Guía de Seguridad de las TIC
CCN-STIC 1248

Procedimiento de Empleo Seguro
Vision Packet Brokers de Keysight

Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
2026.06.26 08:50:25 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN

1. La familia Vision Packet Brokers de Keysight está formada por dispositivos especializados de visibilidad de red diseñados para recibir copias pasivas del tráfico, procedentes normalmente de TAPs, SPANs o enlaces de interconexión, y distribuirlas de forma selectiva hacia herramientas externas de monitorización, análisis y seguridad.
2. Desde el punto de vista operativo, un packet broker actúa como plano intermedio de tratamiento del tráfico: agrega múltiples entradas procedentes de TAPs o SPANs, replica flujos cuando varios consumidores necesitan la misma visibilidad, balancea carga cuando una herramienta debe escalar horizontalmente y filtra el tráfico de interés para reducir el volumen entregado a sondas, IDS, NDR, grabadores o plataformas analíticas.
3. La lógica de valor de un packet broker no reside en almacenar tráfico ni en sustituir a las herramientas de análisis, sino en optimizar el acceso a los flujos relevantes. De este modo, las herramientas externas reciben un flujo más limpio, más preciso y mejor adaptado a su función, evitando sobrecarga, puntos ciegos y duplicación innecesaria de tráfico.
4. Las guías de usuario de la familia muestran que el tratamiento del tráfico se articula alrededor de un conjunto consistente de capacidades: filtrado L2-L4, selección por direcciones y puertos, criterios de sesión, filtros dinámicos, control de acceso granular sobre objetos, estadísticas por puertos, grupos y filtros.
5. En determinados modelos y licencias, la familia amplía estas capacidades con funciones avanzadas como: Filtrado a nivel de aplicación, deduplicación de tráfico, eliminación de cabeceras, *slicing* de paquetes, envío de Netflow y metadatos extendidos o desencriptado de tráfico TLS. No obstante, el núcleo de empleo seguro del producto sigue siendo común: proteger el plano de gestión, controlar el acceso administrativo, asegurar las comunicaciones, mantener trazabilidad de auditoría y preservar la integridad de la configuración.
6. El presente Procedimiento de Empleo Seguro se formula con carácter genérico para toda la familia incluida en el alcance de la cualificación y no únicamente para un modelo concreto. En consecuencia, las posibles referencias a modelos como el Vision ONE, Vision Edge E40/E100 u otros modelos se utilizan únicamente como soporte documental cuando el comportamiento descrito es común a la familia o cuando una guía concreta resulta útil para ilustrar una función común.
7. Capacidades y beneficios principales
    - Agregación de múltiples fuentes de tráfico procedentes de TAPs, SPANs y enlaces de interconexión.
    - Selección y filtrado de flujos de interés, reduciendo ruido y carga innecesaria sobre las herramientas.
    - Replicación controlada hacia varias herramientas de seguridad o monitorización.
    - Balanceo de carga de tráfico entre herramientas cuando la arquitectura lo requiera.
    - Soporte de autenticación local y, opcionalmente, autenticación centralizada mediante AAA.

- Gestión centralizada vía GUI HTTPS, Web API y consola local CRAFT/serie para provisión o recuperación.

Este documento está destinado a un público familiarizado con la configuración de los Packet Brokers de Keysight y no pretende sustituir a la Guía del Usuario, que puede descargarse del portal de soporte de Keysight (Ver REF2 en este documento)

2 OBJETO Y ALCANCE

8. La presente guía establece el procedimiento de empleo seguro para la familia Vision Series Network Packet Broker de Keysight en su versión objetivo 5.10.0. El documento cubre los aspectos de recepción, instalación, administración, autenticación, certificados, sincronización, actualización, auto-chequeos, auditoría y backup que deben considerarse para un despliegue seguro en organizaciones que operan bajo requisitos CPSTIC y ENS
9. Los modelos considerados en el alcance de la certificación son los siguientes: Vision ONE, Vision 7300/7303, Vision E40, Vision E100, Vision E10S, Vision X y TradeVision.
10. El producto Vision Network Packet Broker ha sido incluido en el catálogo de productos y servicios STIC (CPSTIC) y para consultar el listado, categoría o nivel y familia consulte [REF3].

3 ORGANIZACIÓN DEL DOCUMENTO

a. **Apartado 4.** En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto. recepción segura del appliance o software, requisitos de entorno físico y de red, preparación del plano de gestión y componentes externos de soporte, como syslog, NTP o AAA.

b. **Apartado 5.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto, incluyendo montaje, alimentación, configuración inicial del puerto de gestión y uso del puerto CRAFT/serie

c. **Apartado 6.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura: autenticación, administración, interfaces y puertos de gestión, certificados, sincronización, actualización, auto-chequeos, auditoría y backup.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

11. Los Vision Packet Brokers son appliances hardware. Antes de su puesta en servicio se debe verificar la integridad física del equipo y del embalaje, así como la correspondencia entre el material recibido y el material previsto para el despliegue. Las guías de instalación (ver REF2 en este documento) de Vision ONE y Vision Edge indican expresamente que el equipo debe instalarse y mantenerse por personal cualificado y en ubicaciones de acceso restringido.
12. Verificación de la integridad física del equipo antes de su puesta en servicio. Como mínimo, deben revisarse el embalaje externo e interno, el estado del chasis, la ausencia de manipulaciones visibles, el etiquetado, el número de serie y la correspondencia entre el modelo recibido y el modelo programado para el despliegue.
    a. Verificar que el embalaje exterior no presenta daños, aperturas o manipulaciones visibles.
    b. Abrir el embalaje en un entorno controlado y comprobar que los elementos suministrados se corresponden con la documentación de entrega.
    c. Inspeccionar el chasis, los conectores, tornillería, precintos y etiquetas del equipo.
    d. Registrar el número de serie y modelo del equipo.
    e. Documentar cualquier anomalía antes de conectar el appliance a la red o a la alimentación eléctrica.
13. En función del modelo a instalar se recomienda revisar y seguir las instrucciones indicadas en las guías de instalación Hardware disponibles en el site de soporte (ver REF2 en este documento).

4.2 ENTORNO DE INSTALACIÓN SEGURO

14. En general los Packet Brokers son appliances preparados para instalar en bastidor o armario ubicado en un CPD con control físico de acceso donde se encuentran las fuentes de tráfico a monitorizar con control físico de acceso. Las guías de instalación de los Vision Packet Broker establecen que los equipos están previstos para instalación en restricted-access location (RAL), es decir, un área accesible únicamente por personal formado y autorizado. Esta premisa debe reflejarse en el despliegue real del producto.
15. El equipo se instalará en un CPD o armario de comunicaciones con control físico de acceso, condiciones ambientales adecuadas, alimentación protegida y segregación entre el plano de datos y el plano de gestión. El puerto MGMT y el puerto CRAFT/serie deben quedar fuera del alcance de usuarios no autorizados.
16. El rack deberá disponer de puesta a tierra adecuada. Se recomienda además el uso de un SPD en la entrada de alimentación AC.

4.3 REGISTRO Y LICENCIAS

17. El registro y licenciamiento forman parte del control seguro del packet broker, ya que condicionan las funciones disponibles, la velocidad de puertos y determinadas capacidades

avanzadas. Keysight registra las licencias asociadas a cada appliance y proporciona un fichero de licencias. El fichero de licencias proporcionado por Keysight debe instalarse en el appliance conforme a la información disponible en la Guía de usuario.

18. Keysight, junto con la entrega del equipo físico, proporciona, vía email, un fichero de licencia asociado al equipamiento adquirido para su instalación a través de la consola web. El acceso a la consola web está disponible con el usuario admin una vez realizada la primera configuración y puesta en marcha del equipo. Básicamente se requiere la configuración del puerto de gestión. A partir de aquí se puede acceder a la consola web con el usuario admin y password por defecto (el cual se puede cambiar tanto en el acceso por consola como en la consola web). Ver sección 5 en este documento.
19. Para instalar el fichero de licencia recibido se deben seguir los siguientes pasos:
    a) Iniciar sesión con una cuenta administradora.
    b) Acceder a System > License
    c) Acceder a "Enter License Key…" y seleccionar el fichero de licencias.

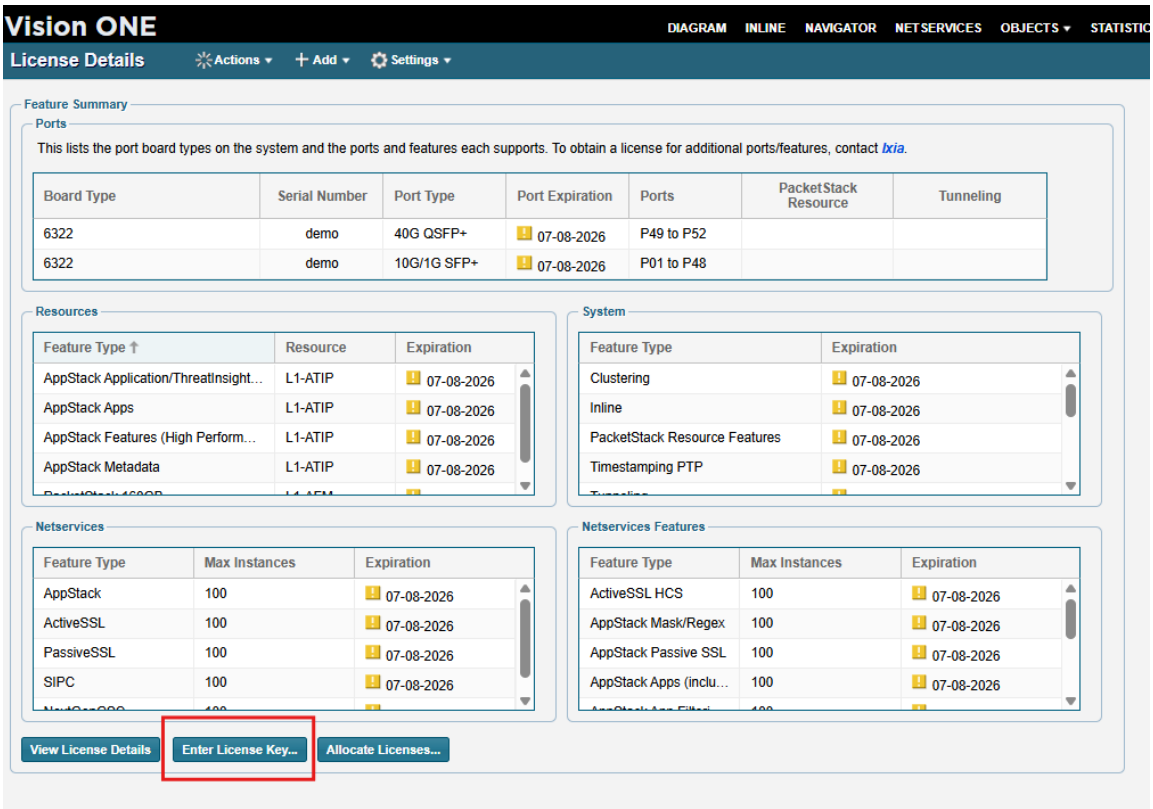

Figura 1. Vista de la sección System > License

20. Antes de la puesta en explotación, un administrador deberá revisar el estado de las licencias desde la consola web y conservar copia controlada del fichero de licencia entregado por Keysight. Las operaciones de actualización también pueden quedar condicionadas por la vigencia del contrato de mantenimiento.
21. En el portal de soporte (ver REF2 en este documento) para los procedimientos de administración general del sistema y gestión de licencias.

4.4 CONSIDERACIONES PREVIAS

22. Antes de iniciar la instalación y configuración segura del producto se deben decidir, al menos, los siguientes aspectos de arquitectura y operación:

- Red o segmento de administración desde el que se operará el equipo.
- Necesidad de autenticación local exclusiva o integración con servicios AAA externos.
- Necesidad de envío de logs a un servidor syslog remoto.
- Necesidad de integración con servicio NTP y, en su caso, autenticación de dicho servicio.
- Necesidad de acceso por WebAPI y automatización.
- Uso o no de perfil más restrictivo gubernamental y, si aplica, de FIPS encryption. En entornos que exijan securización reforzada se recomienda mantener Vision Orchestrator deshabilitado. En la sección *Government Security Configuration Guide* de las Guías de usuarios se indica que, desde la versión 5.7.1, se entrega deshabilitado por defecto y que debe permanecer así para determinados perfiles Common Criteria / DoDIN.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

23. Los siguientes componentes pueden formar parte del entorno de operación del producto, dependiendo del perfil de despliegue.

Componente	Necesidad	Observaciones
Administración	Necesaria	Acceso a Web Console / GUI
Red de gestión dedicada	Necesaria	Separada del plano de datos
Puerto CRAFT/serie	Necesario para provisión/recuperación	Uso restringido a personal autorizado
Servidor NTP	Recomendado	Opcional en el entorno, recomendable para trazabilidad
Servidor syslog remoto	Recomendado	Componente opcional del entorno para auditoría remota
Servidor LDAP / AAA externo	Opcional	Componente opcional del entorno de autenticación
DNS	Opcional	Necesario cuando se usen servicios por nombre

Tabla 1: Componentes del entorno de operación

5 FASE DE INSTALACIÓN

24. La instalación física y lógica del producto debe realizarse conforme a la guía de instalación específica del modelo correspondiente (ver enlace al portal de soporte en REF2 en este documento). No obstante, las medidas de seguridad aplicables son comunes a la familia y se resumen a continuación.

25. Con carácter general, los appliances de la familia se entregan con el firmware instalado de fábrica y siguen una secuencia común de montaje en rack, conexión de alimentación, arranque del sistema y configuración inicial del puerto de gestión. Las diferencias entre modelos afectan principalmente a factores físicos como tamaño de chasis, número y tipo de puertos o accesorios, pero no alteran la lógica general del empleo seguro.

    a) Montar el equipo en un rack estándar apropiado para el modelo, utilizando soporte o ayuda suficiente para sostener el chasis hasta fijar completamente los puntos de anclaje.

    b) Mantener una ventilación adecuada, evitando bloquear el flujo de aire del chasis según la guía de instalación del modelo.

    c) Conectar la alimentación principal y, si existe, la alimentación redundante. Cuando el fabricante lo recomiende, utilizar un dispositivo de protección contra sobretensiones (SPD) en la entrada de alimentación AC.

    d) Esperar al arranque completo del sistema antes de proceder a la configuración de red.

26. **CONFIGURACIÓN INICIAL DE DIRECCIÓN IP DE GESTIÓN:** La configuración inicial de la dirección IP de gestión se debe realizar preferentemente por el puerto CRAFT/serie. Configurar inicialmente la dirección IP de gestión a través del puerto CRAFT/serie o de la interfaz equivalente con funcionalidad CRAFT, (Guías de usuario incluidas en REF2, sección *Direct connect through the CRAFT serial port interface*).

    - **Parámetros serie**: Para la configuración inicial por CRAFT/serie, la documentación de la familia utiliza parámetros de consola de 115200 baudios, 8 bits de datos, 1 bit de parada y sin paridad.
    - **Referencia de modelo**: Para detalles físicos específicos de cada modelo deben consultarse las Installation Guides correspondientes disponibles en el portal de soporte de Keysight (ver REF2 en este documento).

27. Tras establecer la conectividad por la red administrativa, es posible conectarse al equipo a través de la consola web con el usuario Administrador por defecto. Las modificaciones posteriores de password para el usuario admin o de IP, máscara, gateway o parámetros IPv6 podrán realizarse desde la consola web. Adicionalmente, si fuera necesario, es posible realizar el cambio del pasword para el usuario administrador por defecto (admin) desde el acceso por el puerto serie.

28. Debe tenerse en cuenta que cualquier modificación de la configuración IP de gestión reinicia el sistema o la conectividad de administración y fuerza la desconexión de los usuarios activos. En consecuencia, esta operación deberá ejecutarse en ventana de mantenimiento y conservando acceso alternativo por consola local.

    a) Iniciar sesión con una cuenta administradora.

    b) Acceder a System > Settings.

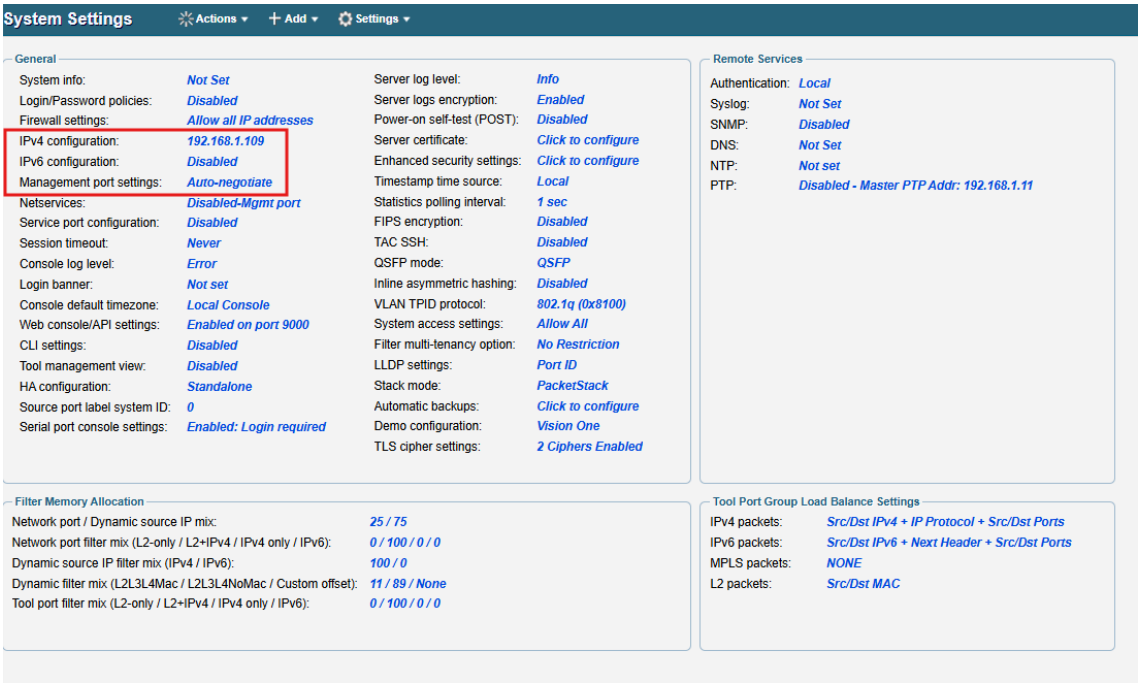

Figura 2. Vista de la sección System > Settings. Configuración puerto de gestión

c) Abrir el enlace de configuración IPv4/IPv6.

d) Introducir dirección, máscara/prefijo y gateway.

e) Confirmar la operación.

f) Reconectar posteriormente utilizando la nueva dirección configurada.

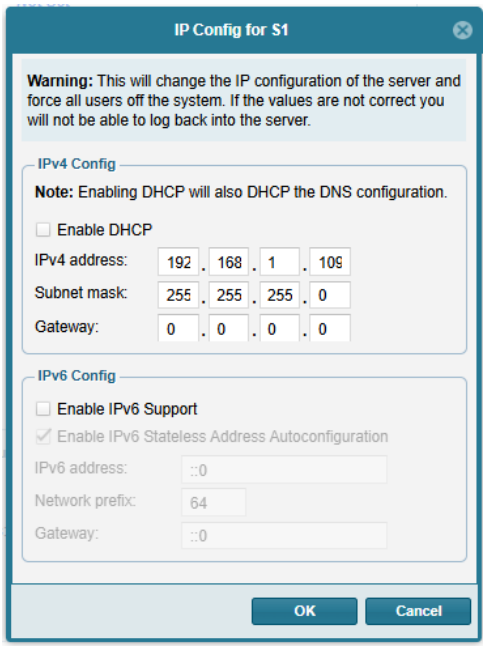

Figura 3. Ventana de configuración de la IP del puerto de gestión

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

29. La configuración segura del producto se basa en la segregación del puerto de gestión, el empleo de servicios administrativos seguros, la limitación del acceso por allowlist, la autenticación robusta, la trazabilidad de los eventos y la gestión controlada de certificados.
30. Las Guías de usuario de cada modelo incluyen un capítulo llamado ***Government Security Configuration Guide*** dedicado a proporcionar los pasos necesarios para una configuración alineada con requisitos gubernamentales o de *common criteria.* Las áreas de configuración a tener en cuenta son:
    a) Habilitar la autenticación local.
    b) Configurar la consola del puerto serie (CRAFT).
    c) Configurar el banner de inicio
    d) Configurar el certificado del servidor para la comunicación Web API/GUI y generar y cargar certificados.
    e) Habilitar las funciones de seguridad mejoradas.
    f) Configurar el tiempo de espera de la sesión (consola web).
    g) Configurar el servicio Web API.
    h) Habilitar el cifrado FIPS para los datos del servidor Vision Network Packet Broker (NPB) cuando el perfil lo requiera.
    i) Configurar la cuenta de administrador predeterminada ("admin") con acceso únicamente a la consola del puerto serie (CRAFT).
    j) Configurar los servidores Syslog si se desea utilizar Syslog.
    k) Habilitar la autenticación en los servidores NTP, si los hay.
31. En consecuencia, el modo de operación seguro de la familia debe basarse en la segregación del puerto de gestión, el uso exclusivo de HTTPS/TLS para administración web, la limitación del acceso por allowlist, la autenticación robusta, el registro de eventos y el empleo de certificados propios de la organización en lugar del certificado por defecto del sistema
32. **HABILITAR LA AUTENTICACIÓN LOCAL:** La autenticación local debe utilizarse como modo base de administración segura del sistema y debe considerarse obligatoria cuando el despliegue requiera un perfil reforzado de cumplimiento. El Government Security Configuration Guide de la familia Vision indica expresamente que, para configurar el equipo conforme a requisitos gubernamentales, debe seleccionarse el modo Local en el campo Authentication Mode dentro de System > Settings.

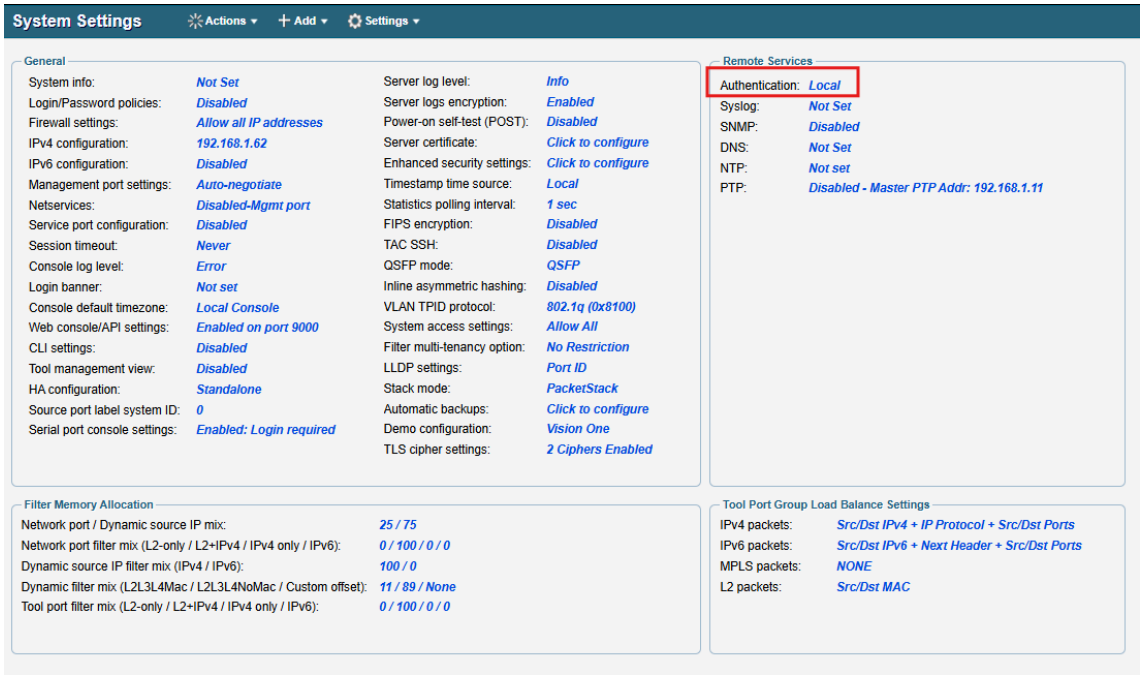

Figura 4. Vista de la sección System > Settings. Configuración de autenticación local

33. En la opción *Login/Password policies* deben activarse las políticas de contraseñas del conjunto DoD Policies, que constituyen la referencia recomendada para este perfil. Ver en este documento la sección 6.3.2.

34. En la configuración local, el sistema permite definir la expiración de contraseñas, la longitud mínima y las reglas de bloqueo de usuarios. Para cumplimiento gubernamental, la longitud mínima por defecto es de 15 caracteres y que deben emplearse, como mínimo, los valores por defecto de 35 días de inactividad y 3 intentos consecutivos fallidos para el bloqueo de usuarios. Asimismo, al modificar la política de contraseñas el sistema cierra las sesiones activas, y los usuarios deberán cambiar su contraseña en el siguiente acceso si esta deja de cumplir la nueva política.

35. Debe tenerse en cuenta que, según la documentación del fabricante, los modos **RADIUS** y **TACACS+** no son compatibles con operación **FIPS**, por lo que no deben utilizarse cuando el despliegue requiera dicho perfil.

36. **CONFIGURACIÓN Y PROTECCIÓN DEL PUERTO SERIE: El puerto CRAFT/serie no debe utilizarse como mecanismo ordinario de administración remota**. Su uso quedará reservado a la provisión inicial, recuperación de acceso, ejecución de diagnósticos y soporte presencial autorizado.

37. Se debe configurar autenticación obligatoria en la consola serie, fijar un tiempo de sesión reducido y mantener la capacidad de acceso únicamente para personal administrador autorizado. La guía de seguridad gubernamental exige habilitar el acceso al menú, activar *Require login*, mantener desactivada la opción *Disable login* y establecer un Session timeout apropiado en Serial port console settings. Debe configurarse también, si procede, un banner de advertencia para la consola local. Estas configuraciones se podrán realizar desde la consola Web:

    a) Acceder a la consola web con una cuenta con privilegios de administración.

b) Seleccionar System > Settings y abrir el enlace correspondiente a la configuración del puerto serie.

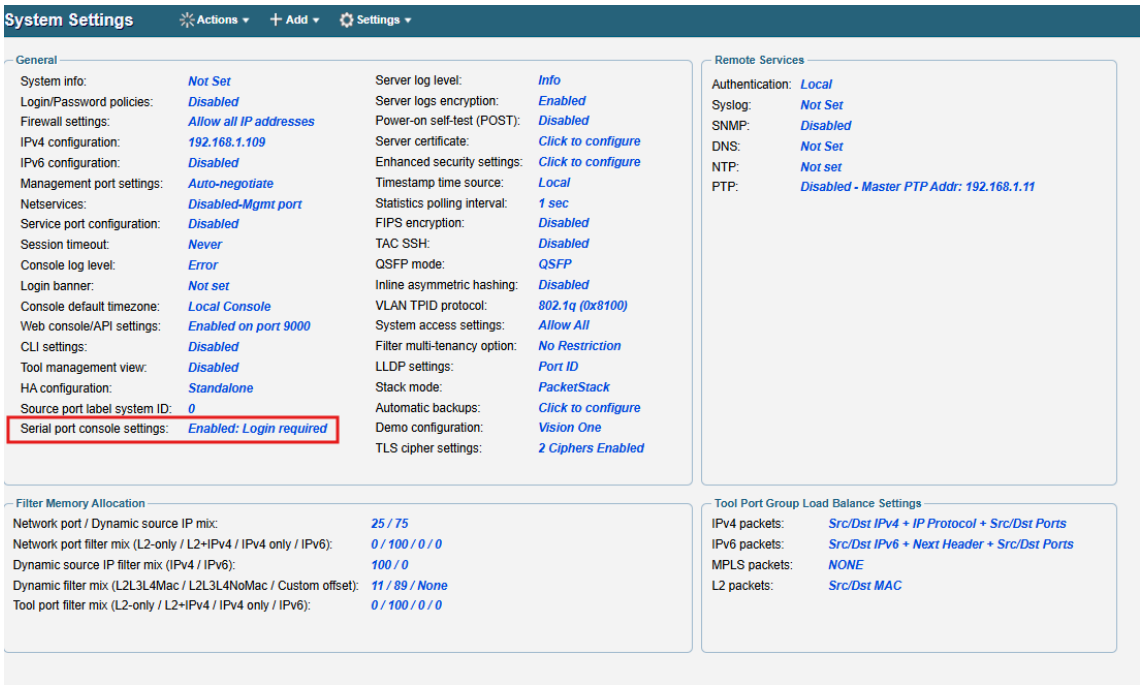

Figura 5. Vista de la sección System > Settings. Serial port console settings

c) Activar la opción “Require login”.

d) Mantener desmarcada la opción que deshabilita el inicio de sesión, salvo necesidad expresa y controlada.

e) Fijar un tiempo de sesión acorde con la política de la organización.

f) Si la política lo exige, configurar un banner de advertencia para la consola local.

g) Guardar la configuración y verificar mediante una prueba controlada que el inicio de sesión en la consola local exige autenticación y que la expiración de la sesión funciona conforme a lo establecido.

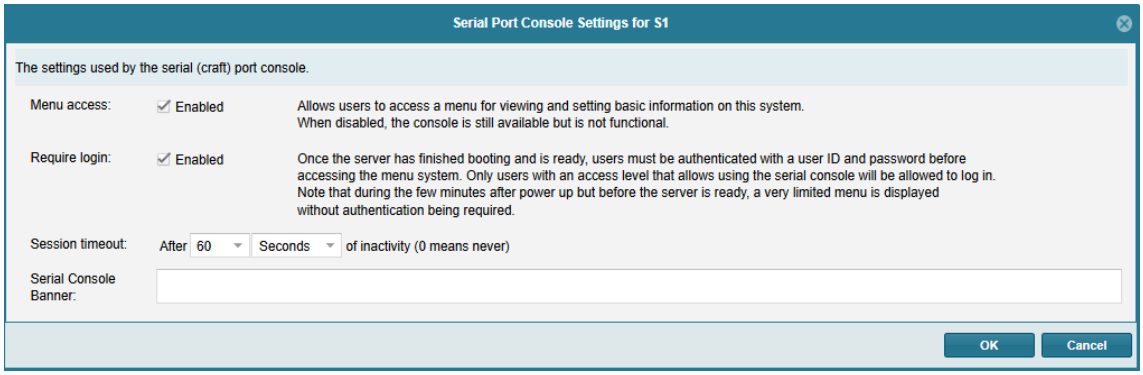

Figura 6. Vista de la sección System > Settings. Serial port console settings

38. **REDUCCIÓN DE LA SUPERFICIE DE ATAQUE DEL PUERTO DE GESTIÓN:** El acceso al puerto de gestión se debe limitar a una red administrativa dedicada y a una lista explícita de direcciones o subredes autorizadas. No se debe permitir acceso administrativo desde redes de usuario, segmentos de herramientas ni redes no gestionadas.

a) Comprobar que existe acceso alternativo por consola CRAFT/serie para recuperación ante un error de configuración.

b) Acceder a System > Settings.

c) Abrir “Firewall settings”.

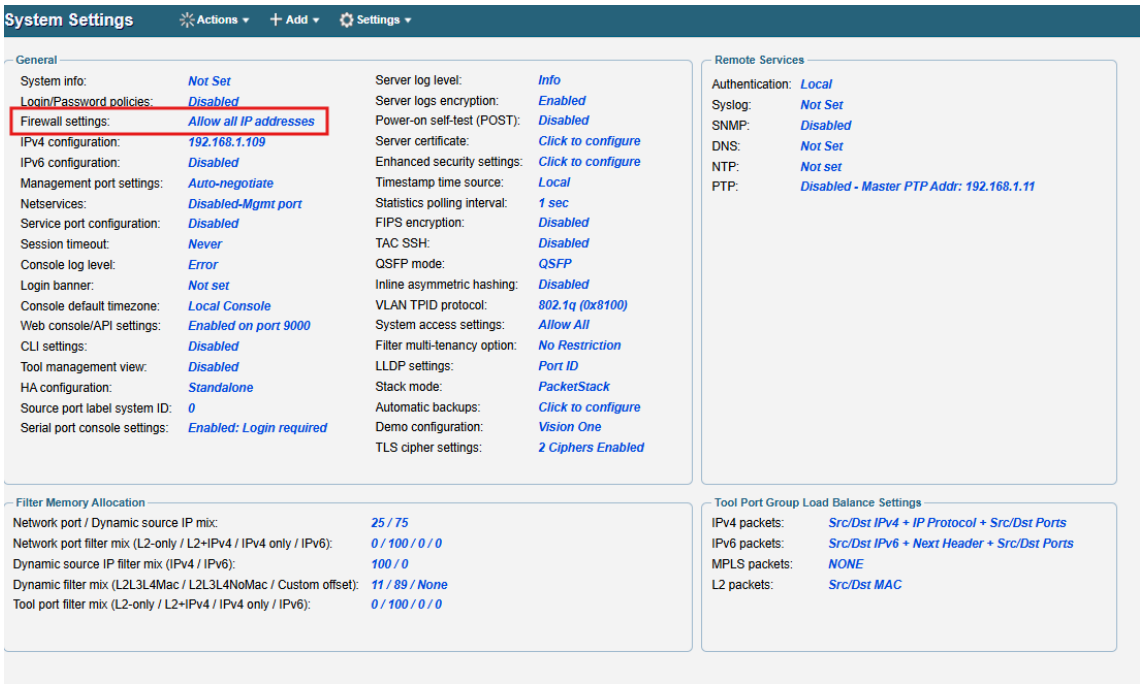

Figura 7. Vista de la sección System > Settings. Firewall settings

d) Configurar la allowlist de direcciones o subredes de confianza.

e) Aplicar la configuración.

f) Validar el acceso desde una estación autorizada.

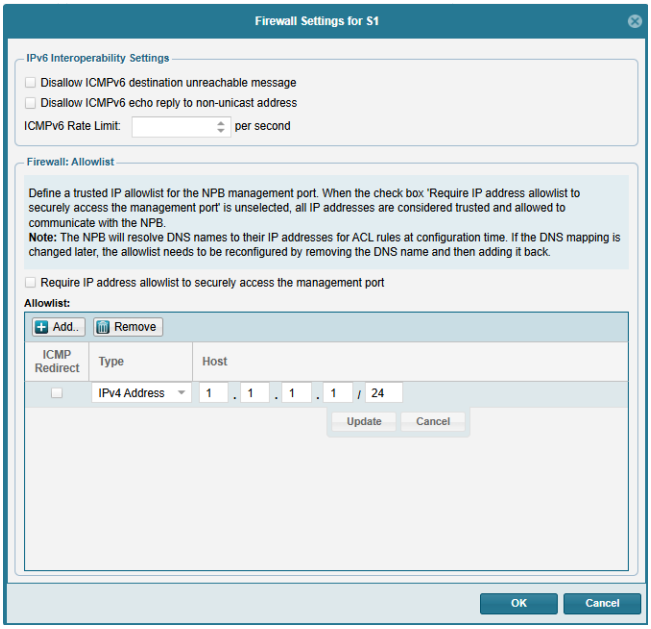

Figura 8. Interfaz asociada a la allowlist / firewall de gestión

39. **BANNER DE ACCESO:** Se debe configurar un banner de advertencia previo al inicio de sesión, visible para todo usuario que acceda a la consola web. El banner debe informar del carácter restringido del sistema y de la posibilidad de monitorización y auditoría. No debe incluir información sensible sobre la topología, el entorno o la misión del sistema.

    a) Acceder a System > Settings.

    b) Abrir "Login banner"

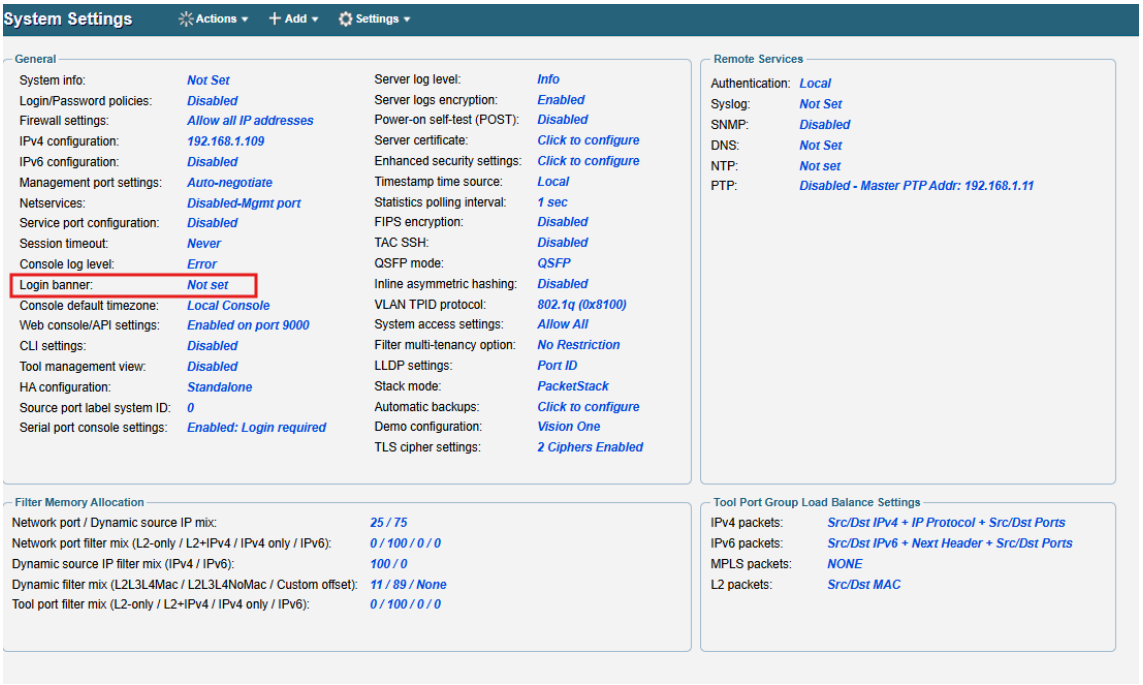

Figura 9. Vista de la sección System > Settings. Login banner

    c) Introducir el texto requerido.

    d) Guardar la configuración.

    e) Verificar que el mensaje se muestra correctamente en el cuadro de acceso.

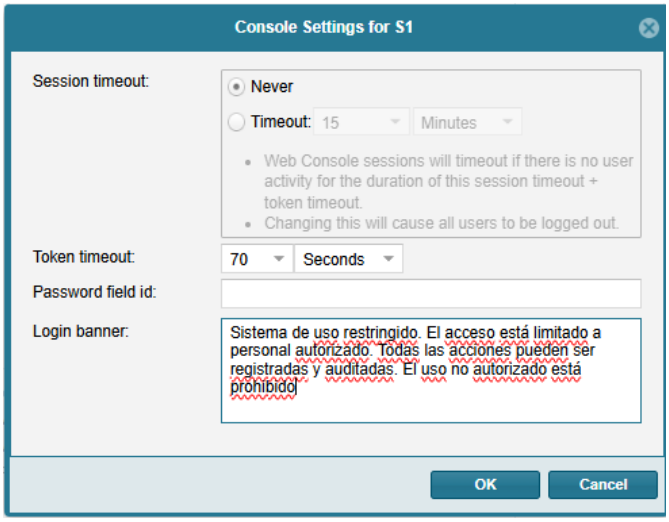

Figura 10. Ventana de configuración del banner de acceso.

40. Texto de referencia sugerido: “Sistema de uso restringido. El acceso está limitado a personal autorizado. Todas las acciones pueden ser registradas y auditadas. El uso no autorizado está prohibido.”

41. **CERTIFICADO DE SERVIDOR Web API / GUI:** La administración web y la Web API deben operar exclusivamente sobre HTTPS con cifrado seguro (mínimo TLS 1.2) No se debe mantener en explotación el certificado por defecto del equipo cuando el entorno exija identidad criptográfica verificable.

42. Se debe generar una solicitud de firma de certificado (CSR) específica para cada equipo y cargar posteriormente un certificado emitido por una autoridad de certificación autorizada para la organización o para el entorno evaluado. El certificado deberá vincularse al nombre de dominio o a la dirección del sistema, según la política aplicable.

    a) Acceder a System > Settings > Server Certificate.

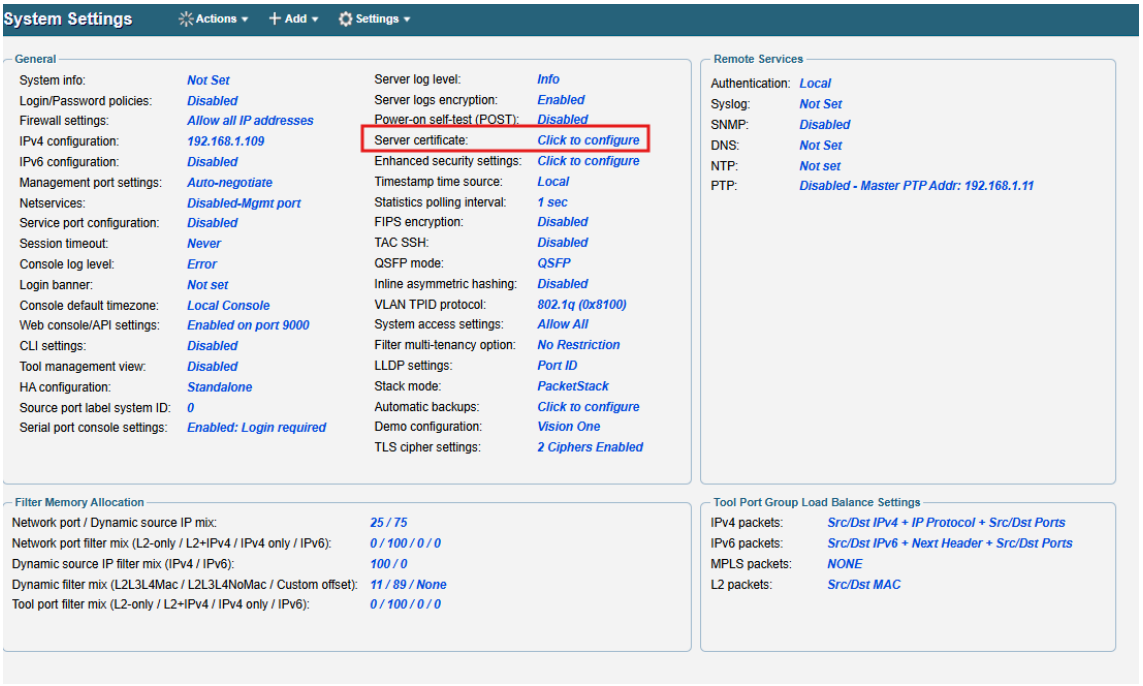

Figura 11. Vista de la sección System > Settings. Configuración de *Server Certificate*

    b) Seleccionar la opción de generación de CSR (“Get CSR”).

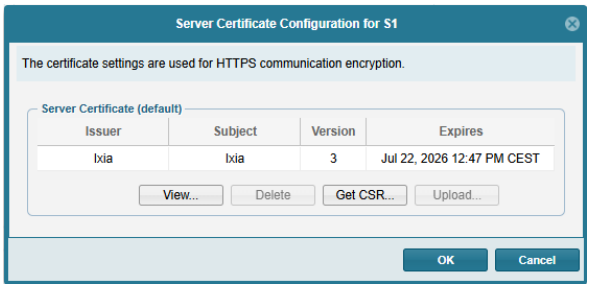

Figura 12. Interfaz de gestión del certificado de servidor y CSR

    c) Cumplimentar los campos requeridos.

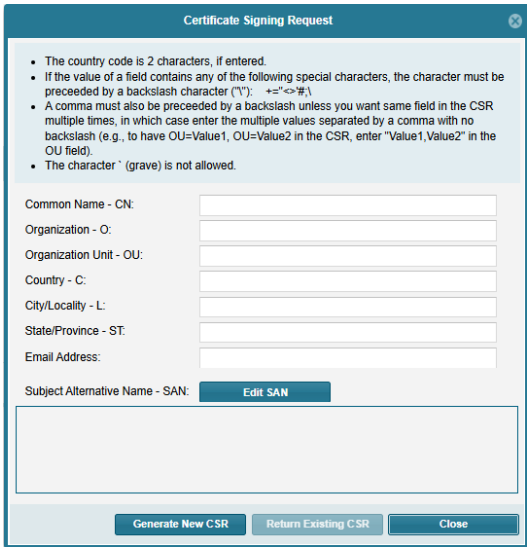

Figura 13. Interfaz para la generación de CSR

d) Descargar la solicitud generada.

e) Tramitar la firma del CSR ante la CA autorizada.

f) Cargar el certificado emitido en la misma pantalla.

g) Verificar el acceso HTTPS y la ausencia de advertencias de identidad no confiable en el cliente autorizado.

43. **ENHANCED SECURITY SETTINGS, WEB API Y TIEMPO DE ESPERA DE LAS SESIONES:** Se debe minimizar la exposición de servicios administrativos. La Web API sólo deberá permanecer habilitada cuando exista una necesidad operacional justificada de automatización o integración. Cuando la plataforma ofrezca la opción, HTTP en claro debe permanecer deshabilitado y la administración web debe concentrarse en HTTPS.

44. Se debe configurar un tiempo de expiración de la sesión web y un tiempo de token para Web API. El timeout de la sesión web debe ser superior al timeout del token Web API. Igualmente, se debe limitar el número máximo de sesiones concurrentes por usuario, evitando valores ilimitados salvo justificación formal.

- **Perfil general**: Se recomienda fijar 15 minutos como timeout de sesión y un valor de token Web API inferior y compatible con la operación.
- **Perfil gubernamental**: Se recomienda limitar a una (1) las sesiones concurrentes por usuario y mantener un token timeout de 70 segundos o inferior, siempre que la operación lo permita.

a) Acceder a System > Settings.

b) Revisar “Enhanced Security Settings” y “Web console/API settings”.

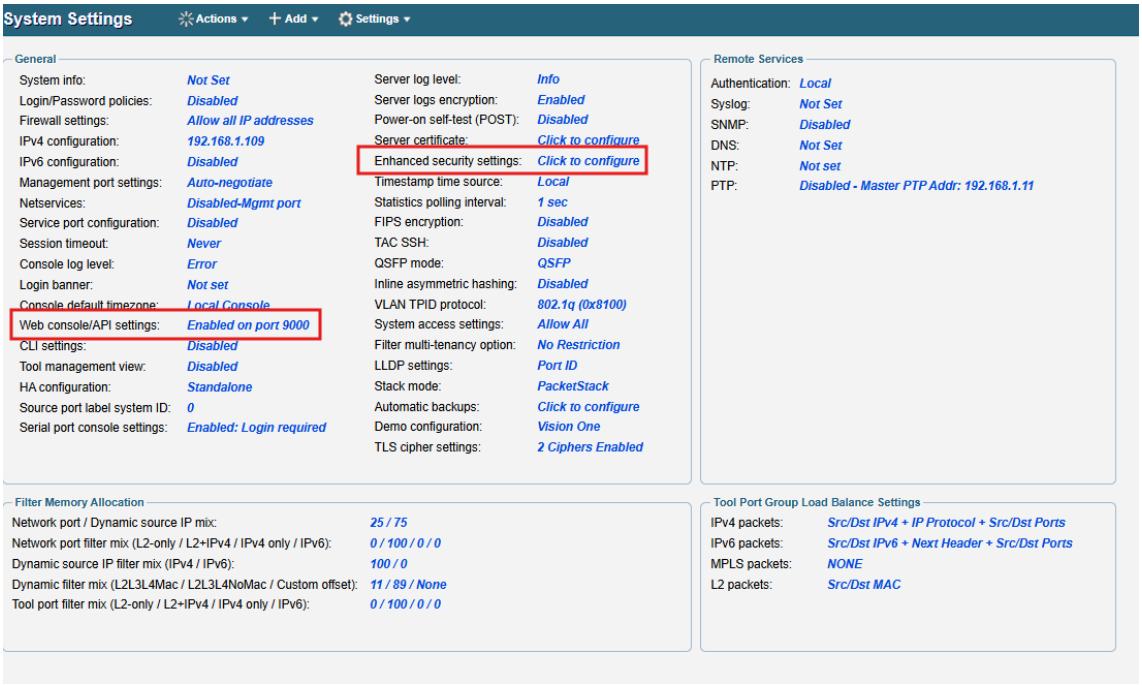

Figura 14. Vista de la sección System > Settings. Configuración avanzada de seguridad y sesiones Web/API

c) Deshabilitar HTTP si la opción está disponible.

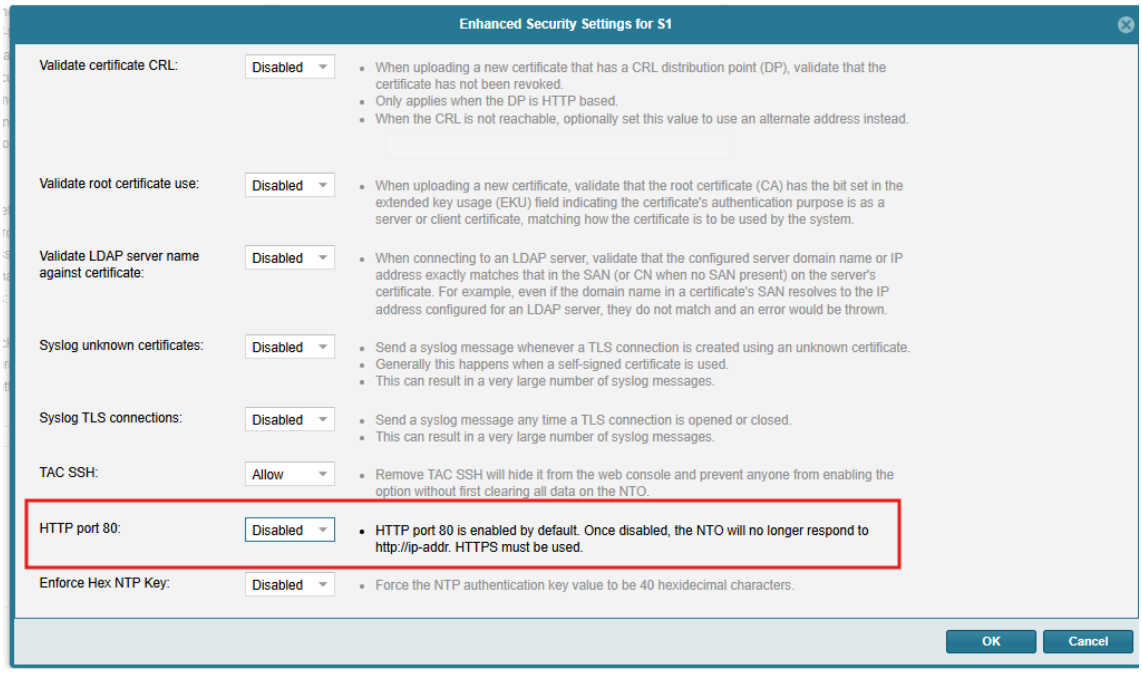

Figura 15. Deshabilitar HTTP en *Enhanced Security Settings*

d) Habilitar la Web API en el puerto deseado (Puerto 8000 por defecto)

e) Definir el número máximo de sesiones concurrentes por usuario (Web API y Web Console).

f) Definir el timeout de sesión y el token timeout, garantizando que el primero sea superior al segundo.

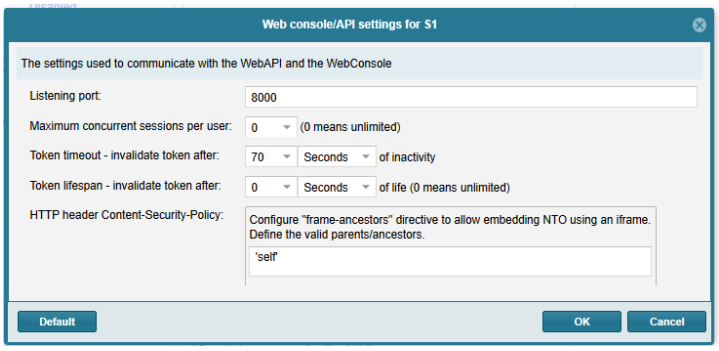

Figura 16. Interfaz de configuración de Web Console / Web API

45. **HABILITAR EL CIFRADO FIPS PARA LOS DATOS DEL SERVIDOR VISION NETWORK PACKET BROKER (NPB) CUANDO EL PERFIL LO REQUIERA**: Cuando el entorno de despliegue exija operación en modo FIPS, debe habilitarse el modo de cifrado **FIPS Encryption** desde la consola web. La documentación indica que este modo obliga al uso de algoritmos criptográficos aprobados FIPS y activa requisitos adicionales de seguridad, entre ellos **auto-chequeos**, **zeroization** y comprobaciones de integridad en el arranque. Además, el sistema modifica su comportamiento operativo para ajustarse a las restricciones FIPS, impidiendo, por ejemplo, el downgrade a versiones anteriores a la 4.5.

46. El procedimiento consiste en abrir el cuadro de diálogo de **FIPS encryption** desde **System > Settings > FIPS encryption** y habilitar dicho modo. La activación de FIPS provoca el cierre de todas las sesiones activas y el reinicio del servidor. Tras el reinicio, los datos del servidor pasan a quedar cifrados utilizando algoritmos conformes con FIPS. Debe tenerse en cuenta que, una vez habilitado este modo, su desactivación no es una operación ordinaria: solo puede realizarse mediante **File > Clear System**, lo que devuelve el equipo al modo no FIPS y **borra toda la configuración**, en la práctica equivalente a un reseteo de fábrica. Por este motivo, la decisión de habilitar FIPS debe adoptarse únicamente cuando exista un requisito formal del entorno.

47. El procedimiento recomendado es el siguiente:

    a) Acceder a System > Settings.

    b) Abrir el enlace correspondiente a **FIPS encryption**.

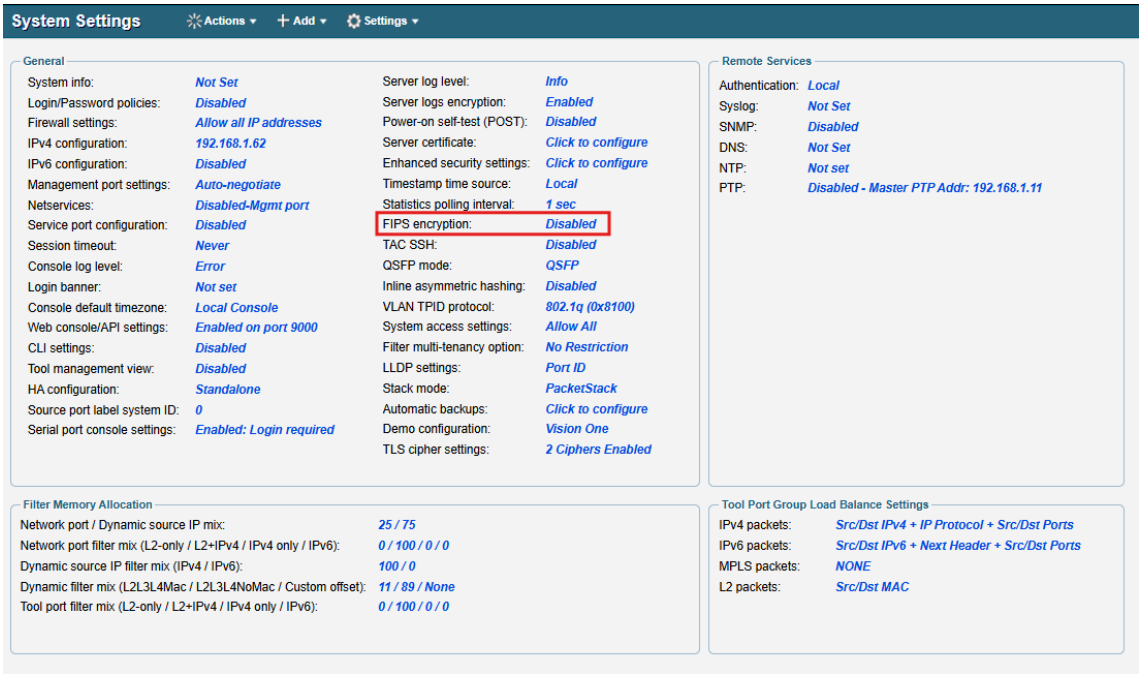

Figura 17. Vista de la sección System > Settings. Configuración FIPS encryption

c) Revisar el aviso del sistema sobre el cambio de comportamiento operativo en modo FIPS.

d) Confirmar la activación del modo FIPS.

e) Aceptar el cierre de sesiones y el reinicio del appliance.

f) Tras el arranque, iniciar sesión nuevamente y verificar que el modo FIPS ha quedado habilitado.

48. Debe documentarse previamente un backup completo de la configuración y un procedimiento de contingencia, ya que la desactivación posterior del modo FIPS exige un **Clear System** con pérdida de configuración. Asimismo, cuando se opere en FIPS deberán evitarse configuraciones no compatibles, en particular el uso de **RADIUS** y **TACACS+** como mecanismos de autenticación administrativa.

49. **CONFIGURAR LA CUENTA DE ADMINISTRADOR PREDETERMINADA ("ADMIN"):** La cuenta “admin” por defecto no debe utilizarse para la administración ordinaria del sistema. En el perfil general se recomienda reservarla como cuenta de contingencia. En el perfil gubernamental / Common Criteria, dicha cuenta se debe restringir a acceso exclusivo por consola serie, manteniendo al menos otra cuenta nominal con privilegios administrativos para la gestión ordinaria del sistema. Para ello:

a) Acceder a Objects > Users.

b) Crear y validar una cuenta administrativa nominal adicional

c) Abrir las propiedades de la cuenta “admin”.

d) Fijar su nivel de acceso a “Serial Console Access Only” cuando aplique el perfil gubernamental.

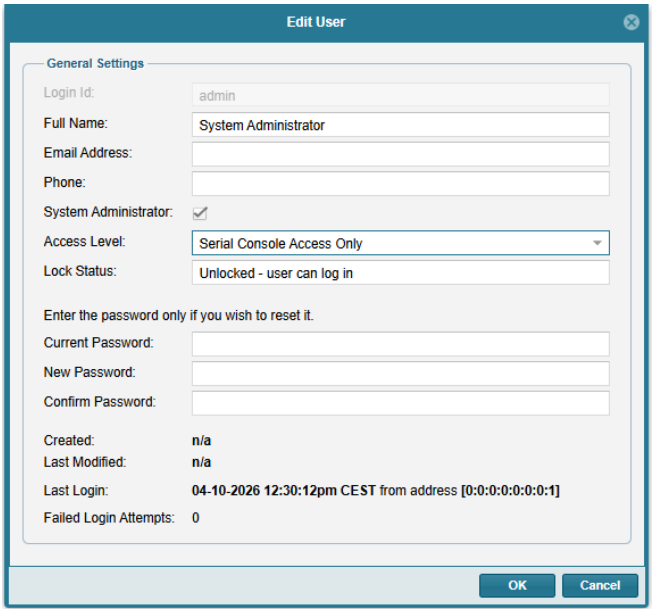

Figura 18. Interfaz de configuración de cuenta "admin"

e) Custodiar las credenciales de la cuenta "admin" conforme al procedimiento de contingencia de la organización.

50. **CONFIGURAR LOS SERVIDORES SYSLOG**: Se debe configurar el envío de registros a servidores syslog corporativos o del entorno evaluado. Para el perfil gubernamental/CommonCriteria, el transporte entre el Vision Packet Broker y el servidor syslog debe protegerse mediante TLS 1.2 o superior.

    a) Acceder a System > Settings > Syslog.

    b) Añadir el servidor o servidores autorizados.

    c) Definir host, puerto, facility y TLS.

    d) Cargar los certificados necesarios conforme a la política del entorno.

    e) Guardar la configuración.

    f) Generar un evento de prueba y confirmar su recepción en el colector autorizado.

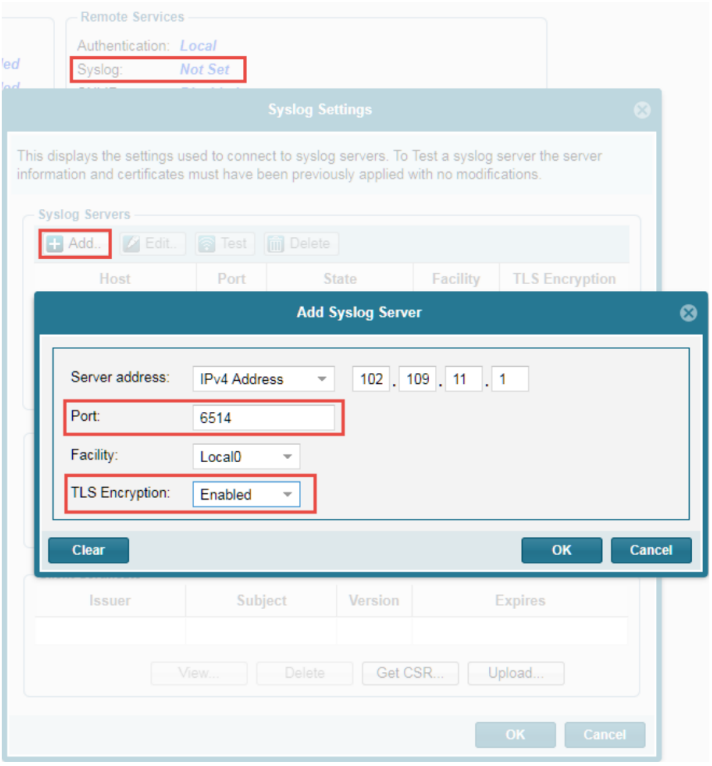

Figura 19. Interfaz de configuración de servidores syslog externos

51. **HABILITAR LA AUTENTICACIÓN EN LOS SERVIDORES NTP:** Acceda a los servidores NTP a través de System > Settings > NTP. Asegúrese de que todos los servidores tengan el estado de autenticación habilitado. Ver guías de usuario en el portal de soporte de Keysight (ver REF2 en este documento)) para más detalles sobre la configuración de servidores NTP.

    a) Acceder a System > Settings > NTP.

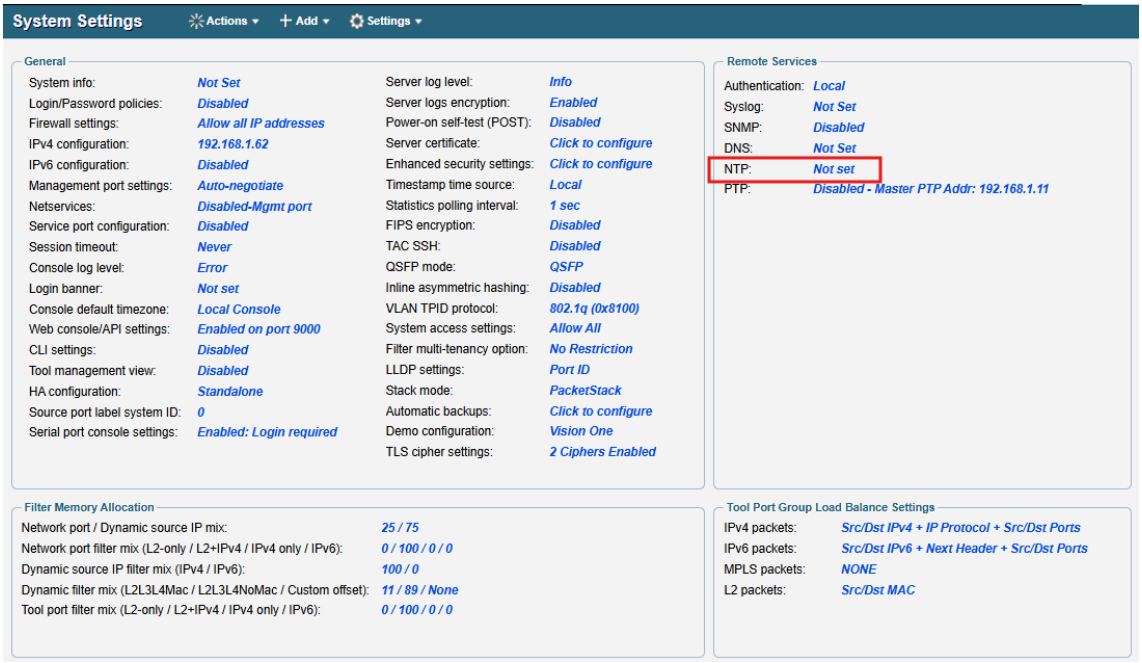

Figura 20. Vista de la sección System > Settings. Configuración de NTP

b) Habilitar NTP Services (Enabled)

c) Añadir los servidores NTP (por ip o hostname) y habilitar la autenticación para cada uno de ellos.

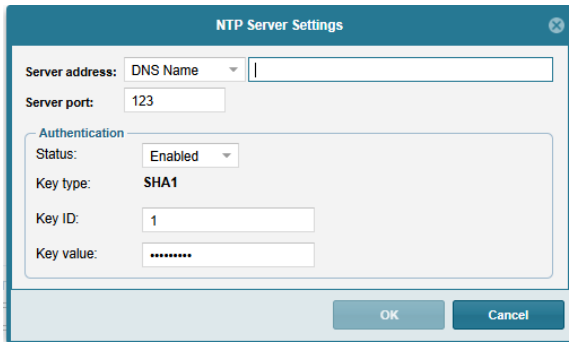

Figura 21. Ventana de configuración de servicio NTP

d) Guardar la configuración.

52. **DNS:** La resolución DNS sólo debe configurarse cuando el despliegue lo requiera para servicios como Syslog, NTP, LDAP/TLS o descarga de actualizaciones. Los servidores definidos deberán pertenecer a la infraestructura autorizada de la organización y no deberán abrir dependencias innecesarias hacia redes no controladas.

a) Acceder a System > Settings > DNS.

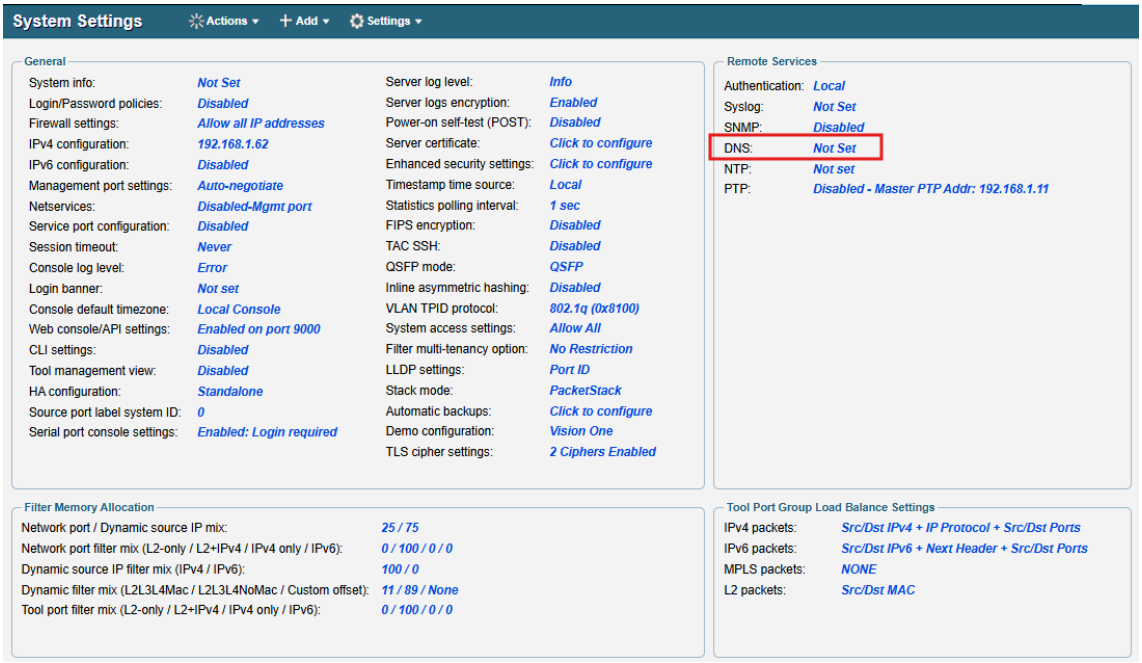

Figura 22. Vista de la sección System > Settings. Configuración de DNS

b) Definir servidor DNS preferente y, si procede, alternativo.

c) Definir los sufijos de búsqueda únicamente si son necesarios.

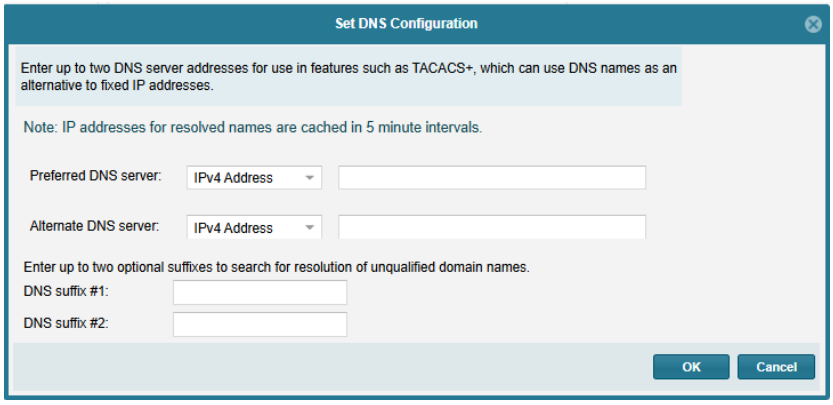

Figura 23. Ventana de configuración de servicio DNS

d) Guardar la configuración.

e) Verificar la resolución de los servicios administrativos que dependan de DNS.

6.2 AUTENTICACIÓN

53. Además de autenticación local, el producto soporta integración con TACACS+, RADIUS y LDAP. Cuando se utilicen servicios externos de autenticación en el perfil general, deberán desplegarse mediante configuraciones seguras y con un procedimiento documentado de recuperación del acceso administrativo.

54. No obstante, para un perfil de cumplimiento reforzado (Common Criteria) debe optarse por autenticación local o LDAP con TLS.

55. En la documentación se indica expresamente que TACACS+ y RADIUS no son FIPS compliant, por lo que no deben emplearse cuando el despliegue requiera operación en FIPS/DoD según ese perfil.

56. LDAP puede configurarse en modo estándar o con TLS. LDAP con TLS se presenta como opción 'Secure Common Criteria NDcPP v2.1 compliant LDAP'. Al activar Enable TLS, las sesiones entre el servidor LDAP y el Packet Broker quedan cifradas con TLS 1.2, usando STARTTLS o LDAPS durante el handshake.

57. Para LDAP con TLS se debe activar Enable TLS en el diálogo Add/Edit LDAP Server, utilizar preferentemente el puerto 636 o, cuando la arquitectura lo exija, 389 con STARTTLS, y cargar el certificado raíz de confianza del servidor LDAP en la sección LDAP Server Authentication Certificate. Tras guardar la configuración, debe reabrirse el diálogo y usarse el botón Test para comprobar la alcanzabilidad del servidor.

58. En LDAP puede mantenerse Authorization = Default, donde todos los usuarios autenticados son regulares, o Authorization = Custom, definiendo grupos de administradores y de usuarios regulares devueltos por el servidor LDAP. La asignación a grupos es remota y no se basa en grupos locales definidos previamente en el NPB.

59. Se recomienda revisar la documentación indicada en REF2 sobre la configuración de servicios de autenticación. En concreto, el resumen del procedimiento descrito para LDAP sería:

    a) Acceder a System > Settings > Authentication Mode y seleccionar LDAP cuando proceda.

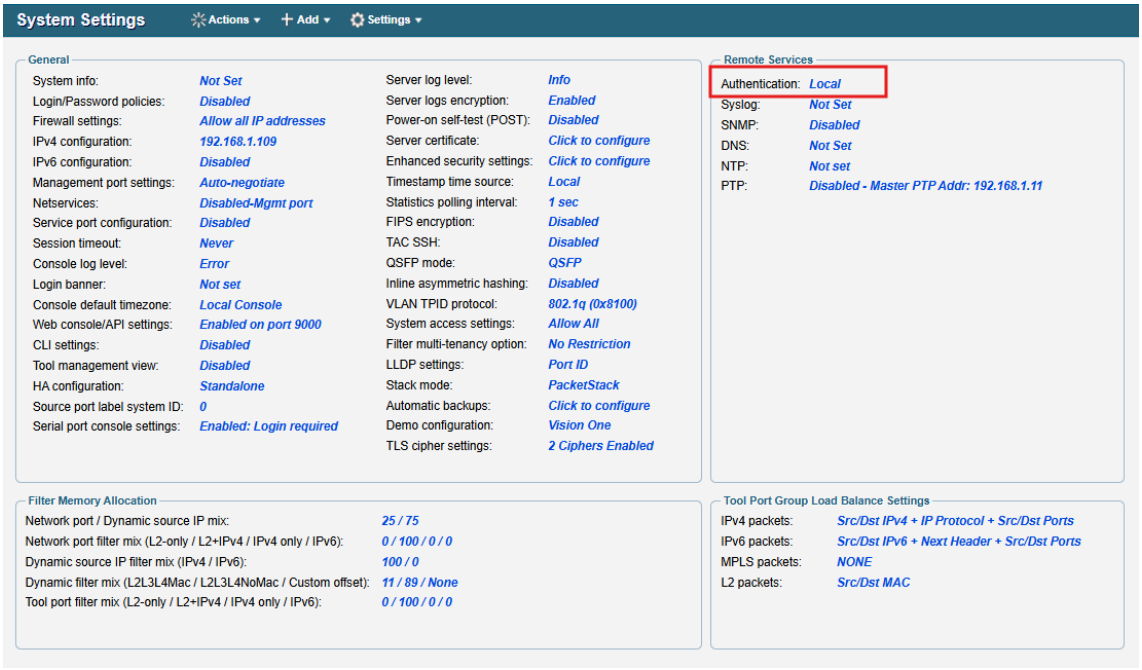

Figura 24. Vista de la sección System > Settings. Sección de Autenticación.

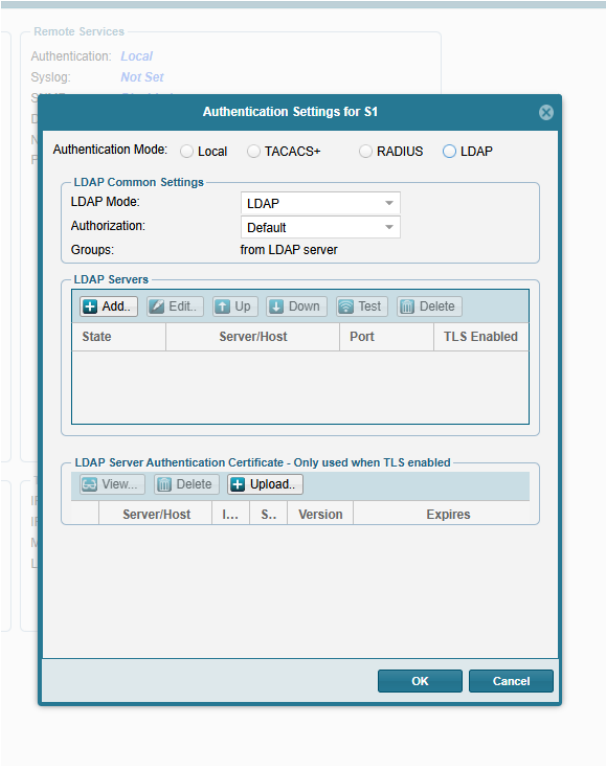

Figura 25. Menú de autenticación para LDAP

b) En LDAP Common Settings, elegir el modo de operación y el tipo de autorización (Default o Custom).

c) En Add/Edit LDAP Server, introducir dirección, Base DN, tiempo de espera y reintentos.

d) Activar Enable TLS y utilizar preferentemente el puerto 636; usar 389 solo cuando el entorno use STARTTLS.

e) Cargar el certificado raíz de confianza del servidor LDAP en la sección LDAP Server Authentication Certificate.

f) Guardar, volver a abrir la configuración y ejecutar Test para validar conectividad y asociación del certificado.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

60. La administración local podrá realizarse por el puerto CRAFT/serie para provisión inicial, recuperación y mantenimiento presencial autorizado. La administración remota se realizará por la consola web y, cuando proceda, por WebAPI siempre bajo mecanismos seguros.
61. Otros métodos de acceso o administración del equipo están deshabilitados. Si fuera necesario, se podría activar un acceso SSH sólo para tareas de soporte del fabricante (TAC SSH) o un acceso CLI (SSH) en un puerto configurable. Ambas opciones se pueden habilitar si fuera necesario en el menú Settings.
62. En el apartado 6.1 se han indicado los pasos necesarios para asegurar que el acceso por puerto serie y a través de la Web console o el Web API (desactivación de HTTP para el acceso Web y la configuración del Server certificate)
63. El appliance admite la versión 1.2 del protocolo TLS (rechazando cualquier otra versión, incluyendo SSL 2.0, SSL 3.0, TLS 1.0 y TLS 1.1, así como cualquier otra cadena de versión TLS desconocida). Los conjuntos de cifrado están restringidos a los siguientes:
    a) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, según se define en la RFC 5289
    b) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, según se define en la RFC 4492
64. Para una configuración segura se recomienda activar únicamente la opción a anterior
65. Los conjuntos de cifrado se pueden habilitar/deshabilitar como se explica en los manuales de usuario a los que se hace referencia, de modo que solo se utilicen los conjuntos de cifrado permitidos según el nivel de seguridad requerido.
    a) Acceder a System > Settings > TLS cipher settings.

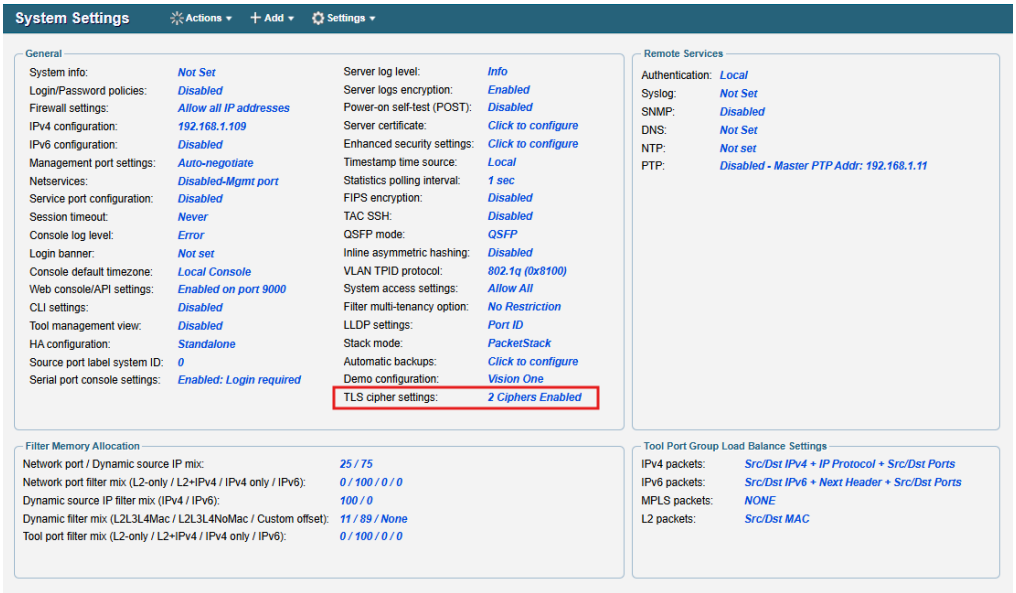

Figura 26. Vista de la sección System > Settings. Configuración de cifrados

b) Seleccionar o deseleccionar los cifrados que están permitidos. Se adjunta una captura de pantalla de la ventana de configuración de los conjuntos de cifrado permitidos para cumplir con la norma "ENS Alta".

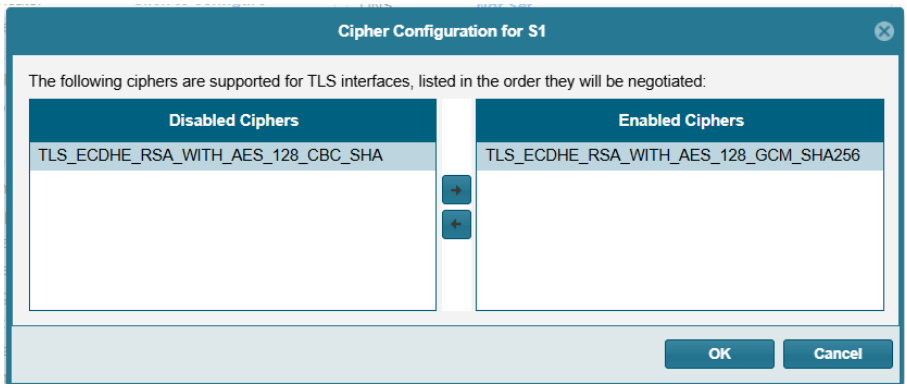

Figura 27. Configuración recomendada de cifrado

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

66. La operación ordinaria del sistema debe realizarse mediante cuentas nominales y permisos mínimos. El control de administradores debe articularse por roles y por nivel de acceso. El Government Security Configuration Guide establece que la cuenta admin por defecto no puede utilizarse para acceso a web console o para autenticación de comandos de Web API, porque no puede bloquearse; por ello debe cambiarse para que solo tenga acceso por consola serie.

67. Antes de aplicar esta restricción debe existir al menos otra cuenta con privilegios de administrador y nivel de acceso Default o All. La modificación se realiza en Objects > Users > admin > Properties, cambiando Access Level a Serial Console Access Only.

68. En las Guías de Usuario de cada modelo (acceder al portal de soporte de Keysight con el link incluido en la referencia REF2 en este documento) se puede encontrar el capítulo

"Manage Users" con los detalles relacionados con la creación y configuración de los diferentes usuarios y grupos de usuarios.

69. Existen dos roles principales para el equipo: "System Administrator" o usuario sin capacidad de administrador. Esto se indica en las propiedades del usuario creado y sólo se pueden configurar con un usuario administrador.

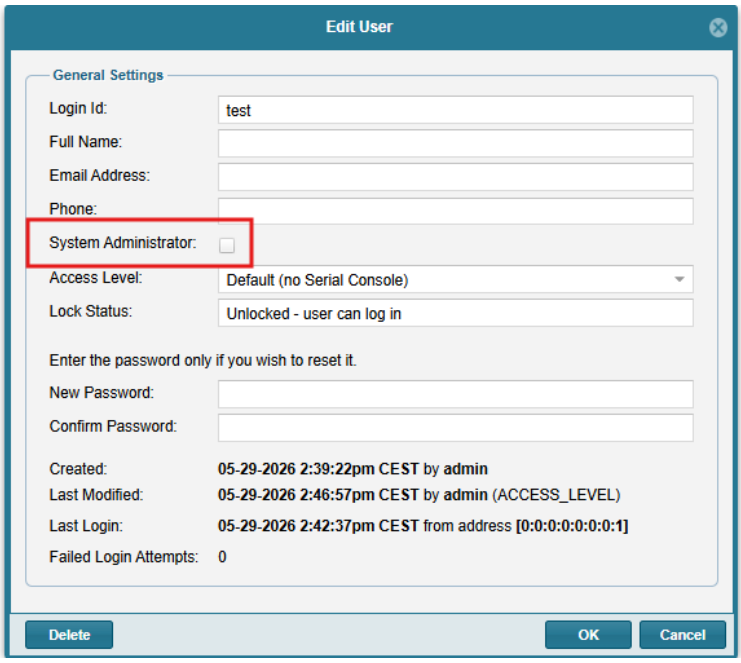

Figura 28. Vista de propiedades de un usuario

70. Los usuarios se pueden asignar a diferentes grupos y un usuario administrador podrá asignar los permisos adecuados (acceso, modificación, etc.) de una manera granular para cada uno de los componentes y capacidades del equipo (configuración de un puerto, modificación de filtros, etc.) En las guías de usuarios que se pueden encontrar en el portal de soporte de Keysight (ver enlace en referencia REF2 en este documento) y se puede encontrar los detalles de configuración de las políticas de control de acceso (Capítulo *Define Access Control Policies)* para cada elemento (puertos, filtros, etc.).

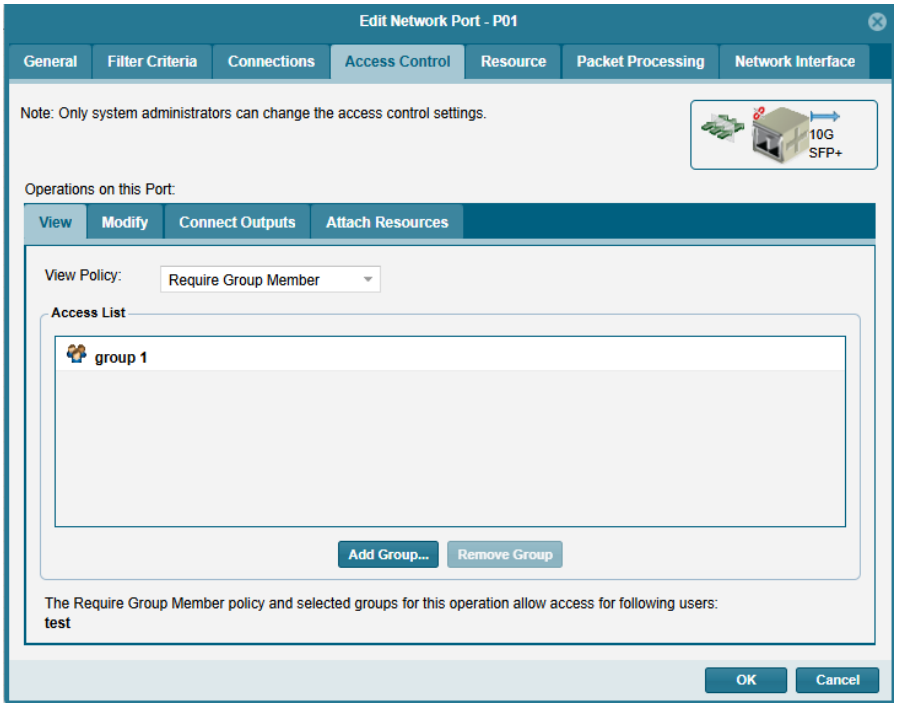

Figura 29. Ejemplo de configuración de control de acceso para un puerto para el *Group 1*

71. **Configuración de la Política segura de contraseñas y parámetros de sesión**: Las cuentas locales deben someterse a una política de contraseñas robusta. Para el perfil general se recomienda una longitud mínima de 12 caracteres. Para el perfil gubernamental se deben aplicar políticas DoD con longitud mínima de 15 caracteres.

72. La plataforma debe configurarse para bloquear usuarios tras un número reducido de intentos fallidos consecutivos y para gestionar adecuadamente la inactividad de las cuentas. En el perfil gubernamental, la guía indica como referencia tres (3) intentos fallidos y 35 días de inactividad.

    a) Acceder a System > Settings > Login/Password Policies.

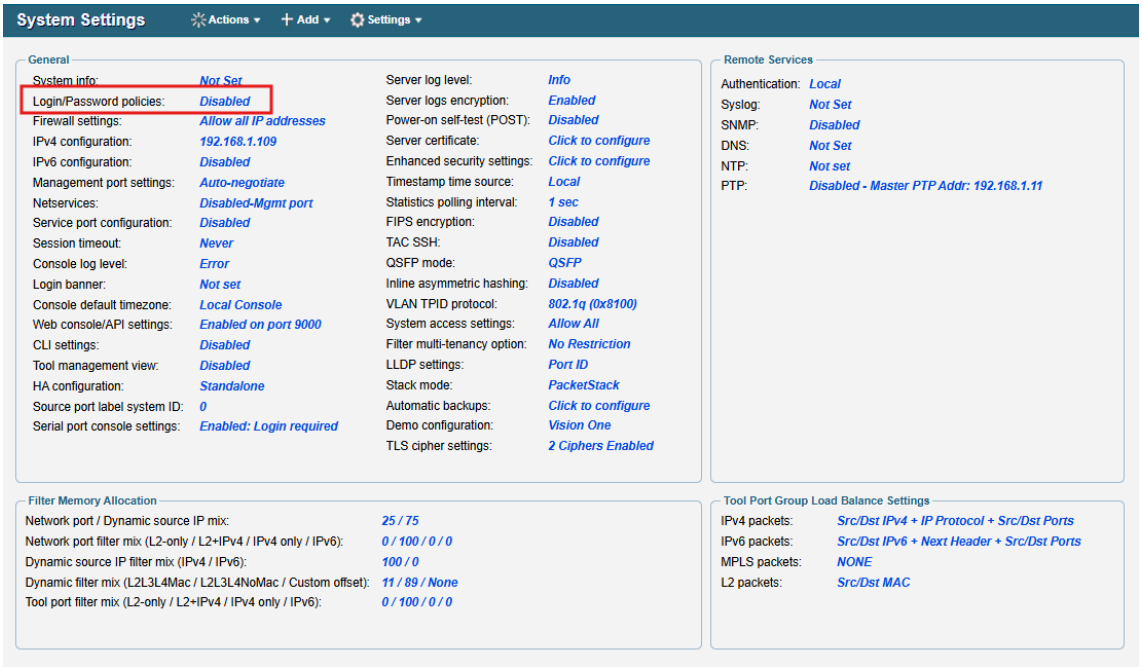

Figura 30. Vista de la sección System > Settings. Gestión de contraseñas

b) Seleccionar el conjunto de políticas aplicable al perfil de despliegue: Standard Policies o DoD Policies.

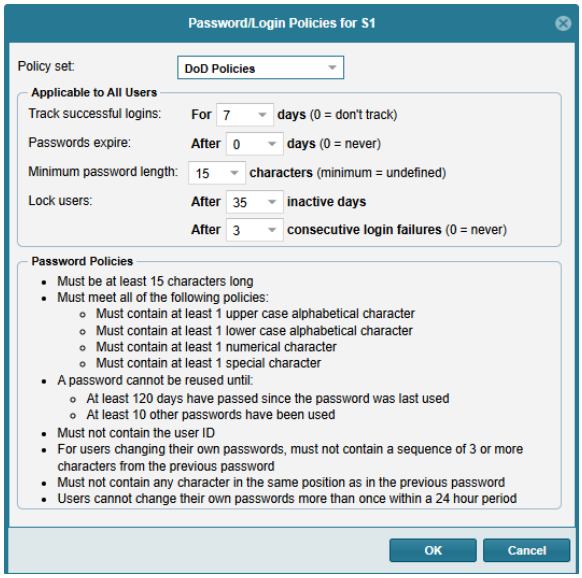

Figura 31. Interfaz de configuración de contraseñas (DoD Policies)

c) Definir la longitud mínima, la expiración y los parámetros de bloqueo e inactividad.

d) Guardar la configuración.

e) Verificar el efecto del cambio con una cuenta de prueba.

73. En cuanto al tiempo máximo de inactividad de las sesiones, se incluyen instrucciones en el apartado 6.1 como parte de los pasos necesarios para la configuración inicial de un perfil gubernamental/Common Criteria (System > Settings > Session timeout).

74. **Configuración del mensaje de aviso y consentimiento en el inicio de sesión (login banner).** Ver sección 6.1 como parte del proceso de configuración inicial para un perfil gubernamental/Common Criteria.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

75. El principal control sobre el plano de gestión es la allowlist de direcciones IP de confianza. En la sección 6.1 se indica el procedimiento para la configuración de una "allowlist" de direcciones IP como parte de los pasos para un modo de operación seguro (System > Settings > Firewall settings).
76. Se recomienda limitar el acceso de gestión exclusivamente a la red administrativa dedicada. No deben autorizarse redes de usuario, segmentos de herramientas ni redes no gestionadas. La guía advierte además de que una mala configuración de la allowlist puede provocar pérdida de acceso web, recuperable únicamente por la consola CRAFT/serie.
77. En la vista de ajustes generales incluye también opciones para control de acceso al puerto serie y parámetros de sesión. En la sección 6.1 se indican los procedimientos para la configuración del control de acceso al puerto serie y los parámetros de inicio de sesión vía Web console y API como parte de los pasos para un modo de operación seguro.

6.5 GESTIÓN DE CERTIFICADOS

78. La administración a través de Web console y la Web API deben operar sobre HTTPS con TLS 1.2. En la sección 6.3.1 se indica la información sobre los cifrados habilitados y la manera de configurarlo para un modo de operación seguro.
79. El sistema se entrega con un certificado firmado por Keysight/Ixia, pero dicho certificado por defecto no es suficiente cuando se requiere identidad criptográfica verificable en el dominio de la organización. Como parte de los pasos necesarios para la configuración del equipo para un modo de operación seguro, en el apartado 6.1 se indican los pasos necesarios para la generación de un certificado CSR y la carga de los certificados apropiados.
80. La solución acepta certificados X.509 en formatos PKCS#7 PEM o DER. En las guías de usuario (REF2) se documentan también ejemplos de conversión de p7b/p7c mediante OpenSSL. El certificado definitivo debe estar emitido por una CA autorizada y vincularse al nombre DNS o a la dirección IP prevista en la política de la organización.

6.6 SERVIDORES DE AUTENTICACIÓN

81. Como se indica en el apartado 6.2 de esta guía sobre Autenticación, El producto soporta integración con TACACS+, RADIUS y LDAP. No obstante, para un perfil de cumplimiento reforzado debe preferirse autenticación local o LDAP con TLS. TACACS+ y RADIUS no son FIPS compliant por lo que no deben emplearse cuando el despliegue requiera operación en FIPS/DoD según ese perfil.
82. En dicho apartado se indica el procedimiento recomendado para la configuración segura de autenticación con LDAP. En las Guías de usuario (REF2) se incluye información para la configuración de otras opciones (TACACS+ o RADIUS) si fueran necesarias.

6.7 SINCRONIZACIÓN

83. La sincronización horaria es necesaria para la trazabilidad de los eventos de auditoría. Se recomienda utilizar exclusivamente servidores NTP internos o autorizados, accesibles desde la red de gestión, y configurar la zona horaria del sistema de forma coherente con la política de auditoría. Cuando la organización requiera homogeneidad temporal, puede fijarse referencia visual en UTC para la consola y la correlación forense, manteniendo en todo caso consistencia con los sistemas de recogida de logs.

84. En la sección 6.1 se indica el procedimiento para la configuración del servicio NTP como parte de los pasos para un modo de operación seguro (cualquier servidor NTP debe configurarse mediante System > Settings > NTP y que, en caso de utilizarlo, debe verificarse que su estado de autenticación figura como Enabled).

6.8 ACTUALIZACIONES

85. La actualización de software debe realizarse de forma planificada, validando previamente la integridad del paquete y exportando un backup completo de la configuración. Los manuales de usuario detallan que antes de instalar una nueva versión debe verificarse el checksum SHA-256 del fichero descargado.

    a) Descargar el paquete únicamente desde el portal de soporte autorizado (Ver link del portal de soporte incluido en la referencia REF2 en este documento).

    b) Verificar el fichero con su checksum SHA-256 antes de usarlo.

    c) Exportar un Full Backup de la configuración antes de iniciar la actualización (Actions > Export config…).

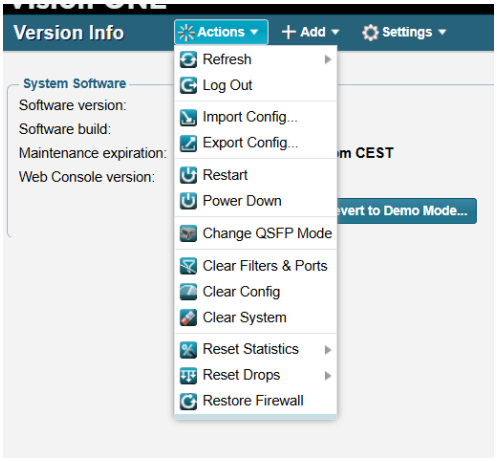

Figura 32. Menú para exportar la configuración

    d) Acceder a System > Version y seleccionar Install Software.

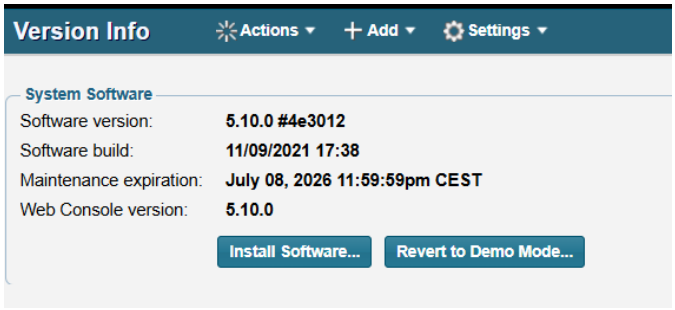

Figura 33. Vista de System > Version para actualización de software

e) Seleccionar el fichero de actualización y confirmar la instalación.

f) Tras la reconexión, iniciar sesión, validar la nueva versión y revisar el estado del sistema.

86. Durante el proceso el sistema muestra una página OFFLINE hasta que la GUI vuelve a reconectar con el servidor. Finalizada la actualización, se debe volver a iniciar sesión y verificar en System > Version que la versión instalada es la esperada. La documentación indica igualmente la posibilidad de revertir a la versión previa con el botón Revert to.

87. En equipos con módulos o netservices adicionales, una actualización mayor puede exigir pasos complementarios de actualización de componentes asociados. En consecuencia, antes de cualquier salto de versión debe revisarse la guía específica del modelo y de los servicios opcionales instalados (REF2, sección *Appendix B. Software Upgrade/Downgrade* de la guía).

6.9 AUTO-CHEQUEOS

88. El producto dispone de un Power-On Self-Test (POST) y, cuando se opera en FIPS, de un Startup System Integrity Check. Desde la consola CRAFT es posible lanzar manualmente el POST (opción 7) y consultar sus resultados (opción 8). Desde la GUI, el parámetro Power-on self-test (POST) puede habilitarse para que se ejecute automáticamente en cada reinicio.

89. El POST añade aproximadamente diez minutos al proceso de reinicio. Si el resultado no es satisfactorio debe contactarse con el soporte técnico del fabricante.

90. En FIPS, el chequeo de integridad de arranque calcula CRC32 sobre los binarios estáticos del sistema. Si cualquier comprobación falla, el sistema entra en estado crítico, detiene operaciones criptográficas, registra el error en /var/log/messages y en el syslog persistente, pone el LED de alarma en rojo y se apaga. El equipo deberá ser reiniciado y superar las comprobaciones para abandonar ese estado.

91. En resumen, las recomendaciones en cuanto a Auto-Chequeos son:

a) Usar el POST manual desde la consola CRAFT antes de la puesta en producción o tras incidencias de hardware.

b) Valorar la activación del POST automático en equipos críticos, asumiendo el incremento del tiempo de reinicio (System > Settings > Power-on-self-test (POST)).

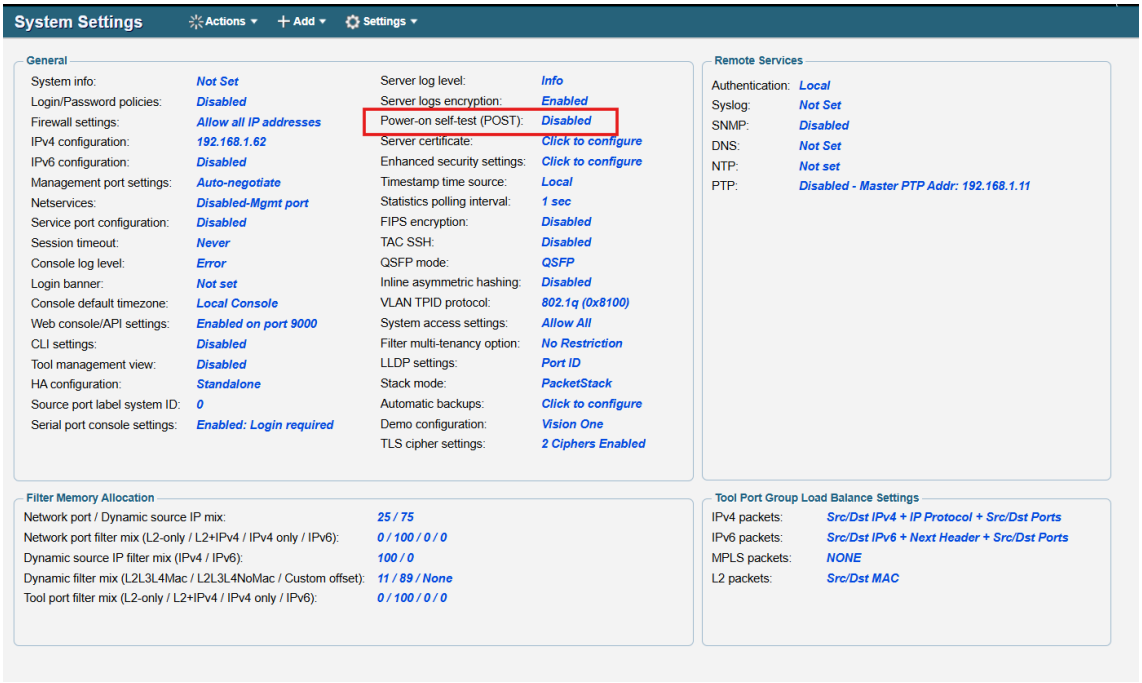

Figura 34. Vista de la sección System > Settings. Configuración POST

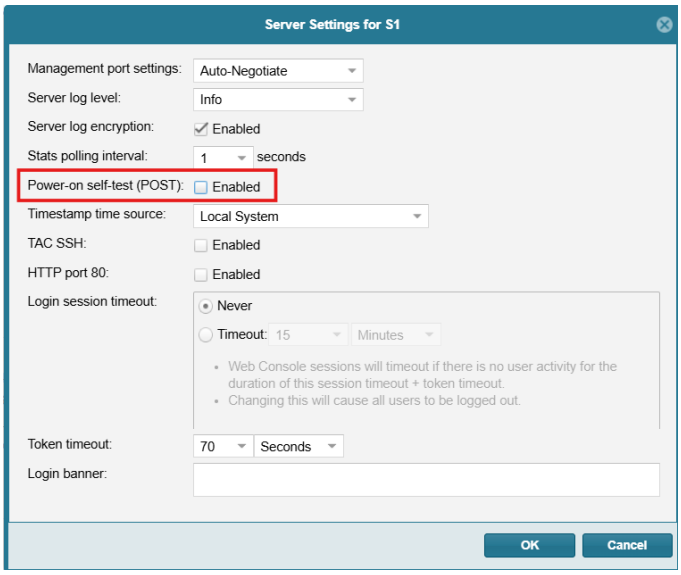

Figura 35. Ventana de configuración de diferentes parámetros de acceso incluyendo POST

c) Cuando se habilite FIPS, verificar el comportamiento del startup integrity check y conservar procedimiento de recuperación.

6.10 ALTA DISPONIBILIDAD

92. Los Network Packet Broker son elementos que normalmente se despliegan independientemente del servicio para la monitorización de copias de tráfico, proporcionadas a través de SPAN ports o de Network TAPs. Este modo de operación se denomina Out-of-Band (OOB, fuera de banda) y en general no requiere un perfil de configuración en HA, más allá de los elementos HW redundados en el appliance (fuentes de alimentación, ventiladores, etc.)

93. En caso de requerir una arquitectura de NPB con alta disponibilidad para mantener el envío de copias de tráfico segura a herramientas de monitorización y seguridad, la familia Vision Packet Broker soporta escenarios avanzados de clustering de equipos en determinados modelos y licencias (IFC Cluster o Keysight Vision Orchestrator). En cualquiera de los casos, implica la utilización de más de un appliance. La inclusión de varios Packet Broker en clustering (interconectados para compartir las copias de tráfico) permitiría la configuración de caminos primarios y secundarios para las copias de tráfico desde las fuentes hasta las herramientas de monitorización y seguridad.

94. No obstante, estas funciones no forman parte del modo mínimo de operación segura descrito en este documento y desde el punto de vista de operación segura, cada elemento del cluster se debe configurar según los requisitos y procedimientos indicados en este documento de manera independiente.

95. En tales casos, deberán aplicarse los mismos criterios de autenticación, cifrado, registro y control de acceso descritos en el presente documento, remitiéndose además a las guías de usuario y operación específicas del modelo correspondiente (REF2).

96. Adicionalmente, los Vision Network Packet Broker permiten un despliegue “en línea” del equipo para alimentar a herramientas de seguridad que además de analizar el tráfico requieran tomar acciones en línea (IPS, WAF, etc.). En este caso existe una funcionalidad específica de HA opcional (Inline HA) que se utiliza para mantener la configuración sincronizada entre dos appliance. La configuración se realiza mediante el campo HA Configuration en System > Settings y la documentación específica del modo Inline HA disponibles en la Guías de instalación (REF2).

    a) System > Settings > HA configuration.

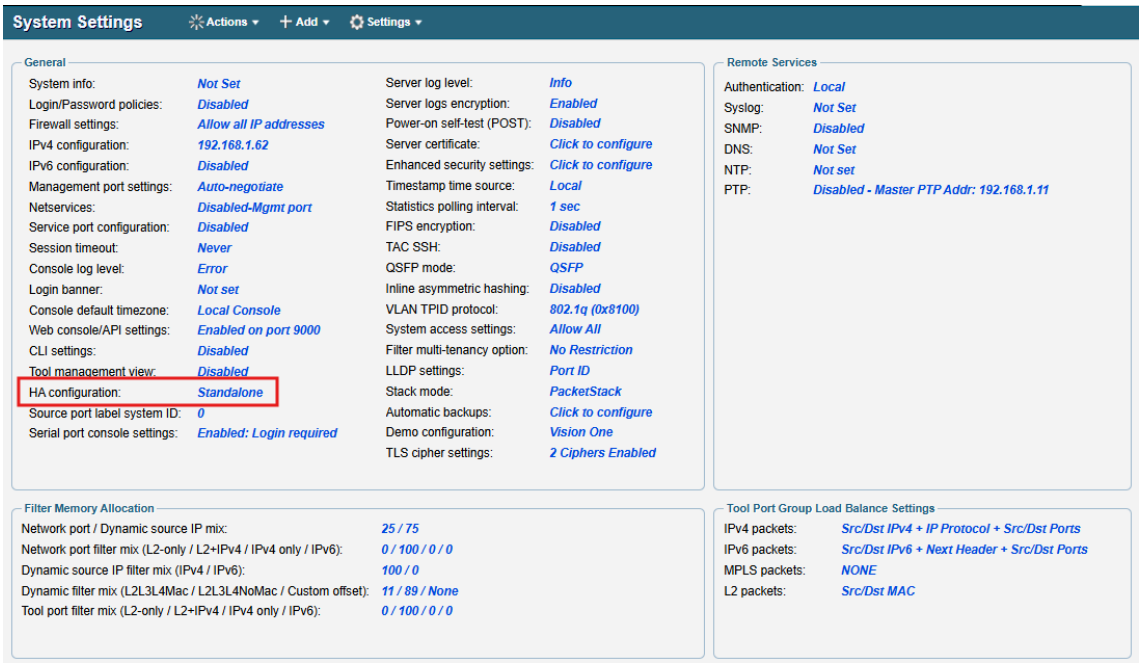

Figura 36. Vista de la sección System > Settings. Configuración Inline HA

    b) En la ventana de configuración de Inline HA configurar los parámetros según las instrucciones de las Guías de usuario (REF2) Sólo aplicable a casos de arquitecturas Inline.

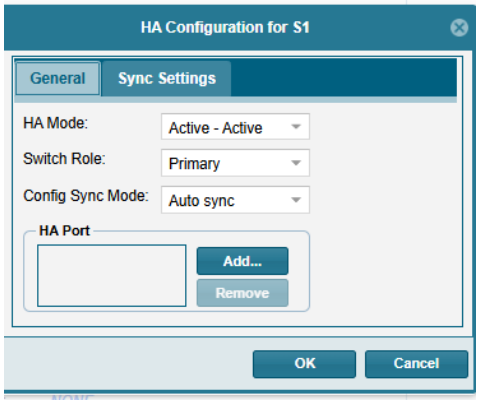

Figura 37. Ventana de configuración para Inline HA

97. Si se utiliza Inline HA, debe diseñarse una pareja controlada de sistemas, con sincronización de configuración y procedimientos de fallo y retorno claramente definidos. Solo debe habilitarse cuando exista un caso de uso real y tras haber validado los puertos, el modo de sincronización y los efectos sobre la detección de fallos de enlace.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

98. Los Vision NPB generan eventos syslog y pueden enviarlos a servidores syslog configurados. Además, disponen de un Local Syslog Viewer accesible desde la barra de control mediante View > Show Syslog Viewer, donde pueden consultarse los eventos producidos y sus datos asociados.

99. A efectos de auditoría, debe considerarse que los eventos de mayor interés para la operación segura incluyen, al menos, cambios de configuración, inicio y cierre de sesiones administrativas, fallos de autenticación, cambios de modo de autenticación, reinicios, ejecución de actualizaciones, eventos asociados al POST o a los chequeos de integridad y errores en servicios de gestión como syslog, NTP, LDAP o HTTPS. Estos eventos deben revisarse tanto en el visor local como, preferentemente, en el colector remoto autorizado. La familia Vision también permite asociar acciones de syslog a monitores de eventos, lo que facilita la generación de alertas ante condiciones operativas relevantes.

100. En cuanto al formato, las guías del producto indican que los mensajes syslog siguen la sintaxis de acuerdo a la RFC 5424 y documentada en el apéndice de *NPB Syslog Messages*, incluyendo severidad, marca temporal y contenido del mensaje.

101. El mensaje RFC 5424 proporciona los siguientes campos:

    a) *Facility*: Local 0, etc.

    b) *Severity*: Gravedad (o Nivel) del mensaje.

    c) *TIMESTAMP* (MARCA DE TIEMPO): Esta es una marca de tiempo formalizada. La MARCA DE TIEMPO indica la fecha y hora en que se registra el evento e incluye la hora de generación del syslog con el año y los milisegundos, con respecto a la zona horaria.

- Los siguientes ejemplos muestran el formato de fecha y hora en RFC 5424. El sufijo "Z", cuando se aplica a una hora, indica una diferencia horaria de 00:00 con respecto al Tiempo Universal Coordinado (UTC).

  Por ejemplo: `2016-07-29T21:10:48.668Z` representa el 29 de julio de 2016 a las 21:10:48, 668 milisegundos después del inicio del segundo. La marca de tiempo está en UTC. La marca de tiempo proporciona una resolución de milisegundos.

d) *HOSTNAME* (NOMBRE DE HOST): Identifica la máquina que envió originalmente el mensaje de Syslog. Este es el nombre del sistema configurado o la dirección IP si no se ha configurado.

e) *APP-NAME* (NOMBRE DE LA APLICACIÓN): Es el modelo del sistema.

f) Los tres (3) campos siguientes están en blanco y se representan con guiones: "- - -"

g) MSG: Contiene el ID de secuencia, seguido de un mensaje de texto libre que proporciona información sobre el evento.

102. Un mensaje de syslog generalmente se registra en el siguiente formato:

```
<system_info>:<user_id/object_type> <object_details>
```

103. Por ejemplo, el siguiente mensaje es un mensaje de prueba que se envía al servidor syslog cada vez que un usuario del sistema configura un servidor syslog en la pestaña *System > Settings* de la consola del sistema para verificar que esté accesible.

```
10.218.80.130:"admin"
```

104. Si un usuario no realiza una acción específica y el mensaje de syslog se activa por cambios internos, el parámetro object_type puede ser un puerto, un filtro dinámico, un grupo de puertos o el sistema. Ejemplo:

```
10.218.80.130:System "main" changed: TOPOLOGY_STATUS=READY
```

105. **Syslog Levels**: Los mensajes de Syslog se registran con diferentes niveles que indican la gravedad del mensaje. Se admiten los siguientes niveles:

a) *ERROR*: Se ha producido un error.

b) *WARNING*: Advertencia.

c) *NOTICE* (AVISO): Situación normal pero significativa.

d) *INFO* (INFORMACIÓN): Información para el usuario.

106. **Pre-Defined Syslog Messages:** Cada propiedad del sistema que los usuarios pueden modificar genera un mensaje de syslog. Siempre que se modifica alguna propiedad del sistema, se genera un mensaje de syslog de nivel informativo (info) con el siguiente formato:

```
<ip_address>:<user_id>  changed  <object_type>  ?<object_id>?:
<object_details>
```

Ejemplos:

```
10.218.80.130:"admin"                    changed                    System:
MEMORY_ALLOCATION=NetworkDynamicSipAllocationType = 25% Network port +
75% Dynamic IP address; Network = 100% L2 and IPv4 L3/L4; Dynamic SIP
= 100% IPv4 address; Dynamic = 100% L2/L3/L4 excluding MAC; Tool = 100%
L2 and IPv4 L3/L4; Custom =None
10.218.80.130:"admin"          changed          Port          "P1-03":
STD_VLAN_STRIP_SETTINGS=Enabled, Strip mode:Ingress, Ingress Count:1
```

107. Las guías de usuario disponibles en el portal de soporte de Keysight (ver link en referencia REF2 en este documento) incluyen información detallada de los eventos y formatos que podrían registrarse en el syslog (*Appendix F - NPB Syslog Messages*)

108. Para un despliegue seguro debe garantizarse la coherencia horaria del sistema, de modo que la marca temporal de los eventos resulte útil para correlación forense con el resto de infraestructuras de seguridad. Cuando se utilice syslog remoto en perfiles Common Criteria o FIPS, el canal de envío debe protegerse mediante **TLS**.

6.11.2 ALMACENAMIENTO LOCAL

109. El almacenamiento local de eventos se consulta mediante el Local Syslog Viewer (*View > Syslog Viewer*) y el syslog persistente del sistema. Este mecanismo permite revisar eventos recientes, incluidos determinados fallos de integridad que, por exigencias FIPS, no llegan a enviarse por canales criptográficos remotos.

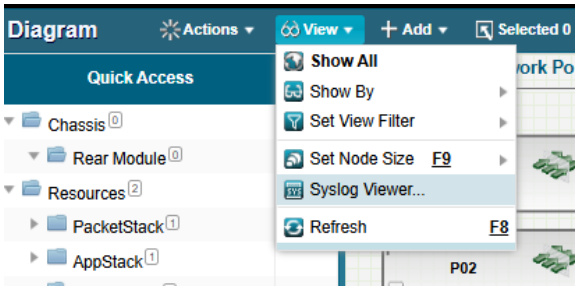

Figura 38. Acceso al visor de syslog local

110. El visor local permite resaltar por severidad (Critical, Alert, Error, Warning, Notice, Info), visualizar el mensaje completo y mantener opciones de vista persistentes para el usuario. Para necesidades de monitorización activa, el producto también ofrece Monitors que pueden desencadenar traps SNMP o mensajes syslog cuando se producen eventos como paquetes inválidos, umbrales de utilización o drops.

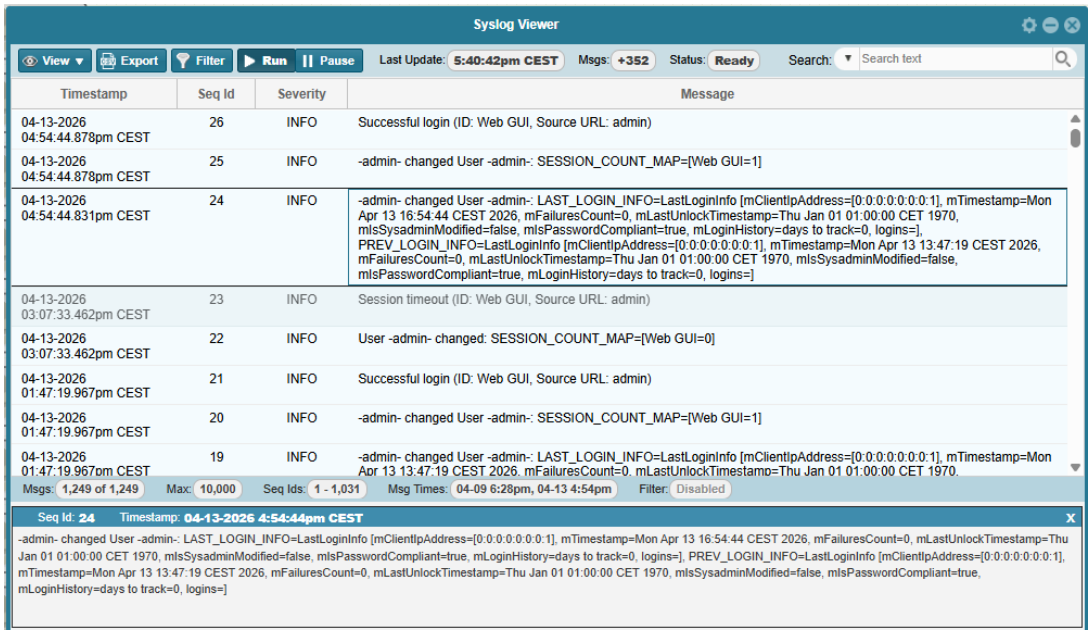

Figura 39. Ventana del visor local de syslog

111. Se recomienda revisar periódicamente el syslog local tras cambios de configuración, reinicios, actualizaciones o incidencias de acceso, y utilizarlo como fuente de apoyo forense en caso de fallo del canal remoto.

6.11.3 ALMACENAMIENTO REMOTO

112. Para cumplir con Common Criteria y con los requisitos FIPS, el envío de eventos a syslog remoto debe realizarse con TLS habilitado entre el Vision NPB y el servidor syslog. Para usar autenticación mutua proporcionada por TLS, el equipo debe disponer del certificado cliente y del certificado raíz de confianza del servidor syslog.

113. Por tanto, el despliegue seguro debe contemplar un servidor syslog remoto autorizado, preferiblemente interno, protegido y accesible desde la red de gestión. La validación del canal debe realizarse verificando tanto la conexión como la correcta recepción de eventos de prueba. En la sección 6.1 se indica el procedimiento para la configuración segura de un servidor de syslog remote como parte de los pasos para un modo de operación seguro.

6.12 BACKUP

114. El producto permite exportar e importar configuraciones como mecanismo de backup manual. Para ello se puede importar o exportar un backup desde el *menú Actions > Import Config…* o *Actions > Export Config…*

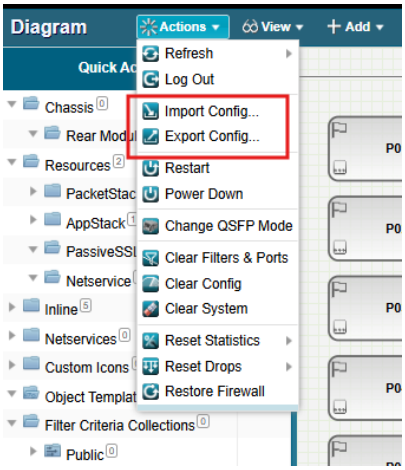

Figura 40. Acceso al menú para importar o exportar un backup

115. Se distinguen tres tipos de exportación: Full Backup, Traffic Configuration y Custom. Un Full Backup contiene toda la configuración, incluidas bibliotecas y asignaciones de licencia; Traffic Configuration guarda puertos, grupos, filtros y parámetros relacionados con tráfico; y Custom permite seleccionar determinados elementos. La cuenta admin por defecto y la configuración IP del sistema no se exportan ni se importan.

116. Las operaciones de exportación e importación solo pueden realizarlas usuarios con rol administrativo. La importación puede provocar reinicios o expulsión de sesiones si modifica los parámetros de management o el modo de autenticación.

117. Existe además la posibilidad de programar Automatic Backups desde System > Settings.

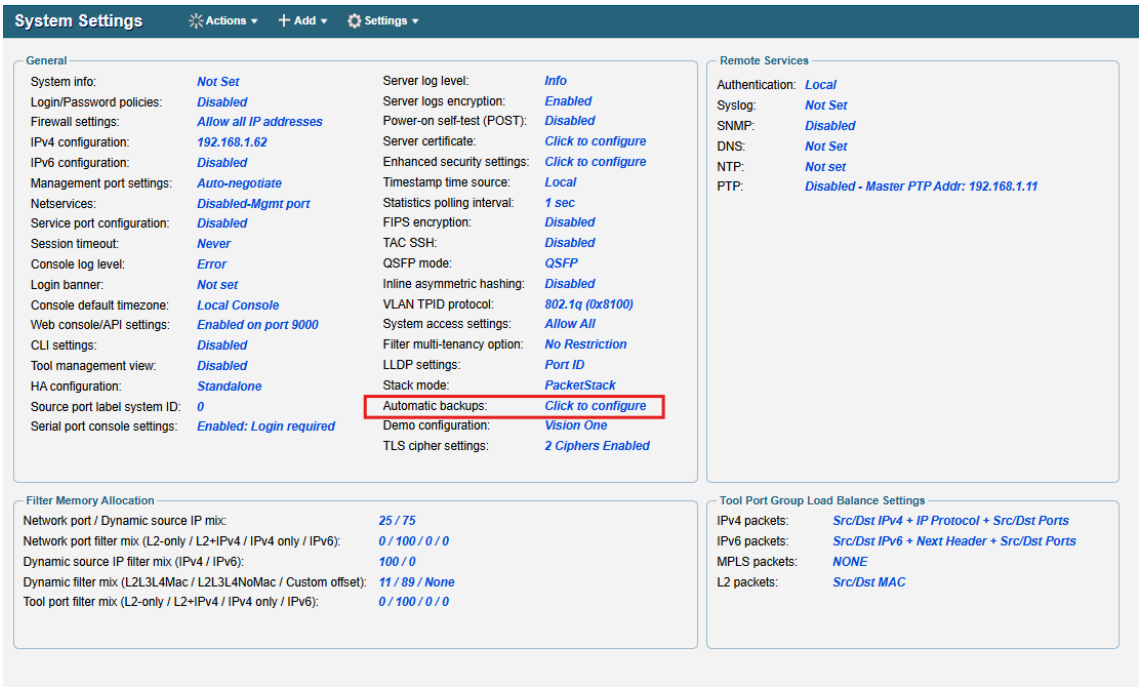

Figura 41. Vista de la sección System > Settings. Configuración de backups automáticos

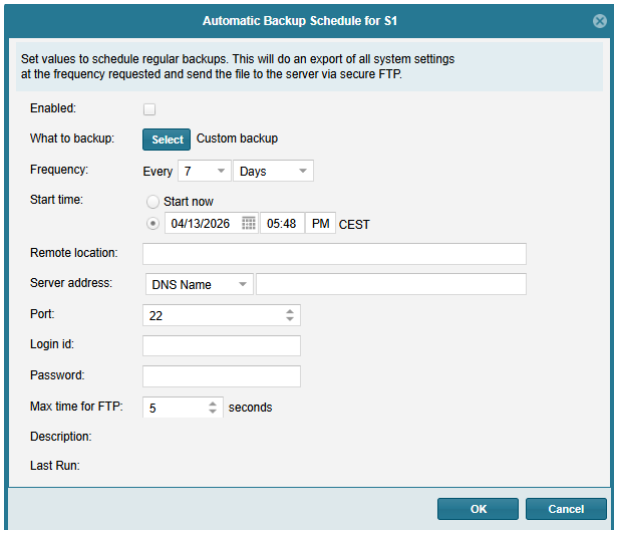

Figura 42. Ventana de configuración de backups automáticos

118. Se recomienda combinar backup manual previo a cambios mayores y backup automático programado.

a) Realizar un Full Backup antes de cualquier actualización o cambio relevante.

b) Conservar copia segura del fichero exportado fuera del appliance.

c) Programar Automatic Backups.

d) Verificar periódicamente la restauración en entorno de laboratorio o equipo de respaldo equivalente.

7 REFERENCIAS

REF1 Keysight Technologies Security Target / Declaración de Seguridad – Vision Series Network Packet Broker v5.10.0 Security Target, Complementary Evaluation v5.2, July 2025.

REF2 Guías de usuario de la familia Vision Packet Broker. Portal de Soporte de Keysight. https://support.keysight.com/s/knowledge-center?type=nas&product=Network+Visibility+Equipment

REF3 CPSTIC:
https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8 ABREVIATURAS

AAA	Authentication, Authorization and Accounting
CA	Certificate Authority
CLI	Command Line Interface
CPD	Centro de Proceso de Datos
CPSTIC	Catálogo de Productos y Servicios STIC
CSR	Certificate Signing Request
DNS	Domain Name System
DoD	Department of Defense
ENS	Esquema Nacional de Seguridad.
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HA	High Availability
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LDAP	Lightweight Directory Access Protocol
MGMT	Puerto o interfaz de gestión
NDR	Network Detection and Response
NPB	Network Packet Broker
NTP	Network Time Protocol
OOB	Out-of-Band
POST	Power-On Self-Test
RAL	Restricted-Access Location
RFC	Request for Comments
SAN	Subject Alternative Name
SHA-256	Secure Hash Algorithm de 256 bits
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SPD	Surge Protective Device
SSH	Secure Shell
SSL	Secure Sockets Layer
STARTTLS	Mecanismo de negociación para elevar una conexión a TLS
TACACS+	Terminal Access Controller Access-Control System Plus
TAP	Test Access Point / punto de acceso de prueba para monitorización
TLS	Transport Layer Security
TOE	Target of Evaluation
WAF	Web Application Firewall
Web API	Interfaz de programación de aplicaciones accesible por HTTPS