centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1103

Procedimiento de Empleo Seguro
Aruba ClearPass 6.11

Diciembre de 2024

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-311-3.
Fecha de Edición: diciembre de 2024.

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.12.23 18:16:28 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. Aruba ClearPass es un producto del fabricante Aruba, de *Hewlett Packard Enterprise Company*. Ofrece **control de acceso a la red y orquestación de seguridad en redes de comunicaciones.**
2. El control de acceso a la red se realiza en base a roles para cualquier infraestructura cableada, inalámbrica y VPN, todo ello con equipamiento de red de múltiples proveedores, así como para todo tipo de usuario (corporativo, visitante, externos) y dispositivo (ofimático IT, doméstico, industrial, IoT y otros).
3. Aruba ClearPass, mediante un motor de políticas basado en contexto y soporte de los protocolos RADIUS y TACACS+, ofrece un amplio conjunto de soluciones para controlar y gobernar todos los aspectos de las conexiones y del acceso a la red: identificación y reconocimiento de los dispositivos conectados, perfilado de los dispositivos conectados, evaluación del estado de seguridad, recibir y procesar las credenciales de los terminales y usuarios y comunicar a los equipos las políticas de seguridad que deben aplicar a cada usuario y dispositivo.
4. Además de un motor de funciones AAA, es capaz de integrarse con el resto de elementos que ofrecen servicios de seguridad e identidad en la organización. Puede integrarse con cortafuegos, IDS, plataformas MDM, correladores de seguridad, bases de datos, directorios activos y LDAPs, proveedores de sistemas antivirus, todo ello de múltiples fabricantes.
5. Proporciona también mecanismos de comunicación con los usuarios, para automatizar la interacción con los mismos. Para ello, puede implementar portales de auto aprovisionamiento de dispositivos (soluciones BYOD).
6. Tiene la capacidad de integrarse con la infraestructura existente de PKI, para la generación subrogada de certificados de dispositivos.
7. También implementa un motor de portales cautivos, con los que se puede implementar portales de gestión de credenciales y acceso a red, tanto a usuarios externos como internos.
8. Para mejorar la interacción con los usuarios y administradores, también es capaz de enviar correos y mensajes SMS (mediante la integración con múltiples proveedores de mercado) en múltiples procesos y tareas, para notificar incidencias, credenciales y otros mensajes.

2. OBJETO Y ALCANCE

9. El presente documento tiene como objetivo detallar las configuraciones de seguridad del producto **Aruba ClearPass, versión 6.11**, de forma que la protección y funcionamiento del producto se realice de acuerdo a unas garantías mínimas de seguridad.
10. El producto Aruba ClearPass, versión 6.11 ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA en la familia Control de acceso a red (NAC), Servidores de Autenticación.
11. No puede ni pretende sustituir a la extensa documentación existente, pero sí desea ser un punto de referencia que recopila todos los aspectos sensibles de configuración y uso seguros del producto.
12. Esta guía, por tanto, no reemplaza a:
    a) La documentación oficial del producto.
    b) Los documentos *Release Notes*.
    c) La documentación formativa.
    d) Las pruebas de maqueta y preproducción.

3. ORGANIZACIÓN DEL DOCUMENTO

13. Este documento está organizado en diferentes capítulos, de acuerdo a diferentes fases del ciclo de vida del producto:

    a) Apartado **4.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e 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, para disponer un dispositivo configurado de forma segura. También se describen algunas facetas de configuración del servicio de ClearPass para proporcionar servicios de seguridad.

    d) Apartado **7.** En este apartado se recogen las tareas recomendadas para la fase de operación focalizándonos en la monitorización, exportación de registros.

    e) Apartado **8.** Se presenta un *checklist* de alto nivel para desplegar un clúster de servidores ClearPass de forma segura.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

14. Desde el punto de vista de licencias de producto, ClearPass consta de dos (2) elementos: las licencias de servidor (*appliance*) y las licencias de uso.

15. El servidor Aruba ClearPass puede ser virtual o físico. Los servidores físicos se entregan con el *software* ya instalado de fábrica. Se trata de un entorno cerrado donde el usuario no interactúa con el sistema operativo que lo soporta, sino con el interfaz de Aruba ClearPass.

16. En la modalidad de servidor virtual, se puede desplegar en un hipervisor en el propio centro de proceso de datos (CPD) o en un proveedor de nube pública. **Se destaca que el despliegue en un proveedor de nube pública debe ser analizado ya que podría ir en contra de las políticas de seguridad del organismo y la normativa aplicable.**

17. El servidor virtual se ofrece como una máquina virtual empaquetada (fichero OVF), que se descarga de forma segura y autenticada desde la página de soporte de Aruba [REF2]. Se soportan actualmente versiones *para ESXi VMware, Microsoft Hyper-V* y *Linux KVM.*

18. Para el acceso a la descarga son necesarias credenciales del portal de *Aruba Networks*. En la página de descarga se puede consultar el valor *hash* del fichero en formato SHA256, para verificar la integridad del fichero descargado.

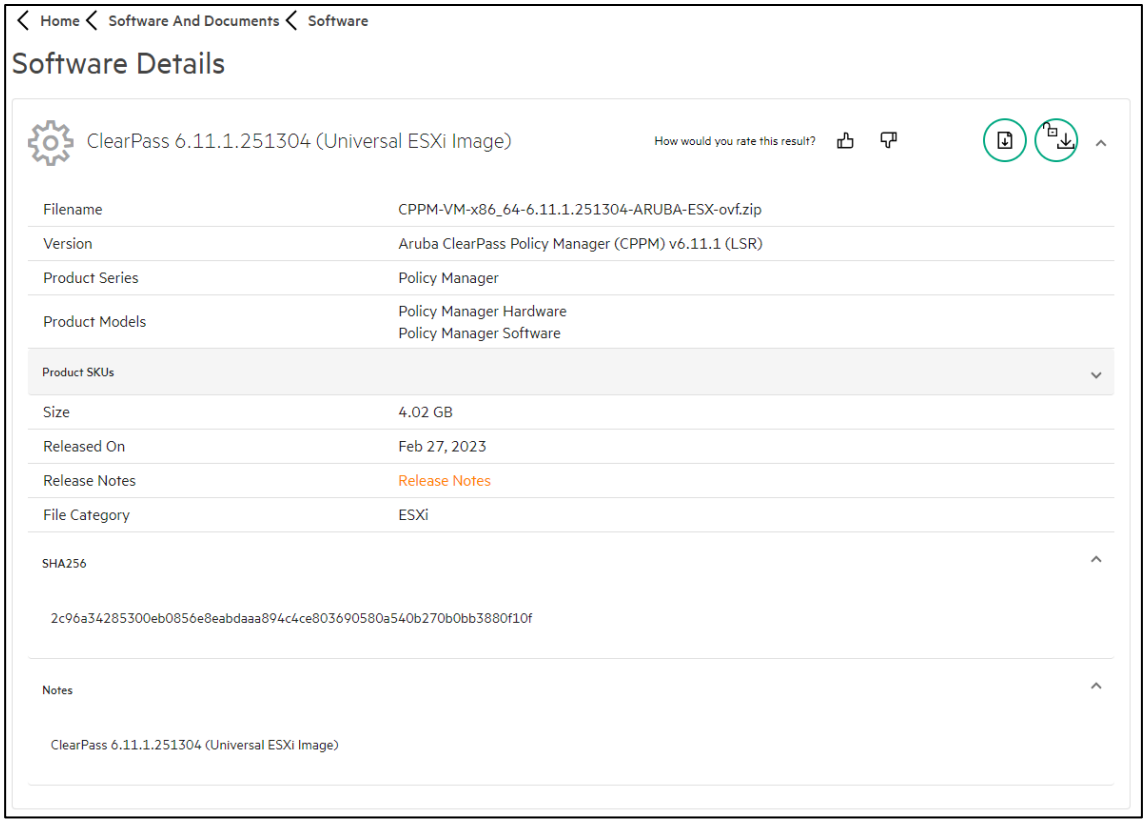


Ilustración 1. Valor *hash* de las imágenes descargables

19. Actualmente es posible ejecutar Aruba ClearPass en los proveedores de nube pública *Microsoft Azure* y *Amazon Web Services*. En el caso de *Azure*, la forma de instalación es

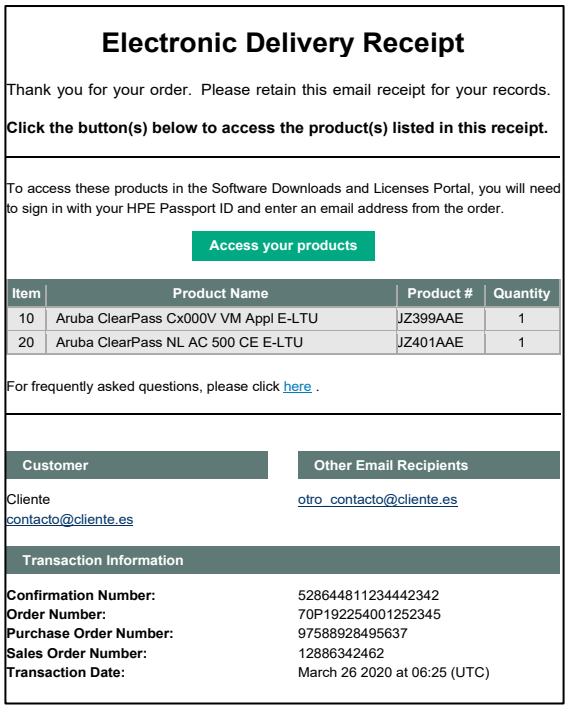
mediante el despliegue de una imagen preconfigurada. En Amazon Web Services, la instalación se realiza desde una AMI (Amazon Machine Image).

4.2 ENTORNO DE INSTALACIÓN SEGURO

20. La ubicación ideal para la instalación es en el CPD, en una ubicación lógica donde se puedan establecer las conexiones necesarias para el desarrollo de su funcionalidad.
21. Es importante tener en cuenta que el producto tiene que poder conectarse tanto a la electrónica de red como a diversos servidores y aplicativos. Por lo tanto, se debe dotar de una ubicación tanto física como lógica que pueda establecer estas conexiones.
22. Para la instalación de Aruba ClearPass únicamente es necesario conocer los datos de la máquina (nombre, FQDN y direccionamiento IP) así como establecer una credencial de administrador.
23. A posteriori, el administrador, podrá configurar el resto de aspectos de Aruba ClearPass, así como modificar los datos introducidos en este paso inicial.

4.3 REGISTRO Y LICENCIAS

24. Se describe a continuación el proceso de entrega y carga de licencias en el sistema.
25. Durante el proceso de adquisición de Aruba ClearPass, se proporciona un contacto en la organización que adquiere el producto. A este contacto, se le hacen llegar los datos y claves necesarias para poder generar las licencias.



Electronic Delivery Receipt

Thank you for your order. Please retain this email receipt for your records.

Click the button(s) below to access the product(s) listed in this receipt.

To access these products in the Software Downloads and Licenses Portal, you will need to sign in with your HPE Passport ID and enter an email address from the order.

Access your products

Item	Product Name	Product #	Quantity
10	Aruba ClearPass Cx000V VM Appl E-LTU	JZ399AAE	1
20	Aruba ClearPass NL AC 500 CE E-LTU	JZ401AAE	1

For frequently asked questions, please click here .

Customer	Other Email Recipients
Cliente contacto@cliente.es	otro_contacto@cliente.es

Transaction Information

Confirmation Number:	528644811234442342
Order Number:	70P192254001252345
Purchase Order Number:	97588928495637
Sales Order Number:	12886342462
Transaction Date:	March 26 2020 at 06:25 (UTC)

Ilustración 2. Ejemplo de correo electrónico con la entrega de las licencias de ClearPass.

26. Desde ese correo, se puede acceder pulsando *Access Your Products* directamente.
27. Se accede entonces a la plataforma de entrega de licencias y claves de producto. En ella, tras introducir diversas credenciales (entre ellas, contacto y número de pedido) se puede

acceder a la obtención de las correspondientes licencias. Se muestra a continuación, un ejemplo.

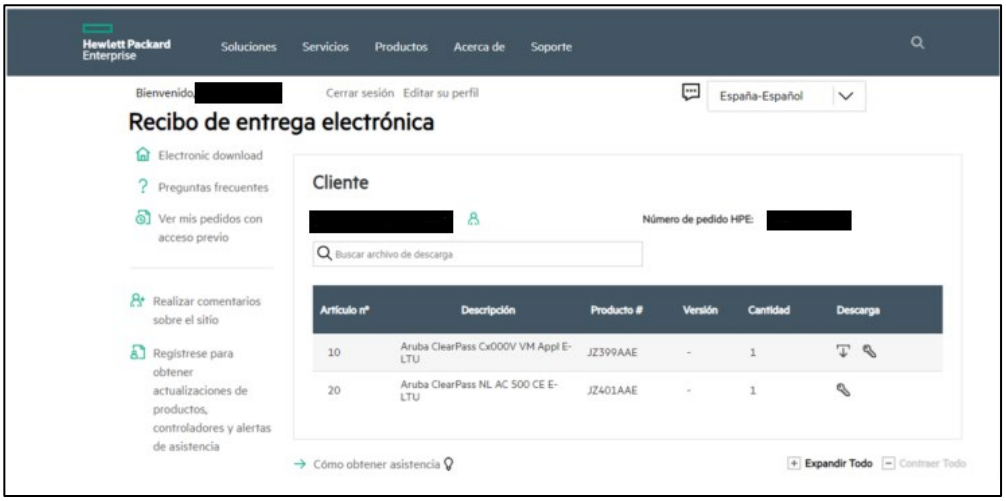


Ilustración 3. Captura de un ejemplo real de la web para obtener las claves de licencia.

28. Se procede a la activación de las diversas licencias. En el caso de que se trate de un *appliance* físico, la licencia de servidor ya viene incluida con el mismo. En el caso de un servidor virtual, esta debe generarse, haciendo clic en el botón situado bajo *Descarga*. El ejemplo anterior refleja un caso con una licencia de servidor.

29. Una vez que se dispone de las licencias, estas deben ser cargadas en el sistema, siguiendo los pasos definidos en la sección **5.1.3 CARGA DE LICENCIAS**.

4.4 CONSIDERACIONES PREVIAS

30. Aruba ClearPass para dar servicio y ofrecer todas sus funcionalidades puede conectarse a múltiples tipos de fuentes de información (servidores de identidad, elementos de seguridad, firewalls, bases de datos, MDM, correladores de eventos, antivirus). Por lo tanto, se requiere que el personal que gestione Aruba ClearPass sea personal adecuado y con las correspondientes autorizaciones para establecer estas asociaciones.

31. La ubicación idónea será el CPD cercano a segmentos de red seguros. A la hora de determinar la ubicación del ClearPass, se debe contemplar que este deberá comunicarse con los equipos de red, así como con diversos servidores (directorios identidad, bases de datos, plataformas SIEM, etc.).

32. En caso de que además se implemente algún tipo de servicio de portal, como, por ejemplo, portales de invitados o portales de auto aprovisionamiento, los usuarios deben poder llegar a este servicio. Por esto, en ocasiones es recomendable instalar un clúster de estos sistemas, dónde algunos de los elementos se ubiquen en una DMZ mientras que otros se ubiquen en redes seguras. Al pertenecer al mismo clúster, se garantiza la administración y operación conjunta, pero se segmentan las funcionalidades entre diversos servidores.

33. El control de acceso a la red se considera un servicio crítico por lo que el producto ofrece soluciones de alta disponibilidad mediante la implementación de clústers. Los clústers son agrupaciones de servidores de Aruba ClearPass (desde 2 hasta un total de 32), donde la capacidad de proceso se consolida y las licencias son compartidas por todo el clúster.

34. Dentro de los clústeres, se implementan los roles de *Publisher* y *Subscriber* desde el punto de vista de las bases de datos (ver apartado **5.3 CONSTITUCIÓN DEL CLÚSTER**).

35. Los clústeres deben ser constituidos por servidores del mismo tamaño y tecnología, como buena práctica. Tanto en físico como en virtual, se dispone de tres tipos *appliance*: C1000´s, C2000´s y C3000´s. Se puede consultar el apartado **5.1** para conocer las diferencias entre los *appliances*.

36. El despliegue más típico suele consistir en un clúster de dos (2) appliances de ClearPass, pero existen muchas instalaciones donde se hace uso de múltiples servidores.

37. Cuando el clúster alcanza un cierto tamaño (alrededor de 6-8 servidores) se recomienda dedicar un equipo a la función de *Publisher*. La configuración detallada del clúster se puede consultar en el apartado **5.3 CONSTITUCIÓN DEL CLÚSTER**.

38. Todos los aspectos relacionados con los clústeres y el diseño funcional de los mismos están descritos en detalle en el documento *ClearPass CPPM Tech Note Clustering Design Guidelines v1.2* [REF4].

4.4.1 DOBLE INTERFAZ DE RED

39. ClearPass ofrece una interfaz de puerto de datos y una interfaz de puerto de gestión. Se debe configurar el puerto de gestión, pero el puerto de datos es opcional.

40. Cuando ClearPass está configurado con una interfaz de administración, pero no con la interfaz de datos, todo el tráfico pasa por la interfaz de administración.

41. La configuración de ambas interfaces se realiza durante el despliegue del producto, en el proceso de instalación inicial. El detalle de dicha configuración se puede consultar en el apartado **5. FASE DE INSTALACIÓN**.

4.4.1.1 SELECCIÓN DE INTERFAZ

42. Cuando ClearPass está configurado con ambas interfaces, se deben tener en cuenta las siguientes pautas:

    a) Si la red/dirección de destino está en la subred de administración, ClearPass usa la interfaz de administración.

    b) Si la red/dirección de destino está en la subred de datos, ClearPass usa la interfaz de datos.

    c) Si la red de destino no está en las subredes de datos o de administración, ClearPass usa la interfaz de datos de manera predeterminada.

    d) Las autenticaciones RADIUS se pueden enviar a ambas interfaces. ClearPass responderá con la respuesta RADIUS en la interfaz donde se recibió inicialmente la solicitud.

    e) Los agentes OnGuard se comunican con ClearPass a través de la interfaz de datos si tanto la interfaz de administración como la de datos están configuradas.

4.4.1.2 COMUNICACIONES EN CLÚSTER

43. La dirección IP de administración del *Publisher* en un clúster debe ser accesible para todos los *Subscribers*. Sin embargo, los *Subscribers* pueden acceder a la IP de administración del

Publisher a través de la interfaz de administración del *Subscriber* o la interfaz de datos. El tráfico del clúster de ClearPass utiliza los siguientes puertos TCP / UDP:

a) Puerto UDP 123 NTP (*Subscriber* a *Publisher*).

b) Puerto TCP 443 HTTPS (bidireccional).

c) Puerto TCP 5432 *PostgreSQL* para replicación de base de datos (*Subscriber* a *Publisher*).

d) Puerto TCP 80 bidireccional: consultas de estado de cambio entre miembros del clúster ClearPass.

e) Puerto TCP 4231 *NetWatch* (módulo de autenticación posterior y el nodo donde está habilitado *Insight*).

f) Puerto TCP 6658 para que los agentes OnGuard se comunique con *ClearPass Policy Manager*. Como se mencionó anteriormente, si ambas interfaces están configuradas, el tráfico de OnGuard va a la interfaz de datos. Por lo tanto, si se han configurado ambas interfaces, este puerto debe abrirse en la interfaz de datos.

4.4.2 CONEXIÓN A INTERNET

44. ClearPass está diseñado para trabajar sin conexión a Internet. Si se dispone de conexión a Internet, las tareas de actualización pueden ser más sencillas, así como las de soporte remoto (ver apartado **6.8 ACTUALIZACIONES**).

5. FASE DE INSTALACIÓN

45. Se distinguen dos (2) procesos distintos de instalación, en función del tipo de servidor (instalación en *appliance* físico e instalación en servidor virtual). El detalle de la instalación del producto se puede consultar en la guía *ClearPass 6.11 Installation Guide* [REF3].

46. En la sección anterior se ha introducido el concepto de clústeres de servidores de ClearPass Policy Manager. Siempre que se instala un servidor, intrínsecamente se le hace partícipe de un clúster.

47. A posteriori, cuando se quiere constituir un clúster de dos (2) elementos, se ejecutará la acción de actualizar un servidor de *Publisher* a *Subscriber* (ver apartado **5.3 CONSTITUCIÓN DEL CLÚSTER**). Para ello será necesario que tengan conectividad entre ellos y se dispongan de las credenciales necesarias de ambos sistemas.

5.1 INSTALACIÓN DE ARUBA CLEARPASS EN APPLIANCE FISICOS

48. El detalle de la instalación del producto en *appliance* físicos se puede consultar en el apartado *Hardware Appliance Installation*, en la guía *ClearPass 6.11 Installation Guide* – [REF3].

49. Actualmente existen tres (3) tamaños de *appliance* físicos, que, a modo de orientación, escalan de la siguiente manera:

    a) Familia Aruba ClearPass C1000. Hasta 1000 sesiones concurrentes. Un disco de 1TB de almacenamiento (SATA) sin redundancia local.

    b) Familia Aruba ClearPass C2000, C2010 y C2020. Hasta 10.000 sesiones concurrentes. Dos discos de 1TB (SATA) en RAID-1.

    c) Familia Aruba ClearPass C3000 y C3010. Hasta 50.000 sesiones concurrentes. Ofrece seis discos de 600GB SCSI (SAS) y una controladora RAID-10 que presenta un disco virtual de 1.

50. Los appliances físicos de ClearPass vienen de fábrica con el aplicativo instalado. Por lo tanto, tras la instalación física, se procede a arrancar el sistema.

5.1.1 CONFIGURACIÓN INICIAL DEL APPLIANCE DE ARUBA CLEARPASS

51. En primer lugar, es necesario conectarse al puerto serie, con un emulador de consola (aplicación tipo *putty.exe* o equivalente).

52. Tras la conexión inicial, se solicitarán credenciales. De fábrica vienen las siguientes credenciales preconfiguradas:

    a) ***login***: *appadmin*

    b) ***password***: *eTIPS123*

53. La contraseña por defecto del usuario appadmin se modificará posteriormente durante la configuración inicial, ver párrafo **56**.

54. Tras la correcta introducción de las credenciales, comienza el dialogo de inicialización. En primer lugar, se solicitan los datos del servidor:

    a) *Enter hostname*: Proporcionar el nombre de máquina del dispositivo.

b) *Enter Management Port IP Address*: Proporcionar la dirección IP del puerto de gestión.

c) *Enter Management Port Subnet* Mask: Proporcionar la máscara de red del puerto de gestión.

d) *Enter Management Port Gateway*: Proporcionar el Gateway del puerto de gestión.

e) *Enter Data Port IP Address*: Proporcionar la dirección IP del puerto de datos.

f) *Enter Data Port Subnet Mask*: Proporcionar la máscara de red del puerto de datos.

g) Enter Data Port Gateway: Proporcionar el Gateway del puerto de datos.

h) *Enter Primary DNS*: Proporcionar el DNS principal.

i) *Enter Secondary DNS*: Proporcionar el DNS secundario.

55. A continuación, se pide la contraseña del clúster. Este paso fija una única contraseña, válida para dos (2) usuarios por defecto importantes:

    a) ***admin*** – Usuario de administrador de la plataforma para su uso como control de acceso. Este usuario se utilizará para la gestión mediante la GUI.

    b) ***appadmin*** – Usuario para las tareas administrativas y de mantenimiento del sistema. Este usuario se utilizará para la gestión mediante CLI/SSH.

56. A posteriori en este documento se especifica cómo cambiar de nuevo la contraseña del usuario *admin* (ver apartado **5.1.5 CAMBIO DE LA CONTRASEÑA DEL ADMINISTRADOR**). Se explica también como cambiar en cualquier momento la contraseña del usuario *appadmin* (ver apartado **5.3.1 CONTRASEÑA DEL CLÚSTER Y DE APPADMIN**).

57. El siguiente paso es configurar la hora y fecha del sistema. Seleccionar la zona horaria correspondiente. En nuestro caso, si se selecciona *Europe*, *Spain*, se preguntará la zona horaria correspondiente, a elegir entre:

    a) Spain (*mainland*).

    b) Ceuta, Melilla.

    c) *Canary Islands*.

58. También podemos especificar los servidores NTP para una correcta sincronización. Esto puede cambiarse a posteriori, para más detalle ver apartado **6.7 SINCRONIZACIÓN HORARIA**. Se recuerda que **el producto debe estar correctamente sincronizado, para disponer de una información y logs fiables**, así como para una mejor interacción con terceros sistemas.

59. El producto solicita la verificación de la información solicitada. Tras verificar y en su caso modificar la información introducida, se puede proceder a validarla. El sistema pasa a inicializar y configurarse en base a dicha información.

60. Tras esta fase, ya se puede conectar el sistema por red.

5.1.2 ACTIVACIÓN DE ARUBA CLEARPASS POLICY MANAGER

61. Para la activación es necesario conectarse mediante navegador web. Durante la primera conexión, Aruba ClearPass hará uso de un certificado autofirmado que se habrá generado automáticamente en el proceso de configuración.

62. Será por tanto necesario aceptar la excepción de conexión a un sistema con certificado autofirmado. **Este certificado debe modificarse posteriormente**. La configuración de los certificados del producto se detalla en el apartado **6.6 GESTIÓN DE CERTIFICADOS** del presente documento.
63. La conexión inicial al sistema se realiza a la página: *https://<ip_gestión>/tips/*
64. Anteriormente se mencionó que Aruba ClearPass tiene dos (2) tipos de licencias
    a) Licencias de Servidor.
    b) Licencias de Funcionalidades y características.
65. En el presente apartado se indica cómo activar las Licencias de Servidor. Para la activación de las Licencias de Funcionalidades y Características, se puede consultar el próximo apartado.
66. En el caso de los servidores físicos, la licencia de servidor ya viene instalada. Solo es necesario activarla.

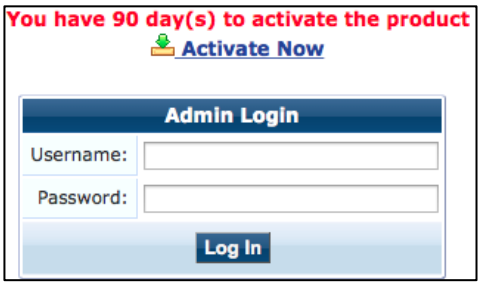


Ilustración 4. Notificación de licencia pendiente de activar

67. La activación supone la notificación expresa de que se hace uso de la licencia, y por tanto, se activan los mecanismos de soporte. Para activar la licencia es necesario hacer clic en *Activate Now*. Tras pulsar en activar, se ofrece el siguiente cuadro de diálogo.

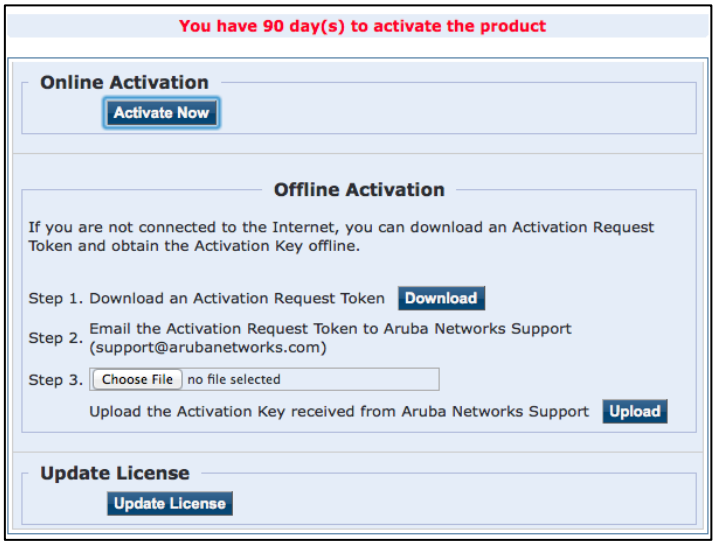


Ilustración 5. Activación del producto. Opciones disponibles

68. Si se dispone de conexión a Internet, se puede activar directamente haciendo clic en *Activate Now*. Se recibirá un mensaje similar a *"Product has been successfully activated"*.

69. En caso de que el sistema esté en una red sin conexión a internet, se pueden seguir los pasos que se describen a continuación:

    a) Descargar el *token* único del sistema. Para ello, hacer clic en *Download*, en la línea *Download an Activation Request Token* (ver Ilustración 5).

    b) Solicitar la activación del producto. Soporte devolverá una clave de activación.

    c) Cargar la clave de activación recibida y activar el producto.

70. Tras este paso, el sistema se encuentra instalado y listo para ser configurado y proporcionar servicio.

71. Para acceder al sistema es necesario ingresar las credenciales del usuario *admin*, antes definidas en el apartado **5.1.1 CONFIGURACIÓN INICIAL DEL APPLIANCE DE ARUBA CLEARPASS.**

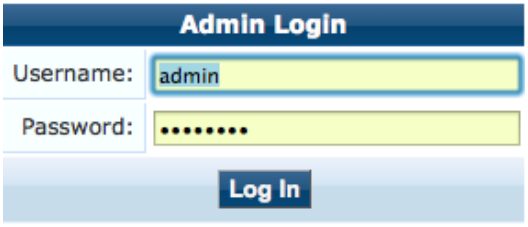


Ilustración 6. Acceso al sistema

72. Tras introducir las credenciales, se accede a la página inicial de ClearPass.

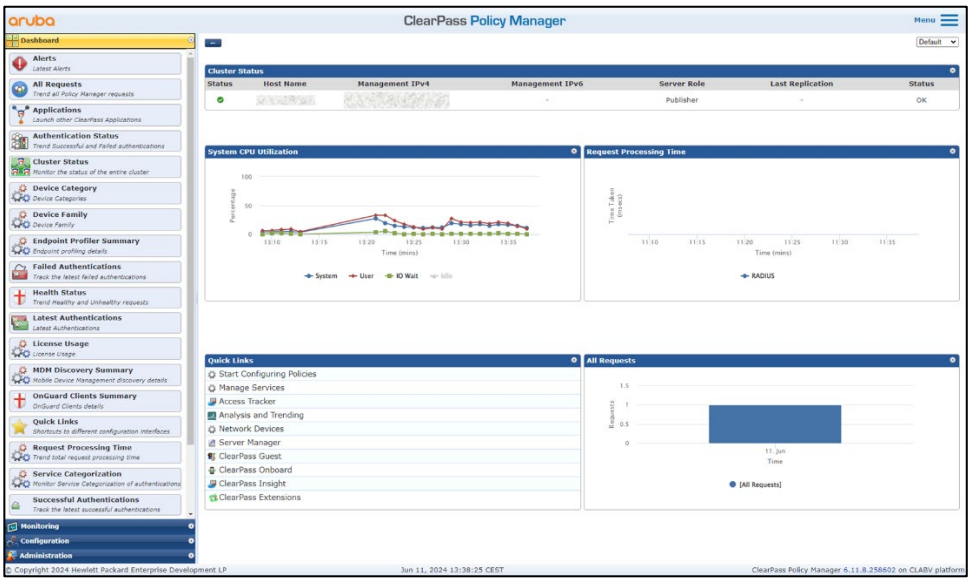


Ilustración 7. Panel inicial de ClearPass.

5.1.3 CARGA DE LICENCIAS

73. Para activar las licencias restantes (Licencias de Funcionalidades y Características), es necesario primero cargarlas en el producto. Para ello, se debe acceder a *Administration Server Manager > Licensing* y seguir los siguientes pasos:

    a) Hacer clic en *+Add License*. Se abrirá la siguiente ventana.

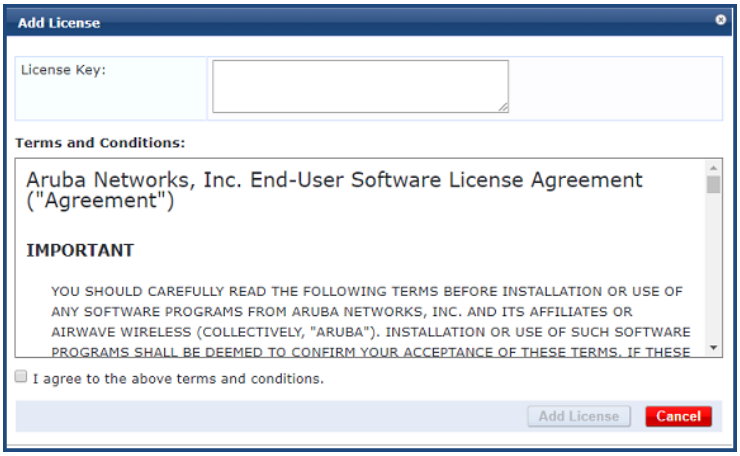


Ilustración 8. Ventana donde se introduce la licencia correspondiente.

b) Introducir la licencia en el cuadro *License Key*. Se deben aceptar los términos y condiciones tras su lectura y hacer clic en *Add License*.

5.1.4 ACTIVACIÓN DE LICENCIAS

74. Una vez que están cargadas las licencias de las diversas funcionalidades, queda pendiente su activación. La activación de las licencias se lleva a cabo desde *Administration > Server Manager > Licensing*. Cuando están pendientes de ser activadas, se visualiza de la siguiente manera.

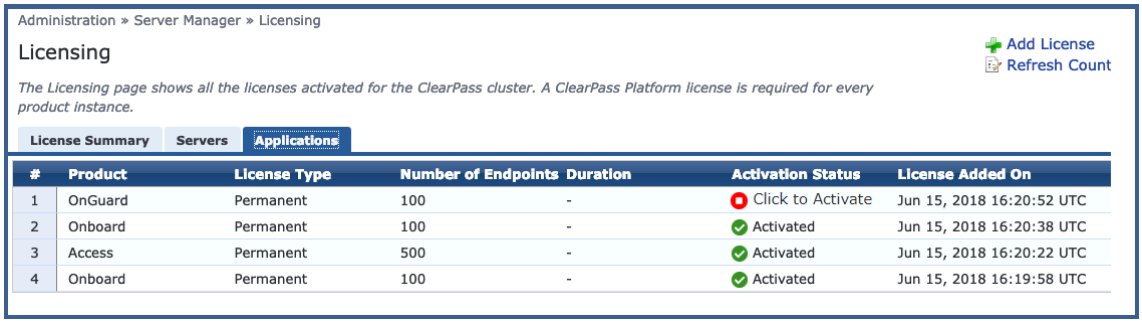


Ilustración 9. Panel con las licencias de aplicación: activas y por activar.

75. Para proceder a la activación, hacer clic en *Click to Activate*. Se abrirá la siguiente ventana de activación.

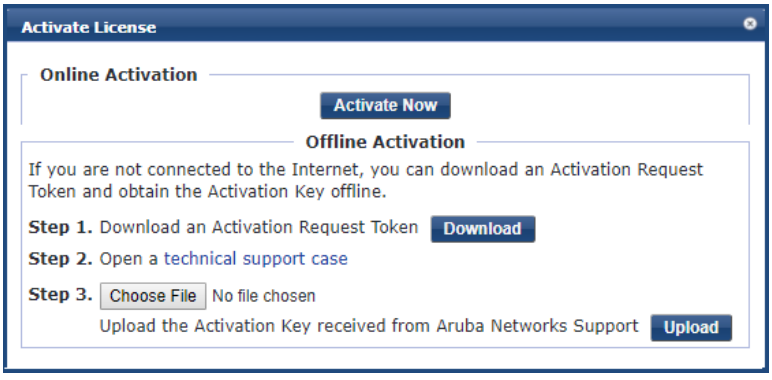


Ilustración 10. Opciones para la activación de la licencia.

76. Se puede proceder en modo *online* u *offline*, de forma similar a como se ha visto en el proceso de instalación anteriormente.

77. Una vez activadas se verán las licencias de la siguiente forma:

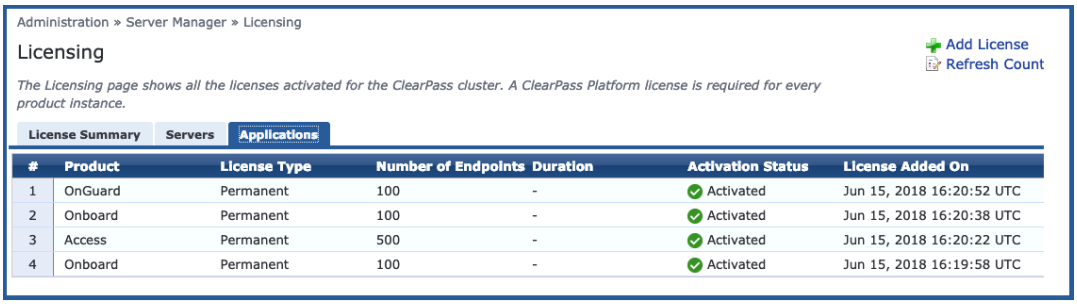


Ilustración 11. Panel con las licencias de aplicación. Todas activadas.

5.1.5 CAMBIO DE LA CONTRASEÑA DEL ADMINISTRADOR

78. Las credenciales del usuario **admin** y **apiadmin** pueden ser modificadas siguiendo los siguientes pasos:

- Ir a *Administration > Users and Privileges > Admin Users*.
- Seleccionar el usuario *Admin* o *apiadmin*. Se abrirá el diálogo *Edit Admin User*.
- Introducir la contraseña deseada y hacer clic en *Save*.

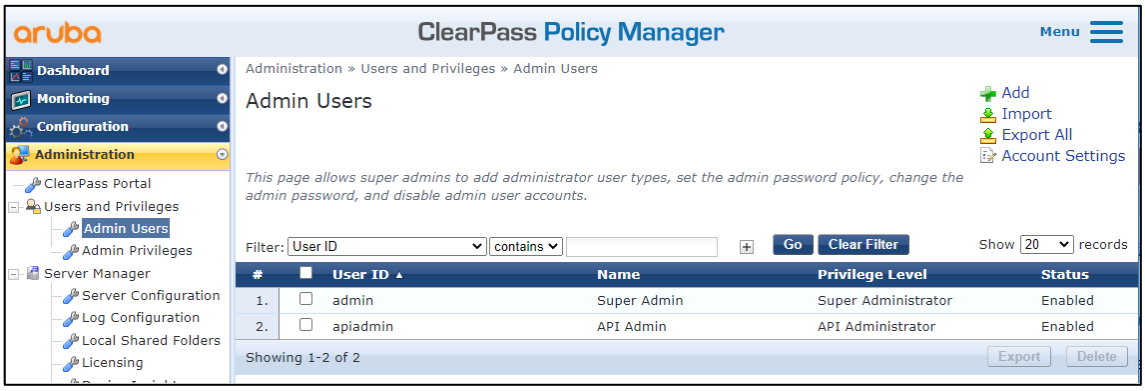


Ilustración 12. Panel de administración de usuarios administradores.

5.1.6 APAGADO SEGURO DEL EQUIPO

79. Se puede realizar un proceso de apagado seguro, mediante consola o mediante el interfaz gráfico.

80. En los accesos locales mediante consola (nunca utilizando SSH), sin necesidad de estar registrado en el sistema, es posible apagar el servidor ClearPass. Para ello simplemente es necesario introducirlas credenciales *poweroff/poweroff*:

    a) *login*: ***poweroff***

    b) *password*: ***poweroff***

81. También puede hacerse desde las tareas de mantenimiento, tras entrar en consola con el usuario ***appadmin***.

82. Asimismo, desde el interfaz gráfico también se puede apagar o resetear el servidor, entre otras opciones. Para ello, ir a *Administration > Server Manager > Server Configuration*. Desde dicha página se pueden realizar las siguientes actividades: recoger logs, hacer un *backup*, restaurar un *backup*, reiniciar un servidor o apagarlo.

5.2 INSTALACION DE ARUBA CLEARPASS EN APPLIANCES VIRTUALES

83. Para las instrucciones detalladas de la instalación en entornos virtuales, se debe consultar el apartado *Virtual Appliance Installation*, de la guía *ClearPass 6.11 Installation Guide* – [REF3].

84. En los tres casos posibles (ESXi VMware, Microsoft Hyper-V y Linux KVM), cuando se despliega la plantilla de máquina virtual en formato OVF, hay que añadir un disco virtual, cuyo tamaño dependerá del tipo de Virtual Appliance que se esté desplegando. El tamaño del disco se describe en las *Release Notes* de la versión, actualmente 6.9 [REF5] en la sección *Virtual Appliance Requirements*:

    a) C1000V: 1000GB.

    b) C2000V: 1000GB.

    c) C3000V: 1800GB.

85. La forma de añadirlo, tipo de disco y demás detalles, se encuentran detallados en las instrucciones mencionadas de la guía *ClearPass 6.11 Installation Guide* - [REF3].

86. A partir de este punto, se dispone de un *appliance* igual que un servidor físico y, por tanto, se procede a una instalación idéntica a un servidor físico.

87. Cuando se finaliza la instalación, a diferencia del servidor físico que ya la lleva instalada, se debe instalar la licencia del servidor. Para ello, se deben seguir los mismos pasos que para las Licencias de Funcionalidades, indicados en los apartados **5.1.3 CARGA DE LICENCIAS** y **5.1.4 ACTIVACIÓN DE LICENCIAS**.

88. Se notifica y aparece una ventana donde se podrá proporcionar la licencia.

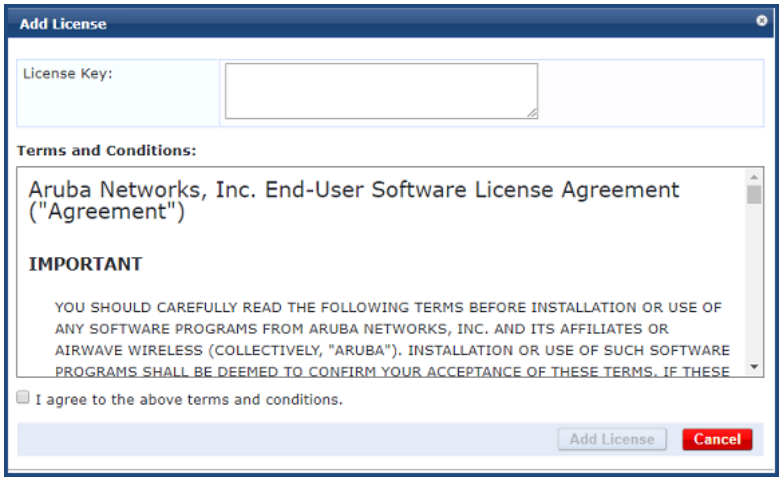


Ilustración 13. Ventana donde se introduce la licencia correspondiente

5.3 CONSTITUCIÓN DEL CLÚSTER

89. En el entorno de clúster de Aruba Policy Manager, el servidor *Publisher* actúa como servidor maestro. Un clúster de Policy Manager puede contener solo un *Publisher*. Las operaciones de administración, configuración y escritura de la base de datos solo pueden ocurrir en él.

90. Siempre que se instala un servidor de Aruba ClearPass Policy Manager se crea por defecto como un *Publisher*. Para cambiar el rol a *Subscriber* es necesario convertirlo y adjuntarlo a otro clúster existente. El clúster existente puede estar formado por un solo servidor o por varios.

91. Para adherir un servidor a otro como *Subscriber*, formando de esta manera un clúster, se deben seguir los siguientes pasos:

    - Desde el servidor que se quiere convertir en *Subscriber*, ir a la página *Administration > Server Manager > Server Configuration*. Se muestra la página de administración del servidor.
    - Se abre la página *Server Configuration*.

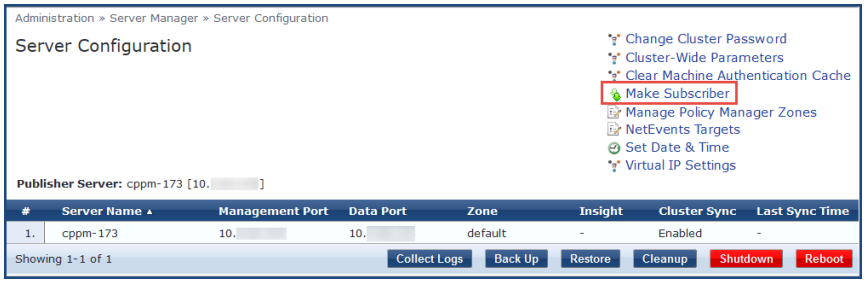


Ilustración 14. Conversión de un servidor ClearPass en *Subscriber*

    - Hacer clic sobre *Make Subscriber* (si el dispositivo ya es un *Subscriber*, el comando *Make Subscriber* no se muestra). Se abrirá la Ventana *Add Subscriber Node*:

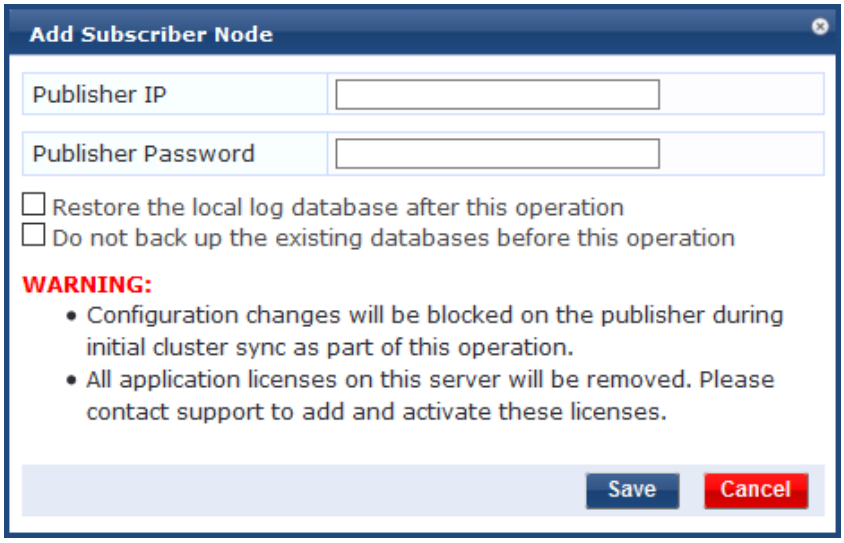


Ilustración 15. Datos para la conversión de un servidor ClearPass en *Subscriber*

    - Introducir la dirección IP del *Publisher* y la contraseña del *Publisher*. Esta contraseña es misma que la de ***appadmin*** configurada previamente.

92. Se recomienda que los clústeres se establezcan entre servidores del mismo tipo de tecnología y tamaño.

93. Desde la versión 6.8, se requiere mutua verificación de certificados. En casos excepcionales, puede evitarse esta verificación, si las circunstancias lo justifican. En la guía *Clustering Certificate Validations* - [REF6] se documenta este proceso en detalle. Sin embargo, por seguridad, se debe mantener la verificación mutua de certificados.

5.3.1 CONTRASEÑA DEL CLÚSTER Y DE APPADMIN

94. La contraseña de clúster es la misma que la contraseña de ***appadmin*** que se configuró en la instalación. Esta contraseña se puede modificar en cualquier momento siguiendo los pasos descritos a continuación. Esto modificará tanto la contraseña del cluster como la del usuario ***appadmin***.

95. Para ello, se puede acceder a *Administration > Server Manager > Server Configuration.*

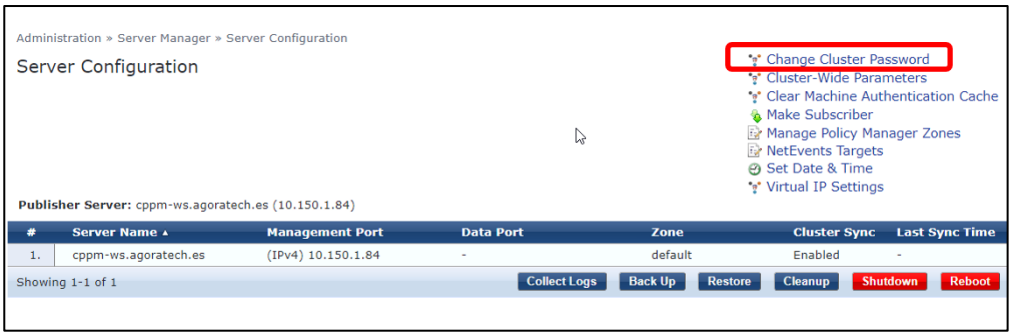


Ilustración 16. Acceso para cambiar la contraseña de todo el clúster

96. La ventana para el cambio de contraseña es la siguiente:

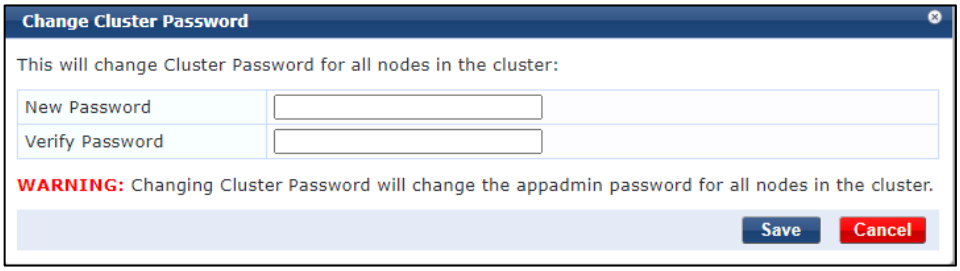


Ilustración 17. Cambio de la contraseña de todo el clúster.

97. Esta contraseña aplica a las operaciones de clúster.

5.3.2 PARÁMETROS DEL CLÚSTER

98. El comportamiento del conjunto del clúster se regula por los parámetros que aplican al clúster. Estos se configuran desde *Administration > Server Manager > Server Configuration.*

99. Hacer clic sobre *Cluster Wide Parameters.*

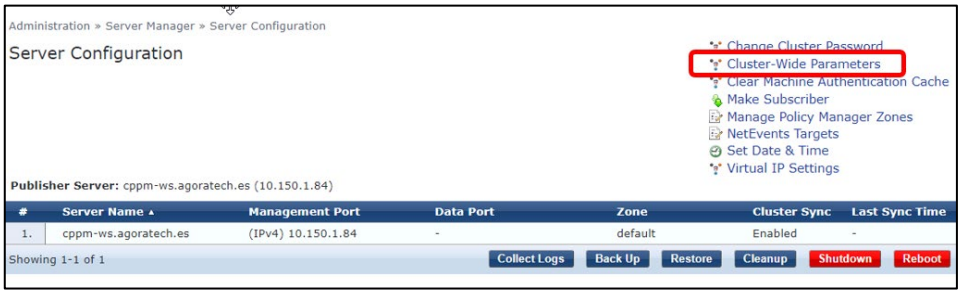


Ilustración 18. Acceso a los parámetros de configuración del clúster de ClearPass

100. Desde dicha página se pueden configurar los parámetros asociados al comportamiento global.

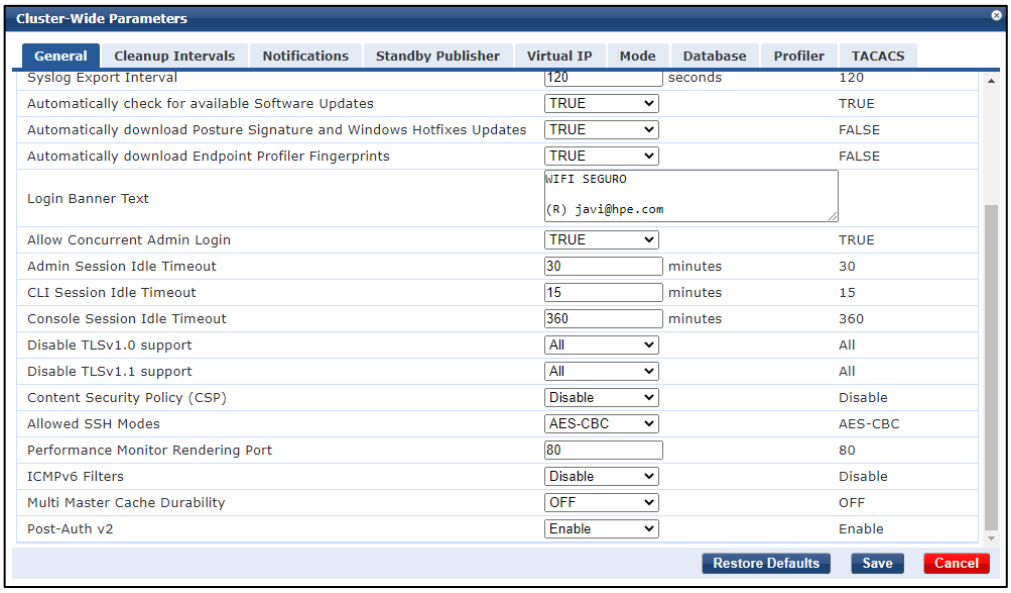


Ilustración 19. Ventana con los parámetros de configuración del clúster de ClearPass

5.3.3 TIPOS DE CLÚSTERES

101. Se pueden implementar dos (2) tipos de clústeres, de nivel 2 o de nivel 3:

a) Los clústeres de nivel 2 se forman cuando los servidores comparten una red virtual (VLAN) y forman parte de la misma red. En ellos se pueden definir IP virtuales que serán atendidas por dos servidores.

b) Los clústeres de nivel 3 se forman cuando los servidores que forman el clúster están conectados a redes diferentes. En este escenario no se pueden definir los interfaces IP virtuales en el clúster. Para repartir carga entre diferentes servicios mediante el uso de una sola dirección IP, será necesario utilizar algún mecanismo de reparto de carga externo (por ejemplo, un balanceador).

5.3.4 INTERFACES IP PARA EL CLÚSTER

102. Cuando se constituye un clúster es necesario proporcionar la forma de comunicarse con el resto de elementos, tanto con la electrónica de red como con terceras aplicaciones y usuarios.

103. Existen dos (2) mecanismos para implementar:

a) Balanceadores de Carga. Permiten la definición de servicios virtuales. Es importante considerar qué protocolos y servicios se van a implementar.

b) Uso de IP Virtuales. Funciona muy bien para clústeres de nivel 2. En los clústeres de nivel 3 puede usarse para los servidores que compartan segmento de nivel 2.

104. En el apartado **6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS** se comenta la configuración de puertos virtuales para los clústeres.

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

105. Aruba ClearPass soporta el **modo de trabajo FIPS**. En este modo todos los servicios criptográficos proporcionan una **fortaleza mínima de 128 bits**. Todos los servicios que proporcionan menos de 128 bits de seguridad (como por ejemplo RSA-1024, SHA1 para firmas digitales, MD5, DES) no deben ser utilizados dado que no proporcionan unas garantías mínimas de seguridad.

106. **Se debe configurar el modo FIPS en Aruba ClearPass** ya que imposibilita la configuración accidental o malintencionada de protocolos inseguros.

107. Es importante tener en cuenta estas consideraciones y restricciones:

    a) El servidor se reinicia cuando se habilita el modo FIPS.

    b) Cuando se activa el modo FIPS el servidor es expulsado del clúster actual.

    c) Todos los miembros de un clúster tienen que trabajar con el mismo modo de seguridad.

    d) Los certificados que han sido creados con autenticación MD5 no pueden ser importados en la lista de fuentes de confianza.

    e) Mecanismos tradicionales de autentificación, como *EAP-MD5* y *MD5 message digest,* no están soportados en modo FIPS.

    f) Cuando se produce un cambio de modo de trabajo la base de datos se restaura en su totalidad.

    g) Una copia de seguridad de la base de datos en modo FIPS puede ser restaurada en un ClearPass en modo no FIPS. Sin embargo, una copia de una base de datos en modo no FIPS no puede ser restaurada en una ClearPass en modo FIPS.

108. La configuración del modo FIPS se hace desde *Administration > Server Manager > Server Configuration >* Se selecciona servidor *> pestaña FIPS > Enable*.

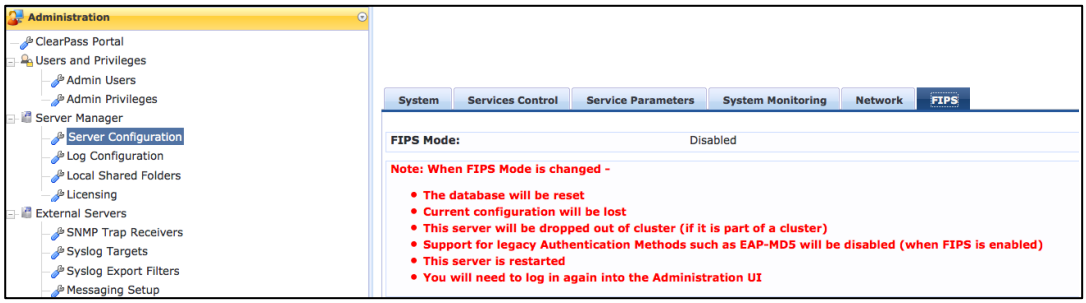


Ilustración 20. Activación de funcionalidad FIPS

6.1.1.1 *CIPHER SUITES* SOPORTADAS POR EL PRODUCTO

109. Se pueden consultar las *cipher suites* disponibles para los distintos protocolos utilizados por el producto (en modo FIPS y en modo no FIPS), en [REF9].

6.1.2 LISTA DE PUERTOS USADOS POR CLEARPASS

110. Debido a que ClearPass se puede comunicar con otros sistemas, este puede ser objeto de ataques externos. Se recomienda que sea protegido convenientemente a través de los servicios de un cortafuegos.

111. En el apartado **6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS** *s*e adjunta la tabla de puertos usados por ClearPass, junto con sus funciones asociadas.

6.2 AUTENTICACIÓN

6.2.1 METODOS Y FUENTES DE AUTENTICACIÓN

112. Al recibir una petición de autenticación, el producto determina contra qué servicio debe ser procesada y el método de autenticación que se utilizará.

113. Por cada servicio, se especifican los métodos de autenticación disponibles, del conjunto que tiene ClearPass configurado (ver apartado **6.14 CLEARPASS POLICY MANAGER**).

6.2.1.1 DEFINICIÓN MÉTODOS DE AUTENTICACIÓN

114. En ClearPass se soportan los siguientes métodos de autenticación:

    a) *Authorize Authentication Method.*
    b) *CHAP Authentication Method.*
    c) *EAP-FAST Authentication Method.*
    d) *EAP-GTC Authentication Method.*
    e) *EAP-MD5 Authentication Method.*
    f) *EAP-MSCHAPv2.*
    g) *EAP-PEAP Authentication Method.*
    h) *EAP-PEAP-Public.*
    i) *EAP-PWD.*
    j) *EAP-TLS.*
    k) *EAP-TTLS.*
    l) *MAC-AUTH Authentication Method.*
    m) *MSCHAP.*
    n) *PAP Authentication Method.*
    o) *TEAP Authentication Method*.

115. En *Configuration > Authentication > Methods* pueden editarse, o bien crearse nuevos.

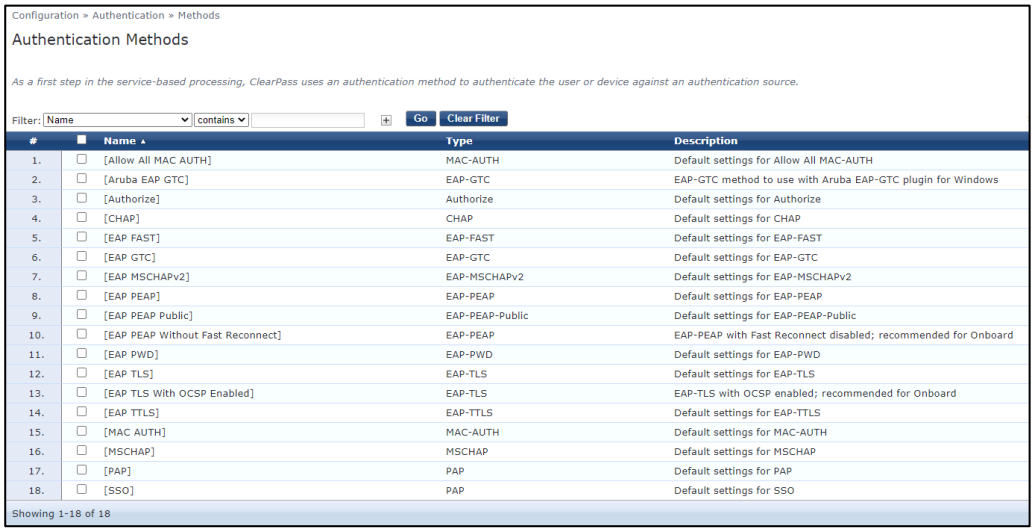


Ilustración 21. Métodos de Autenticación predefinidos.

116. Se recomienda, para mantener un punto de referencia, crear un método nuevo a partir del predefinido, dejando este como referencia. Por ejemplo, si se quiere cambiar el tiempo de sesión *timeout* de EAP-TLS, se puede crear otro método, a partir del predefinido, con este parámetro modificado. Así, por cada servicio, se puede elegir el método predefinido o el modificado.

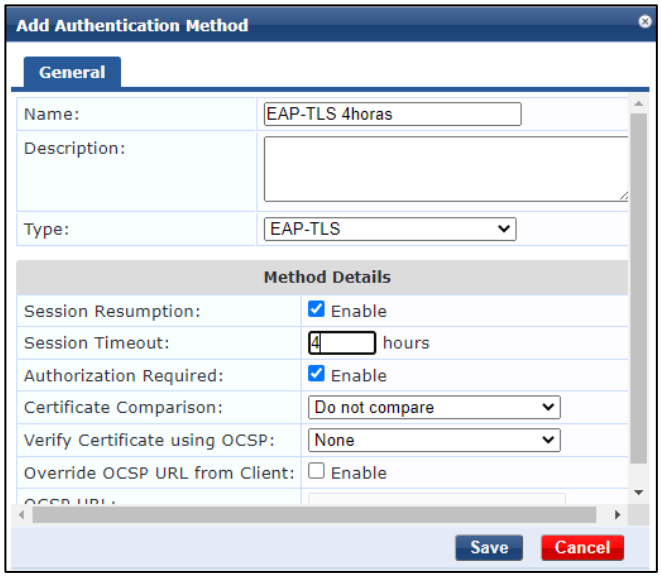


Ilustración 22. Ejemplo de definición de un nuevo método de autenticación.

6.2.1.2 FUENTES DE AUTENTICACIÓN

117. Las fuentes de autenticación son las diversas bases de datos que serán utilizadas para validar las peticiones de autenticación. Pueden ser predefinidas en ClearPass y también definidas por el usuario.

118. El objeto de estas fuentes es, por un lado, contrastar las credenciales, así como obtener información de los usuarios para la toma de decisiones.

119. Las fuentes de autenticación predefinidas en ClearPass son las siguientes:

a) [*Admin User Repository*]. Base de datos local de usuarios administradores.

b) [*Blacklist User Repository*]. Base de datos de usuarios bloqueados que han excedido el ancho de banda o los límites de sesiones.

c) [*Endpoints Repository*]. Base de datos de dispositivos. Esta base de datos permite filtrar las siguientes categorías:

1. Autenticación.
2. *Status*.
3. *Profile.*
4. *Fingerprint*.
5. *MAC Caching*.

d) [*Guest Device Repository*]. Base de datos de dispositivos definidos en el módulo ClearPass Guest.

e) [*Guest User Repository*]. Base de datos de invitados de ClearPass Guest.

f) [*Insight Repository*]. Base de datos del módulo de informes *ClearPassInsight* con información de usuarios y dispositivos.

g) [*Local User Repository*]. Base de datos de usuarios definidos en ClearPass.

h) [*Onboard Devices Repository*]. Base de datos de dispositivos auto provisionados, en el módulo Onboard de ClearPass.

i) [*Social Login Repository*]. Base de datos obtenida de la integración con redes sociales. Permite filtrar en base a autentificación e información social.

j) [*Time Source*]. Base de datos con registros basados en tiempo y fecha.

120. Además de estas bases de datos intrínsecas al sistema, el usuario puede definir fuentes de autenticación adicionales. Para ello, se puede acceder a *Configuration > Authentication > Sources,* hacer clic en *+Add* y seleccionar la deseada.

121. Las fuentes de datos externas pueden ser de estos tipos:

a) *Generic LDAP and Active Directory.*

b) *Generic SQL DB.*

c) *HTTP.*

d) *Kerberos.*

e) *Okta.*

f) *RADIUS/RadSec Server.*

g) *Static Host Lists.*

h) *Token Server.*

6.2.1.3 DEFINICIÓN DE UNA *ACTIVE DIRECTORY* COMO FUENTE DE AUTENTICACIÓN.

122. El producto puede integrarse con el servicio de Directorio Activo de Microsoft como fuente de autentificación. Esto resulta muy interesante no solo para validar las

credenciales, usuario y contraseña, sino para obtener información de contexto del usuario.

123. Para añadir una nueva fuente de datos de autenticación, se deben seguir los siguientes pasos:

a) Acceder a *Configuration > Authentication > Sources* y hacer clic en *+Add*.

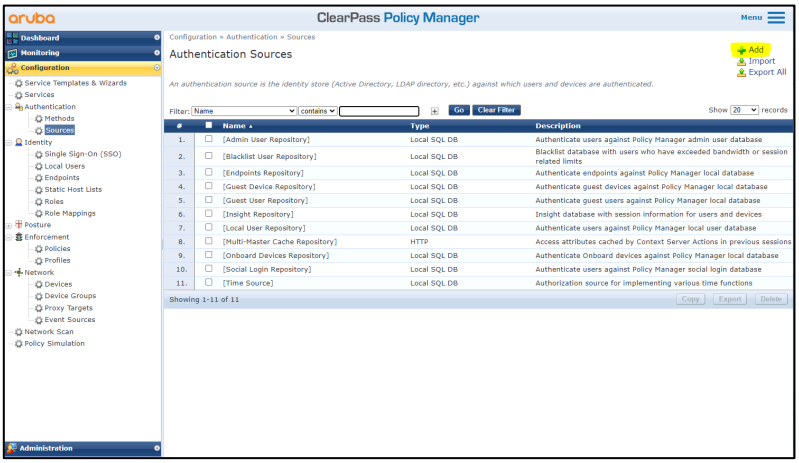


Ilustración 23. Añadir una nueva fuente de autenticación.

b) Elegir el nombre deseado y seleccionar el tipo *Active Directory*. Para otros tipos de fuentes de autenticación, se pueden seguir los mismos pasos indicados en el presente apartado y elegir el tipo correspondiente de fuente.

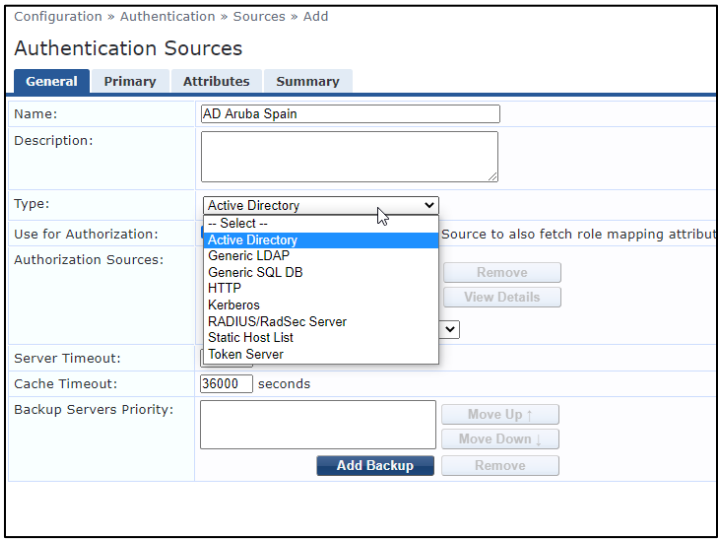


Ilustración 24. Ejemplo de una nueva fuente de autenticación de tipo Directorio Activo.

c) Hacer clic en *Next*. En la siguiente sección, *Primary*, se deben de completar los datos del servidor y la cuenta.

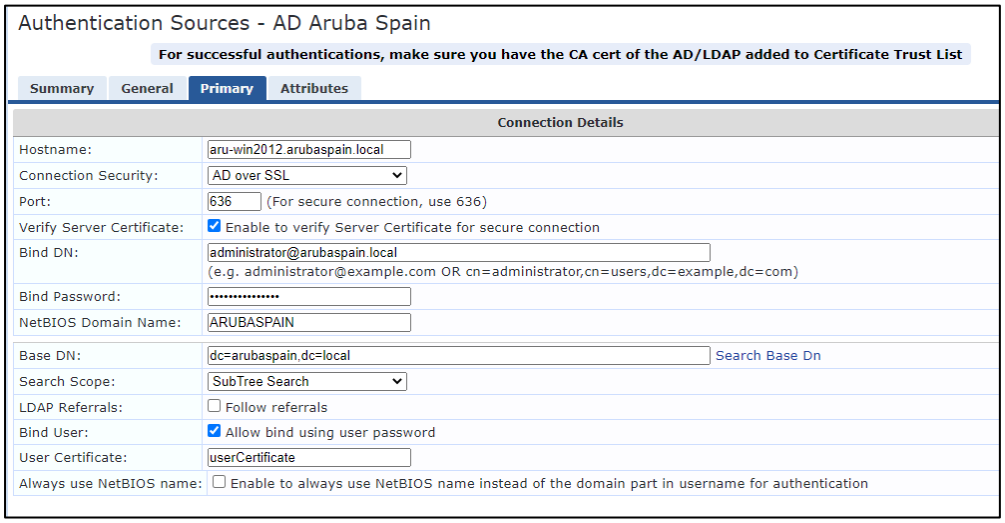


Ilustración 25. Ejemplo de parametrización de una fuente de autenticación de tipo Directorio Activo.

d) Se deben utilizar un canal cifrado en la conexión con el *Active Directory*, por lo que se debe seleccionar *AD over SSL*.

e) Se puede verificar la correcta conexión, pulsando en *Search Base Dn*, que permite seleccionar la rama correcta del Directorio.

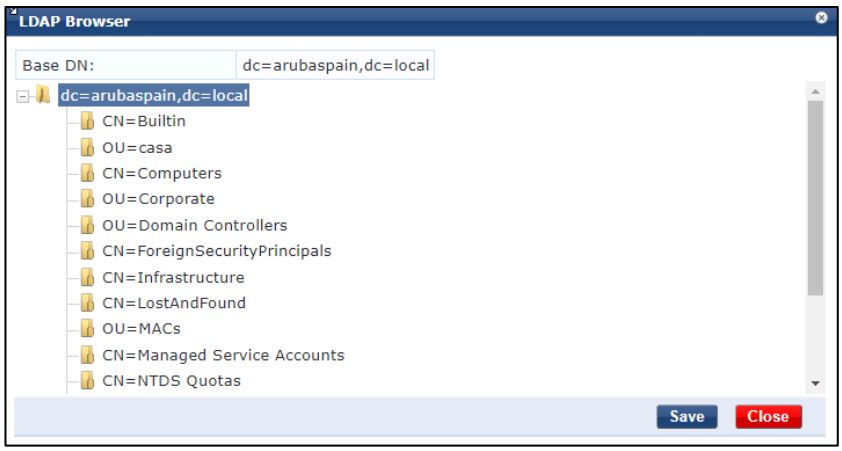


Ilustración 26. Verificación de la correcta conexión en la conexión de una fuente de autenticación de tipo Directorio Activo. Selección del Base DN.

f) En la sección de *Attributes* se valida o modifica la importación de atributos del directorio y su incorporación a ClearPass. Por defecto viene un mapeo preprogramado, pero se puede modificar y personalizar a demanda.

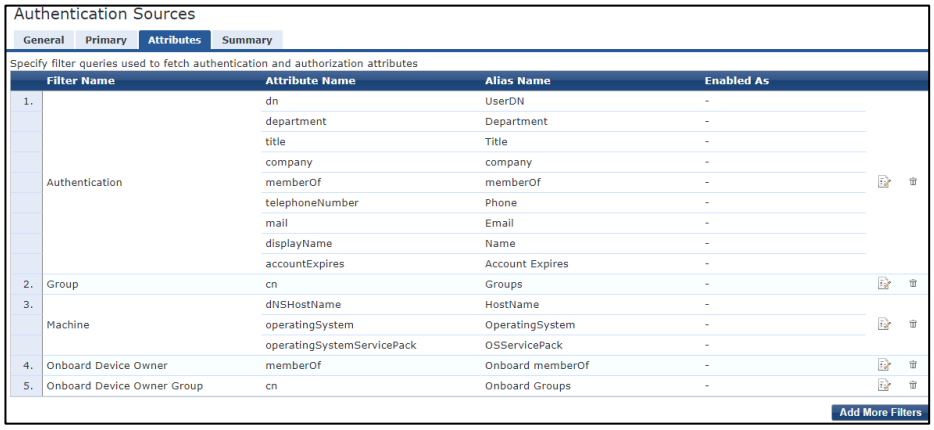


Ilustración 27. Atributos predefinidos en la definición de una fuente de autenticación de tipo Directorio Activo.

124. El detalle de la configuración de un Active Directory como fuente de autenticación de puede consular en la *Guía de usuario online de ClearPass Policy Manager* – [REF8].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

125. Los métodos para interactuar con la plataforma son los siguientes:

    a) CLI. Mediante SSH o mediante conexión al puerto serie (en caso de *appliance* físico).

    b) Interfaz gráfico vía HTTPS.

    c) API.

6.3.2 PROTECCIÓN DEL ACCESO REMOTO

126. Se deben implementar controles de acceso basados en grupos de permisos para todos los usuarios con cable e inalámbricos. En lugar de otorgar acceso único a la red, se debe otorgar el acceso apropiado para los permisos asociado a cada usuario. Por ejemplo, solo los administradores de ClearPass deben tener permisos asignados que permitan el acceso a la interfaz de administración de ClearPass. Ver apartado **6.3.4.1 CONFIGURACIÓN DE PERMISOS DE USUARIOS.**

127. Otro aspecto a considerar es limitar la posibilidad de que los usuarios finales puedan conectarse al interfaz de administración de ClearPass. Se recomienda que en el grupo de permisos que se asigna a los usuarios no se les permita acceso a la interfaz de administración, por prohibición explícita de ese destino de red.

6.3.3 USUARIOS PARA LA ADMINISTRACIÓN DE LA PLATAFORMA

128. ClearPass utiliza una serie de cuentas, creadas por defecto, para la administración de la plataforma. Para la creación de nuevos usuarios, se pueden seguir los siguientes pasos:

- Ir a *Administration > Users and Privileges > Admin Users.*
- Hacer clic en *Add*. Se abrirá una nueva ventana.
- Introducir el ID, nombre de usuario, contraseña y nivel de permisos deseados.

- Finalmente hacer clic en *Add*.

129. Los usuarios creados por defecto son los siguientes:

- Usuario ***admin***: Acceso completo a la GUI. También tiene acceso completo a la API de ClearPass. Se puede cambiar la contraseña del usuario *admin* en cualquier momento (ver apartado **5.1.4 ACTIVACIÓN DE LICENCIAS**).
- Usuario ***appadmin***: Acceso a la consola para ejecutar comandos CLI y actualizar los valores. **Se recuerda que la contraseña debe ser actualizada.** Para ello, consultar el apartado **5.3.1 CONTRASEÑA DEL CLÚSTER Y DE APPADMIN**.
- Usuario ***appexternal*:** Acceso de solo lectura a la base de datos "*tipsLogDb*" (eventos del sistema, registros de sesión, contabilidad RADIUS, alertas, etc.), base de datos "*insightdb*" (información que utiliza *Insight* para generar informes) y algunas tablas en la base de datos "*tipsdb*". La contraseña se puede cambiar desde *Cluster Wide Parameters*. Se recomienda hacer uso de la política de contraseñas expuesta en la sección **6.3.4.3 POLÍTICAS DE CONTRASEÑAS EN USUARIOS LOCALES**, ya que obligará el uso de contraseñas robustas en el usuario *appexternal* también.

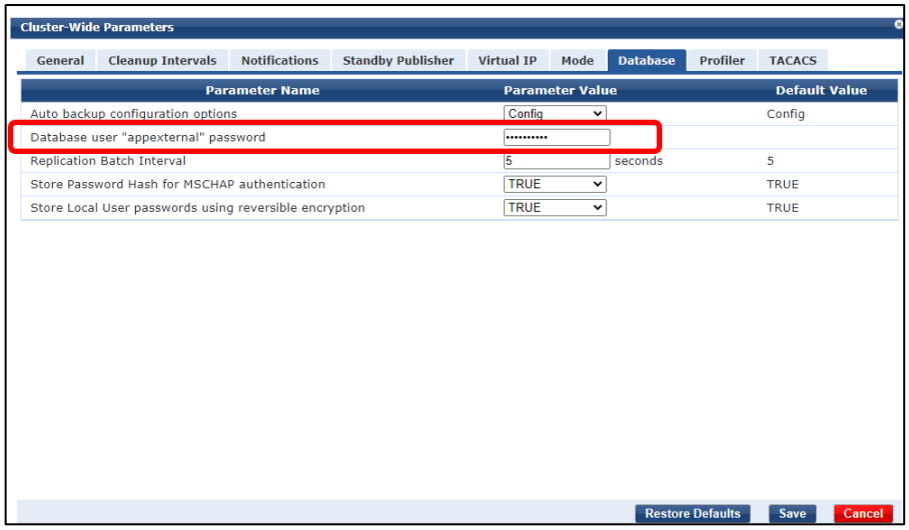


Ilustración 28. Cambio de la contraseña de la clave del usuario *appexternal*.

- Usuario ***apiadmin***: Acceso de lectura y escritura solo a las API. La contraseña de *apiadmin* debe cambiarse siguiendo pasos similares a los del usuario *admin* (ver apartado **5.1.5 CAMBIO DE LA CONTRASEÑA DEL ADMINISTRADOR**).

6.3.4 CONFIGURACIÓN DE ADMINISTRADORES

6.3.4.1 CONFIGURACIÓN DE PERMISOS DE USUARIOS

130. El producto proporciona tres (3) grupos de permisos de usuarios administradores de forma predeterminada:

a) Superadministrador (*Super Administrator*): permite el acceso de lectura y escritura a todos los elementos de configuración.

b) Administrador de API (*API Adm*inistrator): acceso de API permitido a todos los elementos de configuración.

c) Administrador de solo lectura (*Read-Only Administrator*): permite el acceso de solo lectura a todos los elementos de configuración.

131. Además, *Policy Manager* permite agregar los siguientes grupos de permisos de usuarios administradores:

a) Descarga de roles de usuario de Aruba (*Aruba User Role Download*): este grupo de permisos proporciona acceso solo para descargar roles de usuario. El grupo de permisos de Descarga de Roles, tiene relación con la capacidad que los equipos de red Aruba (cableado e inalámbrico) para descargar la definición de políticas de red. **Las políticas de usuario (VLAN, ACL, permisos, timers, y otros) son denominadas roles** (ver apartado **6.14.2.4 *ROLE MAPPING***). En cada dispositivo donde se implemente esta función, requiere disponer de un usuario con permisos para hacer descargas de dichas definiciones. Un dispositivo requerirá descargar esa definición cuando reciba una respuesta RADIUS donde se le indique que debe asignar un Role a un dispositivo y no disponga de la configuración del mismo.

b) Soporte (*HelpDesk*): permite que la mesa de ayuda inicie sesión para solucionar problemas informados por los usuarios finales.

c) Administrador de red (*Network admin*): autorizado para configurar todas las políticas de Policy Manager.

d) Operador (*Receptionist*): Autorizado para acceder a las principales pantallas de monitorización.

132. Los grupos de permisos anteriores están predefinidos. Para ver los permisos asignados, se puede acceder a *Administration > Users and Privileges > Admin Privileges*.

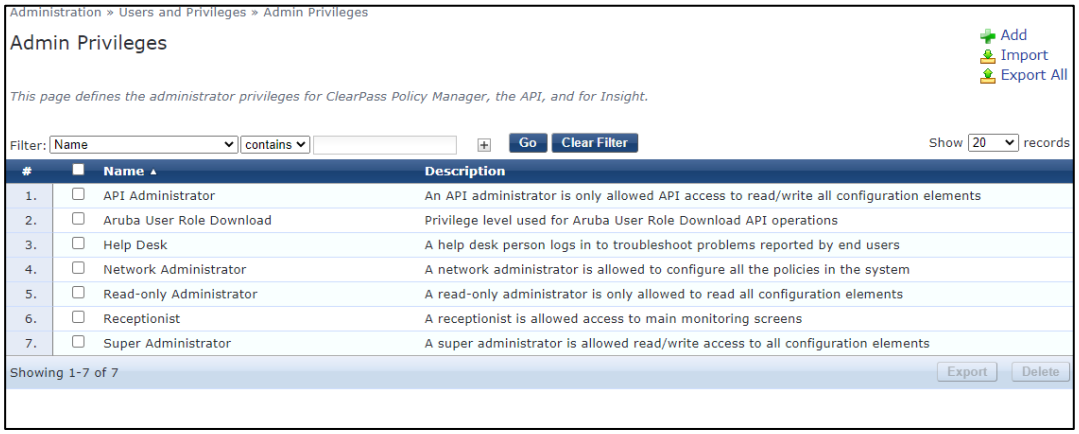


Ilustración 29. Permisos de administración predefinidos.

133. Se puede hacer clic en uno de los grupos de permisos, por ejemplo, *Recepcionist*, para ver los permisos asignados.

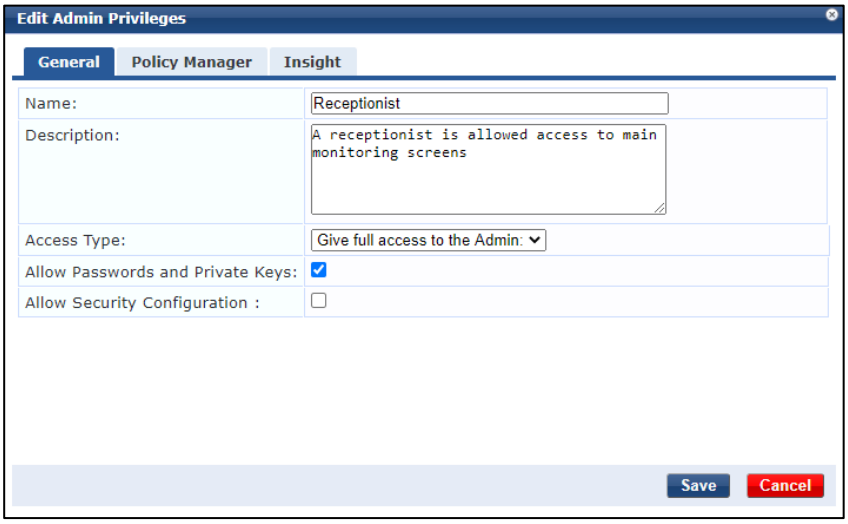


Ilustración 30. Ejemplo de permisos de administración para el grupo de permisos *Recepcionist*.

134. En *Access Type,* se puede determinar si tiene acceso completo a la API y GUI.

135. *Allow Passwords and Private Keys:* se selecciona esta casilla de verificación si se desea permitir el acceso con contraseña y controlar la capacidad de exportar parejas de claves desde *Policy Manager*.

136. *Allow Security Verification:* se selecciona esta casilla de verificación para permitir la configuración de seguridad. Para poder exportar el certificado de servidor y los certificados de servicio y cliente desde el almacén de certificados, se debe habilitar, tanto la opción "*Allow Passwords and Private Keys*", como la opción de "*Allow Security Configuration*". Los certificados de servicio son los que ClearPass ha generado para usuarios finales. Los certificados de servidor son los certificados propios de ClearPass.

137. En la pestaña *Policy Manager* se puede precisar/consultar el conjunto de acciones (permisos) que pueden realizarse en el módulo Policy Manager con dicho grupo de permisos.

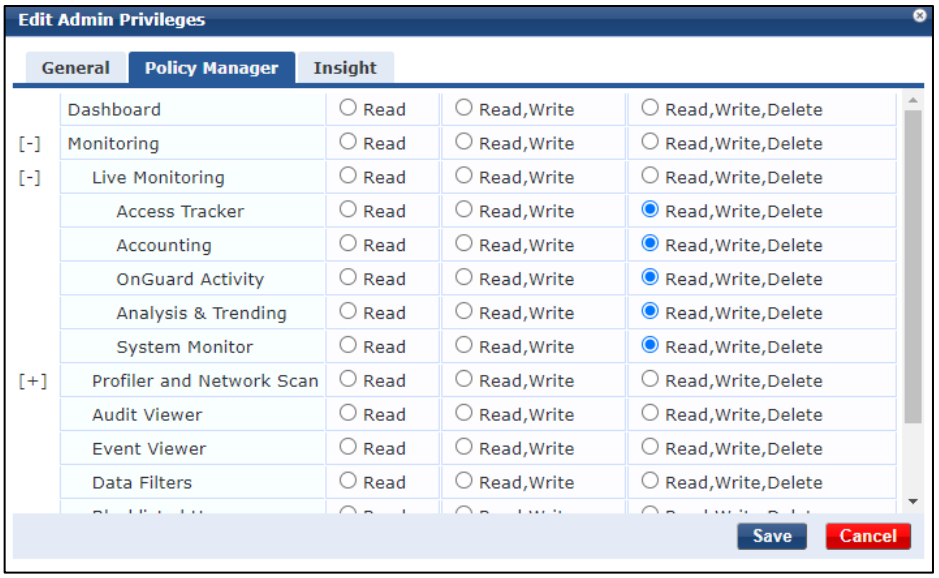


Ilustración 31. Acciones permitidas para el grupo de permisos *Recepcionist* en Policy Manager.

138. También se puede detallar el conjunto de permisos en el módulo *Insight*, desde la correspondiente pestaña.

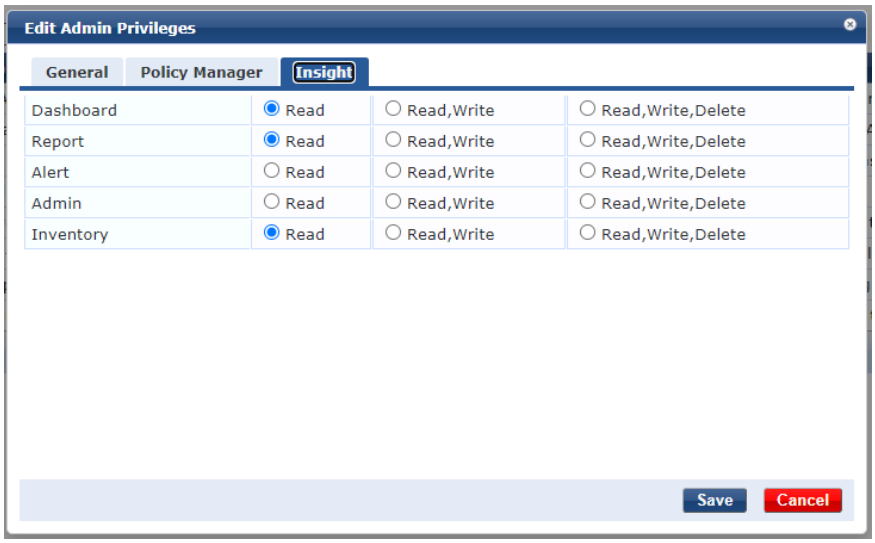


Ilustración 32. Acciones permitidas para el grupo de permisos Recepcionist en ClearPass Insight.

139. Finalmente, se pueden crear grupos de permisos personalizados. Para ello:

- Ir a Administration > Users and Privileges > Admin Privileges.
- Hacer clic sobre Add.
- Incluir el nombre de grupo deseado y configurar los parámetros en la pestaña Basic Information.
- En las pestañas Policy Manager y Insight configurar los distintos permisos de los que dispondrá el grupo.
- Finalmente hacer clic en Save.

6.3.4.2 POLÍTICAS DE CONTRASEÑAS DE ADMINISTRADOR

140. Desde *Administration > Users and Privileges > Admin Users* se puede configurar la política de contraseñas. Para ello hacer clic en *Account Settings.*

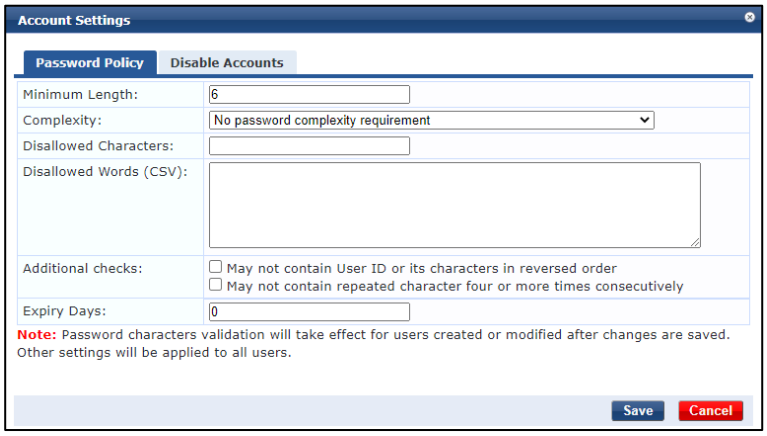


Ilustración 33. Ventana de configuración de contraseñas para administradores.

141. Los distintos parámetros que es posible configurar desde la pestaña *Password Policy* son:

- Longitud mínima de la contraseña. **Se debe configurar un valor de, al menos, 9 caracteres.**
- Complejidad de las contraseñas, cuyas opciones son:
    - Sin requisito de complejidad de contraseña.
    - Al menos una letra mayúscula y una minúscula.
    - Al menos un dígito.
    - Al menos una letra y un dígito.
    - Al menos uno de cada: letra mayúscula, letra minúscula, dígito.
    - Al menos un símbolo.
    - Al menos uno de cada: letra mayúscula, letra minúscula, dígito y símbolo.
- **Se deben configurar contraseñas que utilicen mayúsculas, minúsculas, dígitos y símbolos.**
- Caracteres y palabras prohibidas (*Disallowed characters* y *Disallowed words*). Se pueden prohibir ciertos caracteres y conjuntos de palabras.
- También puede impedirse que el *userID* forme parte de la contraseña, incluso en orden inverso y prevenir la repetición consecutiva de caracteres en las contraseñas. Dichas limitaciones deben ser aplicadas.
- Finalmente, el tiempo de expiración de las contraseñas (valor en días).

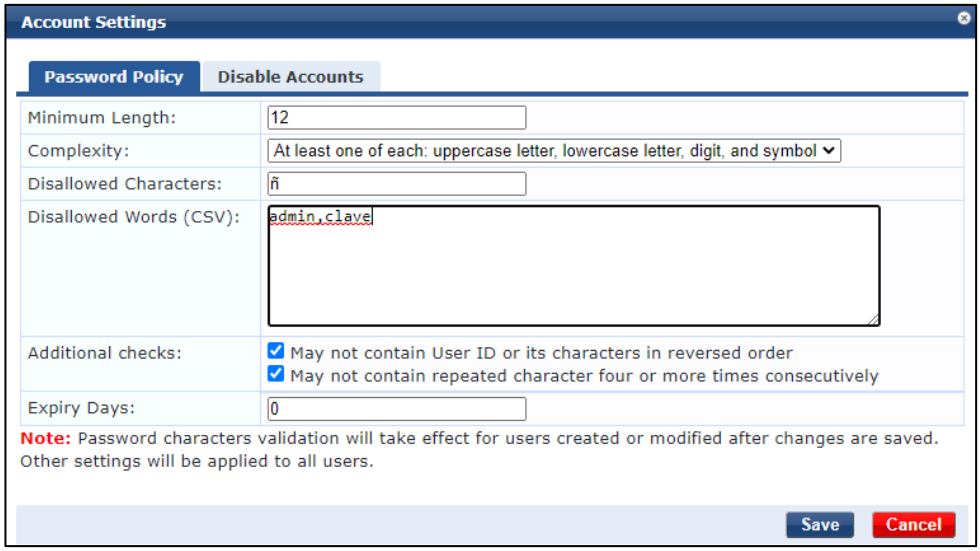


Ilustración 34. Configuración de unas claves de administrador.

- **La vigencia máxima de contraseñas no debe superar los 180 días.**
- También se puede configurar el número de veces consecutivas que se puede introducir erróneamente la contraseña antes del bloqueo de la cuenta, a través de la pestaña *Disable Accounts*.

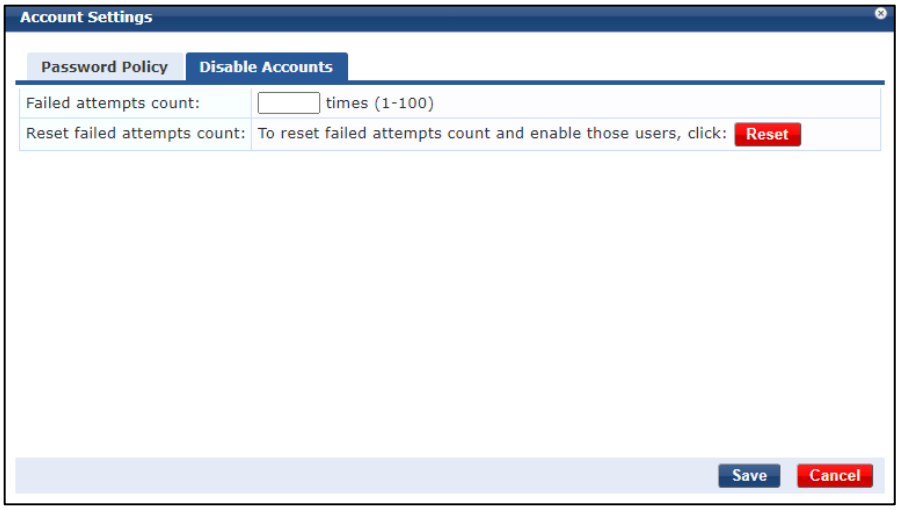


Ilustración 35. Mecanismo de desactivación de cuenta, tras sucesivos fallos.

- **El número de intentos permitidos no debe ser superar a 5.**

6.3.4.3 POLÍTICAS DE CONTRASEÑAS EN USUARIOS LOCALES

142. ClearPass dispone de una base de datos de usuarios locales. Esto se menciona de en el apartado **6.2.1 METODOS Y FUENTES DE AUTENTICACIÓN**.

143. Las políticas de contraseñas de los usuarios locales pueden ser configuradas en *Configuration > Identity > Local Users*, pulsando en *Account Settings.* Se pueden configurar los siguientes parámetros:

    - Longitud mínima de la contraseña. **Se debe configurar un valor de, al menos, 8 caracteres.**
    - Complejidad de las contraseñas, cuyas opciones son:
        - Sin requisito de complejidad de contraseña
        - Al menos una letra mayúscula y una minúscula
        - Al menos un dígito
        - Al menos una letra y un dígito
        - Al menos uno de cada: letra mayúscula, letra minúscula, dígito
        - Al menos un símbolo
        - Al menos uno de cada: letra mayúscula, letra minúscula, dígito y símbolo
    - **Se deben configurar contraseñas que utilicen mayúsculas, minúsculas, dígitos y símbolos.**
    - Caracteres y palabras prohibidas (*Disallowed characters* y *Disallowed words*). Se pueden prohibir ciertos caracteres y conjuntos de palabras.
    - También puede impedirse que el userID forme parte de la contraseña, incluso en orden inverso. Se puede prevenir también la repetición consecutiva de caracteres en las contraseñas. Dichas limitaciones deben ser aplicadas.
    - Puede configurarse el tiempo de expiración de las contraseñas, en días (*Expiry Days*). **La vigencia máxima de contraseñas no debe superar los 180 días.**
    - Se puede configurar el histórico de contraseñas, impidiendo que la contraseña creada sea igual a las anteriores. Se pueden recordar entre 1 y 99 contraseñas. **Se recomienda configurar para que se recuerden las últimas 5 contraseñas.**
    - Se puede añadir un recordatorio, hasta 365 días antes del cambio de contraseña.

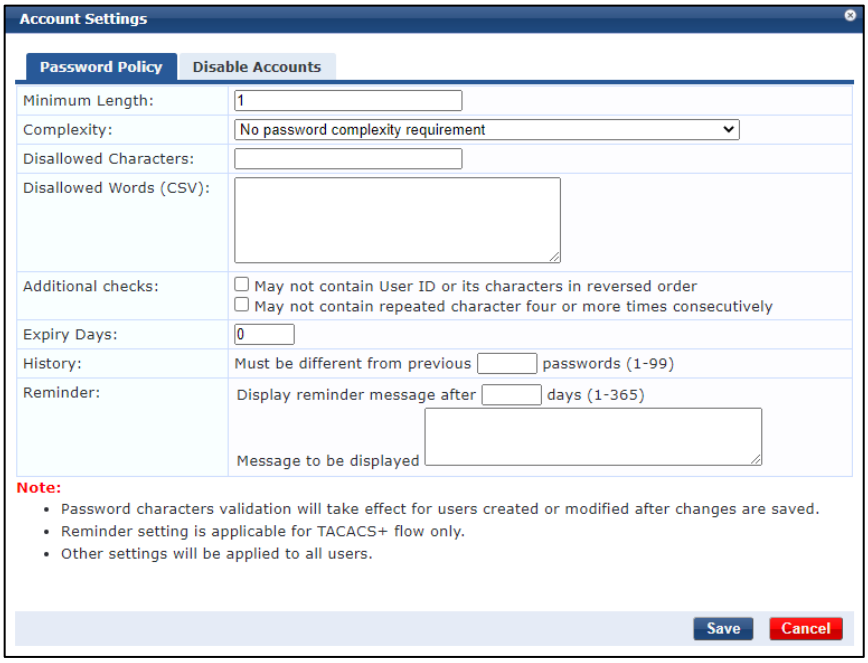


Ilustración 36. Ventana de política de contraseñas para usuarios finales.

144. Adicionalmente, en la pestaña *Disable Accounts* se puede configurar el número de veces consecutivas que se puede fallar el inicio de sesión antes del bloqueo de la cuenta. **El número de intentos fallidos no debe ser superior a 5.**

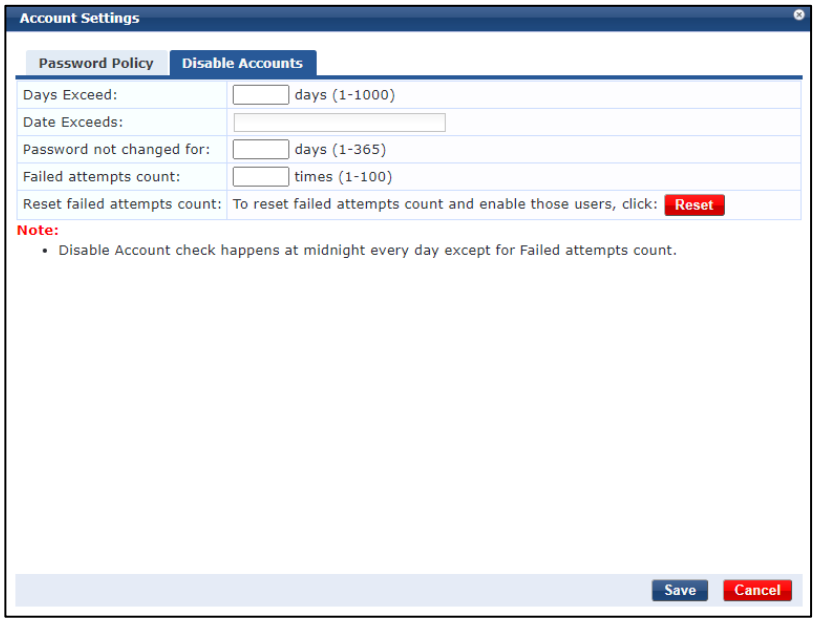


Ilustración 37. Parámetros de expiración e intentos fallidos para los usuarios finales

6.3.4.4 LOGIN DE ADMINISTRADORES BASADO EN CERTIFICADO

145. ClearPass admite el inicio de sesión con tarjeta inteligente y certificado TLS para todas las aplicaciones:

    a) El certificado puede provenir de una tarjeta inteligente o un almacén de certificados.

b) El certificado puede ser obligatorio u opcional.

c) El certificado puede ser adicional al nombre de usuario / contraseña o independiente.

146. Cuando el usuario intente iniciar sesión en la aplicación ClearPass, se le pedirá que seleccione un certificado, desde la pantalla de inicio de sesión.

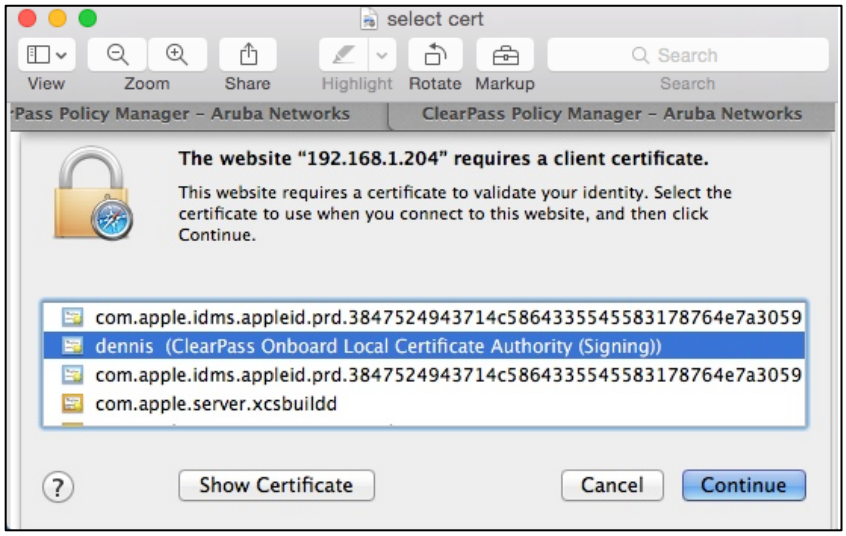


Ilustración 38. Ejemplo de acceso a ClearPass con solicitud de certificado

147. **Se debe, en la medida de lo posible habilitar el doble factor de autenticación**. Para ello, se puede configurar desde un asistente en ClearPass. Desde *Configuration > Service Templates & Wizards* se selecciona el asistente denominado *Certificate/Two-Factor Authentication for ClearPass Application Login*. Se abrirá la siguiente pestaña, donde se deberá rellenar la información requerida:

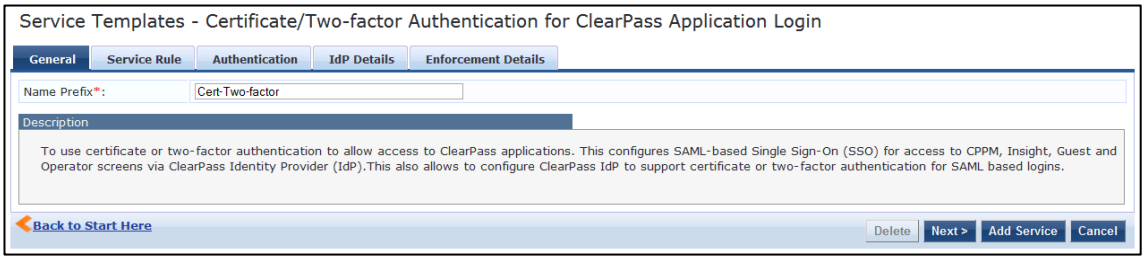


Ilustración 39. Asistente para la configuración de autenticación de doble factor.

148. El detalle sobre la configuración de la autenticación de doble factor se puede consultar en la documentación on-line [REF10].

6.3.4.5 SEGURIDAD AVANZADA PARA CUENTAS DE USUARIO ADMINISTRADORES Y LOCALES

6.3.4.5.1 ALMACENAMIENTO DE HASH PARA CONTRASEÑAS DE CUENTAS DE ADMIN Y LOCALES

149. Las contraseñas de administrador y de usuario local se almacenan, de forma predeterminada, en hashes de contraseña basados en SHA1. Este valor no es configurable.

150. Se proporciona un parámetro global para almacenar opcionalmente también el hash NTLM de la contraseña. Esto es necesario para las autenticaciones basadas en MSCHAPv2 contra la base de datos local. Los campos de contraseña de usuario invitado en la base de datos se cifran individualmente y la base de datos en sí se almacena cifrada.

6.3.4.5.2 *TIMEOUT* DE SESIONES

151. Hay parámetros globales que controlan los tiempos de expiración de las sesiones. Para su configuración, se accede a *Administration > Server Manager > Server Configuration* y seleccionar *Cluster-Wide Parameters*. Desde la pestaña *General* se pueden configurar los siguientes parámetros:

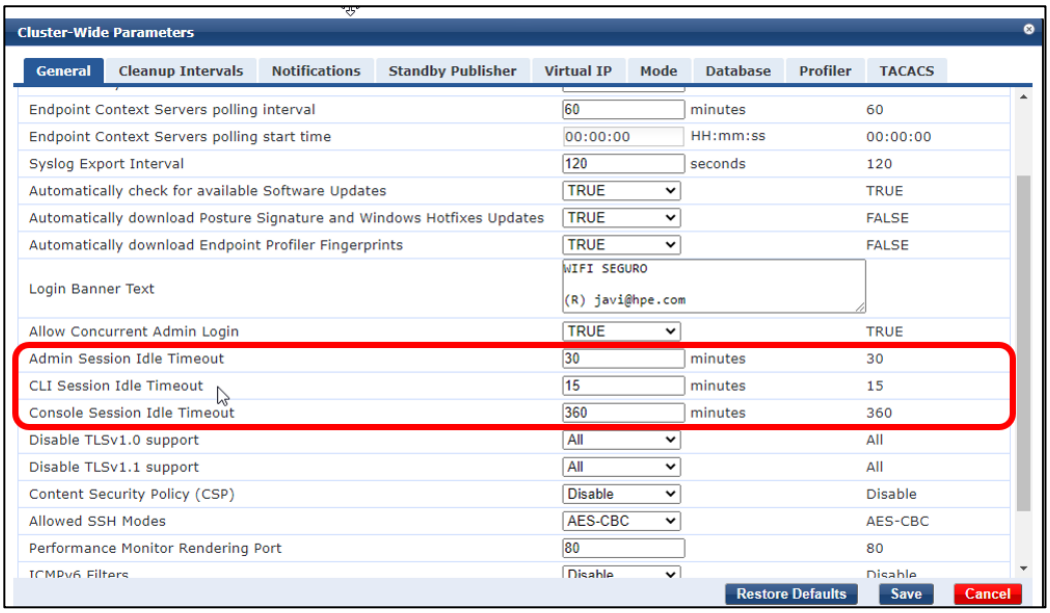


Ilustración 40. Configuración de los *timeouts* de sesión

152. ***Admin Session Timeout***: permite a los administradores configurar el tiempo de inactividad máximo permitido para el acceso de administrador. Este límite se aplica a *Policy Manager*, *Guest* e *Insight*. El valor predeterminado es 30 minutos. Se debe utilizar un valor de tiempo lo más bajo posible.

153. Hay varias pantallas de supervisión en la interfaz de usuario del administrador (panel, rastreador de acceso, actividad de *OnGuard*, etc.) con la actualización automática habilitada de forma predeterminada. Si hay actividad constante en estas pantallas, la sesión de la interfaz de usuario nunca terminará, por lo que los administradores deben tener cuidado de dejar el navegador abierto en estas pantallas o deshabilitar la "Actualización automática", cuando corresponda. La actualización automática se activa o desactiva, en las pantallas que lo ofrecen, pulsando en *Auto Refresh* como se muestra a continuación.

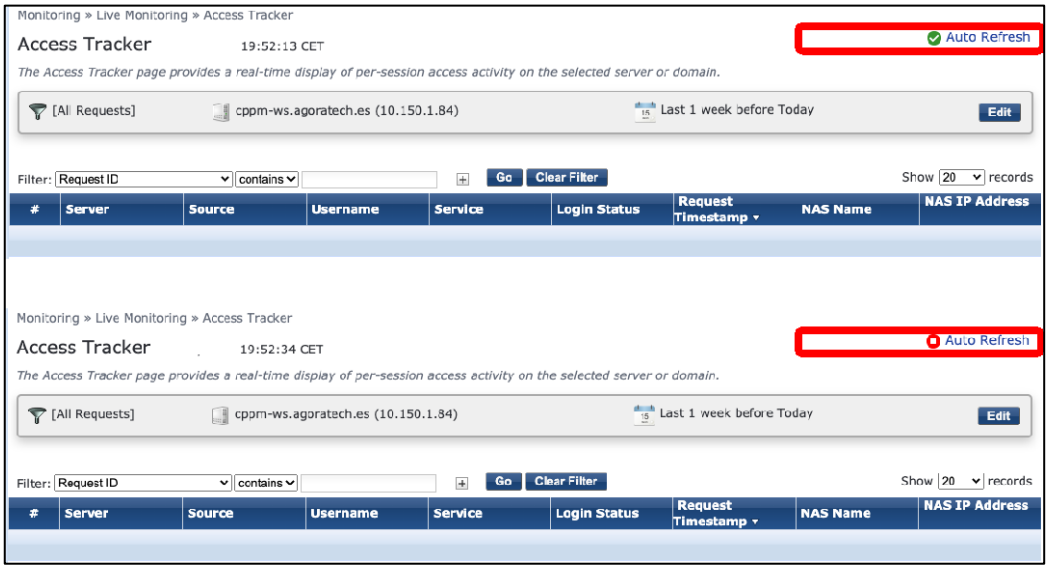


Ilustración 41 Ejemplo de *Auto Refresh* activado o desactivado

154. ***CLI Session Timeout (SSH):*** permite a los administradores controlar cuánto tiempo puede estar inactiva una sesión CLI antes de que finalice automáticamente. Si se cambia este parámetro, los cambios entrarán en vigor cuando el cliente abra una nueva sesión de CLI. Todas las sesiones de CLI activas seguirán utilizando el tiempo de espera anterior o deberán desconectarse y volverse a conectar para que los nuevos cambios surtan efecto.

155. ***Console Session Timeout:*** permite a los administradores controlar cuánto tiempo puede estar inactiva una sesión de consola antes de que finalice automáticamente.

156. Dado que los procesos en segundo plano no se cuentan como parte de una sesión activa, establecer un valor de tiempo de espera de la consola bajo puede provocar el cierre de sesión automático durante la actualización del sistema.

6.3.4.5.3 HABILITAR *PUBLIC KEY AUTHENTICATION*

157. ClearPass admite inicios de sesión SSH basados en claves públicas por dispositivo. Se puede configurar en *Administration > Server Manager > Server Configuration > Network*. Hacer clic en *Add Public Key* e introducir la clave deseada.

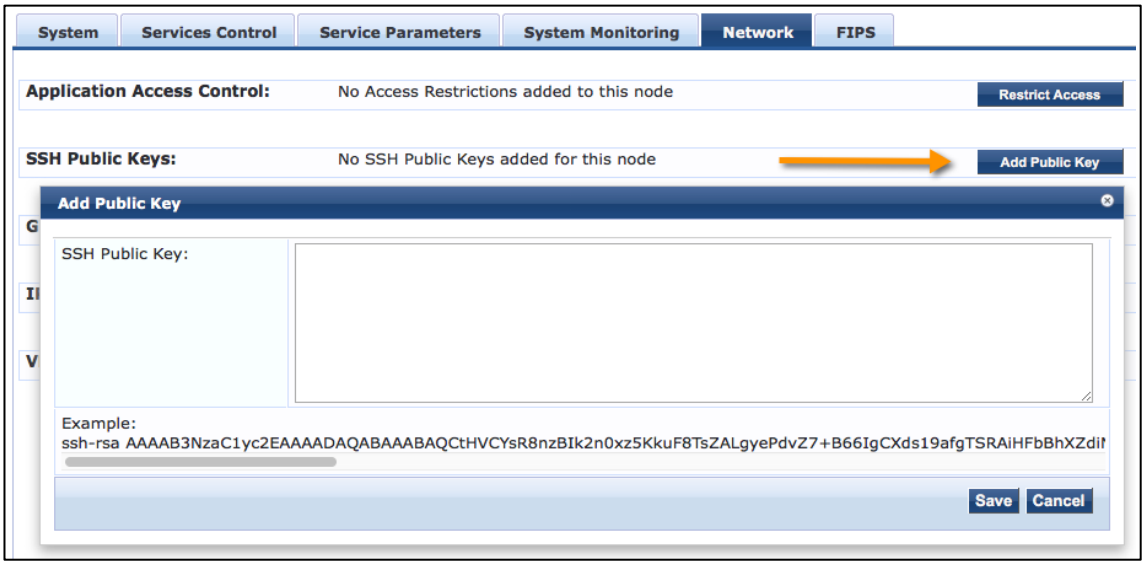


Ilustración 42. Configuración de claves públicas de SSH

6.3.4.6 *BANNER*

158. **Se debe configurar un banner de inicio de sesión**. Para ello, se puede acceder a *Administration > Server Manager > Server Configuration* y hacer clic en *Cluster Wide Parameters.* En el parámetro *Login Banner Text,* se introduce el texto deseado para el banner de inicio de sesión.

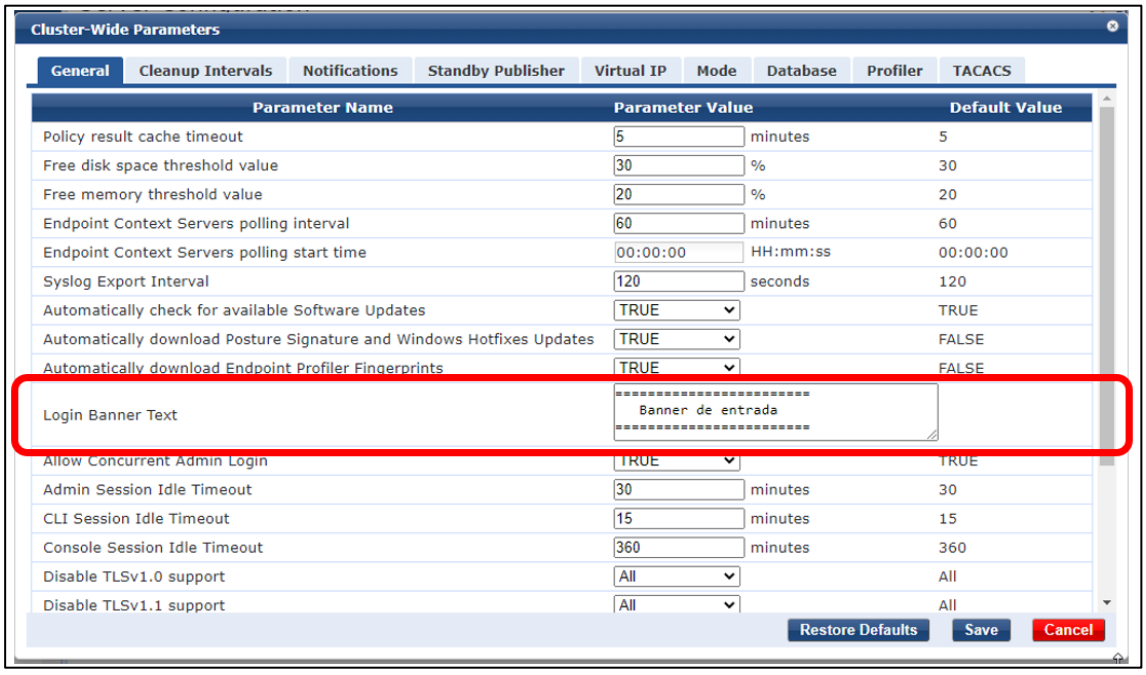


Ilustración 43. Configuración del texto de bienvenida en la introducción de credenciales

159. El efecto que tiene, por ejemplo, en la pantalla de acceso es el siguiente.

Ilustración 44. Ejemplo de texto de bienvenida (*banner*)

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

160. ClearPass ofrece una interfaz de puerto de datos y una interfaz de puerto de gestión. Se debe configurar el puerto de administración, pero el puerto de datos es opcional (ver apartado **4.4.1 DOBLE INTERFAZ DE RED**). No puede configurar solo un puerto de datos.

161. Cuando ClearPass está configurado con una interfaz de administración, pero no con la interfaz de datos opcional, todo el tráfico pasa por la interfaz de administración.

6.4.1.1 LISTA DE PUERTOS USADOS POR CLEARPASS

162. Debido a que ClearPass puede tener una alta capacidad de integración con otros sistemas, pude ser objeto de ataques y, por tanto, debe ser protegido convenientemente tras los servicios de un cortafuegos.

163. Se adjunta, a continuación, la tabla de puertos usados por ClearPass, relacionado con cada una de sus funciones.

	Between		Protocol	Port	Service Description
ClearPass UI	Management Station	ClearPass	TCP	443	HTTPS
Secure Shell	Client	ClearPass	TCP	22	SSH
Guest Portal	Controller	ClearPass	TCP	443 / 80	HTTP not recommended but can be configured
Update service	ClearPass	Update Server	TCP	443	HTTPS
OnGuard Agent	Endpoints	ClearPass	TCP	443	HTTPS
	Endpoints	ClearPass	TCP	6658	OnGuard to CPPM
NAS Devices - AAA Services	NAS Devices	ClearPass	TCP/UDP	1812	RADIUS
	NAS Devices	ClearPass	TCP/UDP	1645	RADIUS
	NAS Devices	ClearPass	TCP/UDP	1813	RADIUS Accounting
	NAS Devices	ClearPass	TCP/UDP	1646	RADIUS Accounting
	ClearPass	NAS Devices	TCP/UDP	3799	RADIUS CoA - RFC3576
	NAS Devices	ClearPass	TCP/UDP	49	TACACS
ClearPass to Active Directory	ClearPass	AD Servers	ICMP echo (8) and echo-reply (0) between CPPM host and Domain Controller used during domain join		
	ClearPass	AD Servers	TCP/UDP	389	LDAP
	ClearPass	AD Servers	TCP/UDP	636	LDAP over SSL
	ClearPass	AD Servers	TCP/UDP	445	NetLogon
	ClearPass	AD Severs	TCP	49152 - 65535	SMBv2 / v3 RPC randomly allocated high TCP ports see SMB Ports Range Note
	ClearPass	AD Severs	TCP	1025 - 5000	SMBv1 RPC randomly allocated low TCP ports see SMB Ports Range Note

Ilustración 45. Lista de puertos (parte 1)

	ClearPass	AD Servers	UDP	88	Kerberos Authentication
	ClearPass	AD Servers	TCP	464	Password Change
	ClearPsss	AD Servers	TCP	139	AD Auth test from CLI
SNMP	ClearPass	Endpoint	UDP	161	SNMP Read / Write
SNMP	Endpoint	ClearPass	UDP	162	SNMP Traps
WMI	ClearPass	Endpoint	TCP	135	WMI Scan
Cluster	Publisher	Subscriber	TCP	443	HTTPS encrypted using SSL
	Subscriber	Publisher	TCP	443	HTTPS encrypted using SSL
	Publisher	Subscriber	TCP	5432	PostgreSQL for DB replication - encrypted using SSL
	Subscriber	Publisher	TCP	5432	
	Subscriber	Publisher	UDP	123	Time synchronization
ClearPass Misc Services	ClearPass	NTP Servers	UDP	123	NTP
	ClearPass	SMTP Servers	TCP	25	SMTP
	ClearPass	SMTP Servers	TCP	465	SMTP Secure
	ClearPass	DNS Servers	TCP	53	DNS
	Network	ClearPass	UDP	67	DHCP Snooper
	Network	ClearPass	UDP	2055	NetFlow collector
	Network	ClearPass	UDP	6343	sFlow collector
Ingress Event Engine	Network	ClearPass	UDP	514	

Ilustración 46. Lista de puertos (parte 2)

6.4.1.2 SERVICIOS

164. Para ver el estado de los servicios del sistema por cada uno de los servidores, se accede a *Administration > Server Manager > Server Configuration.* Se selecciona el servidor a inspeccionar, la pestaña *Service Control y*, como resultado, se observa la lista de servicios, su estado y posibilidad de cambiar su estado.

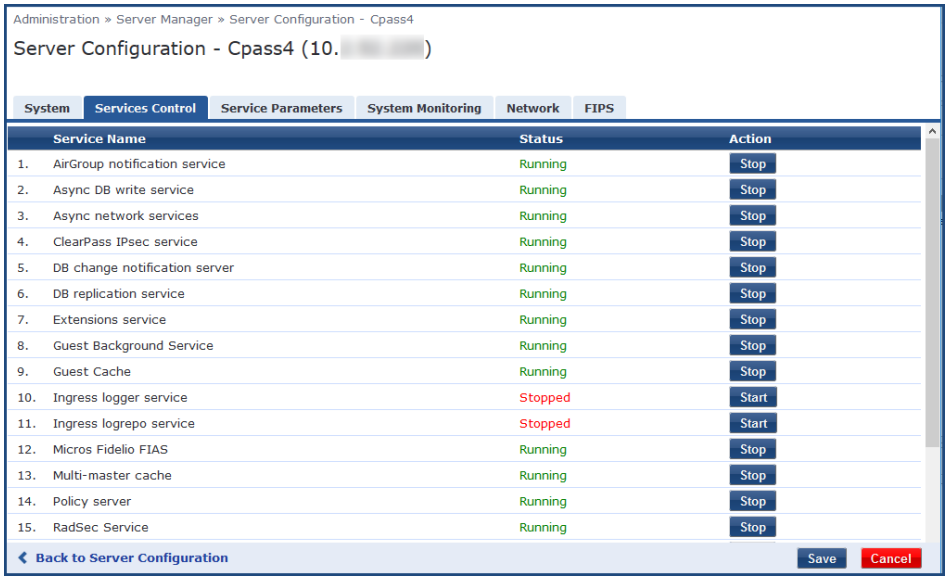


Ilustración 47. Estado de ejecución de los servicios de sistema

165. En función de las funcionalidades activadas, alguno de los servicios puede estar parado.

166. En la pestaña *Service Parameters* se puede inspeccionar los parámetros de cada funcionalidad:

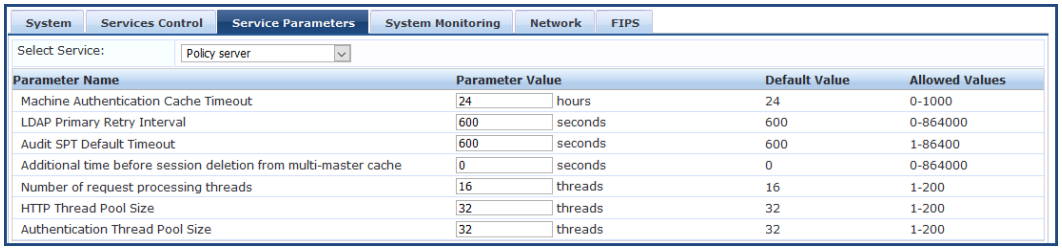


Ilustración 48. Parámetros de cada uno de los servicios del sistema

6.4.1.3 INTERFACES VIRTUALES EN CLEARPASS

167. Se pueden configurar dos (2) nodos en un clúster para compartir una dirección IP virtual. La dirección IP virtual está vinculada al nodo principal de forma predeterminada. El nodo secundario asume el control cuando el nodo principal no está disponible.

168. Para configurar la IP virtual, ir a *Administration > Server Manager > Server Configuration* y seleccionar *Virtual IP Settings*.

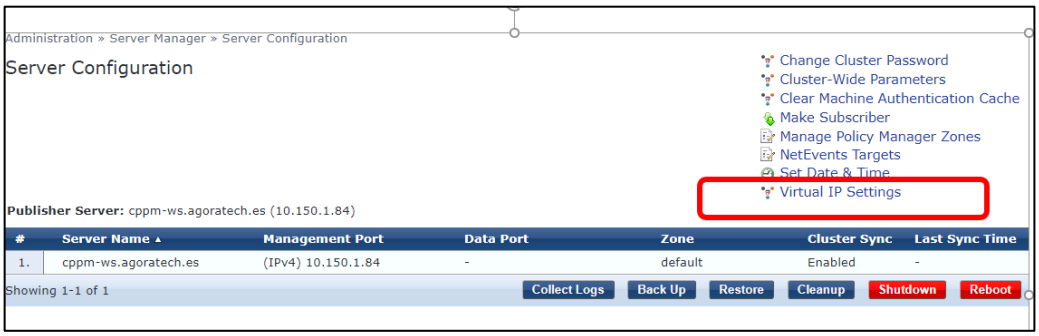


Ilustración 49. Acceso a la configuración de las IPs Virtuales

169. Una vez ahí, se pueden definir las direcciones IP virtuales.

170. Pueden crearse varias IP virtuales por interfaz.

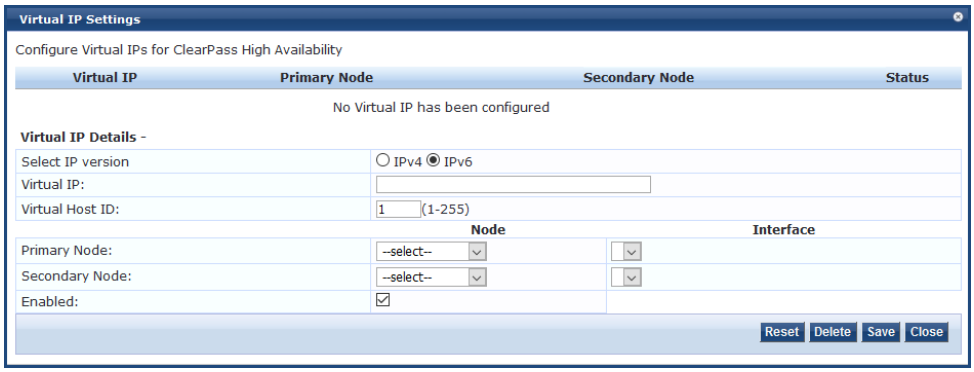


Ilustración 50. Creación de una IP Virtual

171. Pensando en el caso más frecuente de un clúster de nivel 2 de dos servidores, es una buena práctica crear dos IP virtuales en cada segmento, puerto Datos y Gestión. En cada una de ellas sería primario un servidor.

    a) Puerto Management:

        1. VIP1: Primario *Publisher*, secundario *Subscriber*.
        2. VIP2: Primario *Subscriber*, secundario *Publisher*.

    b) Puerto Dados:

        1. VIP3: Primario *Publisher*, secundario *Subscriber*.
        2. VIP4: Primario *Subscriber*, secundario *Publisher*.

172. De esta forma, por ejemplo, podremos configurar servidores RADIUS con continuidad en el servicio. Incluso se podría cambiar direccionamiento IP de los servidores sin dejar de dar servicio.

6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

6.5.1 MODO FIPS

173. Aruba ClearPass soporta el modo de trabajo FIPS. En este modo todos los servicios criptográficos proporcionan una fortaleza mínima de 128 bits cumpliendo la normativa FIPS 140-2. Como se ha comentado anteriormente, se debe configurar este modo de trabajo (ver apartado **6.1 MODO DE OPERACIÓN SEGURO**).

6.5.2 TLS 1.0 Y TLS 1.1

174. Para mayor seguridad, se **debe deshabilitar TLSv1.0 y TLSv1.1** mediante un parámetro de clúster. Para ello, ir a *Administration > Server Manager > Server Configuration*, hacer clic en *Cluster-Wide Parameters* y marcar las opciones *Disable TLSv1.0 support* y *Disable TLSv1.1 support,* con el valor *All.* Es la opción por defecto.

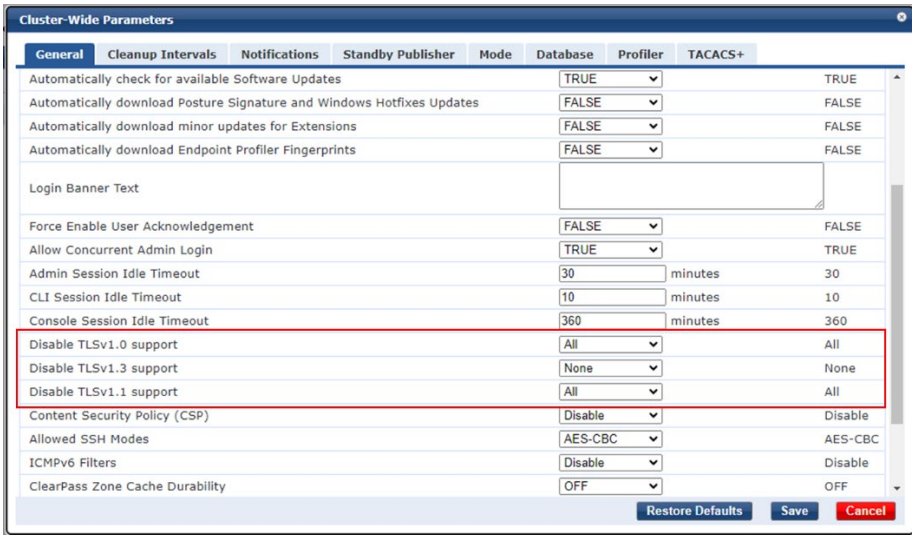


Ilustración 51. Deshabilitar TLS versión 1.0 y 1.1

6.5.3 SSHV2

175. ClearPass sólo soporta SSH versión 2. Admite inicios de sesión SSH basados en claves públicas por dispositivo. La opción de claves públicas SSH está disponible en *Administration > Server Manager > Server Configuration > Network.*

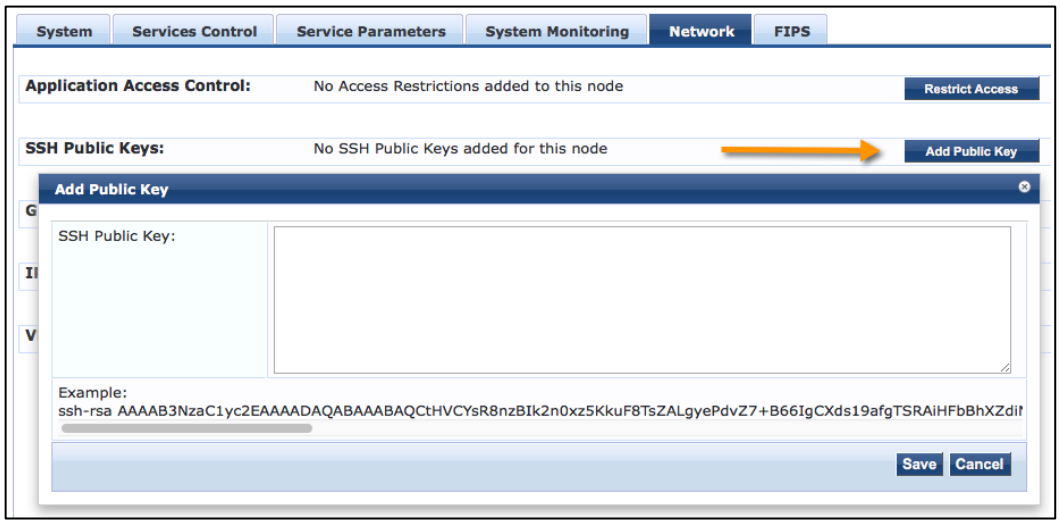


Ilustración 52. Configuración de claves públicas de SSH

6.5.4 SOPORTE SMB V2/V3

176. ClearPass soporta SMBv2/v3 para *PEAPv0/EAP-MSCHAPv2* y Servicios de Dominios *Microsoft Active Directory*. Utilizará la versión superior disponible en el controlador:

a) SMBv3 será automáticamente utilizado por defecto para AD *Joins* y cualquier petición que utilice PEAPv0/EAP-MSCHAPv2.

b) Sí SMBv3 no está habilitado, probará SMBv2.

c) Sí SMBv2 no está habilitado, utilizará SMBv1.

d) Si a posteriori, se habilitan versiones superiores, ClearPass detectará los cambios automáticamente e intentará utilizar la versión más alta posible.

6.5.5 INTERFACES IPSEC

177. ClearPass admite túneles IPsec para la gestión y las interfaces de datos. IPsec proporciona túneles cifrados que garantizan la confidencialidad de las comunicaciones y la identidad de los *endpoints*. Esto es fundamental en entornos de alta seguridad o cuando las comunicaciones salen de un entorno controlado.

178. Desde *Administration > Server Manager > Server Configuration > Network,* se pueden crear interfaces IPSec. Haciendo clic en *Create IPsec Tunnel*.

179. Se debe usar IKEv2, y en general, el máximo nivel de seguridad que ofrezcan ambos extremos. Para ello, en el parámetro *IKE Version* seleccionar 2.

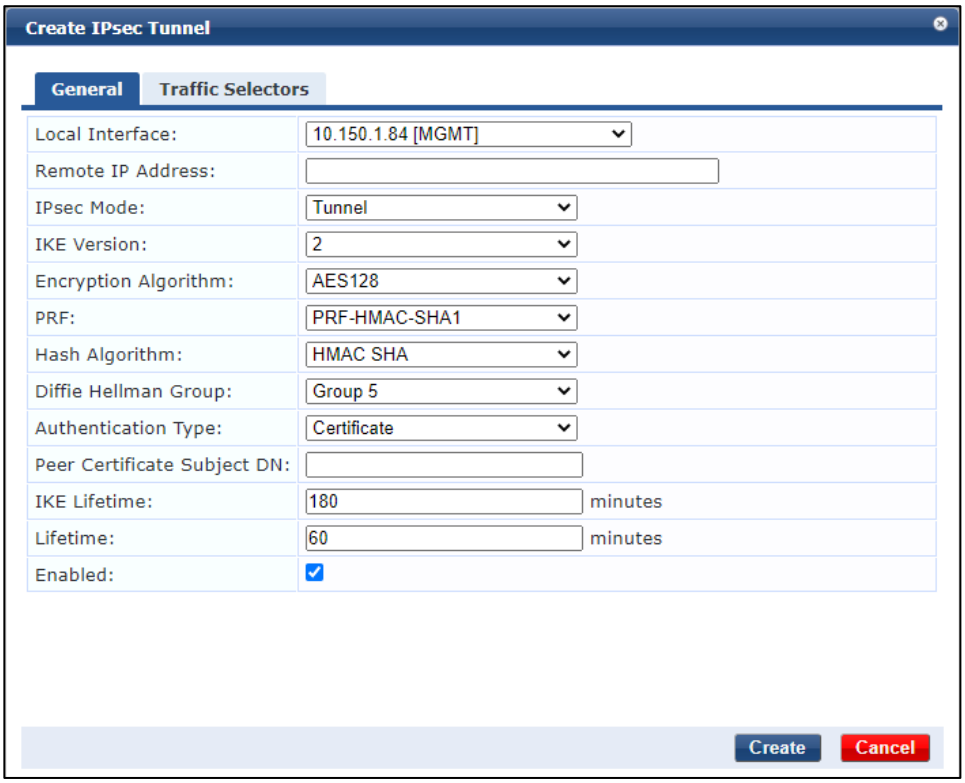


Ilustración 53. Creación de un interfaz túnel IPSEC.

180. Los filtros de tráfico en la definición del túnel permiten:

a) *Encrypt*.

b) *Drop*.

c) *Bypass*.

6.6 GESTIÓN DE CERTIFICADOS

181. ClearPass hace uso de certificados para diversas funciones. En concreto usa cinco (5) tipos de certificados:

a) *RADIUS/EAP Server Certificate*. Este certificado se usa para las transacciones RADIUS.

b) *HTTPS Server Certificate (RSA)*. El certificado que será usado en las páginas web servidas por ClearPass. Estas son las propias del interfaz de administración, los diferentes portales (invitados, provisión) y APIs. Este certificado utiliza criptografía RSA.

c) *HTTPS Server Certificate (ECC)*. El certificado que será usado en las páginas web servidas por ClearPass. Estas son las propias del interfaz de administración, los diferentes portales (invitados, provisión) y APIs. Este certificado utiliza criptografía de curva elíptica.

d) *RadSec Server Certificate*. El certificado que es usado para las transacciones RADSEC.

e) *Database Server Certificate*. El certificado utilizado para la sincronización de las bases de datos por los servidores de ClearPass.

182. Los certificados instalados se pueden ver en *Administration > Certificates > Certificate Store*. En el proceso de instalación del producto se generan unos certificados autofirmados. **Se deben sustituir estos certificados, por unos firmados por una CA de confianza.**

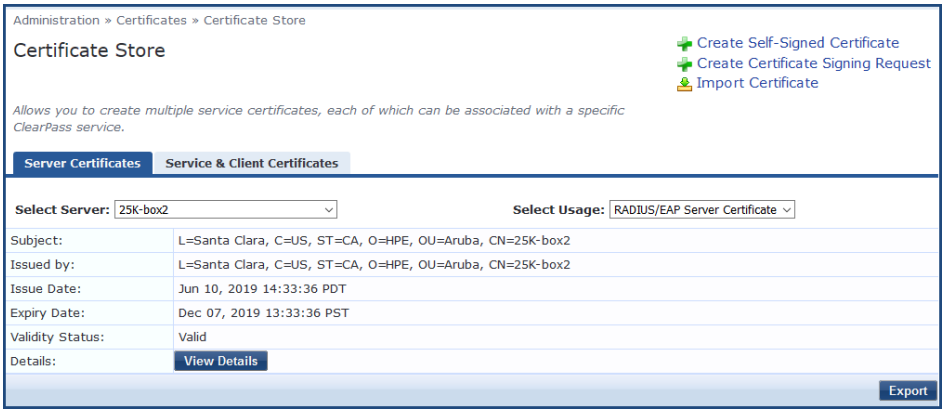


Ilustración 54. Almacén de Certificados

183. Se recomienda que los certificados HTTPS sean públicos y fácilmente validables por los clientes ya que deben poder ser procesados sin necesidad de que el usuario realice ningún tipo de consideración sobre el certificado. Estos certificados se usan en las interacciones HTTPS (consolas de administración y portal de invitados).

184. Los certificados HTTPS(ECC) y HTTPS(RSA) se pueden habilitar o deshabilitar haciendo clic en los botones Habilitar o Deshabilitar en la esquina inferior derecha de la ventana Almacén de certificados. No se puede utilizar un certificado deshabilitado y no se pueden deshabilitar HTTPS(ECC) y HTTPS(RSA) simultáneamente. Si se habilitan los certificados HTTPS (ECC) y HTTPS (RSA), cualquier cliente que admita cifrados ECC obtendrá certificados HTTPS (ECC) cuando se comunique con ClearPass. Si habilita los certificados ECC, las listas de confianza del cliente deben actualizarse en consecuencia.

185. Para el uso de RADIUS se recomienda el uso de una CA privada. Por defecto se muestra el certificado de RADIUS. Para ver otros, seleccionar el deseado en el apartado *Select Usage*.

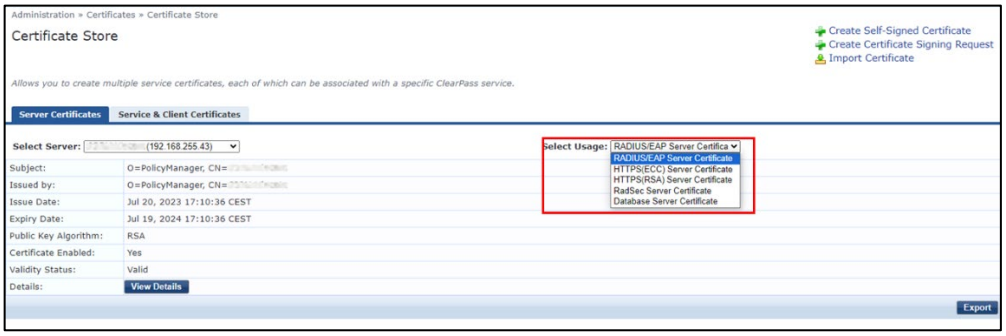


Ilustración 55. Selección de la funcionalidad a mostrar en el Almacén de Certificados.

186. Los certificados con un comodín como nombre común (por ejemplo: **.arubanetworks.com*) y los certificados de validación extendida (EV, "barra verde") no se recomiendan para su uso como certificado de servidor RADIUS / EAP. Es posible que algunos clientes no puedan autenticarse cuando se utilizan estos tipos de certificados.

6.6.1 GENERACIÓN DE UN CSR

187. El producto permite la generación de peticiones CSR (*Certificate Signing Request*), para la obtención de certificados para su posterior uso.

188. Para realizar una petición, se puede ir a *Administration > Certificates > Certificate Store* y hacer clic en *Create Certificate Signing Request.* Completar la información requerida en los campos que se muestran a continuación. **Se debe seleccionar, en el parámetro *Private Key Type*, RSA con una longitud de 3072 bits o superior, o NIST/SECG.**

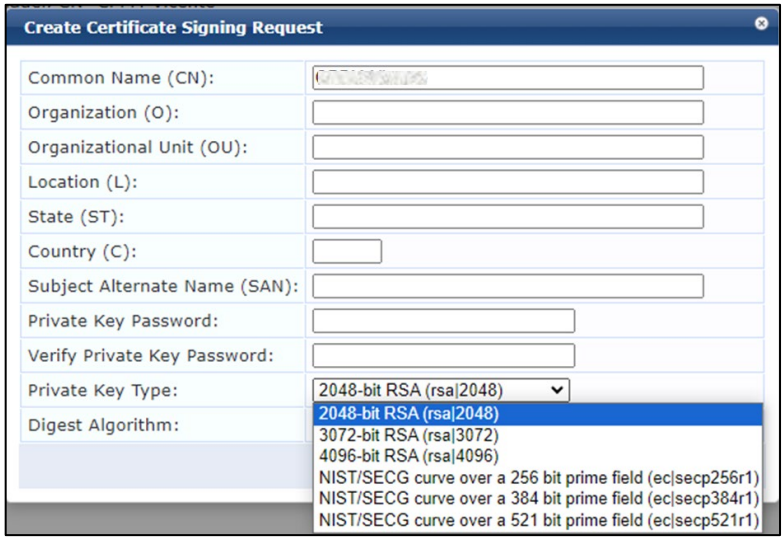


Ilustración 56. Plantilla de creación de un CSR (*Certificate Signing Request*)

189. El campo *Subjet Alternate Name (SAN)*, permite la adición de nombres adicionales. Tras hacer clic en *Submit*, se abre la siguiente ventana mientras se genera la petición.

Ilustración 57. Certificado en generación

190. La petición generada se muestra en la ventana y permite descargarla.

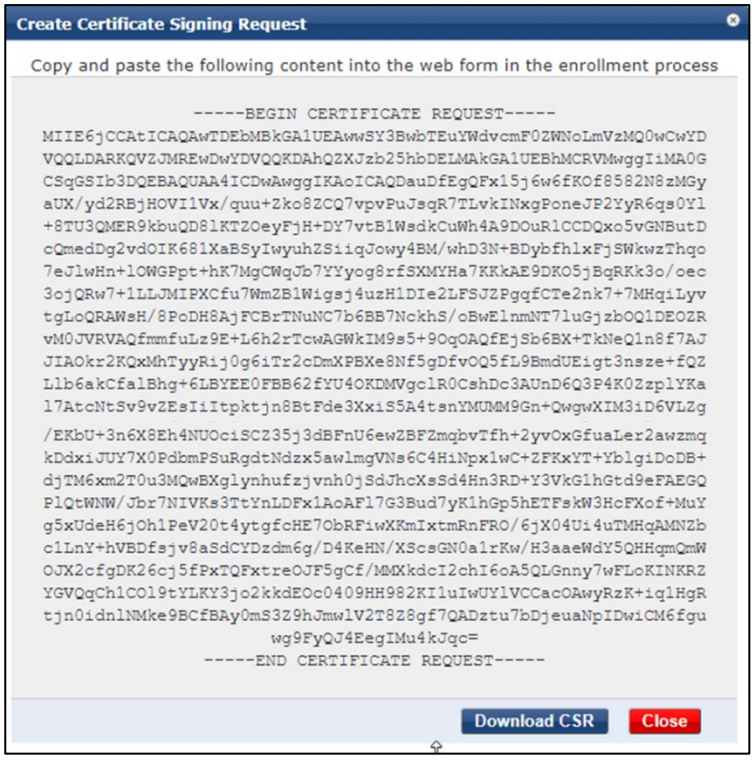


Ilustración 58. Certificado generado (datos ficticios)

191. Por último, hacer clic en *Download CSR*, para proceder a su descarga. Se puede consultar el detalle de la creación de CSR en [REF11].

6.6.2 IMPORTAR UN CERTIFICADO DE SERVIDOR

192. Durante la importación de un certificado de servidor, se proporcionan tres (3) opciones de carga:

    a) ***Upload Certificate and Use Saved Private Key***: esta opción permite al administrador cargar solo el certificado. Este se compara con la clave privada

guardada en el servidor de *Policy Manager*. Esto es válido para certificados generados a partir de un CSR generado desde ClearPass.

b) ***Upload PKCS#12 Certificate (.pfx or .p12 only)**:* con esta opción, el administrador carga el archivo PKCS#12 y proporciona una frase de contraseña.

c) ***Upload Certificate and Private Key Files***: el administrador puede optar por cargar el archivo de clave privada y la contraseña junto con el archivo de certificado del servidor. Esto es válido para certificados generados a partir de un CSR generado desde *ClearPass* y para CSR generados externamente.

193. Para importar un certificado, ir a *Administration > Certificates > Certificate Store* y hacer clic en *Import Certificate.*

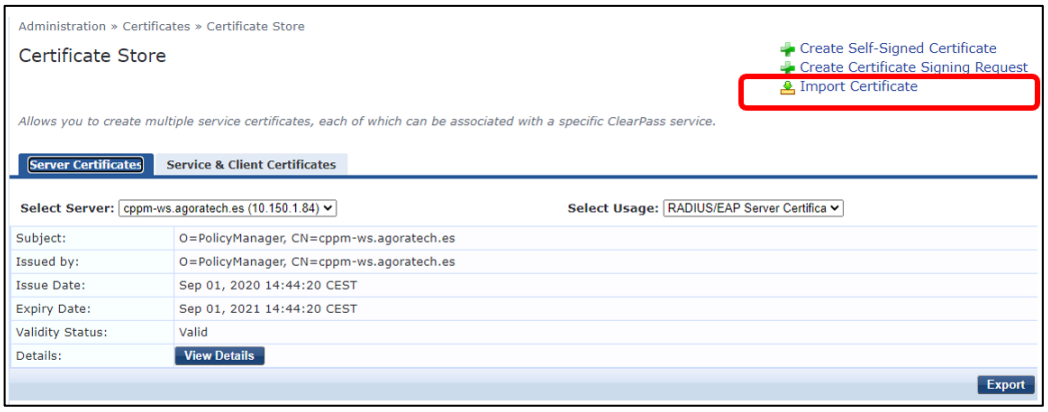


Ilustración 59. Importación de un certificado

194. Seleccionar el tipo de certificado que se quiere cargar y elegir el nodo de ClearPass donde se quiere cargar el certificado.

195. Seleccionar el uso que se va a dar a dicho certificado. Las opciones disponibles son las siguientes:

a) *RADIUS/EAP Server Certificate*

b) *HTTPS Server Certificate(ECC)*

c) *HTTPS Server Certificate(RSA)*

d) *RadSec Server Certificate*

e) *Database Server Certificate*

196. Tras elegir el formato, subimos los ficheros correspondientes.

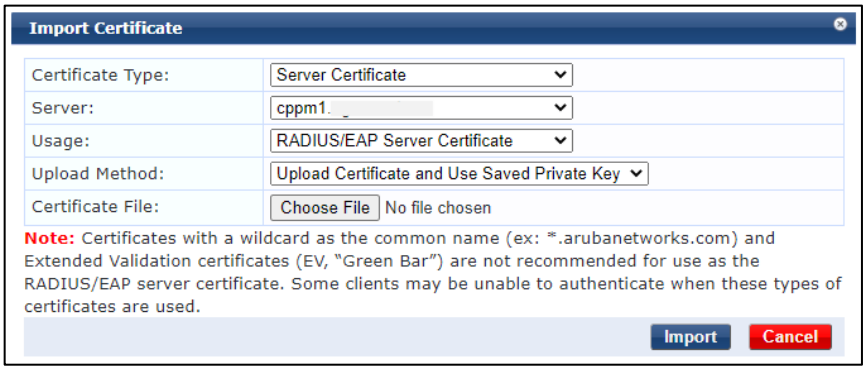


Ilustración 60. Importación de un certificado tipo RADIUS

197. Dependiendo el uso, los certificados pueden ser solicitados en alguna acción posterior (por ejemplo, *re-login* en la plataforma si se trata del servidor HTTPS).

6.6.3 AÑADIR ENTIDADES DE CERTIFICACIÓN DE CONFIANZA.

198. La página *Certificate Trust List*, accesible desde *Administration > Certificates > Trust List,* muestra una lista de Autoridades de certificación (CA) de confianza. En esta página, se puede agregar, ver o eliminar un certificado.

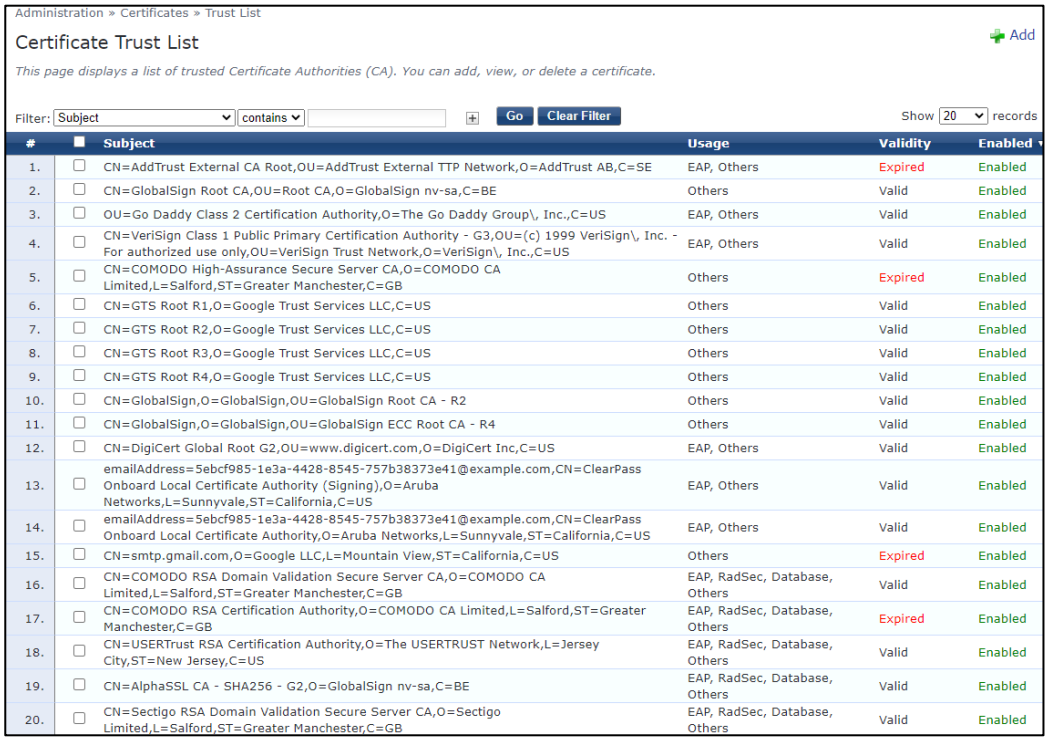


Ilustración 61. Listado de Autoridades de Certificación

199. ClearPass incluye algunas CA por defecto. Algunas de ellas están desactivadas.

200. En el modo seguro, no se pueden importar certificados que se hayan creado con el algoritmo de *MD5 digest*. Tampoco se permite importar un certificado a la lista de confianza con *Basic constraints CA = False*, por lo que no se admite el cifrado SAML IdP cuando ClearPass Policy Manager actúa como IdP.

201. Se pueden añadir CAs adicionales. Para ello ir a *Administration > Certificates > Trust List,* hacer clic en *Add, c*argar el certificado, seleccionar los usos para los que se usará dicha CA y hacer clic en *Add Certificate.*

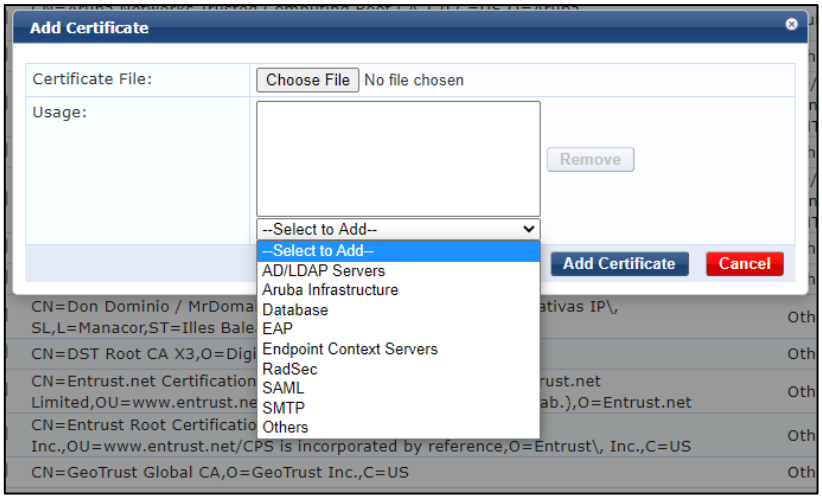


Ilustración 62. Añadir una Autoridad de Certificación

202. Para activarlo o desactivarlo, o bien para cambiarle los usos a una CA ya cargada, sólo hace falta seleccionarla de la lista y editarla. La pantalla que se mostraría es equivalente a la siguiente:

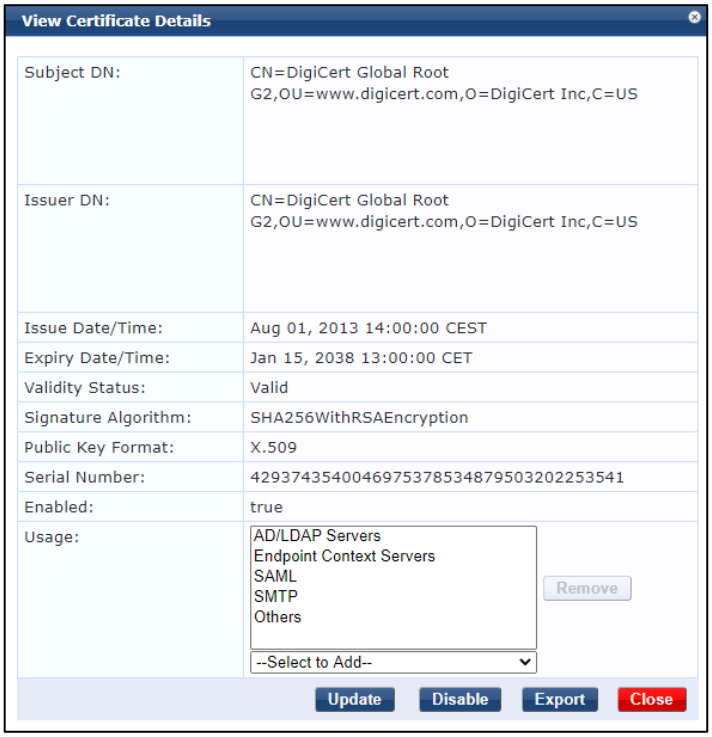


Ilustración 63. Selección del uso autorizado de la Autoridad de Certificación

203. Si no se va a hacer uso de una CA cargada, se recomienda desactivarla. En caso de haber expirado, se recomienda descargarla para su registro y eliminarla de ClearPass.

6.7 SINCRONIZACIÓN HORARIA

204. Si el servicio de sincronización horaria NTP no está autenticado, un atacante podría introducir información horaria falsa. Este servidor de tiempo falso podría provocar que los registros reflejarán información incorrecta. **Se recomienda, por tanto, utilizar fuentes de reloj con autenticación.**

205. Se soporta autenticar las fuentes de tiempo utilizando SHA 1. En modo seguro sólo se permite el uso de SHA1. La autenticación utiliza el servicio de *Linux ntp.* En un clúster, el *publisher* es la fuente de tiempos de todos los *Subscribers*.

206. La configuración de la sincronización horaria se realiza desde *Administration > Server Manager > Server Configuration,* seleccionando *Set Date & Time.*

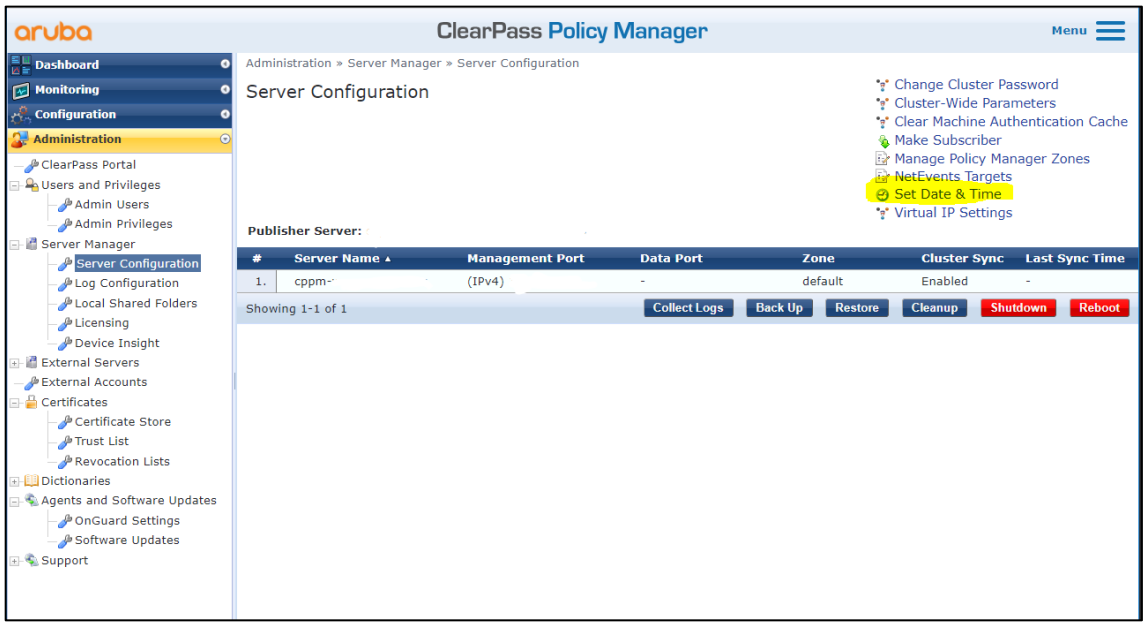


Ilustración 64. Configuración de tiempo y fecha

207. Se abrirá la siguiente ventana, donde se podrá configurar el servidor NTP tras seleccionar la casilla *Synchronize time with NTP server*, con los datos de autenticación incluidos.

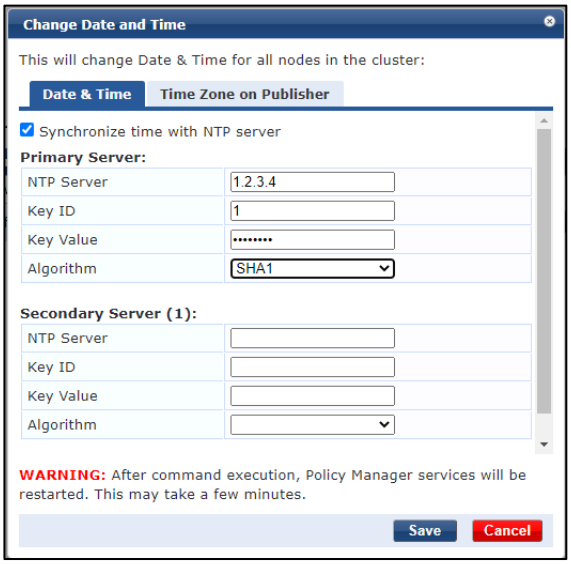


Ilustración 65. Configuración de sincronización horaria por NTP

6.8 ACTUALIZACIONES

208. ClearPass Policy Manager comprueba periódicamente si hay actualizaciones disponibles en el servidor de servicio web de *Policy Manager*.

209. Cuando hay nuevas actualizaciones disponibles, un administrador de red deberá usar la página *Administration > Agents and Software Updates > Software Updates* para descargar e instalar estas actualizaciones.

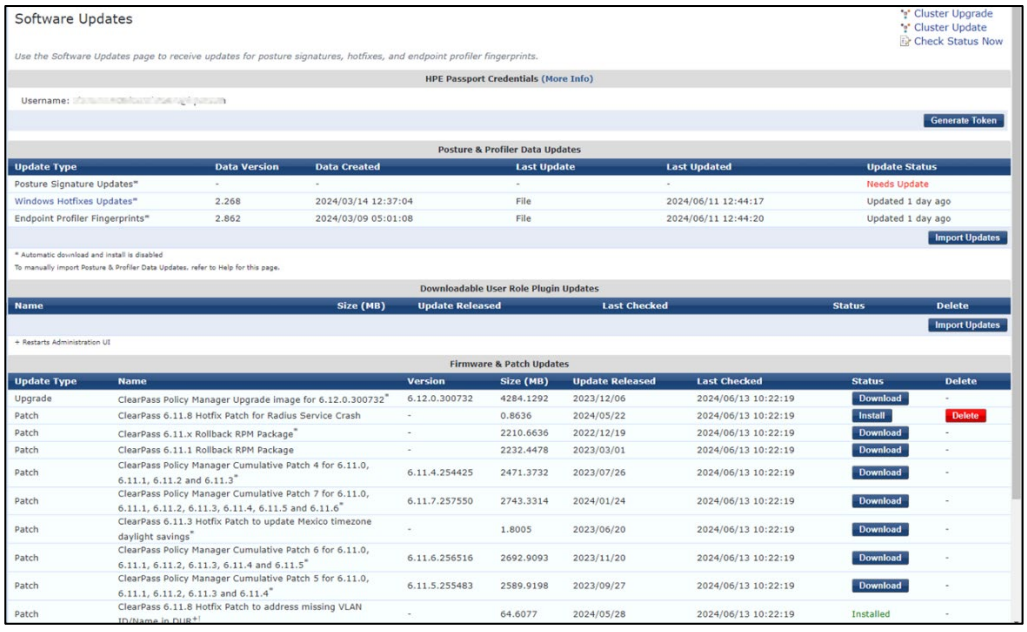


Ilustración 66. Página de actualizaciones de *software*

210. Las actualizaciones de *firmware*, parches y los complementos de función de usuario deben descargarse e instalarse manualmente. Para ello, desde el apartado *Firmware & Patch Updates*, se debe hacer clic sobre *Download* en las actualizaciones disponibles.

211. Las actualizaciones de *Windows hotfixes*, P*osture Signature Updates*, and E*ndoint Profile Fingerprint Updates* pueden descargarse e instalarse automáticamente, pero este comportamiento no está habilitado por defecto.

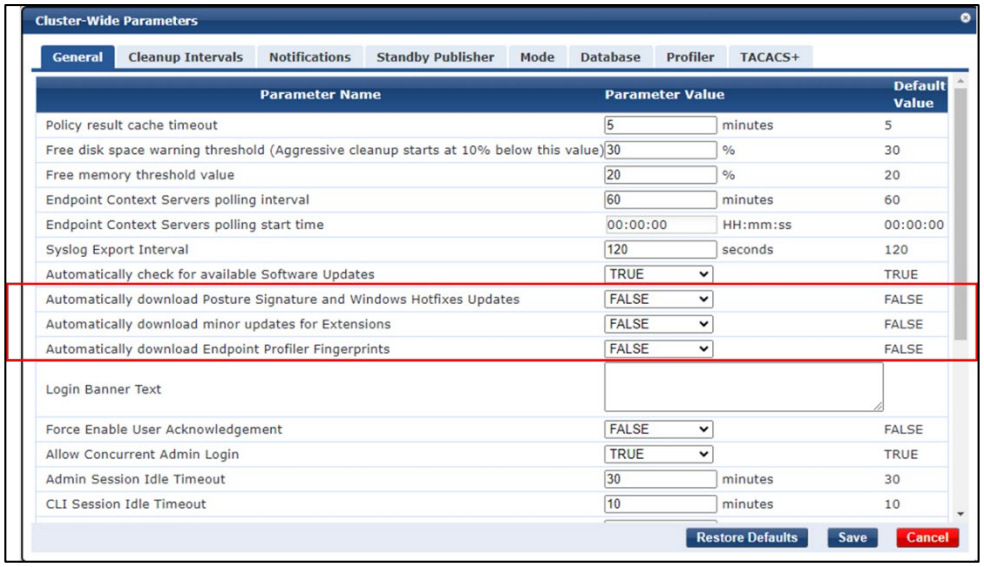


Ilustración 67. Parámetros que controlan la descarga automática de actualizaciones de firmas

212. Para configurar estas actualizaciones para que sean automáticas, se deben habilitar las opciones (seleccionando el valor TRUE) *Automatically download Posture Signature and Windows Hotfixes Updates* y *Automatically download Endpoint Profiler Fingerprints* en las opciones *Cluster-Wide Parameters* de Policy Manager, desde *Administration > Server Manager > Server Configuration*, seleccionando *Cluster-Wide Parameters*.

213. En un clúster de Policy Manager, la opción de importación de actualizaciones está disponible solo en el *Publisher*. Si ClearPass tiene conexión a Internet, y se han cargado credenciales, el sistema informará tanto de los parches instalados como de los descargables.

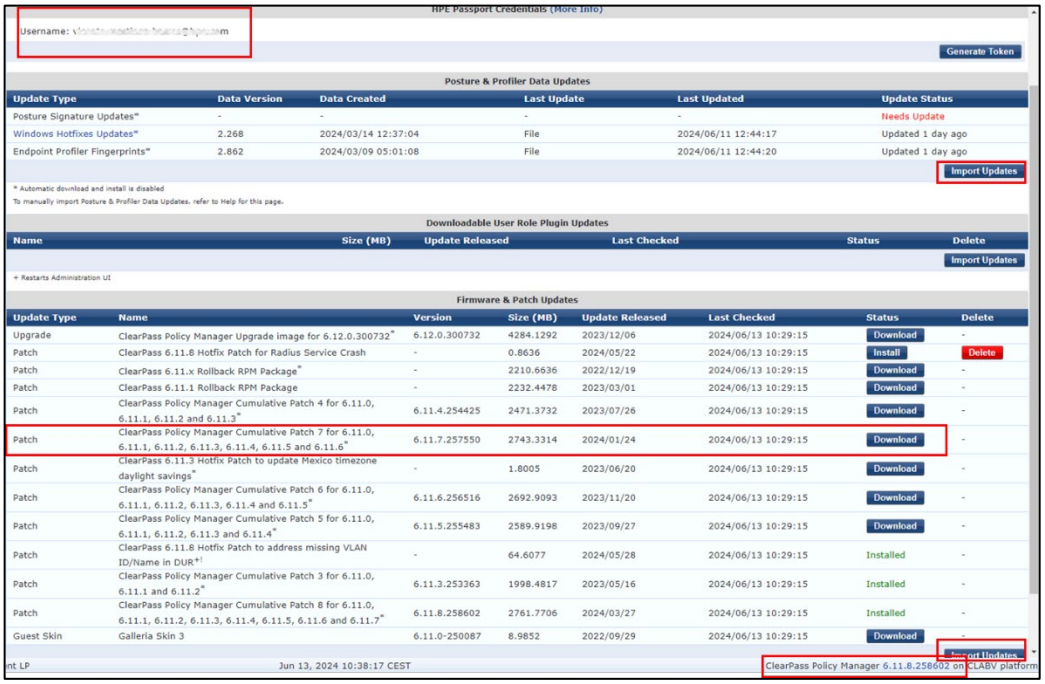
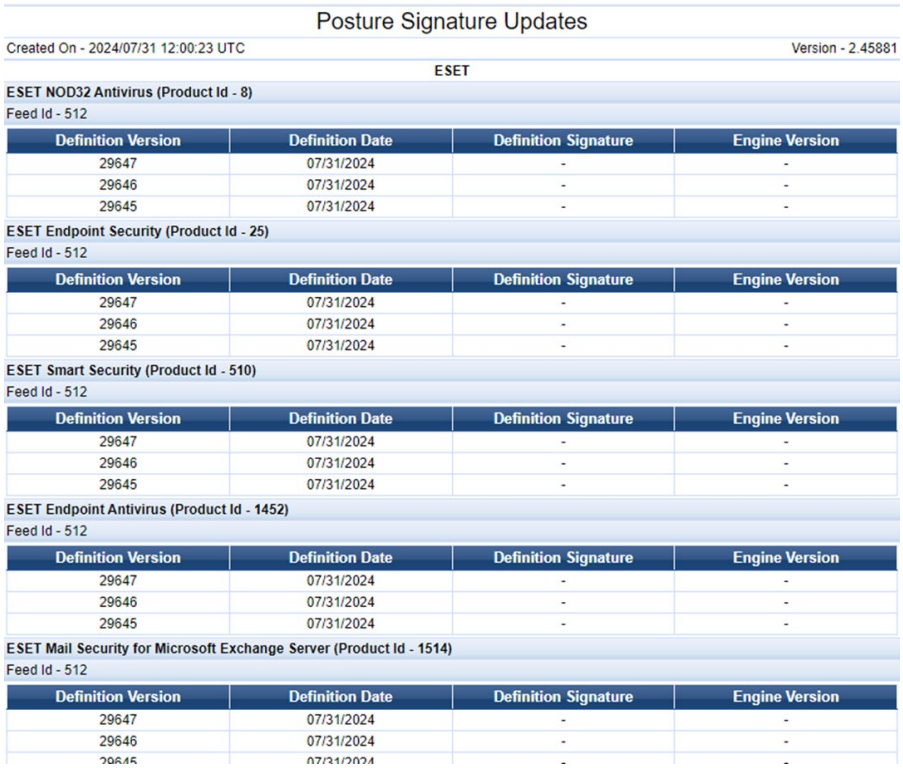


Ilustración 68. Detalles relevantes de la página de actualizaciones de *software*

214. El producto siempre informa en la barra inferior de la fecha y hora del sistema, así como la versión en ejecución.

215. Si no se dispone de conexión a Internet, o disponiendo incluso de ella, se pueden importar parches previamente descargados al terminal del operador. Para ello se debe hacer clic sobre *Import Updates*, en el apartado correspondiente.

216. Si se hace clic en las actualizaciones de *Posture Signature* o bien de *Windows Hotfixes,* se obtiene información sobre las definiciones descargadas.



Posture Signature Updates

Created On - 2024/07/31 12:00:23 UTC — Version - 2.45881

ESET

ESET NOD32 Antivirus (Product Id - 8)

Feed Id - 512

Definition Version	Definition Date	Definition Signature	Engine Version
29647	07/31/2024	-	-
29646	07/31/2024	-	-
29645	07/31/2024	-	-

ESET Endpoint Security (Product Id - 25)

Feed Id - 512

Definition Version	Definition Date	Definition Signature	Engine Version
29647	07/31/2024	-	-
29646	07/31/2024	-	-
29645	07/31/2024	-	-

ESET Smart Security (Product Id - 510)

Feed Id - 512

Definition Version	Definition Date	Definition Signature	Engine Version
29647	07/31/2024	-	-
29646	07/31/2024	-	-
29645	07/31/2024	-	-

ESET Endpoint Antivirus (Product Id - 1452)

Feed Id - 512

Definition Version	Definition Date	Definition Signature	Engine Version
29647	07/31/2024	-	-
29646	07/31/2024	-	-
29645	07/31/2024	-	-

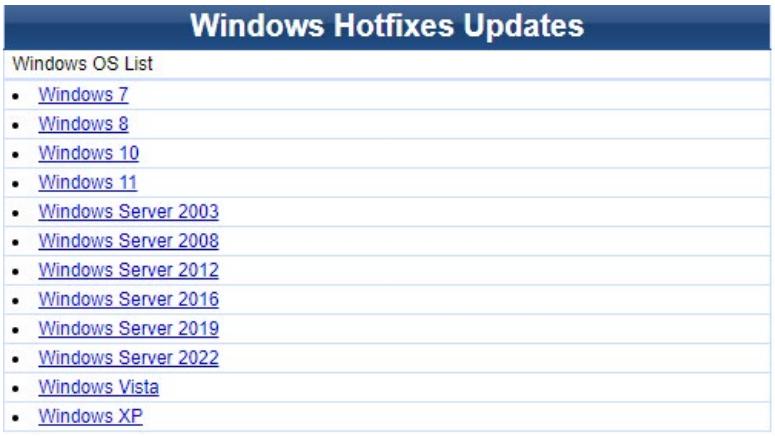
ESET Mail Security for Microsoft Exchange Server (Product Id - 1514)

Feed Id - 512

Definition Version	Definition Date	Definition Signature	Engine Version
29647	07/31/2024	-	-
29646	07/31/2024	-	-
29645	07/31/2024	-	-

Ilustración 69. Actualizaciones de firmas de estado de sistema operativo (*posture*)

217. Para las actualizaciones de *Windows Hotfixes*, se debe seleccionar primero la versión del sistema operativo:



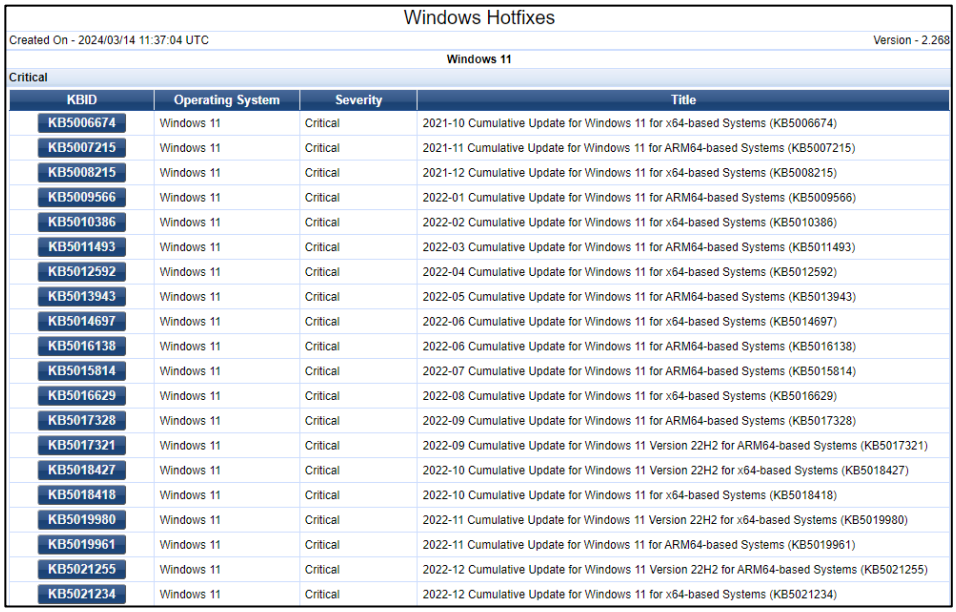
Windows Hotfixes Updates

Windows OS List

- Windows 7
- Windows 8
- Windows 10
- Windows 11
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Vista
- Windows XP

Ilustración 70. *Windows Hotfixes Updates*: Lista de sistemas Operativos Windows

218. Y a posteriori puede verse el detalle.



Windows Hotfixes

Created On - 2024/03/14 11:37:04 UTC — Version - 2.268

Windows 11

Critical

KBID	Operating System	Severity	Title
KB5006674	Windows 11	Critical	2021-10 Cumulative Update for Windows 11 for x64-based Systems (KB5006674)
KB5007215	Windows 11	Critical	2021-11 Cumulative Update for Windows 11 for ARM64-based Systems (KB5007215)
KB5008215	Windows 11	Critical	2021-12 Cumulative Update for Windows 11 for x64-based Systems (KB5008215)
KB5009566	Windows 11	Critical	2022-01 Cumulative Update for Windows 11 for ARM64-based Systems (KB5009566)
KB5010386	Windows 11	Critical	2022-02 Cumulative Update for Windows 11 for x64-based Systems (KB5010386)
KB5011493	Windows 11	Critical	2022-03 Cumulative Update for Windows 11 for ARM64-based Systems (KB5011493)
KB5012592	Windows 11	Critical	2022-04 Cumulative Update for Windows 11 for x64-based Systems (KB5012592)
KB5013943	Windows 11	Critical	2022-05 Cumulative Update for Windows 11 for ARM64-based Systems (KB5013943)
KB5014697	Windows 11	Critical	2022-06 Cumulative Update for Windows 11 for x64-based Systems (KB5014697)
KB5016138	Windows 11	Critical	2022-06 Cumulative Update for Windows 11 for ARM64-based Systems (KB5016138)
KB5015814	Windows 11	Critical	2022-07 Cumulative Update for Windows 11 for ARM64-based Systems (KB5015814)
KB5016629	Windows 11	Critical	2022-08 Cumulative Update for Windows 11 for x64-based Systems (KB5016629)
KB5017328	Windows 11	Critical	2022-09 Cumulative Update for Windows 11 for ARM64-based Systems (KB5017328)
KB5017321	Windows 11	Critical	2022-09 Cumulative Update for Windows 11 Version 22H2 for ARM64-based Systems (KB5017321)
KB5018427	Windows 11	Critical	2022-10 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems (KB5018427)
KB5018418	Windows 11	Critical	2022-10 Cumulative Update for Windows 11 for x64-based Systems (KB5018418)
KB5019980	Windows 11	Critical	2022-11 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems (KB5019980)
KB5019961	Windows 11	Critical	2022-11 Cumulative Update for Windows 11 for ARM64-based Systems (KB5019961)
KB5021255	Windows 11	Critical	2022-12 Cumulative Update for Windows 11 Version 22H2 for ARM64-based Systems (KB5021255)
KB5021234	Windows 11	Critical	2022-12 Cumulative Update for Windows 11 for x64-based Systems (KB5021234)

Ilustración 71. Ejemplo de listado de *Windows Hotfixes Updates*

219. Haciendo clic en cualquiera de ellos, se obtiene información detallada del parche.

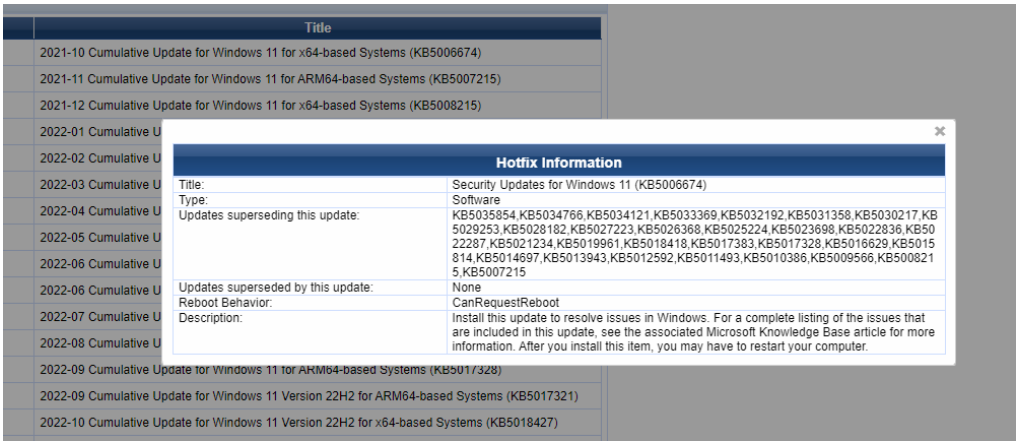


Ilustración 72. Ejemplo detalle de un *Windows Hotfix* en concreto

6.8.1 INSTALACIÓN DE PARCHES DE CLEARPASS

220. Se recomienda leer las instrucciones detalladas de cada *Release Notes* [REF5], tanto para el procedimiento, como para detectar los cambios que introduce y las tareas previas necesarias.

6.9 AUTO-CHEQUEOS

221. El producto ejecuta constantemente diversas verificaciones. Durante el arranque de cada servidor se ejecutan diferentes procesos de verificación de la integridad (entre ellas integridad del sistema de archivos, estado del software, comunicaciones con otros elementos del cluster, estado de la base de datos).

222. En caso de detectarse alguna anomalía se notificará por uno o varios de estos métodos, en función del momento de la detección, tipo y severidad:

a) Mensaje en la consola

b) Mensaje a los ficheros de logs

c) Registro en la vista “Event Viewer”

223. En caso de fallos graves durante el arranque del sistema, se puede llegar a detener el arranque.

224. Una vez en servicio, se van ejecutando diferentes tareas de verificación del funcionamiento de los servidores individualmente, del cluster, así como de los procesos. En la sección de Monitorización se describen los canales de comunicación de eventos de ClearPass. Ver apartado **7.1.5 *LIVE MONITORING: SYSTEM MONITOR***.

6.10 SNMP

6.10.1 RECOLECTOR DE DATOS

225. SNMP Es utilizado para obtener información de los equipos de red. Se recomienda el uso de SNMPv3 siempre que sea posible, pues proporciona autenticación y cifrado.

226. Ir a *Administration > Server Manager > Server Configuration.* Seleccionar el servidor e ir a la pestaña *System Monitoring* para configurar los parámetros SNMP. Seleccionar bajo el parámetro *Version* la opción *V3.*

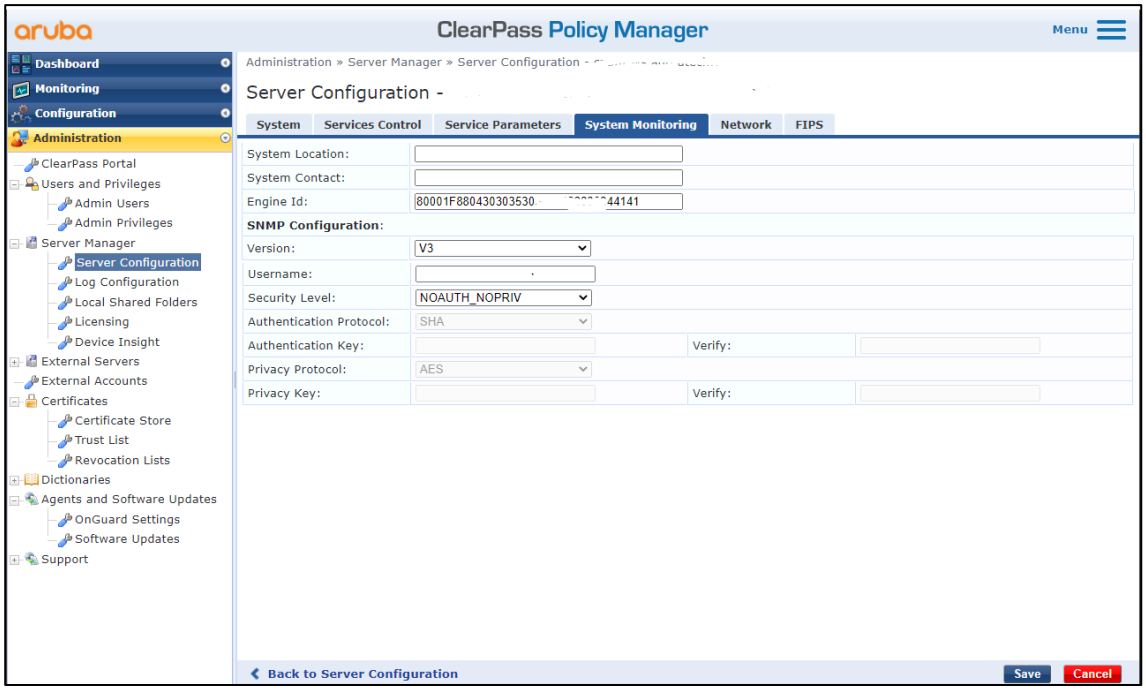


Ilustración 73. Parámetros SNMP

6.10.2 GENERADOR DE *TRAPS* Y SUS TIPOS

227. También puede enviar traps SNMP:

a) *System up time*. Para indicar el tiempo que está en marcha el equipo.

b) Estadísticas de los interfaces de red. Proporciona información si el interfaz de red está levantado o caído.

c) Información de monitorización de procesos. Notifica procesos que deberían estar corriendo. Envía *traps* si hay cambios.

d) Utilización de disco. Chequea el espacio en disco de una partición. Envía *traps* si hay cambios en el valor del disco disponible.

e) Información de la carga de CPU. Monitoriza valores de carga del sistema anormales. Utiliza para ello umbrales predefinidos en porcentaje.

f) Uso de memoria. Informa del uso de memoria del sistema.

228. Los umbrales de carga de disco libre y CPU se configuran como un parámetro de servicio, a través de *Administration > Server Manager > Service Parameter >* y *service > System Monitoring Service*.

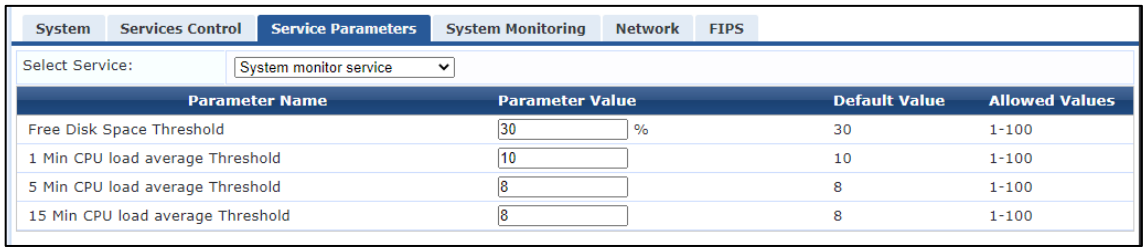


Ilustración 74. Umbrales de monitorización de disco libre y CPU

6.10.3 DESTINO DE LOS TRAPS

229. Es posible configurar el destino de los *traps* que se generan. Esto se configura en *Administration > External Servers > SNMP Trap Receivers.* Se recomienda configurar, en el parámetro *SNMP Version*, la opción *V3 with Authentication using SHA and with Privacy.*

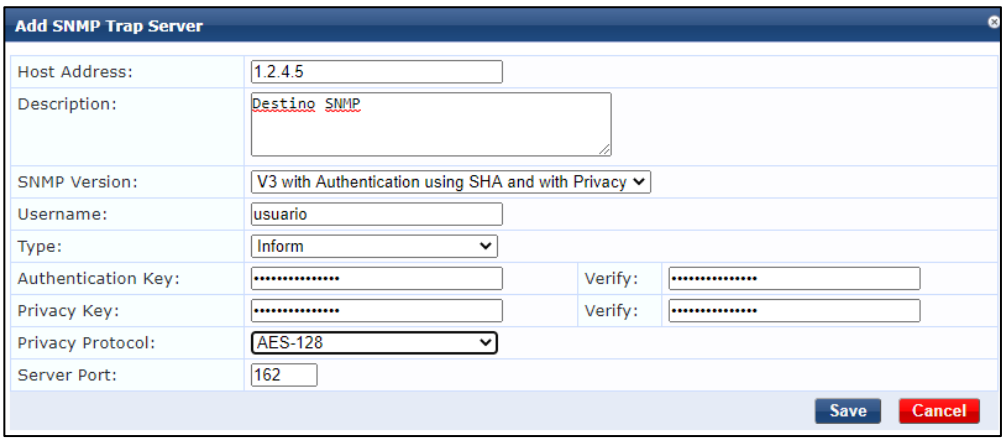


Ilustración 75. Configuración de destinos SNMP

6.11 ALTA DISPONIBILIDAD

230. El producto permite despliegues de Alta Disponibilidad mediante el uso de los clústeres, de tal forma que, ante el fallo de un *appliance*, se mantenga el servicio. La configuración de los clústeres se puede consultar en el apartado **5.3 CONSTITUCIÓN DEL CLÚSTER**.

6.12 AUDITORÍA

6.12.1 ALMACENAMIENTO LOCAL

231. De forma predeterminada, el servidor ClearPass solo retiene los registros de auditoría durante siete (7) días. Este valor puede ser modificado desde *Administration > Server Manager > Server Configuration > Cluster wide Parameters.*

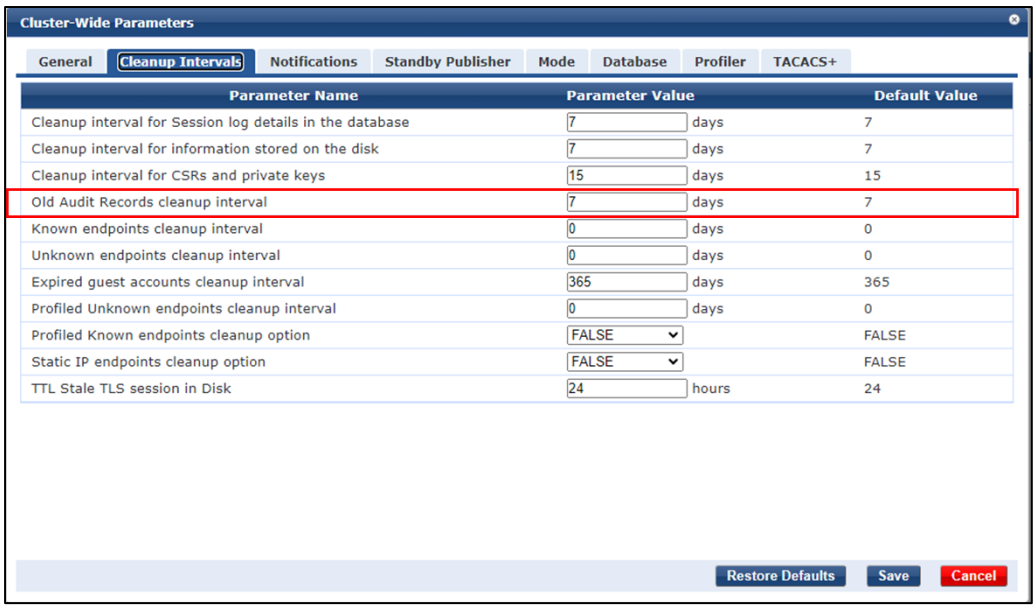


Ilustración 76. Periodo de limpieza de registros de auditoría

232. Si se desea almacenar los registros por más tiempo, se recomienda exportarlos fuera de ClearPass.

6.12.2 ALMACENAMIENTO REMOTO: SYSLOG EXTERNO

233. Es posible enviar la información de los eventos de ClearPass a servidores de log externos. Se puede configurar más de un servidor *Syslog*.

234. Para la configuración de los envíos se define un filtro de mensajes de *syslog* donde se filtra los tipos de mensajes que se quieren reenviar y se asigna a los distintos destinos syslog.

235. La definición de un destino *syslog* se realiza desde *Administration > External Servers > Syslog Targets.* Se abrirá una ventana donde debe incluirse la información del servidor al que se quieren enviar los logs. Se recomienda utilizar el protocolo TCP, en el parámetro *Protocol*.

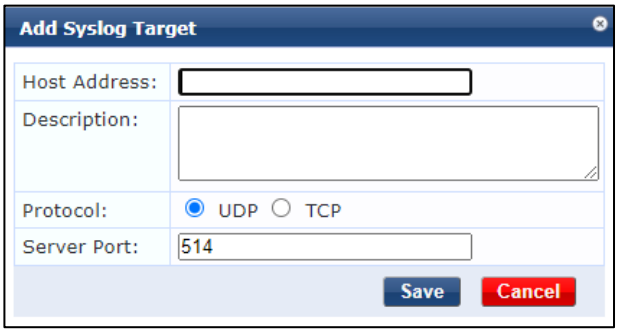


Ilustración 77. Configuración de un destino de *Syslog*

236. La definición de los filtros de *syslog* se realiza desde *Administration > External Servers > Syslog Export Filters***.** En un primer paso, desde la pestaña *General*:

- Se debe seleccionar, en el parámetro *Export Template,* el tipo de registros: logs de Sesiones, logs de *Insights*, eventos de sistema o registros de Auditoria.
- También se puede elegir el formato de *syslog* entre estándar, LEEF, CEF y RFC5424, a través del parámetro *Export Event Format Type.*
- Se selecciona después el valor del recurso[1] (Local Facility Level) así como los destinos seleccionados (servidores *syslog*). También se puede seleccionar desde qué servidores del clúster se enviarán los mensajes (servidores ClearPass).

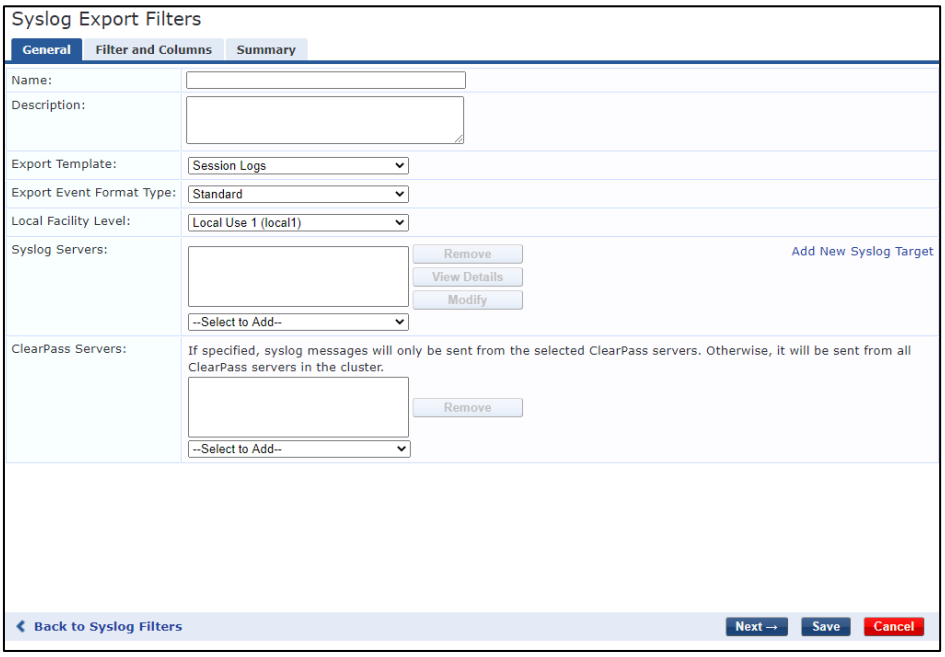


Ilustración 78. Características de configuración de filtro de exportación de Syslog

237. En un segundo paso, desde la pestaña *Filter and Columns*, se seleccionan las columnas deseadas en función de cada categoría. También existe la posibilidad avanzada de crear un filtro SQL que consulte directamente la base de datos local.

[1] Ver https://www.ietf.org/rfc/rfc3164.txt para consultar los distintos recursos (Facility level) disponibles en Syslog.

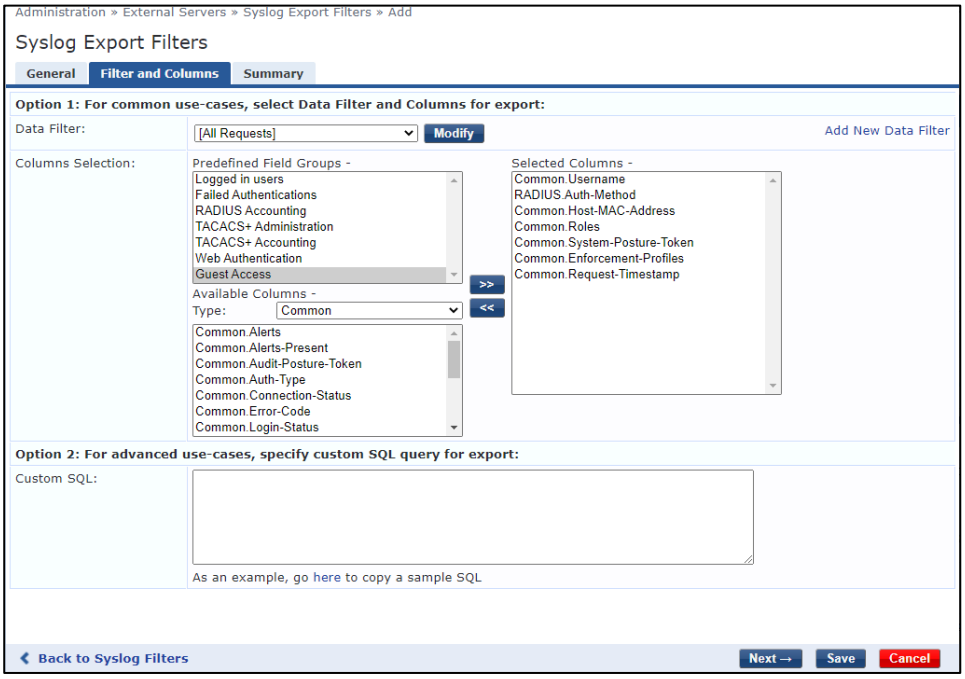


Ilustración 79. Configuración de filtro de exportación de *syslog*

6.13 BACKUP

238. Es posible realizar copias de seguridad manuales de la plataforma, a través del menú *Administration > Server Manager > Server Configuration > Backup.* Se mostrarán las siguientes opciones:

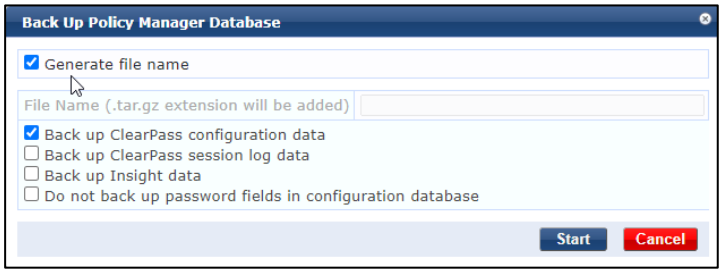


Ilustración 80. Generación de *backup*

239. Se puede seleccionar el nombre fichero y decidir las opciones y configuraciones de la copia de seguridad.

240. También es posible generar el *backup* desde el CLI. Se realiza mediante el comando *backup*, tal como se muestra a continuación:

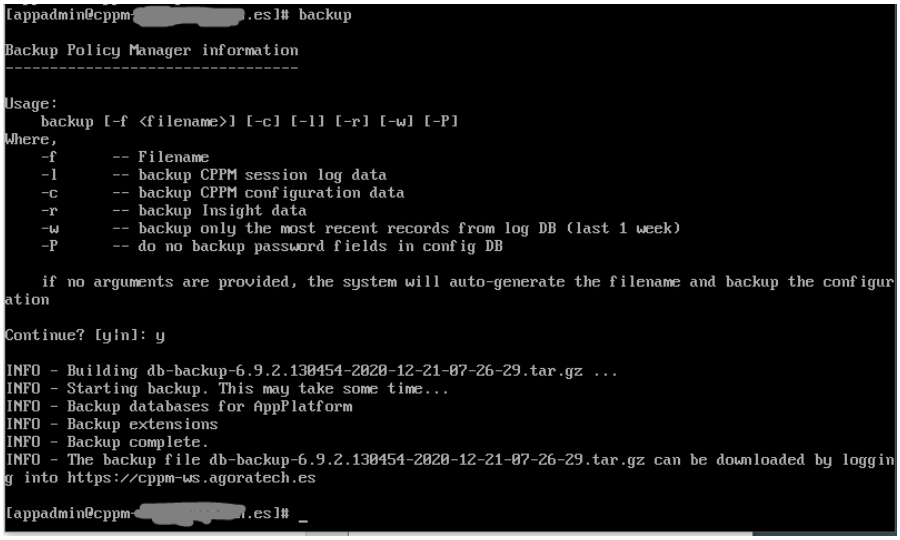


Ilustración 81. Generación de *backup* por línea de comando

241. Tras la generación del *backup*, se puede proceder a su descarga desde *Administration > Server Manager > Local Shared Folders*, seleccionando la opción *Backup files* en el parámetro *Select Folder*.

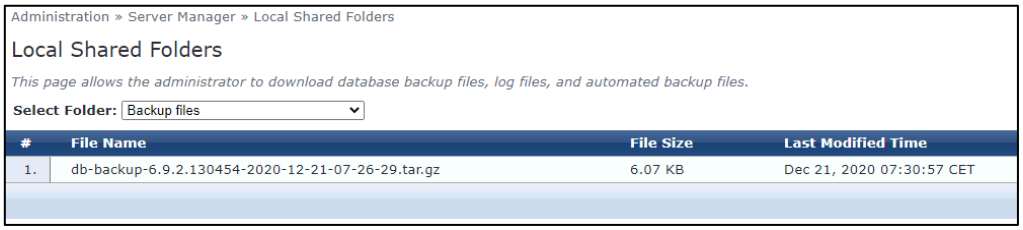


Ilustración 82. Descarga de *backup* generado por línea de comando

6.13.1 PROGRAMACIÓN DE *BACKUPS* CON COPIA A SERVIDOR EXTERNO

242. Desde *Administration > External Servers > File Backup Servers* se puede especificar una ubicación externa para el envío los backups programados. **Se recomienda seleccionar en el apartado *Protocol* la opción *SFTP*, para hacer uso de dicho protocolo seguro.**

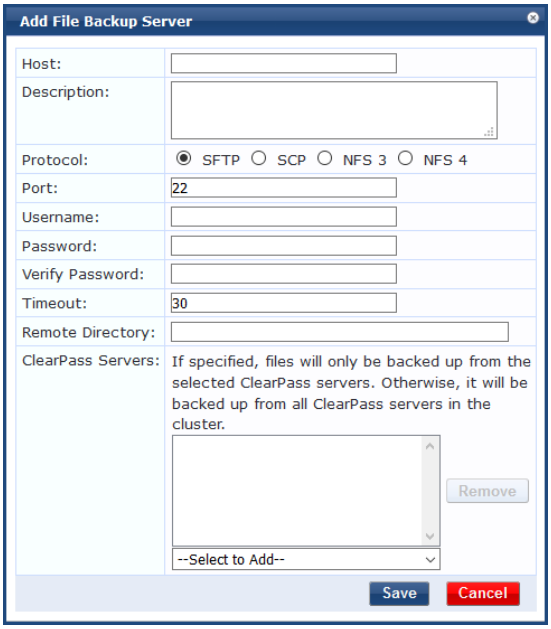


Ilustración 83. Configuración de repositorio para *backup* programados

243. En el caso que configurar el envío de copias a servidores, este se realiza **cada noche**. Este comportamiento se controla desde un parámetro de configuración de *clúster*, seleccionando *Off, Config o Config|SessionInfo,* en función de que se quiera desactivar, copiar sólo la configuración o la configuración y las sesiones registradas. Se accede a dicha configurar desde *Administration > Server Configuration > Cluster Wide Parameters > Database*.

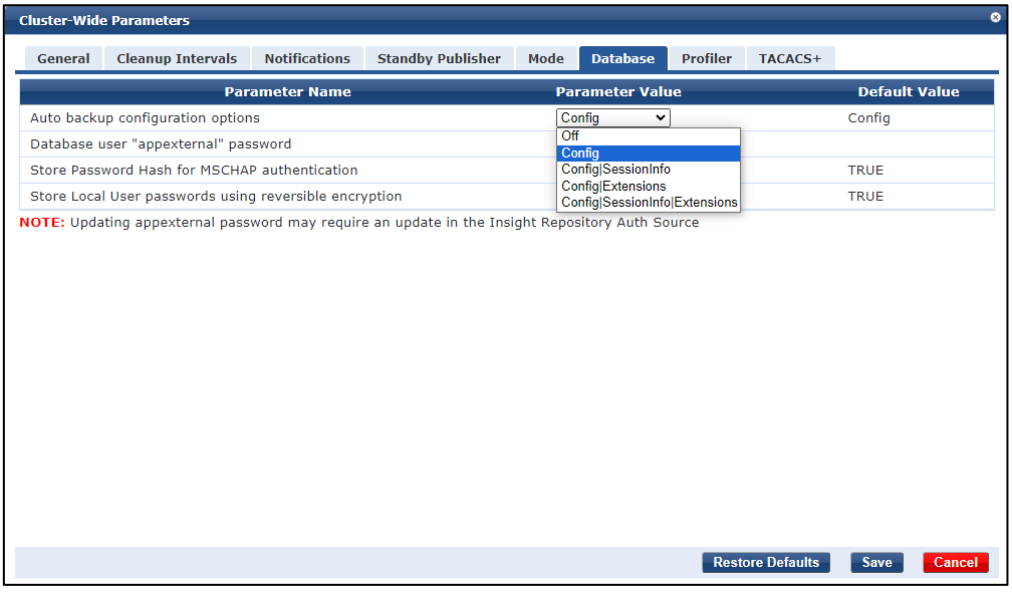


Ilustración 84. Configuración del *backup* automático

6.14 CLEARPASS POLICY MANAGER

244. Como se ha introducido anteriormente, en este módulo se ejecutan todas las configuraciones básicas, configuración del clúster, gestión de las actualizaciones, *backups*, integraciones con sistema y diccionarios RADIUS, entre otros.

245. El motor de gestión de políticas AA y, en general, del resto de funcionalidades se basa en los Servicios de *ClearPass PolicyManager*.

246. Los dispositivos de red u otros sistemas que necesitan servicios de autorización y autenticación consideran a Aruba *ClearPass Policy Manager* como un servidor RADIUS, TACACS+ o como servidor de autenticaciones basado en HTTP/HTTPS. Sin embargo, Aruba proporciona un modelo extensible y variado para ejercer labores de coordinación de la seguridad en la red, convirtiéndole en un orquestador de la seguridad.

247. La funcionalidad para orquestar y organizar todas las peticiones de autorización y/o autenticación viene implementada en la funcionalidad de ***Servicios (Services)*** de ClearPass.

248. Los servicios se organizan en una lista ordenada. Cuando llegan las peticiones a ClearPass, se van enfrentando a cada uno de los servicios para ver si cumplen sus condiciones de ejecución. En caso afirmativo, se procede a ser procesada la petición y ejecutar las acciones previstas. En caso que una petición no pueda ser procesada por ningún servicio, no se atiende y dependiendo se registra en logs.

249. Los servicios de *ClearPass Policy Manager* tienen dos (2) propósitos:

    a) Las reglas de categorización (para cada servicio) permiten a *ClearPass Policy* Manager comparar cada petición recibida con cada uno de los servicios definidos para verificar si cumplen los requisitos de esa regla. Para ello se puede verificar el método de autenticación usado, el equipo que lo genera, la ubicación o cualquier otro atributo.

    b) Mediante el uso de atributos y consultas, ClearPass Policy Manager puede coordinar un conjunto de respuestas, desde la autenticación, evaluación de la salud del terminal, enviar parámetros de vuelta, así como informar a sistemas terceros y disparar acciones en otros sistemas.

250. A la hora de definir los servicios, se puede hacer uso de un asistente que ofrece algunas plantillas preconfiguradas. Estas plantillas permiten la definición no solo del servicio en sí, sino que también crean otras definiciones y objetos en base a la configuración.

251. En el momento que se crean los servicios mediante el asistente, se puede proceder a modificarlos usando la plantilla o manualmente. Si se realiza manualmente (que es lo más habitual) no se puede volver a usar el asistente para configurar ese servicio.

6.14.1 ASISTENTE Y PLANTILLAS DE SERVICIOS

252. Para acceder al asistente en la creación de servicios navegamos a *Configuration > Service Templates & Wildcards***.**

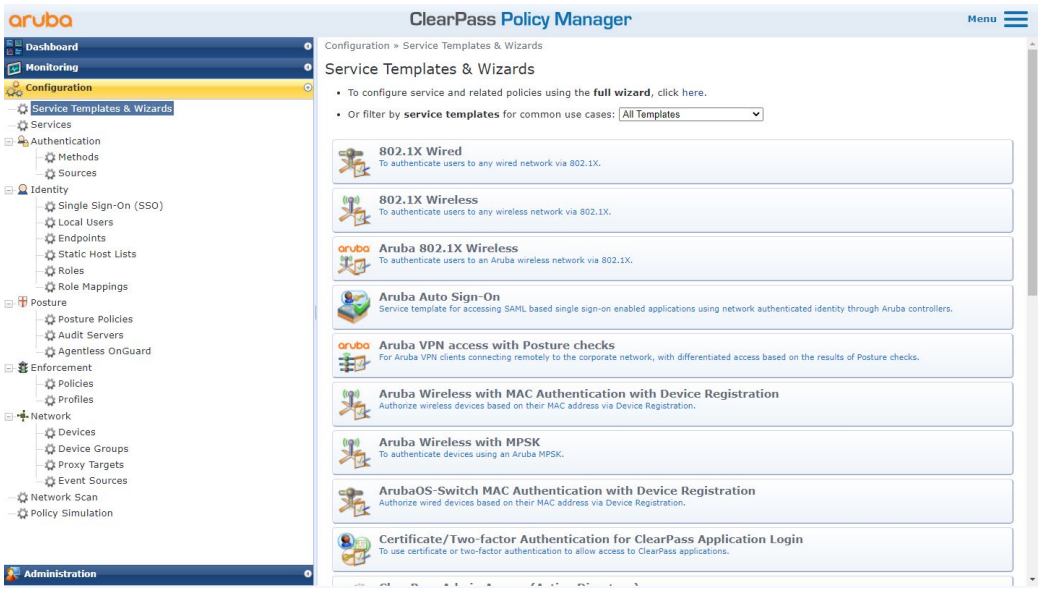


Ilustración 85. Asistentes de configuración de servicios

253. Se pueden consultar las distintas plantillas de servicios predefinidas en el siguiente enlace a la documentación online.

6.14.2 SERVICIOS DE AUTENTICACIÓN Y AUTORIZACIÓN

254. Estos servicios son los más frecuentes. Se utilizan para el control de acceso a la red.

6.14.2.1 TIPO DE SERVICIO Y REGLAS DE SERVICIO

255. Estos servicios están ordenados por prioridades. Cuando llega una petición, se compara progresivamente con los servicios definidos en función a dicha prioridad y se tratará de aplicar el primero posible. Para saber si una petición, debe ser atendida por un servicio se verificará el *Tipo de Servicio* y las *Reglas de Categorización.*

    a) El *Tipo de Servicio* puede ser RADIUS, TACACS, *WebAuth*, *Application* o *Event*.

    b) Las *Reglas de Categorización* pueden filtrar diferentes campos o condiciones de la petición recibida. Por ejemplo, si se quiere distinguir entre peticiones de equipos *Wireless* y *Wired*, se puede utilizar el valor del campo *IETF:Nas-Port-Type* para distinguir las peticiones cableadas (valor 15=*Ethernet*) de las inalámbricas (19=*Wireless*-802.11)

256. El producto permite usar campos de diversas fuentes:

    a) Campos RADIUS estándar incluidos en la petición.

    b) Campos RADIUS propietarios de fabricantes. En *ClearPass* vienen diccionarios de más de 100 fabricantes, pero pueden ser añadidos más

    c) Campos de Autenticación, como *Authe-method*, *username*, *full-username*, y relacionados.

    d) Campos de la conexión (*Connection*) como protocolo, *NAD*, *NAD-IPAddress*, y similares.

    e) Fecha y hora.

f) Datos aprendidos con anterioridad de ese equipo.

257. También se puede diferenciar, dentro de las peticiones de tipo 802.1X, las que vienen de un conjunto de equipos (por ejemplo, un edificio), y tener reglas diferentes durante los días laborales y el fin de semana.

258. Destacar que un servicio puede incorporar múltiples fuentes de autenticación. Un usuario puede ser buscado en diversos directorios, AD y BBDD. De esta forma, un mismo servicio se puede hacer más versátil al consolidar las fuentes.

6.14.2.2 METODOS Y FUENTES DE AUTENTICACIÓN

259. Una vez se ha determinado que una petición debe ser procesada contra una regla en concreto, el siguiente paso es determinar el método de autenticación. En el caso TACACS, como tiene su propio método de autenticación, este paso no está disponible.

260. Dentro del servicio, desde *Configuration > Services*, haciendo clic en *Edit* en el servicio deseado se puede especificar qué métodos serán permitidos para las peticiones que se reciban. Se especificarán en una lista en la que se tiene en cuenta el orden.

Ilustración 86. Definición de un Servicio: selección de fuentes de autorización

261. Los fallos en la categorización se reflejan en *Audit Viewer.*

6.14.2.3 AUTORIZACIÓN

262. En la definición del servicio es posible activar la autorización. En esta etapa de autorización se recogen atributos para después ser usados en la etapa de *role mapping*. En la configuración del servicio se pueden seleccionar las fuentes de autenticación vistas en el apartado **6.2.1.2 FUENTES DE AUTENTICACIÓN**.

263. La configuración de la autorización se realiza desde *Configuration > Services > Edit,* en la pestaña *Authorization.* En este ejemplo, se ha seleccionado como fuentes de *Authorization*, un AD, así como la base de datos de *endpoints*.

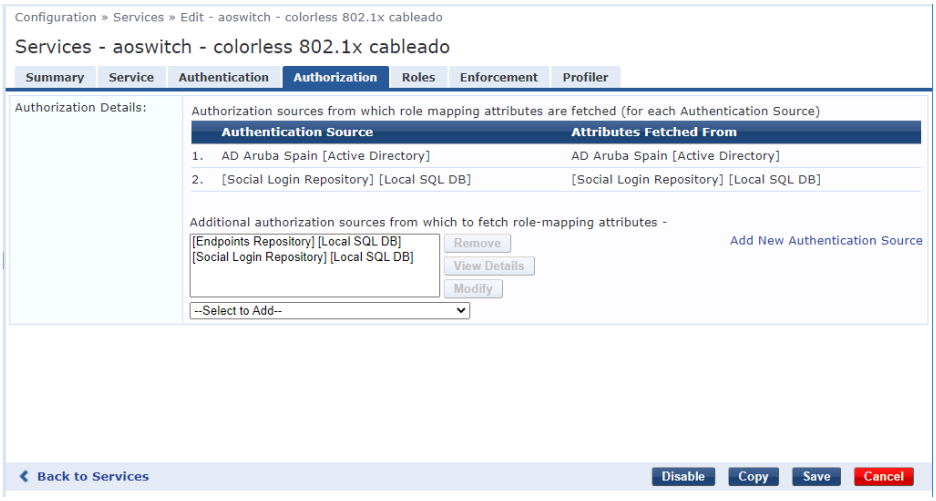


Ilustración 87. Definición de un servicio: selección de fuentes de autorización

6.14.2.4 *ROLE MAPPING*

264. La etapa de *Role Mapping* permite la asignación de ciertas etiquetas o roles en función de la petición recibida y la información que ClearPass extrae de las fuentes de información configuradas. Es una funcionalidad opcional, pero recomendable si se crean políticas muy elaboradas.

265. La asignación de los roles se realiza en base a una lista de condiciones. Se puede establecer que se evalúe toda la lista de condiciones o hasta que la primera condición cumpla. El primer caso proporciona más versatilidad y granularidad.

266. Para el detalle de la configuración de los Roles y las *Role Mapping Policies*, se puede consultar en [REF12].

6.14.2.5 *ENFORCEMENT*

267. El *enforcement* es la parte más importante de la definición del servicio. A partir de los datos de la petición recibida (conexión, usuario, credenciales, dispositivo, etcétera), de la información que se haya podido obtener de las fuentes de autorización y autenticación y de los roles que pueden haber sido asignados en la etapa anterior de *Role Mapping*, se evalúan las condiciones y se ejecutan las acciones.

268. Los dos (2) elementos importantes son:

    a) *Enforcement Policy*: recoge la lógica que se quiere implementar, evaluando una serie de condiciones.

    b) *Enforcement Profiles*: recogen las acciones que se ejecutan como resultado de esas condiciones.

269. Un *Enforcement Profile* es una acción concreta, una instrucción, un comando, como por ejemplo enviar un determinado atributo radius con un valor, hacer una escritura en una BBDD, actualizar un campo del registro de un dispositivo, desconectar una sesión mediante una acción Radius CoA y muchas otras.

270. Los *Enforcement Profile* como acciones básicas, son usados en definiciones posteriores. En particular se usan intensamente en la definición de una *Enforcement Policy*.

271. Por otra parte, una *Enforcement Policy* es la definición de una política, de una lógica que contempla diversos aspectos

    a) Características. Destacamos:

        1. Nombre
        2. Tipo
        3. Acción (*Enforcement Profile*) por defecto
        4. Evaluación de las condiciones: Todas o la primera que cumpla

    b) Reglas: Lista ordenada

        1. Regla: Condición(es) → Acción(es) (*Enforcement Profile*)
        2. Regla: Condición(es) → Acción(es) (*Enforcement Profile*)
        3. ….
        n. Regla: Condición(es) → Acción(es) (*Enforcement Profile*)

272. El caso de uso frecuente, es que los *Enforcement Profile* se asocian a los servicios. Un ejemplo de un *Enforcement Policy* para un servicio de conectividad podría ser este:

    a) Características

        1. Nombre: Servicio Cableado
        2. Tipo RADIUS
        3. Acción (*Enforcement Profile*) por defecto: Enforcement Profile RADIUS REJECT
        4. Evaluación de las condiciones: La primera que cumpla

    b) Reglas: Lista ordenada

        1. Regla: Dispositivo es IPPhone → Enforcement Profile – Enviar Política *teléfono_ip*
        2. Regla: Dispositivo es PC AND está incluido en AD Corporativo AND user es miembro de grupo Usuarios → Enforcement Profile – Enviar Política *corporativo*, Enforcement Profile – Notificar Firewall

6.14.2.5.1 ENFORCEMENT PROFILE

273. Como se ha comentado, los Enforcement Profile son los elementos básicos, acciones básicas, que serán usados en otros objetos y definiciones más complejos. Existen múltiples tipos para proporcionar diferentes tipos de acciones e interacciones con los elementos de red, bases de datos propias de ClearPass así como elementos externos con los que ClearPass se puede integrar.

274. Existen múltiples plantillas de *Enforcement Profile* de tipo Radius, Radius CoA, Agent, CLI, Post_Authentication, Application, HTTP, SNMP y TACACS.

275. Los *Enforcement Profiles* que son de tipo Radius, permiten además seleccionar si van asociados a una acción de *Accept*, *Reject* o *Drop*.

276. Cuando se trata de *Enforcement Profiles* que se envían a los equipos de red, como medida de control y seguridad adicional, también permite seleccionar sobre qué equipos o grupo

de equipos queremos que pueda aplicarse esta acción, mediante la selección de un grupo de dispositivos.

277. Los *Enforcement Profile* no son configuraciones estáticas de un valor, si no que el dato que se desee utilizar puede ser un dato variable, referido a un valor particular en cada petición o contexto. De esta forma son más versátiles.

278. Los *Enforcement Profiles n*o son definiciones cerradas, sino que el administrador puede añadir otros atributos o modificar los existentes. Se ofrece como puntos de partida para arrancar la configuración y no como definiciones cerradas.

279. Tanto la creación, como la modificación de los *Enforcement Profiles*, se puede realizar desde *Configuration > Enforcement > Profiles*. El detalle de configuración de los mismos se puede consultar en el siguiente enlace de la documentación online.

6.14.2.5.2 EJEMPLO DE *ENFORCEMENT PROFILE*

280. El *Enforcement Profile "aosswitch - Rol Teléfono"* manda el atributo *HPE-User-Role* con el valor *Telefono*. Tiene sentido, si en el equipo existe un role definido con ese nombre.

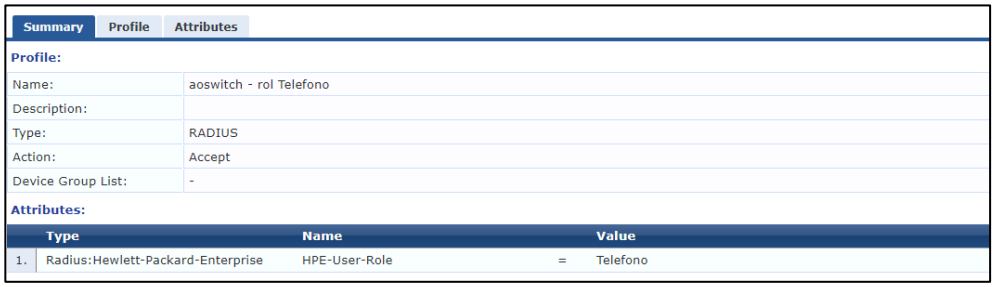


Ilustración 88. Ejemplo de *enforcement profile*

281. A modo de ejemplo, en el caso de un *switch*, si existe una política de usuario llamada "Teléfono" esta sería aplicada a la conexión.

```
policy user "Telefono"
 10 class ipv4 "voice-control-traffic" action rate-limit kbps 100 action dscp af31 action permit
 20 class ipv4 "rt-traffic" action rate-limit kbps 320 action dscp ef action permit
 30 class ipv4 "IP-ANY-ANY" action dscp default action permit
exit
```

282. Este otro *enforcement profile* (Cisco- VLAN Empleado), a continuación, manda el atributo del tipo RADIUS y manda instrucciones a un equipo Cisco para fijar la VLAN 101

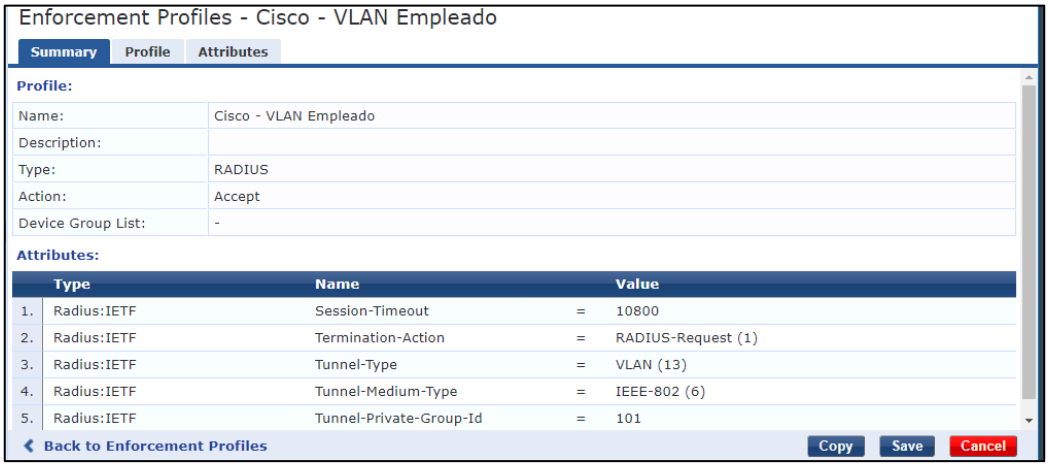


Ilustración 89. Ejemplo de *enforcement profile* – Asignación de múltiples atributos RADIUS

6.14.2.5.3 *ENFORCEMENT PROFILE* TIPO COA

283. Los mensajes de tipo RADIUS CoA son usados para cambios en las condiciones de conexión de los dispositivos. En particular, son muy utilizados los mensajes CoA para terminar una sesión y se ejecutan con diferentes fines. Por ejemplo, al principio de una conexión puede usarse para forzar una reconexión, cambiar al cliente de VLAN y que el cliente adquiera otra IP.

284. También puede hacerse con la sesión ya iniciada, como respuesta a un evento de seguridad, o por decisión del administrador, y realizar algún cambio de contexto de la conexión (VLAN, ACL, *role*). Esto depende de cada modelo de equipo de red.

285. Este tipo de mensajes en muchos casos son diferentes por fabricantes. *ClearPass* tiene predefinidos varios de estos mensajes para varios fabricantes, lo cual resulta muy útil. En general una primitiva de desconexión, requiere de varios datos.

286. Cuando se define un *Enforcement Profile* de tipo *RADIUS Dynamic Authorization*, uno de los datos que se pide es el tipo de plantilla desde la que se desea partir.

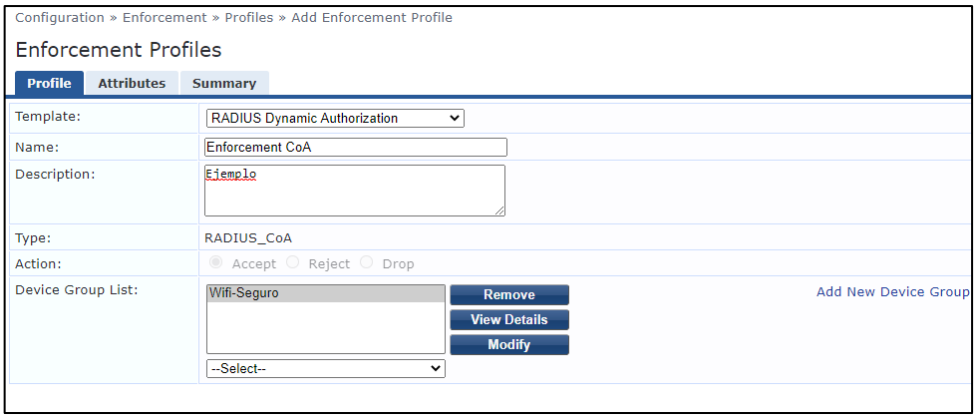


Ilustración 90. Definición de un *Enforcement Profile* tipo RADIUS CoA

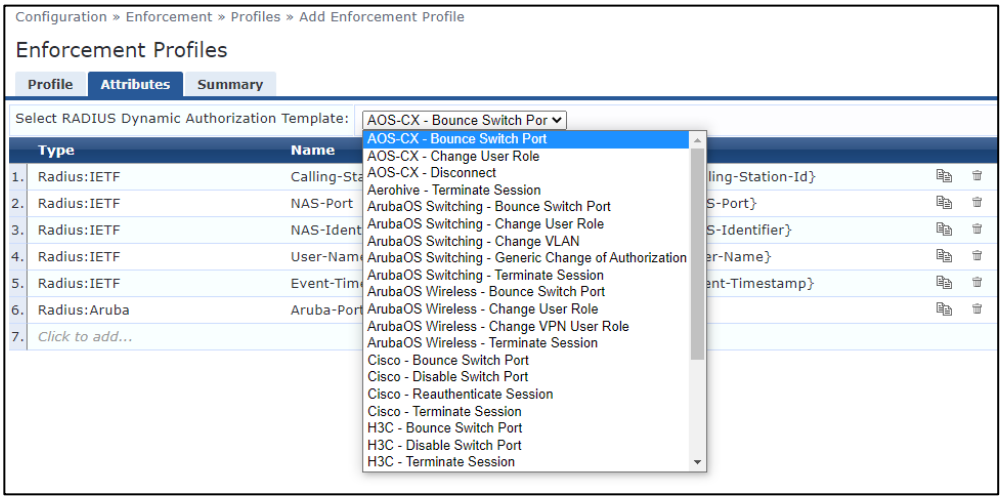


Ilustración 91. *Enforcement Profile* tipo RADIUS CoA – Selección de tipo de atributo

287. El conjunto completo de las plantillas predefinidas, se puede consultar, exportar sus definiciones e importar nuevas desde *Administration > Dictionaries > Radius Dynamic Authorization Templates*.

288. En el caso de tener que realizar una definición para un fabricante del que no se disponga de plantillas, solo hace falta partir de una plantilla, por ejemplo, *IETF – Generic Change of Authorization*, e ir añadiendo los atributos Radius necesarios.

6.14.2.5.4 ENFORCEMENT POLICY

289. Una vez definidos los *Enforcement Profile* necesarios, con los *roles* generados, se procederá a definir la *Enforcement Policy*. Dicho de otra forma, se creará el diagrama de flujo que se quiere seguir para determinar las condiciones de cada conexión.

290. En líneas generales, una *Enforcement Policy* tiene resumidamente esta estructura

    a) Características

        1. Nombre y Descripción
        2. Tipo
        3. Acción (Enforcement Profile) por defecto
        4. Evaluación de las condiciones: Todas o la primera que cumpla

    b) Reglas: Lista ordenada

        1. Regla: Condición(es) → Acción(es) (Enforcement Profile)
        2. Regla: Condición(es) → Acción(es) (Enforcement Profile)
        3. ….
        n. Regla: Condición(es) → Acción(es) (Enforcement Profile)

291. Para definir una *Enforcement Policy,* además de un nombre y una descripción, se debe seleccionar el tipo. Este tipo servirá como condición para ser usado en los diversos tipos de servicios de ClearPass. Los tipos son: RADIUS, TACACS+, *Webauth*, *Application* y *Event*. Esta configuración se lleva a cabo desde *Configuration > Enforcement > Policies.*

292. Los de tipo RADIUS se usan para el control de conexiones. Los de TACACS+ para el control de accesos a las consolas de administración de los equipos. Los de tipo *Webauth* se usan para el control de agentes diversos (*SNMP/Agent/CLI/CoA*). Los de tipo *Application*, regulan el acceso de usuarios y usuarios de aplicación a los diversos módulos de *ClearPass* y los de tipo *Event* regulan el procesado de eventos recibidos de terceros sistemas.

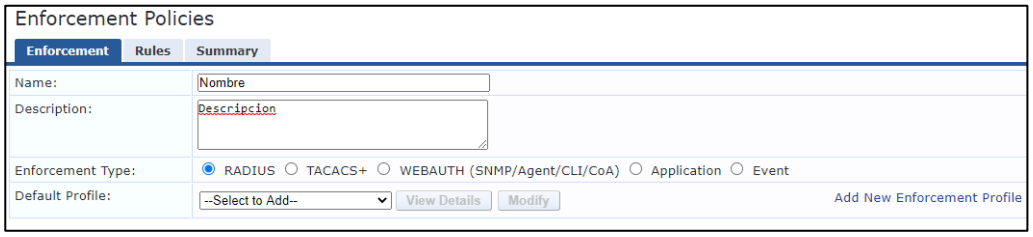


Ilustración 92. Definición de política de *enforcement*: nombre y tipo

293. En todos los casos, se debe seleccionar el *Default Profile*. Se trata de la acción por defecto que se ejecuta en el caso de que ninguna regla se cumpla.

294. Cuando se pasa a la pestaña *Rules*, se tiene la oportunidad de definir muchas condiciones y acciones.

Ilustración 93. Definición de política de *enforcement*: reglas a aplicar.

295. Cuando se añade una regla, aparece una ventana, en la cual se pueden programar las *Condiciones* y las *Acciones*.

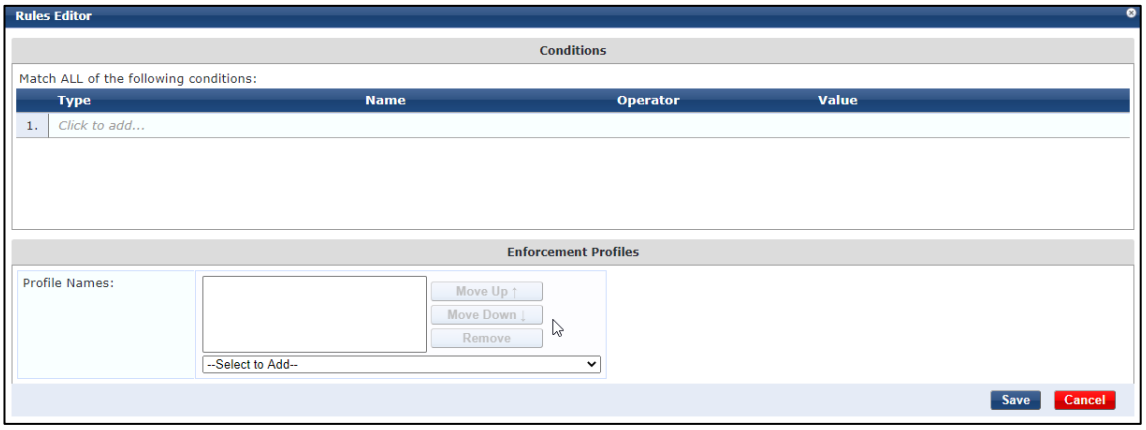


Ilustración 94. Definición de política de enforcement: definición de una regla.

296. Posteriormente, desde *Configuration > Services > Edit,* en la pestaña *Enforcement*, se asocia la *Enforcement Policy* deseada a dicho servicio. Las *Enforcement Policy* siempre se asocian a los Servicios, de forma que indican la lógica a seguir por dicho servicio.

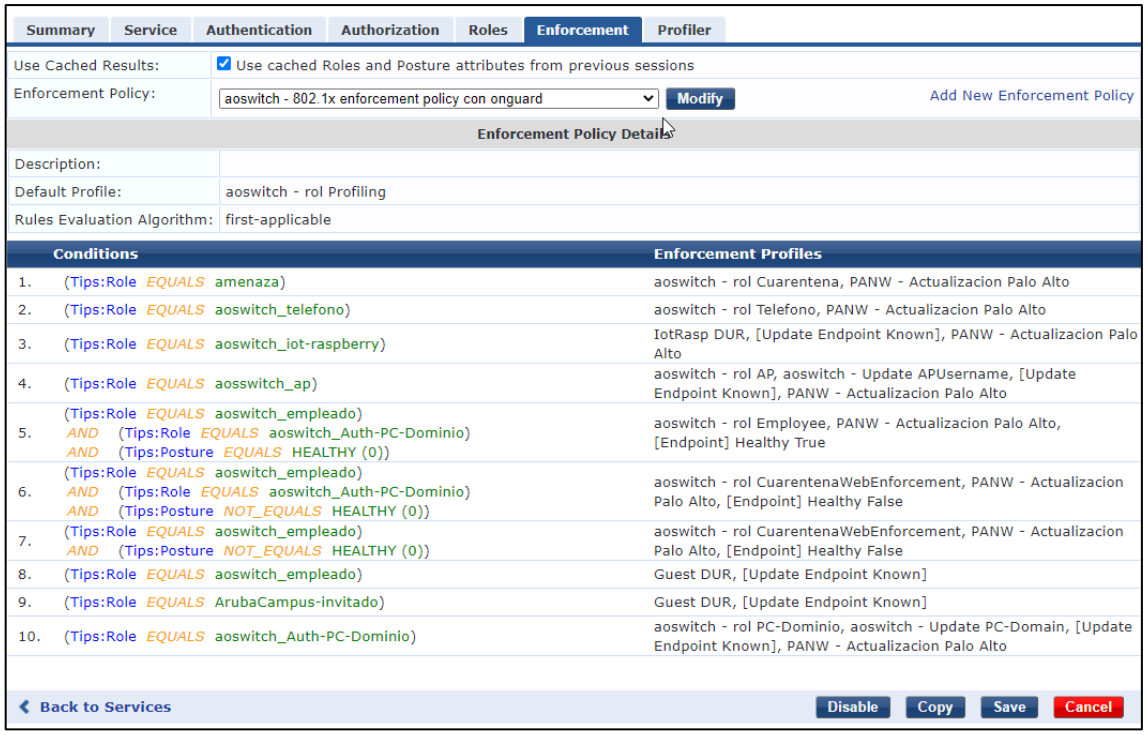


Ilustración 95. Ejemplo de política de *enforcement*

297. En la configuración anterior, se muestra una *Enforcement Policy* ya aplicada en un Servicio. En gran medida, la *Enforcement Policy* implementa la lógica de un servicio.

298. El hecho que las *Enforcement Policy* y los Servicios se definan de forma distinta, es para añadir versatilidad. Ya que permitiría varios servicios que ejecutaran una misma lógica a través de la misma *Enforcement Policy*. Esto podría tener sentido porque diferentes servicios pueden tener diferentes condiciones de ejecución.

299. Continuando con el mismo ejemplo podemos destacar que:

    a) Cuando una petición de conexión cumpla las condiciones de este Servicio, se evaluará la *Enforcement Policy* asociada y no se cumpla ninguna condición se ejecutará el *Enforcement Profile* determinado en *Default Profile*, en este caso *aosswitch - rol Profiling*. Además, la política de evaluación de reglas configurada (parámetro *Rules Evaluation Algorithm*) es que solo se evalúe hasta encontrar una regla que sea aplicable.

    b) La segunda regla, por ejemplo, lanzará la ejecución de dos (2) *Enforcement Profiles* si el role es "*aoswitch*". El primero manda una instrucción a la electrónica para que le aplique el *user-role = Telefono*. Después notifica al firewall. En resumen, en el ejemplo, cuando se conecta un teléfono, se particulariza la política de esta conexión y por otra parte se notifica al firewall del dispositivo, sus datos y role asignado.

6.14.2.6 DEFINICIÓN DE EQUIPOS DE RED Y GRUPOS DE EQUIPOS

300. Es necesario dar de alta en ClearPass los diferentes equipos de red con sus correspondientes credenciales, para que puedan interactuar con ClearPass.

301. Desde *Configuration > Network > Devices,* se configuran las credenciales de equipos. Cuando se da un equipo de alta se muestra la siguiente interfaz.

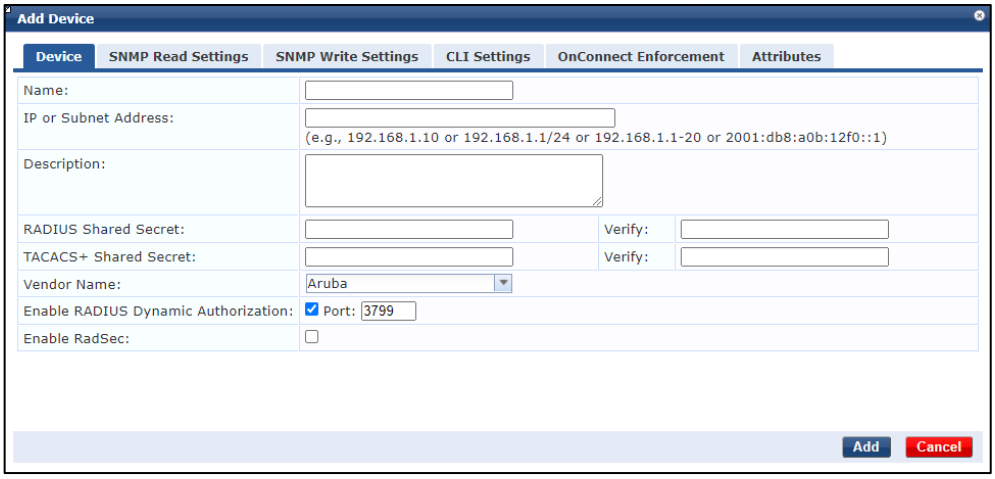


Ilustración 96. Definición de un dispositivo o grupo de dispositivos

302. En la pestaña *Device* se define un nombre para el equipo, o conjunto de equipos. Se introduce la dirección IP, o la de la red. También deben introducirse las credenciales RADIUS, TACACS y seleccionar si soportan o no RADIUS CoA.

303. También se dispone de la posibilidad de interactuar con los equipos vía SNMP (esta opción es usada cuando no soportan 802.1X ni RADIUS). Se pueden introducir credenciales CLI para ejecutar comandos en los equipos de red.

304. **Se recomienda dar de alta únicamente los equipos que se tengan en producción, evitando así dejar IPs autorizadas libres.**

305. **Se recomienda hacer uso de claves RADIUS que cumplan los estándares de complejidad. Las credenciales de los equipos deben almacenarse cifradas.**

306. En *Configuración > Network > Devices Groups* se pueden definir los conjuntos de equipos. Los grupos de dispositivos son un método de categorización de servicios, que permiten distinguir qué servicio (y por tanto qué políticas) se quiere aplicar a un determinado grupo de equipos. Permite, por ejemplo, distinguir entre cableado e inalámbrico, o entre equipos de la sede principal y oficinas remotas.

6.14.3 FUNCIONALIDADES DE NAC: VALIDACIÓN DE LA SALUD DEL TERMINAL (POSTURE)

307. Aruba ClearPass ofrece la funcionalidad de evaluación de la salud de dispositivos. Esta funcionalidad se basa en el uso de un agente *OnGuard* que, además de informar del estado, permite mitigar mediante la remediación e incluso ejecutar *scripts* en los terminales.

308. Actualmente esta funcionalidad está soportada para terminales tipo PC o servidor, de los sistemas operativos *Windows, Apple* y *Linux* (algunas distribuciones).

309. Su implementación se divide en tres (3) partes:

a) Creación de las políticas de evaluación del estado del terminal o *Posture*.

b) Configuración de los aspectos relacionados con los agentes *OnGuard* o *plug-ins*.

c) Definición de los servicios en ClearPass que permita reaccionar ante las notificaciones enviadas por el agente.

6.14.3.1 POSTURE POLICY PLUG-IN

310. ClearPass Policy Manager soporta cuatro (4) tipos de agentes para Windows, uno (1) para Linux y uno (1) para Mac OS. El administrador puede configurar qué tipo de *plugins* ejecuta y qué reglas deben evaluarse en cada caso.

311. Para aquellos otros tipos de dispositivos que no soporten la instalación de un *plugin ClearPass*, se permite recibir información de los terminales por servidores de auditoría de *profiling*, cómo servidores en NMPA, NESSUS *o ClearPass Device Inside*.

312. La definición de políticas asociadas a la salud de los dispositivos se configura desde *Configuration > Posture > Posture Policies*.

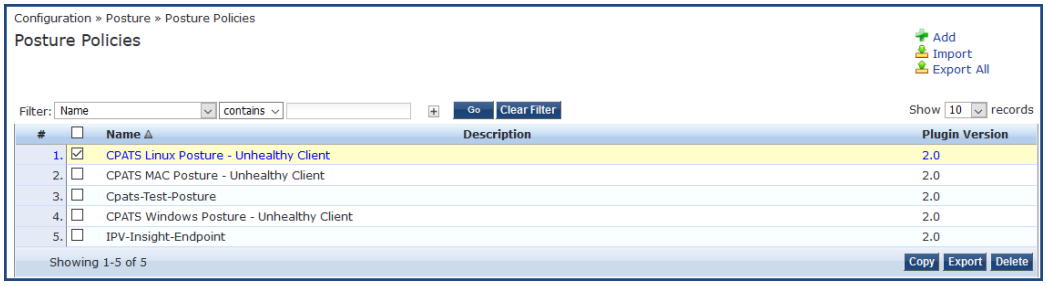


Ilustración 97. Políticas de salud de los dispositivos

313. Para definir una política nueva hacer clic en *+Add*.

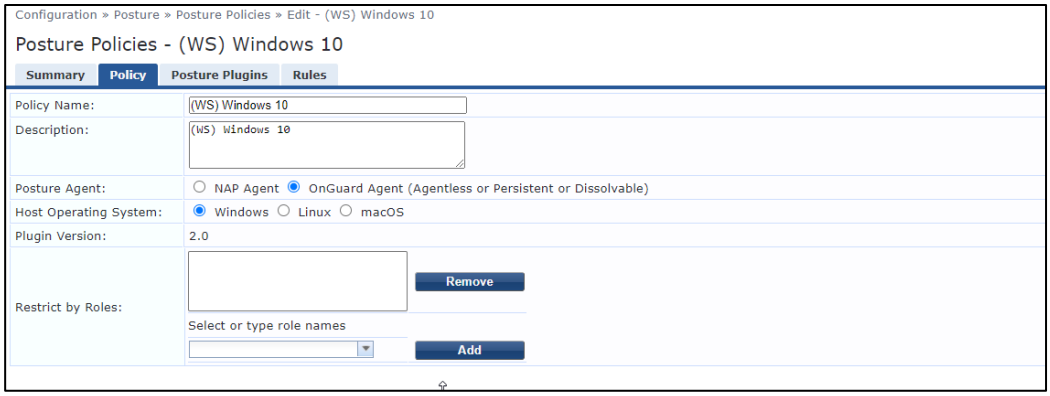


Ilustración 98. Creación de una política de salud del estado de los dispositivos

314. Se elige el tipo de agente. Se puede hacer uso de un agente NAP de Windows o del Agente de *ClearPass OnGuard*.

a) Cuando se selecciona el agente NAP puede hacer uso de:

1. *Windows System Health Validator*. En este caso únicamente se verifica el tipo de sistema operativo y un determinado *Service Pack de Windows*.

2. *Windows Security Health Validator*. En este caso se verifica si están arrancados los siguientes servicios de seguridad: cortafuegos, *Virus Protection, Spyware Protection, Automatic Updates y Security Updates.*

b) Con el agente OnGuard se puede evaluar elementos:

1. Windows: *Services, Processes, Registry Keys, AntiVirus. Patch Management, Firewall, Peer to Peer, Windows HotFixes, USB Devices, Virtual Machines, Network Connections, Disk Encryption, Installed Applications* y *File Check*.
2. MAC OS: *Services, Processes, AntiVirus, Firewall, Patch Management, Peer-to-Peer, USB Devices, Virtual Machines, Network Connections, Disk Encryption, Installed Applications* y *File Check.*
3. Linux: *Services, Antivirus* y scripts personalizados.

315. En el caso de Windows además de poder seleccionar el sistema operativo que se permite o no, se puede definir políticas diferentes por sistema operativo.

316. En función al cumplimiento de las condiciones configuradas, se asigna un valor al token de *posture*. Los token posibles son:

a) *Healthy*

b) *CheckUp*

c) *Transition*

d) *Infected*

e) *Quarentine*

f) *Unknown*

317. Para el detalle de configuración de *Posture Policies Plug-in*, consultar el siguiente enlace de la documentación online.

6.14.3.2 ASPECTOS DEL AGENTE ONGUARD

318. Existen tres (3) modalidades para la ejecución del agente *OnGuard*:

a) Sin Agente (*Agentless*)

b) Agente soluble

c) Agente persistente

319. El agente soluble es la modalidad que descarga el binario mediante navegación. No obstante, las recientes mejoras para protección de los navegadores implican que esta opción requiere una instalación similar al agente pesado.

320. **La opción recomendada es el agente persistente debido a que se obtienen las mejores prestaciones de la solución, tanto para el usuario final, como para el administrador.**

321. La modalidad *agentless* o sin agente local instalado se basa en una ejecución en red del proceso. Consultar el manual del producto para configurar esta opción.

322. En *Administration > Agents and Software Updates > OnGuard Settings* se ofrecen las opciones relacionadas con los agentes

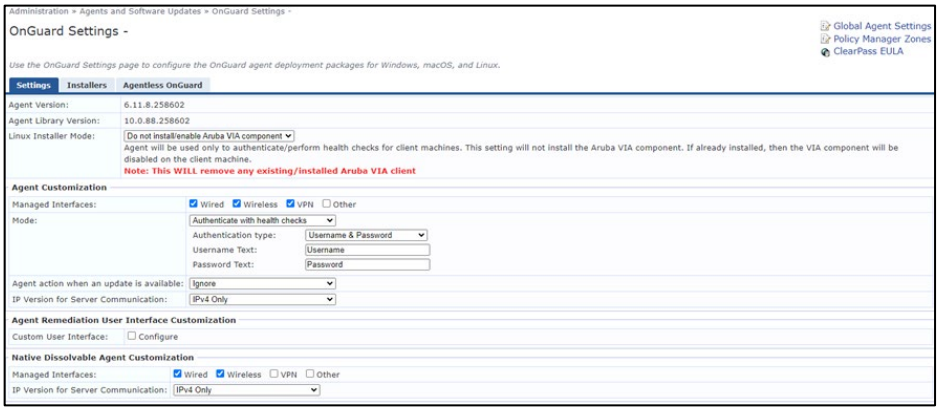


Ilustración 99. Ajustes del agente *OnGuard*

323. En la pestaña de ajustes (*Settings*) se puede determinar para qué tipos de interfaces debe ejecutarse el agente. También se determina si se va a requerir autenticación ejecutada desde el agente, así como si se debe actualizar automáticamente o no el agente.

324. ClearPass implementa recursos web a los que poder redirigir al usuario para remediar la situación que ha derivado en un incumplimiento de la política.

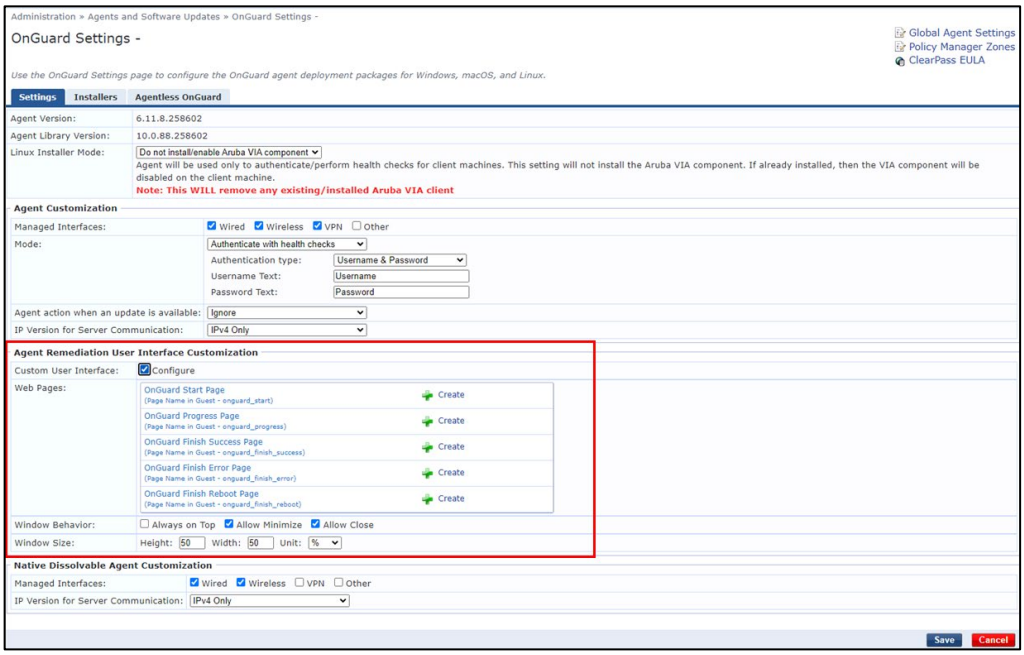


Ilustración 100. Ajustes del agente *OnGuard* – Webs de interfaz con el usuario

325. En la pestaña *Installers* se muestra información de los distintos binarios disponibles en el sistema:

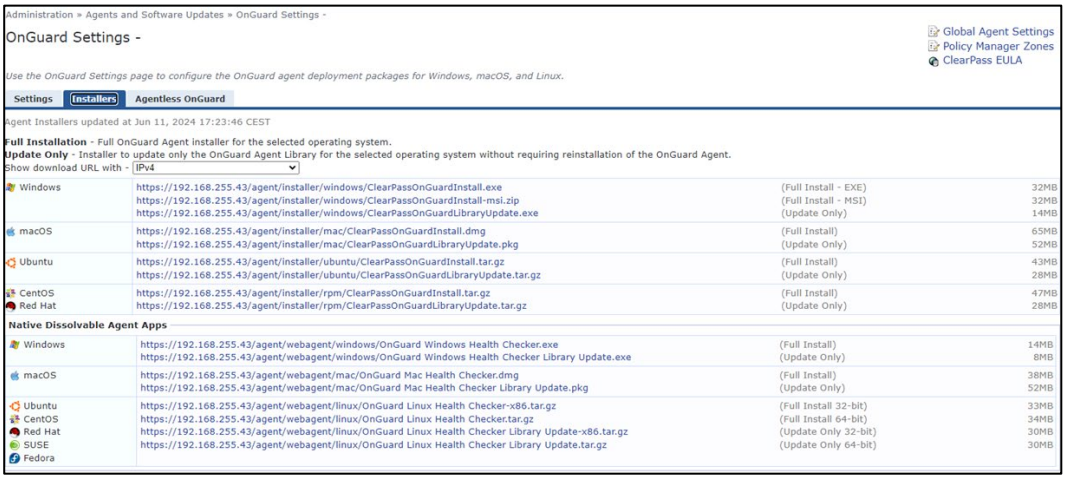


Ilustración 101. Acceso a los agentes *OnGuard*

326. Las URLs mostradas son URLs de descargar de binarios. Dichos binerios llevan la información de los datos de los servidores ClearPass, por lo que no hay que configurar nada en los terminales.

327. En la pestaña *Agentless OnGuard*, se puede acceder a los binarios para su distribución. Esta opción sólo está disponible para Windows.

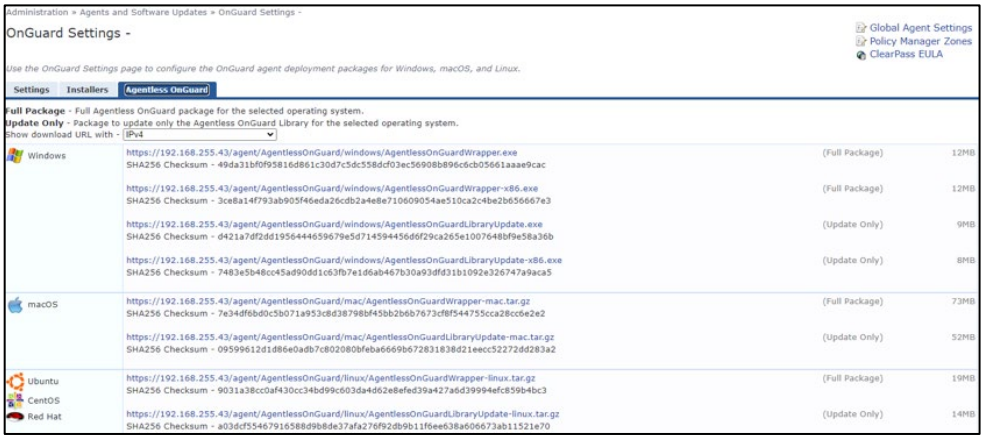


Ilustración 102. Ejecutables *Agentless OnGuard*

328. En [REF13] se detallan las diferencias entre los tres (3) tipos de agentes.

6.14.3.3 FUNCIONALIDAD DE *ONGUARD* EN LOS SERVICIOS DE CLEARPASS

329. En las secciones anteriores se ha descrito cómo generar políticas de salud, así como aspectos relacionados con los agentes y sus tipos. Faltaría conectar la información que genera el agente con ClearPass.

330. El Agente *OnGuard* se comunica, por defecto, con ClearPass mediante notificaciones HTTPS y este se ejecuta cuando hay cambios de estado en las interfaces de red.

331. Estas notificaciones se reciben y se procesan en la parte de servicios de ClearPass, por lo que es necesario decidir qué debe hacer y cómo debe reaccionar ante las notificaciones recibidas.

332. Se utiliza un ejemplo para facilitar la compresión del funcionamiento. Se supone que una organización quiere establecer una política en sus terminales, como condición previa a poder acceder a los servidores internos de la compañía.

333. En primer lugar, se crea un servicio de conexiones 802.1X:

    a) Si el PC tiene asignado el token *HEALTHY*, se asignan los permisos *Saludable.*

    b) Si el PC tiene asignado el token *QUARENTINE*, se asignan los permisos *Cuarentena.*

    c) Si el PC tiene cualquier otro token, se asignan los permisos *Validación,* lo que permite:

        1. Obtener una IP.
        2. Establecer conectividad en VLAN aislada, pero con acceso a *ClearPass*.
        3. Se le deja conectado hasta que *OnGuard* se ejecuta y notifica a ClearPass su estado.

334. El servicio podría tener este aspecto, en la configuración de *enforcement*:

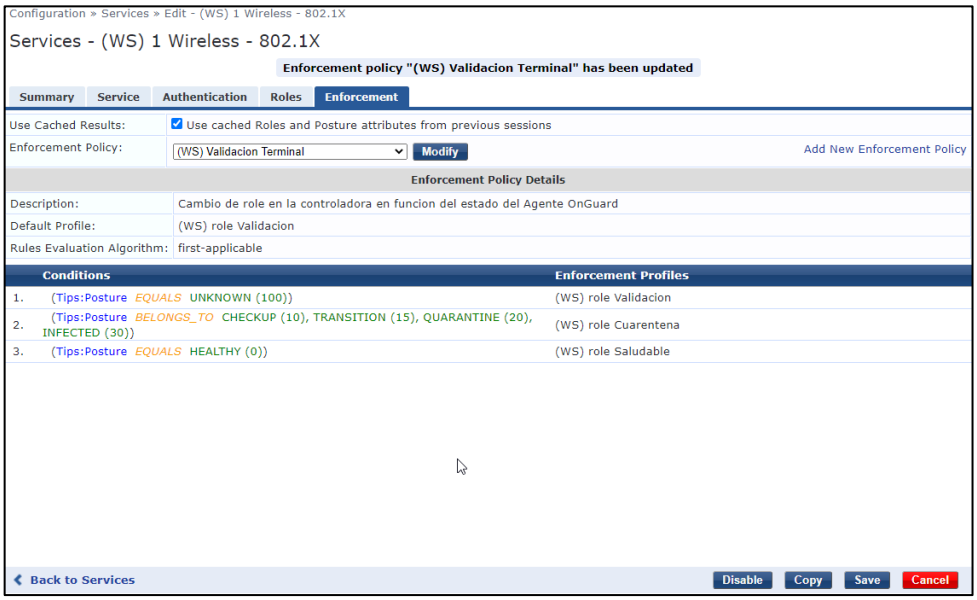


Ilustración 103. Ejemplo de servicio con evaluación de estado de terminal

335. En condiciones normales, la primera vez que se conecte un terminal, no se dispone de información del terminal por lo que se le asignarán los permisos 'Validación'. En ese estado se espera a que el agente se ejecute y se comunique con *ClearPass* (esto suele llevar unos segundos).

336. Se recomienda seleccionar la siguiente opción *de "Use cached Roles and Posture attributes from previous sessions"*, para mantener la información de los dispositivos entre sesiones.

337. En función de cada fabricante de equipos de electrónica de red, la implementación de los permisos *Saludable, Validación* o *Cuarentena* puede diferir. En algunos casos, vía RADIUS, se puede mandar una referencia de una política local (como es el caso de Aruba). En otros casos, se deberá mandar la información por partes.

338. Para configurar un servicio, se debe acceder a *Configuration > Services* y hacer clic en +Add. Se selecciona el tipo de servicio deseado y se asigna nombre y descripción. Se selecciona *Posture Compliance* y aparecerá la pestaña *Posture.*

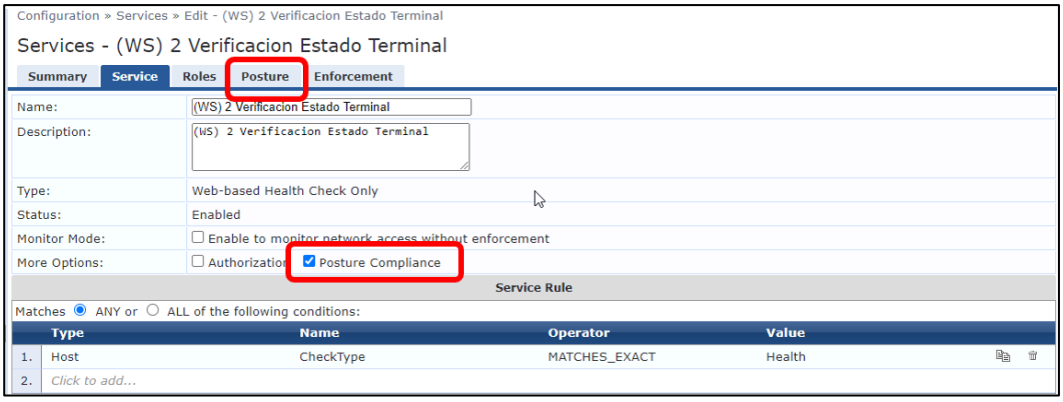


Ilustración 104. Detalle de pestaña *Posture* cuando se selecciona la opción *Posture Compliance*

339. Se seleccionan las *Posture Policies* que sean de aplicación para el servicio y el token por defecto.

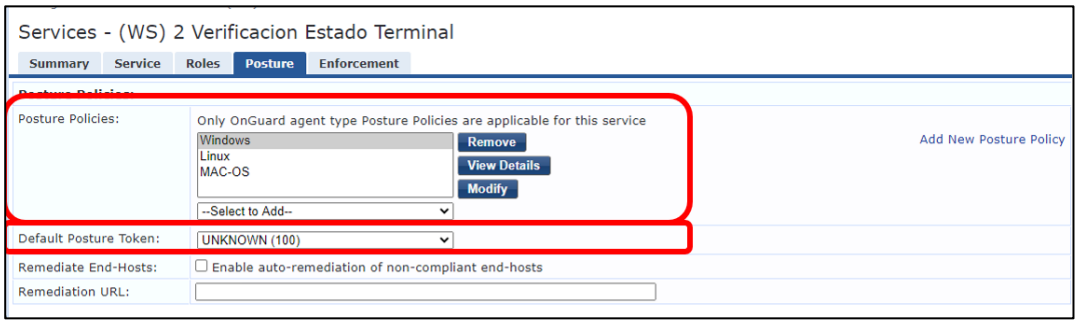


Ilustración 105. Definición de servicio - Selección del tipo de política y evaluación por omisión

340. Por último, en la pestaña de *Enforcement*, se selecciona el *Enforcement Profile* que será de aplicación para el servicio:

Ilustración 106. Definición de servicio - Selección del tipo del *enforcement profile*

6.15 SERVICIOS DE SEGURIDAD

6.15.1 SERVICIOS CON FUNCIONALIDADES DE *PROFILING*

341. *Policy Manager Device Profiler* es un módulo de *Policy Manager* que clasifica automáticamente los dispositivos finales utilizando atributos. Dicho módulo asocia un dispositivo con un usuario o ubicación específicos y ofrece una forma eficiente y precisa de diferenciar el acceso que se proporciona a cada terminal (por ejemplo, un ordenador portátil o una *tablet*).

342. La creación de perfiles de dispositivos permite recopilar información sobre el tipo de dispositivo y el sistema operativo mediante la inspección de los paquetes que envían estos dispositivos en la red.

343. La información recopilada se muestra en el *EndPoint Profiler*.

344. Cuando se conecta un dispositivo nuevo, ClearPass tarda un tiempo en ejecutar el *profiling*. Una vez que se produce, se puede ejecutar una acción RADIUS CoA, para hacer uso de esa información que se ha obtenido.

345. Una buena práctica consiste en asignar permisos restrictivos a dispositivos desconocidos. A continuación, cuando se ha categorizado y se dispone de información, se puede provocar la reconexión en base a la información concreta obtenida del dispositivo.

346. Los métodos que se usan pueden ser activos o pasivos, en función del papel que ejerce ClearPass.

    a) Entre los métodos pasivos, destaca la categorización de las MACs, la información DHCP (mediante *dhcp-relay* de la electrónica hacia los servidores de ClearPass) e información de HTTP y TCP (requiere reenvío de tráfico obtenido por *mirroring*).

    b) Entre los métodos activos, destacamos escaneos de subredes mediante credenciales SSH, SNMP y WMI, así como análisis *NMap* de los terminales.

347. A continuación, se muestra un ejemplo:

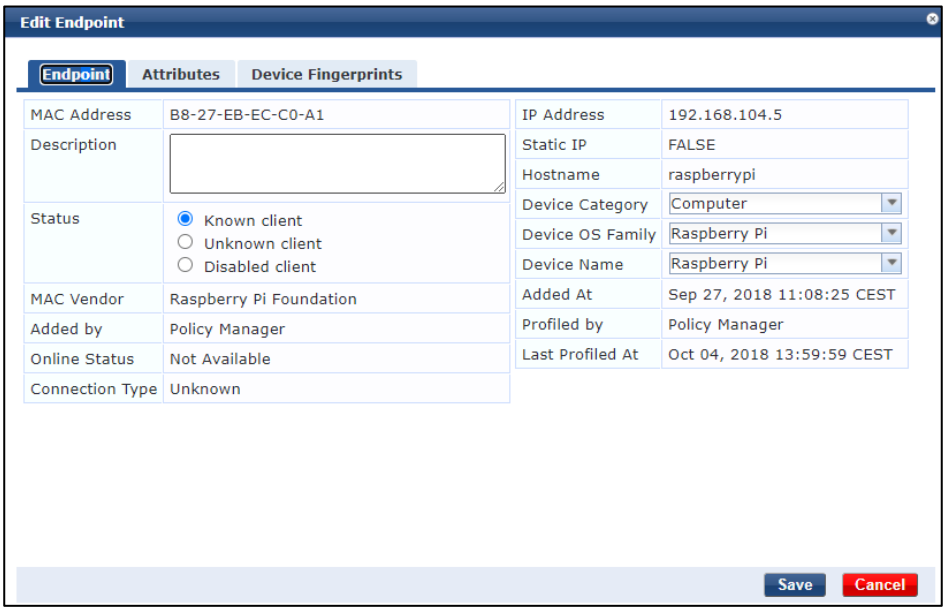


Ilustración 107. Información recopilada de un dispositivo - *Endpoint*

348. Se observa que se trata de un terminal *RaspBerry Pi*. Además de esa información, en la pestaña *Device Fingerprints,* se muestra la información recopilada y que ha sido la base para la categorización:

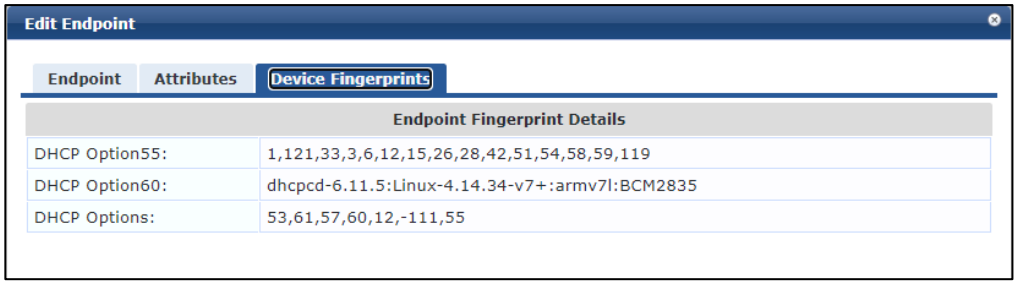


Ilustración 108. Información recopilada de un dispositivo – *Fingerprints*

349. Para configurar esta funcionalidad se debe, en el servicio que se quiera poner en marcha, seleccionar la opción *Profile EndPoints* de la pestaña *Profiler*.

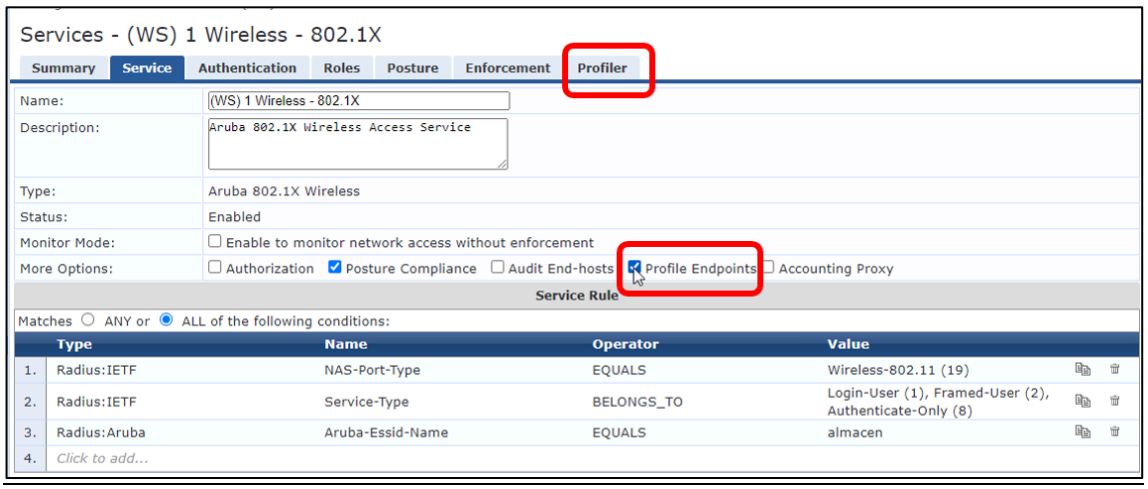


Ilustración 109. Pestaña *Profiler* de un servicio

350. Al seleccionar la pestaña *Profiler*, se debe seleccionar el tipo de dispositivo cuya conexión lanzaría la ejecución de un *Enforcement Profile* de tipo CoA.

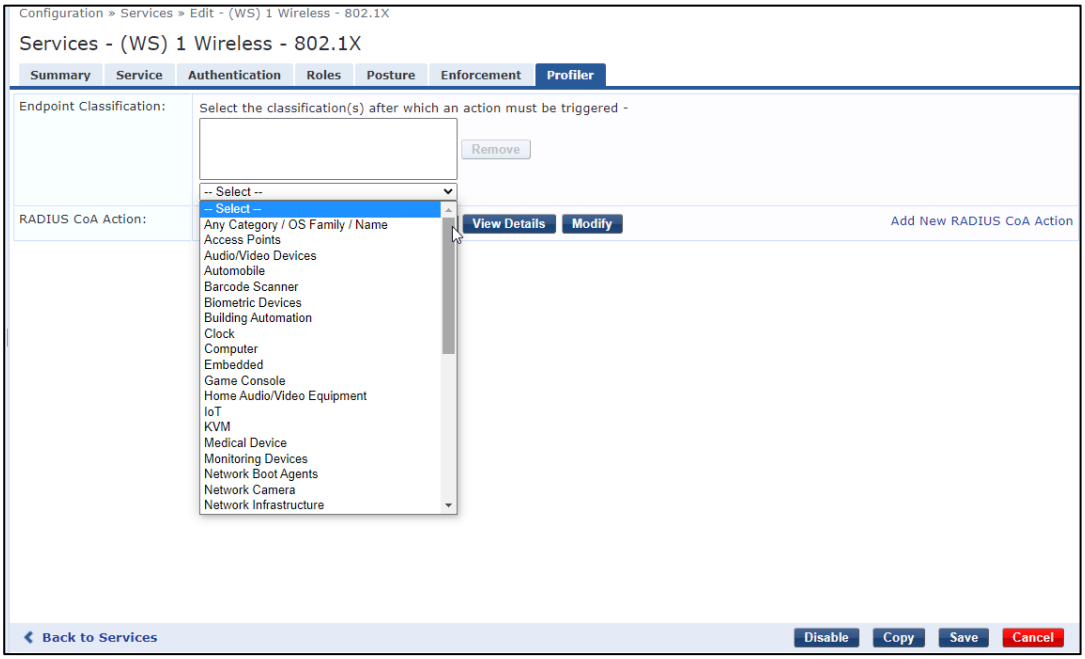


Ilustración 110. *Profiler* – Seleccionar el tipo de dispositivo que disparará la acción

351. Existen diversas posibilidades de seleccionar dispositivos. Por ejemplo, si se quiere configurar una acción cuando se descubra un *smartDevice*, proyector o equipo de audio/video:

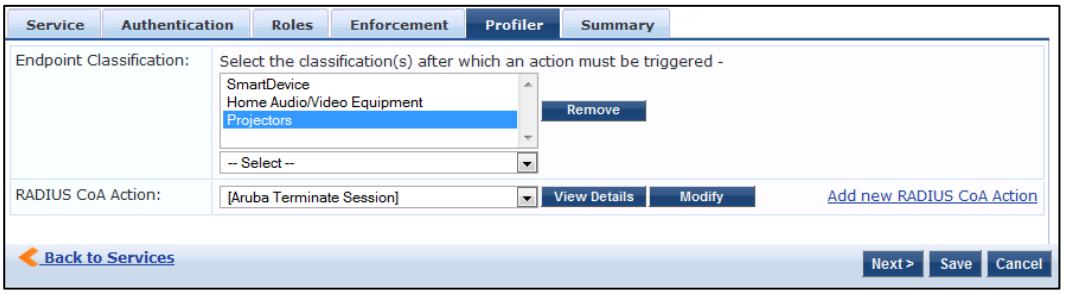


Ilustración 111. Ejemplo *Profiler* con tres tipos de dispositivos

6.15.2 ARUBA *CLEARPASS ON-BOARD*: AUTOREGISTRO DE DISPOSITIVOS

352. El autoprovisionamiento u *Onboarding* es el proceso de preparar un dispositivo para su uso en una red corporativa mediante la creación de las credenciales de acceso adecuadas y la configuración de los parámetros de conexión de red.

353. *ClearPass Onboard* automatiza la configuración y el aprovisionamiento de 802.1X en los terminales. Permite plataformar, instalar credenciales seguras corporativas y distinguir con precisión dispositivos corporativos de otros que no lo sean.

354. Puede usarse para redes cableadas también, aunque su ámbito natural son los terminales móviles y las redes wifi.

355. *ClearPass Onboard* incluye las siguientes características clave:

    a) Configuración automática de la configuración de red para terminales cableados e inalámbricos.

b) Aprovisionamiento de credenciales de dispositivo únicas tanto para dispositivos BYOD como para corporativos.

c) Soporte para dispositivos Windows, *macOS*, *iOS*, *iPadOS* y *Android.*

d) Capacidad de revocar credenciales únicas en el dispositivo de un usuario específico.

e) *ClearPass Profiler* para identificar el tipo, fabricante y modelo de dispositivo.

356. *ClearPass OnBoard* está diseñado para que el proceso pueda ser iniciado por el usuario final, mediante interacción con un portal dedicado a tal fin.

357. Un elemento relevante de esta funcionalidad es que ClearPass participa activamente en la generación de certificados para cada uno de los terminales.

358. *ClearPass*, por tanto, proporciona una plataforma para el control de la identidad de dispositivos, sin tener que delegar en tareas de descubrimiento o detección. El detalle sobre las funcionalidades ofrecidas por *OnBoard* se puede consultar en el siguiente enlace.

6.15.2.1 CONFIGURACIÓN ONBOARD

359. Los pasos necesarios y el detalle sobre la configuración de *OnBoard* se puede consultar en [REF14].

6.15.2.2 CONFIGURACIÓN ONBOARD DE FORMA SEGURA

360. Esta funcionalidad hace uso de https. Se recomienda que se disponga de un certificado SSL de clave pública con CAs de buena reputación. En caso contrario los terminales pueden llegar a repudiar el proceso de OnBoard.

361. Teniendo en cuenta el escenario Wireless, **se recomienda el modelo de funcionamiento de doble SSID.** Este modelo se basa en que un SSID se dedica a la provisión del terminal mientras que el otro es el que se configura para el acceso a la red. Este segundo se configura de forma transparente al usuario.

362. **Se debe configurar OCSP para la validación de los certificados. De esta forma, la revocación de un certificado tendrá un efecto inmediato sobre el terminal afectado.**

6.15.3 *ARUBA CLEARPASS INSIGHT*

6.15.3.1 INTRODUCCIÓN

363. *Policy Manager Insight* es un módulo de *ClearPass Policy Manager* que es capaz de agregar datos de varios servidores *Policy Manager* que contienen registros de acceso a la red. Genera informes y realiza ciertas tareas de mantenimiento y purga de la base de datos.

364. Los "*widgets*" personalizables permiten ver los tipos específicos de información necesaria para monitorizar y comprender lo que está ocurriendo en la red. Puede crear paneles personalizados para visualizar registros de autenticación detallados, pistas de auditoría y detalles sobre tendencias de acceso a la red.

365. La función *Insight Search* permite buscar clientes, usuarios, servidores de *Policy Manager* y dispositivos de acceso a la red.

366. Los informes personalizados analizan la información de autenticación, la creación de perfiles de dispositivos, el estado del cliente, las licencias y los datos de postura, así como los casos de uso de invitados y *OnBoard*.

367. La configuración de alertas permite recibir mensajes casi en tiempo real sobre la actividad anómala de la red. Las alertas se pueden enviar por SMS o por correo electrónico a varios destinatarios.

368. *Insight* debe ser activado ya que no viene activado por defecto. Esto se hace desde *Administration > Server Manager > Server Configuration.*

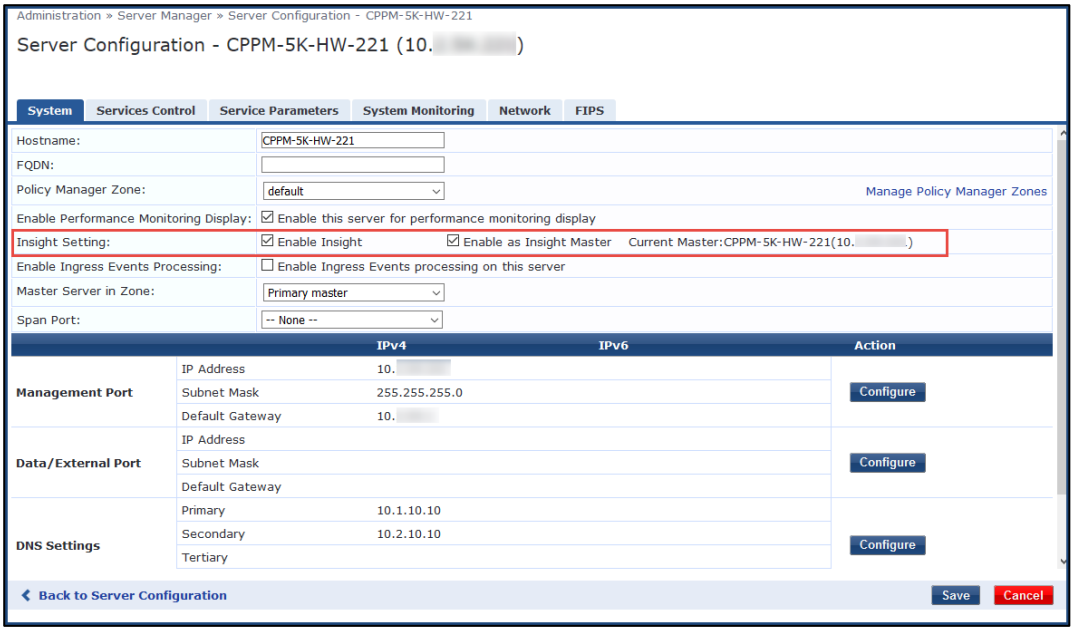


Ilustración 112. Activación de *Aruba ClearPass Insight*

6.15.3.2 ASPECTOS DE SEGURIDAD *CLEARPASS INSIGHT*

369. Las transferencias de ficheros a sistemas externos, se hacen mediante SCP o SFTP. **Sin embargo, se recomienda la utilización de SFTP.**

370. El detalle sobre la configuración de *ClearPass Insight* se puede consultar en [REF15].

6.15.4 OCSP

6.15.4.1 OPCIONES DE OCSP

371. Para configurar OCSP, se debe acceder a *Administration > Server Manager > Server Configuration > Se selecciona servidor > Service Parameters.*

372. La configuración segura que se debe aplicar es la siguiente:

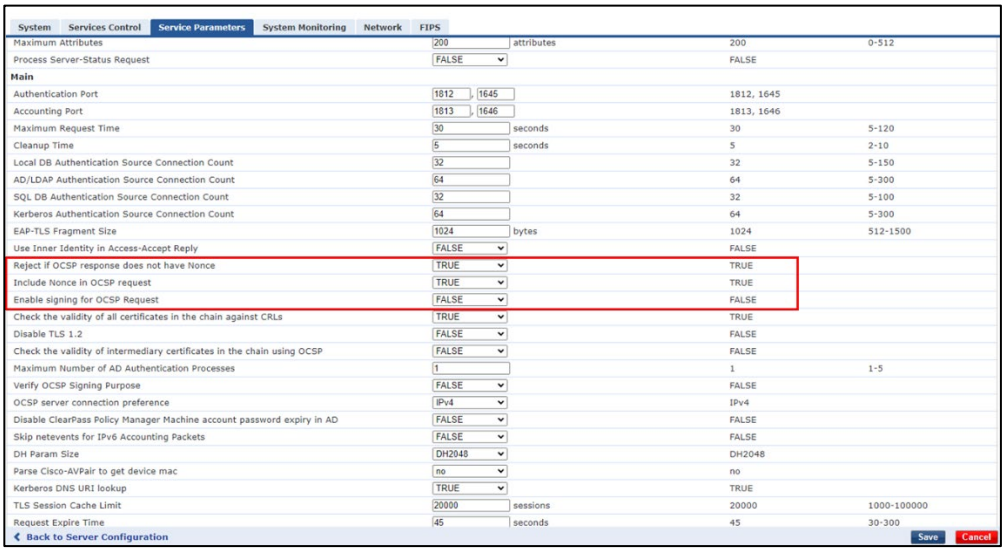


Ilustración 113. Configuración OCSP recomendada

373. ***Reject if OCSP response does not have nonce***. Si el servidor OCSP no soporta la opción *nonce* entonces se debe configurar este valor a FALSE, para evitar un fallo de autenticación en EAP-TLS. *Nonce* es un valor criptográfico que es usado para protegerse de ataques de replicación de peticiones.

374. ***Include Nonce in OCSP request***. Si el servidor OCSP no admite nonce, configure este valor como FALSO para evitar un error de autenticación EAP-TLS. Un nonce es un valor criptográfico aleatorio que se utiliza para proteger contra ataques de grabación y reproducción.

375. ***Enable Signing for OCSP Requests***. Con esta opción habilitada, ClearPass firmará las peticiones OCSP que haga con el certificado del servidor Radius. Este parámetro por defecto se encuentra con valor FALSE, lo que deshabilita el proceso de firma. Se debe activar para verificar la integridad del mensaje y la identidad del remitente.

6.15.4.2 OCSP *SERVER FAIL-OPEN TO CRL*

376. Para autenticaciones EAP-TLS, si el servidor OCSP no está accesible para realizar la validación del certificado ClearPass, se podría validar el estado del certificado contra una CRL, como mecanismo de respaldo.

377. Esta opción se configura, modificando o creando un método de autenticación. Un caso típico sería, modificar el predefinido en el sistema, para usar con EAP-TLS con OCSP.

378. En *Configuration > Authentication > Methods* nos muestra la lista de métodos definidos. Existe un método predefinido llamado *[EAP TLS With OCSP Enabled]*.

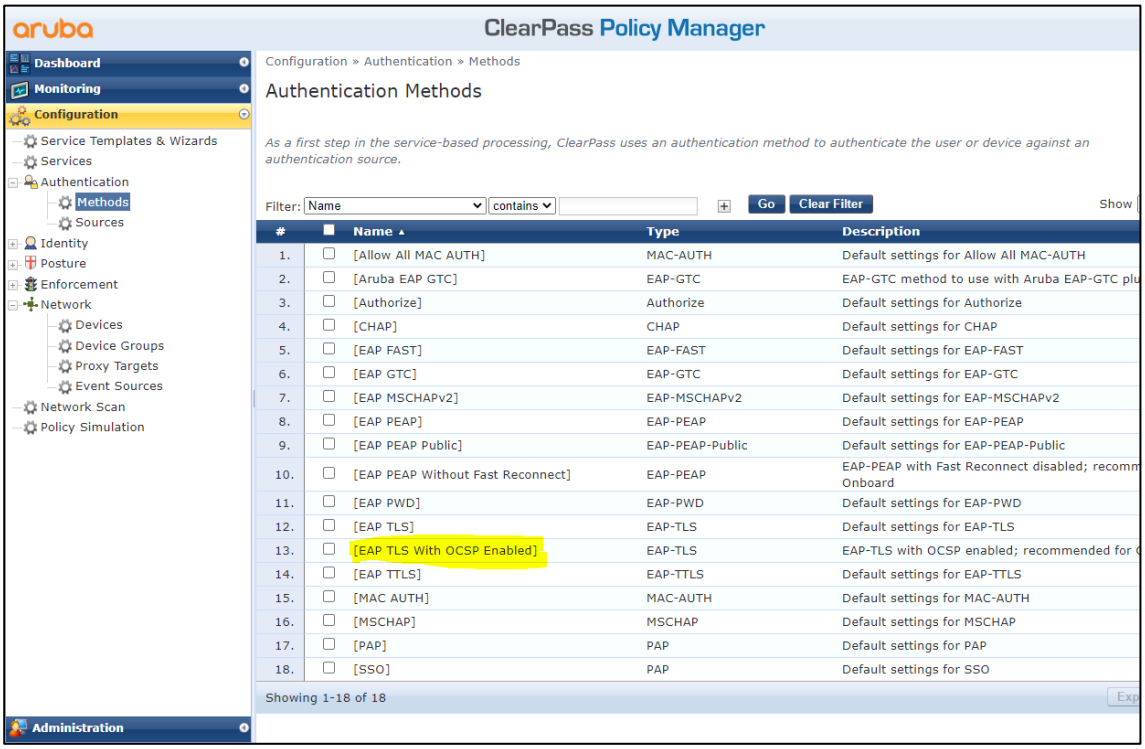


Ilustración 114. Método de autenticación EAP TLS con OCSP habilitado

379. Lo seleccionamos y editamos. Seleccionamos para el campo *Verify Certificate using OCSP:* el valor *Required (CRL Fallback)*.

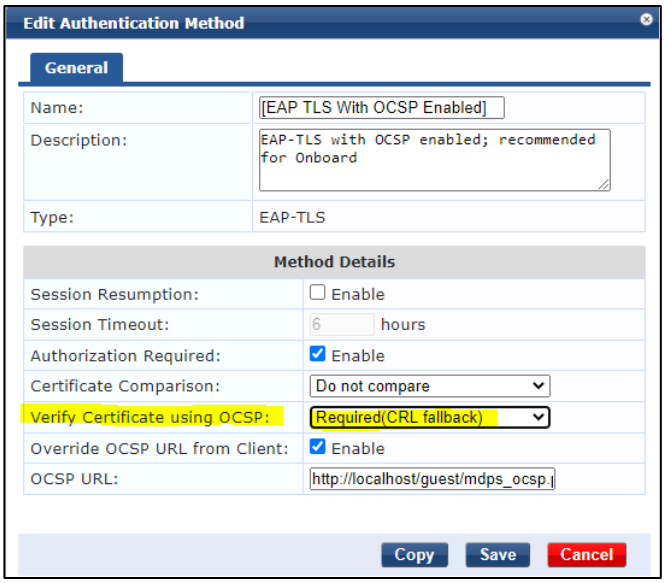


Ilustración 115. Método de autenticación EAP TLS con OCSP habilitado – Verificación de certificado con respaldo CRL.

6.15.4.3 OCSP – VERIFICAR LA VALIDEZ DE LOS CERTIFICADOS INTERMEDIOS

380. Es posible configurar Aruba ClearPass para que valide todos los certificados de la cadena. El uso de esta opción, aunque recomendada, añade una carga extra al sistema.

381. Esta opción se configura desde *Administration > Server Manager > Server Configuration > Seleccionamos servidor > Radius Server*, en la pestaña *Service Parameters*:

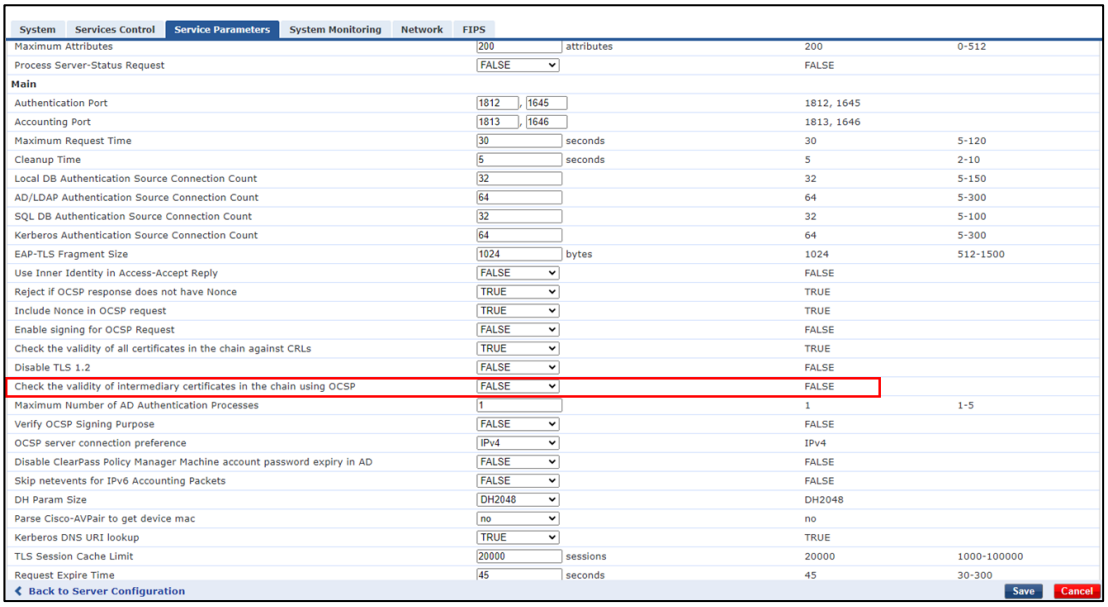


Ilustración 116. Verificar la validez de los certificados intermedios usando OCSP

6.15.5 *CLEARPASS EXCHANGE*

382. ClearPass ofrece un ecosistema de integraciones documentadas y probadas. Estas integraciones, bien permiten exportar información, recibirla o ambas cosas. Toda la información recibida se utiliza en algunos de los mecanismos descritos, pero principalmente como:

    a) Fuente de información para toma de decisiones

    b) Disparador de eventos con información contextual

383. Todas las integraciones con terceros fabricantes y sistemas se pueden encontrar en [REF16].

7. FASE DE OPERACIÓN

7.1 MONITORIZACIÓN

384. En la sección de Monitorización de ClearPass se ofrecen diversas herramientas de monitorización:

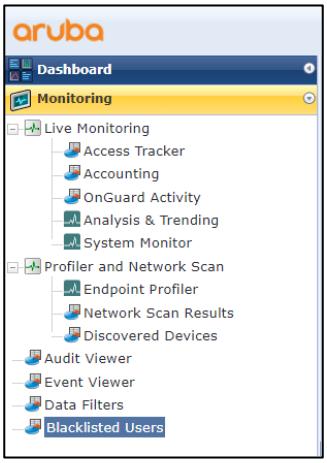


Ilustración 117. Herramientas de Monitorización de *Aruba ClearPass Policy Manager*

7.1.1 LIVE MONITORING: ACCESS TRACKER

385. Access Tracker proporciona una visualización en tiempo real de la actividad de acceso por sesión en el servidor o dominio seleccionado.

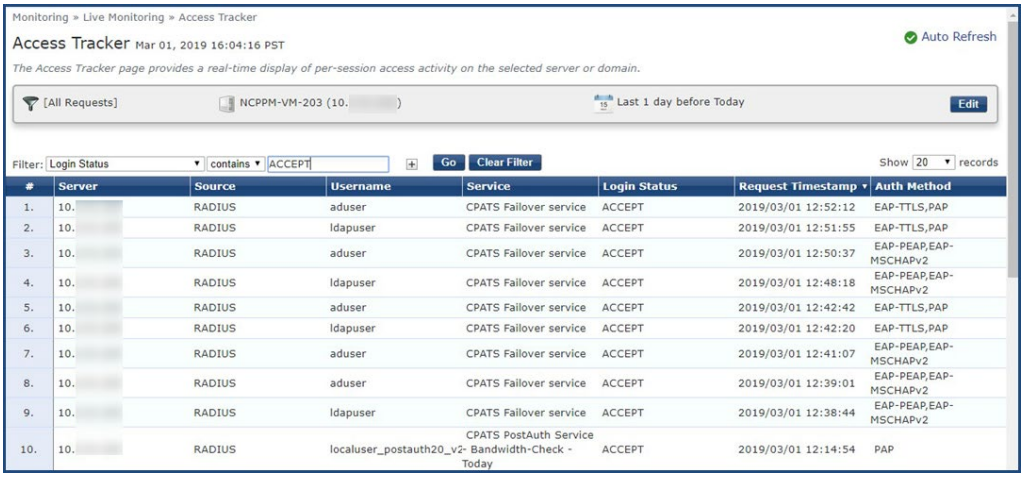


Ilustración 118. *Asset Tracker*

386. Las columnas por defecto que muestra son:

Server	Muestra la IP del servidor de ClearPass que recibe el evento.
Source	Fuente de autenticación. Por ejemplo, *RADIUS* o *web authentication (WEBAUTH).*
Username	Username o *MAC address* del HOST.
Service	Servicio de *ClearPass Policy Manager* que se ha ejecutado.

Login Status	Estado de la petición *Accept, Reject*, or *Timeout*.
Request Timestamp	Fecha y hora de la última actualización.

387. Policy Manager admite el filtrado de *Access Tracker* por atributos de entrada y salida de RADIUS, atributos de autorización, atributos de entrada y salida calculados y atributos de solicitud y respuesta de postura.

7.1.1.1 PERSONALIZACIÓN DE *ASSET TRACKER*

388. La opción de *Auto Refresh*, hace que se actualice la página periódicamente. Se recomienda desactivarlo, para permitir el cierre automático de las sesiones en caso de inactividad.

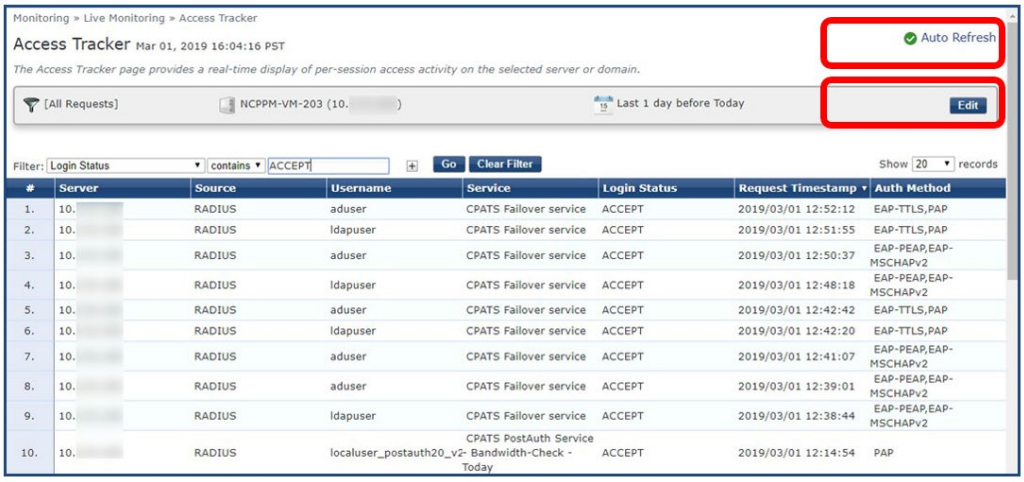


Ilustración 119. Auto-refresco y opciones de *Asset Tracker*

389. Es posible personalizar los eventos que se muestran. Para ello, se puede hacer clic en *Edit* y elegir las opciones de filtrado y las columnas que se desean mostrar.

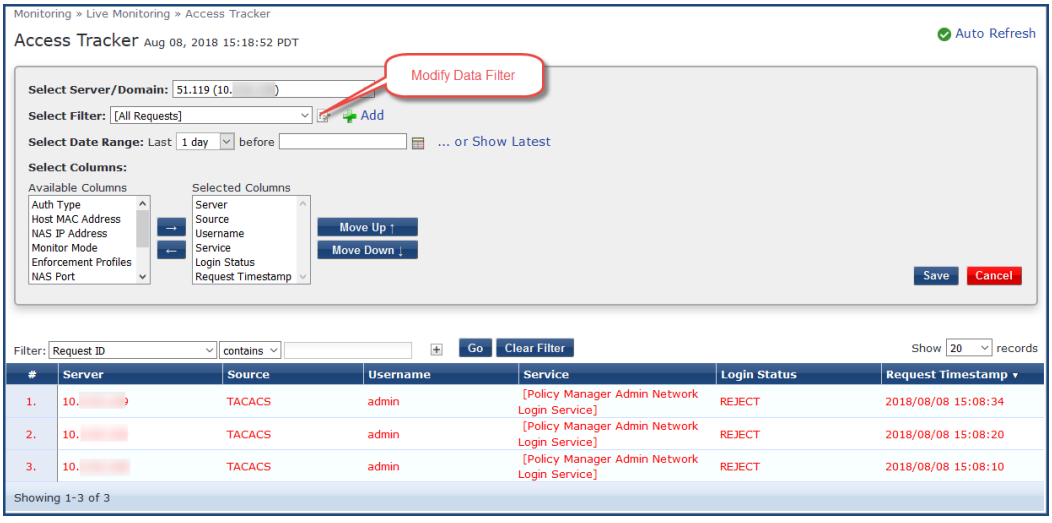


Ilustración 120. Filtrado de *Asset Tracker*

390. Las opciones seleccionadas estarán disponibles para futuras sesiones de operación.

7.1.1.2 DETALLES DE UNA SESIÓN

391. Cuando desde *Access Tracker* se pulsa sobre un registro, aparece la ventana de resumen del mismo.

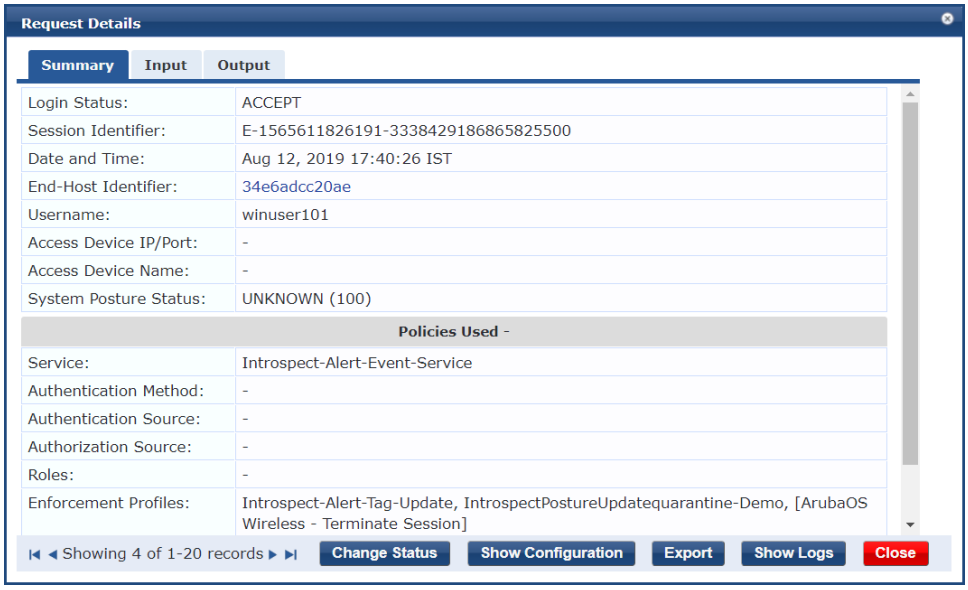


Ilustración 121. *Asset Tracker* – Detalles de una sesión – General

392. Se muestran, por lo menos, tres (3) pestañas: *Summary, Input y Output.*

393. Haciendo clic en *Input*, se pueden ver muchos detalles de todas las fuentes de información usadas, así como de los datos recibidos en la petición.

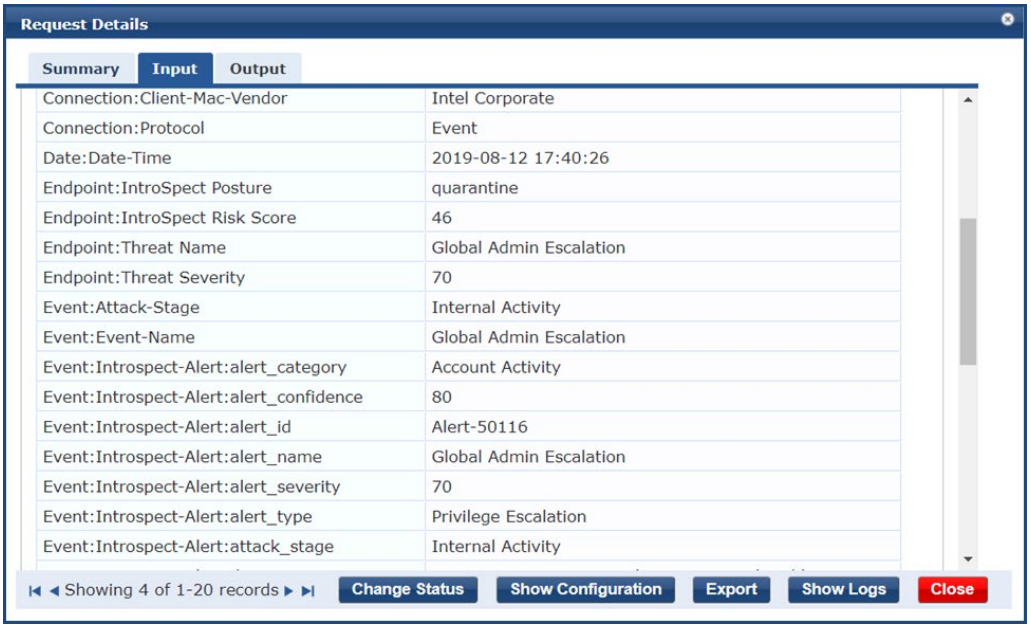


Ilustración 122. *Asset Tracker* – Detalles de una sesión – Input

394. En *Output* se muestra el detalle del resultado y de los atributos enviados, o de la respuesta dada.

395. Si se trata de una sesión de RADIUS, y además esté activado el *accounting*, podrá aparecer una pestaña adicional, con el *accounting* registrado de esa sesión.

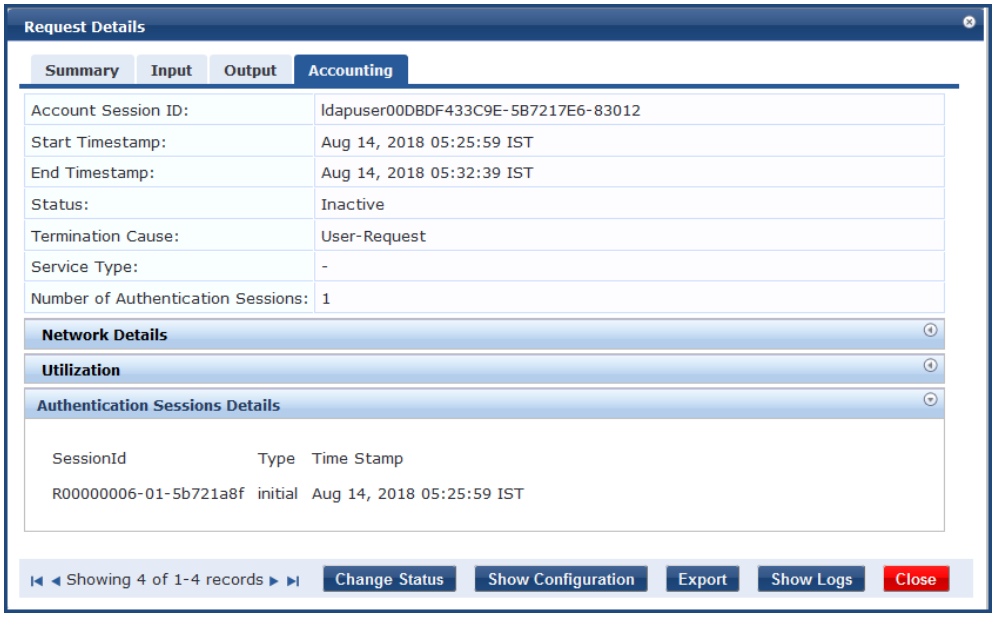


Ilustración 123. *Asset Tracker* – Detalles de una sesión – *Accounting*

396. Además, haciendo clic en el botón *Change Status,* se abrirá una ventana que permite al administrador ejecutar acciones RADIUS COA, o de otros tipos de acciones que estuvieran preconfiguradas, sobre la sesión seleccionada:

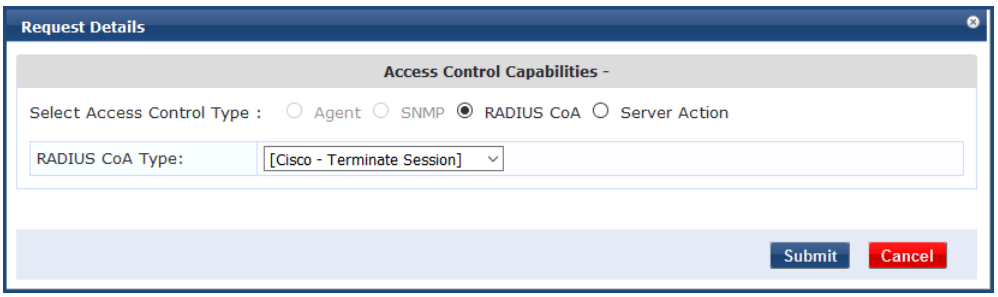


Ilustración 124. *Asset Tracker* – Detalles de una sesión – Ejecutar un cambio de estado

397. El detalle de los registros generados se puede consultar en la guía de usuario online de ClearPass Policy Manager - [REF8].

7.1.2 LIVE MONITORING: ACCOUNTING

398. La página *Accounting* proporciona un informe dinámico que describe el acceso a la sesión, según lo informado por el dispositivo de acceso a la red mediante registros contables RADIUS o TACACS+.

399. Para abrir la página *Accounting*, ir hasta *Monitoring > Live Monitoring > Accounting.* Para consultar la información, hacer clic sobre el registro deseado.

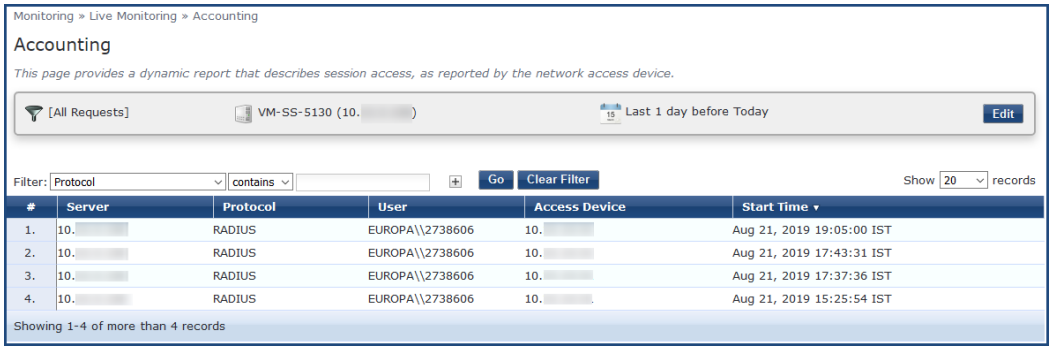


Ilustración 125. Ejemplo de listado de sesiones en *Accounting*

7.1.3 LIVE MONITORING: *ONGUARD ACTIVITY*

400. La página *Actividad de OnGuard* muestra el estado en tiempo real de todos los dispositivos finales que tienen *Policy Manager OnGuard*.

401. Esta página presenta herramientas de configuración para expulsar un terminal, reiniciar una sesión y enviar mensajes de difusión o unidifusión a todos los terminales que disponen del agente *OnGuard*.

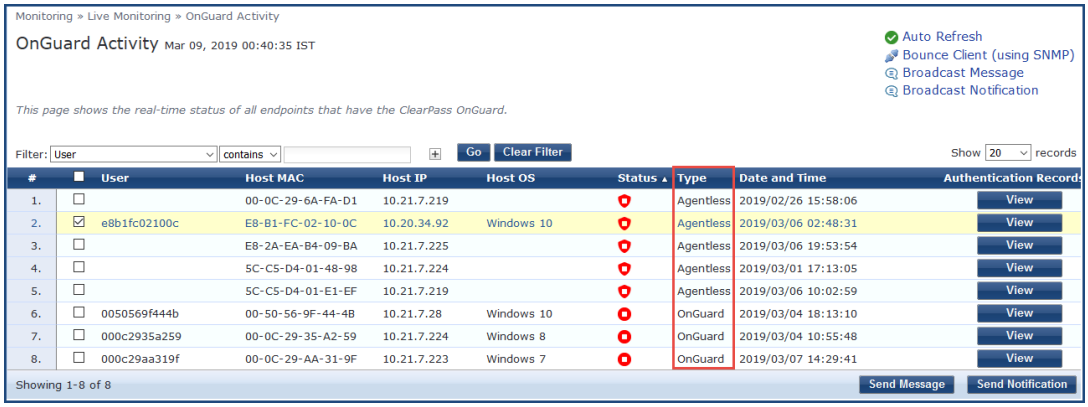


Ilustración 126. Actividad *ClearPass Onguard*

402. Se pueden buscar dispositivos por MAC, en diversos formatos:

a) 112233AABBCC

b) 11:22:33:aa:bb:cc

c) 11-22-33-AA-BB-CC

d) 1111-2222-3333

e) 1111.2222.3333

403. Al hacer clic en un terminal, se verá el detalle de ese terminal.

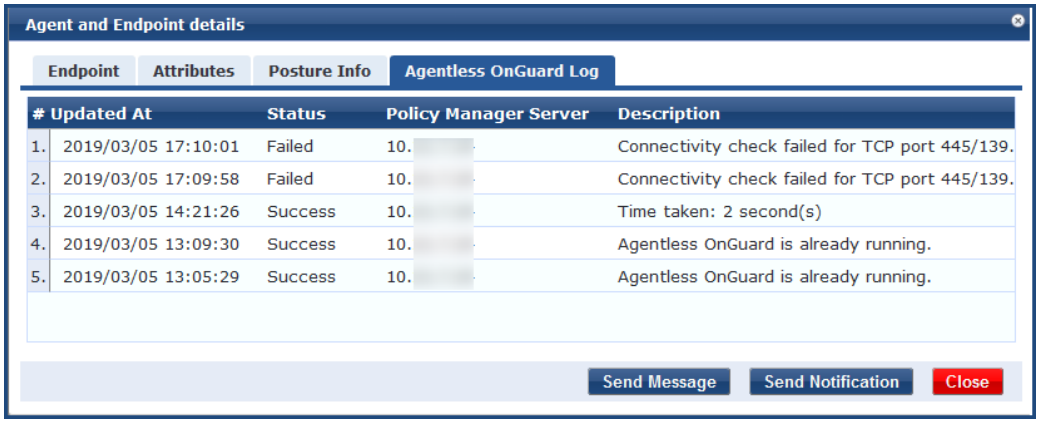


Ilustración 127. Detalle de la actividad de un agente *ClearPass OnGuard*

7.1.3.1 COMUNICACIÓN CON EL USUARIO FINAL

404. Se puede enviar mensajes iniciados por el operador de ClearPass. Para ello, se selecciona *Send Message*, en la ventana de detalle de un equipo terminal o en la ventana de *Actividad OnGuard*.

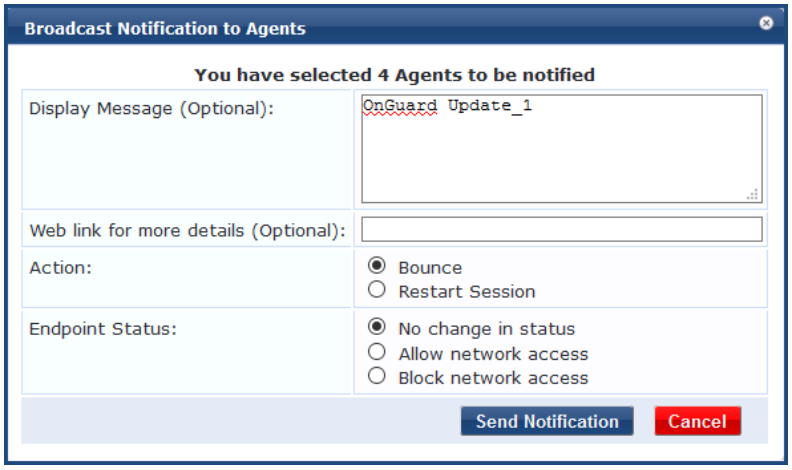


Ilustración 128. Envió de mensajes a terminales

405. Además de enviar un mensaje, se puede provocar una acción en el equipo del usuario final.

406. Existen más opciones de interacción vía SNMP. Se puede consultar en el manual online dichas opciones. En esencia, estas opciones pasan por mandar la orden de desconexión a la electrónica de red vía SNMP.

7.1.4 *LIVE MONITORING: ANALYSIS AND TRENDING*

407. La página *Analysis and Trending* muestra solicitudes para el subconjunto de componentes incluidos en los filtros seleccionados durante un período de tiempo seleccionado: un mes, dos semanas, una semana, un día, 12 horas, 6 horas, 3 horas o una hora.

408. Los datos se pueden agregar por minuto, hora, día o semana.

409. Al hacer clic en una barra, se profundiza en el rastreador de acceso que muestra los datos de la sesión para el intervalo de tiempo específico y para las solicitudes específicas.

Ilustración 129. ***Analysis and Trending***

7.1.5 *LIVE MONITORING: SYSTEM MONITOR*

410. La página *System Monitor* tiene cuatro (4) pestañas. Cada pestaña proporciona cuadros o gráficos que brindan información en tiempo real sobre varios componentes.

7.1.5.1 SYSTEM MONITOR

411. La pestaña *System Monitor* muestra cuadros y gráficos que muestran información sobre la carga de la CPU, el uso de la CPU, el uso de la memoria y el uso del disco para el servidor de Policy Manager seleccionado.

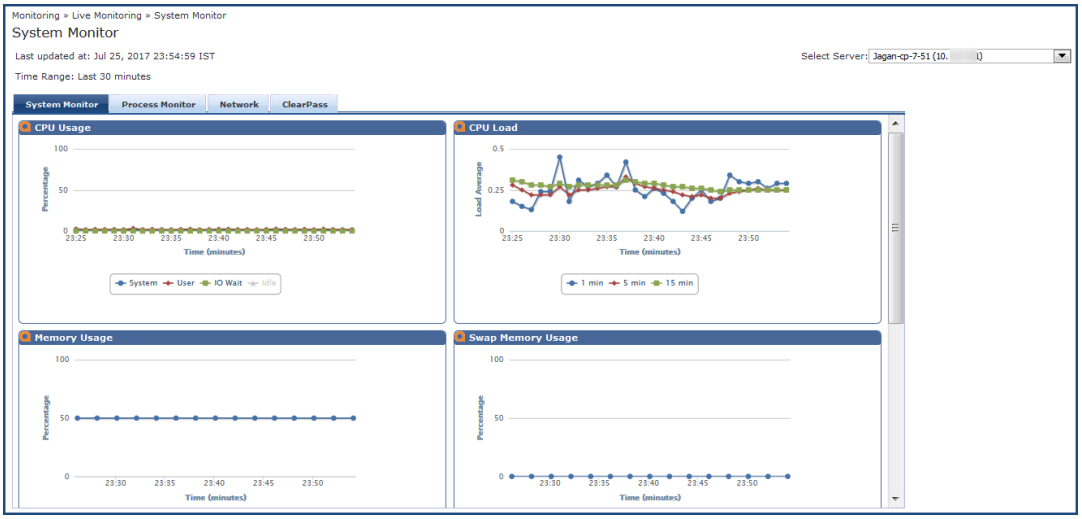


Ilustración 130. ***System Monitor***

7.1.5.2 *PROCESS MONITOR*

412. La pestaña *Process Monitor* muestra el uso de la CPU y el uso de la memoria principal para un proceso o servicio seleccionado.

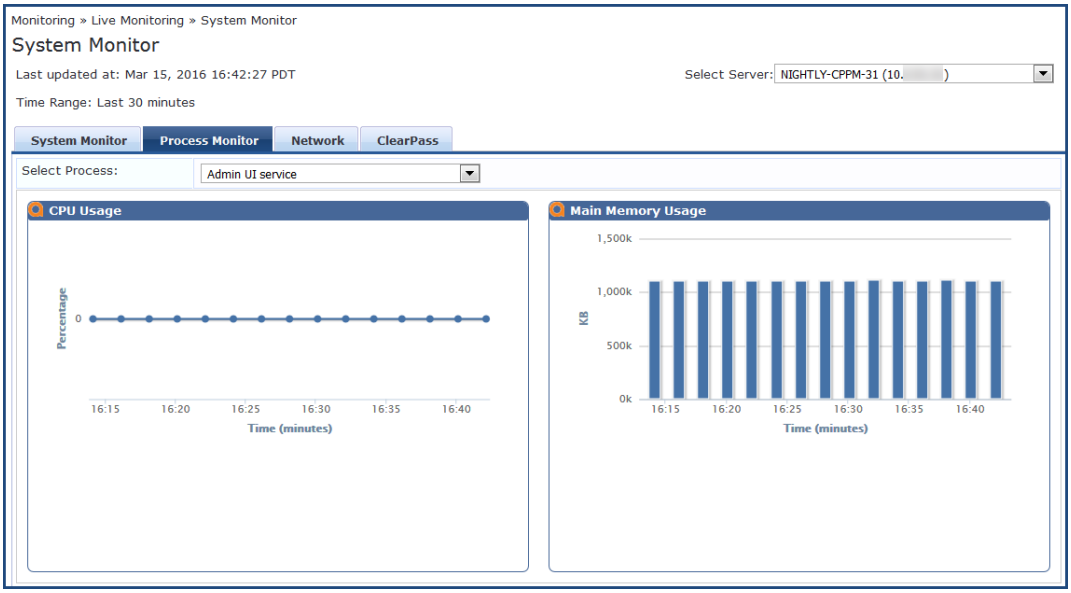


Ilustración 131. *System Monitor - Process Monitor*

7.1.5.3 *NETWORK MONITOR*

413. La pestaña *Network Monitor* muestra información sobre el tipo de tráfico de red seleccionado.

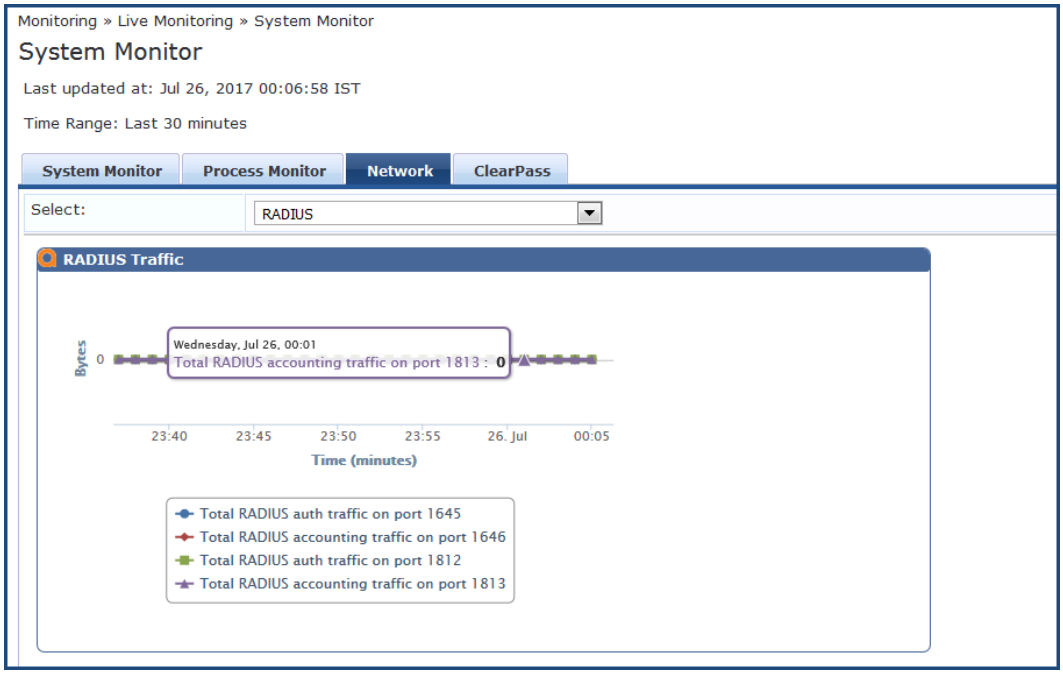


Ilustración 132. *Network Monitor*

7.1.5.4 *CLEARPASS MONITOR*

414. La pestaña *ClearPass Monitoring* muestra contadores y temporizadores de supervisión de rendimiento de los últimos 30 minutos de actividad en varios componentes de Policy Manager.

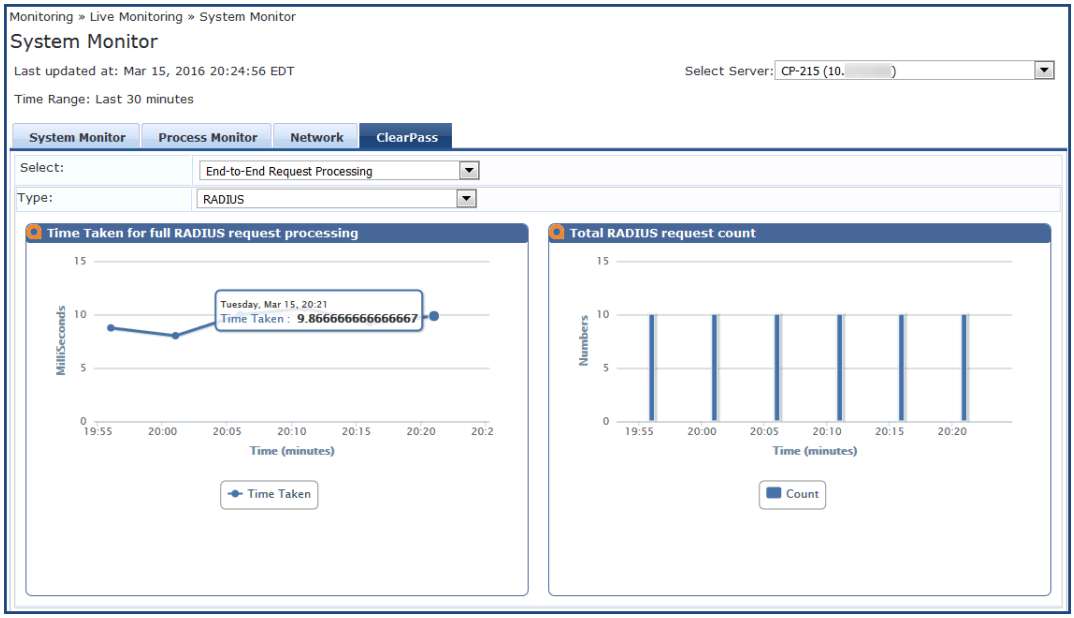


Ilustración 133. *System Monitor – ClearPass*

415. Los componentes que se pueden monitorear son los siguientes:

a) *Service Categorization*

b) *Authentication (RADIUS, TACACS, o WebAuth)*

c) *Authorization*

d) *Role Mapping*

e) *Posture Evaluation*

f) *Audit Scan*

g) *Enforcement*

h) *End-to-End Request Processing (RADIUS, TACACS, o WebAuth)*

i) *Advanced*

7.1.6 *ENDPOINT PROFILER*

416. Esta página permite ver estadísticas agregadas de todos los terminales descubiertos. Se pueden usar los filtros para tener una visión agregada de su distribución.

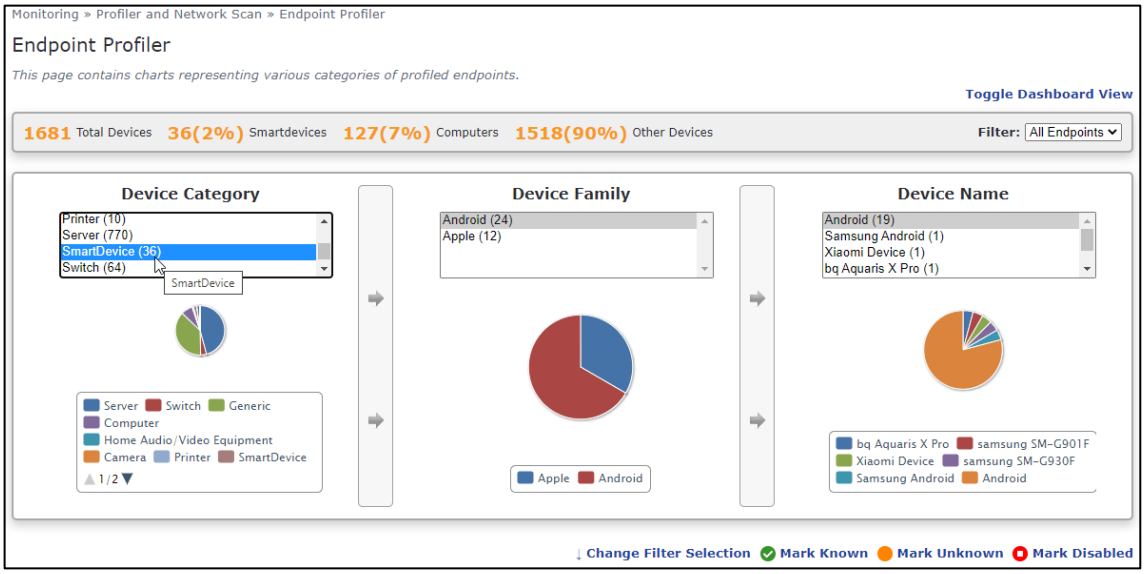
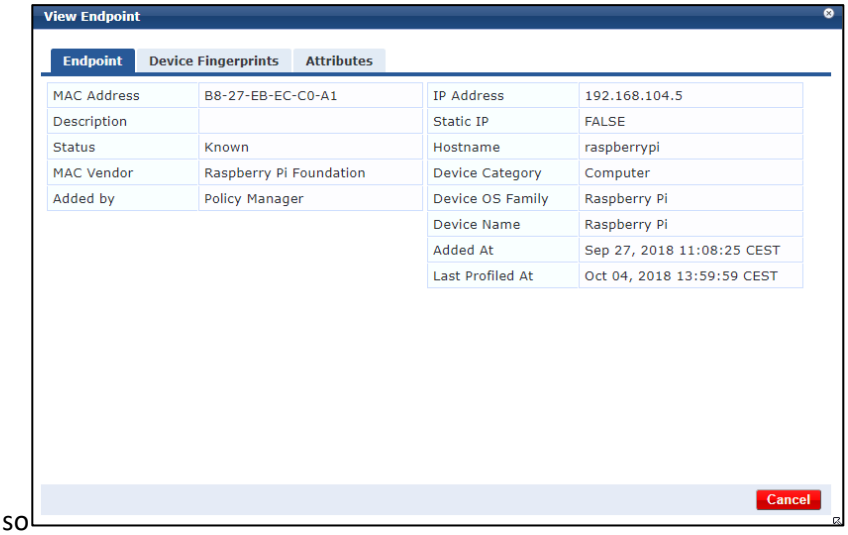


Ilustración 134. *Endpoint Profiler*

417. Es posible mostrar los datos recopilados asociados a cada terminal.



SO

Ilustración 135. Detalles generales de un terminal descubierto por *Endpoint Profiler*

418. Las huellas digitales descubiertas del terminal se ven en la pestaña *Device FingerPrints.*

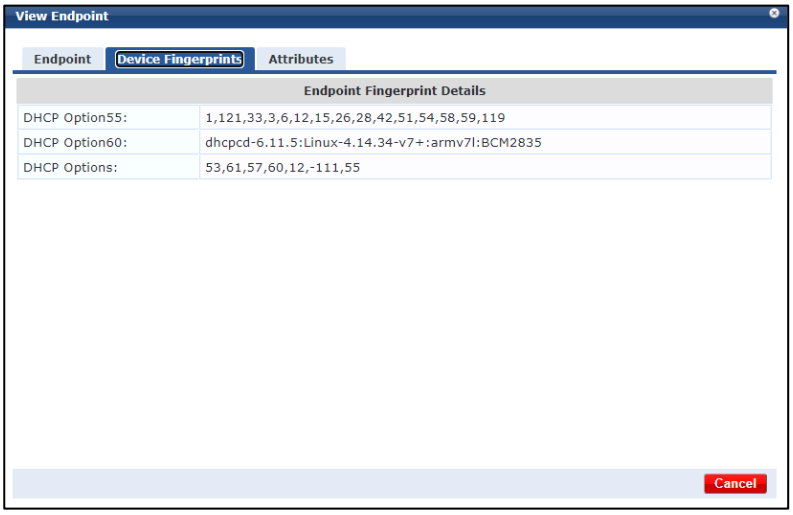


Ilustración 136. Huellas (*fingerprints*) de un terminal descubierto por *Endpoint Profiler*

7.1.7 AUDIT VIEWER

419. La página *Audit Viewer* proporciona un informe dinámico sobre las acciones, el nombre del dispositivo, la categoría del componente *Policy Manager*, el usuario y la marca de tiempo. En otras palabras, se muestran todas las acciones que realizan los operadores:

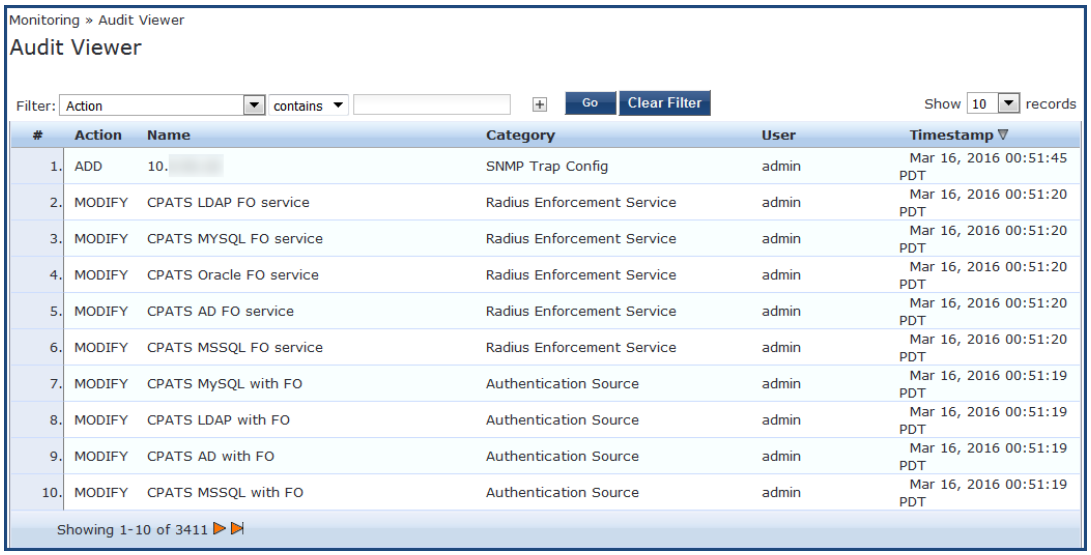


Ilustración 137. *Audit Viewer*

420. El detalle de la configuración de los registros de auditoría se puede consultar en el apartado **6.12 AUDITORÍA**, del presente documento.

7.1.8 *EVENT VIEWER*

421. La página *Event Viewer* proporciona informes sobre eventos a nivel del sistema. Todos los intentos de instalación del sistema, actualizaciones, parches y revisiones se registran en este visor.

422. Esta página también muestra información sobre el exceso de licencias (donde el uso de la licencia excede la disponibilidad de la licencia). Cuando el dispositivo vuelve a caer dentro

de los límites de licencia permitidos, el visor de eventos muestra un mensaje actualizado que indica que *Policy Manager* tiene las licencias adecuadas.

423. En caso de ocurrencia de *Timeouts* en las sesiones de administración, se generan mensajes con una descripción que incluye la dirección IP del cliente y el ID de sesión.

424. Las operaciones de exportación e importación de todos los módulos también se capturan en el visor. Se registran todos los elementos de configuración que se pueden importar o exportar, como servicios, perfiles de cumplimiento, terminales, dispositivos, etc.

425. También se registran accesos no autorizados de distintos tipos:

    a) Equipos de red con claves incorrectas.

    b) Intentos de accesos a la interfaz de línea de comandos (CLI) de administración de *ClearPass Policy Manager* con versiones de protocolo SSH no admitidas, algoritmos de cifrado o hash criptográficos no admitidos. Policy Manager registra esas alertas en el visor si se activa la opción *Enabling Ingress Events Processing* (esta funcionalidad es intensiva en recursos, por lo que se recomienda consultar el manual para más información).

    c) Otros eventos críticos.

7.2 EXPORTACIÓN DE REGISTROS

426. Policy Manager puede exportar datos de sesión (*Access Tracker*), registros de auditoría (*Audit Viewer*) y registros de eventos (*Event Viewer*). La configuración de los servidores externos para exportar los registros se detalla en el apartado **6.12.2 ALMACENAMIENTO REMOTO: SYSLOG EXTERNO**.

7.3 MONITORIZACIÓN *ONBOARD*

427. Los eventos *OnBoarding* se almacenan en el registro de la aplicación durante siete (7) días de forma predeterminada.

428. Después de ese tiempo, los eventos de ejecución importantes se enumeran en *Audit Viewer* en el módulo de Monitorización de *ClearPass Policy Manager*. Los eventos *onboard* que se enumeran incluyen:

    a) Cambiar el certificado de CA.

    b) Emitir un nuevo certificado.

    c) Firma de una solicitud de firma de certificado.

    d) Revocar un certificado.

    e) Eliminar un certificado.

    f) Importar un certificado de confianza.

    g) Cargar una firma de código u otro certificado.

7.3.1 MENSAJES DE ESTADO DE OCSP/CRL

429. En *Event Viewer* se registran notificaciones cuando:

    a) La conexión con un servidor OCSP provoca un *timeout*.

b) No se recibe respuesta del servidor OCSP.

c) CRL ha expirado.

d) La descarga del CRL falla.

7.4 MONITORIZACIÓN *CLEARPASS GUEST* Y *CLEARPASS ONBOARD*

430. Tanto *ClearPass Guest* como *ClearPass OnBoard* funcionan con servicios definidos en *ClearPass Policy Manager*. Por tanto, además de las herramientas propias de *ClearPass Policy Manager* para monitorizar el servicio, se debe monitorizar el Registro de Aplicaciones de *ClearPass Guest* y *OnBoard*.

431. Este registro se encuentra en *Administration > Support > Application Log.*

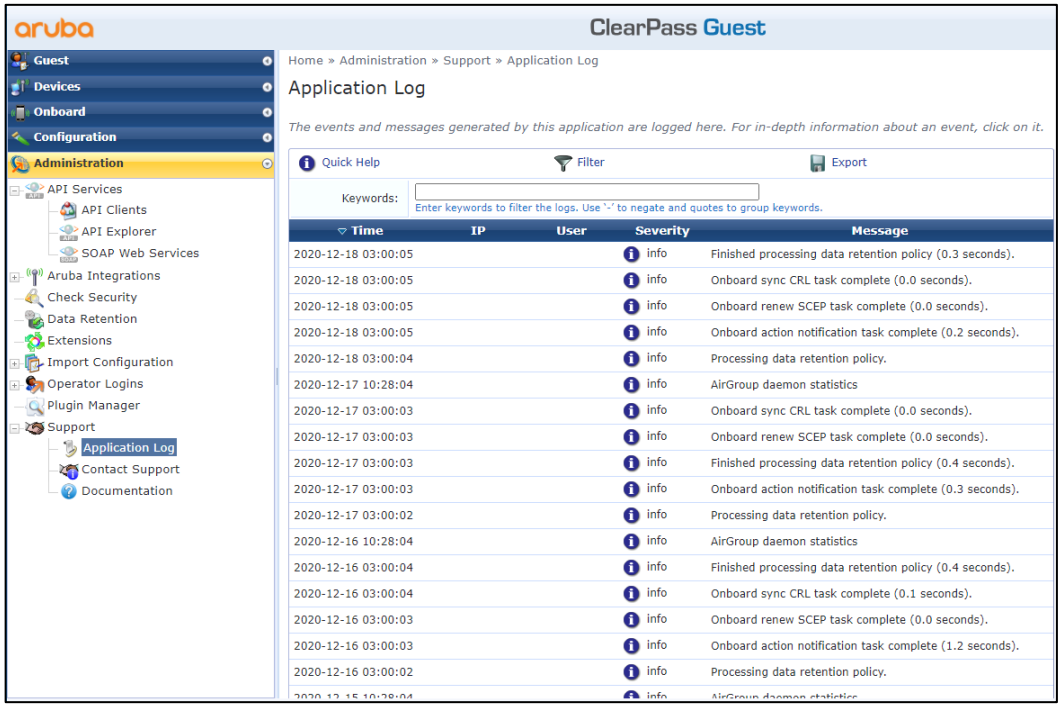


Ilustración 138. Registro de aplicaciones (*Application Log*) de *ClearPass Guest*

7.5 ALERTAS Y NOVEDADES

432. Las dos (2) informaciones relevantes para la correcta administración del producto son:

a) Nuevas versiones, con información de nuevas funcionalidades y en particular relacionadas con la seguridad.

b) Alertas de vulnerabilidades e información de parches que lo solucionan.

433. Ambas informaciones son accesibles desde *Aruba Support Portal,* https://networkingsupport.hpe.com/home. Este portal es un punto de entrada para múltiples funciones, documentación, acceso a *software*, gestión de licencias, etc. Algunas de estas funciones pueden requerir tener una cuenta registrada y/o vinculada a otra con equipos registrados.

434. En el caso de disponer de cuenta de usuario, se puede registrar a las notificaciones vía correo electrónico de alertas, novedades software, productos y documentación.

435. Las vulnerabilidades reconocidas se ofrecen en [REF17] sin necesidad de registro alguno. También se ofrecen a través de *RSS feed*.

8. CHECKLIST

436. Como punto de control se recomienda seguir esta lista de comprobaciones para la realización de una instalación segura de Aruba ClearPass que se ha realizado una instalación segura.

ACCIONES	SÍ	NO	OBSERVACIONES
REQUISITOS PREVIOS			
Acceso a la descarga de las licencias	☐	☐	
Acceso al software necesario	☐	☐	
Identidad de los servidores: IP, FQDN	☐	☐	
Certificados HTTPS para administración segura y/o portales con los usuarios	☐	☐	
Determinación de apertura de puertos para flujos implicados en las tareas de ClearPass	☐	☐	
Servidores DNS, NTP	☐	☐	
Si ClearPass tendrá acceso a Internet disponer de credenciales válidas para descarga. Si ClearPass NO tendrá acceso a Internet pre-descargar los paquetes de software	☐	☐	
INSTALACION DE LOS EQUIPOS			
Verificación de la entrega segura del producto	☐	☐	
Verificación de Instalación en un entorno seguro	☐	☐	
INSTALACION SERVIDOR PRINCIPAL			
Despliegue del servidor principal	☐	☐	
INSTALACION SERVIDOR(ES) SECUNDARIO(S)			
Despliegue del servidor secundario	☐	☐	
CONSTITUCIÓN DEL CLÚSTER			
CONSTITUCION DEL CLÚSTER			
Convertir en subscriber todos los servidores secundarios	☐	☐	
CONFIGURACIÓN FUNCIONAL			
MODO DE OPERACIÓN SEGURO			
Activar modo de operación seguro FIPS-CC	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Configurar la política de passwords para los administradores	☐	☐	
Configurar la política de passwords y control de fallos de login para los usuarios	☐	☐	
Ajustar los temporizadores de las sesiones de administración	☐	☐	
Configurar un mensaje de bienvenida (banner)	☐	☐	
Configurar las interfaces virtuales necesarias	☐	☐	
Instalación de los certificados HTTPS	☐	☐	
Si se dispone de acceso a Internet, configurar usuario para descarga de actualizaciones y firmas.	☐	☐	
Desactivar TLS 1.0 y TLS 1.1	☐	☐	
Configurar envio de syslogs terceros servidores	☐	☐	
Configurar backups programados	☐	☐	
Crear los usuarios administradores adicionales	☐	☐	

9. REFERENCIAS

[REF1] Hoja de Datos, DataSheet, de Aruba ClearPass
https://www.arubanetworks.com/assets/_es/ds/DS_ClearPass_PolicyManager.pdf)

[REF2] Site de soporte de Aruba
https://networkingsupport.hpe.com/home

[REF3] ClearPass 6.11 Installation Guide:
https://www.arubanetworks.com/techdocs/ClearPass/6.11/Installation-Guide/Default.htm

[REF4] ClearPass CPPM Tech Note Clustering Design Guidelines v1.2
https://support.hpe.com/hpesc/public/docDisplay?docId=a00100359en_us
Aruba ClearPass Policy Manager (CPPM)
https://support.hpe.com/hpsc/doc/public/display?docId=a00100342en_us

[REF5] Release Notes Versión 6.11 –
https://networkingsupport.hpe.com/downloads;fileTypes=SOFTWARE;products=Aruba%20ClearPass%20Policy%20Manager%20%28CPPM%29;softwareMajorVersions=6.11

[REF6] Clustering. Certificate Validations.
https://support.hpe.com/hpesc/public/docDisplay?docId=a00100342en_us

[REF7] ClearPass CPPM - Certificates 101 Tech Note V1.2
https://support.hpe.com/hpsc/doc/public/display?docId=a00100345en_us

[REF8] Guía de usuario online de ClearPass Policy Manager
https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/home.htm

[REF9] Cipher Suites
https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPPM_UserGuide/Cipher%20Suites/Cipher_Suites_appendix.htm

[REF10] Certificate/Two-Factor Authentication for Policy Manager Application Login Service Template
https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPPM_UserGuide/Services/ServiceTemplates_CertificatesTwofactoraauth.htm

[REF11] Creating a Certificate Signing Request
https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPPM_UserGuide/Admin/ServerCertificate_Create_Certificate_Signing_Request.htm

[REF12] Configuring a Role and Role-Mapping Policy
https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPPM_UserGuide/identity/ConfiguringRoleMapping.html?Highlight=configure%20role%20mapping%20policyde la documentación online

[REF13] Feature Comparison: Persistent OnGuard, Agentless OnGuard, and Native Dissolvable Agent for Windows, macOS and Supported Linux OS

https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPPM_UserGuide/OnGuard/AO_feature_comparison.htm?Highlight=onguard

[REF14] Onboard Feature List

https://www.arubanetworks.com/techdocs/ClearPass/6.11/Guest/Content/Onboard/OnboardFeatureList.htm?Highlight=onboard%20feature%20lista

[REF15] Policy Manager Insight Reports

https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPPM_UserGuide/Insight/Intro_Insight.htm?Highlight=insight%20report%20tool

[REF16] ClearPass Docs | Configuration & Integration Guides, Solution Guides, Release Notes, User Guides

https://www.arubanetworks.com/clearpassdocs

[REF17] Archive of Security Advisories

https://www.arubanetworks.com/support-services/security-bulletins/

10. ABREVIATURAS

AAA	Authentication, Authorization and Accounting
AAA	Authentication, Authorization and Accounting
ACL	Access List
AD	Active Directory
AMI	Amazon Machine Image
API	Application Programming Interfaces
BYOD	Bring Your Own Device
CA	Certificate Authority
CHAP	Challenge-Handshake Authentication Protocol
CLI	Command-Line Interface
CPD	Centro de Proceso de Datos
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DMZ	Demilitarized Zone
DNS	Domain Name System
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
ENS	Esquema Nacional de Seguridad.
ESXi	Elastic Sky X Integrated
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IoT	Internet of Things
IPSec	Internet Protocol Security
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Management
MSCHAP	Microsoft Challenge-Handshake Authentication Protocol
NAC	Network Access Control

NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OVF	Open Virtualization Format
PAP	Password Authentication Protocol
PKI	Public Key Infraestructure
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RSA	Rivest-Shamir-Adleman
SCP	Secure Copy Protocol
SFTP	Secure File Transfer Protocol
SHA256	Secure Hash Algorithm 256-bit
SIEM	Security Information and Event Management
SMB	Server Message Block
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VMware	Virtual Machine Software
VPN	Virtual Private Network
WMI	Windows Management Instrumentation

PUBLICACIONES DE DEFENSA

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