the feature is enabled or disabled the switch must be rebooted for the changes to be applied.

When the mutual authentication is enabled for the client, the TLS client applications will load the myCliCert.pem and myCliPrivate.key files in “/flash/switch/cert.d” and provide the certificate to server while establishing the TLS connection.

When the mutual authentication is enabled for the server, the TLS server (SNMP) application must require clients to provide their certificate to server while establishing TLS connection.

The server certificate is validated based on:

- TLS mutual authentication using X.509 certificates.
- The presented identifier must match the reference identifier as per RFC 6125 Section 6.
- X.509 certificate validation using OCSP and CRL.

If the server certificate is not validated, then the TLS client connection is terminated.

You can also configure the TLS version (1.0, 1.1, or 1.2) for server and client applications. When the version is configured the TLS client and server will deny all SSL and TLS versions lower than the configured version.

```
-> ssl pki tls version 1.2
```

The command is applicable only for LDAP, RADIUS, SYSLOG and SNMP applications. The switch must be rebooted for the changes to be applied.

Recommendation: Configure PKI to validate client and server certificates to prevent spoofing attacks.

Enforce Strong SSL Cryptographic Ciphers

Many applications use OpenSSL to communicate to external network elements (over TLS). OpenSSL allows the application to select their own cipher suites (a list of cryptography algorithms which will be used for the connection establishment, key exchange and data encryption).

Most of the applications using the OpenSSL do not share common cipher suites, which make it difficult for the network administrator to know which cipher suite is used by which application.

OpenSSL cipher security level configuration allows to configure common SSL cipher suites for RADIUS, LDAP, Captive Portal, Syslog and SNMP applications which use OpenSSL to communicate over TLS.

OpenSSL cipher security level configuration provides four security levels for the network administrator to choose from. Each level specifies the strength of the cipher and indicates the minimum level of ciphers that are supported. The following security levels can be configured:

- All: Includes all the cipher suites, including NULL-SHA.
- Low: Includes all cipher suites, except NULL-SHA.
- Medium: Includes all ciphers suites except NULL-SHA, DES-CBC-SHA, and RC4-MD5.
- High: Includes only AES-256 with SHA-2 ciphers (Applicable only for TLSv1.2).

By default, the cipher security level is set to medium in default switch operation mode and high in common criteria mode. For more details on CC mode, please refer to [Common Criteria](#) section.

Apart from the predefined cipher security level, the administrator can also define custom cipher suites as per requirement using the custom configuration.

The cipher security level can be configured using the ssl cipher command. For example, to set the security level to high, enter:

```
-> ssl cipher level high
```

After running the command, the switch must be rebooted for the security level to be applied.

Recommendation: Set the SSL Cipher level to high.

WebView Certificate

When accessing WebView using the default settings, a self-signed certificate will be used which will generate a certificate warning on the web browser. You can either install this built-in certificate to the Trust Store of your management station, or you can install a custom SSL certificate on the OmniSwitch.

Recommendation: Configure a custom SSL certificate for WebView access and do not rely on the built-in self-signed certificate

To install a custom SSL certificate on the OmniSwitch, please follow the below steps:

1. Have the following certificates ready:
 - Root CA certificates: ca.pem
 - WebView server certificates: wv_server.crt, wv_server.key
2. Copy the contents of wv_server.crt and wv_server.key into the WebView server certificate.

```
# cat wv_server.key wv_server.crt > web.pem
```

3. Copy the WebView server certificate into “/flash/switch/” directory of the OmniSwitch.
4. Install the WebView certificate, the WebView server will automatically restart.

```
-> aaa certificate install-certificate webview web.pem
```

5. Add the Root CA certificate to the browser

Captive Portal Certificate

By default, the OmniSwitch uses a built-in, self-signed certificate for Captive Portal. The certificate is named “default_cportalCert.pem” and is stored in the “/flash/switch” directory on the switch. To replace the default certificate with a well known CA certificate, use the following steps:

1. Backup the existing default certificate:

```
-> cp default_cportalCert.pem default_cportalCert.pem.old
```

2. Rename the new well known CA certificate file to “default_cportalCert.pem”.
3. Copy the certificate file to the “/flash/switch” directory.
4. Use the captive-portal name command to reload the Web configuration (use the CN name as specified in the new certificate):

```
-> captive-portal name CN_name
```

5. Attempt a captive portal log in to verify the change.

The certificate must be in the x509 format. To generate an x509 formatted certificate (.pem), perform the following on a Linux or Unix machine:

1. Have the private key and the CA signed certificate available.
2. Issue the “cat privateKey ca_certificate | tee switch_cert_file”(i.e default_cportalCert.pem) command.

Recommendation: Configure a custom SSL certificate for captive portal authentication and do not rely on the built-in self-signed certificate

Please refer to the [PKI](#) section which explains the PKI feature. This allows to select common certificate and public key security mode and configure the TLS version for the applications (RADIUS, LDAP, Captive Portal, Syslog and SNMP) using OpenSSL.

LDAP Authentication

SSL can be set up on the server for additional security. When SSL is enabled, the server identity is authenticated. The authentication requires a certificate from a CA. If the CA providing the certificate is well-known, the certificate is automatically extracted from the Kbase.img file on the switch (certs.pem). If the CA is not well-known, the CA certificate must be transferred to the switch through FTP to the /flash/certified or /flash/working directory and must be named optcerts.pem. The switch merges either or both of these files into a file called ldapcerts.pem.

Recommendation: Use SSL with LDAP authentication using a custom SSL certificate

```
-> aaa ldap-server ldap2 ssl
```

Please refer to the [PKI](#) section which explains the PKI feature. This allows to select common certificate and public key security mode and configure the TLS version for the applications (RADIUS, LDAP, Captive Portal, Syslog and SNMP) using OpenSSL.

Secure Modes

OmniSwitch supports multiple secure modes which can be enabled which enforce certain additional security measures. The following secure modes will be covered in this section:

- Authenticated Switch Access (ASA) - Enhanced Mode
- Common Criteria (CC) Mode
- Joint Interoperability Test Command (JITC) Mode
- Federal Information Processing Standards (FIPS) Mode

The JITC mode is mutually exclusive of CC mode and Enhanced-mode. If the switch is already running in CC or enhanced-mode it must be disabled before enabling JITC mode and vice versa.

ASA - Enhanced Mode

ASA Enhanced Mode feature allows configuration of enhanced security restrictions to the OmniSwitch. The following command sets the access mode to enhanced mode:

```
-> aaa switch-access mode enhanced
```

Recommendation: For enhanced security restrictions to the OmniSwitch, it is recommended to set the ASA mode to enhanced

The following functionality come into effect when the ASA enhanced mode is activated:

- When the enhanced mode is initially activated, the default password-policy and lockout settings are automatically set to enhanced mode default values. When the switch boots up with a vcboot.cfg configuration file that has the enhanced ASA mode activated, LockoutSetting file will be considered for the modified lockout settings as the modified values will not be stored in vcboot.cfg.
- The user has to re-authenticate before entering to super user mode. The switch verifies whether the user of the current session has the privilege to access the super user mode. If the user has enough privilege, then the switch prompts for a password, if not, the switch prompts for the user credentials too with enough privilege. Only if the authentication is successful, then the user shall be allowed to access the mode prompt.
- Default password **switch** cannot be set anymore as it does not meet the enhanced mode password policy. User 'admin' shall be forced to change the password upon login if the password was not changed from the default password 'switch'.
- The following table lists the factory default and the ASA enhanced mode values for password policy and user lockout parameters:

Parameters	ASA Enhanced Mode Default Values	Factory Default Values
User Password Policy		
Minimum size	9	8
Password expiration	Disable	Disable
Password cannot contain username	No	No
Minimum number of English uppercase characters	1	Disable
Minimum number of English lowercase letters	1	Disable
Minimum number of base-10 digit	1	Disable
Minimum number of non-alphanumeric	1	Disable
Password history	4	4
Password minimum age	Disable	Disable
User Lockout Setting		
Observation window	1 minute	Disable
Duration	5 minutes	Disable
Threshold	3	Disable

- If the mode is changed from default to enhanced and if the user password policy settings and the user lockout settings have the default mode default values, then corresponding enhanced mode default values will be assigned. If the user password policy settings and the user lockout settings are assigned with non-default values in the default mode, then the same values will be carried to the enhanced mode.
- When the mode is changed from enhanced to default, user password policy settings and user lockout settings will be restored back to switch's default mode default values. Only those configurations modified in the enhanced mode will be retained on the switch after reload.
- When the enhanced mode is initially activated, since the password policy is automatically set to enhanced mode default values, any login request through SNMP and FTP that does not follow the enhanced mode password policy shall be considered as authentication failure.
- In enhanced mode, a given user is restricted to only one session. For example, if a user 'admin' has already logged in a session, another session with the same user 'admin' is not allowed, and the new session login is refused. This is applicable for both local and external users. If the user authentication fails, the login failure attempt is considered as an invalid login attempt for IP lockout count.
- A user account will be locked after the authentication failure based on the threshold value within the observation window duration, irrespective of the access method. The user account will remain locked for the lockout duration (lockout-window, lockout-threshold, and lockout-duration is based on the configured or default values.) This is only supported for local users.
- When the enhanced mode is activated, other existing sessions will not be logged out. The change of password for internal or external user will not impact existing sessions until they log out.
- When the ASA mode is set to enhanced or default, the changes will take effect in secondary after write memory flash-synchro.
- Any local user who logs in with the password that does not comply with the enhanced mode password policy will be prompted to change the password.
- Enhanced mode allows the dynamic alignment of IP services like telnet, FTP, SSH, to the AAA authentication status in the default VRF. However, existing command **[no] ip service** can be used to enable or disable individual IP services.
- When enhanced mode is activated, TLS connections use only TLS version 1.2. Connection requests with TLS version 1.1 and lower shall be rejected. This is applicable only for Captive Portal and WebView.
- In the enhanced mode, all login attempts to the switch is logged along with the user name, IP address of the host, switch access type like telnet, SSH, console and so on along with the authentication status.

- In the enhanced mode, when the switch logging file reaches 90% of the configured threshold value, a SWLOG message is displayed in the console and a trap is generated to alert the administrator to take a backup of the SWLOG file before it is overwritten. For example, following message is displayed:

```
Sun Mar 29 12:42:15 : SSAPP main info message:
+++ Switch log file reached 90%, Backup files before overwritten
```

- AOS supports both DSA 1024 and RSA 2048 public key algorithms for SSH private and SSH public keys in enhanced mode. WebView access supports connection over TLS. In the enhanced mode, the default certificates are generated with RSA 2048 bit keys.
- When the switch is in ASA enhanced mode, both user name and password is prompted to view the SWLOG data when **show log swlog** commands are used by the users. Only those users who provide valid ASA credentials are allowed to view the SWLOG data.

Common Criteria Mode

Since CC evaluations depend on specific hardware and software, the details in this section are only to provide general guidance and are not applicable to all OmniSwitch products or AOS software releases.

For more details about preparing and operating CC evaluated OmniSwitch products, you can download the administrative guide which is referenced in the [Related Documents](#) section.

For CC, the OmniSwitch runs in the CC mode under which it will have all the CC functions enabled. CC mode can be enabled/disabled via the below CLI command:

```
-> aaa common-criteria admin-state enable
```

The configuration is applied only after reloading.

After the switch boot up in CC mode, during log on to the switch the user will be prompted to change the password if the password doesn't satisfy the CC password policy. This is applicable for the default "admin" user as well created during initial installation of the Target of Evaluation (TOE). It should be noted that the default "admin" user is considered the privileged administrator and has full administrative privileges for all commands on the TOE. Hence, the default "admin" user must be used only to perform installation and initial configuration of the TOE. The general switch administration or management must be performed by the users with appropriate administrative privileges (created by the "admin" user), but not by the default "admin" user.

The CC mode will only allow console and SSH access to the OmniSwitch. CC Evaluation (CCE) requires each administrative user to be successfully identified and authenticated before allowing any other TOE Security Function (TSF) mediated actions on behalf of that administrative user. In Common Criteria mode, TOE can be accessed locally through serial console and remotely through SSH. SSH communication supports both password based and public-key based authentication. During local/remote access, authentication is done through local switch database. In CC mode the cryptographic algorithms for TLS and SSH are limited to only evaluated encryption algorithms, key exchanges, public key algorithms and data integrity MAC algorithms.

The following functionalities are disabled by default when CC mode is enabled:

- FTP
- Telnet
- WebView access
- HTTP/HTTPS
- RADIUS, LDAP, and SNMP

JITC Mode

Joint Interoperability Test Command (JITC) is a certification agency which provides risk based Test Evaluation & Certification services, tools, and environments for certifying IT products that are used in military and defense networks.

In JITC mode, the OmniSwitch enforces additional security measures as per the JITC certification agency requirements.

The following functionality comes into effect when the JITC mode is activated:

- The switch will display the date and time, the location of the last logon, the number of unsuccessful and successful login attempts of the administrator account on the SSH and Console session.

- The switch will store the successful and unsuccessful login attempts of the user and is displayed in the console session when the administrator logs into the switch. The record is stored for a 24 hour time period after which the login statistics are reset.
- The following user authentication changes are applied when JITC is activated:
 - The minimum password length must be 15 characters or more. The users with shorter password (less than 15 characters) will be forced to change the password.
 - The new password cannot be same as last five passwords.
 - The password expiration is by default set to 60 days.
 - The password expiration policy is applied to all the users except the admin (user with read and write privilege for all domains).
 - During password change it is required the characters are changed in at least eight positions within the password.
- When a user account is created, modified, and deleted on the switch, the administrator is notified in the swlog messages and SNMP traps.
- The switch will capture the successful and unsuccessful attempts to access, modify, or delete privileges. The information can be viewed in the SWlog of the switch.
- The SSH sessions will rekey at a minimum every one gigabyte or every 60 minutes of data received or transmitted.
- SSH uses Diffie-Hellman-Group14-SHA1 algorithm as the preferred key exchange mechanism.
- When the external TLS server does not support renegotiation_info extension (RFC 5746), the AOS TLS client applications actively terminates the TLS session.
- No compression is enabled in TLS communication by default.
- Site-Local IPv6 addresses of range FEC0::/10 (FEC, FED, FEE and FEF) cannot be configured.
- Software upgrades are allowed only after the digital signature of the software component is verified. During software upgrade, the SHA256 checksum of the images is verified against a file "imgsha256sum" stored in the image directory. If the checksum matches, the software upgrade is allowed.
- SWlog displays the start and end time of the administrator access to the system.
- User is required to re-authenticate for certain organization defined circumstances.
- The user session is terminated whenever a change is made to the user access privilege and when user account is deleted.
- The switch will generate audit logs for session timeouts.
- The switch will generate audit logs in an event of successful and unsuccessful attempts to access, modify, delete security levels and access, modify security objects.
- The switch will log destination IP address:
 - When switch acting as LDAP client opens connection to LDAP server in insecure (without TLS) and secured (with TLS) connection, if the username is found and password is correct.
 - When switch acting as RADIUS client opens connection to RADIUS server in insecure (without TLS) and secured (with TLS) connection, if the username is found and password is correct.
 - When switch acting as SYSLOG-NG client opens TLS connection to SYSLOG-NG server in secured connection successfully.
 - When switch acting as SNMP client sends trap to SNMP server in secured and insecure connection successfully.

To enable JITC mode, enter the command below:

```
-> aaa jitc admin-state enable
```

Save the configuration and reboot the switch for the JITC mode to be activated.

Please note that before enabling JITC mode, ensure enhanced mode or CC mode is disabled. JITC mode is mutually exclusive of enhanced mode and CC mode.

FIPS Mode

FIPS is a mode of operation that satisfies security requirements for cryptographic modules. It is a requirement as per the National Institute of Standards and Technology (NIST), FIPS 140-2 standard that strong cryptographic algorithms has to be supported to achieve FIPS compliance. When FIPS mode is enabled on OmniSwitch, FIPS 140-2 compliant encryption is used by the OmniSwitch devices in the various management interfaces such as SFTP, HTTP, SSH and SSL.

These strong cryptographic algorithms ensure secure communication with the device to provide interoperability, high quality, cryptographically-based security for IP networks through the use of appropriate security protocols, cryptographic algorithms, and keys and prevent any form of hijacking/hacking or attack on the device through the secure mode of communication.

FIPS mode functionality includes:

- FIPS operates in OpenSSL mode allowing only highly secure and strong cryptographic algorithms.
- OpenSSH and Web Server which use the OpenSSL as the underlying layer for secure communications also works in the FIPS mode.
- SNMPv3 supports secure SHA+AES. MD5 or DES are not allowed.
- The FIPS mode is enabled/disabled only with a reboot of the switch.

The SNMPv3 module as well as all switch management protocols such as SFTP, HTTP, SSH, and SSL use the FIPS 140-2 compliant encryption algorithms

To enable FIPS mode on OmniSwitch, you can use the following command:

```
-> system fips admin-state enable
WARNING: FIPS Admin State only becomes Operational after write memory and reload
```

Banner

The Login Banner feature allows you to change the banner that displays whenever someone logs into the switch. This feature can be used to display messages about user authorization and security. You can display the same banner for all login sessions or you can implement different banners for different login sessions. You can display a different banner for logins initiated by FTP sessions than for logins initiated by a direct console or a Telnet connection.

Two steps are required to change the login banner. These steps are listed here:

- Create a text file that contains the banner you want to display in the switch's **"/flash/switch"** directory.
- Enable the text file by entering the **"session banner"** CLI command followed by the filename.

To create the text file containing the banner text, you may use the **vi** text editor in the switch or you create the text file using a text editing software package and transfer the file to the switch's **"/flash/switch"** directory.

If you want the login banner in the text file to apply to CLI switch sessions, execute the following CLI command where the text filename is **banner.txt**.

```
-> session cli banner/flash/switch/banner.txt
```

By default, the switch does not display any text before the login prompt for any CLI session. At initial bootup, the switch creates a **"pre_banner.txt"** file in the **"/flash/switch"** directory. The file is empty and may be edited to include text that you want to display before the login prompt.

Recommendation: Setup a warning banner, which are brief messages that are used to inform users of policies and legislation.

Passwords

By default, the password for locally created user accounts will not appear in an ASCII configuration file created via the **"snapshot"** command.

When a new user is created or a password changed, a 16-byte random salt is concatenated with the password and

Recommendation: Configure a strong password policy on the switch to enforce password complexity when a password is created, modified, and used.

hashed. It will store both the salt and the hash to the local user database.

The global password policy settings for the switch define the following requirements that are applied to all user accounts:

- Minimum password size.

```
-> user password-size min 10
```

- Whether or not the password can contain the username.

```
-> user password-policy cannot-contain-username enable
```

- Whether or not the password can contain consecutive identical characters.

```
-> user password-policy cannot-contain-consecutive-characters enable
```

- The minimum number of uppercase/lowercase characters required in a password.

```
-> user password-policy min-uppercase 1
```

```
-> user password-policy min-lowercase 1
```

- The minimum number of base-10 digits required in a password.

```
-> user password-policy min-digit 1
```

- The minimum number of non-alphanumeric characters (symbols) required in a password.

```
-> user password-policy min-nonalpha 1
```

- Password expiration. (default or specific user)

```
-> user password-expiration 3
```

```
-> user bert password techpubs expiration 5
```

```
-> user bert password techpubs expiration 02/19/2025 13:30
```

- The maximum number of old passwords that are saved in the password history.

```
-> user password-history 2
```

- The minimum number of days during which a user is not allowed to change their password.

```
-> user password-min-age 7
```

Password policy settings are applied when a password is created or modified.

Control Plane

The control plane governs everything related to the forwarding of data packets in your network. It is responsible for the management and orchestration of various functions in your networking devices using control plane protocols. These functions include routing decisions and signaling and more. Therefore, it is imperative that the control plane is secure to ensure integrity, service availability, and reliability of your network infrastructure. There are many control plane protocols but they may fall into below categories:

- Routing Protocols such as RIP, OSPF, IS-IS, and BGP
- Label Distribution Protocols such as LDP
- Link Management Protocols such as LACP, STP, and BFD
- Discovery Protocols such as LLDP and ARP
- Network Management Protocols such as syslog, NTP, ICMP, DHCP
- Control Plane Protection Protocols such as DoS Filtering

- Other control plane security features such as switch supplicant

Securing Routing Protocols

RIP

Recommendation: Use MD5 authentication in networks that require RIP protocol.

Both switches on either end of a link must share the same password. Use the “ip rip interface auth-type” command to configure the authentication type. Enter the name of the RIP interface, and then enter an authentication type. For example, to configure the RIP interface rip-1 for MD5 authentication you would enter:

```
-> ip rip interface rip-1 md5 auth-type md5
```

If you configure MD5 authentication you must configure a text string that is used as the password for the RIP interface. If a password is used, all switches that are intended to communicate with each other must share the same password.

After configuring the interface for MD5 authentication as described above, configure the password for the interface by using the “ip rip interface auth-key” command. Enter the IP address of the RIP interface, and then enter a 16-byte text string. For example to configure a password “r1p@uTh” you would enter:

```
-> ip rip interface rip-1 auth-key r1p@uTh
```

OSPF

Open Shortest Path First (OSPF) Routing allows authentication on the configured interfaces. When authentication is enabled, only neighbors using the same type of authentication and the matching passwords or keys can communicate.

There are three types of authentication: simple, MD5, and Keychain authentication. Simple authentication requires only a text string as a password, MD5 is a form of encrypted authentication that requires a key and a password, and a keychain is a form of authentication that allows a regular rotation of keys to be used for limited periods of time. We will cover the keychain authentication as it is the most secure option.

Recommendation: Configure keychain authentication with key rotation between OSPF peers.

To configure the OSPF interface for keychain authentication, enter the “ip ospf interface auth-type” as shown:

```
-> security key 1 algorithm sha256 key O$pf@uTh123 start-time 01/01/2025 lifetime 90
-> security key 2 algorithm sha256 key O$pf@uTh456 start-time 01/04/2025 lifetime 60
-> security key 3 algorithm sha256 key O$pf@uTh789 start-time 31/05/2025
-> security key-chain 1 name "OSPF"
-> security key-chain 1 key 1-3
-> ip ospf interface vlan-101 auth-type key-chain 1
```

Default lifetime of keys is 180 days.

When the OSPF interface receives a packet, the authentication information is carried in the hello packet. If the authentication succeeds, then adjacency is formed. The authentication type can be set to SHA256 when using the **key-chain** parameter. The two remote machines must have the same active current key ID, key, and same authentication type and must use a valid start-time.

IS-IS

Intermediate System-to-Intermediate System (IS-IS) allow to configure authentication between IS-IS peers. When authentication is enabled, only neighbors using the same type of authentication and the matching keys can communicate.

There are three types of authentication: simple, MD5, and Keychain authentication. We will cover the keychain authentication as it is the most secure option.

Recommendation: Configure keychain authentication with key rotation between IS-IS peers.

Keychain authentication can be applied at a global level, capability level, circuit level, and capability level per circuit.

To enable keychain authentication on a router, enter **ip isis auth-type** command with the configured keychain to be used as shown.

```
-> ip isis auth-type key-chain 2
```

If a keychain is applied globally, the authentication algorithm of its active key will be used for adjacency formation with all peers.

To enable keychain authentication for specific IS-IS levels, use **ip isis level auth-type** command. For example, to enable the authentication for IS-IS Level-2, enter the following:

```
-> ip isis level 2 auth-type key-chain 1
```

To enable keychain authentication at a circuit level, use **ip isis vlan hello-auth-type** command. For example, to enable keychain authentication on the IS-IS circuit, enter the following.

```
-> ip isis vlan 100 hello-auth-type key-chain 1
```

Use **ip isis vlan hello-auth-type none** to remove the circuit level keychain authentication.

To enable keychain authentication at different levels of an IS-IS circuit, use **ip isis vlan level hello-auth-type** command. For example, to enable keychain authentication at Level-2 of an IS-IS circuit, enter the following:

```
-> ip isis vlan 100 level 2 hello-auth-type key-chain 1
```

Use **ip isis vlan level hello-auth-type none** to remove the capability level keychain authentication per circuit.

For example, to configure global keychain authentication with key rotation:

```
-> security key 1 algorithm sha256 key i5i5@uTh123 start-time 01/01/2025 lifetime 90
-> security key 2 algorithm sha256 key i5i5@uTh456 start-time 01/04/2025 lifetime 60
-> security key 3 algorithm sha256 key i5i5@uTh789 start-time 31/05/2025
-> security key-chain 1 name "IS-IS"
-> security key-chain 1 key 1-3
-> ip isis auth-type key-chain 1
```

BGP

Border Gateway Protocol (BGP) allows to configure authentication between BGP peers.

Recommendation: Configure MD5 authentication between BGP peers.

You can set which MD5 authentication key this router will use when contacting a peer. To set the MD5 authentication key, enter the peer IP address and key with the **ip bgp neighbor md5 key** command:

```
-> ip bgp neighbor 123.24.5.6 md5 key bGp@uTh123
```

The peer with IP address 123.24.5.6 will be sent messages using “keyname” as the encryption password. If this is not the password set on peer 123.24.5.6, then the local router will not be able to communicate with this peer.

For IPv6 BGP, you can set the MD5 authentication key, enter the peer IPv6 address and key with the **ipv6 bgp neighbor md5 key** command:

```
-> ipv6 bgp neighbor 2001::1 md5 key bGp@uTh123
```

Securing Label Distribution Protocols

The LDP protocol (Label Distribution Protocol) is used in MPLS network which generates and exchanges labels between neighboring routers. It is the set of messages exchanged by LSRs (Label Switched Routers) to establish LSPs (Label Switched Paths). A LSP is a path taken by all packets that belong to the Forwarding Equivalence Class (FEC) corresponding to that LSP.

To maintain integrity of LDP session messages and to prevent introduction of spoofed TCP segments in the LDP session connection stream, AOS provides MD5 key based authentication for LDP sessions. MD5 key (password) for each potential

Recommendation: Configure MD5 authentication between LDP peers.

LDP peer on a LDP enabled router can be configured. This key is used to compute and append a MD5 signature to each TCP segment carried by the corresponding LDP session to that peer. On the receiving end, the MD5 signature is validated to authenticate the peer.

Authentication must be configured on both LDP peers using the same MD5 key (password), otherwise the peer session will not be established.

To set a MD5 password for the TCP session with this LDP peer, use the “mpls ldp neighbor” command.

Use the “key” option to configure MD5 key for the specified LDP peer.

```
-> mpls ldp neighbor 5.5.5.5 md5 key lDp@uTh987
```

Securing Link Management Protocols

STP

Recommendation: Implement the below features to secure your network in addition to [Learned Port Security \(LPS\)](#) feature at the edge ports which provides a mechanism for authorizing source learning of MAC addresses on Ethernet ports.

Restricting Port Roles (Root Guard)

All ports are automatically eligible for root port selection. A port in a CIST/MSTI instance or per-VLAN instance can be prevented from becoming the root port by restricting the role of the port (also referred to as enabling root guard). This is done using the “spantree cist restricted-role” command or the “spantree vlan restricted-role” command regardless of which mode (per-VLAN or flat) is active for the switch. For example:

```
-> spantree cist port 1/1/2 restricted-role enable
-> spantree cist linkagg 10 restricted-role enable
-> spantree vlan 100 port 1/8/1 restricted-role enable
-> spantree vlan 20 linkagg 1 restricted-role enable
```

Note that the above commands also provide optional syntax; restricted-role or root-guard.

When root guard is enabled for a port, it cannot become the root port, even if it is the most likely candidate for becoming the root port. However, this same port is designated as the alternate port when the root port is selected.

Enabling the restricted role status is used by network administrators to prevent bridges external to the core region of the network from influencing the Spanning Tree topology. However, note that enabling the restricted role status for a port may impact connectivity within the network.

Recommendation: Enable Root Guard functionality on the downlink ports from the core (root) switches in your network.

Restricting TCN Propagation

All ports automatically propagate Topology Change Notifications (TCN) or Topology Changes (TC) to other ports. To restrict a port from propagating topology changes and notifications, use the spantree cist restricted-tcn command or the spantree vlan restricted-tcn command regardless of which mode (per-VLAN or flat) is active for the switch. For example:

```
-> spantree cist port 1/2/2 restricted-tcn enable
-> spantree cist linkagg 5 restricted-tcn enable
-> spantree vlan 10 port 1/1/5 restricted-tcn enable
-> spantree vlan 20 linkagg 1 restricted-tcn enable
```

Recommendation: Enable TCN Restriction feature on your edge ports

Enabling the restricted TCN status is used by network administrators to prevent bridges external to the core region of the network from causing unnecessary MAC address flushing in that region. However, note that enabling the restricted TCN status for a port may impact Spanning Tree connectivity.

Filter/Block BPDUs on User Ports

To prevent user ports from receiving unauthorized Bridge Protocol Data Units (BPDUs) from malicious devices, you should filter or block the user port when receiving such types of packets. First you will need to assign member ports of the pre-defined **UserPorts** group.

```
-> policy port group UserPorts 4/1/1-8 5/1/1-8
```

To filter BPDU packets when received on a user port:

```
-> qos user-port filter bpd
```

To shutdown a user port when receiving a BPDU packet:

```
-> qos user-port shutdown bpd
```

Recommendation: Filter or shutdown user port upon receiving a BPDU to protect the network from malicious or unauthorized devices being connected to the network.

Securing Discovery Protocols

LLDP

LLDP specifically defines a standard method for Ethernet network devices and Media Endpoint Devices (MED) to exchange information with its neighboring devices and maintain a database of the information. The exchanged information, passed as LLDPDU, is in TLV (Type, Length, Value) format. Each LLDPDU contains all the five mandatory TLVs and optional TLVs.

LLDP-MED is an extension to 802.1ab (Link Layer Discovery Protocol - LLDP), a link-layer protocol that defines a method for network access devices using Ethernet connectivity to advertise device information, device capabilities and media specific configuration information periodically to peer devices attached to the same network.

In order to secure the network access by detecting rogue devices and preventing them from accessing the internet network, the OmniSwitch LLDP Agent Security mechanism is implemented. LLDP agent security can be achieved by allowing only one trusted LLDP remote agent on a network port.

Recommendation: Configure LLDP Agent security feature

User is provided an option to configure the Chassis ID subtype that can be used in validating the Chassis ID type in the incoming LLDP PDU. If the Chassis ID is not configured, by default, the first LLDP remote agent is learnt with the received Chassis ID. When more than one LLDP agent is learned on a port, the port is moved to a violation state.

For example, when someone tries to take control over the network by connecting non-registered devices to an NNI port, the LLDP Security mechanism is activated. One or both of the following actions are performed according to the security configuration:

- When the rogue device is detected, a violation is reported on the port.
- The NNI port that is connected to the rogue device is blocked. Thus the rogue device is prevented from accessing the internal network.

LLDP security mechanism can be enabled or disabled globally at chassis level, at slot level, or at individual port level. When the LLDP agent security is enabled, the configured ports are monitored for reception of any LLDPDU. When an LLDPDU is received, the remote agent ID is learned and the port is considered as a trusted port if the port does not have any other LLDP remote agent assigned. If the remote agent chassis ID and port IDs received are already present in the trusted remote agent database on the same port, then the port remains in a trusted state.

However, a port is moved to violation state under the following conditions:

- When a link up is received on a LLDP security enabled port, if no LLDPDU is received even after three times the LLDP timer interval period (30 seconds), the port is moved to a violation state.
- If a trusted remote agent exists, and if no LLDP remote agent is learned even after three times the LLDP timer interval period (30 seconds), the port is moved to a violation state.
- If a new LLDP remote agent is learned after the link up and down, then the port is moved to a violation state.

- If the same chassis ID and port ID exist in the trusted remote agent database but on a different port, then the port remote agent is learned and the port is moved to a violation state.
- If a new LLDP remote agent is learned on a port that has a trusted LLDP remote agent, then the port is moved to a violation state.

Three actions can be configured when an LLDP security violation occurs. The different violation actions that can be configured are:

- trap - Generate a trap
- shutdown - Shutdown the port
- trap-and-shutdown - A trap is generated upon shutdown of the port due to violation.

When a shutdown occurs on a port, it can be cleared manually through the CLI interface using the clear violations command.

Example to configure LLDP Trust Agent based on the chassis-component to validate the remote agent. It will send a trap (which is the default) due to violation:

```
-> lldp chassis trust-agent admin-state enable
-> lldp chassis trust-agent violation-action trap
-> lldp chassis trust-agent chassis-id-subtype chassis-component
```

There are other options that can be configured to validate the remote agent. For more information, see the *OmniSwitch AOS Release 8 CLI Reference Guide* referenced in the [Related Documents](#) section.

ARP

ARP Filtering

ARP filtering is used to determine whether the switch responds to ARP requests that contain a specific IP address. ARP filtering is used in conjunction with the Local Proxy ARP application; however, it is available for use on its own or with other applications.

By default, no ARP filters exist in the switch configuration. When there are no filters present, all ARP packets are processed, unless they are blocked or redirected by some other feature.

Use the “arp filter” command to specify the following parameter values required to create an ARP filter:

- An IP address (for example, 193.204.173.21) used to determine whether an ARP packet is filtered.
- An IP mask (for example, 255.0.0.0) used to identify which part of the ARP packet IP address is compared to the filter IP address.
- An optional VLAN ID to specify that the filter is only applied to ARP packets from that VLAN.
- Which ARP packet IP address to use for filtering (sender or target). If the target IP address in the ARP packet matches a target IP specified in a filter, then the disposition for that filter applies to the ARP packet. If the sender IP address in the ARP packet matches a sender IP specified in a filter, then the disposition for that filter applies to the ARP packet.
- The filter disposition (block or allow). If an ARP packet meets filter criteria, the switch is either blocked from responding to the packet or allowed to respond to the packet depending on the filter disposition. Packets that do not meet any filter criteria are responded to by the switch.

Recommendation: Configure ARP filtering to control how ARP traffic is handled and prevent ARP spoofing, ARP poisoning, or Man-in-the-Middle (MiTM) attacks. This is useful in Layer 2 VLAN environments to prevent inter-VLAN spoofing attempts where a malicious device on one VLAN tries to impersonate a device on another VLAN. This ensures that devices only respond to ARP requests within their allowed IP-MAC range.

The following “arp filter” command example creates an ARP filter, which blocks the switch from responding to ARP packets that contain a sender IP address that starts with 198:

```
-> arp filter 198.0.0.0 mask 255.0.0.0 sender block
```

Gratuitous ARP

A Gratuitous ARP is an ARP broadcast in which the source and destination MAC addresses are the same. It is used to inform the network about a host IP address. A spoofed Gratuitous ARP message can

cause network mapping information to be stored incorrectly, causing network malfunction. The OmniSwitch allows to configure the Gratuitous ARP.

The incoming and outgoing Gratuitous ARP packets can be enabled or disabled on the switch.

By default, the outgoing Gratuitous ARP packets are enabled. The switch will send Gratuitous ARP packets every five minutes. To filter the Gratuitous packet, it must be disabled. The outgoing Gratuitous ARP packets can be enabled or disabled using the “arp send-gratuitous-arp” CLI command. For example, to disable:

```
-> ip send-gratuitous-arp disable
```

Recommendation: Block incoming GARP packets to avoid spoofed GARP messages which can be used in MiTM attacks and enable sending GARP packets. This will protect against ARP poisoning attacks.

By default, the incoming Gratuitous ARP packets are not blocked. To block the incoming Gratuitous ARP packets the feature must be enabled. The incoming Gratuitous ARP packets can be configured using the “ip dos type” CLI command.

For example, to block the incoming Gratuitous ARP packets:

```
-> ip dos type gratuitous-arp admin-state enable
```

ARP Poisoning

ARP Poisoning allows an attacker to sniff and tamper the data frames on a network. It also modifies or halts the traffic. The principle of ARP Poisoning is to send false or spoofed ARP messages to an Ethernet LAN.

The OmniSwitch introduces the functionality that detects the presence of an ARP poisoning host on a network. This functionality uses a configured restricted IP addresses, so that the switch does not get ARP response on sending an ARP request. If an ARP response is received, then an event is logged and the user is alerted using an SNMP trap.

Use the “ip dos arp-poison restricted-address” command to add an ARP Poison restricted address. Enter the command, followed by the IP address. For example, to add an ARP Poison restricted address as 192.168.1.1, you would enter:

```
-> ip dos arp-poison restricted-address 192.168.1.1
```

Recommendation: Configure ARP Poisoning detection and define restricted addresses on critical hosts such as servers, gateways and routers, critical IoT devices, firewalls and IDS/IPS systems, and endpoints for critical users.

To verify the number of attacks detected for configured ARP poison restricted addresses, use the “show ip dos arp-poison” command.

Securing Network Management Protocols

NTP

Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver. It provides client time accuracies within a millisecond on LANs, and up to a few tens of milliseconds on WANs relative to a primary server synchronized to Universal Coordinated Time (UTC) (via a Global Positioning Service receiver, for example). Typical NTP configurations utilize multiple redundant servers and diverse network paths in order to achieve high accuracy and reliability. Some configurations include cryptographic authentication to prevent accidental or malicious protocol attacks.

Recommendation: Configure NTP time synchronization for log accuracy and correlation, and for supporting auditing and compliance

There are several modes of operation that an NTP entity can use when synchronizing time in a network. These modes help predict how the entity behaves when requesting or sending time information, listed below:

- A switch can be a client of an NTP server (usually of a lower stratum), receiving time information from the server but not passing it on to other switches.
- A switch can be a client of an NTP server, and in turn be a server to another switch or switches.

- A switch (regardless of its status as either a client or server) must be peered with another switch. Peering allows NTP entities in the network of the same stratum to regard each other as reliable sources of time and exchange time information.
- The OmniSwitch by default will act as an NTP server and be able to respond to NTP client requests, and establish a client or server peering relationship. The OmniSwitch NTP server functionality allows the OmniSwitch to establish an active peering relationship with another server, enable broadcast server functionality, disable a given IP for NTP and employ MD5 authentication or SHA1 authentication for clients and active peers.

The following steps are designed to show the user the necessary commands to set up NTP on an OmniSwitch:

1. Designate an NTP server for the switch using the **ntp server** command. The NTP server provides the switch with its NTP time information. For example:

```
-> ntp server 198.206.181.13
```

NTP server configuration can also be done with hostname/FQDN. For example:

```
-> ntp server clock3.ovcirus.com
```

2. Activate the client side of NTP on the switch using the **ntp client** command. For example:

```
-> ntp client admin-state enable
```

Authentication is used to encrypt the NTP messages sent between the client and server. The NTP server and the NTP client must both have a text file containing the keys.

NTP is designed to use MD5 and SHA1 encryption authentication to prevent outside influence upon NTP timestamp information. This is done by using a key file. The key file is loaded into the switch memory, and consists of a text file that lists key identifiers that correspond to particular NTP entities.

Recommendation: Configure NTP with authentication and encryption to ensure the network switches are synchronized only with trusted and verified NTP servers.

If authentication is enabled on an NTP switch, any NTP message sent to the switch must contain the correct key ID in the message packet to use in decryption. Likewise, any message sent from the authentication enabled switch will not be readable unless the receiving NTP entity possesses the correct key ID.

The key file is a text (.txt) file that contains a list of keys that are used to authenticate NTP servers. Key files are created by a system administrator independent of the NTP protocol, and then placed in the switch memory when the switch boots.

In order to generate a key file, access to a Solaris/Unix environment is recommended. Also recommended is the ntp-keygen utility in Unix to generate the key file. As an alternative, the keys can be manually created.

In a key file, the first token is the key number ID, the second is the key format, and the third is the key itself.

The key file (with identical MD5 keys) must be located on both the local NTP client and the client's server.

The OmniSwitch establishes which key pair it is using for authentication by specifying a key ID for each NTP server configured.

Once both the client and server share a common encryption key, the key identification for the NTP server must be specified on and labeled as trusted on the client side. The Omniswitch will then use authentication. Key files must reside in **/flash/network/ntp.keys**.

Enabling authentication requires the following steps:

- Make sure the key file is located in the **flash/network** directory of the switch. This file must contain the key for the server that provides the switch with its timestamp information.
- Make sure the key file with the NTP server's key is loaded into the switch memory by issuing the **ntp key load** command, as shown:

```
-> ntp key load
```

- Enable server authentication and set the server authentication key identification number using the **ntp server** command with the **key** keyword. This key identification number must be the one the server uses for authentication. For example, to specify key identification number 2 for an NTP server with an IP address of 1.1.1.1, enter:

```
-> ntp authentication enable
-> ntp server 1.1.1.1 key 2
```

- Specify the key identification set above as *trusted*. A key that has been labeled as trusted is ready for use in the authentication process. To set a key identification to be trusted, enter the **ntp key** command with the key identification number and **trusted** keyword. For example, to set key ID 2 to trusted status, enter the following:

```
-> ntp key 2 trusted
```

Untrusted keys, even if they are in the switch memory and match an NTP server, will not authenticate NTP messages.

- A key can be set to untrusted status by using the **ntp key** command with the **untrusted** keyword. For example, to set key ID 5 to untrusted status, enter the following:

```
-> ntp key 5 untrusted
```

ICMP

Internet Control Message Protocol (ICMP) is a network layer protocol within the IP protocol suite that provides message packets to report errors and other IP packet processing information back to the source.

ICMP generates various kinds of useful messages, including Destination Unreachable, Echo Request and Reply, Redirect, Time Exceeded, and Router Advertisement and Solicitation. If an ICMP message cannot be delivered, a second one is not generated thus preventing an endless flood of ICMP messages.

When an ICMP destination-unreachable message is sent by a switch, it means that the switch is unable to send the package to its final destination. The switch then discards the original packet. There are two reasons why a destination is not reachable. Most commonly, the source host has specified a non-existent address. Less frequently, the switch does not have a route to the destination.

ICMP messages are identified by a type and a code. This number pair specifies an ICMP message. For example, ICMP type 4, code 0, specifies the source quench ICMP message. To disable an ICMP message, use the “icmp type” command with the type and code. For example, to disable the source quench the ICMP message (type 4, code 0) enter the following:

```
-> icmp type 4 code 0 disable
```

In addition to the ICMP type command, many commonly used ICMP messages have separate CLI commands for convenience. For example, to disable a network unreachable message, enter the following:

```
-> icmp unreachable net-unreachable disable
```

Recommendation: Disable all unused IPv4 ICMP messages as highlighted in the table below.

ICMP Messages to consider disabling include:

ICMP Type	Purpose	Risk	Recommendation
ICMP Echo Reply (Type 0)	Used as a response to an ICMP Echo Request	Can be used in Smurf DoS attacks	Disable
ICMP Redirect (Type 5)	Informs a host of a better route for traffic	Can be used in MiTM attacks	Disable
ICMP Echo Request (Type 8)	Used in ICMP Ping requests	Can be used as a DoS attack and for network discovery during reconnaissance	Disable unless required
ICMP Router Advertisement and Selection (Types 9 and 10)	Used for discovering and selecting routers	Malicious attackers can spoof advertisements	Disable unless required
ICMP Timestamp Request and Reply (Types 13 and 14)	Used to synchronize time or measure latency	Malicious attackers can deduce network uptime and host activity	Disable unless required
ICMP Address Mask Request and Reply (Types 17 and 18)	Used to discover the subnet mask of a network	Can reveal network configuration to malicious attackers	Disable unless required

ICMP Messages to use cautiously:

ICMP Type	Purpose	Risk	Recommendation
ICMP Unreachable (Type 3)	Used to indicate destination is unreachable	Can be used by malicious attacker for network discovery during reconnaissance	Selectively allow for diagnostics but restrict exposure
ICMP Time Exceeded (Type 11)	Used to indicate that a packet's TTL has expired	Can be used by malicious attacker for network discovery during reconnaissance	Selectively allow for diagnostics but restrict exposure

DHCP

There are two DHCP security features available: DHCP relay agent information option (Option-82) and DHCP Snooping.

- The DHCP Option-82 feature enables the relay agent to insert identifying information into client-originated DHCP packets before the packets are forwarded to the DHCP server.
- The DHCP Snooping feature filters DHCP packets between untrusted sources and a trusted DHCP server and builds a binding database to log DHCP client information.

Although DHCP Option-82 is a subcomponent of DHCP Snooping, these two features are mutually exclusive. If the DHCP Option-82 feature is enabled for the switch, then DHCP Snooping is not available.

The reverse is also true; if DHCP Snooping is enabled, then DHCP Option-82 is not available. In addition, the following differences exist between these two features:

- DHCP Snooping does require and use the Option-82 data insertion capability, but does not implement any other behaviors defined in RFC 3046.
- DHCP Snooping is configurable at the switch level and on a per-VLAN basis, but DHCP Option-82 is only configurable at the switch level.

Recommendation: Configure DHCP Snooping feature along with Dynamic ARP Inspection (IP Source Filtering).

DHCP Option-82

Use the “ip dhcp relay insert-agent-information” command to enable the DHCP Option-82 feature for the switch. For example:

```
-> ip dhcp relay insert-agent-information
```

When the relay agent receives a DHCP packet from a client that already contains Option-82 data, the packet is dropped by default.

DHCP Snooping

In order to identify DHCP traffic that originates from outside the network, DHCP Snooping categorizes ports as either trusted or untrusted. A port is trusted if it is connected to a device inside the network, such as a DHCP server. A port is untrusted if it is connected to a device outside the network, such as a customer switch or workstation.

When DHCP Snooping is first enabled, all ports are considered untrusted.

To enable DHCP Snooping feature at the switch level, use the “dhcp-snooping admin-state” command. For example:

```
-> dhcp-snooping admin-state enable
```

To enable DHCP Snooping at the VLAN level, use the “dhcp-snooping vlan” command. For example, the following command enables DHCP Snooping for VLAN 200:

```
-> dhcp-snooping vlan 200 admin-state enable
```

By default, when DHCP Snooping is enabled for a specific VLAN, MAC address verification and Option-82 data insertion is also enabled for the VLAN by default.

To configure the trust mode for one or more ports, use the “dhcp-snooping port” command:

```
-> dhcp-snooping port 1/2/1 trust
```

DHCP Snooping on a service can be enabled using the dhcp-snooping service admin-state CLI. For example:

```
-> dhcp-snooping service 23 admin-state enable
```

Dynamic ARP Inspection (DAI) - IP Source Filtering

DAI, also called IP Source Filtering, applies to DHCP Snooping ports and restricts port traffic to only packets that contain the proper client source information in the packet. The DHCP Snooping binding table is used to verify the client information for the port that is enabled for IP source filtering.

The IP source filtering configuration for a port or VLAN is not active unless the IP source filtering feature is globally enabled for the switch. By default, the IP source filtering functionality is enabled for the switch.

In addition, the global IP source filtering status is not changed when the DHCP Snooping status is changed. For example, if DHCP Snooping is disabled for the switch and IP source filtering is enabled, IP source filtering functionality is still enabled and applied to static binding table entries.

DHCP Snooping binding and IP source filtering can be combined to enable DAI. For example, to configure DAI, we can enable DHCP Snooping on VLAN 140 and configure port 1/1/5 as a trusted port:

```
-> dhcp-snooping vlan 140 admin-state enable
-> dhcp-snooping binding admin-state enable
-> dhcp-snooping port 1/1/5 trust (DHCP Server Port)
-> dhcp-snooping ip-source-filter vlan 140 admin-state enable
```

DHCPv6 Snooping

DHCPv6 Snooping monitors DHCPv6 client and server exchanges passing through the switch. It builds a binding table database of DHCPv6-assigned addresses based on the contents of those exchanges. The binding table is used by IPv6 Source Filtering to prevent unauthorized hosts from sending packets via the switch.

Recommendation: Configure DHCPv6 snooping and IPv6 source filtering features in IPv6 environments

Note that enabling DHCPv6 snooping feature only inspects DHCPv6 messages and verifies that they come from trusted sources. To prevent unauthorized hosts from sending packets via the switch, IPv6 Source Filtering feature has to be enabled in conjunction with DHCPv6 snooping.

DHCPv6 Snooping can be enabled globally or per-VLAN basis. The global DHCPv6 Snooping and per-VLAN DHCPv6 Snooping are mutually exclusive.

To enable DHCPv6 Snooping at the VLAN level, use the dhcpv6-snooping vlan admin-state command. For example, the following command enables DHCPv6 Snooping for VLAN 200:

```
-> dhcpv6-snooping vlan 200 admin-state enable
```

When enabled on a VLAN, DHCPv6 Snooping will monitor all DHCPv6 client and server exchanges and populate the binding table based on the message contents.

The global DHCPv6 Snooping must be disabled before enabling the per-VLAN DHCPv6 Snooping.

Apart from VLAN-Level DHCPv6 Snooping, DHCPv6 Snooping can be enabled globally for the switch. To enable this feature globally, use the dhcpv6-snooping global admin-state command. For example:

```
-> dhcpv6-snooping global admin-state enable
```


The per-VLAN DHCPv6 Snooping must be disabled before enabling global DHCPv6 Snooping. When global DHCPv6 Snooping is enabled, the DHCPv6 Snooping binding table will be constructed based on DHCPv6 client and server exchanges seen on any VLAN.

IPv6 Source Filtering

IPv6 source filtering applies to DHCPv6 Snooping ports, link aggregates, and VLANs and restricts port traffic to only packets that contain the client source MAC address, IPv6 address, and VLAN combination.

The DHCPv6 Snooping binding table is used to verify the client information for the port or VLAN that is enabled for IPv6 source filtering.

IPv6 source filtering can be enabled per-VLAN or per-port (link aggregate). These two are mutually exclusive.

To support IPv6 source filtering on the OmniSwitch 6560 and OmniSwitch 6570M, the TCAM mode for the switch must be changed to source IPv6 filtering. Also, To support bi-directional source filtering on OmniSwitch 9907, OmniSwitch 9912 and OmniSwitch 6560, the TCAM mode for the switch must be changed to source and destination IPv6 filtering. Please refer to the “AOS 8.x Network Configuration guide” referenced in the [Related Documents](#) section for more details.

Port source filtering is based on the interface number, source MAC address, and source IPv6 address. By default, IPv6 source filtering is disabled for a DHCPv6 Snooping port or a link aggregate. Use the “dhcpv6-snooping ipv6-source-filter” command to enable or disable ISF for a specific port, range of ports, or a link aggregate. For example:

To enable source filtering on individual chassis and port 1/1/1, enter:

```
-> dhcpv6-snooping ipv6-source-filter port 1/1/1 admin-state enable
```

VLAN source filtering is based on the source VLAN ID, interface number, source MAC address, and source IPv6 address. IPv6 source filtering can be enabled at a VLAN level and the ports associated with the VLAN when DHCPv6 Snooping is enabled at the system level or VLAN level.

By default, IPv6 source filtering is disabled for a DHCP Snooping VLAN. Use the “dhcpv6-snooping ipv6-source-filter” command to enable or disable ISF for a VLAN. For example, to enable source filtering on VLAN 10, enter:

```
-> dhcpv6-snooping ipv6-source-filter vlan 10 admin-state enable
```

IPv6 DHCP Guard

DHCPv6 Guard protects the host connected to the switched network against rogue DHCPv6 servers. When this functionality is enabled, DHCPv6 server messages are discarded unless the messages are received on trusted source ports. DHCPv6 Guard functionality can also be applied to client messages to ensure that client messages are sent out only on trusted source ports.

Configuring ports as trusted sources provides a filtering mechanism to allow or drop DHCPv6 messages.

- Enabling DHCPv6 Guard and configuring trusted ports restricts DHCPv6 client and server messages to only those ports designated as trusted.
- Enabling DHCPv6 Guard without configuring any trusted ports helps to prevent unwanted DHCPv6 traffic flow through the switch. For example:
 - DHCPv6 server messages are discarded, which helps to prevent messages from reaching clients on the VLAN.
 - If DHCPv6 Guard for client messages is enabled, then DHCPv6 multicast client messages are also discarded. This helps to prevent DHCPv6 traffic from getting past the switch. If there are no client messages sent out, then there are no responses sent from the DHCPv6 server.

DHCPv6 Guard is configured on a per-VLAN basis. Make sure ports configured as trusted sources are members of the

Recommendation: Configure DHCPv6 Guard in IPv6 environments.

VLAN on which DHCPv6 Guard is configured.

To configure IPv6 DHCP Guard feature, enable DHCPv6 Guard on a VLAN, optionally enable DHCPv6 Guard for client messages, and finally configure switch ports or link aggregates or port range or link aggregate range as trusted DHCPv6 Guard ports. For example:

```
-> ipv6 dhcp guard vlan 200 admin-state enable
-> ipv6 dhcp guard vlan 200 client enable
-> ipv6 dhcp guard vlan 200 trusted port 2/1/11
```

MVRP

Multiple VLAN Registration Protocol (MVRP) provides a mechanism for dynamic maintenance of the contents of dynamic VLAN registration entries for each VLAN, and for propagating the information they contain to other bridges. This information allows MVRP-aware devices to dynamically establish and update their knowledge of the set of VLANs that currently have active members, and through which ports those members can be reached.

The main purpose of MVRP is to allow switches to automatically discover some of the VLAN information that would otherwise have to be manually configured.

Recommendation: Disable MVRP unless required

To disable MVRP globally on the switch, use “disable” option of the “mvrp” command as shown:

```
-> mvrp disable
```

Control Plane Protection Protocols

DoS Filtering

By default, the switch filters denial of service (DoS) attacks, which are security attacks aimed at devices that are available on a private network or the Internet. Some attacks aim at system bugs or vulnerability, while other types of attacks involve generating large volumes of traffic so that network service is denied to legitimate network users. These attacks include the following:

- **ICMP Ping of Death**—Ping packets that exceed the largest IP datagram size (65535 bytes) are sent to a host and crash the system.
- **Land Attack**—Spoofed packets are sent with the SYN flag set to a host on any open port that is listening. The machine can crash or reboot in an attempt to respond.
- **ARP Flood Attack**—Floods a switch with a large number of ARP requests, resulting in the switch using a large amount of the CPU time to respond to these requests. If the number of ARP requests exceeds the preset value of 500 per second, an attack is detected.
- **Invalid IP Attack**—Packets with invalid source or destination IP addresses are received by the switch. When such an Invalid-IP attack is detected, the packets are dropped, and SNMP traps are generated.
- **Multicast IP and MAC Address Mismatch**—This attack is detected when:
 - the source MAC address of a packet received by a switch is a Multicast MAC address.
 - the destination IP and MAC addresses of a packet received by a switch is same as the Multicast IP and MAC addresses, but the Multicast IP and the Multicast MAC addresses do not match.In both the conditions described above in “Multicast IP and MAC Address Mismatch”, packets are dropped and SNMP traps are generated.
 - the destination IP is a unicast IP and the destination MAC address is either a Broadcast or Multicast address. In such a condition, an event is recorded in the DoS statistics. No SNMP traps are generated as valid packets can also fall under this category.
- **Ping overload**—Floods a switch with a large number of ICMP packets, resulting in the switch using a large amount of CPU time to respond to these packets. If the number of ICMP packets exceed 100 per second, a DoS attack is detected. By default, the detection of attack is disabled.
- **Packets with loopback source IP address**—Packets with an invalid source address of 127.0.0.0/8 (loopback network) are received by the switch. When such packets are detected, they are dropped, and SNMP traps are generated.
- **IP options filter**—The ingress packets with IP options are detected and dropped.

The switch can be set to detect various types of port scans by monitoring for TCP or UDP packets sent to open or closed ports. Monitoring is done in the following manner:

- **Packet penalty values set.** TCP and UDP packets destined for open or closed ports are assigned a penalty value. Each time a packet of this type is received, its assigned penalty value is added to a running total. This

total is cumulative and includes all TCP and UDP packets destined for open or closed ports. For example, to assign a penalty value of 10 to TCP/UDP packets destined for closed ports, enter the following:

```
-> ip dos scan close-port-penalty 10
```

- Port scan penalty value threshold. The switch is given a port scan penalty value threshold. This number is the maximum value the running penalty total can achieve before triggering an SNMP trap. For example, to set the port scan penalty value threshold to 2000, enter the following:

```
-> ip dos scan threshold 2000
```

- Decay value. A decay value is set. The running penalty total is divided by the decay value every minute. For example, to set the decay value to 2, enter the following:

```
-> ip dos scan decay 2
```

- Trap generation. If the total penalty value exceeds the set port scan penalty value threshold, a trap is generated to alert the administrator that a port scan can be in progress. To enable SNMP trap generation, enter the ip dos trap command, as shown:

```
-> ip dos trap enable
```

Other Control Plane Security Features

Switch Supplicant

As part of the switch-security feature, the switch can be enabled with supplicant support, allowing the switch to take up the role of an 802.1x client.

Upon enabling this feature, the switch will, by default, be categorized as non-authenticated and subsequently transition to a restricted state. Only the interface connected to the NAS switch will remain in the enabled state, to undergo the 802.1x authentication process.

All other user interfaces which were admin-enabled will be moved to operationally down state, excluding VFL-ports.

Once the switch gets authenticated, based on the authentication result, the switch will be moved out of restricted state, ie, all admin-enabled interfaces will be made operationally up.

For the switch to undergo supplicant authentication, this feature will provide an ALE-default X509 certificate. The switch can also be configured with a custom X509 certificate which will be used for 802.1x authentication of the switch. The custom certificate can be either copied manually or can be downloaded from OmniVista to the switch.

On the NAS switch side, UNP port functionality is enhanced to handle an AOS switch connected as a supplicant. First the supplicant switch will be learnt on the UNP port using 802.1x authentication method. Based on the result of supplicant switch authentication, the clients of the supplicant switch will be learnt in either trust-tag or using UNP learning process.

Recommendation: Configure the switch supplicant feature using custom certificates for enhanced network security and to prevent MiTM attacks.

Before supplicant feature is enabled on the switch, the OmniSwitch has to be loaded with required X509 client certificate, key file and required CA certificates.

Steps to configure default AOS supplicant X509 certificates for switch supplicant feature:

1. By default, the default supplicant features will be generated. To configure usage of default certificates for switch-supplicant feature, use the following command:

```
-> aaa certificate update-supplicant-certificate default
```

2. To upload and configure Custom CA certificates, do the following:

- a. Upload CA certificate to "/flash/switch/ca.d/"
- b. Update the CA certificate for supplicant feature using the following CLI command:

```
-> aaa certificate update-supplicant-ca-cert ca.pem
```

3. To upload and configure Client X509 certificates for switch supplicant feature, do the following:

- a. Upload client X509 certificate file to "/flash/switch/cert.d/"
- b. Upload client key file to "/flash/switch/cert.d/"
- c. Use the following CLI command to update client certificate and key file for switch supplicant feature.

```
-> aaa certificate update-suppliant-certificate "client.pem" key-file
"client.key" identity "ale6560sw" key-passwd alcatel
```

To enable switch-suppliant feature on the switch:

1. Identify the port or linkagg on which the switch is connected to the NAS switch.
2. Use the following CLI command to enable the switch-suppliant feature. For example:

```
-> aaa switch-suppliant port 1/1/10
```

3. Use show aaa switch-suppliant status command to check the status of switch-suppliant authentication. For example:

```
-> show aaa switch-suppliant status
suppliant-status : Enabled,
Port/LAG : 1/1/10,
MAC : 2C:FA:A2:94:D1:EB,
Authentication-state : Init,
Authentication-Time : 01/01/1970 00:00:00,
Certificate Used : Custom,
CA-Certificate : -,
Client-Certificate : "/flash/switch/cert.d/myCliCert.pem",
Client-Key : "/flash/switch/cert.d/myCliPrivate.key",
Identity : "username",
Private-key-passwd : "password"
```

Data Plane

The data plane handles traffic passing through the network device. This can include QoS policies, Access Control Lists (ACLs), and encryption.

MACsec

MACsec (MAC Security) provides point-to-point security on Ethernet links between directly connected nodes. MACsec prevents DoS/M-in-M/playback attacks, intrusion, wire-tapping, masquerading, and so on. MACsec can be used to secure traffic on Ethernet links - LLDP frames, LACP frames, DHCP/ARP packets, and so on.

MACsec-enabled links are secured by matching security keys. Data integrity checks are done by appending an 8-byte or 16-byte header and a 16-byte tail to all Ethernet frames traversing the secured link. Optionally, traffic can also be encrypted, if enabled by user configuration.

On the wire, a MACsec packet starts with an Ethernet header with etherType 0x88E5, followed by an 8- byte or 16-byte SecTag header containing information about the decryption key, a packet number and Secure Channel Identifier. The SecTag header is followed by the payload (which may be optionally encrypted), and the Integrity Check Value (ICV) generated by GCM-AES of size 16 bytes.

Each node in a MACsec-protected network has at least one transmit secure channel associated with a Secure Channel Identifier (SCI). Configuration parameters such as enable encryption or perform replay protection are stored in the context of the transmit secure channel. A single secure channel is unidirectional - that is, it can be applied to either inbound or outbound traffic.

Each node that expects to receive traffic sent in a particular transmit secure channel must configure a 'matching' receive secure channel, with an SCI corresponding to the SCI of the transmit secure channel of the peer.

Within each secure channel, secure associations (SA) are defined. The SAs hold the encryption keys identified by their association number (AN), along with a packet number. On the transmit side, this packet number is put in the MACsec SecTag header and used in the encryption process. On the receive side, the packet number from the SecTag header will be checked against the packet number locally stored in the corresponding secure association to perform replay protection.

The default crypto suite used in MACsec is "128-bit AES-GCM" and the Session key is called a "Secure Association Key (SAK)". Each endpoint in a MACsec-protected network has at least one Tx Secure Channel (SCI-Tx) and multiple Rx Secure Channels (SCI-Rx). Between MACsec secure link, each endpoint point is configured with a matching SCI-Tx and

SCI-Rx pair in both direction. Each Secure- Channel (SC) is associated with Secure Associations (SAs), which in turn holds the Secure Association Keys (SAK) along with a Packet Number (PN).

MACsec supports two SA modes:

- Static SA Mode - MACsec with Static Secure Association Key (static-SAK)
- Dynamic SA Mode - MACsec with Dynamic SAK using MACsec Key Agreement (MKA) Protocol. The MKA, as described in IEEE 802.1X-2010, is an extension to 802.1X, which provides the required session keys and manages the required encryption keys used by the underlying MACsec protocol. The MKA protocol allows peer discovery with confirmation of mutual authentication and sharing of MACsec secret keys to protect data exchanged by the peers.

There are two modes of provisioning connectivity association keys (CAK/CKN) between two MACsec endpoints. OmniSwitch supports the following:

- Dynamic SAK using Pre-Shared Key (PSK). MACsec using Static Connectivity Association Key (static-CAK) using PSK
- Dynamic SAK using Extensible Authentication Protocol (EAP). MACsec using Dynamic Connectivity Association Key (dynamic-CAK) using EAP.

To support non-interrupting MACsec service, four keys are supported for each secure channel in MACsec Static Mode. One key is used for actively protecting the traffic, while the other keys are programmed into hardware to be used as backup. This would reduce the frequency that SW has to be interrupted to setup a new key. In MACsec Dynamic Mode, the key rotation would be handled in SW using packet number (PN) rollover using MKA protocol.

To configure MACsec on an interface, use the “interfaces macsec admin-state” command to :

- Enable or disable MACsec on a physical port or a port range.
- Set the MACsec mode and additional configuration:
 - Static SA Mode
 - Set the MACsec mode to ‘static’. By default, the MACsec mode is set to ‘static’.
 - Create MACsec Tx and Rx channels.
 - Specify the SCI value for Tx and Rx channels.
 - Associate the keychain ID for Tx and Rx channel. The keychain associated with the SCI-Tx and SCI-Rx must have four keys supporting ‘AES-GCM-128’ algorithm, and the number of keys in the keychain associated with both SCI-Tx and SCI-Rx on an interface must be equal.
 - Enable or disable encryption on Tx and Rx channel (optional).
 - Dynamic SA Mode which has two variations: Dynamic SAK using pre-shared keys and Dynamic SAK using EAP.
 - Using PSK:
 - Set the MACsec mode to ‘dynamic’.
 - Configure the keychain for Static-CAK. The keychain or pre-shared key for Static-CAK must have the key mapped either to ‘AES-CMAC-128’ algorithm or ‘AES-CMAC-256’ algorithm. AES-CMAC-256 option would be supported only on platforms supporting 256-bit key. View show interfaces capability output to check if the interfaces has the support for MACsec 256-bit encryption.
 - Configure key server priority (optional).
 - Configure transmit interval for MKPDUs (optional).
 - Enable or disable encryption on dynamic secure channel. (optional)
 - Using EAP:
 - Set the MACsec mode to ‘radius’.
 - Configure transmit interval for MKPDUs (optional).
 - Enable or disable encryption on dynamic secure channel (optional).

For example, the following configures MACsec to static mode:

```
-> security key 1 algorithm aes-gcm-128 hex-key 0x0102030405060708090A0B0C0D0E0F
-> interface port 1/1/1 macsec admin-state enable mode static sci-tx 0x1 key-chain 1
encryption sci-rx 0x1 key-chain 1 encryption
```

The following configures MACsec to dynamic using static CAK:

```
-> security key 1 algorithm aes-cmac-128 hex-key 0x0102030405060708090A0B0C0D0E0F
keyed-name 0x0102030405060708090A0B0C0D0FFF
-> interface port 1/1/1 macsec admin-state enable mode dynamic key-chain 1 server-
priority 10 transmit-interval 3
```

The following configures MACsec to dynamic SAK using EAP:

```
-> interface port 1/1/1 macsec admin-state enable mode dynamic radius
```

Recommendation: Configure MACsec for integrity and encryption between critical endpoints if supported on your switching model.

IPv4 and IPv6

IP-Directed Broadcasts

An IP directed broadcast is an IP datagram that has all zeros or all 1 in the host portion of the destination IP address. The packet is sent to the broadcast address of a subnet to which the sender is not directly attached. Directed broadcasts are used in denial-of-service (DoS) attacks. In a DoS attack, a continuous stream of ping requests is sent from a falsified source address to a directed broadcast address, resulting in a large stream of replies, which can overload the host of the source address. By default, the switch drops directed broadcasts.

Recommendation: Disable directed broadcasts.

Use the “ip directed-broadcast” command to disable IP-directed broadcasts. For example:

```
-> ip directed-broadcast disable
```

If required, you can configure Controlled Directed Broadcasts to direct only the packet from trusted source to the destined network, while the other directed broadcast packets are dropped. IP directed broadcast must be enabled for the controlled IP directed broadcast to work.

Example:

```
-> ip directed-broadcast trusted-source-ip 30.0.0.0/24 destination-ip
10.0.0.255/24
```

IPv6 Route Advertisement Filtering

Router Advertisement (RA) filtering can be used to prevent the spread of rogue RAs from unauthorized systems. If enabled on an interface, any received RAs will be dropped without being forwarded on to any other connected IPv6 clients.

Recommendation: Configure IPv6 RA Filtering in IPv6 environments to prevent rogue RA from unauthorized systems.

One or more trusted ports or linkaggs can be specified for an interface. RAs received on those trusted ports or linkaggs will be allowed to continue on to all other IPv6 clients reached via the interface.

To enable RA filtering on an interface, use the “ipv6 ra-filter trusted” command. For example:

```
-> ipv6 ra-filter vlan-3
```

This example enables RA filtering on the “vlan-3” interface. All RAs received on the interface will be dropped.

To specify a trusted port, use the “ipv6 ra-filter trusted” command with the “trusted-port” option. For example:

```
-> ipv6 ra-filter vlan-3 trusted port 1/1/22
```

This specifies that port 1/1/22 is trusted on the “vlan-3” interface. RAs received on this port will be forwarded to all other clients connected to the interface. RAs received on any other port will still be dropped.

IPv6 Neighbor Cache Limit

The size of the neighbor cache can be limited on a system-wide basis. Once the limit is reached, no new entries will be added. The system-wide limit can be used to control the resources allocated for the IPv6 neighbor cache.

A neighbor cache limit may also be specified on a per-interface basis. Once the interface's limit is reached, no new neighbor entries are allowed. The per-interface limit can be used to prevent any particular node attached to an interface from flooding the cache, either maliciously or due to a malfunction.

To set the system-wide cache limit, use the “ipv6 neighbor limit” command. For example, the following command sets the system-wide cache limit to 9000 entries:

```
-> ipv6 neighbor limit 9000
```

Recommendation: Configure IPv6 Neighbor Cache Limit to prevent DoS attacks that exhaust network resources.

To set the per-interface limit, use the ipv6 interface commands ‘neighbor limit’ option. For example, the following command sets the “vlan_1” interface limit to 100 entries:

```
-> ipv6 interface vlan_1 neighbor-limit 100
```

Learned Port Security

Learned Port Security (LPS) provides a mechanism for authorizing source learning of MAC addresses on Ethernet ports. Using LPS to control source MAC address learning provides the following benefits:

- A configurable source learning time limit that applies to all LPS ports.
- A configurable limit on the number of MAC addresses (bridged and filtered) allowed on an LPS port.
- Dynamic configuration of a list of authorized source MAC addresses.
- Static configuration of a list of authorized source MAC addresses.
- Three methods for handling unauthorized traffic: administratively disable the LPS port, stop all traffic on the port (port remains up), or only block traffic that violates LPS criteria.

LPS functionality is supported on the following port types:

- Fixed
- 802.1Q tagged
- Universal Network Profile (UNP)
- Static and dynamic SAP ports

Recommendation: Configure LPS on all edge ports to protect against unauthorized device connections

Below is an example of how to configure LPS for the following tasks:

- Enabling LPS on a set of switch ports.

```
-> port-security port 1/1/6-8 admin-state enable
```

- Defining the maximum number of learned MAC addresses allowed on an LPS port.

```
-> port-security port 1/1/6-8 maximum 1
```

- Defining the time limit for which source learning is allowed on all LPS ports.

```
-> port-security learning-window 30
```


- Convert all MAC addresses dynamically learned on the LPS port(s) to static MAC addresses.

```
-> port-security port 1/4/8 convert-to-static
```

- Selecting a method for handling unauthorized traffic received on an LPS port.

```
-> port-security port 1/1/6-8 violation shutdown
```

For more details, please refer to the Network Configuration Guide referenced in the [Related Documents](#) section.

Wireless Network Security

Management Plane

Stellar WiFi Express - Change Default Passwords

Recommendation: Change the default passwords for the predefined login accounts.

When accessing the Stellar AP GUI (Wi-Fi Express mode), the configuration wizards guides you to change the administrator password as shown below.

For security purposes, the admin should change the CLI root and support passwords before use. This is available under the “Advanced” window in the setup wizard as shown below.

Setup Wizard

Step 1/3 Change your administrator password

Administrator

Password:

Confirm:

[Advanced](#)

You can also change them in the main page by browsing to General Configuration -> Account Management as shown below:

General Configuration

Group Info Management Account Management Certificate Management Service Management

Support Account

Password: (Please enter 4-16 characters except '\', '~') (4-16 chars)

Confirm:

Root Account

Password: (Please enter 4-16 characters except '\', '~') (4-16 chars)

Confirm:

Certificate Management

Stellar APs support different types of certificates. There are built-in certificates used for some use cases, but users can customize their own certificate on demand:

1. Internal Web Server - The certificate is utilized to setup the secure connection between web browser and AP web server for HTTPS management. By default, there is a build-in CA certificate generated by ALE with the domain 'mywifi.al-enterprise.com'. User can use openssl to generate his/her own CA certificate and replace the default one (User needs to use domain 'mywifi.al-enterprise.com' for your own certificate because the login URL cannot be changed). We will cover the configuration details in this section.
2. Internal/External Portal Server - The certificate is utilized to setup the secure connection between captive portal page and the AP web server for protecting the user login credentials being stolen. Users can define their own captive login URL and replace the certificate accordingly. This will be covered in more details in the Control Plane [Certificate Management](#) section.
3. Local LDAP Certificate - Used to establish a secure connection between an AP and a Local LDAP Server. This will be covered in more details in the Control Plane [Certificate Management](#) section.
4. 802.1X Client Certificate - Used to establish a secure connection between an AP and an OmniSwitch. This will be covered in more details in the Control Plane [Certificate Management](#) section.
5. Stellar BLE Certificate - Used to establish a secure connection between an AP and a BLE destination server for Asset Tracking. This will not be covered in this document. Please refer to the OmniVista User Documentation as referenced in the [Related Documents](#) section for more details.
6. Stellar WiFi RTLS Certificate - Used to establish a secure connection between an AP and an external server to provide real-time location data. This will not be covered in this document. Please refer to the OmniVista User Documentation as referenced in the [Related Documents](#) section for more details.
7. Local Radsec - Used to establish a secure connection between an AP and a local, third-party RADIUS Server that uses RadSec (RADIUS-over-TLS). User can define his/her own certificate for Radsec accordingly. This will be covered in more details in the Control Plane [Certificate Management](#) section.
8. Syslog Over TLS - Used to establish a secure connection between an AP and a remote Syslog Server. User can define his/her own certificate for syslog over TLS accordingly. We will cover the configuration details in this section.

Stellar WiFi Express Internal Web Server - Install Built-in CA certificate to Trust Store

There are two methods to login to the AP group web management system:

1. HTTP protocol with URL `http://AP-IP:8080` (For example: `http://172.16.101.34:8080`) or `http://mywifi.al-enterprise.com:8080`, which is simpler and easier for the user without needing to install the digital certificate;
2. HTTPS protocol with URL `https://AP-IP` (For example: `https://172.16.101.34`) or `https://mywifi.al-enterprise.com`, which is more secure communication between AP and the browser.

Recommendation: Only use HTTPS for AP web management

There are two options for HTTPS access:

1. Use the built-in certificate. If you want to access with HTTPS, a CA root needs to be downloaded from the AP and installed into the trust store of the browser used. The certificate installation procedure varies from operating system and browser combinations. You can follow below illustrated steps to install the root CA accordingly.
2. Use a custom certificate which needs to be generated using openssl or third-party tools such as XCA and replace the existing one.

In the HTTP login page, you can download the root certificate file "ALE-OmniAccess-WLAN.CRT" from AP as shown below:

Administrator

password

Login

Login by https

Https Setting Window

1. Download and Install Certificate
2. Go to HTTPS page for login

Note: Please make sure all the APs in the group have been upgraded to 2.0.1.100 or later version before login with https.

This certificate can then be installed based on the operating system and browser combinations. Please refer to the Stellar AP User Guide referenced in the [Related Documents](#) section for more details.

Stellar WiFi Express Internal Web Server - Generate and Install Custom CA Certificate

We will cover the procedure to generate and install custom certificate for AP running in Cluster mode (Wi-Fi Express Mode) using OpenSSL.

Recommendation: Use a custom signed certificate for AP web management.

Before starting certificate customization, please note the following :

- The Certificate Common Name (CN), also known as the Fully Qualified Domain Name (FQDN), must be equal to "mywifi.al-enterprise.com" otherwise you will not be able to upload it (you might get "illegal certificate" warning when uploading it into the AP).
- Since you will get access to your AP through a FQDN, this FQDN entry must be known by your DNS.

To generate a Web Server/External Portal Server Certificate file, follow the example below:

1. Generate a private Key:

```
openssl genrsa -des3 -out ap_server.key 2048
```

2. Generate a CSR (Certificate Signing Request):

```
openssl req -new -key ap_server.key -out ap_server.csr -sha256
```

Note that you must enter the URL "mywifi.al-enterprise.com" for the Common Name (CN).

3. Sign and generate the AP certificate using a root CA:

```
openssl x509 -req -in ap_server.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out ap_server.crt -days 3560 -sha256
```

4. Merge ap_server.crt and ap_server.key to a single file:

```
type ap_server.crt ap_server.key > ap_server.pem.
```

- Import the PEM file into the AP web management tool (General -> Certificate Management). Please note that only PEM file can be uploaded and it must include both the private key and certificate. Also, ensure there are no special characters in the final PEM file to be uploaded into the AP cluster.

General Configuration

Group Info Management Account Management **Certificate Management** Service Management

Certificate

Name: (4-20 chars)

Certificate Type:

Certificate File: No file chosen

Password: (4-128 chars)

Confirm:

Certificate Format:

Certificate List

Name	Certificate	Type	Format	Status	Operate
PatricePAUL	mywifienterpriseconcerptpluskey.pem	Internal Web Server(Domain)	PEM	disable	<input type="button" value="Enable"/> <input type="button" value="Delete"/>

- Enable the certificate which was just imported in the last step

General Configuration

Group Info Management Account Management **Certificate Management** Service Management

Certificate

Name: (4-20 chars)

Certificate Type:

Certificate File: No file chosen

Password: (4-128 chars)

Confirm:

Certificate Format:

Certificate List

Name	Certificate	Type	Format	Status	Operate
PatricePAUL	mywifienterpriseconcerptpluskey.pem	Internal Web Server(Domain)	PEM	enable	<input type="button" value="Enable"/> <input type="button" value="Delete"/>

- Test your configuration by accessing the HTTPS AP web management. The DNS should be able to resolve the URL: "mywifi.al-enterprise.com"

Stellar Enterprise Internal Web Server - OmniVista Configuration

In OmniVista Cirrus 4.x/2500, you can add a new custom certificate which will be used between the web browser and the AP internal web server in the Network -> AP Registration -> Certificates page as shown below:

Alcatel-Lucent Enterprise

LAN-WLAN menu Home Network > AP Registration > Certificate

Certificate

Certificate List

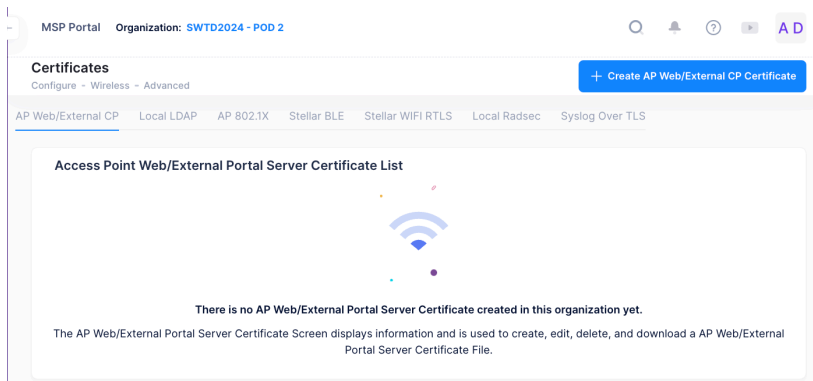
Search ...

☐ Name

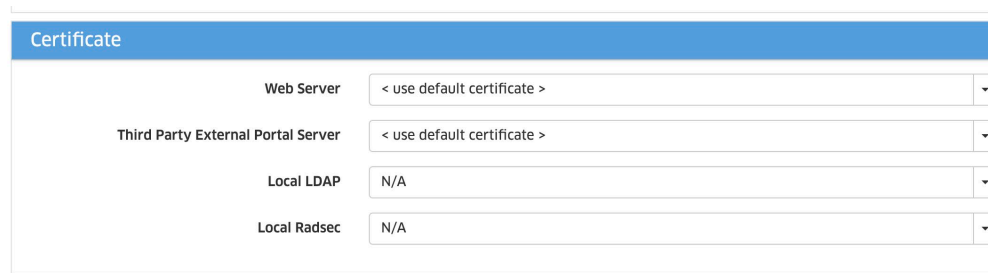
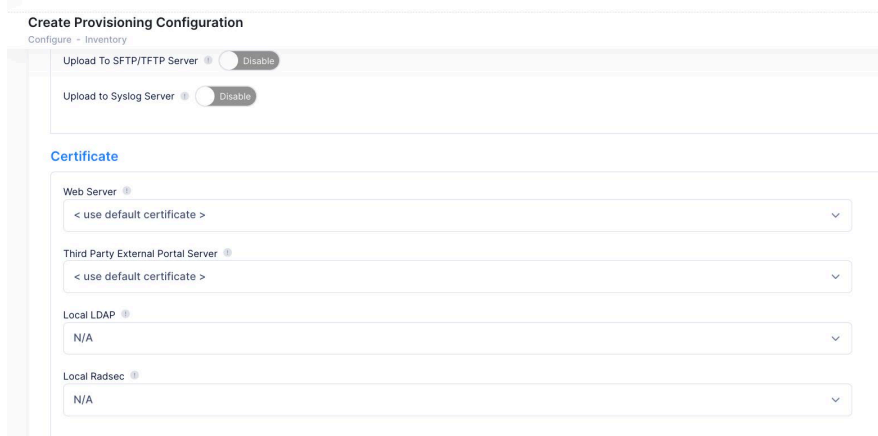
☐ testbis2

Web Server /External Portal Server
Local LDAP
802.1X Client
Local Radsec
Stellar BLE
Syslog Over TLS
Stellar WIFI RTLS

In OmniVista Cirrus 10, this can be configured in the Configure -> Wireless -> Advanced -> Certificates menu as shown below:

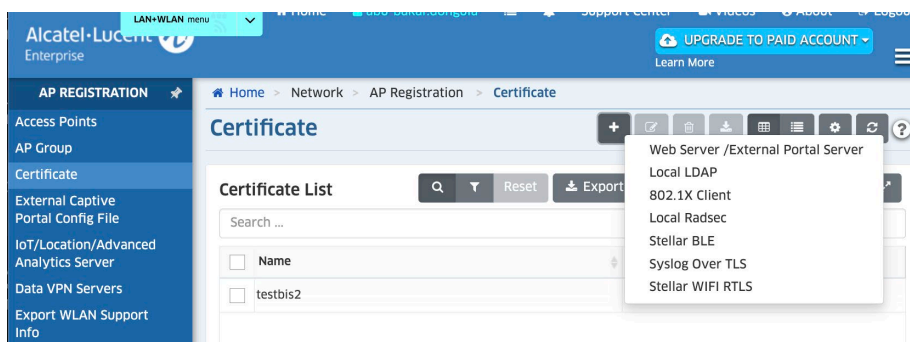


Then you can specify the default or custom certificate to be in use between web browser and the internal web server of the AP in the Provisioning Configuration page (OmniVista Cirrus 10) or the AP Group page (OmniVista Cirrus 4.x/2500) as shown below:

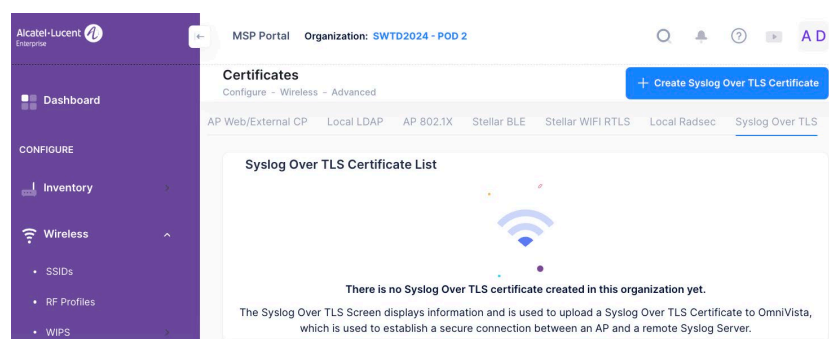


Stellar Enterprise Syslog Over TLS - OmniVista Configuration

In OmniVista Cirrus 4.x/2500, you can add a new custom certificate which will be used between the AP and the syslog server for TLS in the Network -> AP Registration -> Certificates page as shown below:



In OmniVista Cirrus 10, this can be configured in the Configure -> Wireless -> Advanced -> Certificates menu as shown below:



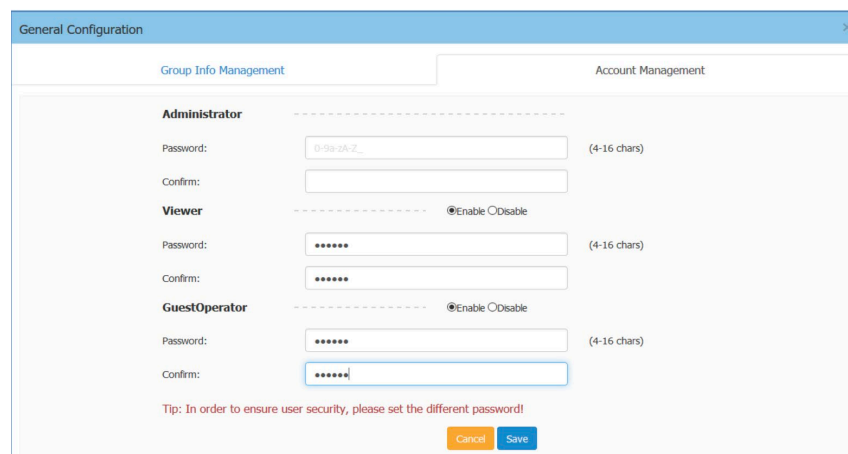
Then you can specify the created custom certificate for Syslog Over TLS in the Provisioning Configuration page (OmniVista Cirrus 10) or the AP Group page (OmniVista Cirrus 4.x/2500) as mentioned in the [Logging](#) section.

Recommendation: Centralize syslog logging using TLS encryption and add a second syslog server for redundancy.

Stellar WiFi Express - Account Management

In Stellar APs working in cluster mode (Wi-Fi Express mode), there are three accounts can login to the Web GUI with different privileges: Administrator, Viewer, and GuestOperator. Administrator account allows configuring and viewing the whole system, Viewer account allows checking configuration and monitoring of WLAN operations, while GuestOperator ONLY has the privilege to edit the guest portal users. Each account can be logged in at the same time. By default, only the Administrator account is enabled; Viewer and GuestOperator are disabled. In the Account Management tab, you can enable/disable the Viewer and GuestOperator account, change the password for Administrator, Viewer and GuestOperator.

Recommendation: Keep the Viewer and GuestOperator accounts disabled unless required to avoid exposure.



Stellar WiFi Express - Banner

User can customize the content for Warning Banner on demand by navigating to General Configuration -> Account Management -> Warning Banner as shown below:

Recommendation: Setup a warning banner, which are brief messages that are used to inform users of policies and legislation regarding the use of Stellar AP group web management system.

General Configuration

Group Info Management Account Management Certificate Management Service Management

Account Lockout

Lockout Threshold: (2-5 invalid logon attempts)

Lockout Duration: (1-15 minutes)

Inactivity Time: (5-60 minutes)

Warning Banner: (0-128 chars)

Cancel Save

Time Synchronization

Recommendation: Configure NTP time synchronization for log accuracy and correlation, and for supporting auditing and compliance

NTP (RFC 1305 - Network Time Protocol) is a networking protocol for time synchronization between the elements across the network. If you don't have a private NTP server in your network, it is suggested to add your favorite NTP server and prioritize it to the top of the NTP Server List, or use the default NTP servers in the system as shown below:

Date and Time: Wed Nov 23 2016 22:31:29

Daylight-Saving Time: ☒ on

Time Zone: (UTC-08:00)Pacific-Time(US and Canada)

NTP Server List:

- pool.ntp.org
- cn.pool.ntp.org
- tw.pool.ntp.org
- 0.asia.pool.ntp.org
- 1.asia.pool.ntp.org

NTP Server: Add

To configure the time settings and for APs, this can be done in the provisioning configuration as shown below in OmniVista Cirrus 10:

MSP Portal Organization: SWTD2024 - POD 2

Create Provisioning Configuration

Configure - Inventory

Time

Timezone *

NTP Server List

pool.ntp.org X Please enter NTP server

This field is required.

In OmniVista Cirrus 4.x/2500 NMS, this can be configured as part of the AP Group configuration as shown below:

AP REGISTRATION

- Access Points
- AP Group
- Certificate
- External Captive Portal Config File
- IoT/Location/Advanced Analytics Server
- Data VPN Servers
- Export WLAN Support Info

Time

Timezone: (UTC-12:00)International-Date-Line-West

Daylight Saving Time: ☐ OFF

NTP Server List: pool.ntp.org

NTP Server: Enter NTP Server (v4 | v6) +

Logging

Syslog is a standard for message logging. Syslog is used for system management and security auditing as well as general informational, analysis, and debugging messages. APs in group generate logs following the standard of syslog, you can view logs and configure corresponding attributes in the Syslog Window:

Recommendation: Centralize syslog logging using TLS encryption and add a second syslog server for redundancy.

Syslog

Title	Level	Source
Device IP conflicts with other hosts IP	err	192.168.50.216
Device IP conflicts with other		Tue Aug 23 16:19:21 2016 68.50.216

Log Level: Notice Save

Log Remote: ☐ off 192.168.100.1 Run

Log File: wanglili Download

You can set the syslog message severity depending on your requirements, but if certain level is specified, the AP group will generate syslog messages including all lower levels. Notice is the default level of Syslog setting, and the system generates logs including levels of Notice, Warning, Error, Critical, Alert and Emergency. Users can specify separate log level for different facilities (System, Security, Wireless, Network, User):

- AP Debug - Detailed log about the AP device
- System - Log about AP configuration and system status
- Security - Log about network security
- Wireless - Log about wireless RF
- Network - Log about network change
- User - Log about client

In OmniVista Cirrus 10 you can configure syslog in the Provisioning Configuration page as shown below. In OmniVista Cirrus 4.x/2500, this can be configured in the AP Group page as shown below:

Syslog

Log Remote ☒ Enable

Syslog Server IP Port TLS Certificate

This field is required.

Syslog

Log Remote

Log Remote ☒ ON

Syslog Server

IP	Port	TLS	Certificate
IPv4 or IPv6	1-65535	On	Select
143.209.0.2	514	Off	Certificate is required.

Please refer to the [Syslog Over TLS](#) in the Certificate Management section for more details on how to upload a custom certificate.

SNMP

With SNMP, users can monitor AP status in the group through a traditional network management platform. For SNMPv3, admin needs to specify the username and passphrase for communication between AP and management platform. For Stellar AP, the SNMPv3 authentication mechanism is fixed to SHA algorithm, privacy mechanism is fixed to AES128.

Recommendation: SNMPv1/2/2c should be avoided entirely as they are insecure. SNMPv3 is significantly more secure with added encryption, robust authentication, message integrity, and role-based access control.

Syslog & SNMP

Syslog

SNMP Agent: ☒ ON

Version:

Username:

Passphrase:

Confirm:

SNMP Trap: ☐ off

Version:

Trap Server:

In OmniVista Cirrus 4.x/2500, you can configure the SNMP settings as part of the AP Group configuration page as shown below:

AP REGISTRATION
Access Points
AP Group
Certificate
External Captive Portal Config File
IoT/Location/Advanced Analytics Server
Data VPN Servers
Export WLAN Support Info

SNMP Setting

SNMP Agent

SNMP Service

ON

*Version

v3

*User Name

*Password

*Confirm

Trap

Trap Service

ON

*Version

v3

*User Name

*Password

*Confirm

*Server IP

Enter Server IP (v4 | v6)

In OmniVista Cirrus 10, this can be configured as part Provisioning Configuration settings page as shown below:

Create Provisioning Configuration
Configure -> Inventory

SNMP Setting

SNMP Service

Enable

SNMP Version

SNMPv3

Username *

Enter the SNMP v3 username

This field is required.

Only ASCII code characters are allowed.

Password *

Enter the SNMP v3 password

This field is required.

Only ASCII code characters are allowed.

Confirm Password *

Confirm the SNMP v3

This field is required.

Trap Service

Enable

Trap Version

SNMPv3

Username *

Enter the SNMP v3 username

This field is required.

Only ASCII code characters are allowed.

Password *

Enter the SNMP v3 password

This field is required.

Only ASCII code characters are allowed.

Confirm Password *

Confirm the SNMP v3

This field is required.

Server IP *

Enter the Server IP (v4 | v6)

This field is required.

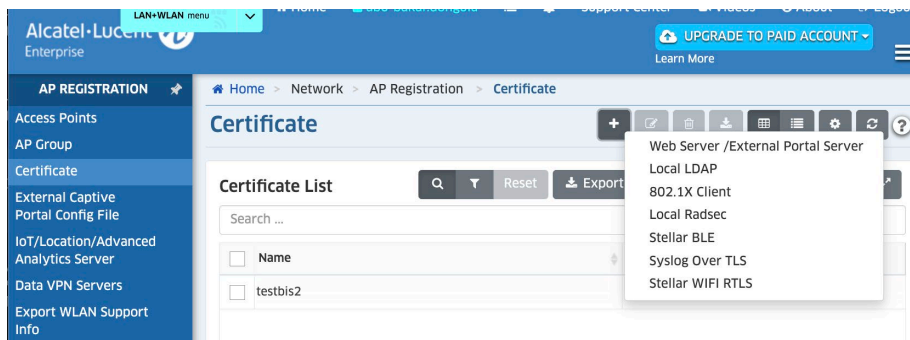
Please enter a valid IP (v4 or v6) address.

Control Plane

Certificate Management

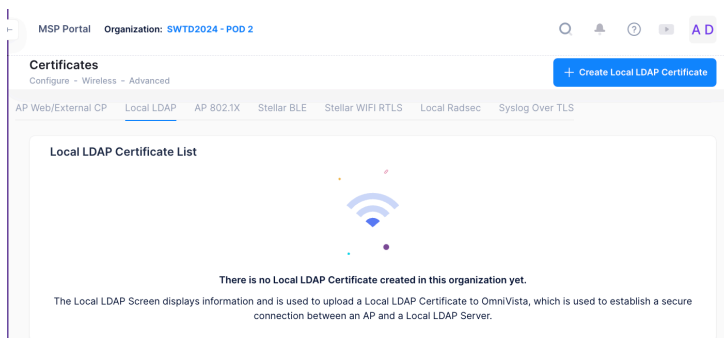
Stellar Enterprise - LDAP Certificate

In OmniVista Cirrus 4.x/2500, you can add a new custom certificate which will be used between the AP and a local LDAP server in the Network -> AP Registration -> Certificates page as shown below:

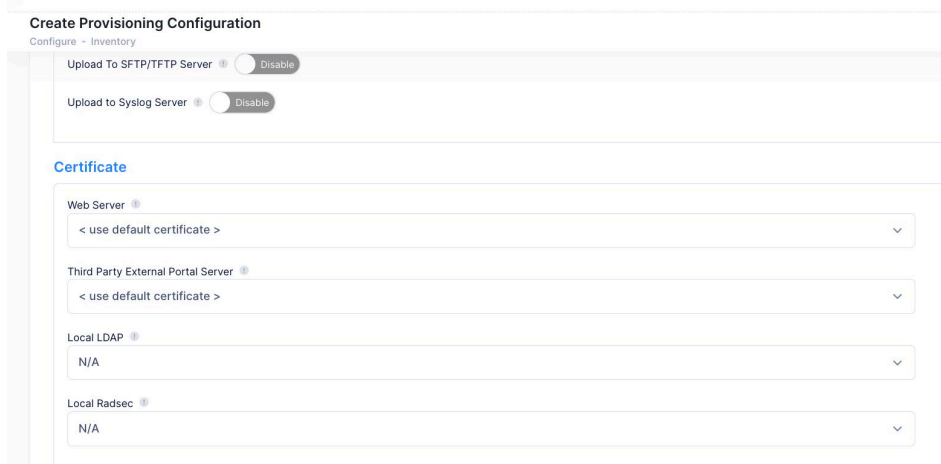


Recommendation: Use custom certificates to establish a secure connection between an AP and a Local LDAP Server.

In OmniVista Cirrus 10, this can be configured in the Configure -> Wireless -> Advanced -> Certificates menu as shown below:



Then you can specify the default or custom certificate to be in use between the AP and the Local LDAP server in the Provisioning Configuration page (OmniVista Cirrus 10) or the AP Group page (OmniVista Cirrus 4.x/2500) as shown below:



Certificate	
Web Server	< use default certificate >
Third Party External Portal Server	< use default certificate >
Local LDAP	N/A
Local Radsec	N/A

Stellar WiFi Express/Enterprise - External Captive Portal Certificate

For Stellar AP working in Cluster mode (WiFi Express mode), this can be enabled at the Authentication Configuration window as shown below:

Recommendation: Enable HTTPS connection for captive portal authentication and use a custom certificate

Authentication Configuration

HTTPS: ☐ off

Dummy IP: 1.1.1.1

Internal Captive Portal ☒ External Captive Portal

Redirect URL: ☐ off

Login by: ☒ Account ☐ Access Code ☐ Terms of use

Username	Starting Date	Ending Date	Operate
Used: 0 , Available: 0			

Buttons: Add, Import Portal Account, Download Template, Batch delete account

Captive Portal Detail

HTTPS: disable

Dummy IP: 1.1.1.1

Portal Type: Internal

Redirect URL:

Authentication Configuration

HTTPS: ☒ on

Internal Captive Portal ☐ External Captive Portal ☒

Captive Portal Server

Hostname: wifi.n2s.es

Redirect URL: /login/hotspot/ale

Redirect URL param: ☐ enable ☒ disable

Authentication Server:

Server IP / Hostname: 80.58.201.230

Authentication Server Port: 1812 (1-65535)

Secret: *****

Confirm: *****

☒ Radius Accounting

Accounting Server Port: 1813 (1-65535)

Client Behavior Tracking: ☒ on

☒ Logging Client Connections ☒ HTTP/HTTPS ☒ ALL

Log To Server: ☐ TFTP Server ☒ SFTP Server

Edit Client Behavior

*Server IP: 192.168.10.201

*Server Port: 22

Remote Path: /test

*Username: root

*Password: *****

Cycles: 1h

Buttons: Save, Upload Now

You can use the built-in certificate or use a custom certificate for HTTPS. The built-in certificate can be installed to the Trust Root Certificate Store to the users using an AD group policy, or a custom certificate can be generated as highlighted in the procedure mentioned in the [Certificate Management](#) section. However, since most use cases for captive portal authentication is used for external guest users, it is recommended to sign your certificate by an official Public CA (e.g. Verisign) and import it into the Certificate Management section for Internal and External Captive Portal certificate types:

General Configuration

Group Info Management | Account Management | **Certificate Management** | Service Management

Certificate

Name: (4-20 chars)

Certificate Type:

Certificate File: No file chosen

Password: (4-128 chars)

Confirm:

Certificate Format:

Certificate List

Name	Certificate	Type	Format	Status	Operate
------	-------------	------	--------	--------	---------

In OmniVista Cirrus 4.x/2500, you can add a new custom certificate which will be used between the AP and the external captive portal server in the Network -> AP Registration -> Certificates page as shown below:

Alcatel-Lucent Enterprise

LAN+WLAN menu

AP REGISTRATION

Home > Network > AP Registration > Certificate

Certificate

Certificate List

Search ...

☐ Name

☐ testbis2

Web Server /External Portal Server
Local LDAP
802.1X Client
Local Radsec
Stellar BLE
Syslog Over TLS
Stellar WIFI RTLS

In OmniVista Cirrus 10, this can be configured in the Configure -> Wireless -> Advanced -> Certificates menu as shown below:

MSP Portal Organization: SWTD2024 - POD 2

Certificates

Configure - Wireless - Advanced

AP Web/External CP | Local LDAP | AP 802.1X | Stellar BLE | Stellar WIFI RTLS | Local Radsec | Syslog Over TLS

Access Point Web/External Portal Server Certificate List

There is no AP Web/External Portal Server Certificate created in this organization yet.

The AP Web/External Portal Server Certificate Screen displays information and is used to create, edit, delete, and download a AP Web/External Portal Server Certificate File.

Then you can specify the default or custom certificate that was just created in Provisioning Configuration page (OmniVista Cirrus 10) or the AP Group page (OmniVista Cirrus 4.x/2500) as shown below:

Create Provisioning Configuration

Configure - Inventory

Upload To SFTP/TFTP Server

Disable

Upload to Syslog Server

Disable

Certificate

Web Server

< use default certificate >

Third Party External Portal Server

< use default certificate >

Local LDAP

N/A

Local Radsec

N/A

Certificate

Web Server

< use default certificate >

Third Party External Portal Server

< use default certificate >

Local LDAP

N/A

Local Radsec

N/A

Stellar Enterprise - Radsec Certificate

Recommendation: Enable Radsec to secure communication between the RADIUS server and Stellar AP using TLS encryption.

When configured, this feature ensures that the RadSec protocol is used for safely transmitting the authentication and accounting data between the Stellar AP and the RadSec server.

LAN+WLAN menu

Home

Support Center

UPGRADE TO PAID ACCOUNT

AP REGISTRATION

Access Points

AP Group

Certificate

External Captive Portal Config File

IoT/Location/Advanced Analytics Server

Data VPN Servers

Export WLAN Support Info

Home > Network > AP Registration > Certificate

Certificate

Certificate List

Search ...

Reset

Export

Web Server /External Portal Server

Local LDAP

802.1X Client

Local Radsec

Stellar BLE

Syslog Over TLS

Stellar WIFI RTLS

MSP Portal

Organization: SWTD2024 - POD 2

AD

Certificates

Configure - Wireless - Advanced

Create Local Radsec Certificate

AP Web/External CP

Local LDAP

AP 802.1X

Stellar BLE

Stellar WIFI RTLS

Local Radsec

Syslog Over TLS

Local RadSec Certificate List

There is no Local RadSec certificate created in this organization yet.

The Local RadSec Screen displays information and is used to upload a Local RadSec Certificate to OmniVista, which is used to establish a secure connection between an AP and a local,third-party RADIUS Server that uses RadSec(RADIUS-over-TLS).

Then you can specify the default or custom certificate to be in use between the AP and the Local RADIUS server for Radsec in the Provisioning Configuration page (OmniVista Cirrus 10) or the AP Group page (OmniVista Cirrus 4.x/2500) as shown below:

Create Provisioning Configuration
Configure - Inventory

Upload To SFTP/TFTP Server ☐ Disable

Upload to Syslog Server ☐ Disable

Certificate

Web Server ☐

Third Party External Portal Server ☐

Local LDAP ☐

Local Radsec ☐

Certificate

Web Server	<input type="text" value="< use default certificate >"/>
Third Party External Portal Server	<input type="text" value="< use default certificate >"/>
Local LDAP	<input type="text" value="N/A"/>
Local Radsec	<input type="text" value="N/A"/>

Stellar Enterprise - AP Device as an 802.1X Client

When an 802.1X (supplicant) device is connected to a UNP port on which 802.1X authentication is enabled, the switch will attempt to authenticate the device using 802.1X EAP frames. If after a configurable amount of time the device does not respond to the EAP frames sent by the switch, the device is identified as a non-802.1X (non-supplicant) device and undergoes MAC address authentication.

When a Stellar AP is connected to an OmniSwitch UNP port on which the AP Mode and 802.1X authentication is enabled, the switch starts to send EAP frames to the AP device. If the AP device does not respond to the EAP frames, the switch will identify the AP as a non-supplicant and will attempt to authenticate the AP with other methods. To ensure that the switch will identify the AP device as a supplicant (802.1X client), enable 802.1X functionality for the AP Group to which the AP belongs and specify an 802.1X client certificate to install on the APs in the group. A built-in 802.1X client certificate is provided by default or you can generate and upload a custom client certificate.

Recommendation: Do not rely on the Default Client Certificate on APs and the Default Server Certificate on UPAM but install Custom Client Certificates on APs/AP Groups and a Custom Server Certificate on UPAM for improved security.

There are many use cases for 802.1x authentication for the AP Device as a client. The below steps involve configuring 802.1X authentication for the AP on OmniVista 2500 platform:

1. OmniVista UPAM 802.1X Server with Built-In Certificate on the AP
 - a. Enable 802.1X Supplicant functionality for the AP Group.
 - b. Select the Built-In Certificate from the drop-down menu
2. OmniVista UPAM 802.1X Server with a Custom Client Certificate on the AP
 - a. Generate the client certificate (Cert, Private Key, CA cert) externally.
 - b. Import the client certificate into the UPAM database in OmniVista.
 - i. Import the client certificate from AP Registration - Certificate menu and assign the certificate a name.

- ii. Import the client CA certificate into UPAM - Settings - AP 802.1X Trust CA
 - c. Push the custom client certificate to the APs.
 - i. Enable 802.1X Supplicant functionality for the AP Group.
 - ii. Select the custom certificate name that was imported in Step b(i).
3. Use an External Radius 802.1x Server with Built-In Certificate on the AP
 - a. Download the UPAM Server CA certificate from UPAM - Settings - AP 802.1X Trust CA. This is the CA used to validate the AP as an 802.1x client. Import this CA into the external Radius server.
 - b. Push the built-in certificate to the APs.
 - i. Enable 802.1X Supplicant functionality for the AP Group.
 - ii. Select the Built-in Certificate.
4. Use an External RADIUS 802.1X Server with a Custom Client Certificate on the AP
 - a. Generate the client certificate (Cert, Private Key, CA cert) externally.
 - b. Import the client CA certificate into the external RADIUS server database so the RADIUS server will trust the AP.
 - c. Push the custom client certificate to the APs.
 - i. Import the client certificate from AP Registration - Certificate menu and assign the certificate a name.
 - ii. Enable 802.1X Supplicant functionality for the AP Group.
 - iii. Select the custom certificate name that was imported in Step c(i).
5. 802.1X Authentication with Username (AP MAC Address)
 - a. An 802.1X (supplicant) AP device can undergo certificate-based (see use cases above) or username-based 802.1X authentication. For username-based authentication, the user/pass = AP MAC address is configured in the UPAM database. When the AP MAC address attempting to authenticate matches the configured user/pass MAC address, UPAM returns a UNP profile/VLAN ID to the switch. This is often done when the user wants to assign a different VLAN based on the authentication result. Note that when configuring username-based 802.1X authentication, the 802.1X Supplicant option for the AP Group should be set to "Off" and Secure Mode is enabled on the switch port. This will ensure that the switch will learn the AP MAC address and perform the 802.1X authentication according to the configuration (Access Auth Profile) on the switch.

Recommendation: Setup an 802.1x Failure Policy on the switch port depending on whether you want the AP (and its clients) to have connectivity to the network even if the AP fails 802.1x authentication; or if you want the AP (and its clients) to be completely blocked from network access if the AP fails 802.1x authentication.

To enable 802.1x supplicant on AP feature and select a custom or built-in certificate, this can be done in the Provisioning Configuration page (OmniVista Cirrus 10) or the AP Group page (OmniVista Cirrus 4.x/2500) as shown below:

The screenshot shows the 'AP REGISTRATION' sidebar on the left with 'Certificate' selected. The main panel is titled '802.1X Supplicant on AP Management Port'. It contains a toggle for '802.1X Supplicant' which is currently 'ON'. Below it, a dropdown menu labeled '*Certificate for 802.1X' is open, displaying a search bar and two options: 'Built-in Certificate' and 'testbis2'. An '+ Add New' button is located at the bottom of the dropdown. Other settings like 'Timezone' and 'Daylight Saving Time' are visible but not the focus of the configuration shown.

MSP Portal Organization: SW102024 - POU 2

Create Provisioning Configuration

Configure - Inventory

802.1X Supplicant on AP Management Port ☒ Enable

Certificate for 802.1X

Select a AP 802.1X Certificate to be applied to Access Points

This field is required.

[Create AP 802.1X Certificate](#)

Wireless Intrusion Protection System (wIPS)

An 802.11 network is open and borderless, making it vulnerable to attack (e.g., rogue APs, unauthorized clients, DoS attacks). The Wireless Intrusion Protection System (wIPS) application in OmniVista NMS platforms monitors the wireless radio spectrum for the presence of unsafe access points and clients, and can take countermeasures to mitigate the impact of foreign intrusions. wIPS provides an overview of wireless network threats/intrusions for Stellar APs, and enables users to set up policies to detect threats and take countermeasures.

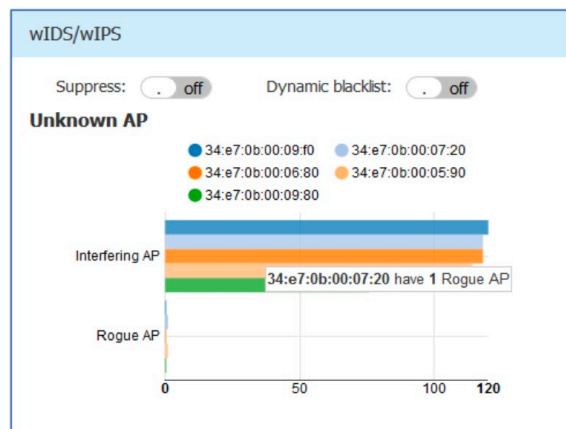
Let's define a few key terms related to WIPS:

- An **interfering AP** is an AP seen in the wireless environment but not connected to the wired network. The interfering AP can provide RF interference potentially, however, it is not considered a direct security threat, because it is not connected to the wired network.
- A **rogue AP** is an unauthorized AP plugged into the wired side of the network or a foreign interfering AP broadcasting the same SSID with the AP group. A rogue AP is considered a security threat to the AP group.

Recommendation: Configure, maintain, and monitor the wIPS policies regularly. wIPS is critical for securing wireless networks against unauthorized access, rogue devices, and various wireless attacks.

Stellar WiFi Express - wIDS/wIPS

In Stellar AP working in Cluster mode (Wi-Fi Express mode), the panel of wIDS/wIPS displays top 5 Stellar APs with interference from surrounding APs, and the top 5 Stellar APs with the most rogue APs surrounding, as shown below:



The below options can be configured for WIPS for Stellar AP (Cluster mode):

- **AP allowlist:** Both interfering APs and rogue APs are foreign unknown APs which can be found by background scanning and are listed in the unknown AP table, shown below.

wIDS/wIPS Configuration

Unknown AP	SSID	Type	AP	Operate
00:02:03:04:05:06	OpenWrt_1_2_4	Interfering	duanmingzhe	Trust
4c:48:da:24:f4:47	chenjun_VLAN_...	Interfering	duanmingzhe	Trust
4c:48:da:24:e4:88		Interfering	duanmingzhe	Trust
00:1f:64:ca:42:a9	NiuBin-work-2.4	Interfering	duanmingzhe	Trust
08:57:00:88:10:4b	SoftAP	Rogue	duanmingzhe	Trust
4c:48:da:24:f1:90		Interfering	duanmingzhe	Trust
4c:48:da:24:11:10		Interfering	duanmingzhe	Trust
4c:48:da:24:cb:b0	y-2	Interfering	duanmingzhe	Trust
00:1f:64:12:13:91	DMZ-TEST2	Interfering	duanmingzhe	Trust
4c:48:da:24:11:11	fdfsd	Interfering	duanmingzhe	Trust
4c:48:da:24:f1:91	Imm123	Interfering	duanmingzhe	Trust
00:1f:64:12:13:92	DMZ-TEST3	Interfering	duanmingzhe	Trust

White List Black List

Unknown AP Information

Unknown AP: 08:57:00:88:10:4b

RSSI: 44

SSID: SoftAP

Channel: 1

Type: Rogue

Already In blacklist: No

AP Name: duanmingzhe

AP MAC: 34:e7:0b:00:09:f0

AP Location: far

Distance: far

Encryption Type: WPA2/RSNA

Attached Clients: 1

64:cc:2e:0a:49:4d

However, some foreign APs found are trusted APs, those are not suitable for being classified as interfering APs or rogue APs. To avoid trusted foreign APs from being classified as interfering APs or rogue APs, you can add the trusted MAC address or MAC prefix to the AP allowlist, as shown below. If a foreign AP MAC address is added to the allowlist, it will not be displayed in the unknown AP list.

wIDS/wIPS Configuration

Unknown AP	SSID	Type	AP	Operate
00:02:03:04:05:06	OpenWrt_1_2_4	Interfering	duanmingzhe	Trust
4c:48:da:24:f4:47	chenjun_VLAN_...	Interfering	duanmingzhe	Trust
4c:48:da:24:e4:88		Interfering	duanmingzhe	Trust
00:1f:64:ca:42:a9	NiuBin-work-2.4	Interfering	duanmingzhe	Trust
08:57:00:88:10:4b	SoftAP	Rogue	duanmingzhe	Trust
4c:48:da:24:f1:90		Interfering	duanmingzhe	Trust
4c:48:da:24:11:10		Interfering	duanmingzhe	Trust
4c:48:da:24:cb:b0	y-2	Interfering	duanmingzhe	Trust
00:1f:64:12:13:91	DMZ-TEST2	Interfering	duanmingzhe	Trust
4c:48:da:24:11:11	fdfsd	Interfering	duanmingzhe	Trust
4c:48:da:24:f1:91	Imm123	Interfering	duanmingzhe	Trust
00:1f:64:12:13:92	DMZ-TEST3	Interfering	duanmingzhe	Trust

White List Black List

White List

MAC

34:e7:0b:*:*:*

Add

- **AP blacklist:** Only rogue APs can be added to the blacklist. If a rogue AP is added to the blacklist, it cannot change its role to act as a client and access to the Stellar AP wireless network, as shown below.

wIDS/wIPS Configuration

Unknown AP	SSID	Type	AP	Operate
01:60:02:00:00:00	OpenWrt-2g	Interfering	AP-00:E0	Trust
00:11:22:33:44:60		Rogue	AP-00:E0	Trust
4c:48:da:27:47:a0		Interfering	AP-00:E0	Trust
4c:48:da:24:f1:c0		Interfering	AP-00:E0	Trust
4c:48:da:24:f4:c0		Interfering	AP-00:E0	Trust
4c:48:da:24:f2:00		Interfering	AP-00:E0	Trust
4c:48:da:24:f0:e0		Rogue	AP-00:E0	Trust
4c:48:da:24:f0:e1	chenjun001	Interfering	AP-00:E0	Trust
4c:48:da:24:f4:c1	test_8021x	Interfering	AP-00:E0	Trust
00:11:22:33:44:61	w33	Rogue	AP-00:E0	Trust
4c:48:da:27:47:a1	test_8021x	Interfering	AP-00:E0	Trust
4c:48:da:24:f2:01	lvshuang	Interfering	AP-00:E0	Trust
4c:48:da:24:f4:a1	fdfsd	Interfering	AP-00:E0	Trust

White List Black List

Black List

MAC

00:11:22:33:44:60 Trust

4c:48:da:24:f0:e0 Trust

00:11:22:33:44:61 Trust

00:1f:64:ca:42:a9 Trust

4c:48:da:04:ef:50 Trust

00:11:22:33:44:50 Trust

4c:48:da:28:ef:50 Trust

4c:48:da:24:11:10 Trust

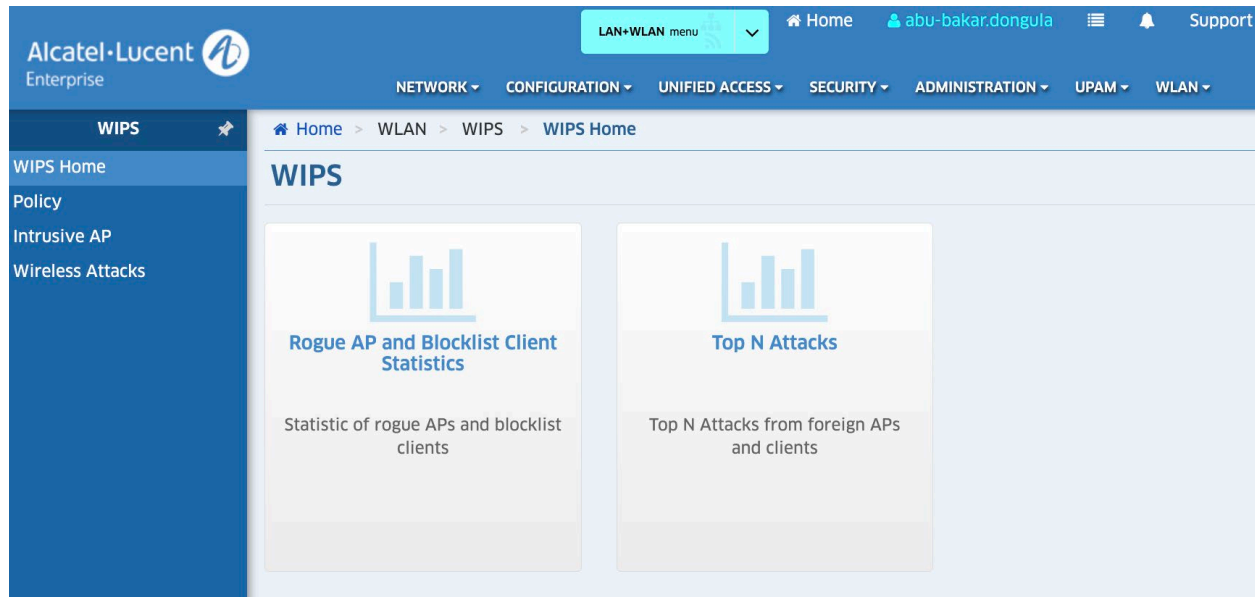
4c:48:da:54:ef:50 Trust

4c:48:da:24:f1:90 Trust

- **Suppress:** Enable/disable the function of rogue AP suppress. If enabled, the detecting Stellar AP will send DEAUTH frames to clients that have associated to the rogue AP, keeping the clients away from the unsafe wireless network. By default, the detecting Stellar AP does not send DEAUTH frames.
- **Dynamic blacklist:** If enabled, all the ad-hoc devices found will be added to the AP blacklist automatically, which prevents the ad-hoc device from changing its role to act as a client and access to Stellar AP wireless network. By default, the ad-hoc device is not added to the blacklist automatically.

Stellar Enterprise - wIPS Policy

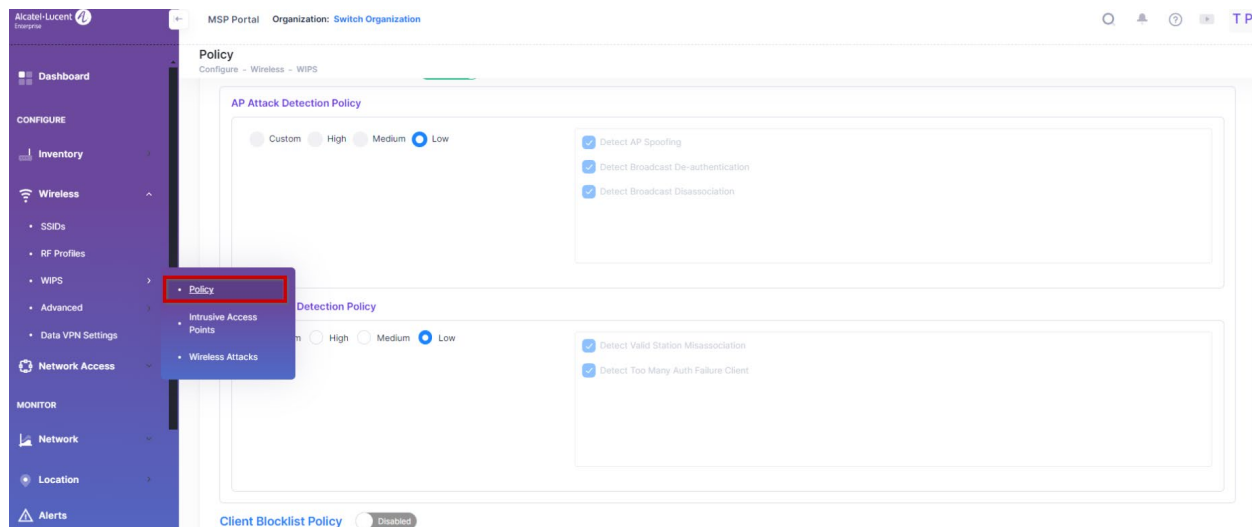
In OmniVista Cirrus 10 and OmniVista Cirrus 4.x/2500 platforms, you can view detailed information on intrusive APs and wireless attacks, and create policies to detect and react to the attacks. Detailed views and policies are configured using the following links under the WIPS application (**Configure > Wireless > WIPS**) of the OmniVista Cirrus 10 Menu and in the WLAN -> WIPS of the OmniVista Cirrus 4.x/2500 menu as show below:



- Policy - Define rules for classifying rogue AP/wireless attacks and specify the measures that will be taken to react to the threats.
- Intrusive Access Points - Display detailed information about interfering APs and rogue APs, as well as clients connecting to the intrusive AP.
- Wireless Attacks - Display detailed wireless attack information.

The WIPS Policy screen is used to configure policies for rogue AP and wireless attacks on the network. You can configure one overall policy for the Stellar wireless network. When an attack is detected based on the policy, the detected device is banned from the network and is displayed on the Client Blocklist for review.

To configure WIPS policies, navigate to the WIPS Policy screen by clicking on **Wireless > WIPS > Policy** under the “Configure” section of the OmniVista Cirrus Menu. The WIPS Policy screen displays with the default settings for a Rogue AP Policy and Wireless Attack Detection Policy.



Rogue AP Policy

You can configure Rogue AP Policy rules to classify interfering APs as rogue APs with the fields shown below such as Signal Strength Threshold, Detect Valid SSID, Detect Rogue SSID Keyword, and Rogue OUI:

The screenshot shows the 'Rogue AP Policy' configuration page. It includes four sections: 'Signal Strength Threshold' with a slider set to 70 dBm and a note 'Please select a value between 50 and 95'; 'Detect Valid SSID' with a 'Disabled' toggle; 'Detect Rogue SSID Keyword' with a text input field containing 'Please input a SSID name and press enter'; and 'Rogue OUI' with a text input field containing 'Please input MAC OUI and press enter'.

You can also add an AP classified as interfering or rogue can be trusted to be a "Friendly" AP by entering the MAC OUI of the AP - essentially creating a Vendor "Allowlist". These interfering APs will never be classified as rogue.

The screenshot shows the 'Friendly AP' configuration page. It features a 'Friendly MAC' section with two input fields: one containing '34:e7:0b' and another containing 'dc:08:56', both with 'X' icons to clear the text. A text prompt 'Please input MAC address or OUI and press enter' is also present.

You can also reduce the impact of rogue AP on valid clients by enabling the Rogue AP Containment function option as shown below:

The screenshot shows the 'Containment Policy' configuration page. It includes a 'Rogue AP Containment' section with a green 'Enabled' toggle switch.

Wireless Attack Detection Policy

You can create Wireless Attack Detection Policies by enabling **Wireless Detection** option. This will allow you to configure AP Attack Detection Policies, Client Attack Detection Policies, and Client Blocklist Policies.

The screenshot shows the 'Wireless Attack Detection Policy' configuration page. At the top, there is a green 'Enabled' toggle. Below it, the 'AP Attack Detection Policy' section is visible. It has a row of four radio buttons: 'Custom', 'High', 'Medium', and 'Low'. The 'Low' button is selected. A red box highlights these buttons, with a red arrow pointing to them and the text 'Select detection level'. To the right, another red box highlights a list of three checked options: 'Detect AP Spoofing', 'Detect Broadcast De-authentication', and 'Detect Broadcast Disassociation'. A red arrow points from this box to the text 'Selection level based on detection level'.

When configuring a policy, each detection policy can be set to one of the following levels. When a level is selected, all detection policies included in that level are displayed and selected.

- **High** - Enables all applicable detection mechanisms, including all the options of low and medium level settings.
- **Medium** - Enables important detection mechanisms. This includes all the options of the low-level settings.
- **Low (Default)** - Enables only the most critical detection mechanisms.
- **Custom** - Enables only the selected detection mechanisms. When this level is selected all detection mechanisms are displayed. Select the ones you want to include in the policy.

Please refer to the OmniVista 2500 or OmniVista Cirrus online user guide for a list of AP and client attack detection policies that can be configured and enabled.

You can also configure a Client Blocklist Policy as part of the Wireless Attack Detection Policy. There are two sources for the Client Blocklist: created manually by the user or added dynamically by the system. If the **Dynamic Client Blocklist** option is enabled, intruders discovered by WIPS are dynamically added into the Client Blocklist and prevented from associating with the network. The following detected items are added to the Client Blocklist by the system: List of Client Attack Detection, ad-hoc clients, and Clients associated to rogue AP.

Client Blocklist Policy

There are two sources for the Client Blocklist: created manually by user or added dynamically by system. If the Dynamic Client Blocklist is enabled, intruders discovered by WIPS are dynamically added into the Client Blocklist and prevented from associating with the network. The discovery of intruders depends on the reporting interval configured for aprobeclient.report event on analytics profile. [Click to configure](#)

Dynamic Client Blocklist 1 ☐ Disabled

Aging Time hour hour(s)
Please select a value between 1 and 8760 Please select an option (day or hour)

Max Auth Failure Times time(s) 60 Seconds(s)
Please select a value between 3 and 10 Please select a value between 5 and 3600

You can also configure a maximum aging time for the client blocklist and an authentication failure times threshold. Once the aging time is expired, a client will be removed from the Blocklist and allowed to be associated to the valid network until it is detected as a threat again. With regards to the Authentication failure times threshold, when a client fails to pass the authentication in the associated phase for too many times in a brief period, it will be classified as an attack and added into the Client Blocklist.

Intrusive Access Points

The WIPS Intrusive Access Points screen displays information about Intrusive APs on the network including Interfering APs, Rogue APs, Friendly APs, Clients Associated to an Interfering AP, and Clients Associated to a Rogue AP. To access the WIPS Intrusive Access Points screen, click on **Wireless > WIPS > Intrusive Access Points** under the “Configure” section of the OmniVista Cirrus Menu.

Intrusive AP
Configure - Wireless - WIPS

Interfering AP | Rogue AP | Friendly AP | Client Associated to Interfering AP | Client Associated to Rogue AP

Interfering AP

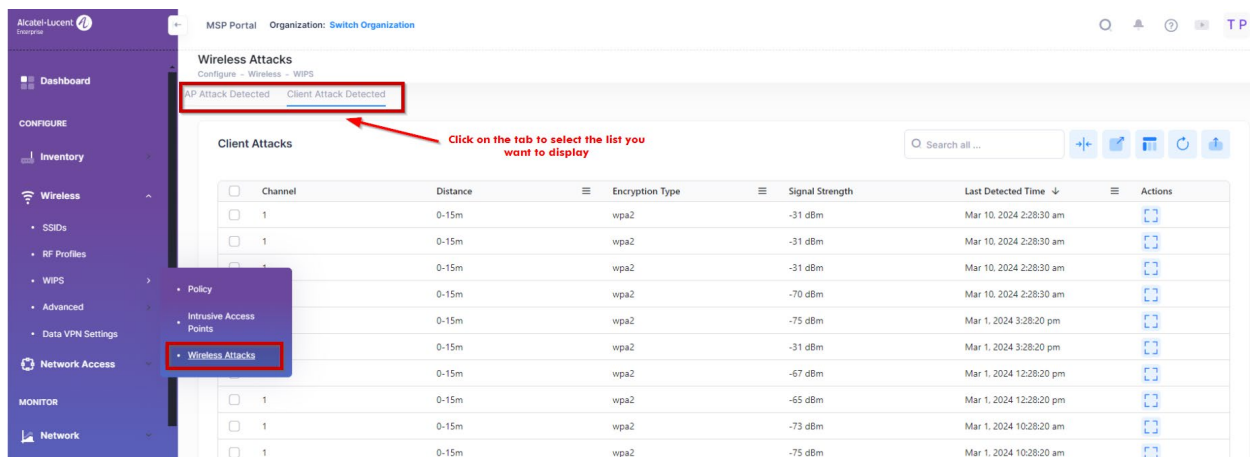
Click on the tab of the list that you want to view

Interfering AP BSSID	SSID	Channel	Scanning AP Name	Scanning AP MAC	Distance	Encryption Type	Actions
bed7130f2fd	DIRECT-og-Android_8b...	36	AP-26:60	DC:08:56:54:26:60	0-15m	wpa2	
00:4e:35:de:91:52	ax-test	36	AP-26:60	DC:08:56:54:26:60	0-15m	open	
00:0c:87:b9:a9:70	Paul_LAB2	116	AP-26:60	DC:08:56:54:26:60	0-15m	open	
01:15:85:50	RecoveryClusterProfile	36	AP-26:60	DC:08:56:54:26:60	0-15m	wpa	
02:bac5:d0	Paul_LAB2	132	AP-26:60	DC:08:56:54:26:60	0-15m	open	
02:5d:e9:1:50	2-test	36	AP-26:60	DC:08:56:54:26:60	0-15m	open	
02:5d:e9:1:42	ax-test	5	AP-26:60	DC:08:56:54:26:60	0-15m	open	

By default, the “Interfering AP” list is displayed. Click on one of the other list names to display the contents of other lists. For example, click on the “Friendly AP” tab to display the list of APs declared as “friendly”.

Wireless Attacks

The WIPS Wireless Attacks Screen displays information about wireless attacks on the network including AP attacks and Client attacks. To access the WIPS Wireless Attacks screen, click on **Wireless > WIPS > Wireless Attacks** under the “Configure” section of the OmniVista Cirrus Menu.



By default, the “AP Attack Detected” list is displayed. Click on **Client Attack Detected** to display that list.

For more details, please refer to the OmniVista 2500 or OmniVista Cirrus online user guide referenced in the [Related Documents](#) section for details on how protect the wireless network from malicious actors.

Data Plane

WPA3 Encryption

With the changing threat landscape, the Wi-Fi Alliance announced new security enhancements for Wi-Fi Protected Access. These new enhancements are released under the WPA3 umbrella, all aiming at better protecting Wi-Fi communications. Also, of important note is WPA3 is backward compatible with WPA2. WPA3 comes in two versions:

1. **WPA3-Personal:** It will utilize Simultaneous Authentication of Equals (SAE) as defined in the IEEE 802.11-2016 standard. With SAE, the user experience is the same (choose a passphrase, use it to connect), but SAE automatically adds a step to the “handshake” that makes brute force attacks ineffective. With SAE, the passphrase is never exposed, making it impossible for an attacker to find the passphrase through brute force dictionary attacks. The other added benefit of WPA3-Personal is that Protected Management Frames (PMF) are required to be utilized for all WPA3 personal connections. In the past PMF was an optional capability that was left up to the user to enable. With WPA3, PMF is required and can be negotiated for all WPA3 connections providing an additional layer of protection from deauthentication and disassociation attacks.
2. **WPA3-Enterprise:** Within the enterprise, one of the subtle changes that will be evident to end users is in keeping in line with the WPA3 goal for PMF to be enabled and negotiated for all WPA3 connections. Additionally, WPA3 also offers an optional CNSA 192-bit cryptographic security.

OmniVista platforms support the latest WPA3 standard encryption for both types of authentication: 802.1X authentication and Pre-Shared Key (PSK).

Recommendation: Use WPA3 Encryption when configuring SSIDs to enable more robust authentication, deliver increased cryptographic strength, and maintain resiliency.

The following WPA3 encryption types are supported for different authentication types:

- **802.1x authentication:**
 - **WPA3_AES:** WPA3 with AES encryption and dynamic keys using 802.1X.
 - **WPA3_AES256:** WPA3 with CNSA (Suite B) using 802.1X. Note that when WPA3_AES256 encryption is applied to an AP that does not support it, the encryption will automatically fall back to WPA2_AES.
- **PSK authentication:**
 - **WPA3_SAE_AES:** WPA3 with AES encryption using a preshared key, which ONLY allows WPA3 capable client accessing. When this encryption type is selected, the PSK, Device Specific PSK, and Private Group PSK parameters are not available.
 - **WPA3_PSK_SAE_AES:** WPA3 and WPA2 mixed mode, which allow both WPA3 capable client as well as ONLY WPA2 capable client accessing

The type of encryption can be selected when creating the Wireless SSIDs. For example, in OmniVista Cirrus 10 platform, it can be selected from the drop-down list as shown below:

WiFi Enhanced Open - OWE

OmniAccess Stellar provides enhanced security and privacy for open SSIDs in WLAN networks with support of the new Wi-Fi Enhanced Open security standard based on Opportunistic Wireless Encryption (OWE). Wi-Fi Enhanced Open™ is a security standard that is based on Opportunistic Wireless Encryption (OWE). When enabled, OWE is used to ensure that communication between each pair of endpoints is protected from other endpoints. Data sent between a client and an AP is provided individualized data protection. Wi-Fi Enhanced Open™ offers improved data privacy, while maintaining convenience and ease-of-use. This functionality is particularly useful for provisioning a secure open SSID in public spaces. Configuring the enabled/disabled status of this attribute is based on the following:

- If 2.4 GHz and/or 5.0 GHz is the allowed band (not 6.0 GHz), you can enable or disable Enhanced Open status
- If 6.0 GHz is the allowed band, then Enhanced Open is automatically enabled, whether or not 2.4 GHz or 5.0 GHz is selected. You cannot disable the Enhanced Open status.

When creating a new Open (Guest) SSID, you can enable the Enhanced Open option as shown below in OmniVista Cirrus 10 platform:

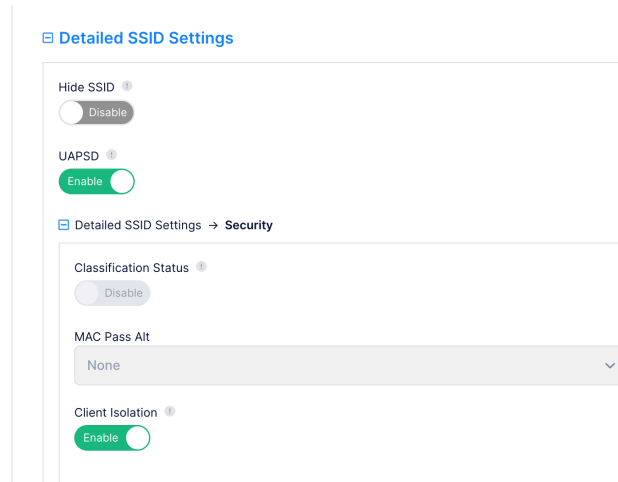
Recommendation: Enable the Enhanced Open feature to secure communication between endpoints if you are using an Open WLAN SSID

Client Isolation


OmniVista platforms support client isolation feature which when enabled, traffic between clients on the same AP in the SSID is blocked; client traffic can only go toward the router. In that case, the rest of the network is not isolated from guests' traffic (and vice versa) and if isolation between guests is required even if they are associated to different APs, then an ACL (at SSID level) may be configured and applied to block traffic between guest clients.

Recommendation: Configure client isolation between guest SSID users.

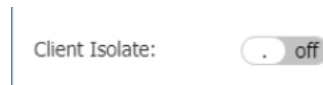
The Client Isolation feature can be enabled at the Detailed SSID Security settings on the Create SSID page as shown below on OmniVista Cirrus 10 platform:



In OmniVista Cirrus 4.x/2500 NMS platforms, the client isolation feature can be enabled at the Advanced WLAN Configuration settings when creating or editing an SSID:




Client isolation can also be enabled In Stellar AP working in Cluster mode (Wi-Fi Express mode) when creating the WLAN:



Encrypting Roaming Client Context

Recommendation: Encrypt the client context exchange between APs when the client is roaming from one AP to another. This is enabled by default.

OmniAccess Stellar APs encrypt the client-context data using DTLS tunnels. It is recommended to enter a password which will be used for the roaming domain. By default, the Roaming Domain is set to "automatic" (password is empty).



Network Management System Security

Management Plane

Firewall Requirements

It is important to maintain the principle of least privilege while ensuring proper communication between the NMS and network devices. Please refer to the OmniVista Cirrus online documentation and the OmniVista 2500 NMS Release Notes as referenced in the [Related Documents](#) section for the firewall ports requirements.

Recommendation: As best practice, you should maintain concept of least privilege between your network components by allowing only the required firewall ports for proper communication.

Change Default Passwords

You will be prompted to set the “cliadmin” password when first installing the OmniVista 2500 NMS VM. It is recommended to set a strong password:

```
You must remember the new passwords in order to manage the Virtual Appliance and OmniVista.
Length of new password must be >= 8 and <= 30 characters
Enter new password:
Retype password:
Changing password for user cliadmin.
passwd: all authentication tokens updated successfully.
```

You can change the default passwords configured on the OmniVista 2500 NMS VM when first installing it as shown below by selecting option 5:

```
*****
* The Virtual Appliance Menu
*****
* [1] Help
* [2] Configure The Virtual Appliance
* [3] Run Watchdog Command
* [4] Upgrade/Backup/Restore VA
* [5] Change Password
* [6] Logging
* [7] Login Authentication Server
* [8] Power Off
* [9] Reboot
* [10] Advanced Mode
* [11] Set Up Optional Tools
* [12] Convert to Cluster
* [13] Join Cluster
* [14] Troubleshoot
* [0] Log Out
*****
(*) Type your option:
```

```

*****
* Change Password
*****
* [1] Help
* [2] Change "cliadmin" Password
* [3] Change Mongo Database Password
* [4] Change Technical Support Code
* [5] Change FTP server Password
* [0] Exit
*****

```

Recommendation: Change all default user passwords including (Admin, Netadmin, Writer, User) after logging into OmniVista 2500 NMS for the first time. Go to the User Management Screen (Security - Users & User Groups - User) to update the passwords. Be sure to store the password(s) in a secure place. Lost passwords cannot be retrieved.

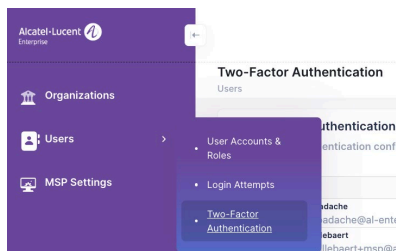
Two-Factor Authentication Login

Two-Factor Authentication (2FA) also referred to as two-step verification, is a security process in which users provide two different authentication factors to verify themselves. Two-Factor authentication adds an extra layer of security to your account by requiring more than just a password to log in.

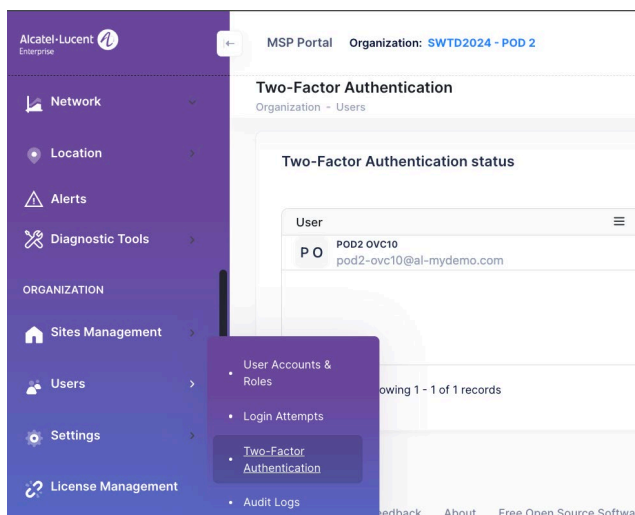
Recommendation: Enable two-factor authentication for all users on the MSP and organization level as it provides a robust defense against unauthorized access

In OmniVista Cirrus R10, there are two ways to enable Two Factor Authentication:

- Two factor authentication implemented by an MSP-Admin on all users from the MSP page.

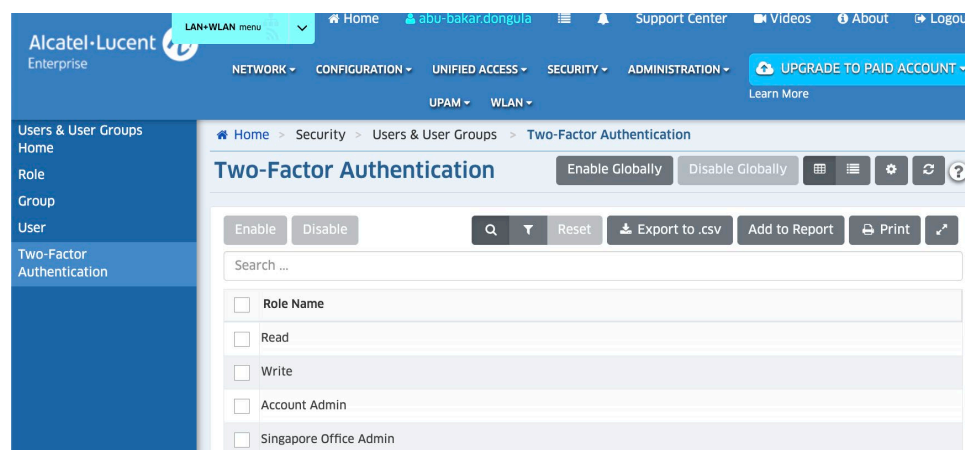


- Two factor authentication implemented by an ORG-Admin on all the users from the ORG page.



There are two modes used for two-factor authentication in OmniVista Cirrus 10, Email and Google authenticator.

In OmniVista Cirrus 4.x/2500 NMS, two-factor authentication can be enabled in the Security -> User & User Groups section as shown below:



Disable Unused Services

If you are not managing a wireless network and will not be using Captive Portal, it is recommended to disable it when first installing the OV 2500 VM as shown below:

Recommendation: Disable any unused services to prevent any unnecessary security exposure.

```
Configure Captive Portal IP & Ports
[1] Configure new Captive Portal IP & Captive Portal Ports
[2] Disable Captive Portal
(*) Type your option: _
```

Time Synchronization

You can configure NTP client and the timezone settings for time synchronization when first installing the OmniVista 2500 VM. The steps are highlighted below for timezone setting:

1. Enter 5 and press Enter to begin setting up the timezone.

```
*****
* Configure Timezones
*****
The available timezones list will be shown (press [q] to exit view mode)
Press [Enter] to continue
_
```

2. Press Enter to display timezones.
3. Press Enter to scroll through the list. After locating your timezone, press q and enter your timezone at the prompt (e.g., America/Los_Angeles). Then press Enter to set the timezone and return to the Configure Current Node Menu.

```
America/La_Paz
America/Lima
America/Los_Angeles
Please input timezones [America/Los_Angeles]: America/Los_Angeles
Would you like to set:
    timezones: America/Los_Angeles
[y;n] (y):
The configuration has been set
Press [Enter] to continue
```

You can verify the change using the (2) Display Current Node Configuration command.

To configure NTP client, the steps are highlighted below:

1. Enter 13 and press Enter to configure an NTP Server.

```
*****
* Configure NTP Client
*****
* [1] Help
* [2] Configure NTP Server IP
* [3] Status NTP Client
* [4] Disable NTP Client
* [5] Enable NTP Client
* [0] Exit
*****
```

2. Enter 2 and press Enter.
3. Enter the IP address of the NTP Server and press Enter.

Recommendation: Configure NTP time synchronization for log accuracy and correlation, and for supporting auditing and compliance

It is not required to configure NTP for the OmniVista Cirrus platforms since they are cloud-based solutions. Logging timestamps are based on the timezone configured in the tenant settings configured in the organization settings:

MSP Portal Organization: SWTD2024 - POD 2

Edit Organization
Organization - Settings - Basic Settings

Organization Information

Basic Information

Name *
SWTD2024 - POD 2

Country/Region *
FR-France

Timezone *
Europe/Paris (GMT+01:00)

Certificate Management

Internal Web Server

Since OmniVista Cirrus platforms are cloud-hosted platforms, they provide publically signed CA certificates for HTTPS connections. For example, this can be verified when accessing the OmniVista Cirrus 10 and verifying the certificate details:

eu.manage.ovcirrus.com/signin

Certificate Viewer: manage.ovcirrus.com

General Details

Issued To

Common Name (CN)	manage.ovcirrus.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	Sectigo RSA Domain Validation Secure Server CA
Organization (O)	Sectigo Limited
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Tuesday, August 6, 2024 at 4:00:00 AM
Expires On	Saturday, September 6, 2025 at 3:59:59 AM

SHA-256 Fingerprints

Certificate	36e2bfc319ae6cde83d84617e9ec16bbfc0dd4020380f65226617ff373d4818a
Public Key	37fe156a0c17cb5589469fdc1b09ec1b44a9fa302ba4a5a03b3e0cd6846fd4b1

For OmniVista 2500 NMS, the user can update the built-in web server certificate when installing the OmniVista 2500 VM. To update the OmniVista Web Server SSL Certificate, you must first generate a *.crt and *.key file and use an SFTP Client to upload the files to the VM. Make sure the destination directory is “keys”. You can follow similar steps mentioned in the [Stellar WiFi Express Internal Web Server - Generate Custom Certificate](#), but make sure the certificate format is “.crt”.

- SFTP User: cliadmin
 - SFTP Password: <password when deploying VA>
 - SFTP Port: 22
1. Enter 11 and press Enter.
 2. Choose a certificate file (.crt) and enter y and press Enter. Choose a private key file (.key) and enter y and press Enter.

Recommendation: Use a custom signed certificate for your internal web server and do not rely on the default self-signed certificate.

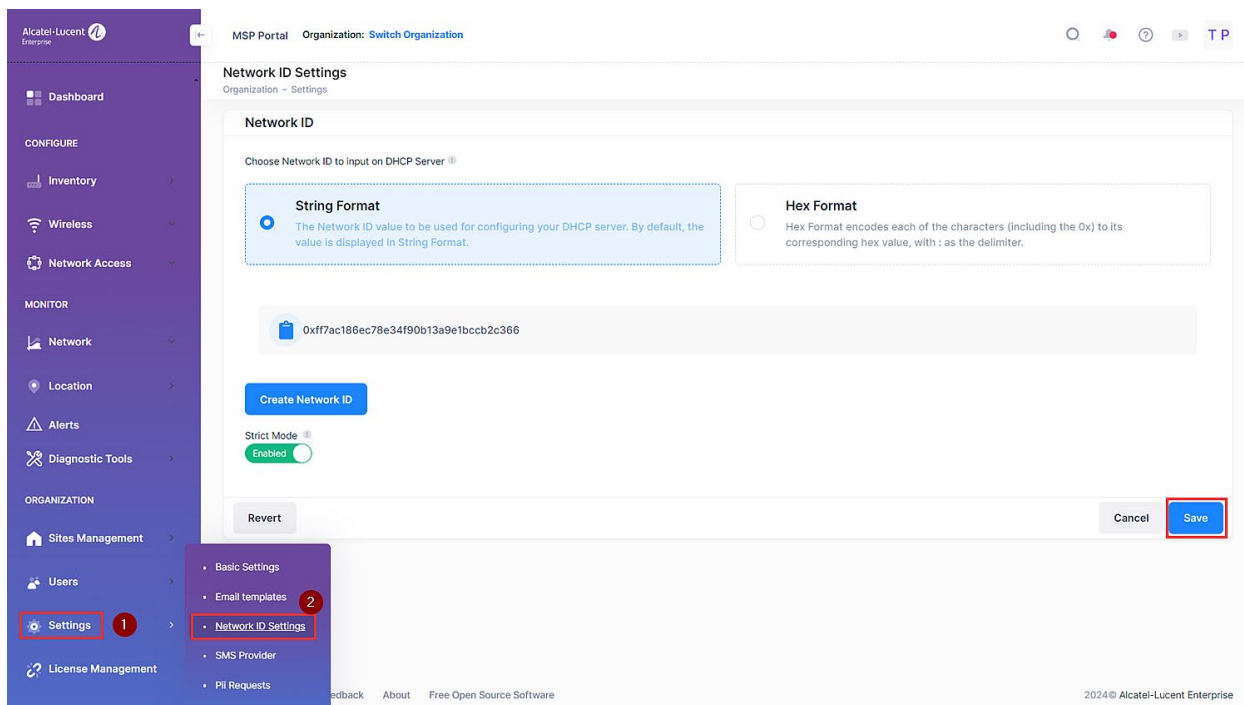
```
=====
* Update OmniVista Web Server SSL certificate
=====
* Available certificate(s)
=====
* [1] ov_server.crt
* [0] Exit
=====
(*) Type your option: 1
Would you like to use this certificate?
    [1] ov_server.crt
[y/n] (n): y
=====
* Available private key(s)
=====
* [1] ov_server.key
* [0] Exit
=====
(*) Type your option: 1
Would you like to use this private key?
    [1] ov_server.key
[y/n] (n):
```

Securely Onboarding Network Devices

In OmniVista Cirrus 4.x/10 platforms, you can secure the onboarding process of your managed network devices by using the Network ID feature. If the DHCP Server is configured with your Network ID, devices will get the Network ID from the DHCP Server and specify it whenever they call home. This will secure the on-boarding process by matching the Network ID from the devices with the Network ID in OmniVista. This helps prevent your devices from being on-boarded/managed by somebody else’s OmniVista.

Recommendation: use the Network ID feature to securely onboard your network devices to OmniVista Cirrus NMS platforms.

In OmniVista Cirrus 10, you can edit the Network ID format to input on the DHCP server, click on **Organization > Settings > Network ID Settings** to bring up the Network ID Information Form.

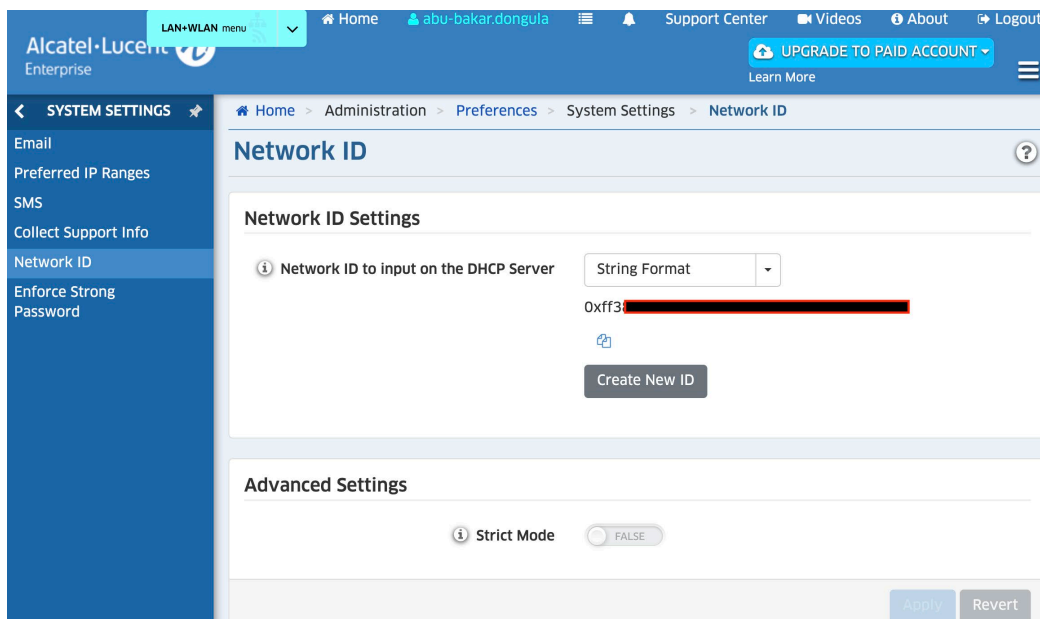


You must configure your DHCP Server Option 43, Sub-Option 133 with your Network ID. The Network ID value to be used for configuring your DHCP server is displayed beneath the drop-down. By default, the value is displayed in **String Format**. Select **Hex Format** to display the Network ID in Hex Format, if your DHCP Server needs the value to be entered in Hex Format. Click on the Clipboard icon to copy the Network ID to the clipboard and use this value to configure your DHCP Server.

After selecting the Network ID format, click on **Create Network ID** to create a network ID. You have the option to provide a user supplied key or allow the system to generate an auto generated key.

It is recommended to also enable Strict Mode option, which does not allow devices that do not send a Network ID to be associated with this OmniVista Cirrus System.

In OmniVista Cirrus 4.x, this can be configured in the Administration -> Preferences -> System Settings -> Network ID as shown below:



Provisioning Management Roles, Groups, and Users

There are two types of OmniVista Cirrus 10 Users:

- **Managed Service Provider (MSP) User** - An MSP User creates the OmniVista Cirrus Management Portal for their Organization (as well as any additional Organization Management Portals that may need to be created). After setting up an Organization for network management, an MSP Network Administrator invites Organization Users via e-mail to create an OmniVista Cirrus Account.
- **Organization User** - After setting up an Organization for network management, an MSP User invites Organization Users via e-mail to create an OmniVista Cirrus Account to access an Organization for management. When creating the invitation, the MSP User specifies the access rights for the Organization User (e.g., Admin, Viewer, Limited). Once the User Account is created and approved, an Organization User is able to access the Organization Management Portal with the access rights specified by the MSP User.

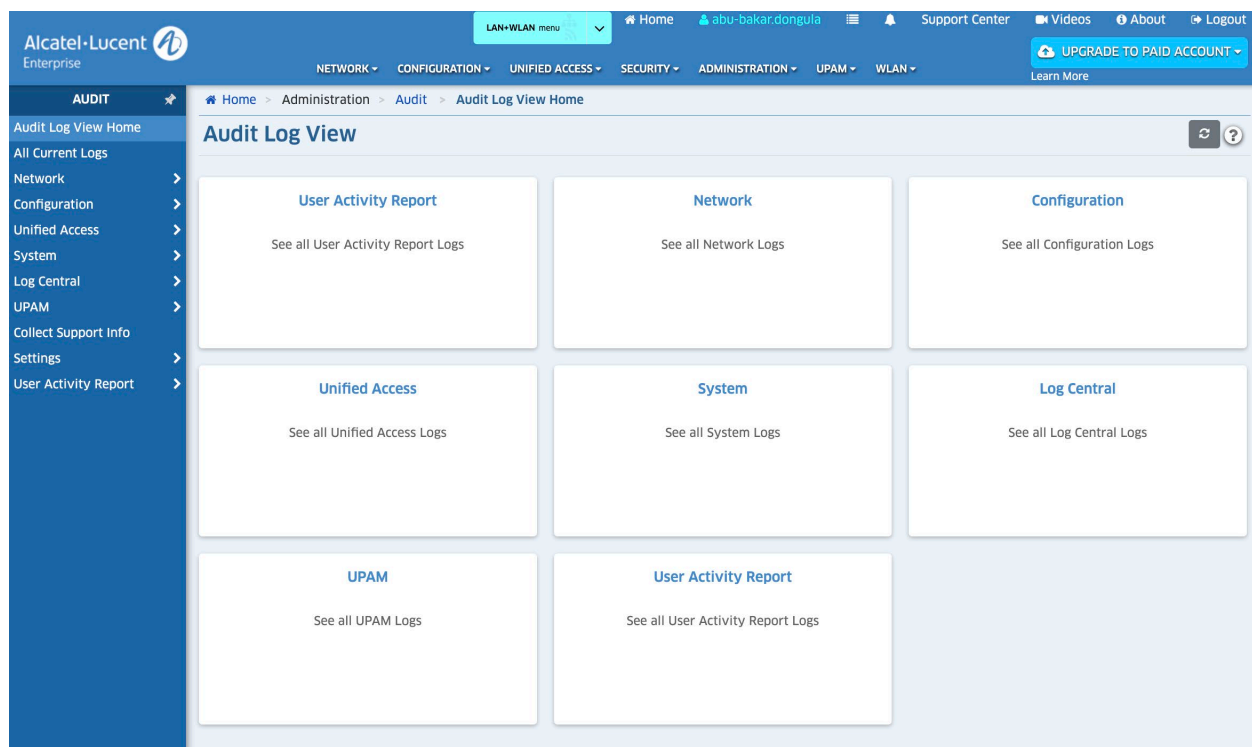
Recommendation: Create role-based access and use the principle of least privilege when creating user accounts.

Logging and Analytics

In OmniVista Cirrus 4.x/2500, the Audit application is used to monitor client and server activity, such as the date and time when a user logged into OmniVista, when an item was added to the discovery database, when a configuration file was saved, or when a particular application was launched. The information is contained in log files, which are organized by type (e.g., Network, Configuration), as shown on the Audit Home Page.

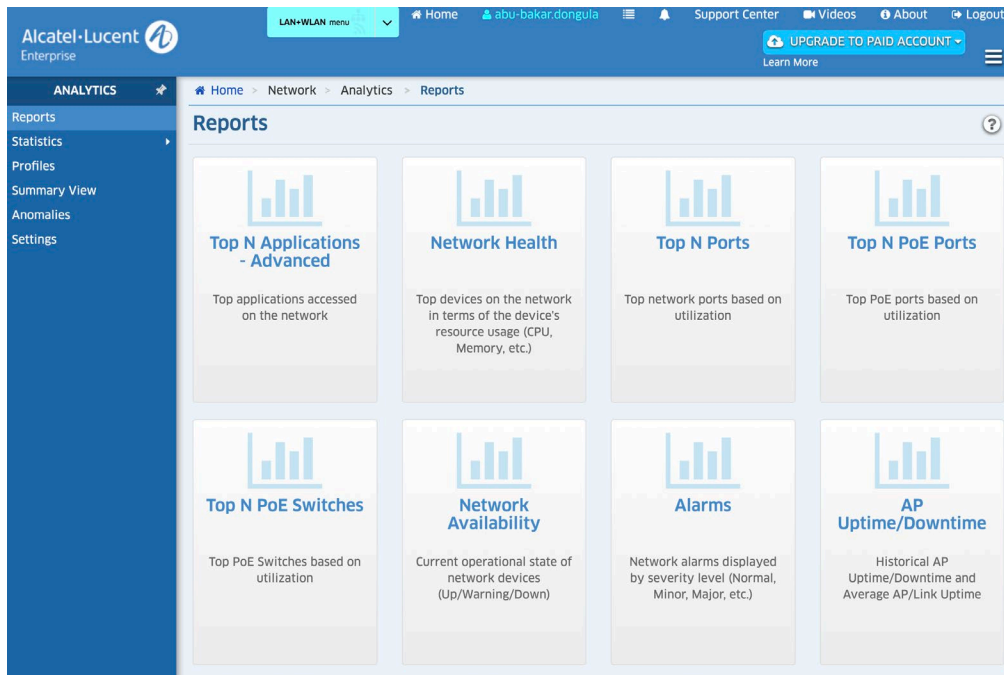
Recommendation: Regularly monitoring your network and client activities is very important from a security standpoint to detect any anomalies and Indicators of compromise (IoC).

The application enables you to view log files, search through log files, and download files. You can view current log files or historical log files that have been archived by OmniVista. Log Files are archived based on preferences configured on the Audit Settings Screen.



The Analytics Application provides users with a comprehensive view of network resource utilization, including views of users, devices, and applications. The application also provides information on usage trends, including predictive analysis of future network resource utilization. The Analytics Application provides real-time viewing of Analytics Reports. You can also schedule Analytics Reports to be generated and stored as PDF documents using the Report

Application. This way, in addition to real-time viewing in the Analytics Application, you can automatically generate and store Analytics Reports that you can view at any time.



You can also detect any anomalies using the Analytics Anomalies Screen which displays any anomalies that are discovered in established port utilization trends. The information is displayed in a list that describes the anomaly and its origins (e.g., IP address, Port). Anomaly detection uses Z-Score to check for anomalies in the latest port utilization data gathered from hourly polling over the past 30 days. Z-Score is a statistical measurement of a score's relationship to the mean in a group of scores. In other words, it measures utilization for a port for a specific hour to determine its relationship with utilization for the same hour over the sampling period (30 days). A data point that deviates considerably from an established pattern is flagged as an anomaly and displayed on the Anomalies Screen. Z-Score parameters are configured on the Preferences - Analytics Screen.

In OmniVista Cirrus 10, whenever an Organization user performs an action (such as inviting a user to join the Organization or updating building information for an Organization site) the action is logged as an event in the Audit Log list as shown below:

MSP Portal Organization: [Switch Organization](#) Q 🔴 ? ⌵ T P

Audit Logs
Organization - Users Last 7 Days: 1:53 pm (Apr 10) - 1:53 pm (Apr 17)

[Click here to select Audit Logs Time Range](#)

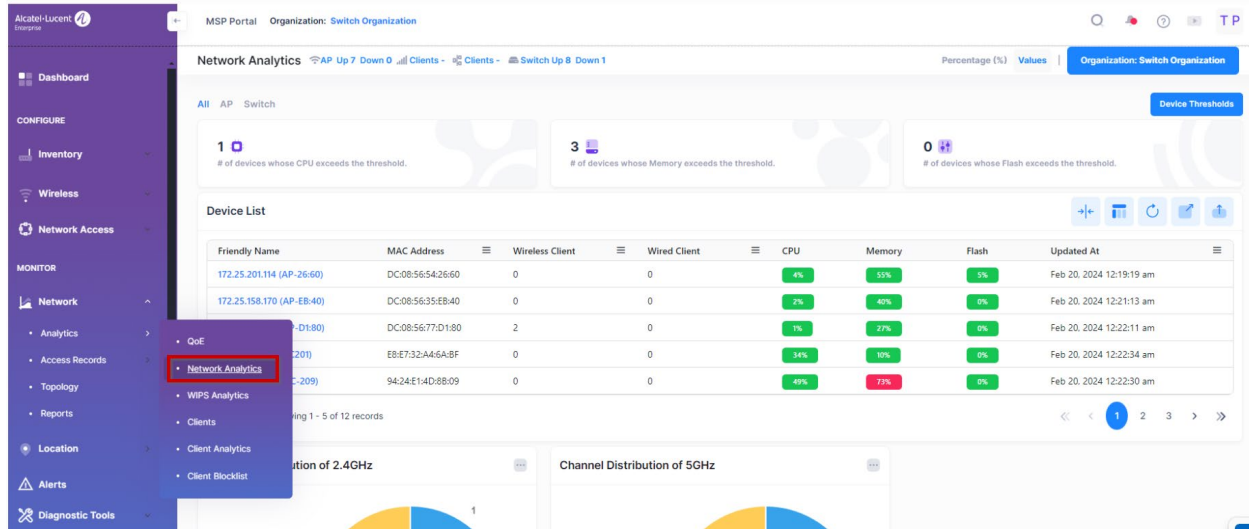
Audit Logs List ↔ 📄 🔄 📧 📌

Timestamp ↓	User	Description	Site	Actions
Apr 17, 2024 12:57:38 pm	T P Tech Pubs tech.pubs.to@gmail.com	Sending an invitation to join the or...	-	📄
Apr 17, 2024 11:10:03 am	T P Tech Pubs tech.pubs.to@gmail.com	Send '4' invitations to join the orga...	-	📄
Apr 17, 2024 10:55:31 am	T P Tech Pubs tech.pubs.to@gmail.com	Sending an invitation to join the or...	-	📄
Apr 17, 2024 10:38:23 am	T P Tech Pubs tech.pubs.to@gmail.com	Delete Wall 'Wall 3' in Building 'Libr...	TestDocs	📄
Apr 17, 2024 10:05:17 am	T P Tech Pubs tech.pubs.to@gmail.com	Update Polygon of the Wall 'Wall 3'	TestDocs	📄
Apr 17, 2024 10:04:54 am	T P Tech Pubs tech.pubs.to@gmail.com	Update Polygon of the Wall 'Wall 3'	TestDocs	📄
Apr 17, 2024 9:21:11 am	T P Tech Pubs tech.pubs.to@gmail.com	Add Wall 'Wall 3' in Building 'Librar...	TestDocs	📄
Apr 17, 2024 4:37:05 am	S M Soudabeh Mirzataraj soudabeh.mirzataraj@al-enterprise.com	Start a SSH connection to '172.25.0...	-	📄
Apr 16, 2024 2:41:27 pm	T P Tech Pubs tech.pubs.to@gmail.com	Delete Floor 'Media Wing' from Bui...	TestDocs	📄
Apr 16, 2024 2:32:15 pm	T P Tech Pubs tech.pubs.to@gmail.com	Update Settings of Floor 'Research ...	TestDocs	📄

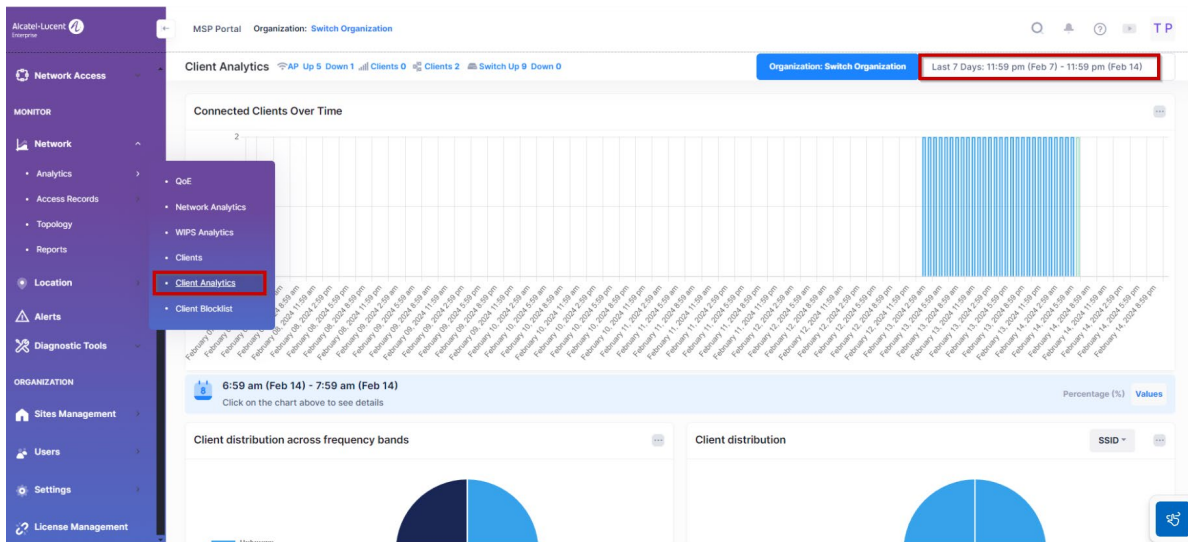
10 Showing 1 - 10 of 130 records ⏪ < 1 2 3 4 5 > ⏩

OmniVista Cirrus 10 platform also provides advanced network and client analytics under the Monitor section.

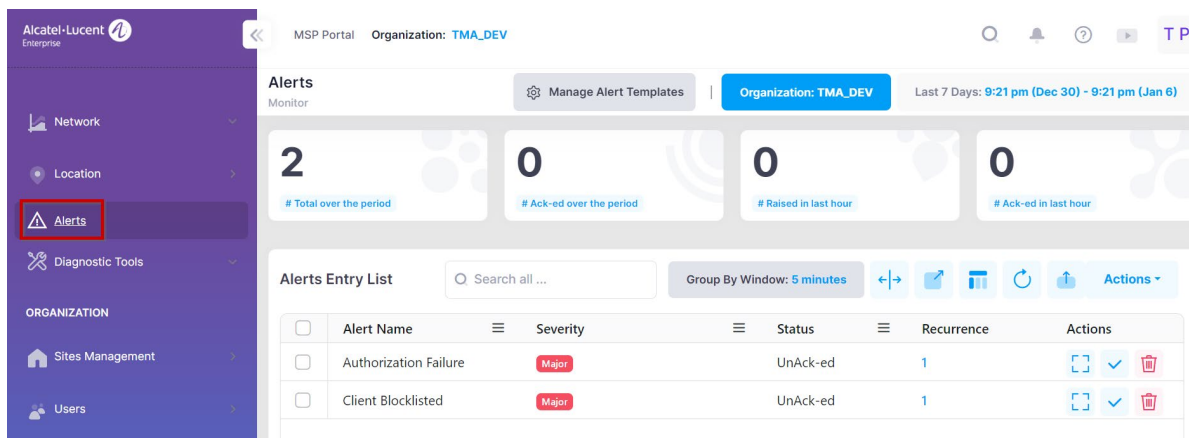
In the Network Analytics sub-section, you can analyze network metrics, generate reports on network utilization, review access records, and define custom dashboards to monitor specific metrics. This is shown below:



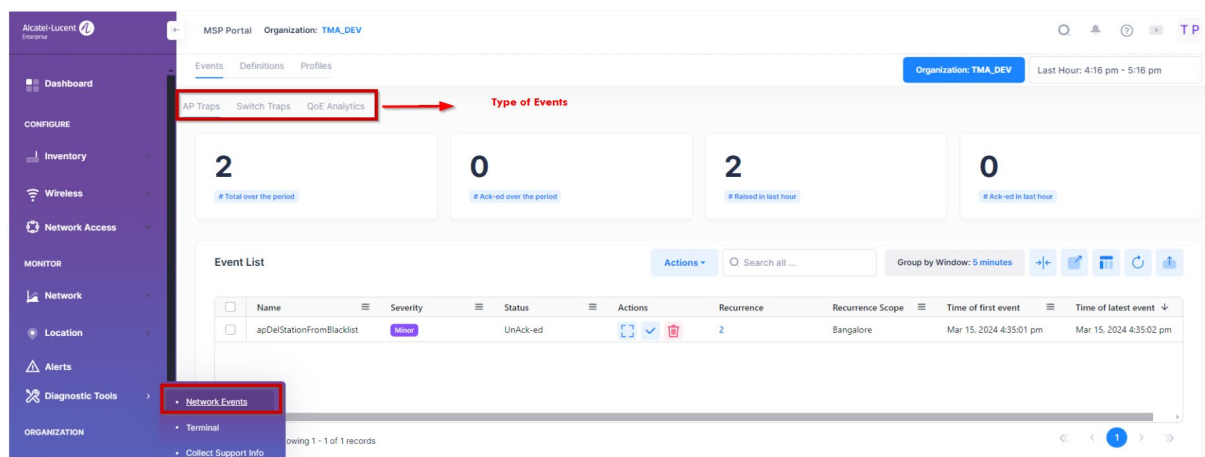
You can also monitor client analytics which allows you to determine the characteristics of the clients that are currently connected or have been connected to your LAN/WLAN network:



The Alerts sub-section allows you to monitor and analyze alerts received from network devices as shown below:



The Diagnostic Tools sub-section allows you to analyze network events, connect to devices, and collect log file information from network devices as shown below:



Control Plane Certificate Management

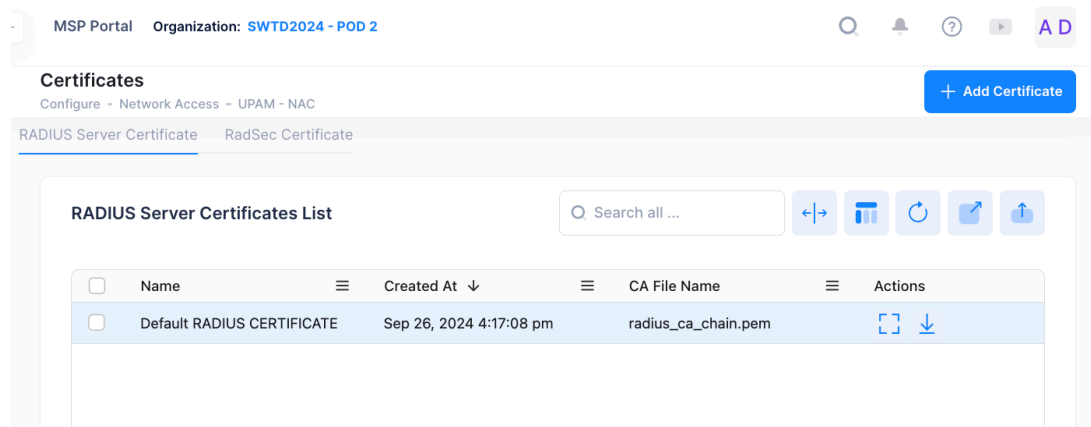
UPAM RADIUS Server Certificate

In OmniVista Cirrus 10, the RADIUS Certificates screen displays information about all RADIUS Server and RadSec Certificates. Use this screen to add, download, and delete the following UPAM RADIUS Server certificates:

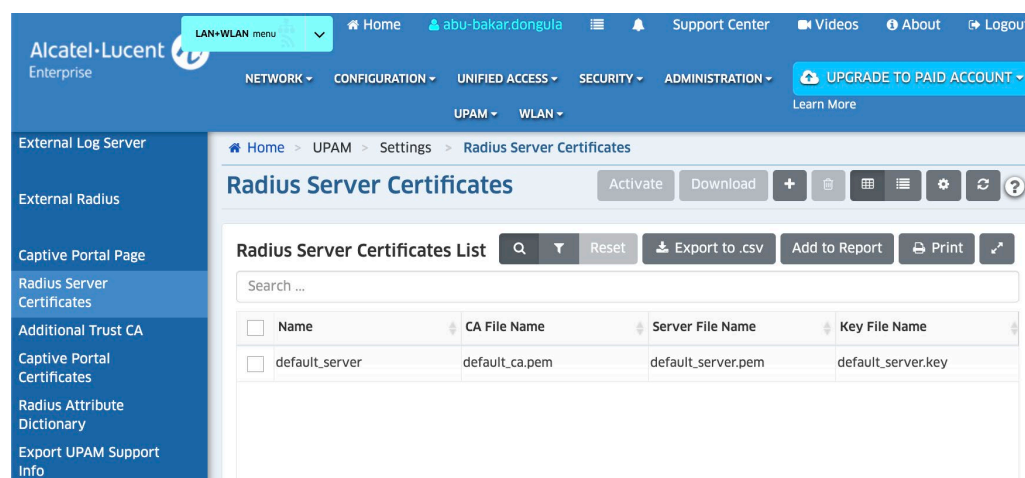
- **RADIUS Server Certificate** - Used to establish a secure connection with a network device for 802.1X or TLS authentication.
- **RadSec Certificate** - Used to establish a secure connection between UPAM and an external RADIUS server that uses RadSec (RADIUS-over-TLS). UPAM acts as a RadSec client when communicating with the RadSec server. This is covered in the coming section.

Recommendation: Do not rely on the Default Server Certificate on UPAM but install a Custom Server Certificate on UPAM for improved security.

In OmniVista Cirrus 10, the RADIUS Server certificates can be configured in the UPAM Certificates section as shown below:

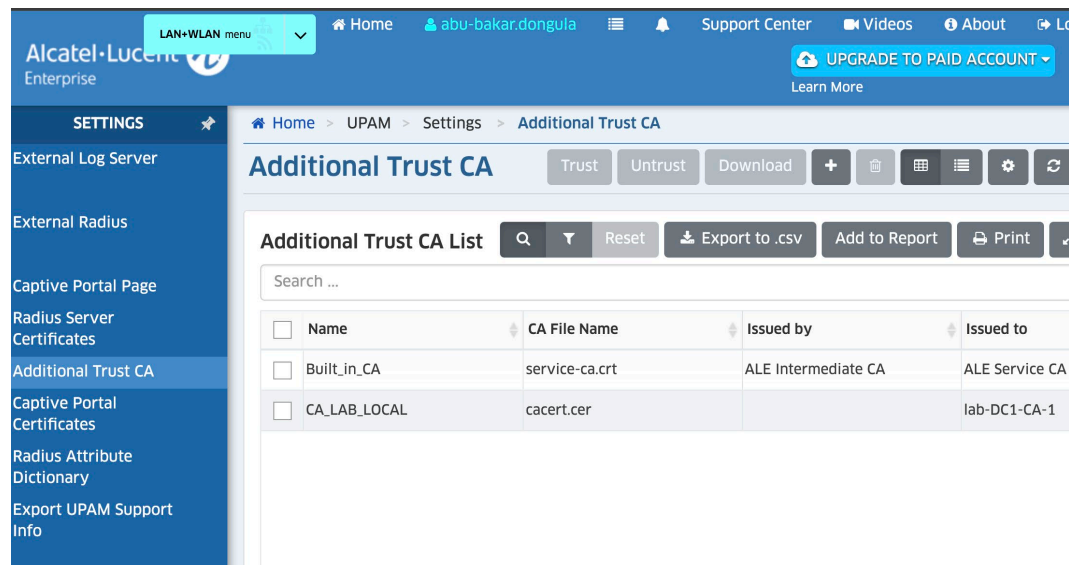


In OmniVista Cirrus 4.x/2500 NMS, you can add and activate RADIUS server certificates in the UPAM settings menu as shown below in OmniVista Cirrus 4.x NMS:

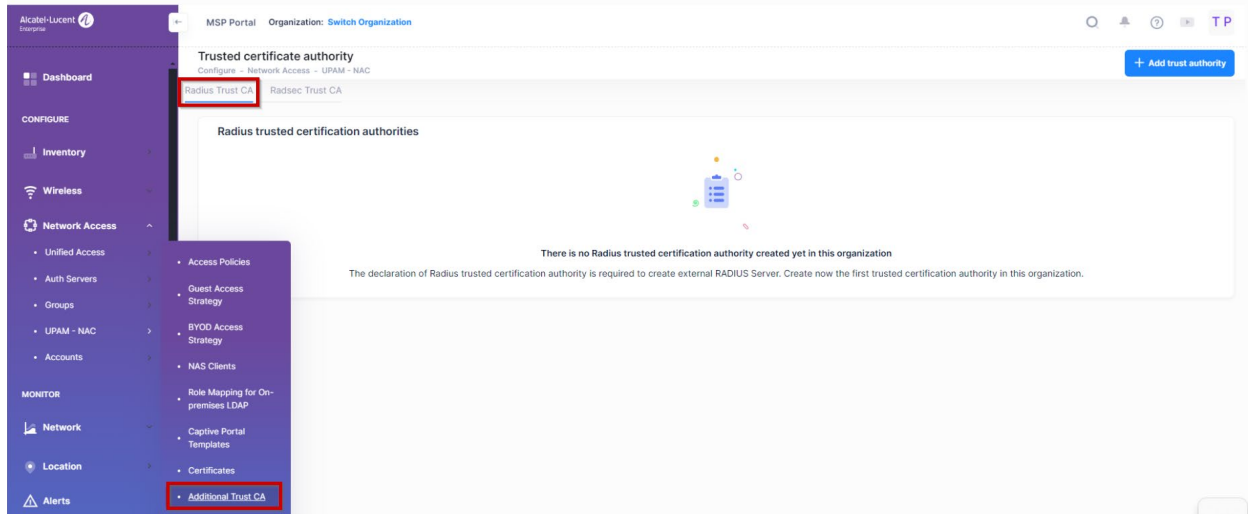


UPAM - Additional Trust CA

In OmniVista Cirrus 4.x/2500 and 10 platforms, you can add an additional Radius trusted CAs in the UPAM Trust RADIUS Store.

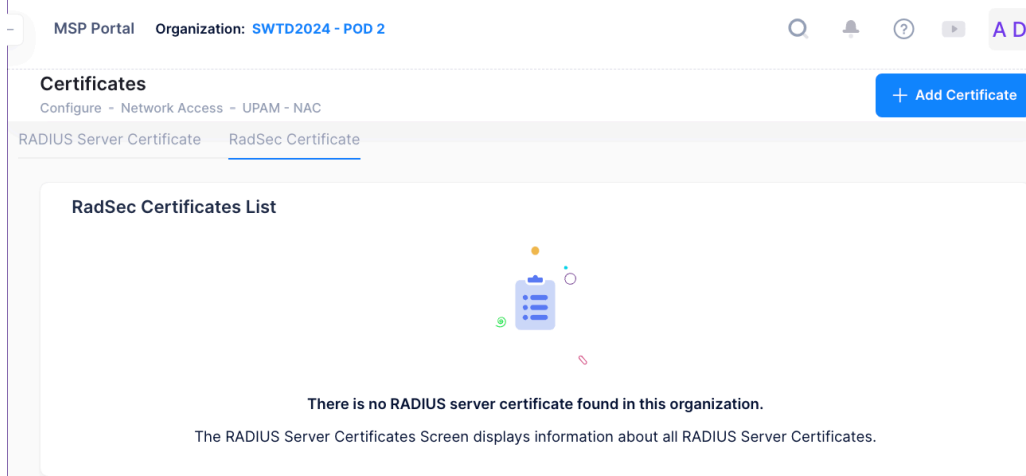


In OmniVista Cirrus 10, to manage Trusted Certificate Authorities, click on **Network Access > UPAM-NAC > Additional Trust CA** under the “Configure” section of the OmniVista Cirrus Menu.



UPAM - External Radsec Certificates

In OmniVista Cirrus 10, you can add Radsec certificates which are used to establish a secure connection between UPAM and an external RADIUS server that uses RadSec in the UPAM Certificates configuration section as shown below:



Recommendation: Enable Radsec to secure communication between UPAM and External RADIUS server using TLS encryption.

After adding the Radsec certificate, it can be selected when adding an external RADIUS server as part of the Configure -> Network Access -> UPAM-NAC -> External Source -> External Radius Server configuration menu to allow UPAM to act as a RadSec client when communicating with the external RadSec server as shown below:

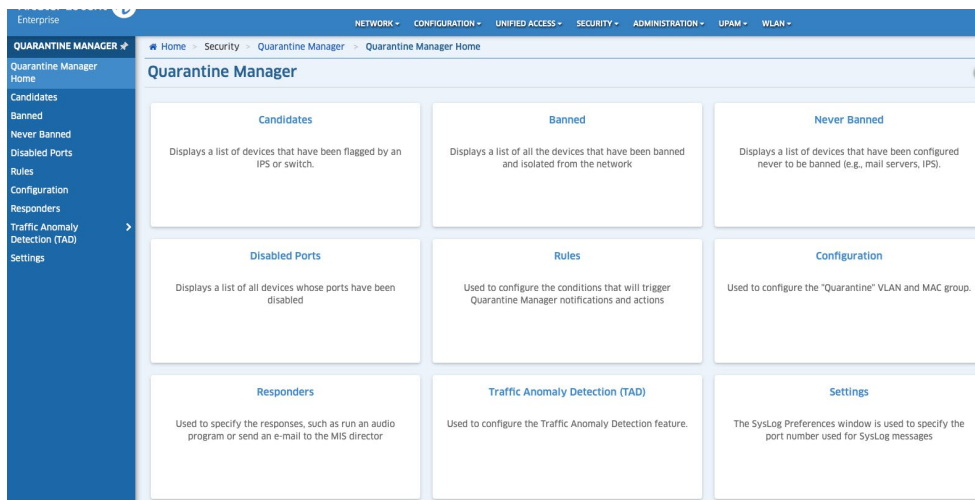
and shutting down the port. This prevents the offending wireless client from gaining network access through another AP.

Recommendation: Integrate Quarantine Manager application with IPS to protect the network from attacks by isolating the malicious device avoiding lateral movement.

The application also includes the optional Quarantine Manager Remediation (QMR) feature. QMR is a switch-based application that interacts with Quarantine Manager to restrict network access of quarantined clients and provide a remediation path for these clients to regain their network access.

By sending a quarantine order for this device/user to OV Quarantine Manager, the suspicious device is isolated at its attached switch or AP level, avoiding lateral movements in the intranet.

For more details on Quarantine Manager feature, please refer to the Zero Trust Series: Quarantine and Remediation video as referenced in the [Related Documents](#) section.



REST API Security Recommendations

API security is crucial for safeguarding data, services, and systems exposed through application programming interfaces (APIs). Here are some of the best practices for securing APIs:

- Enforce HTTPS/TLS Encryption for API communication by disabling HTTP WebView access
- Disable WebView services on your OmniSwitch devices and OmniAccess Stellar APs to disable API exposure in case you are using OmniVista 2500 or Cirrus to manage your network devices. You will still be able to make REST API calls to your OmniVista platform.
- Rely on token-based authentication (OAuth, JWT, etc.).
 - OmniVista Cirrus 4.x/ OmniVista 2500 NMS uses OAuth 2.0 protocol to authorize and authenticate calls. It provides secure access to protect your resources, thereby reducing the hassle of asking for a username and password every time a user logs in. After successfully login, you will be provided with access token which can be used to authorize rest of API.
 - OmniVista Cirrus 10 platform uses an authentication mechanism based on JSON Web Token (JWT) which is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object.
- Create a dedicated user credentials for API access. This will allow you to audit user activities.
- Apply the principle of least privilege: Ensure that users or services accessing your APIs only have the minimum access rights necessary to perform their tasks.
- Use strong and complex passwords
- Avoid exposing APIs to the outside world (internet)
- Store your authentication credentials securely and don't store them in the code. You can use a third-party application to store and manage tokens, passwords, certificates, and API keys.

Switching - Web Services Security

The Web Services feature provides the ability to customize and extend the management interface on AOS devices. It supports the use of CLI scripting in AOS as well as a REST based 'web' interface that interacts with AOS management variables (MIB) and CLI commands. It provides two methods for configuration through either the direct handling of MIB variables or the use of CLI commands and supports both XML and JSON response formats.

Security is maintained through the use of backend sessions and frontend cookies which is the same as current HTTP security for thin clients.

- Authentication - Adheres to a web-service model, through its own REST domain and use of the GET verb.
- Authorization - Follows the usual authorization mechanism already in use in WebView, where WebView checks with Partition Manager what permission families a user belongs to, thus specifying which MIB tables are accessible to that user.

Encryption - Follows the same model as WebView: if unencrypted access ("HTTP") is allowed, then the Web Service is allowed over the same transport. Similarly, if listening HTTP/HTTPS ports are changed, the Web Service will be available through those ports. It is recommended to enforce HTTPS.

Conclusion

Alcatel-Lucent Enterprise products follow a secure by design approach. We have covered the best practice recommendations to secure your ALE products, but due to the diversity of information systems, it is important for the network administrator to have a comprehensive multi-layered cybersecurity strategy to protect critical business assets.

In addition, software should be patched regularly, physical access to network devices should be secure, and information security awareness training should be provided to employees.

It is recommended as well to regularly stay updated with new threats by subscribing to relevant security advisories, such as ALE PSIRT security advisory and US-CERT.

Related Documents

- [1] Zero Trust Architecture eBook - <https://www.al-enterprise.com/-/media/assets/internet/documents/zero-trust-architecture-ebook-en.pdf>
- [2] Zero Trust Series: Quarantine and Remediation - <https://www.youtube.com/watch?v=qjBsqqgUTcsk>
- [3] Network Infrastructure Solutions: Security Best Practices - <https://www.al-enterprise.com/-/media/assets/internet/documents/network-infrastructure-solution-security-tech-brief-en.pdf>
- [4] OmniVista UPAM Architecture Guide - https://spacewalkers.s3.eu-west-3.amazonaws.com/Omni_Vista_2500_UPAM_Architecture_Guide_c1960c592e.pdf
- [5] AOS 8.10 R02 Network Configuration Guide - <https://www.al-enterprise.com/-/media/assets/internet/documents/n-to-s/omniswitch-aos-release-810r2-network-configuration-user-guide-rev-a-en.pdf>
- [6] AOS 8.10 R02 CLI Guide - <https://www.al-enterprise.com/-/media/assets/internet/documents/n-to-s/omniswitch-aos-release-810r2-cli-reference-user-guide-rev-a-en.pdf>
- [7] AOS 8.10 R02 Switch Management Guide - <https://www.al-enterprise.com/-/media/assets/internet/documents/n-to-s/omniswitch-aos-release-810r2-switch-management-user-guide-rev-a-en.pdf>
- [8] AOS 8.10 R02 Advanced Routing Guide - <https://www.al-enterprise.com/-/media/assets/internet/documents/n-to-s/omniswitch-aos-release-810r2-advanced-routing-user-guide-rev-a-en.pdf>
- [9] AOS 8.10 R01 Specifications Guide - <https://www.al-enterprise.com/-/media/assets/internet/documents/n-to-s/omniswitch-aos-release-810r1-specifications-guide-rev-a-en.pdf>
- [10] OmniVista Cirrus 10 Online Documentation - <https://docs.ovcirrus.com/ov/>
- [11] OmniAccess Stellar AP User Guide - AWOS 5.0.1 - https://spacewalkers.s3.eu-west-3.amazonaws.com/oaw_stellar_ap_user_guide_awos_5_0_1_rev_a_en_683c41a696.pdf

- [12] OmniVista 2500 NMS 4.9R1 Installation and Upgrade Guide - https://spacewalkers.s3.eu-west-3.amazonaws.com/OV_2500_NMS_E_4_9_R1_Installation_and_Upgrade_Guide_Rev_A_7c5d36df2e.pdf
- [13] OmniVista 2500 NMS 4.9R1 User Guide - https://spacewalkers.s3.eu-west-3.amazonaws.com/OV_2500_NMS_E_4_9_R1_User_Guide_Rev_A_e7284ba95b.pdf
- [14] OmniVista 2500 NMS 4.9R1 Release Notes - https://spacewalkers.s3.eu-west-3.amazonaws.com/OV_2500_NMS_E_4_9_R1_Release_Notes_Rev_A_263e294dff.pdf
- [15] Preparation and Operation of Common Criteria Evaluated OmniSwitch Products (NDcPP) - Administrative Guide for AOS Release 8.9.R11 - <https://www.niap-ccevs.org/products/11404>
- [16] Multi-Factor Authentication with Google Authenticator or Duo - <https://www.al-enterprise.com/-/media/assets/internet/documents/multi-factor-authentication-with-google-authenticator-or-duo-application-note-en.pdf>