

Sicherung der FPGA-Firmware für Endgeräte auf UCS 6400 Fabric Interconnects

Inhalt

[Problem:](#)

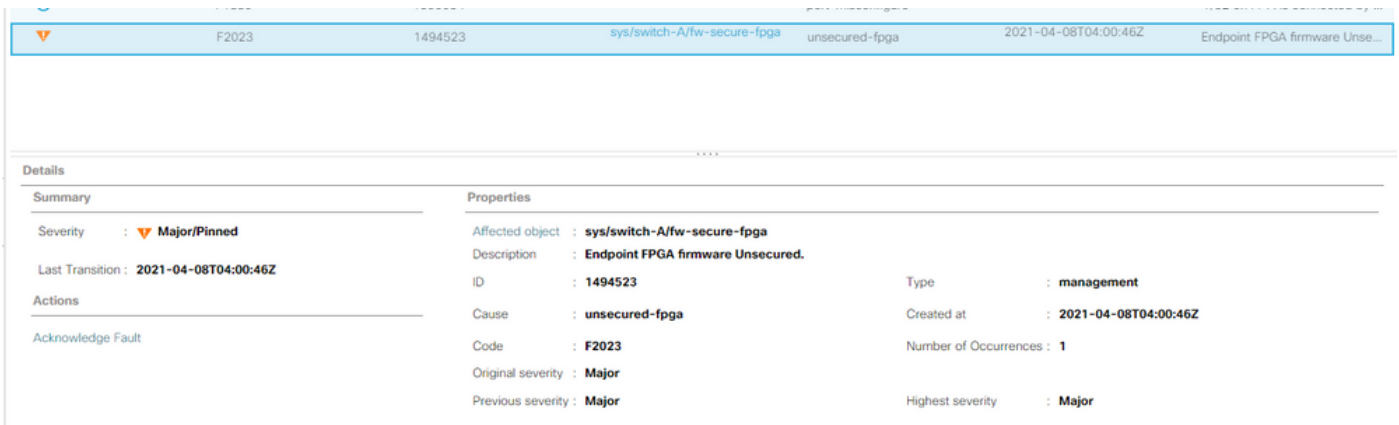
[Lösung:](#)

[SSH-Sitzung](#)

[UCSM-Weboberfläche](#)

Problem:

Bei UCSM-Upgrades auf Version 4.1(3) und höher auf 6400 (4. Generation) Fabric Interconnects wird der folgende schwerwiegende Fehler auftreten:



The screenshot shows a UCSM web interface with a fault entry. The breadcrumb path is: F2023 > 1494523 > sys/switch-A/fw-secure-fpga > unsecured-fpga > 2021-04-08T04:00:46Z > Endpoint FPGA firmware Unse... The fault details are as follows:

Details	
Summary	Properties
Severity : Major/Pinned	Affected object : sys/switch-A/fw-secure-fpga
Last Transition : 2021-04-08T04:00:46Z	Description : Endpoint FPGA firmware Unsecured.
Actions	ID : 1494523
Acknowledge Fault	Cause : unsecured-fpga
	Type : management
	Created at : 2021-04-08T04:00:46Z
	Number of Occurrences : 1
	Code : F2023
	Original severity : Major
	Previous severity : Major
	Highest severity : Major

Beschreibung: FPGA-Firmware für Endgeräte nicht gesichert.

Fehlercode: F2023

Dies ist eine neue Funktion als Reaktion auf eine bekannte sichere Boot-Schwachstelle, bei der goldene Regionen des FPGA möglicherweise Code eingespeist oder modifiziert haben, um sicheres Booten zu verhindern.

Lösung:

+ Dies ist eine erwartete Meldung bei einem Upgrade auf v4.1(3) und höher auf Fabric Interconnects der Serie 6400. Sie kann nur auf einem oder beiden FIs auftreten, je nachdem, mit welchem Code sie ursprünglich geliefert wurden.

+ Es besteht kein anderes Produktionsrisiko als die reduzierte Sicherheit. Dies kann bis zum nächsten geplanten Wartung Fenster.

+ Der FPGA kann gesichert und der Fehler mithilfe der folgenden Schritte (über SSH oder UCSM) behoben werden:

HINWEIS: Dazu muss jedes FI neu gestartet werden. Es wird empfohlen, dies in einem

Service-Fenster zu tun!

SSH-Sitzung

1. Öffnen Sie eine SSH-Sitzung mit der Domäne (die Cluster-IP oder die IP-Adresse eines FI funktioniert).

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

(Das FI wird nach kurzer Zeit neu gestartet. Führen Sie keinen manuellen Neustart des FI durch!)

2. Wiederholen Sie diesen Vorgang für B FI.

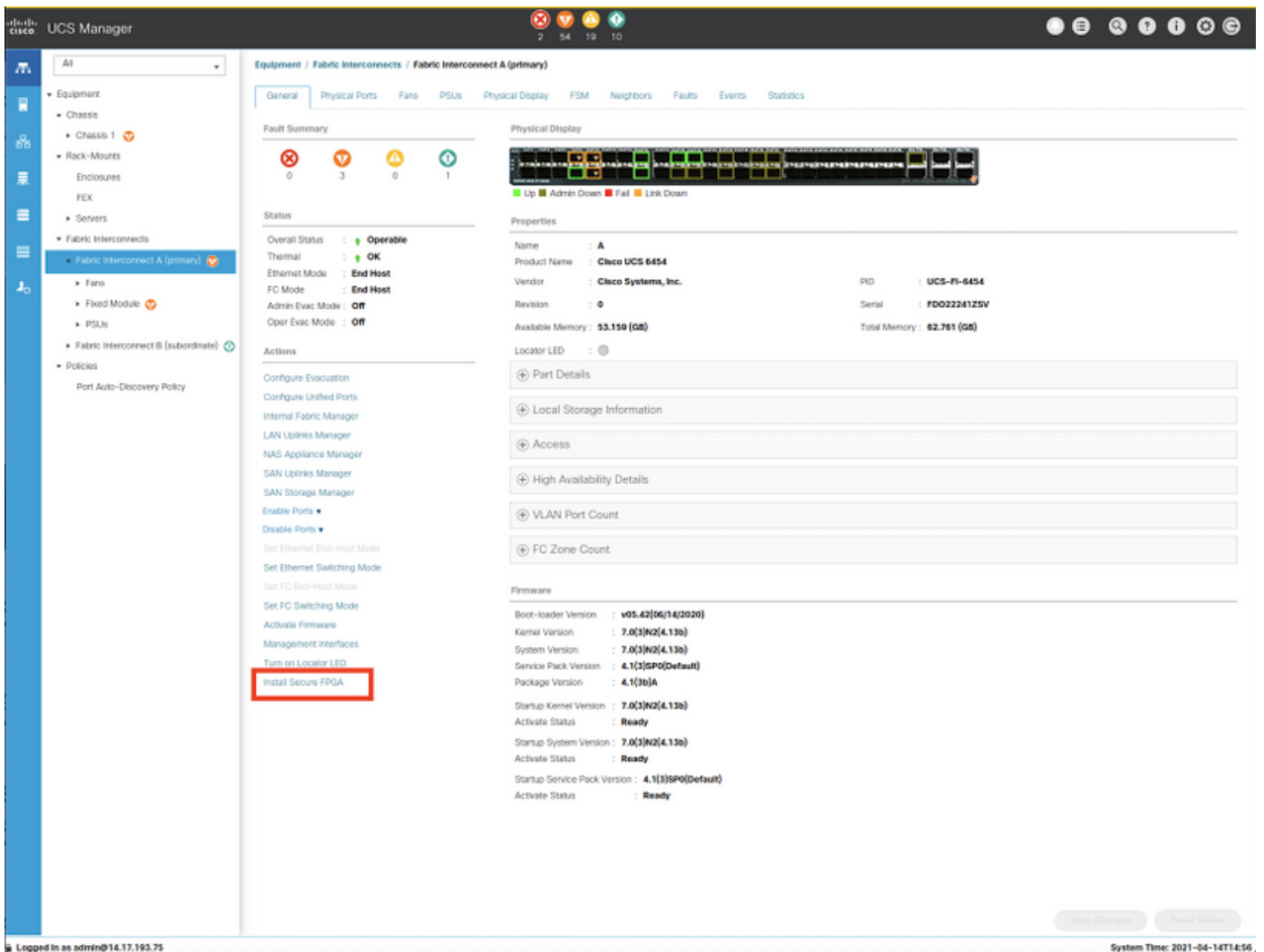
```
UCS-B# top UCS-B# scope fabric-interconnect b UCS-B /fabric-interconnect# activate secure-fpga UCS-B/fabric-interconnect*# commit-buffer
```

(Die FI wird nach kurzer Verzögerung neu gestartet. Führen Sie keinen manuellen Neustart des FI durch!)

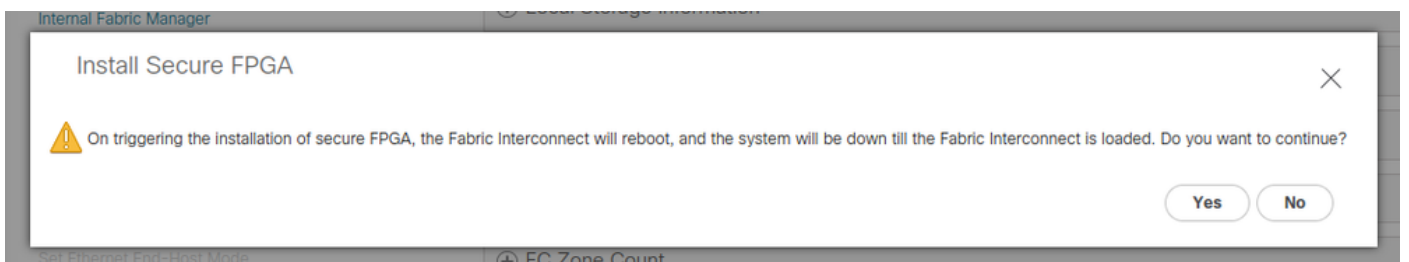
Der Fehler EndpointFPGAfirmwareUnsecured sollte nun den Status Bereinigt haben.

UCSM-Weboberfläche

1. Klicken Sie im Navigationsbereich auf Equipment (Geräte).
2. Erweitern Sie Equipment > Fabric Interconnects > Fabric_Interconnect_Name.
3. Klicken Sie im Arbeitsbereich auf die Registerkarte General (Allgemein).
4. Klicken Sie im Bereich Aktionen der Registerkarte Allgemein auf Sicherer FPGA installieren.



5. Klicken Sie im Dialogfeld auf OK.



Cisco UCS Manager startet das Fabric Interconnect neu, meldet Sie ab und trennt die Benutzeroberfläche von Cisco UCS Manager, wenn in der Warnmeldung Ja ausgewählt wird.

(Die FI wird nach kurzer Verzögerung neu gestartet. Führen Sie keinen manuellen Neustart des FI durch!)

Wenn Sie die Option "Install Secure FPGA" (Sicheres FPGA installieren) nicht sehen, löschen Sie Ihren Browser-Cache oder verwenden Sie eine private Sitzung.

Weitere Informationen zum sicheren FPGA-Upgrade finden Sie in den [Versionshinweisen](#) zu [Version 4.1\(3a\)](#).