Creazione di certificati SAN per l'integrazione IND e ISE pxGrid mediante OpenSSL

Sommario

Introduzione

Questo documento descrive come creare certificati SAN per l'integrazione di pxGrid tra Industrial Network Director (IND) e Identity Services Engine.

Premesse

Quando si creano certificati in Cisco ISE per l'utilizzo con pxGrid, non è possibile immettere nomi host brevi nel server nella GUI di ISE in quanto ISE consente solo l'FQDN o l'indirizzo IP.

Per creare certificati che includono il nome host e il nome di dominio completo (FQDN), è necessario creare un file di richiesta di certificato all'esterno di ISE. A tale scopo, è possibile utilizzare OpenSSL per creare una richiesta di firma del certificato (CSR) con voci del campo SAN (Subject Alternative Name).

Questo documento non include la procedura completa per abilitare la comunicazione pxGrid tra il server IND e il server ISE. Questi passaggi possono essere utilizzati dopo la configurazione di pxGrid ed è stato confermato che il nome host del server è obbligatorio. Se l'errore si verifica nei file di log di ISE Profiler, la comunicazione richiede il certificato del nome host.

```
Unable to get sync statusjava.security.cert.CertificateException: No subject alternative DNS name matcht
```

Le fasi per la distribuzione iniziale di IND con comunicazione pxGrid sono disponibili all'indirizzo https://www.cisco.com/c/dam/en/us/td/docs/switches/ind/install/IND_PxGrid_Registration_Guide_Final.pdf

Applicazioni richieste

- Cisco Industrial Network Director (IND)
- Cisco Identity Services Engine (ISE)
- OpenSSL
    - Nella maggior parte delle versioni Linux moderne, così come in MacOS, il pacchetto OpenSSL viene installato per impostazione predefinita. Se i comandi non sono disponibili, installare OpenSSL utilizzando l'applicazione di gestione dei pacchetti del sistema operativo.

- Per ulteriori informazioni su OpenSSL per Windows, visitare il sito Web all'indirizzo https://wiki.openssl.org/index.php/Binaries

Ulteriori informazioni

Ai fini del presente documento, si utilizzano le seguenti informazioni:

- Nome host server IND: rch-mas-ind
- FQDN: rch-mas-ind.cisco.com
- Configurazione di OpenSSL: rch-mas-ind.req
- Nome file richiesta certificato: rch-mas-ind.csr
- Nome file chiave privata: rch-mas-ind.pem
- Nome file certificato: rch-mas-ind.cer

Fasi del processo

Creare il CSR certificato

1. In un sistema in cui è installato OpenSSL, creare un file di testo della richiesta per le opzioni OpenSSL, incluse le informazioni sulla SAN.
   - La maggior parte dei campi "_default" sono facoltativi, in quanto è possibile immettere le risposte durante l'esecuzione del comando OpenSSL nel passaggio 2.
   - I dettagli della SAN (DNS.1, DNS.2) sono obbligatori e devono includere sia il nome host breve DNS che il nome di dominio completo (FQDN) del server. Se necessario, è possibile aggiungere altri nomi DNS utilizzando DNS.3, DNS.4 e così via.
   - Esempio di file di testo della richiesta:

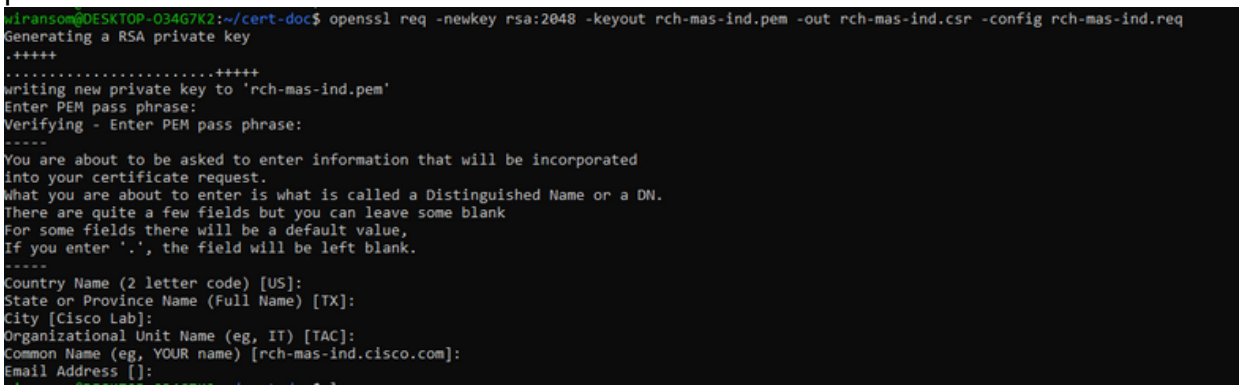
```
[rich.]
nome_distinto = nome
req_extensions = v3_req

[nome]
countryName = Nome del paese (codice a due lettere)
countryName_default = Stati Uniti
stateOrProvinceName = Nome provincia (nome completo)
stateOrProvinceName_default = TX
localityName = Città
localityName_default = Cisco Lab
organizationalUnitName = Nome unità organizzativa (ad esempio, IT)
organizationalUnitName_default = TAC
commonName = Nome comune (ad esempio, NOME UTENTE)
commonName_max = 64
commonName_default = rch-mas-ind.cisco.com
emailAddress = Indirizzo e-mail
emailAddress_max = 40
```

```
[req_v3]
keyUsage = cifraturaChiave, cifraturaDati
extendedKeyUsage = autenticazione server, autenticazione client
subjectAltName = @alt_names

[alt_nomi]
DNS.1 = rch-mas-ind
DNS.2 = rch-mas-ind.cisco.com
```

2. Utilizzare OpenSSL per creare CSR con nome host breve DNS nel campo SAN. Creare un file di chiave privata oltre al file CSR.
    - Comando:
      openssl req -newkey rsa:2048 -keyout <server>.pem -out <server>.csr -config <server>.req
    - Quando richiesto, immettere una password a scelta. Ricordare questa password, come verrà utilizzata nei passaggi successivi.
    - Quando richiesto, immettere un indirizzo e-mail valido oppure lasciare il campo vuoto e premere <INVIO>.



3. Se lo si desidera, verificare le informazioni del file CSR. Per un certificato SAN, verificare "x509v3 Subject Alternative Name" (Nome alternativo soggetto x509v3) come evidenziato in questa schermata.
    - Riga di comando:
      openssl req -in <server>.csr -noout -text

```
wiransom@DESKTOP-O34G7K2:~/cert-doc$ openssl req -in rch-mas-ind.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = US, ST = TX, L = Cisco Lab, OU = TAC, CN = rch-mas-ind.cisco.com, emailAddress = wiransom@cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d5:91:1a:63:df:4e:ee:14:f4:66:d8:86:e8:11:
                    24:11:ab:14:42:34:9d:a7:f1:b1:f3:47:13:b0:83:
                    87:1e:3d:c5:30:bb:59:bd:13:d6:38:e6:bd:70:1b:
                    83:53:9a:fc:a5:22:7e:c0:2f:82:b0:75:31:dd:4f:
                    d2:43:0e:24:e1:22:74:12:2f:a6:a0:0d:35:cb:85:
                    f7:b8:47:4f:16:af:3d:d1:6d:2d:cc:04:ff:e2:d5:
                    dc:68:f1:4f:98:9a:e1:ce:52:45:55:4b:6f:4e:0f:
                    9d:f6:0c:68:f7:b9:ff:33:c9:ed:83:0c:43:ef:
                    b0:43:77:28:6e:ba:51:bd:a7:bb:91:3a:6d:c3:9b:
                    8e:12:c4:80:dc:06:8d:eb:e0:fe:46:11:8d:b2:1b:
                    1f:80:76:a4:40:06:89:6b:1d:59:01:80:00:d4:d2:
                    23:da:df:14:50:aa:08:02:04:9d:87:ff:df:58:39:
                    79:c5:c6:3e:3c:3d:4a:8e:19:c2:c3:16:36:9f:dc:
                    58:69:45:76:bb:e7:47:a6:d0:5b:81:54:6f:24:dc:
                    13:96:49:46:eb:c6:c0:83:ed:94:f1:68:41:97:8b:
                    99:b7:8b:98:d4:3c:2c:0b:4c:1f:4b:96:dc:ed:e1:
                    66:a5:a1:d3:da:3a:85:14:e6:53:f0:ff:ff:02:9d:
                    3d:fd
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                DNS:rch-mas-ind, DNS:rch-mas-ind.cisco.com
    Signature Algorithm: sha256WithRSAEncryption
         9a:57:38:13:a5:4a:15:91:e7:bc:63:be:92:b9:8d:5e:ff:67:
         16:ae:0f:07:3d:71:95:10:ec:7d:db:7d:b8:e7:15:42:8e:84:
         80:9c:3e:80:17:88:e4:5a:90:76:c5:11:2e:ad:76:b1:98:5d:
         15:74:9a:19:8d:61:77:88:de:42:ad:da:48:1e:94:68:eb:03:
         1d:15:1e:87:b0:68:d3:af:50:e9:03:8b:b9:03:a8:c1:a0:d8:
         f5:d2:b4:17:2d:82:8a:a3:0b:71:4a:24:6f:9d:a1:e9:23:ef:
         eb:c3:e6:b5:72:11:93:3f:33:1a:f5:ed:02:14:a6:77:5f:99:
         66:91:33:2d:ad:de:bd:09:32:09:dc:89:c0:4b:2f:d7:a4:e5:
         b9:c8:89:a4:5d:fb:80:bd:db:80:d1:d8:fd:9c:f4:30:79:2a:
         da:81:03:59:f9:7d:4b:79:0c:df:61:bd:c2:15:ee:23:ed:40:
         e2:90:bc:4b:f5:9d:48:5d:10:72:48:23:ef:3f:64:46:f3:ad:
         f3:de:be:15:f8:e7:9f:01:df:6e:a1:95:9f:63:4e:57:d3:45:
         75:93:a4:81:04:d9:06:c8:5d:92:f8:61:f0:ad:7d:da:35:e0:
         13:f4:2b:05:bd:68:4b:5a:0c:c0:24:22:ef:fa:5a:ad:46:42:
         01:ff:6a:74
```

4. Aprire il file CSR in un editor di testo. Per motivi di sicurezza, lo screenshot di esempio è incompleto e modificato. Il file CSR effettivamente generato contiene più righe.

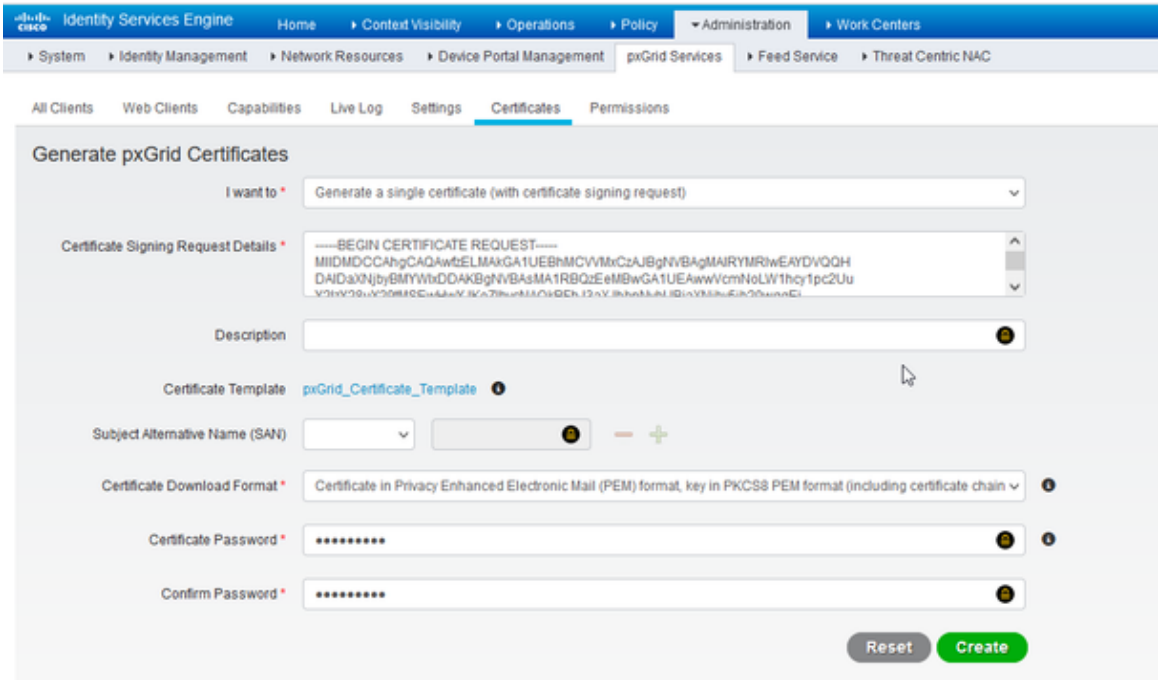
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDMDCCAhgCAQAwfzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMRIwEAYDVQQH
DAlDaXNjbyBMYWIxDDAKBgNVBAsMA1RBQzEeMBwGA1UEAwwVcmNoLW1hcy1pbmQu
Y2lzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJ3aXJhbnNvbUBjaXNjby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVkRpj307uFPRm2IboESQRqxRC
NJ2n8bHzRxOwg4cePcUwu1m9E9Y45r1wG4NTmvylIn7AL4KwdTHdT9JDDiThInQS
L6agDTXLhfe4R08Wrz3RbS3MBP/i1dxo8U+YmuHOUkVVS29OD532DGj3uf8zye2D
@iPa3xRQqggCBJ2H/99YOXnFxj48PUqOGcLDFjaf3FhpRXa750em0FuBVG8k3BOW
AAGgbDBqBgkqhkiG9w0BCQ4xXTBbMAsGA1UdDwQEAwIEMDAdBgNVHSUEFjAUBggr
BgEFBQcDAQYIKwYBBQUHAwIwLQYDVR0RBCYwJIILcmNoLW1hcy1pbmSCFXJjaC1t
YXMtaW5kLmNpc2NvLmNvbTANBgkqhkiG9w0BAQsFAAOCAQEAmlc4E6VKFZHnvGO+
krmNXv9nFq4PBz1xlRDsfdt9uOcVQo6EgJw+gBeI5FqQdsURLq12sZhdFXSaGY1h
d4jeQq3aSB6UaOsDHRUeh7Bo069Q6QOLuQOowaDY9dK0Fy2CiqMLcUokb52h6SPv
Af9qdA==
-----END CERTIFICATE REQUEST-----
```

5. Copiare il file della chiave privata (<server>.pem) nel PC come verrà utilizzato in un passaggio successivo.

Usare Cisco ISE per generare un certificato, usando le informazioni del file CSR creato

Nell'interfaccia grafica di ISE:

1. Rimuovere il client pxGrid esistente.
    - Selezionare Amministrazione > pxGrid Services > Tutti i client.
    - Individuare e selezionare il nome host del client esistente, se elencato,
    - Se è stato trovato e selezionato, fare clic sul pulsante Elimina e scegliere "Elimina selezione". Confermare se necessario.
2. Creare il nuovo certificato.
    - Fare clic sulla scheda Certificati nella pagina dei servizi di pxGrid.
    - Selezionare le opzioni:
        - "Voglio":
            - "Genera un singolo certificato (con richiesta di firma certificato)"
        - "Dettagli richiesta firma certificato:
            - Copiare/incollare i dettagli CSR dall'editor di testo. Assicurarsi di includere le righe BEGIN e END.
        - "Formato download certificato"
            - "Certificato in formato PEM (Privacy Enhanced Electronic Mail), chiave in formato PEM PKCS8."
        - Immettere una password per il certificato e confermarla.
        - Fare clic sul pulsante Crea.



        - Verrà creato e scaricato un file ZIP contenente il file del certificato e altri file per la catena di certificati. Aprire il file ZIP ed estrarre il certificato.
            - Il nome file è normalmente <IND server fqdn>.cer
            - In alcune versioni di ISE, il nome del file è <IND fqdn>_<IND short name>.cer

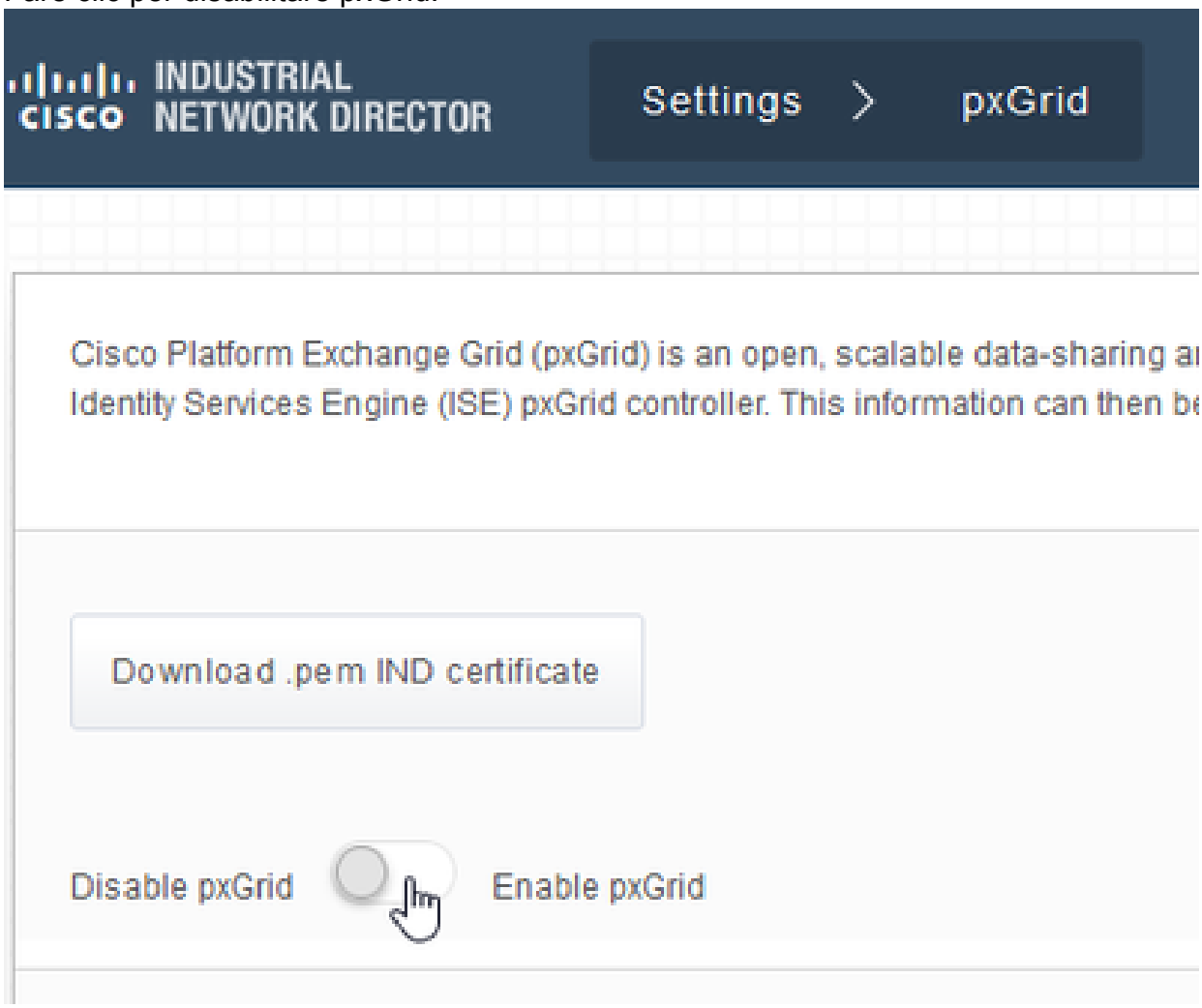
Importare il nuovo certificato nel server IND e abilitarlo per l'utilizzo con pxGrid

Nell'interfaccia dell'IND:

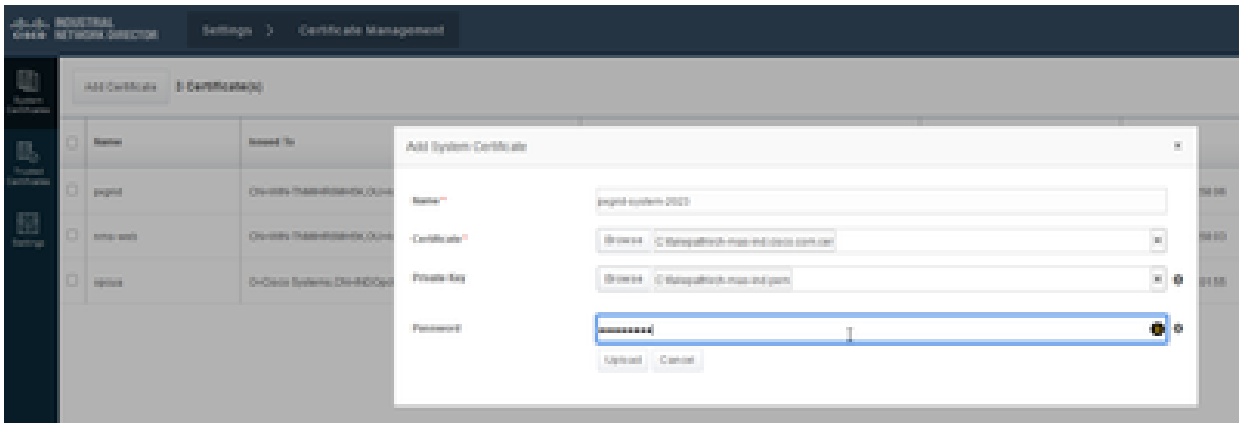
1. Disabilitare il servizio pxGrid in modo che il nuovo certificato possa essere importato e

impostato come certificato attivo.

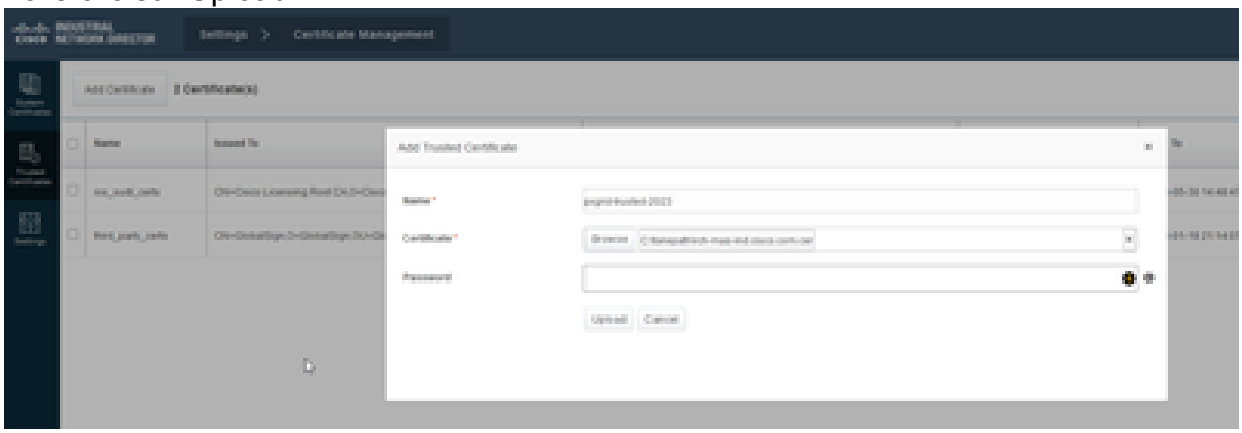
- Selezionare Impostazioni > pxGrid.
- Fare clic per disabilitare pxGrid.



2. Importare il nuovo certificato in Certificati di sistema.
   - Passare a Impostazioni > Gestione certificati.
   - Fare clic su Certificati di sistema.
   - Fare clic su Aggiungi certificato.
   - Immettere il nome di un certificato.
   - Fare clic su "Sfoglia" a sinistra di "Certificato" e individuare il nuovo file di certificato.
   - Fare clic su Sfoglia a sinistra di Certificato e individuare la chiave privata salvata durante la creazione del CSR.
   - Immettere la password utilizzata in precedenza durante la creazione della chiave privata e di CSR con OpenSSL.
   - Fare clic su "Upload".



3. Importare il nuovo certificato come certificato attendibile.
    - Passare a Impostazioni > Gestione certificati e fare clic su "Certificati attendibili".
    - Fare clic su Aggiungi certificato.
    - Immettere un nome di certificato. Il nome deve essere diverso da quello utilizzato nei certificati di sistema.
    - Fare clic su "Sfoglia" a sinistra di "Certificato" e individuare il nuovo file di certificato.
    - Il campo della password può essere lasciato vuoto.
    - Fare clic su "Upload".



4. Impostare pxGrid per utilizzare il nuovo certificato.
    - Passare a Impostazioni > Gestione certificati e fare clic su "Impostazioni".
    - Se non è già stato fatto, selezionare "Certificato CA" in "pxGrid".
    - Selezionare il nome del certificato di sistema creato durante l'importazione.
    - Fare clic su Salva.

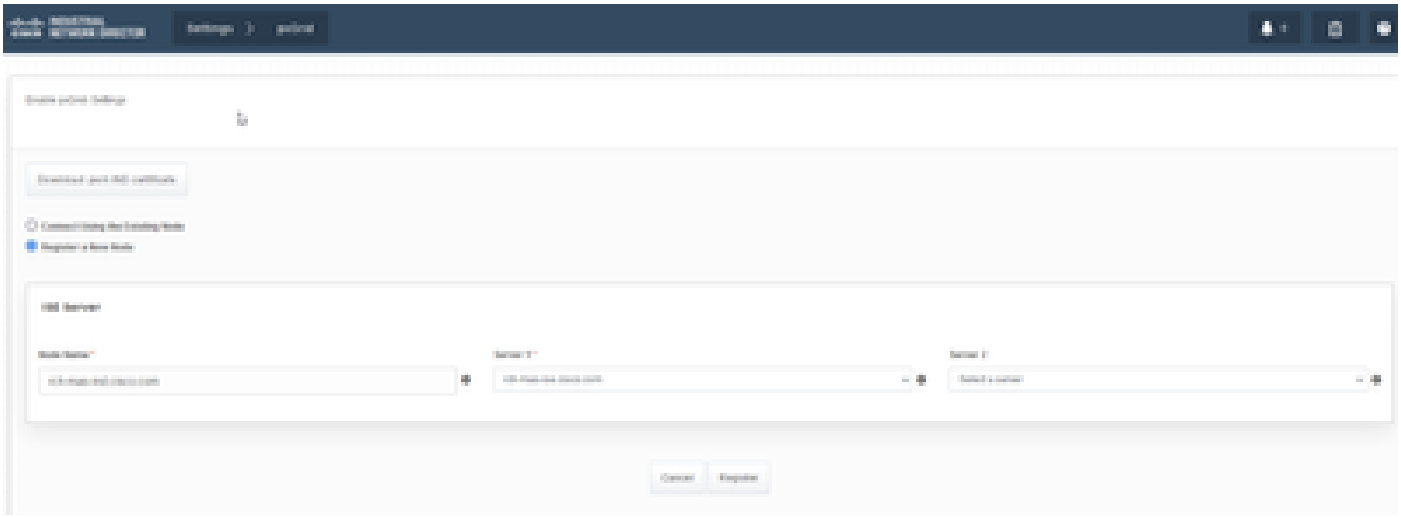
Abilitare e registrare pxGrid con il server ISE

Nell'interfaccia dell'IND:

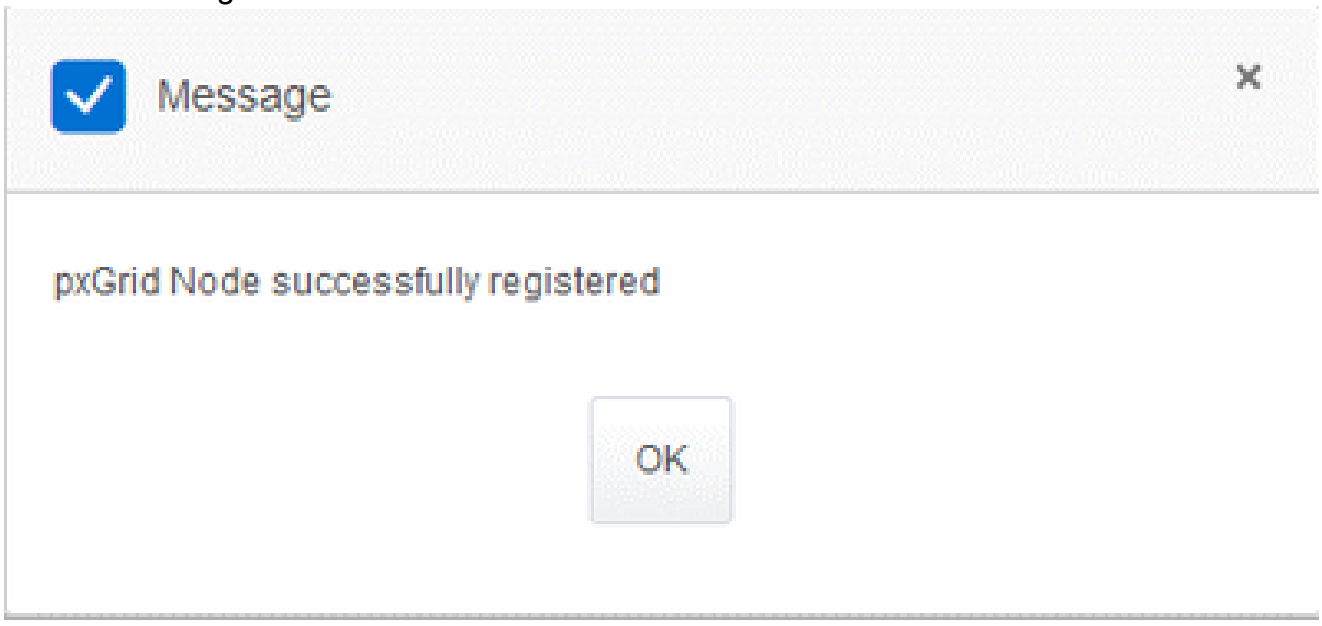
1. Selezionare Impostazioni > pxGrid.
2. Fare clic sul dispositivo di scorrimento per attivare pxGrid.
3. Se non è la prima volta che si registra pxGrid con ISE su questo server IND, scegliere "Connetti usando il nodo esistente". Le informazioni sul nodo IND e sul server ISE vengono inserite automaticamente.
4. Per registrare un nuovo server IND per utilizzare pxGrid, se necessario, scegliere "Registra un nuovo nodo". Immettere il nome del nodo IND e scegliere i server ISE in

base alle esigenze.

- Se il server ISE non è elencato tra le opzioni a discesa per Server 1 o Server 2, può essere aggiunto come nuovo server pxGrid usando Impostazioni > Policy Server



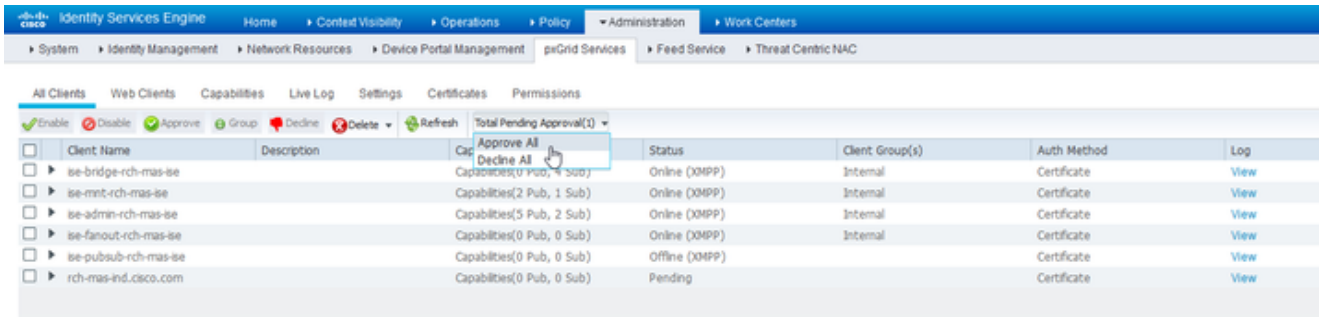
5. Fare clic su Registra. Sullo schermo viene visualizzata una conferma.



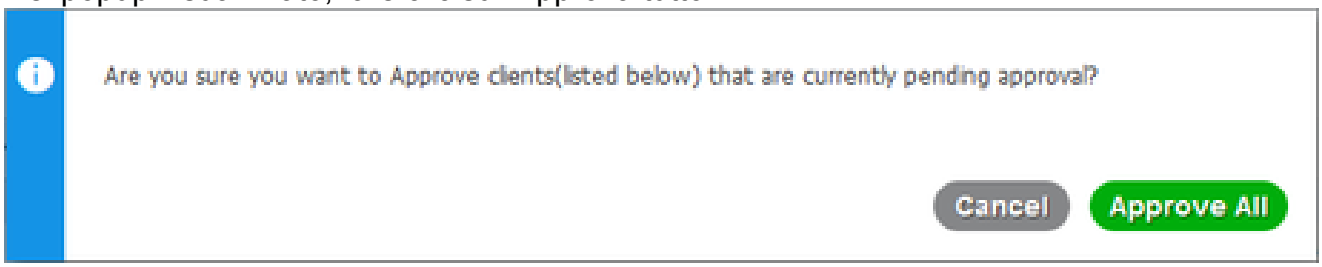
Approva richiesta di registrazione nel server ISE

Nell'interfaccia grafica di ISE:

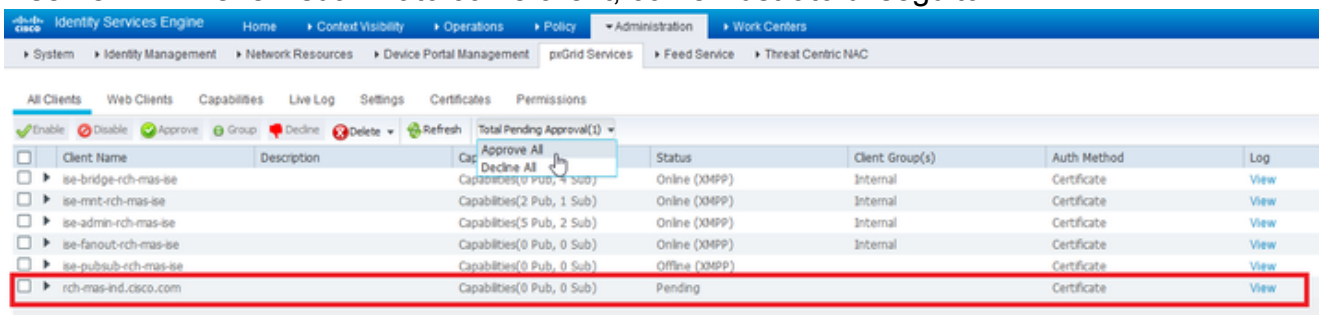
1. Selezionare Amministrazione > pxGrid Services > Tutti i client. Una richiesta Approvazione in sospeso viene visualizzata come "Totale approvazione in sospeso(1)".
2. Fare clic su "Approvazione totale in sospeso(1)" e selezionare "Approva tutto".



3. Nel popup visualizzato, fare clic su "Approva tutto".



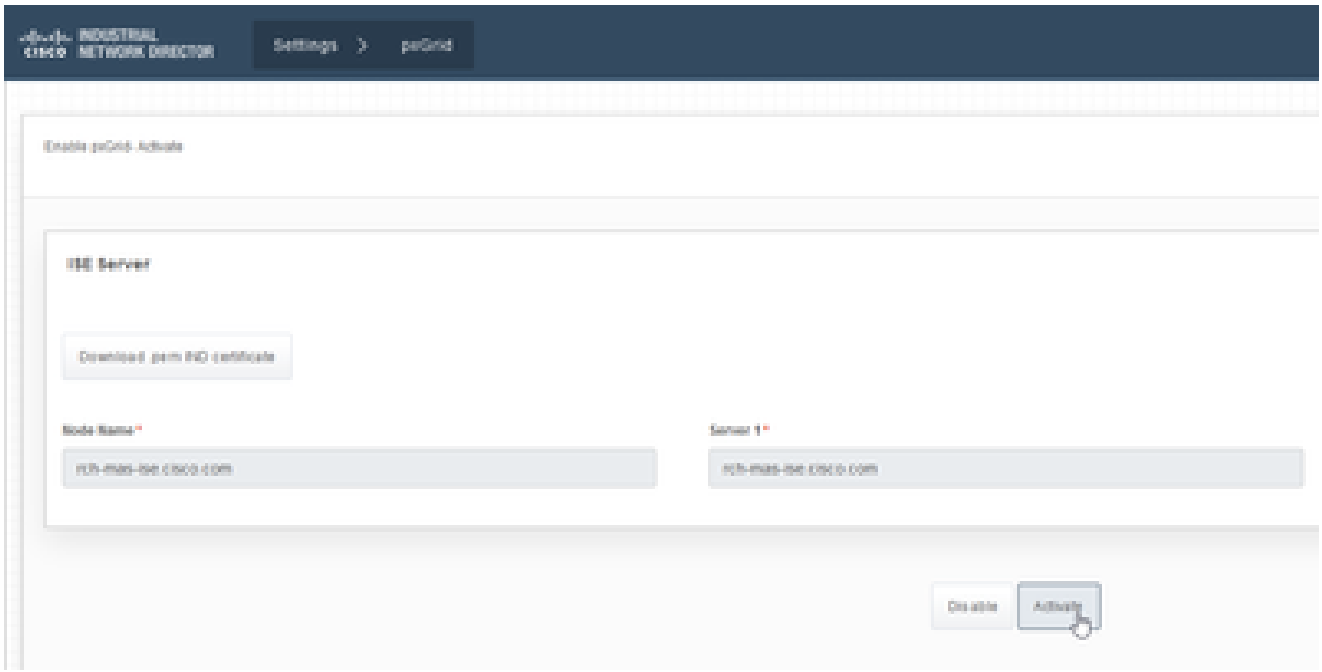
4. Il server IND viene visualizzato come client, come illustrato di seguito.



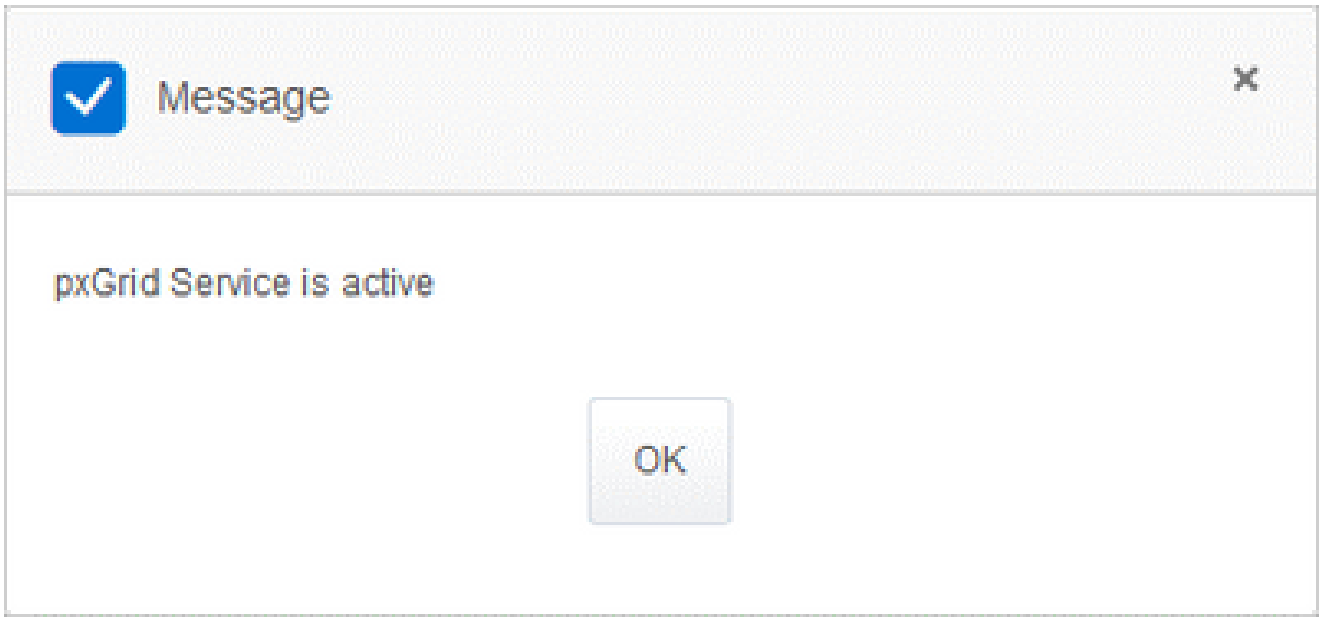
Attiva il servizio pxGrid nel server IND

Nell'interfaccia dell'IND:

1. Selezionare Impostazioni > pxGrid.
2. Fare clic su "Attiva".



3. Sullo schermo viene visualizzata una conferma.


Message
pxGrid Service is active
OK

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).