Utilizzare la registrazione di FMC e FTD Smart License e i problemi comuni per risolvere i problemi

Sommario

Introduzione

In questo documento viene descritta la configurazione di registrazione della licenza intelligente di Firepower Management Center sui dispositivi gestiti da Firepower Threat Defense.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

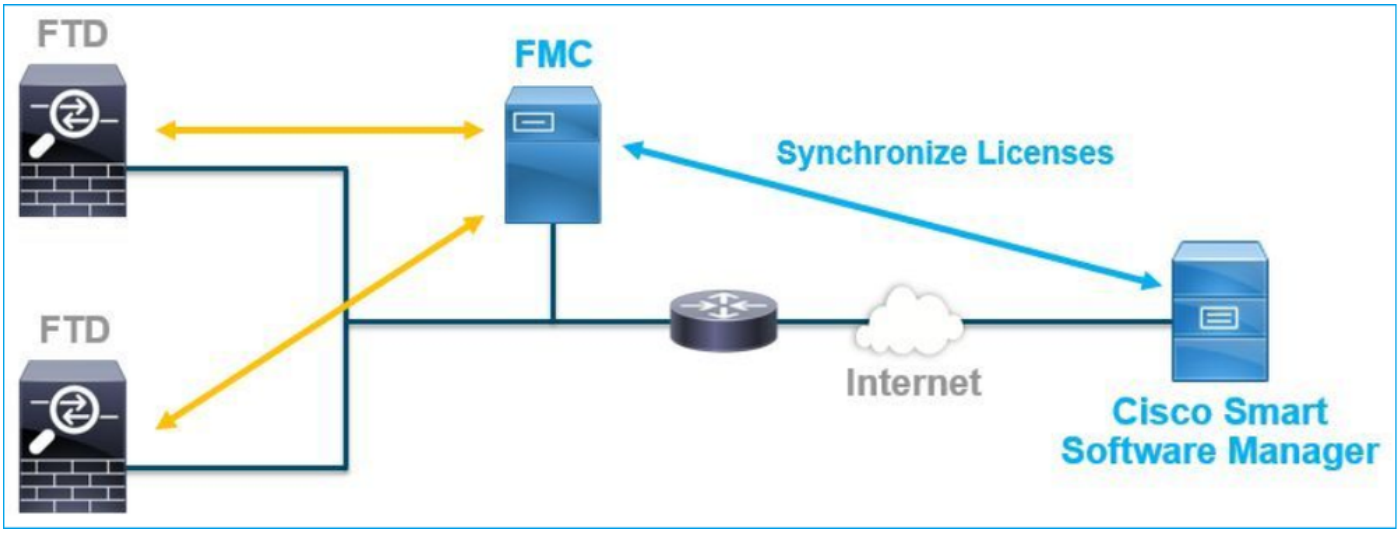
Componenti usati

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

Registrazione di FMC, FTD e Smart License.

La registrazione della Smart License viene eseguita su Firepower Management Center (FMC). Il FMC comunica con il portale Cisco Smart Software Manager (CSSM) via Internet. Nel modulo CSM, l'amministratore del firewall gestisce lo Smart Account e le relative licenze. Il FMC può assegnare ed eliminare liberamente le licenze ai dispositivi Firepower Threat Defense (FTD) gestiti. In altre parole, il FMC gestisce centralmente le licenze per i dispositivi FTD.



Per utilizzare alcune funzionalità dei dispositivi FTD è necessaria una licenza aggiuntiva. I tipi di licenza Smart che i clienti possono assegnare a un dispositivo FTD sono documentati in Tipi di licenza FTD e limitazioni.

La licenza Base è inclusa nel dispositivo FTD. Questa licenza viene registrata automaticamente nello Smart Account quando il CMC viene registrato nel modulo CSM.
Le licenze basate sulla durata: minacce, malware e filtro URL sono facoltativi. Per utilizzare le funzionalità relative a una licenza, è necessario assegnare una licenza al dispositivo FTD.

Per utilizzare una licenza virtuale di Firepower Management Center (FMCv) per la gestione FTD, è

necessaria anche una licenza per dispositivo Firepower MCv in CSSM.

La licenza FMCv è inclusa nel software ed è perpetua.

Inoltre, il documento illustra alcuni scenari per la risoluzione dei problemi più comuni che possono verificarsi durante la registrazione della licenza.

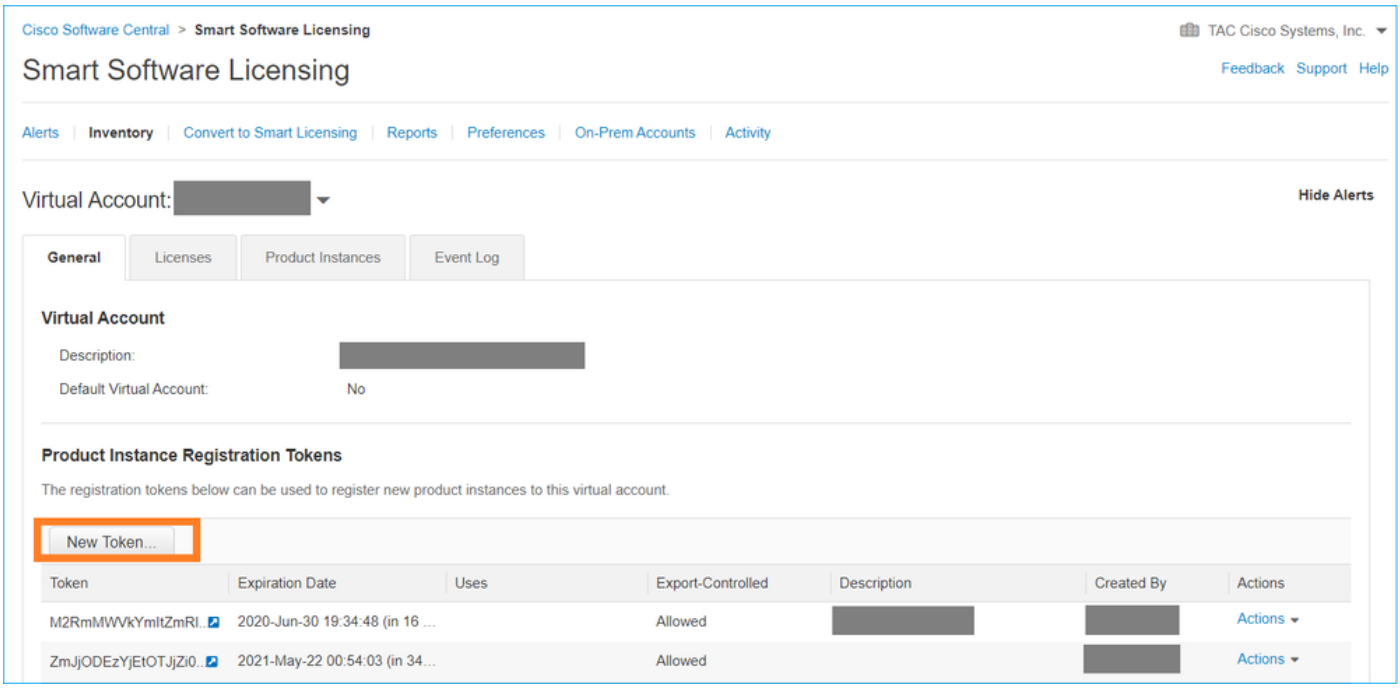
Per ulteriori informazioni sulle licenze, vedere Cisco Firepower System Feature Licenses e Domande frequenti (FAQ) sulle licenze Firepower.

Registrazione delle licenze Smart di FMC

Prerequisiti

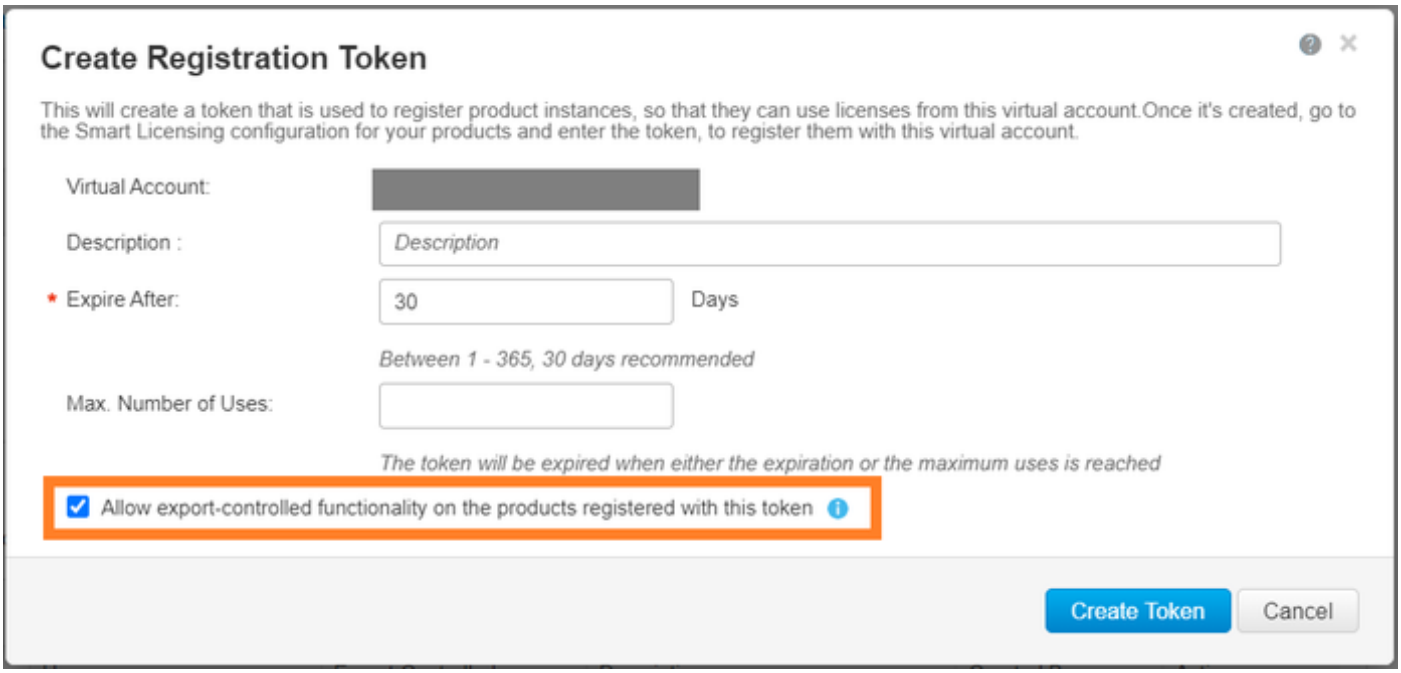
1. Per la registrazione della licenza Smart, il CCP deve accedere a Internet. Poiché il certificato viene scambiato tra FMC e Smart License Cloud con HTTPS, verificare che nel percorso non sia presente alcun dispositivo in grado di influire sulla comunicazione o modificarla. (ad esempio, Firewall, Proxy, dispositivo di decrittografia SSL e così via).

2. Accedere al modulo CSM ed emettere un ID token da Inventory > General > New Token button, come mostrato in questa immagine.



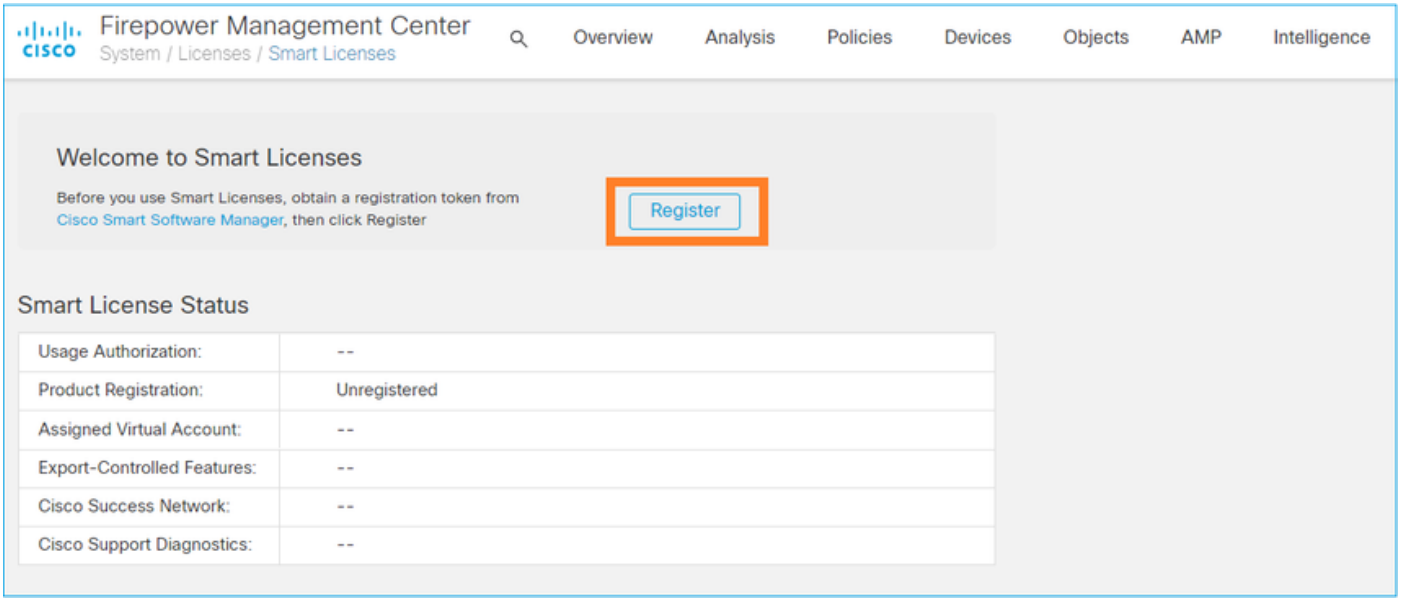
Per utilizzare la crittografia avanzata, abilitare l'opzione Consenti funzionalità di controllo dell'esportazione sui prodotti registrati con questo token. Quando è attivata, nella casella di controllo viene visualizzato un segno di spunta.

3. Selezionare Crea token.

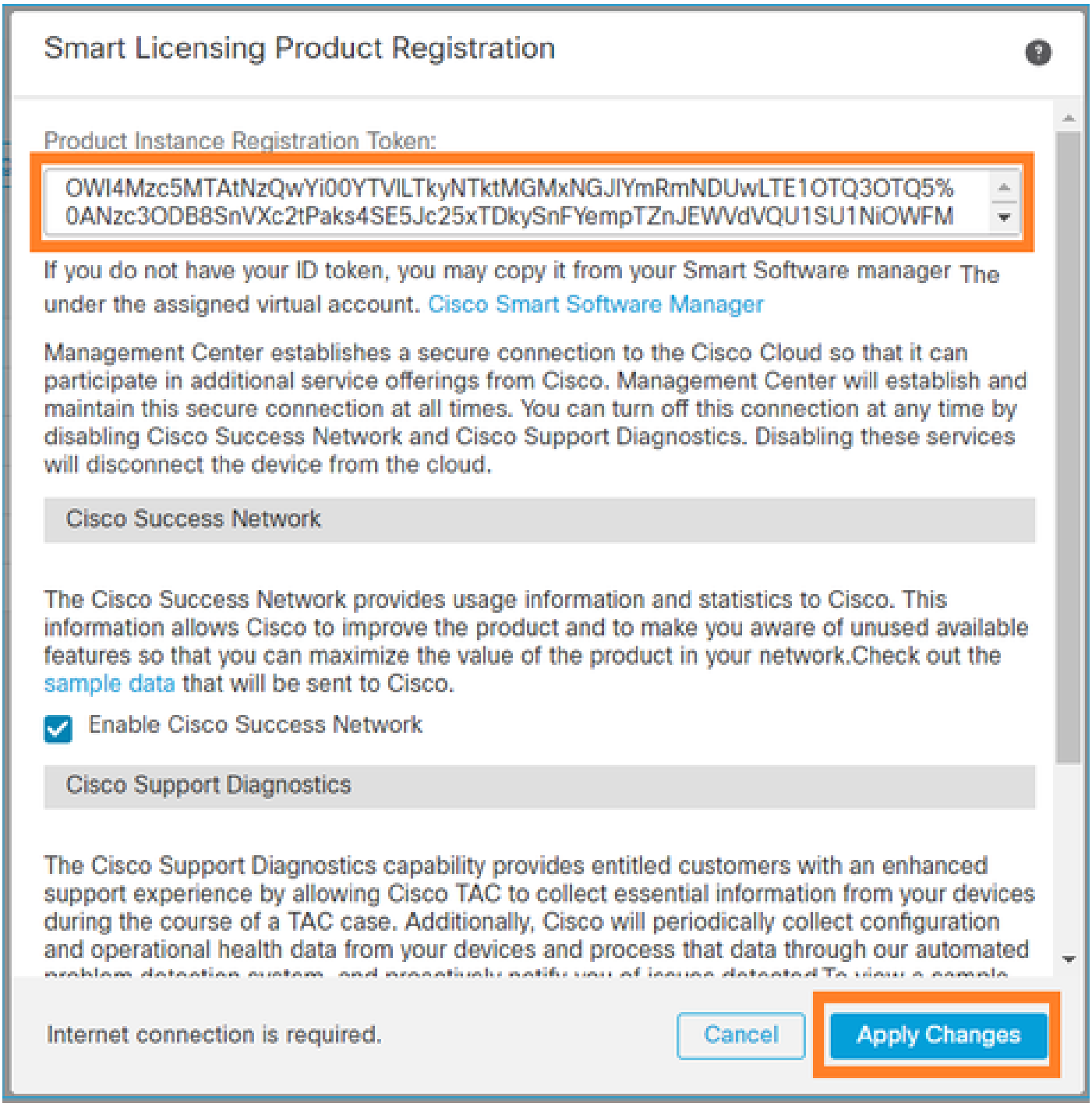


Registrazione delle licenze Smart di FMC

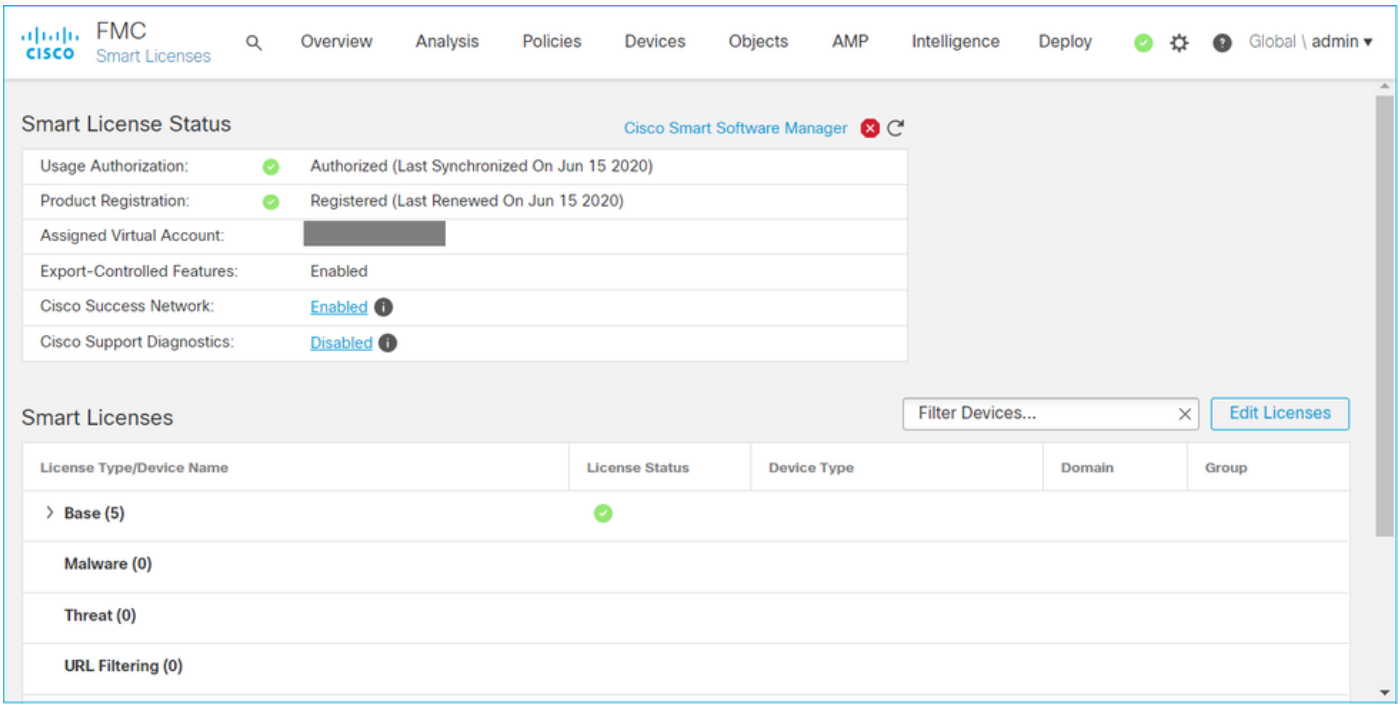
Passare a Sistema > Licenze > Licenze Smart nel FMC e selezionare il pulsante Registra, come mostrato nell'immagine.



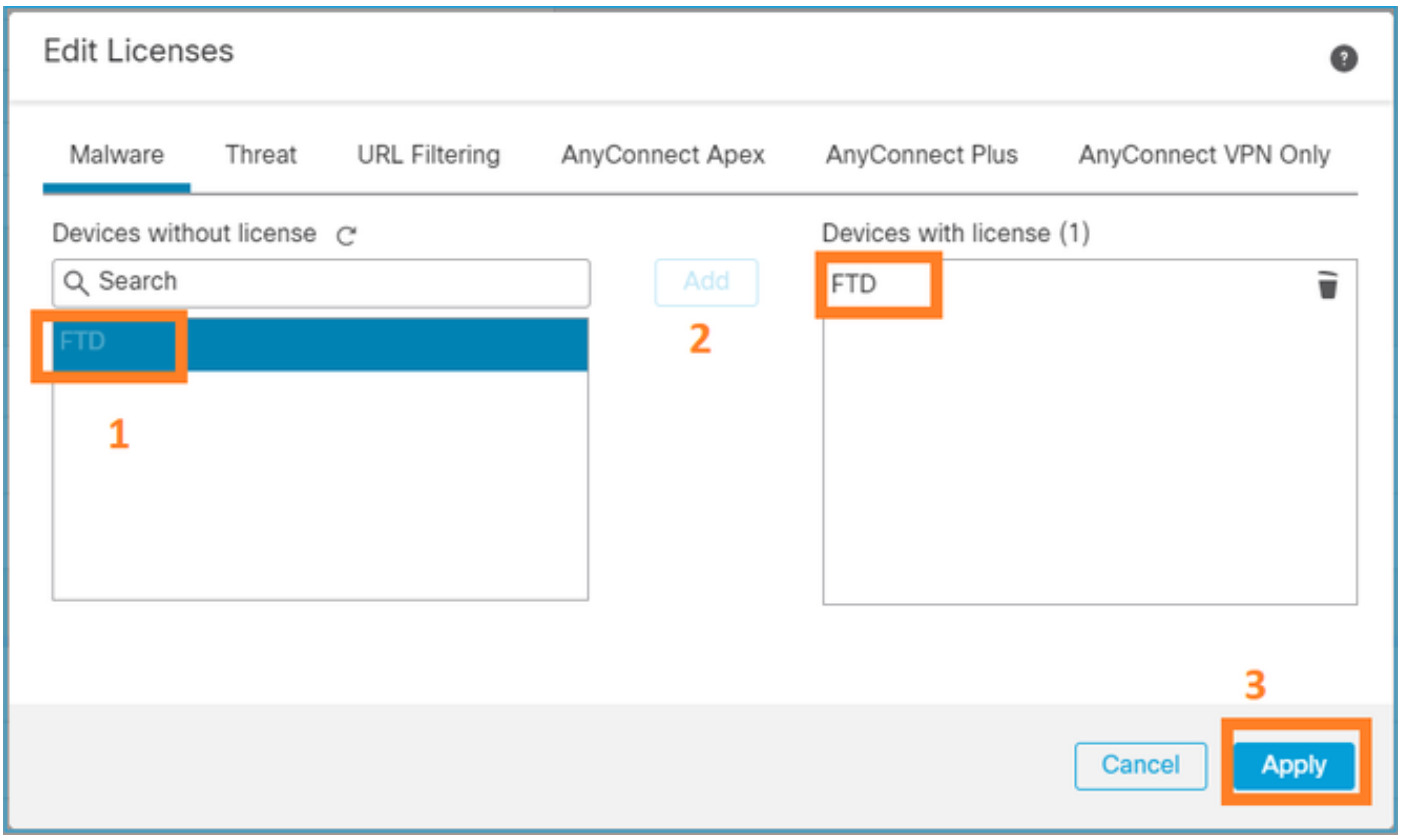
Immettere l'ID token nella finestra di registrazione del prodotto Smart Licensing e selezionare Apply Changes (Applica modifiche), come mostrato nell'immagine.



Se la registrazione della Smart License ha avuto esito positivo, lo stato di registrazione del prodotto viene indicato come Registrato, come mostrato in questa immagine.

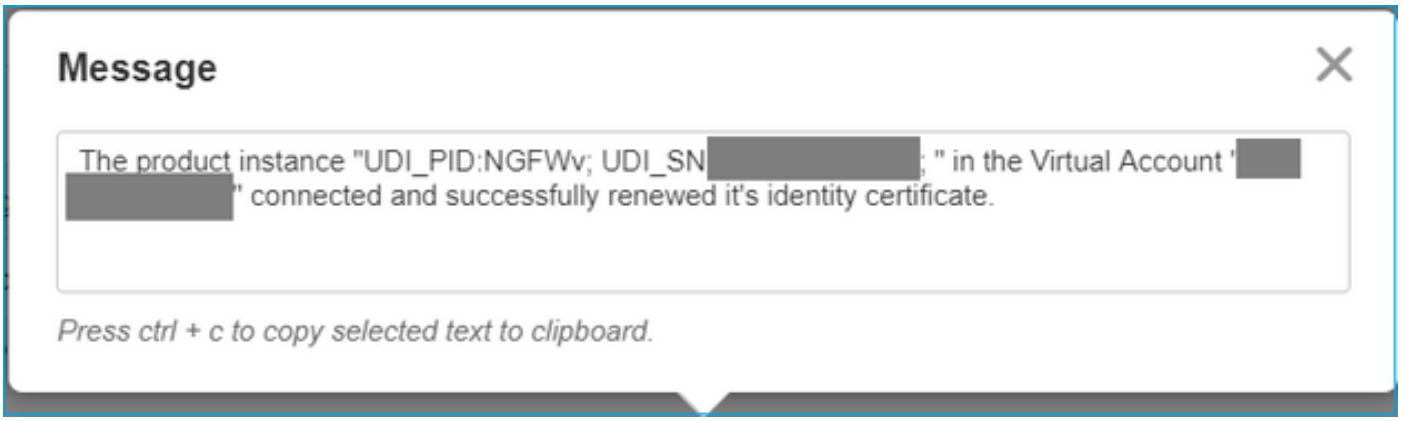


Per assegnare una licenza basata sulla durata al dispositivo FTD, selezionare Modifica licenze. Quindi selezionare e aggiungere un dispositivo gestito alla sezione Dispositivi con licenza. Infine, selezionare il pulsante Applica come mostrato nell'immagine.



Conferma in Smart Software Manager (SSM) Side

Il successo della registrazione della licenza Smart License FMC può essere confermato da Inventario > Registro eventi in CSSM, come mostrato in questa immagine.

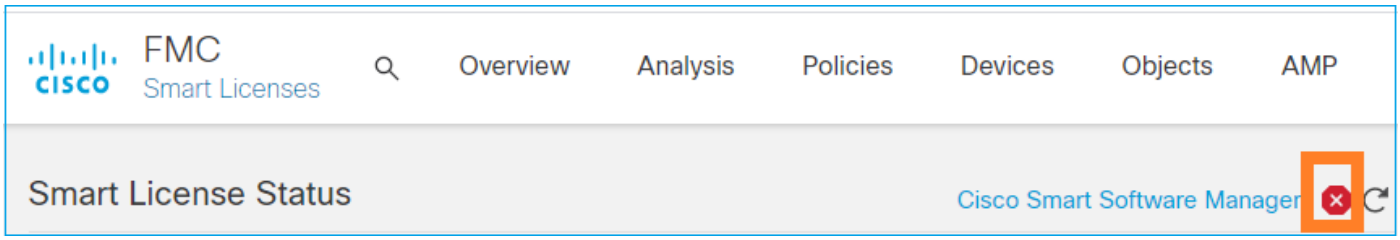


Lo stato di registrazione del CCP può essere confermato da Inventario > Istanze prodotto. Controllare il registro eventi dalla scheda Registro eventi. È possibile controllare lo stato della registrazione e dell'uso delle licenze nella scheda Inventario > Licenze. Verificare che la licenza basata sulla durata acquistata sia utilizzata correttamente e che non siano presenti avvisi che indicano un numero di licenze insufficiente.

Annullamento della registrazione della licenza Smart di FMC

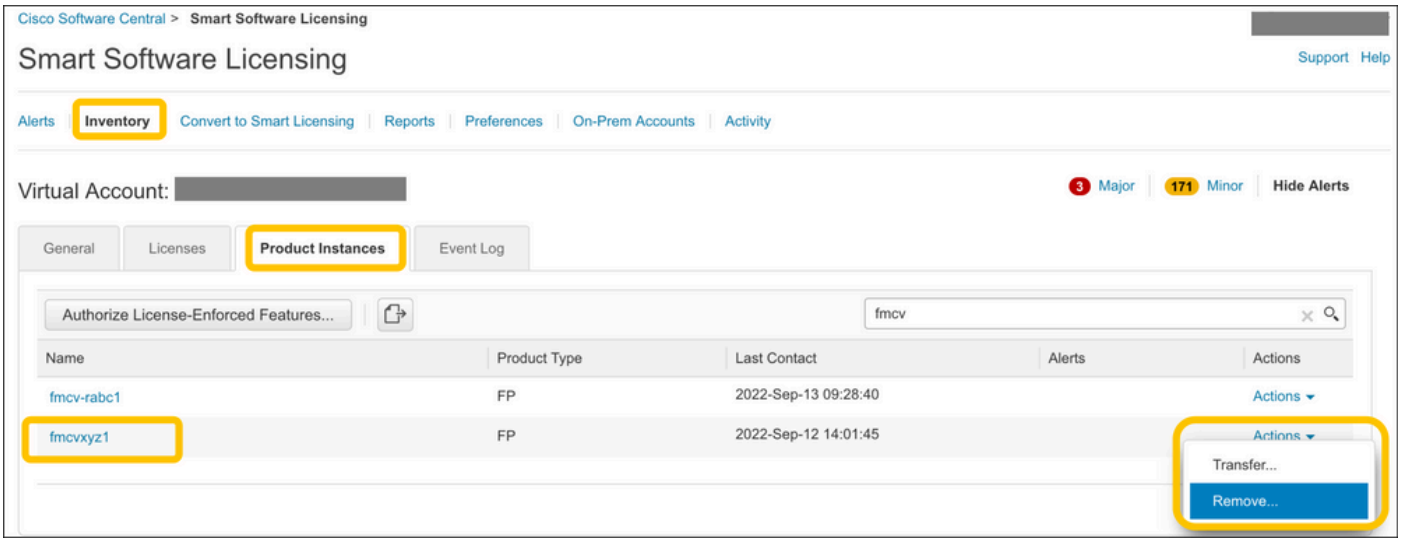
Annulla la registrazione del CCP dal Cisco SSM

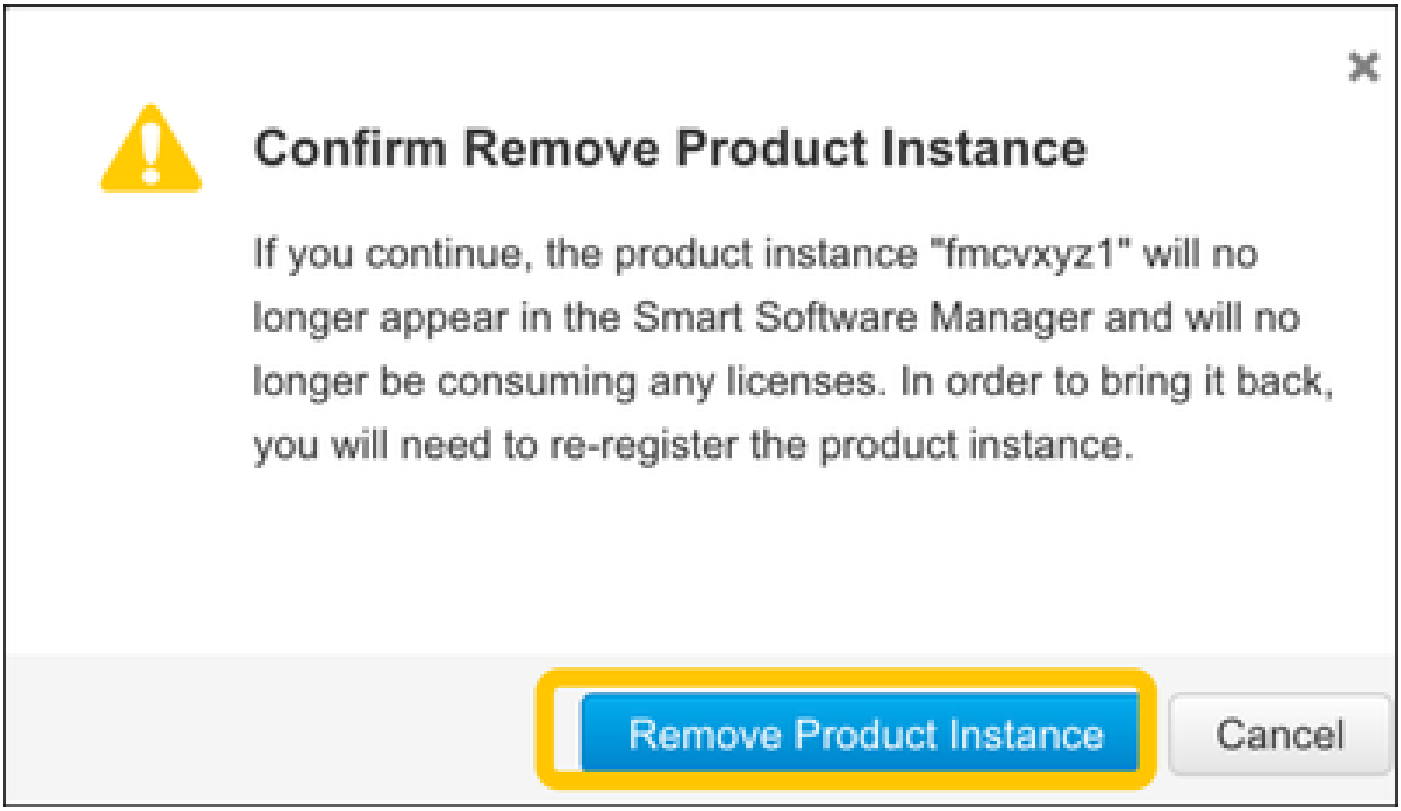
Per rilasciare la licenza o usare un token diverso, selezionare Sistema > Licenze > Smart Licenses e selezionare il pulsante di annullamento della registrazione, come mostrato nell'immagine.



Rimuovi registrazione dal lato SSM

Accedere a Smart Software Manager (Cisco Smart Software Manager) e da Inventario > Istanze prodotto, selezionare Rimuovi sul FMC di destinazione. Quindi selezionare Remove Product Instance (Rimuovi istanza prodotto) per rimuovere il FMC e rilasciare le licenze allocate, come mostrato nell'immagine.





RMA

Se il CCP è protetto da RMA, annullare la registrazione del CCP da Cisco Smart Software Manager (CSSM) seguendo la procedura descritta nella sezione Registrazione della licenza Smart del CCP > Rimuovi registrazione dal lato SSM e quindi registrare nuovamente il CMC con il CSM seguendo la procedura descritta nella sezione Registrazione della licenza Smart del CCP.

Risoluzione dei problemi

Verifica sincronizzazione ora

Accedere alla CLI della FMC (ad esempio, SSH) e verificare che l'ora sia corretta e che sia sincronizzata con un server NTP attendibile. Poiché il certificato viene utilizzato per l'autenticazione Smart License, è importante che il FMC disponga delle informazioni corrette sull'ora:

```
<#root>

admin@FMC:~$

date
Thu

 Jun 14 09:18:47 UTC 2020
admin@FMC:~$
admin@FMC:~$

ntpq -pn

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.0.0.2        171.68.xx.xx     2 u  387 1024  377    0.977    0.469   0.916
 127.127.1.1     .SFCL.          13 l    -   64    0    0.000    0.000   0.000
```

Dall'interfaccia utente di FMC, verificare i valori del server NTP selezionando Sistema > Configurazione > Sincronizzazione ora.

Abilitare la risoluzione dei nomi e verificare la raggiungibilità in tools.cisco.com

Verificare che il CCP sia in grado di risolvere un FQDN e che sia raggiungibile all'indirizzo tools.cisco.com:

```
<#root>

>

expert
admin@FMC2000-2:~$


sudo su

Password:
root@FMC2000-2:/Volume/home/admin# ping tools.cisco.com
PING tools.cisco.com (173.37.145.8) 56(84) bytes of data.
64 bytes from tools2.cisco.com (173.37.145.8): icmp_req=1 ttl=237 time=163 ms
64 bytes from tools2.cisco.com (173.37.145.8): icmp_req=2 ttl=237 time=163 ms
```

Dall'interfaccia utente di FMC, verificare l'IP di gestione e l'IP del server DNS da System > Configuration > Management Interfaces (Sistema > Configurazione > Interfacce di gestione).

Verificare l'accesso HTTPS (TCP 443) da FMC a tools.cisco.com

Utilizzare il comando Telnet o curl per assicurarsi che FMC disponga dell'accesso HTTPS a tools.cisco.com. Se la comunicazione TCP 443 è interrotta, verificare che non sia bloccata da un firewall e che il percorso non contenga un dispositivo di decrittografia SSL.

<#root>

```
root@FMC2000-2:/Volume/home/admin#

 telnet tools.cisco.com 443

Trying 72.163.4.38...

Connected to tools.cisco.com.

Escape character is '^]'.
^CConnection closed by foreign host.

 <--- Press Ctrl+C
```

Prova di ricciolo:

<#root>

```
root@FMC2000-2:/Volume/home/admin#

curl -vvk https://tools.cisco.com

*

Trying 72.163.4.38...

* TCP_NODELAY set

* Connected to tools.cisco.com (72.163.4.38) port 443 (#0)

* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: none
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: C=US; ST=CA; L=San Jose; O=Cisco Systems, Inc.; CN=tools.cisco.com
*  start date: Sep 17 04:00:58 2018 GMT
*  expire date: Sep 17 04:10:00 2020 GMT
*  issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL ICA G2
*  SSL certificate verify ok.
> GET / HTTP/1.1
```

```
> Host: tools.cisco.com
> User-Agent: curl/7.62.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Wed, 17 Jun 2020 10:28:31 GMT
< Last-Modified: Thu, 20 Dec 2012 23:46:09 GMT
< ETag: "39b01e46-151-4d15155dd459d"
< Accept-Ranges: bytes
< Content-Length: 337
< Access-Control-Allow-Credentials: true
< Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
< Access-Control-Allow-Headers: Content-type, fromPartyID, inputFormat, outputFormat, Authorization, Co
< Content-Type: text/html
< Set-Cookie: CP_GUTC=10.163.4.54.1592389711389899; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT; domain=
< Set-Cookie: CP_GUTC=10.163.44.92.1592389711391532; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT; domai
< Cache-Control: max-age=0
< Expires: Wed, 17 Jun 2020 10:28:31 GMT
<
<html>
<head>
<script language="JavaScript">

var input = document.URL.indexOf('intellishield');
if(input != -1) {
 window.location="https://intellishield.cisco.com/security/alertmanager/";
}
else {
 window.location="http://www.cisco.com";
};

</script>
</head>

<body>
<a href="http://www.cisco.com">www.cisco.com</a>
</body>
</html>
* Connection #0 to host tools.cisco.com left intact
root@FMC2000-2:/Volume/home/admin#
```

Verifica DNS

Verificare la corretta risoluzione in tools.cisco.com:

<#root>

```
root@FMC2000-2:/Volume/home/admin#

nslookup tools.cisco.com

Server:         192.0.2.100
Address:        192.0.2.100#53

Non-authoritative answer:

Name:   tools.cisco.com
Address: 72.163.4.38
```

Verifica proxy

Se si utilizza apProxy, controllare i valori sia sul FMC che sul server proxy. Nel CCP verificare che il CCP utilizzi l'indirizzo IP e la porta corretti del server proxy.

<#root>

root@FMC2000-2:/Volume/home/admin#

cat /etc/sf/smart_callhome.conf

KEEP_SYNC_ACTIVE:1
PROXY_DST_URL:https://tools.cisco.com/its/service/oddce/services/DDCEService

PROXY_SRV:192.0.xx.xx

PROXY_PORT:80

Nell'interfaccia utente di FMC, i valori proxy possono essere confermati da Sistema > Configurazione > Interfacce di gestione.

Se i valori sul lato FMC sono corretti, controllare i valori sul lato server proxy (ad esempio, se il server proxy consente l'accesso dal FMC e visitare il sito tools.cisco.com). Consente inoltre lo scambio di traffico e certificati tramite il proxy. Il CCP utilizza un certificato per la registrazione della licenza intelligente).

ID token scaduto

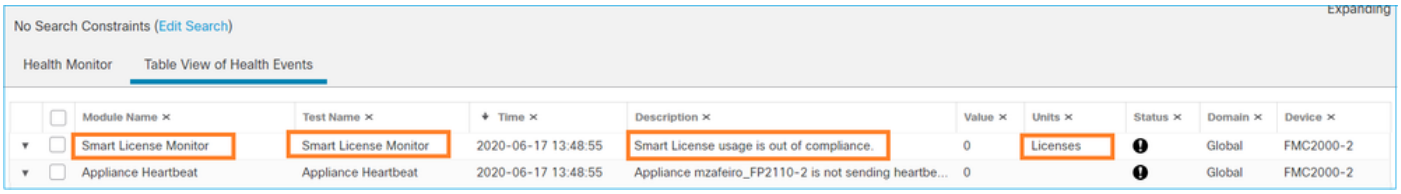
Verificare che l'ID token rilasciato non sia scaduto. Se è scaduta, chiedere all'amministratore di Smart Software Manager di rilasciare un nuovo token e registrare nuovamente la licenza Smart con il nuovo Token ID.

Cambiare il gateway FMC

In alcuni casi, l'autenticazione Smart License non può essere eseguita correttamente a causa degli effetti di un proxy di inoltro o di un dispositivo di decrittografia SSL. Se possibile, modificare il percorso per l'accesso a Internet da FMC in modo da evitare tali dispositivi, quindi riprovare la registrazione della Smart License.

Controllare gli eventi sanitari su FMC

Dal FMC, selezionare Sistema > Stato > Eventi e verificare lo stato del modulo Smart License Monitor per individuare eventuali errori. Ad esempio, se la connessione non riesce a causa di un certificato scaduto, viene generato un errore, come ID certificato scaduto, come mostrato in questa immagine.



Controllare il registro eventi sul lato SSM

Se il CCP è in grado di connettersi al CSM, controllare il registro eventi della connettività in Inventario > Registro eventi. Verificare se nel CSM sono presenti registri eventi o registri errori di questo tipo. Se i valori/il funzionamento del sito del CCP non presentano problemi e non esiste un registro eventi sul lato del CSM, è possibile che si tratti di un problema relativo al percorso tra il CCP e il CSM.

Problemi comuni

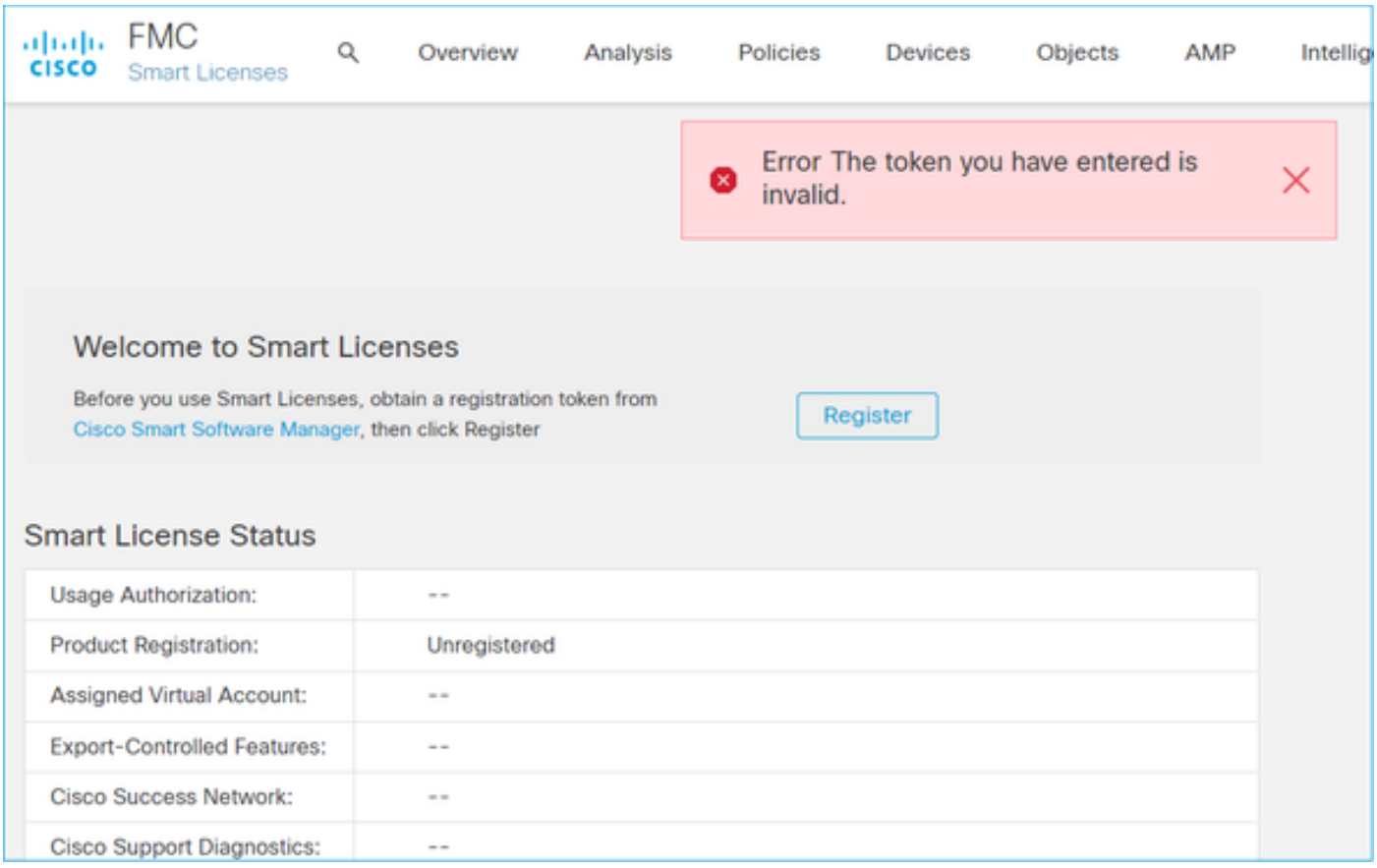
Sintesi degli Stati di registrazione e autorizzazione:

Stato registrazione prodotto	Stato autorizzazione utilizzo	Commenti
UNREGISTERED	—	Il CCP non è né registrato né in modalità di valutazione. Questo è lo stato iniziale dopo l'installazione di FMC o dopo la scadenza della licenza di valutazione per 90 giorni.
Registrato	Autorizzato	Il FMC è registrato in Cisco Smart Software Manager (CSSM) e alcuni dispositivi FTD sono registrati con un abbonamento valido.
Registrato	Autorizzazione scaduta	Il FMC non è stato in grado di comunicare con il back-end delle licenze Cisco per più di 90 giorni.
Registrato	UNREGISTERED	Il FMC è registrato in Cisco Smart Software Manager (CSSM), ma non sono presenti dispositivi FTD registrati nel FMC.
Registrato	Non conformità	Il FMC è registrato in Cisco Smart Software Manager (CSSM), ma sono presenti dispositivi FTD registrati con uno o più abbonamenti non validi.

		Ad esempio, un dispositivo FTD (FP4112) utilizza un abbonamento THREAT, ma con Cisco Smart Software Manager (CSSM) non sono disponibili abbonamenti THREAT per FP4112.
Valutazione (90 giorni)	N/D	Il periodo di valutazione è in uso, ma non vi sono dispositivi FTD registrati nel CCP.

Studio del caso 1. Token non valido

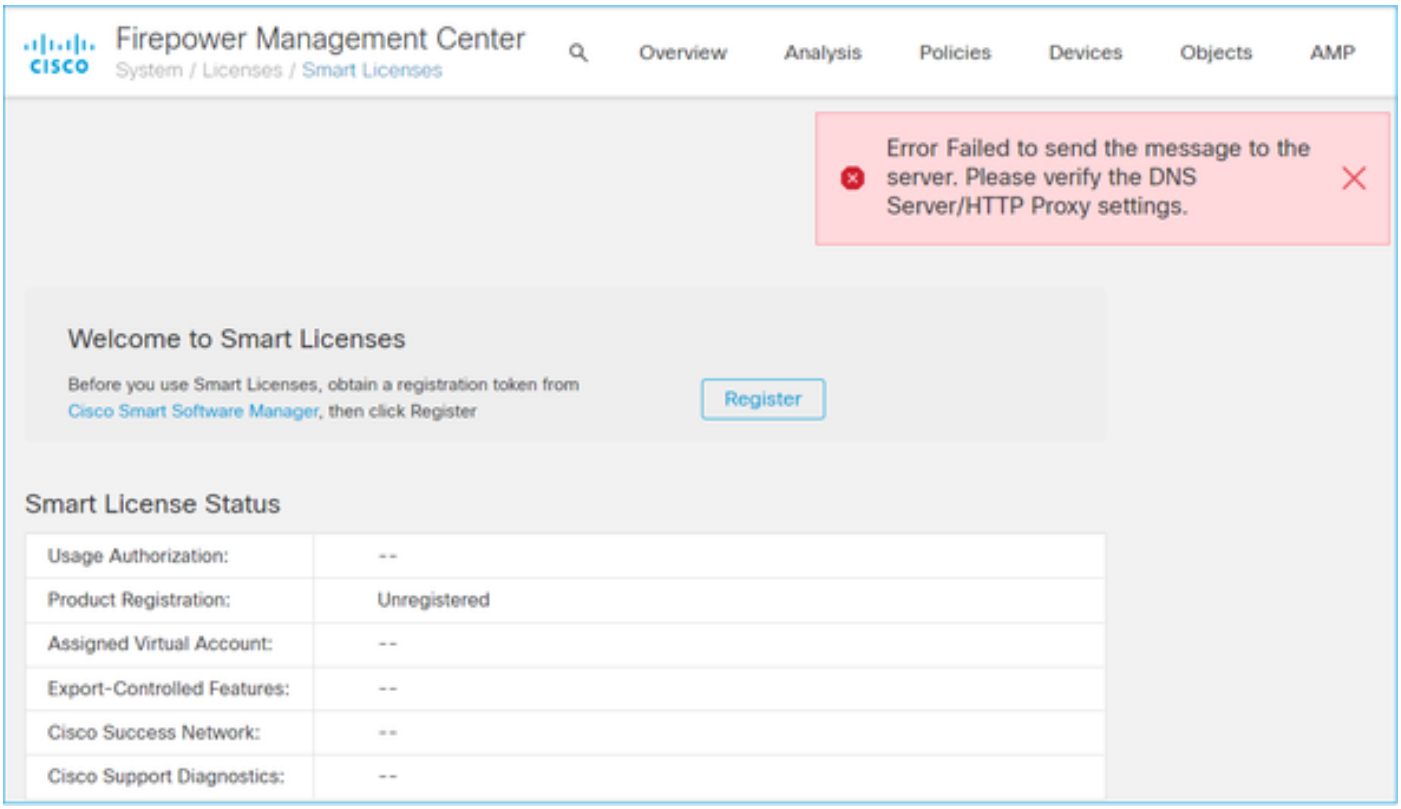
Sintomo: la registrazione al modulo CSM non riesce rapidamente (~10s) a causa di un token non valido, come mostrato in questa immagine.



Risoluzione: utilizzare un token valido.

Studio del caso 2. DNS non valido

Sintomo: la registrazione al modulo CSM non è riuscita dopo un po' (~25s), come mostrato in questa immagine.



Controllare il file /var/log/process_stdout.log. Il problema relativo al DNS è stato rilevato:

<#root>

```
root@FMC2000-2:/Volume/home/admin#
```

cat /var/log/process_stdout.log

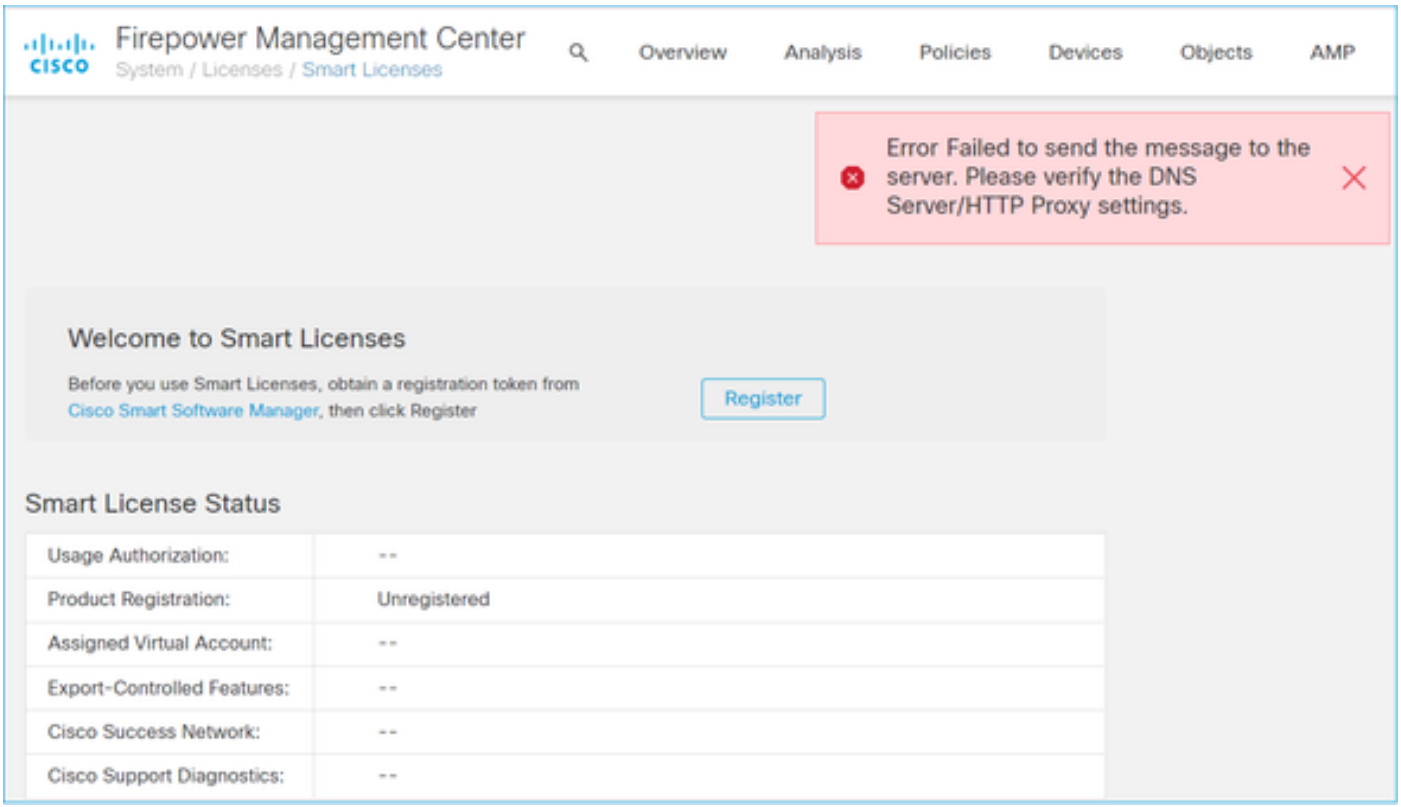
```
2020-06-25 09:05:21 sla[24043]: *Thu Jun 25 09:05:10.989 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[494],
failed to perform, err code 6, err string
```

"Couldn't resolve host name"

Risoluzione: errore di risoluzione del nome host CSM. La risoluzione consiste nel configurare il DNS, se non è stato configurato, o nel risolvere i problemi relativi al DNS.

Studio del caso 3. Valori di ora non validi

Sintomo: la registrazione al modulo CSM non è riuscita dopo un po' (~25s), come mostrato in questa immagine.



Controllare il file /var/log/process_stdout.log. I problemi relativi ai certificati sono:

<#root>

```
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_request_init[59]
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_post_prepare[299
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_post_prepare[302
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_head_init[110],
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[494],
```

failed to perform, err code 60, err string "SSL peer certificate or SSH remote key was not OK"

```
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_http_unlock[330], unl
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_send_http[365], send
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_curl_is_cert_issue[51
```

cert issue checking, ret 60, url https://tools.cisco.com/its/service/oddce/services/DDCEService

Controllare il valore temporale FMC:

<#root>

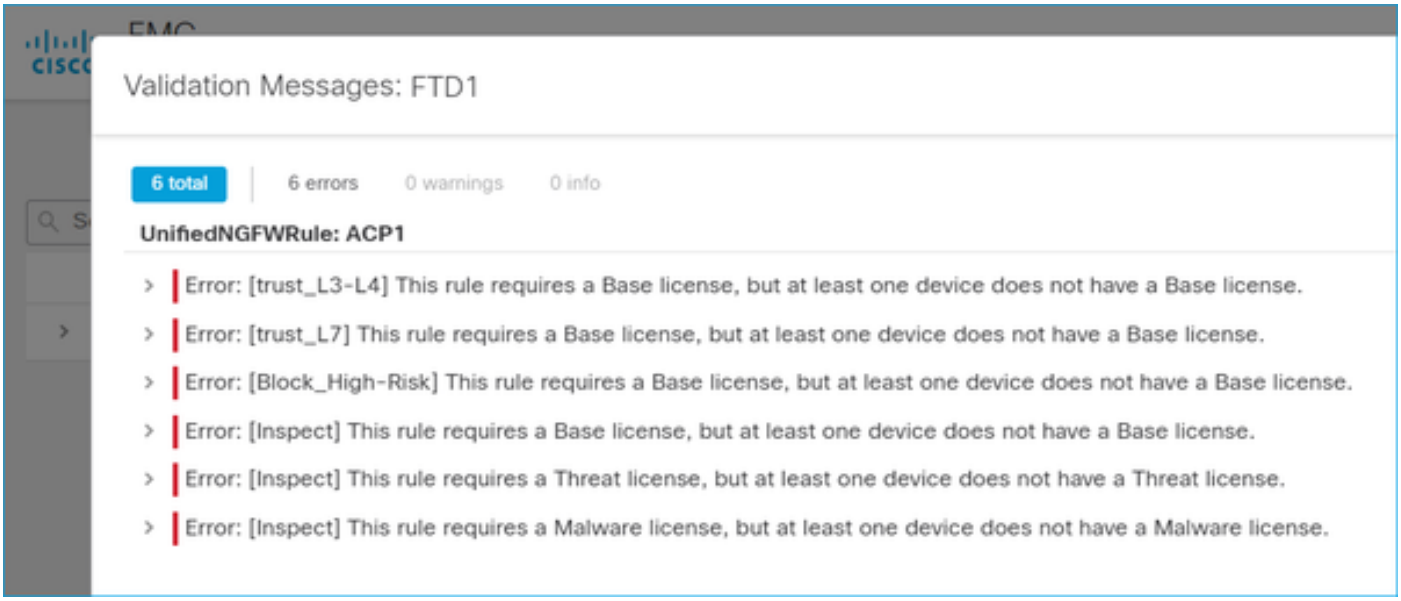
```
root@FMC2000-2:/Volume/home/admin#
```

date

```
Fri Jun 25 09:27:22 UTC 2021
```

Case study 4. Nessuna sottoscrizione

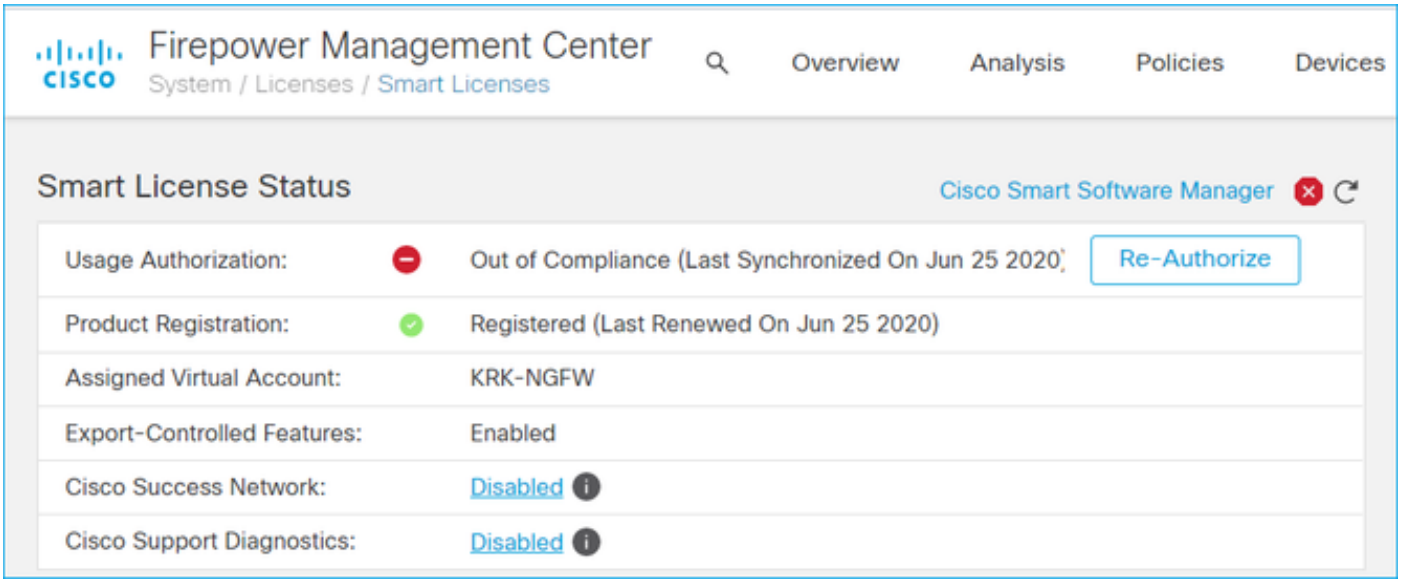
Se non è disponibile una sottoscrizione di licenza per una funzionalità specifica, la distribuzione di FMC non è possibile:



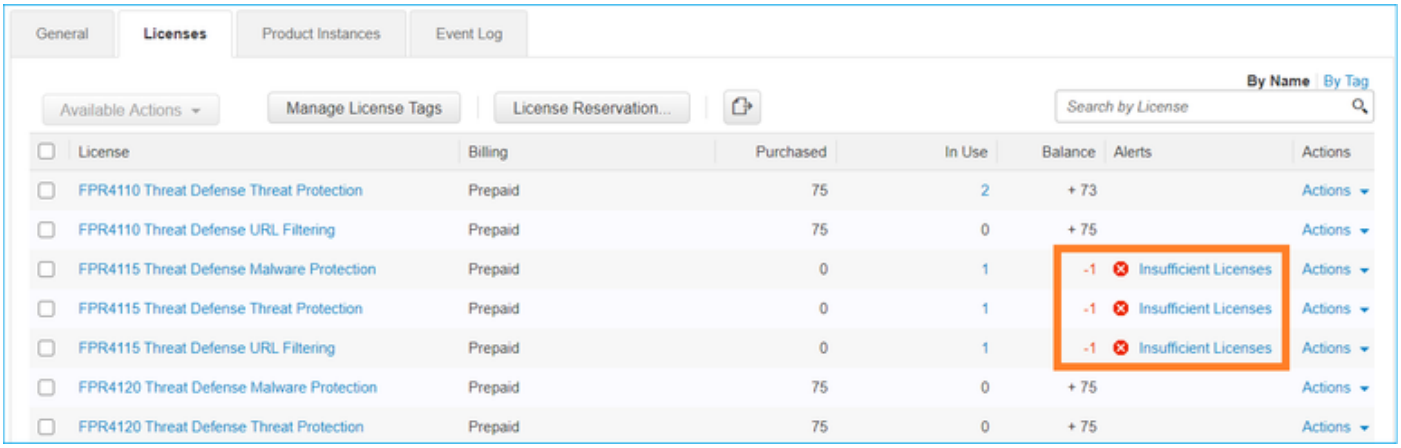
Risoluzione: è necessario acquistare e applicare la sottoscrizione richiesta al dispositivo.

Studio del caso 5. Non conformità (OOC)

Se non esiste alcun diritto per le sottoscrizioni FTD, la Smart License di FMC passa allo stato di non conformità (OOC):

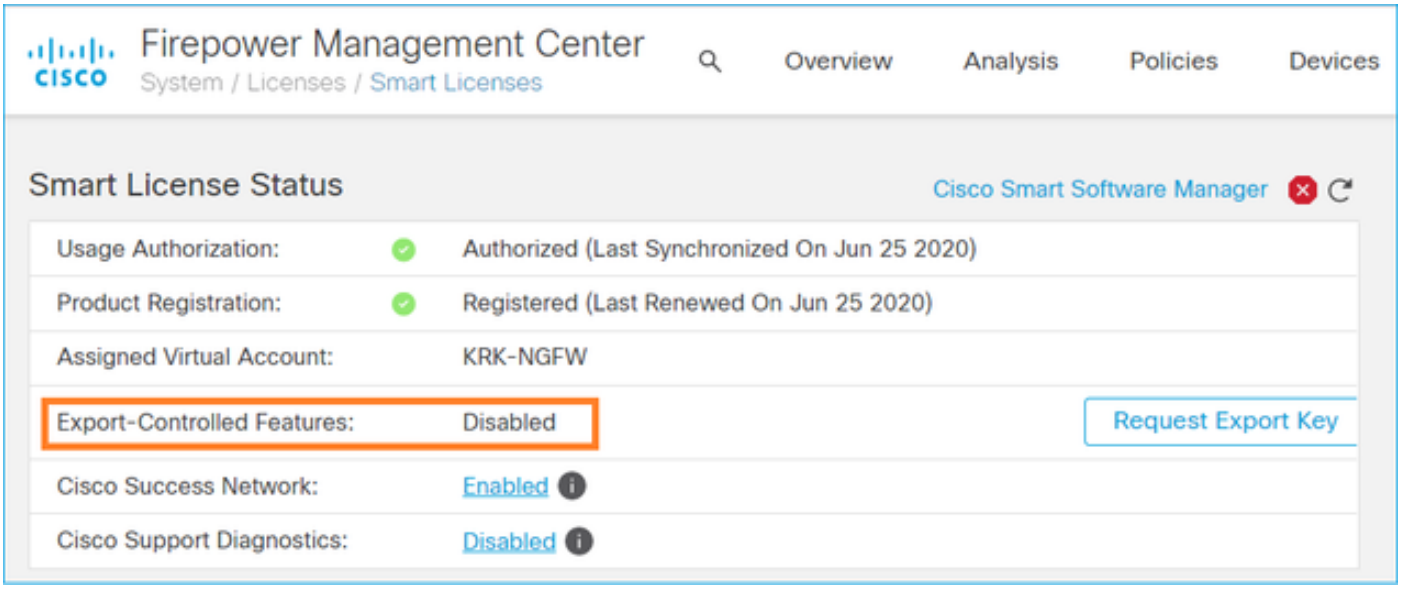


Nel CSSM, controllare gli avvisi per gli errori:



Case study 6. Nessuna crittografia avanzata

Se viene utilizzata solo la licenza di base, la crittografia DES (Data Encryption Standard) è abilitata nel motore LINA FTD. In questo caso, le installazioni come VPN (Virtual Private Network) L2L con algoritmi più avanzati hanno esito negativo:



Risoluzione: registrare la console Gestione risorse di sistema (CSM) e abilitare un attributo Crittografia avanzata.

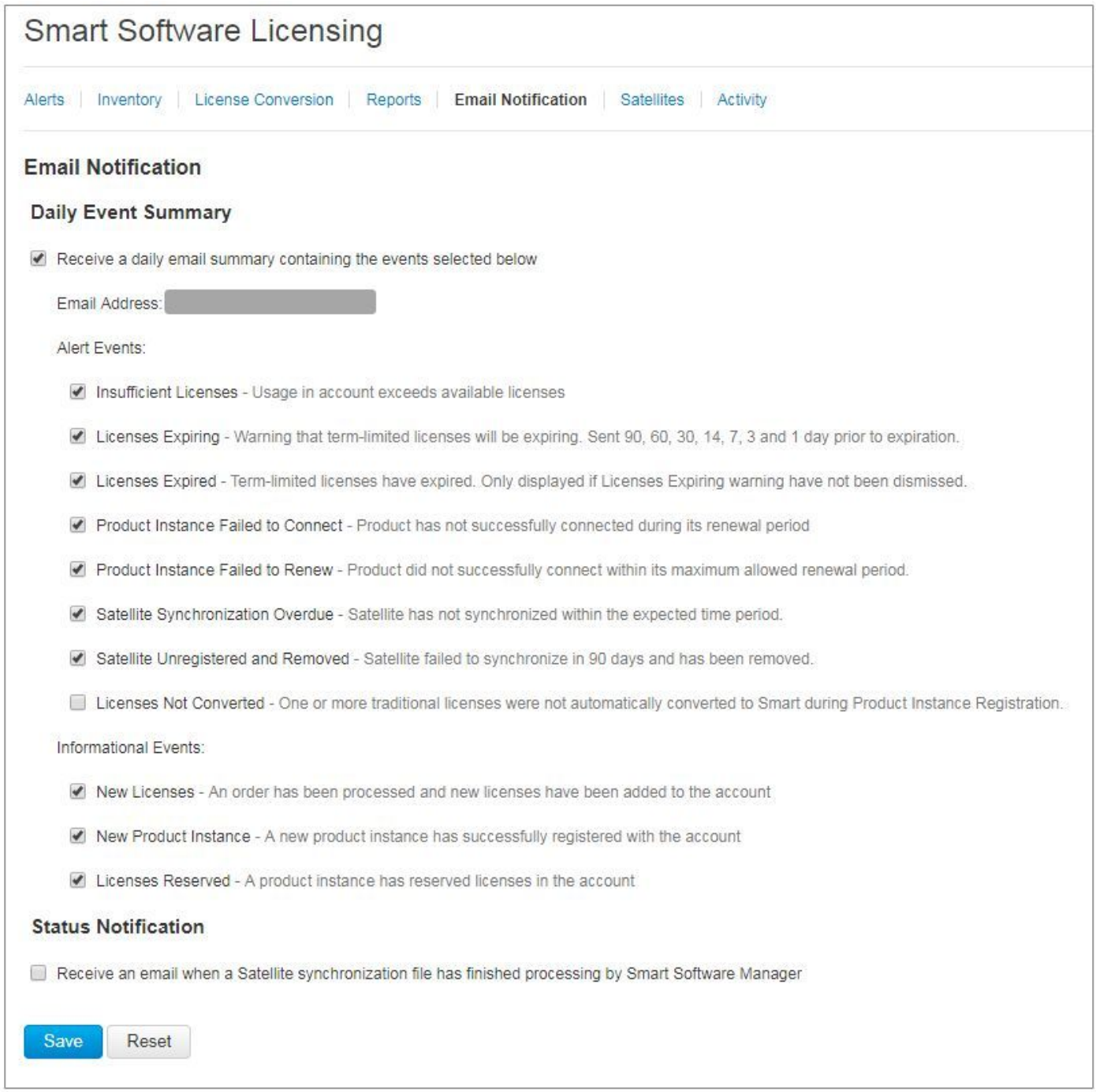
Note aggiuntive

Imposta notifica dello stato della licenza intelligente

Notifica e-mail da SSM

Sul lato SSM, Notifica e-mail SSM consente la ricezione di e-mail di riepilogo per vari eventi. Ad esempio, notifica per mancanza di licenza o per licenze che stanno per scadere. È possibile ricevere notifiche relative alla connessione dell'istanza del prodotto o all'errore di aggiornamento.

Questa funzione è molto utile per notare e prevenire il verificarsi di restrizioni funzionali dovute alla scadenza della licenza.

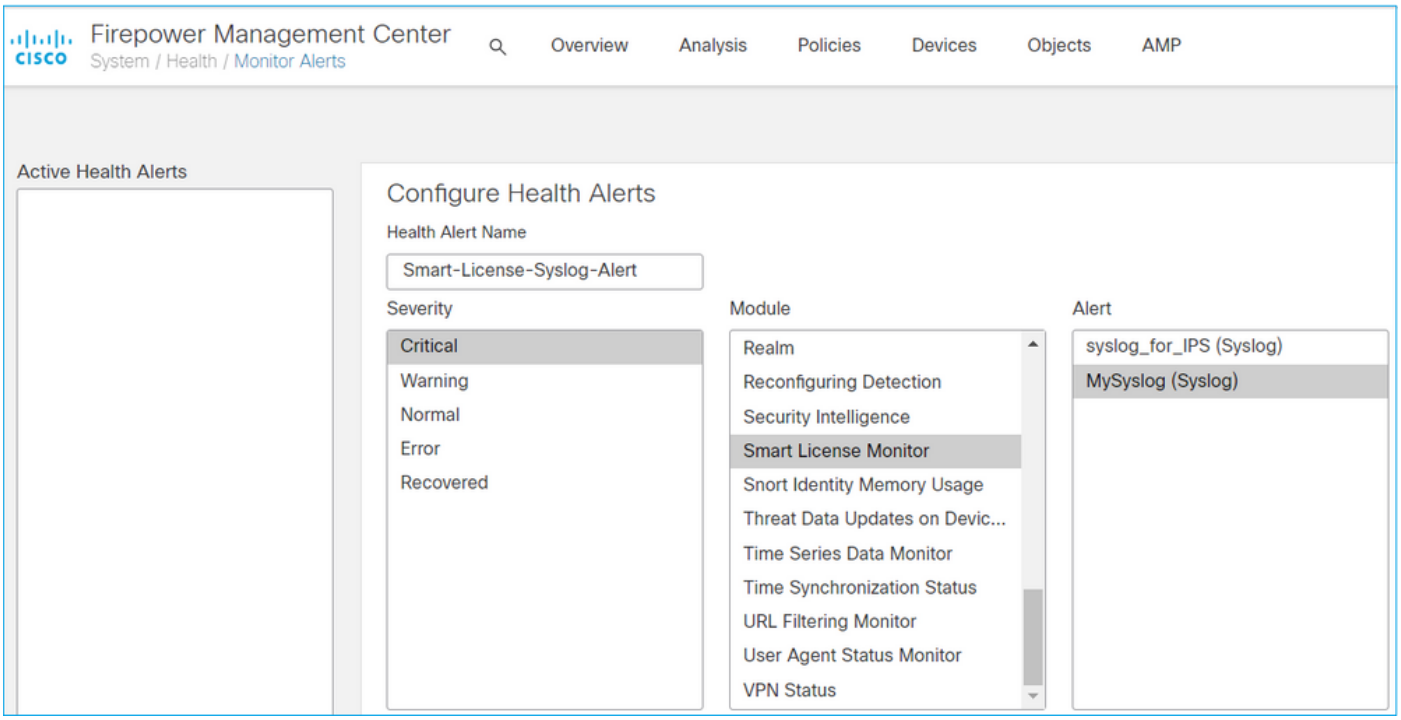


Ricevere notifiche di allarme sanitario dal CCP

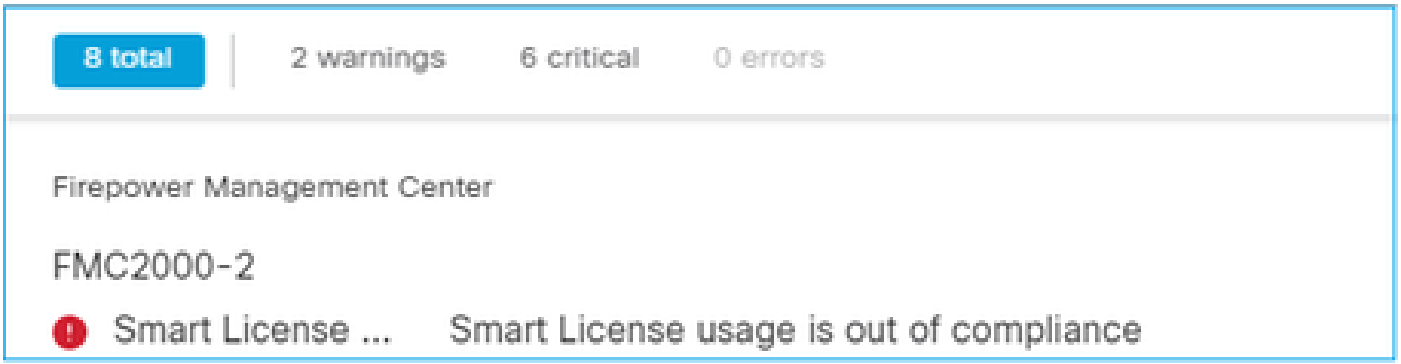
Dal lato FMC, è possibile configurare un avviso di Health Monitor e ricevere una notifica di avviso

di un evento sanitario. Il modulo Smart License Monitor è disponibile per controllare lo stato della Smart License. L'avviso di monitoraggio supporta Syslog, Email e trap SNMP.

Questo è un esempio di configurazione per ottenere un messaggio Syslog quando si verifica un evento di Smart License Monitor:



Questo è un esempio di un avviso di integrità:



Il messaggio Syslog generato dal CCP è:

<#root>

```
Mar 13 18:47:10 xx.xx.xx.xx Mar 13 09:47:10 FMC :
```

`HMNOTIFY: Smart License Monitor (Sensor FMC)`

```
: Severity: critical: Smart License usage is out of compliance
```

Fare riferimento a Monitoraggio stato per ulteriori dettagli sugli avvisi di Monitoraggio stato.

Più CCP nello stesso Smart Account

Se sullo stesso Smart Account vengono utilizzati più CCP, ogni nome host del CCP deve essere univoco. Quando in un CSM sono gestiti più CCP, per distinguere ciascun CCP il nome host di ciascun CCP deve essere univoco. Questa opzione è utile per la manutenzione delle licenze Smart License di FMC durante il funzionamento.

FMC deve mantenere la connettività Internet

Dopo la registrazione, il FMC controlla lo stato di Smart License Cloud e della licenza ogni 30 giorni. Se il CCP non è in grado di comunicare per 90 giorni, la funzione concessa in licenza viene mantenuta, ma rimane nello stato Autorizzazione scaduta. Anche in questo stato, il FMC tenta continuamente di connettersi a Smart License Cloud.

Distribuire più FMCv

Quando si utilizza Firepower System in un ambiente virtuale, la duplicazione (a caldo o a freddo) non è ufficialmente supportata. Ogni FMCv (Firepower Management Center Virtual) è univoco in quanto contiene informazioni di autenticazione. Per installare più FMCv, è necessario crearne uno alla volta a partire dal file OVF (Open Virtualization Format). Per ulteriori informazioni su questa limitazione, fare riferimento alla Guida introduttiva all'installazione di Cisco Firepower Management Center Virtual per VMware.

Domande frequenti

In FTD HA, quante licenze per dispositivi sono richieste?

Se in Alta disponibilità si utilizzano due FTD, è necessaria una licenza per ciascun dispositivo. Ad esempio, sono necessarie due licenze Threat and Malware se sulla coppia FTD HA vengono utilizzate le funzionalità Intrusive Protection System (IPS) e Advanced Malware Protection (AMP).

Perché FTD non usa alcuna licenza AnyConnect?

Dopo aver registrato il FMC sullo Smart Account, verificare che la licenza AnyConnect sia abilitata. Per abilitare la licenza, passare aFMC > Dispositivi, scegliere il dispositivo e selezionare Licenza. Selezionare l'icona Matita, scegliere la licenza da depositare nello Smart Account e selezionare Salva.

Perché nello Smart Account è in uso una sola licenza AnyConnect quando sono connessi 100 utenti?

Questo è il comportamento previsto, in quanto Smart Account tiene traccia del numero di dispositivi per i quali è abilitata questa licenza, mentre gli utenti non attivi sono connessi.

Perché c'è l'errore Device does not have the AnyConnect License dopo la configurazione e l'installazione di una VPN ad accesso remoto da parte del FMC?

Verificare che FMC sia registrato in Smart License Cloud. Il comportamento previsto è che la configurazione di Accesso remoto non può essere distribuita quando la registrazione del FMC viene annullata o in modalità di valutazione. Se il FMC è registrato, verificare che la licenza AnyConnect sia presente nello Smart Account e che sia assegnata al dispositivo.

Per assegnare una licenza: navigare aFMC Dispositivi, selezionare il dispositivo, Licenza (icona matita). Scegliere la licenza nello Smart Account e selezionare Salva.

Perché c'è l'errore Remote Access VPN with SSL cannot be deployed when Export-Controlled Features (Strong-crypto) are disabled quando è disponibile una distribuzione di una configurazione VPN di accesso remoto?

La VPN ad accesso remoto distribuita nell'FTD richiede l'abilitazione di una licenza di crittografia avanzata. ITverificare che nel FMC sia abilitata una licenza di Crittografia avanzata. Per controllare lo stato della licenza con crittografia avanzata, navigare a Sistema FMC > Licenze > Smart Licensinge verificare che le feature controllate da esportazione siano attivate.

Come abilitare una licenza di crittografia avanzata se Export-Controlled Features è disabilitato?

Questa funzionalità viene attivata automaticamente se per il token utilizzato durante la registrazione di FMC nello Smart Account Cloud è attivata l'opzione Consenti funzionalità di controllo dell'esportazione sui prodotti registrati con questo token. Se per il token questa opzione non è attivata, annullare la registrazione del FMC e registrarlo di nuovo con questa opzione attivata.

Cosa fare se l'opzione 'Consenti funzionalità controllate da esportazione sui prodotti registrati con questo token' non è disponibile quando il token viene generato?

Rivolgersi al team Cisco che gestisce gli account.

Perché non viene ricevuto l'errore 'La crittografia avanzata (ovvero l'algoritmo di crittografia è maggiore di DES) per la topologia VPN da sito a sito non è supportata'?

Questo errore viene visualizzato quando il CCP utilizza la modalità di valutazione o lo Smart License Account non ha diritto a una licenza di crittografia avanzata. VVerificare che il CCP sia registrato presso l'autorità di licenza e che sia abilitata la funzionalità Consenti controllo delle esportazioni sui prodotti registrati con questo token. Se allo Smart Account non è consentito utilizzare una licenza per la crittografia avanzata, non è consentita la distribuzione della configurazione da sito a sito VPN con cifratura superiore a DES.

Perché è stato ricevuto lo stato "Non conforme" sul CCP?

Il dispositivo può non essere conforme quando uno dei dispositivi gestiti utilizza licenze non disponibili.

Come si può correggere lo stato di non conformità?

Attenersi alla procedura descritta nella Guida alla configurazione di Firepower:

1. Per stabilire quali licenze sono necessarie, consultare la sezione Smart Licenses in fondo alla pagina.

2. Acquista le licenze richieste tramite i canali abituali.

3. In Cisco Smart Software Manager (https://software.cisco.com/#SmartLicensing-Inventory)verificare che le licenze siano visualizzate nell'account virtuale.

4. Nel FMC, selezionare Sistema > Licenze > Licenze Smart.

5. Selezionare Riautorizza.

La procedura completa è disponibile in Licenza del sistema Firepower.

Quali sono le funzionalità di Firepower Threat Defense Base?

La licenza Base consente:

- Configurazione dei dispositivi FTD da commutare e indirizzare (inclusi DHCP Relay e NAT).
- Configurazione di dispositivi FTD in modalità ad alta disponibilità (HA).
- Configurazione di moduli di sicurezza come cluster all'interno di uno chassis Firepower 9300 (cluster all'interno di uno chassis).
- Configurazione di dispositivi Firepower serie 9300 o Firepower serie 4100 (FTD) come cluster (cluster inter-chassis).
- Configurazione del controllo utente e applicazione e aggiunta di condizioni utente e applicazione alle regole di controllo di accesso.

Come è possibile ottenere la licenza per le funzionalità di base di Firepower Threat Defense?

Con ogni acquisto di un dispositivo virtuale Firepower Threat Defense o Firepower Threat Defense viene fornita automaticamente una licenza Base. Viene aggiunto automaticamente allo Smart Account quando FTD si registra nel FMC.

Quali indirizzi IP devono essere consentiti nel percorso tra FMC e Smart License Cloud?

Il CCP utilizza l'indirizzo IP sulla porta 443 per comunicare con Smart License Cloud.

L'indirizzo IP (https://tools.cisco.com)viene risolto nei seguenti indirizzi IP:

- 72.163.4.38
- 173.37.145.8

Informazioni correlate

- Guide alla configurazione di Firepower Management Center
- Panoramica delle licenze Cisco Live Smart: BRKARC-2034
- Licenze per le funzionalità di Cisco Secure Firewall Management Center
- Domande frequenti (FAQ) sulle licenze Cisco Smart Software

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).