# Risoluzione dei problemi di connettività e registrazione con AMP su FireSIGHT Management Center

## Sommario



## Introduzione

Un centro di gestione FireSIGHT nell'implementazione può connettersi al cloud Cisco. Dopo aver configurato un centro di gestione FireSIGHT per la connessione al cloud, è possibile ricevere i record di scansioni, rilevamenti di malware e quarantene. I record vengono archiviati nel database di FireSIGHT Management Center come eventi malware. Per impostazione predefinita, il cloud invia eventi malware per tutti i gruppi all'interno dell'organizzazione, ma è possibile limitare per gruppo quando si configura la connessione. In questo documento vengono illustrati vari problemi e procedure per la risoluzione dei problemi relativi alla funzionalità Advanced Malware Protection (AMP) di un centro di gestione FireSIGHT.

## Porta o server bloccato nel firewall

Se un centro di gestione FireSIGHT non è in grado di connettersi alla console cloud FireAMP o non riceve eventi malware, è necessario verificare se le porte richieste sono bloccate dal firewall. Un centro di gestione FireSIGHT utilizza la porta 443 per ricevere eventi malware basati su endpoint dalla console FireAMP. La porta 32137 è richiesta per le appliance FirePOWER per eseguire ricerche di malware nel Cisco Cloud.

Per ulteriori informazioni sui numeri di porta e sugli indirizzi server richiesti, consultare i seguenti documenti:

- Porte di comunicazione necessarie per il funzionamento del sistema FireSIGHT
- Server necessari per il funzionamento di AMP

# Indirizzo MAC in uso

## Sintomo

Quando si tenta di registrare un centro di gestione FireSIGHT in un cloud privato ed eseguire la connessione iniziale, è possibile che venga visualizzato un messaggio che indica che l'indirizzo MAC è già in uso.

## Motivo

Quando un centro di gestione FireSIGHT viene sostituito a causa di un guasto hardware e l'unità sostitutiva non viene correttamente annullata dal cloud, è possibile che si verifichi questo problema.

## Soluzione

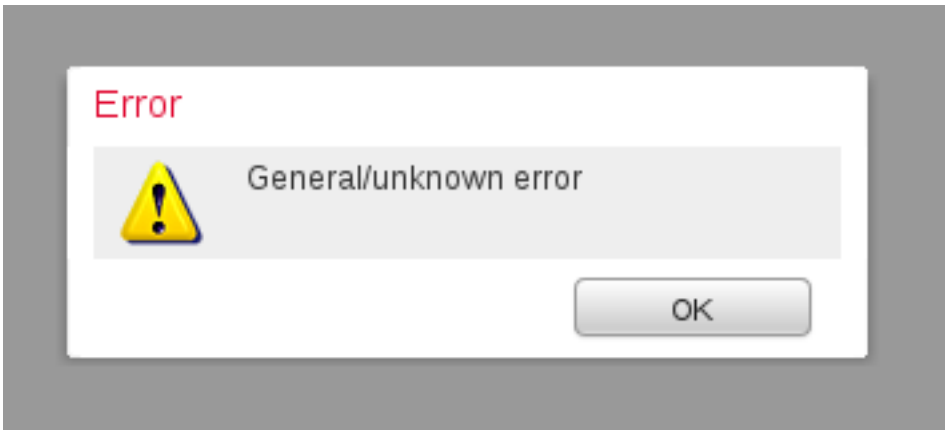
Prima di sostituire un accessorio, è necessario annullare la registrazione di FireSIGHT Management Center da FireAMP Cloud. È inoltre necessario rimuovere il centro di gestione FireSIGHT dal cloud FireAMP. In questo modo si evita che un indirizzo MAC venga percepito come in uso.

> **Suggerimento**: Leggere questo documento per informazioni dettagliate su come annullare la registrazione di un accessorio da FireAMP Cloud ed eliminare un cloud da FireSIGHT Management Center.

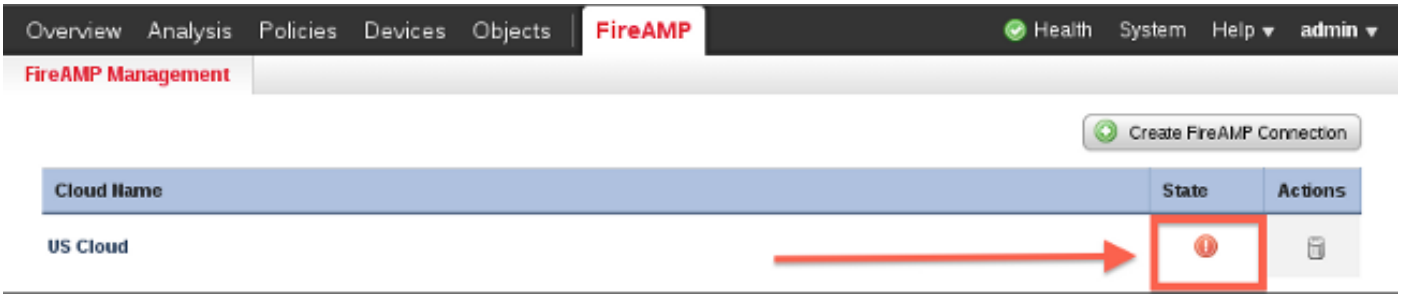
# Viene visualizzato l'errore generale/sconosciuto

## Sintomo

Quando si collega un centro di gestione FireSIGHT ricreato o sostitutivo a una console FireAMP, viene visualizzato un messaggio di errore. Viene visualizzato un errore generale/sconosciuto.




Quando viene visualizzato il messaggio di errore generale/sconosciuto, lo stato della connessione FireAMP su FireSIGHT Management Center diventa critico. L'interfaccia Web visualizza un'icona rossa.




### Motivo

Questo problema si verifica quando un indirizzo MAC di un centro di gestione FireSIGHT, appena ricreato o sostituito, è ancora registrato su una console FireAMP.

### Soluzione

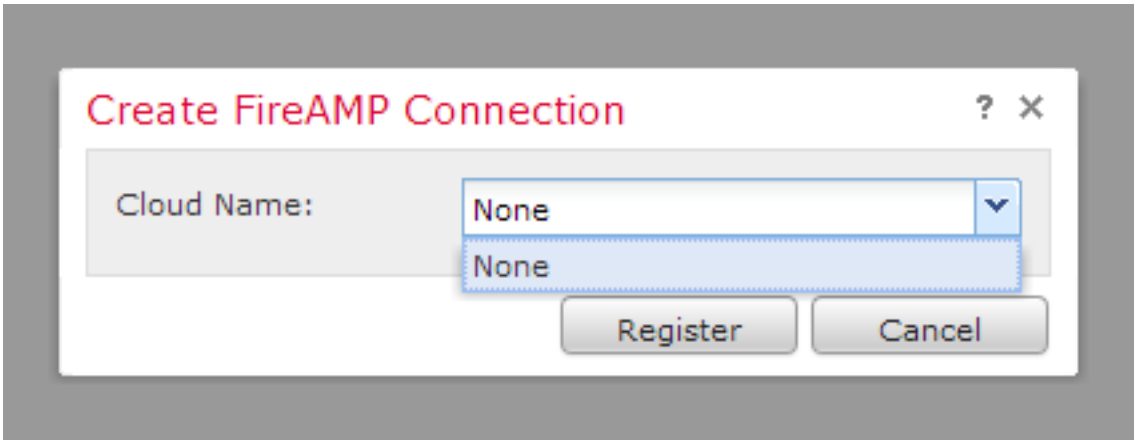
Prima di ricreare l'immagine o sostituire un accessorio, è necessario annullare la registrazione di FireSIGHT Management Center da FireAMP Cloud. È inoltre necessario rimuovere il centro di gestione FireSIGHT dal cloud FireAMP. In questo modo si evita che un indirizzo MAC venga percepito come in uso.

> **Suggerimento**: Leggere questo documento per informazioni dettagliate su come annullare la registrazione di un accessorio da FireAMP Cloud ed eliminare un cloud da FireSIGHT Management Center.

## Impossibile selezionare un cloud

### Sintomo

Quando si crea una connessione tra un centro di gestione FireSIGHT e la console cloud FireAMP, non sono disponibili opzioni di discesa per il cloud US o il cloud EU.




### Motivo

Questo problema si verifica quando un centro di gestione FireSIGHT non è in grado di risolvere il nome host api.amp.sourcefire.com.

Per verificare il problema, eseguire un nslookup sulla CLI del FireSIGHT Management Center.

Verificare che le impostazioni DNS siano configurate correttamente nel centro di gestione FireSIGHT:

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com
```

L'output seguente viene visualizzato quando il DNS non è in grado di risolvere il nome host nel centro di gestione FireSIGHT:

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com

Server:         192.168.45.2
Address:        192.168.45.2#53

** server can't find api.amp.sourcefire.com
```

Di seguito è riportato l'output se il DNS viene risolto correttamente nel centro di gestione FireSIGHT:

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com
Server:         192.168.45.1
Address:        192.168.45.1#53

Non-authoritative answer:
api.amp.sourcefire.com
Name:   xxxx.xxxx.xxxx
Address: xx.xx.xx.xx
```

## Soluzione

- Se un centro di gestione FireSIGHT non è in grado di risolvere il nome host, è necessario verificare che le impostazioni DNS nel centro di gestione siano corrette.
- Se un centro di gestione FireSIGHT è in grado di risolvere il nome host, ma non di accedere a api.amp.sourcefire.com attraverso un firewall, controllare le regole e le impostazioni del firewall.

Se durante il processo di creazione della connessione un centro di gestione FireSIGHT non è in grado di risolvere il nome host, nel file httpsd_error_log viene registrato il seguente messaggio di errore:

```
Error attempting curl for FireAMP: System
```

Ad esempio, il seguente output di log mostra che il Centro difesa non è riuscito a completare il comando curl in api.amp.sourcefire.com:

```
admin@Sourcefire3D:~$ tail -f /var/log/httpd/httpsd_error_log

[Thu Jul 18 12:38:13.433765 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
getCloudData start... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1778., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:38:14.338174 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --
sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H Accept:
```

```
application/vnd.sourcefire.fireamp.dc+json; version=1 https://api.amp.sourcefire.com/clouds at
/usr/local/sf/lib/perl/5.10.1/SF/System.pm line 7491., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352374 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
Error attempting curl for FireAMP: System (/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L
--max-redirs 5 --max-filesize 104857600 --sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H
Accept: application/vnd.sourcefire.fireamp.dc+json; version=1
https://api.amp.sourcefire.com/clouds) Failed at /usr/local/sf/lib/perl/5.10.1/SF/System.pm line
7499., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352432 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
No cloud data returned at /usr/local/sf/lib/perl/5.10.1/SF/FireAMP.pm line 145., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352478 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
getCloudData completed... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1780., referer:
https://192.168.45.45/ddd/
```

Durante il processo di creazione della connessione, se il seguente messaggio viene registrato nel log httpsd_error_log senza errori, FireSIGHT Management Center è in grado di risolvere il nome host:

```
getCloudData completed
```

L'output seguente, ad esempio, mostra che un centro di gestione completa un comando curl in api.amp.sourcefire.com:

```
admin@Sourcefire3D:~$ tail -f /var/log/httpd/httpsd_error_log

[Thu Jul 18 12:42:54.949461 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
getCloudData start... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1778., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:42:55.856432 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --
sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H Accept:
application/vnd.sourcefire.fireamp.dc+json; version=1 https://api.amp.sourcefire.com/clouds at
/usr/local/sf/lib/perl/5.10.1/SF/System.pm line 7491., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:42:55.931106 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
getCloudData completed... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1780., referer:
https://192.168.45.45/ddd/
```