

# Firmware FPGA de endpoint seguro em interconexões de estrutura UCS 6400

## Contents

[Introduction](#)

[Problema](#)

[Solução](#)

[Sessão SSH](#)

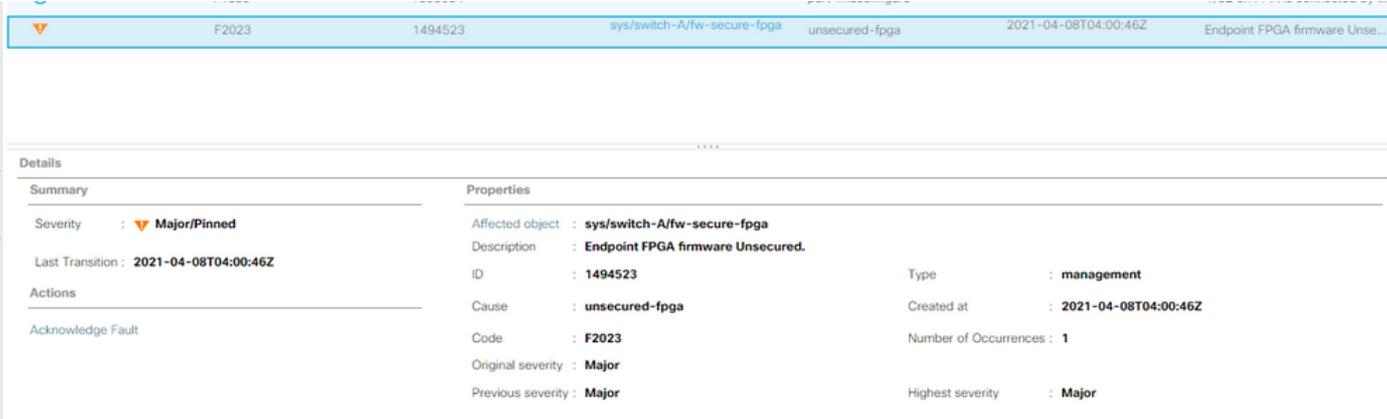
[UI da Web do UCS Manager](#)

## Introduction

Este documento descreve como habilitar o FPGA (Field-Programmable Gate Array) em FIs (Fabric Interconnects, Interconexões em malha) 6400.

## Problema

Nas atualizações do Unified Computing System Manager (UCS Manager) para a versão 4.1(3) ou posterior em FIs 6400 (4ª geração), os clientes verão esse grande erro:



The screenshot shows the UCS Manager web interface with a fault details page. The breadcrumb trail at the top is: F2023 > 1494523 > sys/switch-A/fw-secure-fpga > unsecured-fpga > 2021-04-08T04:00:46Z > Endpoint FPGA firmware Unse... The main content area is divided into two columns: Summary and Properties. The Summary column shows: Severity: Major/Pinned (with a red triangle icon), Last Transition: 2021-04-08T04:00:46Z, and an Actions section with an 'Acknowledge Fault' button. The Properties column shows: 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

Este é um novo recurso em resposta a uma vulnerabilidade de inicialização segura conhecida, na qual regiões douradas do FPGA podem ter um código injetado ou modificado, o que basicamente derrota a inicialização segura.

## Solução

Esta é uma mensagem esperada quando você atualiza para a versão 4.1(3) ou posterior nos FIs 6400 Series. Ele pode ocorrer apenas em um ou em ambos os FIs e depende do código que eles enviaram originalmente.

Não há outro risco para a produção além da redução da segurança. Isso pode ser atrasado até a

próxima janela de manutenção planejada.

O FPGA pode ser protegido e o erro limpo com essas etapas por meio de uma sessão SSH ou na GUI do UCS Manager.

**Note:** Isso exigirá uma reinicialização de cada FI. É recomendável fazer isso em uma janela de serviço.

## Sessão SSH

1. Abra uma sessão SSH no domínio. O endereço IP do cluster ou o endereço IP do FI funcionarão.

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

**Note:** O FI será reinicializado após um pequeno atraso. Não reinicialize manualmente o FI!

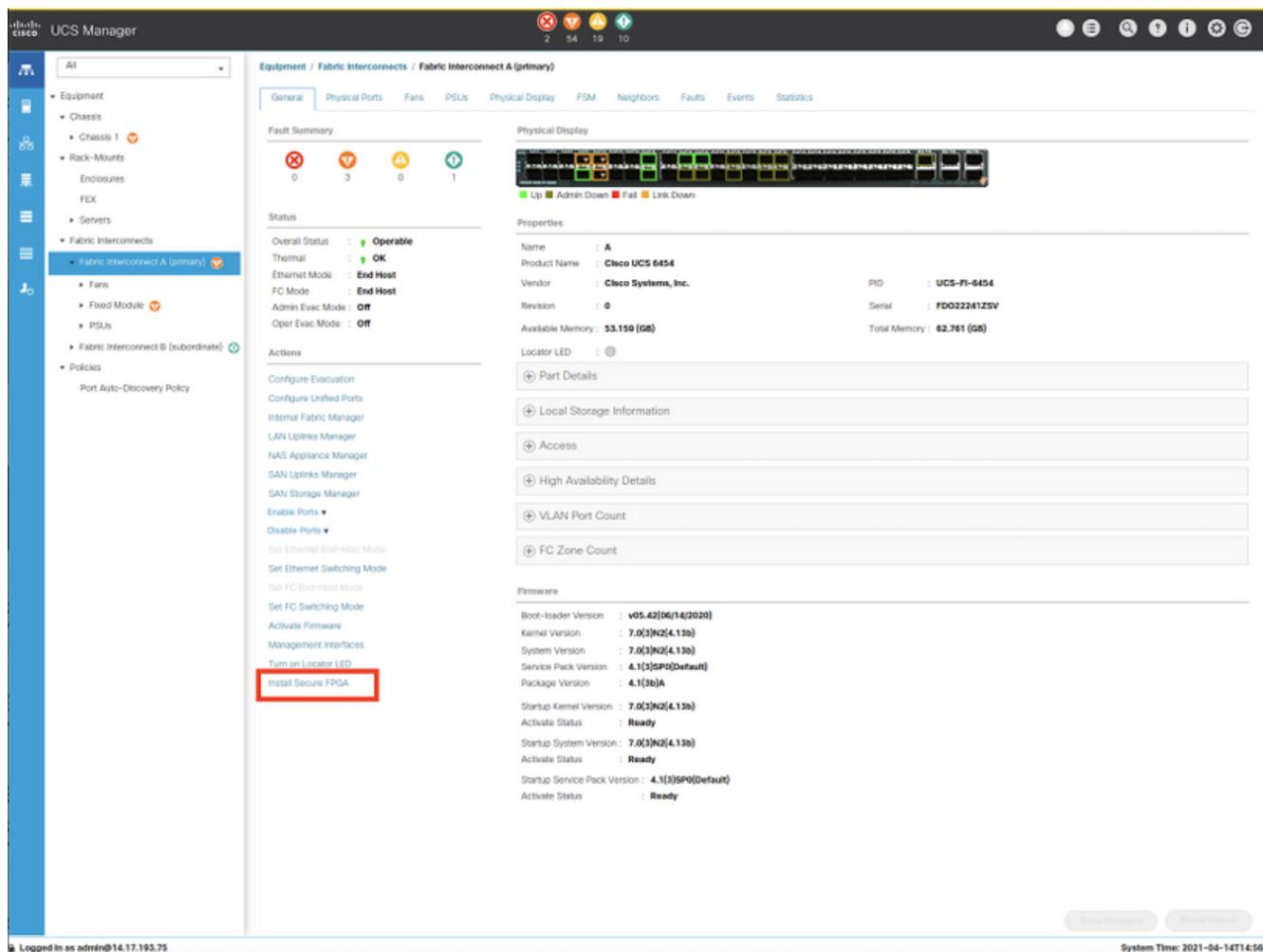
2. Repita esse processo no B FI.

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

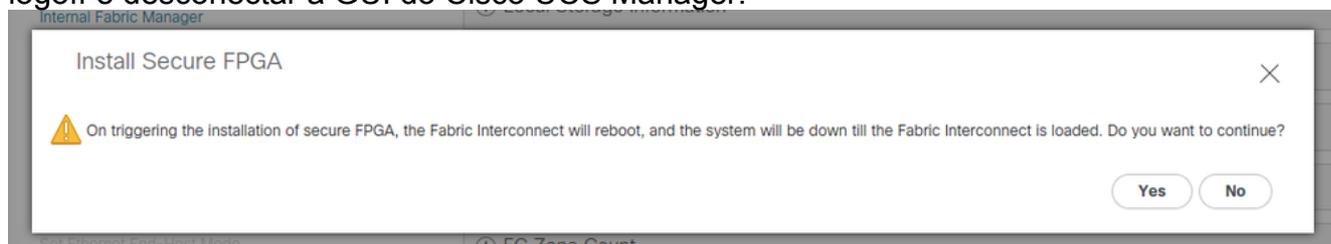
**Note:** O FI será reinicializado após um pequeno atraso. Não reinicialize manualmente o FI! O erro não seguro do firmware FPGA do endpoint deve estar agora no estado limpo.

## UI da Web do UCS Manager

1. No painel Navegação, escolha **Equipment > Fabric Interconnects > *Fabric\_Interconnect\_Name***.
2. No painel Trabalho, clique na guia **Geral**.
3. Na área Ações da guia Geral, clique em **Instalar FPGA seguro**.



4. Na caixa de diálogo, clique em **OK**.
5. Clique em **Sim** na mensagem de aviso do Cisco UCS Manager para reiniciar o FI, fazer logoff e desconectar a GUI do Cisco UCS Manager.



**Note:** O FI será reinicializado após um pequeno atraso. Não reinicialize manualmente o FI! Se você não vir a opção "Install Secure FPGA" (Instalar FPGA seguro), limpe o cache do seu navegador ou use uma sessão de navegação privada.

Para obter mais informações sobre a atualização do Secure FPGA, consulte [Release Notes do Cisco UCS Manager, Release 4.1](#).