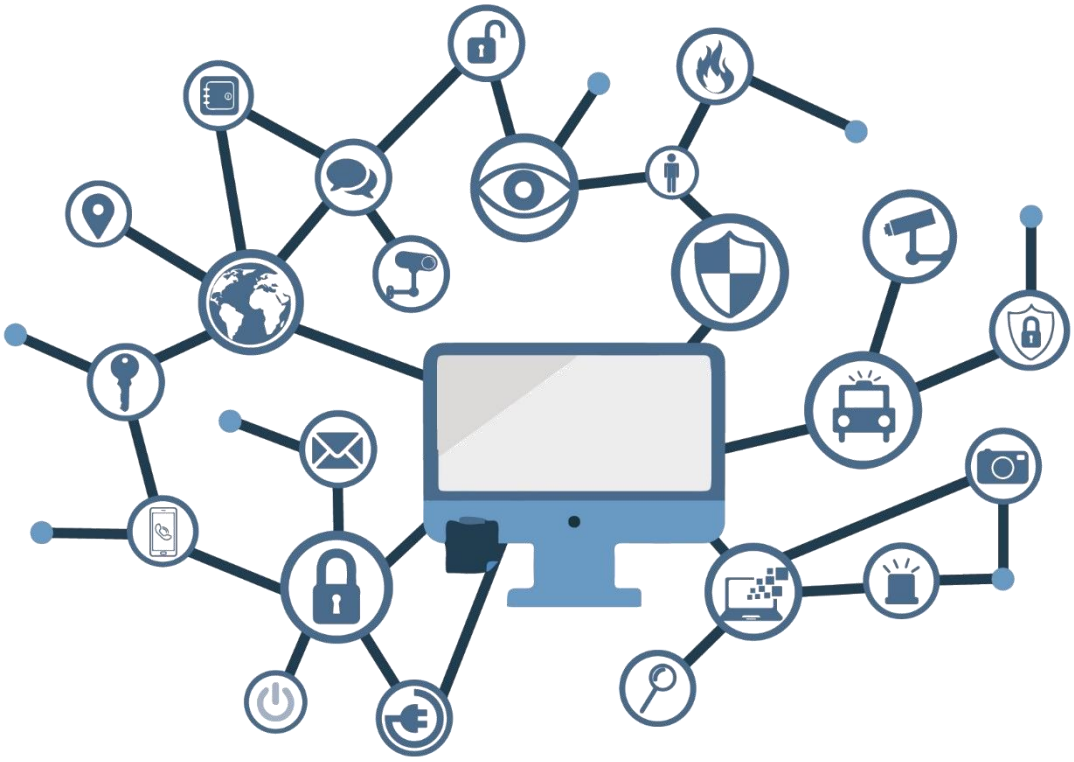
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1423

Procedimiento de empleo seguro
Cisco WLC 5520/8504 bajo AireOS 8.X



Diciembre 2021

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

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.01.17 13:28:42 +01'00'

NIPO: 083-21-210-6
Fecha de Edición: diciembre de 2021

ÍNDICE

1. INTRODUCCIÓN

1. El objetivo de este documento es proporcionar una guía o procedimiento de configuración y empleo seguro de la familia de **controladores inalámbricos Cisco WLC**, tanto en sus versiones de *appliance*, como en sus implementaciones en la variante de máquina virtual (Cisco vWLC).
2. El **sistema operativo** estudiado será el propietario de Cisco para estos equipos, denominado **AireOS**, en su versión 8.X, en contraposición al sistema operativo Catalyst IOS-XE que opera en la nueva familia de controladores inalámbricos Catalyst 9000.
3. Las controladoras inalámbricas que han sido **cualificadas** e incluidas en el Catálogo de Productos y Servicios de Seguridad TIC (**CPSTIC**) en la familia de ***"Dispositivos de Red Inalámbricos"*** son:
    - ***Cisco 3504, 5520, 8540 Wireless Controller con Cisco Aironet 1560, 2800, 3800 Series Access Points AireOS 8.5***
4. Se trata de implementaciones centralizadas de los sistemas inalámbricos de una organización, que pueden realizarse de dos (2) maneras:
    a) Centralizando tanto plano de control como plano de datos (modo centralizado).
    b) Centralizando únicamente el plano de control (modo *flexconnect*).
5. 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.
6. 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**.**

2. OBJETO

7. El objeto de la presente guía es detallar la configuración de los controladores inalámbricos AireOS para utilizarlos de forma segura. De esta forma, es posible establecer un marco de referencia que contemple las recomendaciones STIC en el despliegue y utilización de estos productos.
8. 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).
9. Este documento, salvo menciones especiales, no aporta ajustes de configuración para la operación del producto, fuera de las directamente relacionadas con su operación en modo seguro. Aspectos como las políticas de flujo de información y el control de acceso, deben ser implementadas de acuerdo a las políticas vigentes en la organización.

3. ALCANCE

10. 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.
11. El alcance del presente documento queda enfocado en todos los aspectos de configuración de los equipos que tengan relación con la seguridad, tanto en la comunicación entre los puntos de acceso y la controladora, como entre los clientes y dichos puntos de acceso.
12. 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:
    a) Configuración de canales radio para baja interferencia cocanal (CCI).
    b) Configuración de elementos de modulación para mejora del ancho de banda en las comunicaciones inalámbricas (índices de modulación).
    c) 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.
13. 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 WLC bajo su responsabilidad.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

14. El dispositivo *Wireless LAN Controller* debe ser examinado para comprobar que no ha sido manipulado durante su entrega siguiendo los pasos descritos a continuación [1] [2]:

    a) Antes de abrir el paquete donde fue entregado el *Wireless LAN Controller*, se debe comprobar que el paquete contenga 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).

    b) 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 parece haber sido abierto y después sellado de nuevo, es recomendable contactar con el proveedor del equipo (*Cisco Systems* o un distribuidor autorizado).

    c) 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.

    d) Es importante chequear el número de serie del *Wireless LAN Controller* 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).

    e) 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.

15. 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).

a) 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 Wireless LAN Controller 5520, el contenido del embalaje debe incluir:

- Unidad Cisco Wireless LAN Controller 5520 (formato servidor UCS de Cisco de tamaño 1U).
- Disco duro o tarjeta de memoria FlexFlash (una de las dos opciones debe ser seleccionada expresamente en el momento de la compra).
- Módulo/s SFP (deben ser solicitados expresamente).
- Cable de alimentación (comprobar que es de la región a usar).
- Kit de montaje en rack (deben ser solicitados expresamente).
- Documento informativo sobre Seguridad y Cumplimiento Normativo (Regulatory Compliance and Safety Information).
- Cuartilla para el registro del producto e información sobre la documentación de Cisco.

b) Para el equipo Cisco Wireless LAN Controller 8504, el contenido que debe incluir es el siguiente:

- Unidad Cisco Wireless LAN Controller 8504 (formato servidor UCS de Cisco de tamaño 2U).
- Disco duro (debe ser seleccionado expresamente en el momento de la compra).
- Módulo/s SFP (deben ser solicitados expresamente).
- Fuente de alimentación
- Cable de alimentación (comprobar que es de la región a usar)
- Documento informativo sobre Seguridad y Cumplimiento Normativo (*Regulatory Compliance and Safety Information*).
- Cuartilla para el registro del producto e información sobre la documentación de Cisco.

16. Tras realizar los procedimientos iniciales de configuración, y antes de poner la unidad en su entorno productivo, es recomendable comprobar que el *software* de la unidad no ha sido comprometido [3] [4]. Se recomienda revisar el apartado 8.2 sobre actualización/verificación de *firmware* para tal efecto.

4.2 ENTORNO DE CONFIGURACÓN INICIAL SEGURO

17. El dispositivo Cisco WLC Series debe instalarse en una ubicación físicamente segura donde **solo se permita acceso físico al personal autorizado.**

18. Los Cisco WLC Series requieren los siguientes componentes para disponer de un entorno de configuración inicial seguro:

    a) Puesto de gestión con navegador Web seguro: Es posible configurar el equipo de forma remota mediante un navegador web. El equipo se actuará 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 utilizar únicamente HTTPS**, con un certificado válido para las máquinas de gestión, que evite errores de validez de certificado.

    b) 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 WLC Series para su administración a través de los canales protegidos de SSH. Cualquier cliente SSH que soporte SSHv2 puede ser utilizado, con una longitud de clave mínima RSA de 256.

    c) Consola local: Esto incluye cualquier entorno de consola que esté directamente conectado a los Cisco WLC 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 DATOS INICIALES DE CONFIGURACIÓN

19. 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, 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:

    a) 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 5.2.8.3 del presente documento.

    b) Activación de protocolos de monitorización/gestión remota, tales como SNMP.

    c) Disponibilidad de servidor de tiempos (NTP) y zona horaria.

d) Configuración de gestión (IP de gestión con máscara y puerta de enlace, VLAN de gestión en caso de ser necesaria). En el caso de los dispositivos mencionados, 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 permitir enrutamiento.

4.4 PRIMEROS PASOS

4.4.1 INSTALACIÓN FISICA

20. Consultar las guías "*Cisco WLC 5520 Hardware Installation Guide*" o [5] [6] para la preparación del sitio físico y la instalación del hardware.

4.4.2 CONFIGURACIÓN INICIAL CON ASISTENTE

21. En una unidad Cisco WLC 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 está creado, un administrador privilegiado puede utilizar cualquiera de los métodos disponibles de configuración para añadir configuración adicional.

22. En los dispositivos Cisco WLC en su versión 8.X este asistente puede presentar las siguientes formas:

    a) Herramienta Cisco WLAN Express, mediante conexión por cable a cualquier puerto.

    b) Manera tradicional mediante interfaz de línea de comandos (CLI) a través del puerto serie, utilizando el asistente de configuración por consola (*Autoinstall*).

    c) Herramienta Cisco WLAN Express, de manera inalámbrica, conectando un AP en cualquiera de los puertos, que tras registrarse en el controlador emitirá un identificador de red inalámbrica (SSID) denominado "C*iscoAirProvi*sion", con clave WPA2-PSK "*password*" (solo para el modelo 2504).

23. A continuación, se describe el proceso de configuración inicial usando el asistente de configuración mediante CLI. La sección "*Performing Device Setup Configuration*" en [5] [6] describe cómo usar el configurador para construir una configuración básica y también como modificarla.

    (Cisco Controller)
    Welcome to the Cisco Wizard Configuration Tool
    Use the '-' character to backup
    AUTO-INSTALL: starting now...

AUTO-INSTALL: process terminated -- no configuration loaded
Would you like to terminate autoinstall? [yes]: ***yes***
System Name [Cisco_c7:18:04] (31 characters max): ***WLC-NAME***
Enter Administrative User Name (24 characters max): ***admin***
Enter Administrative Password (3 to 24 characters): **************
*Re-enter Administrative Password : *********
Service Interface IP Address Configuration [static][DHCP]: ***static***
Service Interface IP Address: ***172.16.0.100***
Service Interface Netmask: ***255.255.255.0***
Enable Link Aggregation (LAG) [yes][NO]: ***NO***
Management Interface IP Address: ***10.0.0.4***
Management Interface Netmask: ***255.255.255.0***
Management Interface Default Router: ***10.0.0.1***
Management Interface VLAN Identifier (0 = untagged): ***100***
Management Interface Port Num [1 to 8]: ***1***
Management Interface DHCP Server IP Address: ***10.0.0.1***
Enable HA [yes][NO]: ***NO***
Virtual Gateway IP Address: ***192.0.2.1***
Mobility/RF Group Name: ***Movilidad***
Network Name (SSID): ***Test-SSID***
Configure DHCP Bridging Mode [yes][NO]: ***NO***
Allow Static IP Addresses [YES][no]: ***no***
Configure a RADIUS Server now? [YES][no]: ***no***
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code list (enter 'help' for a list of countries) [US]: ***ES***
Enable 802.11b Network [YES][no]: ***YES***
Enable 802.11a Network [YES][no]: ***YES***
Enable 802.11g Network [YES][no]: ***YES***
Enable Auto-RF [YES][no]: ***YES***
Configure a NTP server now? [YES][no]: ***YES***
Enter the NTP server's IP address: ***10.12.0.1***
Enter a polling interval between 3600 and 604800 secs: ***3600***
Would you like to configure IPv6 parameters[YES][no]: ***no***
Configuration correct? If yes, system will save it and reset. [yes][NO]: ***yes***
Configuration saved! Restarting system

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

    a) 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.

    b) Los tipos de usuarios que existen en un *dispositivo Cisco Wireless LAN Controller* son tres (3):

- *ReadWrite*: Permisos absolutos sobre el equipo.
- *ReadOnly*: Permisos para revisión de configuración (no podrá modificar parámetros).
- *LobbyAdmin*: Es una cuenta de anfitrión, que se emplea para dar de alta usuarios para redes inalámbricas configuradas con usuarios locales.

c) El número de administradores que se creen y sus consiguientes niveles de acceso deben basarse en la política de la organización. No obstante, se recomienda **aplicar los principios del mínimo privilegio**.

d) 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.

25. 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. [7]

26. Finalmente, se debe confirmar que una vez que el dispositivo ha arrancado, la versión ejecutada es la correcta. Utilice el comando *"**show sysinfo**"* y revise la línea acerca de la versión de imagen empleada. Se muestra a continuación una versión reducida del resultado de este comando:

(Cisco Controller) > ***show sysinfo***
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... ***8.5.161.0***
Bootloader Version..... ***1.0.2z***
<<--resto del output omitido-->>

27. De una forma más reducida, se puede obtener la misma información sobre la versión de imagen que se está ejecutando con el comando "***show boot***", donde indica la versión cargada actualmente en memoria y la versión existente de backup. Se muestra a continuación el resultado de este comando:

(Cisco Controller) > ***show boot***
Primary Boot Image..... 8.5.161.0 (default) (active)
Backup Boot Image..... ***8.5.151.0***

5. GESTIÓN SEGURA DEL EQUIPO

5.1 MODOS DE OPERACIÓN

28. Un dispositivo Cisco WLC tiene varios modos de operación, que se detallan en esta sección:

a) 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 progresa automáticamente hacia el modo de operación Normal. Durante el arranque, un usuario podría presionar la tecla de interrupción en una conexión de consola en los primeros 3 segundos del encendido para entrar en el modo de operación *Bootloader* [8]. En este modo de operación, hay disponible ciertas opciones (que se reducen en caso de usar una imagen FIPS).

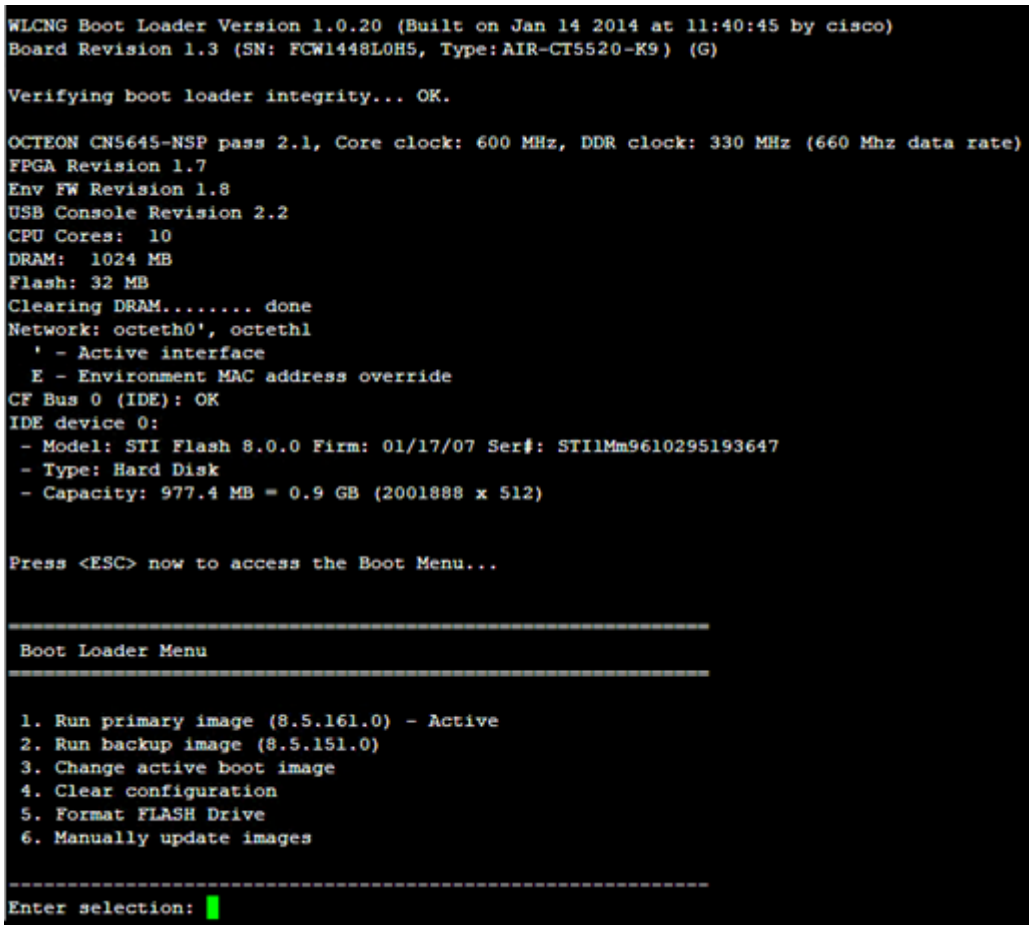


Ilustración 1. Modo *Bootloader* (versión 1.0.2z)

b) Modo de operación Normal: Tras pasar la fase de arranque y el *power-on self test,* la imagen de AireOS 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.

5.2 ENTORNO DE CONFIGURACIÓN Y OPERACIÓN REMOTA SEGURO

29. 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:

30. Se recomienda utilizar protocolos remotos de configuración seguros:

    a) HTTPS con TLS V1.2

    b) **SSHv2** en lugar de SSHv1, con la longitud mínima de clave para RSA descrita en este documento.

    c) No usar SNMP en versiones inseguras, **usar SNMPv3**.

31. Ciertas comunicaciones con servicios sensibles, como el *syslog*, el servidor de *SNMP* o el servidor de AAA se recomiendan proteger con IPSec, siguiendo el procedimiento descrito en la presente guía, en el apartado 5.2.3.

32. 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.

33. 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 importantes del dispositivo.

34. Estas recomendaciones de seguridad y otras buenas prácticas de uso del Controlador WLC se recogen en la sección *"Security"* del documento "*Cisco Wireless LAN Controller (WLC) Configuration Best Practices"* [9].

5.2.1 GESTIÓN SEGURA DEL EQUIPO MEDIANTE INTERFAZ SSH

35. La línea de comandos puede ser accesible por dos (2) modos: modo local, a través del puerto de consola, o modo remoto mediante protocolos de gestión remota seguros, tales como SSHv2.

36. En el interfaz de configuración mediante comandos (CLI) existen diferentes contextos de gestión. El gestor únicamente puede ejecutar comandos circunscritos al ámbito del contexto actual, que estará identificado en el *prompt* de línea de comandos. La importancia de esta información radica en que los comandos tienen su propia jerarquía y sólo se pueden ejecutar bajo las ramas apropiadas. Esto ocurre cuando se introducen comandos sin argumentos, como por ejemplo "*config*", "*debug*" o "*show*". Para salir de ese nivel jerárquico basta con pulsar "*Ctrl+Z*" o bien introducir el comando "*exit*".

37. Se debe confirmar que el acceso mediante SSH se encuentra habilitado, y que el **acceso Telnet se encuentra deshabilitado**. Por defecto, SSH se encuentra habilitado, permitiendo establecer una sesión SSH con el controlador usando el

usuario administrador generado en el asistente de configuración inicial (apartado 4.4.2 de la presente guía).

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

Cisco Controller) > ***show network summary***
Web Mode..... Enable
Secure Web Mode..... Enable
Secure Web Mode Cipher-Option High..... Enable
Secure Web Mode Cipher-Option SSLv2..... Enable
Secure Shell (ssh)..... Enable
Telnet..... Enable

39. **Para deshabilitar Telnet:**

Cisco Controller) > ***config network telnet disable***

40. Para habilitar SSH, en caso de que se hubiera deshabilitado en alguna situación:

Cisco Controller) > ***config network ssh enable***

41. En caso de que los clientes SSH lo soporten, es recomendable mejorar la seguridad de la conexión SSH habilitando cifrados de 256 bits para las sesiones SSH mediante el siguiente comando:

Cisco Controller) > config network ssh cipher-option high enable
(Cisco Controller) > ***show network summary***
RF-Network Name..... 3500
DNS Server IP..... 0.0.0.0
Web Mode..... Enable
..
Secure Shell (ssh)..... Enable
Secure Shell (ssh) Cipher-Option High..... Enable

5.2.2 GESTIÓN DE CERTIFICADOS

42. Se recomienda configurar el dispositivo para utilizar certificados X.509v3 para la autenticación segura del equipo en HTTPS, o para la autenticación de pares entre dispositivos críticos, tales como servidores de syslog, servidores SNMP o servidores de AAA mediante IPsec, tal y como se detalla en el apartado **5.2.3** de la presente guía.

43. La creación de estos certificados y su carga en el dispositivo está detallado en [10]. Los aspectos más destacados de la configuración del dispositivo para el uso de estos certificados se explica en las subsecciones siguientes.

44. 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 a la interfaz GUI se hagan sobre una unidad que tenga un certificado HTTPS confiable.

45. Por tanto, como ejemplo de instalación de certificado, se detalla 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.

5.2.2.1 CREACIÓN DE LA SOLICITUD DE CERTIFICADO (CSR)

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

47. 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 del mismo, por lo que no hay exposición de la misma.

48. 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. De todas formas, la mayoría de CA permiten incluir este atributo en el momento de la firma, aunque la recomendación es informarse de antemano.

49. Cuando se genera la petición CSR se emplea, por defecto, una clave con una longitud de 2048 bits y una clave ECDSA con un tamaño de 256 bits. La longitud puede ser configurada con un menor valor. Sin embargo, no es una opción recomendada.

50. Es importante conocer que una vez se haya generado la solicitud de certificado (CSR) hay que finalizar el proceso, es decir, 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.

51. Para generar la solicitud de certificado CSR, hay que ejecutar el siguiente comando en la terminal de consola del dispositivo, con especial cuidado como se comentará tras el ejemplo:

    *(Cisco Controller) > config certificate generate **csr-webadmin** Siglas_Pais Estado Ciudad Organización Departamento Common_Name email {RSA | ECDSA}*

52. Un ejemplo del resultado de aplicar el anterior comando es el siguiente:

    (Cisco Controller) > config certificate generate csr-webadmin ES MA Malaga Cisco Infraestructura wlc.cisco.com tac@cisco.com RSA

    -----BEGIN CERTIFICATE REQUEST-----
    MIICqjCCAZICAQAwZTELMAkGA1UECAwCQllxETAPBgNVBAcMCEJydXNzZWxzMQ4wDAYDVQQKDA
    VDaXNjbzEMMAoGA1UECwwDVEFDMSUwIwYDVQQDDBxteXdlYmF1dGhwb3J0YWwud2lyZWxlc3
    MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnssc0BxlJ2ULa3xgJH5lAUtbd9CuQ
    Vqqf2nflh+V1tu82rzTvz38bjF3g+MXJiaBbKMA27VJH1J2K2ycDMlhjyYpH9N59T4fXvZr3JNGVfmHIRu
    YDnCSdil0ookKFU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NlZqg1hNemnhqVgbXEd90sgJmaF20ts
    L0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJiaI2JpbO0afRO3kSgx3XDkZiR7Z9a8rK6Xd
    8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjIMzKT6OOjFGOGuyNkgYefrrBN+WkDdc6c55bxErwIDAQ
    ABoAAwDQYJKoZIhvcNAQELBQADggEBAB0KZvEpAafoovphlcXIEIL2DSwVzjlbd9u7T5JRGgqri1l9/0wz
    xFjTymQofga427mj5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidu+0T8O46s/stbhj9nuInmoTgPaA0s3Y
    HtDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69XdYHPLnD2ygR1

Q+3Is4+5Jw6ZQAaqlPWyVQccvGyFacscA7L+nZK3SSITzGt9B2HAaPQ8DQOaCwnqt2efYmaezGiHOR8
XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4Wkc/wH4DyYdH7x5jzHc=
-----END CERTIFICATE REQUEST-----

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. Esa salida (el CSR) se puede volver a recuperar, aunque lo recomendable es anotarla y continuar el proceso. Se puede emplear el menú o comandos para subir el CSR a algún servidor externo. Desde el interfaz web se puede realizar esta tarea en el menú "*Commands*", sección "*Upload File*" y seleccionar la opción "*CSR WebAdmin Certificate*".

53. Aunque existe esa posibilidad, en la medida de lo posible es recomendable realizar el proceso completo en una sesión continua, para así no extraer el CSR del controlador inalámbrico. De esta forma, la clave permanece siempre en el controlador y se evita su exposición.

54. Una vez empleado el CSR en la correspondiente entidad o infraestructura existen comúnmente dos posibilidades, que devuelva el certificado firmado en un único fichero o bien que devuelvan las tres cadenas de certificados que conformarán el certificado final, que deben ser los siguientes:

    a) Certificado raíz

    b) Certificado intermedio

    c) Certificado del dispositivo

55. De tener los certificados por separado, se deberán unir en un único fichero de formato pem. Si los tres certificados son facilitados en dicho formato, se pueden visualizar con un editor de textos y copiar el contenido en el fichero final. La estructura de este fichero debe ser como se muestra a continuación:

-----BEGIN CERTIFICATE REQUEST-----
Certificado del dispositivo
-----END CERTIFICATE REQUEST-----
-----BEGIN CERTIFICATE REQUEST-----
Certificado Intermdio de la CA
-----END CERTIFICATE REQUEST-----
----BEGIN CERTIFICATE REQUEST-----
Certificado Raíz de la CA
-----END CERTIFICATE REQUEST-----

56. A continuación, y mediante transferencia de ficheros tftp, se procede a transferir los elementos necesarios del certificado al controlador:

(Cisco Controller) > transfer download mode tftp
(Cisco Controller) > transfer download datatype webadmincert
(Cisco Controller) > transfer download serverip IP_Servidor_TFTP
(Cisco Controller) > transfer download path Ubicación_absoluta_fichero_cert
(Cisco Controller) > transfer download filename Nombre_fichero_certificado
(Cisco Controller) > transfer download start

Mode..... TFTP
Data Type..... Site Cert
TFTP Server IP..... IP_Servidor_TFTP
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... Ubicación_absoluta_fichero_certificado
TFTP Filename..... Nombre_fichero_certificado

This might take some time.
Are you sure you want to start? (y/N) y
TFTP EAP Dev cert transfer starting.
Certificate installed.
Reboot the switch to use new certificate.

57. Tras estos comandos y el reinicio del equipo, el certificado debería quedar instalado y en uso. Es posible comprobar que el certificado ha quedado correctamente instalado mediante los comandos:

(Cisco Controller) >show certificate summary

Web Administration Certificate..... 3rd Party

Web Authentication Certificate..... Locally Generated

Certificate compatibility mode:..... off

Lifetime Check Ignore for MIC ..... Enable

Lifetime Check Ignore for SSC ..... Disable

…

(Cisco Controller) >show certificate webadmin

58. Tras la instalación, el acceso mediante HTTPS no debería generar 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).

59. Para cargar el resto de tipos de certificado, es posible hacerlo igualmente a través de la línea de comandos (CLI) o mediante GUI. En caso de usar el CLI, el proceso para cargar otro tipo de certificado (por ejemplo, de tipo "*ipsecCACert*" o "*ipsecDevCerts*" para IPSec), el comando es idéntico al usado en el ejemplo anterior, pero cambiando el tipo de certificado en el comando "*transfer download datatype*", donde aparecen las siguientes opciones:

```
(Cisco Controller) >transfer download datatype ?

avc-protocol-pack Download an AVC Protocol Pack to the system.
ca-serv-ca-cert Download CA server CA cert for getting LSC certificate
cmx-serv-ca-cert Download CMX server CA cert for NMSP over TLS
code            Download an executable image to the system.
config          Download Configuration File.
device-mapping-pfile Download Device mapping file for Apple clients
device-profile Download an Device Profile file to the system.
eapcacert       Download a eap ca certificate to the system.
eapdevcert      Download a eap dev certificate to the system.
icon            Download a graphic icon to the system.
image           Download a web page logo to the system.
ipseccacert     Download a IPSec ca certificate to the system.
ipsecdevcert    Download a IPSec dev certificate to the system.
login-banner    Download controller login banner. (Only Text file supported: Max 1500 bytes & 18 lines,
naServerCaCert Download NA server CA cert for NA over TLS
opendns-serv-ca-cert Download OpenDNS server CA certificate for https
oui-update      Download an OUI Update file to the system.
radius-avplist Download a Radius AVPs List file.
signature       Download a signature file to the system.
ssh-public-key Download CMX server CA cert for NMSP over TLS
webadmincert    Download a certificate for web administration to the system.
webauthbundle   Download a custom webauth bundle to the system.
webauthcert     Download a web certificate for web portal to the system.
```

Ilustración 2. Instalación de otros tipos de certificado en el controlador (mediante CLI)

60. Desde el GUI también es posible subir cualquier tipo de certificado, en el menú "*Commands*", sección "*Download file*" y especificando el tipo de fichero deseado, en este caso, un *Webadmin Certificate*:

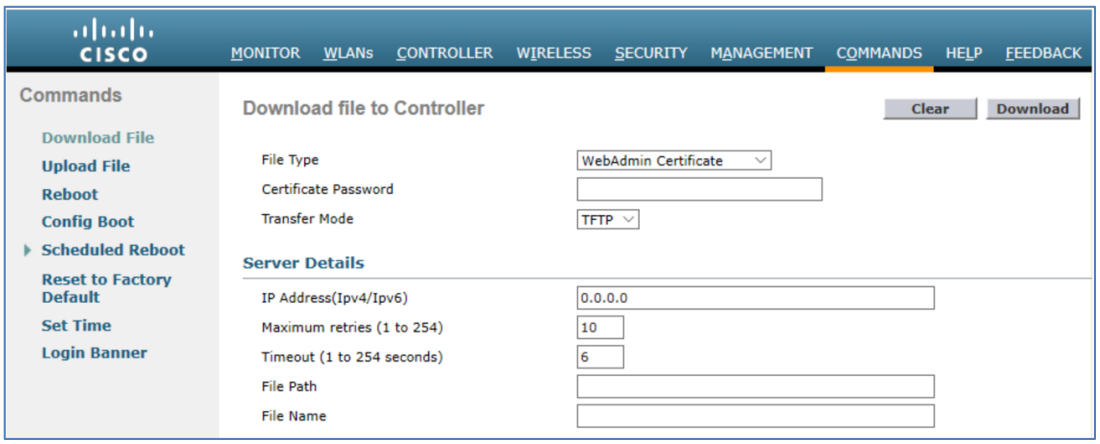


Ilustración 3. Instalación de otros tipos de certificado en el controlador (mediante GUI)

5.2.3 GESTION SEGURA DEL EQUIPO MEDIANTE EL INTERFAZ WEB

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

62. Además, la unidad debe 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 5.2.2 de la presente guía.

63. El primer paso, que sería activar el protocolo HTTPS, se realizaría a través del menú "*Management*", y en el menú vertical izquierdo a la sección "*HTTP-HTTPS*".

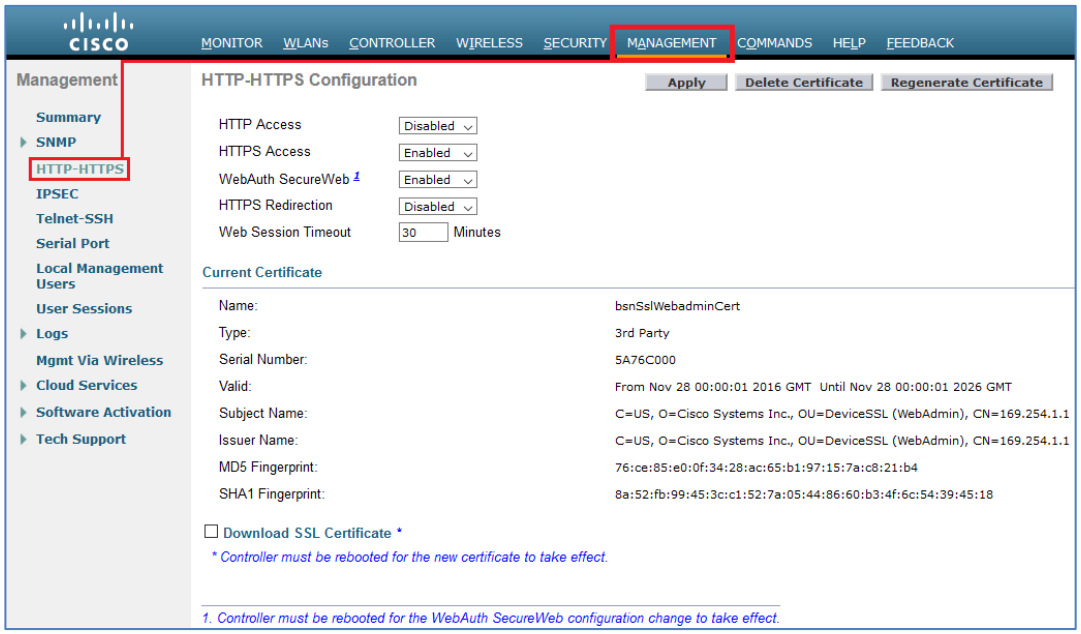


Ilustración 4. Activación de HTTPS

64. 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.

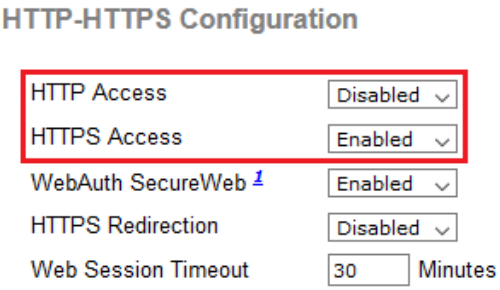


Ilustración 5. Selección de HTTPS

65. Con respecto al tiempo máximo de sesión inactiva, se debe configurar el menor valor posible que permita la correcta administración del dispositivo.

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

    a) Deshabilitar el acceso mediante HTTP [11]:

       (Cisco Controller) > config network webmode disable

    b) Habilitar el acceso mediante HTTPS [11]:

       (Cisco Controller) > config network secureweb enable

    c) Se puede incrementar la seguridad con el comando listado bajo estas líneas. Lo que realiza es un cifrado de al menos 128-bit, por lo que navegadores que no lo soporten serán incapaces de entrar a la gestión del equipo por interfaz web. Cuando se emplea esta opción, las claves de tipo SHA1, SHA256 y

SHA384 se siguen listando, pero TLS v1.0 y TLS v.1.1 son deshabilitados (aplica al interfaz de gestión y al usado para *webauth*, pero no para SNMP):

(Cisco Controller) > config network secureweb cipher-option high enable

d) Deshabilitar SSLv2. Al realizarlo, obliga a que los navegadores deban usar un protocolo más seguro (al menos SSLv3 en adelante):

(Cisco Controller) > config network secureweb cipher-option sslv2 disable

e) Habilitar cifrado de 256 bit para sesiones SSH (es necesario debido a que se generará un certificado nuevo para la gestión del dispositivo):

(Cisco Controller) > config network ssh cipher-option high enable

f) Habilitar/Deshabilitar preferencia de esquemas de cifrado RC4-SHA (*Rivest Cipher 4-Secure Hash Algorithm*) frente a esquemas CBC para la gestión web del dispositivo (afecta también a la autenticación web -*webauth*-):

(Cisco Controller) > config network secureweb cipher-option rc4-preference enable

g) Salvar la configuración y reiniciar el dispositivo:

(Cisco Controller) > save config
Are you sure you want to save? (y/n) y
Configuration Saved!
(Cisco Controller) > reset System
Are you sure you would like to reset the system? (y/N) Y
System is now restarting….

67. En el apartado 5.2.2 de 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.

68. Para comprobarlo, desde el propio GUI es posible verificar los datos del certificado instalado para el acceso mediante HTTPS, en el menú "*Management*" y en el menú vertical en la parte izquierda seleccionar la sección "HTTP-HTTPS". En la ventana principal nos mostrará diversas opciones, entre la que se encuentra el certificado actual (*current certificate*).

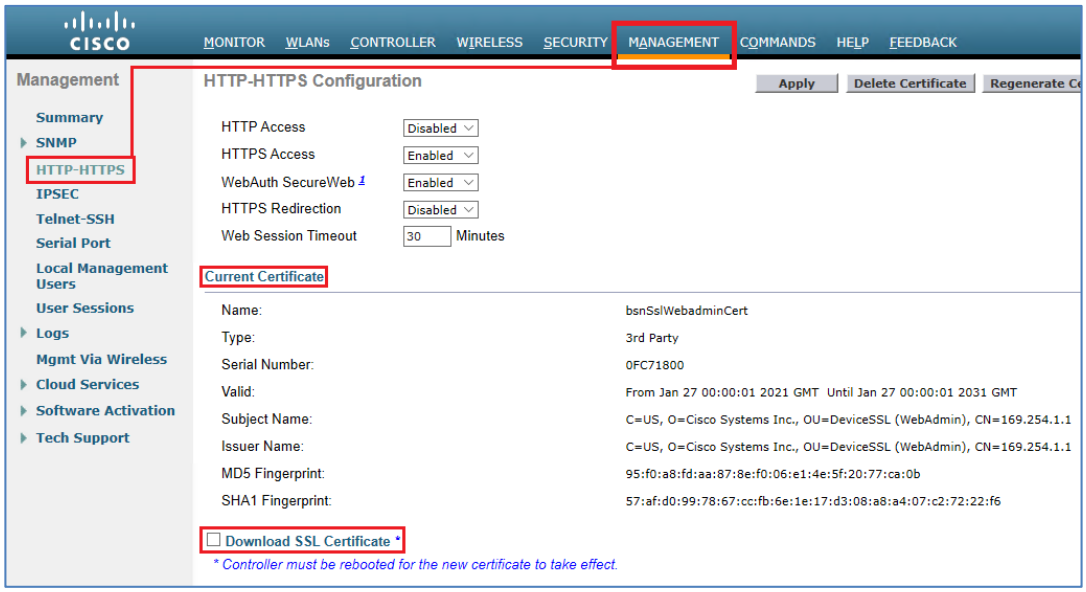


Ilustración 6. Comprobación del certificado *webamin* de acceso HTTPS al controlador

69. Justo al pie, se debe habilitar la opción "*Download SSL Certificate*" para configurar las opciones de descarga del certificado, por si las siguientes actualizaciones del certificado (una vez caducado, por ejemplo) desean realizarse desde del GUI, en lugar desde el CLI. En ese caso, dentro de esa misma pantalla, habría que completar los campos de información del servidor y ubicación del certificado, de manera idéntica a cómo se ha realizado en el CLI para la carga del primer certificado. La clave se debe dejar en blanco en este caso. Finalmente se debe pulsar sobre el botón "*Apply*" en la esquina superior derecha para que comience la descarga.

Ilustración 7. Carga de un certificado de *webadmin* nuevo al controlador mediante GUI

5.2.4 CONFIGURACIÓN DE PERFIL DE IPSEC

70. IPSec es un conjunto de protocolos que permite asegurar las comunicaciones autenticando y/o cifrando cada paquete en el flujo de datos. **En los controladores**

inalámbricos, IPSec se debe configurar para añadir un elemento de seguridad adicional en la comunicación con servidores RADIUS o SNMP.

71. Para configurar IPSec, es necesario acceder al menú "*Management*", sección "*IPSEc*". En esta primera ventana principal aparecerán los perfiles de IPSEc ya configurados. Para crear uno nuevo, pulsar sobre el botón "*New*" que se encuentra en la esquina superior derecha.

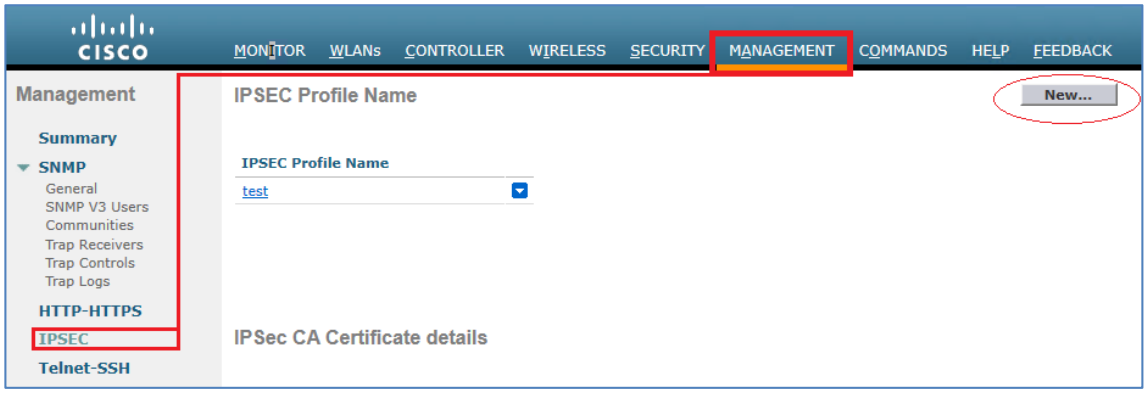


Ilustración 8. Vista general de perfiles IPSec configurados

72. Aparecerán en pantalla las diferentes opciones a configurar en el perfil IPSec, que son:

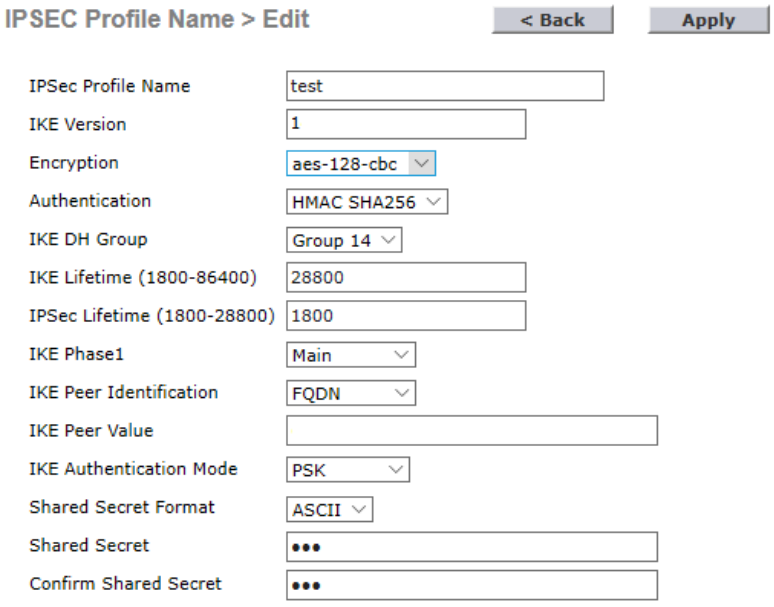


Ilustración 9. Parámetros a configurar en un perfil IPSec

a) *IPSec Profile Name*: Es un nombre para identificar el perfil IPSec a crear.

b) *IKE Version*: Es la versión del protocolo de intercambio de claves en redes (*Internet Key Exchange*), usado para dar confiabilidad al canal de comunicaciones. Las versiones soportadas son IKEv1 e IKEv2. Sin embargo, **se debe utilizar IKEv2.**

c) *Encryption*: Es el esquema de cifrado empleado para proteger los datos y no puedan ser legibles para terceros. Las opciones posibles AES-128-CBC, AES-256-CBC, AES-128-GCM o AES-256-GCM. Sin embargo, **la opción recomendada es AES-256-GCM.**

d) *Authentication*: Es el algoritmo de autenticación que verifica la integridad y autenticidad de los datos de un mensaje. En este caso, se emplean técnicas criptográficas basadas en funciones HASH (HMAC) combinadas con funciones SHA. Las opciones posibles son "HMAC SHA1", "HMAC SHA256" o "HMAC SHA384".

e) *IKE DH Group*: Es la variable de grupo *Diffie-Hellman (DH)* que determina la robustez de la clave empleada en el proceso de intercambio de claves. Existe una relación directa entre grupos altos y tiempo para computar la clave. Las opciones posibles son Group 14 (grupo de 2048-bits), Group 19 (grupo de 256-bits de curva elíptica) y Group 20 (grupo de 384-bits de curva elíptica). **No se debe utilizar Group 14 dado que no presenta la fortaleza suficiente.**

f) *IKE Lifetime*: Es el tiempo de sesión válido para la sesión de fase 1 de IPSec, se permite un valor entre 1800 y 86400 segundos. Se recomienda la configuración del menor valor posible.

g) *IPSec Lifetime*: El el tiempo de sesión válido para la sesión de fase 2 de IPSec, se permite un valor entre 1800 y 28800 segundos. Se recomienda la configuración del menor valor posible.

h) *IKE Phase1*: Este parámetro se emplea para determinar cómo debe ser protegido el protocolo IKE. Existen dos (2) opciones [12]:

- *Main*: La transferencia de información requiere de un mayor número de mensajes. En concreto, la fase 1 requiere de un total de 6 mensajes, siendo el primero el que contiene las políticas ISAKMP (contienen información acerca de los algoritmos de cifrado y autenticación que se desean emplear). El segundo mensaje contiene las claves públicas *Diffie-Hellman*, y el tercero envía la información del extremo con el correspondiente Hash para permitir autenticar la sesión ISAKMP.

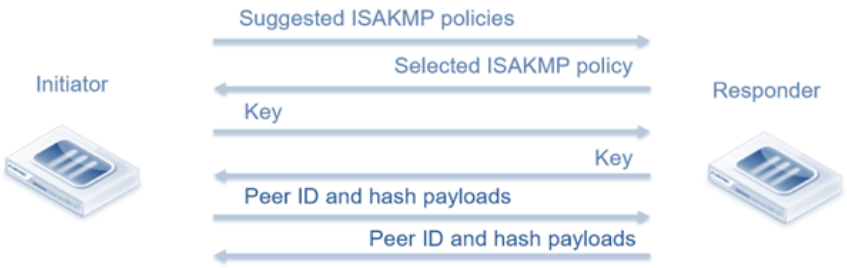


Ilustración 10. Intercambio de mensajes– Fase 1 - Método *Main*

- *Aggressive*: en este modo, se pasa más información en una cantidad menor de paquetes, con el beneficio de establecer una conexión ligeramente más rápida a cambio de transmitir la identidad de los extremos en claro. En concreto, la fase 1 requiere en este caso de tan sólo

3 mensajes, en el primero, se envían todos los para iniciar una comunicación segura (políticas ISAKMP, claves *Diffie-Hellman* y la identidad del extremo). En el segundo, el otro extremo responde de forma similar añadiendo el hash, y en el tercero el extremo original responde con su hash para finalizar esta fase

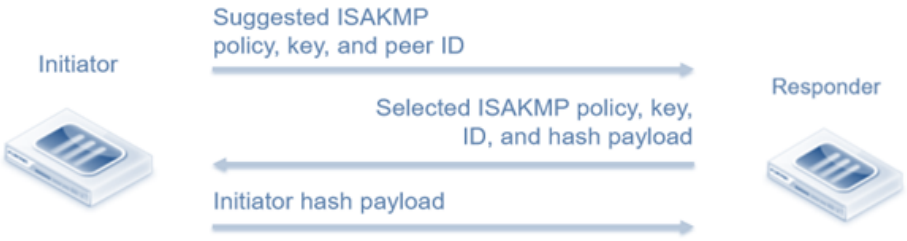


Ilustración 11. Intercambio de mensajes – Fase 1 - Método *Aggressive*

i) *IKE Peer Identification*: Es la identificación del nodo o extremo que se puede introducir mediante "*FQDN*", "*user FQDN*", "CN" o "IP". La identificación del par remoto puede hacerse indicando un nombre de equipo plenamente cualificado (FQDN), un nombre de usuario incluyendo el dominio (User FQDN) o una dirección IP concreta.

j) *IKE Peer Value*: Es el campo que permite introducir el valor de identificación del extremo (el tipo se selecciona justo en el punto anterior).

k) *IKE Authentication Mode*: Es el modo de autenticación empleado para IKE, que puede ser:

- *PSK*: Los extremos comparten una clave predefinida, es la opción más sencilla, aunque la más complicada de mantener en redes a gran escala. Se debe introducir la clave en los campos destinados a ello (clave y confirmación de la misma).
- *Certificate*: En este caso, la autenticación se realiza empleando certificados de confianza. Se debe tener en cuenta, que el controlador inalámbrico empleará los certificados "*ipsecCACert*" y "*ipsecDevCerts*" para sesiones SNMP. El procedimiento para añadir estos certificados se realiza, como en otras ocasiones, mediante el menú "*Commands*", sección "*Download F*ile" y seleccionando las opciones "*Ipsec Device Certificate*" e "*Ipsec CA Certificate".*

Se recomienda la utilización de certificados en lugar de claves pre-compartidas (PSK), por dos (2) motivos principales: cualquier parte que sepa la PSK podría autenticarse y conectarse a la VPN y suelen ser vulnerables a ataques de diccionario.

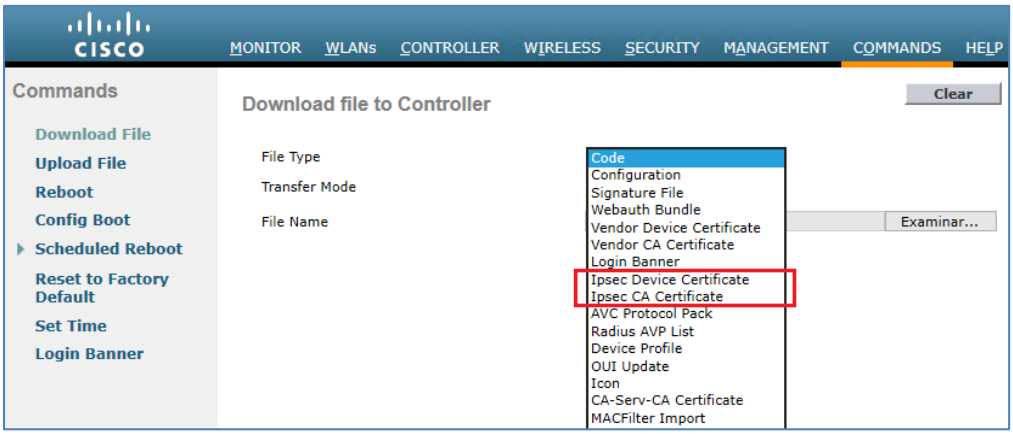


Ilustración 12. Selección de certificados IPSec para añadirlos al controlador

73. Toda la configuración anterior realizada mediante GUI puede reproducirse mediante comandos CLI, que se resumen a continuación:

    a) Crear un perfil IPSec, donde el parámetro a indicar es el nombre del perfil:

    (Cisco Controller) > config ipsec-profile create <Nombre_perfil>

    b) Configurar la versión del protocolo IKE para el perfil en cuestión, los parámetros a introducir son la versión y el nombre del perfil IPSec sobre el que aplicará:

    (Cisco Controller) > config ipsec-profile ike version 2 <Nombre_perfil>

    c) Configurar el tipo de cifrado, introduciendo los parámetros del esquema de cifrado deseado y el nombre del perfil IPSec sobre el que aplicará:

    (Cisco Controller) > config ipsec-profile encryption {aes-128-cbc | aes-256-cbc | aes-128-gcm | aes-256-gcm} <Nombre_perfil>

    d) Configurar el tipo de autenticación empleado, los parámetros a introducir son el esquema de autenticación y el perfil IPSec sobre el que aplicará:

    (Cisco Controller) > config ipsec-profile authentication {hmac-sha1 | hmac-sha256 | hmac-sha384} <Nombre_perfil>

    e) Configurar el tipo de cifrado, introduciendo los parámetros del esquema de cifrado deseado y el nombre del perfil IPSec sobre el que aplicará:

    (Cisco Controller) > config ipsec-profile encryption {aes-128-cbc | aes-256-cbc | aes-128-gcm | aes-256-gcm} <Nombre_perfil>

    f) Configurar el grupo *Diffie-Hellman*, introduciendo los parámetros del grupo deseado y el nombre del perfil IPSec sobre el que aplicará:

    (Cisco Controller) > config ipsec-profile ike dh-group {group-14 | group-19 | group-20} <Nombre_perfil>

    g) Configurar el tiempo fase 1, donde se especificará el tiempo en segundos y el nombre del perfil IPSec sobre el que aplicará:

    (Cisco Controller) > config ipsec-profile life-time-ike [1800-86400] <Nombre_perfil>

h) Configurar el tiempo fase 2, donde se especificará el tiempo en segundos y el nombre del perfil IPSec sobre el que aplicará:

(Cisco Controller) > config ipsec-profile life-time-ike [1800-28800] <Nombre_perfil>

i) Configurar la identificación del extremo, donde se indicará en qué formato está expresado, la identificación y el nombre del perfil IPSec sobre el que aplicará:

(Cisco Controller) > config ipsec-profile ike peer-identification {fqdn | user-fqdn | dn | ip} <id_peer> <Nombre_perfil>

j) Configurar el método de autenticación de fase 1, siendo los parámetros a introducir el modo y el nombre del perfil IPSec sobre el que aplicará:

(Cisco Controller) > config ipsec-profile ike phase1 {aggressive | main} <Nombre_perfil>

k) Configurar el modo de autenticación IKE, siendo los parámetros a introducir el modo (PSK o mediante certificado), el nombre del perfil IPSec sobre el que aplicará y la clave o certificado:

(Cisco Controller) > config ipsec-profile ike auth-mode {pre-shared-key | certificate} <Nombre_perfil> [[ascii | hex] <clave_compartida>]

74. En general, para la configuración IPSEC, se deben seguir las recomendaciones de seguridad detallas en la píldora **Nº3 Seguridad para VPN IPSEC**, publicada por el Centro Criptológico Nacional.

5.2.5 GESTIÓN SEGURA DEL EQUIPO MEDIANTE SNMP

75. Se deben configurar los dispositivos WLC para que el protocolo SNMP permanezca desactivado en sus versiones no seguras (SNMPv1 y SNMPv2c). Para deshabilitar estas versiones del protocolo SNMP es necesario dirigirse al menú "*Management*", y sobre el menú vertical izquierdo dirigirse a la sección "*SNMP→General*".

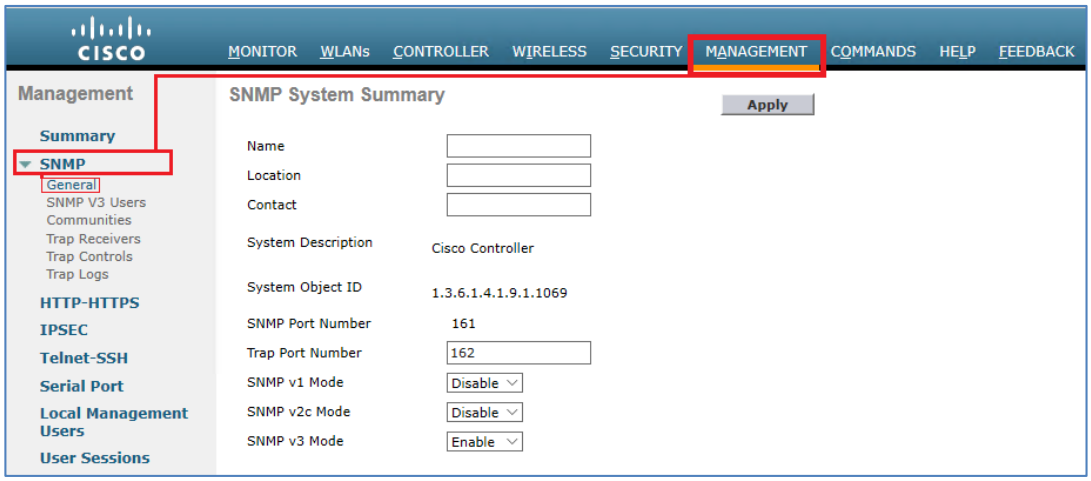


Ilustración 13. Gestión del SNMP en los controladores Cisco WLC

76. En la ventana principal aparecerán los campos de información del dispositivo que se enviarán en las *traps*, y justo al pie, la posibilidad de deshabilitar los protocolos.

cambiarse debe configurar la opción de "*SNMP v1 Mode*" y "*SNMP v2c Mode*" a "*Disable*".

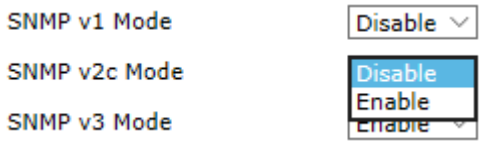


Ilustración 14. Anulación de protocolos inseguros SNMP

77. Aunque permanezcan deshabilitados, se recomienda eliminar la *community* "*public*" que se encuentra configurada por defecto para SNMPv1 y SNMPv2c. Para ello, sobre la misma sección anterior de SNMP, acceder a "*Communities*", y aparecerán en pantalla las *communities* configuradas. Estos elementos denominados "*SNMPv1 / v2C Community*" son unos 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.

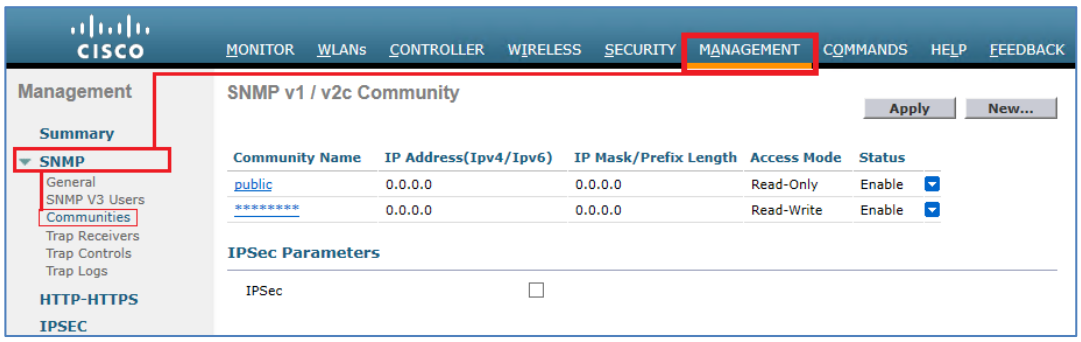


Ilustración 15. Cambio de las claves SNMP por defecto

78. Situando el puntero sobre la flecha con fondo azul, aparecerá la opción de eliminar la *community* deseada:

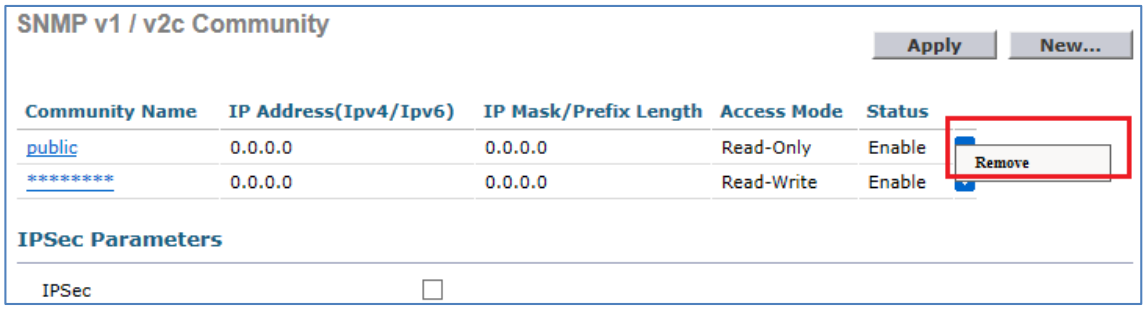


Ilustración 16. Cambio de la clave asignada

79. Para configurar el equipo mediante SNMPv3, en primer lugar, debe estar habilitado para su uso (se realiza de manera similar a lo explicado anteriormente). Después, es necesario configurar el usuario. Para ello, hay que dirigirse a la sección "*SNMP-> SNMP V3 Users*" dentro del menú "*Management*":

80. Una vez en la pantalla indicada en la siguiente ilustración, se mostrarán los usuarios existentes. Para crear uno nuevo, es necesario pulsar sobre el botón "*New*" de la esquina superior derecha.

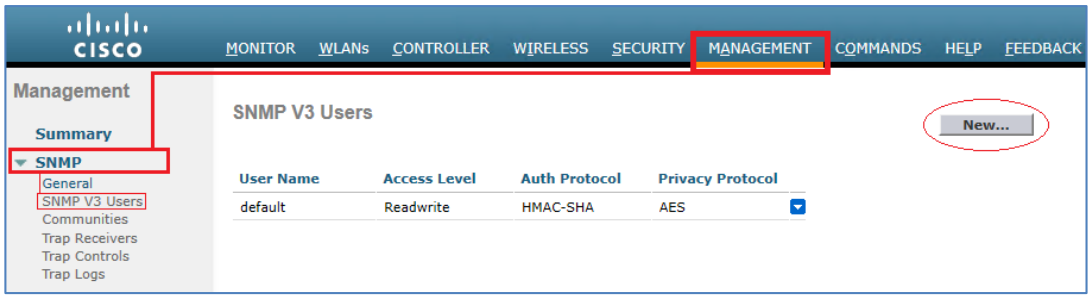


Ilustración 17. Definición de nuevo usuario SNMPv3

81. Tras ese paso, se mostrará una pantalla para introducir los datos del nuevo usuario. Los datos solicitados son:

    a) *User Profile Name*: Nombre de usuario.

    b) *Access Mode*: Es el rol o privilegios que tendrá el usuario, en este caso las opciones posibles son "*Read Only* | *Read Write*". **Se recomienda utilizar la opción de "*Read Only*".**

    c) *Authentication Protocol*: Es el protocolo de autenticación que se empleará. En este caso las opciones posibles son "*None* | *HMAC-MD5* | *HMAC-SHA*" y, entre estas, **se debe configurar HMAC-SHA.**

    d) *Auth Password*: Clave de autenticación, debe ser una cadena alfanumérica de **al menos 12 dígitos.**

    e) *Privacy Protocol*: Es el protocolo de privacidad que se empleará. En este caso, las opciones posibles son "*None* | *CBC-DES* | *CFB-AES-128*". **La opción recomendada es CFB-AES-128.**

    f) *Privacy Password*: Clave de privacidad, deber ser una cadena alfanumérica de al menos 12 dígitos.

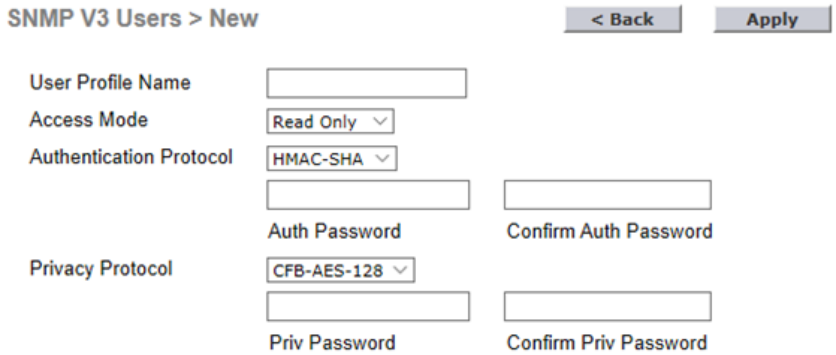


Ilustración 18. Configuración de nuevo usuario SNMPv3

82. Como en el resto de configuraciones, también se puede realizar mediante la consola de comandos:

(Cisco Controller) > config snmp v3user create Nombre_Usuario {ro|rw} {none | hmacmd5 | hmacsha} {none | aescfb128 | des} Clave_autenticacion Clave_encriptacion

83. En cualquier caso, una vez creado el usuario la recomendación es reiniciar el controlador para que tenga efecto, en especial si se modifican los datos del usuario por defecto (aunque no es un requisito necesario en versiones iguales o superiores a 8.X).

84. Otro aspecto 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).

85. Para configurar los servidores que recibirán las traps, hay que navegar hasta el menú "*Management*", sobre la sección "*SNMP -> Trap receivers*". En la ventana principal aparecerá la información de los servidores ya configurados, y para crear uno nuevo bastará con pulsar sobre el botón "*New*" situado en la esquina superior derecha.

Ilustración 19. Gestión de receptores de traps (traps-receivers) SNMP

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

    a) *Community Name*: En las versiones inferiores a 8.10, no se utiliza SNMPv3 para los *trap-receivers*, por lo que es necesario definir un valor de *community* para que el receptor de los *traps* los considere válidos (aunque se use IPSec como elemento adicional de seguridad) [13].

    b) *IP Address*: Dirección IP (versión 4 o 6) del sistema receptor de *traps*.

    c) Status: Permite habilitar o deshabilitar el envío de *traps* a dicho servidor.

    d) *IPSec*: Permite activar/desactivar una comunicación mediante túnel IPSec con el receptor de las traps. Se recomienda activarlo para dotar de protección a la comunicación entre el controlador y su receptor de *traps*.

    e) *IPSec Profile Name*: En el caso de que IPSec esté habilitado, será necesario especificar un perfil de túnel IPSec [14], tal y como se especifica en el apartado 5.2.3 del presente documento.

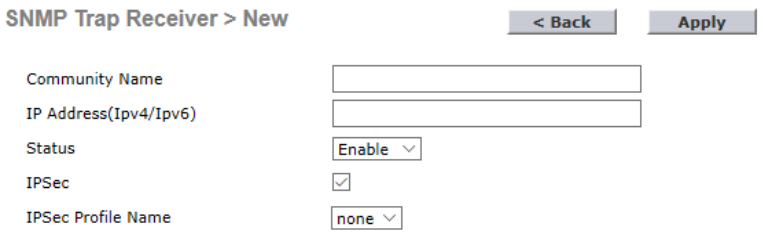


Ilustración 20. Configuración de un receptor de traps SNMP

87. Por último, aplicar la configuración nueva (o los cambios) pulsando sobre el botón "*Apply*" de la esquina superior derecha

88. Para la configuración de los *trap-receivers*, se puede emplear el siguiente conjunto de comandos [15]:

    a) El siguiente comando crea un *trap-receiver*, especificando como parámetros el nombre y la dirección IP:

    (Cisco Controller) > config snmp trapreceiver create <Nombre_receiver> <IP>

    b) El siguiente comando habilita un *trap-receiver*, indicando la *community*:

    (Cisco Controller) > config snmp trapreceiver mode enable <community>

    c) El siguiente comando habilita la opción IPSec en un *trap-receiver* indicado por el nombre (deberá estar creado previamente):

    (Cisco Controller) > config snmp trapreceiver ipsec enable <Nombre_receiver>

    d) El siguiente comando aplica un perfil de IPSec (creado previamente) sobre un *trap-receiver*:

    (Cisco Controller) > config snmp trapreceiver ipsec profile <Perfil_IPSec> <Nombre_receiver>

    e) El siguiente comando configura los métodos de autenticación IKE:

    (Cisco Controller) > config snmp trapreceiver ipsec ike auth-mode {certificate | pre-shared-key <key>}

5.2.6 CONFIGURACIÓN DEL MENSAJE DE AVISO EN EL INICIO DE SESIÓN

89. El producto proporciona al administrador privilegiado la habilidad de configurar un mensaje de aviso/*banner* que se muestra tanto en la interfaz de administración CLI como en el interfaz web antes de permitir cualquier acceso administrativo al dispositivo. Esta funcionalidad se provee a través de la subida de un fichero de texto donde se proporciona el banner.

90. **Se debe configurar este *banner* de acceso**. Para ello, es necesario preparar un fichero de texto plano con el banner deseado, y guardarlo con extensión "*txt*".

91. El fichero de texto que contiene el *banner* debe ser incorporado al WLC, mediante los menús de subida de ficheros ya comentados en varias ocasiones. Hay que dirigirse al menú "*Commands*" y dirigirse a la sección "*Download File*". Una vez en la pantalla principal, hay que seleccionar como "*File Type*" la opción "*Login Banner*"

e introducir el resto de datos del servidor a emplear con las recomendaciones dadas en esta misma guía.

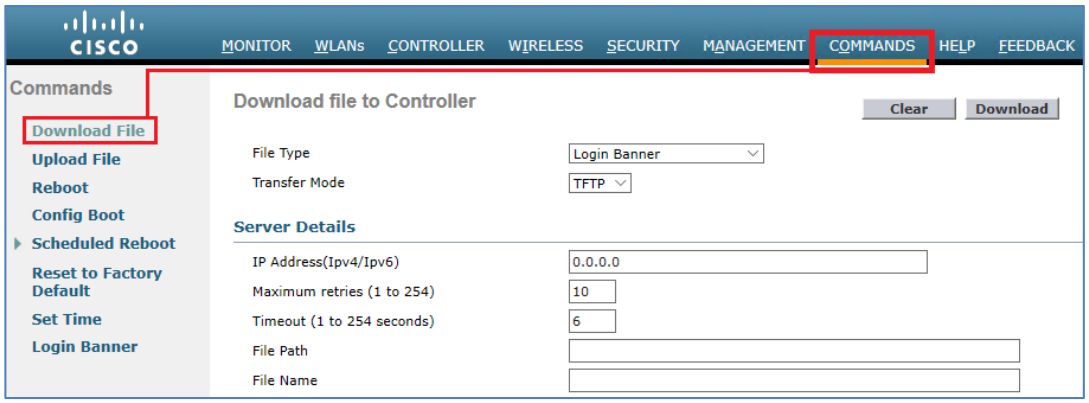


Ilustración 21. Subida al controlador del *banner* de inicio de sesión

92. Toda la información relacionada con la configuración del *banner* puede encontrarse en *"Management of Controllers -> Managing Configuration -> Downloading a Login Banner File"* [16].

5.2.7 FINALIZACIÓN DE LA SESIÓN

93. 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.

94. 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):

    (Cisco controller) > config sessions timeout [0-160]

95. 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, aunque en esta ocasión el tiempo es expresado en segundos):

    (Cisco controller) > config sessions timeout [0-9600]

96. **Se debe configurar la opción de cierre de sesión inactiva, con el menor tiempo posible antes del bloqueo.**

97. 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.

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

5.2.8 GESTIÓN LOCAL DE USUARIOS Y SESIONES

99. En los controladores WLC la autenticación de usuarios 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.

100. 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.

5.2.8.1 CONFIGURACIÓN LOCAL DE USUARIOS

101. Los dispositivos Cisco WLC 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, y esta última opción es la recomendación (también es la opción habilitada por defecto). El algoritmo de cifrado empleado para esto es AES-128 y la clave de cifrado empleada es una clave preconfigurada de fábrica y distinta por cada dispositivo. Las contraseñas cifradas se almacenan en el fichero de configuración. En caso de que no estuviera habilitado, se debe habilitar manualmente mediante el siguiente comando:

    (Cisco Controller) > config switchconfig secret-obfuscation enable

102. Cuando está habilitado el cifrado de contraseñas, todas las 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.

103. Si se deshabilita el cifrado de contraseñas, 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.

104. 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 del cifrado añadiendo una clave de cifrado, que se empleará junto con la clave por defecto que tiene el dispositivo para cifrar las contraseñas. 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.

105. El cifrado de tipo 6 está deshabilitado por defecto.

106. El cifrado de tipo 6 es empleado en las siguientes configuraciones de credenciales:

a) Usuarios de red local [17].

b) *Pre-shared Key* de servidores RADIUS (Autentación, *Accounting* y DNS).

c) Claves de servidores TACACS+ (Autenticación, *Accounting*, Autorización y DNS).

d) Claves IPSec.

e) Claves LDAP.

f) SXP.

g) Claves WPA2 PSK.

h) Usuarios de gestión local.

107. Existen una serie de recomendaciones y limitaciones para el cifrado de contraseñas, que se exponen a continuación:

a) No es posible recuperar configuraciones que contienen claves cifradas mediante el método de cifrado tipo 6.

b) El cifrado de tipo 6 únicamente se puede emplear tras haber habilitado el cifrado general y haber configurado la clave adicional.

c) No es posible modificar la clave adicional del método tipo 6 si está habilitado. Se debe deshabilitar este método de forma previa a la modificación de la clave adicional.

d) Si en algún momento es necesario emplear una versión de *software* que no soporta el cifrado de tipo 6, la recomendación es descifrar todas las claves y cifrarlas como tipo 7, o bien deshabilitar el cifrado de forma global.

e) Si se desea trasladar la configuración entre dos (2) dispositivos, se recomienda descifrar la configuración, cargarla sobre el dispositivo destino y posteriormente configurar la misma clave adicional que en el dispositivo original.

f) Si existe un fallo en la unidad y no se puede leer la clave adicional, se lanza un mensaje sobre la sesión SSH o por puerto de consola. Puede usar la información de ese mensaje para recuperar el dispositivo, aunque con una configuración en blanco.

g) El método de cifrado tipo 6 no se puede emplear en el método de configuración *Cisco WLAN Express*.

h) La clave adicional del método de cifrado tipo 6 siempre va seguido de una comprobación de clave segura.

i) Para usuarios locales de grupos *FlexConnect* no es posible habilitar cifrado de tipo 6 mediante modificación del fichero de configuración. Es decir, no se podrá obtener un fichero de configuración con cifrado tipo 7, habilitar el

cifrado tipo 6 (por línea de comandos) y cargar la configuración de nuevo con el fichero de cifrado tipo 7.

108. Para configurar este método de cifrado tipo 6, se deben ejecutar los siguientes comandos:

a) Habilitar cifrado de claves:

(Cisco Controller) > config switchconfig secret-obfuscation enable

b) Configurar la clave adicional usada para el método de cifrado tipo 6:

(Cisco Controller) > config switchconfig password-encryption key valor-ascii

c) Habilitar el cifrado de tipo 6:

(Cisco Controller) > config switchconfig password-encryption enable

d) Comprobar el estado del cifrado tipo 6:

(Cisco Controller) > show switchconfig

5.2.8.2 ROLES DE USUARIO

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

a) Rol de administrador (usuario tipo *Read-Write*): El usuario con este perfil tiene acceso completo al equipo, incluyendo comandos avanzados por terminal de consola o SSH. Puede crear, editar y eliminar una configuración sin restricciones.

b) 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 o eliminar configuraciones de ningún tipo.

c) 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-Only*. 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.

5.2.8.3 CONFIGURACIÓN LOCAL DE LA POLÍTICA DE CONTRASEÑAS

110. 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.

111. 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.

112. Las políticas de contraseñas se configuran bajo el menú "*Security*", dentro de la sección "*AAA -> Password Policies*". Dentro de esta sección, en la pantalla principal

nos aparecerán todas las posibles opciones organizadas en tres categorías: *Local Management User and AP*, *Management User* y *SNMPv3 User*.

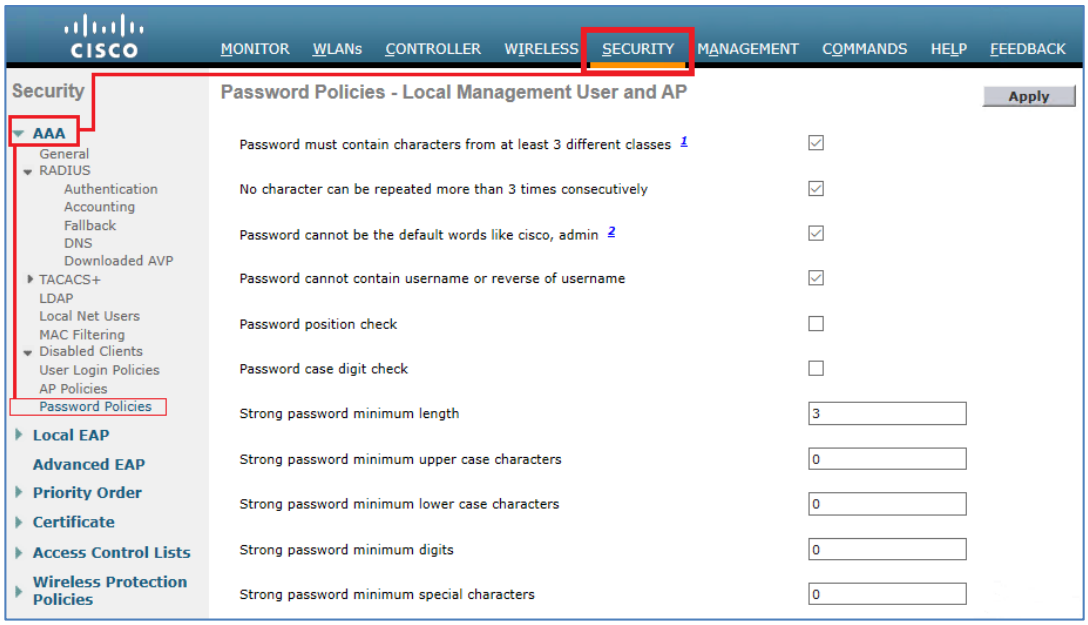


Ilustración 22. Gestión de la política de contraseñas

113. En la categoría "*Local Management User and AP*", se encuentran los siguientes campos configurables (en orden de aparición):

a) Obligar a que la clave contenga tres o cuatro tipos de caracteres distintos (mayúsculas, minúsculas, dígitos y caracteres especiales '(' , '!', '@', '#', '$', '%', '^', '&', '*', ')'. **Se recomienda habilitar esta opción.**

b) No se puede concatenar el mismo carácter más de tres veces seguidas (por ejemplo, no se puede dar el caso de una contraseña tipo "*Paaasword", "ClaVVVe*"). **Se recomienda habilitar esta opción.**

c) Las claves no pueden ser como el nombre del fabricante ("cisco") o del usuario de gestión principal ("*admin*"). Tampoco pueden ser una variante de su orden inverso ("*ocsic*", "*nimda*"), ni variantes que sean sustituciones del carácter "i" por alguno de los caracteres {1, |, !}, o del carácter "o" por "0" ni "s" por "$". **Se recomienda habilitar esta opción.**

d) Las claves de usuarios con nombre genérico no podrán contener dicho nombre ni su variante en orden inverso. **Se recomienda habilitar esta opción.**

e) Comprobar un rango de cuatro caracteres para evitar su repetición en la nueva contraseña.

f) Longitud mínima de clave segura. **Se recomienda una longitud mínima de 12 caracteres.**

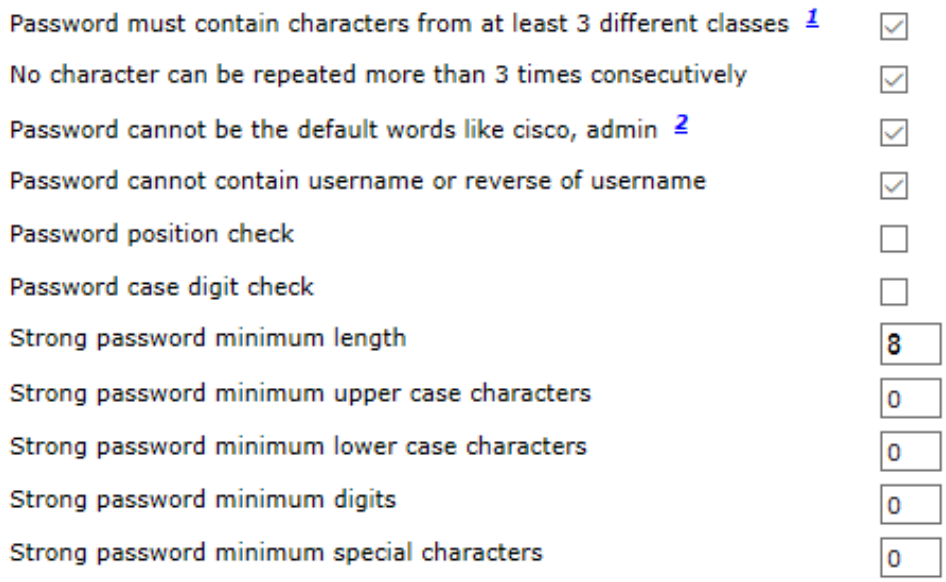


Ilustración 23. Gestión de las propiedades de la contraseña

Las cuatro últimas opciones son el mínimo número de apariciones que debe tener en la clave los cuatro tipos de caracteres (mayúsculas, minúsculas, dígitos y caracteres especiales respectivamente).

114. Para estos campos, existe su correspondiente versión de comandos, que de forma resumida sería el siguiente [18]:

(Cisco Controller) > config swtichconfig strong-pwd {case-check | consecutive-check | default-check | username-check | all-checks | position-check | case-digit-check} {enable | disable}

Donde:

a) *Case-check*: comprueba la triple aparición consecutiva de un carácter.

b) *Consecutive-check*: comprueba si se intentan usar los valores por defecto o variantes de los mismos.

c) *Default-check*: Comprueba si se intenta usar el nombre de usuario o su orden inverso.

d) *All-checks*: Habilita/Deshabilita todas las comprobaciones de claves seguras.

e) *Position-check*: Comprueba un rango de cuatro caracteres para evitar su repetición en la nueva contraseña.

f) *Case-digit-check*: Comprueba si los cuatro tipos de caracteres se están empleando (mayúsculas, minúsculas, dígitos y caracteres especiales.

Con el siguiente comando se configura el mínimo número de caracteres mayúsculas (*uppser-case*), minúsculas (*lower-case*), dígitos (*digits*) y caracteres especiales que debe contener una contraseña:

(Cisco Controller) > config swtichconfig strong-pwd mínimum {upper-case | lower-case | digits | special-chars} num-of-chars

Con este comando se configura el mínimo número de caracteres que debe contener una contraseña:

(Cisco Controller) > config swtichconfig strong-pwd min-length pwd-length

115. Tanto en la categoría "*Management User*" como "*SNMPv3 User*" los campos que se pueden configurar son iguales, por lo que, para simplificar esta guía, se muestra el siguiente que es aplicable a ambas categorías. Se dispone de las siguientes opciones (en orden de aparición):

a) Bloqueo del usuario de gestión. Se debe activar esta opción para evitar ataques de fuerza bruta.

b) Número de intentos fallidos antes de bloquear al usuario de gestión**. La opción recomendada es 3.**

c) Minutos que permanecerá bloqueado el usuario de gestión.

d) Días en los que expirará la contraseña para el usuario de gestión (0 días indica que no expira nunca). **Se recomienda que no exceda de 60 días.**

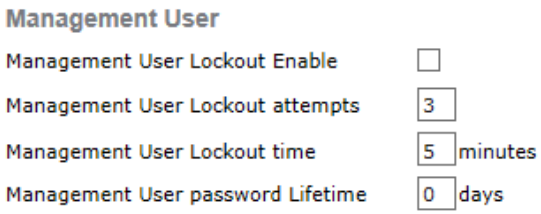


Ilustración 24. Propiedades de gestión del usuario

116. Los comandos que se deben emplear para configurar estas secciones son los que se muestra a continuación (teniendo en cuenta que una de las variables configurables es el tipo de usuario, siendo "*mgmtuser*" para usuario de gestión y "*snmpv3user*" para usuario de SNMP v3):

Configuración del bloqueo de la cuenta de usuario:

(Cisco Controller) > config swtichconfig strong-pwd lockout {mgmtuser | snmpv3user} {enable | disable}

Configuración del tiempo que permanece bloqueada de la cuenta de usuario:

(Cisco Controller) > config swtichconfig strong-pwd lockout time {mgmtuser | snmpv3user} timeout-en-minutos

Configuración del número de intentos para introducir la contraseña del usuario. Superado ese número se bloqueará la cuenta:

(Cisco Controller) > config swtichconfig strong-pwd lockout attempts {mgmtuser | snmpv3user} numero-de-intentos

Configuración del número de días en el que será válida la contraseña:

(Cisco Controller) > config swtichconfig strong-pwd lifetime {mgmtuser | snmpv3user} numero-de-dias

5.2.8.4 SINCRONIZACIÓN HORARIA (NTP)

117. **Los controladores inalámbricos deben estar sincronizados** a través de un servidor NTP/SNTP proporcionado por el entorno. 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.

118. 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.

119. De forma adicional, y para aumentar el nivel de seguridad, la conexión al servidor NTP externo para la sincronización de tiempo debe ser autenticada, para evitar sufrir algún tipo de ataque basado en la manipulación de la señalización horaria en el controlador [19]. Se debe configurar la autenticación de la fuente de tiempo

120. Aunque la recomendación es usar un servidor de sincronización horaria, esta opción presenta el inconveniente de que, si la diferencia de tiempo entre el servidor NTP y el controlador supera los 1000 segundos, el proceso *ntpd* será abortado y añade un mensaje de alerta en el registro de mensajes del sistema (*logs*). En este caso se debe volver a una configuración horaria manual.

121. Para configurar el servidor SNTP, basta con acceder al menú "*Controller*" y seleccionar la sección "*NTP->Server*" o "*NTP->Keys*". En primer lugar, se debe acceder a esta última sección para crear una nueva clave de autenticación. Para ello, se debe pulsar el botón "*New…*" en la parte superior derecha.

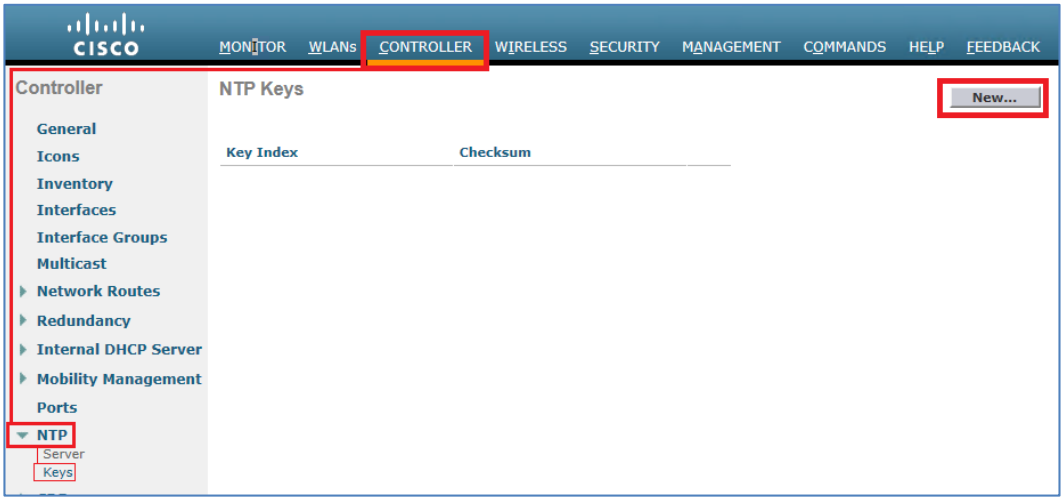


Ilustración 25. Gestión del NTP en el controlador

122. En la ventana principal aparecerán las siguientes opciones a completar:

    a) *Key index*: Se trata de un identificador numérico que se empleará posteriormente en la configuración del servidor NTP/SNTP.

b) *Key format*: Es un parámetro que indica el formato en el que se introduce la clave. Las posibilidades que ofrece es clave en formato ASCII (con el mismo nombre) o en formato Hexadecimal (aparecerá como "HEX").

c) *Key*: Es el campo donde se debe introducir la clave en el formato especificado anteriormente.

d) Una vez finalizada la inserción de los datos, se deben aplicar los cambios pulsando en el botón "*Apply*" de la esquina superior derecha.

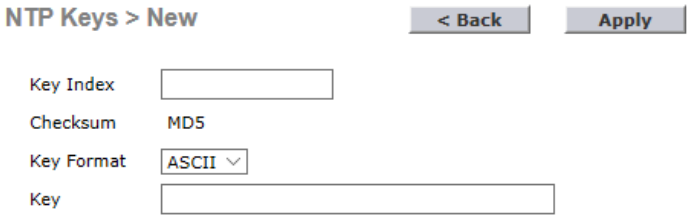


Ilustración 26. Gestión de claves para NTP/SNTP

123. A continuación, se debe configurar la información del servidor NTP/SNTP. Para ello, hay que dirigirse a la sección "*NTP->Server*" bajo el menú "*Controller*". En la ventana principal aparecerá la siguiente información o campos configurables:

a) *NTP Polling Interval seconds*: Es el parámetro que indica el tiempo de intervalo de sondeo hacia los servidores NTP/SNTP que realizará el controlador inalámbrico.

b) *NTP Version*: Indica la versión del protocolo de sincronización horaria (las opciones son "3" o "4"). Marcar 4.

c) Las dos opciones anteriores tendrán efecto en esta misma ventana principal, pulsando sobre el botón "*Apply*" que aparece en la esquina superior derecha.

d) En el caso de que se emplee la versión 4 del protocolo NTP, aparecerá el estado de los sondeos hacia el servidor NTP/SNTP.

e) Para añadir un nuevo servidor, se debe pulsar el botón "*New*" que aparece en la esquina superior derecha.

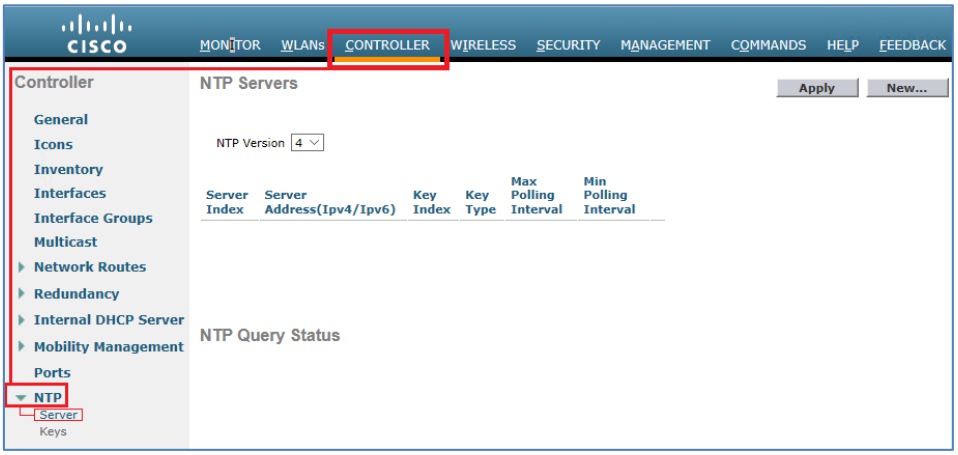


Ilustración 27. Configuración del servidor NTP/SNTP

124. Una vez pulsada la opción de añadir un nuevo servidor, aparecerá en la ventana principal la siguiente información a completar:

    a) *Server Index* (*Priority*): Es un valor numérico que indicará el orden de preferencia a la hora de realizar sondeos entre distintos servidores NTP/SNTP.

    b) *Server*: Es un valor en formato ASCII que indicará la dirección del servidor, que puede ser "IPv4", "IPv6" o bien un nombre *FQDN* mediante la opción "DNS". 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 ('..')

    c) *Enable NTP Authentication*: Habilita/Deshabilita la opción de autenticación contra el servidor. Se debe habilitar esta opción.

    d) *Key Index*: Es el índice de la base de datos de claves que se empleará al realizar sondeos contra el servidor. Este valor debe haber sido configurado previamente (en este guía aparece justo antes de configurar el servidor por este mismo motivo).

125. Para finalizar el proceso de alta de un nuevo servidor se debe utilizar el botón "*Apply*", que aparece en la esquina superior derecha.

Ilustración 28. Finalización del proceso de alta de un controlador

126. Para la configuración de NTP se pueden usar una serie de comandos que, de forma esquematizada, se pueden consultar en el siguiente diagrama (donde se marca entre los signos "< >" las variables a introducir por el gestor del controlador inalámbrico.

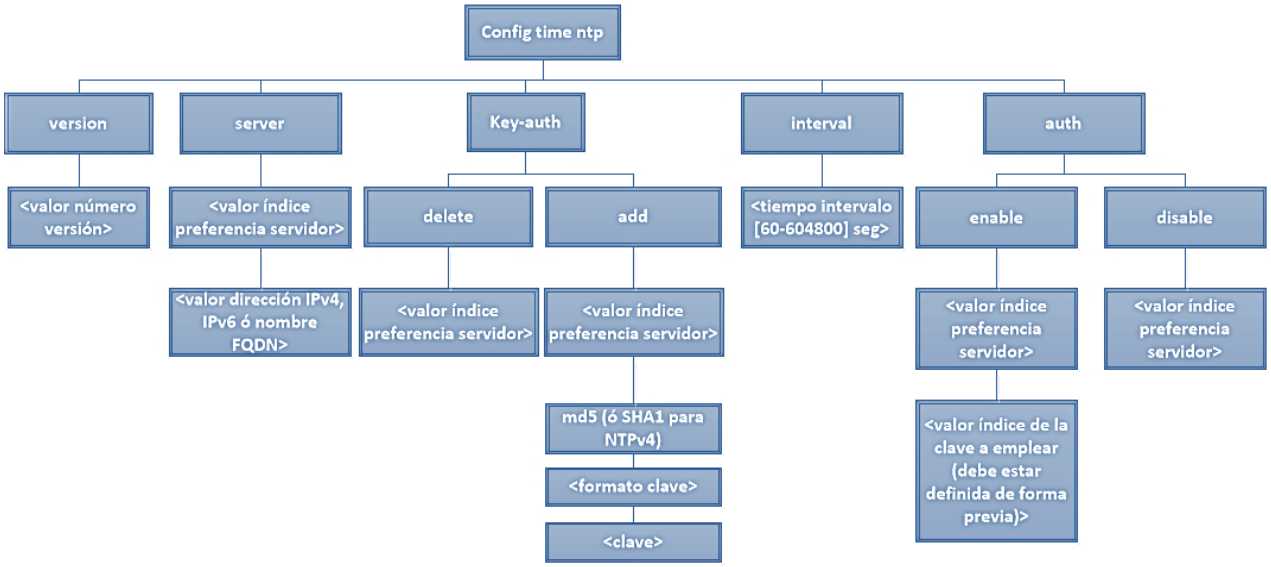


Ilustración 29. Jerarquía de comandos NTP

127. De forma más explícita, se muestran los comandos a continuación:

a) El siguiente comando muestra la configuración de la versión del protocolo NTP/SNTP que empleará el controlador inalámbrico (aplica de forma global).

(Cisco Controller) > config time ntp version {3 | 4}

b) El siguiente comando (que es opcional ya que existirá un valor por defecto) especifica el intervalo de sondeo entre las consultas del controlador inalámbrico al servidor NTP/SNTP.

(Cisco Controller) > config time ntp interval [60-604800]

c) El siguiente comando crea una clave de autenticación, donde se indica el índice de la clave en la base de datos, el tipo de clave (SHA1 disponible pero para NTP versión 4), el formato de la misma y la clave en sí.

(Cisco Controller) > config time ntp key-auth add key-index sha1 {ascii | hex} key

d) El siguiente comando habilita la autenticación, teniendo en cuenta que los parámetros que aparecen son los índices de preferencia de consulta de servidor NTP y el índice de la clave de autenticación configurada previamente (en orden de aparición).

(Cisco Controller) > config time ntp auth enable server-index key-index

e) El siguiente comando elimina una clave de autenticación ya creada, indicándole el índice que ocupa en la base de datos.

(Cisco Controller) > config time ntp key-auth delete key-index

f) El siguiente comando deshabilita la autenticación contra un servidor NTP ya existente. El servidor se selecciona mediante el parámetro de índice de preferencia de consulta.

(Cisco Controller) > config time ntp auth disable server-index

6. LICENCIAMIENTO

128. Para asociar los puntos de acceso a los controladores inalámbricos de Cisco se requieren licencias. El tipo de licenciamiento puede ser varios tipos:

   a) Licenciamiento tradicional: Requiere de un fichero de licencias que debe ser cargado de forma manual en el controlador. Este fichero, tras la compra, está disponible en el perfil de licencias del usuario que gestiona el perfil en los portales correspondientes de Cisco. Las licencias estarán asociadas a un equipo físico concreto mediante el número de serie del mismo.

   b) Licenciamiento tipo RTU (*Right to Use*): En este tipo de licencias, tras el pago de las mismas, se pueden aumentar directamente las licencias sobre el controlador sin necesidad de un fichero adicional.

   c) *Smart Licensing*: En este caso, las licencias residen en el perfil del usuario Cisco, y se asocian al controlador correspondiente por validación de *Token*.

129. Para todas ellas, se deberá tener en consideración el uso de protocolos seguros, así como de las precauciones al realizar el proceso de registro y *login* en el portal de Cisco.

6.1.1 LICENCIAMIENTO TRADICIONAL

130. Como se ha expuesto, este tipo de licenciamiento requiere de un fichero de licencia que está asociado al controlador al que se desea aumentar la capacidad de puntos de acceso soportados. En este caso, se obviará el proceso de obtención del fichero ya que requiere de una compra previa e interacción con el portal, que no es objeto de esta guía. Es decir, se asumirá que ya se dispone del fichero.

131. Para realizar la carga del mismo, la única opción disponible es mediante protocolo TFTP, que no ofrece seguridad en la transferencia de archivos. Por tanto, **se debe evitar el uso de este licenciamiento**. En caso de ser necesario, la recomendación es limitar al controlador y a un único usuario los accesos hacia ese servidor TFTP. El usuario subirá el fichero al servidor TFTP, el controlador lo descargará, y una vez realizada esta operación, se debe eliminar el fichero del servidor para evitar filtración de información sensible.

132. Para realizar esta descarga a través del controlador, hay que dirigirse al menú "*Management*", y sobre la sección izquierda navegar hasta la sección "*Software Activation → Commands*".

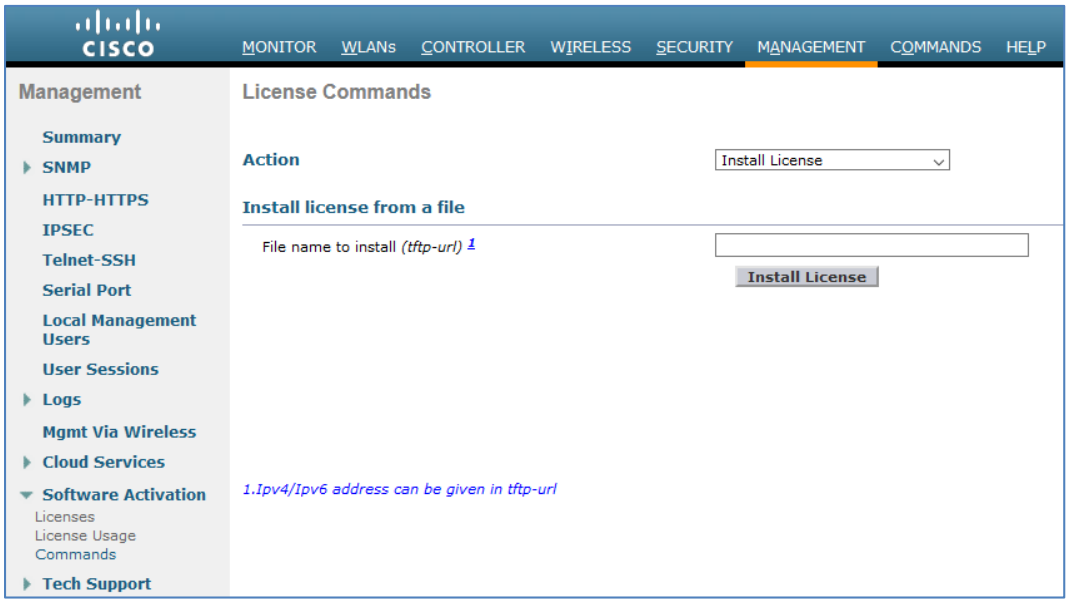


Ilustración 30. Comandos de licenciamiento tradicional en el interfaz gráfico

133. Una vez en esa sección, será necesario indicar la URL junto con el nombre del fichero de licencias que reside en el servidor TFTP. Para que aplique las licencias es necesario realizar un reinicio del controlador, teniendo en cuenta que esto afectará de forma global al servicio inalámbrico que se presta (si es que no se dispone de una arquitectura HA, o de un segundo controlador inalámbrico).

6.1.2 LICENCIAMIENTO DE TIPO RTU

134. Este tipo de licenciamiento es el más sencillo y seguro, ya que no hay traspaso de información en forma de ficheros de licencia. **Se recomienda, por tanto, esta opción frente a la anterior.** Las licencias son adquiridas y residen en el perfil del usuario de Cisco, siendo únicamente necesario indicar en el controlador el número de licencias a añadir.

135. Para ello, hay que dirigirse al menú "*Management*", y sobre la sección izquierda navegar hasta la sección "*Software Activation → Licenses*". En esta sección aparecerá la opción de añadir licencias, basta con indicar el número y aplicar pulsando sobre "*Set Count*".

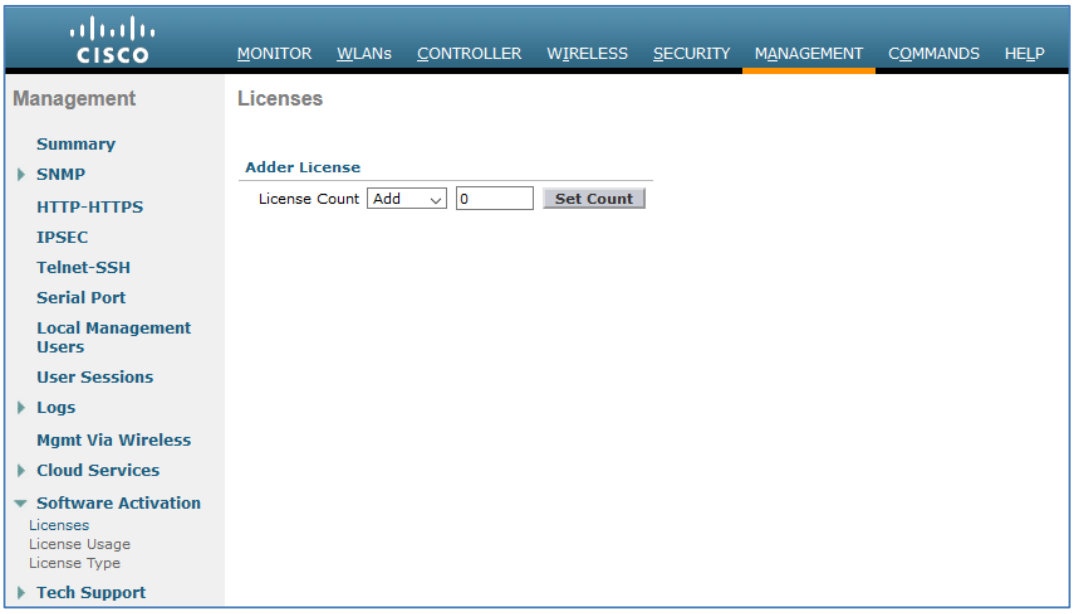


Ilustración 31. Comandos de licenciamiento RTU en el interfaz gráfico

6.1.3 SMART LICENSING

136. En este caso, las licencias residen en el perfil de Cisco.

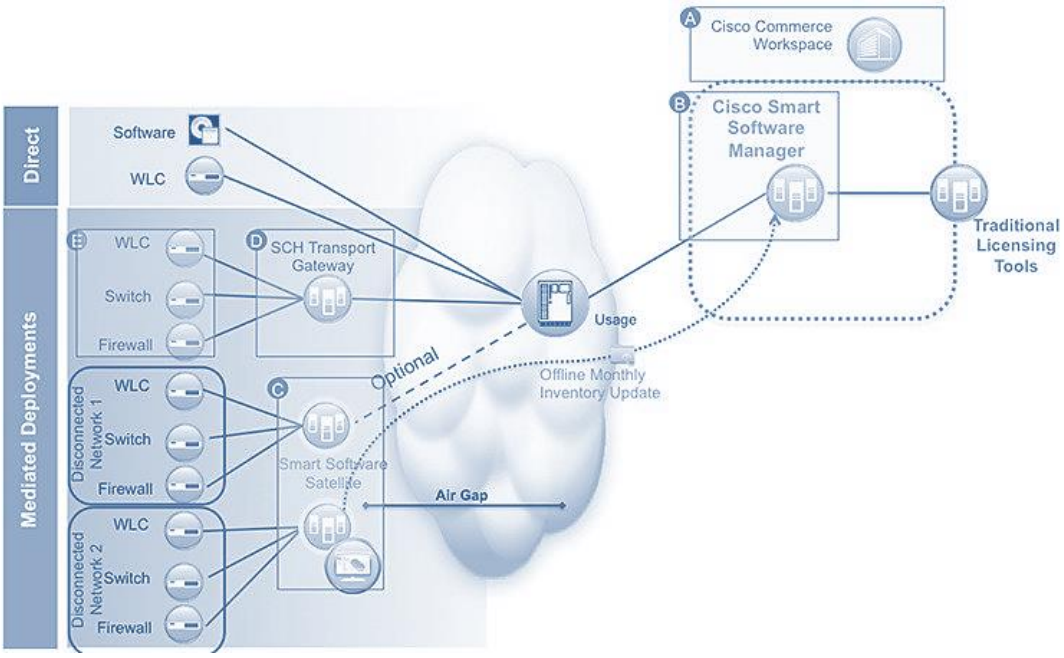


Ilustración 32. Tráficos implicados en el *Smart Licensing*

137. En este sentido, hay cuatro (4) opciones, cuya sencillez es inversamente proporcional a la seguridad:

a) Realizar una transferencia HTTPS desde los dispositivos hacia el servidor en la nube a través de Internet.

b) Realizar una transferencia de ficheros a través de un proxy HTTPS (como puede ser *el Smart Call Home Transport Gateway*).

c) Emplear el software "*Cisco Smart Software Satellite*", que envía información de forma periódica basado en una sincronización de la red hacia el servidor en la nube. Ese *software* será el único que manda información y se puede configurar sobre qué dispositivos se desea enviar información.

d) La última opción es emplear el software nombrado en el punto anterior, pero usando una sincronización manual (recomendada una vez al mes). En este modelo, el sistema no está directamente conectado, sino que existe un aislamiento entre la red del dispositivo y la nube de Cisco.

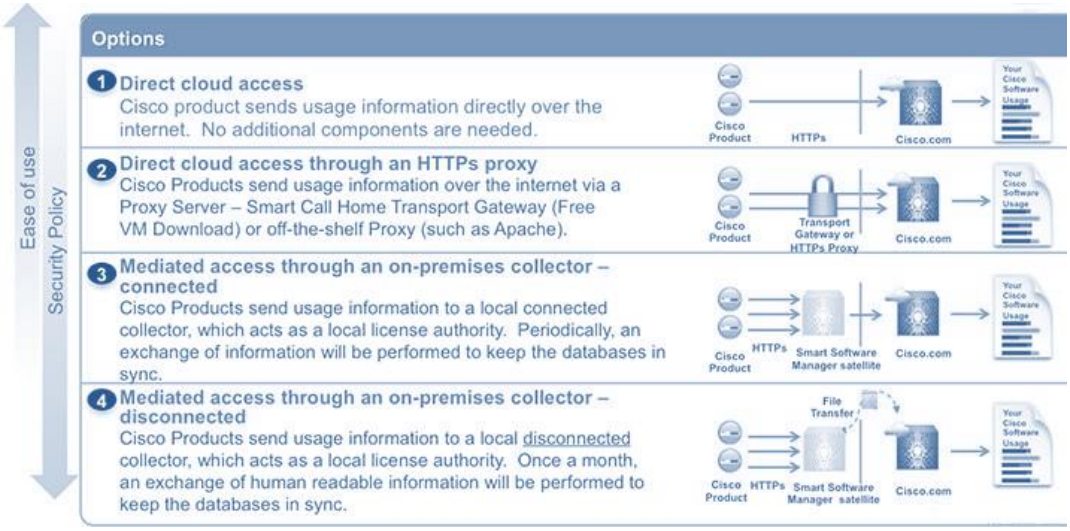


Ilustración 33. Opciones para la implementación del Smart Licensing

138. Se detalla a continuación el proceso, omitiendo el paso de obtener una *Smart Account* de Cisco. Se detallarán los tres (3) principales modos de funcionamiento (el último es una manera alternativa del tercero en modo offline).

Modo 1: Direct Cloud, o acceso directo a la nube de Cisco

a) Registro y Activación – Creación del *token*: Para activar el equipo es necesario obtener un *token*. Los *tokens* de activación se almacenan en la *Smart Account*, en la tabla de *token* de instancia de registros de productos. Una vez finalizado el procedimiento completo, no se necesitará más el *token* por lo que puede ser eliminado de esta tabla y así añadir un paso de seguridad. Los *tokens* tienen una validez de entre 1 y 365 días.

b) En la *Smart Account*, sobre la pestaña general, pulsar sobre "*New Token*".

c) En la ventana emergente, introducir una descripción y el número de días que se desea sea válido el *token*. Seleccionar la opción "*Allow export-controlled functionality*" y "*Aceptar términos y condiciones*".

d) Pulsar "Create Token".

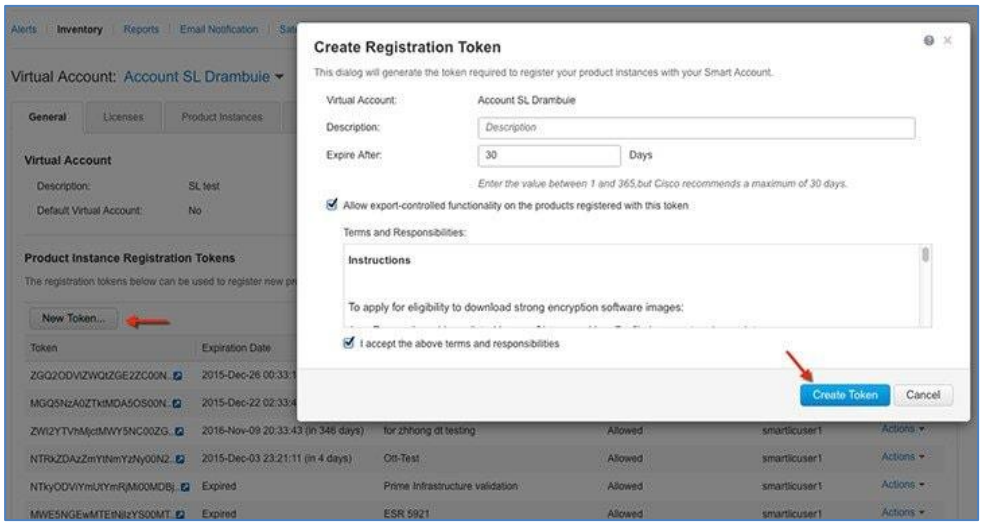


Ilustración 34. Creación de un *token* para *Smart Licensing*

e) Una vez creado, copiar el nuevo *token*, que será necesario incorporar en el controlador inalámbrico.

f) Si el controlador inalámbrico no está en el modo *Smart Licensing*, activarlo dirigiéndose al menú "*Management*", y sobre la sección izquierda navegar hasta la sección "*Software Activation → License Type*". Requiere de un reinicio del controlador si no estaba ya activado.

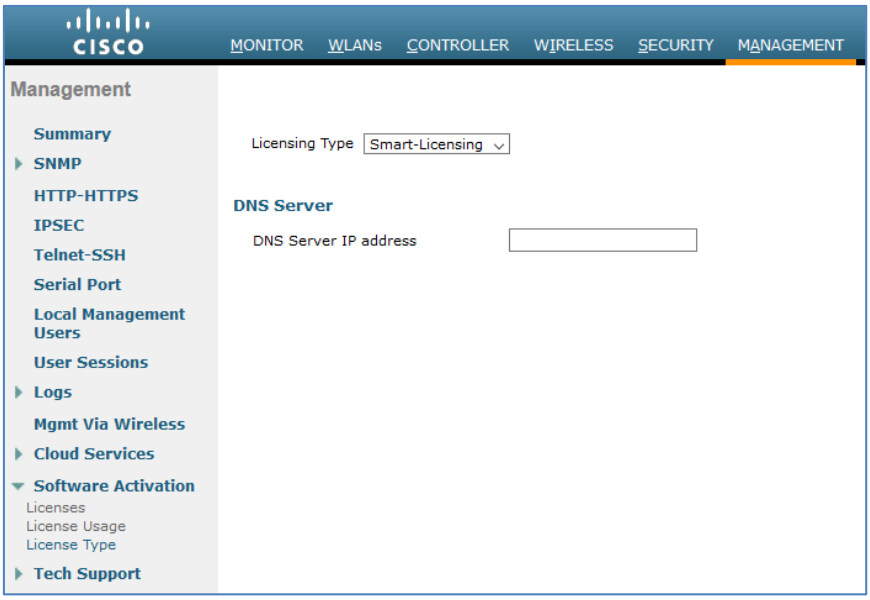


Ilustración 35. Configuración del controlador para *Smart Licensing*

g) Introducir el *token* generado en la gestión de la *Smart Account*. Para ello, navegar sobre el menú "*Management*" y, en la sección izquierda, en "*Smart-License->Device Registration*". Aparecerá en pantalla el tipo de acción, que debe ser "*Registration*" y un campo donde poder introducir el *token*.

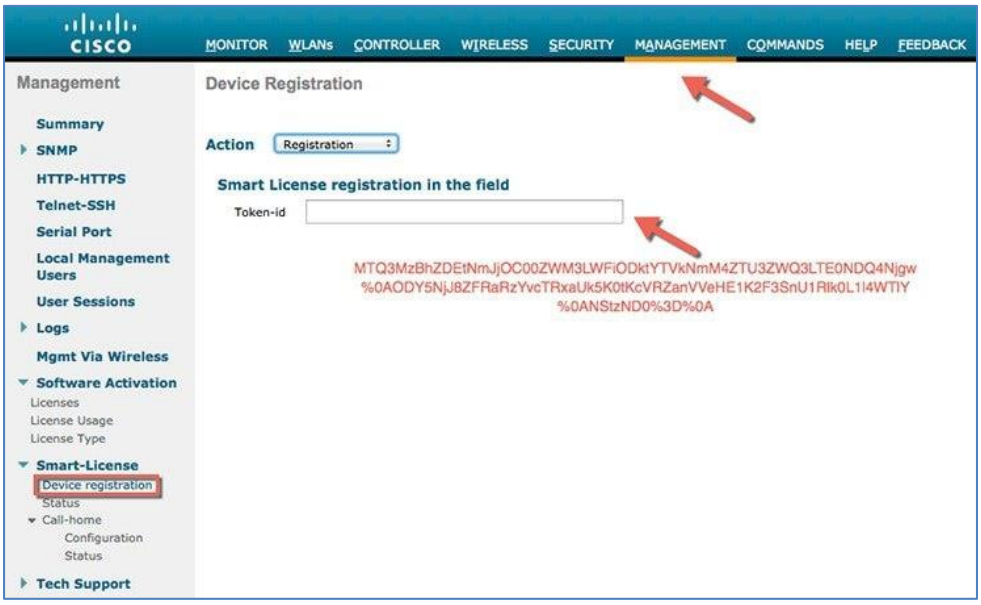


Ilustración 36. Registro de un *token* en *Smart Licensing*

h) Verificar el estado del registro y autorización en la pestaña "*Management*" en la sección "*Smart-License->Status*", seleccionando como parámetro "*Status*". Deberá aparecer como estado "**Registered**".

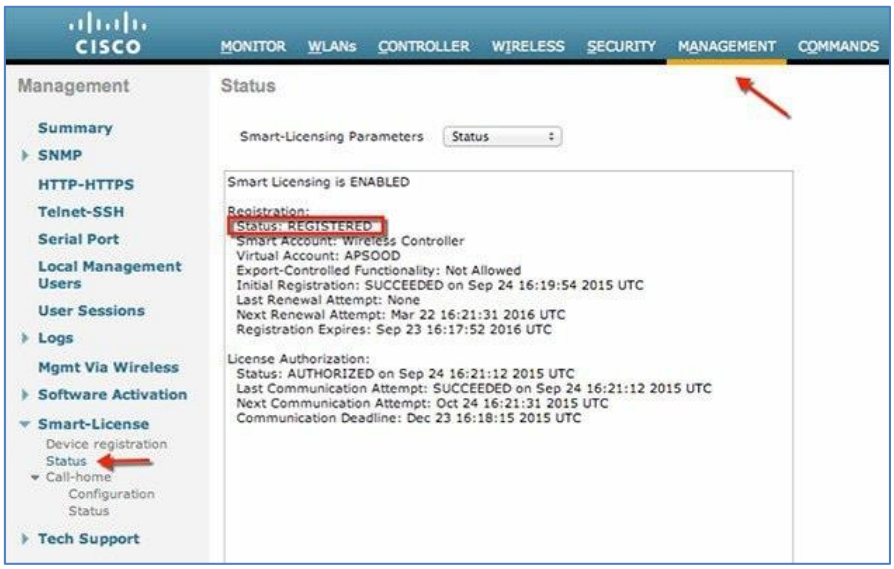


Ilustración 37. Verificación del estado de registro

i) En la *Smart Account* aparecerá bajo la pestaña "*Product instances*" que el equipo ha sido registrado.

j) Una vez que los puntos de accesos se registran en el controlador, las licencias son solicitadas en un plazo máximo de 24 horas. Las licencias consumidas se pueden ver en la pestaña "*Management*", en la sección "*Smart-License->Status*" y con el parámetro "*In-Use*".

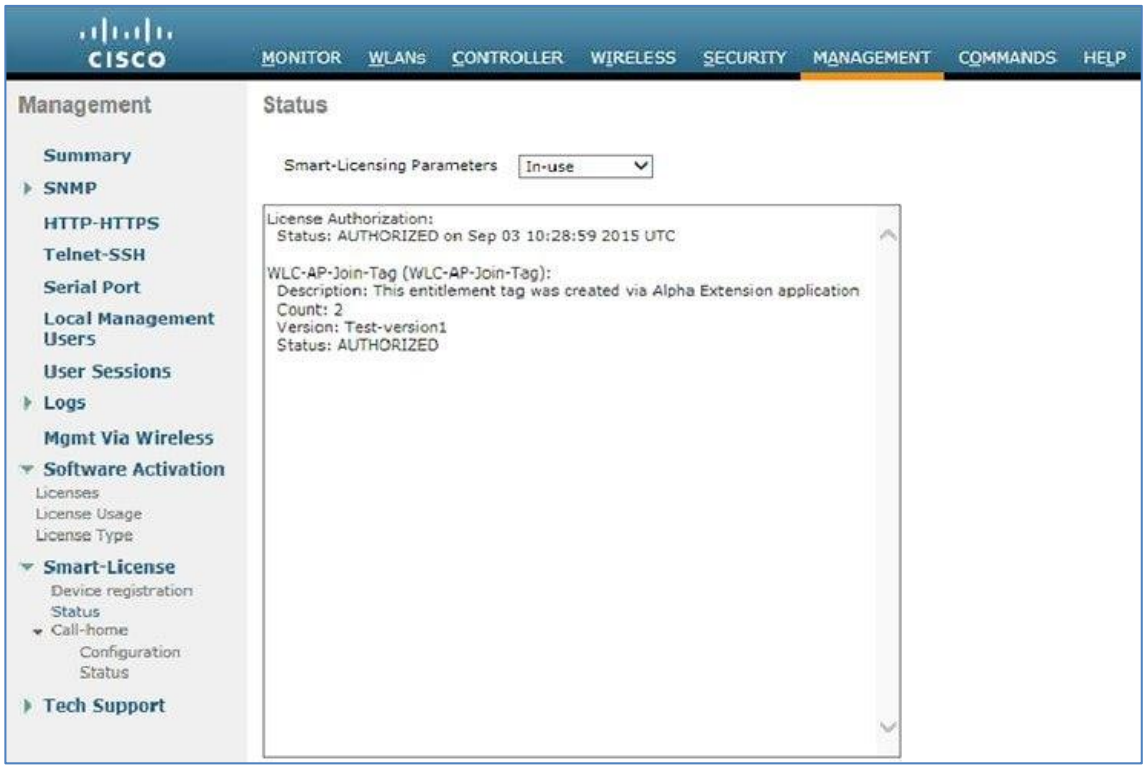


Ilustración 38. Comprobación de licencias consumidas

k) También se pueden ver en la misma sección, con el parámetro "*Summary*":

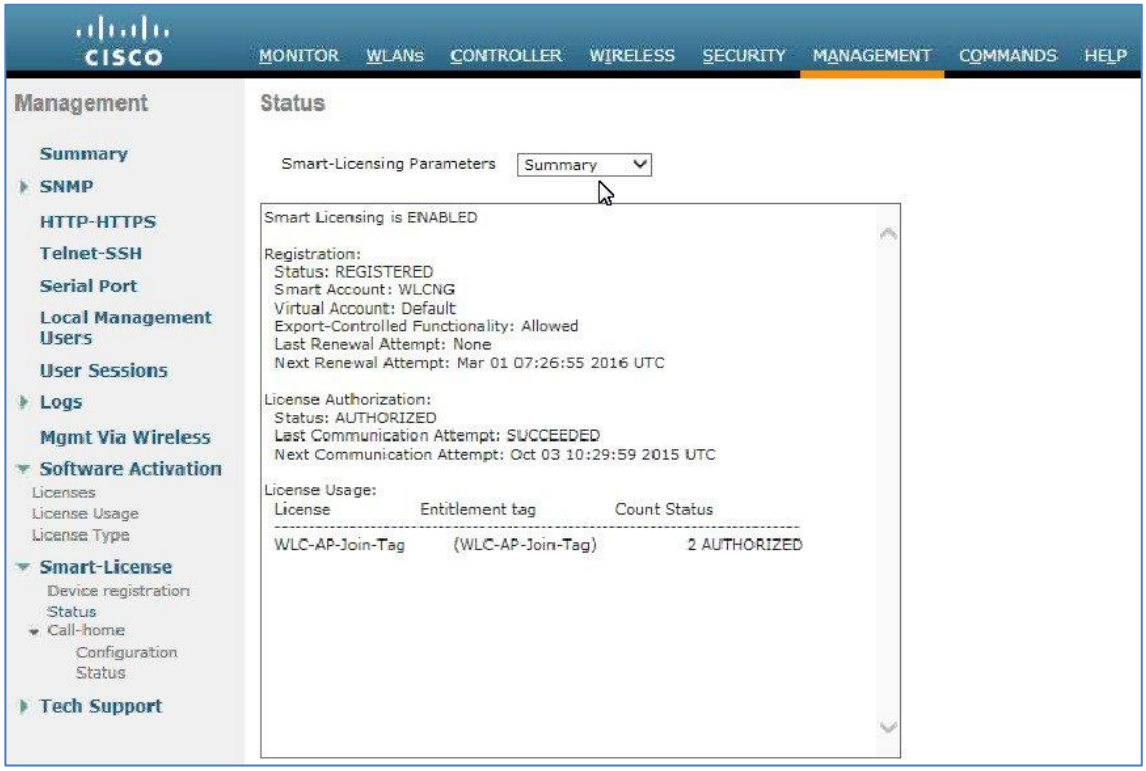


Ilustración 39. Comprobación de licencias consumidas

Modo 2: Con *proxy* o *Transport Gateway*

a) En este método, los equipos envían la información de consumo de licencias a través de un servidor Proxy (*Smart Call Home Transport Gateway*). Es necesario tenerlo instalado, y se recomienda usar la guía del propio fabricante [20].

b) En el controlador, esta opción se configura de la siguiente manera:

- Ir a la pestaña "*Management*" y navegar hasta la sección "*Smart-License->Call-home->Configuration*".
- Verificar que el perfil TAC por defecto está habilitado y aplicar cambios.
- La configuración puede ser consultada en la sección "*Smart-License->Call-home->Status*".

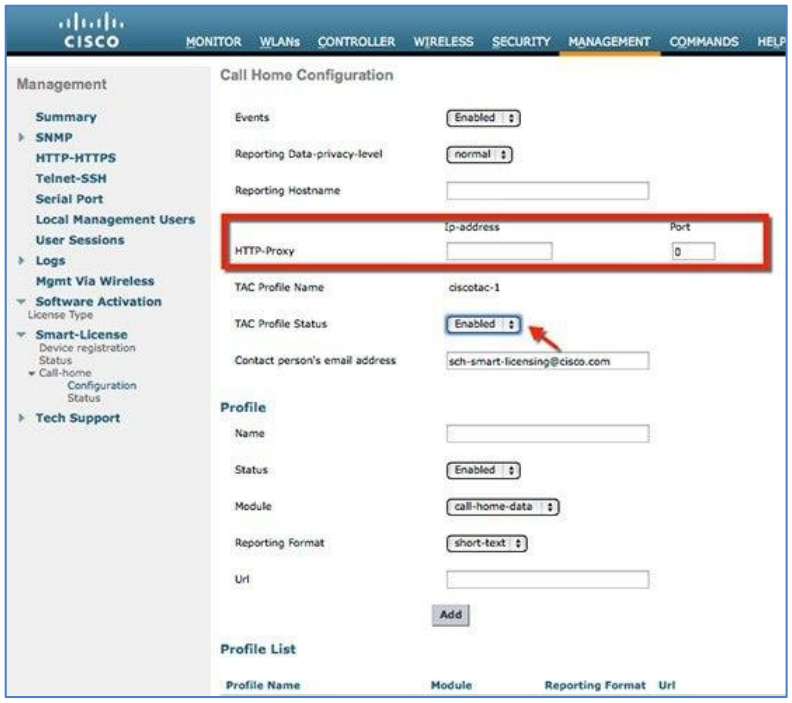


Ilustración 40. *Smart Licensing* con *Transport Gateway*

Modo 3: Acceso controlado a través del *software Smart Software Satellite*.

a) El software "Cisco Smart Software *Manager Satellite*" es un componente de *Cisco Smart Licensing* y trabaja de forma conjunta con *Cisco Smart Software Manage*r. Estos programas ayudan a gestionar de forma óptima las licencias de los equipos, proporcionando casi a tiempo real la visibilidad de las mismas e informando de las licencias que se comprar y consumen.

b) Para maximizar la seguridad, se puede instalar *Smart Software Manager Satellite* de manera que proporciona un subconjunto de funcionalidades de *Cisco Smart Software Manager*. Las siguientes funciones se pueden realizar de forma local sin necesidad de enviar información a través de Internet:

- Activar o registrar licencias.

- Obtener visibilidad de las licencias corporativas.
- Transferir licencias entre entidades corporativas.

c) Para descargar, instalar y configurar este *software*, se recomienda seguir la guía del fabricante [21].

d) En el controlador, hay que configurar lo siguiente:

- Dirigirse a la pestaña "*Management*". Navegar a la sección "*Smart-License->Call-Home->Configuration*" y configurar un nuevo perfil de "*Call-Home*", especificando nombre, estado, módulo, formato de informes y URL donde reside el programa *Smart Software Manager Satellite*. Finalizar añadiendo el perfil pulsando sobre "*Add*".

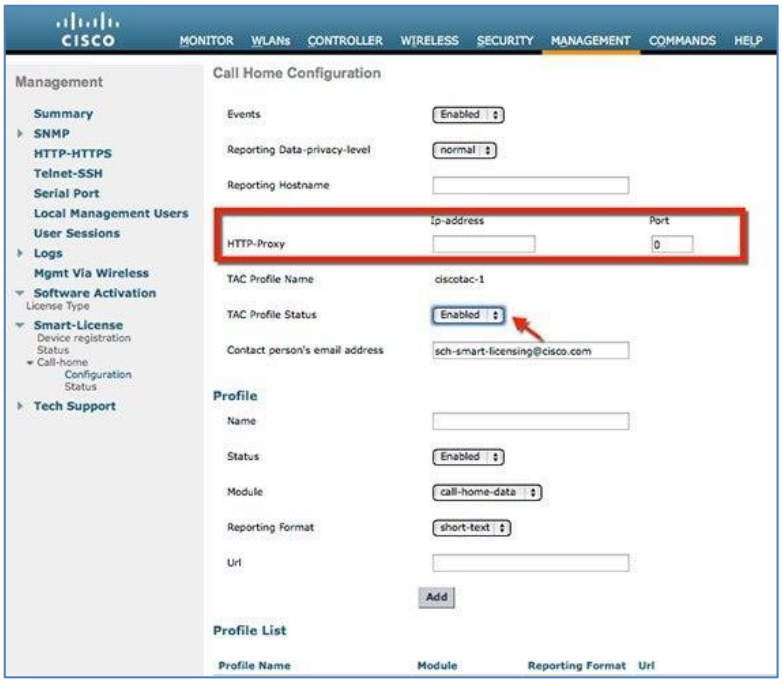


Ilustración 41. *Smart Licensing* con *Smart Software Satellite*

- Dirigirse a la pestaña "*Management*". Navegar a la sección "*Smart-License->Call-Home->Configuration*" y configurar un nuevo perfil de "*Call-Home*", especificando nombre, estado, módulo, formato de informes y URL donde reside el programa *Smart Software Manager Satellite*. Finalizar añadiendo el perfil pulsando sobre "*Add*".

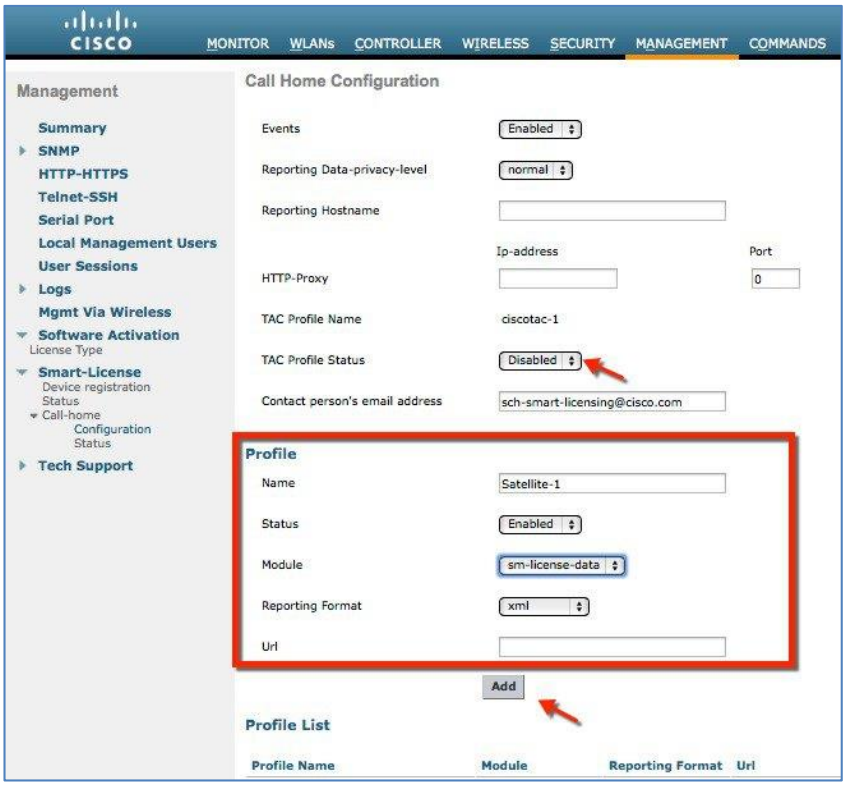


Ilustración 42. Instalación de perfil en *Smart Software Satellite*

7. CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD DEL ENS PARA INFRAESTRUCTURAS INALÁMBRICAS EN CONTROLADORES CISCO WLC

139. A continuación, se detallan los elementos más importantes a tener en cuenta dentro de un despliegue de un controlador Cisco WLC 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

140. La guía indica como requisito (CCN-STIC-816 Apdo. 5.2.4) el despliegue en modo infraestructura, de tal forma 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*).

141. En el caso de los controladores Cisco WLC, es su modo normal y único de funcionamiento por lo que no es necesario realizar ninguna acción sobre el equipo para que actúe en este modo.

7.2 ASPECTOS GENERALES DE SEGURIDAD DE LA RED INALÁMBRICA EN CONTROLADORES CISCO WLC

7.2.1 ASPECTOS DE SEGURIDAD RELACIONADOS CON EL SSID

142. El primer aspecto de seguridad 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).

143. **Se recomienda ocultar el SSID de la red para reducir el perfil de ataque** (según CCN-STIC-816 Apdo. 5.2.4) y, si no es posible por alguna incompatibilidad con dispositivos inalámbricos obsoletos pero críticos, que dicho identificador no tenga relación con la organización en sí (requisito según CCN-STIC-816 Apdo. 4.3.2). Para ello, en el menú *WLAN->General->Broadcast SSID*, desmarcar la opción.

Ilustración 43. Configuración de emisión del identificador inalámbrico de red (SSID)

7.2.2 IMPLEMENTACIÓN DE FILTRADO MAC EN UN PERFIL

144. Otro aspecto recomendado en el cumplimiento del ENS es el uso de un listado de direcciones MAC permitidas para conexión inalámbrica (recomendación según CCN-STIC-816 Apdo. 5.2.4).

145. Para su implementación, dentro de un perfil de red inalámbrica deseado, se selecciona dicho perfil dentro de los diferentes perfiles WLAN creados en el equipo *(WLAN->WLANs)*:

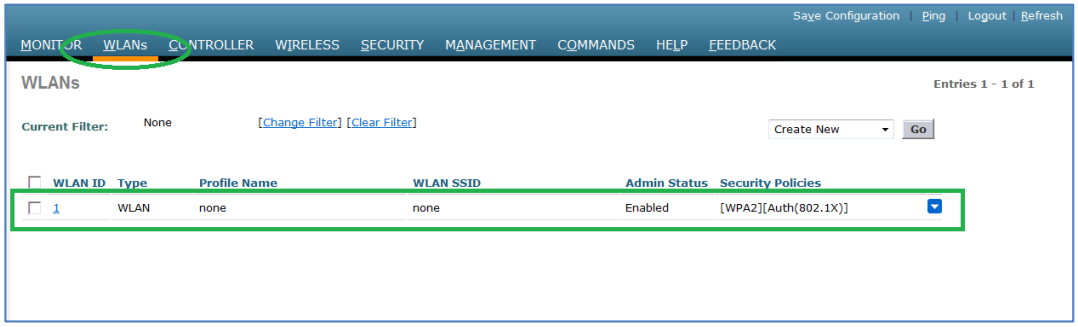


Ilustración 44. Configuración de emisión del identificador inalámbrico de red (SSID)

146. Dentro de su correspondiente apartado de seguridad, se debe seleccionar la opción *Security->MAC Filtering* y pulsar en *New*:

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

147. A continuación, introducir la dirección MAC del equipo que se desea permitir en la red, y configurar los valores apropiados del perfil inalámbrico e interfaz afectados por el filtrado MAC:

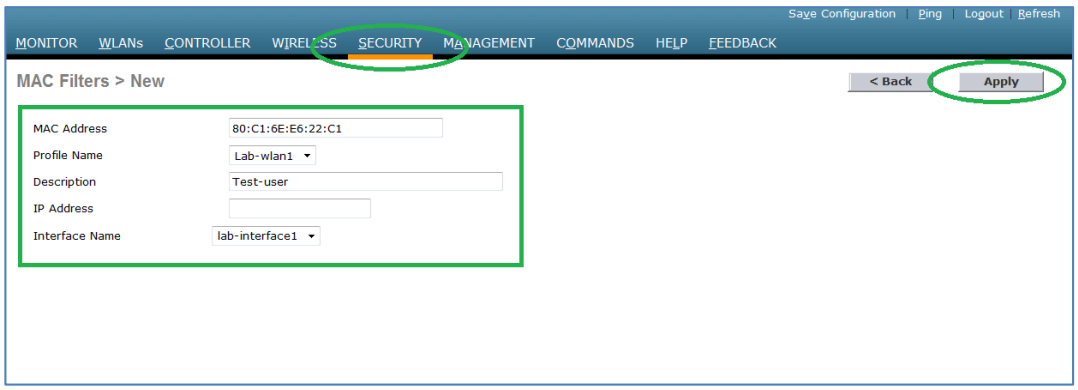


Ilustración 46. Creación de una nueva entrada dentro del filtrado MAC del controlador

148. Por último, comprobar que la lista es correcta, una vez configurado el primer elemento. A partir de ese momento, y tras pulsar el botón de *Apply*, únicamente los elementos cuya dirección MAC coincidan con los de esa lista podrán tener acceso a la red:

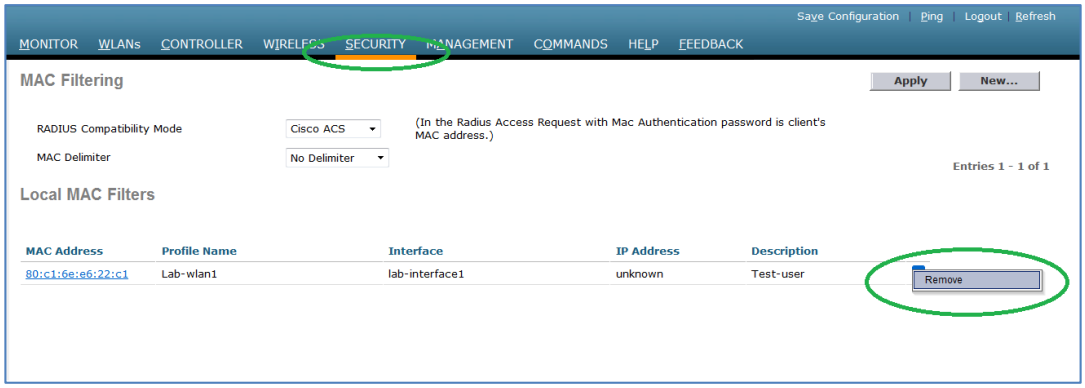


Ilustración 47. Revisión del listado de MAC autorizadas en el perfil inalámbrico

7.2.3 MONITORIZACIÓN DE LA ACTIVIDAD DE LOS USUARIOS

149. La infraestructura inalámbrica debe poder enviar un registro de la actividad de los usuarios (conexión/desconexión, datos de equipo, datos de usuario) a un servidor de logs centralizado. Para ello, es posible 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).

150. Para su implementación, dentro del menú *Management->Logs->Config* se pueden configurar los datos relacionados con un servidor de *syslog*:

a) Dirección IP del servidor de *syslog*.

b) Nivel de *syslog* deseado. Los valores permitiros, de mayor nivel de criticidad a menor (de arriba abajo), son los siguientes:

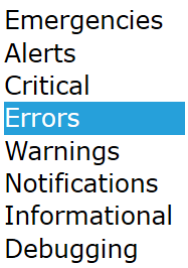


Ilustración 48. Niveles de severidad de *syslog*

c) Instancia de syslog a utilizar (*facility*). Permite diferenciar varios flujos de syslog diferentes dentro de un *syslog* centralizado. Los valores permitidos son:

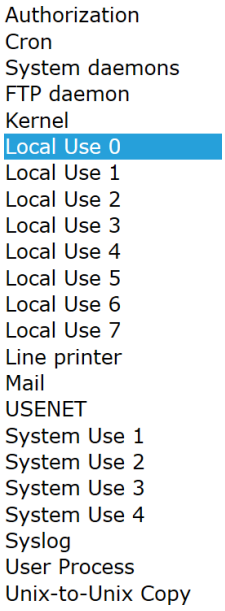


Ilustración 49. *Syslog facilities* disponibles

d) Utilización de un perfil de IPSec para la conexión con el servidor de *syslog*, utilizando un perfil de IPSec previamente establecido.

e) Configuración del almacenamiento de los mensajes de log dentro del propio controlador (*Buffered Log Level*). Indica el nivel de los mensajes de *logs* que se almacenarán en el buffer rotatorio del dispositivo.

f) Configuración de los mensajes de *log* que se emitirán por consola.

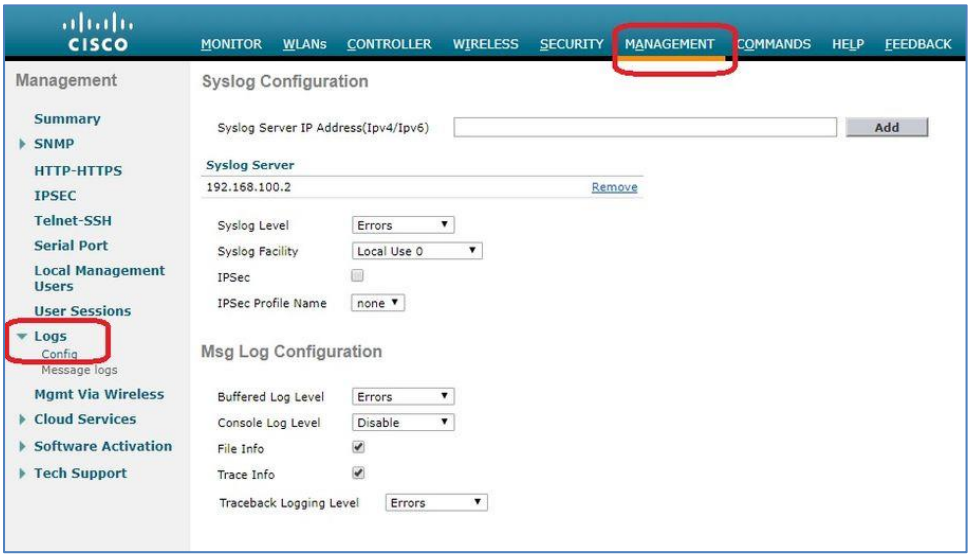


Ilustración 50. Definición de un servidor de *syslog*

7.2.4 ESTABLECIMIENTO DE UN VALOR MÁXIMO DE SESIÓN DEL USUARIO

151. El sistema también debe poder permitir la configuración de 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).

152. Este valor es propio para cada uno de los perfiles inalámbricos definidos en el dispositivo, por lo que, para su configuración, primero es necesario escoger el perfil inalámbrico donde se va a implementar, y dentro del menú *WLAN->Edit <perfil>->Advanced*, se habilita la opción y el valor en segundos deseado.

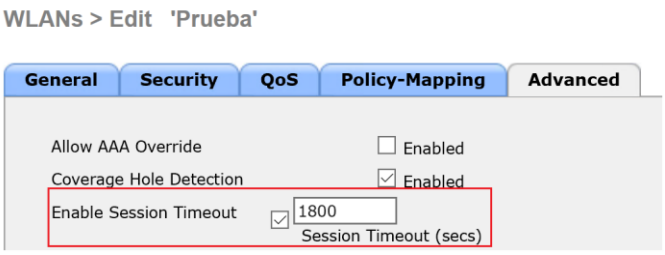


Ilustración 51. Establecimiento del valor máximo de sesión

7.2.5 PROTECCIÓN DE LAS TRAMAS DE GESTIÓN

153. Otro aspecto importante a tener en cuenta es la protección de las tramas de gestión, a nivel de confidencialidad, integridad, autenticación de origen y protección anti-reenvíos.

154. 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 autenticación), por lo que el cliente desechará las tramas de gestión que no vengan correctamente firmadas desde la infraestructura inalámbrica.

155. Existen dos (2) variantes de protección de trama de gestión:

a) A nivel de infraestructura (*Infrestructure MFP Functionality*), en la que todos los puntos de acceso comparten un sistema criptográfico de *hash* de las tramas de gestión, de modo que cuando un AP recibe una trama de gestión que no lleva el sistema de integridad verificado, dicha trama es descartada y se reporta al controlador al que está registrado el AP. En este modo, las tramas de gestión son protegidas y validadas para todos los puntos de acceso que se registren en el controlador, y la autenticación a nivel de punto de acceso es automáticamente deshabilitada. En este caso, tanto las tramas de gestión de cliente como de controlador son protegidas. Es recomendable habilitar la protección MFP a nivel de infraestructura, para poder detectar y e informar de tramas no válidas de gestión enviadas a clientes sin capacidad de MFP a nivel de cliente, así como tramas no válidas de gestión de clase 1 y 2:

   - Clase 1: tramas de *Probe request/respond*, tramas de *Beacon*, tramas de solicitud de autenticación / deautenticación.
   - Clase 2: tramas de petición y respuesta de asociación, tramas de petición y respuesta de deasociación, y tramas de deasociación enviadas por el AP.

Esto se traduce en que MFP a nivel de infraestructura protege en los escenarios no cubiertos por MFP a nivel de cliente, por lo que se recomienda su implantación.

b) A nivel de cliente (*Client MFP Functionality*), en la cual se cifran las tramas de gestión entre los puntos de acceso y los clientes CCXv5, de modo que los clientes puedan descartar tramas de gestión que no vengan correctamente cifradas.

156. 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 CCXv5 que pueden soportar el cifrado de las 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 CCXv5, o no podrán conectarse satisfactoriamente a la red. Esta es la protección a nivel de cliente recomendada.

157. Para definir el modo de protección MFP de manera global a nivel de controlador, es necesario seguir los siguientes pasos:

a) En la opción de *Security-> AP Authentication/MFP*, seleccionar el siguiente valor:

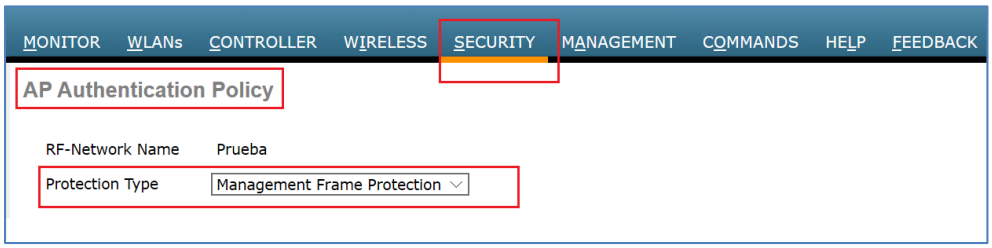


Ilustración 52. Protección de MFP a nivel de infraestructura

b) En *Security->Management Frame Protection* aparecerá la opción habilitada, y todos los puntos de acceso que la implementan:

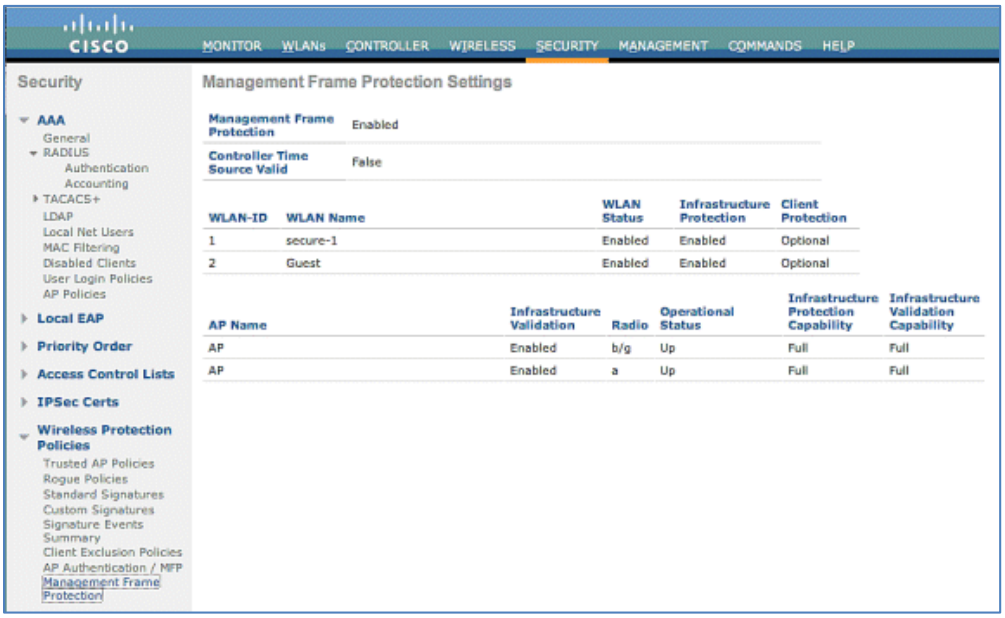


Ilustración 53. Comprobación de MFP a nivel de infraestructura

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

159. 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.

b) Dentro de la opción de *WLAN-> Edit <perfil> -> Layer 2 Security* seleccionamos el tipo de protección MFP deseado:

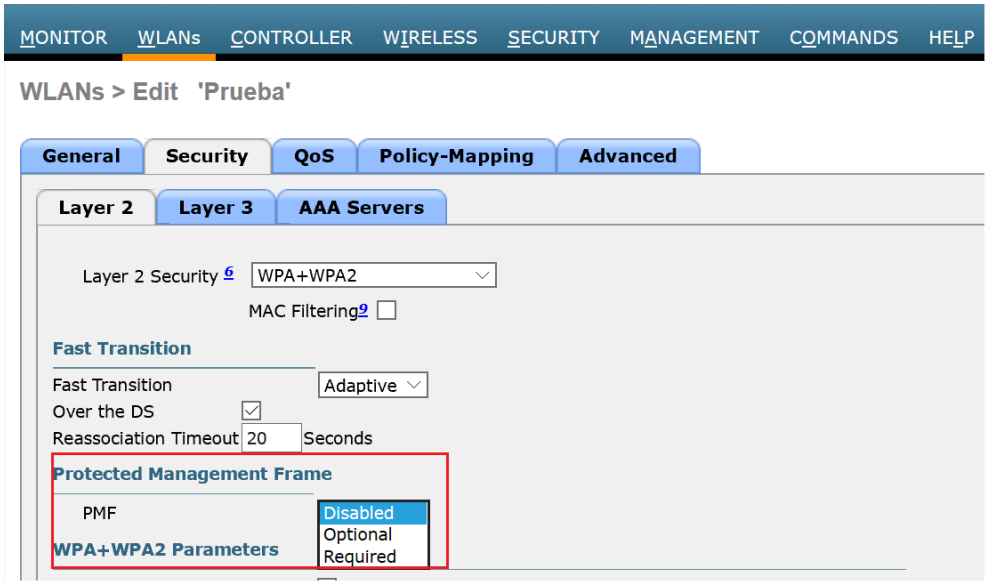


Ilustración 54. Protección de MFP de cliente a nivel de WLAN

7.3 MECANISMOS DE CIFRADO Y AUTENTICACIÓN

7.3.1 DEFINICIÓN DE LOS ALGORITMOS DE CIFRADO

160. El estándar 802.11i, de implantación recomendada en el despliegue de redes inalámbricas según CCN-STIC-816 Apdo. 5.4, permite utilizar dos (2) *suites* criptográficas para la protección de la comunicación, TKIP y CCMP, ambas soportadas por el controlador Cisco WLC.

161. En entornos donde las dimensiones de integridad [I], confidencialidad [C] y autenticidad [A] permitan un nivel bajo, no se especifica ningún requisito sobre el cifrado de la comunicación, lo que permitiría el uso de cifrado TKIP (bajo estándar WPA). Esto sólo se debe utilizar en equipos inalámbricos de uso crítico no permitan el uso de herramientas de cifra más complejas (modo *legacy*).

162. Para la configuración de los algoritmos de cifrado en un perfil inalámbrico existente, dentro del menú *WLAN->Edit <perfil>->Security:*

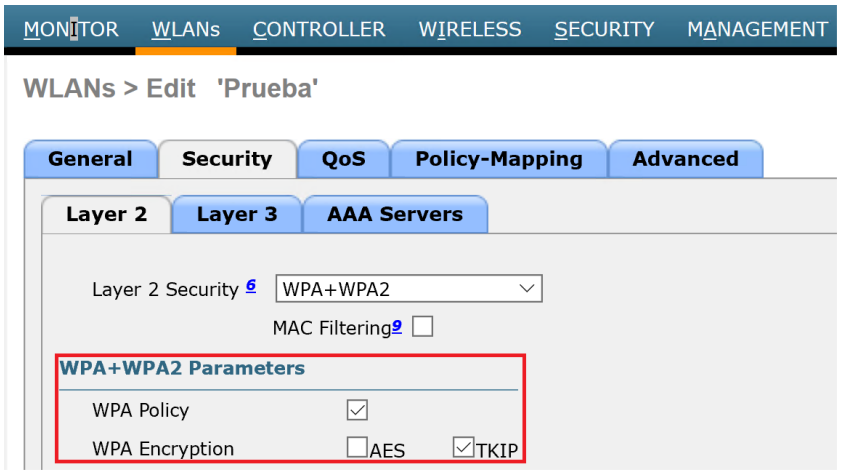


Ilustración 55. Configuración de WPA + TKIP

163. En entornos donde las dimensiones [I], [C] y [A] tienen que ser de nivel medio/alto, no se permite el uso de algoritmos de cifra no autorizados 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.

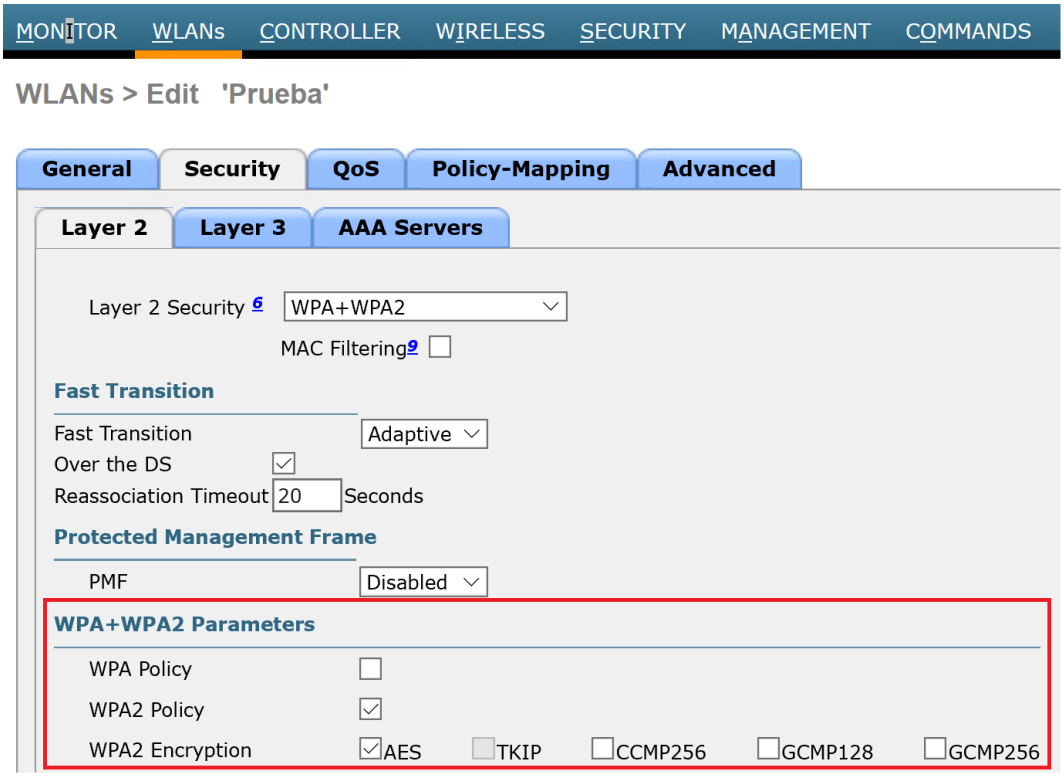


Ilustración 56. Configuración de WPA2 + AES

7.3.2 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

7.3.2.1 MECANISMOS DE PROTECCIÓN EN MODO CLAVE PRE-COMPARTIDA

164. Para la protección de las claves criptográficas, la guía CCN-STIC-816 Apdo. 5.4.2 contempla tres (3) escenarios, de los cuales solo uno hace referencia al uso de mecanismos de autenticación en modo clave pre-compartida.

165. Se trataría de un escenario de Categoría BÁSICA (para el resto no se deben utilizar claves pre-compartidas), donde es posible usar claves pre-compartidas (PSK). A través de ellas y mediante los mecanismos de jerarquía de claves descritos en el estándar 802.11i, dentro del RSN, se derivarían las claves reales para la protección de la comunicación inalámbrica.

166. Como recomendación: clave PSK de 12 caracteres al menos, generada de manera automática a través de algún dispositivo de generación de claves aleatorias (PRNG).

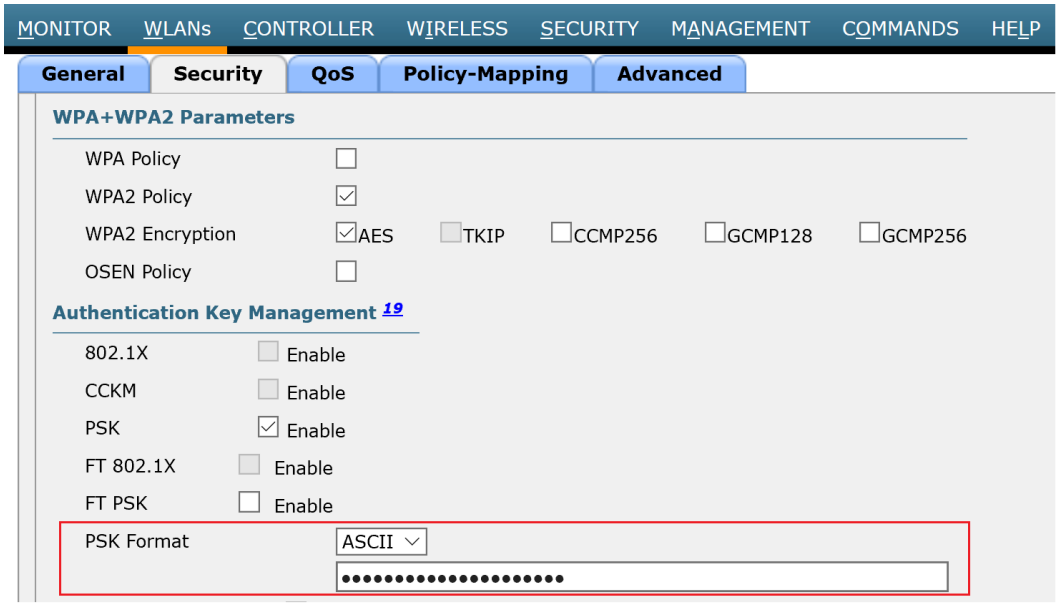


Ilustración 57. Configuración de gestión de claves mediante claves precompartidas

167. Las claves PSK deberían renovarse de manera periódica en la infraestructura inalámbrica.

7.3.2.2 MECANISMOS DE PROTECCIÓN EN MODO SERVIDOR DE AUTENTICACIÓN

168. En los escenarios de categoría MEDIA/ALTA, el mecanismo de generación y distribución de claves que debe utilizarse está basado en **802.1X y EAP**. En estos escenarios, las claves maestras de sesión son generadas y distribuidas entre el servidor de autenticación (AAA) y el dispositivo cliente. Para la protección de este proceso de distribución se usa CCMP con valores aleatorios negociados entre ambos.

169. La distribución de las claves maestras MSK (*Master Session Key*) hacia los puntos de acceso debe realizarse mediante un canal seguro. En el caso de los controladores Cisco WLC, se usan sesiones DTLS basadas en el estándar TLS v1.2, con certificados de dispositivo entre el controlador y el AP en cuestión. Esto forma parte de la definición del estándar CAPWAP comentado en anteriores apartados.

7.3.3 MECANISMOS DE AUTENTICACIÓN

7.3.3.1 MECANISMOS DE AUTENTICACIÓN EN MODO CLAVE PRE-COMPARTIDA

170. Este método implica que sólo existe una única clave para la conexión inalámbrica. Esta clave es compartida por todos los equipos y todos los usuarios.

171. Es solo recomendado en casos con bajos requisitos de seguridad, por los problemas de gestión y distribución que dicha clave PSK genera, además de la falta de autenticación mutua efectiva y falta de trazabilidad de las acciones de los usuarios.

172. Para su configuración en un controlador Cisco WLC:

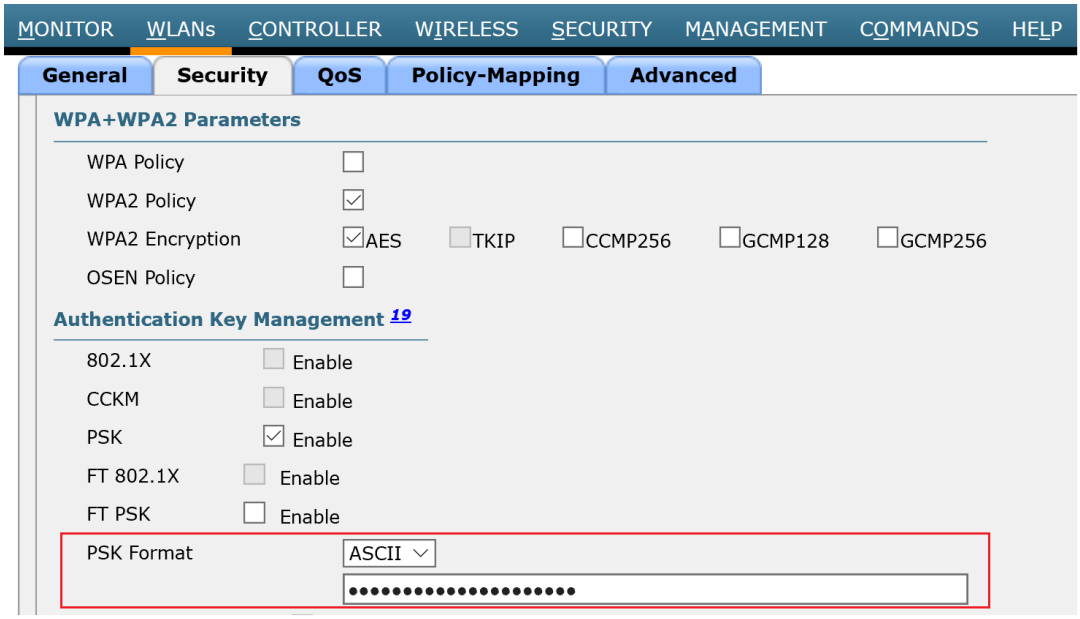


Ilustración 58. Configuración de gestión de claves mediante claves precompartidas

7.3.3.2 MECANISMOS DE AUTENTICACIÓN EN MODO 802.1X/EAP

173. Es el **método de autenticación recomendable**, 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).

174. La autenticación basada en 802.1X/EAP será el tipo de autenticación requerido cuando las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] alcancen cualquiera de ellas un nivel MEDIO o ALTO.

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

176. Como modo de autenticación recomendado, se propone el método más seguro, que sería **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.

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

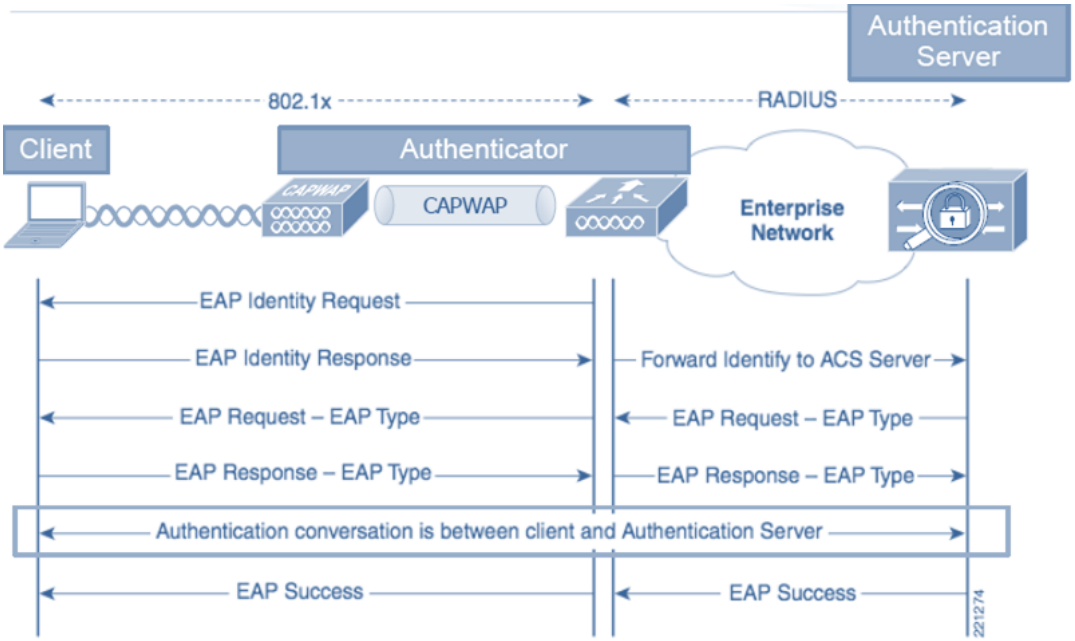


Ilustración 59. Escenario de autenticación EAP

178. En este caso concreto, únicamente se va a proporcionar la configuración relacionada con el elemento autenticador, que sería el controlador inalámbrico WLC. 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).

179. 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 *Security->AAA->Authentication-> New…*

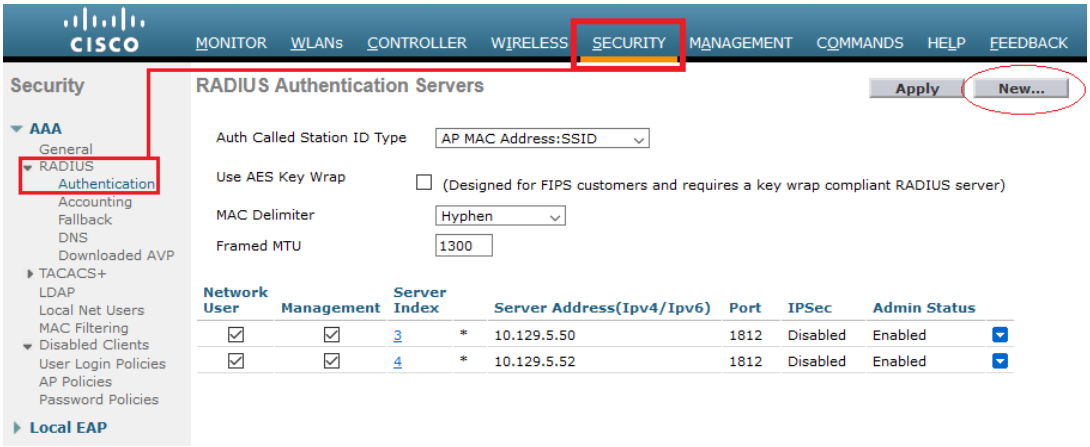


Ilustración 60. Creación de un nuevo servidor de autenticación

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

- Su IP.
- 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.
- Si el servidor estará activo o no, es decir, si estará disponible para su selección dentro de las WLANs definidas en el sistema.
- 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.
- Si el paquete se va a mandar por el puerto de gestión (*Management*), o se va a mandar por la tabla de rutas existente en el dispositivo.
- Si se va a usar IPSec para establecer un túnel seguro con el servidor de autenticación. Es requisito de implantación configurar un túnel VPN con el servidor de autenticación (CCN-STIC-816 Apdo. 5.2.4).
- Finalmente, se crea pulsando el botón de *Apply.*

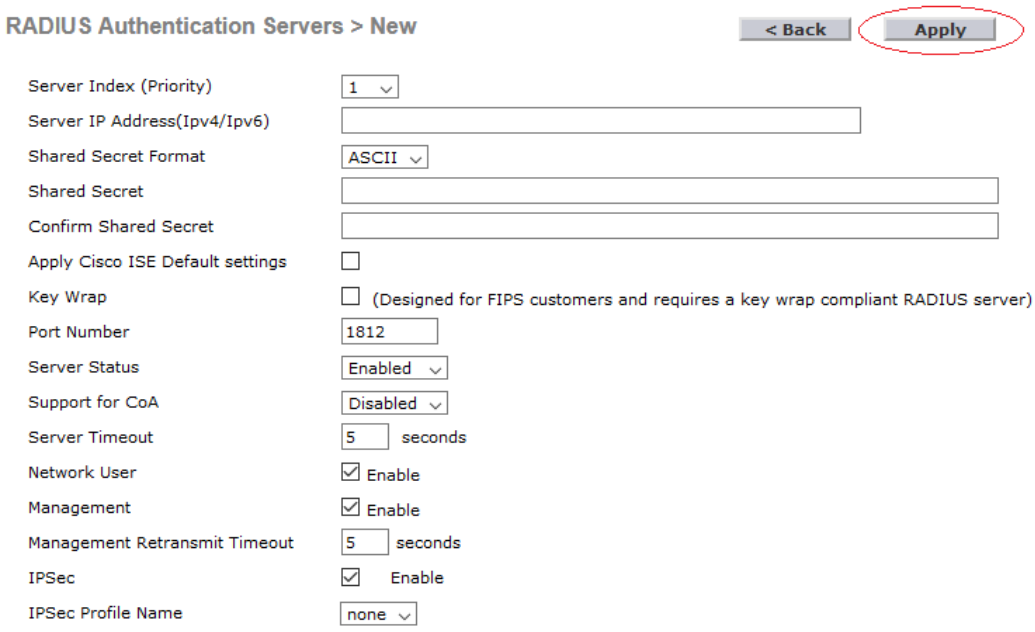


Ilustración 61. Configuración del nuevo servidor de autenticación

181. 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 la definición de *WLAN->Security->Layer2.*

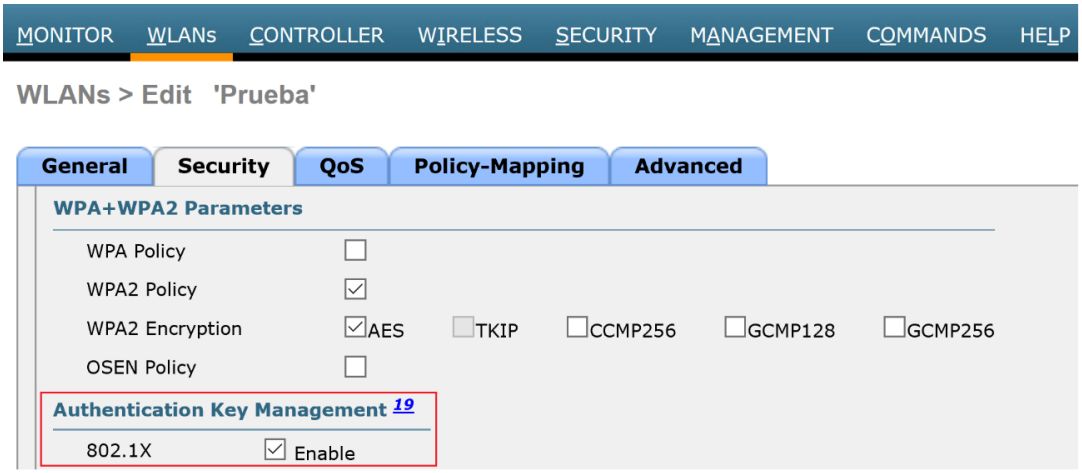


Ilustración 62. Configuración del SSID para uso de EAP-TLS

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

183. Por último, dentro de la misma pestaña, pero en la sección de *WLAN->Security->AAA Servers*, ya es posible seleccionar el servidor previamente definido. Para aplicarlo, se debe pulsar en el botón *Apply*.

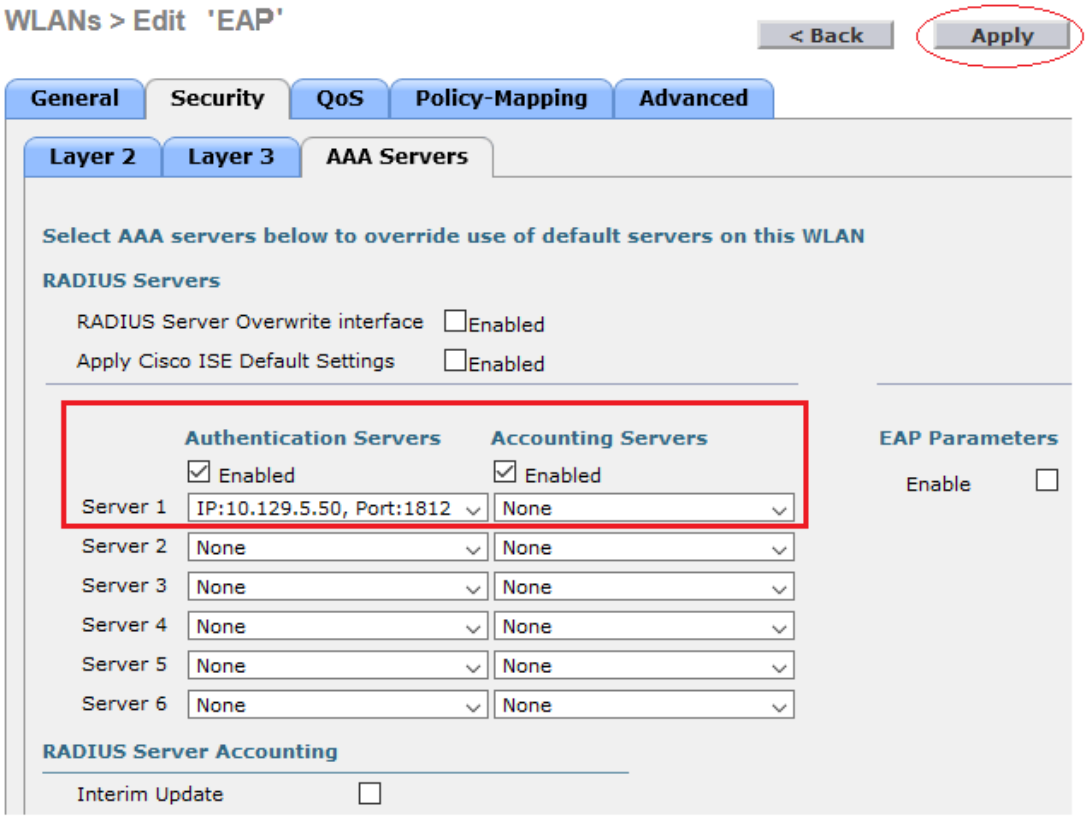


Ilustración 63. Definición del servidor de AAA para usar en EAP-TLS

7.3.4 MECANISMOS DE DETECCIÓN DE INTRUSIÓN (WIDS)

184. En caso de que la categoría sea MEDIA o ALTA, se requiere 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.

185. En un controlador inalámbrico Cisco WLC, es posible configurar firmas o patrones de bit que identifiquen varios tipos de ataques en el estándar 802.11. Cuando el sistema está activado, y cargado con firmas, los APs asociados al sistema realizan análisis en las tramas de datos y gestión, y reportan los resultados al controlador, donde se alerta, y se decide si procede realizar remediación automática.

186. El controlador Cisco WLC permite diferenciar 17 tipos de firmas de ataques estándares, divididas en seis (6) grandes grupos:

- Ataques de deautenticación por *broadcast*.
- Ataques de NULL PROBE.
- Ataques de inundación de tramas de gestión.
- Detección de herramientas de escaneo (*Wellenreiter*).
- Ataques de inundación de tramas EAPOL.
- Detección de herramientas de escaneo (*NetStumbler*).

187. Existe un fichero de firmas por defecto en el controlador que se puede cargar en cualquier momento, pero además es posible crear firmas personalizadas para la detección de ataques más sofisticados.

188. En caso de que se deseen habilitar las firmas por defecto, se puede implementar en el menú *Security->Wireless Protection Policies->Standard Signatures*:

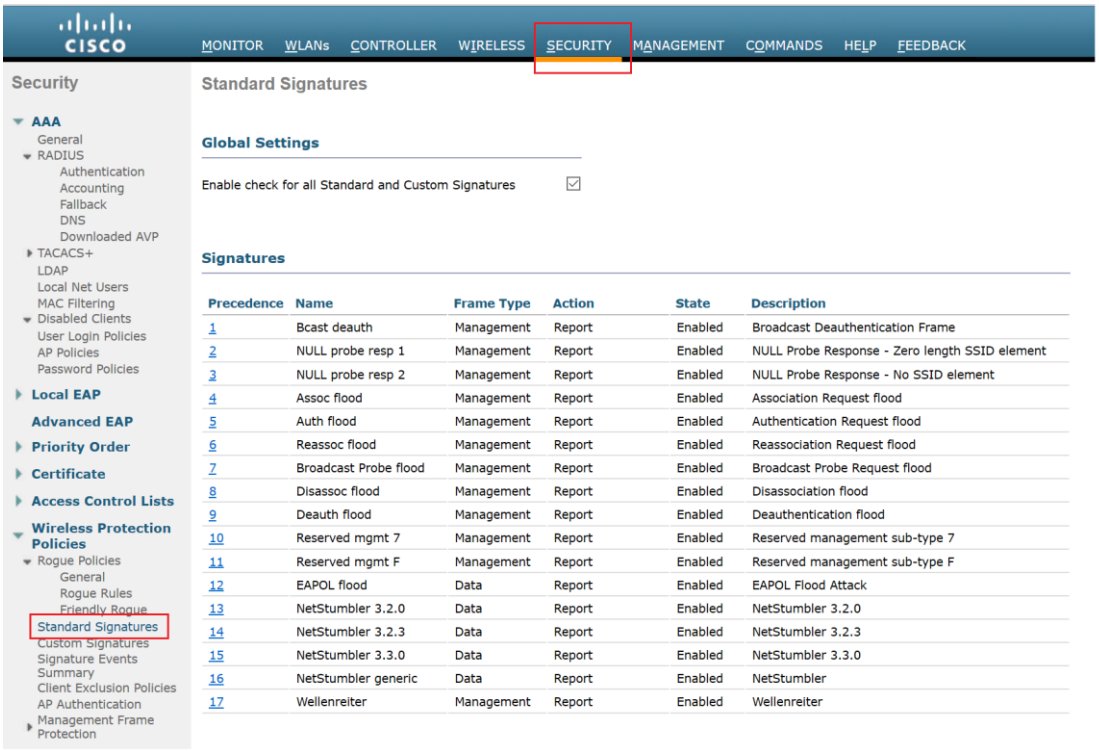


Ilustración 64. Listado de firmas de detección por defecto

189. Cada firma tiene un ordinal de precedencia, un nombre descriptivo, si afecta a trama de gestión o datos, una acción a realizar (se recomienda *Report* para evitar incidencias en falsos positivos), su estado (habilitado o no habilitado) y una descripción.

190. Para cada firma, también es posible configurar un ajuste fino en su comportamiento, para evitar falsos positivos. Se accede a cada firma a través de su ordinal de precedencia:

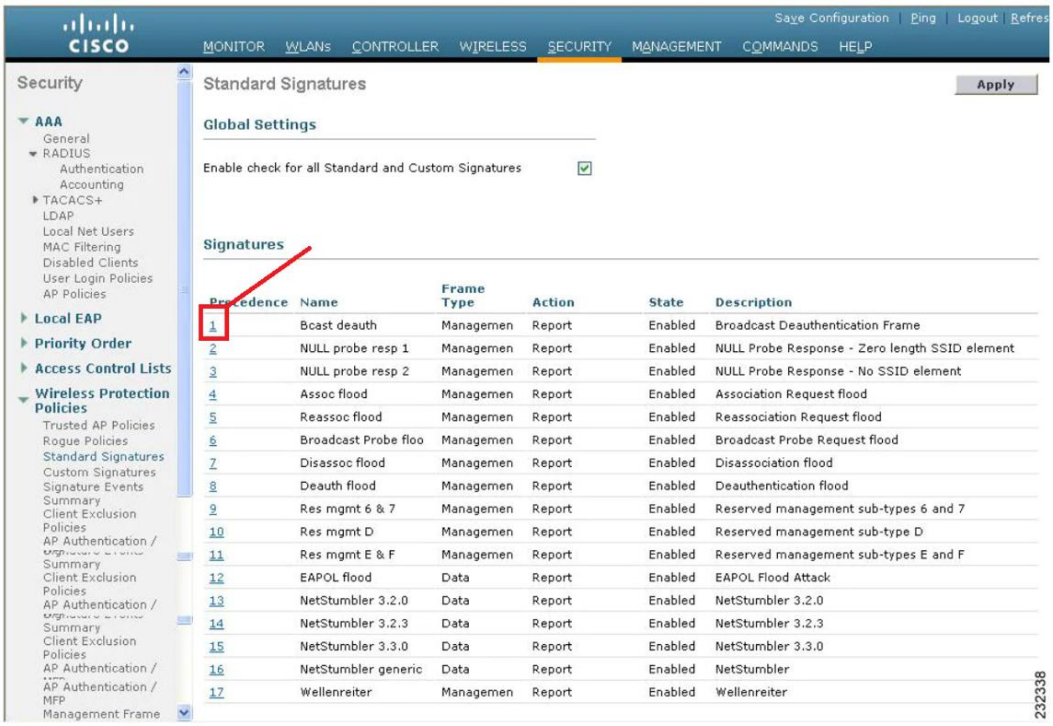


Ilustración 65. Ajuste para la firma de detección de deautenticación de tramas por *broadcast*

191. Para la firma de ataque de deautenticación por *broadcast*, por ejemplo:

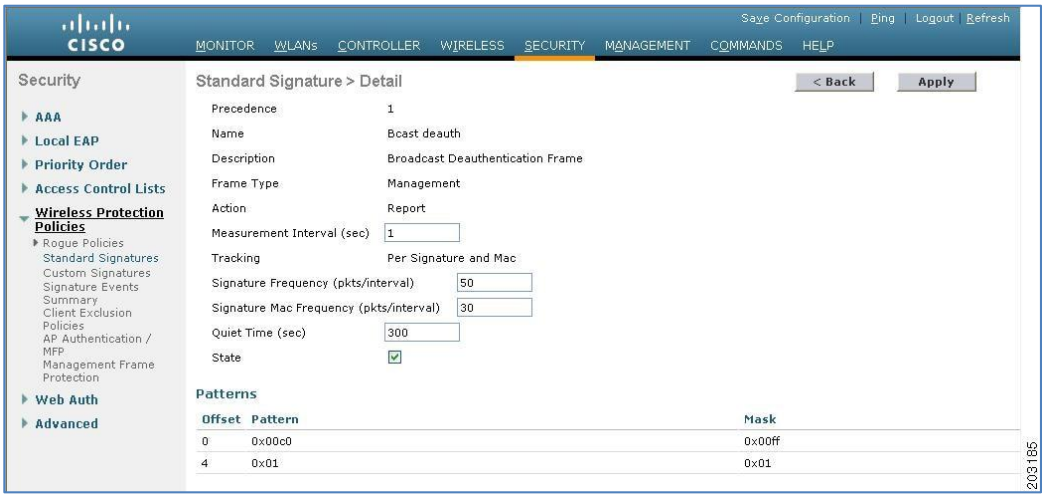


Ilustración 66. Ejemplo de ajuste fino para la firma de detección de deautenticación de tramas por broadcast

192. Por último, es posible ver un resumen de eventos de seguridad detectados por el WIDS en el menú *Security->Signature Events Summary*:

Ilustración 67. Resumen de eventos de seguridad detectados

7.3.5 INTERCONEXIÓN ENTRE PUNTOS DE ACCESO Y CONTROLADORA

7.3.5.1 SEGURIDAD EN LA CONEXIÓN

193. Los controladores inalámbricos Cisco WLC, a partir de su versión 7.x, 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.

194. 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 control, el cifrado es obligatorio, mientras que, en el plano de datos, es opcional. Para el uso del cifrado DTLS en el plano de datos, en el caso de los controladores de la gama 5520, es necesario que dispongan de una imagen que permita el uso de cifrado DTLS.

195. Para **habilitar el cifrado de datos**, es necesario que el punto de acceso permita realizar dicha tarea mediante *hardware* en los dispositivos de tipo AP cualificados para operar con la plataforma (1560, 2800, 3800). La configuración de dicha funcionalidad se realizaría a través del siguiente elemento de menú:

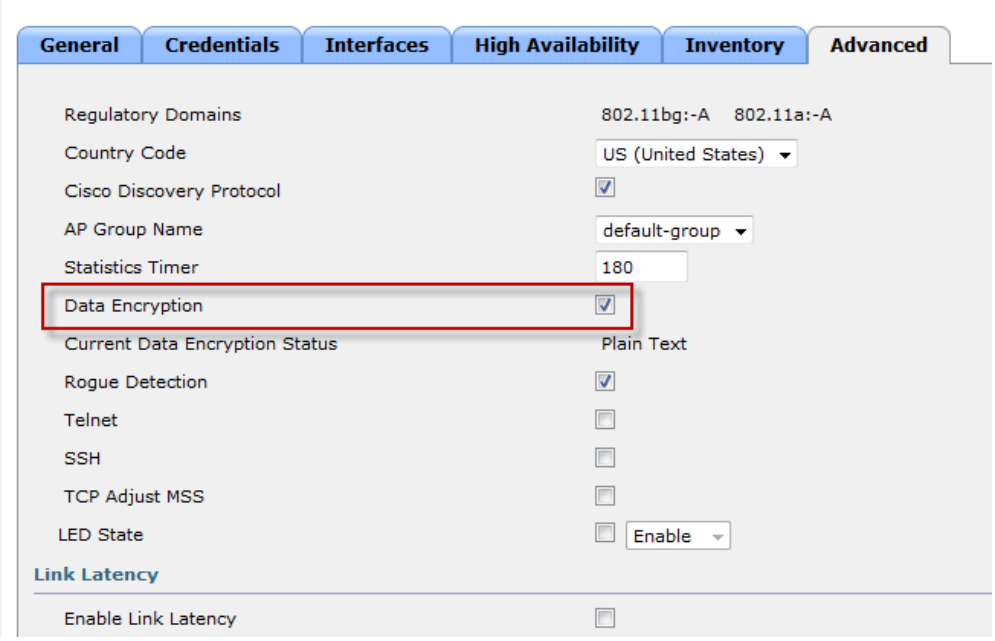


Ilustración 68.Activación del cifrado en el plano de datos

196. Es importante el impacto que tiene el cifrado del plano de datos en los dispositivos que no dispongan de aceleración por *hardware* para criptografía (como por ejemplo los equipos Cisco WLC 2504 o Cisco vWLC).

197. DTLS es un estándar de cifrado del IETF basado directamente en TLS, y se puede implementar en diferentes versiones, aunque a partir de la versión de *firmware* 8.3.11.X se **debe activar DTLS v1.2**, siempre y cuando el punto de acceso lo permita. Es posible configurar DTLS v1.2 como mínimo algoritmo permitido de cifrado mediante el siguiente comando de CLI:

    # config ap dtls-version {dtls1.0 | dtls1.2 | dtls_all}

198. También se debe fijar la suite de cifrado dentro del algoritmo DTLS entre el AP y el controlador, mediante el siguiente comando:

    # config ap dtls-cipher-suite {RSA-AES256-SHA256 | RSA-AES256-SHA | RSA-AES128-SHA | ECDHE-RSA-AES128-GCM-SHA256}

199. Se debe utilizar la suite que presente mayor fortaleza, en este caso **RSA-AES256-SHA256**.

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

    # show ap dtls-cipher-suite

7.3.5.2 REGISTRO DE PUNTOS DE ACCESO EN EL SISTEMA

201. 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.

202. Por motivos de seguridad se debe garantizar que ún**icamente 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.

203. 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.

204. 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.

205. En los puntos de acceso, los certificados instalados de fábrica son conocidos como "*Manufacturing Installed Certificates*" (MIC), y se incorporaron a todos los APs fabricados con posterioridad al 18 de Julio de 2005.

206. Además de esta autenticación mutua, los controladores también pueden restringir el registro 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.

207. La autorización de los APs se puede llevar a cabo de dos (2) maneras:

- Usando la lista interna de autorización del controlador inalámbrico.
- Usando una lista de MAC en un servidor de autenticación.

208. Como nota previa a los detalles de configuración, comentar que puede diferir en función del tipo de certificado que incorporen los APs:

- Puntos de acceso con SSCs (*Self-Signed Certificate*): El controlador usara únicamente la lista de autorización interna. Esto quiere decir que no enviará consultas de autorización a un servidor de autenticación (como puede ser un RADIUS).
- Puntos de acceso con MICs (*Manufacturing Installed Certificates*): El controlador podrá usar indistintamente la lista de autorización interna o realizar consultas de autorización a un servidor de autenticación (como puede ser un RADIUS).

7.3.5.3 EJEMPLO: AUTENTICACIÓN DE PUNTOS MEDIANTE LISTA DE AUTORIZACIÓN

209. Para emplear una lista de autorización en el controlador inalámbrico hay que dirigirse al menú "*Security*", y navegar hasta la sección "*AAA->AP Policies*".

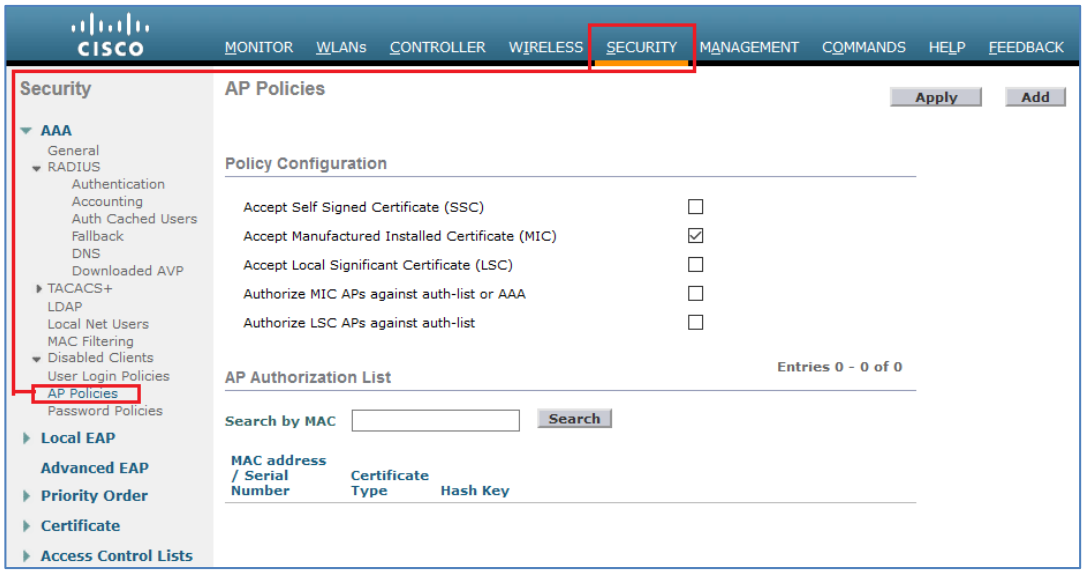


Ilustración 69. Políticas de autorización de registro de puntos de acceso

210. En el menú que aparece en pantalla principal, pulsar sobre "*Add*", y se habilitarán los campos necesarios para añadir la MAC del punto de acceso deseado.

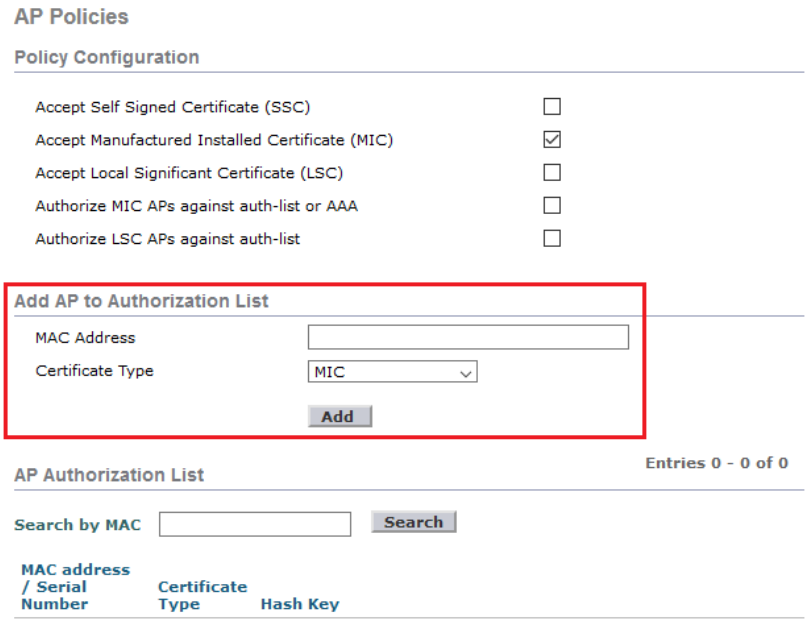


Ilustración 70. Añadir AP a lista de autorización

211. En esos campos disponibles, añadir la dirección MAC del AP (asegurarse de que es la dirección MAC física, no la MAC Radio). Concretar el tipo de certificado del punto de acceso (MIC o SSC).

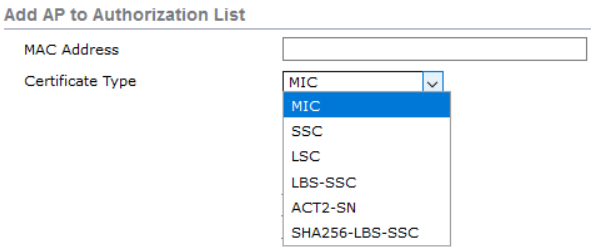


Ilustración 71. Selección de tipo de certificado

212. Una vez introducida la MAC deseada y el certificado correcto, pulsar sobre el botón "*Add*".

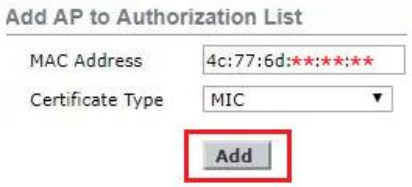


Ilustración 72. Instalación del AP en la lista

213. La MAC del punto de acceso debe aparecer en el listado "*AP Authorization list*".

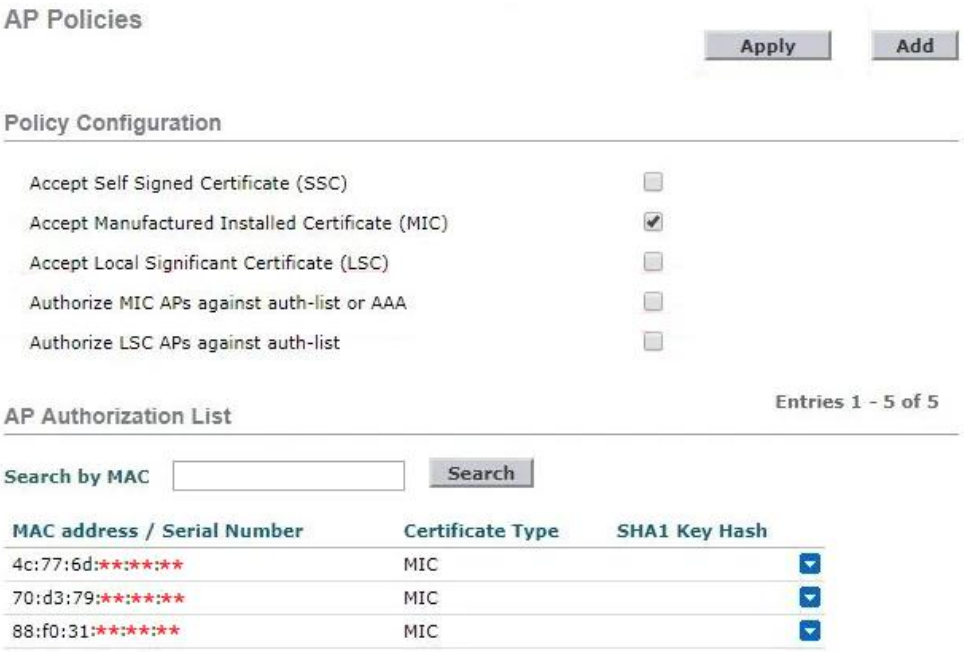


Ilustración 73. Comprobación del AP en la lista

214. Seguidamente activar la autorización de la lista de autenticación o servidor de autenticación, bajo el epígrafe "*Policy Configuration*". Para finalizar, pulsar en "*Apply*" y así tendrá efecto la configuración.

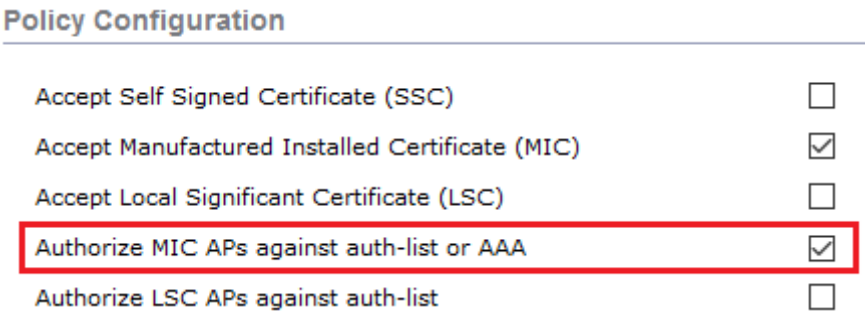


Ilustración 74. Activación del mecanismo de autorización

215. 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.
216. En la consola del controlador, introducir los siguientes comandos:

(Cisco Controller) >debug capwap events enable
(Cisco Controller) >debug capwap errors enable
(Cisco Controller) >debug aaa all enable

217. El resultado, una vez introducida la MAC del AP en la lista de autorización, debería ser el siguiente:

**spamApTask2: Jan 28 07:58:22.300: b0:aa:77:3a:2b:80 Join Priority Processing status = 0, Incoming Ap's Priority 1, MaxLrads = 500, MaxLicense=500 joined Aps =0*

**spamApTask2: Jan 28 07:58:22.300: b0:aa:77:3a:2b:80 apType = 77 apModel: AIR-CAP1702I-E-K9*

**spamApTask2: Jan 28 07:58:22.300: b0:aa:77:3a:2b:80 Discovery Response sent to 10.0.0.5 port 62800*

**spamApTask2: Jan 28 07:58:22.300: b0:aa:77:3a:2b:80 Discovery Response sent to 10.0.0.5:62800*

**spamApTask2: Jan 28 07:58:32.293: a8:9d:21:07:55:0c DTLS connection not found, creating new connection for 10.0.0.5 (62800) 10.0.0.4 (5246)*

**spamApTask2: Jan 28 07:58:32.734: a8:9d:21:07:55:0c acDtlsPlumbControlPlaneKeys: lrad:10.0.0.5(62800) mwar:10.0.0.4(5246)*

**spamApTask2: Jan 28 07:58:32.734: a8:9d:21:07:55:0c Allocated index from main list, Index: 3*

**spamApTask2: Jan 28 07:58:32.735: a8:9d:21:07:55:0c Reserved LCB index for 10.0.0.5:3*

**spamApTask2: Jan 28 07:58:32.735: a8:9d:21:07:55:0c Using CipherSuite AES128-SHA*

**spamApTask2: Jan 28 07:58:32.735: a8:9d:21:07:55:0c DTLS Session established server (10.0.0.4:5246), client (10.0.0.5:62800)*

**spamApTask2: Jan 28 07:58:32.736: a8:9d:21:07:55:0c Starting wait join timer for AP: 10.0.0.5:62800*

**spamApTask2: Jan 28 07:58:32.737: b0:aa:77:3a:2b:80 Join Request from 10.0.0.5:62800*

**spamApTask2: Jan 28 07:58:32.737: b0:aa:77:3a:2b:80 using already alloced index 3*

**spamApTask2: Jan 28 07:58:32.738: b0:aa:77:3a:2b:80 Allocate database entry for AP 10.0.0.5:62800, already allocated index 3*

**spamApTask2: Jan 28 07:58:32.738: b0:aa:77:3a:2b:80 AP Allocate request at index 3 (reserved)*

**spamApTask2: Jan 28 07:58:32.739: b0:aa:77:3a:2b:80 In AAA state 'Idle' for AP b0:aa:77:3a:2b:80*

**aaaQueueReader: Jan 28 07:58:32.740: User a89d2107550c authenticated*

**aaaQueueReader: Jan 28 07:58:32.740: b0:aa:77:3a:2b:80 Returning AAA Success for mobile b0:aa:77:3a:2b:80*

**aaaQueueReader: Jan 28 07:58:32.740: AuthorizationResponse: 0x2cee30c4*

**aaaQueueReader: Jan 28 07:58:32.740:structureSize.....146*

**aaaQueueReader: Jan 28 07:58:32.740:resultCode.....0*

**aaaQueueReader: Jan 28 07:58:32.740: rotocolUsed.....0x00000008*

**aaaQueueReader: Jan 28 07:5:32.740: Packet contains 2 AVPs:*

**aaaQueueReader: Jan 28 07:58:32.740: AVP[01] Service-Type.....0x00000065 (101) (4 bytes)*

**aaaQueueReader: Jan 28 07:58:32.740: AVP[02] Airespace / WLAN-Identifier.....0x00000000 (0) (4 bytes)*

**aaaQueueReader: Jan 28 07:58:32.740: b0:aa:77:3a:2b:80 User authentication Success with File DB on WLAN ID :0*

**spamApTask0: Jan 28 07:58:32.741: b0:aa:77:3a:2b:80 Join Version: = 134586624*

**spamApTask0: Jan 28 07:58:32.742: 00:00:00:00:00:00 apType = 77 apModel: AIR-CAP1702I-E-K9*

**spamApTask0: Jan 28 07:58:32.742: b0:aa:77:3a:2b:80 Join Response sent to 0.0.0.0:62800*

**spamApTask0: Jan 28 07:58:32.742: b0:aa:77:3a:2b:80 CAPWAP State: Join*

7.3.6 SEGREGACIÓN DE REDES Y ASIGNACIÓN AL ESPACIO INALÁMBRICO

218. 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.

219. 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).

220. 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.

221. En el caso de los controladores inalámbricos Cisco WLC, es posible segregar el tráfico de cada red inalámbrica mediante VLANs, a través de la definición de interfaces en el dispositivo. La configuración se realizaría en el menú *Controller-> Interaces*, donde cada interfaz dispondrá de los siguientes elementos:

- Puerto físico del controlador por el que la información va a circular.
- Un identificador de VLAN (VLAN id).
- Una IP asignada al interfaz, que el controlador pueda usar para peticiones *unicast* dentro de la VLAN asignada, incluyendo la correspondiente máscara de red y puerta de enlace por defecto.

- Si no se utiliza el servidor de DHCP interno (opción deseable), la dirección IP de un servidor DHCP primario, y otro secundario, para las peticiones de direccionamiento por parte de los clientes inalámbricos, en caso de que se permita dicha configuración en la red.
- Si se usa un servidor DHCP externo, es posible convertir la petición de DHCP tradicional, enviada como *broadcast* dentro del segmento de red, como una petición *unicast* dirigida específicamente al servidor DHCP configurado (*DHCP Proxy* en modo Global).
- De modo opcional, como medida de seguridad adicional, es posible definir una lista de control de acceso (ACL) para filtrar el tráfico que circulará hacia y desde la red inalámbrica en relación con el segmento cableado.

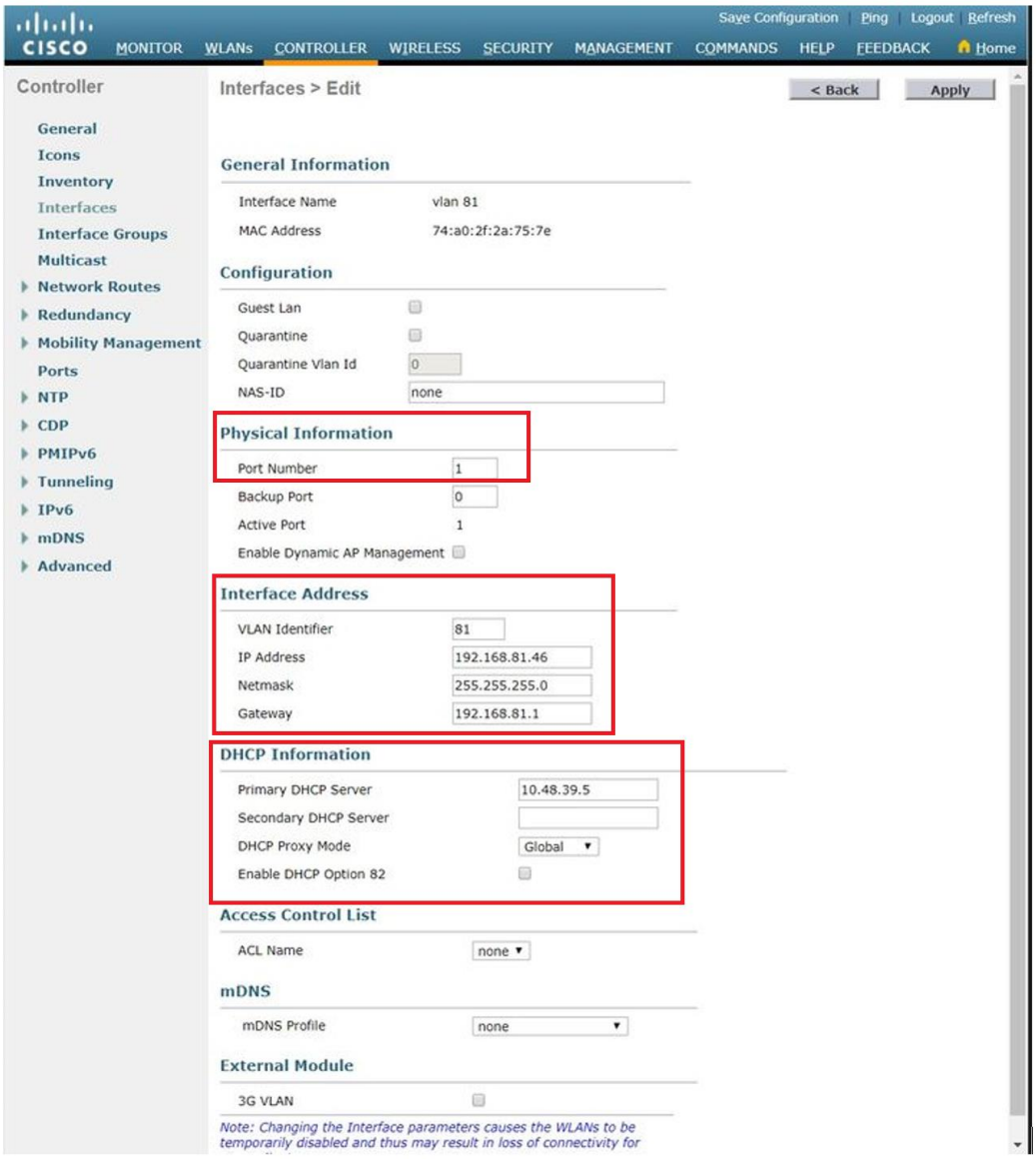


Ilustración 75. Definición de interfaces en el controlador

222. Una vez definido el interfaz mediante el cual el controlador interacciona con la red cableada, es necesario realizar un mapeo de dicho interfaz con la red inalámbrica propagada en el segmento aire, de modo que el tráfico inalámbrico con destino o procedente de dicha red inalámbrica (SSID) quede integrado en el interfaz definido en el apartado anterior. Dicha configuración se debe realizar en el apartado *WLAN-> General-> Interface/Interface Group (G)*:

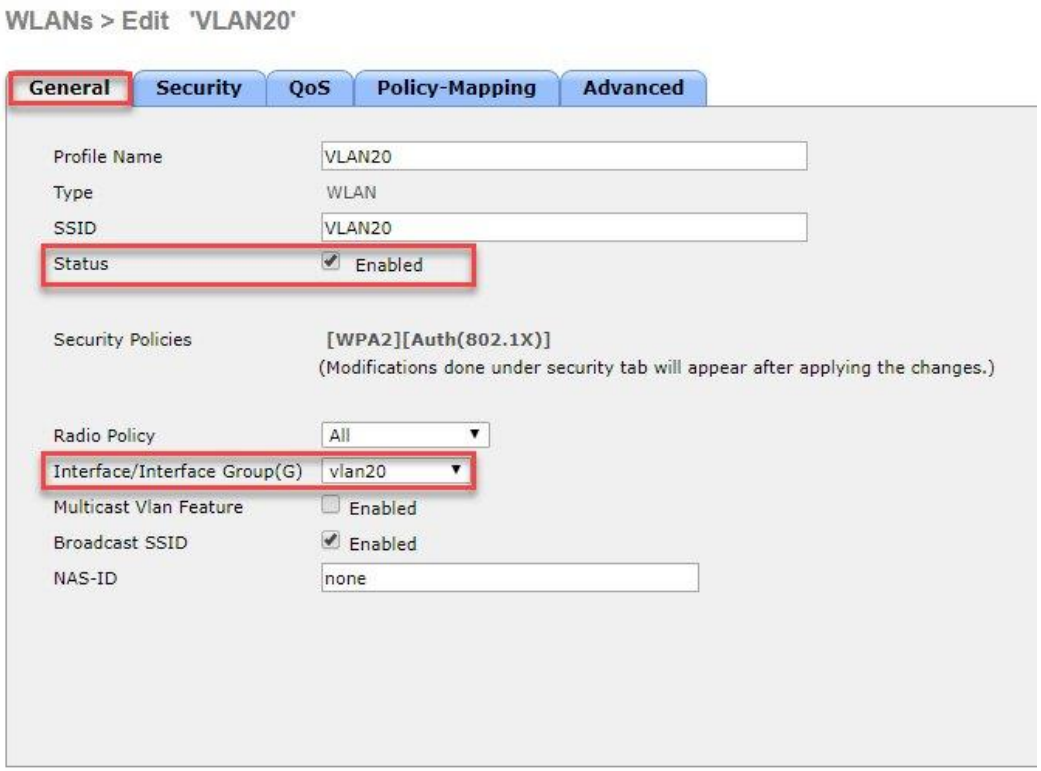


Ilustración 76. Mapeo del interfaz con el identificador de red inalámbrica (SSID) correspondiente

8. GUARDADO DE LA CONFIGURACIÓN Y ACTUALIZACIÓN DE *FIRMWARE*

8.1 GUARDADO DE CONFIGURACIÓN EN DISCO Y TRANSFERENCIA DE ARCHIVOS

223. 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, incorporar aspectos visuales al portal cautivo interno (*webauth-bundle*) y certificados SSL, tanto para la administración web del propio controlador como para un portal cautivo externo.

224. Hay que tener en cuenta que los protocolos permitidos para estas operaciones son TFTP, FTP y SFTP. Se debe hacer uso del protocolo SFTP, ya que de las opciones permitidas es el único que en la autenticación y transferencia usa algún tipo de cifrado (las mismas características que SSH ya que se basa en dicho protocolo).

225. Para realizar estas tareas de transferencia, en primer lugar, se necesita dicho servidor SFTP y, una vez configurado, en el controlador, realizar la parametrización correcta en la pestaña "*Commands*" y navegar hasta la sección "*Download file*" si se desea incorporar algún fichero al controlador, o "*Upload file*" si se requiere descargar un fichero desde el controlador hasta el servidor SFTP.

226. Una vez aquí, seleccionar:

- Tipo de fichero a cargar/subir: Puede ser un fichero de configuración, un certificado SSL, una personalización del portal cautivo, etc.
- Modo de transferencia: De las diferentes opciones, seleccionar SFTP.
- IP del servidor SFTP.
- Directorio donde se aloja el fichero deseado.
- Nombre del fichero.
- Usuario de acceso al servidor.
- Clave del usuario anterior.
- Número del puerto (en SFTP se emplea el puerto 22 al estar basado en SSH).

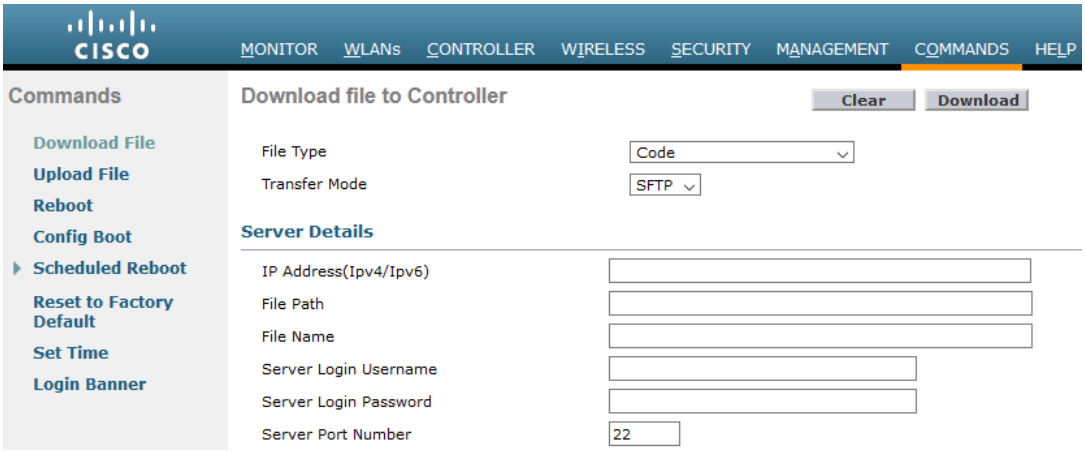


Ilustración 77. Carga/descarga en el controlador

227. La única opción diferenciadora entre la carga/descarga de ficheros, es que en la descarga (subir ficheros desde el controlador hasta el servidor) permite cifrar el fichero con una clave.

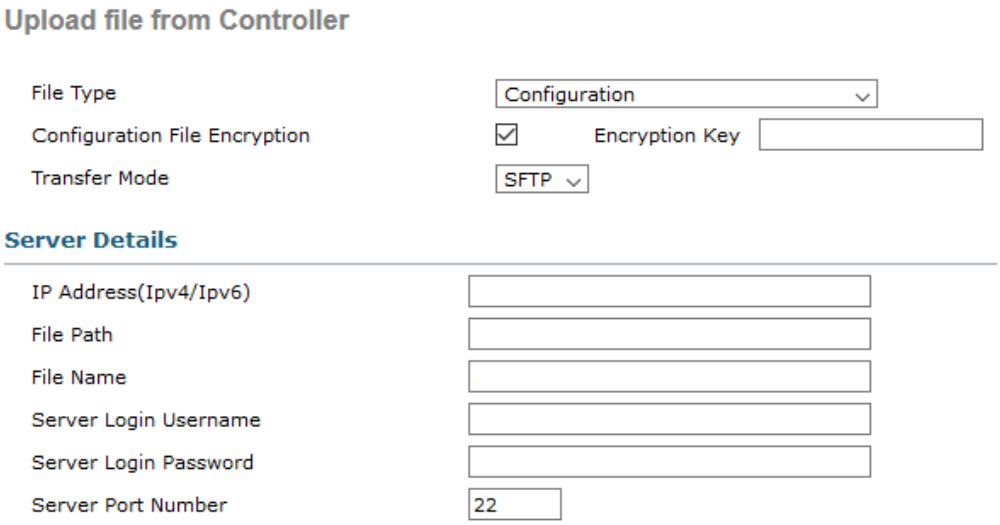


Ilustración 78. Cifrado con clave de los ficheros

228. Se recomienda 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.

8.2 ACTUALIZACIONES Y COMPROBACIONES DE *FIRMWARE*

229. Los dispositivos WLC, como cualquier otro dispositivo de red, deben estar protegidos ante 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**.

230. Cisco recomienda una serie de versiones de *software* en concreto, que se pueden consultar en las "*Troubleshooting TechNotes*", en la sección "*TAC Recommended*

AireOS Builds" [22]. 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) pero siempre se debe **garantizar que el *software* desplegado en los dispositivos dispone de soporte de seguridad por parte de Cisco.**

231. Para consultar las versiones disponibles de los dispositivos, se debe acceder a la página oficial de Cisco, a través de un navegador Web seguro y consultar la URL "*https://software.cisco.com/download/home*". En esta página, se deberá comprobar el listado de los equipos, dirigiéndose a "*Wireless->Wireless LAN Controller->Sandalone Controllers*". Aparecerá el listado completo de familias de controladores inalámbricos. Se deberá navegar en la familia deseada y seleccionar el modelo concreto.

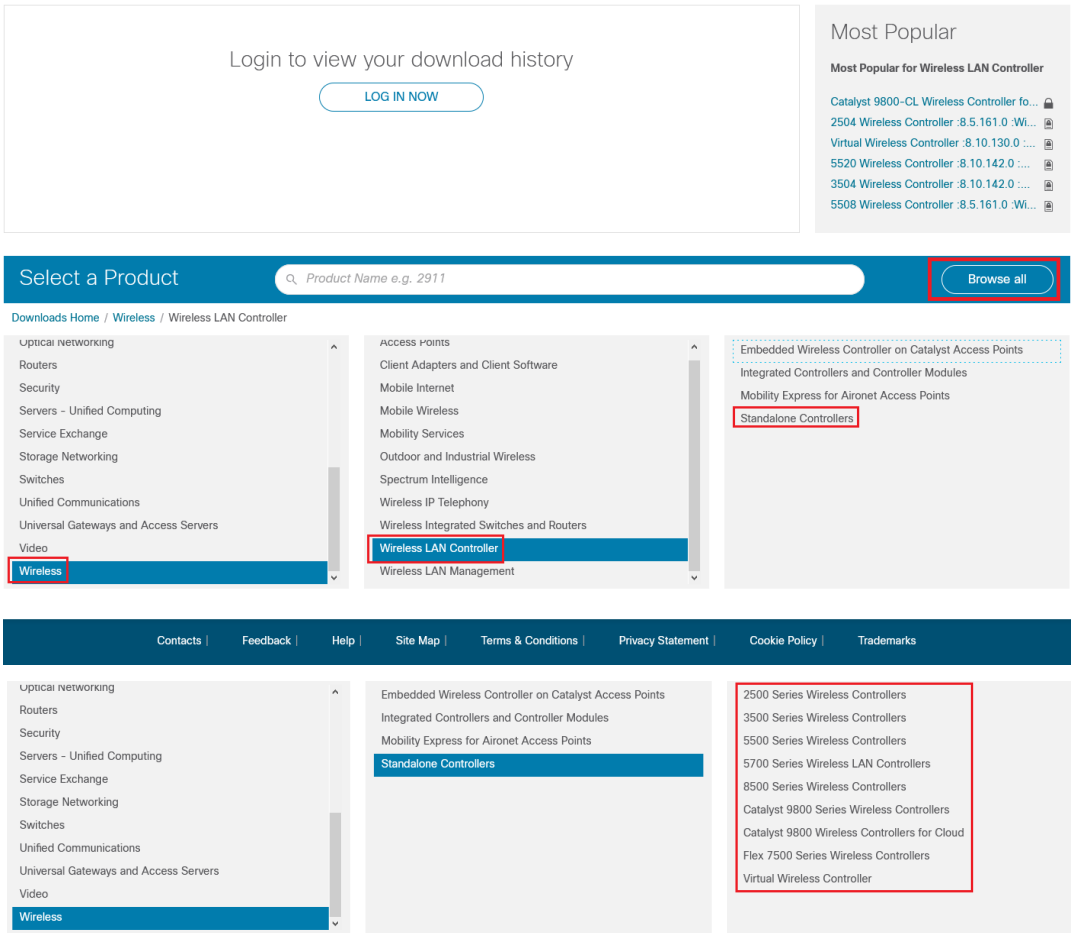


Ilustración 79. Navegación por el apartado de *Downloads* de la web de Cisco

232. También puede usar la herramienta "*buscador*" que ofrece la página web. De cualquier forma, una vez seleccionado el modelo se puede consultar toda la información disponible para el mismo. Para consultar las versiones de *firmware* disponibles, se debe navegar a la sección "*Wireless LAN Controller Software*".

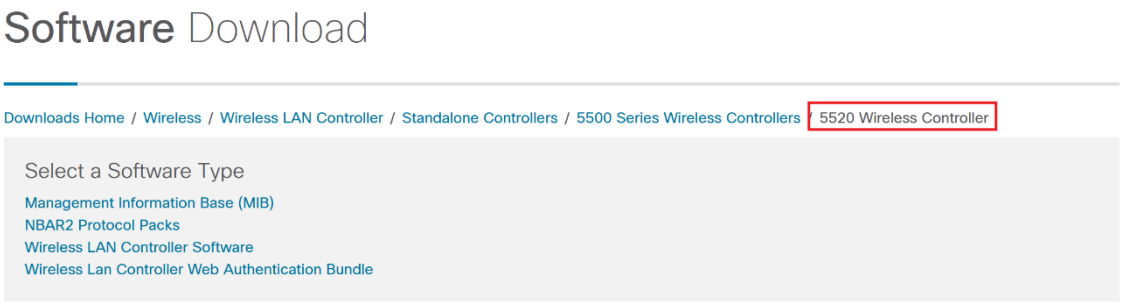


Ilustración 80. Selección de objeto de la descarga

233. El proceso de actualización de la unidad 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 5520, para la versión 8.10.162.0, aunque para cualquier versión y modelo se encuentra de forma similar.

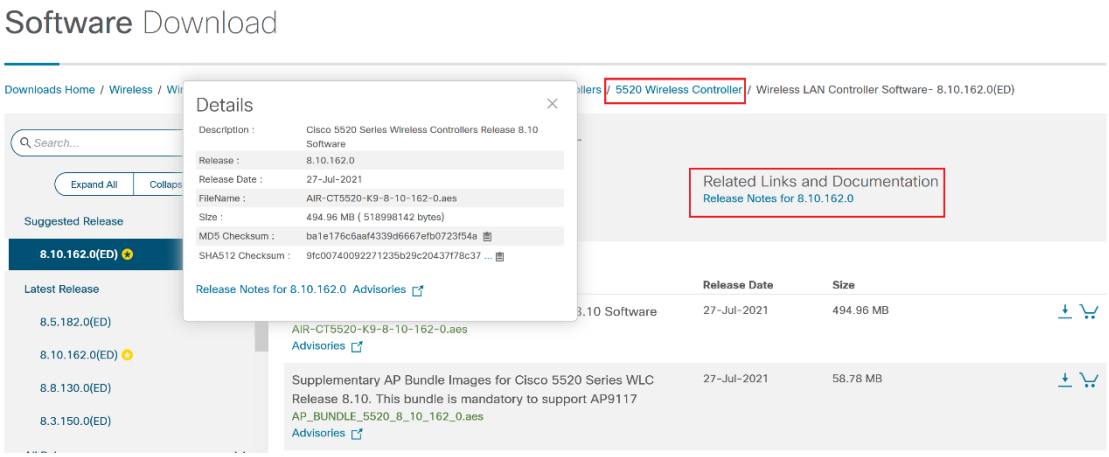


Ilustración 81. Descarga de las "*Release notes*" de la versión escogida

234. Es importante dentro de este documento observar el "*Upgrade Path*", que indica desde qué versión se puede actualizar directamente y desde cuál se recomienda hacer actualizaciones intermedias hasta llegar a la versión deseada. Se muestra el ejemplo para el equipo 5520, versión 8.10.162.0.

Table 2. Upgrade Path to Cisco Wireless Release 8.10.162.0

Current Software Release	Upgrade Path to Release 8.10.162.0
8.5.x	You can upgrade directly to Release 8.10.162.0.
8.6.x	You can upgrade directly to Release 8.10.162.0.
8.7.x	You can upgrade directly to Release 8.10.162.0.
8.8.x	You can upgrade directly to Release 8.10.162.0.
8.9.x	You can upgrade directly to Release 8.10.162.0.
8.10.x	You can upgrade directly to Release 8.10.162.0.

Ilustración 82. Comprobación del camino de actualización (*Upgrade Path*)

235. 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 "*Compatibility Matrix*" 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.

8.5.164.0	15.3(3)JF12i	Lightweight APs: 1600, 1700, 1800i, 1810 OEAP, 1810W, 1815i, 1815m, 1815t, 1815w, 1830, 1850, 2600, 2700, 2800, 3500e, 3500i, 3500p, 3600e, 3600i, 3600p, 3702e, 3702i, 3702p, 3800, 700, 700W, AP802, AP803, Integrated Access Point on Cisco 1100 ISR, ASA5506W-AP702 Outdoor and Industrial APs: 1532E, 1532I, 1540, 1552E, 1552H, 1552I, 1552C, 1552EU, 1552CU, 1552S, 1560, 1570, and IW3700 **Note** The Cisco Aironet 1550 Series APs with 64-MB memory are not supported. Modules: AIR-RM3010L-x-K9 and AIR-RM3000M
8.5.161.0	15.3(3)JF12	
8.5.160.0	15.3(3)JF11	
8.5.151.0	15.3(3)JF10	
8.5.140.0	15.3(3)JF9	
8.5.135.0	15.3(3)JF8	
8.5.131.0	15.3(3)JF7	
8.5.120.0	15.3(3)JF5	
8.5.110.0	15.3(3)JF4	
8.5.105.0	15.3(3)JF1	
8.5.103.0	15.3(3)JF	

Ilustración 83. Comprobación de compatibilidad de puntos de acceso tras actualización

236. Respecto al fichero de *firmware*, una vez se haya descargado, la recomendación es comprobar que es el realmente el fichero que indica la plataforma, y que no ha sufrido alteraciones. Para ello, se debe comprobar la firma HASH 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.

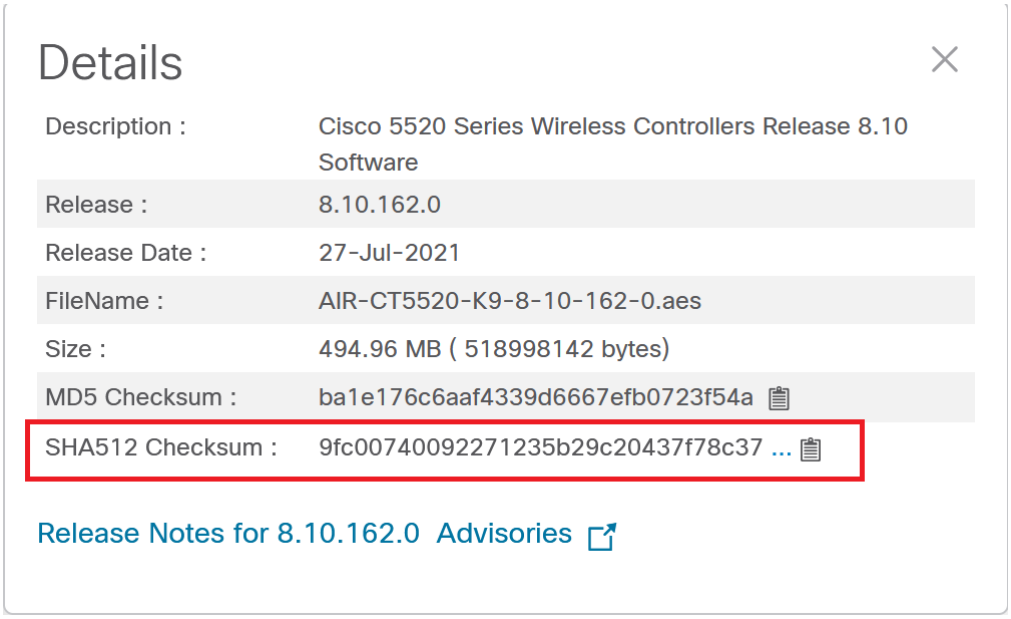


Ilustración 84. Comprobación del hash SHA-512 del fichero descargado

237. Sea una actualización directa o varias, el procedimiento de actualización es el mismo, y, de forma resumida, es el siguiente:

a) Guardar la configuración actual del dispositivo, ya sea a través del interfaz web (en cualquier vista de menú, esquina superior derecha, enlace "*Save Configuration*" o a través de comandos mediante sesión segura a través de SSH ejecutando "*save config*").

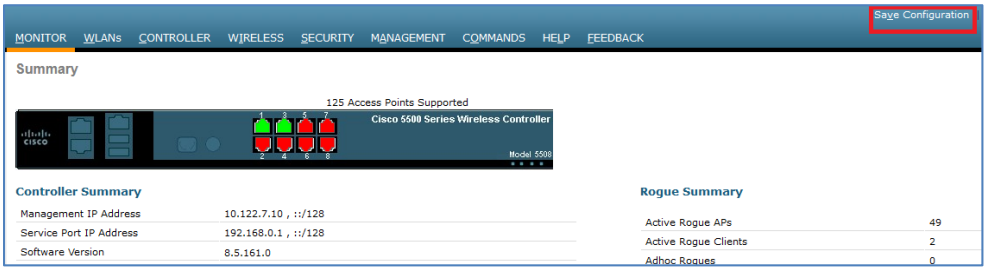


Ilustración 85. Enlace "*Save configuration*" disponible en cualquier vista del interfaz

b) Extraer la configuración del dispositivo de forma segura. Para ello, se puede realizar como se ha explicado en esta guía, a través del interfaz web, en el menú "*Commands*", sección "*Upload File*". En el menú que aparecerá en pantalla principal, se debe seleccionar la opción "*Configuration*" junto a la información del servidor en el que se desee almacenar la configuración.

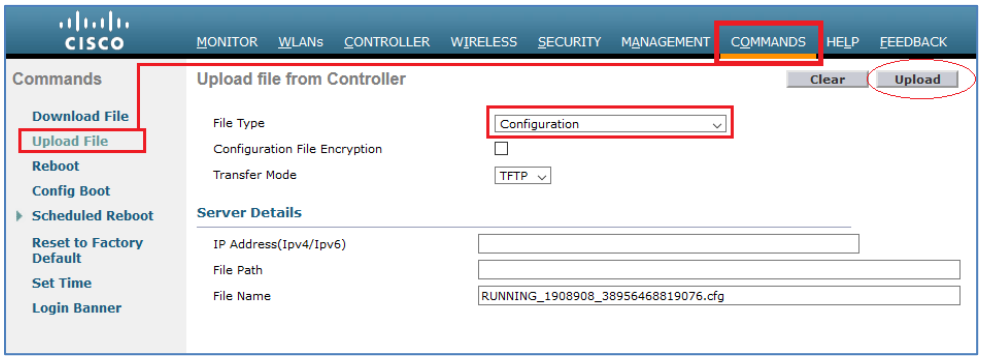


Ilustración 86. Menú "*Upload File*" para extraer a un servidor externo la configuración

c) Seguidamente, se puede subir la nueva versión al controlador inalámbrico, desde el menú "*Commands*", sección "*Download File*". En el menú que aparecerá, seleccionar la opción "*Code*" y completar la información del servidor donde está almacenada la versión. Durante la subida, una de las tareas del *script* interno que contiene el controlador inalámbrico es comprobar la firma del fichero de *firmware* que se está intentando incorporar al controlador, por lo que la comprobación de MD5 se realiza de un modo u otro, aunque no se haya realizado en un equipo externo confiable.

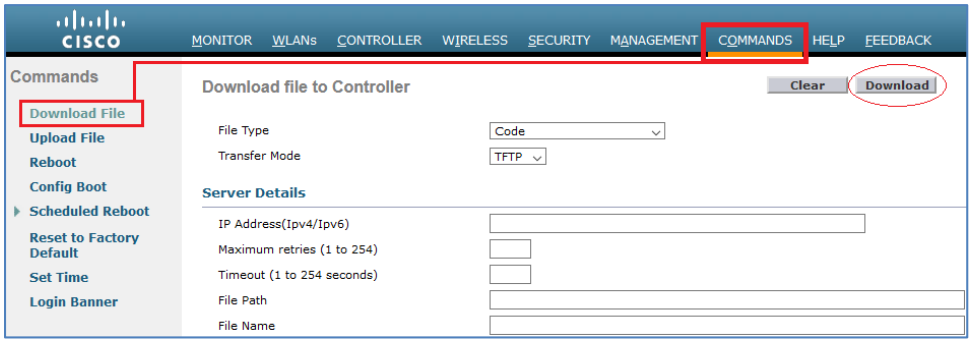


Ilustración 87. Menú "*Download File*" empleada para subir un *firmware* al dispositivo

d) Finalizado el proceso de reinicio del controlador, se deberá comprobar que la versión de firmware que está ejecutándose es la deseada.

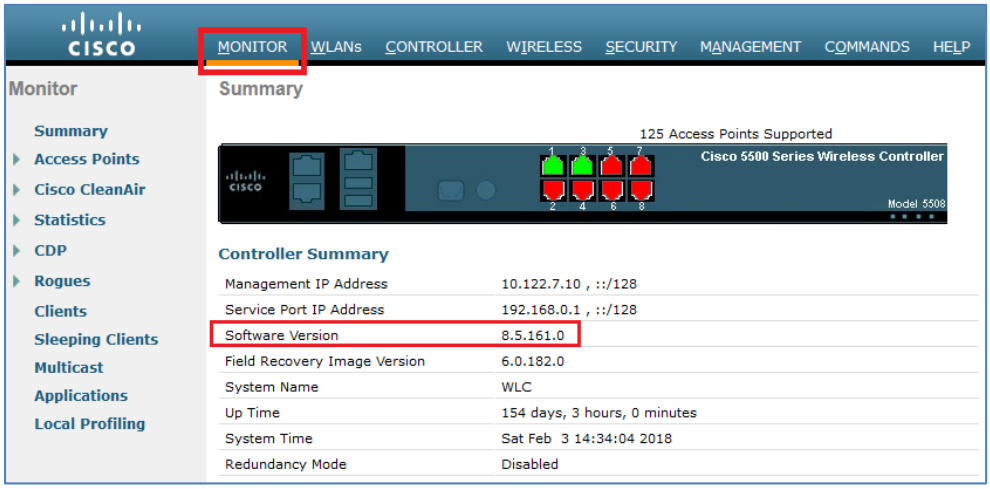


Ilustración 88. Menú "*Monitor*" empleado para confirmar la versión de *firmware*

9. LISTA DE COMPROBACIÓN

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto - Serigrafía y logo de Cisco en el embalaje. - Embalaje sellado, sin signos de haber sido manipulado. - Localización de la etiqueta resistente a manipulaciones. - Concordancia entre el número serie embalaje y el dispositivo. - Elementos incluidos por defecto en el embalaje.	☐	☐	
Configuración inicial - Ubicación segura del dispositivo (control de acceso físico y anclaje). - Equipo seguro (navegador web, cliente SSH, consola). - Uso de Cisco WLAN Express, CLI o SSID (*CiscoAirProvision*). - Cuenta/s administrador/es del dispositivo. - Verificación de la versión incorporada en el dispositivo. - Configuración de la 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.	☐	☐	
Crear perfiles IPSec (futuro uso para SNMP, RADIUS, etc.).	☐	☐	
Mensaje de aviso (*banner*) en el inicio de sesión.	☐	☐	
Configurar SNMP v3 y deshabilitar SNMP v1 y v2-v2c..	☐	☐	
Configurar SNMP *traps receiver* y aplicar perfil IPSec	☐	☐	
IPsec: Empleo del modo principal..	☐	☐	
Establecer tiempos máximos de inactividad de sesiones.	☐	☐	
Configurar política de contraseñas (cifrado, longitud, etc).	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Configurar sincronización horaria .	☐	☐	
Limitar usuarios y orígenes que alcanzan el dispositivo.	☐	☐	
LICENCIAMIENTO			
Según el tipo de licenciamiento: - Tradicional: Habilitar servidor para alojar fichero de licencias y deshabilitarlo tras su uso, o limitar el alcance al controlador inalámbrico. - RTU: Habilitar número de licencias adicionales desde interfaz web seguro. - *Smart Licensing*: o *Direct Cloud*: Usar navegador web (obtener token) e interfaz web seguro del controlador o *Proxy – Transport Gateway*: Equipo seguro con Proxy de Cisco instalado e interfaz web seguro del controlador. o *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, definir servidor *Syslog* y aplicar perfil *IPSec.*	☐	☐	
Habilitar tiempo máximo de sesión de usuario en la red.	☐	☐	
Activar protección de tramas de gestión.	☐	☐	
Definir algoritmo de cifrado por SSID WPA2: TKIP o AES-CCMP.	☐	☐	
Protección de claves criptográficas: - En modo de clave pre-compartida: PSK, uso reducido e indispensable por limitaciones de dispositivos clientes. Longitud de clave mínima de 12 caracteres, aleatoria y con cambio periódico. - En modo servidor de autenticación: Definir servidor/es AAA.	☐	☐	
Autenticación: - En modo 802.1X/EAP: Definir servidor/es AAA y método EAP-TLS	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Habilitar mecanismos de detección e intrusión (WIDS) con revisiones periódicas para evitar falsos positivos o falsos negativos.	☐	☐	
Proteger 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 (a través de una 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: - Guardar 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.	☐	☐	
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 HASH SHA-512 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.	☐	☐	

10. REFERENCIAS

CÓDIGO	REFERENCIA
CCN-STIC-816	Seguridad en Redes Inalámbricas en el ENS
[1]	*Cisco 5520 Wireless Controller Installation Guide* https://www.cisco.com/c/en/us/td/docs/wireless/controller/5500/5520/install-guide/b-wlc-ig-5520/m-overview.html?referring_site=RE&pos=3&page=https://www.cisco.com/c/en/us/support/wireless/5520-wireless-controller/model.html
[2]	*Cisco 8504 Series Wireless Controller Getting Started Guide* https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/8540-WLC-DG/b_Cisco-8540-WLC-deployment-guide.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/en/us/support/wireless/8540-wireless-controller/model.html#topic_5C2F636B64D743DAAEF01FB56A496361
[3]	*Cisco 5508 Wireless Controller Installation Guide* https://www.cisco.com/c/en/us/td/docs/wireless/controller/5500/5520/install-guide/b-wlc-ig-5520/m-installing.html#con_1369176
[4]	*Cisco 8504 Series Wireless Controller Getting Started Guide* https://www.cisco.com/c/en/us/td/docs/wireless/controller/8500/8540/install-guide/b-wlc-ig-8540/m-installing_the_controller.html#con_1414156
[5]	*Cisco 5520 Wireless Controller Installation Guide* https://www.cisco.com/c/en/us/td/docs/wireless/controller/5500/5520/install-guide/b-wlc-ig-5520/m-installing.html
[6]	*Cisco 8504 Series Wireless Controller Getting Started Guide* https://www.cisco.com/c/en/us/td/docs/wireless/controller/8500/8540/install-guide/b-wlc-ig-8540.html
[7]	*Cisco Wireless Controller Configuration Guide, Release 8.5* *https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/managing_users.html*
[8]	*Cisco Wireless LAN Controller Configuration Guide, Release 7.3* *https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-3/configuration/guide/b_cg73/b_wlc-cg_chapter_01010.html*

CÓDIGO	REFERENCIA
[9]	*Cisco Wireless LAN Controller (WLC) Configuration Best Practices* https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-6/b_Cisco_Wireless_LAN_Controller_Configuration_Best_Practices.html#concept_A9D3A22B47B64644B10E6EDF473A79FE
[10]	*Cisco Wireless Controller Configuration Guide, Release 8.5* https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/managing_certificates.html
[11]	*Cisco Wireless Controller Configuration Guide, Release 8.0* https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_011.html
[12]	*Main vs. Aggressive – Cisco Support* https://community.cisco.com/t5/security-documents/main-mode-vs-aggressive-mode/ta-p/3123382
[13]	*Cisco Wireless Controller Configuration Guide, Release 8.10* https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/snmp.html
[14]	*Cisco Wireless Controller Configuration Guide, Release 8.0* https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_01010.html
[15]	*Cisco Wireless Controller Configuration Guide, Release 8.0* https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/snmp.html?bookSearch=true
[16]	*Cisco Wireless Controller Configuration Guide, Release 8.0* https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_0110.html#ID1471
[17]	*Cisco Wireless Controller Configuration Guide, Release 8.10* https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/managing_configuration.html#password-encryptionl
[18]	*Cisco Wireless Controller Configuration Guide, Release 8.5* https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/managing_users.html#ID1404

CÓDIGO	REFERENCIA
[19]	*Cisco Wireless Controller Configuration Guide, Release 8.5* https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/network_time_protocol_setup.html
[20]	*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
[21]	*Smart Software Manager* https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html
[22]	*Troubleshooting TechNotes* https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-tech-notes-list.html

11. ABREVIATURAS

AAA	Autenticación, Autorización y Auditoría
ACL	*Access Control List*
AH	*Authentication Header*
CA	Autoridad de Certificación
CAPWAP	*Control And Provisioning of Wireless Access Points*
CBC	*Cipher-block Chaining*
CC	Common Criteria
CCI	*Co-channel interference*
CCMP	*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*
CCN	Centro Criptológico Nacional
CCX	*Cisco Compatible Extensions*
CHAP	*Challenge-Handshake Authentication Protocol*
CLI	Interfaz de Línea de Comandos
CLI	*Command Line Interface*
CoA	*Change of Authentication*
CRL	Lista Revocación Certificados
CSR	*Certificate Signing Request*
DBRG	*Digital Random Number Generator*
DH	*Diffie-Hellman*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
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*
EEPROM	*Electrically Erasable Programmable Read-Only Memory*
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*
FTP	*File Transfer Protocol*
HMAC	*Hash Message Authentication Code*
HTTP/S	*Hypertext Transfer Protocol / Secure*
IKE	*Internet Key Exchange*
IKE	*Internet Key Exchange*

IP	*Internet Protocol*
IPSec	*Internet Protocol Security*
ISAKMP	*Internet Security Association and Key Management Protocol*
LDAP	*Lightweight Directory Access Protocol*
MD5	*MEssage-Digest Algorithm 5*
MFP	*Management Frame Protection*
MIC	*Manufacturing Installed Certificate*
MKA	*MACsec Key Agreement*
MS-CHAP	*MicroSoft Challenge-Handshake Authentiacion Protocol*
NTP	*Network Time Protocol*
NTP	*Netowrk Time Protocol*
NVRAM	*Non-Volatile Random Access Memory*
PAP	*Password Authentication Protocol*
PEAP	*Protected Extensible Authentication Protocol*
PSK	*Pre-Shared Key*
RADIUS	*Remote Authentication Dial-In User Service*
RC4-SHA	*Rivest Cipher 4-Secure Hash Algorithm*
RFC	*Request for Comments*
ROM	Read-Only Memory
RSA	*Rivest Shamir and Adleman*
RTU	*Right To Use*
SA	Security Association
SNMP	*Simple Network Management Protocol*
SSC	*Self-Signed Certificate*
SSH	*Secure Shell*
SSID	*Service Set Identfier*
SSL	*Secure Sockets Layer*
SXP	*SGT Exchange Protocol*
TAC	*Technical Assistance Center*
TACACS	*Terminal Access Control Access Control System*
TKIP	*Temporal Key Integrity Protocol*
TLVS	*Threshold Limit Values*
URL	*Uniform Resource Locator*
USB	*Universal Serial Bus*
VPN	*Virtual Private Network*
vWLC	*Virtual Wireless LAN Controller*
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