

配置ISE 2.4和FMC 6.2.3 pxGrid整合

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[配置ISE](#)

[步驟1.啟用pxGrid服務](#)

[步驟2.配置ISE以批准所有pxGrid基於證書的帳戶](#)

[步驟3.匯出ISE MNT管理員證書和pxGrid CA證書](#)

[配置FMC](#)

[步驟4.向FMC新增新領域](#)

[步驟5.生成FMC CA證書](#)

[步驟6.使用OpenSSL從產生的憑證中提取憑證和私密金鑰](#)

[步驟7.將證書安裝到FMC](#)

[步驟8.將FMC證書匯入ISE](#)

[步驟9.在FMC上配置pxGrid連線](#)

[驗證](#)

[在ISE中驗證](#)

[在FMC中驗證](#)

[疑難排解](#)

簡介

本文檔介紹整合ISE pxGrid版本2.4和FMC版本6.2.3的配置流程。

必要條件

需求

思科建議您瞭解以下主題：

- ISE 2.4
- FMC 6.2.3
- Active Directory/輕量目錄訪問協定(LDAP)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 獨立ISE 2.4

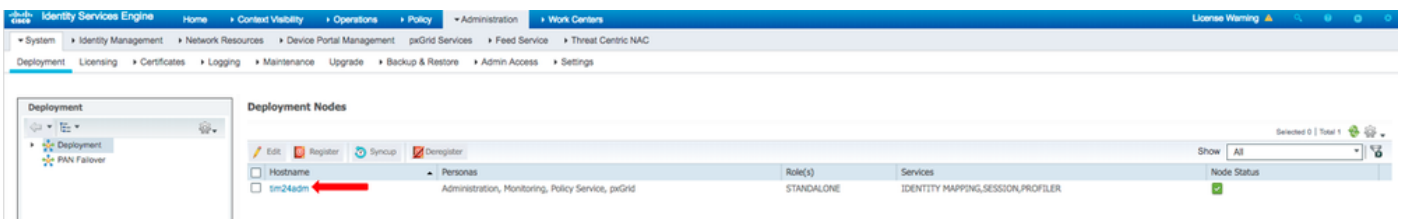
- FMCv 6.2.3
- Active Directory 2012R2
- 身分識別服務引擎(ISE)pxGrid版本2.4
- Firepower管理中心(FMC)版本6.2.3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

配置ISE

步驟1.啟用pxGrid服務

1. 登入ISE管理員GUI，導航至**管理>部署**。
2. 選擇要用於pxGrid角色的ISE節點。



3. 啟用pxGrid服務，然後按一下**Save**，如下圖所示。

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. 驗證pxGrid服務是否從CLI運行。

注意：如果使用多個pxGrid節點，該過程最多需要5分鐘時間，pxGrid服務才能完全啟動並確定高可用性(HA)狀態。

5. 通過SSH進入ISE pxGrid節點CLI並檢查應用狀態。

```
# 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. 訪問ISE管理員GUI並驗證服務是否線上且正常運行。導航到**管理 > pxGrid服務**。

7. 在頁面底部，ISE顯示**Connected to pxGrid <pxGrid node FQDN>**。

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
ise-mnt-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
fireightsitest-freepower-20762a...		Capabilities(0 Pub, 0 Sub)	Offline (DHPP)		Certificate	View

步驟2.配置ISE以批准所有pxGrid基於證書的帳戶

1. 導航到**管理 > pxGrid服務 > 設定**。

2. 選中覈取方塊：「自動批准基於證書的新帳戶」，然後按一下**儲存**。

PxGrid Settings

Automatically approve new certificate-based accounts

Allow password based account creation

Use Default Save

Test

Connected to pxGrid tim24adm.rtpaaa.net

注意：如果未啟用此選項，管理員必須手動批准與ISE的FMC連線。

步驟3.匯出ISE MNT管理員證書和pxGrid CA證書

1. 定位至**管理 > 證書 > 系統證書**。

2. 如果未在「主要管理」節點上啟用，請展開「主要監視(MNT)」節點。

3. 使用Used-By "Admin"欄位選擇證書。

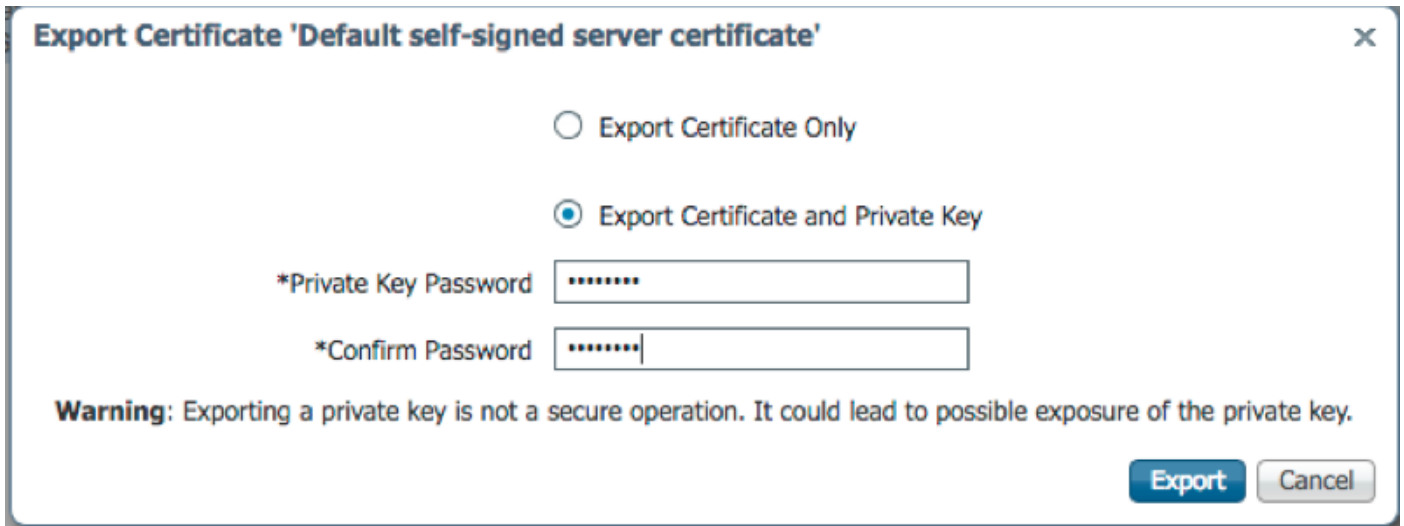
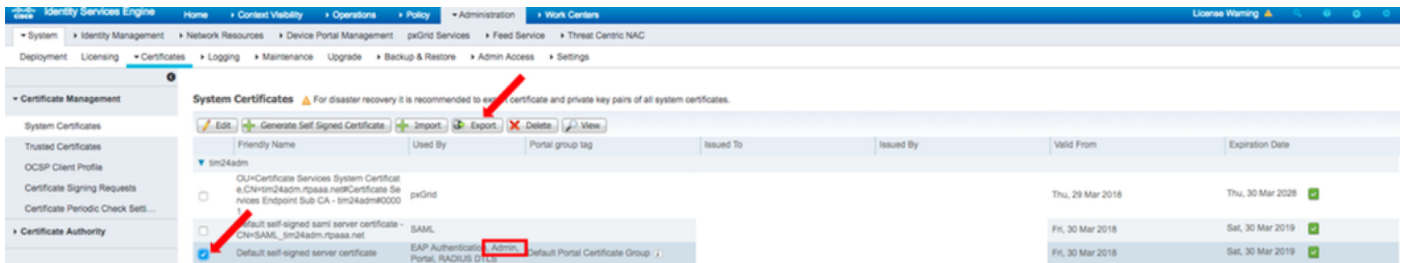
注意：本指南使用管理員使用的預設ISE自簽名證書。如果您使用證書頒發機構(CA)簽名的管理員證書，請匯出在ISE MNT節點上簽名的管理員證書的根CA。

4. 按一下**匯出**。

5. 選擇匯出證書和私鑰的選項。

6. 設定加密金鑰。

7. **Export**和**Save**檔案，如下圖所示。

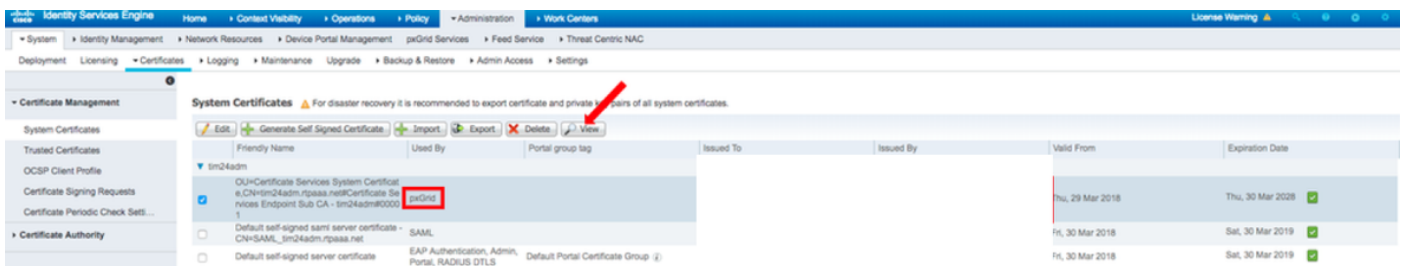


9. 返回ISE系統證書螢幕。

10. 使用「使用者」列中的「pxGrid」用法確定證書上的「頒發者」欄位。

註：在舊版ISE中，這是一個自簽名證書，但自2.2起，預設情況下此證書由內部ISE CA鍵頒發。

11. 選擇「Certificate」，然後按一下View，如下圖所示。



12. 確定頂級（根）證書。在本例中為「Certificate Services Root CA - tim24adm」。

13. 關閉「certificate view (證書檢視)」視窗，如下圖所示。

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)

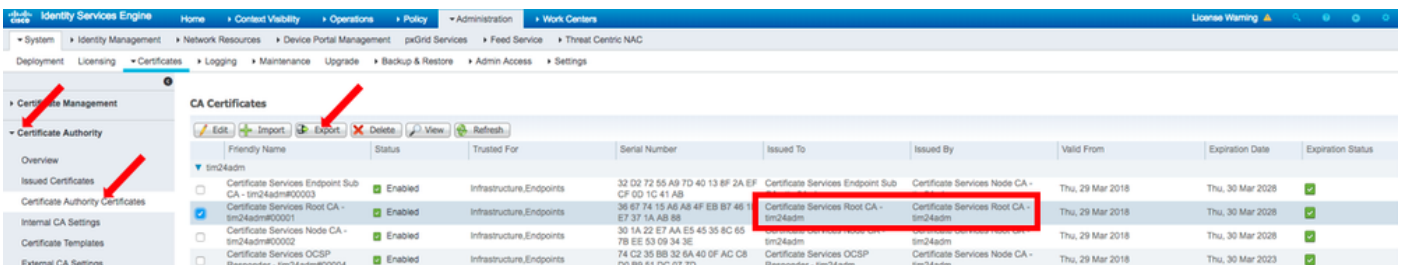
Serial Number **58:2A:91:45:E8:23:42:74:98:53:06:94:33:9E:AD:83**

Close

14. 展開ISE證書頒發機構選單。

15. 選擇證書頒發機構證書。

16. 選擇已識別的根證書，然後按一下匯出。然後儲存pxGrid根CA證書，如下圖所示。

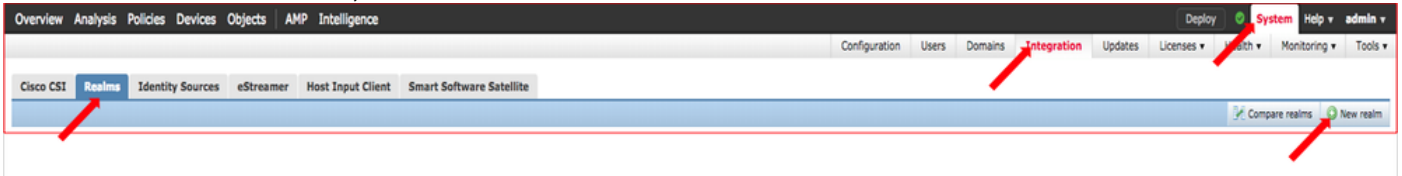


Friendy Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
<input type="checkbox"/> Certificate Services Endpoint Sub CA - tim24adm#00003	Enabled	Infrastructure.Endpoints	32 D2 72 55 A9 TD 40 13 8F 2A EF CF 0D 1C 41 AB	Certificate Services Endpoint Sub	Certificate Services Node CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
<input checked="" type="checkbox"/> Certificate Services Root CA - tim24adm#00001	Enabled	Infrastructure.Endpoints	36 67 74 15 A6 AB 4F EB B7 46 E7 3F 1A AB 56	Certificate Services Root CA - tim24adm	Certificate Services Root CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
<input type="checkbox"/> Certificate Services Node CA - tim24adm#00002	Enabled	Infrastructure.Endpoints	30 1A 22 E7 AA E5 45 35 8C 65 7B EE 53 09 34 3E	tim24adm	sm24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
<input type="checkbox"/> Certificate Services OCSP Responder - tim24adm#00004	Enabled	Infrastructure.Endpoints	74 C2 35 B8 32 6A 40 0F AC C8 D9 B9 51 DC 07 D7	Certificate Services OCSP Responder - tim24adm	Certificate Services Node CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2023	✓

配置FMC

步驟4.向FMC新增新領域

1. 訪問FMC GUI並導航至System > Integration > Realms。
2. 按一下New Realm，如下圖所示。



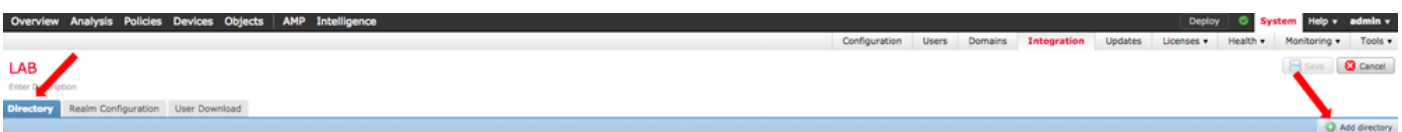
3. 填寫表單並按一下「測試Active Directory(AD)加入」按鈕。

注意:AD加入使用者名稱必須採用使用者主體名稱(UPN)格式，否則測試失敗。

4. 如果測試AD加入成功，請按一下確定。

A screenshot of the 'Add New Realm' form in the FMC GUI. The form has a title 'Add New Realm' and a close button. It contains several fields: 'Name *' (text box with 'ISEpxGrid'), 'Description' (text box with 'Realm for use with pxGrid'), 'Type *' (dropdown menu with 'AD'), 'AD Primary Domain *' (text box), 'AD Join Username' (text box), 'AD Join Password' (password field), 'Directory Username *' (text box with 'admin'), 'Directory Password *' (password field), 'Base DN *' (text box with 'CN=Users, DN=rtpaaa, DN=net'), 'Group DN *' (text box with 'DN=rtpaaa, DN=net'), and 'Group Attribute' (dropdown menu with 'Member'). There are example values for several fields: 'ex: domain.com', 'ex: user@domain', 'ex: user@domain', 'ex: ou=user, dc=cisco, dc=com', and 'ex: ou=group, dc=cisco, dc=com'. A 'Test AD Join' button is located next to the 'AD Join Password' field. At the bottom, there are 'OK' and 'Cancel' buttons. A legend indicates that '*' denotes a required field.

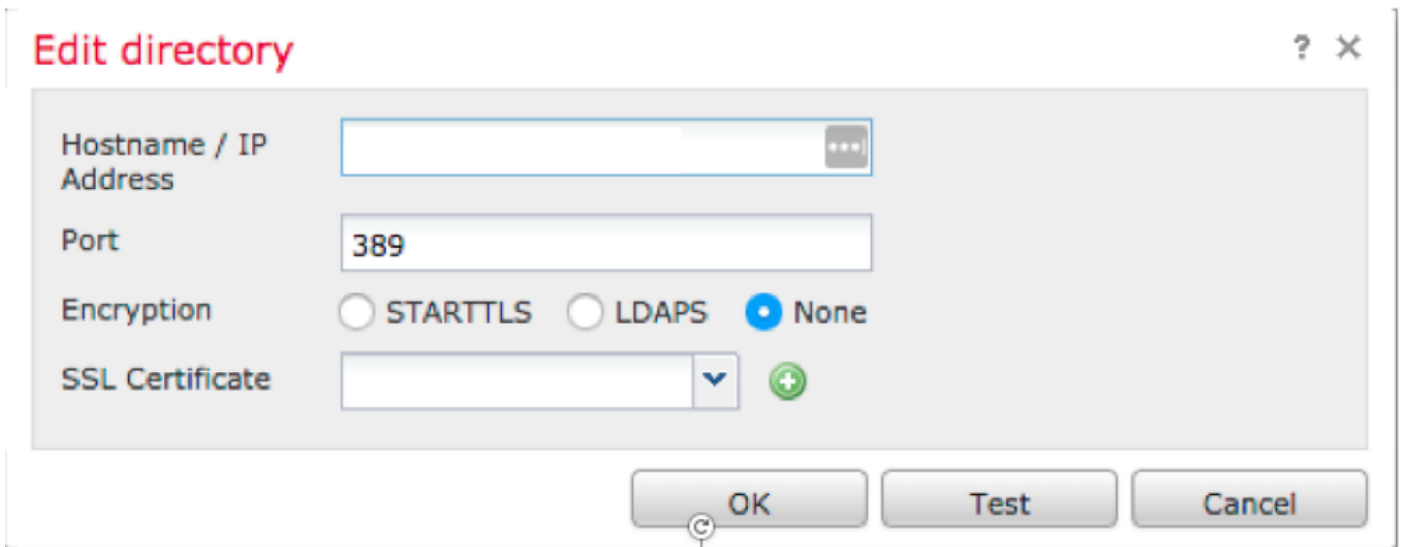
5. 按一下Directory頁籤，然後按一下Add directory，如下圖所示。



6. 配置IP/主機名並測試連線。

注意：如果測試失敗，請在「領域配置」頁籤上驗證憑據。

7.按一下**確定**。



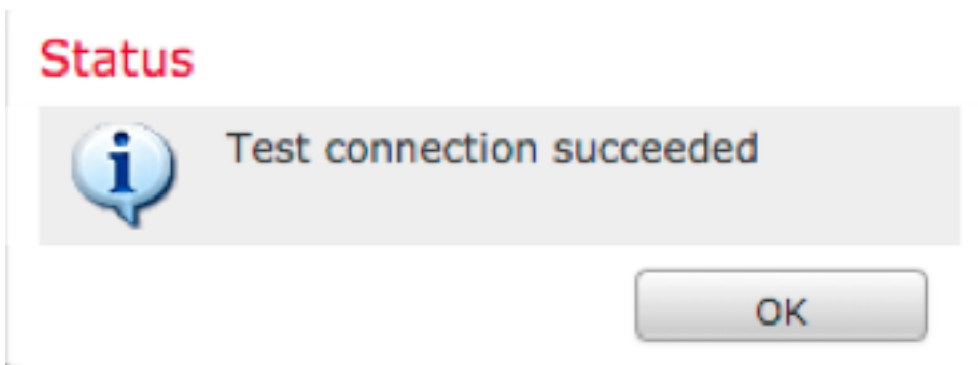
Edit directory ? X

Hostname / IP Address

Port

Encryption STARTTLS LDAPS None

SSL Certificate



Status

Test connection succeeded

8.按一下**User Download**頁籤。



Overview Analysis Policies Devices Objects AMP Intelligence Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

LAB Enter Description

Directory Realm Configuration **User Download**

9.如果尚未選擇，請啟用使用者和組下載

10.按一下「立即下載」



LAB

Enter Description

Directory Realm Configuration **User Download**

Download users and groups

Begin automatic download at America/New York Repeat Every Hours

11.填寫清單後，新增所需的組，然後選擇**Add to Include**。

12. 儲存領域配置。

Overview Analysis Policies Devices Objects AMP Intelligence

LAB

Download users and groups

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

Download Now

Available Groups

Groups to Include (35)

Groups to Exclude (0)

Save

13. 啟用「領域狀態」。

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=rtpaaa,DC=net	CN=Users,DC=rtpaaa,DC=	member	Compare realms

步驟5. 生成FMC CA證書

1. 導覽至對象>對象管理>內部CA，如下圖所示。

Overview Analysis Policies Devices Objects AMP Intelligence

Object Management Intrusion Rules

Name	Value	Type	Override
any		Group	X
any-ipv4		Network	X
any-ipv6		Host	X
IPv4-Benchmark-Tests		Network	X
IPv4-Link-Local		Network	X
IPv4-Multicast		Network	X
IPv4-Private-10.0.0.0-9		Network	X
IPv4-Private-172.16.0.0-12		Network	X
IPv4-Private-192.168.0.0-16		Network	X
IPv4-Private-A8-RFC1918		Group	X
IPv6-IPv4-Mapped		Network	X
IPv6-Link-Local		Network	X
IPv6-Private-Unique-Local-Addresses		Network	X
IPv6-to-IPv4-Relay-Anycast		Network	X

2. 按一下生成CA。

3. 填寫該表單並按一下Generate self-signed CA。



Generate Internal Certificate Authority

Name:

Country Name (two-letter code):

State or Province:

Locality or City:

Organization:

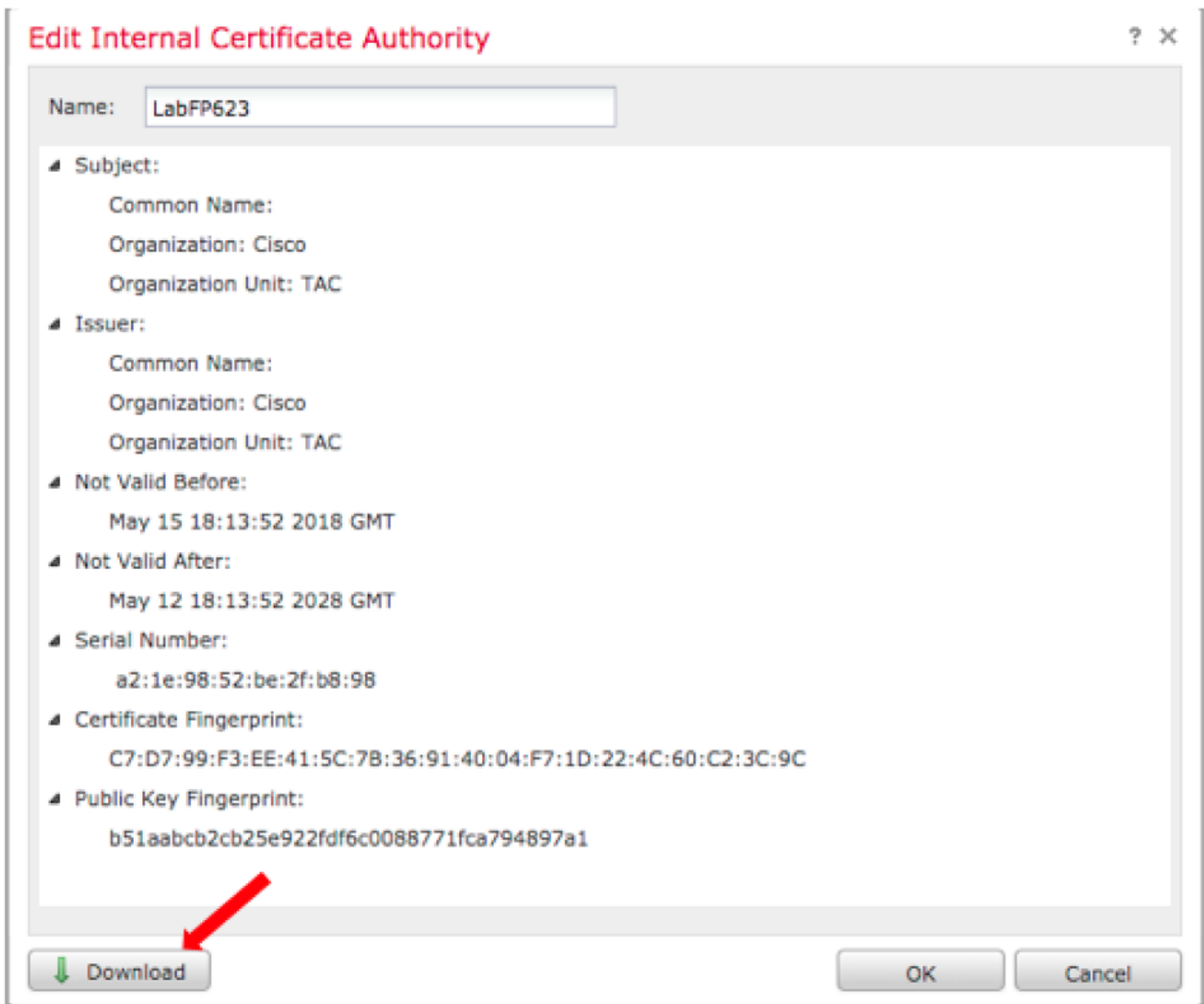
Organizational Unit (Department):

Common Name:

4. 生成完成後，按一下生成的CA證書右側的鉛筆，如下圖所示。



5. 按一下「Download」。



6. 配置並確認加密密碼，然後按一下OK。

7. 將公鑰加密標準(PKCS)p12檔案儲存到本地檔案系統。

步驟6. 使用OpenSSL從產生的憑證中提取憑證和私密金鑰

此操作在FMC的根目錄上或在任何支援OpenSSL命令的客戶端上完成。此示例使用標準的Linux shell。

1. 使用openssl從p12檔案中提取憑證(CER)和私鑰(PVK)。

2. 提取CER檔案，然後配置FMC上證書生成的證書匯出金鑰。

```
~$ 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. 提取PVK檔案，配置證書匯出金鑰，然後設定新的PEM密碼短語並進行確認。

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

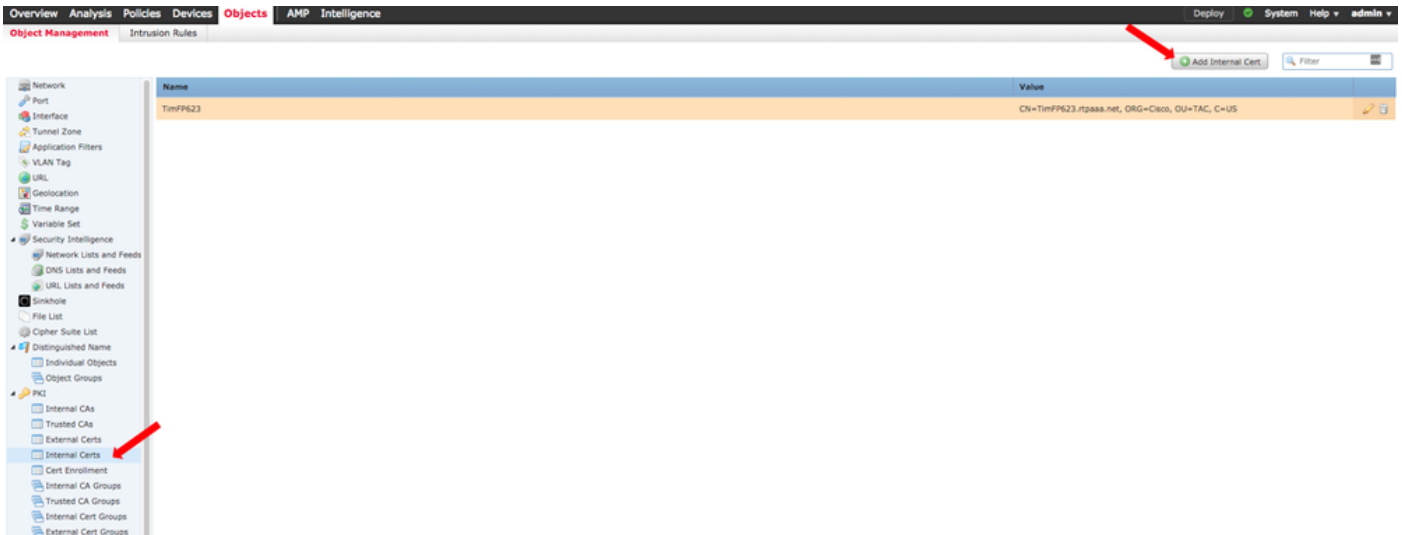
Password: Last login: Tue May 15 18:46:41 UTC 2018 Enter Import Password: MAC verified OK

4. 下一步需要使用PEM短語。

步驟7. 將證書安裝到FMC

1. 導航到對象>對象管理> PKI >內部證書。

2. 按一下「Add Internal Cert」，如下圖所示。



3. 配置內部證書的名稱。

4. 瀏覽到CER檔案的位置並將其選中。填寫「Certificate Data」後，選擇第二個。

5. 瀏覽選項並選擇PVK檔案。

6. 刪除PVK部分中的任何前導「Bag attributes」和所有尾隨值。PVK以-----BEGIN ENCRYPTED PRIVATE KEY (開始加密私鑰) 開頭，以-----END ENCRYPTED PRIVATE KEY (結束加密私鑰) 結束。

註：如果PVK文本的前導和尾隨連字元之外有任何字元，則無法按一下OK。

7. 選中Encrypted框並配置在步驟6匯出PVK時建立的密碼。

8. 按一下確定。

Add Known Internal Certificate



Name:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDFTCCAmWgAwIBAgIJAKIemFK+L7iYMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNV
BAYTAIVTMQswCQYDVQQIDAJOQzEMMAoGA1UEBwwDUIRQMQ4wDAYDVQQKDAVDaXNj
bzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDDBNMYWJGUDYyMy5ydHBhYWEubmV0MB4X
DTE4MDUxNTE4MTM1MloXDTI4MDUxMjE4MTM1MlowZDELMAkGA1UEBhMCVVMxCzAJ
BgNVBAGMAK5DMQwwCgYDVQQHDANSVFaxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQJL
DANUQUxHDAaBgNVBAMME0xhYkZQNjIzLnJ0cGFhYS5uZXQwgwEIMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQMjtS5IUIFIZkZK/TSGtkOCmuivTK5kk1WzAy6
D7Gm/c69cXw/VfIPWnSBzhEkiRTyspmTMdyf/4TJvUmUH60h1O8/8dZeqJOzbjon
-----
```

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="">

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABGkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI5uV3MsiHZsICAggA
MBQGCCqGSIb3DQMHBAAhgGVm1+xHLIASCBMjjJxkffXUNUcdB22smybvWotwbcRrt
xL0qjEStmwuyExVp+TWC3AyIJN1DE7/rRssjRAqsnSOxIvDGmg0dVsvnbqZwjFP
74POu/O2Vy99iFoVgW2q9DyXyL/h64TH9CZtwLKIOGOeEunNKpamDnpfyN8QC4DC
fXvNZ8jNG4HrEcFmnnij0EwJ0QT8Jn5gAUj+AIPMe32zPqwocCRNYrRXMVM9+Jwp
-----
```

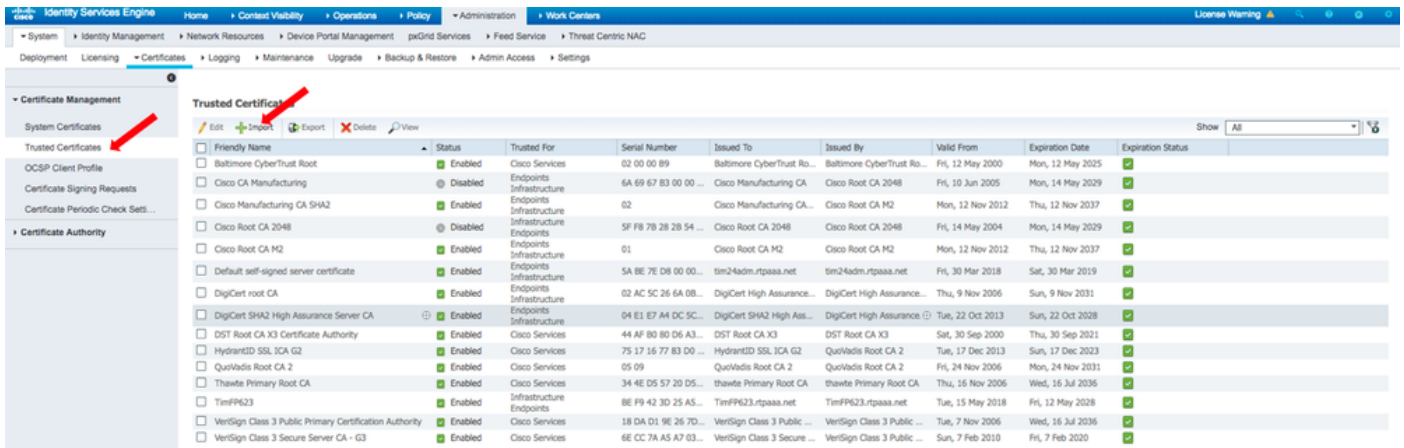
Encrypted, and the password is:

```
cfCJU2QGI4jT0SorN4u2Lk+S+Qd1s7Ii2wIQMWKPI2R9UGv1tyM6HTPCGoCo6VDI
acCICUasecVrYY081GKTVVJ3bWgWfPtR3OH12YCA2whcCKcG50MByB4tjhHN036q
O/g=
-----END ENCRYPTED PRIVATE KEY-----
</no> ← DELETE
```

Encrypted, and the password is:

步驟8.將FMC證書匯入ISE

- 1.訪問ISE GUI並導航到管理>系統>證書>受信任證書。
- 2.按一下匯入。



3.按一下**Choose File**，然後從本地系統中選擇FMC CER檔案。

可選：配置友好名稱。

4.檢查ISE內的Trust身份驗證。

可選：配置說明。

5.按一下「**Submit**」，如下圖所示。

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

步驟9.在FMC上配置pxGrid連線

1.導覽至System > Integration > Identity Sources，如下圖所示。



2.按一下ISE。

3.配置ISE pxGrid節點的IP地址或主機名。

4.選擇pxGrid伺服器CA右側的+。

5.命名伺服器CA檔案，然後瀏覽到步驟3中收集的pxGrid根簽名CA。然後按一下**Save**。

6.選擇MNT Server CA右側的**+**。

7.命名伺服器CA檔案，然後瀏覽到步驟3中收集的Admin證書。然後按一下**Save**。

8.從下拉選單中選擇**FMC CER**檔案。

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.按一下**測試**。

10.如果測試成功，請按一下**確定**，然後按一下螢幕右上角的**儲存**。

Status

ISE connection status:
Primary host: Success

Additional Logs

注意：運行兩個ISE pxGrid節點時，一個主機顯示成功(Success)和一個主機顯示失敗(Failure)是正常現象，因為pxGrid一次只在一個ISE節點上主動運行。這取決於配置哪個主主機可能會顯示Failure，哪個輔助主機可能會顯示Success。這取決於ISE中的哪個節點是活動的pxGrid節點。

驗證

在ISE中驗證

1.開啟ISE GUI並導航到**管理 > pxGrid服務**。

如果成功，客戶端清單中將列出兩個firepower連線。一個用於實際FMC(iseagent-hostname-33bytes)，另一個用於測試裝置(firesightstest-hostname-33bytes)。



iseagent-firepower連線顯示六(6)個子並線上顯示。

firesightstestest-firepower連線顯示零(0)個子網，並且顯示為離線。

iseagent-firepower客戶端的展開檢視顯示六個訂閱。

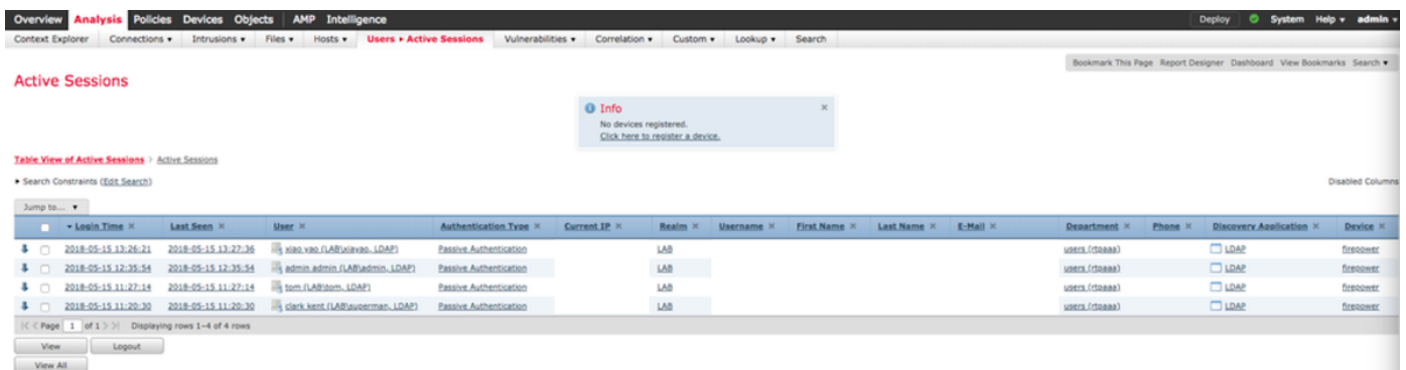


註：由於Cisco錯誤[IDCSCvo75376](#) 存在主機名限制，批次下載失敗。FMC上的測試按鈕顯示連線故障。這會影響2.3p6、2.4p6和2.6。當前建議運行2.3補丁5或2.4補丁5，直到發佈正式補丁。

在FMC中驗證

1. 開啟FMC GUI並導航至分析>使用者>活動會話。

通過ISE中的會話目錄功能發佈的所有Active Sessions都顯示在FMC上的Active Sessions表中。



在FMC CLI sudo模式下，「adi_cli session」顯示從ISE傳送到FMC的使用者會話資訊。

```
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.
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。