

Risoluzione dei problemi di registrazione delle licenze Hyperflex

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Premesse](#)

[Cos'è Smart License?](#)

[Come funzionano le licenze per Hyperflex?](#)

[Criteri di applicazione rigorosi](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Scenario 1: connettività HTTP/HTTP](#)

[Scenario 2: Problemi dei proxy](#)

[Scenario 3: Ambiente cloud](#)

[Scenario 4: Protocollo OCSP \(Online Certificate Status Protocol\)](#)

[Scenario 5: Certificato modificato](#)

[Procedura aggiuntiva](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come risolvere i problemi più comuni relativi alle licenze Hyperflex.

Prerequisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Hyperflex Connect
- Registrazione della licenza
- HTTP/HTTPS

Componenti usati

Le informazioni fornite in questo documento si basano su:

Hyperflex Data Platform (HXDP) 5.0(2a) e versioni successive

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.

Premesse

Cos'è Smart License?

Cisco Smart Software Licensing (Smart Licensing) è una soluzione intelligente di gestione delle licenze software basata su cloud che semplifica le tre funzioni principali delle licenze (acquisto, gestione e report) nell'intera organizzazione.

[Qui](#) è possibile accedere all'account Smart License.

Come funzionano le licenze per Hyperflex?

Cisco Hyperflex si integra con Smart Licensing e viene automaticamente attivato per impostazione predefinita quando si crea un cluster di memoria Hyperflex.

Tuttavia, affinché il cluster di memoria Hyperflex possa utilizzare e segnalare le licenze, è necessario registrarlo con Cisco Smart Software Manager (SSM) tramite Cisco Smart Account.

A Smart Account è un repository basato su cloud che fornisce visibilità completa e controllo dell'accesso a tutte le licenze software Cisco acquistate e alle istanze dei prodotti nell'intera azienda.

 Nota: nei cluster Hyperflex la registrazione è valida per un anno, dopo che Hyperflex tenta automaticamente di registrare di nuovo in modo che non sia necessaria alcuna interazione umana.

Criteri di applicazione rigorosi

A partire dalla versione HXDP 5.0(2a), alcune funzionalità vengono bloccate dall'interfaccia utente di Hyperflex Connect se il cluster non è conforme alla licenza.

Scenari di esempio relativi allo stato della licenza:

In questo scenario, il cluster **In compliance** con il **License Status**

The screenshot shows the VMware vSphere System Overview for a HyperFlex cluster. The cluster name is 'nitin-sl' and its status is 'ONLINE'. The license type is 'Datacenter Premier' and the license status is 'In compliance'. The vCenter URL is 'https://10.33.16.26'. The Hypervisor version is '6.7.0-17700523' and the HXDP Version is '5.0.2a-41522'. The cluster has a total capacity of 4.82 TiB and an available capacity of 4.66 TiB. The data replication factor is 3. The HyperFlex Controller is 'Online'. The nodes are 'ucsblr530' and 'HXAF240C-M5SX'. The disk overview shows 1 in use and 18 empty slots.

Node	Hypervisor	HyperFlex Controller
ucsblr530	Online	Online
HXAF240C-M5SX	10.20.16.96	10.20.16.102
	6.7.0-17700523	5.0.2a-41522

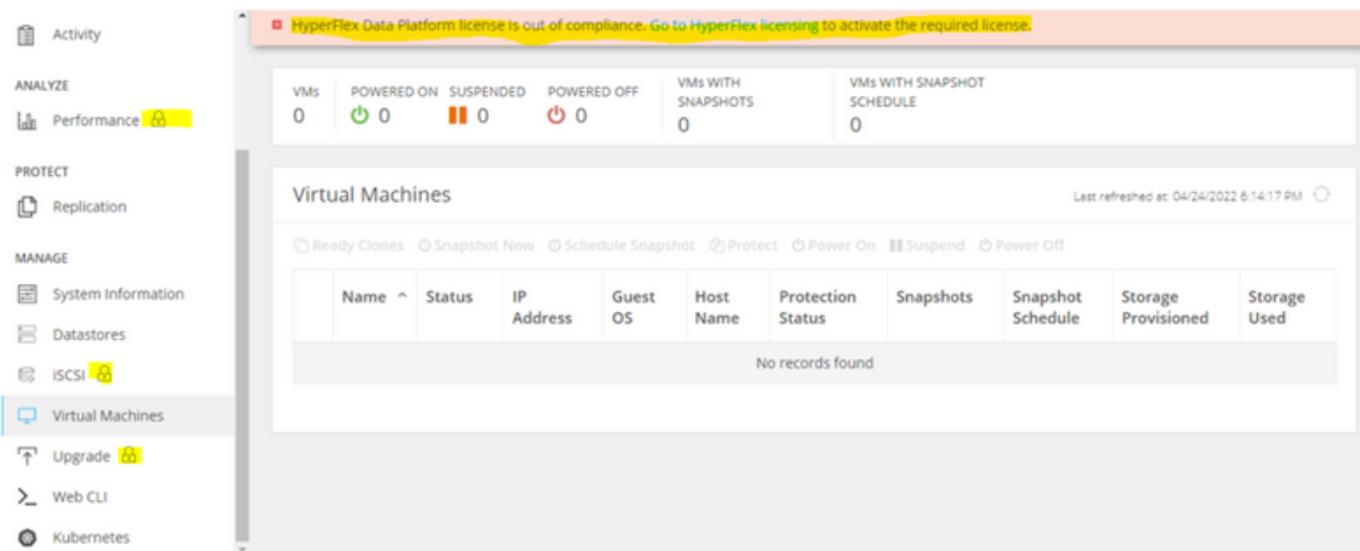
Nello scenario successivo, il cluster viene registrato ma il License Status è Out of Compliance e il periodo di tolleranza è compreso tra uno (1) e novanta (90) giorni.

In questo caso, nessuna funzionalità è bloccata, ma nella parte superiore del menu viene visualizzato un banner che chiede di attivare la licenza richiesta prima della scadenza del periodo di prova.

The screenshot shows the VMware vSphere System Overview for a HyperFlex cluster. The cluster name is 'nitin-sl' and its status is 'ONLINE'. The license type is 'Datacenter Premier' and the license status is 'Out of Compliance'. A banner at the top indicates: 'HyperFlex Data Platform license is out of compliance and there are 90 days remaining in the grace period after which features will be blocked. Go to HyperFlex licensing to activate the required license.' The vCenter URL is 'https://10.33.16.26'. The Hypervisor version is '6.7.0-17700523' and the HXDP Version is '5.0.2a-41522'. The cluster has a total capacity of 4.82 TiB and an available capacity of 4.66 TiB. The data replication factor is 3. The HyperFlex Controller is 'Online'. The nodes are 'ucsblr530' and 'HXAF240C-M5SX'. The disk overview shows 1 in use and 18 empty slots.

Node	Hypervisor	HyperFlex Controller
ucsblr530	Online	Online
HXAF240C-M5SX	10.20.16.96	10.20.16.102
	6.7.0-17700523	5.0.2a-41522

In questo scenario, il cluster viene registrato, il License Status è Out of Compliance e il periodo di tolleranza è zero (0).



Configurazione

Per informazioni su come registrare Hyperflex con il proprio Smart License account, controlla [questo video](#).

Verifica

Verificare che la configurazione funzioni correttamente.

Verificare lo stato della licenza tramite CLI. Visualizzare lo stato di registrazione e lo stato di autorizzazione.

```
admin:~$ stcli license show all
```

Registration:

Status: REGISTERED

Smart Account: TAC Cisco Systems, Inc.

Virtual Account: DC TAC

Export-Controlled Functionality: Allowed

Initial Registration: SUCCEEDED on Apr 12 15:59:46 2022 EDT

Last Renewal Attempt: SUCCEEDED on Apr 12 15:59:46 2022 EDT

Next Renewal Attempt: Oct 9 15:59:46 2022 EDT

Registration Expires: Apr 12 15:54:43 2023 EDT

Registration Status:

Registered

Registered – Specific License Reservation

Unregistered

Unregistered – Registration Pending

License Authorization:

Status: AUTHORIZED on Jul 14 08:55:08 2022 EDT

Last Communication Attempt: SUCCEEDED on Jul 14 08:55:08 2022 EDT

Next Communication Attempt: Aug 13 08:55:08 2022 EDT

Communication Deadline: Oct 12 08:50:08 2022 EDT

Authorization Status:

Authorized

Eval Mode

Evaluation Period Expired

Authorized – Reserved

Authorized Expired

No licenses in use

Evaluation Period:

Evaluation Mode: Not In Use

EVALUATION PERIOD EXPIRED on Apr 11 10:09:30 2022 EDT

Risoluzione dei problemi

Esistono alcuni scenari comuni in cui questi due stati possono non riuscire, entrambi causati dalla stessa causa principale.

Scenario 1: connettività HTTP/HTTPS

La registrazione della licenza avviene su TCP e più specificamente su HTTP e HTTPS, quindi è fondamentale consentire questa comunicazione.

Verifica della connettività da ogni Storage Controller VM (SCVM), ma principalmente Cluster Management IP (CMIP) SCVM.

```
curl https://tools.cisco.com/its/service/oddce/services/DDCEService
```

È necessario ottenere l'output mostrato nell'esempio, altrimenti il traffico è bloccato.

```
<h1>DDCEService</h1>
<p>Hi there, this is an AXIS service!</p>
<i>Perhaps there will be a form for invoking the service here...</i>
```

Se l'output ricevuto è diverso da quello precedente, verificare la connettività e verificare che le porte vengano aperte con questi comandi:

```
ping tools.cisco.com -c 5
nc -zv tools.cisco.com 80
nc -zv tools.cisco.com 443
```

Scenario 2: Problemi dei proxy

A volte, un proxy viene configurato tra tutti i client Web e i server Web pubblici quando questi eseguono ispezioni di sicurezza del traffico.

In questo caso, tra SCVM con CMIP e cisco.com, verificare che il proxy sia già configurato nel cluster (come mostrato nell'esempio).

<#root>

```
hxshell:/var/log/springpath$ stcli services sch show
cloudEnvironment: production
enabled: True
emailAddress: johndoe@example.com
portalUrl:

enableProxy: True
```

```
proxyPassword:
encEnabled: True
proxyUser:
cloudAsupEndpoint: https://diag.hyperflex.io/
proxyUrl:
proxyPort: 0
```

se il proxy è già configurato, verificare la connettività con l'URL o l'indirizzo IP del proxy e la porta configurata.

```
curl -v --proxy https://url:
```

<https://tools.cisco.com/its/service/oddce/services/DDCEService>

```
curl -v --proxy <Proxy IP>:<Proxy Port> https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Verificare inoltre la connettività al proxy.

```
nc -vzw2 x.x.x.x 8080
```

Scenario 3: Ambiente cloud

In alcune situazioni, l'ambiente cloud è impostato su devtest che causa il fallimento della registrazione. In questo esempio è impostato su **production**.

```
<#root>
```

```
hxshell:/var/log/springpath$ stcli services sch show
```

```
cloudEnvironment: production
```

```
cloudAsupEndpoint: https://diag.hyperflex.io/
```

```
portalUrl:
```

```
proxyPort: 0
```

```
enabled: True
```

```
encEnabled: True
```

```
proxyUser:
```

```
proxyPassword:
```

```
enableProxy: True
```

```
emailAddress: johndoe@example.com
```

```
proxyUrl:
```

Dai log è possibile visualizzare errori specifici quando l'ambiente è impostato in modo errato come devtest.

```
cat hxLicenseSvc.log | grep -ia "Name or service not known"
```

```
2021-09-01-18:27:11.557 [] [Thread-40] ERROR event_msg_sender_log - sch-alpha.cisco.com: Name or service
```

 **Suggerimento:** a partire dalla versione 5.0(2a), diag user è disponibile per consentire agli utenti di disporre di più privilegi per la risoluzione dei problemi relativi all'accesso a cartelle e comandi con restrizioni non accessibili tramite la riga di comando priv introdotta in Hyperflex versione 4.5.x.

È possibile modificare il tipo di ambiente in `production` e ritentare la registrazione.

```
diag# stcli services sch set --email johndoe@example.com --environment production --e
```

Scenario 4: Protocollo OCSP (Online Certificate Status Protocol)

Hyperflex sfrutta OCSP e **Certificate Revocation Lists** (CRL) per convalidare i certificati HTTPS durante il processo di registrazione della licenza.

Questi protocolli sono progettati per distribuire lo stato di revoca su HTTP. I CRL e i messaggi OCSP sono documenti pubblici che indicano lo stato di revoca dei certificati X.509 quando la convalida OCSP ha esito negativo e la registrazione della licenza ha esito negativo.

 Suggerimento: se l'OCSP ha esito negativo, significa che un dispositivo di sicurezza tra le due interrompe la connessione HTTP

Per verificare se la convalida OCSP è valida, è possibile provare a scaricare il file nella partizione SCVM /tmp CMIP, come mostrato nell'esempio.

```
hxshell:~$cd /tmp
hxshell:/tmp$ wget http://www.cisco.com/security/pki/trs/ios_core.p7b
--2022-08-18 00:13:37-- http://www.cisco.com/security/pki/trs/ios_core.p7b
Resolving www.cisco.com (www.cisco.com)... x.x.x.x aaaa:aaaa:aaaa:aaaa::aaaa
Connecting to www.cisco.com (www.cisco.com)|x.x.x.x|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 25799 (25K)
Saving to: 'ios_core.p7b'
```

```
ios_core.p7b 100%[=====]
2022-08-18 00:13:37 (719 KB/s) - 'ios_core.p7b' saved [25799/25799]
```

```
hxshell:/tmp$ ls -lath ios*
-rw-rw-r-- 1 diag diag 26K Jun 30 18:00 ios_core.p7b
-rw-rw-r-- 1 diag diag 26K Jun 30 18:00 ios_core.p7b.1
-rw-rw-r-- 1 diag diag 26K Jun 30 18:00 ios_core.p7b.2
-rw-rw-r-- 1 diag diag 26K Jun 30 18:00 ios_core.p7b.3
-rw-r--r-- 1 admin springpath 26K Jun 30 18:00 ios_core.p7b.4
```

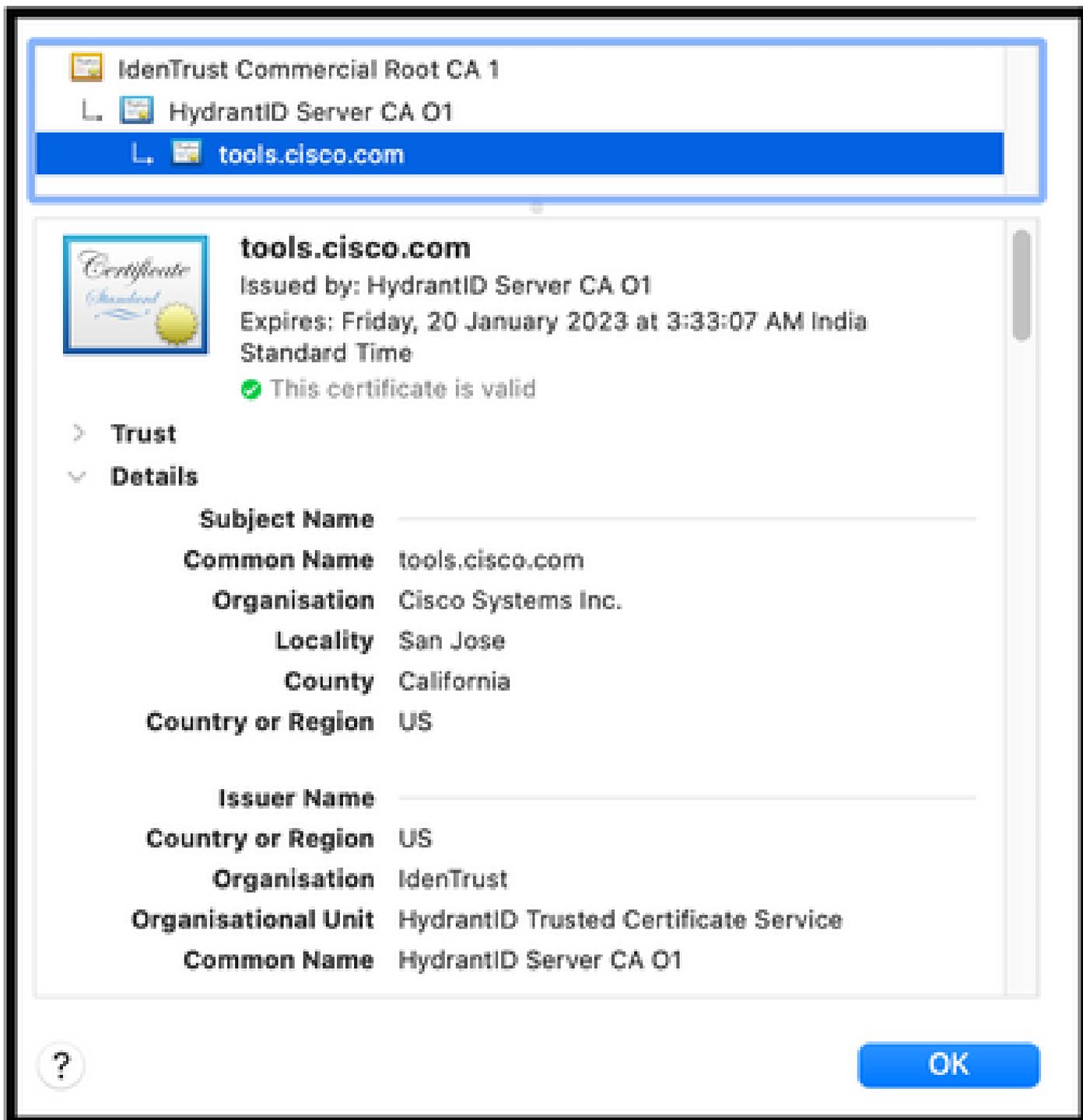
Scenario 5: Certificato modificato

In alcune reti vengono eseguiti dispositivi di protezione proxy e firewall Secure Sockets Layer (SSL) e possono danneggiare il certificato che Hyperflex si aspetta di ricevere da tools.cisco.com:443.

Per verificare che il certificato non venga modificato da un proxy o da un firewall, eseguire il comando nel SCVM che contiene il CMIP:

```
diag# openssl s_client -connect tools.cisco.com:443 -showcerts < /dev/null
```

è importante osservare che il Subject Name e Issuer Name le informazioni devono corrispondere al certificato illustrato in questo esempio.



⚠ Avviso: se almeno un campo nell'oggetto o nell'emittente è diverso, la registrazione non riesce. Una regola di bypass in Ispezione SSL di sicurezza per IP di gestione cluster Hyperflex e tools.cisco.com:443 può risolvere il problema.

In questo esempio viene illustrato come convalidare le stesse informazioni ricevute dal certificato in SCVM Hyperflex CMIP.

<#root>

hxshell:~\$ su diag

```
diag# openssl s_client -connect tools.cisco.com:443 -showcerts < /dev/null
CONNECTED(00000003)
depth=2
```

```
 C = US, O = IdenTrust, CN = IdenTrust Commercial Root CA 1
```

```
verify return:1
depth=1
```

```
 C = US, O = IdenTrust, OU = HydrantID Trusted Certificate Service,
```

```
 CN = HydrantID Server CA 01
```

```
verify return:1
depth=0
```

```
 CN = tools.cisco.com, O = Cisco Systems Inc., L = San Jose, ST = California, C = US
```

```
verify return:1
```

```
---
```

```
Certificate chain
```

```
0 s:/
```

```
 CN=tools.cisco.com
```

```
 /
```

```
 O=Cisco Systems Inc.
```

```
 /
```

```
 L=San Jose
```

```
 /
```

```
 ST=California
```

```
 /
```

```
 C=US
```

```
 i:/
```

```
 C=US
```

```
 /
```

```
 O=IdenTrust
```

```
 /
```

```
 OU=HydrantID Trusted Certificate Service
```

```
 /C
```

```
 N=HydrantID Server CA 01
```

```
...
```

```
<TRUNCATED>
```

```
...
```

```
1 s:/
```

C=US
/
O=IdenTrust
/
OU=HydrantID Trusted Certificate Service
/
CN=HydrantID Server CA 01

i:/
C=US
/
O=IdenTrust
/
CN=IdenTrust Commercial Root CA 1

...
<TRUNCATED>

...
2 s:/

C=US
/
O=IdenTrust
/
CN=IdenTrust Commercial Root CA 1

i:/
C=US
/
O=IdenTrust
/
CN=IdenTrust Commercial Root CA 1

...
<TRUNCATED>

...

Server certificate
subject=/
CN=tools.cisco.com

/
O=Cisco Systems Inc.

```
/
L=San Jose
/
ST=California
/
C=US

issuer=/
C=US
/
O=IdenTrust
/
OU=HydrantID Trusted Certificate Service
/
CN=HydrantID Server CA 01

---
...
<TRUNCATED>
...
---
DONE
```

Procedura aggiuntiva

Questa procedura può essere utilizzata se gli scenari coperti sono corretti o risolti, ma la registrazione della licenza non riesce.

Annulla la registrazione della licenza

```
hxshell:~$stcli license disable
hxshell:~$stcli license enable
hxshell:~$stcli license deregister
```

Acquisire un nuovo token dalle licenze Smart, riavviare il processo di gestione delle licenze, quindi riprovare a registrare la licenza.

```
hxshell:~$priv service hxLicenseSvc stop  
hxshell:~$priv service hxLicenseSvc start  
hxshell:~$stcli license register --idtoken IDTOKEN --force
```

Informazioni correlate

- [Cisco HyperFlex HX Data Platform - Guide per l'utente finale](#)

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).