

# Configurazione dell'integrazione di ISE 2.4 e FMC 6.2.3 pxGrid

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurare ISE](#)

[Passaggio 1. Abilita servizi PxGrid](#)

[Passaggio 2. Configurazione di ISE per l'approvazione di tutti gli account basati su certificato pxGrid](#)

[Passaggio 3. Esporta certificato di amministrazione ISE NT e certificati CA pxGrid](#)

[Configura FMC](#)

[Passaggio 4. Aggiungi un nuovo realm a FMC](#)

[Passaggio 5. Genera certificato CA FMC](#)

[Passaggio 6. Estrarre il certificato e la chiave privata dal certificato generato con OpenSSL](#)

[Passaggio 7. Installa certificato in FMC](#)

[Passaggio 8. Importazione del certificato FMC in ISE](#)

[Passaggio 9. Configura connessione pxGrid in FMC](#)

[Verifica](#)

[Verifica ad ISE](#)

[Verifica nel CCP](#)

[Risoluzione dei problemi](#)

## Introduzione

Questo documento descrive il processo di configurazione per l'integrazione di ISE pxGrid versione 2.4 e FMC versione 6.2.3.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ISE 2.4
- CCP 6.2.3
- Active Directory/Lightweight Directory Access Protocol (LDAP)

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

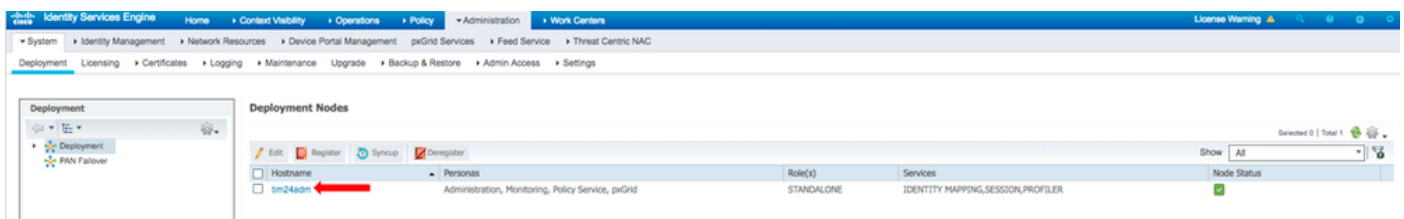
- Standalone ISE 2.4
- FMCv 6.2.3
- Active Directory 2012R2
- Identity Services Engine (ISE) pxGrid versione 2.4
- Firepower Management Center (FMC) versione 6.2.3

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.

## Configurare ISE

### Passaggio 1. Abilita servizi PxGrid

1. Accedere alla GUI di ISE Admin e selezionare **Amministrazione > Distribuzione**.
2. Selezionare il nodo ISE da utilizzare per la persona pxGrid.



3. Abilitare il servizio pxGrid e fare clic su **Salva** come mostrato nell'immagine.

Deployment Nodes List > tim24adm

### Edit Node

General Settings | Profiling Configuration

Hostname  
FQDN  
IP Address  
Node Type: Identity Services Engine (ISE)

Role: STANDALONE **Make Primary**

Administration

Monitoring

Role: PRIMARY

Other Monitoring Node

Policy Service

Enable Session Services ⓘ

Include Node in Node Group: None ⓘ

Enable Profiling Service ⓘ

Enable Threat Centric NAC Service ⓘ

Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

pxGrid ⓘ

Save Reset

4. Verificare che i servizi pxGrid vengano eseguiti dalla CLI.

**Nota:** il processo richiede fino a 5 minuti per l'avvio completo dei servizi pxGrid e per determinare lo stato di elevata disponibilità (HA) se sono in uso più nodi pxGrid.

5. SSH nella CLI del nodo ISE pxGrid e controllare lo stato dell'applicazione.

```
# show application status ise | in pxGrid
pxGrid Infrastructure Service running 24062
pxGrid Publisher Subscriber Service running 24366
pxGrid Connection Manager running 24323
pxGrid Controller running 24404
#
```

6. Accedere all'interfaccia utente di ISE Admin e verificare che i servizi siano online e funzionino. Selezionare **Amministrazione > pxGrid Services**.

7. Nella parte inferiore della pagina, ISE visualizza **Connected to pxGrid <FQDN nodo pxGrid>**.

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
ise-irst-tim24adm		Capabilities(2 Pub, 1 Sub)	Online (DHPP)	Internal	Certificate	View
ise-fincut-tim24adm		Capabilities(0 Pub, 0 Sub)	Online (DHPP)	Internal	Certificate	View
ise-pubsub-tim24adm		Capabilities(0 Pub, 0 Sub)	Online (DHPP)	Internal	Certificate	View
ise-bridge-tim24adm		Capabilities(0 Pub, 4 Sub)	Online (DHPP)	Internal	Certificate	View
ise-admin-tim24adm		Capabilities(4 Pub, 2 Sub)	Online (DHPP)	Internal	Certificate	View
iseagent-freepower-20762a2962d...		Capabilities(0 Pub, 6 Sub)	Online (DHPP)		Certificate	View
freightstest-freepower-20762a...		Capabilities(0 Pub, 0 Sub)	Offline (DHPP)		Certificate	View

## Passaggio 2. Configurazione di ISE per l'approvazione di tutti gli account basati su certificato pxGrid

1. Passare ad **Amministrazione** > **pxGrid Services** > **Impostazioni**.

2. Selezionare la casella "Approva automaticamente i nuovi account basati sui certificati" e fare clic su **Salva**.

**PxGrid Settings**

Automatically approve new certificate-based accounts

Allow password based account creation

Use Default Save

Test

Connected to pxGrid tim24adm.rtpaaa.net

**Nota:** se questa opzione non è attivata, l'amministratore deve approvare manualmente la connessione FMC ad ISE.

## Passaggio 3. Esporta certificato di amministrazione ISE NT e certificati CA pxGrid

1. Passare ad **Amministrazione** > **Certificati** > **Certificati di sistema**.

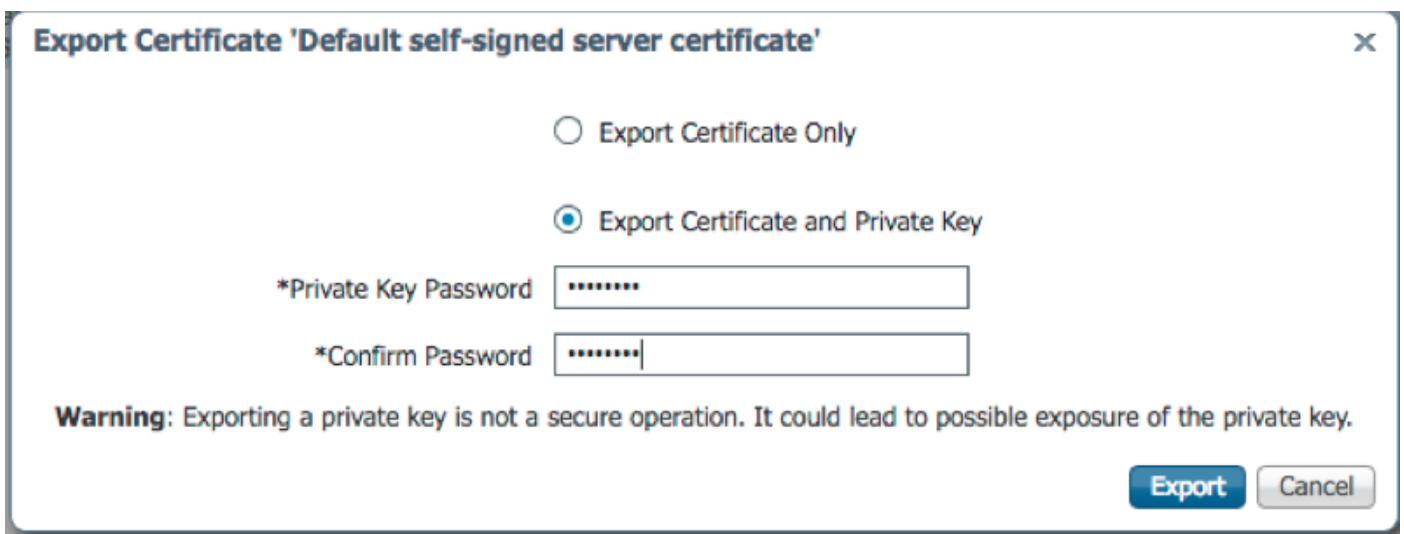
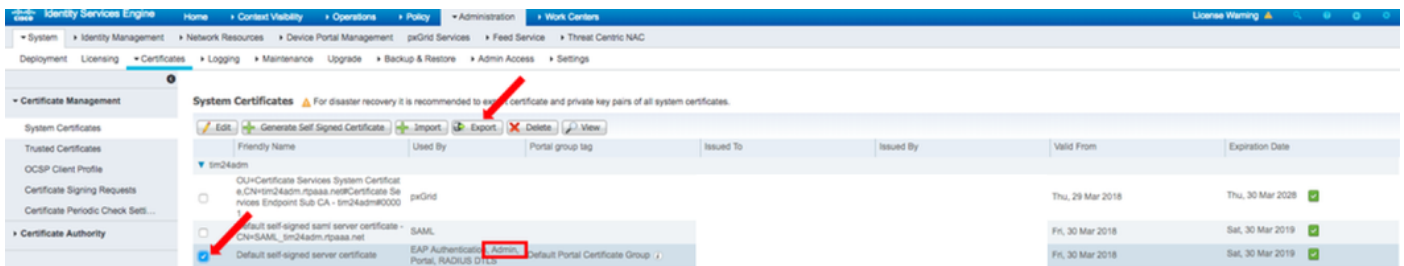
2. Espandere il nodo Monitoraggio primario (MNT) se non è abilitato nel nodo Amministrazione primaria.

3. Selezionare il certificato con il campo Utilizzato da "Amministratore".

**Nota:** questa guida utilizza il certificato autofirmato ISE predefinito per l'utilizzo da parte dell'amministratore. Se si utilizza un certificato di amministrazione firmato da un'Autorità di certificazione (CA), esportare la CA radice che ha firmato il certificato di amministrazione sul nodo ISE NT.

4. Fare clic su **Esporta**.

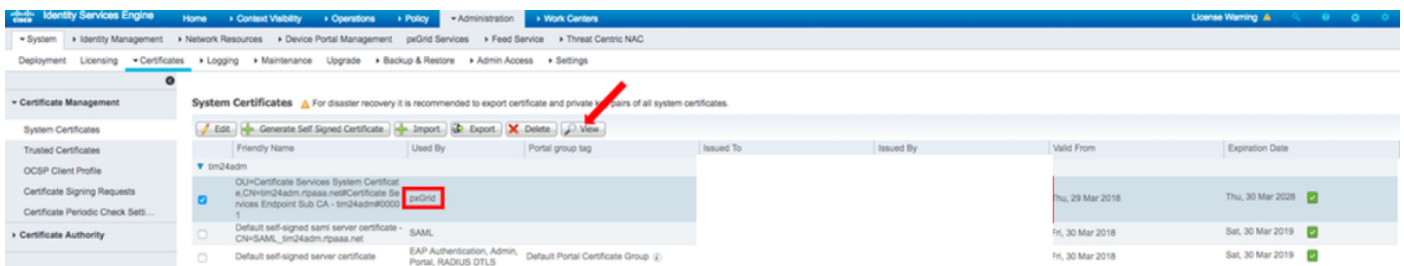
- Scegliere l'opzione Esporta certificato e chiave privata.
- Impostare una chiave di crittografia.
- Esportare e salvare** il file come mostrato nell'immagine.



- Tornare alla schermata ISE System Certificates (Certificati di sistema ISE).
- Determinare il campo Rilasciato da nel certificato con l'uso "pxGrid" nella colonna Utilizzato da.

**Nota:** nelle versioni precedenti di ISE, si trattava di un certificato autofirmato, ma a partire dalla versione 2.2 in poi questo certificato viene emesso dalla catena interna di CA ISE per impostazione predefinita.

- Selezionare il certificato e fare clic su **Visualizza** come mostrato nell'immagine.




- Determinare il certificato di livello superiore (radice). In questo caso si tratta di **"CA radice Servizi certificati - tim24adm"**.
- Chiudere la finestra di visualizzazione del certificato come illustrato nell'immagine.

# Certificate Hierarchy



Certificate Services Root CA - tim24adm  
Certificate Services Node CA - tim24adm  
Certificate Services Endpoint Sub CA - tim24adm

tim24adm.rtpaaa.net

 tim24adm.rtpaaa.net  
Issued By : Certificate Services Endpoint Sub CA - tim24adm  
Expires : Thu, 30 Mar 2028 14:17:12 EDT

Certificate status is good

**Details**

**Issued To**

Common Name (CN)

Organization Unit (OU) **Certificate Services System Certificate**

Organization (O)

City (L)

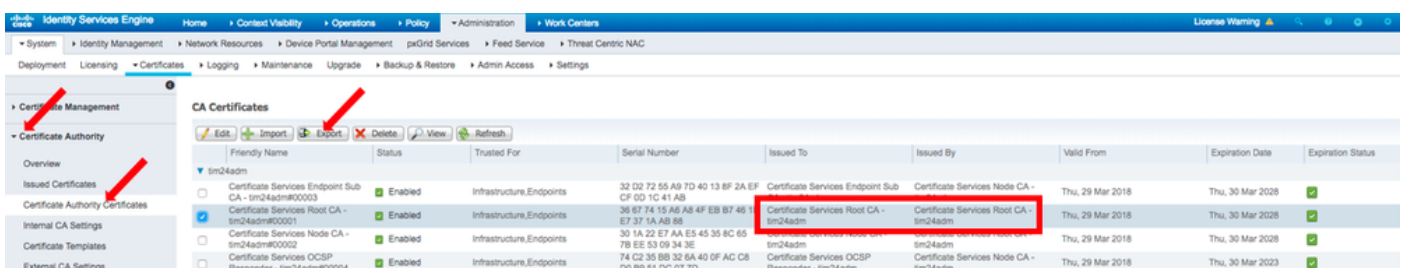
State (ST)

Country (C)

Serial Number **58:2A:91:45:E8:23:42:74:98:53:06:94:33:9E:AD:83**

Close

14. Espandere il menu ISE Certificate Authority.
15. Selezionare **Certificati Autorità di certificazione**.
16. Selezionare il certificato radice identificato e fare clic su **Esporta**. Quindi salvare il certificato CA radice pxGrid come mostrato nell'immagine.



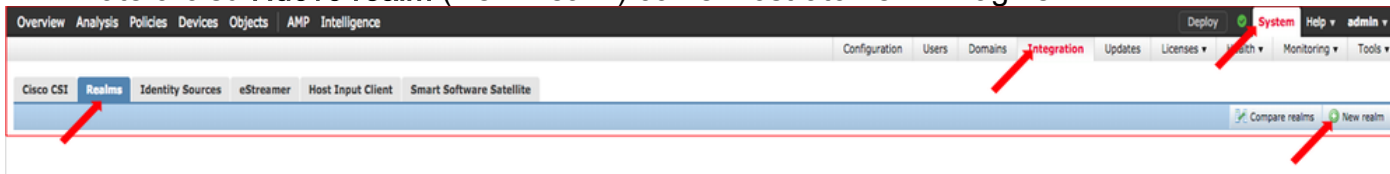
The screenshot shows the 'CA Certificates' table in the ISE interface. Red arrows point to the 'Certificate Authority' menu, the 'Certificates' sub-menu, and the 'Export' button. A red box highlights the row for 'Certificate Services Root CA - tim24adm'.

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
tim24adm								
Certificate Services Endpoint Sub CA - tim24adm0003	Enabled	Infrastructure.Endpoints	32 D2 72 55 A9 7D 40 13 8F 2A EF CF 03 10 41 A8	Certificate Services Endpoint Sub	Certificate Services Node CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
Certificate Services Root CA - tim24adm00001	Enabled	Infrastructure.Endpoints	36 67 74 15 A6 A8 4F EB B7 46 1 E7 37 1A A8 B8	Certificate Services Root CA - tim24adm	Certificate Services Root CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
Certificate Services Node CA - tim24adm00002	Enabled	Infrastructure.Endpoints	30 1A 22 E7 AA E5 45 35 8C 65 78 EE 03 09 34 3E	tim24adm	tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
Certificate Services OCSP Responder - tim24adm00004	Enabled	Infrastructure.Endpoints	74 C2 35 B8 32 6A 40 DF AC C8 D0 B9 51 DC 07 7D	Certificate Services OCSP Responder - tim24adm	Certificate Services Node CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2023	✓

# Configura FMC

## Passaggio 4. Aggiungi un nuovo realm a FMC

1. Accedere alla GUI di FMC e selezionare **Sistema > Integrazione > Realm**.
2. Fate clic su **Nuovo realm** (New Realm) come mostrato nell'immagine.



3. Compilare il modulo e fare clic sul pulsante Verifica l'aggiunta ad Active Directory (AD).

**Nota:** il nome utente per l'aggiunta ad Active Directory deve essere in formato UPN (User Principal Name). In caso contrario, il test non riesce.

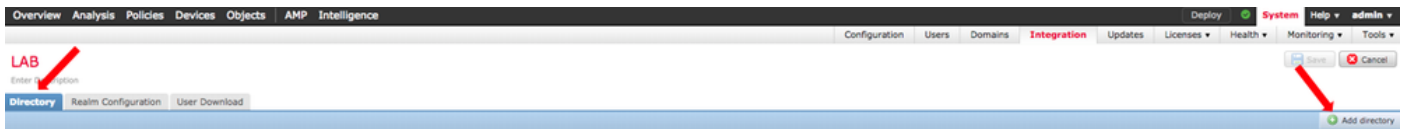
4. Se il test di partecipazione ad Active Directory ha esito positivo, fare clic su **OK**.

A screenshot of the 'Add New Realm' dialog box. The form contains the following fields and options:

- Name \***: ISEpxGrid
- Description**: Realm for use with pxGrid
- Type \***: AD
- AD Primary Domain \***: (empty) ex: domain.com
- AD Join Username**: (empty) ex: user@domain
- AD Join Password**: (masked) Test AD Join button
- Directory Username \***: admin ex: user@domain
- Directory Password \***: (masked)
- Base DN \***: CN=Users,DN=rtpaaa,DN=net ex: ou=user,dc=cisco,dc=com
- Group DN \***: DN=rtpaaa,DN=net ex: ou=group,dc=cisco,dc=com
- Group Attribute**: Member

A legend at the bottom left indicates that fields with an asterisk (\*) are required. 'OK' and 'Cancel' buttons are at the bottom right.

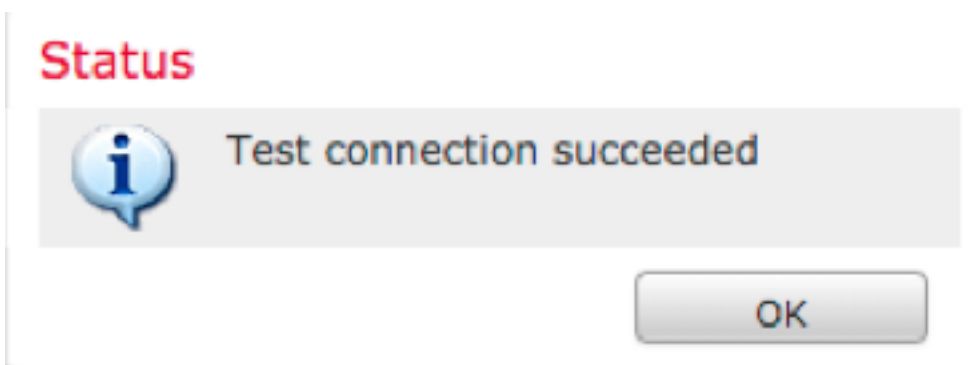
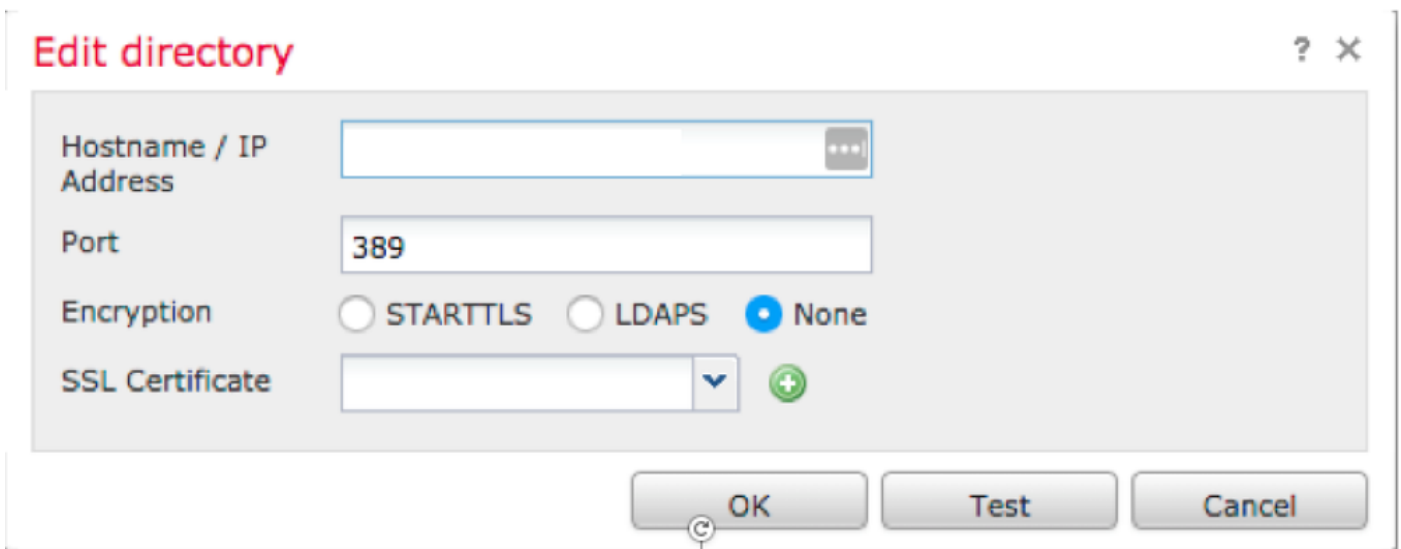
5. Fare clic sulla scheda **Directory**, quindi fare clic su **Add directory** (Aggiungi directory), come mostrato nell'immagine.



6. Configurare IP/Nome host e verificare la connessione.

**Nota:** se il test ha esito negativo, verificare le credenziali nella scheda Configurazione realm.

7. Fare clic su OK.



8. Fare clic sulla scheda **Download utente**.



9. Se non è già selezionato, abilitare il download per utenti e gruppi

10. Fare clic su Download



Enter Description

Directory

Realm Configuration

User Download

 Download users and groups

Begin automatic download at 8 PM America/New York Repeat Every 24 Hours

Download Now

11. Una volta completata la lista, aggiungere i gruppi desiderati e selezionare **Aggiungi a inclusione**.

12. Salvare la configurazione del realm.

Overview Analysis Policies Devices Objects AMP Intelligence

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

LAB

Enter Description

Directory Realm Configuration User Download

Download users and groups

Begin automatic download at 8 PM America/New York Repeat Every 24 Hours

Download Now

Available Groups

Search by name

Groups to Include (35)

Groups to Exclude (0)

Add to Include

Add to Exclude

Enter User Inclusion Add

Enter User Exclusion Add

You have unsaved changes Save Cancel

13. Abilitare lo stato del realm.

Overview Analysis Policies Devices Objects AMP Intelligence

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

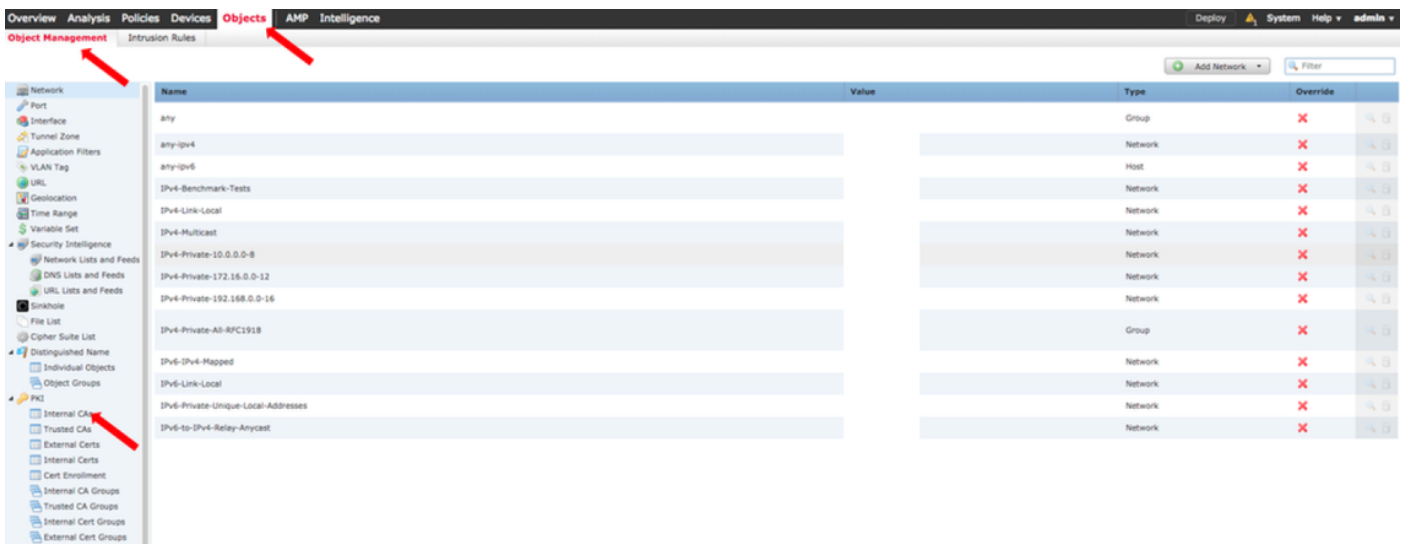
Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
LAB		Global	AD	DC=rt2aaa,DC=net	CN=Users,DC=rt2aaa,DC=member		Enabled

Compare realms New realm

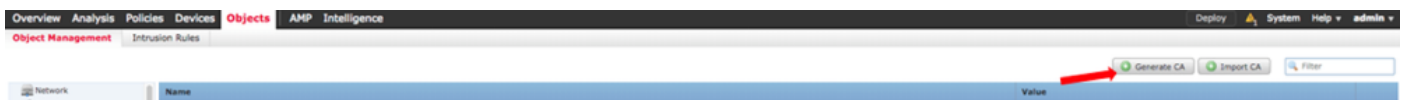
## Passaggio 5. Genera certificato CA FMC

1. Passare a **Oggetti > Gestione oggetti > CA interne** come mostrato nell'immagine.



2. Fare clic su **Genera CA**.

3. Compilare il modulo e fare clic su **Genera CA autofirmata**.



**Generate Internal Certificate Authority** ? X

Name:

Country Name (two-letter code):

State or Province:

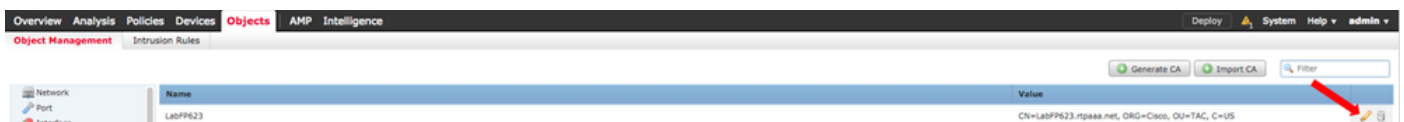
Locality or City:

Organization:

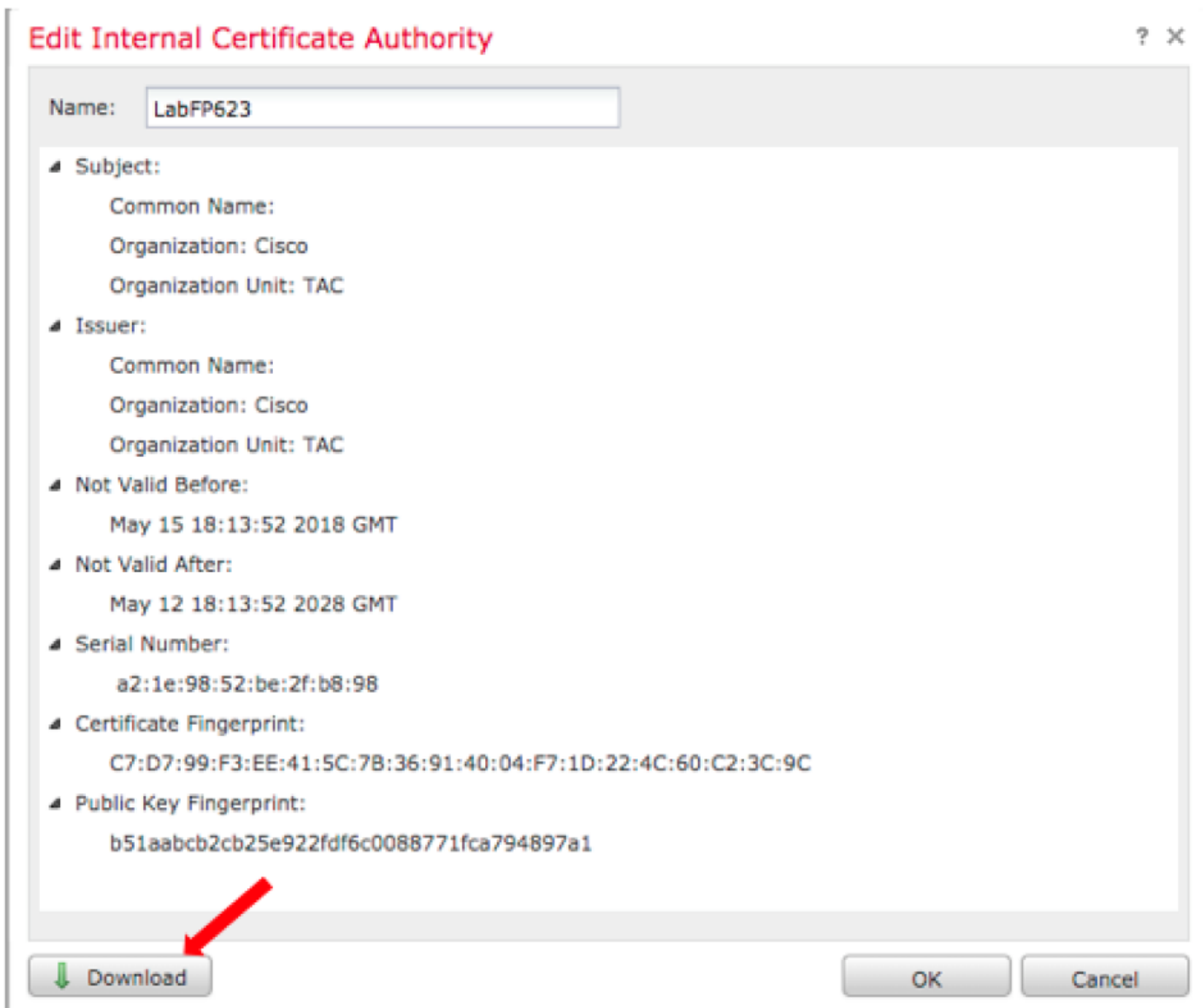
Organizational Unit (Department):

Common Name:

4. Al termine della generazione, fare clic sulla matita a destra del certificato CA generato, come mostrato nell'immagine.



5. Fare clic su **Download**.



6. Configurare e confermare la password di crittografia e fare clic su **OK**.

7. Salvare il file PKCS (Public-Key Cryptography Standards) p12 nel file system locale.

## Passaggio 6. Estrarre il certificato e la chiave privata dal certificato generato con OpenSSL

Questa operazione viene eseguita nella directory principale della console Gestione configurazione di Microsoft o in qualsiasi client in grado di utilizzare i comandi OpenSSL. Questo esempio utilizza una shell Linux standard.

1. Utilizzare **openssl** per estrarre il certificato (CER) e la chiave privata (PVK) dal file p12.
2. Estrarre il file CER, quindi configurare la chiave di esportazione del certificato dalla generazione del certificato in FMC.

```
~$ openssl pkcs12 -nokeys -clcerts -in <filename.p12> -out <filename.cer>
Password:
Last login: Tue May 15 18:46:41 UTC 2018
Enter Import Password:
MAC verified OK
```

3. Estrarre il file PVK, configurare la chiave di esportazione del certificato, quindi impostare una nuova passphrase PEM e confermare.

```
~$ openssl pkcs12 -nocerts -in <filename.p12> -out <filename.pvk>
```

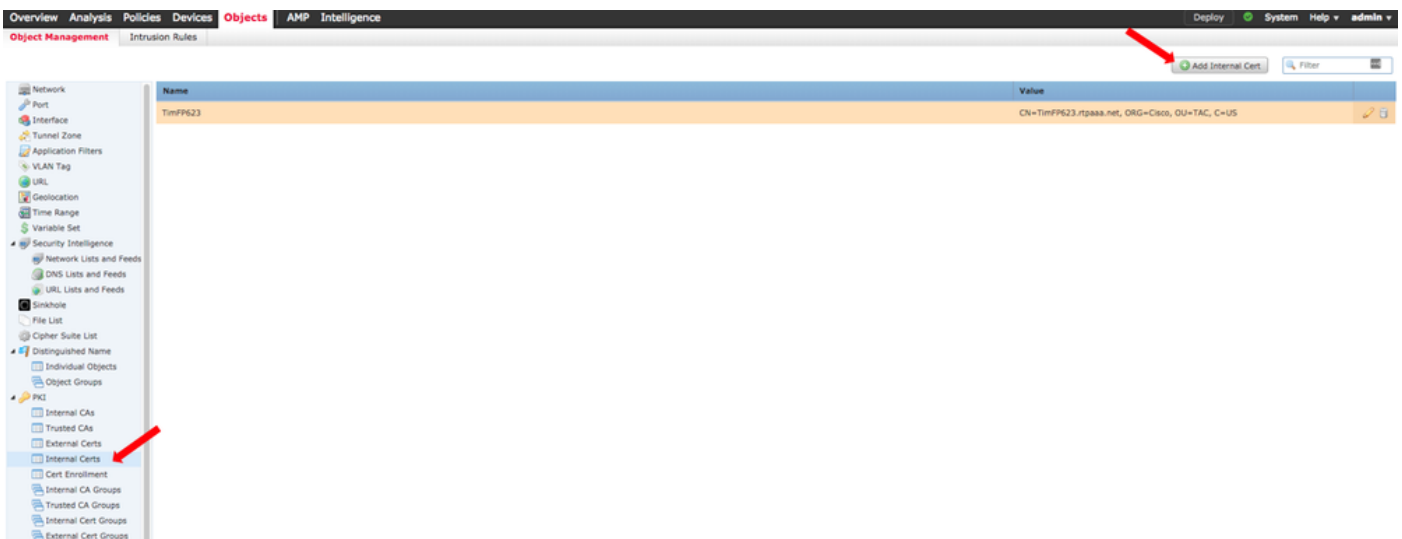
Password: Last login: Tue May 15 18:46:41 UTC 2018 Enter Import Password: MAC verified OK

4. Questa frase PEM è necessaria nella fase successiva.

## Passaggio 7. Installa certificato in FMC

1. Passare a **Oggetti > Gestione oggetti > PKI > Certificati interni**.

2. Fare clic su **Add Internal Cert** (Aggiungi certificato interno) come illustrato nell'immagine.



3. Configurare un nome per il certificato interno.

4. Individuare la posizione del file CER e selezionarlo. Una volta inseriti i dati del certificato, selezionare il secondo.

5. Selezionare **Option (Opzione)** e selezionare il file PVK.

6. Eliminare tutti gli "attributi del sacchetto" iniziali ed eventuali valori finali nella sezione PVK. La chiave PVK inizia con **—BEGIN ENCRYPTED PRIVATE KEY—** e termina con **—END ENCRYPTED PRIVATE KEY—**.

**Nota:** non è possibile fare clic su **OK** se il testo PVK contiene caratteri non compresi nei segni meno iniziali e finali.

7. Selezionare la casella **Encrypted (Crittografato)** e configurare la password creata al momento dell'esportazione della chiave PVK al punto 6.

8. Fare clic su **OK**.

## Add Known Internal Certificate



Name:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDFTCCAmWgAwIBAgIJAKIemFK+L7iYMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNV
BAYTAIVTMQswCQYDVQQIDAJOQzEMMAoGA1UEBwwDUIRQM4wDAYDVQQKDAVDAxNj
bzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDDBNMYWJGUDYyMy5ydHBhYWEubmV0MB4X
DTE4MDUxNTE4MTM1MloXDTI4MDUxMjE4MTM1MlowZDELMAkGA1UEBhMCVVMxZzAJ
BgNVBAGMAK5DMQwwCgYDVQQHDANSVFAXDjAMBgNVBAoMBUNpc2NmMQwwCgYDVQQQL
DANUQUxHDAaBgNVBAMME0xhYkZQNjIzLnJ0cGFhYS5uZXQwgwEIMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQMjtS5IUIFIZkZK/TSGtkOCmuivTK5kk1WzAy6
D7Gm/c69cXw/VfIPWnSBzhEkiRTyspmTMdyf/4TJvUmUH60h1O8/8dZeqJOzbjon
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABGkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI5uV3MsiHZsICAggA
MBQGCCqGSIb3DQMHBABGVM1+xHLIASCBMjjJxkffXUNUcdB22smybvWotwbcRrt
xL0qjEStmwuyExVp+TWC3AyIJN1DE7/rRssjRAqsnSOxIvDGmg0dVsvnbqZwjFP
74POu/O2Vy99iFoVgW2q9DyXyL/h64TH9CZtwLKIOGOeEunNKpamDnpfyN8QC4DC
fXvNZ8jNG4HrEcFmnnij0EwJ0QT8Jn5gAUj+AIPMe32zPqwocCRNYrRXMVM9+Jwp
-----END ENCRYPTED PRIVATE KEY-----
</no>
```

Key or, choose a file:

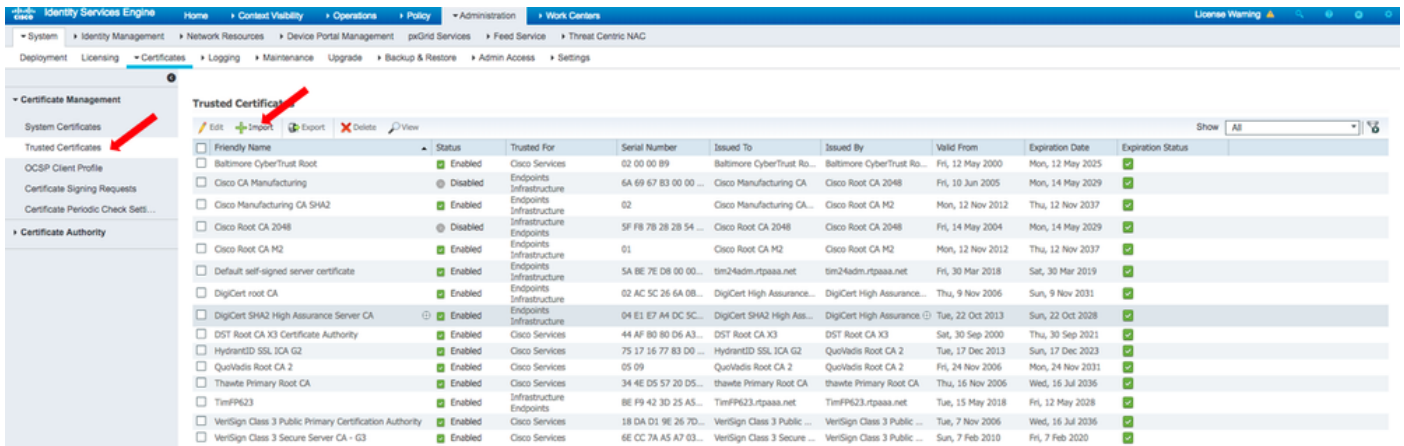
Bag Attributes  
localKeyID: C7 D7 99 F3 EE 41 5C 7B 36 91 40 04 F7 1D 22 4C 60 C2 3C 9C ← DELETE  
Key Attributes: <no attributes="">

Encrypted, and the password is:

Encrypted, and the password is:

### Passaggio 8. Importazione del certificato FMC in ISE

1. Accedere alla GUI di ISE e selezionare Amministrazione > Sistema > Certificati > Certificati attendibili.
2. Fare clic su Importa.



3. Fare clic su **Scegli file** e selezionare il file CER FMC dal sistema locale.

Facoltativo: configurare un nome descrittivo.

4. Controllare l'attendibilità per l'autenticazione in ISE.

Facoltativo: configurare una descrizione.

5. Fare clic su **Submit** (Invia) come mostrato nell'immagine.

### Import a new Certificate into the Certificate Store

\* Certificate File  TZfpcert.cer

Friendly Name

**Trusted For:**

Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

Description

## Passaggio 9. Configura connessione pxGrid in FMC

1. Passare a **Sistema > Integrazione > Origini identità** come mostrato nell'immagine.



2. Fare clic su **ISE**.

3. Configurare l'indirizzo IP o il nome host del nodo ISE pxGrid.

4. Selezionare il segno + a destra di pxGrid Server CA.

5. Assegnare un nome al file CA del server, quindi individuare la CA di firma radice pxGrid raccolta nel passaggio 3 e fare clic su **Salva**.

6. Selezionare il segno + a destra di CA del server NT.

7. Assegnare un nome al file della CA del server, quindi individuare il certificato amministratore raccolto nel passaggio 3 e fare clic su **Salva**.

8. Selezionare il file **FMC CER** dall'elenco a discesa.

Identity Sources

Service Type:  None  Identity Services Engine  User Agent

Primary Host Name/IP Address \*

Secondary Host Name/IP Address

pxGrid Server CA \*  +

MNT Server CA \*  +

FMC Server Certificate \*  +


ISE Network Filter  ex. 10.89.31.0/24, 192.168.8.0/24, ...

\* Required Field

9. Fare clic su **Test**.

10. Se il test ha esito positivo, fare clic su **OK**, quindi su **Salva** nella parte superiore destra della schermata.

## Status

 ISE connection status:  
Primary host: Success

[Additional Logs](#)

**Nota:** quando si eseguono due nodi ISE pxGrid, è normale che un host visualizzi il risultato positivo e uno il risultato negativo, in quanto pxGrid viene eseguito attivamente su un solo nodo ISE alla volta. A seconda della configurazione, la modalità di visualizzazione degli errori dell'host primario e degli errori dell'host secondario dipende dalla configurazione. Tutto questo dipende da quale nodo in ISE è il nodo pxGrid attivo.

## Verifica

### Verifica ad ISE

1. Aprire la GUI di ISE e selezionare **Administration > pxGrid Services**.

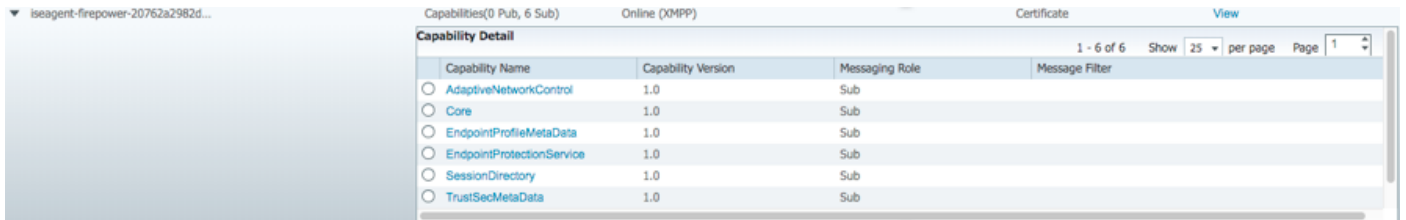
Se l'operazione ha esito positivo, nell'elenco dei client sono elencate due connessioni firepower. Uno per il CCP effettivo (iseagent-hostname-33bytes) e uno per il dispositivo di test (firesightisetest-hostname-33bytes).



La connessione iseagent-firepower visualizza sei (6) subs e appare online.

La connessione firesightisetest-firepower visualizza zero (0) subs e appare offline.

La visualizzazione estesa del client iseagent-firepower visualizza le sei sottoscrizioni.

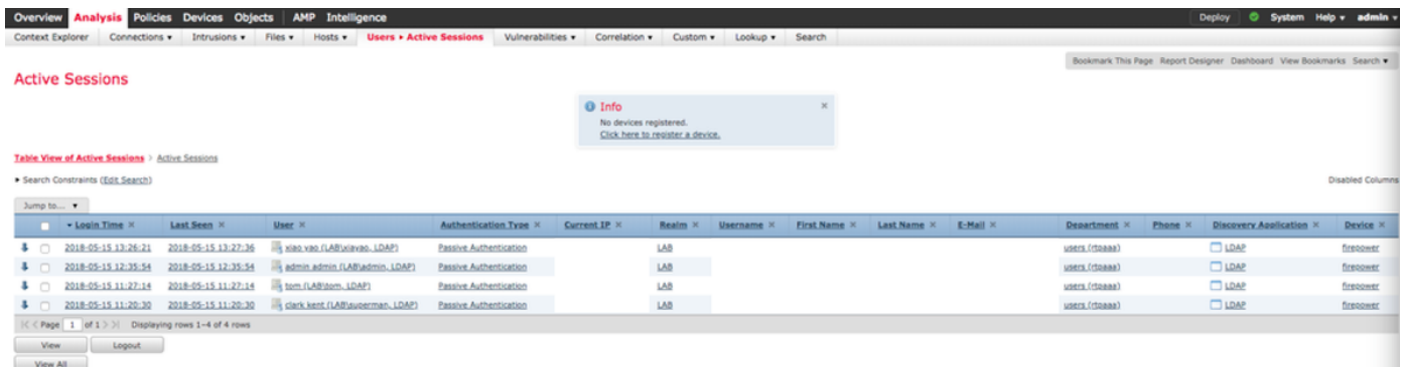


**Nota:** a causa del bug Cisco [IDCSCvo75376](#) esiste un limite per il nome host e il download bulk non riesce. Il pulsante di prova del CCP visualizza un errore di connettività. Ciò influisce su 2,3p6, 2,4p6 e 2,6. Si consiglia di eseguire la patch 2.3 5 o 2.4 5 fino al rilascio di una patch ufficiale.

## Verifica nel CCP

1. Aprire la GUI di FMC e selezionare **Analisi > Utenti > Sessioni attive**.

Tutte le sessioni di Active Directory pubblicate tramite la funzionalità Directory di sessione in ISE vengono visualizzate nella tabella Active Sessions in FMC.



In modalità sudo CLI FMC, il comando `'adi_cli session'` visualizza le informazioni sulla sessione utente inviate dall'ISE al FMC.



```
ssh admin@<FMC IP ADDRESS>
Password:
Last login: Tue May 15 19:03:01 UTC 2018 from dhcp-172-18-250-115.cisco.com on ssh
Last login: Wed May 16 16:28:50 2018 from dhcp-172-18-250-115.cisco.com
```

Copyright 2004-2018, Cisco and/or its affiliates. All rights reserved.  
Cisco is a registered trademark of Cisco Systems, Inc.  
All other trademarks are property of their respective owners.

```
Cisco Fire Linux OS v6.2.3 (build 13)
Cisco Firepower Management Center for VMWare v6.2.3 (build 83)
```

```
admin@firepower:~$ sudo -i
Password:
Last login: Wed May 16 16:01:01 UTC 2018 on cron
root@firepower:~# adi_cli session
```

```
received user session: username tom, ip ::ffff:172.18.250.148, location_ip ::ffff:10.36.150.11,
realm_id 2, domain rtpaaa.net, type Add, identity Passive.
received user session: username xiayao, ip ::ffff:10.36.148.98, location_ip ::, realm_id 2,
domain rtpaaa.net, type Add, identity Passive.
received user session: username admin, ip ::ffff:10.36.150.24, location_ip ::, realm_id 2,
domain rtpaaa.net, type Add, identity Passive.
received user session: username administrator, ip ::ffff:172.18.124.200, location_ip ::,
realm_id 2, domain rtpaaa.net, type Add, identity Passive.
```

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

## 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).