

Configuración de CIMC en FMC y resolución de problemas comunes

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Contraseñas predeterminadas](#)

[Troubleshoot](#)

Introducción

Este documento describe la configuración de CIMC (Cisco Integrated Management Controller) en FMC y cómo resolver problemas comunes.

Prerequisites

Es importante tener en cuenta que el CIMC solo se puede configurar en un FMC físico.

Algunos FMCs vienen con una versión obsoleta de CIMC, y la única manera de actualizarlo es aplicando la revisión de la BIOS: Cisco_Firepower_Mgmt_Center_BIOSUPDATE_XXX_EN-11.sh.REL.tar (En la versión 6.2.3, el nombre de archivo es: Sourcefire_3D_Defense_Center_S3_BIOSUPDATE_623_EL-7.sh.REL.tar).

El hotfix se identifica como 7.4 (a excepción de 6.2.3, que se identifica como 7.1); sin embargo, el dispositivo no va a actualizar a esa versión, solo afecta a la versión de BIOS y CIMC. El error que explica con más detalle por qué se detecta como 7.1 es el Id. de error de Cisco [CSCwd47327](#). Esto también se aplica al punto 7.4.

Adobe ha desaprobado el contenido basado en flash desde 2020-12-31, con este acceso a cualquier página con Flash ya no es posible.

La actualización es necesaria, ya que las versiones antiguas de CIMC requieren Flash, esto significaría que los trenes de versiones anteriores a la 3.1(3a), que incluye la versión 2.2(x) están basados en Java, por lo tanto, es necesario actualizarlos para poder acceder de nuevo a través de la GUI. Esta información se puede verificar en [Versiones específicas de UCS Manager afectadas por el fin de vida útil de Adobe Flash](#).

Requirements

- Acceso físico al CSP.
- Teclado USB
- Monitor VGA

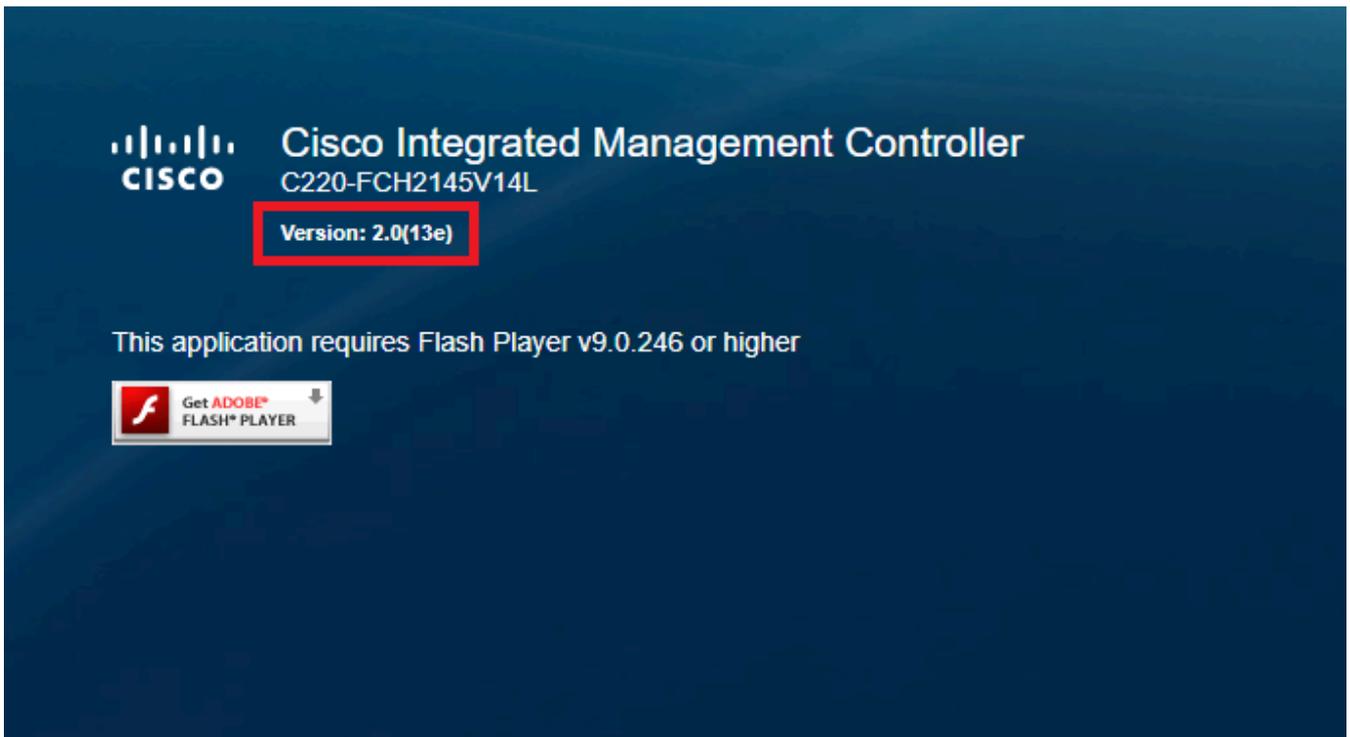
Componentes Utilizados

- FMC 2600

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

1. Como se dijo inicialmente, es importante asegurarse de que el CIMC está en una versión que no requiere Flash. La única forma de conseguirlo es acceder a través de la GUI. Por lo tanto, se recomienda actualizar si no ha aplicado BIOSUPDATE con anterioridad; de lo contrario, puede saltar al paso 6.



Versión de CIMC basada en Flash

Cisco Integrated Management Controller (Cisco IMC) Information

Hostname: CIMC-FMC-2600-2

IP Address: [REDACTED]

MAC Address: A4:88:73:5A:92:18

Firmware Version: 4.1(1f)

Versión CIMC de HTML5

2. Para actualizar, debe buscar el archivo file Cisco_Firepower_Mgmt_Center_BIOSUPDATE_XXX_EN-11.sh.REL.tar, que se encuentra en la versión base (con la excepción de 6.2.3).

Por ejemplo:

si está ejecutando la versión 7.0.3, debe buscar en 7.0.0:

Firepower Management Center 2600

Release 7.0.0

My Notifications

Related Links and Documentation
[Release Notes for 7.0.0](#)
[7.0.0 Documentation](#)

File Information	Release Date	Size	
Firepower Management Center BIOS Update Hotfix EN Do not untar Cisco_Firepower_Mgmt_Center_BIOSUPDATE_700_EN-11.sh.REL.tar Advisories	17-Jan-2024	519.79 MB	+ - 📄
Firepower Management Center BIOS Update Hotfix EL Do not untar Cisco_Firepower_Mgmt_Center_BIOSUPDATE_700_EL-7.sh.REL.tar Advisories	13-Dec-2021	517.53 MB	+ - 📄
Firepower Management Center install package Cisco_Firepower_Mgmt_Center-7.0.0-94-Restore.iso Advisories	26-May-2021	2450.83 MB	+ - 📄
Firepower Management Center upgrade Do not untar Cisco_Firepower_Mgmt_Center_Upgrade-7.0.0-94.sh.REL.tar Advisories	26-May-2021	2027.59 MB	+ - 📄

BIOSUPDATE en 7.0.0

Si está ejecutando la versión 6.6.7, debe buscar en 6.6.0:

Search...

Expand All Collapse All

7.0.0.1
7.0.0
6.7
6.6
6.6.7.1
6.6.7
6.6.5.2
6.6.5.1
6.6.5
6.6.4
6.6.3
6.6.1
6.6.0.1
6.6.0
6.4

Firepower Management Center 2600

Release 6.6.0

My Notifications

Related Links and Documentation
[Firepower Hotfix Release Notes](#)
[Release Notes for 6.6.0](#)
[Documentation Roadmap](#)

⚠ We recommend upgrading to our Suggested Release, as indicated by a gold star for each product, to take advantage of resolved issues. For details, see the release notes.

File Information	Release Date	Size
Firepower Management Center BIOS Update Hotfix EN Do not untar Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EN-11.sh.REL.tar Advisories	17-Jan-2024	519.79 MB
Firepower Management Center BIOS Update Hotfix EL Do not untar Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EL-7.sh.REL.tar Advisories	13-Dec-2021	517.53 MB
Firepower Management Center install package Cisco_Firepower_Mgmt_Center-6.6.0-90-Restore.iso Advisories	06-Apr-2020	2652.96 MB
Firepower Management Center upgrade Do not untar Cisco_Firepower_Mgmt_Center_Upgrade-6.6.0-90.sh.REL.tar Advisories	06-Apr-2020	2087.93 MB

BIOSUPDATE en 6.6.0

Si está ejecutando la versión 6.2.3, puede buscar con seguridad la versión 6.2.3:

6.2

6.2.3.18
6.2.3.17
6.2.3.16
6.2.3.15
6.2.3.14
6.2.3.13
6.2.3.12
6.2.3.11
6.2.3.10
6.2.3.9
6.2.3.7
6.2.3.6
6.2.3.5
6.2.3.4
6.2.3.3
6.2.3.2
6.2.3.1
6.2.3

File Information	Release Date	Size
Firepower Management Center BIOS Update Hotfix EL Do not untar Sourcefire_3D_Defense_Center_S3_BIOSUPDATE_623_EL-7.sh.REL.tar Advisories	13-Dec-2021	517.53 MB
Firepower Management Center upgrade from 6.1.0 or 6.2.0 to 6.2.3 Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.3-113.sh Advisories	01-Jun-2020	1835.84 MB
Firepower Management Center upgrade from 6.2.1 or 6.2.2 to 6.2.3 Do not untar Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.3-113.sh.REL.tar Advisories	01-Jun-2020	1835.86 MB
Firepower Management Center system software Sourcefire_Defense_Center_M4-6.2.3-113-Restore.iso Advisories	01-Jun-2020	2327.92 MB
Firepower Management Center 6.2.3 Hotfix - Local Malware Certificate Do not untar Hotfix_Local_Malware_Cert-6.2.3.999-4.sh.REL.tar Advisories	15-Nov-2018	0.89 MB
Firepower Management Center 6.2.3 Hotfix H Sourcefire_3D_Defense_Center_S3_Hotfix_H-6.2.3.999-5.sh.REL.tar Advisories	28-Sep-2018	5.95 MB

BIOSUPDATE en 6.2.3

3. Cargue el archivo en el FMC a través de System > Updates:

Product Updates | Rule Updates | Geolocation Updates

Download Updates | **Upload Update**

Currently running software version: 7.0.4

Currently installed VDB version: build 370 (2023-08-21 08:59:13)

Type	Version	Date	Reboot
Cisco Vulnerability And Fingerprint Database Updates	370	Mon Aug 21 09:01:06 UTC 2023	No
Cisco Firepower Mgmt Center Hotfix EL	7.1.0-7	Mon Nov 8 14:50:06 UTC 2021	Yes
Cisco FTD SSP FP2K Upgrade	7.0.4-55	Sun Aug 7 20:06:38 UTC 2022	Yes

Cargar revisión

4. Una vez que se carga el archivo, se procede a hacer clic en "instalar" e instalar la revisión:
5. Una vez finalizada la actualización, el CIMC ya no requiere Flash.
6. Ahora, reinicie el FMC para configurar el CIMC.
 - a. A través de la GUI, vaya a System > Configuration > Process y elija Reboot Management Center:

- Access List
- Access Control Preferences
- Audit Log
- Audit Log Certificate
- Change Reconciliation
- Console Configuration
- DNS Cache
- Dashboard
- Database
- Email Notification
- External Database Access
- HTTPS Certificate
- Information
- Intrusion Policy Preferences
- Language
- Login Banner
- Management Interfaces
- Network Analysis Policy Preferences
- ▶ Process**
- REST API Preferences
- Remote Storage Device
- SNMP
- Session Timeout
- Time
- Time Synchronization
- UCAPL/CC Compliance
- User Configuration
- Vulnerability Mapping
- Web Analytics

Name	
Shutdown Management Center	➔ Run Command
Reboot Management Center	➔ Run Command
Restart Management Center Console	➔ Run Command

Reiniciar GUI de FMC

b. A través de CLI, realice el "reinicio del sistema":

```
> system reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': YES

The system is going down for reboot NOW!
```

Reiniciar CLI de FMC

7. Ahora, comienza a arrancar, puede verificar la IP de CIMC asignada en "Cisco IMC IPv4", esto puede modificarse más adelante. Inicialmente, puede mostrarse como 0.0.0.0:

```
Cisco Systems, Inc.
Configuring and testing memory..

Cisco IMC IPv4 : 0.0.0.0
MAC ADDR : A4:88:73:5A:92:18
```

IP CIMC

8. Una vez que llegue al menú para acceder a Configuración de BIOS y CIMC, presione F8:



Copyright (c) 2020 Cisco Systems, Inc.

Press <F2> BIOS Setup : <F6> Boot Menu : <F7> Diagnostics

Press <F8> CIMC Setup : <F12> Network Boot

BIOS Version : C220M5.4.1.1c.0.0404202345

Platform ID : C220M5

Processor(s) Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz

Total Memory = 64 GB Effective Memory = 64 GB

Memory Operating Speed 2400 Mhz

M.2 SWRAID configuration is not detected. Switching to AHCI mode.

Cisco IMC IPv4 Address : 0.0.0.0

Cisco IMC MAC Address : A4:8B:73:5A:92:18

Entering CIMC Configuration Utility ...

Introducir configuración CIMC

9. La configuración de CIMC se muestra a continuación:

```
Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode                               NIC redundancy
Dedicated:      [X]                   None:           [X]
Shared LOM:     [ ]                   Active-standby: [ ]
Cisco Card:
  Riser1:       [ ]                   Active-active:  [ ]
  Riser2:       [ ]                   VLAN (Advanced)
  MLOm:         [ ]                   VLAN enabled:   [ ]
Shared LOM Ext: [ ]                   VLAN ID:        650
                                          Priority:        0
IP (Basic)
IPV4:           [X]                   IPV6:           [ ] IPV4 and IPV6: [ ]
DHCP enabled   [ ]
CIMC IP:       [REDACTED]
Prefix/Subnet: 255.255.255.0
Gateway:       10.0.0.1
Pref DNS Server: 8.8.8.8
Smart Access USB
Enabled        [ ]
*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F1>Additional settings
```

Configuración de IP de CIMC

- a. Para el modo NIC puede elegir Dedicado para utilizar la interfaz etiquetada como "M" en el FMC.
- b. Para la redundancia NIC, puede elegir None (Ninguno).
- c. VLAN puede dejarlo como inhabilitado, ya que puede causar problemas de conectividad a menos que sepa cómo configurar dispositivos externos.
- d. Para IP, puede elegir IPv4, IPv6 o IPv4 e IPv6 según cómo desee configurar la configuración.
- e. Si tiene un servidor DHCP para esto, puede habilitarlo, de lo contrario configure la IP.
- f. Una vez que haya terminado la configuración de red, puede utilizar F10 para guardar.

Para obtener más información sobre los modos de NIC, consulte [Configuración del sistema con la configuración de Cisco IMC](#).

h. Ahora, presione F1 para configurar el nombre de host y la contraseña.

```
Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
Common Properties
  Hostname:      IMC-FMC-2600-2
  Dynamic DNS:  [X]
  DDNS Domain:
FactoryDefaults
  Factory Default:      [ ]
Default User(Admin)
  Enter New Default User password:
  Re-Enter New Default User password:
Port Properties
  Auto Negotiation:      [X]
                               Admin Mode      Operation Mode
  Speed[1000/100/10Mbps]:      Auto          1000
  Duplex mode[half/full]:      Auto          full
Port Profiles
  Reset:                  [ ]
  Name:
*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F2>PreviousPageettngs
```

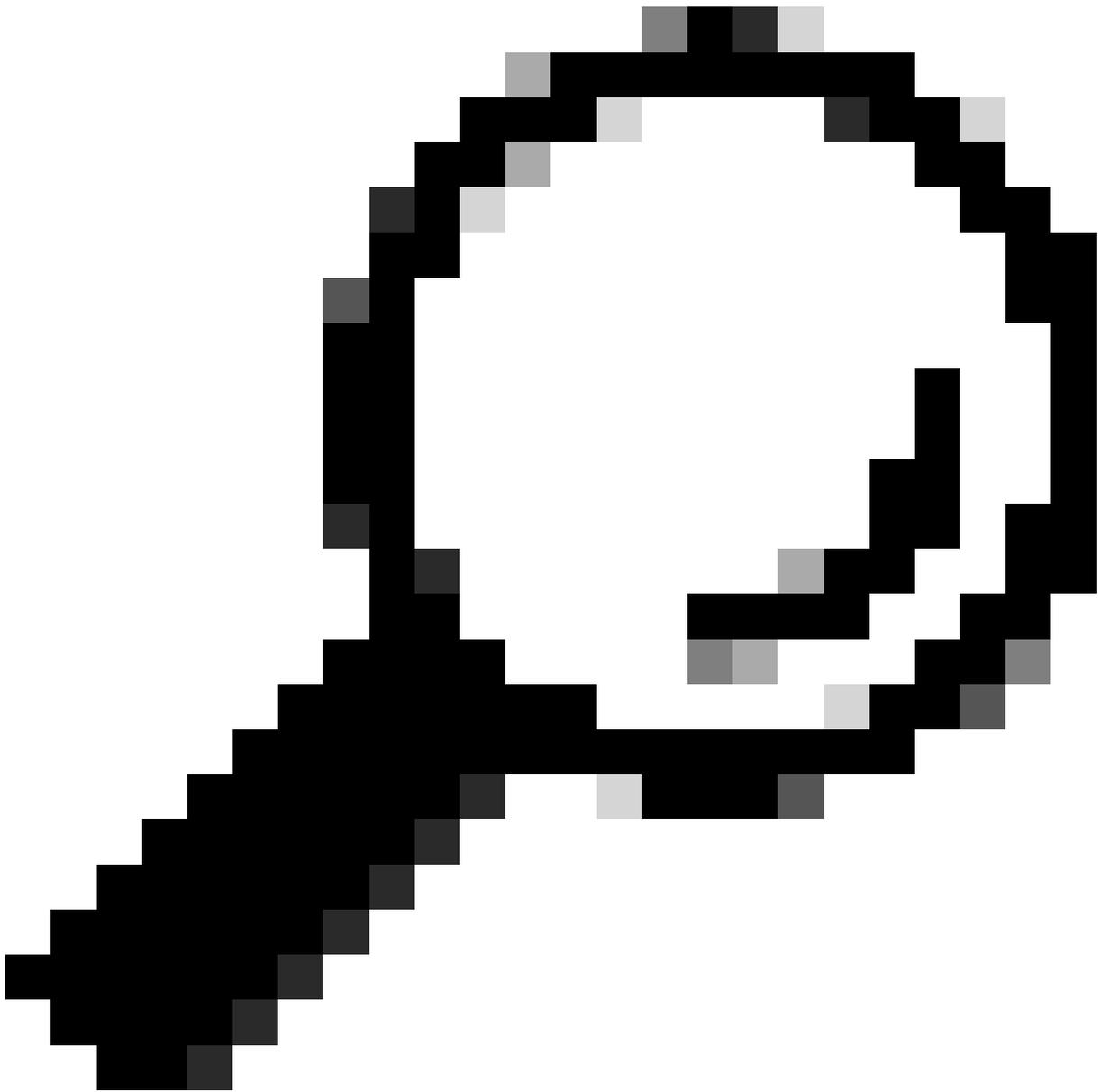
Contraseña de CIMC y guardar la configuración

- a. Aquí puede configurar el nombre de host como desee.
- b. Para el usuario predeterminado, puede establecer la contraseña como desee.
- c. Cuando haya terminado, presione F10 y el ESC.

Contraseñas predeterminadas

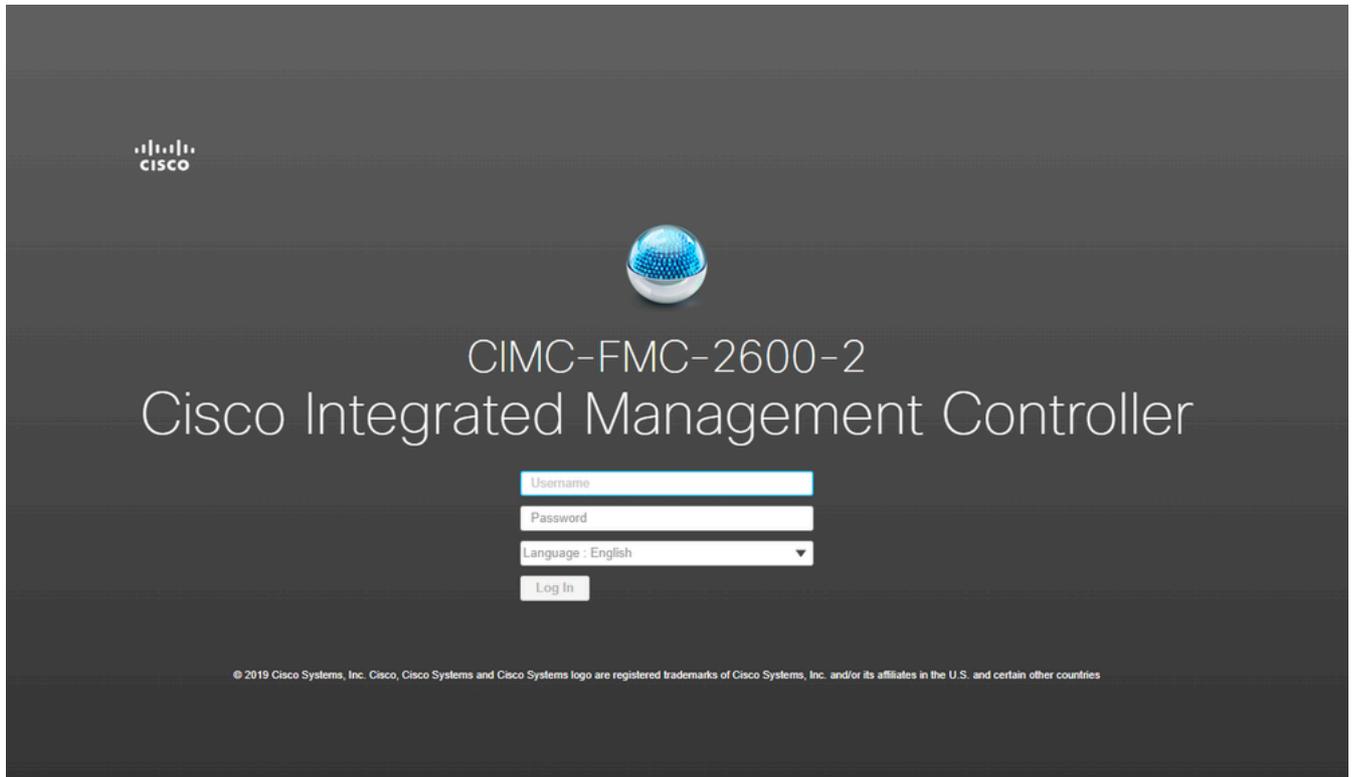
Si ha utilizado el restablecimiento de fábrica o el CIMC solicita una contraseña, puede probar una de las siguientes opciones:

Cisco12345
password
Cisco
p@ssw0rd.



Sugerencia: asegúrese de que BLOQ NUM del teclado está deshabilitado.

Ahora debe poder acceder a la GUI de CIMC:



GUI de CIMC

Troubleshoot

Hay un problema conocido en el que si se reinicia el FMC, puede entrar en una CLI llamada "startup.nsh":

Press ESC in 0 seconds to skip startup.nsh or any other key to continue.

Shell> _

Para salir de este shell, escriba "exit" y lo siguiente que sucederá es arrancar automáticamente la imagen.

En esta situación, es una cuestión de orden de arranque que se puede verificar en el CIMC. La razón por la que el dispositivo se inicia en este arranque es que el componente "EFI" se está iniciando primero que los otros componentes:

1. Haga clic en las tres líneas de la parte superior izquierda y busque "COMPUTE"
2. Una vez que esté en proceso, asegúrese de que el orden de arranque y cualquier otra configuración sean los siguientes:

BIOS Properties

Running Version C220M5.4.1.1c.0_M5_FMC
UEFI Secure Boot
Actual Boot Mode Uefi
Configured Boot Mode
Last Configured Boot Order Source BIOS
Configured One time boot device

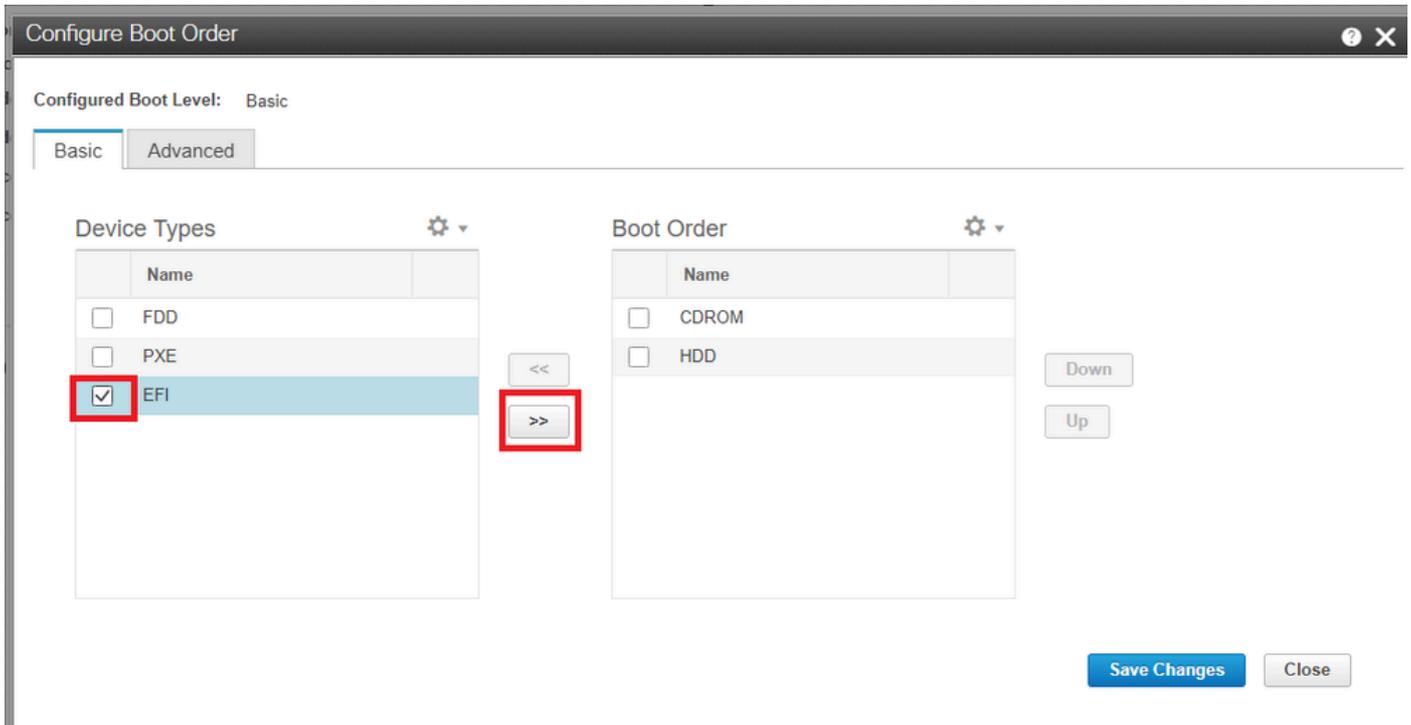
Save Changes

<p>Configured Boot Devices</p> <ul style="list-style-type: none">BasicCDROMHDDAdvanced	<p>Actual Boot Devices</p> <ul style="list-style-type: none">Cisco Firepower Management Center (NonPolicyTarget)Cisco EFI System Restore (NonPolicyTarget)UEFI: Built-in EFI Shell (NonPolicyTarget)UEFI: PXE IP4 Intel(R) Ethernet Controller X550 (NonPolicyTarget)UEFI: PXE IP4 Intel(R) Ethernet Controller X550 (NonPolicyTarget)
---	--

Configure Boot Order

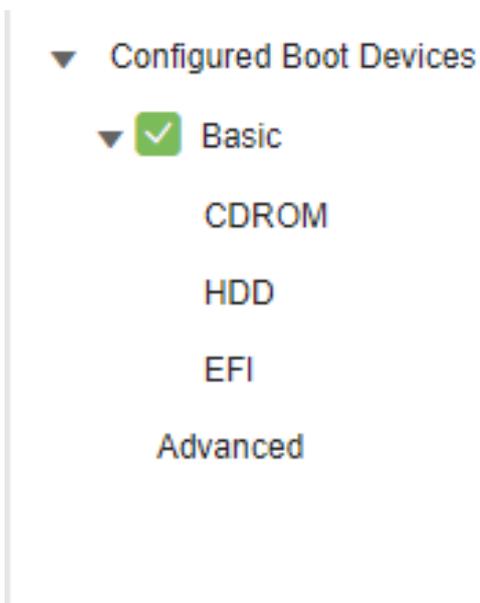
Opciones de arranque CIMC

3. Si el problema persiste, haga clic en "Configure Boot Order" (Configurar orden de arranque), elija "EFI" y haga clic en la flecha derecha:



Configuración de arranque CIMC

4. Asegúrese de que es el último elemento y haga clic en "Guardar cambios" y luego "Cerrar":



Se cambió la configuración de arranque CIMC

5. Ahora, puede reiniciar el dispositivo y ya no debe mostrar el shell anterior.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).