centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1020

Procedimiento de Empleo Seguro
Ivanti Connect Secure (ICS)



Noviembre 2026

Edita:





CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 7
2 OBJETO Y ALCANCE 7
3 ORGANIZACIÓN DEL DOCUMENTO 8
4 FASE PREVIA A LA INSTALACIÓN 9
4.1 ENTREGA SEGURA DEL PRODUCTO 9
4.2 ENTORNO DE INSTALACIÓN SEGURO 10
4.3 REGISTRO Y LICENCIAS 10
4.4 CONSIDERACIONES PREVIAS 10
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 10
5 FASE DE INSTALACIÓN 12
5.1 INSTALACIÓN INICIAL MEDIANTE CONSOLA SERIE LOCAL 12
5.2 CONFIGURACIÓN DEL MODO DISPOSITIVO DE RED 14
5.3 VERIFICACIÓN DE LA VERSIÓN DEL SOFTWARE 15
5.3.1 VERIFICACIÓN DE LA VERSIÓN A TRAVÉS DE LA INTERFAZ GRÁFICA DE USUARIO 15
5.3.2 VERIFICACIÓN DE LA VERSIÓN A TRAVÉS DE LA CONSOLA SERIE LOCAL 15
6 FASE DE CONFIGURACIÓN 17
6.1 MODO DE OPERACIÓN SEGURO 17
6.2 AUTENTICACIÓN 17
6.3 ADMINISTRACIÓN DEL PRODUCTO 17
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 17
6.3.2 CONEXIÓN A LA INTERFAZ WEB DE ADMINISTRACIÓN 18
6.3.3 CONFIGURACIÓN DEL CONTROL DE ACCESO A LA CONSOLA SERIE LOCAL 18
6.3.4 CONEXIÓN A LA CONSOLA SERIE LOCAL 19
6.3.5 CONFIGURACIÓN DE ADMINISTRADORES 20
6.3.6 CONFIGURACIÓN DE LA LONGITUD MÍNIMA DE LA CONTRASEÑA 22
6.3.7 CONFIGURACIÓN DEL BANNER DE ADMINISTRACIÓN 23
6.3.8 CONFIGURACIÓN DEL TIEMPO DE ESPERA POR INACTIVIDAD 25
6.3.9 CONFIGURACIÓN DEL BLOQUEO POR FALLOS DE AUTENTICACIÓN 26
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 28
6.4.1 CONFIGURACIÓN DEL PUERTO INTERNO 28
6.4.2 CONFIGURACIÓN DEL PUERTO DE GESTIÓN 29
6.4.3 CONFIGURACIÓN DEL SERVIDOR DNS 30
6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS 31
6.5.1 ACTIVACIÓN DE LAS OPCIONES DE SSL ENTRANTE 32
6.5.2 ACTIVACIÓN DE LAS OPCIONES DE SSL SALIENTE 36
6.6 GESTIÓN DE CERTIFICADOS 38
6.6.1 IMPORTAR UN CERTIFICADO DE CA DE CLIENTE DE CONFIANZA 38
6.6.2 IMPORTAR DE UN CERTIFICADO DE CA DE SERVIDOR DE CONFIANZA 39
6.6.3 INSTALACIÓN DE UN CERTIFICADO DE AUTENTICACIÓN DE CLIENTE 40
6.6.4 IMPORTACIÓN DEL CERTIFICADO Y LA CLAVE PRIVADA PARA LA AUTENTICACIÓN DE CLIENTE 40
6.6.5 GENERACIÓN DE UNA CSR PARA UN CERTIFICADO DE AUTENTICACIÓN DE CLIENTE 41
6.6.6 INSTALACIÓN DE UN CERTIFICADO DE DISPOSITIVO 43
6.6.7 IMPORTACIÓN DEL CERTIFICADO Y LA CLAVE PRIVADA DEL CERTIFICADO DE DISPOSITIVO 44
6.6.8 GENERACIÓN DE UNA CSR PARA UN CERTIFICADO DE DISPOSITIVO 44

6.6.9 HABILITACIÓN DE COMPROBACIÓN CRL 47
6.7 SERVIDORES DE AUTENTICACIÓN 48
6.8 SINCRONIZACIÓN 48
6.9 ACTUALIZACIONES DE SOFTWARE 49
6.10 AUTO-CHEQUEOS 50
6.11 AUDITORÍA 51
6.11.1 REGISTRO DE EVENTOS 51
6.11.2 ALMACENAMIENTO LOCAL 53
6.11.3 ALMACENAMIENTO REMOTO 56
7 REFERENCIAS 63
8 ABREVIATURAS 64

ÍNDICE DE ILUSTRACIONES

Ilustración 1: Representación del despliegue del Producto en un Appliance Físico 12
Ilustración 2: Representación del despliegue del Producto en un Appliance Virtual 12
Ilustración 3: Menú Información de Versión 15
Ilustración 4: Detalles de la Versión 16
Ilustración 5: Menú configuración de Acceso por Consola de Serie Local 18
Ilustración 6: Mensaje de Confirmación de Acceso en la Consola Serie Local 19
Ilustración 7: Mensaje de Inicio de Sesión mediante Consola Serie Local 20
Ilustración 8: Configuración de Roles de Usuario Administrador 21
Ilustración 9: Asignación de Roles de Usuario Administrador 21
Ilustración 10: Menú de Configuración de Opciones de Contraseña de Usuario Administrador 22
Ilustración 11: Menú Notificaciones de Inicio de Sesión 23
Ilustración 12: Menú de Configuración del Banner de Inicio de Sesión 24
Ilustración 13: Menú Notificaciones de Inicio de Sesión 24
Ilustración 14: Menú de Configuración del Banner de Inicio de Sesión 25
Ilustración 15: Menú de Configuración de Roles 25
Ilustración 16: Menú de Opciones de Sesión de Usuario Administrador 26
Ilustración 17: Menú de Servidores de Autenticación 27
Ilustración 18: Menú de Configuración de Bloqueo de Cuentas de Usuario Administrador 27
Ilustración 19: Opciones de Bloqueo de Cuenta 28
Ilustración 20: Menú Configuración de Red 28
Ilustración 21: Configuración de IP 29
Ilustración 22: Configuración del Puerto de Gestión 30
Ilustración 23: Configuración del DNS 31
Ilustración 24: Menú de Configuración de los Protocolos de Conexiones Entrantes 32
Ilustración 25: Opción Activación Modo FIPS 32
Ilustración 26: Menú de Configuración de Protocolos TLS 33
Ilustración 27: Menú de Aceptación de Configuraciones de Cifrado 33
Ilustración 28: Menú de Selección de Ciphersuites Entrantes 34
Ilustración 29: Menú de Compatibilidad de Negociación SSL Heredado 34
Ilustración 30: Puerto de Autenticación de Certificados TLS 35
Ilustración 31: Menú de Selección de Ciphersuites Entrantes 35
Ilustración 32: Menú de Confirmación de Selección de Ciphersuites 35
Ilustración 33: Menú de Configuración de los Protocolos de Conexiones Salientes 36
Ilustración 34: Menú de Aceptación de Configuraciones de Cifrado 36
Ilustración 35: Menú de Selección de Ciphersuites Salientes 37
Ilustración 36: Menú de Selección de Ciphersuites Salientes 38
Ilustración 37: Menú de Configuración de Certificado CA de Cliente de Confianza 39
Ilustración 38: Menú de Configuración de Certificado CA de Servidor de Confianza 39
Ilustración 39: Menú de Importación de Certificado CA de Cliente de Confianza 40
Ilustración 40: Menú de Configuración de Importación del Certificado y la Clave Privada para la Autenticación De Cliente 41
Ilustración 41: Menú de Generación de una CSR para un Certificado de Autenticación de Cliente 42
Ilustración 42: Menú de Generación de una CSR para un Certificado de Dispositivo 45
Ilustración 43: Menú de Configuración de los Detalles del Certificado 46
Ilustración 44: Menú de Activación del Puerto de Gestión del Certificado 47
Ilustración 45: Menú de Configuración de Certificados 47

Ilustración 46: Menú de Configuración de CRL 48
Ilustración 47: Configuración de la Fecha y Hora 49
Ilustración 48: Menú de Configuración de Tamaño Máximo de Registros de Auditoría 54
Ilustración 49: Menú de Configuración de Tamaño Máximo de Registros de Auditoría de Acceso de Usuario 55
Ilustración 50: Menú de Configuración de Tamaño Máximo de Registros de Auditoría de Acceso de Administrador 55
Ilustración 51: Configuración del Servidor Syslog 62

ÍNDICE DE TABLAS

Tabla 1: Plataformas Hardware 7
Tabla 2: Despliegues Virtuales 8
Tabla 3: Componentes del Entorno de Operación 11
Tabla 4: Campos de los Registros de Auditoría 53
Tabla 5: Configuración de los Parámetros del Servicio de Auditoría 60
Tabla 6: Configuración de los Parámetros del Servicio de Auditoría de Acceso de Usuario 60
Tabla 7: Configuración de los Parámetros del Servicio de Auditoría de Acceso de Administrador 61
Tabla 8: Configuración de los Parámetros del Servidor Syslog 61

1 INTRODUCCIÓN

El producto **Ivanti Connect Secure (ICS) versión 22.7R2.13 (build 6095),** a partir de ahora nombrado como ICS, es una solución de acceso seguro que permite a usuarios y administradores acceder de forma controlada a aplicaciones y recursos corporativos ubicados tanto en centros de datos como en entornos cloud. El producto está diseñado para proporcionar funcionalidades de administración segura, autenticación de administradores, protección criptográfica de las comunicaciones, registro de eventos de seguridad y gestión segura del propio sistema.

El producto ICS se ejecuta sobre el sistema operativo IVE OS 3.0, pudiéndose desplegar tanto sobre plataformas hardware dedicadas de la familia ISA como sobre plataformas virtualizadas soportadas.

Entre las principales capacidades de seguridad incluidas en la configuración de seguridad se encuentran la administración remota segura mediante HTTPS/TLS, la autenticación de administradores, la protección criptográfica de las comunicaciones, la generación y protección de registros de auditoría, la comunicación segura con servidores Syslog mediante TLS, la ejecución de autocomprobaciones de integridad y la verificación criptográfica de las actualizaciones de software antes de su instalación.

2 OBJETO Y ALCANCE

La presente Guía de Empleo Seguro aplica al producto **ICS**, como dispositivo de red y dispositivo virtual de red privada. El producto se ejecuta sobre el sistema operativo **IVE OS 3.0** y constituye la configuración de seguridad incluida en el certificado de seguridad correspondiente.

La guía es aplicable a las siguientes plataformas hardware evaluadas:

Modelo	Procesador	Opciones de Red
ISA 6000	Intel Core i3 10100E (10ª generación – Comet Lake)	2 x 10 Gigabit Copper Ethernet traffic ports 1 x 1GbE Management port 1 x RJ-45 Console Port
ISA 8000C	Intel Xeon Gold 5317 (Ice Lake)	2 x 10 Gigabit Ethernet copper traffic ports with link redundancy 1 x 1GbE Management port 1 x RJ-45 Console Port
ISA 8000F	Intel Xeon Gold 5317 (Ice Lake)	2 x 10 Gigabit fiber traffic ports with link redundancy 1 x 1GbE Management port 1 x RJ-45 Console Port

Tabla 1: Plataformas Hardware

Asimismo, la guía es aplicable a los siguientes despliegues virtuales evaluados:

Modelo Virtual	Plataforma hardware soportada y procesador	Hipervisor
ISA 6000-V	Dell PowerEdge R640 con Intel Xeon Gold 6252 (Cascade Lake)	VMware ESXi 8.0.3
ISA 8000-V	Dell PowerEdge R640 con Intel Xeon Gold 6252 (Cascade Lake)	VMware ESXi 8.0.3

Tabla 2: Despliegues Virtuales

La presente guía únicamente es válida para la configuración de seguridad correspondiente a la versión **22.7R2.13 (build 6095)** de ICS, ejecutándose sobre las plataformas anteriormente indicadas y configurada de acuerdo con las condiciones establecidas en la documentación de evaluación Common Criteria y en la guía de configuración de seguridad del producto en [REF1].

El producto ICS ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF5].

3 ORGANIZACIÓN DEL DOCUMENTO

El presente documento se estructura en los siguientes apartados:

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

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

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

d) Apartado 7. Listado de documentación referenciada en este documento.

e) Apartado 8. Listado de abreviaturas que aparecen en este documento.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Para garantizar que se recibe el producto correcto y que éste no ha sido manipulado durante su transporte o entrega, el producto debe inspeccionarse cuidadosamente antes de su puesta en servicio.

Verifique que el software y el hardware del producto no han sido manipulados durante el proceso de entrega realizando las siguientes comprobaciones:

- Antes de desembalar el producto, inspeccione el embalaje físico del equipo. Compruebe que la caja exterior de cartón dispone de los logotipos y elementos identificativos de Ivanti. Si no es así, contacte con el proveedor del equipo (Ivanti o un distribuidor/socio autorizado de Ivanti).
- Compruebe que el embalaje no haya sido abierto y sellado nuevamente. Para ello, examine las cintas de cierre del paquete. Si observa indicios de manipulación o re-precintado, contacte con el proveedor del equipo.
- Verifique que la caja incorpora una etiqueta de seguridad blanca de Ivanti, resistente a manipulaciones y con evidencias de apertura, situada sobre el embalaje exterior. Esta etiqueta contiene, entre otros datos, el número de producto, el número de serie y la identificación del contenido suministrado.
- Anote el número de serie indicado en la documentación de envío y compruebe que coincide con el número de serie mostrado en la etiqueta exterior del equipo y con el reflejado en la factura correspondiente. En caso de discrepancia, contacte con el proveedor.
- Verifique que el envío procede realmente del proveedor esperado (Ivanti o distribuidor autorizado). Para ello, confirme con el proveedor los datos del envío, la empresa de transporte utilizada y el identificador de seguimiento correspondiente. Asimismo, compruebe que los números de serie de los equipos enviados coinciden con los recibidos. Esta verificación debe realizarse por un medio independiente al propio proceso de entrega (por ejemplo, teléfono, correo electrónico o servicio de seguimiento del transportista).
- Una vez desembalado el producto, inspeccione físicamente el dispositivo y confirme que el número de serie indicado en el propio equipo coincide con el reflejado en la documentación de envío y en la factura.

Para las implementaciones virtuales, el cliente debe registrarse previamente en el portal de clientes de Ivanti. Tras la validación del registro, Ivanti proporciona acceso al paquete de la máquina virtual junto con el valor de comprobación SHA-256 correspondiente.

Una vez descargado el paquete de la appliance virtual:

- Calcule el hash SHA-256 del fichero descargado utilizando una herramienta de confianza.
- Compare el valor SHA-256 calculado con el valor SHA-256 proporcionado por Ivanti.
- Si ambos valores coinciden, se confirma la integridad y autenticidad del paquete y puede continuarse con el despliegue.
- Si existe cualquier discrepancia, no se debe desplegar el paquete y deberá contactarse inmediatamente con el soporte de Ivanti para iniciar las acciones correspondientes.

Este procedimiento permite garantizar que el appliance virtual no ha sido alterada, manipulada o comprometida durante su distribución o descarga.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Los componentes del producto deben instalarse en un Centro de Proceso de Datos (CPD) o entorno seguro, al cual solo personal técnico limitado dispondrá de acceso y estará autorizado para realizar actividades de configuración, despliegue y mantenimiento del producto.

4.3 REGISTRO Y LICENCIAS

Para instalar licencias en el producto, hay que seguir estos pasos:

1. Obtener un código de autenticación: El administrador recibe por correo electrónico un código de autenticación correspondiente a su derecho de uso.
2. Introducir el código de autenticación:
3. Vaya a Sistema > Configuración > Descargar licencias.
4. En la sección «Descargas de licencias bajo demanda», introduzca el código de autenticación.
5. Haga clic en «Descargar e instalar».
6. Ver las licencias instaladas:
7. Una vez validadas correctamente, consulte las licencias instaladas en la pestaña «Resumen de licencias».

El proceso se encuentra en la sección “Using Licenses without a License Server” en [REF2].

4.4 CONSIDERACIONES PREVIAS

El producto no requiere de una configuración adicional relativa a la seguridad, previa a iniciar la instalación y configuración del producto.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

El producto debe contar con los siguientes elementos en su entorno de operación:

Componentes	Descripción
Servidor Syslog	Recibe y almacena los registros de auditoría generados por el producto ICS. Debe soportar Syslog conforme a RFC 5424 y Syslog sobre TLS (RFC 5425), actuando como servidor TLS 1.2 y/o TLS 1.3 con autenticación mediante certificados de cliente.

Estación de administración	Utilizada para la administración remota segura del producto mediante interfaz web HTTPS. Debe disponer de un navegador compatible (Microsoft Edge 101, Google Chrome 102, or Firefox 100) con soporte TLS 1.2/TLS 1.3 y capacidad para cargar actualizaciones de software a través de la interfaz gráfica.
Servidor CRL (Certificate Revocation List)	Proporciona las listas de revocación de certificados (CRLs) utilizadas para validar certificados X.509. Debe implementar los puntos de distribución CRL definidos en RFC 5280 y publicar la información mediante HTTP a los clientes.
Servidor DNS	Permite la resolución de nombres de dominio (FQDN) necesarios para las comunicaciones de red y validación de servicios externos. Usa protocolos UDP y TCP en el puerto 53. Debe operar conforme a RFC 1035.
Consola Serie Local	Proporciona acceso local de administración mediante conexión serie al puerto de consola del dispositivo utilizando un cable serie tipo null-modem
Hipervisor VMware ESXi	Requerido únicamente en despliegues virtuales (ISA 6000-V e ISA 8000-V). Aloja la máquina virtual que ejecuta el producto ICS y proporciona recursos de procesamiento, memoria y almacenamiento.

Tabla 3: Componentes del Entorno de Operación

5 FASE DE INSTALACIÓN

5.1 INSTALACIÓN INICIAL MEDIANTE CONSOLA SERIE LOCAL

El producto ICS puede implementarse como dispositivo físico o virtual. Para las implementaciones virtuales, Ivanti proporciona un archivo OVF para su uso con los hipervisores compatibles. En la configuración de seguridad, el dispositivo virtual se implementa en VMware ESXi 8.0.3, que se ejecuta en hardware Intel Xeon Gold 6252 (Cascade Lake) en una plataforma Dell PowerEdge R640.

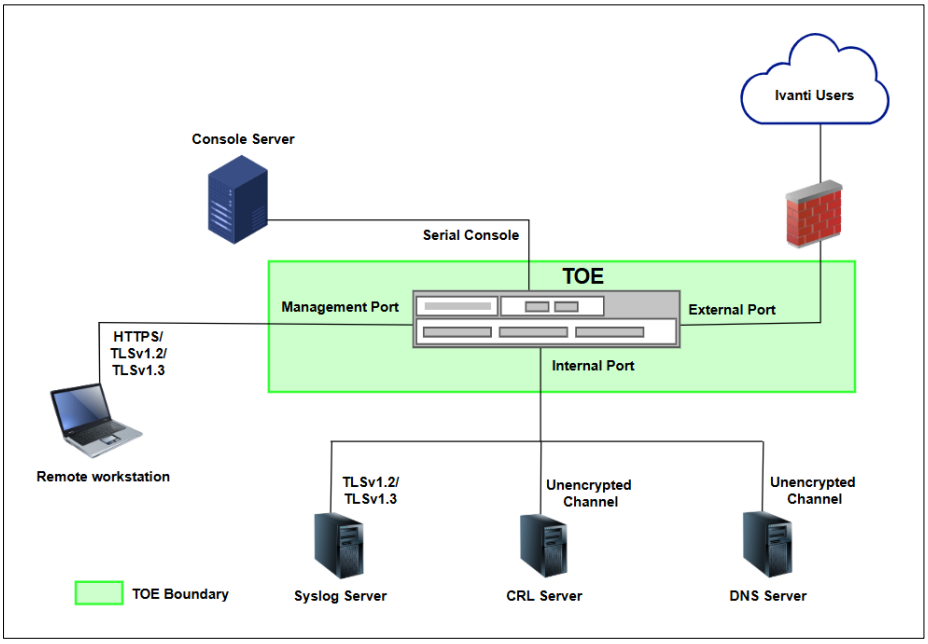


Ilustración 1: Representación del despliegue del Producto en un Appliance Físico

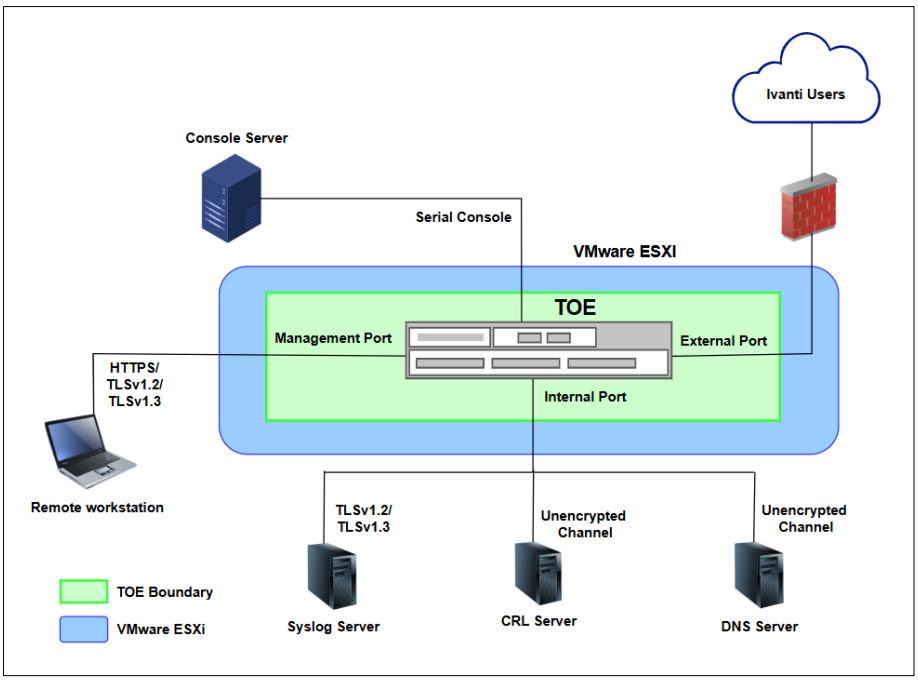


Ilustración 2: Representación del despliegue del Producto en un Appliance Virtual

Una vez implementado y encendido, sigue las instrucciones que se indican a continuación para completar la configuración inicial. Estos pasos se aplican a ambos tipos de implementación, salvo que se especifique lo contrario.

Nota: En el caso de las implementaciones de dispositivos virtuales, una vez que el OVF se ha implementado en el hipervisor, la consola virtual queda disponible de inmediato y puede utilizarse para realizar la configuración inicial. Los pasos relativos a la consola serie local (pasos 1-3) solo son aplicables al dispositivo físico.

Solo para dispositivos físicos:

1. Conecta un cable cruzado de módem nulo desde un servidor de consola al puerto serie del dispositivo. Este cable se incluye en la caja del producto. No utilices un cable serie directo.
2. Configure una utilidad de emulación de terminal, como HyperTerminal, con los siguientes parámetros de conexión serie:
   a) 9600 bits por segundo
   b) bits sin paridad (8N1)
   c) bit de parada
   d) Sin control de flujo

Nota: En el caso de las implementaciones de dispositivos virtuales, este paso no es aplicable. Utilice en su lugar la consola virtual del hipervisor.

3. Pulse Intro hasta que aparezca la consola serie local.

Tanto para dispositivos físicos como virtuales:

4. Aparece el siguiente texto en la consola serie local:

Elija una de las siguientes imágenes de personalización con restablecimiento de fábrica:

[1] Ivanti Connect Secure <versión base>

Nota: Esta es la versión de ICS con restablecimiento de fábrica. Una vez configurada, el administrador debe actualizarla a la versión CC designada.

5. Introduzca 1 para instalar el paquete de ICS. El sistema iniciará la instalación y se reiniciará. El proceso puede tardar unos minutos.
6. Introduzca y para aceptar los términos de la licencia (o introduzca r para leer primero la licencia).
7. Seleccione n para rechazar el acuerdo de licencia que permite que este sistema actúe como servidor de licencias virtual.
8. Siga las instrucciones que aparecen en la consola serie local e introduzca la información del equipo que se le solicita al administrador de seguridad:
   a) Configurar el puerto interno
      i. Dirección IP
      ii. Máscara de red
      iii. Dirección de la puerta de enlace predeterminada
   b) Configurar el DNS

i. Dirección del servidor DNS primario

ii. Dirección del servidor DNS secundario (opcional)

iii. Nombre de dominio DNS predeterminado (por ejemplo, acmegizmo.com)

c) Se muestran al administrador de seguridad los ajustes de red configurados para que los revise. Introduzca «y» para aceptarlos o «n» para modificarlos.

d) Configurar el administrador

i. Nombre de usuario del administrador: introduzca un nombre de usuario de administrador. Esto creará una cuenta de usuario de administrador con todos los privilegios necesarios. Este nombre de usuario y esta contraseña se utilizarán a partir de ese momento a través de la interfaz gráfica de usuario web para las funciones de gestión del administrador.

ii. Contraseña de administrador: debe cumplir los requisitos de complejidad de la contraseña. Consulte la sección 6.3.6 CONFIGURACIÓN DE LA LONGITUD MÍNIMA DE LA CONTRASEÑA para conocer los requisitos y recomendaciones relativos a la contraseña.

e) Introduzca la información para crear un certificado auto firmado

i. Nombre común del equipo (por ejemplo, connect.acmegizmo.com)

ii. Nombre de la organización (por ejemplo, Acme Gizmo, Inc.)

iii. Introduzca texto aleatorio (utilizado para el certificado de autenticación)

Nota: Una vez creados los certificados autofirmados iniciales, el administrador puede acceder a la interfaz gráfica de usuario (GUI) del ICS, cargar el certificado adecuado siguiendo los pasos mencionados en la sección **6.6.6 INSTALACIÓN DE UN CERTIFICADO DE DISPOSITIVO** y, a continuación, proceder a la actualización a la versión CC designada.

El producto en la configuración de seguridad puede gestionarse a través de la interfaz gráfica de usuario web. Por lo tanto, la única consola serie local disponible para un administrador es la consola serie local, que proporciona una identificación clara para el acceso local.

Antes de que se complete con éxito la autenticación, el producto muestra un banner de acceso tal y como se describe en la sección **6.3.7 CONFIGURACIÓN DEL BANNER DE ADMINISTRACIÓN** de este documento. Este banner aparece tanto en la interfaz gráfica de usuario web como en la consola serie local.

Además, el producto responde a las solicitudes ICMP Echo (ping) en todas las interfaces de red antes de iniciar sesión; este comportamiento no requiere ninguna configuración y es el predeterminado.

5.2 CONFIGURACIÓN DEL MODO DISPOSITIVO DE RED

Los pasos para configurar el modo dispositivo de red (NDcPP) se describen en las secciones **6.5.1 ACTIVACIÓN DE LAS OPCIONES DE SSL ENTRANTE** y **6.5.2 ACTIVACIÓN DE LAS OPCIONES DE SSL SALIENTE** de este documento.

Una vez activado el modo dispositivo de red (NDcPP), se aplican automáticamente los siguientes comportamientos sin necesidad de realizar cambios adicionales en la configuración:

- El producto admite el cifrado y descifrado AES en los modos CBC y GCM utilizando claves de 128 y 256 bits.
- El producto admite la generación y verificación de firmas digitales mediante:
  - RSA (claves de 2048, 3072 y 4096 bits) con SHA-1, SHA-256, SHA-384 y SHA-512, de conformidad con las normas FIPS 186-4 y FIPS 186-5.
  - ECDSA con las curvas NIST P-256, P-384 y P-521 utilizando los algoritmos SHA-1, SHA-256, SHA-384 y SHA-512, también de conformidad con las normas FIPS 186-4 y FIPS 186-5.
- Cuando se utilizan conjuntos de cifrado ECDHE, el producto incluye automáticamente la extensión «Supported Groups» en el mensaje ClientHello.
- El producto incluye de forma predeterminada la extensión «signature_algorithms» en el mensaje «ClientHello», y esta no se puede modificar.
- El producto no admite la reanudación de sesión; no es necesaria ninguna configuración para aplicar esta restricción.
- Las claves precompartidas (PSK) no son compatibles con TLS 1.3, por lo que el aprovisionamiento de PSK fuera de banda no es posible en la configuración de seguridad.

5.3 VERIFICACIÓN DE LA VERSIÓN DEL SOFTWARE

5.3.1 VERIFICACIÓN DE LA VERSIÓN A TRAVÉS DE LA INTERFAZ GRÁFICA DE USUARIO

La versión actual del software, 22.7R2.13, se puede consultar en la interfaz gráfica de usuario web.

Para verificar la información de la versión del dispositivo, acceda a «Mantenimiento» > «Sistema» > «Plataforma».

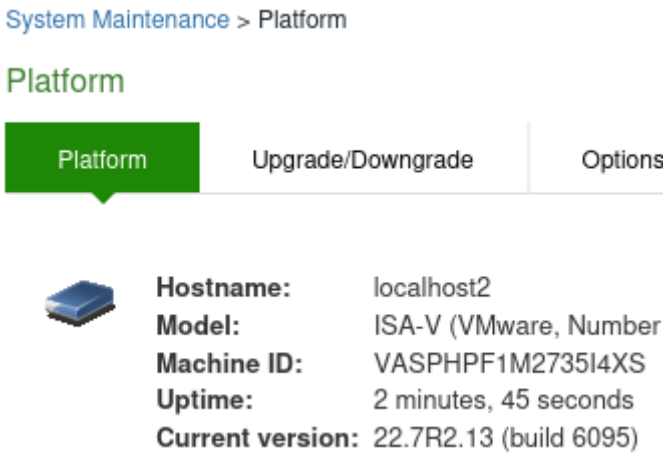


Ilustración 3: Menú Información de Versión

5.3.2 VERIFICACIÓN DE LA VERSIÓN A TRAVÉS DE LA CONSOLA SERIE LOCAL

La versión actual del software también se puede consultar en la consola serie local.

Los detalles de la versión se mostrarán una vez que el usuario de administración haya iniciado sesión en la consola serie local.

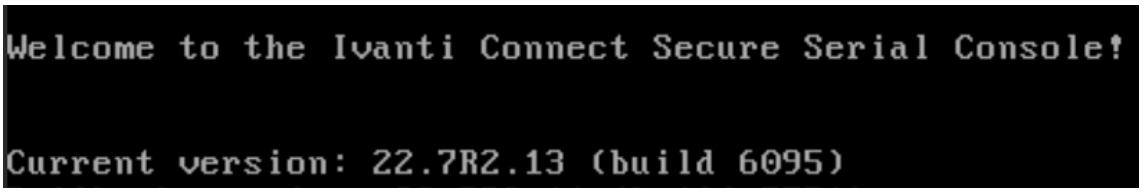


Ilustración 4: Detalles de la Versión

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

No es necesario ningún comando especial para activar el modo de operación seguro en el dispositivo. La configuración necesaria para que el producto opere de forma segura consistirá en aplicar una serie de configuraciones y políticas de seguridad a través de la interfaz de línea de comandos que se irán indicando en los siguientes apartados.

6.2 AUTENTICACIÓN

Los mecanismos de autenticación que utiliza el producto para la autenticación de usuarios son los siguientes (según la configuración evaluada y certificada. El producto soporta otros adicionales):

- **Credenciales:** mediante nombre de usuario y contraseña. Este mecanismo se utiliza para la autenticación de administradores tanto a través de la interfaz web de administración HTTPS como mediante la consola serie local.
- **Certificados X.509:** mediante la combinación de nombre de usuario y certificado digital X.509. El producto soporta certificados basados en algoritmos de firma RSA y ECDSA para la autenticación administrativa.

Los mecanismos de autenticación que utiliza el producto para la autenticación de otros sistemas o dispositivos son los siguientes:

- **Certificados TLS X.509:** utilizados para el establecimiento de comunicaciones seguras con servidores externos de auditoría (Syslog remoto) mediante autenticación mutua TLS.
- **Validación de certificados X.509:** utilizada durante el establecimiento de canales TLS seguros con sistemas externos. El producto verifica la validez temporal del certificado, la cadena de certificación, el estado de revocación mediante CRL y la integridad de las firmas digitales asociadas a los certificados presentados.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

El producto puede ser administrado de forma local o remota:

- **Administración local:** se realiza a través de la consola serie local. Para ello es necesario conectar un equipo al producto con un cable de consola. Para acceder a las funciones de administración de la línea de comandos (CLI) es necesario autenticarse como usuario administrador.
- **Administración remota:** se realiza a través de SSL. Para acceder a las funciones de administración remota es necesario autenticarse con las credenciales de un usuario autorizado en la interfaz web.

6.3.2 CONEXIÓN A LA INTERFAZ WEB DE ADMINISTRACIÓN

La interfaz gráfica de usuario web del administrador está disponible tras la configuración inicial a través de la consola serie local:

1. Abre un navegador web desde un ordenador portátil conectado al puerto de gestión del dispositivo.
2. Introduzca en el navegador la misma dirección IP que se asignó al puerto interno, seguida de /admin (por ejemplo, https://a.b.c.d/admin).
3. Cuando aparezca la alerta de seguridad para continuar sin un certificado firmado, haga clic en «Sí». La ausencia de certificado solo se produce durante la configuración inicial y no cuando el producto se encuentra en su configuración de evaluación. Cuando aparezca la página de inicio de sesión del administrador, significará que el dispositivo se ha conectado correctamente a la red.
4. En la página de inicio de sesión, introduzca el nombre de usuario y la contraseña de administrador que se crearon anteriormente. A continuación, haga clic en «Iniciar sesión».
5. Se abrirá la interfaz gráfica de usuario web del administrador en la página «Sistema > Estado > Resumen».

6.3.3 CONFIGURACIÓN DEL CONTROL DE ACCESO A LA CONSOLA SERIE LOCAL

La configuración del control de acceso del administrador a la consola serie local es un proceso que consta de dos pasos.

Paso 1: Habilitar el acceso a la consola serie local para el administrador. En la interfaz gráfica de usuario web del administrador,

1. Vaya a Autenticación > Servidores de autenticación.
2. Haga clic en Administradores.
3. En la pestaña Usuarios, seleccione el nombre del administrador configurado en la configuración inicial a través de la consola serie local.
4. Marque la casilla de verificación «Permitir acceso a la consola».

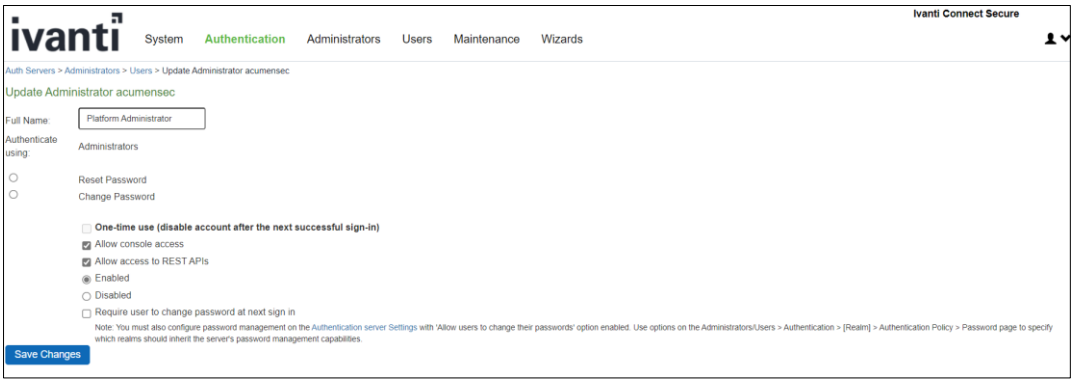


Ilustración 5: Menú configuración de Acceso por Consola de Serie Local

5. Haga clic en «Guardar cambios».

Nota: En la configuración de seguridad, no se debe habilitar el acceso a la consola serie local para los usuarios que no sean administradores.

Paso 2: Habilitar la protección con contraseña para la consola serie local.

1. Conéctese a la consola serie local; el menú de la consola serie local se muestra a continuación.
2. Seleccione la opción 5 en la consola serie local. El administrador debería ver un mensaje de confirmación: «Protección con contraseña habilitada; asegúrese de que el producto esté configurado con al menos un administrador local».

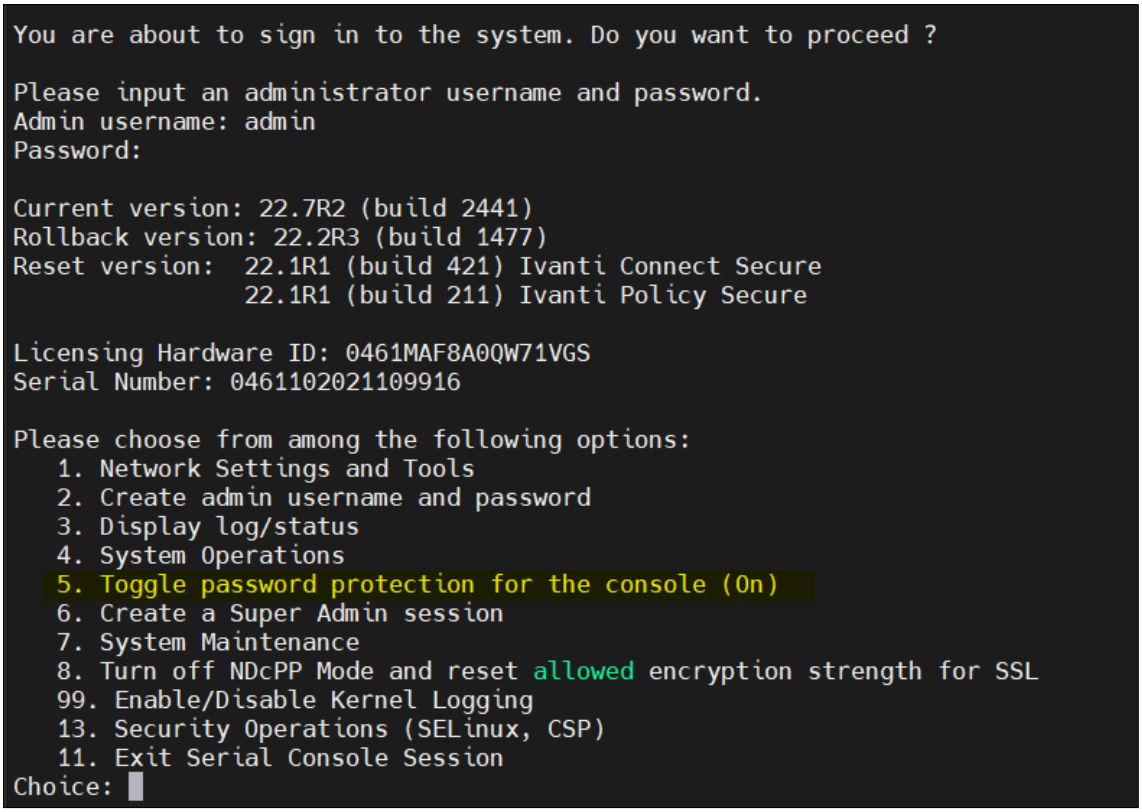


Ilustración 6: Mensaje de Confirmación de Acceso en la Consola Serie Local

Esta consola serie local solo está disponible para los administradores del producto. La autenticación impide que los usuarios que no sean administradores accedan a las funciones de manipulación de datos de la funcionalidad de seguridad del producto.

6.3.4 CONEXIÓN A LA CONSOLA SERIE LOCAL

Una vez configurada la autenticación, al acceder a la consola serie local se muestra al usuario una solicitud de autenticación.

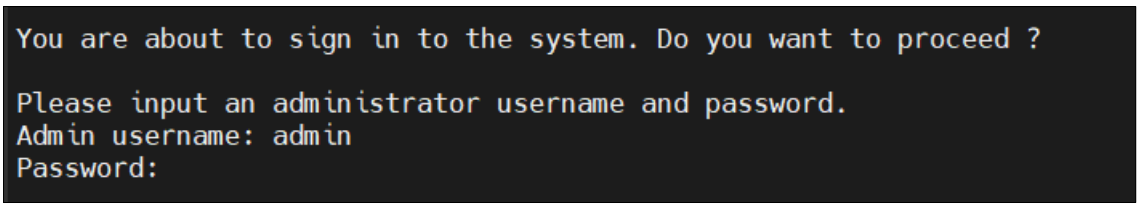


Ilustración 7: Mensaje de Inicio de Sesión mediante Consola Serie Local

Las siguientes opciones están disponibles desde la consola serie local.

- Configuración de red y herramientas
- Crear nombre de usuario y contraseña de administrador
- Mostrar registro/estado
- Operaciones del sistema
- Activar/desactivar la protección con contraseña de la consola serie local (Activada)
- Crear una sesión de superadministrador
- Mantenimiento del sistema
- Desactivar el modo dispositivo de red (NDcPP) y restablecer el nivel de cifrado permitido para SSL
- Habilitar/deshabilitar el registro del núcleo
- Operaciones de seguridad (SELinux, CSP)
- Salir de la sesión de la consola serie local

No se requieren pasos preparatorios para garantizar que los datos de autenticación no se revelen al introducir las credenciales. El producto no proporciona ninguna respuesta durante la introducción de la contraseña, tanto en el indicador de inicio de sesión conectado directamente como en el remoto.

6.3.5 CONFIGURACIÓN DE ADMINISTRADORES

El producto admite los siguientes roles de usuario de administración:

- **Administrador del sistema:** dispone de acceso completo de lectura y escritura a la interfaz administrativa, tanto a través de la interfaz gráfica de usuario web remota como de la consola serie local.
- **Administradores de solo lectura:** el administrador del sistema puede habilitar estos roles, cuyo acceso de escritura está restringido y que solo pueden leer la interfaz gráfica de usuario web. (En la configuración de seguridad, el usuario de solo lectura no tiene acceso a la consola serie local).

Para asignar un nivel de privilegios a los usuarios de administración mediante la asignación de roles.

1. Vaya a Administradores > Ámbitos de administración.
2. Haga clic en Usuarios de administración.
3. En la pestaña «Asignación de roles», haga clic en «Nueva regla…».

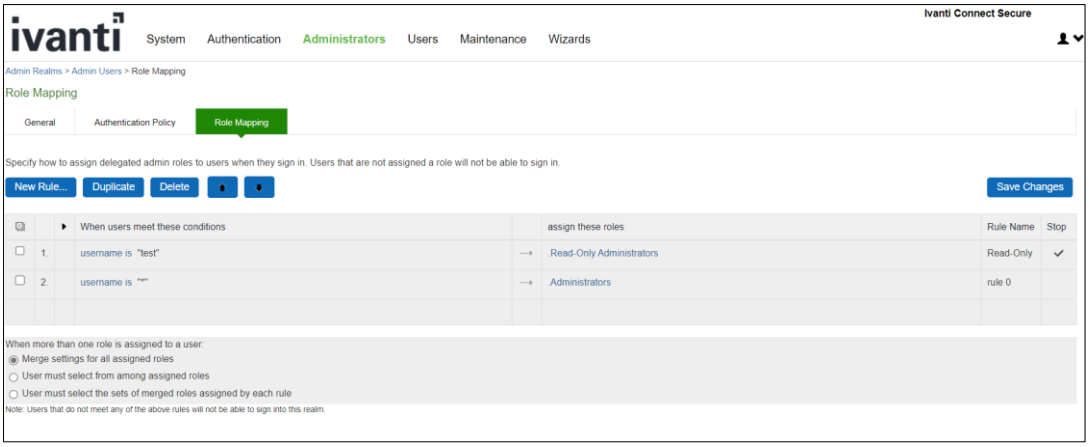


Ilustración 8: Configuración de Roles de Usuario Administrador

4. Nota: La funcionalidad de seguridad del producto protege los datos de auditoría frente a modificaciones y eliminaciones no autorizadas mediante interfaces administrativas restrictivas.
5. Los administradores de solo lectura tienen un nivel de privilegios más bajo y no pueden modificar ni eliminar parámetros relacionados con la seguridad ni el almacén de confianza. Los administradores del sistema tienen un nivel de privilegios alto y disponen de derechos para modificar la configuración del dispositivo.
6. En la selección «Regla basada en», seleccione la opción «Nombre de usuario» para crear una regla basada en los nombres de usuario.

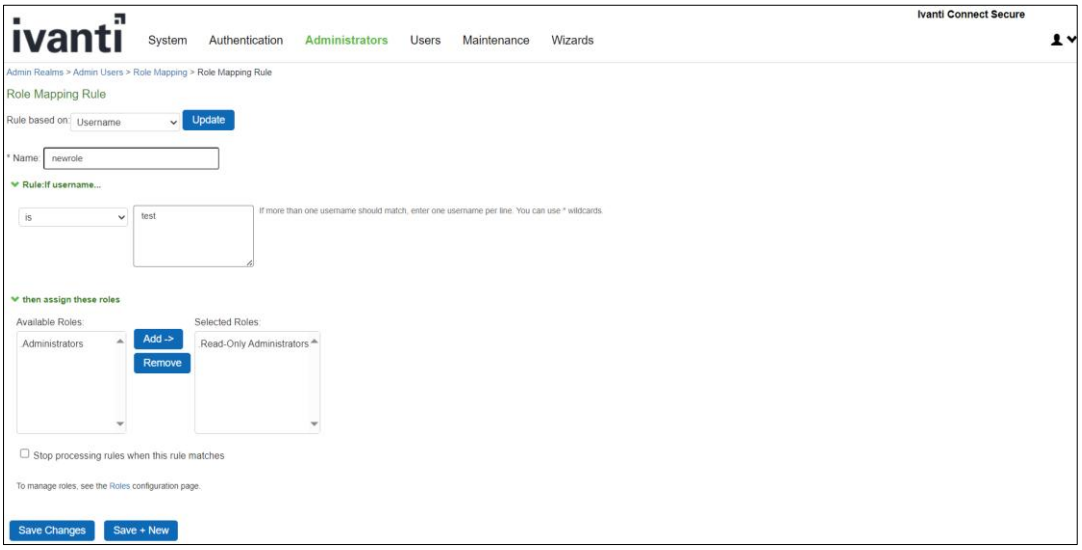


Ilustración 9: Asignación de Roles de Usuario Administrador

7. Introduzca un nombre para la regla y defina una condición de regla.
8. Asigne un rol al nombre de usuario administrador según la regla creada. Haga clic en «Guardar cambios».

Para más información sobre los privilegios de usuario administrador, consultar el apartado "adminuser privilege level" de [REF1]. Se debe asignar a los usuarios los mínimos privilegios necesarios para realizar sus labores de administración.

Para la creación de usuarios de administración, se debe consultar los apartados "Configuring a Local User" y "Configuring an SSH User" de [REF1] para el procedimiento en detalle sobre la configuración y creación de usuarios.

6.3.6 CONFIGURACIÓN DE LA LONGITUD MÍNIMA DE LA CONTRASEÑA

En la interfaz gráfica de usuario web del administrador, sigue las instrucciones que se indican a continuación para establecer la longitud mínima de la contraseña de administrador, que se puede configurar dentro del rango establecido de entre 12 y 15 caracteres.

1. Configura lo siguiente en la configuración del servidor de autenticación local:
   a) Vaya a Autenticación > Servidores de autenticación.
   b) Haga clic en Administradores.
   c) En la pestaña Configuración, en la sección Opciones de contraseña.
      i. Configure la longitud mínima entre 12 y 15 caracteres.
      ii. Configure la longitud máxima según la política de la organización.

Nota: La longitud máxima de la contraseña se puede configurar hasta un máximo de 999 caracteres.

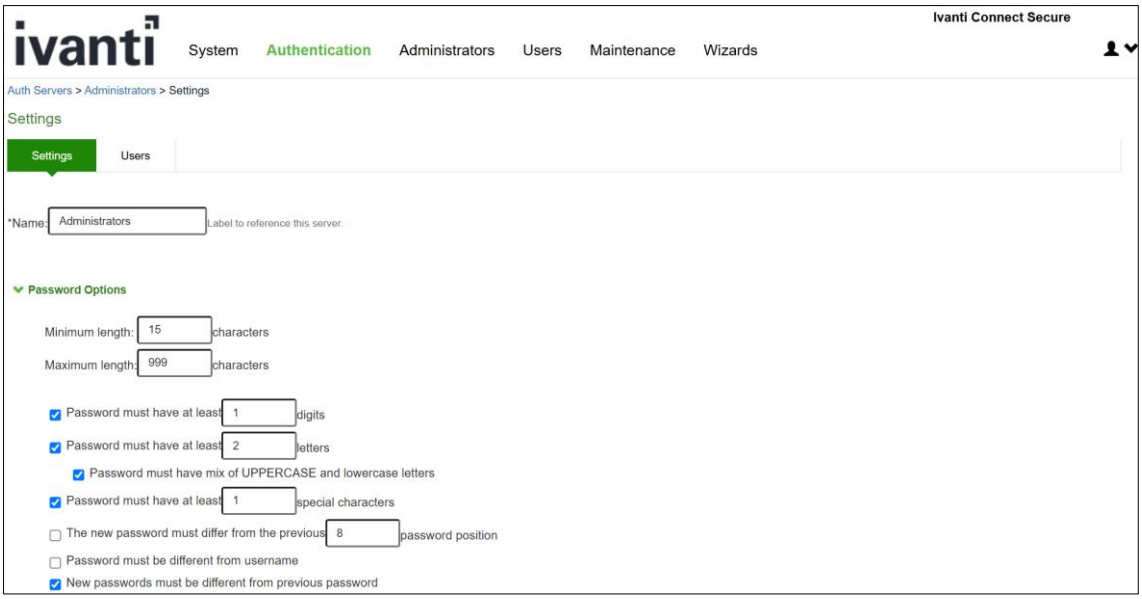


Ilustración 10: Menú de Configuración de Opciones de Contraseña de Usuario Administrador

2. Revisa todas las contraseñas de administrador configuradas anteriormente y actualízalas para asegurarte de que todas tengan al menos 12 caracteres.

3. Por defecto, las contraseñas no se muestran en pantalla y pueden incluir los siguientes caracteres: «!», «@», «#», «$», «%», «^», «&», «*», «(», «)».

Los administradores de seguridad deben utilizar contraseñas seguras que incluyan una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Evite palabras comunes, frases o patrones fáciles de adivinar, como números secuenciales o secuencias de teclado, y exija actualizaciones periódicas de las contraseñas.

6.3.7 CONFIGURACIÓN DEL BANNER DE ADMINISTRACIÓN

La configuración del banner de administrador para la interfaz gráfica de usuario web del administrador y la consola serie local es un proceso de dos pasos que se puede realizar a través de la interfaz gráfica de usuario web.

Paso 1: Para configurar y aplicar las notificaciones de inicio de sesión:

En la interfaz gráfica de usuario web del administrador:

1. Acceda a Autenticación > Inicio de sesión > Notificaciones de inicio de sesión.

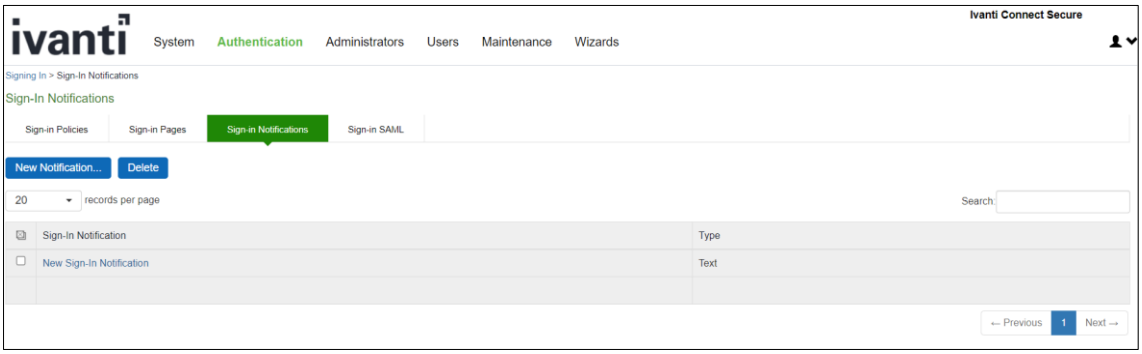


Ilustración 11: Menú Notificaciones de Inicio de Sesión

2. Haga clic en «Nueva notificación…»
    a) Introduzca un nombre para la nueva notificación en el campo «Nombre:».
    b) Introduzca el mensaje del banner en el campo «Texto:».

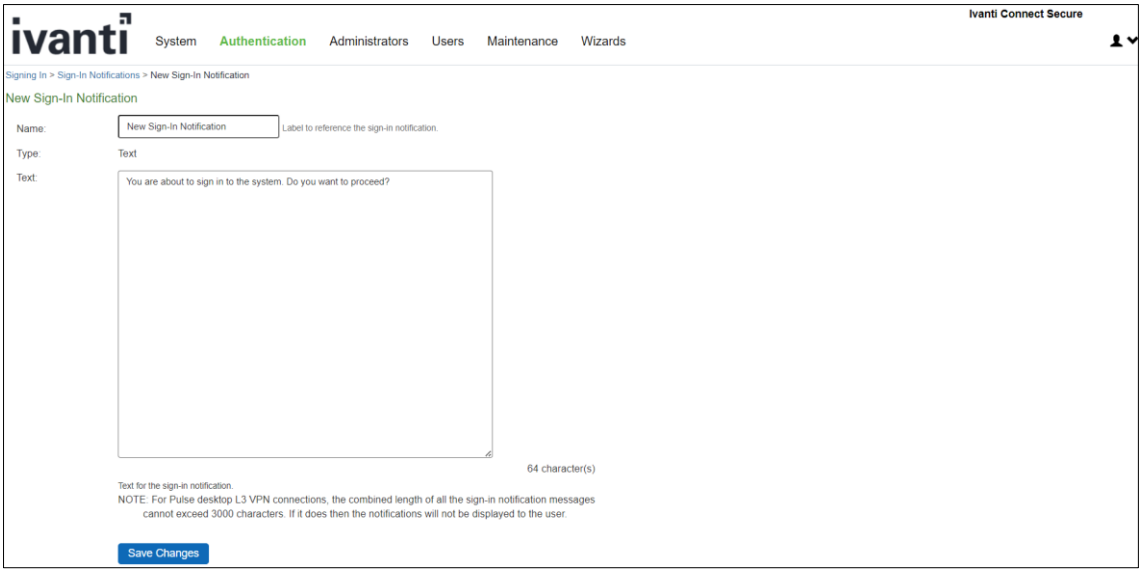


Ilustración 12: Menú de Configuración del Banner de Inicio de Sesión

3. Haga clic en «Guardar cambios».

Paso 2: Para habilitar las notificaciones de inicio de sesión:

En la interfaz gráfica de usuario web del administrador,

1. Vaya a «Autenticación» > «Inicio de sesión» > «Políticas de inicio de sesión».
2. Seleccione una URL existente (por ejemplo: */admin/) o crea una nueva URL.
3. En la sección «Configurar notificaciones de inicio de sesión», marque la casilla «Notificación de inicio de sesión previa a la autenticación» o «Notificación de inicio de sesión posterior a la autenticación», o ambas.
4. En «Notificación de inicio de sesión previa a la autenticación», seleccione una notificación de inicio de sesión configurada previamente en el menú desplegable.



Ilustración 13: Menú Notificaciones de Inicio de Sesión

5. En «Notificación de inicio de sesión posterior a la autenticación», seleccione la opción «Utilizar una notificación de inicio de sesión común para todos los roles» o «Utilizar la notificación de inicio de sesión asociada al rol asignado».



Ilustración 14: Menú de Configuración del Banner de Inicio de Sesión

6. Si un administrador selecciona «Utilizar una notificación de inicio de sesión común para todos los roles», seleccione una notificación de inicio de sesión configurada previamente en el menú desplegable.
7. Si un administrador selecciona «Utilizar la notificación de inicio de sesión asociada al rol asignado», se utilizará la notificación de inicio de sesión configurada para el rol asignado.
8. Evita que se muestre la notificación de inicio de sesión tras la autenticación a los usuarios administrador que ya la hayan visto, marcando la casilla «Omitir si ya se ha mostrado».
9. Haga clic en «Guardar cambios».

El banner configurado en la interfaz gráfica de usuario administrador se aplicará tanto a las conexiones locales como a las remotas.

6.3.8 CONFIGURACIÓN DEL TIEMPO DE ESPERA POR INACTIVIDAD

El producto admite la finalización automática de las sesiones administrativas locales y remotas tras un periodo configurable de inactividad; no admite el bloqueo de sesiones.

En la interfaz gráfica de usuario de administración,

1. Acceda a Administradores > Roles de administrador.
2. Seleccione el nombre del rol que deseas configurar.

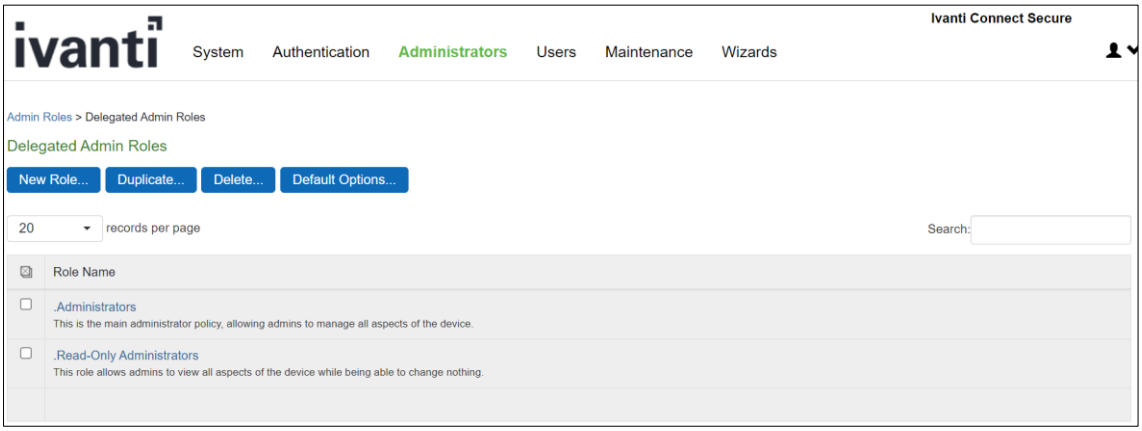


Ilustración 15: Menú de Configuración de Roles

3. En la pestaña Opciones de sesión, en la sección Duración de la sesión, introduzca el tiempo de espera por inactividad en minutos. El tiempo de espera por inactividad predeterminado es de 10 minutos, y el rango configurable va de 5 a 9 999 999 minutos. Aunque el tiempo de espera por inactividad se puede configurar dentro de un amplio rango, se recomienda encarecidamente que el administrador de seguridad establezca el valor entre 5 y 15 minutos.

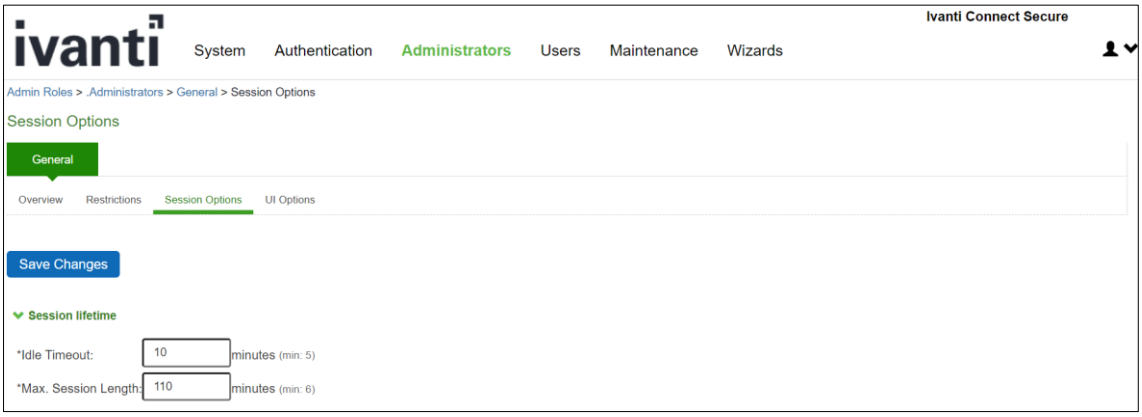


Ilustración 16: Menú de Opciones de Sesión de Usuario Administrador

4. Haga clic en «Guardar cambios».

Este periodo de tiempo de espera configurado se aplica tanto a las sesiones remotas de la interfaz gráfica de usuario administrador como a las sesiones de la consola serie local.

Nota: La tarea periódica que comprueba los tiempos de espera de inactividad de las sesiones se ejecuta cada 10 minutos. Como resultado, la finalización efectiva de una sesión inactiva puede retrasarse. Si el tiempo de espera de inactividad se configura en el valor mínimo de 5 minutos, la sesión puede finalizar hasta 5 minutos después de la última actividad.

6.3.9 CONFIGURACIÓN DEL BLOQUEO POR FALLOS DE AUTENTICACIÓN

El bloqueo por fallos de autenticación se configura en la interfaz gráfica de usuario web del administrador.

En la interfaz gráfica de usuario del administrador:

1. Acceda a Autenticación > Servidores de autenticación.
2. Haga clic en Administradores.

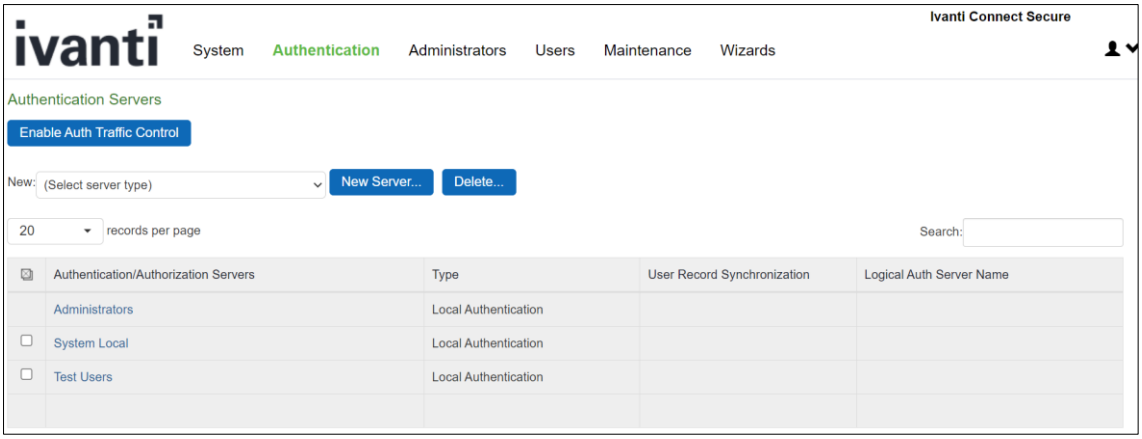


Ilustración 17: Menú de Servidores de Autenticación

3. En la pestaña Configuración, en la sección Bloqueo de cuentas, configura el Número máximo de intentos fallidos de contraseña y el Periodo de bloqueo de la cuenta.

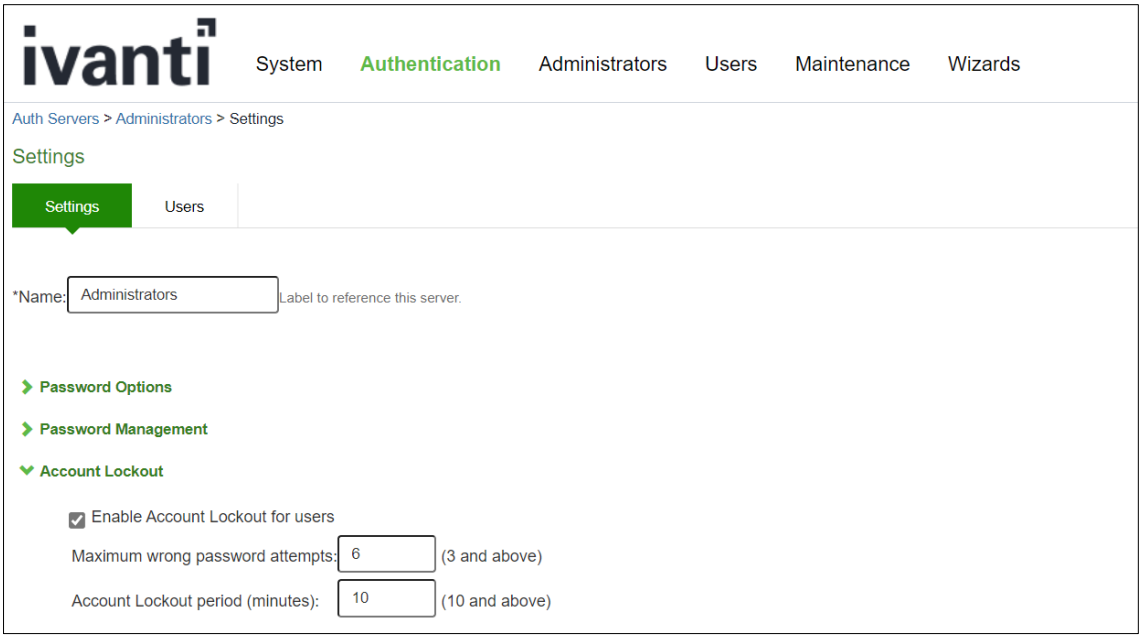


Ilustración 18: Menú de Configuración de Bloqueo de Cuentas de Usuario Administrador

- La configuración de seguridad requiere que este parámetro esté comprendido entre 3 y 10. La duración del bloqueo se puede configurar entre 3 y 999 minutos.
- Si el usuario administrador introduzca una contraseña incorrecta el número de veces configurado, se le bloquea el acceso y no podrá iniciar sesión a través de ninguna interfaz remota en el producto.
- Una vez transcurrido el tiempo de bloqueo, el administrador podrá volver a autenticarse en el producto.
- Los bloqueos no se aplican en la interfaz de la consola serie local del producto. Esto garantiza que los errores de autenticación no puedan dar lugar a una situación en la que no se disponga de acceso de administrador.

Además, los siguientes ajustes determinan cómo se gestionan los intentos fallidos de inicio de sesión. Cuando se supera el número de intentos permitidos, la dirección IP utilizada para iniciar sesión se bloqueará temporalmente para evitar ataques de inicio de sesión automatizados.

1. Acceda a Sistema > Configuración.
2. En la pestaña Seguridad, vaya a Varios.
3. En la sección Opciones de bloqueo, configure los intentos de inicio de sesión y el periodo de bloqueo.

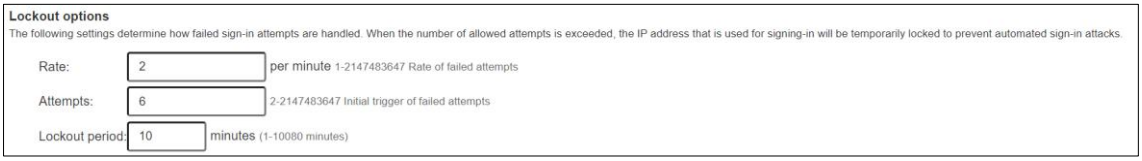


Ilustración 19: Opciones de Bloqueo de Cuenta

Nota: El número de intentos de inicio de sesión y el periodo de bloqueo deben ser los mismos en ambas configuraciones («Bloqueo de cuenta» y «Opciones de bloqueo»). El bloqueo de la cuenta se activa tras el primer intento fallido de inicio de sesión inmediatamente posterior al límite configurado para el bloqueo de la cuenta. Por ejemplo, si el límite es de «n» intentos, la cuenta se bloquea tras el (n+1)º intento fallido.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

6.4.1 CONFIGURACIÓN DEL PUERTO INTERNO

El puerto interno está conectado a la LAN interna, donde están activos los servidores Syslog, DNS y CRL.

Para configurar el puerto interno en la interfaz gráfica de usuario web del administrador,

1. Acceda a Sistema > Red.

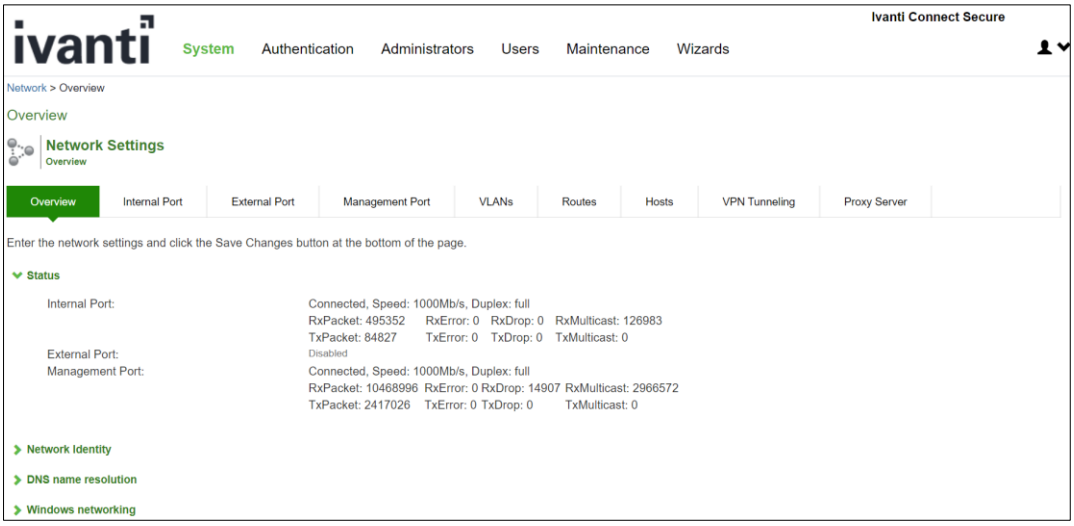


Ilustración 20: Menú Configuración de Red

2. En la pestaña «Puerto interno», vaya a «Configuración».
3. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada.

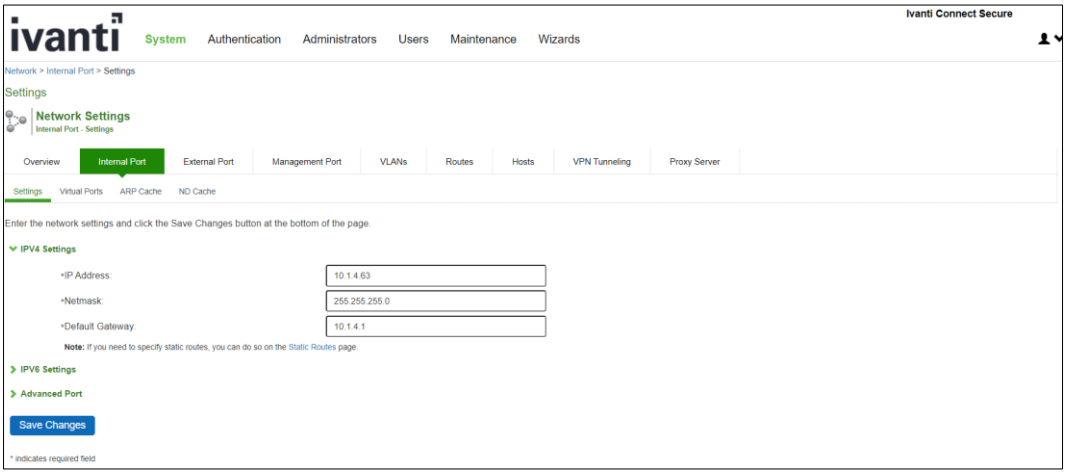


Ilustración 21: Configuración de IP

4. Haga clic en Guardar cambios.

6.4.2 CONFIGURACIÓN DEL PUERTO DE GESTIÓN

El puerto de gestión está conectado a la estación de trabajo remota para permitir el acceso de gestión al producto.

Para configurar el puerto de gestión en la interfaz gráfica de usuario web del administrador:

1. Vaya a Sistema > Red.
2. En la pestaña «Puerto de gestión», vaya a «Configuración».
3. Haga clic en «Habilitado» en la sección «Usar puerto».
4. Haga clic en «Habilitado» en la sección «Configuración de IPv4».
5. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada.

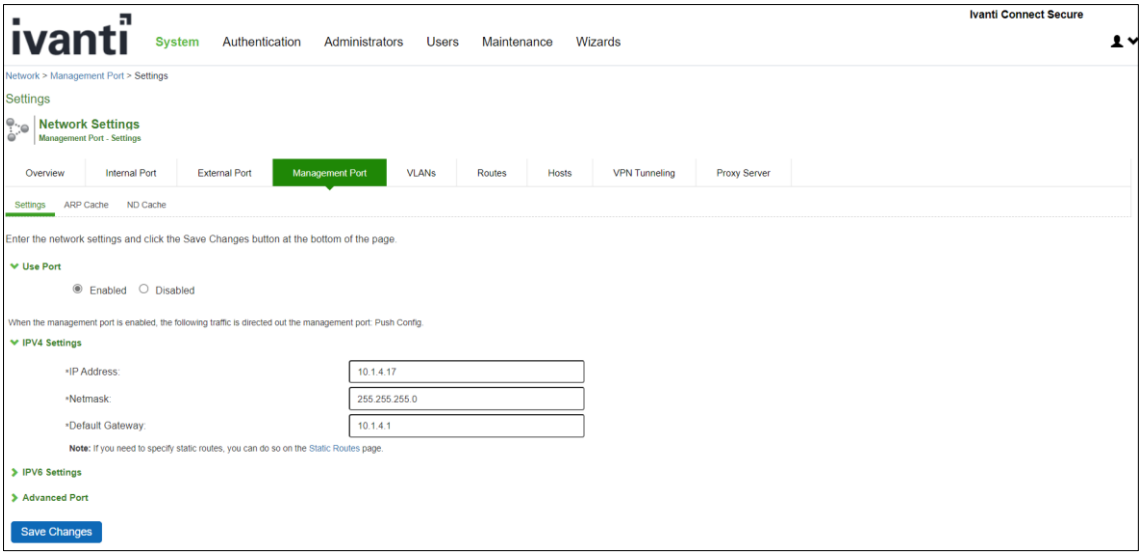


Ilustración 22: Configuración del Puerto de Gestión

6. Haga clic en «Guardar cambios».

6.4.3 CONFIGURACIÓN **DEL SERVIDOR DNS**

Para configurar el servidor DNS en la interfaz gráfica de usuario web del administrador,

1. Navegar a Sistema > Red.
2. En la pestaña «Resumen», en la sección «Resolución de nombres DNS», introduzca la dirección IPv4/IPv6 para el DNS primario y los dominios DNS.
3. El DNS secundario es un campo opcional.
4. Seleccione la respuesta DNS preferida: IPv4.
5. Seleccione el puerto para el tráfico DNS: puerto interno.
6. Haga clic en «Guardar cambios».

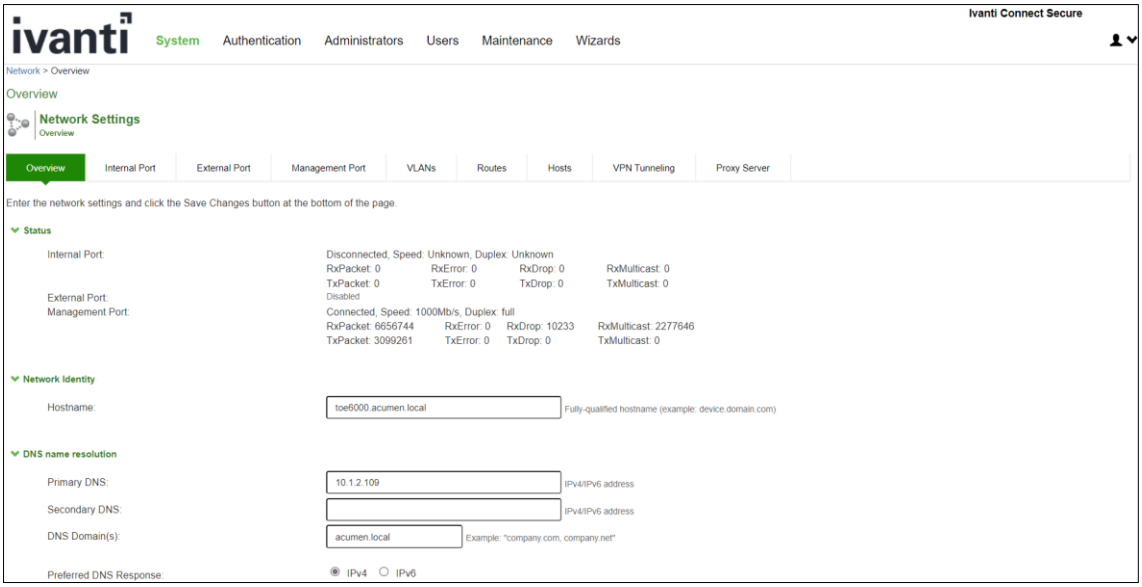


Ilustración 23: Configuración del DNS

6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

Los pasos para configurar el modo dispositivo de red (NDcPP) se describen en las secciones 6.5.1 ACTIVACIÓN DE LAS OPCIONES DE SSL ENTRANTE y 6.5.2 ACTIVACIÓN DE LAS OPCIONES DE SSL SALIENTE.

Una vez activado el modo dispositivo de red (NDcPP), se aplican automáticamente los siguientes comportamientos sin necesidad de realizar cambios adicionales en la configuración:

- El producto admite el cifrado y descifrado AES en los modos CBC y GCM utilizando claves de 128 y 256 bits.
- El producto admite la generación y verificación de firmas digitales mediante:
  - RSA (claves de 2048, 3072 y 4096 bits) con SHA-1, SHA-256, SHA-384 y SHA-512, de conformidad con las normas FIPS 186-4 y FIPS 186-5.
  - ECDSA con las curvas NIST P-256, P-384 y P-521 utilizando los algoritmos SHA-1, SHA-256, SHA-384 y SHA-512, también de conformidad con las normas FIPS 186-4 y FIPS 186-5.
- Cuando se utilizan conjuntos de cifrado ECDHE, el producto incluye automáticamente la extensión «Supported Groups» en el mensaje ClientHello.
- El producto incluye de forma predeterminada la extensión «signature_algorithms» en el mensaje «ClientHello», y esta no se puede modificar.
- El producto no admite la reanudación de sesión; no es necesaria ninguna configuración para aplicar esta restricción.
- Las claves precompartidas (PSK) no son compatibles con TLS 1.3, por lo que el aprovisionamiento de PSK fuera de banda no es posible en la configuración de seguridad.

6.5.1 ACTIVACIÓN DE LAS OPCIONES DE SSL ENTRANTE

En la interfaz gráfica de usuario web del administrador,

1. Acceda a Sistema > Configuración > pestaña Seguridad > Opciones de SSL entrante.
2. Marque la casilla «Activar modo NDcPP» en la opción «Modo SSL NDcPP» para que el dispositivo cumpla con los criterios comunes.

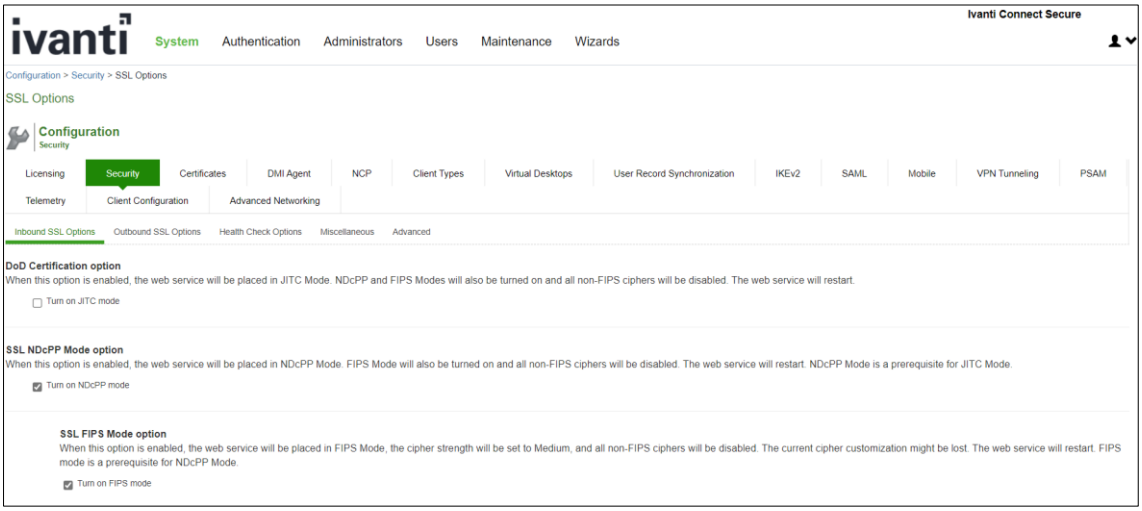


Ilustración 24: Menú de Configuración de los Protocolos de Conexiones Entrantes

3. Una vez activada la opción «Activar modo NDcPP», la opción «Activar modo FIPS» también se activa automáticamente.

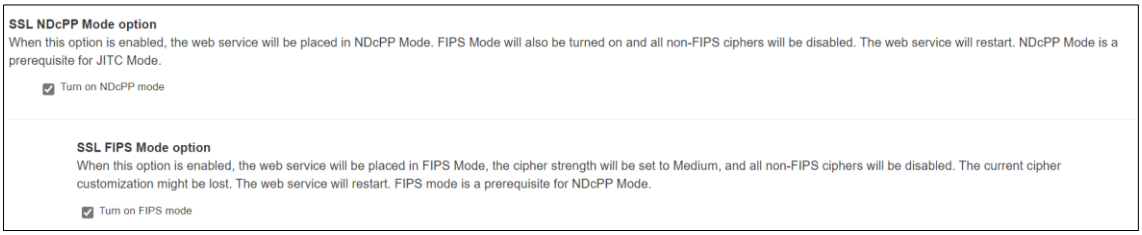


Ilustración 25: Opción Activación Modo FIPS

4. Una vez seleccionado el modo dispositivo de red (NDcPP), seleccione las versiones de TLS que el dispositivo debe admitir, es decir, «Aceptar solo TLS 1.2 y posteriores», y seleccione la opción «Habilitar TLS 1.3» en «Versiones de SSL y TLS permitidas».
   Nota: Si La funcionalidad de seguridad del producto recibe un mensaje «ClientHello» que solicita TLSv1.1 o una versión anterior, la funcionalidad de seguridad del producto envía un mensaje de error grave «handshake_failure» y termina la conexión.

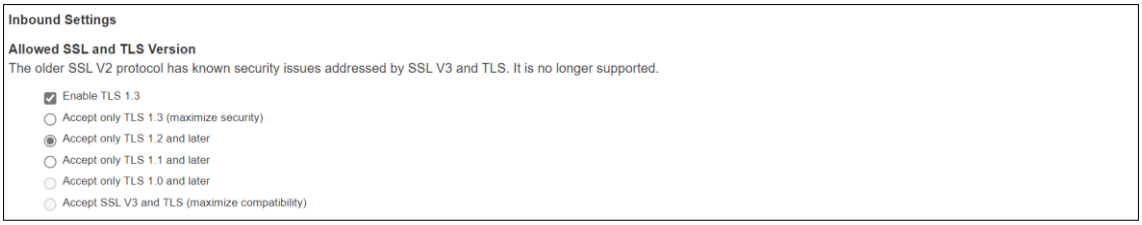


Ilustración 26: Menú de Configuración de Protocolos TLS

5. Seleccione la opción «Selección personalizada de cifrado SSL» en el campo «Nivel de cifrado permitido».

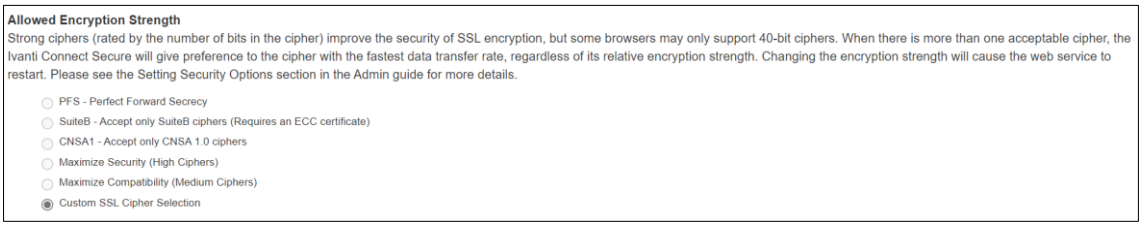


Ilustración 27: Menú de Aceptación de Configuraciones de Cifrado

6. Se muestran los dos paneles «Cifrados compatibles» y «Cifrados seleccionados». «Cifrados compatibles» contiene la lista completa de cifrados compatibles con la versión de SSL o TLS seleccionada. «Cifrados seleccionados» muestra la lista de cifrados seleccionados actualmente.
7. Para añadir un cifrado que se utilizará para proteger una conexión, haga clic en la cadena del cifrado en el panel de la izquierda y, a continuación, haga clic en el botón «Añadir >».
8. Para eliminar el cifrado, haga clic en el nombre del cifrado en el panel de la derecha y, a continuación, haga clic en el botón «< Eliminar».
9. Los algoritmos de cifrado seleccionados a la derecha aparecen ordenados por prioridad, de arriba abajo. Para cambiar la prioridad de los algoritmos, haga clic en el nombre del algoritmo y, a continuación, haga clic en «Subir» para aumentar la prioridad o en el botón «Bajar» para reducirla.
   Nota: Solo se deben seleccionar y habilitar los siguientes conjuntos de cifrado TLS indicados. Cualquier conjunto de cifrado que no figure en la lista debe deseleccionarse para garantizar la conformidad con la configuración de seguridad.

   Conjuntos de cifrado TLS 1.2:
   - TLS_RSA_WITH_AES_128_CBC_SHA
   - TLS_RSA_WITH_AES_256_CBC_SHA
   - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
   - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
   - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
   - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
   - TLS_RSA_WITH_AES_128_CBC_SHA256
   - TLS_RSA_WITH_AES_256_CBC_SHA256
   - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
   - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Conjuntos de cifrado TLS 1.3:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

La siguiente figura muestra la configuración de las selecciones personalizadas de cifrado SSL:

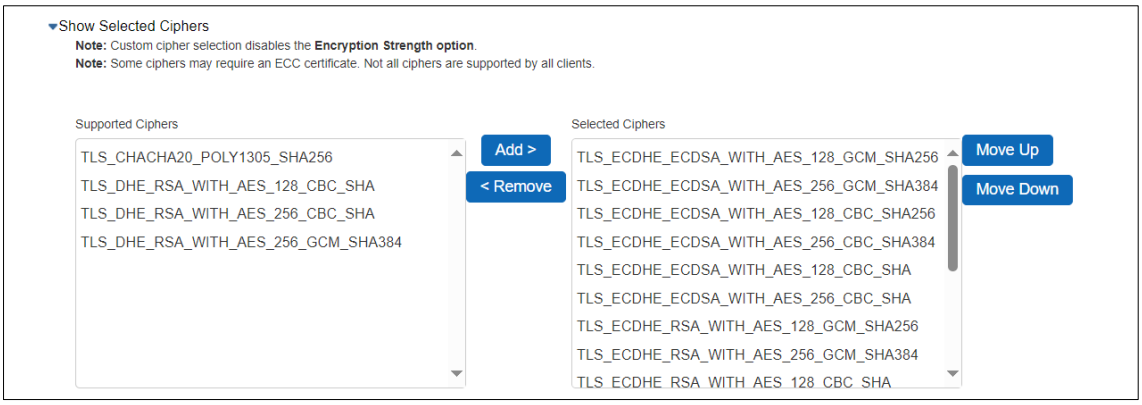


Ilustración 28: Menú de Selección de Ciphersuites Entrantes

Las funciones criptográficas —entre las que se incluyen la generación de claves, el establecimiento de claves, el cifrado de datos y la generación de firmas— dependen de la configuración del conjunto de cifrado en el producto. El conjunto de cifrado determina los algoritmos utilizados para estas funciones; por ejemplo, especifica cómo se generan las claves (p. ej., pares de claves RSA), cómo se intercambian las claves (p. ej., RSA, ECDH), qué algoritmos de cifrado se utilizan (p. ej., AES) y qué algoritmos se utilizan para la generación de firmas (p. ej., RSA, ECDSA).

10. La opción «Compatibilidad con renegociación SSL heredada» está desactivada de forma predeterminada y no permite la renegociación entre clientes y servidores.



Ilustración 29: Menú de Compatibilidad de Negociación SSL Heredado

11. Seleccione «Habilitar redirección de puertos para la autenticación de certificados TLSv1.3» para permitir la autenticación mediante certificado de cliente a través de conexiones TLSv1.3 para navegadores o clientes que no admitan la autenticación posterior al protocolo de enlace (PHA). Es posible que sea necesario realizar cambios en la configuración de red para que el cliente pueda acceder al puerto especificado.

Nota: Cuando la redirección de puertos está habilitada, el proceso de autenticación se gestiona en el puerto configurado, incluida la autenticación secundaria, si la hubiera.

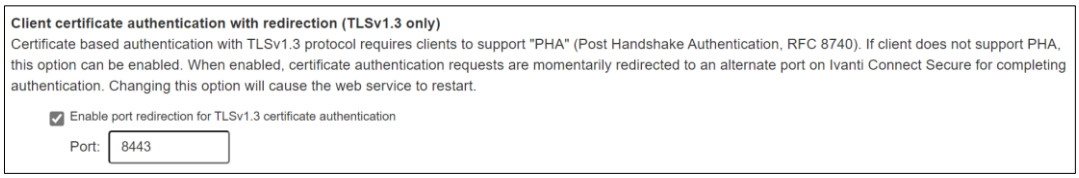


Ilustración 30: Puerto de Autenticación de Certificados TLS

12. Haga clic en Guardar cambios.
13. Aparecerá una advertencia en la que se pedirá al administrador de seguridad que confirme la configuración. Haga clic en Continuar para seguir adelante.

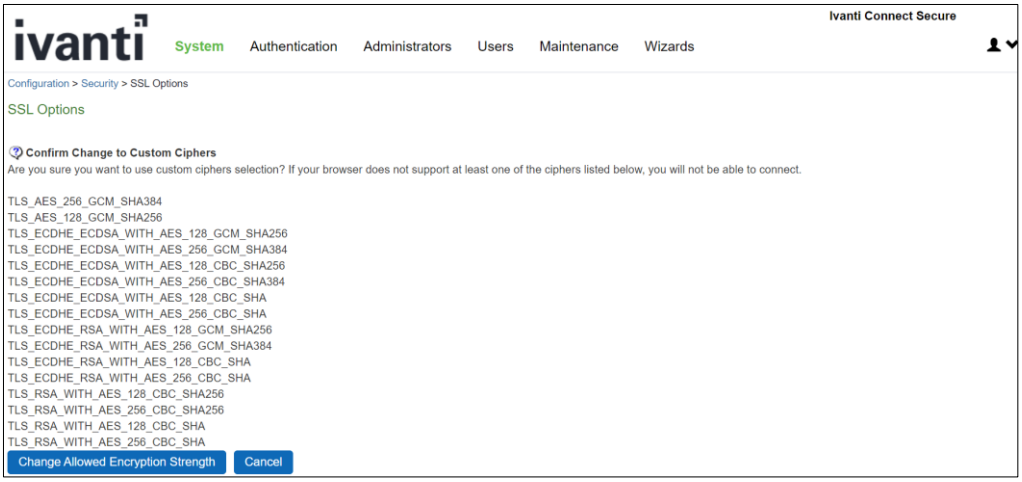


Ilustración 31: Menú de Selección de Ciphersuites Entrantes

14. Se muestra una lista de los algoritmos de cifrado personalizados que se utilizarán en el puerto del dispositivo, en el orden en que el servidor web los seleccionará.

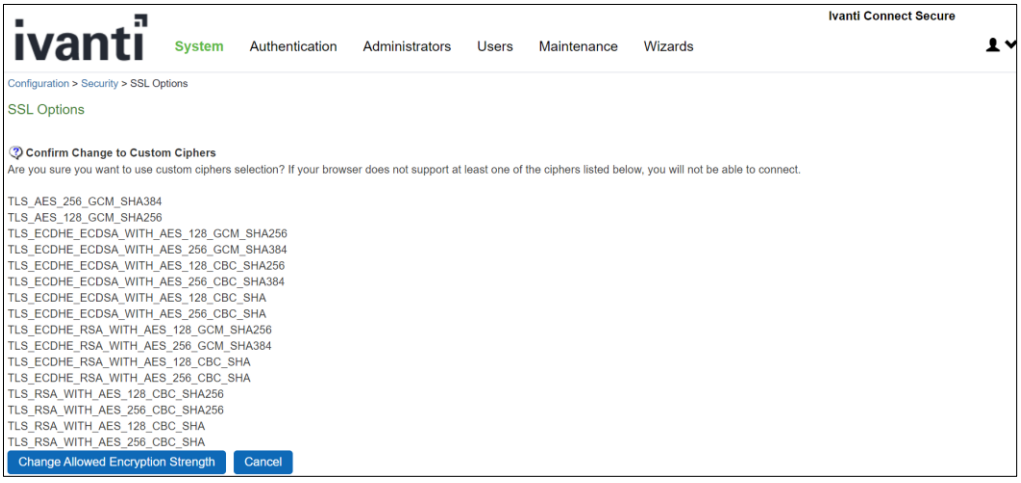


Ilustración 32: Menú de Confirmación de Selección de Ciphersuites

15. Haga clic en «Cambiar el nivel de cifrado permitido».

6.5.2 ACTIVACIÓN DE LAS OPCIONES DE SSL SALIENTE

En la interfaz gráfica de usuario web del administrador,

1. Acceda a Sistema > Configuración > pestaña Seguridad > Opciones de SSL saliente.
2. Seleccione las versiones de TLS que el dispositivo debe admitir: «Aceptar solo TLS 1.2 y posteriores» en el campo «Versiones de SSL y TLS permitidas».

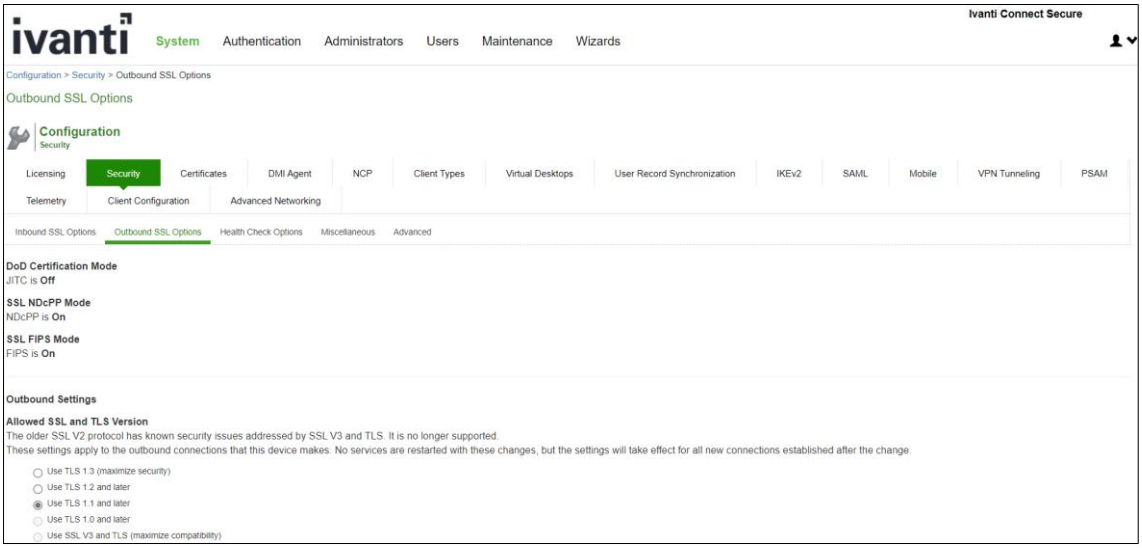


Ilustración 33: Menú de Configuración de los Protocolos de Conexiones Salientes

3. Seleccione la opción «Selección personalizada de cifrado SSL» en el campo «Nivel de cifrado permitido».

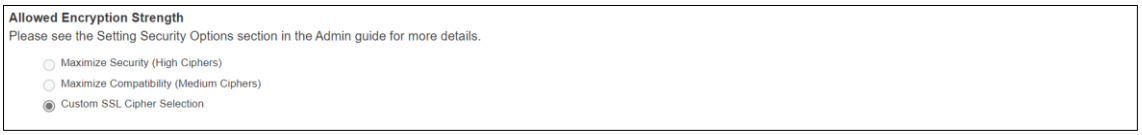


Ilustración 34: Menú de Aceptación de Configuraciones de Cifrado

4. Los cifrados seleccionados a la derecha aparecen ordenados por prioridad de arriba abajo. Para cambiar la prioridad de los cifrados, haga clic en el nombre del cifrado y, a continuación, haga clic en «Subir» para aumentar la prioridad o en el botón «Bajar» para reducirla.
   Nota: Solo deben seleccionarse y habilitarse los siguientes conjuntos de cifrado TLS declarados. Cualquier conjunto de cifrado que no figure en la lista debe deseleccionarse para garantizar la conformidad con la configuración de seguridad.

Conjuntos de cifrado TLS 1.2:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Conjuntos de cifrado TLS 1.3:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

La siguiente figura muestra la configuración de las selecciones de cifrado SSL personalizadas:

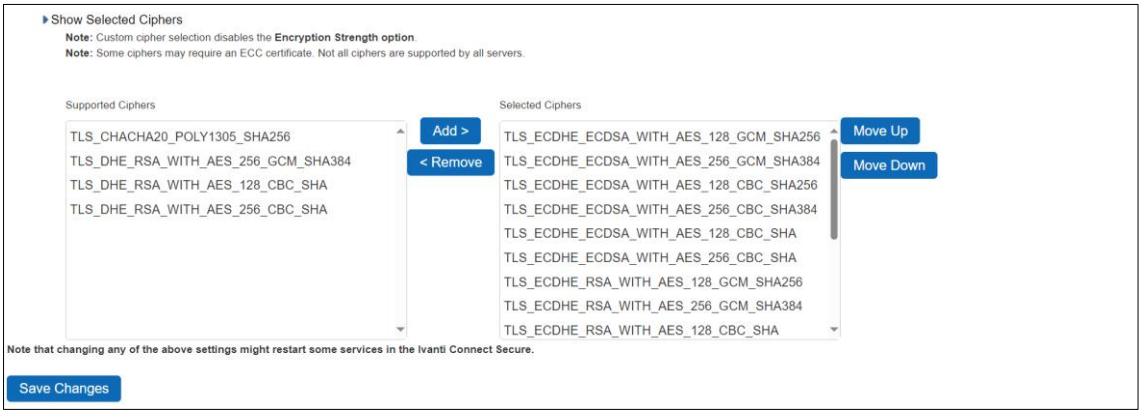


Ilustración 35: Menú de Selección de Ciphersuites Salientes

Las funciones criptográficas —entre las que se incluyen la generación de claves, el establecimiento de claves, el cifrado de datos y la generación de firmas— dependen de la configuración del conjunto de cifrado en el producto.

5. Aparecerá una advertencia en la que se le pedirá al administrador de seguridad que confirme la configuración. Haga clic en «Continuar» para seguir adelante.
6. Se muestra una lista de los cifrados personalizados que se utilizarán en el puerto del dispositivo, en el orden en que el servidor web los seleccionará.

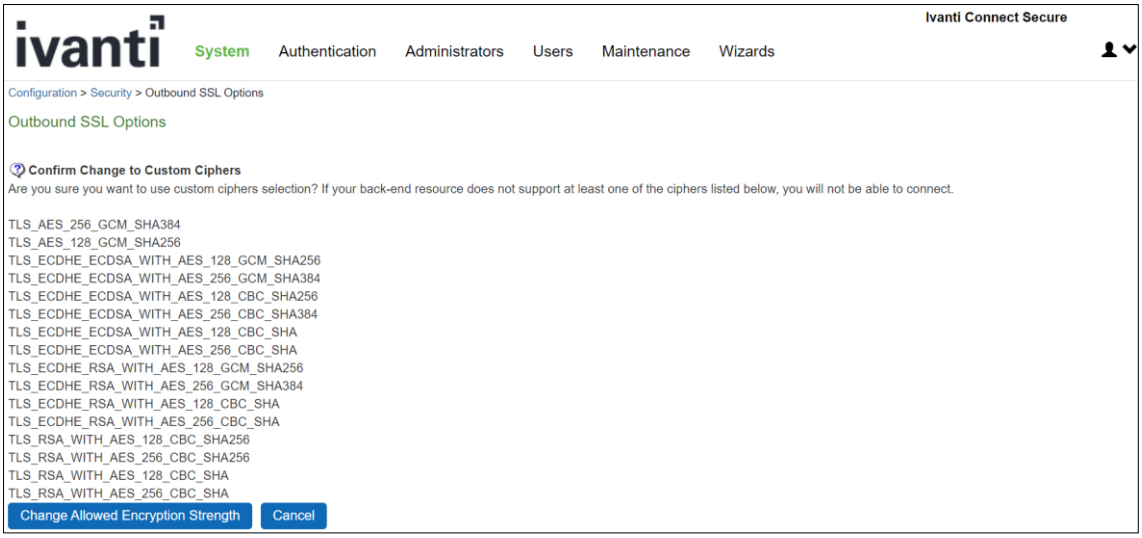


Ilustración 36: Menú de Selección de Ciphersuites Salientes

7. Haga clic en «Cambiar la intensidad de cifrado permitida».

6.6 GESTIÓN DE CERTIFICADOS

6.6.1 IMPORTAR UN CERTIFICADO DE CA DE CLIENTE DE CONFIANZA

Se requieren autoridades de certificación (CA) de cliente de confianza para validar el certificado de cliente que utiliza el producto para autenticarse en el servidor Syslog.

En la interfaz gráfica de usuario web del administrador,

1. Acceda a Sistema > Configuración > Certificados > Autoridades de certificación de cliente de confianza para mostrar la página de configuración.
2. Haga clic en Importar certificados de CA… para importar una CA o una cadena de CA una por una, tal y como se indica a continuación.
3. Haga clic en Examinar, seleccione el certificado y haga clic en Importar certificado.
4. Las CA de cliente de confianza importadas aparecerán entonces en la tabla «Autoridades de certificación de cliente de confianza».

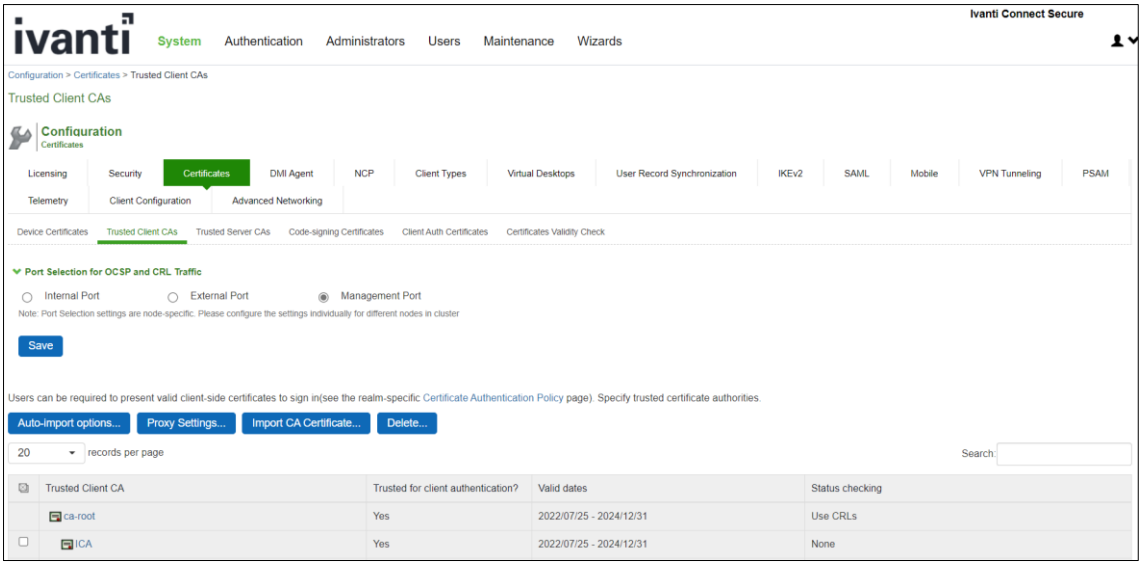


Ilustración 37: Menú de Configuración de Certificado CA de Cliente de Confianza

6.6.2 IMPORTAR DE UN CERTIFICADO DE CA DE SERVIDOR DE CONFIANZA

Las CA de servidor de confianza se utilizan en dos situaciones:

- Para validar el certificado del dispositivo que se genera para el protocolo de enlace TLS cuando un cliente TLS se conecta al producto.
- Para validar el certificado de servidor recibido en el protocolo de enlace TLS cuando el producto se conecta al servidor Syslog.

Para cargar certificados de CA de servidor en la interfaz gráfica de usuario web del administrador,

1. Acceda a Sistema > Configuración > Certificados > CA de servidores de confianza.
2. Haga clic en «Importar CA de servidor de confianza…»

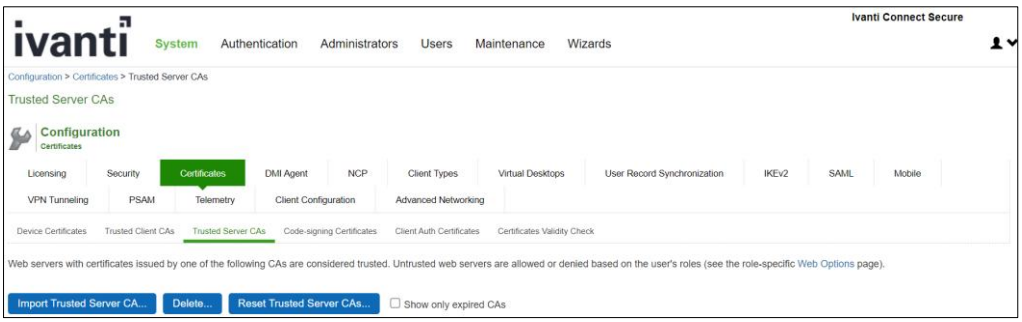


Ilustración 38: Menú de Configuración de Certificado CA de Servidor de Confianza

3. En la pantalla «Importar CA de servidor de confianza», haga clic en «Examinar» para seleccionar el archivo del certificado de la CA y, a continuación, haga clic en «Importar certificado».

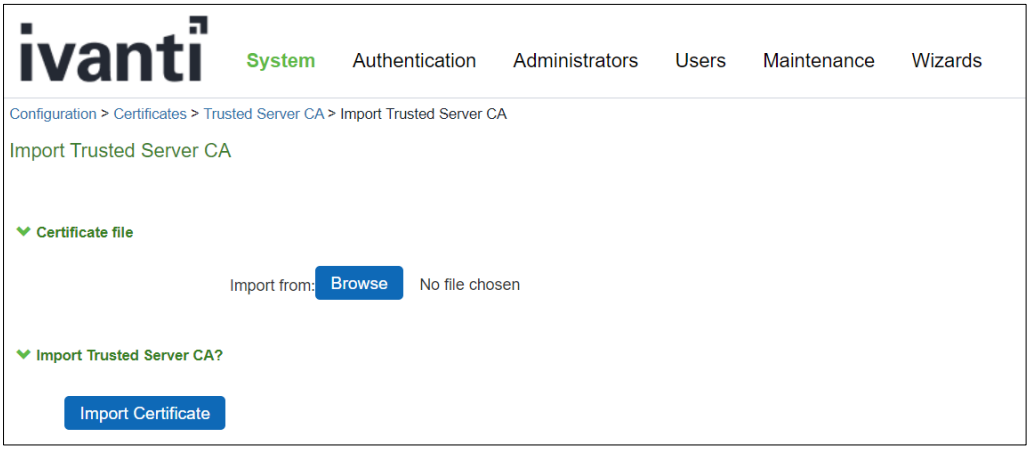


Ilustración 39: Menú de Importación de Certificado CA de Cliente de Confianza

El certificado de la CA importado se añadirá entonces a la lista de certificados de CA de servidor de confianza.

El producto no proporciona un mecanismo explícito para designar manualmente un certificado como ancla de confianza.

Tanto el certificado de la CA raíz como el de la CA intermedia (ICA) asociada deben cargarse en el almacén de confianza y, una vez que estén presentes, la cadena de certificados combinada se considera el punto de confianza.

Nota: Para garantizar la correcta validación de los certificados durante el protocolo de enlace TLS, es necesario importar los certificados de CA tanto en el almacén de CAs de cliente de confianza como en el de CAs de servidor de confianza del producto.

6.6.3 INSTALACIÓN DE UN CERTIFICADO DE AUTENTICACIÓN DE CLIENTE

El producto requiere que su certificado de autenticación de cliente esté configurado para la autenticación mutua cuando actúa como cliente TLS y se comunica con un servidor Syslog.

Sigue las instrucciones que se indican a continuación para importar un certificado de autenticación de cliente al producto.

El certificado de autenticación de cliente se puede instalar de dos formas:

- Importando el certificado y la clave privada para la autenticación de cliente.
- Generando una solicitud de certificado (CSR) para el certificado de autenticación de cliente.

6.6.4 IMPORTACIÓN DEL CERTIFICADO Y LA CLAVE PRIVADA PARA LA AUTENTICACIÓN DE CLIENTE

Para importar un certificado de cliente y una clave privada:

1. Seleccione Sistema > Configuración > Certificados > Certificados de autenticación de cliente.
2. Haga clic en Importar certificado y clave… para mostrar la página de configuración.

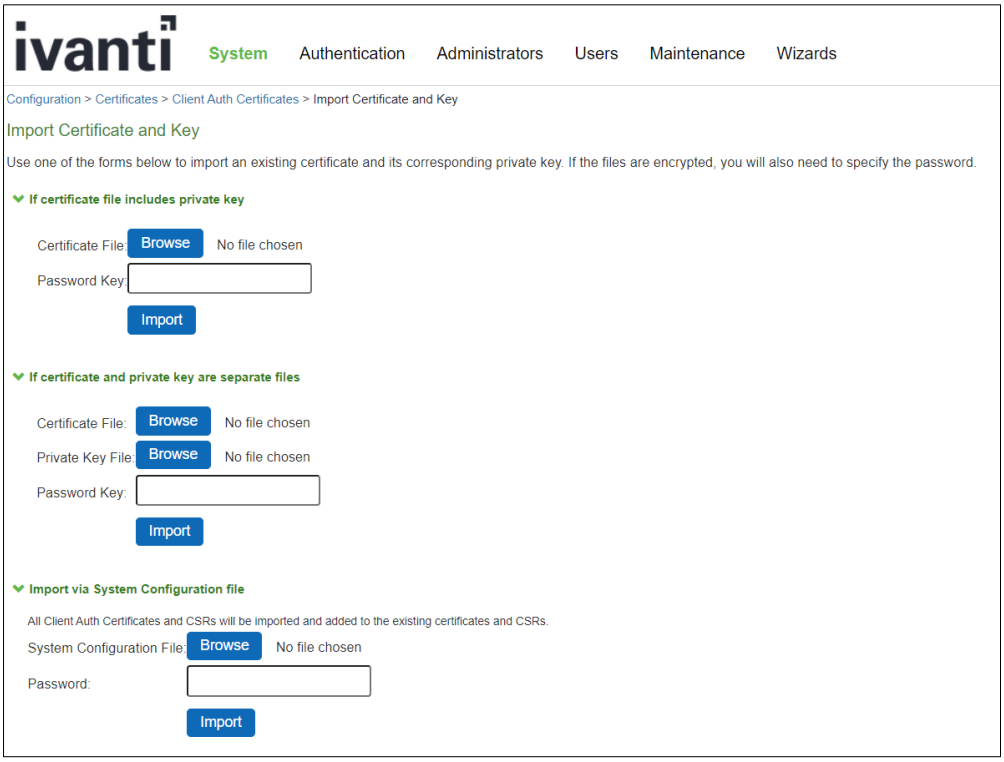


Ilustración 40: Menú de Configuración de Importación del Certificado y la Clave Privada para la Autenticación De Cliente

3. Una de las siguientes opciones para completar el procedimiento de importación:
   - Si el archivo del certificado incluye la clave privada: cuando el certificado y la clave se encuentran en un mismo archivo.
   - Si el certificado y la clave privada son archivos independientes: cuando el certificado y la clave se encuentran en archivos distintos.
   - Importar mediante un archivo de configuración del sistema: cuando el certificado y la clave se encuentran en un archivo de configuración del sistema.

En la sección correspondiente, busque los archivos del certificado y de la clave. Si el archivo está protegido con contraseña, introduzca la contraseña.

4. Haga clic en «Importar».

6.6.5 GENERACIÓN DE UNA CSR PARA UN CERTIFICADO DE AUTENTICACIÓN DE CLIENTE

Para crear una solicitud de firma de certificado:

1. Seleccione Sistema > Configuración > Certificados > Certificados de autenticación de cliente.
2. Haga clic en Nueva CSR… para mostrar la página de configuración.
3. Rellena los datos necesarios:
   Nombre común: Se debe especificar el nombre de dominio completo (FQDN) o la dirección IP. Debe coincidir exactamente (p. ej.: secure.ivanti.com o 192.168.1.10).
   Nombre de la organización: El nombre legal exacto de la organización. No abrevies el nombre de la organización. P. ej.: acumensecurity.pvt.ltd
   Nombre de la unidad organizativa: Se puede dejar en blanco si no es aplicable al administrador de seguridad. P. ej.: CC
   Localidad: La ciudad en la que la organización tiene su sede legal. Por ejemplo: Rockville
   Estado: El estado en el que la organización tiene su sede legal. No debe abreviarse. Por ejemplo: Maryland
   País: La abreviatura ISO de dos letras del país. Por ejemplo: US
   Dirección de correo electrónico: La dirección de correo electrónico utilizada para ponerse en contacto con la organización. Por ejemplo: test@ivanti.com
   Tipo de clave: Tipo de par de claves pública/privada.
   Para generar un certificado de autenticación de cliente RSA, seleccione la opción RSA y, a continuación, elija 2048 bits, 3072 bits o 4096 bits como longitud de la clave. Opcionalmente, se pueden introducir 20 caracteres de datos aleatorios para generar el par de claves, lo que básicamente aumenta el valor de entropía del certificado.
   Para generar un certificado de autenticación de cliente ECC, seleccione la opción «ECC» y, a continuación, elija P-256, P-384 o P-521 como curva ECC.

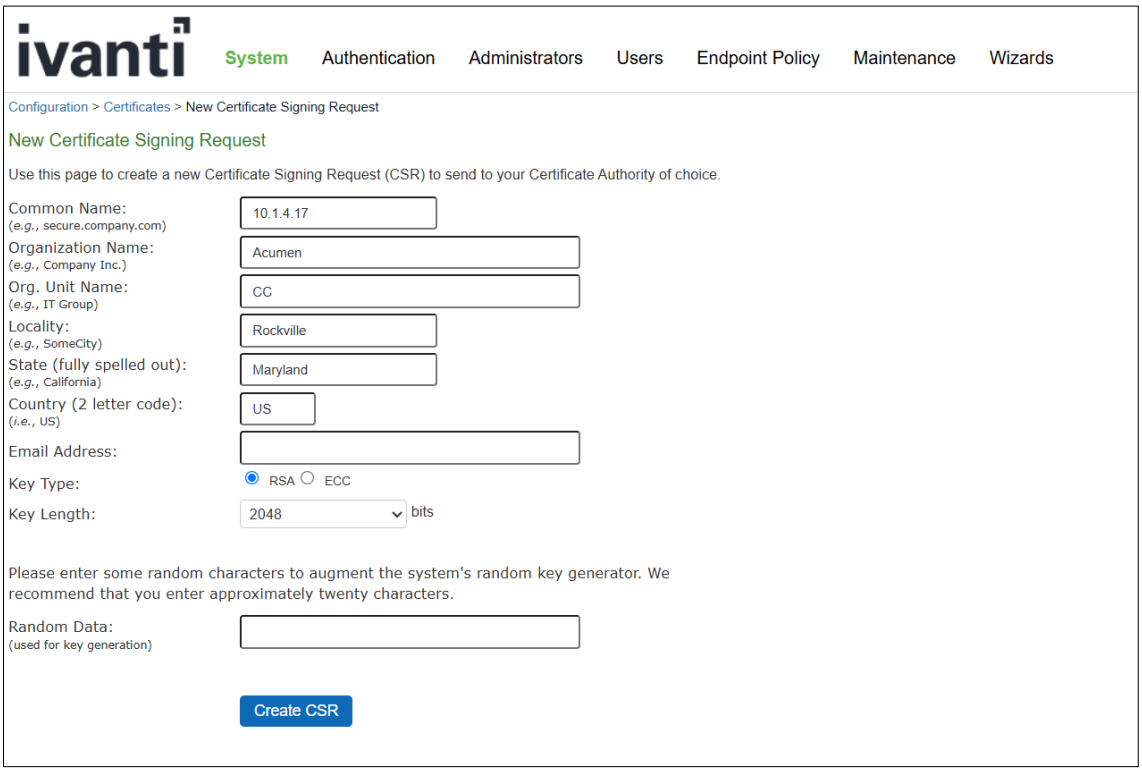


Ilustración 41: Menú de Generación de una CSR para un Certificado de Autenticación de Cliente

Nota: Los campos «Nombre común», «Organización», «Unidad organizativa» y «País» del sujeto son obligatorios y deben rellenarse.

4. Una vez completada la información requerida, haga clic en «Crear CSR».
5. Sigue las instrucciones que aparecen en pantalla, en las que se explica qué información debes enviar a la CA y cómo hacerlo.

Para importar un certificado de cliente firmado creado a partir de una CSR:

1. Seleccione Sistema > Configuración > Certificados > Certificados de autenticación de cliente.
2. En «Solicitudes de firma de certificados», haga clic en el enlace «CSR pendiente» que corresponda al certificado firmado.
3. En «Importar certificado firmado», haga clic en «Examinar» y seleccione el archivo de certificado firmado por la CA; a continuación, haga clic en «Importar».

6.6.6 INSTALACIÓN DE UN CERTIFICADO DE DISPOSITIVO

El producto requiere que se configure un certificado de dispositivo para su uso en los intercambios de mano a mano TLS cuando un cliente TLS se conecta al producto. El producto admite tanto certificados de dispositivo RSA como certificados de dispositivo ECC.

Certificado de dispositivo RSA

- Cuando se instala un certificado de dispositivo RSA, se admiten los siguientes conjuntos de cifrado para conexiones TLSv1.2:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384

y se admiten los siguientes conjuntos de cifrado para conexiones TLSv1.3:

  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
- El establecimiento de claves no se puede configurar cuando hay instalado un certificado de dispositivo RSA. El producto puede negociar el establecimiento de claves mediante ECDHE o RSA.

Certificado de dispositivo ECC

- Cuando se instala un certificado de dispositivo ECC, se admiten los siguientes conjuntos de cifrado para conexiones TLSv1.2:
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

y se admiten los siguientes conjuntos de cifrado para conexiones TLSv1.3:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

- Cuando se instala un certificado de dispositivo ECC, solo se utiliza el establecimiento de claves ECDHE.

El certificado de dispositivo se puede instalar de dos formas:

- Importando el certificado y la clave privada del certificado de dispositivo
- Generando una CSR para el certificado de dispositivo

6.6.7 IMPORTACIÓN DEL CERTIFICADO Y LA CLAVE PRIVADA DEL CERTIFICADO DE DISPOSITIVO

Para importar un certificado de servidor y una clave privada:

1. Seleccione Sistema > Configuración > Certificados > Certificados de dispositivo.
2. Haga clic en Importar certificado y clave… para mostrar la página de configuración.
3. Elige una de las siguientes opciones para completar el procedimiento de importación:
   - Si el archivo de certificado incluye la clave privada: cuando el certificado y la clave se encuentran en un mismo archivo.
   - Si el certificado y la clave privada son archivos separados: cuando el certificado y la clave se encuentran en archivos distintos.
   - Importar mediante un archivo de configuración del sistema: cuando el certificado y la clave se encuentran en un archivo de configuración del sistema.

En la sección correspondiente, busque los archivos del certificado y de la clave. Si el archivo está protegido con contraseña, introduzca la contraseña.

4. Haga clic en Importar.

6.6.8 GENERACIÓN DE UNA CSR PARA UN CERTIFICADO DE DISPOSITIVO

Para crear una solicitud de firma de certificado:

1. Seleccione Sistema > Configuración > Certificados > Certificados de dispositivo.
2. Haga clic en Nueva CSR… para mostrar la página de configuración.
3. Rellena los datos necesarios:
   Nombre común: Se debe especificar el nombre de dominio completo (FQDN) o la dirección IP. Debe coincidir exactamente (p. ej.: secure.ivanti.com o 192.168.1.10).
   Nombre de la organización: El nombre legal exacto de la organización. No abrevies el nombre de la organización. P. ej.: acumensecurity.pvt.ltd
   Nombre de la unidad organizativa: Se puede dejar en blanco si no es aplicable al administrador de seguridad. P. ej.: CC
   Localidad: La ciudad en la que la organización tiene su sede legal. Por ejemplo: Rockville
   Estado: El estado en el que la organización tiene su sede legal. No debe abreviarse. Por ejemplo: Maryland

País: La abreviatura ISO de dos letras del país. Por ejemplo: US
Dirección de correo electrónico: La dirección de correo electrónico utilizada para ponerse en contacto con la organización. Por ejemplo: test@ivanti.com
Tipo de clave: Tipo de par de claves pública/privada.

Para generar un certificado de dispositivo RSA, seleccione la opción RSA y, a continuación, elige 2048 bits, 3072 bits o 4096 bits como longitud de clave. Si lo deseas, puedes introducir 20 caracteres de datos aleatorios para generar el par de claves, lo que básicamente aumenta el valor de entropía del certificado.
Para generar un certificado de dispositivo ECC, seleccione la opción «ECC» y, a continuación, elija P-256, P-384 o P-521 como curva ECC.

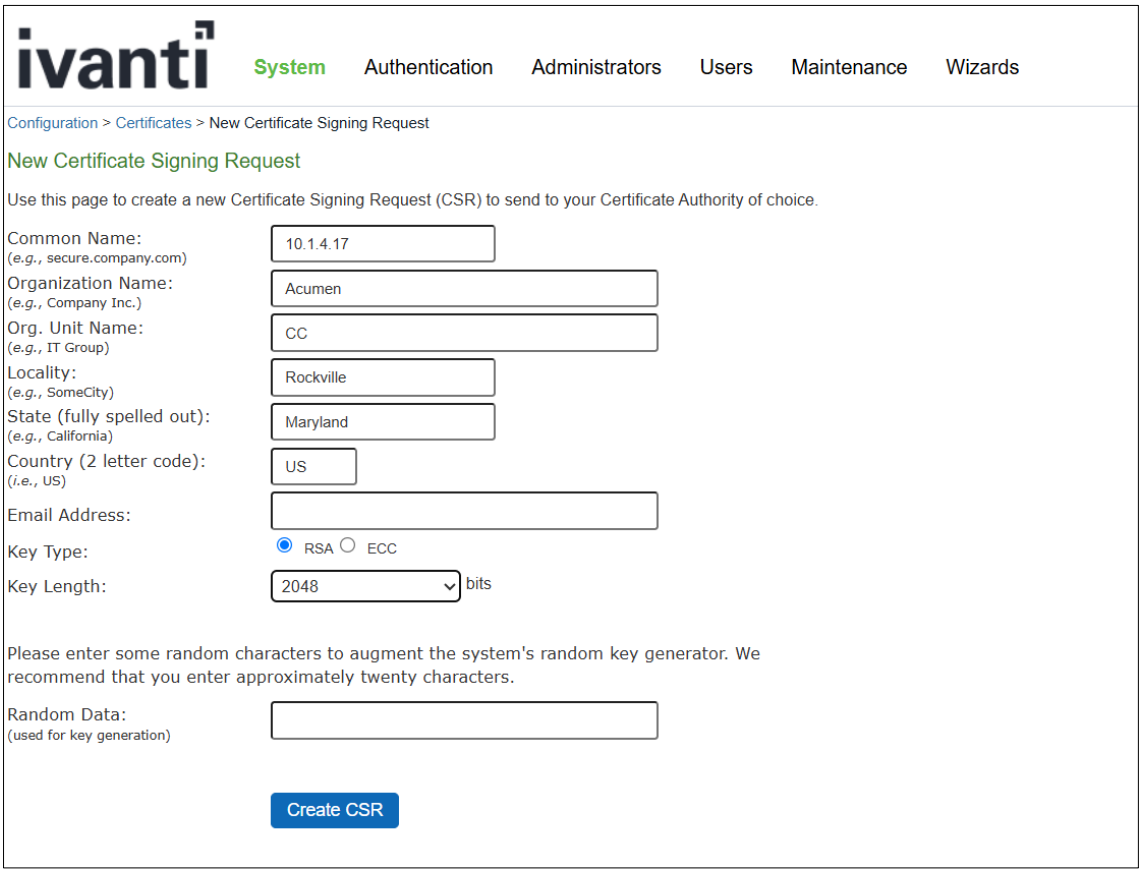


Ilustración 42: Menú de Generación de una CSR para un Certificado de Dispositivo

Nota: Los campos «Nombre común», «Organización», «Unidad organizativa» y «País» del sujeto son obligatorios y deben especificarse.

4. Una vez completada la información requerida, haga clic en «Crear CSR».
5. Sigue las instrucciones que aparecen en pantalla, que explican qué información enviar a la CA y cómo hacerlo.

Para importar un certificado de dispositivo firmado creado a partir de una CSR:

1. Seleccione Sistema > Configuración > Certificados > Certificados de dispositivo.

2. En «Solicitudes de firma de certificados», haga clic en el enlace «CSR pendiente» que corresponda al certificado firmado.
3. En «Importar certificado firmado», haga clic en «Examinar» y seleccione el archivo de certificado firmado por la CA; a continuación, haga clic en «Importar».

Para asociar certificados a puertos virtuales:

1. Seleccione Sistema > Configuración > Certificados > Certificados de dispositivo.
2. Haga clic en un certificado de dispositivo para mostrar su página de configuración.

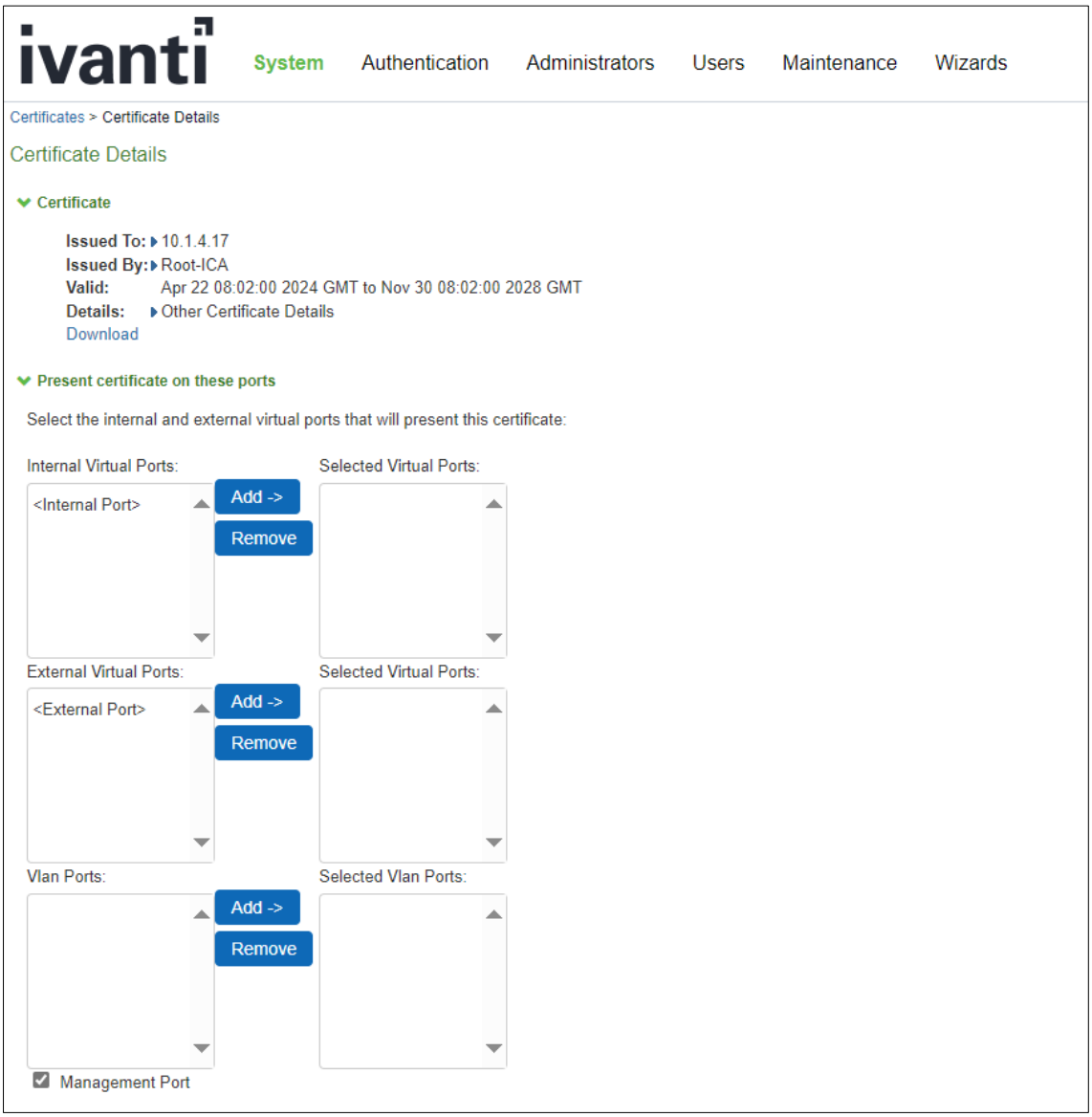


Ilustración 43: Menú de Configuración de los Detalles del Certificado

3. Utiliza los controles de la sección «Mostrar certificado en estos puertos» para asociar puertos al certificado.
4. Seleccione la opción «Puerto de gestión» para asignar el certificado seleccionado a la conexión del servidor HTTPS/TLS a través del puerto de gestión.

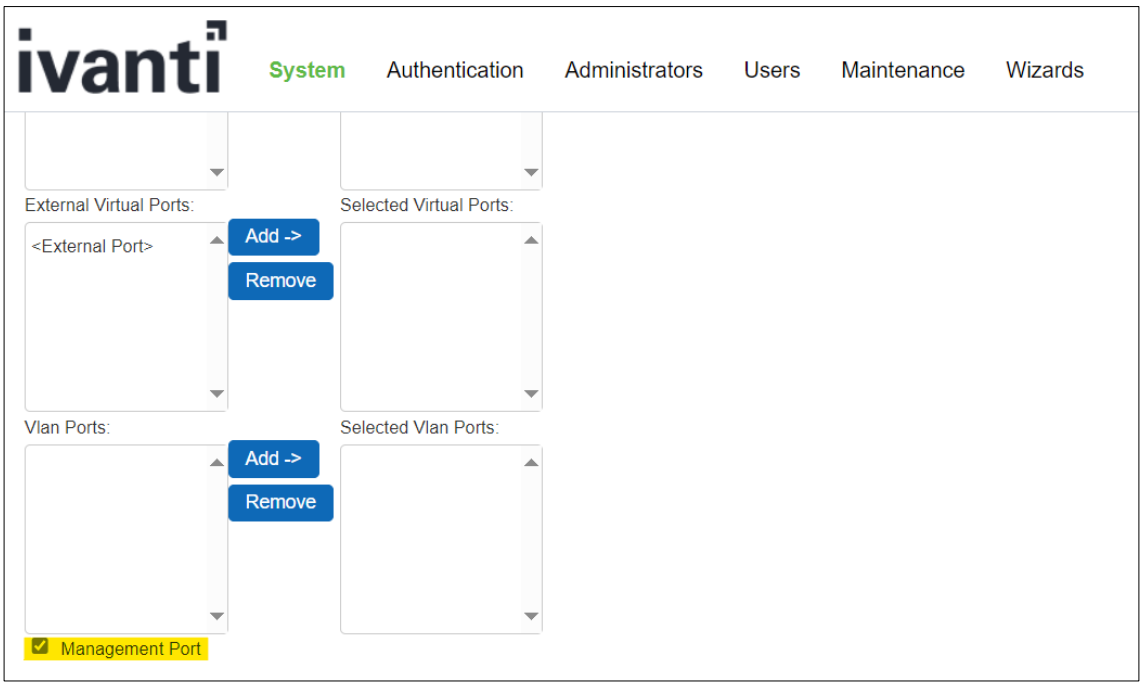


Ilustración 44: Menú de Activación del Puerto de Gestión del Certificado

Un administrador solo puede asignar un certificado de dispositivo al puerto de gestión. Si ya hay un certificado asignado al puerto de gestión, la opción no estará disponible para otros certificados de dispositivo. Para asignar otro certificado al puerto de gestión, el administrador de seguridad debe desmarcar primero la opción «Puerto de gestión» del certificado de dispositivo configurado actualmente.

6.6.9 HABILITACIÓN DE COMPROBACIÓN CRL

1. Acceda a Sistema > Configuración > CA de clientes de confianza.
2. Seleccione el puerto para el tráfico de CRL.

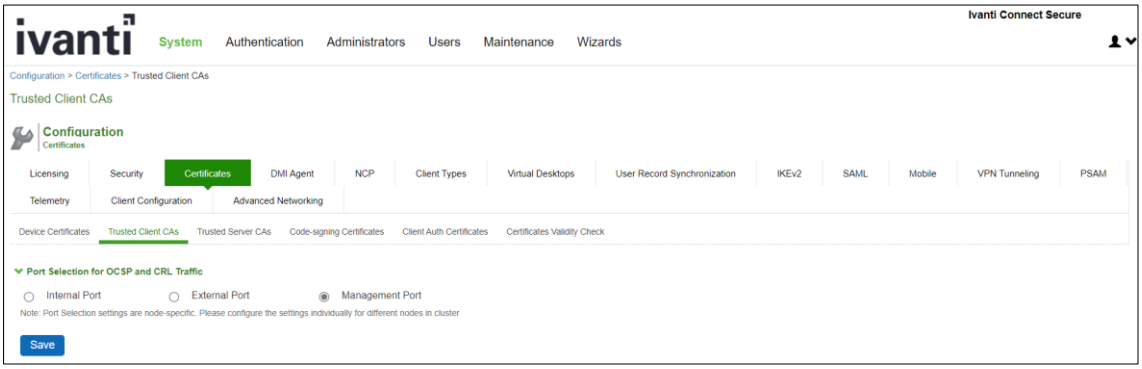


Ilustración 45: Menú de Configuración de Certificados

3. Seleccione el certificado de CA que deseas configurar.
4. En la sección «Comprobación del estado del certificado de cliente», seleccione la opción «Usar CRL (listas de revocación de certificados)».

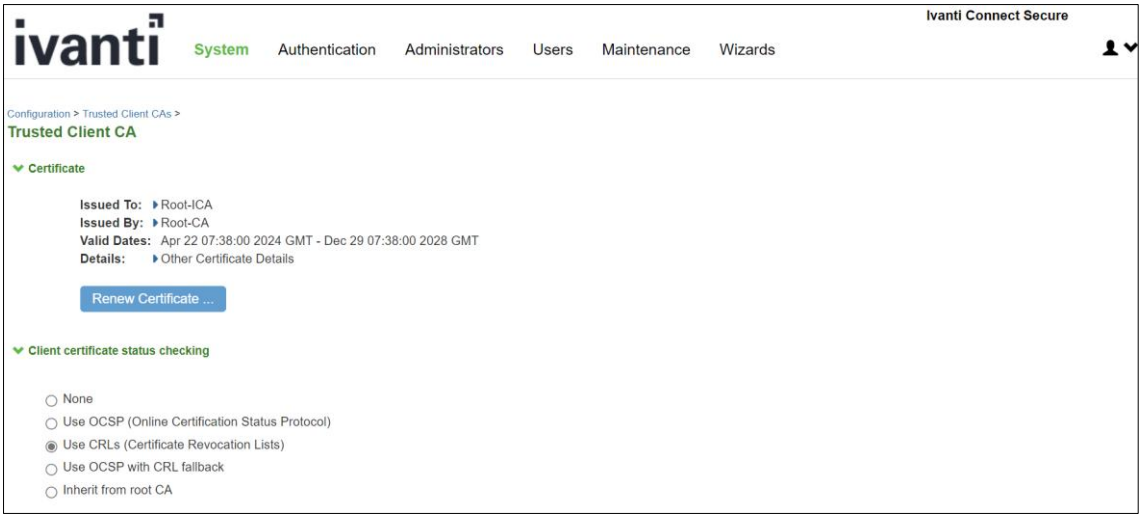


Ilustración 46: Menú de Configuración de CRL

5. Haga clic en «Guardar cambios».

Si el certificado no aparece en la CRL, pero la funcionalidad de seguridad del producto tiene una respuesta almacenada en caché que no ha caducado, la funcionalidad de seguridad del producto utiliza dicha respuesta en lugar de consultar el servidor de la CRL.

Si la funcionalidad de seguridad del producto no puede ponerse en contacto con el servidor de la CRL o si el servidor no responde, la funcionalidad de seguridad del producto registra el error y considera que el certificado es válido.

Para más información sobre los mecanismos de cifra recomendamos, se recomienda consultar la guía CCN-STIC 807 Criptología de Empleo en el ENS [REF4].

6.7 SERVIDORES DE AUTENTICACIÓN

El producto no requiere ni utiliza servidores externos de autenticación para la autenticación administrativa, según la configuración evaluada y certificada. Los administradores se autentican localmente mediante nombre de usuario y contraseña o mediante nombre de usuario combinado con certificado digital X.509 gestionado por el propio producto como se describe en la sección **6.2 AUTENTICACIÓN** de este documento.

6.8 SINCRONIZACIÓN

El producto se basa en los datos de fecha y hora de un reloj local en tiempo real. El administrador de seguridad es responsable de gestionar y actualizar manualmente este reloj de forma periódica, de acuerdo con la política de la organización.

1. Vaya a Sistema > Estado.
2. En la página «Resumen», haga clic en el enlace «Editar» situado junto a «Fecha y hora del sistema».

3. Para configurar la fecha y la hora manualmente, en la página «Fecha y hora»:

   a) Seleccione la opción «Establecer la hora manualmente».

   b) Modifique la fecha y la hora que desea configurar.

   c) Especifique la hora y seleccione AM o PM.

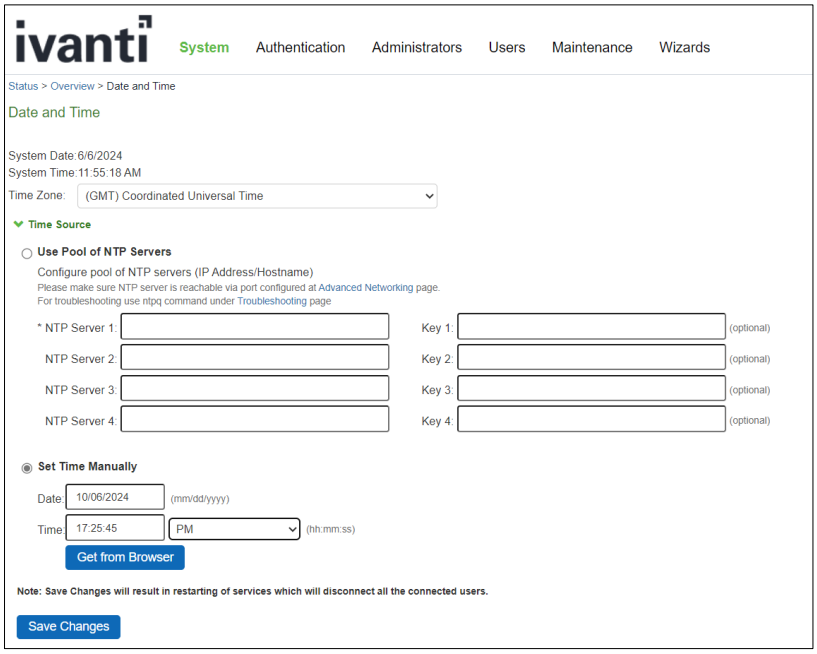


Ilustración 47: Configuración de la Fecha y Hora

   d) Haga clic en el botón «Guardar cambios».

6.9 ACTUALIZACIONES DE SOFTWARE

El Administrador de Seguridad deberá verificar periódicamente la existencia de nuevas actualizaciones de software y la publicación de vulnerabilidades que afecten al producto ICS mediante la consulta de los canales oficiales de Ivanti. Cuando existan actualizaciones de seguridad o vulnerabilidades aplicables, deberá evaluar su impacto y aplicar las medidas correctoras oportunas, incluyendo la instalación de las actualizaciones correspondientes conforme al procedimiento descrito en esta sección.

En este sentido, si hay disponible un nuevo paquete de software compatible, siga las instrucciones de esta sección para actualizar el paquete de software en el producto. La verificación de la autenticidad del paquete de software se realiza mediante la verificación de la firma digital.

a) Descargue el paquete de software del producto recibido de Ivanti en un sistema informático de confianza.

b) En la interfaz gráfica de usuario web del administrador, vaya a Mantenimiento > Sistema.

c) En la pestaña Actualización/Retroceso, dentro de la sección «Instalar paquete del servidor» (desplegada), seleccione la opción «Desde archivo» y, a continuación, haga clic en «Examinar» para seleccionar el paquete del servidor descargado anteriormente.

d) Haga clic en «Instalar» para iniciar el proceso de instalación.

e) Una vez cargado el paquete, el sistema realiza una comprobación de integridad y valida la imagen. A continuación, se completa la instalación.

Nota: La interfaz web no estará disponible mientras el sistema se reinicia. La consola serie local estará disponible para consultar los registros y mensajes. Cuando finalice el reinicio del sistema, la interfaz web estará disponible para su uso.

El producto no admite la funcionalidad de activación diferida para las actualizaciones de confianza. Cuando se instala una actualización de confianza, esta se activa inmediatamente sin la opción de retrasar su activación.

Cuando el administrador de seguridad carga una actualización de software, la funcionalidad de seguridad del producto realiza una verificación de la firma digital RSA 2048 SHA-512 de la actualización utilizando la clave pública de actualización de firmware del producto ICS.

La clave pública se distribuye como parte del paquete de firmware. El producto ICS mantiene el control sobre la clave privada utilizada para firmar las actualizaciones de firmware. Si la comprobación de la firma digital se realiza con éxito, la funcionalidad de seguridad del producto instala la actualización.

Si la comprobación de la firma digital detecta que la actualización o la firma han sido manipuladas, la funcionalidad de seguridad del producto muestra un mensaje de error al usuario y descarta la actualización.

6.10 AUTO-CHEQUEOS

Las autocomprobaciones de integridad del sistema, tanto de hardware como de software, se ejecutan automáticamente al arrancar el sistema. No se requiere ninguna intervención por parte del usuario administrador.

La funcionalidad de seguridad del producto realiza las siguientes autocomprobaciones de hardware al encenderse:

- Comprobación de la integridad de los archivos al encenderse
  - Verificación de la firma digital SHA-512 del archivo de manifiesto.
  - Comprobación de integridad SHA-256 de cada archivo ejecutable de la funcionalidad de seguridad del producto utilizando los hash pre-calculados del archivo de manifiesto.

La finalización satisfactoria de la comprobación de integridad de los archivos garantiza que el firmware no ha sido manipulado.

Si falla una comprobación de integridad, el producto genera una entrada de registro con el mensaje «Fallo en la comprobación de integridad» y permite al administrador elegir entre Reiniciar, Reversión o Continuar con el arranque. Si estas opciones no se ejecutan, el administrador debe ponerse en contacto con el servicio de atención al cliente del producto en [REF3].

- Pruebas de la biblioteca criptográfica

- Comprobación de integridad HMAC-SHA-256 de la biblioteca.
- HMAC-SHA-1 KAT.
- HMAC-SHA-256 KAT.
- KAT HMAC-SHA-384.
- KAT de cifrado y descifrado AES 128 ECB.
- KAT de cifrado y descifrado AES 256 GCM.
- KAT de firma y verificación RSA 2048 SHA-256.
- PCT de firma y verificación ECDSA P-224 SHA-512.
- KAT de DRBG AES-CTR-256 (invocando las funciones instantiate, reseed y generate).
- La funcionalidad de seguridad del producto solo comprueba un único conjunto de parámetros para cada algoritmo criptográfico.

La prueba de la biblioteca criptográfica verifica que cada algoritmo criptográfico especificado en el requisito FCS_COP.1 supere una prueba KAT. La prueba KAT demuestra que el algoritmo funciona correctamente ejecutándolo con claves y mensajes codificados de forma fija y comparando el resultado con un valor precalculado, del que se sabe que es correcto. La prueba PCT de ECDSA comprueba que el algoritmo ECDSA funciona correctamente firmando un valor conocido con una clave conocida y verificando que la firma calculada indica que la firma es válida.

Si las pruebas de la biblioteca criptográfica fallan, la funcionalidad de seguridad del producto no se iniciará y se generará una entrada en el registro de errores con el mensaje «No se puede establecer el modo FIPS para el servidor web». Cuando esto ocurra, el administrador deberá apagar el producto y ponerse en contacto con el servicio de atención al cliente del producto en [REF3].

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

El producto genera registros de auditoría para eventos de seguridad relevantes relacionados con autenticación, administración, cambios de configuración, gestión de certificados, actualizaciones de software, establecimiento de sesiones TLS, comunicaciones seguras con servidores Syslog y otras funciones de seguridad del producto. Cada registro incluye, al menos, fecha y hora, identidad del sujeto que origina el evento, tipo de evento y resultado de la operación (éxito o fallo).

Los registros son almacenados localmente y pueden ser enviados en tiempo real a un servidor Syslog externo mediante **Syslog sobre TLS**, garantizando la confidencialidad e integridad de la información registrada.

El producto mantiene localmente tres categorías diferenciadas de registros:

- Events Log (eventos del sistema y seguridad).
- User Access Log (accesos de usuarios tanto administradores como usuarios VPN).
- Admin Access Log (accesos y acciones administrativas).

El acceso a estos registros se realiza a través de las interfaces administrativas del producto, permitiendo su visualización y exportación manual por parte de administradores autorizados.

Asimismo, cuando se configura un servidor Syslog externo, los registros son reenviados automáticamente mediante canales TLS autenticados.

Los eventos que se registran son:

- Inicio de sesión administrativo.
- Cierre de sesión administrativo.
- Cambios en los datos de la funcionalidad de seguridad del producto relacionados con cambios de configuración.
- Generación de una CSR (Certificate Signing Request) y del par de claves asociado.
- Importación de certificados.
- Eliminación de certificados.
- Restablecimiento de contraseñas.
- Inicio de la función de auditoría.
- Parada de la función de auditoría.
- Espacio de almacenamiento de auditoría bajo o insuficiente.
- Fallo al establecer una sesión HTTPS/TLS.
- Fallo al establecer una sesión TLS.
- Configuración de un nuevo servidor de tiempo.
- Eliminación de un servidor de tiempo configurado.
- Todo uso de los mecanismos de identificación y autenticación (conexiones locales y remotas a la funcionalidad de seguridad del producto).
- Intentos fallidos de validación de certificados.
- Inicio de una actualización de software.
- Resultado de una actualización de software.
- Cambios en la hora del sistema.
- Modificación del comportamiento de la funcionalidad de seguridad del producto.
- Fallo de las pruebas de autocomprobación (self-tests).
- Inicio de un canal confiable (trusted channel).
- Finalización de un canal confiable (trusted channel).
- Inicio de una ruta confiable (trusted path).
- Finalización de una ruta confiable (trusted path).
- Intentos de desbloqueo de una sesión interactiva.
- Terminación de una sesión por el mecanismo de bloqueo de sesión.
- Problemas de confianza ("trust issue") con un certificado, por ejemplo debido a un fallo en la validación de la cadena de certificación.
- Uso de un certificado expirado.
- Ausencia de la extensión basicConstraints.
- Indicador CA no establecido para un certificado presentado como autoridad de certificación.
- Fallo de validación de firma para cualquier certificado de la cadena de certificación.
- Imposibilidad de determinar el estado de revocación de un certificado.
- Detección de un certificado revocado.

Cada registro de auditoría incluye los siguientes campos:

Campo	Descripción
Fecha y hora	Fecha y hora del evento.

Tipo de evento	Tipo de evento registrado (ejemplo: login, iniciación de una actualización software, etc..).
Autor que produce el evento	Identidad del sujeto que origina el evento (nombre de usuario, dirección IP, nombre de host o proceso según corresponda).
Resultado	Resultado de la operación (éxito o fallo).
Información adicional	Información adicional específica del evento cuando aplica (por ejemplo, motivo del fallo, certificado afectado o dirección IP origen).

Tabla 4: Campos de los Registros de Auditoría

6.11.2 ALMACENAMIENTO LOCAL

El producto almacena localmente los registros de auditoría generados por el sistema, permitiendo su consulta por parte de los administradores autorizados. El producto mantiene diferentes categorías de registros, incluyendo eventos del sistema, accesos de usuarios y actividades administrativas, proporcionando información relevante para las tareas de supervisión, auditoría e investigación de incidentes de seguridad.

6.11.2.1 CONFIGURACIÓN DE PARÁMETROS DE AUDITORÍA LOCAL

El producto mantiene tres archivos de registro independientes: «Eventos», «Acceso de usuario» y «Acceso de administrador». De forma predeterminada, la funcionalidad de seguridad del producto asigna 200 MB a cada archivo de registro, pero el administrador puede configurar el tamaño de cada uno de ellos hasta un máximo de 1024 MB para plataformas de hardware y de 200 MB para plataformas virtuales. La funcionalidad de seguridad del producto divide el almacenamiento local de auditoría entre dos archivos de auditoría: activo e inactivo. Durante la configuración inicial, solo existe el archivo de registro activo. Cuando este archivo alcanza su capacidad por primera vez, la funcionalidad de seguridad del producto crea un archivo de registro inactivo, traslada a él los registros de auditoría existentes y continúa escribiendo nuevos registros en un archivo activo actualizado. A partir de ese momento, cada vez que el archivo activo alcance su capacidad, su contenido se transfiere al archivo inactivo, sobrescribiendo su contenido anterior, y el archivo activo se actualiza para almacenar nuevos registros de auditoría. Se genera una entrada de registro de auditoría cada vez que el archivo activo alcanza su capacidad.

Nota: Para verificar que los registros antiguos se están sobrescribiendo con los nuevos, el administrador de seguridad debe realizar una instantánea del sistema (Mantenimiento > Instantánea del sistema) y enviarla al servicio de asistencia de Ivanti para su descifrado. Una vez recibida la instantánea descifrada, el administrador puede confirmar que el archivo de registro inactivo se ha sobrescrito con el contenido del archivo activo, y que este último se ha actualizado para almacenar nuevos registros de auditoría.

La funcionalidad de seguridad del producto protege los datos de auditoría frente a modificaciones y eliminaciones no autorizadas mediante interfaces administrativas restrictivas. Aunque el sistema de archivos no queda directamente expuesto al usuario administrativo a través de la interfaz gráfica de usuario (GUI) HTTPS o la interfaz de línea de comandos (CLI) local, el administrador dispone de opciones específicas dentro de la GUI para borrar los registros de

auditoría o modificar la configuración de auditoría. Estas acciones requieren que el administrador sea identificado y autenticado de forma fehaciente. Los registros se envían al servidor Syslog en tiempo real; es decir, cuando se genera un evento de auditoría, este se envía simultáneamente al servidor externo y se almacena localmente. Esta protección se aplica de forma predeterminada y no requiere ninguna configuración adicional.

6.11.2.2 CONFIGURACIÓN DEL TAMAÑO DEL BÚFER DE REGISTROS

Para configurar el tamaño del búfer del registro de eventos:

- Acceda a Sistema > Registro/Supervisión > Eventos > Configuración.
- Establezca el valor de «Tamaño máximo del registro» entre 512 y 1024 MB para plataformas de hardware, y entre 100 y 200 para plataformas virtuales.

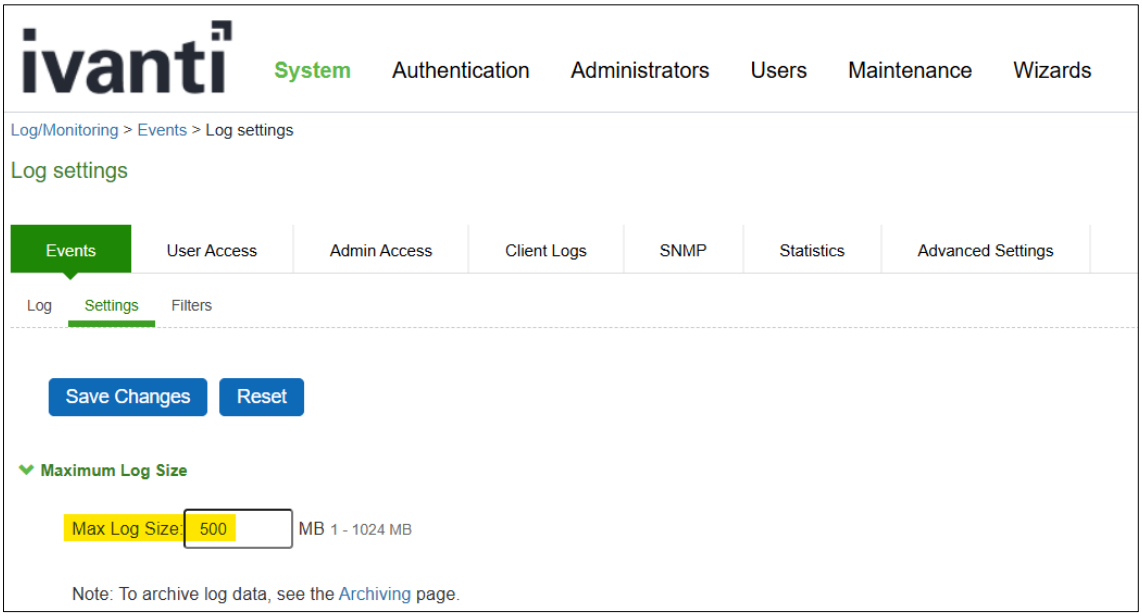


Ilustración 48: Menú de Configuración de Tamaño Máximo de Registros de Auditoría

Para configurar el tamaño del búfer del registro de acceso de usuarios (tanto administradores como usuarios de conexiones VPN),

- Acceda a Sistema > Registro/Supervisión > Acceso de usuario > Configuración.
- Establece el valor de «Tamaño máximo del registro» entre 512 y 1024 MB para plataformas de hardware, y entre 100 y 200 para plataformas virtuales.

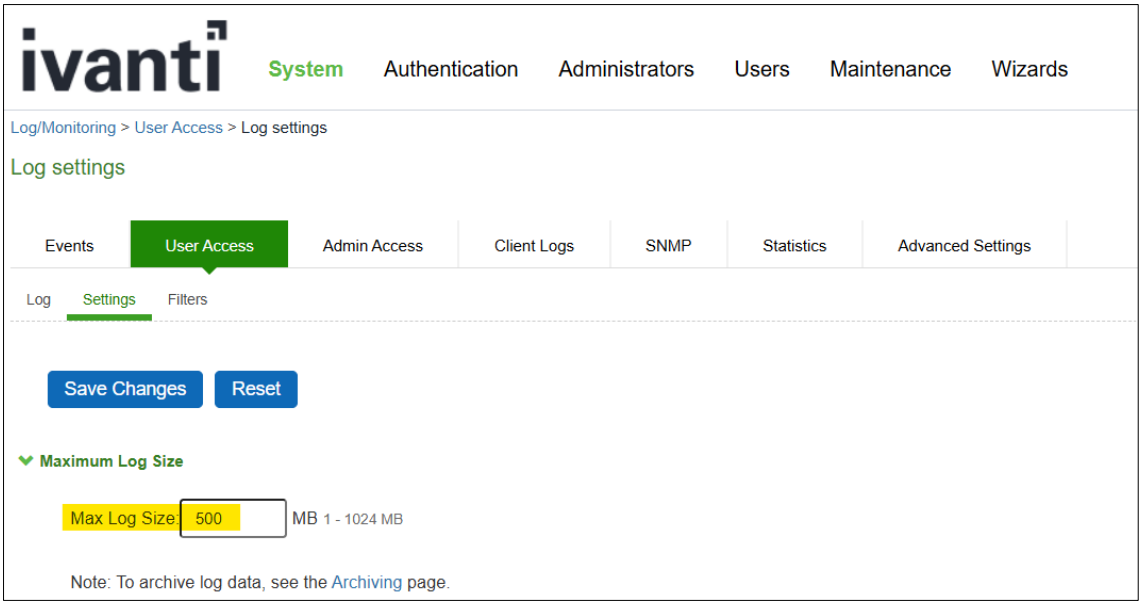


Ilustración 49: Menú de Configuración de Tamaño Máximo de Registros de Auditoría de Acceso de Usuario

Para configurar el tamaño del búfer del registro de acceso de administrador:

- Vaya a Sistema > Registro/Supervisión > Acceso de administrador > Configuración.
- Establezca el valor de «Tamaño máximo del registro» entre 512 y 1024 MB para plataformas de hardware, y entre 100 y 200 para plataformas virtuales.

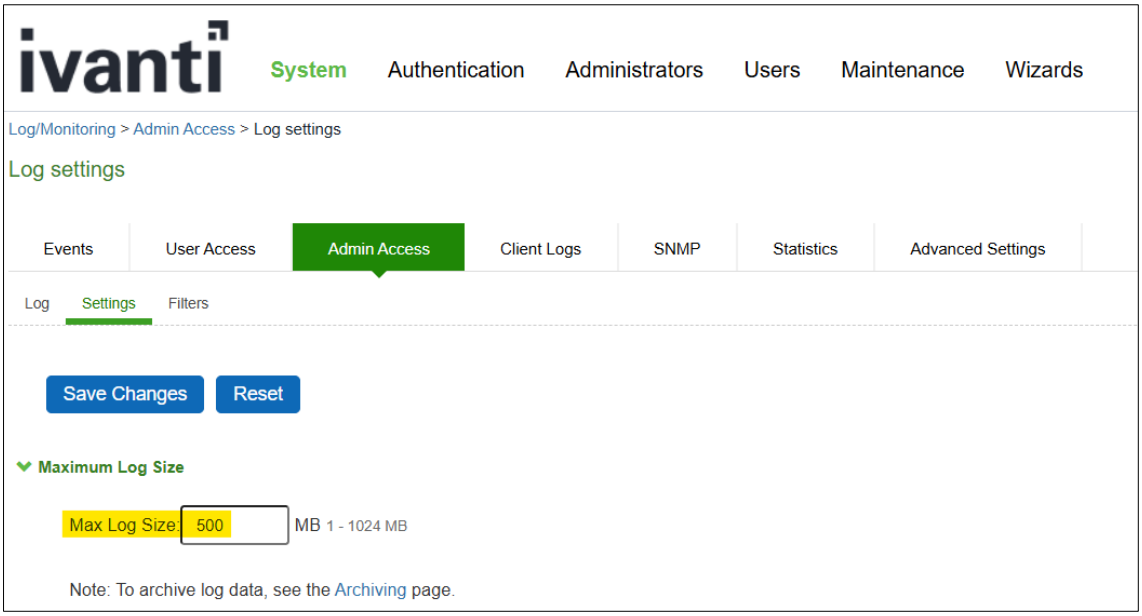


Ilustración 50: Menú de Configuración de Tamaño Máximo de Registros de Auditoría de Acceso de Administrador

6.11.3 ALMACENAMIENTO REMOTO

El producto permite el envío de los registros de auditoría a un servidor Syslog remoto con el objetivo de centralizar el almacenamiento de los eventos de seguridad y facilitar las tareas de monitorización, supervisión e investigación de incidentes.

La monitorización periódica de los registros de auditoría por parte del Administrador de Seguridad constituye una medida esencial para el seguimiento de la actividad de seguridad del producto, permitiendo detectar intentos de acceso no autorizados, errores de operación, cambios de configuración relevantes y otros eventos que puedan afectar al estado de seguridad del entorno.

En la configuración de seguridad, la transmisión de los registros debe realizarse mediante **Syslog sobre TLS**, garantizando la confidencialidad e integridad de la información durante su envío.

Los registros almacenados en el servidor Syslog remoto pueden ser integrados en plataformas SIEM (Security Information and Event Management) para realizar funciones avanzadas de correlación de eventos, generación de alertas y monitorización centralizada de la seguridad.

Para obtener información detallada sobre la configuración del almacenamiento remoto de registros y su integración con infraestructuras de monitorización de seguridad, el administrador debe consultar la documentación oficial del producto [REF1], en particular la guía de administración del producto ICS y la ayuda en línea relativa a la configuración de servidores Syslog remotos. **Nota**: esta funcionalidad está incluida en el producto ICS pero no forma parte de la configuración de seguridad.

6.11.3.1 CONFIGURACIÓN DEL CANAL SEGURO AL SERVIDOR SYSLOG

La configuración de seguridad utiliza TLSv1.2 y TLSv1.3 para proteger las comunicaciones entre el producto y el servidor externo de almacenamiento de auditoría (Syslog). Para configurar un canal seguro desde el producto hasta el servidor Syslog, se requiere la siguiente configuración:

- Es necesario importar las CA de servidores de confianza en el producto para autenticar el servidor Syslog. Consulte la sección **6.6.2 IMPORTAR DE UN CERTIFICADO DE CA DE SERVIDOR DE CONFIANZA** para obtener instrucciones sobre cómo importar la CA de servidor de confianza para la comunicación con el servidor Syslog.
- Es necesario importar un certificado de autenticación de cliente para que el producto se autentique ante el servidor Syslog. Consulte la sección 6.6.3 INSTALACIÓN DE UN CERTIFICADO DE AUTENTICACIÓN DE CLIENTE.
- Se deben importar las CA de cliente de confianza para validar el certificado de autenticación de cliente. Consulte la sección **6.6.1 IMPORTAR UN CERTIFICADO DE CA DE CLIENTE DE CONFIANZA**, para obtener instrucciones sobre cómo importar un certificado de CA de cliente de confianza.

Si la conexión TLS se interrumpe de forma involuntaria, el producto se vuelve a conectar automáticamente utilizando un temporizador que aumenta exponencialmente. El temporizador de reconexión comienza en 15 segundos y se duplica tras cada intento fallido de reconexión hasta alcanzar los 15 minutos. A partir de entonces, el producto intenta continuamente volver a conectarse a intervalos de 15 minutos. Para restablecer la conectividad, los administradores deben verificar y restablecer primero tanto la conectividad física (cables, alimentación de los

dispositivos de red) como la lógica (configuración de IP, enrutamiento, reglas de cortafuegos, servicios de red). Una vez confirmadas estas y resueltos los problemas, el producto volverá a intentar la conexión automáticamente siguiendo el temporizador descrito. Los administradores también pueden reiniciar manualmente el producto o su servicio para acelerar la reconexión tras solucionar los problemas de conectividad subyacentes.

Cuando se utiliza un certificado (para identificar la funcionalidad de seguridad del producto o a una entidad externa a la funcionalidad de seguridad del producto), la funcionalidad de seguridad del producto verifica los certificados comprobando lo siguiente:

1. La fecha actual entre las fechas «Válido desde» y «Válido hasta».
2. Que el certificado no figure en la LCR. Si la funcionalidad de seguridad del producto dispone de una respuesta almacenada en caché que no haya caducado, la funcionalidad de seguridad del producto utiliza dicha respuesta en lugar de consultar el servidor de la CLR.
3. La cadena de certificados es válida si:
    - Cada certificado de la cadena de certificados supera las comprobaciones descritas en los puntos 1 y 2.
    - Cada certificado (excepto el primero) de la cadena de certificados tiene activado el indicador «Subject Type=CA».
    - Cada certificado está firmado por:
        - un certificado de la cadena de certificados, o
        - una CA raíz de confianza que se haya instalado en la funcionalidad de seguridad del producto

La funcionalidad de seguridad del producto verifica la validez de un certificado en las siguientes situaciones:

- Certificado de CA intermedia: cuando se carga un certificado de CA intermedia en el almacén de confianza del producto, la funcionalidad de seguridad del producto verifica su autenticidad y validez, incluido el estado de revocación, antes de aceptarlo en el almacén de anclajes de confianza.
- Verificación del certificado del servidor Syslog: cuando la funcionalidad de seguridad del producto se conecta a un servidor Syslog, verifica el certificado del servidor para confirmar su autenticidad y validez, incluido el estado de revocación, antes de establecer una conexión de confianza.
- Autenticación mediante certificado de cliente: cuando la funcionalidad de seguridad del producto utiliza su certificado de cliente para autenticarse ante el servidor Syslog, verifica que su propio certificado sea válido y haya sido emitido correctamente. Si falta la EKU de autenticación de cliente, la funcionalidad de seguridad del producto rechaza el certificado durante la carga y no permite que se utilice para la autenticación mutua con el servidor Syslog.

Si el administrador de seguridad carga un certificado con un «Subject Type=CA», la funcionalidad de seguridad del producto no valida la ruta del certificado.

Las reglas para los campos «extendedKeyUsage» se siguen en todos los casos; se comprueba la finalidad de «autenticación de servidor» para todos los certificados de servidor presentados.

6.11.3.2 CONFIGURACIÓN DEL SERVIDOR SYSLOG

La funcionalidad de seguridad del producto implementa Syslog sobre TLS utilizando TLS v1.2 o TLS v1.3. La funcionalidad de seguridad del producto admite TLS con autenticación mutua mediante certificados X509v3 para proteger las comunicaciones con el servidor Syslog. Los registros se envían a los servidores Syslog en tiempo real.

El servidor Syslog se puede configurar en el producto para enviar simultáneamente registros de eventos, de acceso de usuario y de acceso de administrador al servidor Syslog. En la configuración de seguridad, todos los registros relevantes para la auditoría deben enviarse a Syslog para evitar su pérdida en caso de que se sobrescriban los registros locales.

Cuando se configura el servidor Syslog, el dispositivo enviará automáticamente los registros al servidor especificado y no existe ninguna opción de configuración explícita para habilitar o deshabilitar la transmisión de registros. Sin embargo, si el servidor Syslog no está configurado, el dispositivo no enviará registros.

Cuando se genera un evento de auditoría, este se transmite simultáneamente tanto al servidor externo como al almacenamiento local.

La configuración del servidor Syslog en el producto admite el uso de un nombre de dominio completo (FQDN) o una dirección IP como identificador de referencia.

La funcionalidad de seguridad del producto establece los identificadores de referencia para el servidor remoto de la siguiente manera:

- Cuando el servidor se especifica mediante un nombre de dominio, según la sección 6 del RFC 6125, la funcionalidad de seguridad del producto comprueba que el nombre de dominio coincida con un campo «Nombre DNS de nombre alternativo del sujeto» del certificado, utilizando la coincidencia exacta o con comodines especificada en la sección 3.1 del RFC 2818, que establece que un certificado con comodines puede contener un único carácter asterisco (*) al principio de una etiqueta de nombre de dominio, y que coincide con cualquier etiqueta de nombre de dominio única. Si el certificado no contiene ningún campo de «Nombre alternativo del sujeto», la funcionalidad de seguridad del producto compara el nombre de dominio con el «Nombre común» del certificado.
- Cuando el servidor se especifica mediante una dirección IP, la funcionalidad de seguridad del producto verifica que la dirección IP coincida exactamente con un campo de «Dirección IP del nombre alternativo del sujeto» del certificado, utilizando las reglas especificadas en la sección 3.1 del RFC 2818. Si el certificado no contiene ningún campo de «Nombre alternativo del sujeto», la funcionalidad de seguridad del producto compara la dirección IP con el «Nombre común» del certificado.
- Cuando el identificador de referencia es una dirección IP, el producto la convierte a una representación binaria en orden de bytes de red. Para las direcciones IPv4, el producto aplica el formato canónico decimal con puntos, tal y como se define en el RFC 3986, antes de la conversión a binario. El producto compara la dirección IP binaria con todas las entradas de «Dirección IP» del «Nombre alternativo del sujeto».

El producto permite el uso de direcciones IP como identificadores de referencia en los certificados. Sin embargo, según [RFC 6125, secciones 1.7 y 6.4.4], se desaconseja el uso de direcciones IP como identificadores en los certificados debido a la falta de flexibilidad y al mayor riesgo de configuración incorrecta o de vulnerabilidades de seguridad.

Se recomienda que los administradores de seguridad utilicen nombres DNS en lugar de direcciones IP como identificadores de referencia en los certificados siempre que sea posible. Si es necesario utilizar direcciones IP, el certificado debe incluir la dirección IP en el campo «Nombre alternativo del sujeto» (SAN) utilizando el tipo «Dirección IP», tal y como se especifica en [RFC 5280, sección 4.2.1.6]. El administrador también debe asegurarse de que las direcciones IP se asignen de forma estática y no cambien, ya que la validación del certificado fallará si el identificador no coincide exactamente con la entrada del SAN.

La funcionalidad de seguridad del producto admite comodines, pero no admite la fijación de certificados y determina si el certificado es válido para el servidor especificado basándose en el nombre DNS o la dirección IP del servidor. Los comodines solo se admiten en la etiqueta situada más a la izquierda del identificador.

La funcionalidad de seguridad del producto limita la capacidad de modificar el comportamiento de las funciones relacionadas con la auditoría a los administradores de seguridad. Para la transmisión de datos de auditoría a una entidad informática externa, los administradores de seguridad pueden configurar la dirección de destino, el protocolo TLS y el puerto de origen para la comunicación con un servidor Syslog externo. El reenvío de auditoría se activa automáticamente cuando existe esta configuración y se desactiva automáticamente cuando se elimina; no existe un control independiente para activar o desactivar explícitamente esta función. En lo que respecta al tratamiento de los datos de auditoría, los administradores de seguridad tienen control sobre las funciones locales de gestión de auditoría, incluida la capacidad de borrar los registros existentes y configurar el tamaño máximo de los registros. Cuando el espacio de almacenamiento local de auditoría se llena, el producto sobrescribe automáticamente los registros de auditoría más antiguos. Este comportamiento de sobreescritura de registros es fijo y no puede ser configurado por el administrador de seguridad.

6.11.3.3 CONFIGURACIÓN DEL SERVIDOR SYSLOG PARA REGISTROS DE EVENTOS

Para configurar los parámetros del servidor Syslog para los registros de eventos,

- Acceda a Sistema > Registros/Supervisión > Eventos > Configuración.

Configura los parámetros según los ajustes evaluados a continuación:

Parámetros	Selección
Max Log Size	200 MB (Range: 512–1024 MB for HW, 100–200 MB for VM)
Select Events to Log	
Connection Requests	Enable
System Status	Enable
System Errors	Enable
Rewrite	Enable
Statistics	Enable
Performance	Enable
License Protocol Events	Disable
Reverse Proxy	Enable

Syslog Servers	**See Section 6.11.3.6 CONFIGURACIÓN DE LOS PARAMETROS DEL SERVIDOR SYSLOG**

Tabla 5: Configuración de los Parámetros del Servicio de Auditoría

6.11.3.4 CONFIGURACIÓN DEL SERVIDOR SYSLOG PARA REGISTROS DE ACCESO DE USUARIO

Para configurar el servidor Syslog para el registro de administración,

- Acceda a Sistema > Registro/Supervisión > Acceso de usuario > Configuración.

Seleccione los siguientes ajustes para las opciones de registro de acceso de administración en la configuración de seguridad:

Parámetros	Selección
Maximun Log Size	
Max Log Size	200 MB (Range: 512–1024 MB for HW, 100–200 MB for VM)
Select Events to Log	
Login/logout	Enable
SAM/Java	Disable
User Settings	Enable
Meeting Events	Disable
Client Certificate	Enable
Active Sync Proxy	Disable
IF-MAP Client User Messages	Disable
Pulse Client Messages	Disable
HTML5 Access	Disable
Web Requests	Enable
File Requests	Enable
Meeting	Disable
Secure Terminal	Enable
VPN Tunneling	Enable
SAML	Disable
Syslog Servers	**See Section 6.11.3.6 CONFIGURACIÓN DE LOS PARAMETROS DEL SERVIDOR SYSLOG**

Tabla 6: Configuración de los Parámetros del Servicio de Auditoría de Acceso de Usuario

6.11.3.5 CONFIGURACIÓN DEL SERVIDOR SYSLOG PARA REGISTROS DE ACCESO DE ADMINISTRADOR

Para configurar el servidor Syslog para el registro de administración,

- Acceda a Sistema > Registro/Supervisión > Acceso de administración > Configuración.

Seleccione los siguientes ajustes para las opciones de registro de acceso de administración en la configuración de seguridad:

Parámetros	Selección
Maximun Log Size	
Max Log Size	200 MB (Range: 512–1024 MB for HW, 100–200 MB for VM)
Select Events to Log	
Administrator changes	Enable
Administrator logins	Enable
License changes	Enable
Syslog Servers	**See Section 6.11.3.6 CONFIGURACIÓN DE LOS PARAMETROS DEL SERVIDOR SYSLOG**

Tabla 7: Configuración de los Parámetros del Servicio de Auditoría de Acceso de Administrador

6.11.3.6 CONFIGURACIÓN DE LOS PARAMETROS DEL SERVIDOR SYSLOG

En la sección desplegable «Servidores Syslog», introduzca la información tal y como se indica en la tabla siguiente:

Parámetros	Selección
Server name/IP	Fully qualified domain name or IP address for the syslog server. This should match with the CN or SAN of the TLS Syslog server certificate.
Facility	Syslog server facility level (LOCAL0 - LOCAL7). Choose the option that is appropriate based on the administrator's Syslog configuration.
Type	TLS
Client Certificate	Select the client auth certificate imported in **6.6.1IMPORTAR UN CERTIFICADO DE CA DE CLIENTE DE CONFIANZA** to authenticate to the syslog server.
Filter	Standard (Default)
Source Interface	Internal

Tabla 8: Configuración de los Parámetros del Servidor Syslog

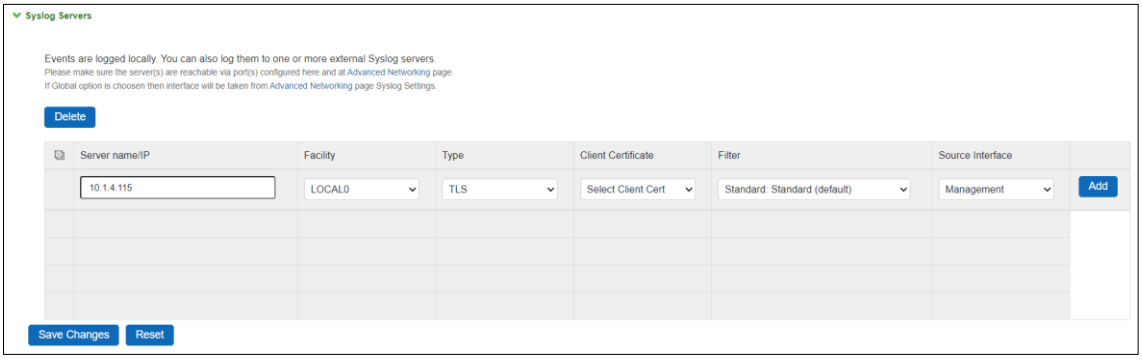


Ilustración 51: Configuración del Servidor Syslog

Haga clic en «Añadir» y, a continuación, en «Guardar cambios».

7 REFERENCIAS

REF1 Ivanti Connect Secure, 22.7.R2.13 Product documentation https://help.ivanti.com/ps/help/en_US/ICS/22.x/22.xICSAG.pdf

REF2 Ivanti Connect Secure, License Management Guide https://help.ivanti.com/ps/help/en_US/ICS/22.x/lmg/ics_gw_licensing.htm

REF3 Servicio de Atención al Cliente https://forums.ivanti.com/s/contactsupport?language=en_US

REF4 CCN-STIC-807 https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

REF5 CPSTIC https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8 ABREVIATURAS

AES	Advanced Encryption Standard
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CLI	Command Line Interface
CN	Common Name
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CTR	Counter Mode
DMI	Desktop Management Interface
DN	Domain Name
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
EC	Elliptic Curve
EC-DH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
EP	Extended Package
GCM	Galois Counter Mode
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ICS	Ivanti Connect Secure
IP	Internet Protocol
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission.
KDF	Key Derivation Function
MAC	Message Authentication Code
MB	Megabyte
ND	Network Device
NDcPP	Network Device Collaborative Protection Profile
NIAP	Nation Information Assurance Partnership
NIST	National Institute of Standards and Technology
NIT	New Item Ticket
OCSP	Online Certificate Status Protocol

OID	Object Identifier
OS	Operating System
OSP	Organizational Security Policies
PIN	Personal Identification Number
pND	Physical Network Device
PP	Protection Profile
PSK	Pre-Shared Key
RAM	Random Access Memory
RFC	Request for Comments
RSA	Rivest, Shamir & Adleman
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SP	Special Publication
SSL	Secure Sockets Layer
SSO	Single Sign-On
ST	Security Target
TD	Technical Decision
TLS	Transport Layer Security
TOE	Target of Evaluation
TSS	TOE Summary Specification
UI	User Interface
VM	Virtual Machine
vND	Virtual Network Device
VS	Virtual System