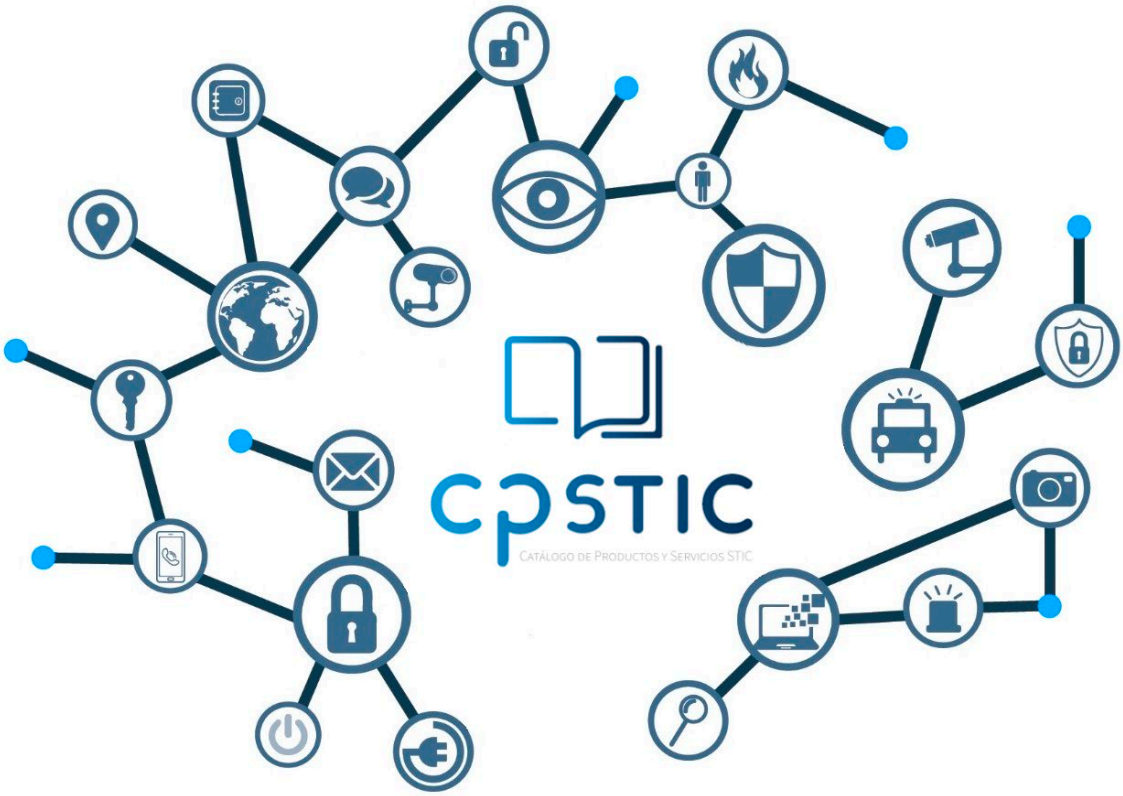
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1438

Procedimiento de empleo seguro Controlados inalámbricas CISCO WLC 9800 y Puntos de Acceso Cisco Catalyst



Febrero de 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-074-6.
Fecha de Edición: febrero de 2024.

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.02.19 09:31:55 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. El objetivo de este documento es proporcionar una guía o procedimiento de configuración y empleo seguro de la familia de **controladoras inalámbricas Cisco WLC**, tanto en su forma de appliance (Cisco Catalyst 9800), como en sus implementaciones en la variante de máquina virtual (Cisco Catalyst 9800-CL).
2. El sistema operativo estudiado será el propietario de Cisco para estos equipos, denominado IOS-XE en su versión 17.6, en contraposición al sistema operativo Catalyst AireOS que opera en la anterior familia de controladores inalámbricos de la serie 5500 o 2500.
3. Se trata de implementaciones centralizadas de los sistemas inalámbricos de una organización, que pueden realizarse de dos (2) maneras:
    - Centralizando tanto plano de control como plano de datos (modo centralizado).
    - Centralizando únicamente el plano de control (modo flexconnect).
4. En ambos casos, el protocolo subyacente, tanto para el envío de los paquetes de control como el encapsulamiento de los planos de datos es el CAPWAP (*Control and Provisioning of Wireless Access Points*), en una implementación propia de Cisco que no permite interoperabilidad con otros fabricantes que usen dicho protocolo.
5. **Las controladoras Wireless 9800-80-K9, 9800-40-K9, 9800-L (C9800-L-F-K9 Y C9800-L-C-K9) y 9800-CL-K9, con IOS XE 17.6, han sido cualificadas e incluidas en el Catálogo de Productos y Servicios STIC (CPSTIC), para categoría ALTA del Esquema Nacional de Seguridad, en la familia '*Dispositivos de Red Inálambricos*'.** Los puntos de acceso cualificados son:
    - Cisco Aironet 1562i, Cisco Aironet 1562e y Cisco Aironet 1562d.
    - Cisco Aironet 2802i y Cisco Aironet 2802e.
    - Cisco Aironet 3802i, Cisco Aironet 3802e y Cisco Aironet 3802p.
    - Cisco Aironet 4800 Access Point.
6. Se recomienda consultar el CPSTIC para conocer los modelos y *firmware* cualificado en cada momento.
7. Hay que tener en cuenta que los puntos de acceso en las controladoras Cisco WLC 9800 utilizan el protocolo CAPWAP, por lo que su firmware dispone de únicamente un subconjunto del plano de control de las controladoras, que es donde realmente se procesan la mayor parte de los aspectos relacionados con la seguridad. En el punto de acceso quedan principalmente las tareas puramente relacionadas con el entorno radioeléctrico, y el establecimiento del túnel CAPWAP (bajo DTLS) con la controladora, lo cual hace de dicho túnel el principal aspecto de seguridad relacionado específicamente con los puntos de acceso. Dicho aspecto se abordará en el apartado correspondiente al establecimiento de los túneles CAPWAP, disponible en la presente guía.

2. OBJETO Y ALCANCE

8. El objeto de la presente guía es poner en conocimiento del administrador de la unidad los mecanismos de seguridad necesarios para proteger los sistemas de información y comunicaciones que empleen en sus instalaciones controladoras inalámbricas IOS-XE en su versión 17.6. Con este conocimiento, es posible establecer un marco de referencia que contemple las recomendaciones STIC en el despliegue y utilización de esta categoría de comunicaciones inalámbricas.
9. Las recomendaciones explicitadas en este documento **aplican principalmente a entornos de red inalámbrica operando en modo centralizado (mediante controlador central)**, aunque algunos conceptos y prácticas pueden hacerse extensibles a entornos operando en modo autónomo, o con otros fabricantes de equipamiento inalámbrico centralizado.
10. El alcance del presente documento queda enfocado en todos los aspectos de configuración de seguridad de los equipos, tanto en la comunicación entre los puntos de acceso y la controladora, como entre los clientes y dichos puntos de acceso.
11. Por tanto, en la presente guía no se van a detallar elementos de operación de entornos WiFi relacionados con su configuración en cuanto a operación básica, o rendimiento, como, por ejemplo:
    - Configuración de canales radio para baja interferencia cocanal (CCI).
    - Configuración de elementos de modulación para mejora del ancho de banda en las comunicaciones inalámbricas (índices de modulación).
    - Elementos relacionados con las capacidades de transición (roaming) entre las celdas inalámbricas, salvo aquellos que tienen relación con elementos de seguridad, como el pre-cacheo de contraseñas.
    - Políticas de flujo de información y el control de acceso, deben ser implementadas de acuerdo a las políticas vigentes en la organización.
12. Las autoridades responsables de la aplicación de la política de seguridad de las TIC (STIC) determinarán el análisis y aplicación de este documento a los equipos Cisco Catalyst 9800 bajo su responsabilidad.
13. La aplicación de las recomendaciones y configuraciones de la presente guía deben cumplir además las normas dadas en la guía de seguridad de redes inalámbricas (CCN-STIC-816).
14. La estructura del documento y sus contenidos no exigen una lectura lineal del mismo. Se recomienda al lector utilizar el índice de contenidos para localizar el capítulo que trate el aspecto concreto sobre el que se desee obtener información.

3. ORGANIZACIÓN DEL DOCUMENTO

15. En esta sección se muestra la estructura del documento:

- Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
- Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
- Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- Apartado **7**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto para cumplir con las medidas de seguridad para infraestructuras inalámbricas.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

16. El dispositivo Catalyst 9800 en formato *appliance* debe ser examinado para comprobar que no ha sido manipulado durante su entrega siguiendo los pasos descritos a continuación (ver [1][2][3]):

    - Antes de abrir el paquete donde fue entregado el Catalyst 9800, se debe comprobar que el paquete contiene la serigrafía y logo de Cisco Systems. Si no es así, se recomienda contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).
    - Es necesario comprobar que el paquete no ha sido abierto y sellado de nuevo, mediante inspección de la cinta que lo cierra. Si el paquete tuviera signos de haber sido abierto y después sellado de nuevo, es recomendable contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).
    - Se debe verificar que el paquete contiene la impresión resistente a manipulaciones de Cisco en la cara externa de la caja de cartón. Si no es así, se deberá contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado). Esta impresión contiene el número de producto de Cisco, su número de serie e información adicional sobre el contenido de la caja.
    - Es importante chequear el número de serie del Catalyst 9800 especificado en la documentación del pedido. El número de serie que figura en la etiqueta blanca de la caja se debe corresponder con el número de serie del dispositivo. Por tanto, es necesario verificar que este número concuerda con el número de serie en la factura enviada por correo. Si no es así, se debe contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).
    - En la recepción de la unidad, es necesario comprobar que el pedido fue enviado por el proveedor esperado (Cisco Systems o un distribuidor autorizado). Este proceso puede llevarse a cabo verificando el código de envío/paquete junto con la empresa de transporte. También es recomendable comprobar que los números de serie de los productos enviados concuerdan con los números de serie de los productos recibidos. Esta verificación debe ser llevada a cabo por algún mecanismo externo que no pertenezca al proceso de envío. Por ejemplo, teléfono, fax o un servicio online de rastreo de paquetes.

17. Una vez que el paquete ha sido abierto, es recomendable inspeccionar el dispositivo. Aquí es necesario comprobar que el número de serie mostrado en él concuerda con el número de serie que aparece en la documentación del envío y la factura. Si no es así, se debe contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).

18. De igual forma, una vez realizada la apertura del paquete que contiene la unidad Wireless LAN Controller, se debe asegurar que contiene todos los elementos que el fabricante indica. En el caso del dispositivo *Cisco Catalyst 9800-40/-80 Wireless LAN Controller*, el contenido del embalaje debe incluir (ver [1][2]):

    - Unidad Cisco Catalyst 9800-40/-80 Wireless LAN Controller.
    - Dos pletinas frontales y otras dos traseras para sujeción a armario (se deben solicitar si la unidad se compró como una unidad de repuesto).

- Pletinas para sujeción de cable de gestión (se deben solicitar si la unidad se compró como una unidad de repuesto).
- Juego de tornillos para las pletinas frontales, traseras y sujeción de cable de gestión.
- Cable RJ45 en ambos extremos configurado como cable cruzado.
- Cable de consola RJ45 – DB9 (hembra).
- Muñequera anti electricidad estática desechable.
- Documento informativo sobre Seguridad y Cumplimiento Normativo (Regulatory Compliance and Safety Information).
- Cable de alimentación (si fue solicitada una fuente de alimentación).

19. Para el equipo Cisco Catalyst 9800-L, el contenido que debe incluir es el siguiente (ver [3]):
    - Unidad Catalyst 9800-L Wireless LAN Controller.
    - Fuente de alimentación.
    - Cable de alimentación.
    - Cuatro piezas adhesivas de goma.
    - Documento informativo sobre Seguridad y Cumplimiento Normativo (Regulatory Compliance and Safety Information).
    - Cuartillo para el registro del producto e información sobre la documentación de Cisco.
20. Tras realizar los procedimientos iniciales de configuración, y antes de poner la unidad en su entorno productivo, **se debe comprobar que el software de la unidad no ha sido comprometido (ver** [4][5][6]**)**. Se recomienda revisar el apartado **6.5** sobre actualización/verificación de firmware para tal efecto.

4.2 ENTORNO DE INSTALACIÓN SEGURO

21. El dispositivo Cisco Catalyst WLC 9800 Series debe instalarse en una ubicación físicamente segura donde solo se permita acceso físico al personal autorizado.
22. Se requieren los siguientes componentes para disponer de un entorno de configuración inicial seguro:
    - **Puesto de gestión con navegador Web seguro:** Es posible configurar el equipo de forma remota mediante un navegador web. El equipo se comportará como servidor web y será necesario el uso de un navegador para acceder a él. Aunque está disponible el acceso tanto por protocolo HTTP como HTTPS, se debe implementar una configuración inicial para implementar HTTPS, y con un certificado interno válido para las máquinas de gestión, que evite errores de validez de certificado.
    - **Puesto de gestión con cliente SSH:** Adicionalmente, es posible configurar el equipo desde un puesto de gestión con cliente SSH. Este puesto hace referencia a cualquier estación de trabajo con un cliente SSH instalado que se emplea por

el administrador de los Cisco Catalyst WLC 9800 Series para su administración a través de los canales protegidos de SSH v2 (ver [7]).

- **Consola local:** Esto incluye cualquier entorno de consola que esté directamente conectado a los Cisco Catalyst WLC 9800 Series por un puerto serie de consola. El administrador usa esta consola para la administración de los Cisco WLC. Los requisitos para la conexión mediante consola a un dispositivo Cisco Wireless LAN Controller son:
  - Velocidad: 9600 baudios
  - Bits de datos: 8
  - Bits de parada: 1
  - Paridad: Sin paridad
  - Control de Flujo: XON / XOFF

4.3 REGISTRO Y LICENCIAS

23. Para que los puntos de acceso se puedan asociar a los controladores inalámbricos de Cisco de la serie 9800, estos requieren de licencias. Para el caso de controladores que ejecuten el sistema operativo IOS-XE, el tipo de licenciamiento es necesariamente del tipo *Smart-licensing*. En este caso, todos los puntos de acceso consumen dos licencias: "*AIR Network License*" y "*AIR DNA License*". Una vez adquiridas por los canales comerciales oportunos, las licencias serán añadidas a la *Smart Account*.

24. Ambos tipos de licencia pueden ser del nivel "*Essential*" o "*Advantage*. Todos los puntos de acceso que se conecten al controlador inalámbrico deben tener el mismo tipo y nivel de licencia. Esto se debe a que el nivel de licencia se configura en el lado del controlador inalámbrico.

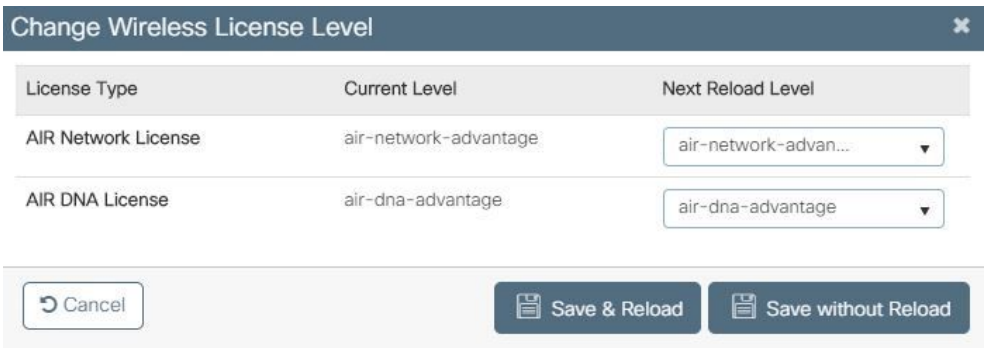


Ilustración 1. Nivel de licencias del controlador inalámbrico

25. De los diferentes modos existentes para el licenciamiento *Smart-licensing* se contemplan (ver [20]):

    - *CSSM (Cisco Smart Software Manager):* Mediante este procedimiento, la unidad requiere de una configuración que le permita realizar consultas DNS y acceder a "*tools.cisco.com*" a través de los protocolos HTTP y HTTPS.
    - *SLR (Specific License Reservation):* En este modo de licenciamiento, si la unidad no tiene acceso al exterior, ésta puede ser licenciada a través de este procedimiento. La reserva de licencias se a través de la *Smart Account*, aunque

es posible que no esté activa esta opción y se requiera de una solicitud a Cisco para activar esta característica.

- On-prem satellite server

26. Se recomienda consultar [19],[20],[21] y [22], para obtener más información sobre el licenciamiento.

4.4 CONSIDERACIONES PREVIAS

27. Como se ha mencionado previamente, el propósito del documento no es ofrecer una guía de configuración completa del equipo, si no ofrecer información sobre la operación segura del equipo en los entornos productivos. Pero sí que se recomienda, como preparación previa al despliegue de la unidad, tener presente una serie de valores operativos para poder luego facilitar/implementar los procedimientos de operación segura. Entre esos elementos relacionados con la seguridad del equipo, se encuentran:

    - Contraseña de administrador, y de usuarios adicionales. Estos valores pueden ser configurados en el asistente inicial de configuración, o con posterioridad accediendo al equipo mediante conexión web/serie/SSH. Los valores de la contraseña deberán cumplir los requisitos expresados en el apartado 6.2.6.3 del presente documento.
    - Activación de protocolos de monitorización/gestión remota, tales como SNMPv3.
    - Disponibilidad de servidor de tiempos (NTP) y zona horaria.
    - Configuración de gestión (IP de gestión con máscara y puerta de enlace, VLAN de gestión en caso de ser necesaria). En todos los dispositivos Cisco Catalyst WLC 9800 Series tipo appliance, es opcional (aunque recomendable) configurar el puerto de servicio, disponiendo así de un puerto físico desde el que alcanzar el interfaz web del equipo. Este puerto debe estar configurado en una subred diferente a la red de gestión, y no permite enrutamiento.

5. FASE DE INSTALACIÓN

5.1 INSTALACIÓN FISICA

28. Consultar las guías "*Cisco Catalyst 9800-L/-40/-80 Wireless Controller Hardware Installation Guide"* o [8][9][10] para la preparación del sitio físico y la instalación del *hardware*.

5.2 CONFIGURACIÓN INICIAL CON ASISTENTE

29. En una unidad Cisco Catalyst WLC 9800 sin configuración previa, es decir, sin ningún fichero de configuración en NVRAM, se inicia un asistente de configuración inicial. Una vez cargado el asistente, presenta un diálogo de configuración donde se van presentando las opciones de configuración más importantes para la operación inicial del dispositivo. Este asistente guía al administrador a través de la configuración inicial preguntándole información básica acerca del dispositivo y de la red, creando finalmente un fichero de configuración que permite a la máquina disponer de una configuración mínima funcional de arranque. Después de que el fichero sea creado, un administrador privilegiado puede utilizar cualquiera de los métodos disponibles de configuración para añadir configuración adicional.

30. En los dispositivos Cisco Catalyst 9800 en su versión 17.6 este asistente puede presentar las siguientes formas:

    - Mediante interfaz de línea de comandos (CLI) a través del puerto serie, utilizando el asistente de configuración por consola (*Autoinstall*).
    - Mediante el interfaz web, que es accesible si el equipo viene configurado por defecto para que obtenga una dirección por DHCP. Este método sólo es recomendable una vez que el dispositivo cuente con los certificados que permitan verificar la autenticidad del mismo.

31. A continuación, se describe el proceso de configuración inicial usando el asistente de configuración mediante CLI. La sección "*Performing Device Setup Configuration*" en [11][12][13] describe cómo usar el configurador para construir una configuración básica y también como modificarla.

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
yes

Configure device management interface?[yes]: yes

Configure static IP address? [yes]: yes

Enter the interface IP [TenGigabitEthernet0/0/2]: 192.168.1.10

Enter the subnet mask [TenGigabitEthernet0/0/2] [255.0.0.0]:
255.255.255.0

Interface belongs to VRF "Mgmt-intf". Please configure a static route
on the VRF

Enter the destination prefix: 0.0.0.0

Enter the destination mask: 0.0.0.0
```

```
Enter the forwarding router IP: 10.104.170.1
Enter the management username: cisco
Enter the password: ********
Reenter the password: ********
Basic management setup is now complete.
Configuring wireless management interface
Select interface to be used for wireless management
   1. TenGigabitEthernet0/0/1 [Up]
   2. TenGigabitEthernet0/0/2 [Up]
   3. TenGigabitEthernet0/0/3 [Up]
Choose the interface to config [1]: 1
Enter the vlan ID (1-4094): 112
Configure IPv4 address? [yes]: yes
Enter the interface IP [TenGigabitEthernet0/0/1]: 9.11.112.40
Enter the subnet mask [TenGigabitEthernet0/0/1] [255.0.0.0]:
255.255.255.0
Configure IPv6 address? [yes]: no
Do you want to configure a VLAN DHCP Server? [yes]: yes
Enter the VLAN DHCP Server IP [TenGigabitEthernet0/0/1]: 9.11.112.45
Configure static route? [yes/no]: yes
  Enter the destination prefix [0.0.0.0]:
  Enter the destination mask [0.0.0.0]:
  Enter the forwarding router IP: 9.11.112.1
Basic management setup is now complete. At this point, it is possible
to save the above and continue Wireless setup using the webUI (for
this, choose 'no' below)
Would you like to continue with the wireless setup? [yes]: yes
Choose the deployment mode
    1. Standalone
    2. Active
    3. Standby
 Enter your selection [1]: 1
Enter the hostname [WLC]: WLC-NAME
Configure credentials for management access on Access Points? [yes]:
yes
  Enter the management username: cisco
  Enter the management password: ****
  Reenter the password: ****
  Enter the privileged mode access password: ****
```

```
  Reenter the password: ****
Configure country code for wireless operation in ISO format ? [US]: ES
Configure a NTP server now? [yes]: yes
Enter ntp server address : 9.11.112.45
Enter a polling interval between 16 and 131072 secs which is power of
2: 16
Configure timezone? [yes]:no
Configure Wireless client density? [yes]: no
Configure AAA servers? [yes]: no
Configure Wireless network settings? [yes]: no
Configure virtual IP? [yes]: yes
  Enter the virtual IP [192.0.6.1]: 192.0.2.1
Configure RF-Network Name? [yes]: yes
  Enter the RF-Network Name: ciscorf
Use this configuration? {yes/no}: yes
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.
<Additional messages omitted.>
WLC-Name>
```

32. Una vez finalizado el proceso, se deben tener en cuenta las siguientes consideraciones:

    - La cuenta creada durante la instalación inicial es considerada como administrador con permisos de lectura/escritura y, por lo tanto, tiene concedido el acceso a todos los comandos del producto.
    - Los tipos de usuarios que existen por defecto en un dispositivo Cisco Wireless LAN Controller son:
    - *Admin*: Permisos absolutos sobre el equipo.
    - *ReadOnly*: Permisos para revisión de configuración (no podrá modificar parámetros).
    - *No Access*: Permisos para acceso por CLI, pero no por interfaz web.
    - *LobbyAdmin*: Es una cuenta de anfitrión, que se emplea para dar de alta usuarios para redes inalámbricas configuradas con usuarios locales.
    - El número de administradores que se creen y sus consiguientes niveles de acceso deben basarse en la política de la organización. No obstante, **se debe atender a los principios del mínimo privilegio.**
    - El término administrador privilegiado se utiliza en este documento para referirse a cualquier administrador autenticado satisfactoriamente y que tiene acceso a los privilegios apropiados para realizar las tareas requeridas.

33. Se recomienda consultar las referencias "*Cisco Wireless Controller Configuration Guide", capítulo "Managing users"* para saber más acerca de los comandos disponibles y roles asociados a los distintos usuarios (ver [14]).

34. Finalmente, se debe confirmar que una vez que el dispositivo ha arrancado, la versión ejecutada es la correcta. Para ello, se puede utilizar el comando "*show version*" y revisar la línea acerca de la versión de imagen empleada. Se muestra a continuación una versión reducida del resultado de este comando ejecutado sobre un dispositivo 9800-CL:

```
WLC-Name> show version

Cisco IOS XE Software, Version 17.6

Cisco IOS Software [Bengaluru], C9800-CL Software (C9800-CL-K9_IOSXE),
Version 17.16.5.a, RELEASE SOFTWARE (fc1)

<<--resto del output omitido-->>
```

6. FASE DE CONFIGURACIÓN

6.1 MODOS DE OPERACIÓN

35. Un dispositivo Cisco WLC tiene varios modos de operación. Hay que tener en cuenta que a algunos modos de operación se accede en el arranque del dispositivo sin proporcionar credenciales de usuario y se pueden hacer modificaciones de seguridad, por lo que habrá que tomar medidas procedimentales y físicas para evitar el acceso no autorizado al dispositivo.

36. Los modos de operación son los siguientes:

- Modo de operación *Booting*: En el arranque, el controlador descarta todo el tráfico de red hasta que su imagen y su configuración han sido cargadas. Este modo de operación se accede en modo consola. Progresa automáticamente hacia el modo de operación Normal. Durante el arranque, un usuario podría interrumpir el modo de arranque en un controlador 9800-CL (Virtual) manipulando el gestor de arranque *grub*, para, por ejemplo, cambiar el configurador de registro en un proceso de recuperación de contraseña, pulsando la tecla "c" mientras el menú de arranque aparece en la consola.

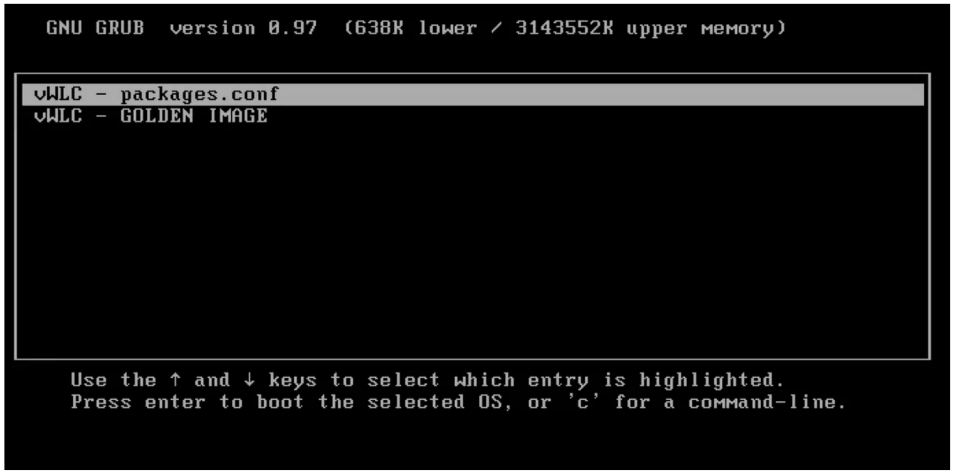


Ilustración 2. Cargador de arranque *grub* en un 9800-CL

Ilustración 3. Manipulación del gestor para entrar modo en *password-recovery*

- Modo de operación ROM Monitor (rommon): En el caso de un controlador tipo *appliance* Catalyst 9800-L, se dispone de este modo de operación en modo consola, que permite realizar tareas de mantenimiento, depuración y recuperación ante fallos. En este estado, la controladora podría ser configurada para cargar una nueva imagen de arranque desde un servidor TFTP determinado, realizar tareas de configuración y lanzar varios comandos de depuración. Este modo de operación no requiere contraseña de administrador para acceder y

únicamente se requiere acceso físico, pulsando *Ctrl+Break* durante el proceso de arranque.

- Modo de operación Normal: Tras pasar la fase de arranque y el *power-on self test*, la imagen de IOS-XE del controlador y su configuración han sido cargadas y el controlador está operando tal y como se ha configurado. Todos los niveles de acceso administrativo suceden en este modo y todas las funciones de seguridad están operativas.

6.2 ADMINISTRACIÓN DEL PRODUCTO

37. Una vez configurado de manera local, el equipo deberá contar con un entorno de operación y configuración remota seguro, donde se contemplen los siguientes aspectos, principalmente relacionados con las funciones criptográficas y protocolos de comunicación con los que va a operar el equipo:
38. Se deben utilizar protocolos remotos de configuración seguros:
    - HTTPS con TLS V1.2.
    - SSHv2.
    - No usar SNMP en versiones inseguras, **usar SNMPv3.**
39. Se recomienda que la gestión remota de usuarios se realice mediante servidores de AAA centralizados, para poder gestionarlos de manera más eficiente, y para poder mejorar su seguridad al estar en un único repositorio.
40. Esta guía se centra en la configuración mediante el interfaz web (HTTPS), aunque en la mayor parte de los casos existe una configuración equivalente a la expuesta mediante el uso de la línea de comandos (CLI). Usando cualquiera de ambas opciones, es posible configurar todos los aspectos de seguridad del dispositivo.
41. En entornos de gestión donde las dimensiones de integridad [I], confidencialidad [C] y autenticidad [A] requieran un perfil alto, según se recomienda en la Guía CCN-STIC-816, **es necesario que la gestión de la infraestructura inalámbrica se realice mediante protocolos de gestión seguros, como puede ser SSH, SSL/TLS o SNMPv3.**
42. Estas recomendaciones de seguridad, y muchas más relacionadas con las buenas prácticas de uso del Controlador WLC se recogen en la sección "*Security*" del documento *"Cisco Catalyst 9800 Series Configuration Best Practices"* (ver [15]).

6.2.1 ADMINISTRACIÓN DEL EQUIPO MEDIANTE INTERFAZ SSH

43. La línea de comandos puede ser accesible por dos (2) modos:
    - Modo local, a través del puerto de consola (excepto en el caso del controlador virtual).
    - Modo remoto mediante protocolos de gestión remota seguros, tales como SSHv2.
44. En el interfaz de configuración mediante comandos (CLI) de un controlador Cisco Catalyst 9800 WLC, existen diferentes contextos de gestión, donde cada uno se identifica al gestor por el *prompt* y la familia de comandos disponibles. La importancia de esta información radica en que los comandos tienen su propia jerarquía y solo se pueden ejecutar bajo los

contextos apropiados, como por ejemplo puede ocurrir si se está en el *prompt* de usuario (>), usuario privilegiado (#), configuración global ((config)#) o configuración de un interfaz ((config-if)#).

45. Por defecto, el protocolo SSH debería encontrarse habilitado, por lo que debe ser posible establecer una sesión SSH con el controlador usando el usuario administrador generado en el asistente de configuración inicial (apartado **5.2** de la presente guía).

46. Para comprobar el estado de los accesos remotos mediante CLI, se utiliza el siguiente comando:

```
WLC-9800# show ip ssh
SSH Enabled - version 2.0
<<--output omitido-->>
```

47. Para habilitar SSH, en caso de que se hubiera deshabilitado en alguna situación, se debe emplear el siguiente comando:

```
WLC-9800# ip ssh version 2
```

6.2.2 ADMINISTRACIÓN DEL EQUIPO MEDIANTE EL INTERFAZ WEB

48. Para realizar gestiones de forma segura a través del interfaz web del dispositivo, **se debe emplear el protocolo HTTPS (en lugar de HTTP)**.

49. También se recomienda que la unidad esté identificada por un certificado de dispositivo X.509v3 que sea confiable para la organización, de modo que en el acceso vía HTTPS no se produzca un error de certificado, y se tenga la seguridad de que se está accediendo a un dispositivo confiable. La carga de este tipo de certificados se ha contemplado en el apartado **6.2.2** de la presente guía.

50. El primer paso, que sería activar el protocolo HTTPS, se realizaría a través del menú vertical "Administration-->*Management*-->*HTTP/HTTPS/Netconf*".

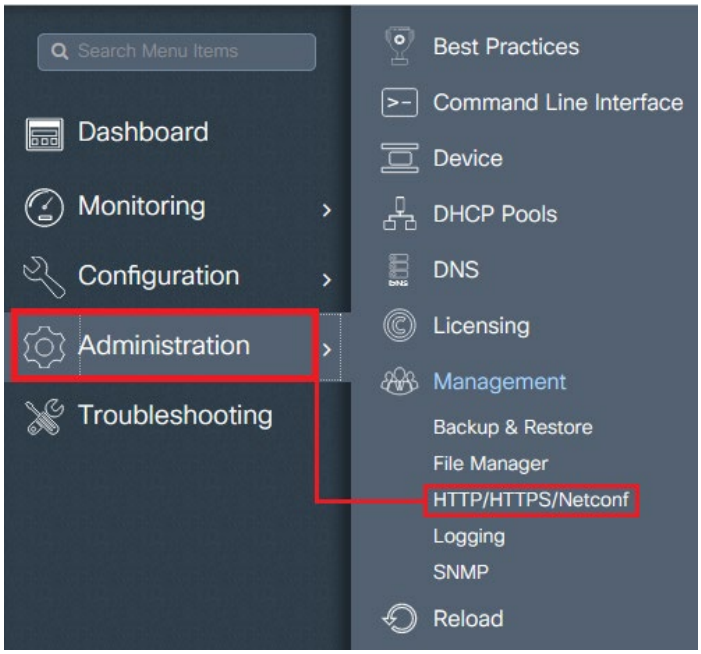


Ilustración 4. Acceso al menú HTTP/HTTPS/Neconf

51. En el menú en pantalla principal que ofrece esta sección, se pueden habilitar/deshabilitar distintas opciones, entre las que se encuentran las deseadas de HTTP/HTTPS. Se muestra a continuación el estado final deseable para operar con seguridad sobre el interfaz web del dispositivo. Hay que prestar especial atención a seleccionar el '*trustpoint*' adecuado para que aplique correctamente sobre el interfaz web de administración del dispositivo.

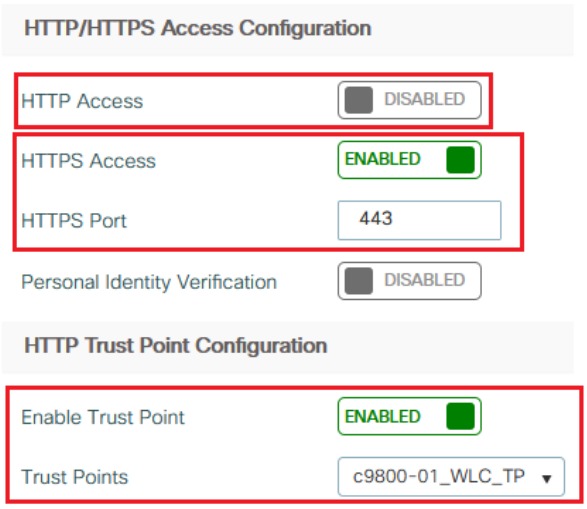


Ilustración 5. Activación de HTTPS

52. Por último, y como precaución ya que viene por defecto habilitado SSH, **se debe comprobar que Telnet está deshabilitado**. Para ello, se puede navegar sobre el menú vertical en "*Administration-->Device*".

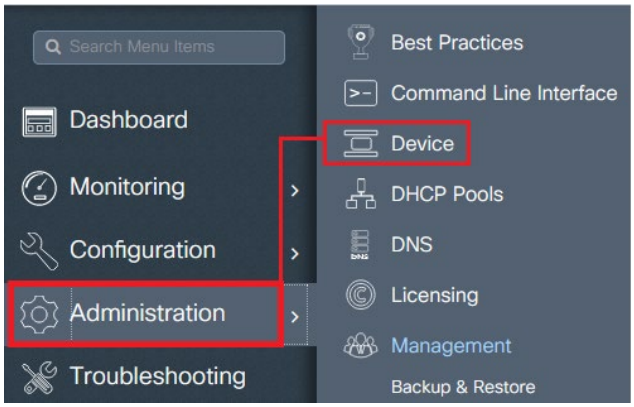


Ilustración 6. Acceso al menú Device

53. En la pantalla principal, pulsar sobre la pestaña general, y comprobar las opciones actuales de las líneas virtuales pulsando sobre "*View VTY options*".

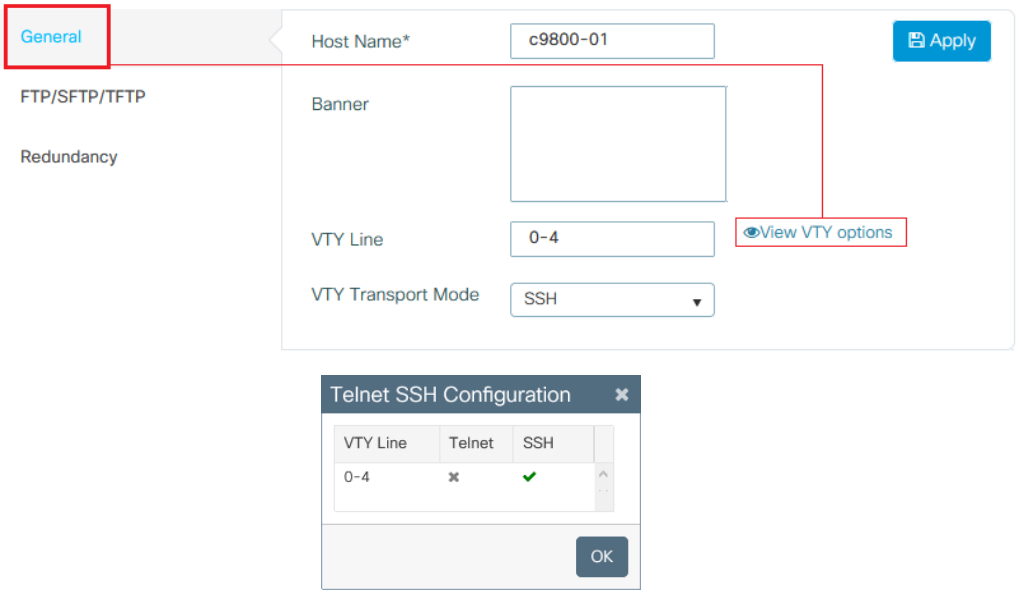


Ilustración 7. Estado actual de protocolos Telnet y SSH

54. **En caso de que Telnet se encuentre habilitado, se debe deshabilitar**. Para ello, se debe seleccionar las líneas virtuales correspondientes y el modo SSH. Una vez finalizada la configuración, se debe pulsar sobre el botón "*Apply*" que se encuentra en la esquina superior derecha.

Ilustración 8. Estado actual de protocolos Telnet y SSH

55. Para realizar esta operación mediante la línea de comandos, se deben realizar los siguientes pasos:

- Deshabilitar el acceso mediante Telnet:

```
WLC-9800 # configure terminal
WLC-9800 (config) # line vty 0 4
WLC-9800 (config) # transport input ssh
```

- Deshabilitar el acceso mediante HTTP:

```
WLC-9800 (config) # no ip http server
```

- Habilitar el acceso mediante HTTPS:

```
WLC-9800 (config) # ip http secure-server
WLC-9800 (config) # ip http secure-port [numero_puerto] (por defecto
443)
WLC-9800 (config) # ip http secure-truspoint [nombre_trustpoint]
```

- Se debe incrementar la seguridad, a través del uso de **TLSv1.2 y de esquemas de cifrado adecuados.**

```
(Cisco Controller) >
WLC-9800 (config) # ip http tls-version [TLSv1.2]
WLC-9800 (config) # ip http secure-ciphersuite {ecdhe-ecdsa-aes-gcm-
sha2 | ecdhe-rsa-aes-gcm-sha2}
```

- Reiniciar el servicio web y salvar la configuración:

```
WLC-9800# configure terminal
WLC-9800 (config) # no ip http server
WLC-9800 (config) # ip http server
WLC-9800 (config) # end
WLC-9800 # write memory
Building configuration…
[OK]
```

56. Ya en el apartado **6.3 GESTIÓN DE CERTIFICADOS** de la presente guía se instaló el certificado de administración web para que, al acceder por HTTPS desde una estación que esté dentro de la infraestructura de PKI de la organización no ofrezca error de certificado.

57. Para comprobar la validez del certificado, basta con introducir el siguiente comando, donde se puede especificar el nombre concreto del certificado u omitirlo para que muestre todos los que están incorporados en el dispositivo.

```
WLC-9800# show crypto pki certificates nombre_certificado
```

6.2.3 ADMINISTRACIÓN DEL EQUIPO MEDIANTE SNMP

58. **El protocolo SNMP debe estar desactivado en sus versiones no seguras (SNMPv1 y SNMPv2c)**. Para ello, basta con no configurar ninguna *community*, en el menú *"Administration → SNMP"*.

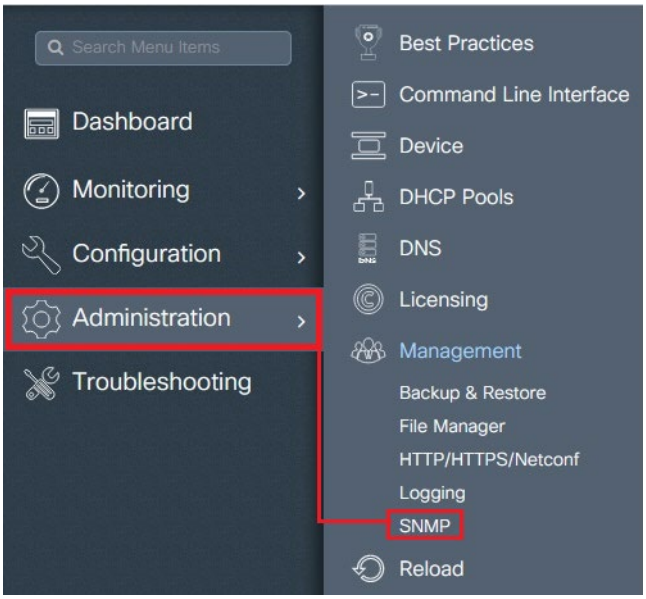


Ilustración 9. Acceso al menú SNMP

59. Una vez allí, pulsar sobre la pestaña "*Community Strings*", y el aspecto debe ser el mostrado en la imagen bajo estas líneas. De no ser así, deberá seleccionar cada una de las *Community* que aparezcan y eliminarlas, pulsando sobre el botón "*Delete*".

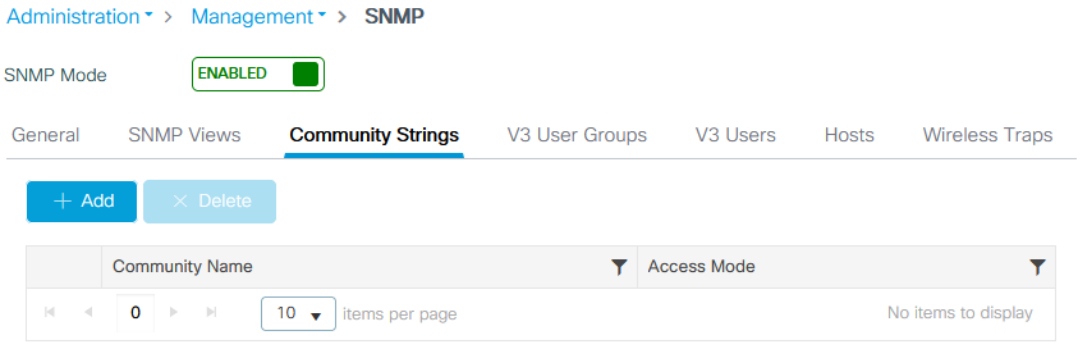


Ilustración 10. Configuración de *Community Strings*

60. En la ventana principal se debe comprobar que el protocolo de gestión está habilitado (botón superior "*SNMP Mode*") y que no existen "*Community Strings*" en la pestaña del mismo nombre. Las "*Community Strings*" son valores alfanuméricos que, en los protocolos menos seguros, v1 y v2c, se usan para proporcionar relaciones de confianza entre agentes externos SNMP y el propio dispositivo. Para que un mensaje SNMP se procese correctamente es necesario que los valores de *Community* entre agente SNMP y dispositivo SNMP coincidan. Al no ser tan seguros como SNMP v3 se recomienda que no existan valores de "*Community Strings*" configurados.

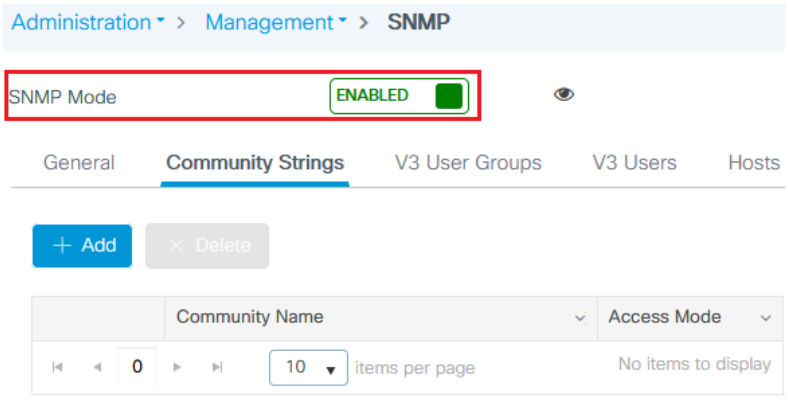


Ilustración 11. Habilitar SNMP y comprobación de *Community*

61. Para configurar el dispositivo mediante SNMPv3, en primer lugar, debe existir algún grupo y usuario. Para ello, sobre la misma ventana principal anterior, configurar el grupo en la pestaña "*V3 User Groups*". Se deberá visualizar los grupos existentes, para añadir uno nuevo, pulsar sobre el botón *"+Add*".

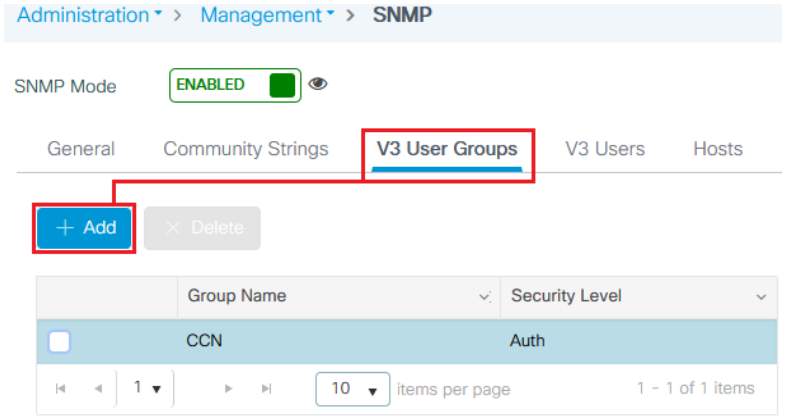


Ilustración 12. Grupos usuarios SNMP v3

62. Aparecerá un nuevo cuadro de diálogo solicitado los distintos parámetros de configuración para el grupo, que son:

- *Group Name*: Nombre del grupo de usuarios
- Security Level: Donde se podrá seleccionar,
  - *Auth*: Grupo con autenticación
  - *no Auth*: Grupo sin autenticación
  - *Priv*: Grupo con protocolo de privacidad

63. De estos tres tipos, sólo uno puede escogerse, si se especifica por CLI primero Auth y luego Priv, se crea un nuevo grupo. Se recomienda por tanto el uso de éste último tipo dado que dispone de más opciones disponibles en su nivel de seguridad:

```
WLC-9800(config)#snmp-server group SNMP-GRP v3 priv ?
  access   specify an access-list associated with this group
  context  specify a context to associate these views for the
group
  match    context name match criteria
  notify   specify a notify view for the group
```

```
  read      specify a read view for the group
  write     specify a write view for the group
  <cr>

WLC-9800 (config) #snmp-server group SNMP-GRP v3 priv
configure terminal
```

- *Read View*: Parámetro que permite consultar OIDs o sub-árboles de la MIB.
- Write View: Parámetro que permite escribir OIDs o sub-árboles de la MIB.

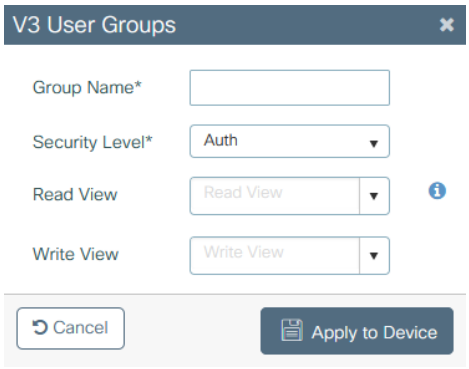


Ilustración 13. Campos para crear un grupo SNMP v3

64. Seguidamente, será necesario añadir un usuario. Navegar a la pestaña "*V3 Users*", donde aparecerá el listado de usuarios ya creados, para crear uno nuevo pulsar sobre el botón *"+Add"*.

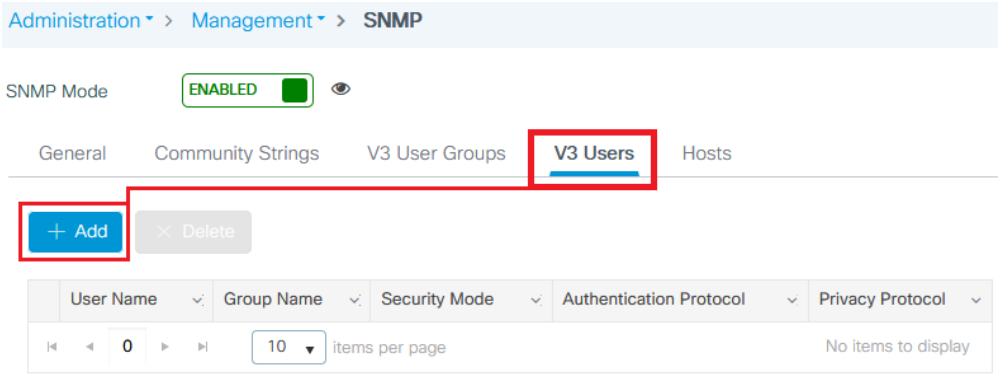


Ilustración 14. Definición de nuevo usuario SNMPv3

65. Tras ese paso, se nos ofrecerá una pantalla para introducir los datos deseados del nuevo usuario. Los datos solicitados son:

- *User Name:* Nombre de usuario.
- *Group Name:* Es el grupo de usuarios al que pertenecerá, puede ser creado en el mismo instante pulsando sobre el botón "+" que aparece a la derecha, aunque lo recomendable es que esté creado de forma previa.
- *Security Mode:* Es el esquema de seguridad que cumplirá el usuario, las opciones son:
- *AuthPriv*: Seguirá un esquema de seguridad con autenticación y protocolo de seguridad.

- *AuthNoPriv*: Seguirá un esquema de seguridad con autenticación, pero sin protocolo de privacidad
- *NoAuthNoPriv*: Seguirá un esquema sin autenticación ni protocolo de privacidad.

66. En este caso, el valor recomendado es el de AuthPriv, dado que dota al usuario de un mayor nivel de seguridad, con autenticación y protocolo de seguridad. Se recomienda el uso de valores en negrita para el cumplimiento de los parámetros de seguridad óptimos.

```
WLC-9800(config)#snmp-server user <name> <group>  v3 encrypted
auth {md5 | sha} <AUTH_PASSWORD> priv aes [128-192-256]
<PRIVACY_PASSWORD>
```

- *Authentication Protocol:* Es el protocolo de seguridad, que las opciones posibles son "MD5" y "SHA". Se debe seleccionar SHA.
- *Authentication Password:* Clave de autenticación, debe ser una cadena alfanumérica de al menos 12 dígitos.
- *Privacy Protocol:* Es el protocolo de cifrado que se empleará. En este caso las opciones posibles son "DES | 3DES | AES-128 | AES-192 | AES-256". **Se debe configurar AES-192 y AES-256.**
- *Privacy Password:* Clave de privacidad, deber ser una cadena alfanumérica de al menos 12 dígitos.

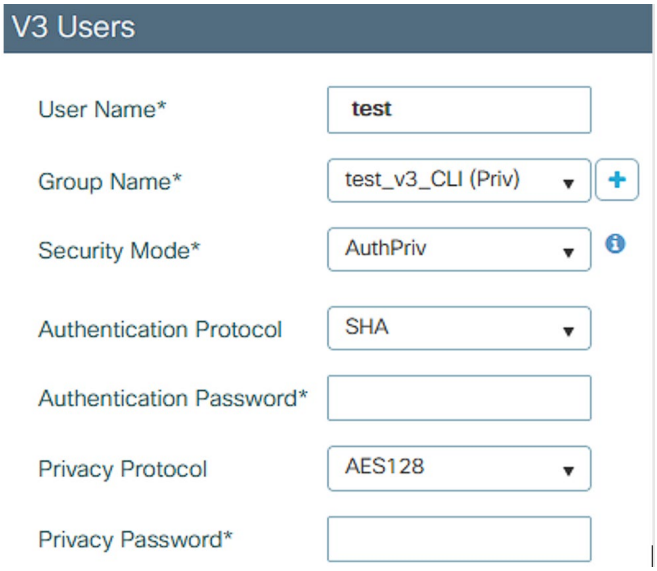


Ilustración 15. Configuración de nuevo usuario SNMPv3

67. Como en el resto de configuraciones, existe una forma alternativa para realizarlo mediante la consola de comandos, que sería la siguiente:

```
WLC-9800 (config) # snmp-server group Nombre_Grupo v3 {auth | noauth |
priv} {read | write} Nombre_vista

WLC-9800 (config) # snmp-server user Nombre_Usuario Nombre_Grupo v3
auth {md5 | sha} Clave_Autenticación priv {3des | aes | des}
Clave_cifrado
```

68. El último elemento importante a tener en cuenta en la configuración de SNMP son los llamados "*Trap-receivers*" que no son más que los equipos destinados a decodificar las *traps* y representar la información de forma visual a los usuarios de administración (del sistema de SNMP, no confundirlo con los del propio controlador inalámbrico). Estos *"Trap-Receivers"* son llamados simplemente "*Hosts*" en la serie 9800 de controladores inalámbricos.

69. Para configurar los servidores que recibirán las *traps*, hay que navegar en este caso a la pestaña "*Hosts*". En la ventana principal aparecerá la información de los servidores ya configurados, y para crear uno nuevo bastará con pulsar sobre el botón "*+Add*".

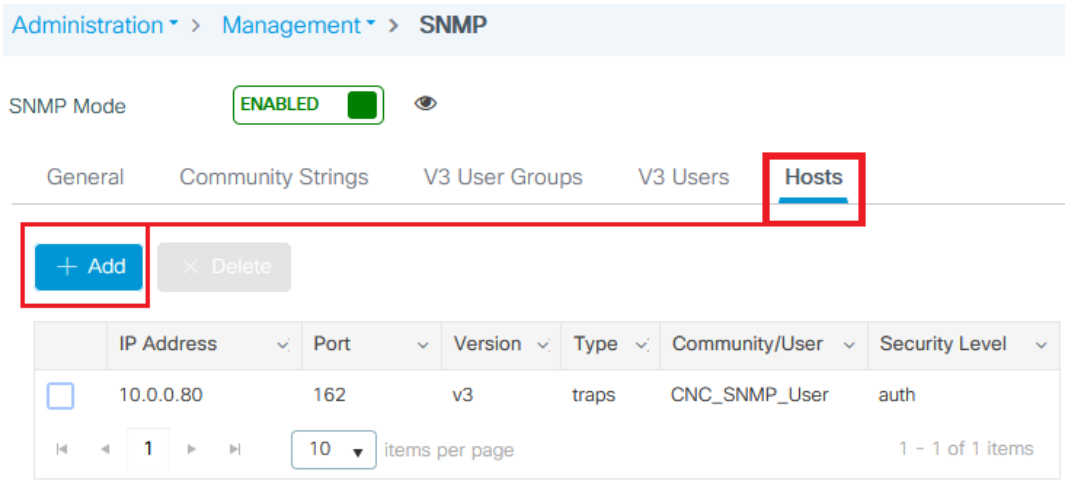


Ilustración 16. Gestión de receptores de traps (*traps-receivers*) SNMP

70. Una vez pulsado dicho botón, en la ventana principal aparecerán los diferentes campos a configurar, que son los siguientes:

- *IPv4/IPv6 Address*: Dirección IP (versión 4 o 6) del sistema receptor de traps.
- *Version*: Versión del protocolo SNMP con opciones "*V1 | V2C | V3*". Indicar V3.
- V3 Users: Usuario que reportará o contestará peticiones del servidor SNMP.
- Port: Puerto de comunicaciones UDP en el que el servidor SNMP espera las traps. Usualmente, y por defecto, el puerto 162.
- *Type*: Tipo de *traps* que se enviarán al servidor SNMP. Las opciones son *"Traps | Informs"*
- *Security Level*: Es el esquema de seguridad que se seguirá en la comunicación al enviar las traps. En este caso, las opciones son "*auth | noauth | priv*". La configuración dependerá del nivel de seguridad que se haya configurado en el servidor SNMPv3 receptor de las traps, recomendándose "auth" si se ha habilitado algún nivel de protocolo de autenticación (MD5/SHA) o "priv" si se ha habilitado algún protocolo de privacidad (DES/AES).

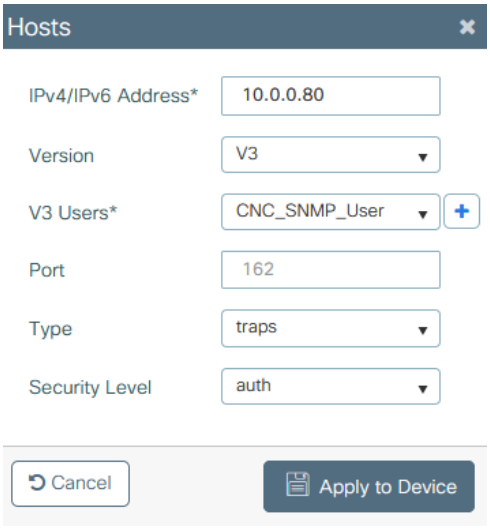


Ilustración 17. Configuración de un receptor de traps SNMP

```
WLC-9800(config)#snmp-server host <Dirección_IP> {informs | traps} version
3 priv <nombre de usuario>
```

71. Por último, aplicar la configuración nueva (o los cambios) pulsando sobre el botón "*Apply to Device*" de la esquina inferior derecha.

72. Para la configuración de los *trap-receivers*, se puede emplear el siguiente conjunto de comandos especificando como parámetros el nombre y la dirección IP:

```
WLC-9800 (config) # snmp-server host Dirección_IP {informs | traps}
version 3 {auth | noauth | priv} Nombre_usuario
```

6.2.4 CONFIGURACIÓN DEL MENSAJE DE AVISO EN EL INICIO DE SESIÓN

73. El producto proporciona la posibilidad de configurar mensajes de aviso/banner, que se muestran en la interfaz de administración CLI y GUI antes de permitir cualquier acceso administrativo al dispositivo.

74. Para crear el *banner* previo al *login*, se puede realizar desde el interfaz web, desde el menú vertical "*Administration-->Device*".

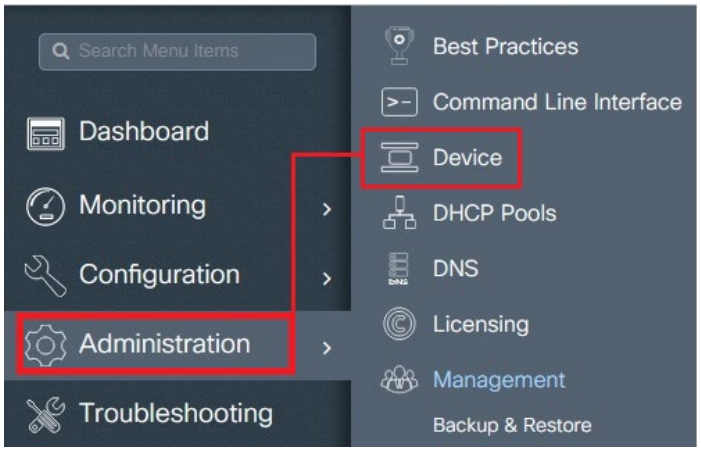


Ilustración 18. Acceso al menú Device

75. En la pantalla principal, en la sección "*General*" se podrá visualizar un cuadro de diálogo nombrado como "*Banner*". En ese espacio se podrá incluir el *Banner* previo al *login* en el dispositivo, y se debe pulsar sobre el botón "*Apply*" de la parte superior derecha para que tenga efecto.

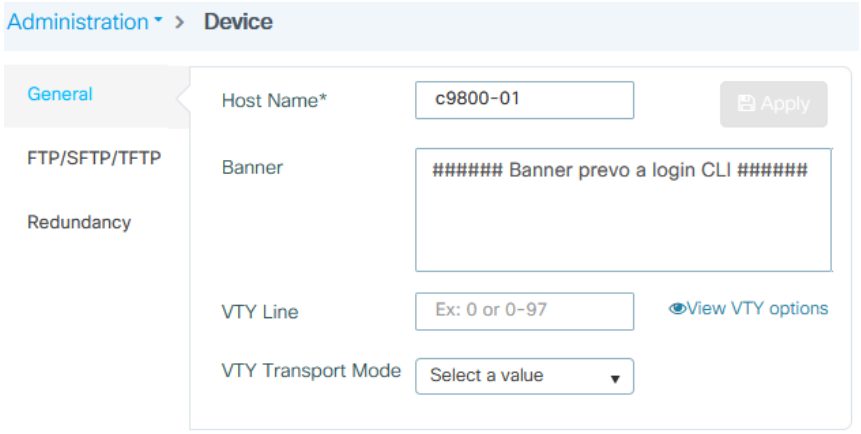


Ilustración 19. Configuración del banner de inicio de sesión

76. A continuación, se muestra el resultado tanto en el interfaz web como en el interfaz de consola.

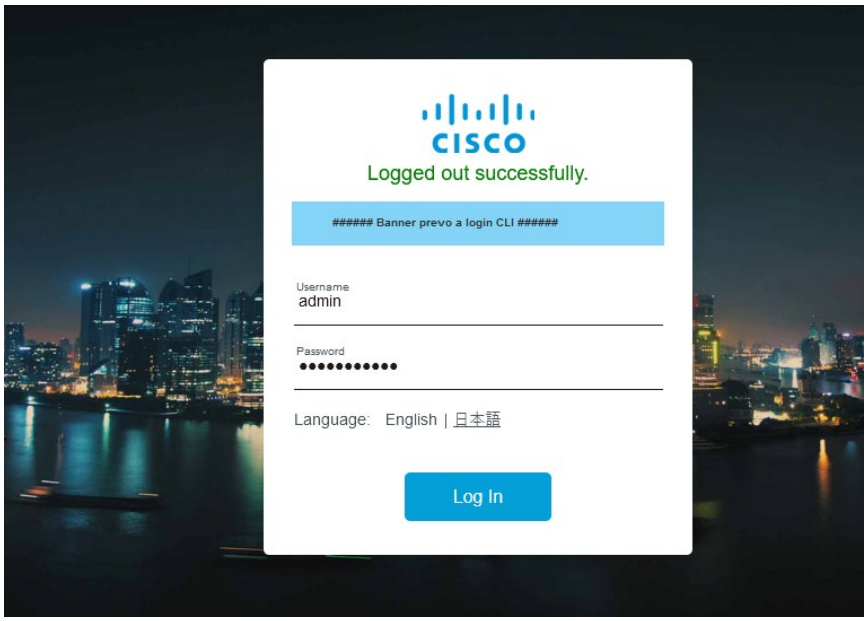


Ilustración 20. Efecto del banner de inicio de sesión por interfaz web

```
login as: ******
Pre-authentication banner message from server:
###### Banner prevo a login CLI ######
End of banner message from server
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
```

Ilustración 21. Efecto del banner de inicio de sesión por CLI

77. Este *banner* se puede configurar a través del interfaz de consola mediante el comando que se muestra a continuación. El carácter 'c' se emplea como carácter delimitador del banner (ver [18]).

```
WLC-9800 (config) # banner login c Texto de banner c
```

78. Existen otros tipos de *banner*, pero que únicamente se pueden configurar por consola. Se indica a continuación los comandos de cada uno y su utilidad:

```
WLC-9800 (config) # banner config-save c Texto de banner configuración salvada c

WLC-9800 (config) # banner exec c Texto de banner c

WLC-9800 (config) # banner motd c Texto de banner diario, aparece tras login c

WLC-9800 (config) # banner prompt-timeout c Texto de banner login timeout c
```

6.2.5 FINALIZACIÓN DE LA SESIÓN

79. El dispositivo permite al administrador privilegiado configurar el tiempo máximo de inactividad de una sesión. Después de que pase el tiempo configurado, la sesión se bloquea y la pantalla en ocasiones se queda sobre el último menú visitado, pero al intentar operar sobre él solicitará las credenciales. No se permite realizar ninguna otra actividad hasta que el administrador vuelva a autenticarse.

80. El comando que se utiliza para configurar el tiempo de inactividad de sesión SSH es el siguiente (expresado el tiempo en minutos, el valor 0 indica una sesión permanente):

```
WLC-9800 (config) # line vty 0 4

WLC-9800 (config-line) # transport input ssh

WLC-9800 (config-line) # session-timeout [0-35791]
```

81. **El tiempo de inactividad de las sesiones no debe ser superior a 5 minutos.**

82. De igual manera se puede configurar el término de sesión para la conexión serie, es decir, por el puerto de consola. Para ello se emplea este comando (nuevamente, el valor 0 indica una sesión permanente, y el tiempo está expresado en minutos):

```
WLC-9800 (config) # line console 0

WLC-9800 (config-line) # session-timeout [0-35791]
```

83. Para que la configuración realizada tenga efecto, la sesión de consola actual debe ser cerrada. Cuando el usuario inicie sesión otra vez se le aplicará el nuevo *timeout* configurado.

84. Un administrador también puede cerrar la sesión manualmente mediante el comando: *logout*.

6.2.6 GESTIÓN LOCAL DE USUARIOS Y SESIONES

85. La autenticación de usuarios en las controladoras puede ser local o remota. En el primer caso, los usuarios y sus credenciales de acceso se definen localmente en cada controlador;

en el segundo, la autenticación se realiza en servidores de autenticación externos de tipo RADIUS o TACACS. Aunque, desde el punto de vista de la seguridad es mejor autenticación externa, se comenzará con la autenticación y gestión local de usuarios, porque es el punto inicial de toda configuración, y en muchas organizaciones no se dispone de dichos servidores de autenticación remotos.

86. Por defecto, y con el objeto de facilitar su puesta en marcha inicial, la configuración de fábrica de los conmutadores no incluye ninguna autenticación activa: cualquier persona con acceso físico a la consola puede acceder a la autenticación local del sistema.

6.2.6.1 CONFIGURACIÓN LOCAL DE USUARIOS

87. Los dispositivos Catalyst 9800 requieren de cuentas de usuarios para poder administrarlos, y permite utilizar un nombre de usuario y contraseña por cada administrador. Las contraseñas se pueden almacenar en texto plano o de forma cifrada. Esta última opción es la recomendada (opción por defecto). Las claves cifradas se almacenan en el fichero de configuración. En caso de que no estuviera habilitado, y se quisiera habilitar manualmente, se realizaría mediante el siguiente comando:

```
WLC-9800 (config) # service password-encryption
```

88. Cuando está habilitado el cifrado de claves, todas las claves que están en texto plano se cifran usando la clave de cifrado que viene insertada en los equipos de fábrica. Esto es conocido en equipos Cisco como cifrado de tipo 7.

89. Si se deshabilita el cifrado de claves, estas se pasan a texto plano descifrándolas empleando la misma clave que tiene configurada de fábrica. Esto es conocido en equipos Cisco como cifrado tipo 0.

90. Una conclusión evidente, es que este tipo de cifrado es débil, ya que es reversible. Sin embargo, una vez habilitada la opción de cifrado de claves, se puede incrementar la robustez de encriptación añadiendo una clave de encriptación, que se empleará junto con la clave por defecto que tiene el dispositivo para cifrar las claves. Esto es conocido en equipos Cisco como cifrado tipo 6. El valor de la clave configurable se puede modificar periódicamente para dificultar que exista una posible revelación de datos. La longitud de esta clave debe estar entre 16 y 127 caracteres alfanuméricos, se recomienda usar al menos tres de las cuatro categorías {Mayúsculas, Minúsculas, Dígitos, Caracteres especiales}, y a su vez es cifrada con la clave privada del certificado del dispositivo.

91. El cifrado de tipo 6 está deshabilitado por defecto por lo que **debe específicamente ser habilitado**. Para ello, se deben que ejecutar los siguientes comandos (ver [15]):

    - Definir una clave de cifrado:

    ```
    WLC-9800 (config) # passwd key obfuscate ascii clave
    ```

    - Habilitar la encriptación mediante claves definidas de forma manual:

    ```
    WLC-9800 (config) # passwd key obfuscate
    ```

6.2.6.2 ROLES DE USUARIO

92. Los dispositivos Cisco WLC consideran los siguientes roles de usuario:

- Rol de administrador (usuario tipo *Admin*): El usuario con este perfil tiene acceso completo al equipo, incluyendo comandos avanzados por terminal de consola o SSH. Puede crear/editar/eliminar configuración sin restricciones.
- Rol de supervisor (usuario tipo *Read-Only*): El usuario con este perfil tiene acceso limitado al dispositivo, reduciendo sus posibilidades a simplemente una supervisión del equipo y configuración realizada sobre el mismo. No podrá crear/editar/eliminar configuración de ningún tipo.
- Rol de acceso a consola (usuario tipo *No-Access*): El usuario con este perfil tiene acceso al interfaz de comandos, pero no podrán acceder al interfaz web.
- Rol de embajador (usuario tipo *LobbyAdmin*): El usuario con este perfil tiene acceso limitado al dispositivo, de tal forma que ni siquiera se le muestra la configuración o los menús usuales que pueden visualizar los usuarios de tipo *Read-Write* o *Read-Onl*y. Este tipo de usuario está destinado para dar de alta usuarios locales que se autentican contra alguna red inalámbrica configurada previamente por un usuario administrador.

6.2.6.3 CONFIGURACIÓN LOCAL DE LA POLÍTICA DE CONTRASEÑAS

93. Las políticas de contraseñas tienen como objetivo hacer cumplir una serie de reglas para asegurar unas credenciales seguras cuando se crean nuevos usuarios de gestión para el dispositivo WLC.
94. Se debe tener en cuenta que, si el controlador inalámbrico es actualizado desde una versión antigua a una más reciente y se habilita la política de contraseña segura, las claves se mantendrán tal cual incluso en el caso de que sean débiles. Todas las claves previas no se comprobarán ni se alterarán en ningún caso.
95. De forma general, las claves de usuario siguen estos criterios mínimos:
    - Longitud mínima de 6 caracteres.
    - La clave debe incluir al menos un carácter numérico.
    - La clave debe incluir al menos un carácter alfabético.
96. Las políticas de contraseñas se configuran bajo el menú "*Configuration->Security->AAA".*

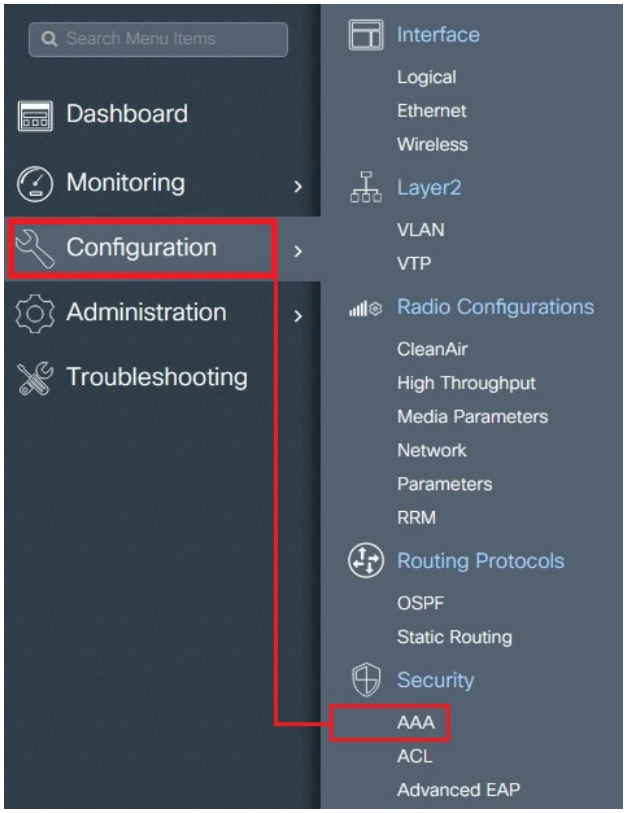


Ilustración 22. Acceso al menú AAA

97. En el menú que aparece en la ventana principal, se debe dirigir a la pestaña *"AAA Advanced"* y seleccionar la opción "*Password Policies*". Aparecerán los distintos perfiles de políticas de claves creados, si existen. Para crear una nueva política de claves basta con pulsar sobre el botón *"+ Add"*.

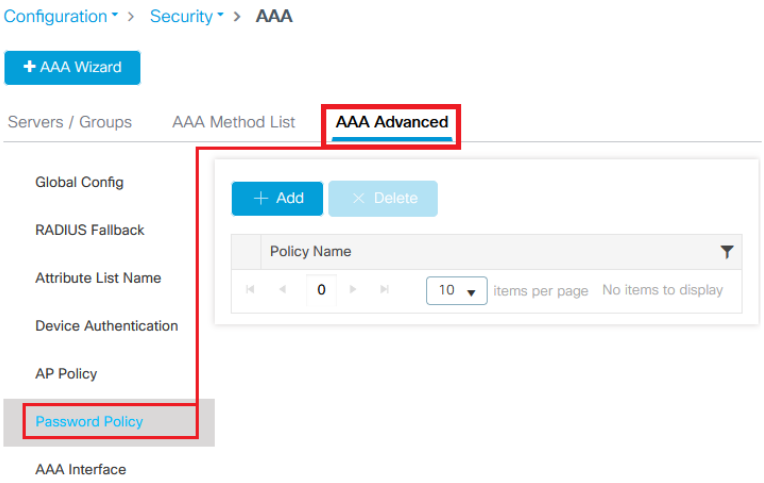


Ilustración 23. Gestión de políticas de contraseñas

98. Aparecerá entonces un cuadro de diálogo solicitando los siguientes datos:

    - *Policy Name*: Será el nombre que tendrá la política de claves.
    - *Minimum/Maximum Length*: Indica la longitud mínima y máxima de las claves. **La longitud mínima debe ser 12 caracteres**.

- *Upper/Lower Count*: Indica el número de veces que debe aparecer un carácter alfabético en mayúsculas/minúsculas. **Debe requerirse, al menos, una mayúscula y una minúscula.**
- *Numeric Count*: Indica el número de veces que debe aparecer un carácter numérico. **Debe requerirse, al menos, uno.**
- *Special Count*: Indica el número de veces que debe aparecer un carácter especial. **Debe requerirse, al menos, uno.**
- *Character changes*: Número de caracteres mínimos que deben variar entre una clave actual y la nueva. Se recomienda, al menos, tres caracteres mínimos.
- *Validity*: Indica si la clave es permanente o durante cuánto tiempo es válida (expresado en años, meses, días, horas, minutos y segundos). **La validez de la contraseña no debe ser superior a 60 días.**

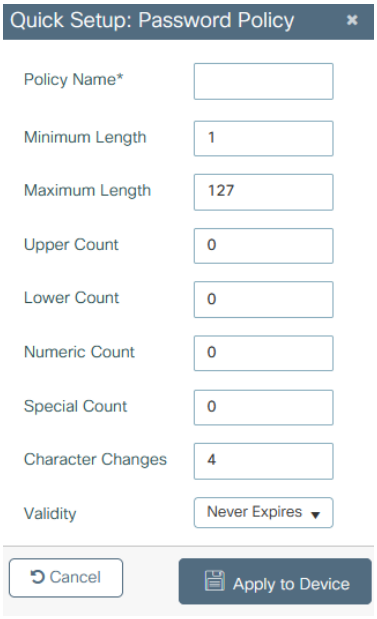


Ilustración 24. Configuración del perfil de política de contraseña

99. Para poder limitar el número de intentos de autenticación fallidos para el bloqueo de un usuario local, el comando a introducir en el controlador sería el siguiente:

```
WLC-9800 (config) # aaa local authentication attempts max-fail 3
```

6.3 GESTIÓN DE CERTIFICADOS

100. Se recomienda configurar el dispositivo para utilizar certificados X.509v3 para varios modos de funcionamiento, incluyendo autenticación segura del equipo en HTTPS, o durante la autenticación de pares entre dispositivos críticos, tales como servidores de *syslog*, servidores SNMP o servidores de AAA mediante IPsec.
101. La creación de estos certificados y su carga en el dispositivo está detallada en [16]. Los aspectos más destacados de la configuración del dispositivo, para el uso de estos certificados, se explica en las subsecciones siguientes.
102. Antes de continuar, merece mención que, en los Cisco Catalyst 9800 Series Wireless Controller, una CA de confianza se denomina '*trustpoint*'. Una vez que se ha confiado

(creado un '*trustpoint*') el sistema de claves confiará en cualquier certificado firmado por esa CA de confianza ('*trustpoint*'). Por ejemplo, en estos dispositivos se suele emplear para estas funciones y protocolos:

- DTLS, SSH, SSL
- HTTPS (Interfaz Web)
- Redirección para *WebAuth*
- Túneles de información de movilidad

103. Todos los certificados se solicitan, generan e instalan de la misma manera. Se recomienda el interfaz CLI para la instalación del primer certificado (el que protege la sesión HTTPS), para que las subsiguientes conexiones de configuración mediante el interfaz GUI se hagan sobre una unidad que tenga un certificado HTTPS confiable.

104. Por tanto, como ejemplo de instalación de certificado se ofrece a continuación el proceso a seguir para un certificado de tipo *webadmin*. Este certificado se encargaría de identificar a la unidad de manera correcta frente accesos HTTPS.

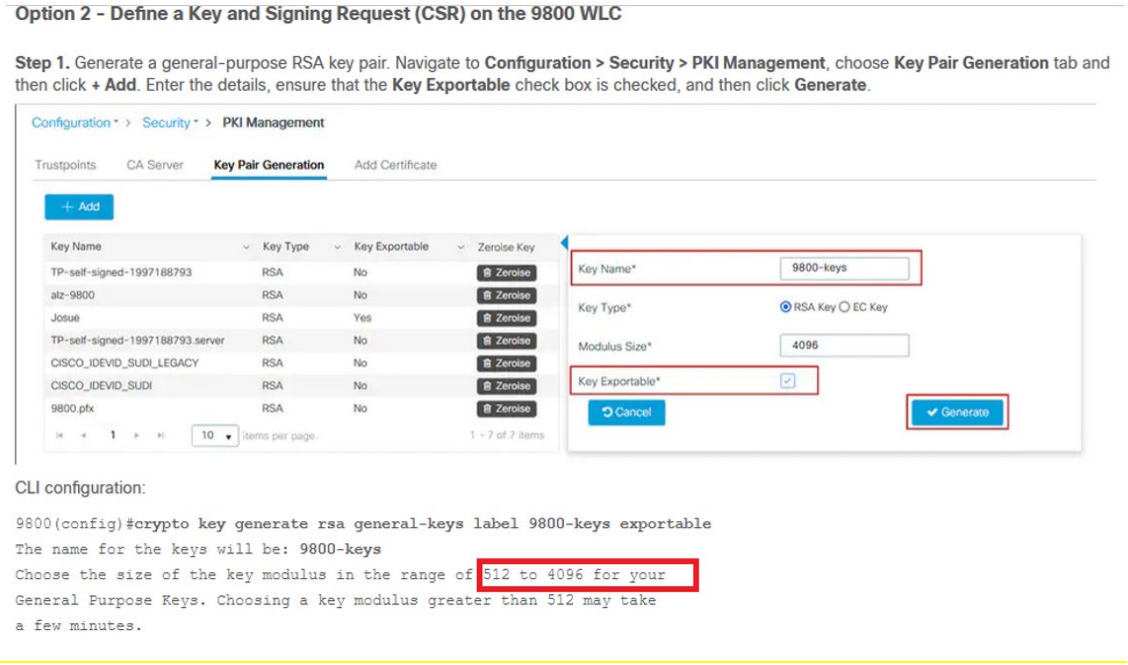
6.3.1 CREACIÓN DE LA SOLICITUD DE CERTIFICADO (CSR)

105. Para generar la solicitud de certificado hay dos (2) vertientes: emplear OpenSSL o usar el propio dispositivo. En el ámbito de esta guía, se explicará únicamente el proceso de obtención empleando directamente el dispositivo.

106. **Generar la solicitud de certificado (CSR) mediante el dispositivo es la opción más segura**, ya que la clave privada es generada internamente en el mismo y nunca sale de él, por lo que no hay exposición de la misma.

107. Emplear el dispositivo para crear la CSR tiene como inconveniente que no se puede configurar el campo SAN, que podría incurrir en errores en ciertos navegadores que requieran del mismo (ver [17]). De todas formas, la mayoría de CA permiten incluir este atributo en el momento de la firma, aunque la recomendación es informarse de antemano.

108. Cuando se genera la petición CSR se emplea una clave con una longitud de hasta 4096 bits, valor recomendable para tener una adecuada fortaleza en la clave, y una cipher suite basado en ECDSA con un tamaño de 256 bits.



109. Una vez se haya generado la solicitud de certificado (CSR), se debe instalar el certificado final. De no ser así, si se reinicia el dispositivo, no se podrá gestionar el equipo por interfaz web mediante HTTPS. Esto se debe a que contendrá un CSR que no se corresponde con el certificado instalado en ese momento.

110. Para generar la solicitud de certificado CSR, hay que ejecutar en primer lugar un comando para obtener el par de claves pública-privada. Este comando se ejecuta en modo privilegiado:

```
WLC-9800# configure terminal
WLC-9800 (config)# crypto key generate rsa general-keys label nombre_id_par_claves exportable modulus 2084
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 1 seconds)
```

111. Una vez obtenido el par de claves público-privada se genera la solicitud de certificado CSR con los comandos descritos más abajo (donde se emplea el par de claves ya generadas):

```
WLC-9800# configure terminal
WLC-9800 (config)# crypto pki trustpoint nombre_certificado
WLC-9800 (ca-trustpoint) # enrollment terminal pem
WLC-9800 (ca-trustpoint) # revocation-check none
WLC-9800 (ca-trustpoint) # subject-name C=País, ST=Estado, L=Localidad, O=Organización, OU=Departamento, CN=nombre.dominio.com
WLC-9800 (ca-trustpoint) # exit
WLC-9800 (config) # crypto pki enroll nombre_certificado
```

```
% Start certificate enrollment ..
% The subject name in the certificate will include: C=País, ST=Estado,
L=Localidad, O=Organización, OU=Departamento, CN=nombre.dominio.com
% The subject name in the certificate will include: 9800
nombre.dominio.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----
*9800 WLC CSR*
-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: no
```

112. Este resultado debe ser facilitado a una entidad certificadora o usado en la infraestructura PKI. Se debe tener en cuenta un aspecto importante una vez se obtiene la salida que ofrece el comando que genera la solicitud de certificado, no se puede volver a recuperar esa información.

113. De esta forma, al tener que realizar el proceso completo en una sesión continua, la clave permanece siempre en el controlador y se evita su exposición.

114. Una vez empleado el CSR en la correspondiente entidad o infraestructura se debe obtener el certificado raíz de la CA en formato *pem* e introducirlo en el controlador inalámbrico. Una vez obtenido hay que copiar y pegar el certificado, tal como se indica a continuación:

```
WLC-9800# configure terminal

WLC-9800 (config) # crypto pki authenticate nombre_certificado

Enter the base 64 encoded CA certificate.

End with a blank line or the word “quit” on a line by itself

-----BEGIN CERTIFICATE-----
*Certificado raíz de la CA, copiado y pegado directamente*
-----END CERTIFICATE-----

quit
Certificate has the following attributes:

Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C

Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809

% Do you accpet this certificate? [yes/no]: yes

Truspoint CA certificate accepted.

% Certificate successfully imported
```

115. En el caso de que existan diversos niveles de certificación, en el paso anterior únicamente se debe copiar y pegar el certificado de la CA que firma el certificado del dispositivo, y únicamente ese (nunca la cadena completa de certificación). Se necesitará crear un *trustpoint* para cada nivel de certificación y repetir el paso anterior para cada uno de esos niveles.

116. Para finalizar, se debe incorporar el certificado firmado:

```
WLC-9800# configure terminal
WLC-9800 (config) # crypto pki import nombre_certificado certificate
Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself
-----BEGIN CERTIFICATE-----
*Certificado del dispositivo firmado*
-----END CERTIFICATE-----
quit
% Router Certificate successfully imported
```

117. Una vez importados los certificados, la forma de emplearlos es sencilla. En el caso de la gestión del propio controlador inalámbrico basta con introducir el siguiente comando indicando el nombre del certificado:

```
WLC-9800# configure terminal
WLC-9800 (config) # ip http secure-truspoint nombre_certificado
```

118. Cuando ya ha sido aplicado el certificado para la gestión, normalmente se requiere de un reinicio del controlador inalámbrico, aunque reiniciar el servicio web debería ser suficiente:

```
WLC-9800# configure terminal
WLC-9800 (config) # no ip http server
WLC-9800 (config) # ip http server
WLC-9800 (config) # end
```

119. En el caso de que se deseara para una red donde se realiza autenticación web, el formato sería el siguiente:

```
WLC-9800# configure terminal
WLC-9800 (config) # parameter-map type webauth global
WLC-9800 (config-parameter-map) # trustpoint <trustpoint name>
WLC-9800 (config-parameter-map) # virtual-ip ipv4 IP_Interfaz_Virtual
virtual-host nombre.dominio.com
```

120. Con este último comando se define un *hostname* sobre la IP virtual (usualmente la 192.0.2.1) que coincidirá con el campo CN del certificado en cuestión.

121. En el caso de que existan controladores inalámbricos formando un clúster HA, los certificados son replicados en la unidad secundaria una vez que se han emparejado. Esto es una notable diferencia de lo que ocurría en los clúster AireOS, en los que se debía realizar una carga manual en ambas unidades.

122. Si se desea comprobar la configuración de certificados, se debe ejecutar el comando descrito más abajo, prestando especial atención al campo CN y a qué trustpoint está asociado. Si existe una cadena de certificación, se deberá comprobar cada uno de ellos.

```
WLC-9800# show crypto pki certificates nombre_certificado

Certificate
 Status: Available
 Certificate Serial Number (hex): 00A2020356CF31C818
 Certificate Usage: General Purpose
 Issuer:
 <<--output omitido-->
 Subject:
 Name: *.dominio.com
 cn=url.dominio.com
 ou=lab-mex-wireless
  <<--output omitido-->
 Validity Date:
 start date: 17:14:54 UTC Feb 15 2020
 end date: 17:14:54 UTC Mar 11 2023
 Associated Trustpoints: cert-name
 Storage: nvram:CA-KCG-lab#C818.cer
```

123. Se debe comprobar a su vez, si la administración por interfaz web está apuntando al certificado correcto. Esto se comprueba con el siguiente comando:

```
WLC-9800# show ip http server secure status

HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha aes-128-cbc-sha
 aes-256-cbc-sha dhe-aes-128-cbc-sha ecdhe-rsa-3des-ede-cbc-sha
 rsa-aes-cbc-sha2 rsa-aes-gcm-sha2 dhe-aes-cbc-sha2 dhe-aes-gcm-sha2
 ecdhe-rsa-aes-cbc-sha2 ecdhe-rsa-aes-gcm-sha2
HTTP secure server TLS version: TLSv1.2 TLSv1.1 TLSv1.0
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: cert-name
HTTP secure server active session modules: ALL
```

124. Para verificar que el servidor HTTP opera en un cifrado TLSv1.2 (recomendado como seguro en la guía CCN STIC-807) se puede configurar con el siguiente comando:

```
WLC-9800# ip http tls-version TLSv1.2
```

125. Tras la instalación, el acceso mediante HTTPS no debería ofrecer un error de certificado en el navegador (dado que ya no se usa un certificado autofirmado por el dispositivo, sino que se usa un certificado confiable para la organización).

126. Para cargar el resto de tipos de certificado, es posible hacerlo igualmente a través de la línea de comandos (CLI) o mediante GUI. Destacar que, en el entorno de controladores inalámbricos ejecutando IOS-XE, no se hace una distinción especial para el objetivo del certificado. Es decir, en el momento de su incorporación al dispositivo no se indica para qué se usará, a diferencia de los dispositivos ejecutando AireOS que diferenciaban la finalidad del certificado (*webadmin*, *webauth*, etc.)

127. Desde el GUI también es posible gestionar los certificados, aunque es requisito subirlos en formato pfx. Para ello, sobre el menú vertical izquierdo, dirigirse a *"Configuration-->Security-->Web Auth*", y en la ventana principal que aparece, acceder a la pestaña "*Certificate*".

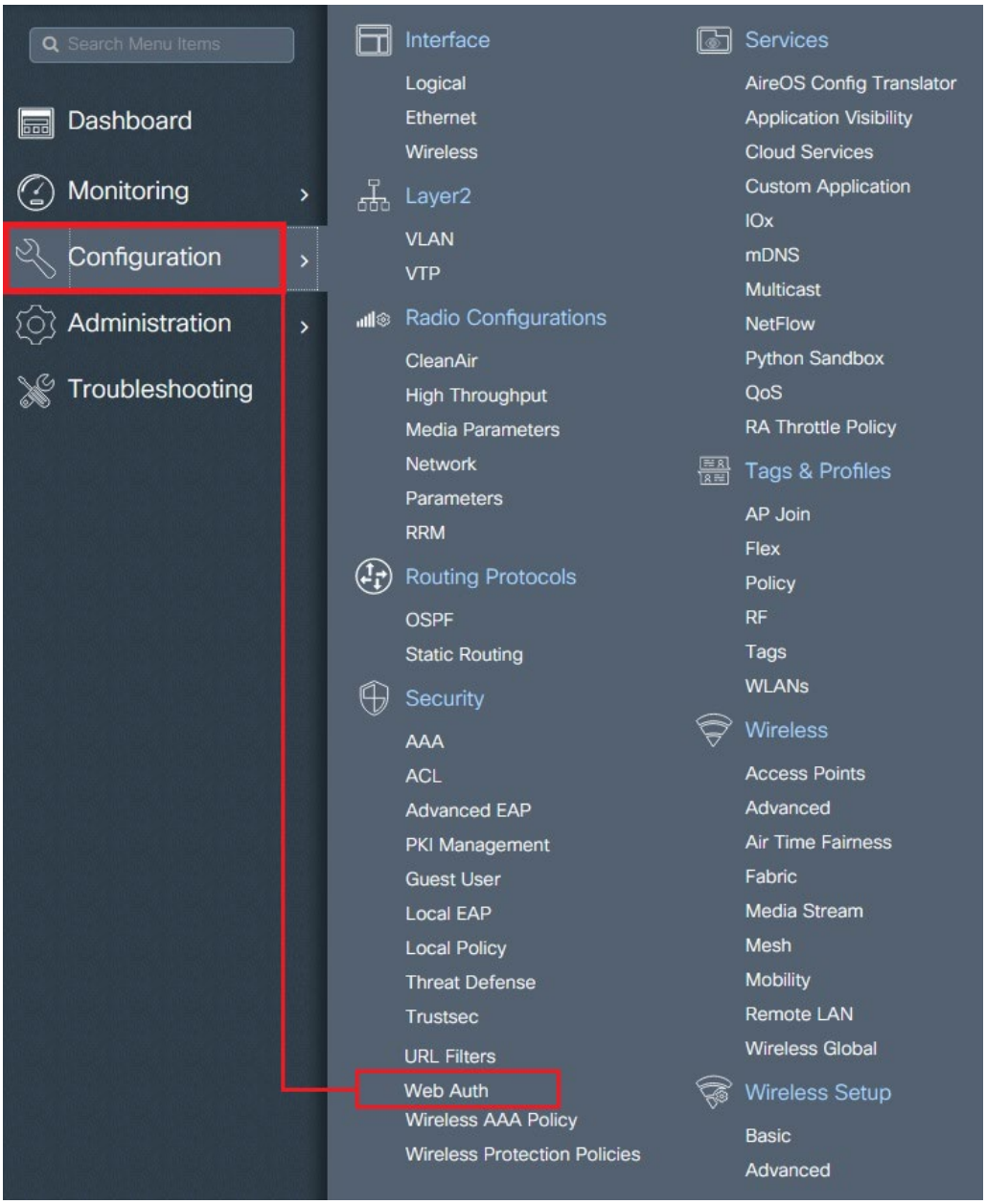


Ilustración 25. Acceso al menú *WebAuth*

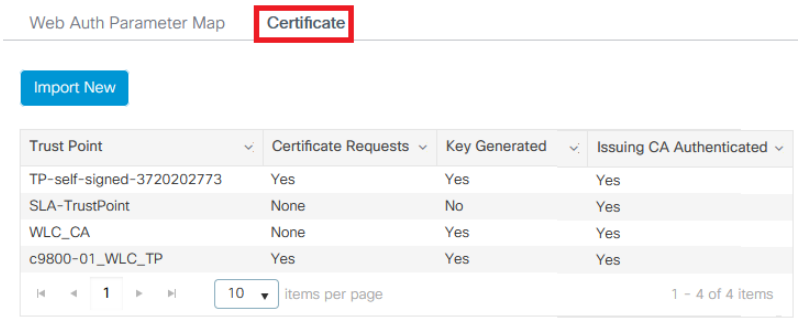


Ilustración 26. Instalación de otros tipos de certificado en el controlador (mediante GUI)

128. Una vez en la pestaña "*Certificate*", basta con pulsar sobre el botón "*Import New*" y aparecerá un cuadro de diálogo para insertar los datos del servidor, ubicación del certificado, nombre del certificado y clave.

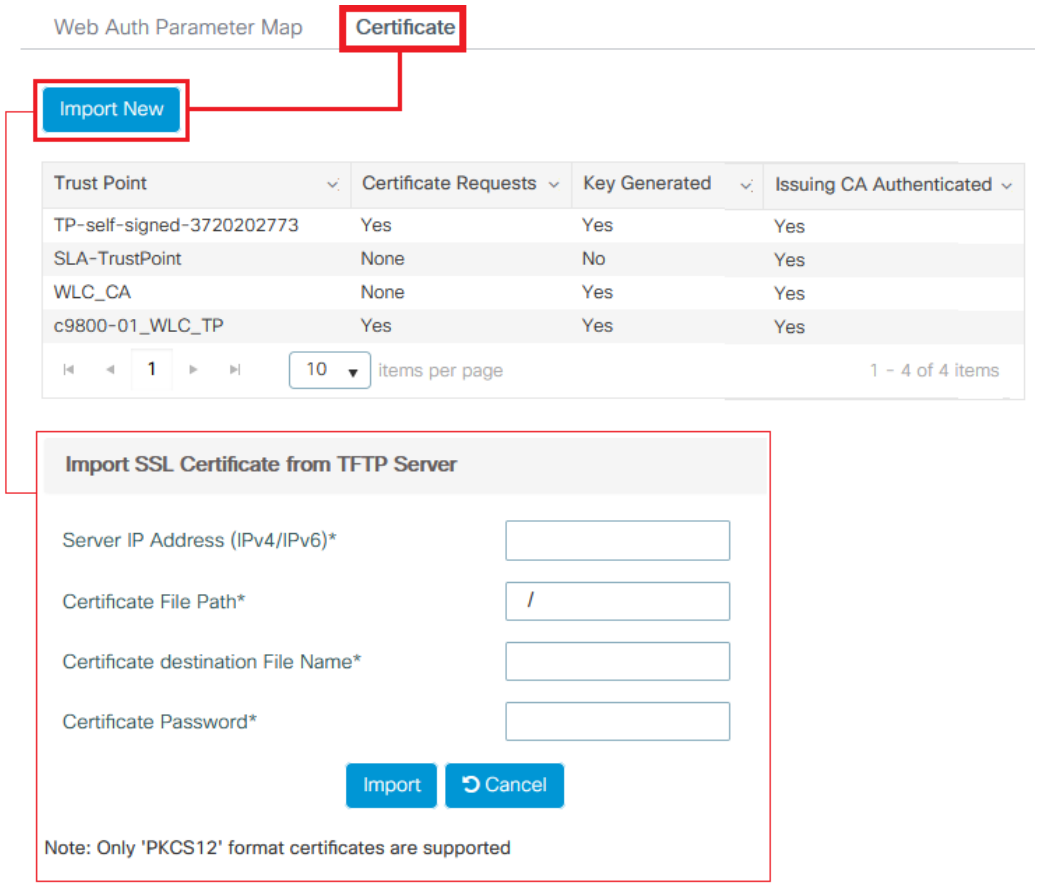


Ilustración 27. Importar certificado en el controlador (mediante GUI)

6.4 SINCRONIZACIÓN

129. **Las controladoras inalámbricas deben estar sincronizadas**, a través de un servidor NTP/SNTP.

130. Cada servidor NTP/SNTP se añade a la base de datos del controlador inalámbrico, entonces sondea cada servidor NTP/SNTP en el orden indicado por el índice con el que se configuró al añadirlo. Cuando reciba respuesta de cualquiera de los servidores sondeados por cada intervalo de tiempo definido, el controlador inalámbrico sincronizará su fecha.

Por defecto el intervalo de sondeo es de 600 segundos. Una sincronización fuera de ese intervalo se produce únicamente en el primer momento tras un reinicio del controlador.

131. El servidor NTP, si está configurado, es proporcionado por el entorno IT. Sin autenticación o control de acceso, NTP es inseguro y puede ser usado por un atacante para enviar paquetes NTP e intentar sobrecargar o bloquear los dispositivos. Para aumentar el nivel de seguridad, **la conexión al servidor NTP externo debe ser autenticada**, para evitar sufrir ataques basados en la manipulación de la señalización horaria en el controlador.

132. Para configurar el servidor SNTP, basta con acceder al menú "*Administration->Time*".

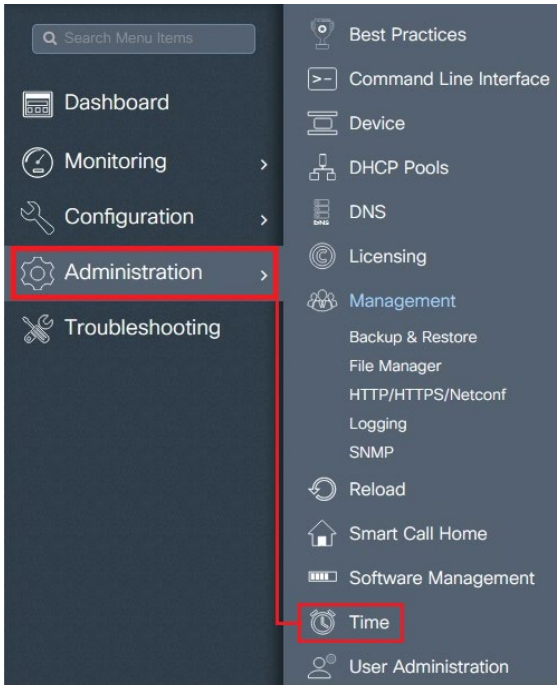


Ilustración 28. Acceso al menú horario

133. En la ventana principal aparecerá la hora actual y el listado de servidores NTP configurados en el dispositivo, si los hubiera. Para crear un nuevo servidor basta con pulsar el botón *"+Add"*.

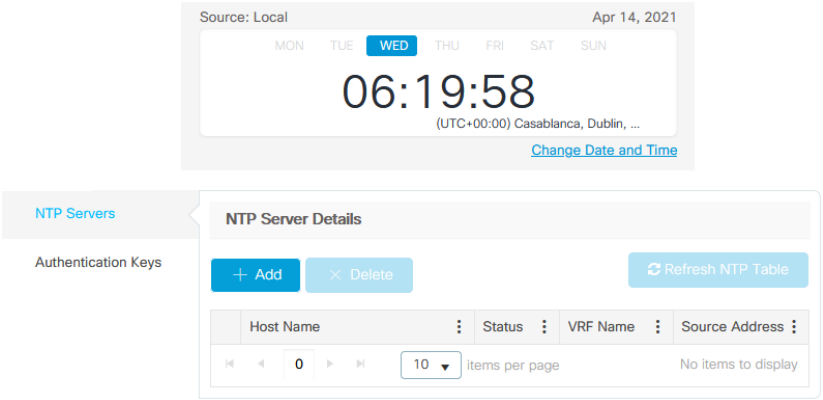


Ilustración 29. Configuración servidor NTP

134. Surgirá un nuevo menú, donde se solicitan los siguientes datos:

- *Host Name*: Nombre identificativo para el nuevo servidor NTP, puede ser una dirección IPv4/IPv6 o un nombre de puede ser "IPv4", "IPv6" o bien un nombre FQDN mediante. De ser esta última opción, se debe asegurar que el nombre cumple los siguientes criterios:
- Debe contener únicamente caracteres comprendidos entre a-z, A-Z y 0-9.
- No puede comenzar por punto ('.') o guion ('-').
- No puede terminar en punto ('.').
- No puede contener dos puntos consecutivos ('..').
- *Prefer*: Indica si será el servidor NTP a usar por defecto.
- *IP for DNS Resolution*: Indica si la resolución se hará con el protocolo IPv4 o IPv6.
- *VRF y VRF Name*: Si se habilita la opción VRF, se deberá introducir el nombre de la VRF que aplica para el servidor NTP.
- *Source Address*: Indica el interfaz que se empleará para comunicarse con el servidor NTP. Las opciones son "*None | VLAN | Interface*".
- *Enable Authentication*: Indicará que se requiere (o no) autenticación contra el servidor NTP. **Se debe marcar esta opción.**
- *Authentication Key*: Indica el índice de clave que se empleará, si la autenticación está habilitada (debe ser previamente creada).

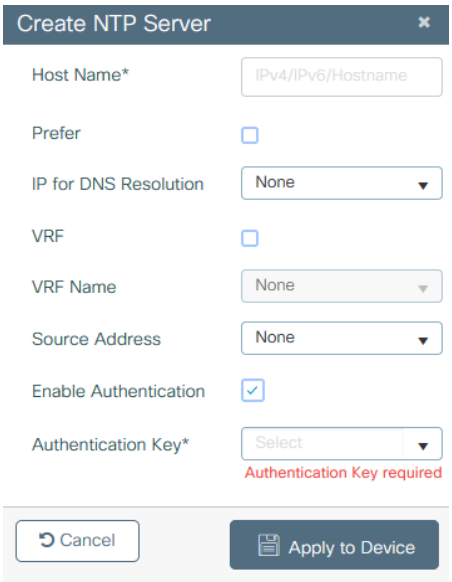


Ilustración 30. Configuración servidor NTP

135. Para la configuración de NTP se pueden usar una serie de comandos, que se muestran los comandos a continuación:

```
WLC-9800 (config) # ntp server Hostname
WLC-9800 (config) # ntp server IP_ó_FQDN
```

```
WLC-9800 (config) # ntp server Hostname  {prefer | source <VLAN | Gi#> | key #}
WLC-9800 (config) # ntp authentication-key número hmac-sha2-256 clave
 WLC-9800 (config) # ntp authenticate
WLC-9800 (config) # ntp trusted-key 1
```

6.5 ACTUALIZACIONES

136. Los dispositivos Catalyst 9800, como cualquier otro dispositivo de red, deben estar protegidos de vulnerabilidades de su propio sistema operativo, así como corregir posibles fallos de operación detectados tras el uso del mismo. Estas vulnerabilidades y fallos normalmente se suelen corregir con actualizaciones de la versión del *firmware*. El personal encargado de la administración de los dispositivos, **deberá revisar de forma periódica las actualizaciones que Cisco despliegue.**

137. Cisco recomienda una serie de versiones de *software* en concreto, que se pueden consultar en las "*Troubleshooting TechNotes*", en la sección "*TAC Recommended IOS-XE Builds for Catalyst 9800 Wireless LAN Controllers*" (ver [23]). Es posible que existan versiones más modernas que la recomendada, pero no significa que sean las más estables. De cualquier modo, es una tarea del personal administrador de los dispositivos el evaluar si es necesario actualizar a versiones superiores (por ejemplo, porque solucione un fallo de operación por el que se vea afectado de forma directa el servicio inalámbrico que prestan).

138. Para consultar las versiones disponibles de los dispositivos, se debe realizar a través de la página oficial de Cisco, a través de un navegador Web seguro y consultando la URL "https://software.cisco.com/download/home". En esta página, deberá comprobar el listado de los equipos, dirigiéndose a "*Wireless->Wireless LAN Controller->Standalone Controllers*". Aparecerá el listado completo de familias de controladores inalámbricos, se debe navegar en la deseada y seleccionar el modelo concreto (las dos familias de controladoras Catalyst 9800, las que son en formato físico, y las que son en formato *cloud*).

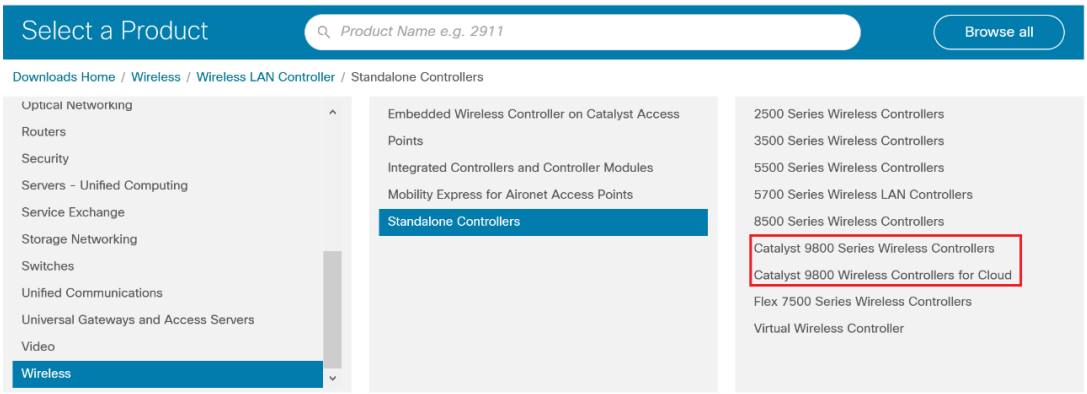


Ilustración 31. Navegación por el apartado de Downloads de la web de Cisco

139. También puede usar la herramienta "buscador" que ofrece la misma página web. De cualquier forma, una vez seleccionado el modelo se puede consultar toda la información disponible para el mismo. Se muestra en la siguiente imagen el resultado de seleccionar

el controlador Catalyst 9800. Para consultar las versiones de firmware disponibles, se debe navegar a la sección "*Wireless LAN Controller Software*".

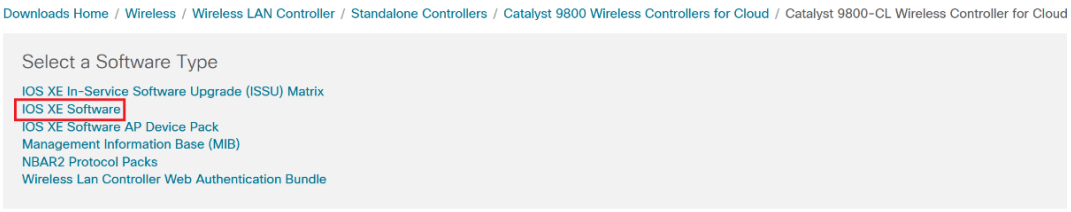


Ilustración 32. Selección de objeto de la descarga

140. El proceso de actualización debe comenzar por un trabajo previo, que consiste en determinar si la versión deseada es soportada por los puntos de acceso desplegados. Para ello, hay que informarse a través del documento "*Releases Notes*" de la versión a la que se desea migrar. Estos documentos se pueden encontrar en la sección de descarga del *software* nombrada en el párrafo anterior. En la siguiente imagen, se muestra dónde puede encontrarse este documento para un controlador modelo Catalyst 9800:

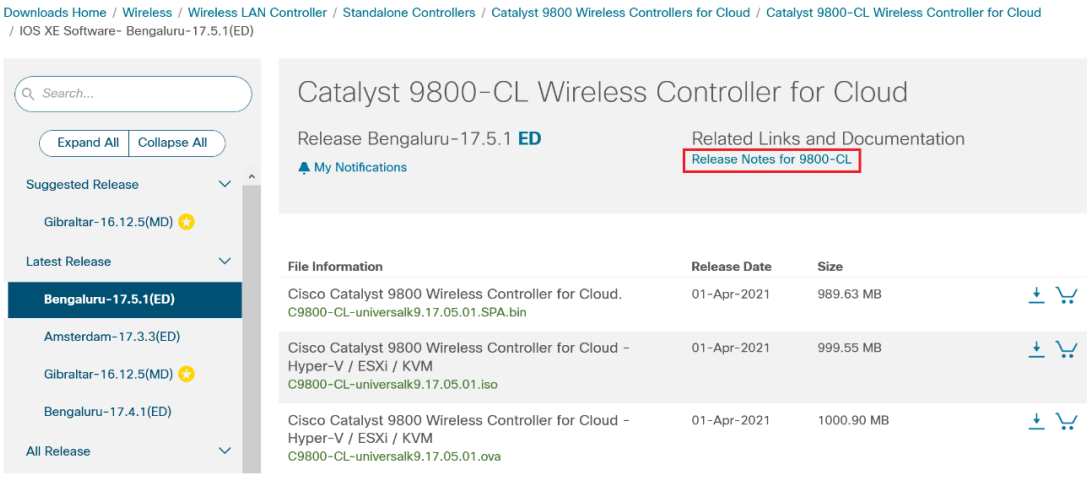


Ilustración 33. Descarga de las "*Release notes*" de la versión escogida

141. Es importante dentro de este documento observar el apartado "*Read Before You Upgrade*", que indica si es necesario tomar alguna precaución sobre la actualización, partiendo de la versión y tipología de configuración actual.

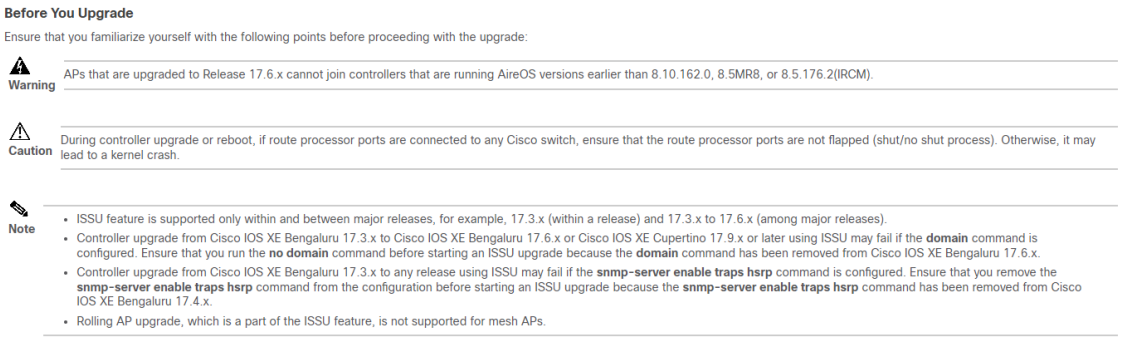


Ilustración 34. Comprobaciones previas a la actualización

142. También es importante comprobar que, terminada la actualización, el nuevo *firmware* es compatible con todos los modelos de AP presentes en el sistema. Para ello es de gran

utilizad comprobar la "*Supported APs*" que suele acompañar dichas "*Release Notes*" de versión. Si hay puntos de acceso existentes en la infraestructura que no se encuentren como compatibles dentro de la nueva versión, se recomienda su sustitución como paso previo a la actualización.

Supported APs

The following Cisco APs are supported in this release.

Indoor Access Points

- Cisco Catalyst 9105AX (I) Access Points
  - VID 04 or later - supported from 17.6.4
  - VID 03 or earlier - supported in all 17.6.x releases
- Cisco Catalyst 9105AX (W) Access Points
  - VID 02 or later - supported from 17.6.4
  - VID 01 or earlier - supported in all 17.6.x releases
- Cisco Catalyst 9115AX (I/E) Access Points
- Cisco Catalyst 9117AX (I) Access Points
- Cisco Catalyst 9120AX (I/E) Access Points
  - VID 07 or later - supported from 17.6.4
  - VID 06 or earlier - supported in all 17.6.x releases
- Cisco Catalyst 9120AX (P) Access Points
- Cisco Catalyst 9130AX (I/E) Access Points
  - VID 03 or later - supported from 17.6.4
  - VID 02 or earlier - supported in all 17.6.x releases

(For information about Cisco Catalyst 9105, 9120, or 9130 Access Points version support, see the Field Notice 72424.)

- Cisco Aironet 1815 (I/W), 1830 (I), 1840 (I), and 1852 (I/E) Access Points
- Cisco Aironet 2800 (I/E) Series Access Points
- Cisco Aironet 3800 (I/E/P) Series Access Points
- Cisco Aironet 4800 Series Access Points

Outdoor Access Points

- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points
- Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point
- Cisco 6300 Series Embedded Services Access Point
- Cisco Catalyst 9124AX (I/D/E) Access Points

Integrated Access Points

- Integrated Access Point on Cisco 1100 ISR (ISR-AP1100AC-x, ISR-AP1101AC-x, and ISR-AP1101AX-x)

Network Sensor

- Cisco Aironet 1800s Active Sensor

Ilustración 35. Comprobación de compatibilidad de puntos de acceso antes de la actualización

143. Respecto al fichero de *firmware*, una vez se haya descargado, la recomendación es comprobar que es el fichero que indica la plataforma, y que no ha sufrido alteraciones. Para ello, se debe comprobar la firma SHA-512 en un equipo confiable de la organización. El valor a obtener debe comprobarse en los detalles del fichero disponible para descargar. Si no coinciden, el proceso de actualización debe detenerse.

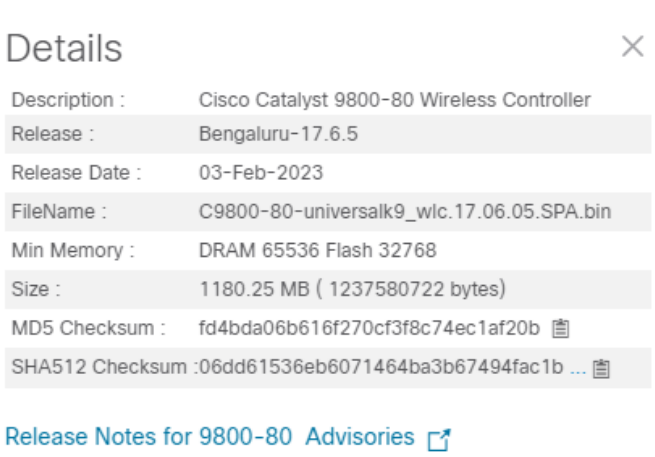


Ilustración 36. Comprobación del hash MD5/SHA512 de la versión de firmware seleccionada

144. Sea una actualización directa, o varias, el procedimiento de actualización es el mismo. Se muestra a continuación de forma resumida:

- Salvar la configuración actual del dispositivo, ya sea a través del interfaz web (en cualquier vista de menú, esquina superior derecha, enlace indicado por el icono del disco y "*Save Configuration*" o a través de comandos mediante sesión segura a través de SSH ejecutando *"#write memory*").

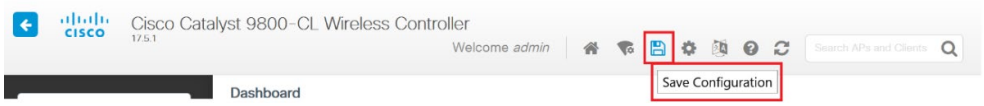


Ilustración 37. Enlace "*Save configuration*" disponible en cualquier vista del interfaz web

- Extraer la configuración del dispositivo de forma segura. Para ello se puede realizar como se ha explicado, a través del interfaz web, en el menú "*Administration->Management->Backup&Restore*". En el menú que aparecerá en pantalla principal, se debe seleccionar la opción "*Config File Management->Copy to Device->Configuration*" junto a la información del servidor en el que se desee almacenar la configuración.

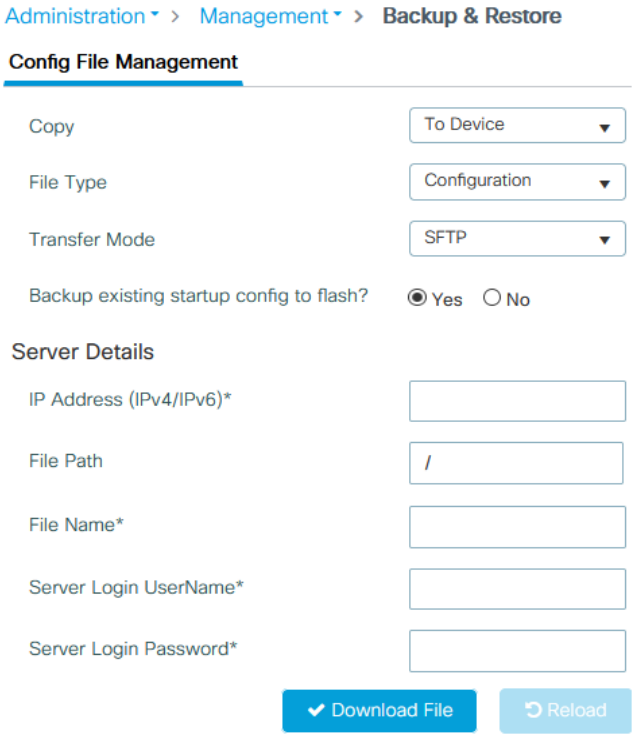


Ilustración 38. Menú para extraer a un servidor externo la configuración

- Seguidamente, se puede subir la nueva versión al controlador inalámbrico, desde el menú "*Administration->Software Management*", y completar las opciones:
- *Upgrade Mode*: INSTALL usa un sistema de paquetería más eficiente en memoria que BUNDLE, por lo que se recomienda dicha opción.
- *One-Shot Install Upgrade*, en caso de que se desee que el equipo se reinicie de manera automática tras la instalación de la nueva versión.
- *Transport type*: SFTP, FTP, TFTP, Desktop (HTTP).
- *Filesystem*: sistema de ficheros de destino, normalmente *bootflash:*, para que pueda usarse la nueva imagen para el arranque.
- *Source File Path*: con la ruta hacia el fichero de actualización, y el nombre del fichero propiamente dicho.

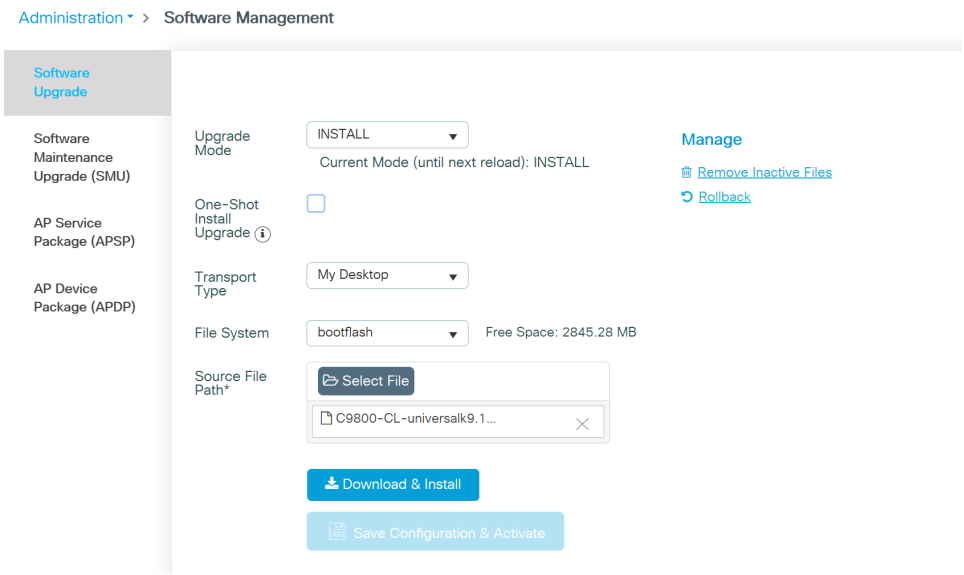


Ilustración 39. Menú de actualización de firmware "*Software upgrade*"

- Por último, se utiliza la opción "*Download&Install*", con lo cual se descargará el fichero y se descomprimirá en *bootflash*:, pero para que el equipo pueda ejecutar el nuevo código, será necesario reiniciar. Opcionalmente, está la opción de *"Save Configuration & Activate*" que guarda la configuración y realiza el reinicio para la activación de la nueva versión de *software*. Durante la subida, una de las tareas del script interno que contiene el controlador inalámbrico es comprobar la firma *hash* del fichero de *firmware* que se está intentando incorporar al controlador, por lo que la comprobación de la integridad se realiza de un modo u otro, aunque no se haya realizado en un equipo externo confiable. Durante el proceso, es posible consultar el log de la instalación, para comprobar que todos los pasos se están realizando correctamente:

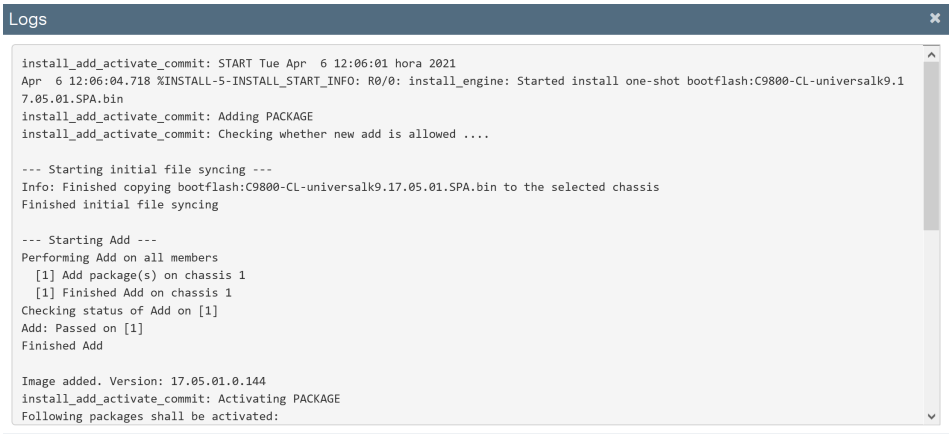


Ilustración 40. Log de instalación para comprobar el despliegue de la nueva versión

- Si todo el proceso ha ido correctamente, tanto el GUI como el log informan de que se ha instalado correctamente la nueva versión:

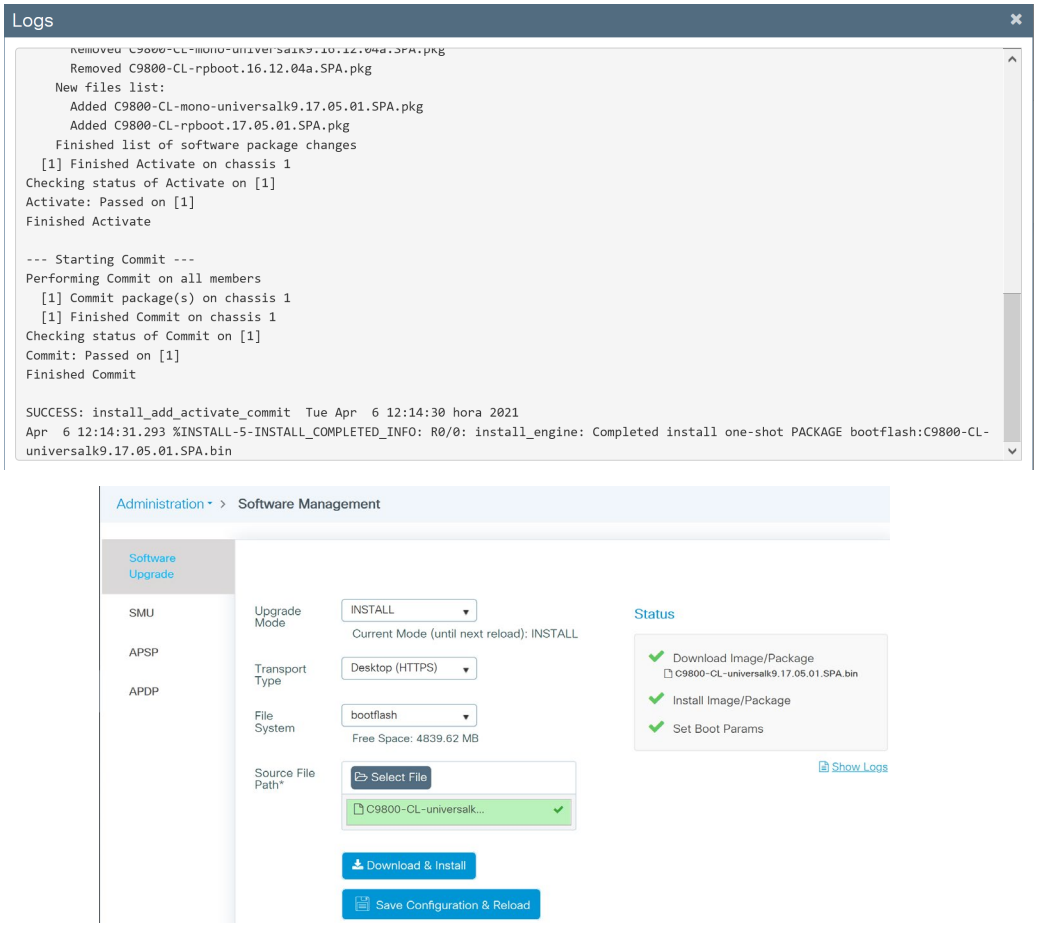


Ilustración 41. Verificación de instalación correcta de firmware

- Por último, sólo queda proceder con el reinicio del equipo para que la nueva versión de *firmware* se active y se cargue en memoria.

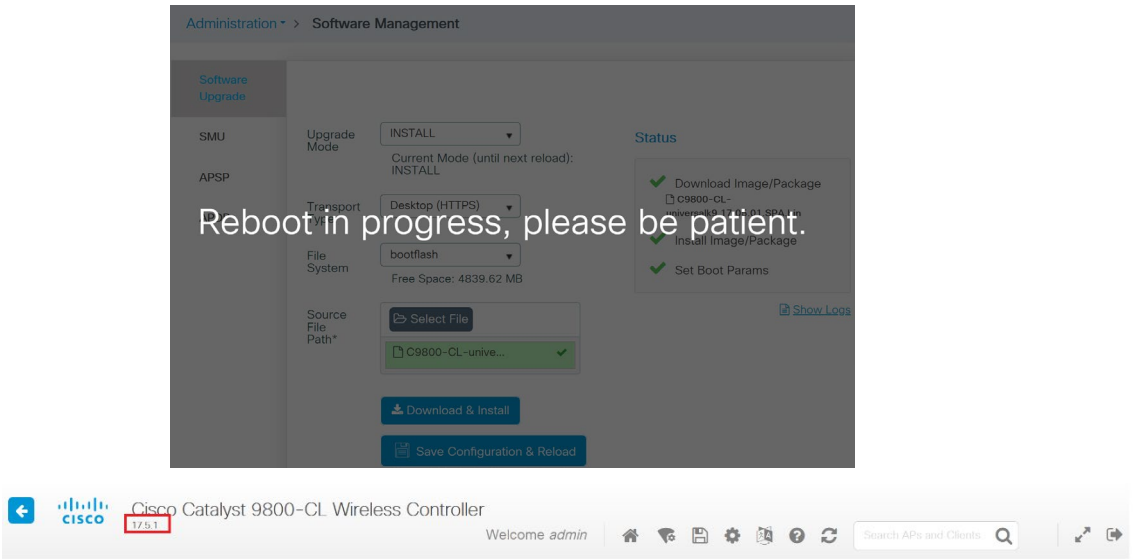


Ilustración 42. Reinicio y comprobación de que la imagen ha cargado correctamente

6.6 BACKUKP

145. En el controlador inalámbrico se pueden realizar operaciones de carga y descarga de transferencia de ficheros, siendo las más comunes copias de seguridad de la configuración, junto con la de incorporar aspectos visuales al portal cautivo interno (*webauth-bundle*). La subida de certificados al controlador en la serie Catalyst 9800 se realiza desde otro menú distinto, a diferencia de la gama 5508 que usaba el mismo menú.

146. Hay que tener en cuenta que los protocolos permitidos para estas operaciones son TFTP, FTP, SFTP y HTTPS. **Se debe hacer uso del protocolo SFTP o HTTPS**, ya que de las opciones permitidas son las que permiten el uso de algún tipo de cifrado (SFTP en este caso de las mismas características que SSH ya que se basa en dicho protocolo, y HTTPS sobre TLS).

147. Para realizar estas tareas de transferencia, en primer lugar, se necesita preparar el servidor (en caso de usar SFTP) y realizar la configuración correcta en *Administration->Management->Backup&Restore*.

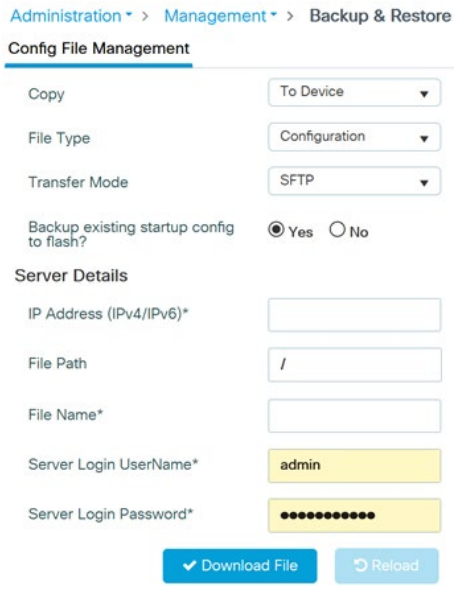


Ilustración 43. Carga de ficheros en el controlador

148. Una vez aquí, seleccionar:

- Tipo de fichero a cargar/subir: Puede ser un fichero de configuración o una personalización del portal cautivo.
- Modo de transferencia: De las diferentes opciones, se recomienda SFTP o HTTP.
- IP del servidor SFTP (si se usa dicha opción).
- Directorio donde se aloja el fichero deseado.
- Nombre del fichero.
- Usuario de acceso al servidor.
- Clave del usuario anterior.

149. La única opción diferenciadora entre la carga/descarga de ficheros, es que en la descarga (llevar ficheros desde el controlador hasta el servidor) solo existe la opción para descarga de la configuración (ya se la de arranque o la actualmente cargada en memoria).

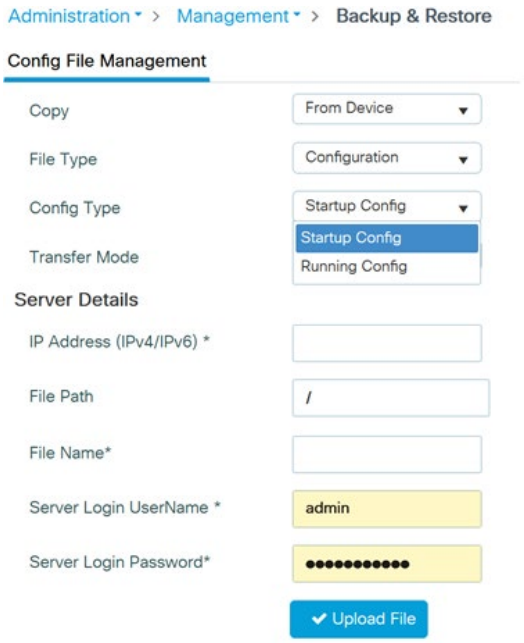


Ilustración 44. Descarga de ficheros desde el controlador

150. **Se deben realizar copias de seguridad de forma frecuente, para así poder recuperar la operatividad con el menor impacto posible en caso de una configuración errónea o malintencionada por terceros.**

7. CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDA DEL ENS PARA INFRAESTRUCTURAS INALÁMBRICAS

151. A continuación, se detallan los elementos más importantes a tener en cuenta dentro de un despliegue que incorpore un controlador Cisco Catalyst 9800 como infraestructura inalámbrica, de modo que se cumplan los principios básicos de seguridad descritos en la guía **CCN-STIC-816 Seguridad en Redes Inalámbricas en el ENS**.

7.1 MODO INFRAESTRUCTURA

152. La guía indica como requisito (CCN-STIC-816 Apdo. 5.2.4) el despliegue en modo infraestructura, de modo que un equipo inalámbrico para conectarse a otro equipo, debe acceder a través de un punto de acceso (AP), no pudiendo hacerlo directamente (como ocurriría en una red *ad hoc*).

153. En el caso de los controladores Cisco Catalyst 9800, es su modo normal y único de funcionamiento, no siendo necesario realizar ninguna función sobre el equipo para que actúe en este modo.

7.2 ASPECTOS GENERALES DE SEGURIDAD

7.2.1 ASPECTOS DE SEGURIDAD RELACIONADOS CON EL SSID

154. El primer aspecto a contemplar a la hora de crear una red, es definir su nombre, y determinar si dicho identificador se va a radiar (es decir, si va a ser visible para los dispositivos inalámbricos que lleven a cabo un escaneo pasivo del entorno).

155. **Se recomienda ocultar el SSID de la red** para reducir el perfil de ataque a la misma (recomendación según CCN-STIC-816 Apdo. 5.2.4), y si no es posible por alguna incompatibilidad con dispositivos inalámbricos obsoletos pero críticos para la instalación, que dicho identificador no tenga relación con la organización en sí (requisito según CCN-STIC-816 Apdo. 4.3.2).

156. Para ello, en el menú *WLAN->General->Broadcast SSID*, desmarcar la opción, y aplicar cambios.

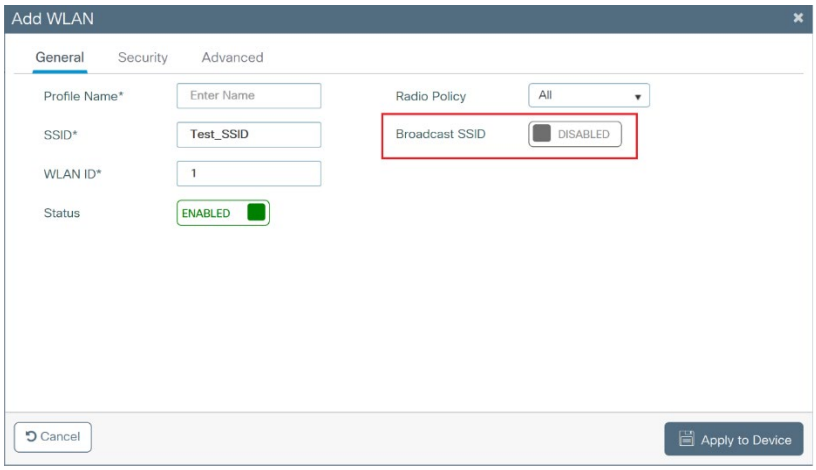


Ilustración 45. Configuración de emisión del identificador inalámbrico de red (SSID)

7.2.2 IMPLEMENTACIÓN DE FILTRADO MAC EN UN PERFIL

157. Otro aspecto recomendado en el cumplimiento del ENS e**s la limitación de las direcciones MAC permitidas para conexión inalámbrica** (recomendación según CCN-STIC-816 Apdo. 5.2.4).

158. En primer lugar, se crea un método de AAA de Autorización (*Configuration-> Security->AAA->AAA Method List->Add*)

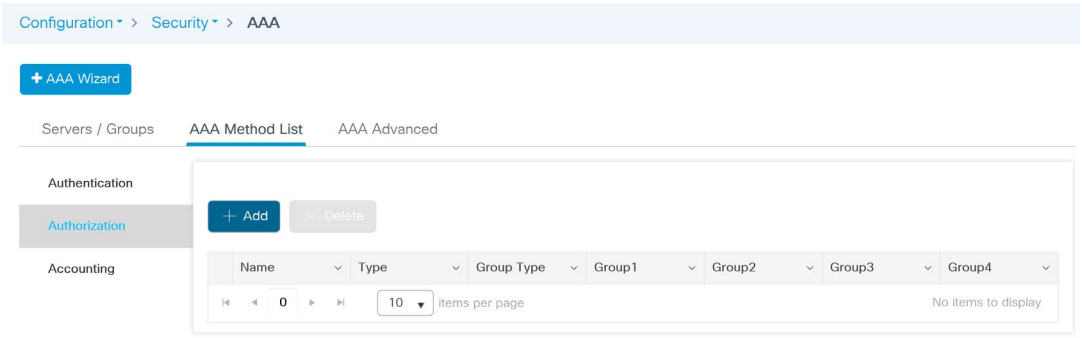


Ilustración 46. Configuración de un método de autorización de AAA

159. Es necesario especificar un nombre, de tipo red (*Type: network*) y tipo de grupo local (*Group Type: Local*), y se aplican los cambios:

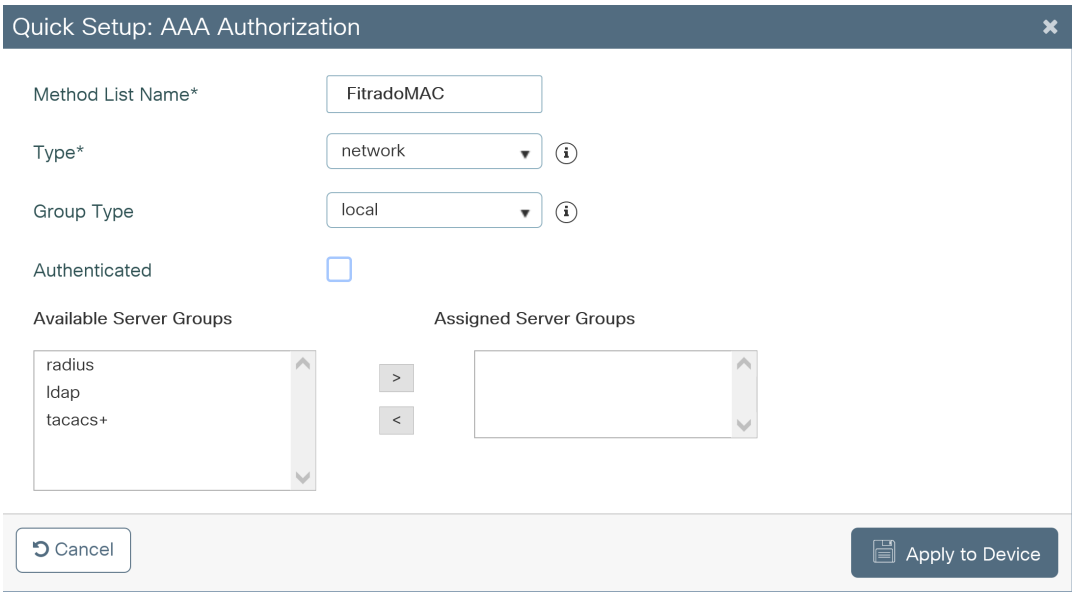


Ilustración 47. Configuración del método de AAA de autorización para MAC Filtering

160. Es necesario indicar a qué SSID se le va a aplicar este tipo de método de AAA. Para ello, en la pestaña de opciones avanzadas (*Configuration-> Security->AAA->AAA Advanced)* seleccionamos *Attribute List Name* y añadimos un nuevo atributo (*Add*):

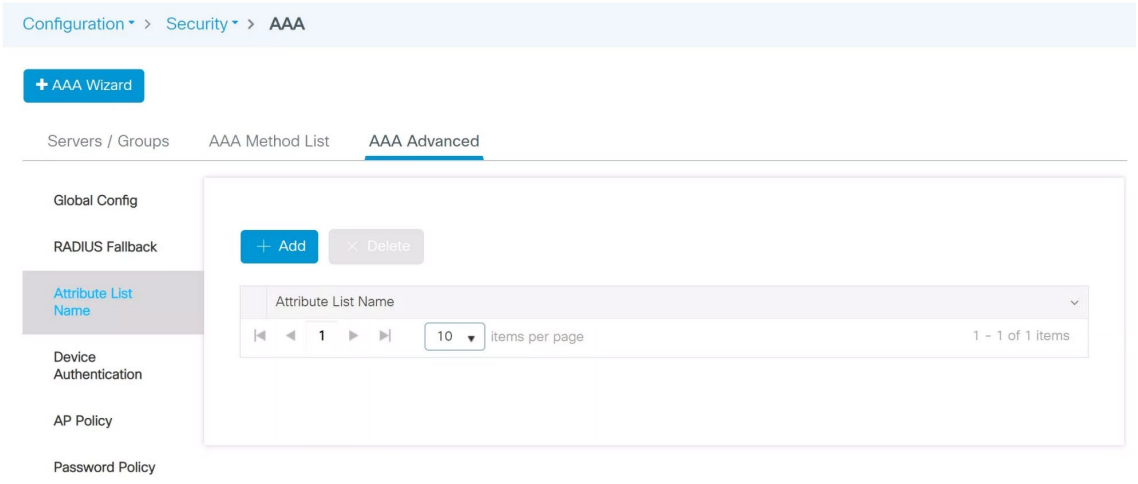


Ilustración 48. Asignación de atributos al método AAA

161. Se introduce un nombre indicativo (p. ej. *Test_MacAuth*) y ya es posible seleccionar como atributo el SSID al que se le desea aplicar el filtrado (en el ejemplo, el SSID sería *TestWLAN*), y se aplican los cambios al dispositivo:

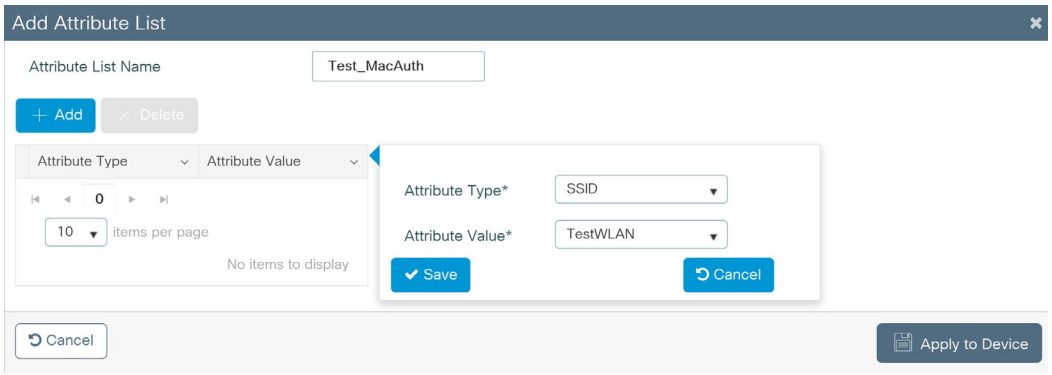
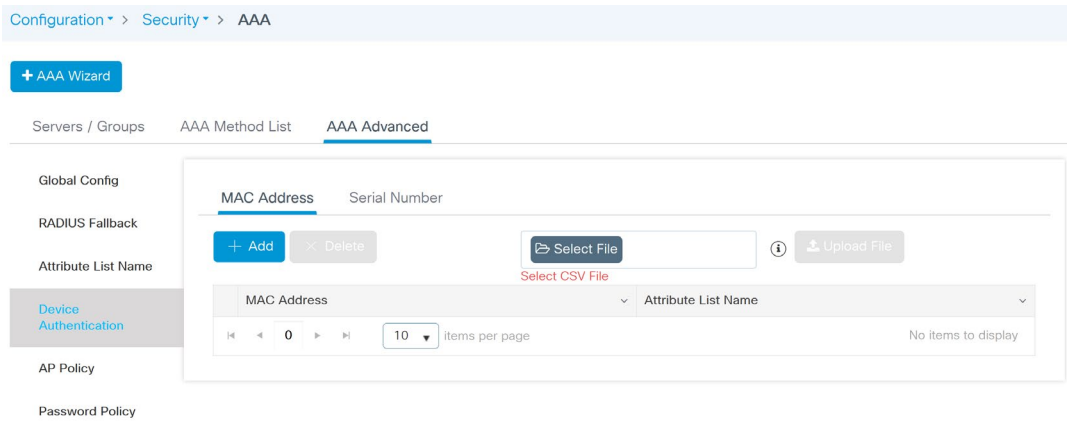


Ilustración 49. Configuración del atributo SSID aplicado al método de AAA

162. Por último, se crea la lista de dispositivos autorizados por MAC, que irán asociados al SSID anteriormente seleccionado. Para ello, dentro de la pestaña de Autenticación de Dispositivos (*Configuration->Security->AAA->AAA Advanced ->Device Authentication)* se pueden añadir los dispositivos uno a uno, manualmente, o importando un listado .CSV:



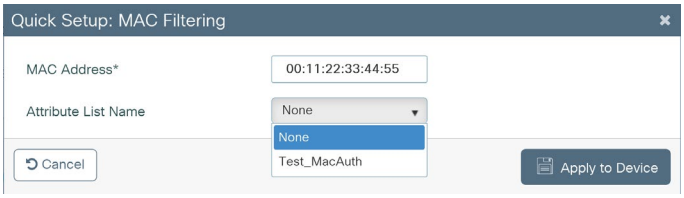


Ilustración 50. Configuración del listado de dispositivos autorizados por MAC

7.2.3 MONITORIZACIÓN DE LA ACTIVIDAD DE LOS USUARIOS

163. **Se debe implementar la configuración necesaria para enviar la actividad de los usuarios (conexión/desconexión, datos de equipo, datos de usuario) a un servidor de logs centralizado**. Para ello, se debe definir un servidor de Syslog remoto para la recopilación de los eventos de actividad de los usuarios (requisito según CCN-STIC-816 Apdo. 5.2.6).

164. Para su implementación, dentro del menú *Troubleshooting->Syslog* se pueden configurar los datos relacionados con un servidor de syslog pulsando sobre la opción *Manage Syslog Servers*.

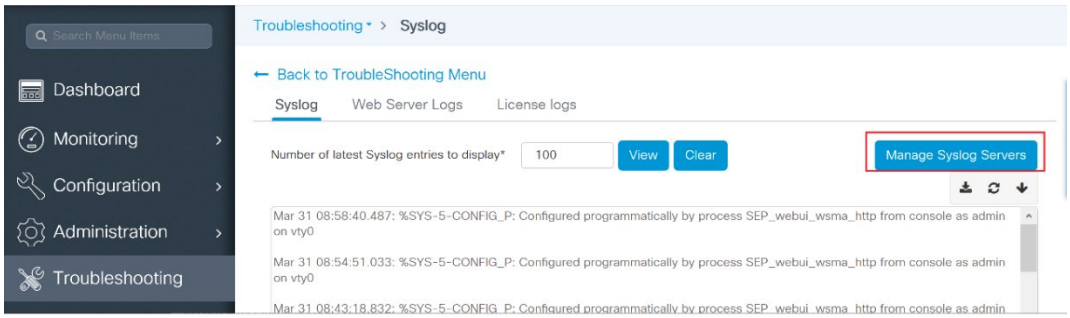


Ilustración 51. Mensajes de syslog y configuración de servidores

165. Entre los siguientes datos a proporcionar se encuentran:

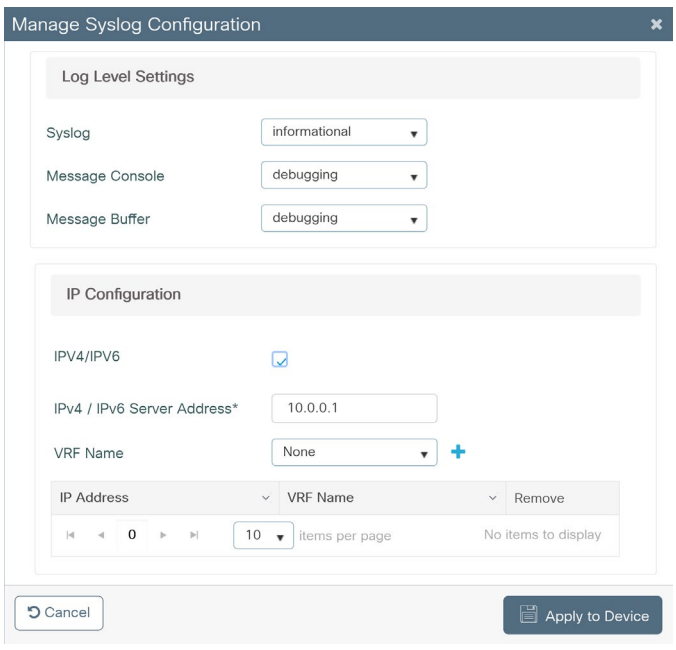


Ilustración 52. Configuración de un servidor de Syslog

- Dirección IP del servidor de syslog, con opción de usar un VRF de gestión, si se encuentra configurado. De este modo, se separan las tablas de enrutamiento del plano de usuarios del plano de gestión.
- Nivel de *syslog* deseado. Es posible definir valores separados para el propio servidor (*Syslog*), para la consola (*Message Console*) y para el buffer circular de almacenamiento de mensajes (*Message Buffer*). Los valores permitidos, de mayor nivel de criticidad a menor, son los siguientes: *Emergencies, Alerts, critical, errors, warnings, notifications, informational, debugging*.

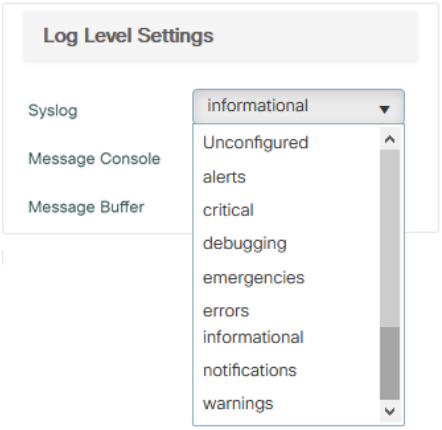


Ilustración 53. Niveles de Syslog

166. Además de esto, los siguientes comandos permiten obtener información adicional sobre la actividad de usuarios:
    - Para crear entradas de log que indiquen un intento fallido de inicio de sesión:

```
WLC-9800(config)# login on-failure log
```

    - Para crear entradas de log que indiquen un éxito de inicio de sesión:

```
WLC-9800(config)# login on-success log
```

7.2.4 ESTABLECIMIENTO DEL TIEMPO MÁXIMO DE SESIÓN DEL USUARIO

167. El sistema también debe poder permitir un tiempo de sesión limitado, para obligar a un dispositivo inalámbrico a autenticarse pasado un cierto tiempo (recomendación según CCN-STIC-816 Apdo. 5.2.4).
168. Este valor es propio para cada uno de los perfiles inalámbricos definidos en el dispositivo (*Policy Profiles*), que luego se asocia a la WLAN (o WLANs) que tenga asociado dicho perfil.
169. Para su configuración, en *Configuration->Tag&Profiles->Policy*, se edita el perfil deseado (en este caso, *Test_WLANID_1*), y en la pestaña de ajustes avanzados (*Advanced*) se puede establecer el tiempo máximo sesión (*Session Timeout*):

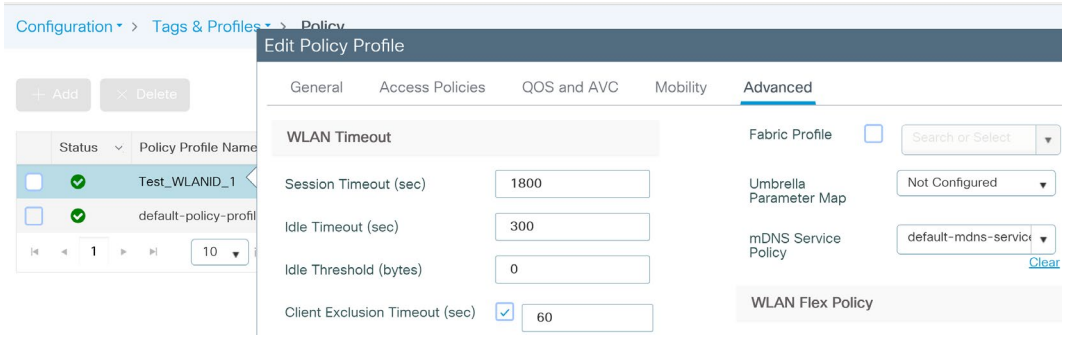


Ilustración 54. Establecimiento del tiempo máximo de sesión

7.2.5 PROTECCIÓN DE LAS TRAMAS DE GESTIÓN

170. Otro aspecto importante a tener en cuenta es la protección de las tramas de gestión, para que dichas tramas puedan disfrutar de las facilidades de confidencialidad, integridad, autenticación de origen y protección anti-reenvíos.

171. Con esta funcionalidad, se protege a la red de los principales ataques de suplantación de puntos de acceso (*broadcast deauth*, por ejemplo). El motivo es que el punto de acceso atacante no dispone de los conocimientos necesarios para firmar las tramas de gestión (entre ellas, las de deautenticación), por lo que el cliente desechará las tramas de gestión que no vengan correctamente firmadas desde la infraestructura inalámbrica.

172. En la controladora Catalyst 9800 se implementa protección de trama de gestión a nivel de cliente (*Client MFP Functionality*) bajo el estándar 802.11w:

    a) Se añade protección de cliente añadiendo protección criptográfica a las tramas de deautenticación y desasociación, impidiendo ataques de tipo DoS.

    b) Se añade protección a nivel de infraestructura, mediante mecanismos que evitan la falsificación de este tipo de tramas, evitándose ataques de replicación tras provocar una desconexión del cliente.

    c) Uso de un nuevo tipo de clave, IGTK, usada para la protección de tramas de broadcast/multicast dentro del RSN IE.

173. Para ello, se usan dos (2) mecanismos:

    a) Control del tiempo de asociación (*Association comeback timer*).

    b) Uso de una solicitud de SA (*Secutiry Association Query*) para evitar ataques de replicación de tramas, en los que un dispositivo trata de repetir el tráfico de un dispositivo que ha sido previamente desconectado de la red.

174. Dentro de la protección de trama de gestión a nivel de cliente, es posible definir tres (3) valores para su configuración:

    a) Deshabilitado.

    b) Opcional. En este modelo, la infraestructura inalámbrica lleva un registro de los clientes que pueden soportar el cifrado tramas de gestión, y los que no disponen de dicha funcionalidad, de modo que sólo implementa MFP con los primeros.

c) Obligatorio. En este caso, todos los clientes deben soportar la funcionalidad, o no podrán conectarse satisfactoriamente a la red. **Esta es la opción recomendada.**

175. Si la configuración se realiza únicamente dentro de perfil inalámbrico específico, sólo se habilitará la protección MFP de cliente para ese perfil.

176. Para su configuración, es necesario seguir los siguientes pasos:

a) Seleccionar el perfil inalámbrico específico para el que se desea habilitar FMP a nivel de cliente (*Configuration->Tag&Profiles->WLANs*)

b) Dentro de la pestaña de *Layer 2 Security* seleccionamos el tipo de protección MFP deseado:

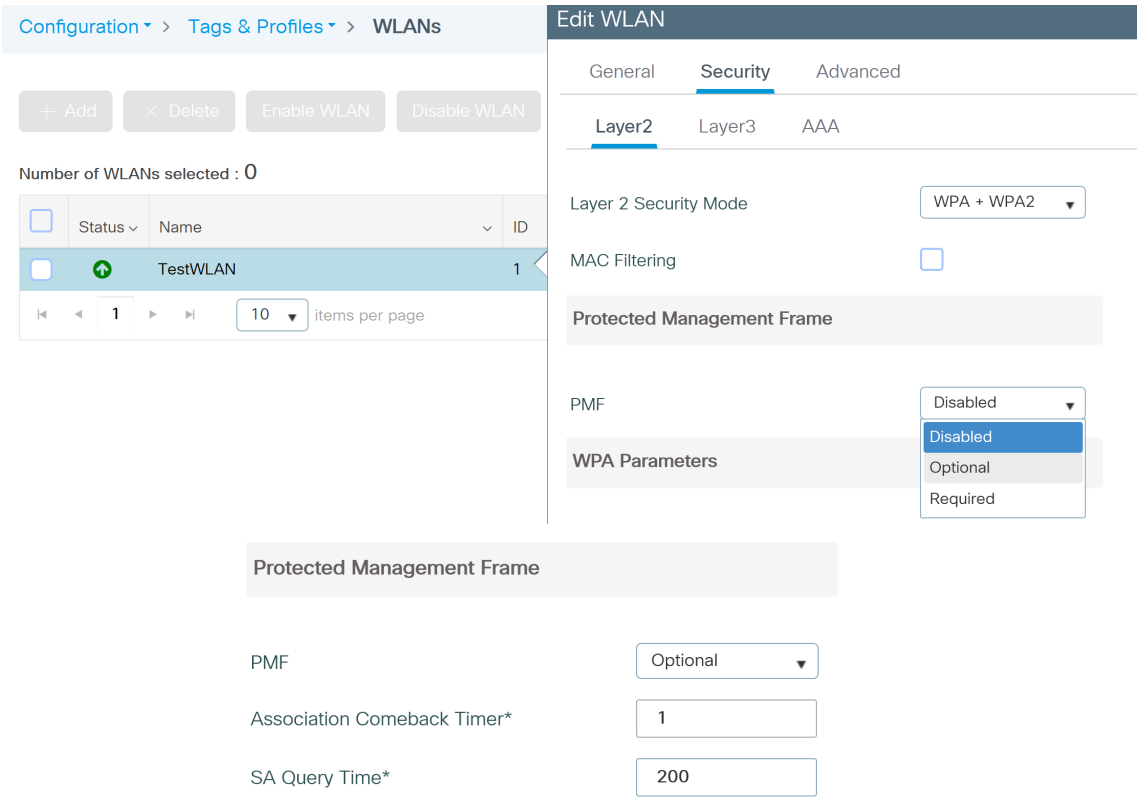


Ilustración 55. Protección de MFP de cliente a nivel de WLAN

7.3 MECANISMOS DE CIFRADO Y AUTENTICACIÓN

7.3.1 DEFINICIÓN DE LOS ALGORITMOS DE CIFRADO

177. Para la protección de las comunicaciones, no se permite el uso de algoritmos de cifra no recomendados por el CCN, lo cual descarta el uso de TKIP (dado que RC4, que forma parte de dicho estándar, no es un algoritmo de cifra confiable). Se debe implementar, por lo tanto, el estándar WPA2 con AES-CCMP.

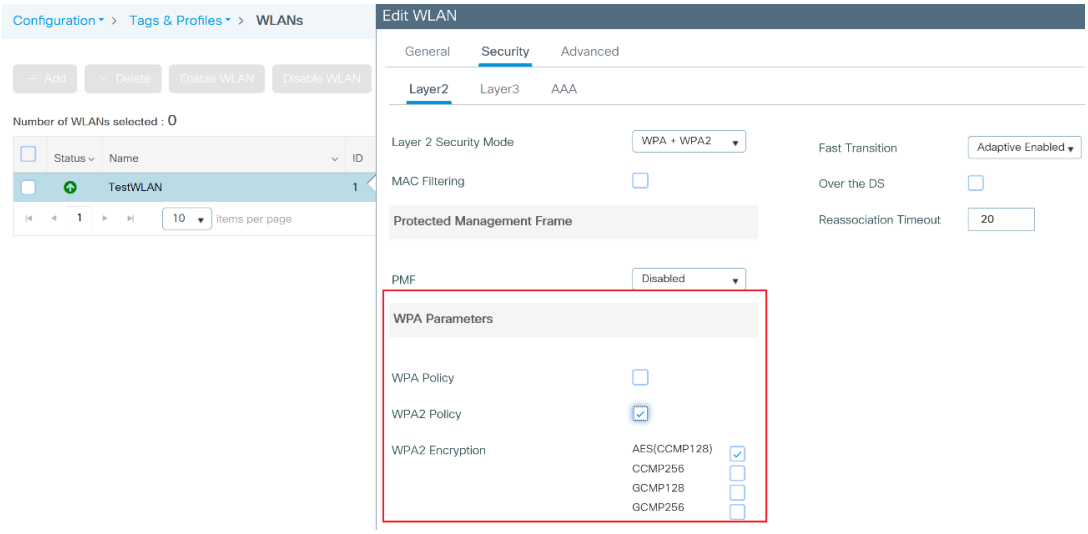


Ilustración 56. Configuración de WPA2 + AES

7.3.2 MECANISMOS DE AUTENTICACIÓN EN MODO 802.1X/EAP

178. Es el método de autenticación más seguro, ya que permite un proceso explícito de autenticación mutua, en la que cada cliente dispondrá de sus propias credenciales de acceso, proporcionando trazabilidad. Sin embargo, es un método más complejo, y que requiere de una infraestructura de servidores de autenticación (AAA).

179. En el caso de configurarlo en un dispositivo Cisco Catalyst 9800, están disponibles todos los métodos clásicos de autenticación, incluyendo PAP, CHAP, MS-CHAP, PEAP, EAP-TTLS o FAST (propietario de Cisco).

180. **Se debe utilizar el mecanismo de autenticación más fuerte, EAP-TLS**. Para este tipo de autenticación, es necesario contar con una infraestructura que permita generar los certificados de cliente y servidor (PKI), así como de bases de datos para almacenar dichas credenciales, como podrían ser un LDAP, un Directorio Activo o cualquier otro tipo de base de datos.

181. La arquitectura de seguridad en un escenario de estas características se puede definir a continuación:

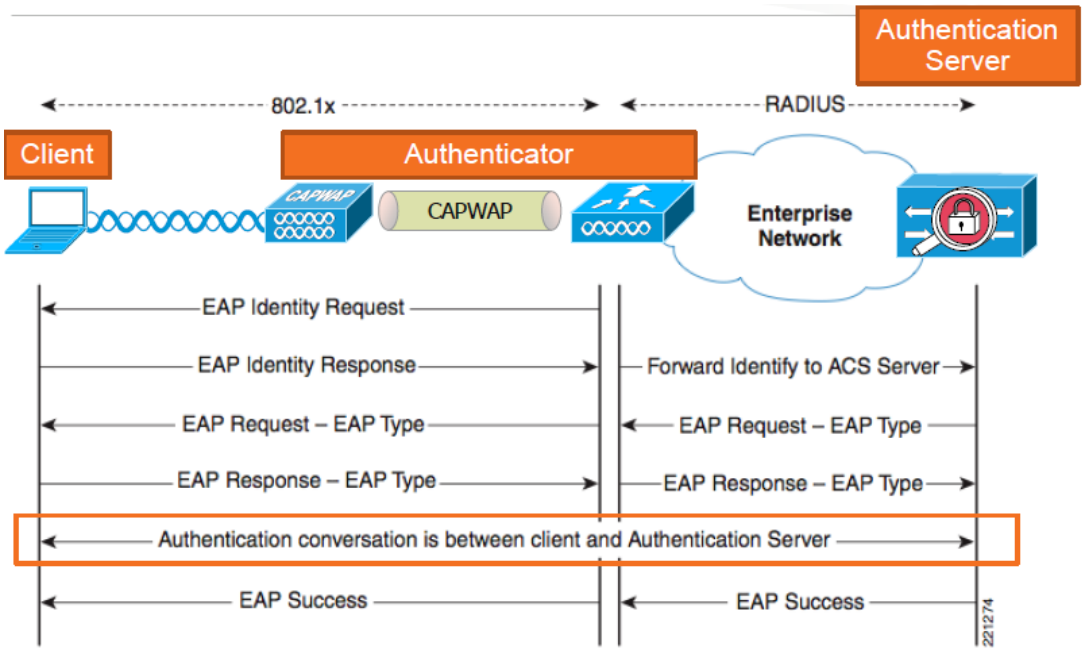


Ilustración 57. Escenario de autenticación EAP

182. En este caso concreto, únicamente se va a proporcionar la configuración relacionada con el elemento autenticador, que sería el controlador inalámbrico Catalyst 9800. Se considera que el resto de elementos (suplicante y servidores de autenticación) están configurados de acuerdo a las recomendaciones especificadas en las guías de seguridad de redes inalámbricas (CCN-STIC-816 y guías relacionadas con la misma).

183. El principal elemento a configurar en este escenario es la definición de los servidores de autenticación, tanto para Autorización como para Registro de los procesos de autenticación. Esto se configura dentro de *Configuration->Security->AAA->Server/Groups->RADIUS->Server->Add…*

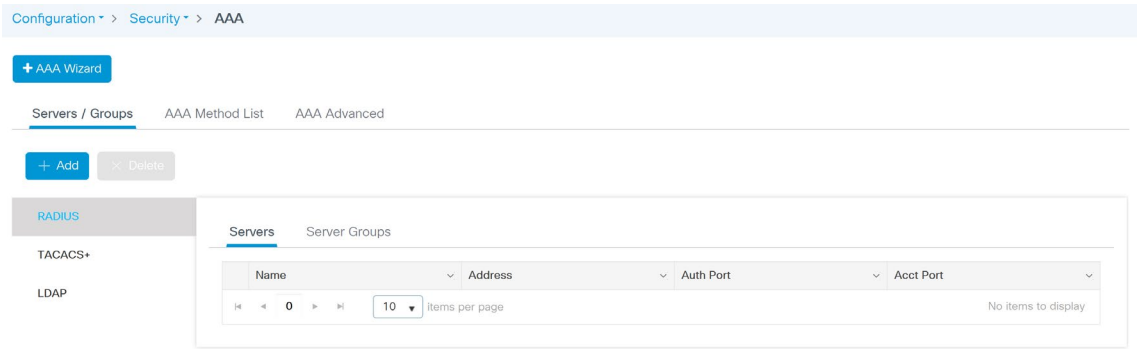


Ilustración 58. Creación de un nuevo servidor de autenticación

184. Dentro el servidor de autenticación, es necesario definir:

- Su nombre identificativo.
- Su IP.
- Si se desea usar un sistema PAC (*Protected Access Credentials*) de autenticación/autorización con el servidor RADIUS, dentro de un sistema

TrustSec. En caso de ser un servidor que no soporte dicha funcionalidad, se recomienda no habilitar esta opción.

- Su clave compartida con el RADIUS (para la validación de los mensajes de autenticación).
- El puerto que se va a usar en UDP para la conexión con el servidor de AAA para los paquetes de autorización (*Authorization*).
- El puerto que se va a usar en UDP para la conexión con el servidor de AAA para los paquetes de contabilización (*Accounting*).
- El tiempo de inactividad tras el cual se categoriza el intento de conexión al servidor RADIUS como no disponible (*Server Timeout*).
- El número de veces que se realizan reintentos de conexión, antes de determinar al servidor RADIUS como no utilizable, y pasar al siguiente miembro del grupo (en caso de haberlo).
- Si permitirá CoA (*Change of Authentication*), lo cual permitiría cerrar una sesión de manera externa, en lugar de esperar a que se cierre por finalización del tiempo de sesión.
- Finalmente, se crea pulsando el botón de *Apply to Device*.

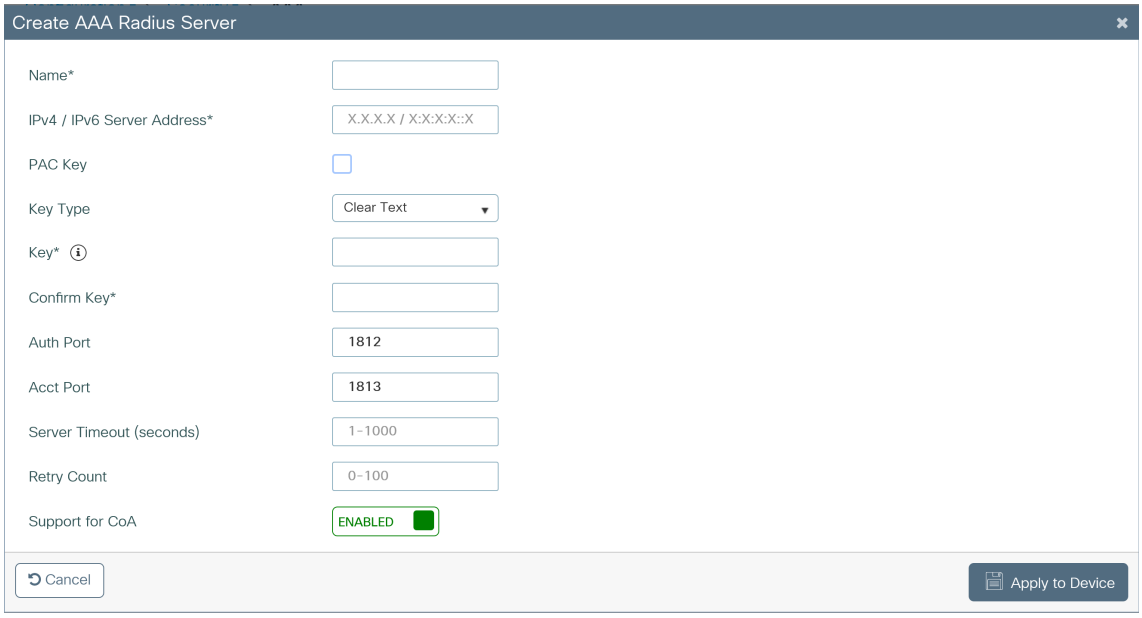


Ilustración 59. Configuración del nuevo servidor de autenticación

185. Tras definir el servidor RADIUS, es necesario incorporarlo a un grupo (aunque se trate de un único servidor). Se realiza dentro de *Configuration->Security->AAA->Server/Groups->RADIUS->Server Groups->Add…*

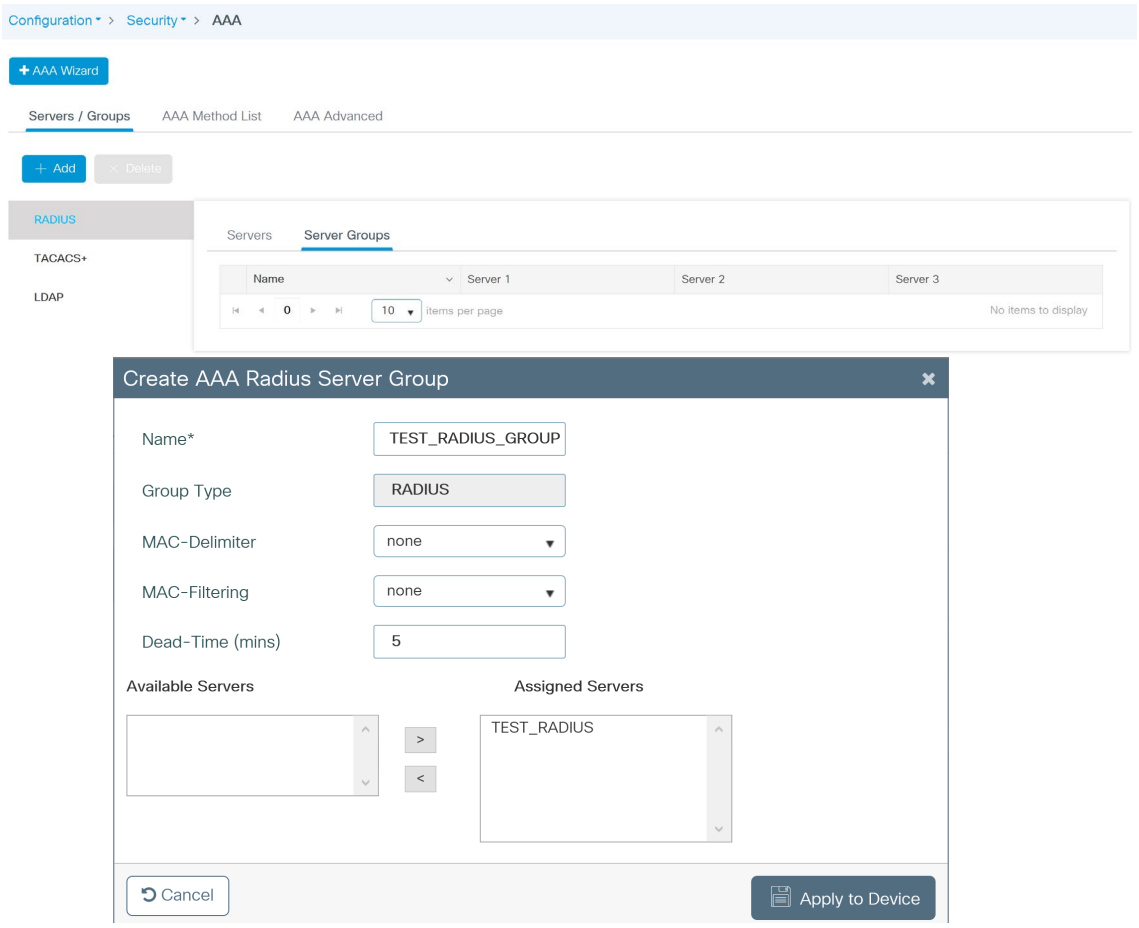
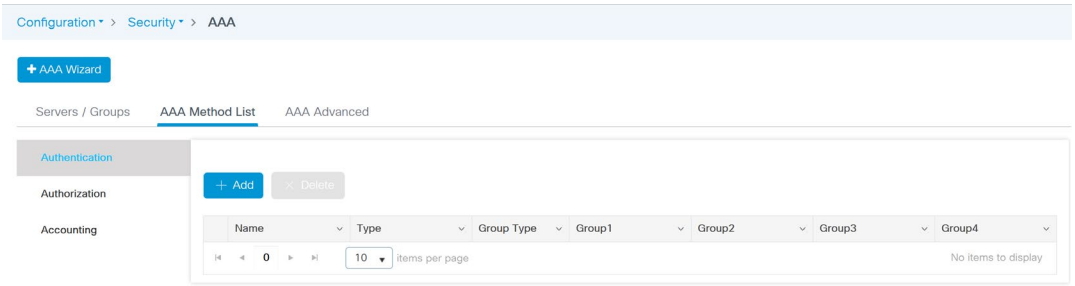


Ilustración 60. Configuración del nuevo grupo de servidores de autenticación

186. El siguiente paso sería definir un método de autenticación que incorpore este grupo de servidor/servidores RADIUS, tras lo cual, ya puede ser configurado dentro del perfil de WLAN. Esta acción se realiza dentro de *Configuration->Security->AAA->AAA Method List->Authentication->Add…*, configurando el método de autenticación como "dot1x", y añadiendo el grupo de servidores.



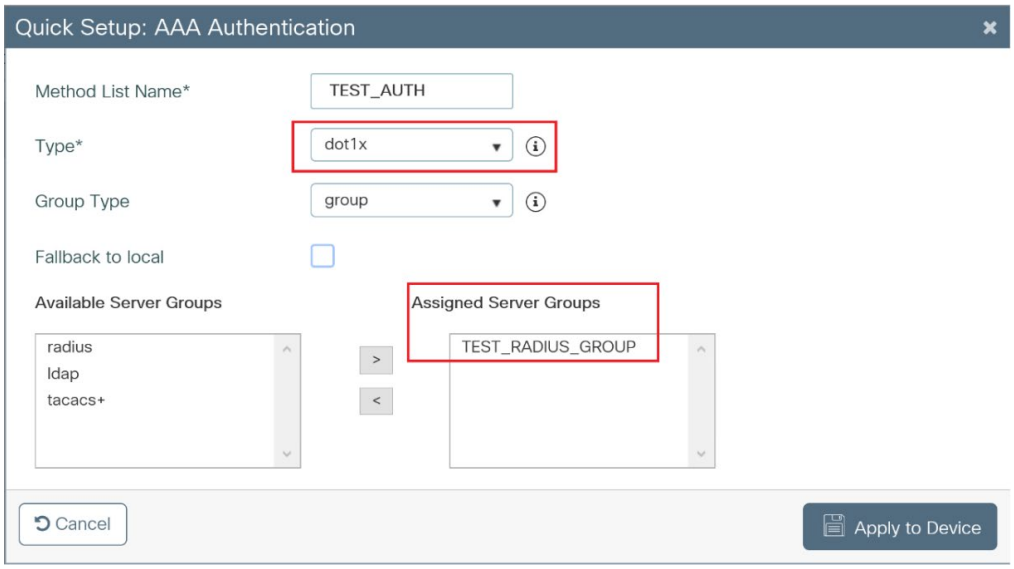


Ilustración 61. Configuración del nuevo grupo de servidores de autenticación

187. Una vez definido, el siguiente paso es incorporarlo a la política de seguridad del SSID radiado que utiliza el protocolo EAP-TLS. Para ello, se debe definir como política de nivel 2 de seguridad *WPA+WPA2* y tipo de gestión de claves 802.1X dentro del SSID en concreto. Esto se realiza dentro de *Configuration->Tags&Profiles->WLANs->Security->Layer2.*

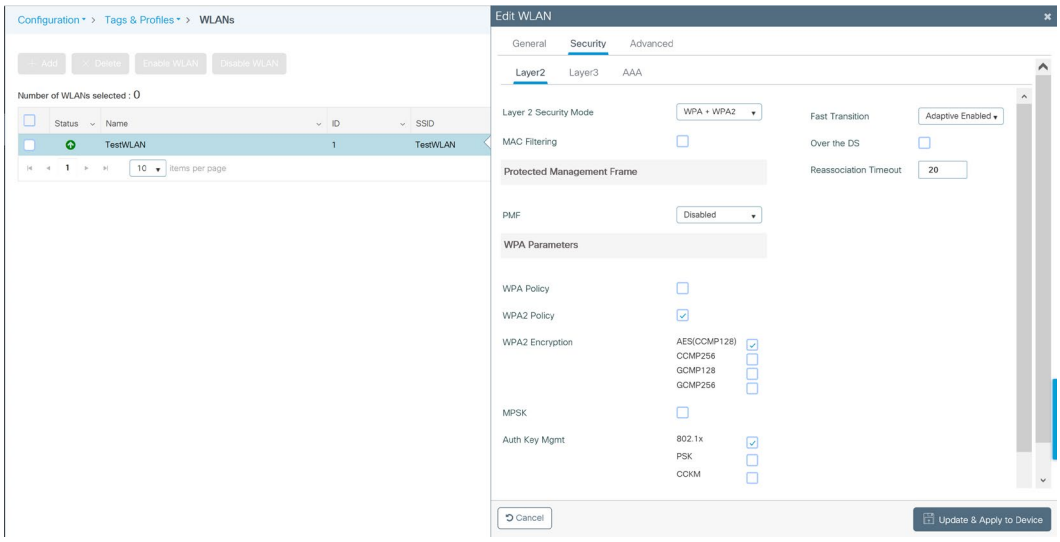


Ilustración 62. Configuración del SSID para uso de EAP-TLS

188. Dicha configuración no es válida únicamente para EAP-TLS, sino que es válida para cualquiera de los principales métodos EAP compuestos, de entre los que podemos destacar EAP-PEAP y EAP-TTLS.

189. Por último, dentro de la misma pestaña, pero en la sección de *Security->AAA Servers*, ya es posible seleccionar el método de autenticación previamente definido. Para aplicarlo, se debe pulsar en el botón *Update & Apply to device*.

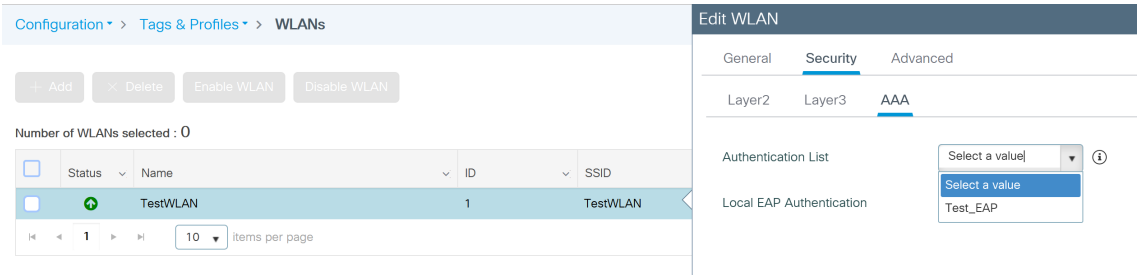


Ilustración 63. Definición del método de autenticación a usar en EAP-TLS

7.3.3 MECANISMOS DE DETECCIÓN DE INTRUSIÓN (WIDS)

190. En caso de que la categoría del sistema bajo el alcance del ENS sea MEDIA o ALTA, es requisito que la monitorización de la seguridad se lleve a cabo de manera automática a través de sistemas inalámbricos de detección y prevención de intrusos (WIDS), tal y como se recomienda en la guía CCN-STIC-816 Apdo. 5.2.7.

191. En un controlador inalámbrico Cisco Catalyst 9800, es posible habilitar el uso de este tipo de protecciones a partir de la versión 17.4.X, tanto desde el CLI como desde el GUI. En caso de que se quiera utilizar la interfaz gráfica, es necesario disponer de un orquestador DNA Center, pero usando el CLI, es posible habilitar y monitorizar las alarmas derivadas de esta herramienta.

192. La funcionalidad en esta familia de controladores se denomina aWIPS (Advanced WIPS), y tiene las siguientes funcionalidades:

    - Repositorio de firmas estáticas.
    - Detección de firmas autónoma.
    - Alarmas.
    - Paquete de ficheros de firmas estáticas para firmware de controlador y de AP.

193. Es importante destacar que para poder usar la funcionalidad de aWIPS, el equipo debe estar funcionando en modo FIPS, con todas las implicaciones a nivel de seguridad que ello conlleva.

194. El controlador Cisco Catalyst 9800 agrupa las firmas en 10 grandes grupos, que reflejan los tipos de ataques más frecuentes en entornos inalámbricos:

    - Authentication flood.
    - Association flood.
    - CTS Flood.
    - RTS Flood.
    - Broadcast probe.
    - Disassociation flood.
    - Disassociation broadcast.
    - Deauthentication flood.
    - Deauthentication broadcast.
    - EAPOL logoff flood.

195. **Se debe habilitar la funcionalidad de aWIPS** en un perfil de AP ya existente, de modo que se inyecte la funcionalidad en todos los APs asociados a dicho perfil:

```
#configure terminal
#ap profile mi_perfil_AP
```

```
#awips
```

196. Es posible verificar el estado del aWIPS en un AP concreto:

```
# show awips status radio_mac

AP Radio MAC    AWIPS Status                Forensic capture Status
Alarms

-------------------------------------------------------------------------
---------------------------------------

0xx7.8xx8.2xx0      ENABLED          CONFIG_NOT_ENABLED   14691
```

197. Para ver detalles de una firma específica, es posible mediante el siguiente comando de CLI:

```
# show awips alarm signature signature_id

AP Radio MAC    Source/Dest MAC          AlarmID           Timestamp
SignatureID    Alarm Description     Message Index

-------------------------------------------------------------------------
-------------------------------------------------------------------------
------------------

0xx7.8xx8.2xx0      0023.6xx0.2xxb          1714        11/02/2020
13:02:19  100001        Authentication Flood   3966
```

198. Para ver información detallada de las alarmas:

```
# show awips alarm detailed

AP Radio MAC    Source/Dest MAC          AlarmID           Timestamp
SignatureID    Alarm Description     Message Index

-------------------------------------------------------------------------
-------------------------------------------------------------------------
------------------

0xx7.8xx8.2xx0      0xx3.6xx0.235b          1714        11/02/2020
13:02:19  100001        Authentication Flood   3966

0xx7.8xx8.2xx0      0xx4.dxxc.f3cc          1714        11/02/2020
13:02:19  100001        Authentication Flood   3971

…….

0xx7.8xx8.2xx0      0xx3.6xx0.235b          1715        11/02/2020
13:02:20  100001        Authentication Flood   3982

0xx7.8xx8.2xx0      0xx4.dxxc.f3cc          1715        11/02/2020
13:02:20  100001        Authentication Flood   3987
```

7.3.4 INTERCONEXIÓN ENTRE PUNTOS DE ACCESO Y CONTROLADORA

7.3.4.1 SEGURIDAD EN LA CONEXIÓN

199. Los controladores inalámbricos Cisco Catalyst 9800 en todas sus versiones utilizan el protocolo CAPWAP (*Control and Provisioning of Wireless Access Points*), estándar del IETF, para la comunicación entre el punto de acceso y el controlador.

200. Dentro de dicho estándar, se especifica el protocolo DTLS como sistema de cifrado para los paquetes que se intercambian el punto de acceso y el controlador. En el caso del plano de datos, el cifrado es obligatorio, mientras que, en el plano de datos, es opcional. Para el uso de los algoritmos de cifrado DTLS, es necesario que la *Smart Account* asociada al controlador tenga el control de exportaciones habilitado (*Export-Controlled Functionality enabled*).

201. Se debe activar el cifrado en la comunicación del plano de datos. Para ello, se debe acceder a *Configuration->Tags&Profiles->AP Join->CAPWAP->Advanced*:

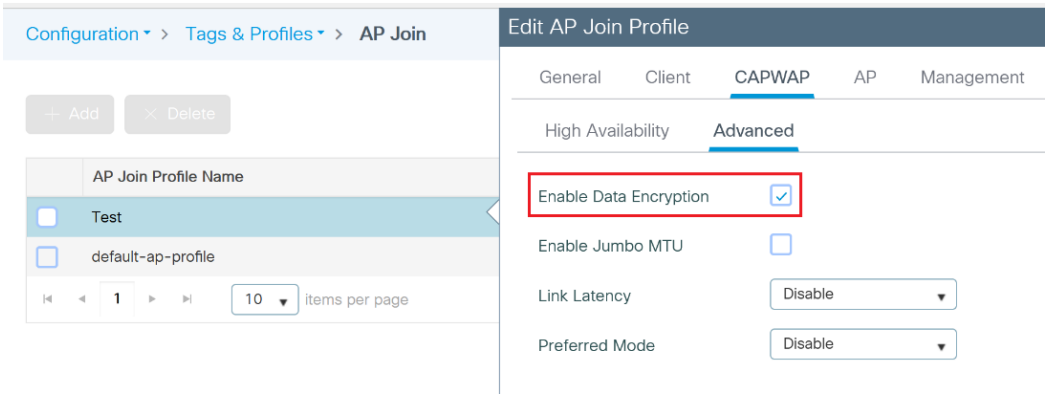


Ilustración 64.Activación del cifrado en el plano de datos

202. Para utilizar suites de cifrado y modos DTLS más seguros, los controladores usan el modo FIPS. Más información, en el apartado 7.3.5 correspondiente a la configuración en modo FIPS del dispositivo.

203. Para DTLS se recomienda activar DTLS v1.2, siempre y cuando el punto de acceso y la versión de firmware lo permitan. Esta recomendación es la ofrecida en los *Common Criteria* de Cisco para el cumplimiento de los estándares FIPS.

204. Dado que todos los puntos de acceso cualificados corresponden al grupo de Cisco AP Wave 2, todos los APs pertenecientes a dicho grupo lo permiten. Para poder usar DTLS v1.2, la versión de firmware debe ser igual o superior a la 16.12. Es posible configurar DTLS v1.2 como mínimo algoritmo permitido de cifrado mediante el siguiente comando de CLI:

```
#configure terminal
#wireless wlancc
#ap dtls-version  dtls_1_2
```

205. También es posible fijar la suite de cifrado dentro del algoritmo DTLS entre el AP y el controlador, mediante el siguiente comando:

```
9800(config)#ap dtls-cipher ?
  AES128-SHA                    Configure
TLS_RSA_WITH_AES_128_CBC_SHA
  DHE-RSA-AES128-SHA            Configure
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  DHE-RSA-AES256-SHA            Configure
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

```
  DHE-RSA-AES256-SHA256          Configure
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256  Configure

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  ECDHE-ECDSA-AES256-GCM-SHA384  Configure

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  ECDHE-RSA-AES128-GCM-SHA256    Configure
                                 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  default                        Configure default cipher(s)
```

206. En negrita aparecen los recomendados (R) en la guía CCN-STIC-807 en su apartado de TLS v1.2.

207. Por último, es posible mostrar el resumen de las suites de cifrado utilizadas entre cada AP y controlador mediante el siguiente comando CLI:

```
#sho wireless dtls connections
AP Name                  Local Port     Peer IP       Peer Port
Version     Ciphersuite
-------------------------------------------------------------------------
-------------------
Aud_1                    Capwap_Ctrl    192.168.40.156 5264
DTLSv1.2    TLS_NUM_RSA_WITH_AES_128_CBC_SHA
Aud_2                    Capwap_Ctrl    192.168.40.160 5272
DTLSv1.2    TLS_NUM_RSA_WITH_AES_128_CBC_SHA
Pab1_D8                  Capwap_Ctrl    192.168.40.175 64214
DTLSv1.0    TLS_NUM_RSA_WITH_AES_128_CBC_SHA
Pab1_E7                  Capwap_Ctrl    192.168.40.208 5273
DTLSv1.2    TLS_NUM_RSA_WITH_AES_128_CBC_SHA
Pab1_F8                  Capwap_Ctrl    192.168.40.191 5268
DTLSv1.2    TLS_NUM_RSA_WITH_AES_128_CBC_SHA
Aud_1_S1                 Capwap_Ctrl    192.168.40.154 5256
DTLSv1.2    TLS_NUM_RSA_WITH_AES_128_CBC_SHA
Aud_1_S2                 Capwap_Ctrl    192.168.40.203 5273
DTLSv1.2    TLS_NUM_RSA_WITH_AES_128_CBC_SHA
Aud_1_S3                 Capwap_Ctrl    192.168.40.206 5278
DTLSv1.2    TLS_NUM_RSA_WITH_AES_128_CBC_SHA
Aud_2_S1                 Capwap_Ctrl    192.168.40.158 5264
DTLSv1.2    TLS_NUM_RSA_WITH_AES_128_CBC_SHA
```

7.3.4.2 REGISTRO DE PUNTOS DE ACCESO EN EL SISTEMA

208. Si los puntos de acceso y el controlador negocian una sesión DTLS exitosa (acordando una suite de cifrado común, y con certificados integrados en el equipo válidos), el siguiente elemento es el registro del punto de acceso en el controlador.

209. Por motivos de seguridad se recomienda que únicamente los puntos de acceso que pertenecen a la infraestructura sean capaces de asociarse al controlador inalámbrico, para evitar que puntos de acceso no autorizados puedan extender la red inalámbrica más allá de las ubicaciones predefinidas en la arquitectura de seguridad.

210. Sirva como ejemplo, en redes Mesh, donde los puntos de acceso se asocian a través del aire con puntos de acceso pertenecientes a la red. Si un atacante emplea un punto de acceso para conectarse a la red vía Mesh, desde el propio punto de acceso tendría capacidad para intentar realizar diversos ataques u obtener información sensible. Es por esto que los puntos de acceso que se asocien al controlador deben estar legitimados de alguna manera.

211. Durante el proceso de registro, los puntos de acceso y el controlador se autentican mutuamente a través de certificados X.509 como base para la negociación de la sesión DTLS anteriormente mencionada, que son incorporados en los equipos de forma permanente en una memoria protegida. Todos los equipos *hardware* disponen de MIC desde 2005 (*Manufacturing Installed Certificates*), mientras que los equipos virtuales, como podría ser el Catalyst 9800 en formato virtual disponen de SSC (*Self Signed Certificate*).

212. Por tanto, existen varias maneras de asegurar que los puntos de acceso y los controladores de la infraestructura se encuentran autenticados entre sí:

    - Comprobación contra una lista interna de direcciones MAC de puntos de acceso, con lo cual sólo los APs que tengan estas direcciones MAC podrán registrarse.
    - Usando los certificados SSC (únicamente posible en controladoras virtuales) y desplegándolos en los puntos de acceso.
    - Usando los LSC (*Locally Significant Certificates*), que implicaría usar una CA externa para cargar certificados firmados X.509 tanto en la controladora como en los puntos de acceso.

213. En el escenario de lista interna, además de esta autenticación mutua mediante los certificados implicados, los controladores restringen el acceso de APs basándose en la MAC de los mismos. La falta de una contraseña segura debido al uso de la MAC como método de validación no es un problema debido a que el controlador autentica los APs mediante los certificados MIC como paso previo a la autorización. El uso de MIC favorece una autenticación segura.

214. El escenario de certificados autofirmados (*Self Signed Certificates*) solo es posible cuando la controladora Catalyst 9800 se encuentra en formato virtual, no como *appliance*, por lo que, al ser un escenario muy concreto, no se va a detallar en el presente documento.

215. Por último, el caso de uso de certificados localmente significativos (*Locally Significant Certificates*) depende de la presencia de una infraestructura de PKI (*Public Key Infraestructure*) para la generación y firma de los mismos, que luego posteriormente pueden ser instalados tanto en puntos de acceso como en los controladores. De este

modo, en lugar de usar certificados propios, como los SSC o MIC, se utilizarían los generados y validados por la PKI de la organización, o una de terceros.

216. Dado que el ejemplo de uso de SSC está restringido a la versión virtual de la controladora, y que el uso de LSC depende de una infraestructura de PKI, se describe a continuación el caso de uso de control de acceso por MAC del AP, dado que presenta un escenario con un adecuado nivel de seguridad (validación mutua, verificación de *hash* de certificados) sin requerir de infraestructura adicional.

7.3.4.2.1 EJEMPLO: AUTENTICACIÓN DE PUNTOS MEDIANTE LISTA DE AUTORIZACIÓN

217. El primer paso sería la creación de una lista local de autorización, en el menú *Configuration->Security->AAA->AAA Method List->Authoriztation-> Add.* El tipo debe ser "*credential-download*" y el tipo de grupo debe ser "*local*".

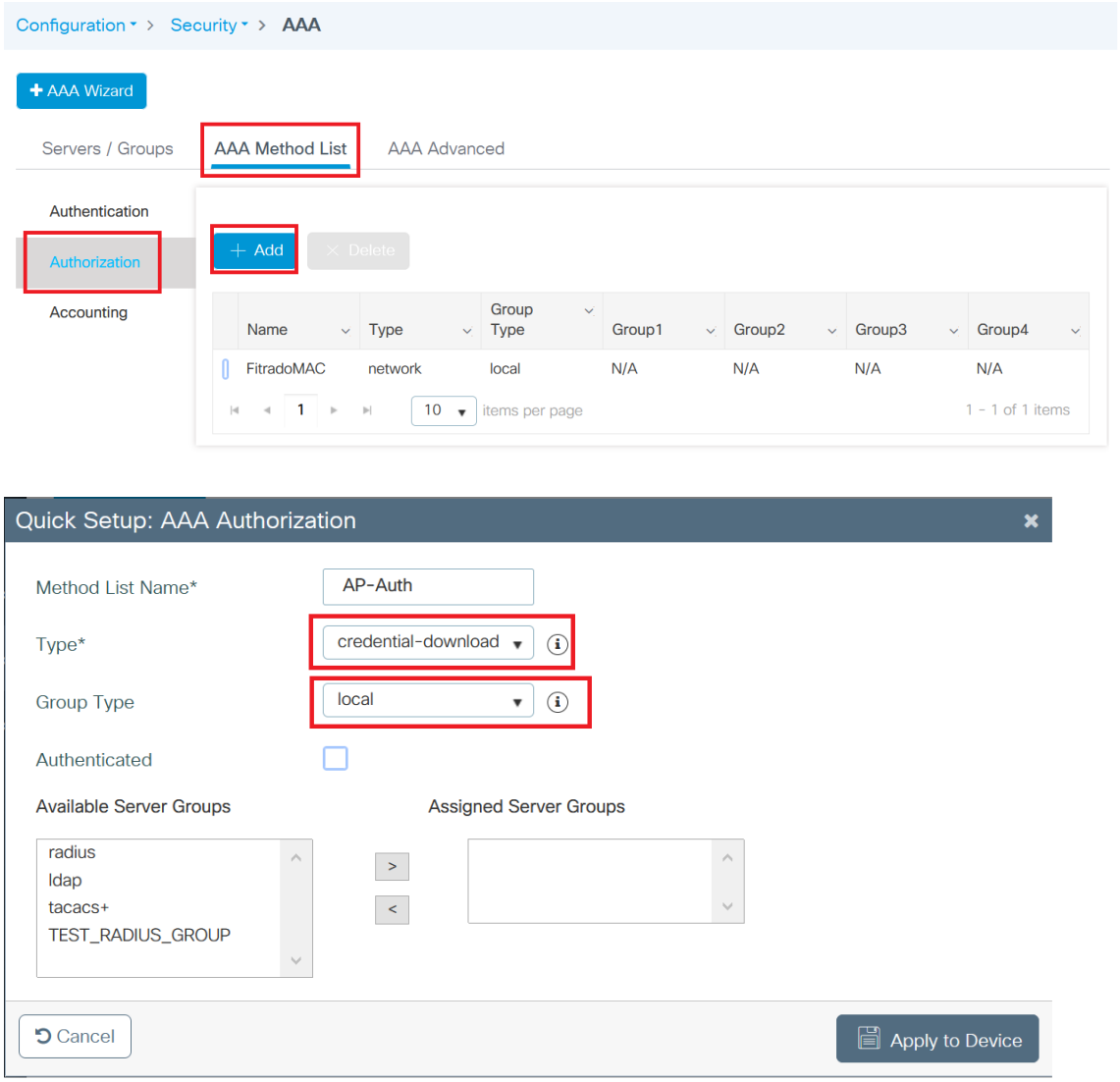


Ilustración 65. Creación de lista de autorización para AP de tipo local

218. Para habilitar la autenticación de MAC a nivel de AP: *Configuration->Security->AAA->Advanced->AP Policy* y habilitar la autorización de MAC contra la lista creada anteriormente.

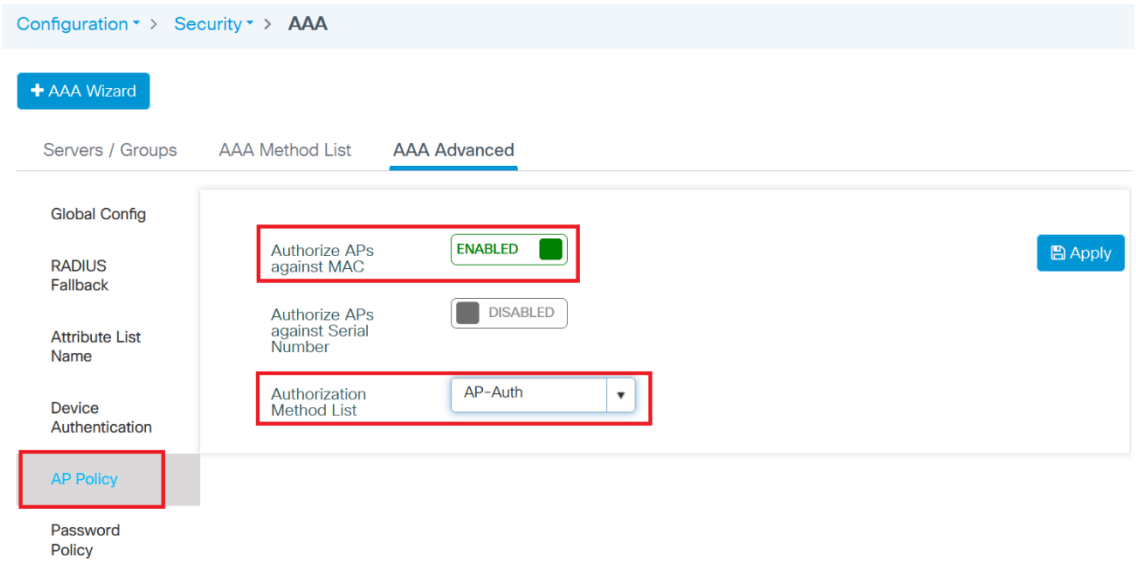


Ilustración 66. Habilitación de registro de AP mediante lista de autorización local

219. Por último, se van añadiendo las direcciones MAC de los dispositivos autorizados en el menú de autenticación de dispositivos: *Configuration->Security->AAA->AAA Advanced -> Device Authentication->MAC Address-> Add.*

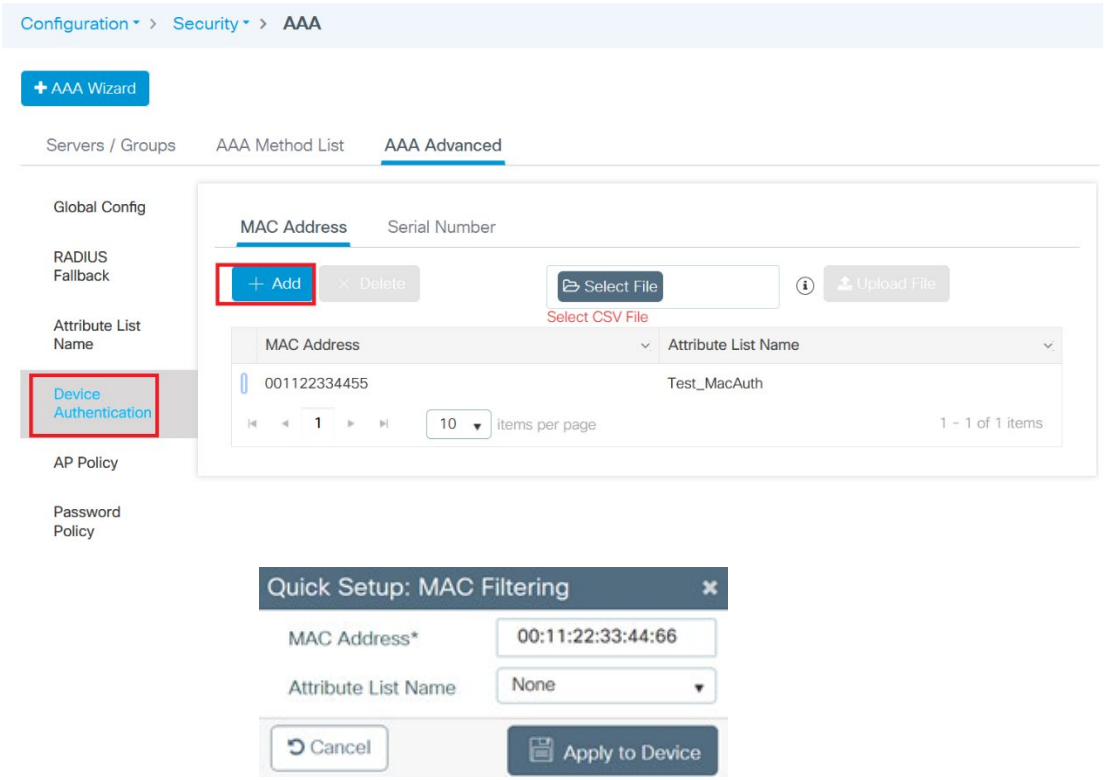


Ilustración 67. Políticas de autorización de registro de puntos de acceso

220. Una vez introducida la MAC deseada y el certificado correcto, se debe pulsar sobre el botón *"Apply to Device"*. La MAC del AP deseado debe aparecer dentro de la lista de autorización de dispositivos:

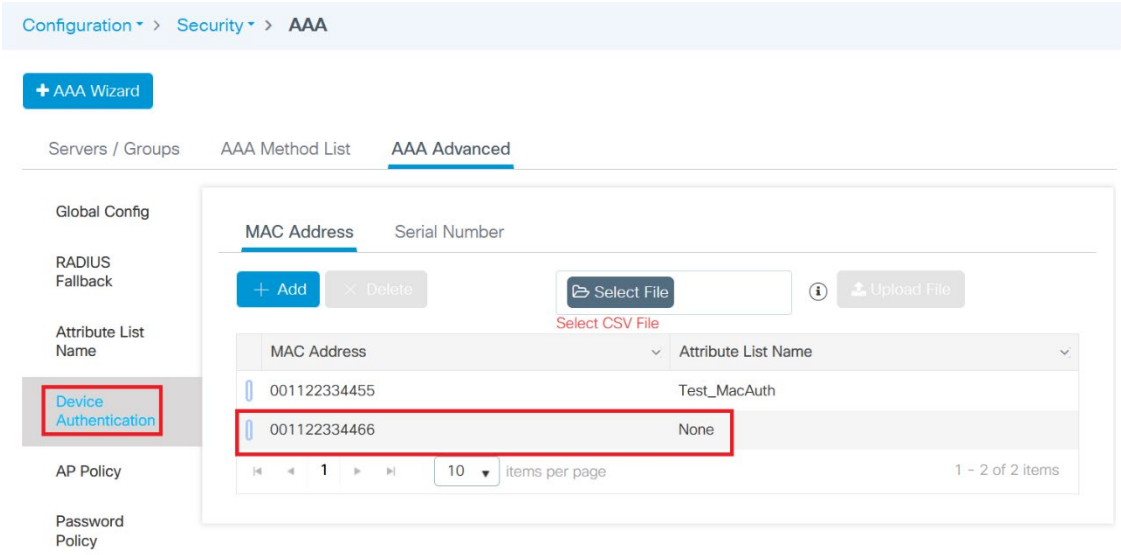


Ilustración 68. Instalación del AP en la lista

221. Para verificar la autorización de puntos de acceso mediante lista, es necesario:

- Punto de acceso cuya MAC esté dada de alta en la lista de autorización.
- Conectividad entre el punto de acceso y el controlador inalámbrico.
- Acceso a la consola del controlador inalámbrico.

222. Aspectos a verificar en el *debug*:

- No hay derivación temporal entre el AP y el controlador.
- El nivel de *debug* es el deseado.
- La MAC sobre la que se desea realizar el *debug* está habilitada como MAC a trazar.

223. En la consola del controlador, introducir los siguientes comandos:

```
c9800-01#show clock

c9800-01#show debugging

c9800-01# show logging profile wireless filter mac 00:11:22:33:44:66
to-file bootflash:example01.txt

Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds

executing cmd on chassis 1 ...

Files being merged in the background, result will be in
bootflash:example01.txt log file.

Collecting files on current[1] chassis.

# of files collected = 1

btrace decoder: [1] number of files, [2107] number of messages

will be processed. Use CTRL+SHIFT+6 to break.

2021-04-05 16:10:16.082 - btrace decoder processed 47%

2021-04-05 16:10:16.087 - btrace decoder processed 94%
```

```
2021-04-05 16:10:16.088 - btrace decoder processed 100%
```

224. El resultado del *debug* queda almacenado en el fichero *bootflash:example01.txt*.

7.3.5 MODO FIPS Y RESTRICCIONES EN LOS ALGORITMOS

225. La controladora Cisco 9800-WLC puede operar tanto en modo FIPS como en modo no-FIPS. En este último modo, se pueden utilizar ciertas versiones de algoritmos de cifrado, tamaños de clave y modos de operación no recomendados para un entorno criptográfico seguro. Por tanto, en un entorno de operación seguro es recomendable habilitar el modo FIPS para que se realicen el mayor número de auto chequeos criptográficos en el arranque, y la operación en modo seguro de la unidad sea lo más efectiva posible.

226. Los modos que están recomendados en modo FIPS son los siguientes:

- SSH:version 2
- ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group16-sha512
- cifrados aes128-ctr aes192-ctr aes256-ctr (con HMAC-SHA2)
- ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521

  x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp521
- hmac-sha2-512, hmac-sha2-256
- TLS v1.2, principalmente para el servidor HTTPS interno.

```
c9800-01(config)#  ip http secure-server
c9800-01(config)# ip http secure-trustpoint <Truspoint usado para la carga del certificado interno>
c9800-01(config)# ip https tls-version tlsv1.2
```

- DTLS v1.2 para el túnel de cifrado CAPWAP.

```
c9800-01(config)# wireless wlancc
c9800-01(config)# ap dtls-version  dtls_1_2
```

- SNMPv3 (Server Group con en modo AuthPriv, comentado en el apartado **6.2.3** correspondiente a SNMPv3).
- Para ciertos modos de operación (SD-Access, ISAKMP) la longitud mínima de clave debe ser de 14 caracteres.
- Habilitar el cifrado del plano de datos en el túnel CAPWAP, que no viene cifrado por defecto (sí que viene cifrado siempre el plano de control).

```
c9800-01# sh ap sum
c9800-01# conf t
c9800-01(config)# ap profile <ap profile en uso>
c9800-01(config)# link-encryption
```

```
Enabling link-encryption globally will reboot the APs with
no link-encryption. Are you sure you want to continue?
(y/n)[y]: y
```

227. Además, para cumplir este modo de funcionamiento, será necesario:

    Deshabilitar Telnet.

    Deshabilitar SNMPv1 y SNMPv2. Solo se permite SHA para autenticación y AES para privacidad en SNMPv3.

    Borrar todas las claves SSH RSA1.

228. Para habilitar el modo, se usa el comando "**fips mode enable**", y se requiere de un reinicio.

```
c9800-01(config)# fips-authorization key <clave hexadecimal
de 32 caracteres>

c9800-01(config)# platform ipsec fips-mode
```

229. Cuando el sistema arranca en modo FIPS, el módulo criptográfico realiza una serie de chequeos en el arranque. El sistema sólo pasa a modo FIPS si se superan todos estos auto-chequeos. Si cualquiera de los chequeos fallara, el sistema registra un mensaje de log y pasa a estado de error.

230. El auto test criptográfico en el arranque incluye los siguientes apartados:

    - *Known Answer Tests*: el dispositivo utiliza un algoritmo criptográfico de respuesta conocida (*Known Answer Test*, KAT), para cada una de las funciones criptográficas aprobadas en el estándar FIPS 140-2 (cifrado, descifrado, autenticación y generación de números aleatoria).
    - *Conditional Self-Tests* (se ejecutan periódicamente durante la ejecución normal del sistema, cada vez que una función de seguridad que lo puede utilizar es invocada):
    - *Continuous Random Number Generator* .
    - *Pairwise Consistency Test*, que se ejecuta cuando un par clave pública-clave privada es generado.
    - Bypass Test, para asegurar que el texto cifrado nunca es mostrado en claro

231. En el diseño de la seguridad de la red inalámbrica debe tenerse en cuenta cómo esta red puede afectar a otras redes con las que se tenga conexión (como, por ejemplo, la red cableada de la organización), tal y como se indica en el requisito expresado en la guía CCN-STIC-816 Apdo. 5.3.1.

7.3.6 SEGREGACIÓN DE REDES Y ASIGNACIÓN AL ESPACIO INALÁMBRICO

232. En el diseño de la seguridad de la red inalámbrica debe tenerse en cuenta cómo esta red puede afectar a otras redes con las que se tenga conexión (como, por ejemplo, la red cableada de la organización), tal y como se indica en el requisito expresado en la guía CCN-STIC-816 Apdo. 5.3.1.

233. En el caso de una implantación de categoría BÁSICA o MEDIA, la red deberá estar segmentada en caso de que existan diferentes dominios de seguridad. Como ejemplo, el

caso de que exista un dominio inalámbrico para usuarios corporativos internos, y otro diferente para usuarios invitados (personal externo a la organización).

234. Una práctica recomendable es segregar el tráfico de la red cableada a través de VLAN dedicadas. El uso de estas VLAN facilita la implementación de listas de control de acceso a la red, o su circulación a través de un dispositivo lógico o físico asegurado, donde se implementen las reglas de seguridad pertinentes.

235. En el caso de los controladores inalámbricos Cisco Catalyst 9800, es posible segregar el tráfico de cada red inalámbrica mediante VLANs, a través de la definición de perfiles (*Policy Profiles*) en el dispositivo. Estos perfiles luego podrán asociarse con una red inalámbrica concreta (SSID) mediante una etiqueta de perfil (*Profile Tag*). De este modo, todo el tráfico inalámbrico asociado a dicha SSID, irá etiquetado con la correspondiente etiqueta 802.1Q, con lo cual se podrá controlar el grado de difusión de la información en la red.

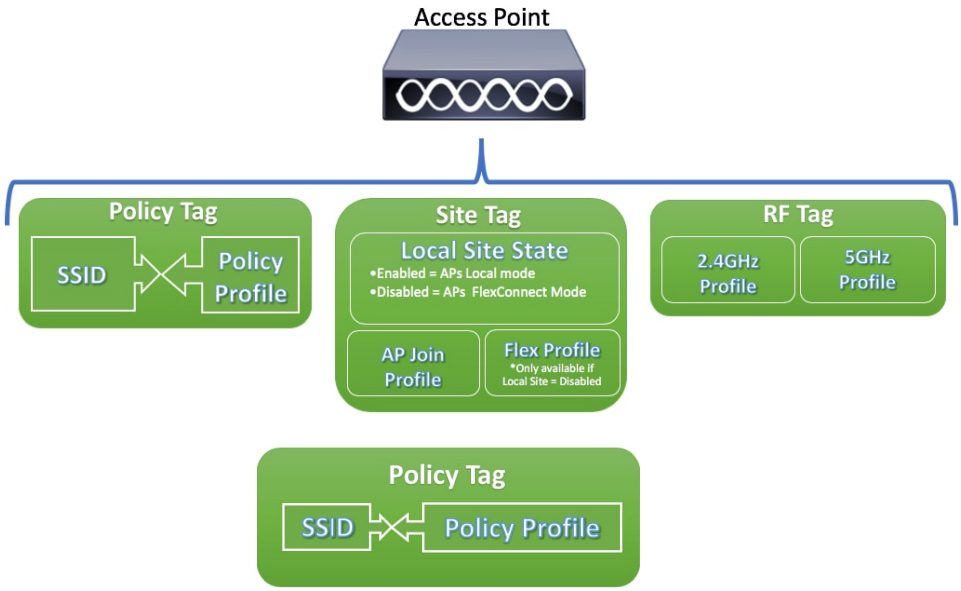


Ilustración 69. Asociación entre red radiada (SSID) y VLAN en el segmento cableado

236. Antes de que se pueda definir la VLAN dentro de un perfil (*Policy Profile*), es necesario indicarle al dispositivo:

- Las VLAN IDs de cliente y/o gestión disponibles en la red para la inyección del tráfico inalámbrico en el segmento cableado.
- Los niveles de agrupación de dichos VLAN IDs (es posible agruparlos para compartir características comunes (*VLAN Groups*).
- La disponibilidad de dichas etiquetas 802.1Q en el interfaz entre el controlador y la red cableada, o entre el punto de acceso y la red cableada, si se utiliza el modo de trabajo *FlexConnect*.

237. Para declarar el VLAN ID a utilizar (ya sea para tráfico de cliente o para tráfico de gestión), el primer paso es definirla dentro del grupo de VLANs utilizables por el equipo, en *Configuration->Layer 2->VLAN->Add..*

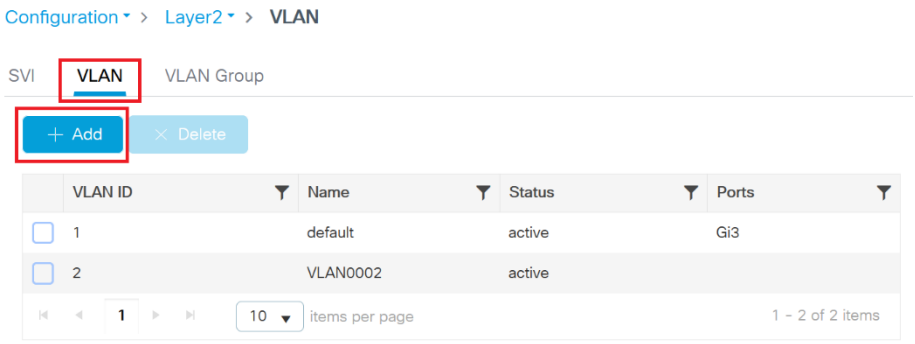


Ilustración 70. Adición de una nueva VLAN para su uso

238. Es necesario definir, al menos, el VLAN ID a utilizar. También es recomendable habilitar la VLAN (si se va a utilizar inmediatamente), y los interfaces por donde el controlador puede recibir/tratar dicha VLAN.

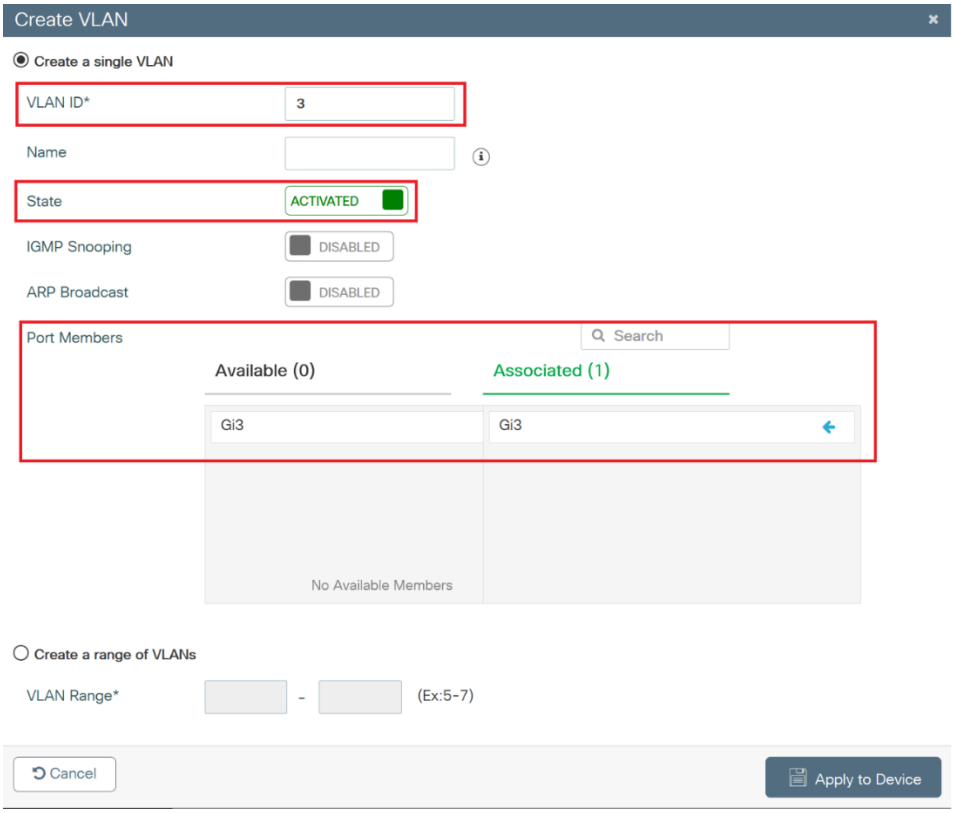


Ilustración 71. Definición de los parámetros de uso de la VLAN

239. Tras su definición, ya es posible utilizar la VLAN dentro de un perfil (*Policy Profile*), que más tarde será posible asociar al SSID correspondiente. Para ello, en *Configuration->Tags & Profiles->Policy* es posible crear uno nuevo, o editar uno ya existente. En la pestaña de "*Access Policies*" es posible invocar la VLAN anteriormente creada del menú *drop-down*.

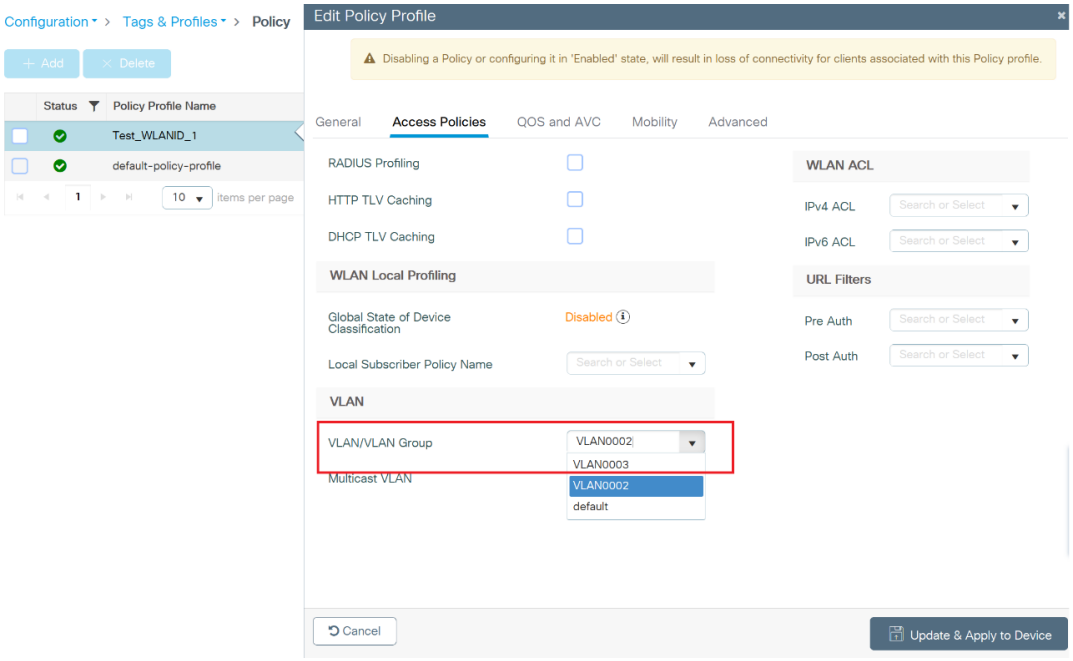


Ilustración 72. Configuración de una VLAN dentro de un perfil (Policy Profile)

240. Por último, la asociación de una red inalámbrica (SSID) existente y este perfil creado (*Policy Profile*) se realizará en una etiqueta de perfil (*Policy Tag Profile*), dentro de *Configuration->Tags&Profiles->Tags->Policy->Add…*

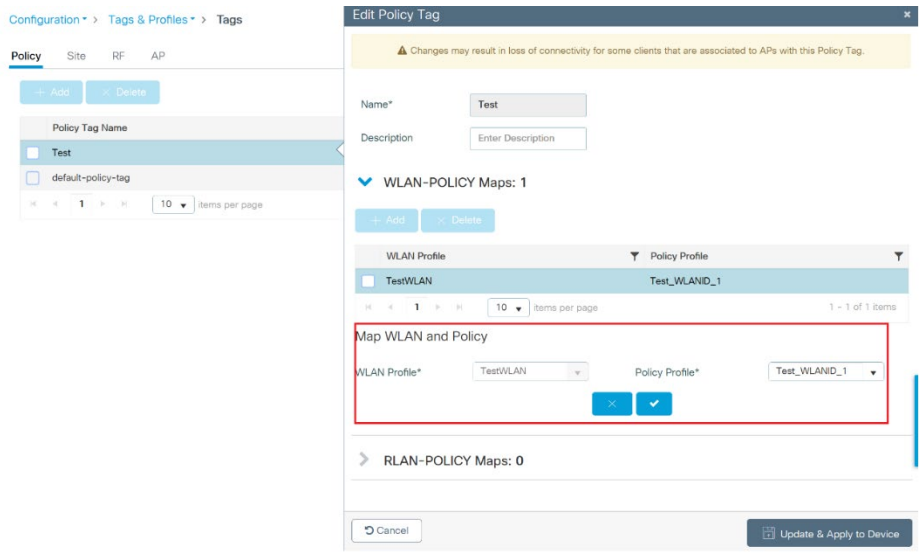


Ilustración 73. Asociación de un perfil a un SSID mediante una *Policy Tag*

8. LISTA DE COMPROBACIÓN

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto: - Fecha de entrega - Serigrafía y logo de Cisco embalaje - Embalaje sellado sin signos de haber sido manipulado - Localización etiqueta resistente a manipulaciones - Número y tipo de interfaces acorde al pedido - Concordancia número serie embalaje y dispositivo - Elementos incluidos por defecto en el embalaje	☐	☐	
Configuración inicial: - Ubicación segura del dispositivo (acceso y anclaje) - Verificación toma de corriente estabilizada - Cables de corriente y datos disponibles - Equipo seguro (navegador web, cliente SSH, consola) - Uso de CLI o Interfaz Web - Encendido del dispositivo comprobando que el LED de STATUS está encendido y con el color correcto tras arranque - Cuenta/s administrador/es del dispositivo - Verificación versión incorporada en el dispositivo - Verificación de las licencias incorporadas - Configuración de red interfaz de gestión	☐	☐	
GESTIÓN DEL DISPOSITIVO			
Habilitar protocolo seguro SSH y deshabilitar protocolo Telnet	☐	☐	
Incorporar certificados (gestión web, IPSec)	☐	☐	
Habilitar protocolo HTTPS y deshabilitar protocolo HTTP	☐	☐	
Mensaje de aviso en el inicio de sesión	☐	☐	
Configurar SNMP v3 y deshabilitar SNMP v1 y v2-v2c	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Configurar SNMP *traps receiver y* aplicar perfil IPSec	☐	☐	
Configurar *banner* de bienvenida	☐	☐	
Establecer tiempos máximos de sesiones	☐	☐	
Configurar política de contraseñas de usuarios (cifrado, longitud, etc)	☐	☐	
Configurar sincronización horaria	☐	☐	
LICENCIAMIENTO			
Limitar usuarios y orígenes que alcanzan el dispositivo	☐	☐	
Licenciamiento *Smart Licensing*: • *Direct Cloud*: Usar navegador web (obtener token) e interfaz web seguro del controlador • *Proxy – Transport Gateway*: Equipo seguro con Proxy de Cisco instalado e interfaz web seguro del controlador • *Smart Software Satellite*: Equipo seguro con este software instalado e interfaz web seguro del controlador	☐	☐	
MEDIDAS DE SEGURIDAD PARA INFRAESTRUCTURAS INALÁMBRICAS			
Ocultar SSID y/o declararlo con nombre no descriptivo relacionado con el servicio que presta	☐	☐	
Implementar filtrado MAC	☐	☐	
Habilitar registros y definir servidor de *Syslog*	☐	☐	
Habilitar tiempo máximo de sesión de usuario en la red	☐	☐	
Activar protección de tramas de gestión	☐	☐	
Definir algoritmo de cifrado por SSID WPA2: AES-CCMP	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Autenticación: - En modo 802.1X/EAP: Definir servidor/es AAA y método EAP-TLS.	☐	☐	
Habilitar mecanismos de detección e intrusión (WIDS) con revisiones periódicas para evitar falsos positivos o casos no detectados.	☐	☐	
Proteger la interconexión entre puntos de acceso y controladora: - Uso de CAPWAP para gestión (obligado cumplimiento) y cifrado DTLS para los datos (precaución según modelos controlador, puntos de acceso y problemas con clientes limitados en funciones criptográficas) - Limitar a los puntos de acceso de la infraestructura confiable la capacidad de asociarse al controlador inalámbrico (Lista interna del controlador inalámbrico o usando un servidor de autenticación)	☐	☐	
Segregar redes inalámbricas (configurar VLAN)	☐	☐	
GUARDADO DE CONFIGURACIÓN Y ACTUALIZACIÓN SOFTWARE			
Guardado de configuración: - Salvar la configuración internamente - Exportar la configuración a servidor externo (precaución con mantener activo el servidor externo una vez usado), y usar clave de cifrado del fichero.	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Actualizar *software*: - Uso navegador web seguro para consultar periódicamente posibles actualizaciones del fabricante y usar la versión recomendada por el mismo - Prestar atención a la "*Release Note*" de la versión que se desea instalar, en especial al "*upgrade path*" y a compatibilidad con la infraestructura existente. - Descargar versión deseada y comprobar que la firma SHA512 indicada por el fabricante coincide con el fichero descargado a través de un equipo confiable. - Salvar y extraer configuración del controlador inalámbrico de forma segura. - Subir el fichero de forma segura con la versión de *firmware* deseada - Reinicio del controlador - Comprobación de la versión en ejecución tras reinicio	☐	☐	

9. REFERENCIAS

CCN-STIC-816 Guía de Seguridad de las TIC Seguridad en Redes Inalámbricas en el ENS

[1] *Cisco Catalyst 9800-40 Wireless Controller Hardware Installation Guide*
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-40/installation-guide/b-wlc-ig-9800-40/preparing-your-site-for-installation.html#Checking-Shipping-Container-Contents

[2] *Cisco Catalyst 9800-80 Wireless Controller Hardware Installation Guide*
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-80/installation-guide/b-wlc-ig-9800-80/preparing-your-site-for-installation.html#Checking-Shipping-Container-Contents

[3] *Cisco Catalyst 9800-L Wireless Controller Hardware Installation Guide*
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-L/installation-guide/b-wlc-ig-9800-L/Preparing-Your-Site-for-Installation.html#package-contents

[4] *Cisco Catalyst 9800-40 Wireless Controller Hardware Installation Guide*
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-40/installation-guide/b-wlc-ig-9800-40/power-up-and-initial-configuration.html#t_Powering_Up_Controller

[5] *Cisco Catalyst 9800-80 Wireless Controller Hardware Installation Guide*
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-80/installation-guide/b-wlc-ig-9800-80/power-up-and-initial-configuration.html#t_Powering_Up_Controller

[6] *Cisco Catalyst 9800-L Wireless Controller Hardware Installation Guide*
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-L/installation-guide/b-wlc-ig-9800-L/Power-Up-and-Initial-Configuration.html#Checking_Conditions_Prior_to_System_Startup

[7] *Configuring secure shell*
Version 17.X:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg/m_config_secure_shell_ewlc.html
Version 16.X:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/secure-shell.html#reference_C1663FA5A6ED4FB4B2B863E10F55DBF2

[8] *Cisco Catalyst 9800-40 Wireless Controller Hardware Installation Guide*
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-40/installation-guide/b-wlc-ig-9800-40/installing-the-controller.html

[9] *Cisco Catalyst 9800-80 Wireless Controller Hardware Installation Guide*
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-80/installation-guide/b-wlc-ig-9800-80/installing-the-controller.html

[10] *Cisco Catalyst 9800-L Wireless Controller Hardware Installation Guide* https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-L/installation-guide/b-wlc-ig-9800-L/Preparing-Your-Site-for-Installation.html

[11] *Cisco Catalyst 9800-40 Wireless Controller Hardware Installation Guide*
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-40/installation-guide/b-wlc-ig-9800-40/power-up-and-initial-configuration.html#Performing_Initial_Configuration_on_Controller

[12] *Cisco Catalyst 9800-80 Wireless Controller Hardware Installation Guide*
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-80/installation-guide/b-wlc-ig-9800-80/power-up-and-initial-configuration.html#Performing_Initial_Configuration_on_Controller

[13] *Cisco Catalyst 9800-L Wireless Controller Hardware Installation Guide* https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-L/installation-guide/b-wlc-ig-9800-L/Power-Up-and-Initial-Configuration.html#Checking_Conditions_Prior_to_System_Startup

[14] *Lobby Ambassador Account*
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg/m_lobby_admin.html

[15] *Cisco Catalyst 9800 Series Configuration Best Practices*
https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html#Securitysettings

[16] *Generate CSR for Third-Party Certificates and Download Chained Certificates to Catalyst 9800 Wireless Controllers*
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213917-generate-csr-for-third-party-certificate.html

[17] *Support SAN field attr as part of CSR generation*
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt15177

[18] *Cisco Catalyst 9800 Series Wireless Controller, Login Banner*
Version 17.X:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg/m_login_banner.html
Version16.X:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-12/config-guide/b_wl_16_12_cg/b_wl_16_12_cg_chapter_01111110.html

[19] *Licensing on 9800 Wireless LAN Controllers: FAQs*
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215635-licensing-on-9800-wireless-lan-controlle.html#anc4

[20] *Cisco Catalyst 9800 Series Wireless Controller, Smart Licensing*
Version 17.X:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg/m-sl-using-policy.html

Version16.X:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/smart-licensing.html

[21] *Transport Gateway Resitration / Installation / Configuration*
https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/smart_call_home/user_guides/SCH_Ch4.pdf

[22] *Smart Software Manager*
https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html

[23] *Cisco TAC Recommended IOS-XE Builds for Catalyst 9800 WLC*
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214749-tac-recommended-ios-xe-builds-for-wirele.html

10.ABREVIATURAS

AAA	Autenticación, Autorización y Auditoría
ACL	*Access Control List*
AES	Advanced Encryption Standard
AWIPS	*Adaptive Wireless Intrusion Prevention System*
CA	Autoridad de Certificación
CAPWAP	*Control And Provisioning of Wireless Access Points*
CBC	*Cipher-block Chaining*
CCI	*Co-channel interference*
CCMP	*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*
CCN	Centro Criptológico Nacional
CHAP	*Challenge-Handshake Authentication Protocol*
CLI	Interfaz de Línea de Comandos
CoA	*Change of Authentication*
CSR	*Certificate Signing Request*
CSSM	*Cisco Smart Software Manager*
CTS	*Clear to Send*
DES	*Data Encryption Standard*
DH	*Diffie-Hellman*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DoS	*Deny of Service*
DTLS	*Datagram Transport Layer Security*
EAP	*Extensile Authentication Protocol*
EAP-FAST	*Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling*
EAPOL	*Extensible Authentication Protocol Over LAN*
EAP-PEAP	*EAP-Protected EAP*
EAP-TLS	*EAP – Transport Layer Security*
EAP-TTLS	*Extensible Authentication Protocol – Tunnel Transport Layer Security*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ENS	Esquema Nacional de Seguridad.
ESP	*Encapsulating Security Payload*

FIPS	Estándares Federales de Procesamiento de la Información
FQDN	*Fully Qualified Domain Name*
FTP	*File Transfer Protocol*
HA	*High Availability*
HMAC	*Hash Message Authentication Code*
HTTP/S	*Hypertext Transfer Protocol / Secure*
IGTK	tipo de clave nueva para protección de tramas multicast
IP	*Internet Protocol*
IPSec	*Internet Protocol Security*
LAN	*Local Area Network*
LDAP	*Lightweight Directory Access Protocol*
LSC	*Locally Significant Certificate*
MAC	*Media Access Control*
MD5	*MEssage-Digest Algorithm 5*
MFP	*Management Frame Protection*
MIB	*Management Information Base*
MIC	*Manufacturing Installed Certificate*
MS-CHAP	*MicroSoft Challenge-Handshake Authentiacion Protocol*
NTP	*Network Time Protocol*
NVRAM	*Non-Volatile Random Access Memory*
OID	*Object IDentifier*
PAP	*Password Authentication Protocol*
PEAP	*Protected Extensible Authentication Protocol*
PKI	*Public Key Infraestructure*
PLR	*Permanent License Reservation*
PSK	*Pre-Shared Key*
RADIUS	*Remote Authentication Dial-In User Service*
RC4-SHA	*Rivest Cipher 4-Secure Hash Algorithm*
ROM	Read-Only Memory
RSA	*Rivest Shamir and Adleman*
RTS	*Ready to Send*
RTU	*Right To Use*
SA	*Security Association*
SFTP	*SSH File Transfer Protocol*

SLR	*Specific License Reservation*
SNMP	*Simple Network Management Protocol*
SSC	*Self-Signed Certificate*
SSH	*Secure Shell*
SSID	*Service Set Identfier*
SSL	*Secure Sockets Layer*
TAC	*Technical Assistance Center*
TACACS	*Terminal Access Control Access Control System*
TFTP	*Trivial File Transfer Protocol*
TKIP	*Temporal Key Integrity Protocol*
TLS	*Transport Layer Security*
UDI	*Unique Device Identifier*
URL	*Uniform Resource Locator*
VLAN	*Virtual Local Area Network*
WIPS	*Wireless Intrusion Prevention System*
WLAN	*Wireless Local Area Network*
WLC	*Wireless LAN Controller*
WPA2	*Wi-Fi Protected Access 2*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL