Guía de Seguridad de las TIC
CCN-STIC 1021

Procedimiento de Empleo Seguro
Switches RUCKUS ICX 10.0.10



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 3
2 OBJETO Y ALCANCE 3
3 ORGANIZACIÓN DEL DOCUMENTO 3
4 FASE PREVIA A LA INSTALACIÓN 4
4.1 ENTREGA SEGURA DEL PRODUCTO 4
4.1.1 DESCARGA SEGURA DE SOFTWARE 5
4.2 ENTORNO DE INSTALACIÓN SEGURO 5
4.3 REGISTRO Y LICENCIAS 5
5 FASE DE INSTALACIÓN 8
6 FASE DE CONFIGURACIÓN 11
6.1 MODO DE OPERACIÓN SEGURO 11
6.2 AUTENTICACIÓN 15
6.3 ADMINISTRACIÓN DEL PRODUCTO 16
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 16
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 17
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 18
6.5 GESTIÓN DE CERTIFICADOS 18
6.6 SERVIDORES DE AUTENTICACIÓN 20
6.7 SINCRONIZACIÓN 20
6.8 ACTUALIZACIONES 21
6.9 AUTO-CHEQUEOS 21
6.10 ALTA DISPONIBILIDAD 22
6.11 AUDITORÍA 23
6.11.1 REGISTRO DE EVENTOS 23
6.11.2 ALMACENAMIENTO LOCAL 24
6.11.3 ALMACENAMIENTO REMOTO 25
6.12 BACKUP 26
7 REFERENCIAS 27
8 ABREVIATURAS 29

TABLAS

Tabla 1: Familias, modelos y versiones cualificados 3
Tabla 2: Credenciales por defecto 8

ILUSTRACIONES

Ilustración 1: Identificación en embalaje externo 4
Ilustración 2: Identificación del equipo 4
Ilustración 3: Descarga del software y de las notas de versión 5
Ilustración 4: Registro y licencias 6
Ilustración 5: Correo con código de activación 7
Ilustración 6: Código de activación 7
Ilustración 7: Arquitectura de alta disponibilidad de nivel 1-2 23

1 INTRODUCCIÓN

La familia RUCKUS ICX de switches de nivel 2 y 3 dispone de una amplia gama de modelos tanto para campus y redes empresariales con arquitectura de acceso, agregación y núcleo, como para Data Center con arquitectura Spine *and Leaf*.

2 OBJETO Y ALCANCE

El producto RUCKUS ICX ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF1].

En la siguiente tabla se muestran las familias y modelos de hardware junto con la versión de software para la que han sido cualificados:

Familia	Modelos cualificados	Versión cualificada
ICX7150	ICX7150-C10ZP, ICX7150-C12P, ICX7150-24, ICX7150-24F, ICX7150-24P, ICX7150-48, ICX7150-48P, ICX7150-48PF, ICX7150-48ZP	10.0.10h
ICX7550	ICX7550-24, ICX7550-48, ICX7550-24P, ICX7550-48P, ICX7550-24ZP, ICX7550-48ZP, ICX7550-24F, ICX7550-48F	10.0.10h
ICX7650	ICX7650-48P, ICX7650-48ZP, ICX7650-48F	10.0.10h
ICX7850	ICX7850-48F, ICX7850-48FS, ICX7850-48C, ICX7850-32Q	10.0.10h
ICX8200	ICX8200-C08PF, ICX8200-C08ZP, ICX8200-24, ICX8200-24P, ICX8200-48, ICX8200-48P, ICX8200-48PF, ICX8200-48PF2, ICX8200-24ZP, ICX8200-48ZP2, ICX8200-24F, ICX8200-48F, ICX8200-24FX	10.0.10h
ICX8100	ICX8100-24, ICX8100-24-X, ICX8100-48, ICX8100-48-X, ICX8100-24P, ICX8100-24P-X, ICX8100-48P, ICX8100-48P-X, ICX8100-48PF, ICX8100-48PF-X, ICX8100-C08PF, ICX8100-C08PF-X, ICX8100-C16P, ICX8100-C16P-X	10.0.10h

Tabla 1: Familias, modelos y versiones cualificados

3 ORGANIZACIÓN DEL DOCUMENTO

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

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

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

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Los switches RUCKUS ICX (hardware) se entregan por correo ordinario mediante uno de nuestros distribuidores autorizados. Para verificar la entrega segura del producto, se deben seguir los siguientes pasos:

- **Embalaje externo**. Se debe comprobar que el paquete contiene la serigrafía y logo de RUCKUS, y que tanto la cinta de embalaje como la caja están intactas sin cortes ni daños que permitan el acceso a su interior. También debe examinarse la etiqueta blanca pegada a la caja con información del modelo de switch (SKU/Model) y el número de serie (Serial #). Ejemplo:



Ilustración 1: Identificación en embalaje externo

  Tanto el modelo como el número de serie deben coincidir con los proporcionados por el distribuidor.

- **Embalaje interno**. Al abrir la caja, el equipo debe encontrarse en el interior de una bolsa de plástico cerrada y perfectamente encajado dentro de los protectores de goma espuma que, a su vez, deben encajar perfectamente con las dimensiones de la caja.

- **Equipo**. Se debe comprobar que el equipo coincide con el esperado y realizar un examen visual completo para asegurarse de que no presenta ningún tipo de daño ni desperfecto. También debe examinarse la etiqueta blanca pegada en la parte inferior del mismo con información del modelo y número de serie (SN), los cuales deben coincidir con los de la etiqueta del embalaje externo y con los proporcionados por el distribuidor.



Ilustración 2: Identificación del equipo

- Si alguna de las comprobaciones anteriores no resultase satisfactoria, se recomienda ponerse en contacto con el distribuidor o directamente con el Soporte de RUCKUS.

4.1.1 DESCARGA SEGURA DE SOFTWARE

En el apartado 2 se indica la versión de software cualificada para cada modelo.

Se recomienda consultar la última versión disponible, descargar las notas de versión y revisar los cambios que introduce con respecto a la versión de software cualificada.

El software y sus notas de versión pueden descargarse de forma segura en el Portal de Soporte de RUCKUS [REF2] en los enlaces correspondientes de la página de descarga que aparece cuando se selecciona una versión de software:

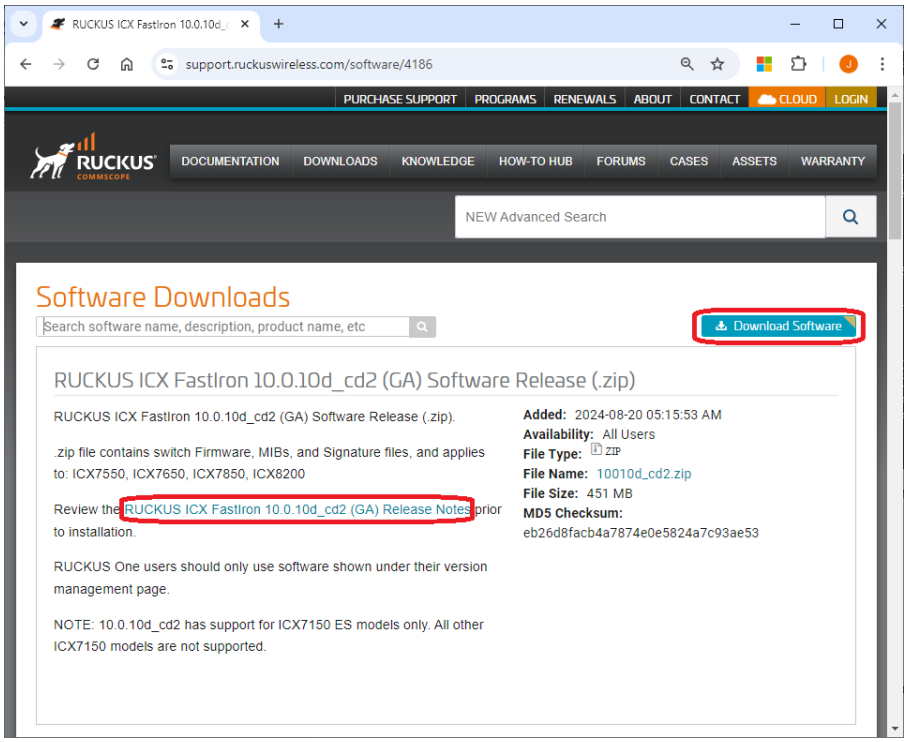


Ilustración 3: Descarga del software y de las notas de versión

El software descargado es un ZIP que contiene varias carpetas, una por familia de switch. Dentro de la carpeta de cada familia se encuentran a su vez varias carpetas, entre ellas:

- Carpeta “Images”: contiene la imagen “XXR10010XXXufi.bin” a cargar en el equipo.
- Carpeta “Signatures”: contiene el archivo de firma “XXR10010XXXufi.sig” que garantiza la integridad de la imagen de software.

4.2 ENTORNO DE INSTALACIÓN SEGURO

La instalación del equipo debe realizarse en un lugar seguro, como un CPD o similar, con acceso restringido al personal autorizado a trabajar en el proyecto y debe estar vigilado constantemente hasta su instalación en su ubicación definitiva.

4.3 REGISTRO Y LICENCIAS

El registro de los switches RUCKUS ICX se realiza en el Portal de Soporte de RUCKUS [REF3].

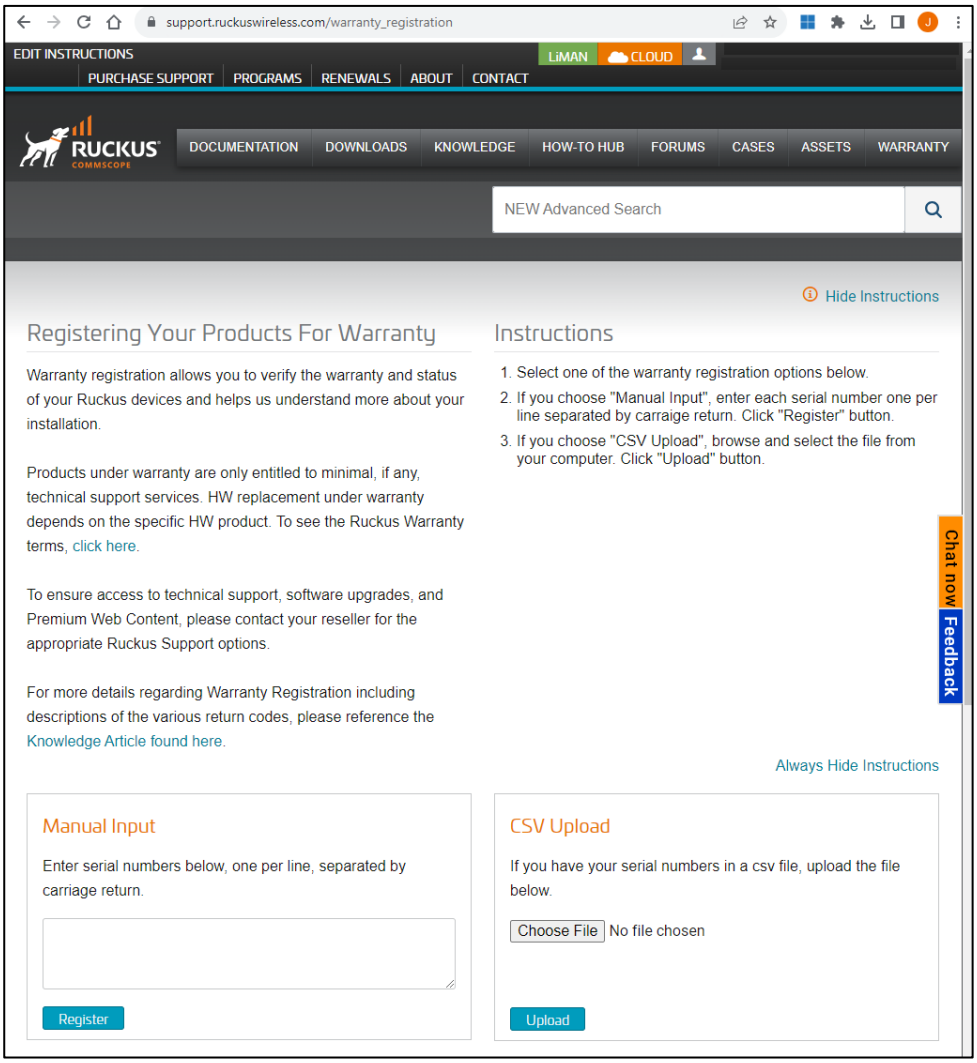
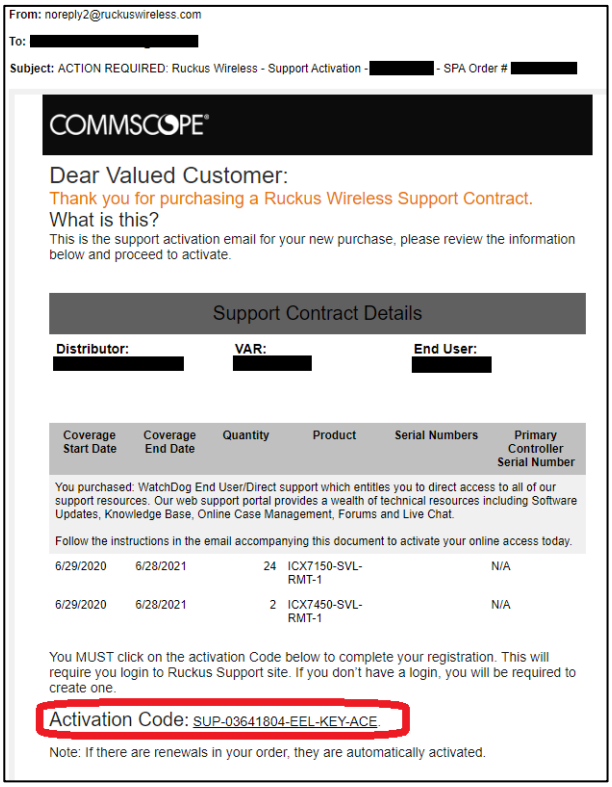


Ilustración 4: Registro y licencias

En caso de haber adquirido Soporte RUCKUS adicional de cualquier tipo, el cliente y/o partner que haya realizado el pedido recibirá por correo electrónico el código de activación del mismo. A continuación un ejemplo:



From: noreply2@ruckuswireless.com

To: [redacted]

Subject: ACTION REQUIRED: Ruckus Wireless - Support Activation - [redacted] - SPA Order # [redacted]

COMMSCOPE®

Dear Valued Customer:

Thank you for purchasing a Ruckus Wireless Support Contract.

What is this?

This is the support activation email for your new purchase, please review the information below and proceed to activate.

Support Contract Details

Distributor: [redacted] VAR: [redacted] End User: [redacted]

Coverage Start Date	Coverage End Date	Quantity	Product	Serial Numbers	Primary Controller Serial Number
You purchased: WatchDog End User/Direct support which entitles you to direct access to all of our support resources. Our web support portal provides a wealth of technical resources including Software Updates, Knowledge Base, Online Case Management, Forums and Live Chat. Follow the instructions in the email accompanying this document to activate your online access today.					
6/29/2020	6/28/2021	24	ICX7150-SVL-RMT-1		N/A
6/29/2020	6/28/2021	2	ICX7450-SVL-RMT-1		N/A

You MUST click on the activation Code below to complete your registration. This will require you login to Ruckus Support site. If you don't have a login, you will be required to create one.

Activation Code: SUP-03641804-EEL-KEY-ACE

Note: If there are renewals in your order, they are automatically activated.

Ilustración 5: Correo con código de activación

El código de activación es un enlace. Para maximizar el nivel de seguridad y garantizar que el correo recibido es legítimo, no se debe pinchar el enlace sino copiar el código de activación y pegarlo en el campo "Code" de la página de activación del Portal de Soporte [REF4]:

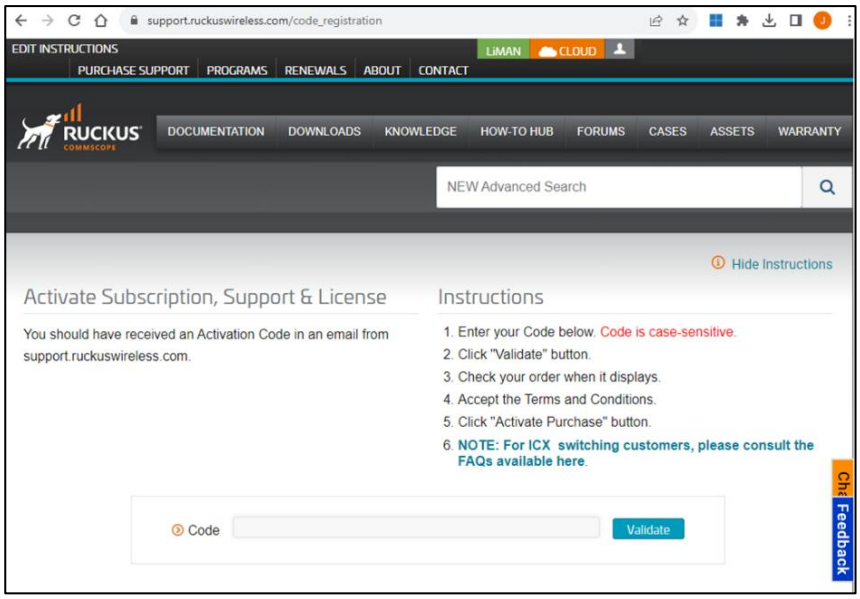


Ilustración 6: Código de activación

El código de activación será aceptado si y sólo si es válido y está asociado al cliente correcto.

En caso de haber adquirido licenciamiento adicional, es necesario seguir las instrucciones indicadas en la guía de licenciamiento [REF5].

5 FASE DE INSTALACIÓN

La instalación física del equipo puede realizarse siguiendo las instrucciones de las guías de instalación disponibles en el Portal de Soporte [REF6].

El acceso al CLI por primera vez debe realizarse **por consola** siguiendo las instrucciones de la guía correspondiente del punto anterior **antes de conectar el equipo a cualquier red operativa** para forzar el cambio de contraseña.

Las credenciales de acceso por defecto son:

Usuario	Super
Contraseña	sp-admin

Tabla 2: Credenciales por defecto

En el primer acceso, el equipo forzará el cambio de contraseña solicitando una nueva antes de proporcionar acceso al CLI.

El CLI tiene tres modos de comando:

- ***User EXEC***: Es el modo por defecto. Se pueden ejecutar comandos básicos de ejecución (no de configuración) como *ping*, *traceroute* y algunos comandos *clear*, *show* y *debug*.

```
Ruckus-ICX login: admin
Password:

ICX8200>
```

- ***Privileged EXEC***: Se pueden ejecutar todos los comandos *clear*, *show*, *debug* y demás comandos de ejecución que no hacen cambios en la configuración. Se puede acceder desde el modo anterior *User EXEC* con el comando *enable*:

```
ICX8200>enable
No password has been assigned yet...
ICX8200#
```

- ***Global Configuration***: Se pueden ejecutar todos los comandos de configuración. Se puede acceder desde el modo anterior *Privileged EXEC* con el comando *configure terminal*:

```
ICX8200#configure terminal
ICX8200(config)#
```

Se puede volver al modo anterior *Privileged EXEC* con el comando *end*:

```
ICX8200(config)#end
ICX8200#
```

Antes de comenzar con la configuración, hay que verificar la versión de software del equipo. Para ello, es necesario acceder al CLI, introducir el siguiente comando y fijarse en los recuadros en rojo:

```
ICX8200>show version
  Copyright (c) Ruckus Networks, Inc. All rights reserved.
    UNIT 1: compiled on Jul 10 2024 at 23:41:01 labeled as RDR10010d_cd2
      (104954212 bytes) from Primary RDR10010d_cd2.bin (UFI)
        SW: Version 10.0.10d_cd2T253
      Compressed Primary Boot Code size = 2097664, Version:10.2.06T255
(rdu1026)
```

```
       Compiled on Thu Jan  1 00:00:00 1970

  HW: Stackable ICX8200-C08ZP-POE
==========================================================================
=====
UNIT 1: SL 1: ICX8200-C08ZP POE 8-port Management Module
      Serial  #:XXXXXXXXXXX
      Software Package: ICX8200_BASE_L3_SOFT_PACKAGE
      Current License: 2X25G
      P-ASIC  0: type 9822, rev 01  Chip 98DX3520
==========================================================================
=====
UNIT 1: SL 2: ICX8200-2x25G 2-port 50G Module
==========================================================================
=====
 1500 MHz ARMv8.2 Cortex-A55 processor 857 MHz bus
    8 MB boot flash memory
    8 GB code flash memory
    4 GB DRAM
STACKID 1  system uptime is 3 minute(s) 47 second(s)
The system started at 23:41:06 GMT+00 Wed Jul 10 2024

The system : started=cold start

ICX8200>
```

Descargar el software siguiendo las instrucciones del apartado 4.1.1.

Extraer del archivo ZIP descargado:

- La imagen de software: es el archivo “XXR10010XXXufi.bin” que se encuentra en la carpeta “Images”.
- El archivo de firma: es el archivo “XXR10010XXXufi.sig” que se encuentra en la carpeta “Signatures”.

La copia del archivo de firma y de la imagen de software en el equipo puede realizarse utilizando un servidor SCP o una memoria USB.

Para realizar la copia mediante SCP, el equipo necesita una dirección IP. Se recomienda configurar por consola una dirección IP estática conocida y válida con los siguientes comandos:

- Para utilizar un puerto en banda:

```
enable
configure terminal
   interface ve <VLAN-de-gestión>
      ip address <ip-address>/<mask-length>
      exit
   ip route 0.0.0.0/0 <default-gateway>
   end
```

- Para utilizar el puerto de gestión fuera de banda:

```
enable
configure terminal
   interface management 1
      ip address <ip-address>/<mask-length>
      exit
   ip route 0.0.0.0/0 <default-gateway>
   end
```

Para copiar el archivo de firma y la imagen de software en el equipo mediante SCP:

```
copy scp flash <server-ip> XXR10010XXXufi.sig fips-ufi-primary-sig
copy scp flash <server-ip> XXR10010XXXufi.bin primary
copy scp flash <server-ip> XXR10010XXXufi.sig fips-ufi-secondary-sig
copy scp flash <server-ip> XXR10010XXXufi.bin secondary
```

Para realizar la copia mediante memoria USB, asegurarse de que la memoria USB es fiable, formatearla antes de utilizarla y realizar la copia con los siguientes comandos:

```
copy disk0 flash XXR10010XXXufi.sig fips-ufi-primary-sig
copy disk0 flash XXR10010XXXufi.bin primary
copy disk0 flash XXR10010XXXufi.sig fips-ufi-secondary-sig
copy disk0 flash XXR10010XXXufi.bin secondary
```

Una vez cargada la imagen de software en las dos particiones (primaria y secundaria) satisfactoriamente, reiniciar el equipo:

```
reload
```

y comprobar de nuevo la versión:

```
show version
```

El uso de TFTP también está soportado pero es inseguro y únicamente debe contemplarse en entornos aislados y temporales donde SCP no sea viable. En tal caso, se recomienda instalar un servidor TFTP en local en el PC donde se han descargado los archivos a transferir y conectar el PC directamente al switch sin ningún otro dispositivo conectado, ni al switch ni al PC. Los comandos para copiar los archivos son:

```
copy tftp flash <server-ip> XXR10010XXXufi.sig fips-ufi-primary-sig
copy tftp flash <server-ip> XXR10010XXXufi.bin primary
copy tftp flash <server-ip> XXR10010XXXufi.sig fips-ufi-secondary-sig
copy tftp flash <server-ip> XXR10010XXXufi.bin secondary
```

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Acceder por consola al CLI del equipo y entrar en el modo *Privileged EXEC*:

```
ICX8200>enable
No password has been assigned yet...
ICX8200#
```

Comprobar que el modo FIPS no está habilitado:

```
fips show
ICX8200#fips show
Cryptographic Module Version: FI-IP-CRYPTO
FIPS mode: Administrative status OFF: Operational status OFF
Common-Criteria: Administrative status OFF: Operational status OFF
SW Version: 10.0.10
FIPS status is not available
ICX8200#
```

Habilitar modo FIPS CC (Common Criteria):

```
configure terminal
  fips enable common-criteria
ICX8200#configure terminal
ICX8200(config)#fips enable common-criteria
CLI-FIPS: Common Criteria is enabled with FIPS status Disabled

FIPS: Disabling HTTP..HTTP already disabled

FIPS: Disabling Telnet..
Error - No active TELNET sessions

FIPS: Disabling Tftp..

FIPS: Deleting SSH Keys..RSA Key pair is successfully deleted
EC key pair is successfully deleted
This device is now running in CC administrative mode.
At this time you can alter this system's CC default security policy
and then enter CC operational mode.

Note: Making changes to the default policy makes the device non-
compliant
with CC and FIPS 140-3 Level 1, design assurance Level 1
The default security policy defined in the FIPS
Security Policy Document ensures that the device complies with all
FIPS 140-3 specifications. Commands to alter the default security policy
are available to the crypto-officer; however, Ruckus Wireless does not
recommend
making changes to the default security policy at any time.
====================================

To enter CC mode, complete the following steps:
1. Optionally, configure FIPS policy commands that meets your network
   requirements. You must explicitly configure the following services
if you
   want to use them when the device is operational in CC mode:
```

```
2. Enter the "fips zeroize all" command, which zeroes out the shared
secrets
    used by various networking protocols, including the host access
passwords,
    SSH and HTTPS host-keys with the digital signature based on the
configured
    FIPS Security Policy. If SSH ReKey Exchange value was not configured
then
    the default value of 30Mins and 500MB will be configured
3. Save the running configuration.
4. Reload the device.
5. Do not press "b" during reload, else FIPS or CC will not be enabled
properly.
6. Enter the "fips show" command to verify that the device entered
    FIPS or CC operational mode.
====================================

The system will disable the following services or commands after reload:
1. Telnet server will be disabled. The "telnet server" command will be
removed.
2. SCP will be enabled. The "ip ssh scp disable" command will be removed.
3. HTTP server will be disabled. The "web-management http" command will
be removed.
Passwords/Keys which dont comply FIPS standards will be removed on
reload.
aaa authentication method must be configured.
Disabling user when invalid password is entered is default in FIPS and
above modes.
Default value of login recovery time is 3 mins/180 secs.
No command sets the login recovery time to 3 mins/180 secs and disables
the user after 3 invalid attempts.
Default values of 3 attempts and 180 secs are not displayed in running
config.
Please see FIPS config guide for complete details.
====================================
Additionally, in CC mode, the system will disable the following
services or commands after reload:
UDP Syslog servers will be deleted from configuration(only in the CC
operational mode).
DSA keys will be deleted from configuration, and will be disabled .
RSA key sizes will be restricted to 2048 and above in the configuration.
Non-TLS TACACS+ servers will be disabled from configuration.
ICX8200(config)#end
ICX8200#
```

Comprobar que el modo FIPS CC ha sido habilitado administrativamente pero no operacionalmente:

```
fips show
ICX8200#fips show
Cryptographic Module Version: FI-IP-CRYPTO
FIPS mode: Administrative status ON: Operational status OFF
Common-Criteria: Administrative status ON: Operational status OFF
SW Version: 10.0.10
------------------------------------------------------------
 Some shared secrets inherited from non-fips mode may
 not be fips compliant and must be zeroized
 The system needs to be reloaded to operationally enter FIPS mode.
------------------------------------------------------------
```

```
System Specific:
OS monitor access status is: Disabled

Management Protocol Specific:
Telnet server: Disabled
Telnet client: Disabled
TFTP client: Disabled
SNMP Access to security objects: Disabled

Critical security Parameter updates across FIPS boundary:
Protocol Shared secret and host passwords: Clear
Password Display: Disabled


Certificate Specific:
HTTPS RSA Host Keys and Signature: Clear
SSH DSA Host keys: Clear
SSH RSA Host keys: Clear
CC Enable AAA Server Any: Clear
ICX8200#
```

Una vez el equipo ha entrado en modo FIPS CC administrativamente, se realiza automáticamente durante el arranque del equipo un chequeo de integridad de software y de la operación de los algoritmos y funciones criptográficas. Si falla, el arranque se aborta y el equipo se reinicia, entrando en un bucle de reinicio que requiere contactar con el soporte de RUCKUS. Para asegurarse de que el chequeo va a ser satisfactorio, conviene realizar el chequeo manualmente y asegurarse de que el resultado es satisfactorio:

```
fips self-tests
ICX8200#fips self-tests
FIPS-CLI: Received msg:
Shutting down all interfaces
FIPS Power On Self Tests and KAT tests successful.
Running continuous DRBG check.
Running continuous DRBG check successful.
Pairwise consistency check successful.
fips crypto drbg health check tests ran successful.
Enabling all interfaces again
FIPS: Image verification passed

FIPS KAT and Conditional Tests successful.
ICX8200#
```

Si no fuera satisfactorio, copiar de nuevo el archivo de firma y/o la imagen de software en el equipo asegurándose de que son los correctos y volver a realizar el chequeo.

Poner a cero las contraseñas y claves:

```
fips zeroize all
ICX8200#fips zeroize all
FIPS-CLI: Zeroizing all certificates
FIPS-CLI: Zeroizing hostkeys

Deleting certificate, please wait...

Trusted Certificate is successfully deleted.
RSA Key pair not found
```

```
RSA client Key pair not found
SSH pub-key file not found
FIPS-CLI: Clearing protocol shared keys
ICX8200#
```

Guardar la configuración y reiniciar:

```
write memory
reload
ICX8200#write memory
write memory is in progress, please wait...

 There is no startup config file, unable to save legacy config

Flash Memory Write (8192 bytes per dot)
.
Write startup-config done.
Copy Done.
ICX8200#reload
Are you sure ? (enter 'y' or 'n'): y
```

Comprobar que tras el reinicio el equipo ha entrado en modo FIPS CC también operacionalmente:

```
fips show
ICX8200#fips show
Cryptographic Module Version: FI-IP-CRYPTO
FIPS mode: Administrative status ON: Operational status ON
Common-Criteria: Administrative status ON: Operational status ON
SW Version: 10.0.10

System Specific:
OS monitor access status is: Disabled

Management Protocol Specific:
Telnet server: Disabled
Telnet client: Disabled
TFTP client: Disabled
SNMP Access to security objects: Disabled

Critical security Parameter updates across FIPS boundary:
Protocol Shared secret and host passwords: Clear
Password Display: Disabled


Certificate Specific:
HTTPS RSA Host Keys and Signature: Clear
SSH DSA Host keys: Clear
SSH RSA Host keys: Clear
CC Enable AAA Server Any: Clear
ICX8200#
```

Se puede configurar una contraseña para pasar del modo *User EXEC* (modo por defecto) al modo *Privileged EXEC* con el comando *enable*. Sin embargo, es una protección obsoleta con un nivel de seguridad muy bajo, se recomienda desactivarla y utilizar en su lugar uno de los sistemas de autenticación indicados en el apartado 6.2.

Para desactivarla:

```
aaa authentication login privilege-mode
```

Al acceder al CLI, una vez finalizado con éxito el proceso de autenticación seguro, se entrará directamente en el modo *Privileged EXEC* sin necesidad de introducir el comando *enable*.

Configurar un usuario administrador según las instrucciones del apartado 6.3.2. Aunque se utilicen otros métodos de autenticación para acceder al equipo, se recomienda tener al menos un usuario local para el acceso en caso de emergencia.

Borrar el usuario por defecto super:

```
no username super
```

Si SNMP no es necesario, se recomienda desactivarlo y verificar:

```
no snmp-server
show snmp
```

Por ejemplo:

```
ICX8200(config)#no snmp-server
ICX8200(config)#show snmp
SNMP is disabled, please enable SNMP to run show snmp commands
ICX8200(config)#
```

Si no se va a utilizar el cliente DHCP, se recomienda desactivarlo:

```
ip dhcp-client disable
```

Si no se va a utilizar el protocolo de descubrimiento LLDP, se recomienda desactivarlo:

```
no lldp enable ports all
```

Configurar interfaces, puertos y servicios según el apartado 0.

En modo FIPS CC, los métodos de intercambio de claves, los algoritmos de encriptación y los algoritmos de clave de dispositivo más débiles no están soportados, todos los soportados están admitidos en la guía CCN-STIC-807. No obstante, hay algunos cuya categoría según la guía CCN-STIC-807 es “Heredado o Legacy (L)”, por lo que se recomienda desactivarlos:

```
no ip ssh key-exchange-method diffie-hellman-group14-sha256
no ip ssh encryption aes128-cbc
no ip ssh encryption aes256-cbc
no ip ssh host-key-method ssh-rsa
no ip ssh host-key-method rsa-sha2-256
no ip ssh host-key-method rsa-sha2-512
no ip ssh message-authentication-code hmac-sha1
```

Configurar sincronización horaria según apartado 0.

Guardar todos los cambios realizados:

```
write memory
```

6.2 AUTENTICACIÓN

La autenticación para acceso a la interfaz de gestión del equipo puede realizarse de las siguientes formas:

- Usuario y contraseña configurados localmente en el equipo. Pueden configurarse hasta 32 usuarios con distintos privilegios de acceso.

- Autenticación de usuario y contraseña contra un servidor de autenticación RADIUS o TACACS+ externo.
- Autenticación basada en clave pública ECDSA y RSA (sólo para el acceso SSH). Se pueden almacenar hasta 16 claves públicas en el equipo. Los clientes que tengan una clave privada que se corresponda con alguna de las claves públicas almacenadas, podrán acceder al equipo.

Autenticación entre el equipo y dispositivos externos:

- Servidor RADIUS:
  - RadSec (RFC 6614): Comunicación sobre túnel TLS 1.2 con autenticación PKI basada en certificado.
- Servidor TACACS+:
  - Comunicación sobre túnel TLS 1.2 con autenticación PKI basada en certificado.
- Servidor SNMP:
  - Autenticación estándar proporcionada por SNMPv3.
- Servidor NTP:
  - Autenticación mediante clave pre-compartida con cifrado MD5 o SHA1.
- Servidor SYSLOG:
  - Comunicación sobre túnel TLS 1.2 con autenticación PKI basada en certificado.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

El acceso a la administración del equipo puede realizarse de las siguientes formas:

- **Acceso local por consola**: Consiste en un acceso local al CLI mediante la conexión directa a un puerto serie de consola, que puede ser:
  - Puerto serie de consola RJ45.
  - Puerto serie de consola USB tipo C.

  Requiere acceso físico al equipo. En el apartado 5 se cubre cómo conectarse por consola al equipo.
- **Acceso remoto**: Consiste en acceder al equipo mediante comunicación IP, la cual puede realizarse de manera remota a través de la red de dos formas:
  - **Conexión en banda**: conexión a una de las direcciones IP configuradas en el equipo y accesibles a través de los puertos de datos. Se recomienda reservar una VLAN para la administración de los equipos.
  - **Conexión fuera de banda**: El equipo dispone de un puerto de gestión fuera de banda, totalmente aislado del resto de puertos. Para utilizarlo, es necesario configurarlo previamente con una dirección IP.

El acceso remoto puede realizarse mediante los siguientes métodos de acceso:

- **SSH**: Está habilitado por defecto y proporciona acceso al CLI a través de un cliente SSH.

El acceso por HTTP, HTTPS y Telnet no están soportados en modo FIPS CC.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

Los roles de usuarios de administración están definidos por el denominado nivel de privilegio, que puede ser uno de los siguientes:

- 0 - Nivel de superusuario (por defecto) - Permite acceso completo de lectura y escritura al sistema. Se usa generalmente para los administradores del sistema y es el único nivel de privilegio que le permite configurar contraseñas.
- 4 - Nivel de configuración de puertos - Permite acceso de lectura y escritura para puertos específicos, pero no para parámetros globales.
- 5 - Nivel de Sólo Lectura - Permite acceso de sólo lectura.

Se recomienda configurar usuarios nominales de manera que cada persona tenga su usuario.

Para configurar un usuario de administración con su nivel de privilegio y su contraseña:

```
username <username> privilege <privilege-level> password <password>
```

La contraseña debe tener una longitud mínima de 12 caracteres. Por ejemplo:

```
ICX8200(config)#username user1 privilege 0 password 5tyHt4$gwQ#T
```

Para activar la caducidad de las contraseñas:

```
enable user password-aging
```

Por defecto, caducan cada 90 días. Cuando una contraseña caduca, se obliga al usuario a introducir una nueva. Para cambiar el tiempo de caducidad de un usuario a un valor entre 1 y 365 días:

```
username <username> expires <days>
```

Por defecto, se guarda un histórico de 5 contraseñas anteriores. Para modificar el número de contraseñas guardadas a un valor entre 1 y 15:

```
enable user password-history <num>
```

Por defecto, una cuenta se bloquea después de 3 intentos fallidos. Para modificar el número máximo de intentos fallidos de autenticación a un valor entre 1 y 10, y el tiempo de espera antes de permitir un nuevo intento a un valor entre 3 y 120 minutos:

```
enable user disable-on-login-failure <intentos> login-recovery-time
{in-hours|in-mins|in-secs} <n>
```

Si no se especifica el *login-recovery-time*, al alcanzar el umbral de intentos fallidos el usuario queda bloqueado de manera indefinida hasta que se desbloquee de manera manual por otro administrador.

Para proteger los usuarios de su modificación o eliminación:

```
service local-user-protection
```

Si está activado, para poder modificar o borrar un usuario se exige introducir la contraseña actual de ese usuario.

Por defecto, el tiempo de inactividad de una sesión es de 2 minutos, transcurridos los cuales se finaliza la sesión automáticamente. Para modificarlo a un valor entre 0 y 240 minutos:

```
cli timeout <min>
```

Si se especifica 0, las sesiones no caducan nunca.

Es recomendable configurar un mensaje de aviso y consentimiento en el inicio de sesión (*login banner*):

```
banner motd <caracter-delimitador> <texto> <caracter-delimitador>
```

El carácter delimitador tiene que ser el mismo al principio y al final y no debe aparecer en el texto. Las tildes no están permitidas en el texto.

Ejemplo típico, usando un asterisco "*" como carácter delimitador:

```
ICX8200(config)#banner motd *
Enter TEXT message, End with the character '*'.
######################################################################
##
##                                                                  ##
##   ACCESO RESTRINGIDO                                             ##
##   Este sistema es confidencial y propiedad de ORGANIZACION.      ##
##   Cualquier acceso no autorizado esta terminantemente prohibido  ##
##   y sera perseguido con todo el rigor de la ley aplicable.       ##
##                                                                  ##
######################################################################
##
*
ICX8200(config)#
```

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Desactivar todos los puertos que no vayan a ser utilizados, tanto los datos como el PoE:

```
interface ethernet 1/1/1
   disable
   no inline power
```

Introducir una etiqueta que identifique el uso para el que está destinado cada interfaz:

```
interface ethernet 1/1/1
   port-name <etiqueta descriptiva>
```

En los puertos de acceso donde se conecten dispositivos finales, se recomienda configurar, donde aplique, funcionalidades de seguridad como *Port MAC Security*, *Dynamic ARP Inspection*, *DHCP Snooping*, *IP Sourceguard* y *STP BPDU guard* o *STP Root guard*. Los detalles de configuración de estas funcionalidades pueden consultarse en las guías [REF7], [REF8] y [REF9].

6.5 GESTIÓN DE CERTIFICADOS

El equipo permite importar el certificado de la CA raíz de confianza que se utilizará para validar los servidores con los que se establezca comunicación TLS:

```
copy scp flash <server-ip-address> <filename> ssl-trust-cert
```

El equipo permite importar el certificado cliente y la clave privada asociada generados por la CA que se utilizarán en las comunicaciones TLS con los servidores:

```
copy scp flash <server-ip-address> <filename> ssl-client-cert
copy scp flash <server-ip-address> <filename> ssl-client-private-key
```

Para cumplir con el nivel de seguridad recomendado en la guía CCN-STIC-807, es necesario que los certificados importados utilicen solamente los siguientes algoritmos y funciones:

- RSA con claves de, al menos, 3072 bits de longitud.
- ECDSA con curvas P-256 o superior.
- DSA con claves de, al menos, 3072 bits de longitud.
- Funciones Hash SHA-256 o superior.

El equipo validará los certificados con los siguientes mecanismos:

- La CA raíz del certificado debe ser de confianza.
- El campo CN/SAN debe coincidir con el configurado en el perfil asociado.
- El certificado debe estar vigente (no caducado).
- Se puede configurar CRL y OCSP para validar la revocación.

Crear un punto de confianza (corresponde a la CA raíz) e introducir la huella que puede copiarse del certificado de la CA raíz:

```
pki trustpoint <trustpointname>
   fingerprint <value>
end
```

Cargar en la base de datos PKI el certificado de CA raíz de confianza, el certificado cliente y la clave privada asociada previamente importados en la memoria *flash*:

```
pki import key {rsa|ec} <keylabel> pem url flash: <keyname>.key.pem
pki import <trustpointname> pem url flash: rootca.pem
pki import <trustpointname> pem url flash: localcert.pem
```

Asociar la clave cargada al punto de confianza:

```
pki trustpoint <trustpointname>
   {rsakeypair|eckeypair} key-label <keylabel>
end
```

Autenticar el punto de confianza:

```
pki authenticate <trustpointname>
```

Configurar validación de revocación por CRL:

```
pki trustpoint <trustpointname>
   crl-query <url-name>
   crl-update-time <hours>
   revocation-check crl
end
```

Configurar validación de revocación por OCSP:

```
pki trustpoint <trustpointname>
   ocsp-url <url-name>
   revocation-check ocsp
end
```

Crear un perfil SSL, asociar el punto de confianza creado y especificar el domino del servidor remoto:

```
ip ssl profile <profilename>
```

```
    trustpoint <trustpointname>
    remotedomain <domain>
end
```

Configurar los servidores RADIUS, TACACS+ o SYSLOG con los que comunicarse mediante TLS utilizando la configuración del perfil SSL creado:

```
radius-server host <ip-address> ssl-auth-port 2083 profile
<profilename>
tacacs-server host <ip-address> ssl-auth-port 2083 profile
<profilename>
logging host <ip-address> ssl-port 6514 profile <profilename>
```

Téngase en cuenta que, aunque en los comandos aparece la nomenclatura SSL heredada del pasado, la comunicación se produce por defecto utilizando TLS 1.2.

Para más información, se puede consultar la sección “Configuring PKI” (pág. 50) de la guía [REF10].

6.6 SERVIDORES DE AUTENTICACIÓN

El equipo soporta autenticación con servidores externos RADIUS o TACACS+.

Los detalles de funcionamiento y configuración de servidores RADIUS externos se encuentran en la sección “RADIUS Authentication” (pág. 43) de la guía [REF7].

Los detalles de funcionamiento y configuración de servidores TACACS+ externos se encuentran en la sección “TACACS+ Server Authentication” (pág. 29) de la guía [REF7].

6.7 SINCRONIZACIÓN

La sincronización horaria puede realizarse mediante el protocolo NTPv4.

Se recomienda activar autenticación NTP. Puede llevarse a cabo mediante clave MD5 o SHA1.

La configuración básica NTP como cliente, incluyendo autenticación, puede realizarse con los siguientes comandos:

```
ntp
   authenticate
   authentication-key key-id <id> {md5|sha1} <key-string>
   server <ip-address> key <id>
```

Comandos útiles para verificar el estado del cliente NTP:

```
show ntp status
show ntp associations [detail]
```

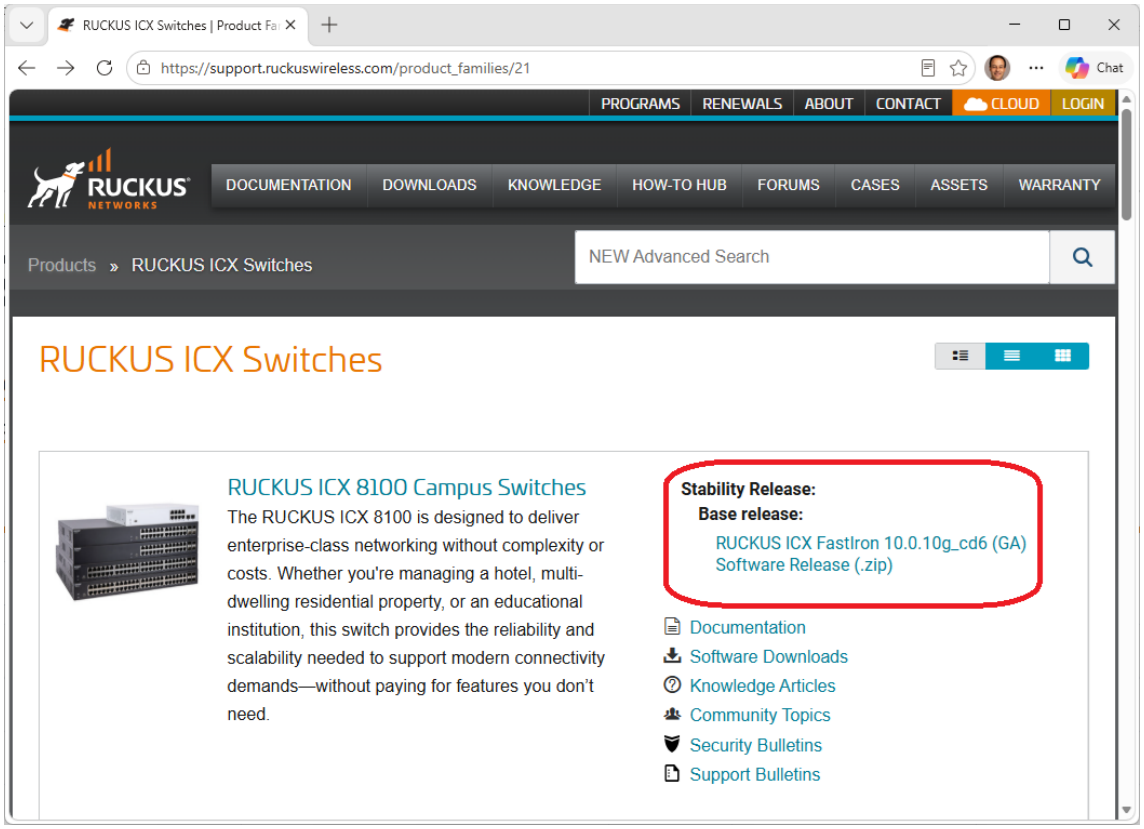
Para verificar la hora del sistema:

```
show clock
```

Los detalles de funcionamiento y configuración del protocolo NTP se encuentran en la sección “Network Time Protocol Version 4 (NTPv4)” (pág. 101) de la guía [REF11].

6.8 ACTUALIZACIONES

Debe revisarse de manera periódica la disponibilidad de nuevas versiones de software que incorporen corrección de vulnerabilidades y actualizaciones. La última versión recomendada puede verse en el Portal de Soporte en la sección de switches ICX [REF2]:



Para actualizar el equipo a una nueva versión, deben seguirse las instrucciones de la sección "Upgrading FIPS-enabled Devices" (pág. 15) de la guía [REF10].

6.9 AUTO-CHEQUEOS

El equipo realiza chequeos automáticos de integridad de software cuando se copia una nueva versión de software en una de las particiones:

```
ICX8200#copy flash flash secondary
Parameter Validation Successful
Image Copy Started

Image Download Done
Image Validation Started
FIPS: Image verification passed and stored in flash
FIPS: Shutting down all interfaces
Image Write Done
FIPS: Enabling all interfaces again
Image Download Complete
ICX8200#
```

En caso de éxito, la nueva versión queda instalada correctamente en la partición destino y será utilizada cuando el equipo arranque desde esa partición.

En caso de fallo, se descarta la operación y la partición destino queda intacta con la versión que tuviera anteriormente.

En modo FIPS CC, el equipo también realiza chequeos automáticos de integridad del software y de la operación de los algoritmos y funciones criptográficas cada vez que arranca:

```
<--- output truncated --->
**************************************************************
FIPS: Firmware Integrity Test: Uboot Checksum Verification: PASS
**************************************************************
104954212 bytes read in 3762 ms (26.6 MiB/s)
**************************************************************
FIPS: Firmware Integrity Test: Image Checksum Verification: PASS
**************************************************************
<--- output truncated --->
**********************************************************************
FIPS: Removing all checksum results
FIPS: Firmware Integrity Test: Package Checksum Verification: PASS
**********************************************************************
<--- output truncated --->
Jul 10 23:42:28:255756:info:fi_debug:debug_logs:1:0: FIPS Power On Self
Tests and KAT tests successful.
Jul    10    23:42:28:255882:info:fi_debug:debug_logs:1:0:    Running
continuous DRBG check.
Jul    10    23:42:28:256089:info:fi_debug:debug_logs:1:0:    Running
continuous DRBG check successful.
Jul    10    23:42:29:687623:info:fi_debug:debug_logs:1:0:    Pairwise
consistency check successful.
Jul 10 23:42:29:690828:info:fi_debug:debug_logs:1:0: fips crypto drbg
health check tests ran successful.
Jul  10  23:42:29:691014:info:fi_debug:debug_logs:1:0:  Crypto  module
initialization and Known Answer Test (KAT) Passed
<--- output truncated --->
```

En caso de éxito, el arranque finaliza con normalidad y el equipo comienza a funcionar según lo esperado.

En caso de fallo, el equipo aborta el arranque y se reinicia, entrando en un bucle en el que el equipo está constantemente reiniciándose, dejándolo inútil. Cuando esto ocurre, se puede abrir un caso de Soporte con RUCKUS para recibir ayuda y recuperar el equipo.

6.10 ALTA DISPONIBILIDAD

Con switches RUCKUS ICX se puede establecer una arquitectura de alta disponibilidad tanto de nivel 1-2 como de nivel 3.

La alta disponibilidad de nivel 1-2 consiste en instalar 2 o más switches conectados entre sí para que los dispositivos finales con varios puertos de red puedan conectarse físicamente a varios switches, de manera que las conexiones se mantengan activas ante la caída de alguno de ellos (o varios siempre que se mantenga activo al menos uno de los enlaces).

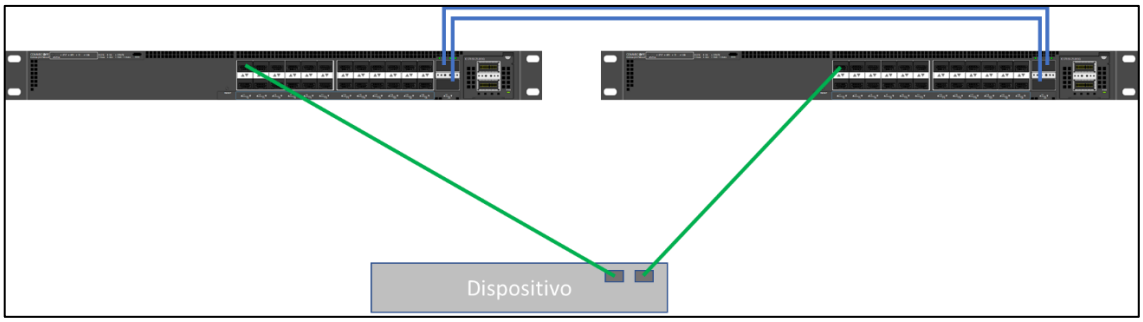


Ilustración 7: Arquitectura de alta disponibilidad de nivel 1-2

El método recomendado para este tipo de alta disponibilidad es mediante agregación de enlace LAG definida en el estándar 802.3ad. Los detalles de funcionamiento y configuración de la agregación de enlace pueden encontrarse en la sección "Link Aggregation Group" (pág. 63) de la guía [REF9].

La unión entre los switches RUCKUS ICX puede realizarse mediante **Multi-Chassis Trunking**: Este método permite la unión de dos nodos. Cada nodo puede ser un switch o, con switches de la familia 7850, una pila de switches. Los nodos mantienen su independencia, pero establecen una comunicación entre ellos que permite configurar agregaciones de enlace LAG entre puertos de los dos nodos. Los detalles de funcionamiento y configuración de *Multi-Chassis Trunking* pueden encontrarse en la sección "Multi-Chassis Trunking" (pág. 89) de la guía [REF9].

La alta disponibilidad de nivel 3 consiste en que el servicio de nivel 3 (*gateway*) de una red pueda proporcionarse por dos o más nodos (switches o pilas) de manera que el servicio se mantenga siempre y cuando al menos uno se mantenga operativo. Se recomienda el uso del protocolo estándar VRRP.

Los detalles de funcionamiento y configuración de VRRP pueden encontrarse en las secciones "VRRPv2" (pág. 375) y "VRRPv3" (pág. 403) de la guía [REF12].

6.11 AUDITORÍA

Es necesario revisar y/o analizar periódicamente los logs generados por el equipo para detectar posibles problemas o situaciones que requieran atención.

6.11.1 REGISTRO DE EVENTOS

Los eventos generados por el sistema (SYSLOG) tienen el formato que se define en el estándar RFC 3164 con los siguientes campos:

- **Recurso (*facility*)**: código de 5 bits que especifica el tipo de sistema que genera el evento. Se utiliza por defecto siempre el código 1 correspondiente al recurso "usuario", pero puede configurarse otro código si se desea:

```
logging facility <facility-name>
```

- **Severidad**: se definen 8 niveles de severidad:
  - Emergencia (0): el sistema está inutilizable.
  - Alerta (1): se debe actuar inmediatamente.
  - Crítico (2): condiciones críticas.

- Error (3): condiciones de error.
- Peligro (4): condiciones de peligro.
- Aviso (5): normal, pero condiciones notables.
- Información (6): mensajes informativos.
- Depuración (7): mensajes de bajo nivel.

- **Fecha y hora**: momento en el que se produce el evento.
- **Nombre de dispositivo**: nombre del dispositivo que genera el evento.
- **Aplicación**: nombre de la aplicación que genera el evento.
- **Mensaje**: Descripción del evento.

Los eventos generados se almacenan localmente y también se envían mediante protocolo SYSLOG a los servidores de SYSLOG que haya configurados.

Para deshabilitar SYSLOG:

```
no logging on
```

Para habilitar SYSLOG de nuevo:

```
logging on
```

Para configurar los niveles de severidad de los eventos se deben deshabilitar los niveles de severidad no deseados:

```
no logging buffered emergencies
no logging buffered alerts
no logging buffered critical
no logging buffered errors
no logging buffered warnings
no logging buffered notifications
no logging buffered informational
no logging buffered debugging
```

Los detalles de funcionamiento y configuración de los eventos generados por el sistema pueden encontrarse en la sección “Syslog” (pág. 109) de la guía [REF13].

La lista de todos los eventos posibles generados por el sistema (excepto los de severidad depuración) se encuentra especificada en la sección “Syslog Messages” (pág. 121) de la guía [REF13].

6.11.2 ALMACENAMIENTO LOCAL

El equipo por defecto almacena los eventos generados por el sistema en la memoria local con capacidad de almacenar hasta 4000 eventos. Si la memoria local llega a su límite, los eventos más antiguos se eliminan para poder almacenar los nuevos.

Cada evento se almacena con el siguiente formato:

```
mmm dd hh:mm:ss:<s>:<app>: <msg>
```

donde:

- “mmm dd hh:mm:ss” representa la fecha y la hora.

- <s> es una letra que indica la severidad:
  - M: Emergencia
  - A: Alerta
  - C: Crítico
  - E: Error
  - W: Peligro
  - N: Aviso
  - I: Información
  - D: Depuración
- <app>: nombre de la aplicación que genera el evento.
- <msg>: Descripción del evento.

Para mostrar los eventos almacenados:

```
show logging
```

Para cambiar el tamaño, en número de eventos, de la memoria local:

```
logging buffered <1-4000>
```

Para habilitar que se genere un evento de aviso cuando la memoria local llegue a un porcentaje determinado de su capacidad:

```
logging buffered threshold <1-100>
```

6.11.3 ALMACENAMIENTO REMOTO

Se pueden configurar hasta 6 servidores a los que el sistema enviará los eventos generados mediante protocolo SYSLOG. El envío de eventos en plano está soportado, pero se recomienda configurar SYSLOG sobre TLS con autenticación PKI siguiendo las instrucciones del apartado 6.5.

Los eventos se envían a los servidores SYSLOG con el formato definido en el estándar RFC 3164:

- **Prioridad**: byte compuesto por los campos recurso (*facility*) (5 bits) y severidad (3 bits).
- **Mensaje**: texto con el siguiente formato:

  ```
  mmm dd hh:mm:ss <hostname> <app>: <msg>
  ```

  donde:
  - “mmm dd hh:mm:ss” representa la fecha y la hora.
  - <hostname>: nombre del dispositivo que genera el evento.
  - <app>: nombre de la aplicación que genera el evento.
  - <msg>: Descripción del evento.

El estándar RFC 5424 define campos adicionales en la cabecera de los mensajes con información más detallada acerca del evento. Para habilitar este formato:

```
logging enable rfc5424
```

6.12 BACKUP

Para realizar copia de seguridad de la configuración del equipo se recomienda el uso del protocolo seguro SCP.

Para copiar la configuración en un servidor SCP externo:

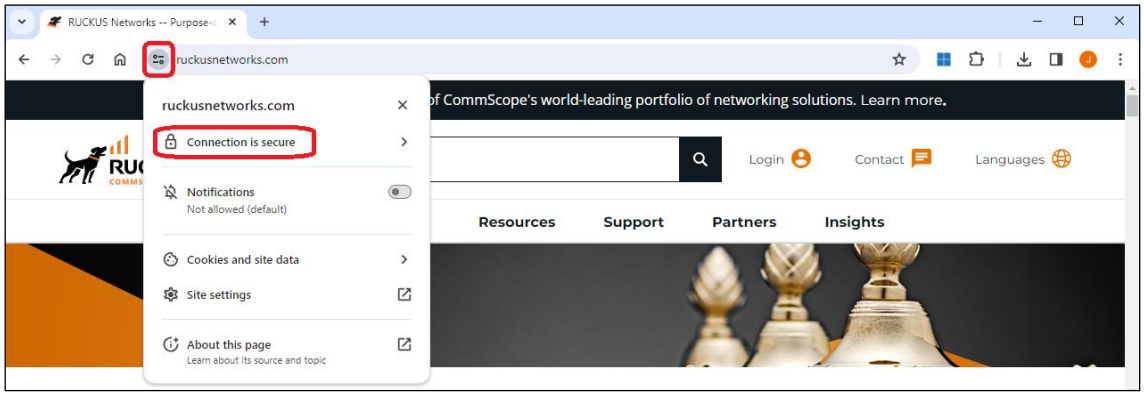
```
copy startup-config scp {<ip-address>|<FQDN>} <filename>
```

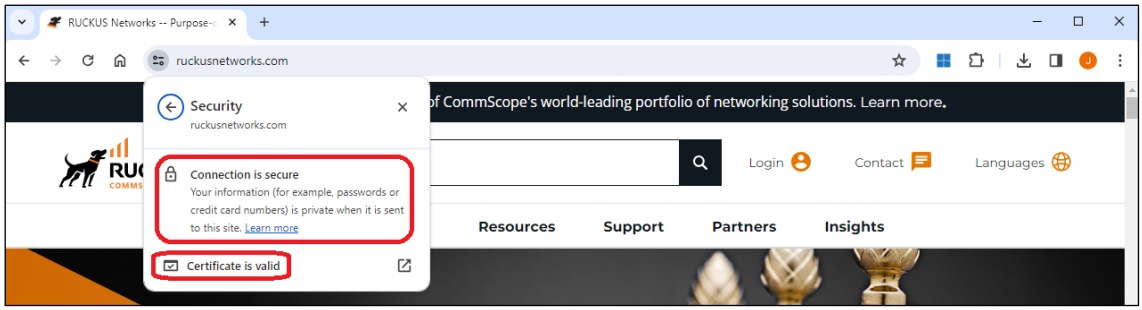
Para restaurar la configuración desde un servidor SCP externo:

```
copy scp startup-config {<ip-address>|<FQDN>} [<port>] <filename>
```

7 REFERENCIAS

Al acceder a las URLs proporcionadas a continuación, es importante asegurarse de comprobar que la URL de la barra del navegador coincide exactamente con la proporcionada y que el certificado del servidor es válido, lo que se puede comprobar en el icono de conexión segura que hay justo a la izquierda de la URL:





REF1	CPSTIC https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic
REF2	Descarga de Software https://support.ruckuswireless.com/product_families/21
REF3	Registro de garantía https://support.ruckuswireless.com/warranty_registration
REF4	Activación de licencias https://support.ruckuswireless.com/code_registration
REF5	*FastIron 10.0.10 (GA) Software Licensing Guide* https://support.ruckuswireless.com/documents/4474

REF6	*RUCKUS ICX 8100 Switch Hardware Installation Guide* https://support.ruckuswireless.com/documents/4995 *RUCKUS ICX 8200 Switch Hardware Installation Guide* https://support.ruckuswireless.com/documents/4379 *RUCKUS ICX 7550 Switch Hardware Installation Guide* https://support.ruckuswireless.com/documents/3484 *RUCKUS ICX 7850 Switch Hardware Installation Guide* https://support.ruckuswireless.com/documents/2678
REF7	*FastIron 10.0.10 (GA) Security Configuration Guide* https://support.ruckuswireless.com/documents/4473
REF8	*FastIron 10.0.10 (GA) DHCP Configuration Guide* https://support.ruckuswireless.com/documents/4462
REF9	*FastIron 10.0.10 (GA) Layer 2 Switching Configuration Guide* https://support.ruckuswireless.com/documents/4465
REF10	*RUCKUS FastIron FIPS and Common Criteria Configuration Guide, 10.0.10* https://www.niap-ccevs.org/api/file/get_public_file/?file_id=30677
REF11	*FastIron 10.0.10 (GA) Management Configuration Guide* https://support.ruckuswireless.com/documents/4467
REF12	*FastIron 10.0.10 (GA) Layer 3 Routing Configuration Guide* https://support.ruckuswireless.com/documents/4466
REF13	*FastIron 10.0.10 (GA) Monitoring Configuration Guide* https://support.ruckuswireless.com/documents/4469

8 ABREVIATURAS

ACK	Acknowledge
ACL	Access Control List
API	Application Programming Interface
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CA	Certification Authority
CC	Common Criteria
CLI	Command Line Interface
CRL	Certificate Revocation List
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
LAG	Link Aggregation
LLDP	Link Layer Discovery Protocol
MAC	Medium Access Control
MD5	Message Digest 5
NBD	Next Business Day
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PC	Personal Computer
PKI	Public key infrastructure
PMS	Port MAC Security
PoE	Power over Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RSA	Rivest, Shamir, Adleman
SCP	Secure Copy Protocol

SDN	Software Defined Network
SHA1	Secure Hash Algorithm 1
SKU	Stock Keeping Unit
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VXLAN	Virtual Extensible Local Area Network