

Secure Endpoint FPGA-firmware op UCS 6400 fabric interconnects

Inhoud

[Inleiding](#)

[Probleem](#)

[Oplossing](#)

[SSH-sessie](#)

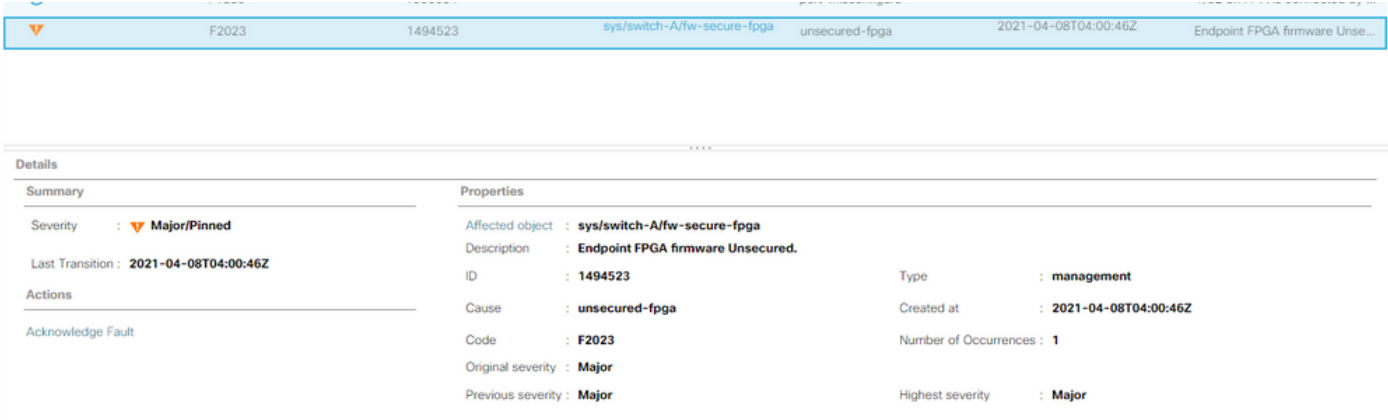
[UCS Manager Web UI](#)

Inleiding

Dit document beschrijft hoe u Secure Field-Programmable Array (FPGA) kunt inschakelen op 6400 Fabric Interconnect (FI's).

Probleem

In Unified Computing System Manager (UCS Manager)-upgrades om 4.1(3) of later op 6400 (4e generatie) FI's te wissen, zien klanten deze belangrijke fout:



The screenshot shows the UCS Manager Web UI interface. At the top, there is a breadcrumb trail: F2023 > 1494523 > sys/switch-A/fw-secure-fpga > unsecured-fpga > 2021-04-08T04:00:46Z > Endpoint FPGA firmware Unse... Below this, the 'Details' section is visible, divided into 'Summary' and 'Properties'.

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
		Code	: F2023
		Original severity	: Major
		Previous severity	: Major
		Type	: management
		Created at	: 2021-04-08T04:00:46Z
		Number of Occurrences	: 1
		Highest severity	: Major

Description: Endpoint FPGA firmware Unsecured.

Fault Code: F2023

Dit is een nieuw element in reactie op een bekende veilige 'bootkwetsbaarheid' waar gouden regio's van de FPGA code zouden kunnen hebben geïnjecteerd of aangepast, wat in wezen de beveiligde laars verslaat.

Oplossing

Dit is een verwacht bericht wanneer u een upgrade uitvoert naar release 4.1(3) of later op 6400 Series FI's. Het kan alleen op een of beide FI's voorkomen en is afhankelijk van de code waarmee ze oorspronkelijk zijn verzonden.

Er is geen ander risico voor de productie dan de verminderde zekerheid. Dit kan worden uitgesteld

tot het volgende geplande onderhoudsvenster.

De FPGA kan worden beveiligd en de fout kan met deze stappen worden gewist via een SSH-sessie of in de UCS Manager GUI.

Opmerking: Hiervoor moet elke FI opnieuw worden opgestart. Dit doet u aanbevolen in een servicevenster.

SSH-sessie

1. Open een SSH-sessie naar het domein. Het IP-adres van het cluster of het IP-adres van een van de FI werkt.

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

Opmerking: De FI start na een kort uitstel opnieuw. Start de FI niet handmatig opnieuw op.

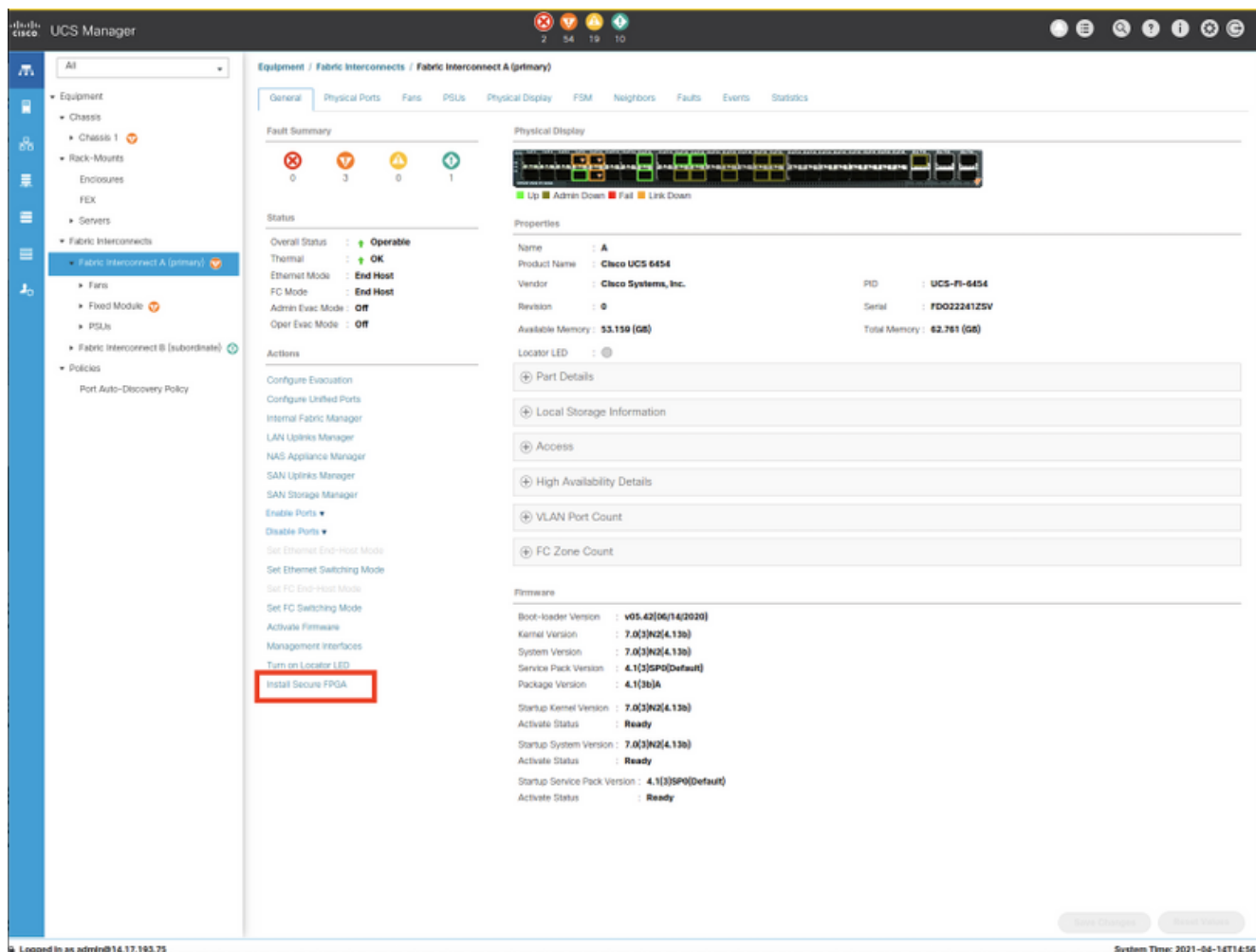
2. Herhaal dit proces op de B FI.

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

Opmerking: De FI start na een kort uitstel opnieuw. Start de FI niet handmatig opnieuw op. Het eindpunt FPGA firmware onbeveiligde fout moet nu uit de klaring zijn.

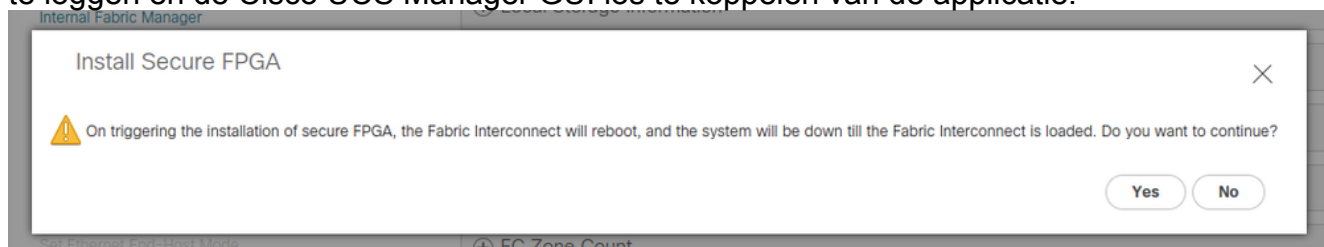
UCS Manager Web UI

1. Kies in het navigatiedeelvenster **apparatuur > Fabric-interconnects > *Fabric_Interconnect_name***.
2. Klik in het werkvenster op het tabblad **Algemeen**.
3. Klik in het gedeelte Handelingen van het tabblad Algemeen op **Secure FPGA installeren**.



4. Klik in het dialogvenster op **OK**.

5. Klik op **Ja** in het waarschuwingsbericht voor Cisco UCS Manager om de FI te hervatten, u uit te loggen en de Cisco UCS Manager GUI los te koppelen van de applicatie.



Opmerking: De FI start na een kort uitstel opnieuw. Start de FI niet handmatig opnieuw op. Als u de optie "Installeer Secure FPGA" niet ziet, dient u de zoekfunctie te wissen of een privésessie te gebruiken.

Zie [Releaseopmerkingen](#) van [Cisco UCS Manager, release 4.1](#) voor meer informatie over de Secure FPGA-upgrade.