# PNP عم PNP مادختساب ةقلعتملا لكاشملا ثدحألا Cisco IOS® تارادصإ ىلع

# تايوتحملا

## ەمدقملا

ةيساسألا ةينبلا" نم اهريدصتو ةحيحصلا ةداهشلا ءاشنا ةيفيك دنتسملا اذه حضوي ريدم" ىلع (PNP) "ليغشتلاو ليصوتلا" عم مادختسالل (Windows" (PKI) ل صاخلا حاتفملل لقحلا ةكبش.

# ةلكشملا

نم ثدحأ قالطإ ىلع (ZTD) سمل نودب رشن متي نأ PNP لمعتسي نأ تنأ لواحي امدنع Cisco نم ثدحأ قالطإ ىلع (IOS®-XE، اطخ اذه نم دحاو عم لشفي ةيلمعل

Error while creating FND trustpoint on the device. errorCode: PnP Service Error 3341, errorMessage: SSL Server ID check failed after cert-install Error while creating FND trustpoint on the device. errorCode: PnP Service Error 3337, errorMessage: Cant get PnP Hello Response after cert-install

ليدبلا مسالا" لقح علم Cisco IOS® /Cisco IOS®-XE يف PNP زمر بلطتي ،تقولا ضعب ذنم (قراحلا هذه يف FND) مكحتلا ةدحو/مداخ لبق نم ةمدقملا ةداهشلا يف "(SAN) عوضوملل.

ليكو ققحتي PNP Cisco IOS® قداهش لقح نم طقف®PNP Cisco IOS ليكو ققحتي عئاشلا مسالا لقح نم (CN).

تارادصإلا ەذەل حلاص اذە:

- ثدحألا تارادصإلاو Cisco IOS® رادصإلا ®Cisco IOS جمانرب ∙
- Cisco IOS®، ثدحألا تارادصإلاو 15.6(3)M4 رادصإلا
- ثدحألا تارادصإلاو Cisco IOS®، (ادصإلا، ®Cisco IOS جمانرب ∙
- Cisco IOS® XE Denali 16.3.6 ثدحألا تارادصإلاو
- Cisco IOS® XE Everest، ثدحألاا تارادصإلاا الماع الماع المعاليا الماية الماية الماية الماية الماية الماية الم
- ثدحألاا تارادصإلاو 16.6.3 رادصإلا، Cisco IOS® Everest ،
- ثدحألا تارادصإلاو 16.7.1 نم ©Cisco IOS تارادصإ عيمج •

انه تامولعملا نم ديزم ىلع روثعلا نكمي: <u>https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-</u> <u>Play/solution/guidexml/b\_pnp-solution-guide.html#id\_70663</u>

# الحل

ةكبش لقح نأ دعب ةيمنتلاا لجأ نم ةينطولا تاوقلاب ةصاخلا قئاثولاو ةلدألا مظعم ركذت ال ميمعتلا يل قجاحب نيزختلا ةقطنم.

حيتافملا نزخم ىلا اەتفاضاو PNP عم مادختسالل اەريدصتو ةحيحصلا ةداەشلا ءاشنال، قيلاتلا تاوطخلا عبتا.

Windows CA مداخ ىلع FND/NMS بلاق مادختساب ةديدج ةداەش ءاشنإ

ح **ةفاضإ < تاداەش < ..ةيفاضإ ةادأ ةلاز/ةفاضإ < فلم < MMC > ليغ<b>شت < أدبا** ىلإ لقتنا تاداەشلل MMC ةيفاضإلا ةادألا حتفاو **قفاوم < يلحم رتويبمك < رتويبمك باسح**.

تاداهش < يصخش < (يلحم رتويٻمك) تاداهشلا ديدمت

يف حضوم وه امك **..ةديدج قداهش بلط < ماهملا لك** ددحو تاداهشلا ىلع نميألا سواملا رزب رقنا ةروصلا.

Console Root	Issued To 🔺		Issued By
🖃 🔜 Certificates (Local Computer)	🛱 fndserver.fnd.iot		rootca
🖃 🧮 Personal	😨 nms.fnd.iot		rootca
🚞 Certifica <del>tor</del>	l @		
	<u> </u>	Request New Certificat	e
🛨 🧮 Enterprise T 🛛 <sub>View</sub>	+	Import	
🗉 🦰 Intermediat			

.ةروصلا يف حضوم وه امك **Active Directory ليجست جهن** ددحو **يلاتلا** قوف رقنا



مداخ ل اقحال كلذ راركت) NMS/FND-Server ل هؤاشنا مت يذلا بلاقلا ددجو **يلاتلا** قوف رقنا تا يو حضوم وه امك تامولعملا نم ديزم طابترا قوف رقناو ((TelePresence (TPS)

Request Certificates		
You can request the following types of certifica	ates. Select the certificates you want to reque	est, and then click Enrol
Active Directory Enrollment Polic	×V	
Directory Email Replication	i) STATUS: Available	Details 🛞
Domain Controller	i) STATUS: Available	Details 🛞
Domain Controller Authentication	i) STATUS: Available	Details 🛞
EFAD	) CTATUS Auditio	Datail-

:تامولعملا هذه ريفوتب مق ،ةداهشلا صئاصخ يف

عوضوملا مسا:

- كتسسؤم مسا :ةسسؤملا •
- كلذ ناك اذإ TPS وأ) FND مداخب صاخلا (FQDN) لماكلاب لەؤملا لاجملا مسا :ع&اشلا مسالا) (انكمم

((SAN)): نيزختالا ةقطنم ةكبش لقح) ليدبالا مسالا

- مقف ،FND مداخ نم PNP ءزجب لاصتالل (DNS) لاجملا مسا ماظن مدختست تنك اذإ ل DNS لخدا ةفاضإب FQDN ل
- IP ل IPv4 لاخدا ةفاضإب مقف ،FND مداخ نم PNP ءزجب لاصتالل IP مدختست تنك اذا •

فالتخأ ةلااح يف ،قداهشلاا يف قددعتم (SAN) نيزخت ةقطنم ةكبش ميق نيمضتب ىصوي مكحتلا قدحول FQDN نم لك نيمضت كنكمي ،لاثملا ليبس ىلع .قلاحلا فاشتكا قرط مقف ،امەيلك نيمضتب تمق اذإ .(SAN) نيزختلا ةكبش لقح يف (NAT IP ناونع وأ) IP ناونعو تيوعتب IP، ناونعب اعوبتم ،(SAN) نيزختلا قكبشل قميق لوأك FQDN نيوعتب

ليكشت لاثم:

Certificate Properties		×		
🔥 Subject General Extension	s Private Key Certificatio	n Authority Signature		
The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.				
Subject of certificate The user or computer that is receiv	ving the certificate			
Subject name:				
Туре:		O=Cisco		
Common name	Add >			
Value:				
	< Remove			
Alkaurasti uz anazu				
	]	DNS		
TD address (u4)		nms.fnd.iot		
IP address (V4)		10.48.43.229		
Value:	odd S			
	Aug >			
	< Remove			

مث ،ةداەشلا ءاشنال **لجس** مث ،ةداەشلا صﺉاصخ راطا يف **قڧاوم** قوف رقنا ،اەلامتكا درجمبو ءاشنالا لامتكا دنع **ءاەنا** قوف رقنا.

### اەؤاشنإ مت يتلا ةداەشلا يف (SAN) نيزختلا ةكبش لقح نم ققحت

كنكمي ،ةحيحصلا تامولعملا ىلع يوتحت اەۋاشنإ مت يتلا ةداەشلا تناك اذا امم ققحتلل يلي امك اەصحف:

تاداەشلا عسوو (Microsoft Management Console (MMC) يف تاداەشلا قادألا حتفا تاداەش < يصخش < (يلحملا رتويبمكلا).

مق .**ليصافت** بيوبتلا ةمالع حتفاو اهؤاشنا مت يتلا ةداهشلا ىلع اجودزم ارقن رقنا ةروصلا يف حضوم وه امك (SAN) نيزختلا ةكبش لقح نع ثحبلل لفسأل ريرمتلاب.

rtificate General Details Certification Path		×
Show: <ali></ali>	<b>T</b>	
Field	Value	
<ul> <li>Enhanced Key Usage</li> <li>Key Usage</li> <li>Application Policies</li> <li>Subject Key Identifier</li> <li>Subject Alternative Name</li> <li>Authority Key Identifier</li> <li>CRL Distribution Points</li> <li>Authority Information Access</li> </ul>	Server Authentication (1.3.6 Digital Signature, Non-Repudia [1]Application Certificate Polic 8b 3b 34 3d da 09 ae 49 30 d8 DNS Name=nms.fnd.iot, IP Ad KeyID=6a 73 6b c7 e2 2c 43 1 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc	
DNS Name=nms.fnd.iot IP Address=10.48.43.229		

### FND حيتافم نزخم ىلإ ةداەشلا ريدصت

ىلإ جاتحت ،FND حيتافم نزخم يف ةدوجوملا ةداەشلا لادبتسإ وأ داريتسإ نم نكمتت نأ لبق فلم ىلإ اەريدصت **.pfd**.

**ي**صخش < (يلحم رتويٻمك) تاداەشلا</mark> عيسوتب مق ،MMC يف تاداەشلل ةيفاضإلا ةادألا يف تاداەش <

وه امك ..**.ريدصت < ماهملا ةفاك** ددحو اهؤاشنإ مت يتلا ةداهشلا قوف نميألا سواملا رزب رقنا .ةروصلا يف حضوم

Consoler - Econsole Kooc/cercin	caces (cocar con	ipucery/rerson	arvereneaces]		
🚠 File Action View Favorites	Window Help				
🧇 🔿 🖄 📅 🖌 👫 🗮 🗶 🛛	1 🔒 🛛 🖬				
Console Root	Issued To 🔺		Issued By	Expi	
🖃 🔜 Certificates (Local Computer)	🔄 🖾 🖾	iot	rootca	5/03	
🖃 🧮 Personal	🙀 nms.fnd.iot 👔		rootca	6/03	
Certificates	😨 ra	😨 ra	Open	rootca	4/03
🕀 🚞 Trusted Root Certification A	🤹 ra	All Tasks 🔹 🕨	Open	4/03	
🕀 🚞 Enterprise Trust	🤹 ra			4/03	
🕀 🚞 Intermediate Certification A	🤹 ra	Cut	Request Certificate with New Key	4/03	
🛨 🚞 Trusted Publishers	電ra 電ra 電rootca 気rootca.fnd.iot	Сору	Renew Certificate with New Key	4/03	
🕀 🚞 Untrusted Certificates		Delete	Managa Dviuska Kaus	4/03	
표 🚞 Third-Party Root Certificati			Manage Private Reys	5/03	
🛨 🚞 Trusted People		Properties	Advanced Operations	- 4/02	
🕀 🚞 Remote Desktop		Help	Export	4703	
🛨 🚞 Certificate Enrollment Requ					
l 🗁 🍽 e lie le lie i 📗	1				

#### Certificate Export Wizard

#### **Export Private Key**

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

×

Do you want to export the private key with the certificate?

- Yes, export the private key
- 🔘 No, do not export the private key

ةروصلا يف حضوم وه امك صيخرتلا راسم يف تاداهشلا لك نيمضتل ددح.

Tranne all celaricates in a le celaricador harrur hossine.

- Personal Information Exchange PKCS #12 (.PFX)
  - Include all certificates in the certification path if possible
  - Delete the private key if the export is successful
  - Export all extended properties
- C Microsoft Serialized Certificate Store (.SST)

.فورعم ناكم يف pf**x.** لا ظفحاو ريدصتلل رورم ةملك ددح ،**كلذ دعب** رقنا

### PNP عم مادختسالل FND حيتافم نزخم ءاشنإ

. FND ل بولطملا حيتافملا نزخم ءاشنإ كنكمي ،ةداهشلا ريدصتب تمق نأ دعب نآلا

لقنب مق (NMS) ةكبشلا ةرادا ةمظنأ زاهج ىلإ نامأب ةقباسلا ةوطخلا نم **مؤاشنا مت يذلا pfx.** لقنب مق (NMS) فيضم وأ مادختساب لاثملا ليبس ىلع ،(FND مداخ) SCP.

:ريدصتلا يف ايئاقلت ەؤاشنإ مت يذلا راعتسملا مسالا ىلع فرعتلل **pfx.** تايوتحم درس

[root@iot-fnd ~]# keytool -list -v -keystore nms.pfx -srcstoretype pkcs12 | grep Alias Enter keystore password: keystore Alias name: le-fnd-8f0908aa-dc8d-4101-a526-93b4eaad9481 زرمال اذه مادختس اب دیدج حیتاف م نزخم عاش ن 93b4eaad9481 -destalias cgms -destkeypass keystore Importing keystore nms.pfx to cgms\_keystore\_new... Enter destination keystore password: Re-enter new password: Enter source keystore password: [Storing cgms\_keystore\_new]

Warning:

The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore cgms\_keystore\_new - destkeystore cgms\_keystore\_new -deststoretype pkcs12".

ةميق نأو (Windows CA نم ردصملا) حيحصلا فلملاب **nms.pfx** لابتسإ نم دكأت ،رمألا يف srcalias قراطت (**keyTool -list**).

حرتقم وه امك ديدجلا قيسنتلا ىل المليوحتب مق ،هديلوتب موقت نأ دعب:

[root@iot-fnd ~]# keytool -importkeystore -srckeystore cgms\_keystore\_new -destkeystore
cgms\_keystore\_new -deststoretype pkcs12 Enter source keystore password: Entry for alias cgms
successfully imported. Import command completed: 1 entries successfully imported, 0 entries
failed or cancelled Warning: Migrated "cgms\_keystore\_new" to Non JKS/JCEKS. The JKS keystore is
backed up as

"cgms\_keystore\_new.old".

### حيتافملا نزخم ىلإ ،اقباس اەريدصت مت يتلا ،قدصملا عجرملا ةداەش ةفاضإ:

[root@iot-fnd ~]# keytool -import -trustcacerts -alias root -keystore cgms\_keystore\_ new -file rootca.cer Enter keystore password: Owner: CN=rootca, DC=fnd, DC=iot Issuer: CN=rootca, DC=fnd, DC=iot ... Trust this certificate? [no]: yes Certificate was added to keystore

ةداەش ةفاضإب مق ،اريخاو SUDI، نم لسلستب قي ان مقى انم قىقىت مىل بەل انم قىقىت بەل بەل انم قى بارىخاو مدختست امدن ع

بيكرتل RPM، بيف اهيلع روثعلا نكميو مزحلا عم SUDI ةداهش عيمجت متي PPM، بيكرتل /opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem

:فيضملا يل SUDI ةداهش خسنب الوأ مق ،OVA تيبثتل

[root@iot-fnd ~]# docker cp fnd-container:/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem

:SUDI راعتسملا مسالاً عم هب قوثوم وه امك حيتافملاً نزخم ىلاٍ هتفاضإب مق مث

[root@iot-fnd ~]# keytool -import -trustcacerts -alias sudi -keystore cgms\_keystore\_new -file cisco-sudi-ca.pem Enter keystore password: Owner: CN=ACT2 SUDI CA, O=Cisco Issuer: CN=Cisco Root CA 2048, O=Cisco Systems ... Trust this certificate? [no]: yes Certificate was added to keystore ةيمنتلل ينطولا قودنصلا عم مادختسالل ازهاج حيتافملا رجتم نوكي ،ةطقنلا هذه دنعو.

### FND عم مادختسالل لدعملا/ديدجلا حيتافملا نزخم طيشنت

رورملا ةملك ثيدحتب مقو قباسلا رادصإلا لادبتساب مق ،حيتافملا نزخم مادختسإ لبق فلم يف يرايتخإ لكشب cgms.properties.

:لعفلاب دوجوملا حيتافملا نزخمل يطايتحإ خسن ةيلمع ءارجإب مق ،الوأ

تيبثتل RPM:

[root@fndnms ~]# cp /opt/cgms/server/cgms/conf/cgms\_keystore cgms\_keystore\_backup تىىثتل OVA:

[root@iot-fnd ~]# cp /opt/fnd/data/cgms\_keystore cgms\_keystore\_backup ةديدجلاب قمئاقلا لدبتسا

RPM: تيبثتل

[root@fndnms ~]# cp cgms\_keystore\_new /opt/cgms/server/cgms/conf/cgms\_keystore تىبثتل OVA:

[root@iot-fnd ~]# cp cgms\_keystore\_new /opt/fnd/data/cgms\_keystore فلم يف حيتافملا نزخمل رورملا قملك ثيدحتب مق ،يرايتخإ لكشب:

.ةديدج ةرفشم رورم ةملك ةلسلس ءاشنإب مق ،الوأ

تيبثتل RPM:

[root@fndnms ~]# /opt/cgms/bin/encryption\_util.sh encrypt keystore
7jlXPniVpMvat+TrDWqh1w==

OVA: تيبثتل

[root@iot-fnd ~]# docker exec -it fnd-container /opt/cgms/bin/encryption\_util.sh encrypt keystore 7jlXPniVpMvat+TrDWqh1w== حيتافملا نزخمل ةحيحصلا رورملا قملكب حيتافملا نزخم لادبتسإ نم دكأت.

تيبثتلل cgms.properties رييغتب مق

نيمضتل OVA ىلإ دنتسملا تيبثتلل **opt/fnd/data/cgms.properties وأ** RPM ىلإ دنتسملا ةديدجلا ةرفشملا رورملا ةملك.

نيديدجلا رورملا ةملكو حيتافملا نزخم مادختسإ ءدبل FND ليغشت ةداعإب مق ،اريخأو.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما