Guía de Seguridad de las TIC
CCN-STIC 1426

Procedimiento de Empleo Seguro
Huawei WLAN AirEngine Series V600R024C00SPC100



Julio 2026

Edita:

Centro Criptológico Nacional, 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.07.28 09:04:22 +02'00'

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

AVISO LEGAL
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1 INTRODUCCIÓN 4
2 OBJETO Y ALCANCE 4
3 ORGANIZACIÓN DEL DOCUMENTO 4
4 FASE PREVIA A LA INSTALACIÓN 5
4.1 ENTREGA SEGURA DEL PRODUCTO 5
4.2 ENTORNO DE INSTALACIÓN SEGURO 5
4.3 REGISTRO Y LICENCIAS 5
4.4 CONSIDERACIONES PREVIAS 6
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 6
5 FASE DE INSTALACIÓN 8
6 FASE DE CONFIGURACIÓN 15
6.1 MODO DE OPERACIÓN SEGURO 15
6.2 AUTENTICACIÓN 15
6.3 ADMINISTRACIÓN DEL PRODUCTO 15
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 15
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 16
6.5 SERVIDORES DE AUTENTICACIÓN 16
6.6 SINCRONIZACIÓN 16
6.7 ACTUALIZACIONES 17
6.8 ALTA DISPONIBILIDAD 18
6.9 AUDITORÍA 19
6.10 BACKUP 19
7 REFERENCIAS 20
8 ABREVIATURAS 21

ÍNDICE DE FIGURAS

Ilustración 1: Conexión mediante puerto serie al Controlador. 8
Ilustración 2: Conexión mediante puerto serie al Controlador haciendo uso de Putty. 9
Ilustración 3: Menú de configuración del AC. 9
Ilustración 4: Sección de configuración básica del AC. 10
Ilustración 5: Sección de configuración de puertos del AC. 10
Ilustración 6: Estado del servidor DHCP ON. 10
Ilustración 7: Sección de configuración de interfaces del AC. 10
Ilustración 8: Configuración de interfaz del AC. 11
Ilustración 9: Creación de pool DHCP. 11
Ilustración 10: Configuración del conjunto de direcciones DHCP. 11
Ilustración 11: Sección de configuración de backups. 11
Ilustración 12: Sección de configuración de VLAN de servicio del AC. 12
Ilustración 13: Sección de revisión de configuración del AC. 12
Ilustración 14: Sección de autenticación de APs en el AC. 12
Ilustración 15: AP autenticado en el AC. 13
Ilustración 16: Enlace de AP a un grupo en el AP. 13
Ilustración 17: Revisión de APs autorizados en el AC. 13
Ilustración 18: Creación de SSID. 13

Ilustración 19: Configuración del nombre de SSID, VLAN de servicio y modo de redirección. .. 14
Ilustración 20: Configuración de seguridad del AP. 14
Ilustración 21: Enlace del grupo al AP y selección de radio y tasa de transferencia en el AP. ... 14
Ilustración 22: Escenario HSB. 18
Ilustración 23: Escenario HSB en caso de que el AC maestro falle. 19

1 INTRODUCCIÓN

1. El **Huawei WLAN AirEngine Series** es un Punto de Acceso (AP). destinado a proporcionar conectividad Wi-Fi empresarial en redes corporativas. En la configuración considerada en esta guía de empleo seguro, el AP opera en el denominado modo FIT, por lo que no funciona como un dispositivo autónomo, sino como un elemento gestionado por un controlador WLAN o Access Controller (AC).
2. En el modo FIT, el AP aplica las configuraciones, políticas de seguridad y parámetros operativos definidos y distribuidos por el AC. Las funciones de administración centralizada, autenticación de usuarios, integración con servicios externos de autenticación y gestión de eventos se realizan desde el AC o a través de los componentes del entorno operacional asociados.
3. El producto se distribuye como equipo dedicado o appliance, compuesto por el hardware y software necesarios para desempeñar las funciones propias del AP. No obstante, para su operación en el modo FIT requiere la existencia de un AC compatible, que actúa como componente necesario del entorno operacional para la configuración, administración y operación segura del AP.
4. Los APs en el modo FIT son dependientes de un AC, el cual permite gestionar de forma centralizada múltiples AP, distribuir configuraciones, controlar los parámetros de seguridad WLAN y coordinar la operación de la infraestructura inalámbrica.

2 OBJETO Y ALCANCE

5. La configuración incluida en la presente guía de empleo seguro es la evaluada y cualificada en el Catálogo de Productos y Servicios de STIC (CPSTIC). La versión del firmware evaluada es la **V600R024C00SPC100**.
6. El producto **Huawei WLAN AirEngine Series** ha sido incluido en el catálogo de productos y servicios STIC (CPSTIC) y para consultar el listado, categoría o nivel y familia consulte [REF3].

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. El producto evaluado se distribuye en forma de appliance hardware que incluye el firmware necesario para su operación segura. Antes de proceder con la instalación y configuración del producto, se recomienda verificar la integridad física del dispositivo y la autenticidad del firmware instalado. Se debe comprobar:

    - **Información de envío.** Se debe comprobar la documentación de envío para verificar que concuerda con la orden de compra original y que el envío ha sido realizado por Huawei.
    - **Embalaje externo.** Se debe inspeccionar el embalaje y la cinta de embalaje con la marca de Huawei. Se debe comprobar que la cinta esté intacta y que no haya sido cortada ni se haya deteriorado en ningún punto. Además, se debe inspeccionar que la caja no presente cortes ni daños que permitan acceder al dispositivo.
    - **Embalaje interno.** Se debe comprobar el embalaje interior de la misma manera que el embalaje exterior. Adicionalmente, se debe comprobar que la etiqueta presente en el embalaje exterior concuerda con el modelo de dispositivo adquirido.
    - **Sello de garantía.** Se deberá verificar que la placa de identificación del producto, alojada en el chasis, es consistente con la etiqueta del embalaje del producto.

8. En caso de que exista algún desperfecto o alguna inconsistencia será necesario contactar con el soporte de Huawei de manera inmediata para recibir instrucciones. No se recomienda realizar la instalación en este caso.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. El Huawei WLAN AirEngine Series deberá instalarse en un entorno físicamente seguro y controlado. El acceso físico a los dispositivos Huawei WLAN AirEngine Series y a los AC deberá estar restringido exclusivamente a personal autorizado con funciones de administración o mantenimiento.

10. Se recomienda que los componentes críticos del entorno operacional, incluyendo:

    - Controladoras de Acceso (AC)
    - Estaciones de administración se desplieguen en ubicaciones con medidas de protección física adecuadas y mecanismos de control de acceso.

4.3 REGISTRO Y LICENCIAS

11. En la configuración evaluada en modo FIT, la gestión y activación de licencias no se realiza directamente sobre el Huawei WLAN AirEngine Series sino sobre un AC, encargado de gestionar centralizadamente el número de APs autorizados para operar en la red.

12. Antes de iniciar el proceso de activación de licencias, es necesario disponer del número de serie electrónico (ESN) del AC. Asimismo, deberá cargarse previamente en la controladora el fichero de licencia proporcionado por Huawei, utilizando un mecanismo seguro de transferencia de archivos, preferiblemente SFTP.

13. Una vez transferido el fichero de licencia, deberá verificarse que este corresponde correctamente con el dispositivo utilizando el siguiente comando:

```
license verify [licencia]
```

14. Tras validar correctamente el fichero, deberá activarse la licencia mediante el siguiente comando:

```
license active [licencia]
```

15. Posteriormente, se recomienda comprobar que la licencia ha quedado correctamente activada y que su estado es válido, ya sea permanente o temporal (demo), utilizando el siguiente comando:

```
display license
```

16. Para más información consultar la sección “Installing Licenses” de [REF1].

4.4 CONSIDERACIONES PREVIAS

17. El producto evaluado opera exclusivamente en modo FIT, lo que implica que el punto de acceso inalámbrico no funciona como un dispositivo autónomo e independiente, sino como un elemento gestionado centralmente por un AC. En este modo de operación, el Huawei WLAN AirEngine Series delega las funciones de control, gestión y aplicación de políticas de seguridad en el AC, limitándose principalmente a proporcionar conectividad inalámbrica y ejecutar las configuraciones distribuidas por la controladora.

18. Debido a esta arquitectura centralizada, todas las configuraciones de seguridad relevantes del entorno inalámbrico se realizan desde el AC. Esto incluye, entre otros aspectos, la definición de SSIDs, políticas de autenticación, configuración de cifrado, parámetros de seguridad inalámbrica, políticas de acceso y perfiles de red. Por tanto, la seguridad efectiva del despliegue depende en gran medida de la correcta protección y configuración del AC.

19. Asimismo, la autenticación centralizada de usuarios mediante servidores RADIUS es gestionada exclusivamente por el AC. El Huawei WLAN AirEngine Series no establece comunicaciones directas con servidores RADIUS ni implementa funcionalidades de protección IPsec asociadas a este tráfico. Todas las comunicaciones relacionadas con autenticación 802.1X y validación de credenciales son realizadas por el AC, quedando estos mecanismos fuera del alcance directo del producto evaluado.

20. Adicionalmente, el Huawei WLAN AirEngine Series no realiza el envío directo de registros de auditoría a servidores Syslog remotos. La recopilación centralizada de eventos y logs podrá realizarse desde la infraestructura de gestión o desde el propio AC.

21. Finalmente, el AC debe contar con el firmware con una versión mínima V200R024C00SPC100 o superior instalada. En caso de no contar con esa versión, se deberá instalar, el cual puede ser obtenido exclusivamente del paquete oficial suministrado con el producto o del portal oficial de soporte de Huawei [REF2]. Para ello, se deberá transferir mediante SFTP al AC.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

22. El entorno de operación del producto debe estar compuesto por los siguientes elementos hardware en su entorno:

- Controladora de Acceso (AC): Dispositivo utilizado para la administración y configuración centralizada del Huawei WLAN AirEngine Series.
- Equipo de Administración: equipo utilizado por los administradores autorizados para la gestión del producto a través del AC.

23. El Huawei WLAN AirEngine Series deberá conectarse físicamente al AC mediante interfaces autorizadas dentro del entorno.

5 FASE DE INSTALACIÓN

24. La instalación física de los AC (ya sea en un rack, en un escritorio o en una pared), así como las medidas de precaución a tomar para cada uno de los diferentes casos se puede encontrar en la [REF1] en los módulos bajo "Installation" → "Hardware Installation and Maintenance Guide" → "Access Controllers". No obstante, se puntualiza que el lugar de instalación debe consistir en un lugar aislado y con buena ventilación, al que solo tenga acceso el personal autorizado.
25. La instalación física de los AP (ya sea en pared o raíles), así como las medidas de precaución a tomar en cada uno de los diferentes casos se puede encontrar en la [REF1] en los módulos bajo "Installation" → "Hardware Installation and Maintenance Guide" → "Indoor/Outdoor Access Points".
26. El AC se instalará en una ubicación apropiada y se conectará a la corriente. Cabe aclarar que el AC no forma parte del producto evaluado, si bien constituye un componente necesario del entorno operacional, por lo que deberá obtenerse de forma adicional.
27. El AP se conectará a la corriente y a algún puerto del GigabitEthernet del AC , bien sea punto a punto o mediante dispositivos de red. En caso de que el AP use alimentación mediante PoE, el AP se conectará únicamente mediate un cable rj45 al inyector PoE, mientras que el inyector se conectará a la corriente y al AC.
28. Para la configuración inicial del AC se utilizará un PC de administración, para acceder al AC.
29. El PC de administración se conectará al AC mediante el puerto serie/consola para realizar el acceso inicial por CLI. Asimismo, cuando sea necesario acceder a la interfaz de administración de red, el PC de administración se conectará a la interfaz Ethernet de gestión del AC, identificada como puerto ETH. La dirección IP de gestión configurada por defecto en el AC para dicha interfaz es 169.254.1.1.

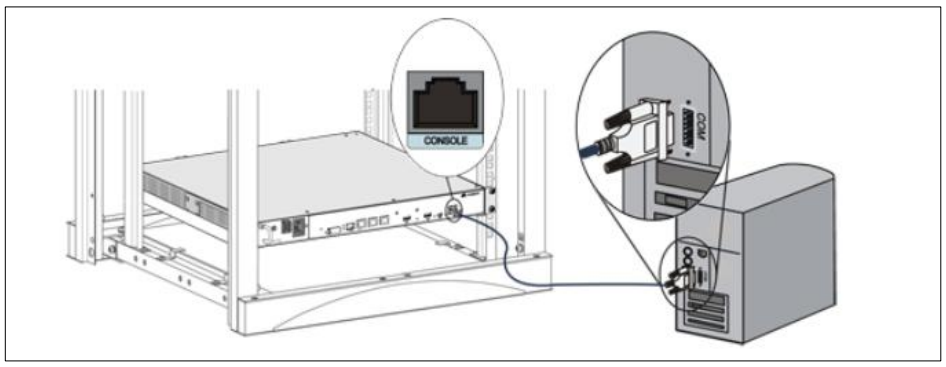


Ilustración 1: Conexión mediante puerto serie al Controlador.

30. Una vez todo esté debidamente conectado, se procederá a iniciar sesión mediante el puerto serie. En el PC se hará uso del software *Putty* con los siguientes parámetros para iniciar sesión en el dispositivo. Es importante destacar que el parámetro "*Serial Line*" dependerá del número de puertos de cada PC.

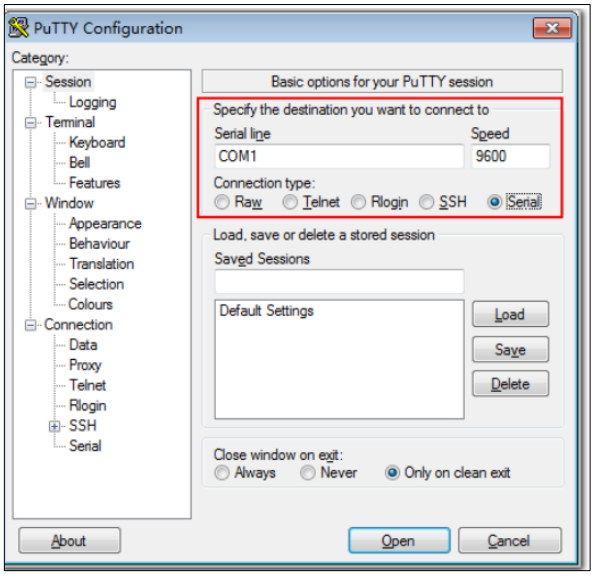


Ilustración 2: Conexión mediante puerto serie al Controlador haciendo uso de Putty.

31. Al conectarse por primera vez, se requerirá introducir el nombre de usuario y la contraseña por defecto, los cuales son "admin:admin@huawei.com". Se deberá cambiar la contraseña del dispositivo.

32. De esta forma, ya estaría operativa la interfaz de comandos a través de la conexión *serial*.

33. Las medidas de seguridad aplicables a las interfaces, puertos y servicios utilizados durante la instalación y operación se recogen en la sección *6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS*.

34. Para establecer la conexión entre el AP y el AC mediante la CLI es necesario seguir las secciones "*Configuring a DHCP Server*", "*Configuring Network Interconnections*", "*Configuring Country Codes*", "*Configuring a Source Interface or a Source Address*" y "*Adding APs*" de [REF1], en el orden mencionado. Dichas secciones se encuentran bajo el módulo "*Configuration*" → "*CLI-based Configuration*" → "*WLAN Service Configuration Guide*" → "*Configuring APs to Go Online*" de [REF1].

35. En caso de que se desee realizar la instalación mediante la interfaz web, se debe acceder mediante el PC conectado al puerto de gestión a la dirección web https://169.254.1.1/. Se hará login con el usuario admin y la contraseña establecida previamente en el puerto serie. De esta manera podrá accederse a la interfaz HTTPS de administración.

36. Desde la interfaz web, acceda a la sección "*Configuration*" y la sección "*Config Wizard*". Clic en "*AC*".

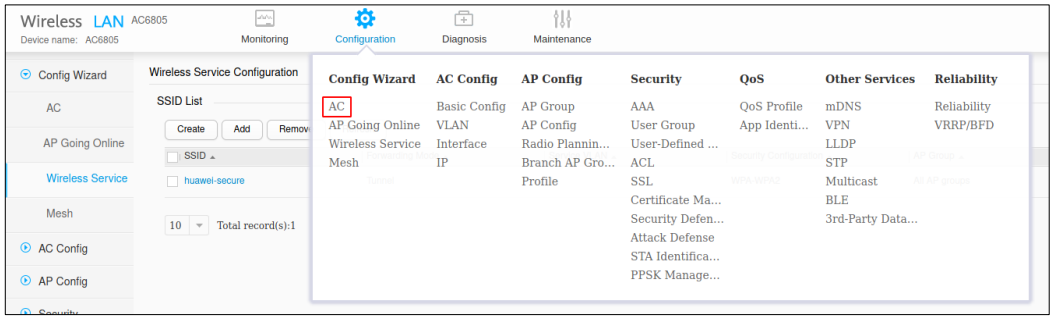


Ilustración 3: Menú de configuración del AC.

37. Establezca el nombre del AC, la región, la hora y carga la licencia si no se ha hecho previamente.



Ilustración 4: Sección de configuración básica del AC.

38. Clic "*Next*".

39. Compruebe que el puerto en el que el AP está conectada es de color verde y que su VLAN por defecto es la VLAN 1. En esta instalación se usa la VLAN 1 como VLAN por defecto, aunque no es obligatorio usar exactamente dicha VLAN.

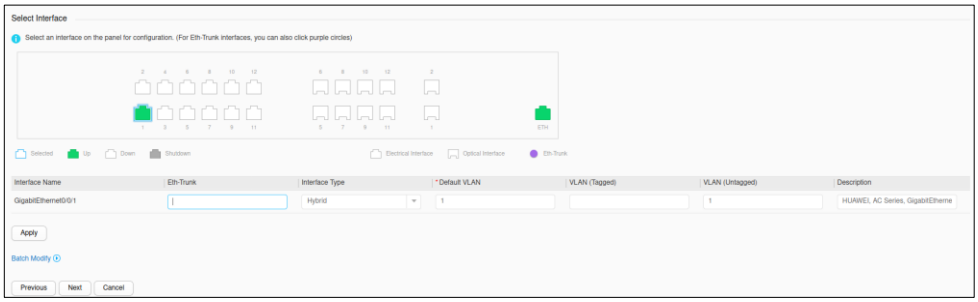


Ilustración 5: Sección de configuración de puertos del AC.

40. Clic "*Next*".

41. Asegure que el estado de DHCP se encuentra "*ON*".

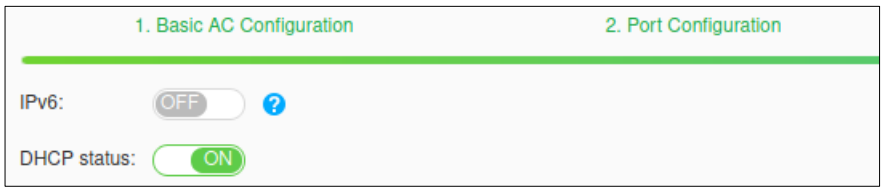


Ilustración 6: Estado del servidor DHCP ON.

42. En la sección "Interface Configuration", clic en la VLAN establecida como VLAN por defecto para el puerto del AP.



Ilustración 7: Sección de configuración de interfaces del AC.

43. Establezca una dirección IP para la VLAN por defecto y clic "OK".

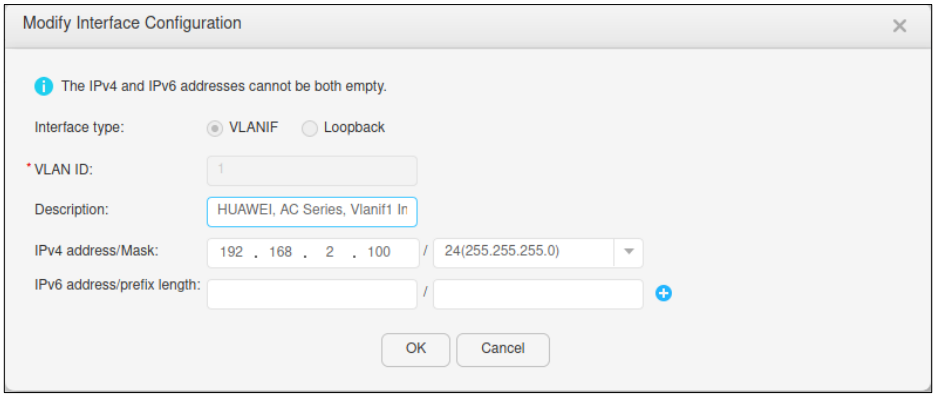


Ilustración 8: Configuración de interfaz del AC.

44. En la sección "DHCPv4 Address Pool List", clic en "Create".



Ilustración 9: Creación de pool DHCP.

45. Seleccione "*Interface Address Pool*" y seleccione la interfaz por defecto usada en el puerto conectado al AP.

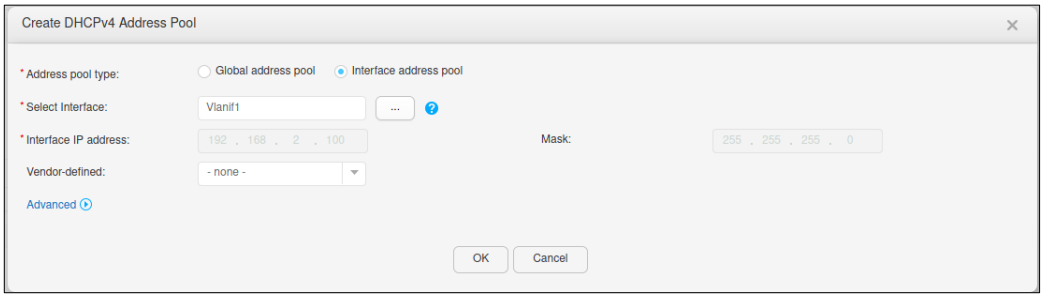


Ilustración 10: Configuración del conjunto de direcciones DHCP.

46. Clic "*OK*".
47. Clic "*Next*" de nuevo.
48. Configure la dirección de la interfaz virtual recién creada. Seleccione la VLAN recién creada en el campo "*Select interface*". Seleccione el tipo de dirección IP (IPv4 en este caso) e introduzca la dirección deseada.
49. Clic "*Next*".
50. Clic "Next" de nuevo en la sección de "AC Backup Configuration".

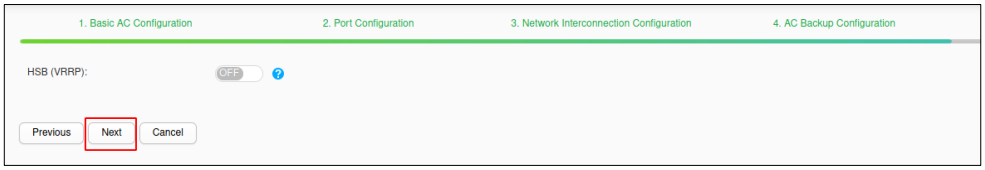


Ilustración 11: Sección de configuración de backups.

51. Establezca la VLAN de servicio, la cual será la establecida en el puerto conectado al AP. Para ello, selecciónala en la sección de "*AC Source Address*".

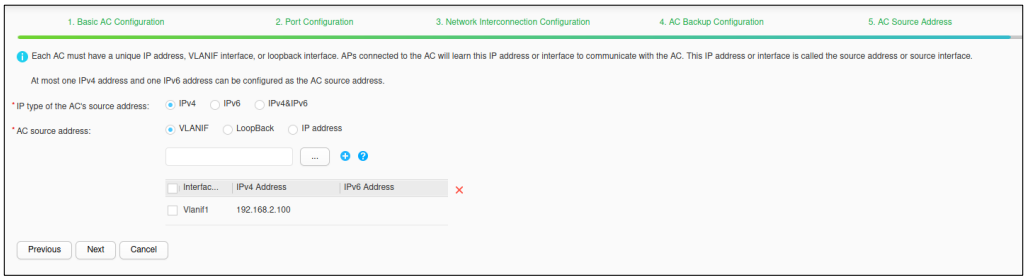


Ilustración 12: Sección de configuración de VLAN de servicio del AC.

52. Clic "*Next*".

53. Revise la configuración y clic en "*Continue With AP Online*".

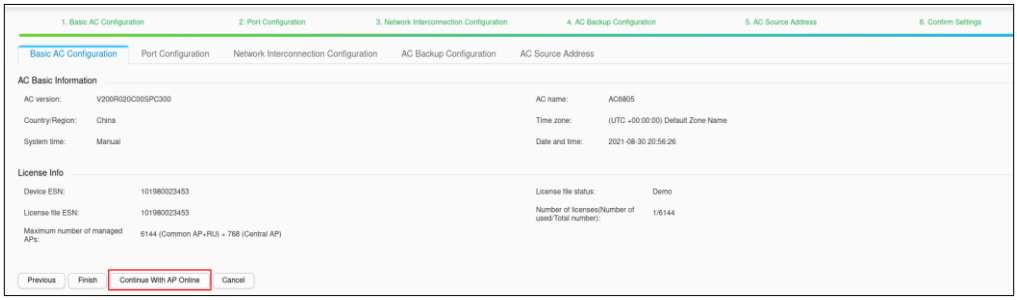


Ilustración 13: Sección de revisión de configuración del AC.

54. Verifique que aparece el AP sin autenticar.



Ilustración 14: Sección de autenticación de APs en el AC.

55. Seleccione el AP y autentícalo pulsando en "*Authenticate*". Una vez autenticado debería añadir un valor al campo "*AP Name*".



Ilustración 15: AP autenticado en el AC.

56. Pulsa "*Next*".
57. En este caso se incluirá el AP en el grupo default. Pulsa "*Next*".

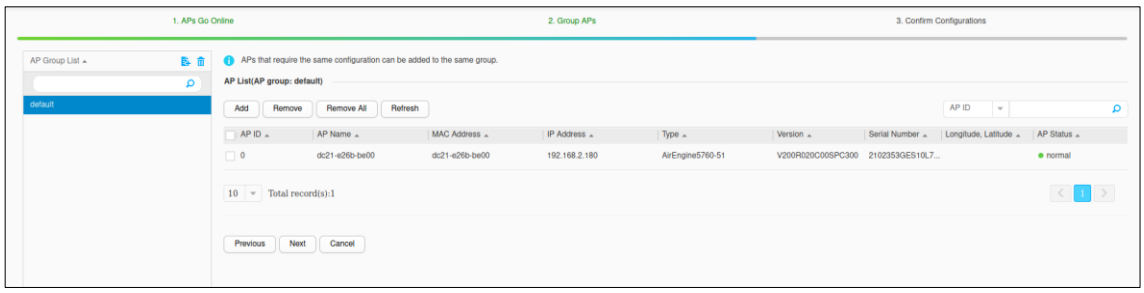


Ilustración 16: Enlace de AP a un grupo en el AP.

58. Compruebe que se ha añadido el AP al grupo default y pulsa "*Continue With Wireless Service Configuration*".

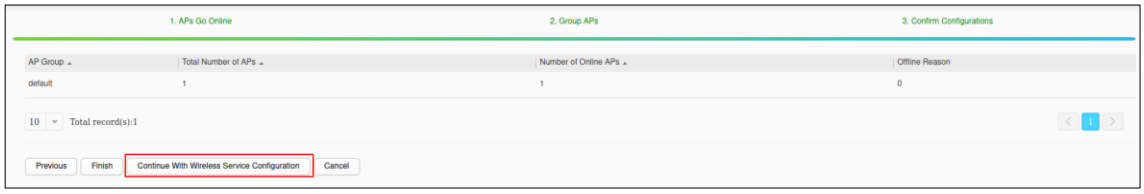


Ilustración 17: Revisión de APs autorizados en el AC.

59. En la sección "*Wireless Service Configuration*", cree un SSID. Para ello clic en "*Create*".



Ilustración 18: Creación de SSID.

60. Establezca el nombre del SSID, la VLAN de servicio (en este caso corresponde a la VLAN la cual corresponde al puerto conectado al AP) y el modo de redireccionamiento (en este caso se usará el modo directo).

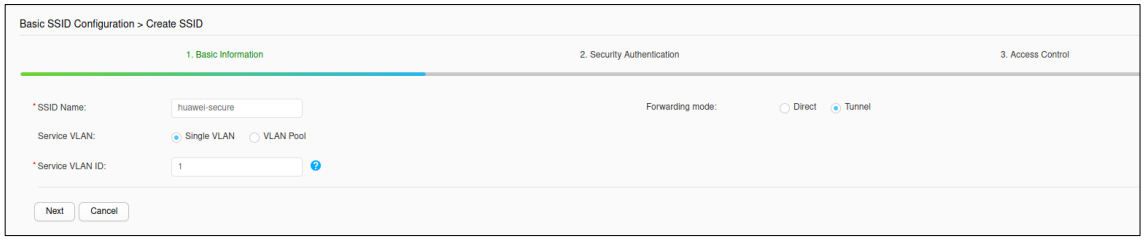


Ilustración 19: Configuración del nombre de SSID, VLAN de servicio y modo de redirección.

61. Clic "*Next*".

62. Establezca la seguridad del Punto de Acceso. En caso de escoger una clave, asegure usar únicamente WPA2/3-Enterprise (AES), y junto con una contraseña de longitud y complejidad considerable.

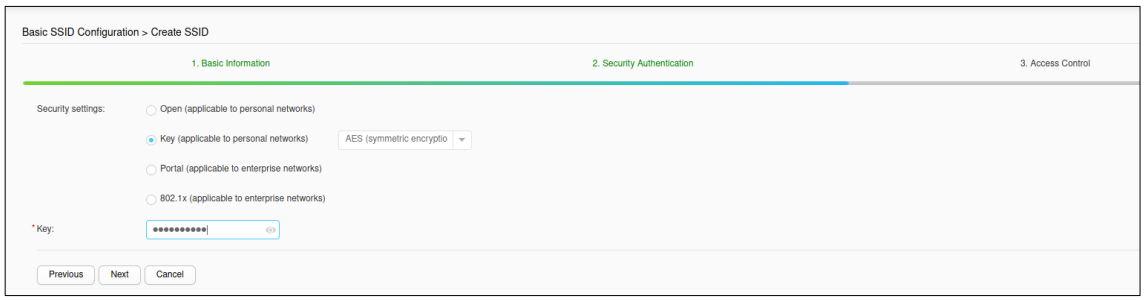


Ilustración 20: Configuración de seguridad del AP.

63. Clic "*Next*".

64. Enlace el grupo de AP que se haya configurado. En este caso se usará el grupo "*default*". Seleccione la tasa de *uplink* y *downlink*.

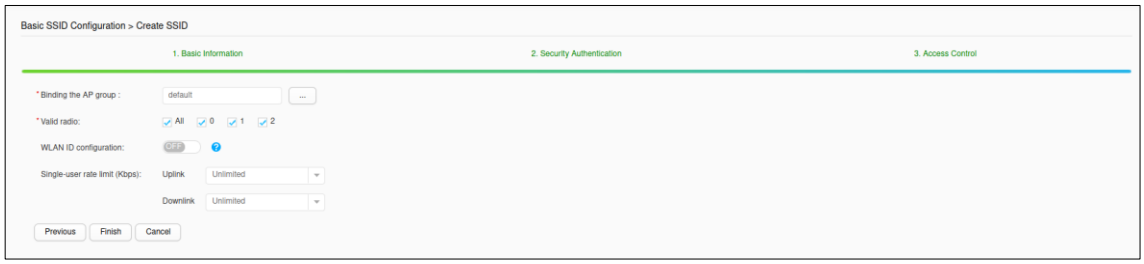


Ilustración 21: Enlace del grupo al AP y selección de radio y tasa de transferencia en el AP.

65. Clic "*Finish*".

66. Con esta configuración tanto el AP como el AC quedarán instalados.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

67. El Huawei WLAN AirEngine Series opera en modo FIT por lo que toda la gestión y distribución de configuración deberá realizarse desde el AC.

68. Se debe habilitar el cifrado DTLS del canal CAPWAP de control y, cuando sea compatible con el despliegue, también del canal de datos.

69. Para ello se deberán ejecutar los siguientes comandos desde el modo system-view:

```
system-view
capwap dtls control-link encrypt on
capwap dtls data-link encrypt on
```

6.2 AUTENTICACIÓN

70. El Huawei WLAN AirEngine Series opera en modo FIT, por lo que las funcionalidades de autenticación y control de acceso inalámbrico son gestionadas centralizadamente por el AC. En esta arquitectura, el punto de acceso no realiza autenticación directa frente a servidores externos.

71. Todas las comunicaciones con servidores de autenticación externos, incluyendo servidores RADIUS utilizados para autenticación 802.1X/WPA2-Enterprise o WPA3-Enterprise, son realizadas exclusivamente por la controladora AC, quedando dichas comunicaciones fuera del alcance del producto evaluado. Se recomienda que la infraestructura de controladora utilice mecanismos de autenticación robustos, preferiblemente EAP-TLS con certificados digitales, así como protocolos y algoritmos criptográficos seguros.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

72. Debido a que el Huawei WLAN AirEngine Series opera en modo FIT, la administración, configuración y monitorización de los APs se realiza centralizadamente desde el AC.

73. La administración local de la infraestructura WLAN se realiza a través de la interfaz serie del AC, desde donde se gestionan centralizadamente los APs FIT. Para ello es necesario conectarse al puerto serie del AC con un cable de consola. Para acceder a las funciones de administración de la línea de comandos es necesario autenticarse con la contraseña de usuario admin establecida en la fase de instalación en la sección *5 FASE DE INSTALACIÓN*.

74. La administración remota del AC se realiza a través de SSH, para ello es necesario conectarse al producto con un cable de Ethernet en una interfaz física habilitada para tal propósito. Para acceder a las funciones de administración de la línea de comandos es necesario autenticarse con las credenciales de un usuario autorizado por SSH al AC. También es posible la gestión a través de la interfaz web del AC por HTTPS.

75. La administración remota del AP se realizará, a través del AC, al cual se accede mediante SSH o mediante la interfaz web por HTTPS, como se indica en el punto anterior.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

76. Durante la operación segura del entorno, deberán habilitarse únicamente las interfaces, puertos y servicios estrictamente necesarios para la administración y funcionamiento del AP en modo FIT.

77. En el modo FIT, el AP opera como dispositivo gestionado por el AC. Por tanto, las interfaces y servicios de administración se concentran principalmente en el AC, mientras que el AP aplica las configuraciones y políticas distribuidas por el AC.

78. Como mínimo, se deberán aplicar las siguientes medidas:

    a) Utilizar la interfaz serie del AC únicamente para la configuración inicial y tareas de mantenimiento autorizadas.

    b) Utilizar HTTPS para la administración web del AC, evitando el uso de HTTP no cifrado.

    c) Utilizar SSH para la administración remota por CLI, evitando Telnet.

    d) Limitar el acceso a las interfaces de administración del AC a redes de administración autorizadas.

    e) Configurar únicamente las VLAN necesarias para la gestión del AC, la conexión con los AP y los servicios WLAN definidos.

    f) Deshabilitar servicios no utilizados o no necesarios para la configuración evaluada.

    g) Proteger el canal CAPWAP entre AP y AC mediante DTLS para el enlace de control y, cuando sea compatible con el despliegue, para el enlace de datos.

6.5 SERVIDORES DE AUTENTICACIÓN

79. El AC es capaz de utilizar un servidor RADIUS externo como servidor de autenticación tanto para sus puertos físicos como para los usuarios que se conecten mediante el AP. Existe una gran cantidad de posibilidades a la hora de configurar el AC en función del entorno y de la funcionalidad concreta deseada. En la [REF1] se puede encontrar un ejemplo de configuración que puede ser de utilidad en la sección "*Configuration*" → *"Typical Configuration Examples"* → "Authentication Configuration Examples" → "Example for Configuring 802.1X Authentication".

6.6 SINCRONIZACIÓN

80. En lugar de establecer el tiempo manualmente, se recomienda el uso de un servidor NTP para la sincronización horaria. Se deben ejecutar las siguientes instrucciones desde el modo system-view en el AC para establecer un servidor externo NTP:

```
system-view
ntp-service unicast-server <IP_NTP>
```

81. Por defecto, se utiliza a versión 3 del protocolo NTP.

82. Se recomienda habilitar autenticación NTP mediante claves compartidas para proteger la integridad de la sincronización horaria.

83. Para ello, una vez configurada la clave en el servidor NTP, se deben ejecutar las siguientes instrucciones desde el modo system-view en el AC:

```
system-view
ntp-service authentication enable
ntp-service authentication-keyid <ID_Clave> authentication-mode hmac-sha256 cipher <Clave>
ntp-service reliable authentication-keyid <ID_clave>
```

6.7 ACTUALIZACIONES

84. La disponibilidad de nuevas versiones, parches o actualizaciones de seguridad será notificada al usuario final a través de los canales oficiales de Huawei, tales como el portal de Huawei [REF2], boletines de seguridad, comunicaciones del servicio de soporte contratado o notificaciones emitidas por el fabricante autorizado.

85. El administrador del producto deberá revisar periódicamente dichos canales para identificar actualizaciones aplicables a la versión desplegada. Antes de instalar cualquier actualización, se deberá verificar que el paquete procede de una fuente oficial de Huawei, que corresponde a la versión del producto instalada y que su integridad y validez han sido comprobadas por los mecanismos previstos por el fabricante.

86. En la configuración segura evaluada no se requiere que el producto descargue automáticamente actualizaciones desde Internet. La obtención de paquetes podrá realizarse de forma manual por un administrador autorizado y su instalación deberá seguir el procedimiento descrito en la sección “Configuring System Startup Files” de [REF1].

87. Tanto el AC, como el AP, contemplan dos tipos de actualizaciones:

    a) Parches: Actúan sobre una versión del software del sistema. El producto comprueba la validez del parche antes de cargarlo en el sistema. Su extensión es (.pat).

    b) *Software/firmware* del sistema: Se puede definir como el sistema operativo del producto. Al igual que los paquetes de parches, el producto comprueba la validez e integridad del software del sistema. Su extensión es (.cc).

88. Ambos tipos de actualizaciones puede descargarse de la web oficial de Huawei [REF2] y deben de subirse al directorio raíz del AC mediante SFTP.

89. Para establecer un parche en el AC es necesario ejecutar la siguiente instrucción:

```
startup patch <Parche>
```

90. Para establecer un firmware en el AC es necesario ejecutar la siguiente instrucción:

```
startup system-software <Firmware>
```

91. En el caso de que se quiera establecer un parche en el AP, es necesario subir el archivo al directorio raíz del AC y ejecutar en el mismo los siguientes comandos:

```
system-view
wlan
ap-patch update load ap-name <Nombre_AP> update-filename <Parche>
```

92. En el caso de querer establecer un firmware nuevo en el AP, también es necesario hacerlo desde el AC como en el caso anterior. Se debe subir el archivo al AC y ejecutar:

```
system-view
wlan
ap update load ap-name <Nombre_AP> update-filename <Firmware>
```

93. Para listar el firmware del sistema y el paquete de parches configurados en el producto se debe de ejecutar el siguiente comando en el AC:

```
display startup
```

94. Para listar el firmware de los puntos de acceso debe ejecutar el siguiente comando en el AC:

```
display ap version all
```

6.8 ALTA DISPONIBILIDAD

95. El producto cuenta con la funcionalidad HSB, la cual permite que los AP no pierdan conectividad en caso de que el AC o los enlaces entre ellos se caigan.

96. Como se puede observar en la Ilustración 22, el AC1 actúa como maestro, de forma que el AC2 se dedica a realizar copias de seguridad de la configuración del AC1.

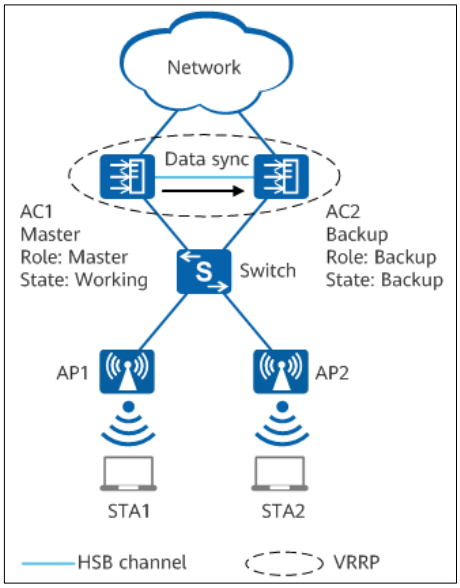


Ilustración 22: Escenario HSB.

97. Como se puede observar en la Ilustración 23, al producirse un error en AC1, en el Switch o en el enlace a la red, la conexión se deriva a AC2 y por tanto los APs no pierden conexión.

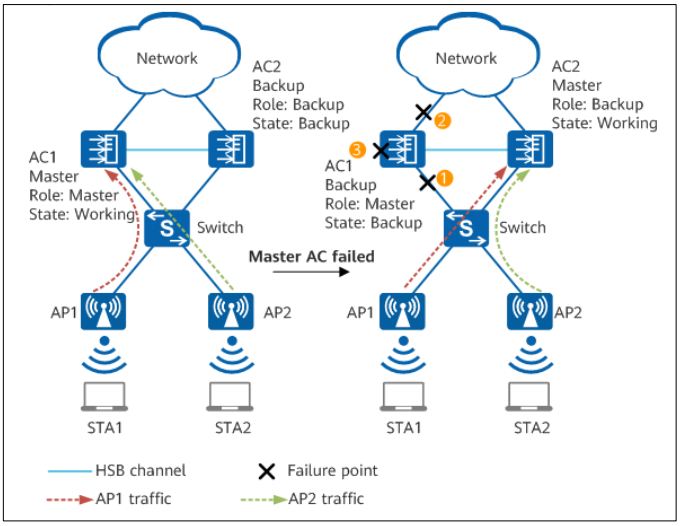


Ilustración 23: Escenario HSB en caso de que el AC maestro falle.

98. La configuración del servicio VRRP HSB se puede consultar en la sección "Configuration" → "CLI-based Configuration" → "Reliability Configuration Guide" → "AC Backup Configuration" → "VRRP HSB Configuration" → "Configuring an HSB Service" de la [REF1].

6.9 AUDITORÍA

99. No aplica directamente al AP en la configuración evaluada. En el modo FIT, la recopilación, almacenamiento, consulta y envío remoto de registros de auditoría se realiza desde el AC o desde componentes del entorno operacional asociados, no desde el AP de forma autónoma. Por tanto, las subsecciones relativas a registro de eventos, almacenamiento local y almacenamiento remoto de logs se consideran no aplicables al AP evaluado. La configuración de auditoría deberá realizarse, cuando proceda, en el AC conforme a la sección "Configuring Information Center" de [REF1].

6.10 BACKUP

100. No aplica directamente al AP en la configuración evaluada. En el modo FIT, el AP aplica la configuración distribuida por el AC, pero no mantiene de forma autónoma la configuración principal ni proporciona mecanismos propios de backup gestionables por el administrador dentro del alcance evaluado.

101. Las copias de seguridad deberán realizarse sobre el AC y/o la plataforma de gestión correspondiente, donde residen las configuraciones, perfiles WLAN, políticas de seguridad y parámetros operativos del despliegue. Se recomienda realizar backups periódicos del AC conforme a la sección "Managing Configuration Files" de [REF1].

7 REFERENCIAS

[REF1] Wireless Access Controller (AC and Fit AP) V200R024C00 Configuration Guide
https://support.huawei.com/enterprise/en/doc/EDOC1100407652/f4443c85/about-this-document

[REF2] Huawei Support webpage
https://support.huawei.com

[REF3] Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN. https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8 ABREVIATURAS

AC	Access Controller
AES	Advanced Encryption Standard
AP	Access Point
CAPWAP	Control And Provisioning of Wireless Access Points
CLI	Command Line Interface.
CPSTIC	Catálogo de Productos y Servicios de STIC.
DHCP	Dynamic Host Configuration Protocol
DTLS	Datagram Transport Layer Security
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ENS	Esquema Nacional de Seguridad.
ESN	Equipment Serial Number
HSB	Hot Standby
HTTPS	HyperText Transfer Protocol Secure
NTP	Network Time Protocol
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial-In User Service
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SSID	Service Set Identifier
SSH	Secure Shell
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
VLAN	Virtual Large Area Network
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access