

Firmware FPGA de terminal seguro en Fabric Interconnects UCS 6400

Contenido

[Introducción](#)

[Problema](#)

[Solución](#)

[Sesión SSH](#)

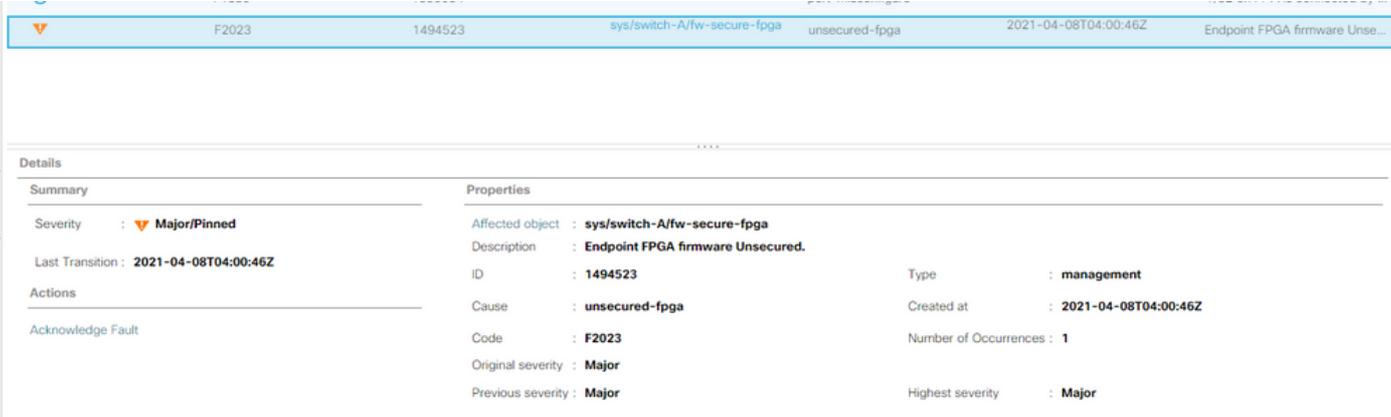
[UCS Manager Web UI](#)

Introducción

Este documento describe cómo habilitar una matriz de puertas programable en campo (FPGA) segura en Fabric Interconnects (FI) 6400.

Problema

En las actualizaciones de Unified Computing System Manager (UCS Manager) a la versión 4.1(3) o posterior en las FI 6400 (cuarta generación), los clientes verán este error principal:



The screenshot shows the UCS Manager Web UI interface. At the top, there is a navigation bar with the following text: F2023, 1494523, sys/switch-A/fw-secure-fpga, unsecured-fpga, 2021-04-08T04:00:46Z, and Endpoint FPGA firmware Unse... Below this, there is a 'Details' section with two columns: 'Summary' and 'Properties'. The 'Summary' column contains: Severity : Major/Pinned, Last Transition : 2021-04-08T04:00:46Z, and an 'Actions' section with 'Acknowledge Fault'. The 'Properties' column contains: Affected object : sys/switch-A/fw-secure-fpga, Description : Endpoint FPGA firmware Unsecured., ID : 1494523, Cause : unsecured-fpga, Code : F2023, Original severity : Major, Previous severity : Major, Type : management, Created at : 2021-04-08T04:00:46Z, Number of Occurrences : 1, and Highest severity : Major.

Description: Endpoint FPGA firmware Unsecured.

Fault Code: F2023

Esta es una nueva función en respuesta a una vulnerabilidad de arranque segura conocida donde las regiones doradas del FPGA podrían tener código insertado o modificado, lo que básicamente impide el arranque seguro.

Solución

Este es un mensaje esperado cuando actualiza a la versión 4.1(3) o posterior en las FI de la serie 6400. Puede ocurrir solamente en una o ambas FI, y depende del código con el que se enviaron originalmente.

No existe ningún riesgo para la producción que no sea la seguridad reducida. Esto se puede

retrasar hasta la siguiente ventana de mantenimiento planificada.

El FPGA puede protegerse y el error puede eliminarse con estos pasos a través de una sesión SSH o en la GUI de UCS Manager.

Nota: Esto requerirá un reinicio de cada FI. Se recomienda hacerlo en una ventana de servicio.

Sesión SSH

1. Abra una sesión SSH en el dominio. La dirección IP del clúster o la dirección IP de FI funcionarán.

```
UCS-A# scope fabric-interconnect a  
UCS-A /fabric-interconnect# activate secure-fpga  
UCS-A/fabric-interconnect*# commit-buffer
```

Nota: La FI se reiniciará después de un breve retraso. No reinicie manualmente la FI.

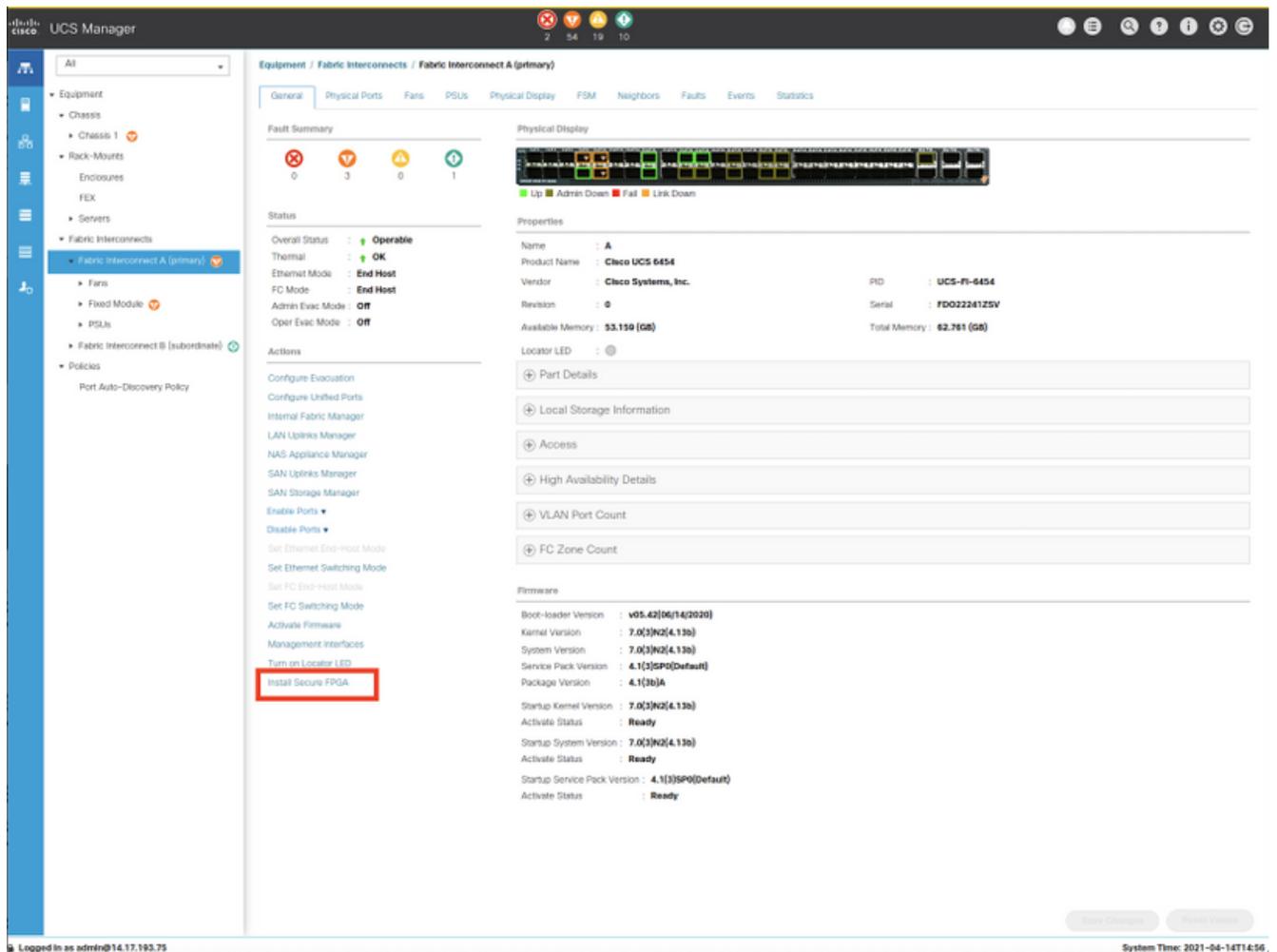
2. Repita este proceso en el FI B.

```
UCS-B# top  
UCS-B# scope fabric-interconnect b  
UCS-B /fabric-interconnect# activate secure-fpga  
UCS-B/fabric-interconnect*# commit-buffer
```

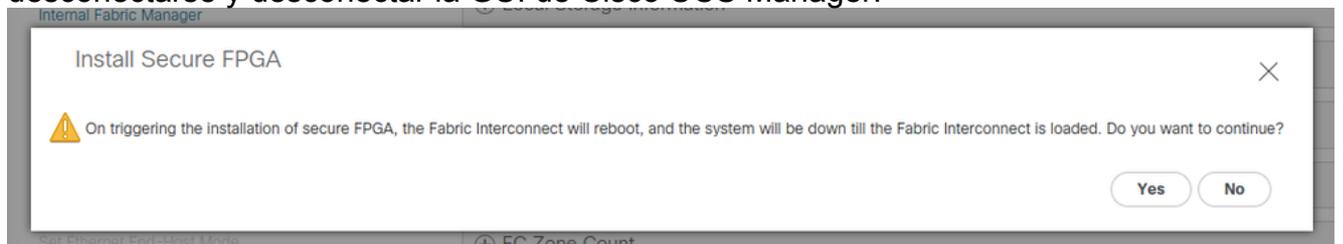
Nota: La FI se reiniciará después de un breve retraso. No reinicie manualmente la FI. El error no seguro del firmware FPGA del punto final debe estar en el estado despejado.

UCS Manager Web UI

1. En el panel de navegación, elija **Equipo > Fabric Interconnects > Fabric_Interconnect_Name**.
2. En el panel Trabajo, haga clic en la ficha **General**.
3. En el área Acciones de la ficha General, haga clic en **Instalar FPGA seguro**.



4. En el cuadro de diálogo, haga clic en **Aceptar**.
5. Haga clic en **Yes** en el mensaje de advertencia de Cisco UCS Manager para reiniciar la FI, desconectarse y desconectar la GUI de Cisco UCS Manager.



Nota: La FI se reiniciará después de un breve retraso. No reinicie manualmente la FI. Si no ve la opción "Instalar FPGA seguro", borre la memoria caché del navegador o utilice una sesión de exploración privada.

Para obtener más información sobre la actualización de Secure FPGA, vea [Release Notes para Cisco UCS Manager, versión 4.1](#).