

Secure Endpoint FPGA Firmware on UCS 6400 Fabric Interconnects

Contents

[Introduction](#)

[Problem](#)

[Solution](#)

[SSH Session](#)

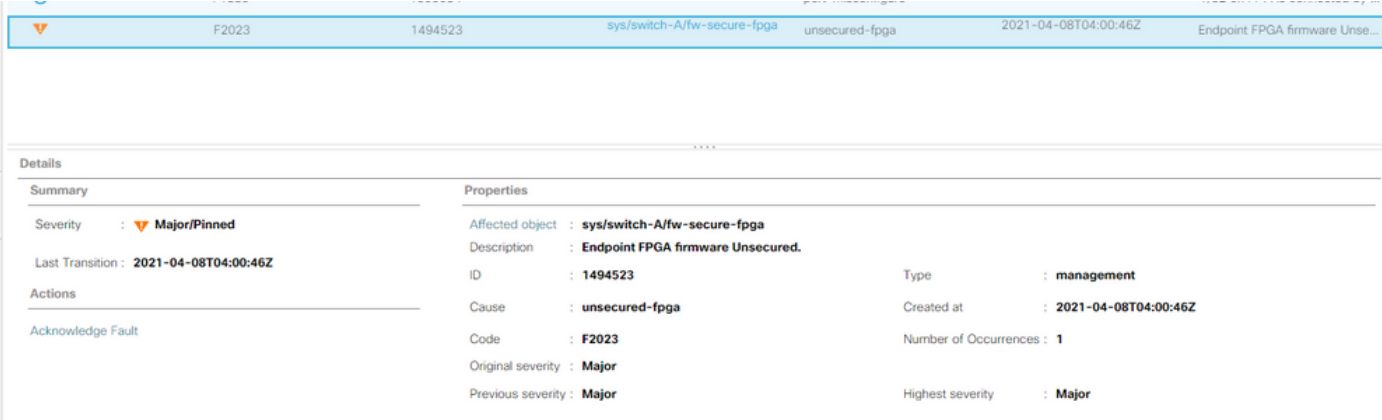
[UCS Manager Web UI](#)

Introduction

This document describes how to enable secure Field-Programmable Gate Array (FPGA) on 6400 Fabric Interconnects (FIs).

Problem

In Unified Computing System Manager (UCS Manager) upgrades to Release 4.1(3) or later on 6400 (4th Generation) FIs, customers will see this major error:



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, the main content area is titled 'Details' and is divided into 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

This is a new feature in response to a known secure boot vulnerability where golden regions of the FPGA could have code injected or modified, which essentially defeats secure boot.

Solution

This is an expected message when you upgrade to Release 4.1(3) or later on 6400 Series FIs. It might only occur on one or both FIs, and depends on the code they originally shipped with.

There is no risk to production other than the reduced security. This can be delayed until the next planned maintenance window.

The FPGA can be secured and the error cleared with these steps via an SSH session or in the UCS Manager GUI.

Note: This will require a reboot of each FI. It is recommended to do this in a service window.

SSH Session

1. Open a SSH session to the domain. The cluster IP address or either FI's IP address will work.

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

Note: The FI will reboot after a short delay. Do not manually reboot the FI!

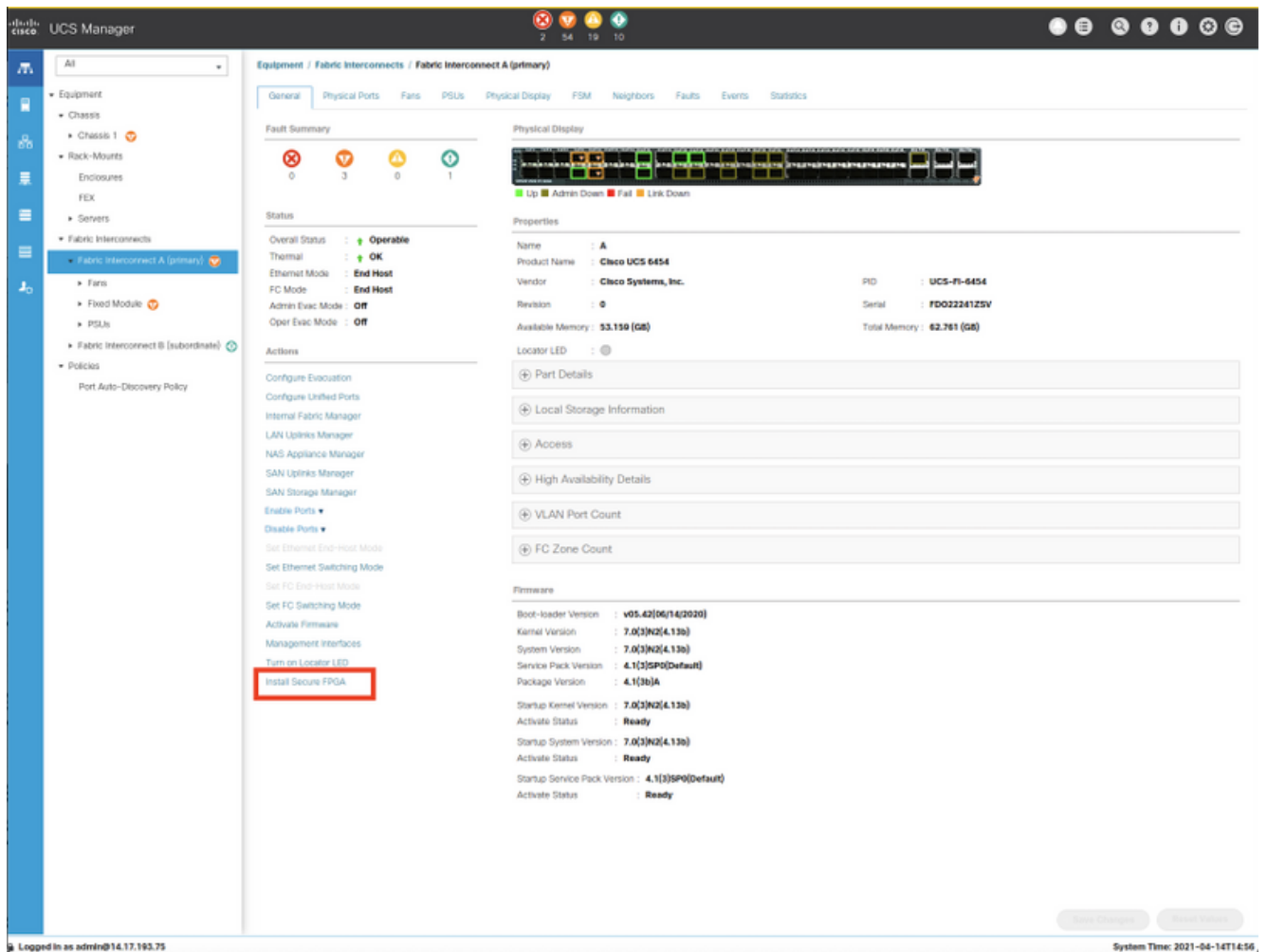
2. Repeat this process on the B FI.

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

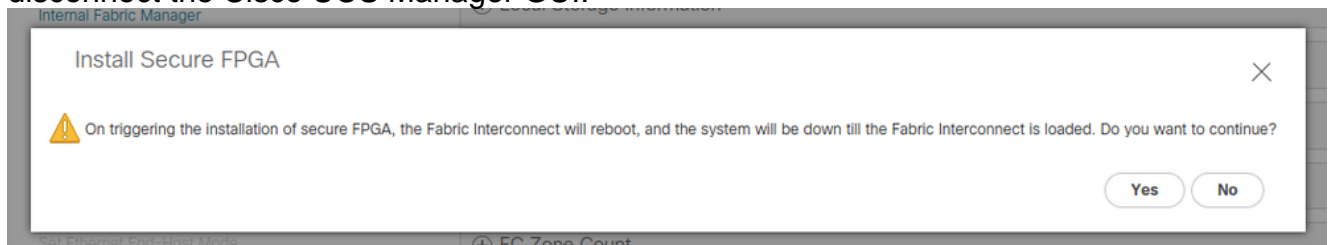
Note: The FI will reboot after a short delay. Do not manually reboot the FI!The Endpoint FPGA firmware unsecured error should now be in the cleared state.

UCS Manager Web UI

1. In the Navigation pane, choose **Equipment > Fabric Interconnects > *Fabric_Interconnect_Name***.
2. In the Work pane, click the **General** tab.
3. In the Actions area of the General tab, click **Install Secure FPGA**.



4. In the dialog box, click **OK**.
5. Click **Yes** in the warning message for Cisco UCS Manager to restart the FI, log you out, and disconnect the Cisco UCS Manager GUI.



Note: The FI will reboot after a short delay. Do not manually reboot the FI! If you do not see the "Install Secure FPGA" option, clear your browser cache or use a private browsing session.

For more information about the Secure FPGA upgrade, see [Release Notes for Cisco UCS Manager, Release 4.1](#).