

Configurazione di CIMC su FMC e risoluzione dei problemi più comuni

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Password predefinite](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive la configurazione di CIMC (Cisco Integrated Management Controller) su FMC e come risolvere i problemi comuni.

Prerequisiti

È importante notare che il CIMC può essere configurato solo su un CCP fisico.

Alcuni FMC vengono forniti con una versione obsoleta di CIMC e l'unico modo per aggiornarla è applicare l'hotfix del BIOS: Cisco_Firepower_Mgmt_Center_BIOSUPDATE_XXX_EN-11.sh.REL.tar (nella versione 6.2.3, il nome del file è: Sourcefire_3D_Defense_Center_S3_BIOSUPDATE_623_EL-7.sh.REL.tar).

L'aggiornamento rapido è identificato come 7.4 (con l'eccezione della versione 6.2.3, identificata come 7.1). Tuttavia, il dispositivo non verrà aggiornato a tale versione, ma influirà solo sulle versioni BIOS e CIMC. Il bug che spiega ulteriormente il motivo per cui viene rilevato come 7.1 è l'ID bug Cisco [CSCwd47327](#). Ciò vale anche per il punto 7.4.

Adobe ha deprecato il contenuto basato su flash dal 2020-12-31, con questo accesso a qualsiasi pagina con Flash non è più possibile.

L'aggiornamento è necessario in quanto le versioni precedenti di CIMC richiedono Flash, ciò significa che i treni di rilascio precedenti alla 3.1(3a), che include il treno di rilascio 2.2(x) sono basati su Java, quindi deve essere aggiornato per essere nuovamente accessibile attraverso la GUI. Queste informazioni possono essere verificate in [specifiche release di UCS Manager interessate da Adobe Flash End-of-Life](#).

Requisiti

- Accesso fisico al CCP.
- Tastiera USB
- Monitor VGA

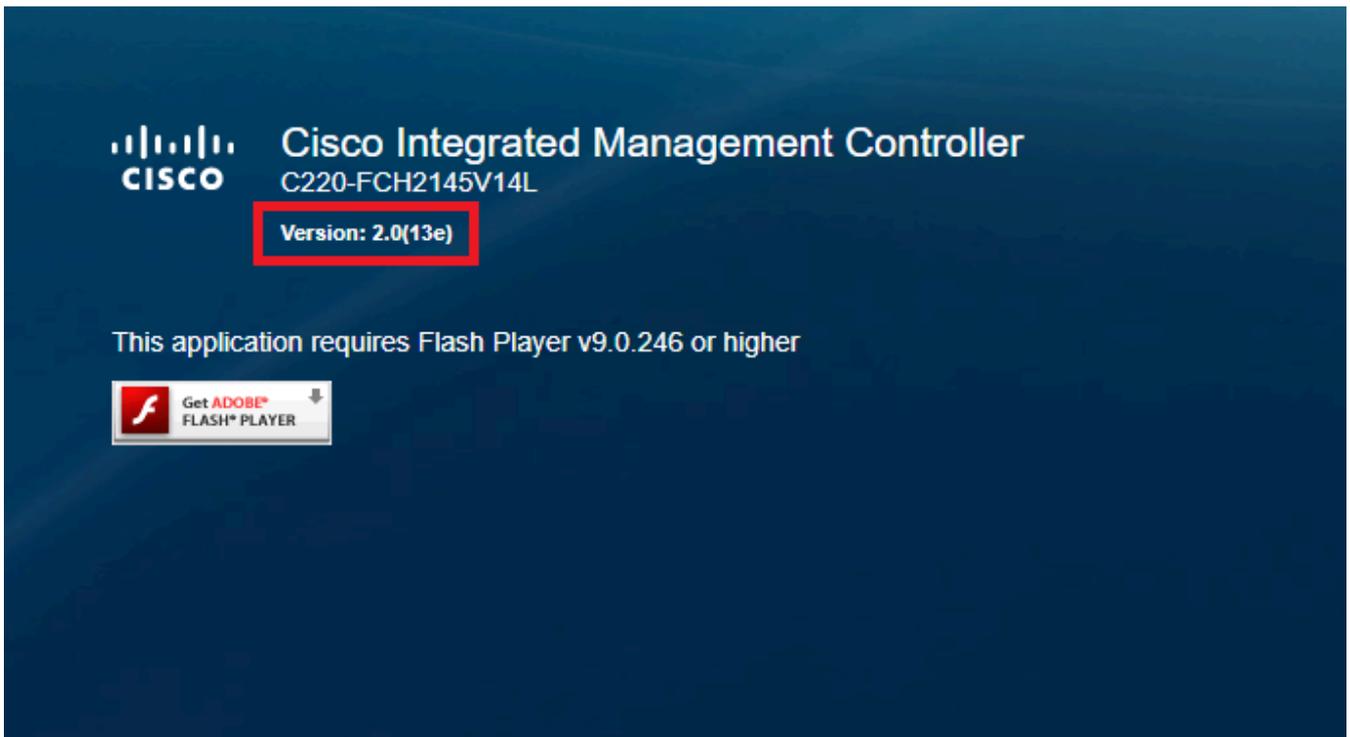
Componenti usati

- FMC 2600

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

1. Come indicato in origine, è importante verificare che la versione del CIMC in uso non richieda Flash. L'unico modo per farlo, è tramite l'accesso tramite l'interfaccia grafica. Pertanto, si consiglia di eseguire l'aggiornamento se non è stato applicato il parametro BIOSUPDATE in precedenza, altrimenti è possibile passare al punto 6.



Versione CIMC basata su 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)

Versione CIMC HTML5

2. Per eseguire l'aggiornamento, cercare il file file Cisco_Firepower_Mgmt_Center_BIOSUPDATE_XXX_EN-11.sh.REL.tar, nella versione base (ad eccezione della 6.2.3).

Ad esempio:

se è in esecuzione la versione 7.0.3, è necessario esaminare la versione 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 su 7.0.0

Se è in esecuzione la versione 6.6.7, è necessario esaminare la versione 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 su 6.6.0

Se è in esecuzione la versione 6.2.3, è possibile cercare in modo sicuro 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 su 6.2.3

3. Caricare il file nel FMC selezionando Sistema > Aggiornamenti:

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

Carica hotfix

4. Una volta caricato il file, si procede facendo clic su "install" (installa) e si installa l'aggiornamento rapido:
5. Al termine dell'aggiornamento, CIMC non richiede più Flash.
6. Riavviare il CCP per configurare il CCP.
 - a. Dalla GUI, selezionare System > Configuration > Process (Sistema > Configurazione > Processo) e selezionare Reboot Management Center (Riavvia centro di gestione):

- 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

Riavvia interfaccia utente FMC

b. Tramite CLI, eseguire il "riavvio 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!
```

Riavvia CLI FMC

7. Ora che ha avviato l'avvio, è possibile controllare l'indirizzo IP CIMC assegnato a "Cisco IMC IPv4", che può essere modificato in un secondo momento. Inizialmente può essere visualizzato come 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
```

CIMC IP

8. Una volta raggiunto il menu per accedere a BIOS e CIMC Configuration, premere 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 : A4:88:73:5A:92:18

Entering CIMC Configuration Utility ...

92

Accedere a CIMC Setup

9. La configurazione CIMC è illustrata come segue:

```

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

```

Configurazione IP CIMC

- a. Per la modalità NIC è possibile scegliere Dedicato per utilizzare l'interfaccia contrassegnata come "M" sul FMC.
- b. Per la ridondanza NIC, è possibile scegliere Nessuno.
- c. La VLAN può essere lasciata disabilitata perché potrebbe causare problemi di connettività a meno che non si sappia come configurare le periferiche esterne.
- d. Per IP, è possibile scegliere IPv4, IPv6 o IPv4 e IPv6 in base alla configurazione desiderata.
- e. Se si ha un server DHCP per questo, è possibile abilitarlo, altrimenti configurare l'IP.
- f. Una volta completata la configurazione di rete, è possibile utilizzare F10 per salvare i dati.

Per ulteriori informazioni sulle modalità NIC, selezionare [Setting Up the System With the Cisco IMC Configuration](#).

- h. Premere F1 per la configurazione del nome host e della password.

```
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
```

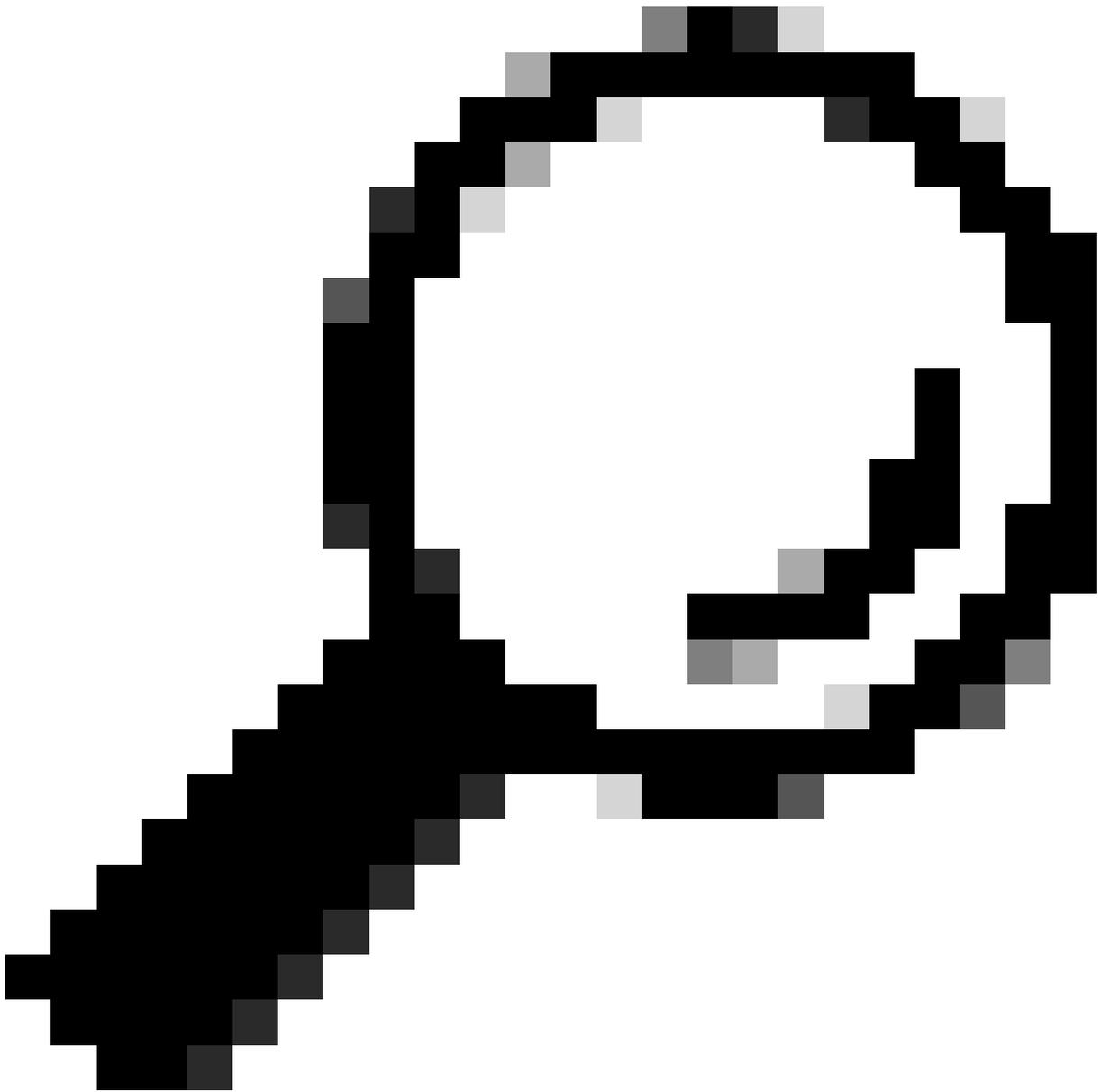
Password CIMC e salvataggio delle impostazioni

- a. Impostare il nome host come desiderato.
- b. Per l'utente predefinito, è possibile impostare la password come desiderato.
- c. Al termine, premere F10 e premere ESC.

Password predefinite

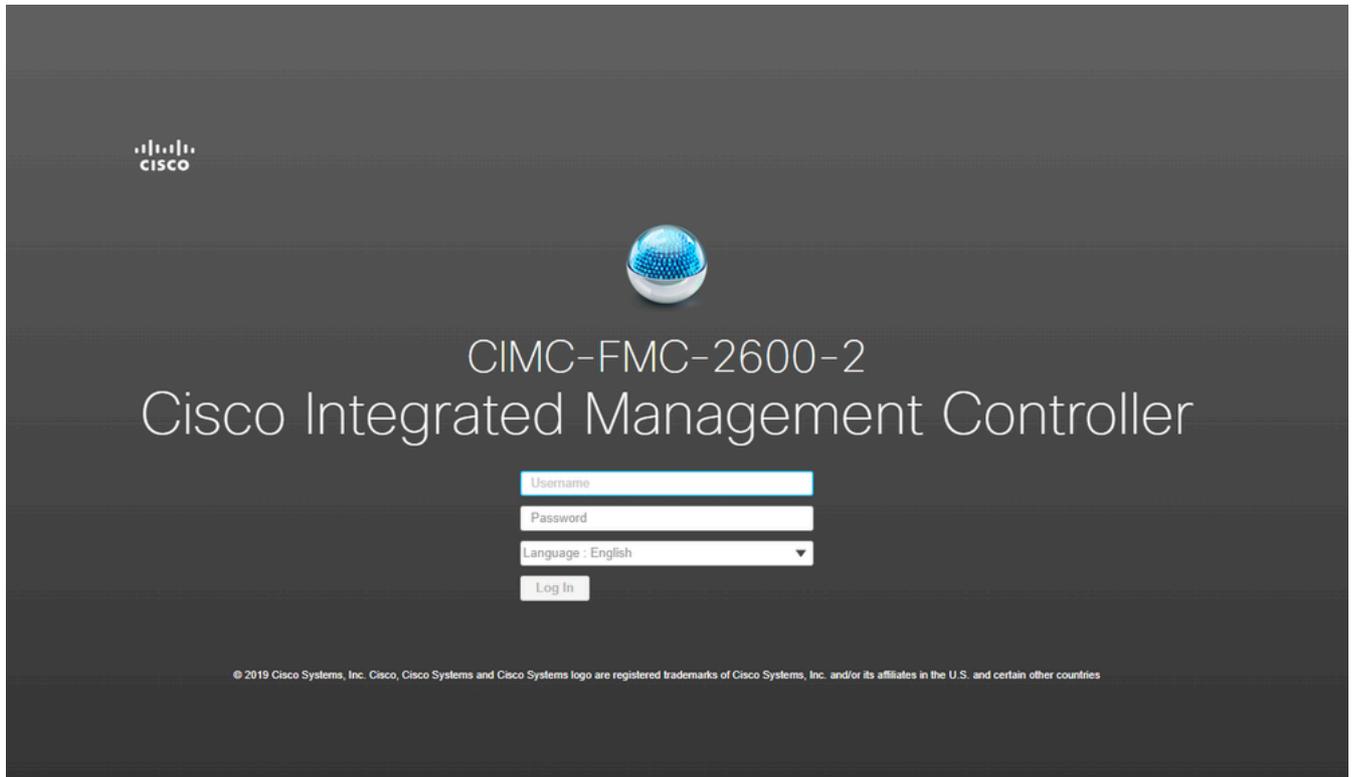
Se è stata utilizzata la funzione di ripristino predefinito o il CIMC richiede una password, è possibile provare a eseguire una delle operazioni seguenti:

Cisco12345
password
Cisco
p@ssw0rd.



Suggerimento: assicurarsi che BLOC NUM sulla tastiera sia disattivato.

A questo punto, è necessario essere in grado di accedere all'interfaccia GUI CIMC:



GUI CIMC

Risoluzione dei problemi

In caso di problema noto, se il FMC viene riavviato, potrebbe passare alla CLI denominata "startup.nsh":

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

Shell> _

Per uscire da questa shell, digitare "exit" e il passo successivo consiste nell'avviare automaticamente l'immagine.

In questo caso, è possibile controllare l'ordine di avvio sul CIMC. Il motivo per cui il dispositivo viene avviato è che il componente "EFI" viene avviato per primo rispetto agli altri componenti:

1. Fare clic sulle tre righe in alto a sinistra e cercare "COMPUTE"
2. Dopo aver eseguito l'elaborazione, accertarsi che l'ordine di avvio e qualsiasi altra configurazione siano i seguenti:

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

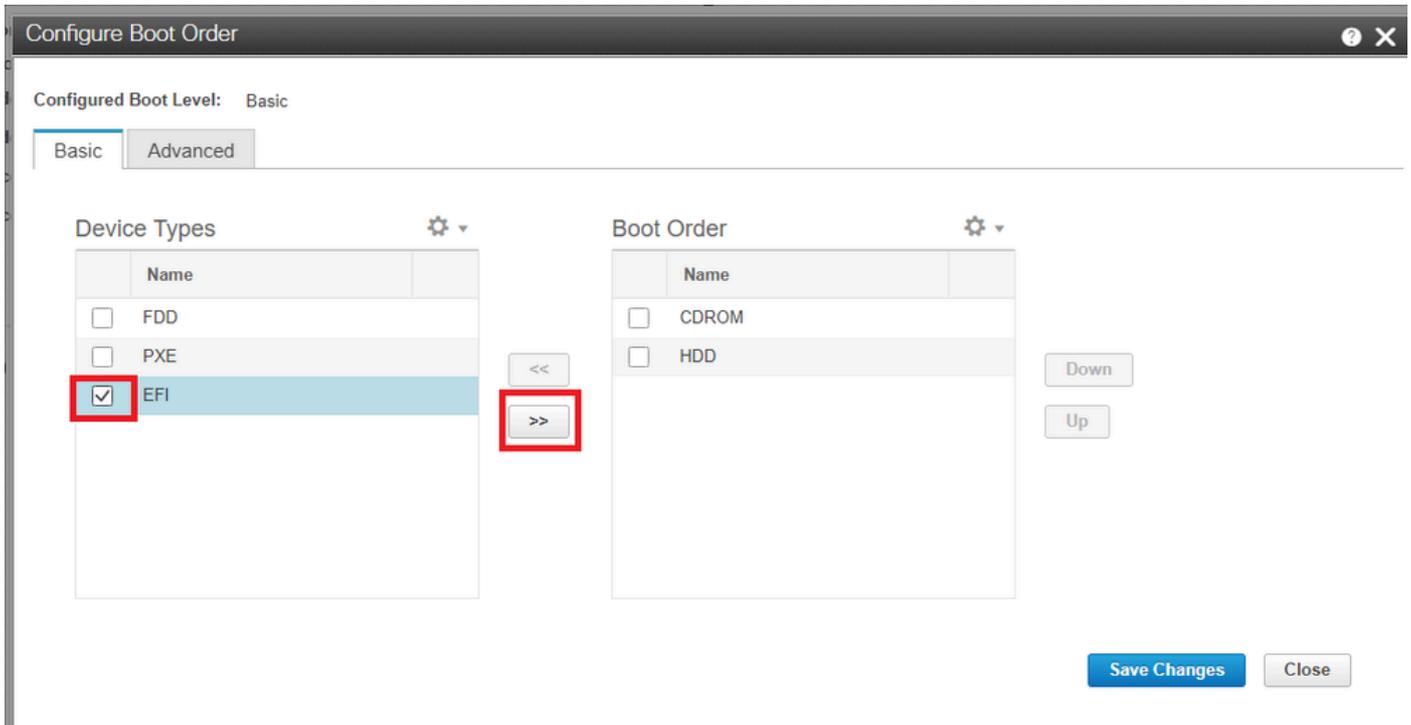
[Save Changes](#)

<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](#)

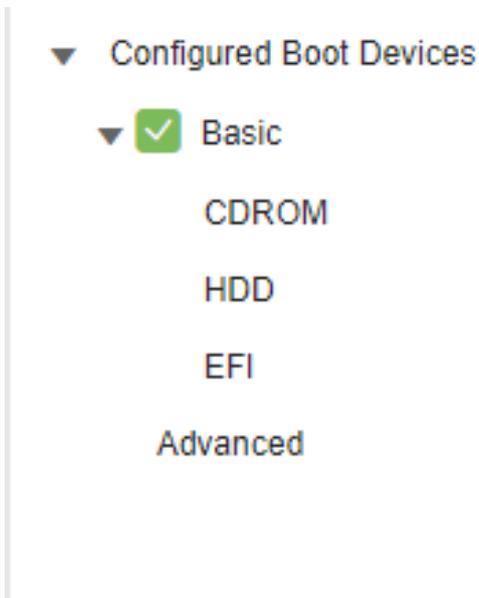
Opzioni di avvio CIMC

3. Se il problema persiste, fare clic su "Configure Boot Order" (Configura ordine di avvio), selezionare "EFI" (EFI) e fare clic sulla freccia destra:



Configurazione di avvio CIMC

4. Accertarsi che si tratti dell'ultimo elemento e fare clic su "Salva le modifiche" e quindi su "Chiudi":



Configurazione di avvio CIMC modificata

5. È ora possibile riavviare l'accessorio e la shell precedente non dovrà più essere visualizzata.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).