Configurazione della registrazione dei certificati con il protocollo ACME su Secure Firewall Threat Defense Gestito da FMC

Introduzione

In questo documento viene descritto il processo di registrazione di un certificato TLS (Transport Layer Security) tramite il protocollo ACME (Automated Certificate Management Environment) sulla piattaforma FTD (Secure Firewall Firepower Threat Defense).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Processi manuali di registrazione dei certificati e nozioni fondamentali su SSL (Secure Sockets Layer).
- Concetti di autenticazione di base per VPN ad accesso remoto.
- Esperienza con le Autorità di certificazione (CA).

Componenti usati

- Cisco FTDv versione 10.0.0-35.
- Cisco FMC versione 10.0.0-35.
- Server CA che supporta il protocollo ACME.

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.

Requisiti e limitazioni

Gli attuali prerequisiti e vincoli per la registrazione ACME su FTD Secure Firewall includono:

- Supportato su FTD e FMC versioni 10.0.0 e successive.
- ACME non consente il rilascio di certificati jolly; ogni richiesta di certificato deve specificare un nome di dominio preciso.
- Ogni trust point registrato tramite ACME è limitato a una singola interfaccia, pertanto i certificati ottenuti tramite ACME non possono essere condivisi tra più interfacce.
- Le coppie di chiavi vengono generate automaticamente e sono univoche per ogni certificato registrato tramite ACME, impedendo il riutilizzo delle chiavi e migliorando la sicurezza.

Considerazioni sul downgrade

Quando si esegue il downgrade a una versione FTD Secure Firewall che non supporta la registrazione ACME (versione 7.7 o precedente):

- Tutte le configurazioni di trust point relative all'ACME introdotte nella versione 10.0.0 o successive vengono perse.
- I certificati registrati tramite ACME sono ancora accessibili; tuttavia, le relative chiavi private vengono dissociate dopo il primo salvataggio e il riavvio dopo il declassamento.

Se è necessario un downgrade, utilizzare la soluzione consigliata:

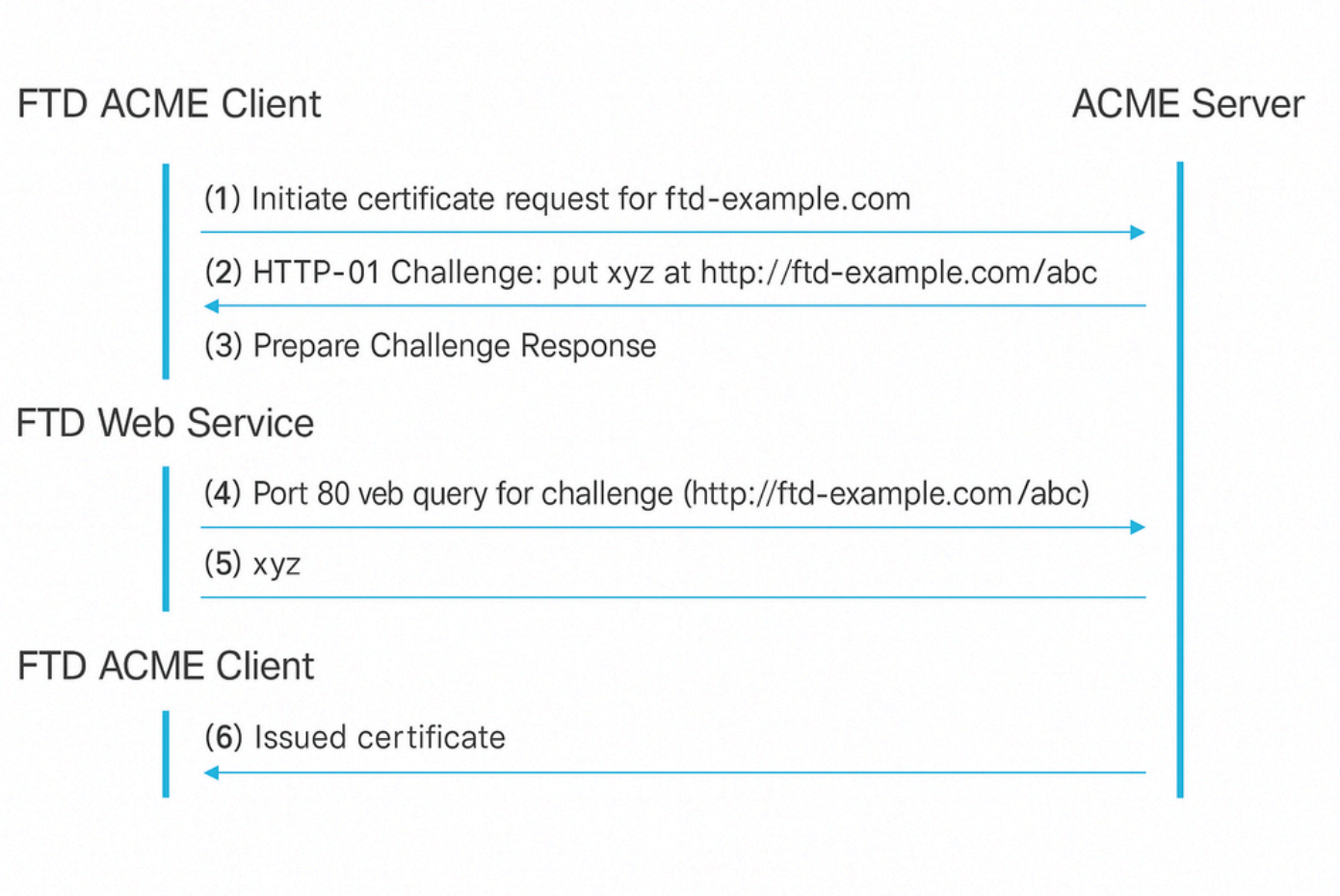
- Prima di effettuare il downgrade, esportare i certificati ACME in formato PKCS12.
- Prima di eseguire il downgrade, rimuovere la configurazione del trust point ACME.
- Dopo il downgrade, importare il certificato PKCS12. Il trust point importato rimane valido fino alla scadenza del certificato rilasciato da ACME.

Premesse

Il protocollo ACME ha lo scopo di semplificare la gestione dei certificati TLS per gli amministratori di rete. Tramite ACME, gli amministratori possono automatizzare le attività relative all'acquisizione e al rinnovo dei certificati TLS. Questa automazione è particolarmente utile quando si lavora con autorità di certificazione (CA) quali Let's Encrypt, che forniscono certificati gratuiti, automatizzati e accessibili pubblicamente tramite il protocollo ACME.ACME facilita il rilascio di certificati di convalida del dominio (DV). Questi certificati verificano che il richiedente del certificato abbia il controllo sui domini specificati. La convalida viene in genere eseguita tramite un processo di verifica basato su HTTP, in cui il richiedente inserisce un file designato nel proprio server Web. L'autorità di certificazione (CA) accede quindi al file tramite il server HTTP del dominio per confermare il controllo del dominio. Il superamento di questa verifica consente alla CA di rilasciare il certificato DV.

Il processo di iscrizione prevede i passi riportati di seguito.

1. Avvia richiesta certificato: Il client invia una richiesta di certificato al server ACME, specificando i domini per i quali il certificato è necessario.
2. Receive HTTP-01 Challenge: Il server ACME risponde con una richiesta HTTP-01 contenente un token univoco che il client deve utilizzare per dimostrare la proprietà del dominio.
3. Preparazione risposta di verifica:
    1. Il client genera un'autorizzazione della chiave combinando il token del server ACME con la relativa chiave account.
    2. Il client configura il proprio server Web in modo che venga utilizzata l'autorizzazione della chiave in un percorso URL specifico.
4. Il server ACME recupera la sfida: Il server ACME esegue una richiesta HTTP GET all'URL fornito per ottenere l'autorizzazione della chiave.
5. Il server ACME verifica la proprietà: Il server confronta l'autorizzazione della chiave recuperata con il valore previsto per verificare il controllo del client sul dominio.
6. Rilascia certificato: Dopo la convalida, il server ACME rilascia il certificato SSL/TLS al client.



Flusso di autenticazione HTTP-01 della registrazione ACME.

I vantaggi principali dell'utilizzo del protocollo ACME per la registrazione di certificati TLS su FTD

Secure Firewall includono:

- Automazione della gestione dei certificati: ACME semplifica il processo di ottenimento e gestione dei certificati di dominio TLS per le interfacce TLS FTD Secure Firewall, riducendo in modo significativo le attività amministrative manuali.
- Rinnovo automatico certificati: Con i trust point abilitati ACME, i certificati vengono rinnovati automaticamente in prossimità della scadenza, riducendo al minimo la necessità di interventi amministrativi continui.
- Garanzia di sicurezza continua: Questa automazione garantisce che i certificati rimangano validi senza interruzioni, impedendo scadenze impreviste dei certificati e mantenendo comunicazioni sicure.

Questi vantaggi collettivamente migliorano l'efficienza operativa e la sicurezza per le installazioni FTD Secure Firewall.

Configurazione

Configurazione prerequisiti

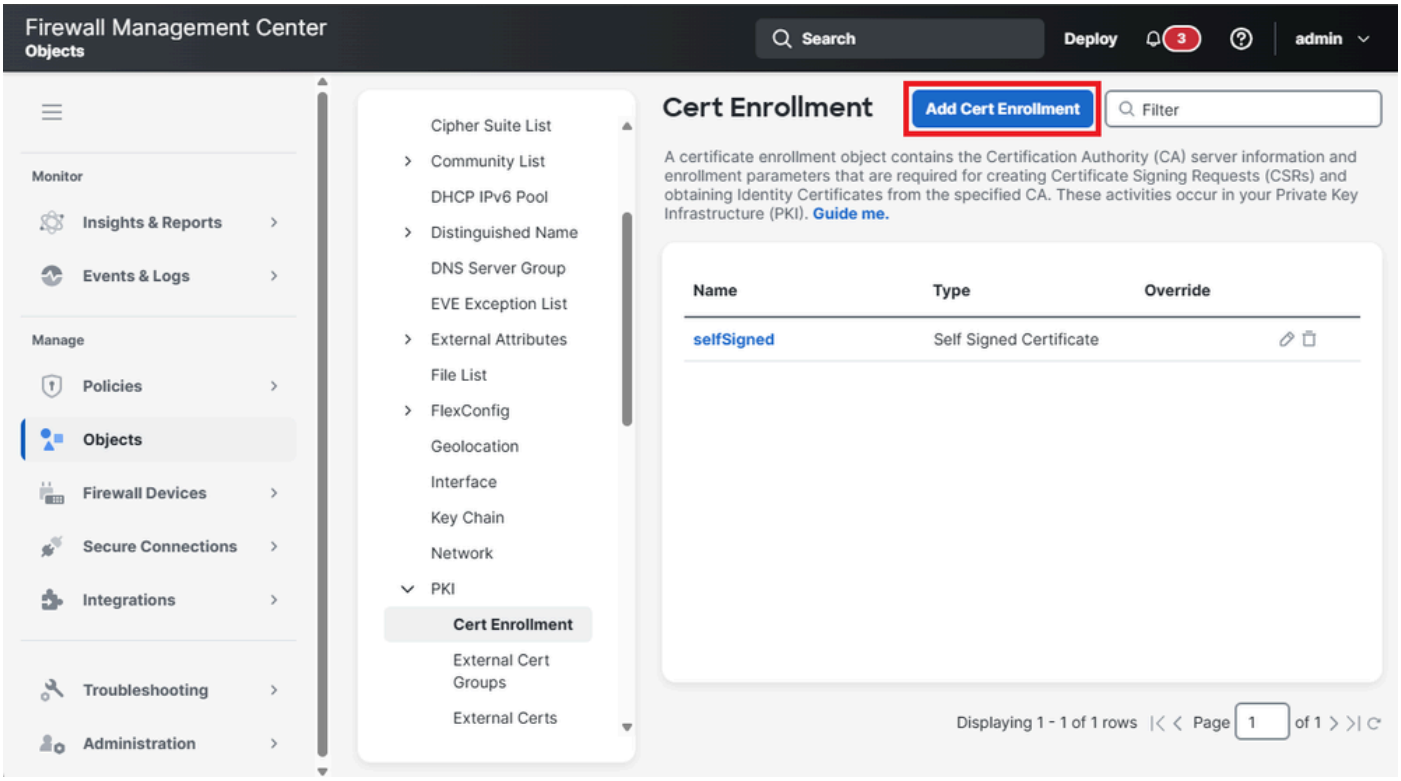
Prima di avviare il processo di registrazione ACME, verificare che siano soddisfatte le seguenti condizioni:

1. Nome dominio risolvibile: il nome di dominio per il quale si richiede un certificato deve essere risolvibile dal server ACME. In questo modo il server può verificare la proprietà del dominio.
2. Accesso sicuro del firewall al server ACME:il firewall sicuro deve avere la capacità di accedere al server ACME attraverso una delle sue interfacce. Non è necessario che l'accesso venga eseguito tramite l'interfaccia per cui è richiesto il certificato.
3. Disponibilità porta TCP 80: consente alla porta TCP 80 dal server CA ACME di accedere all'interfaccia che corrisponde al nome di dominio. Questa operazione è necessaria durante il processo di scambio ACME per completare la richiesta HTTP-01.

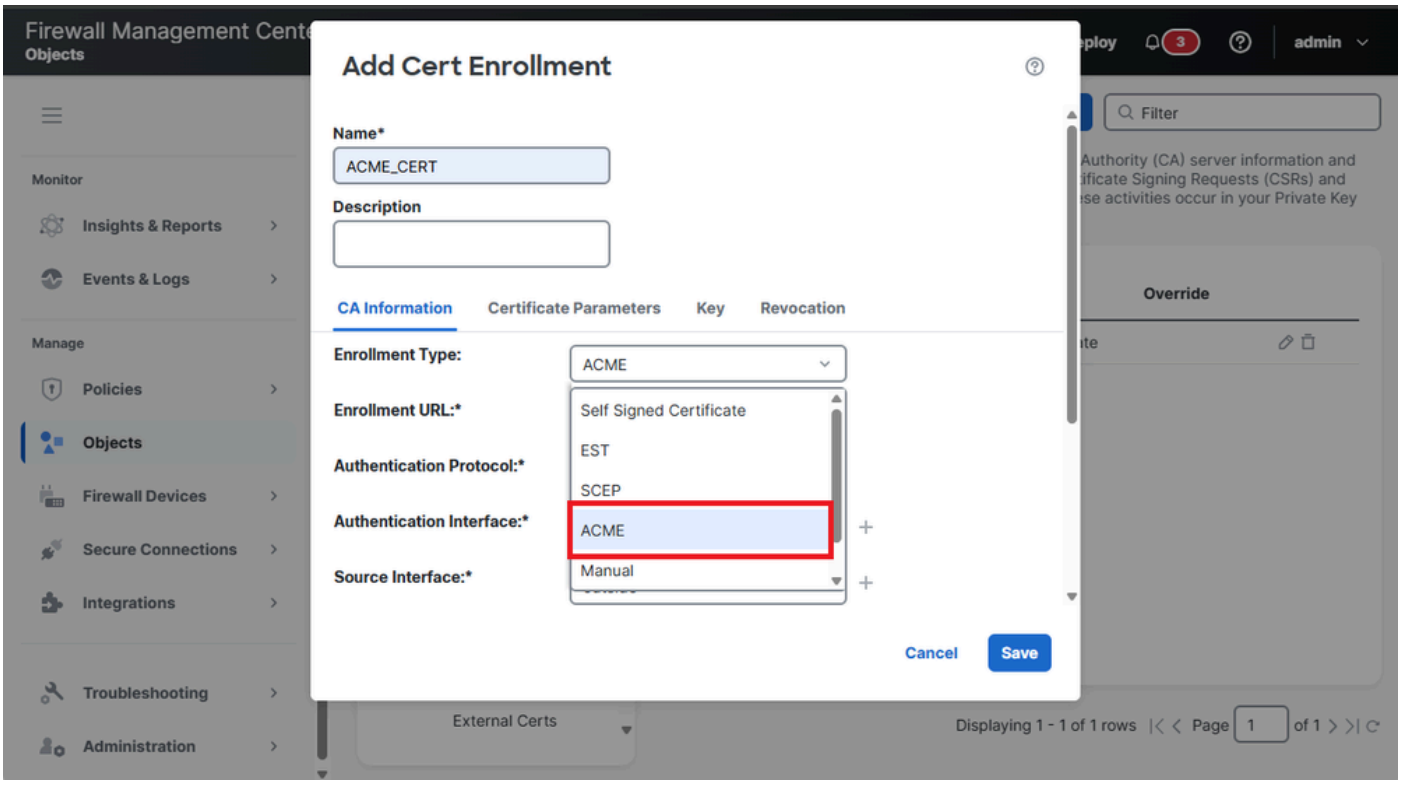
Nota: Durante il periodo in cui la porta 80 è aperta, sono accessibili solo i dati di richiesta ACME.

Creazione oggetto di registrazione certificato ACME

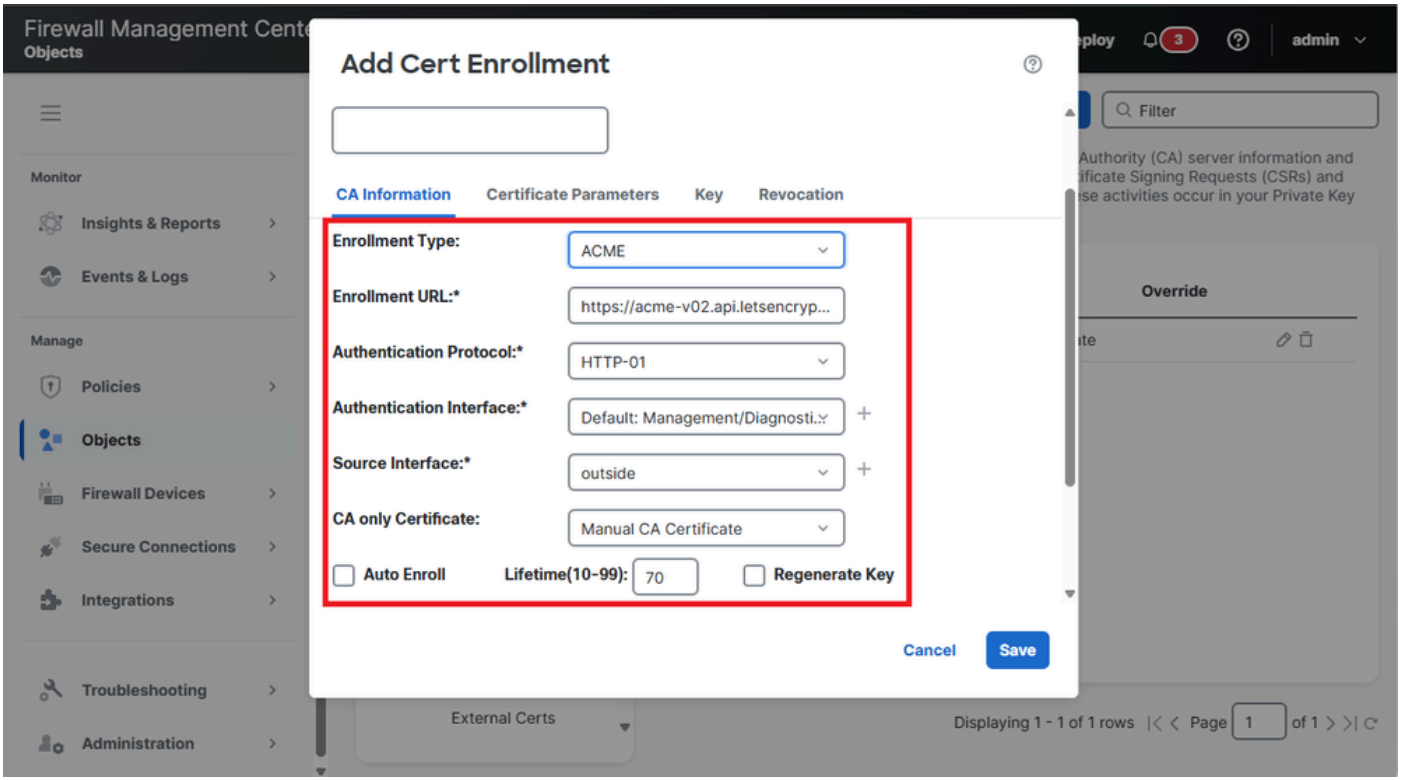
1. Passare a Oggetti > PKI > Iscrizione certificato e fare clic su Aggiungi registrazione certificato per avviare il processo di configurazione.



2. L'opzione di iscrizione ACME è elencata nel menu a discesa insieme ad altri metodi di iscrizione. Selezionare ACME dall'elenco a discesa Tipo di iscrizione per continuare.



3. Vengono visualizzate le opzioni per la configurazione dei parametri del certificato. Completare i campi con le informazioni appropriate.

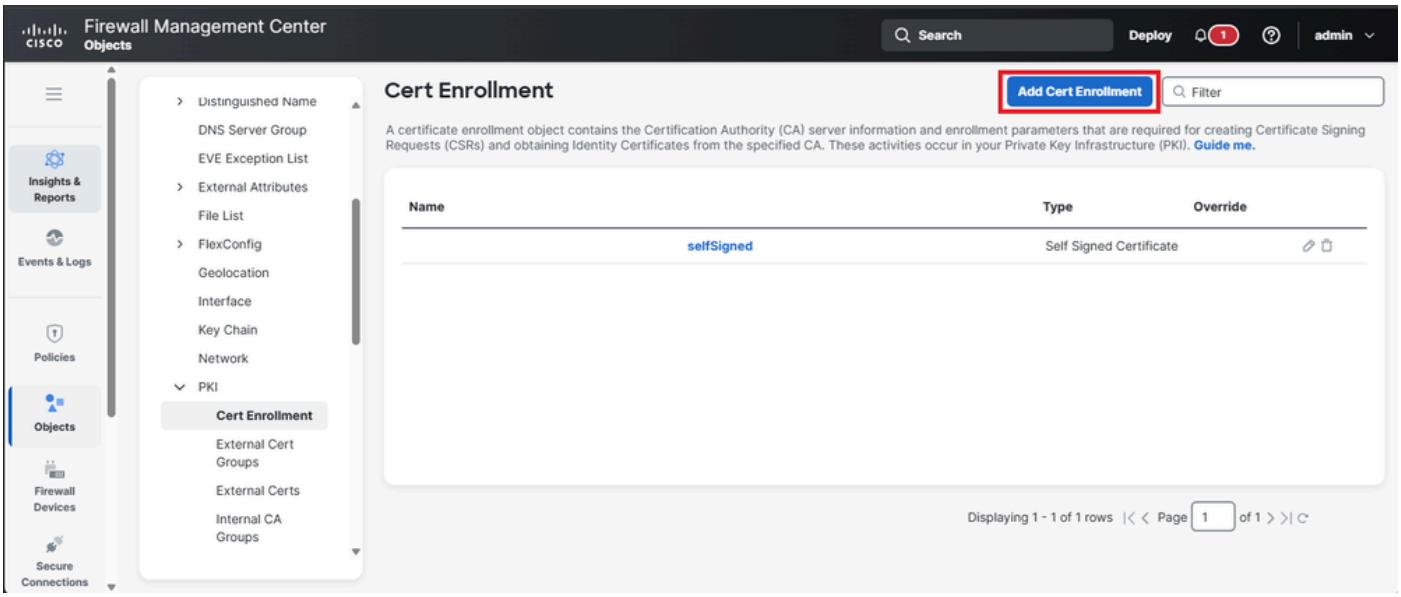


- URL di registrazione: Indirizzo del server ACME (ad esempio Let's Encrypt) utilizzato per richiedere e recuperare i certificati.
- Protocollo di autenticazione: Specifica il metodo utilizzato per verificare la proprietà del dominio. Il protocollo supportato per le sfide ACME è HTTP-01.
- Interfaccia di autenticazione: L'interfaccia di rete sul dispositivo FTD che riceve la richiesta HTTP-01 dal server ACME.
- Certificato solo CA: È necessario scegliere un certificato da un'Autorità di certificazione (CA) per considerare attendibile il server ACME.

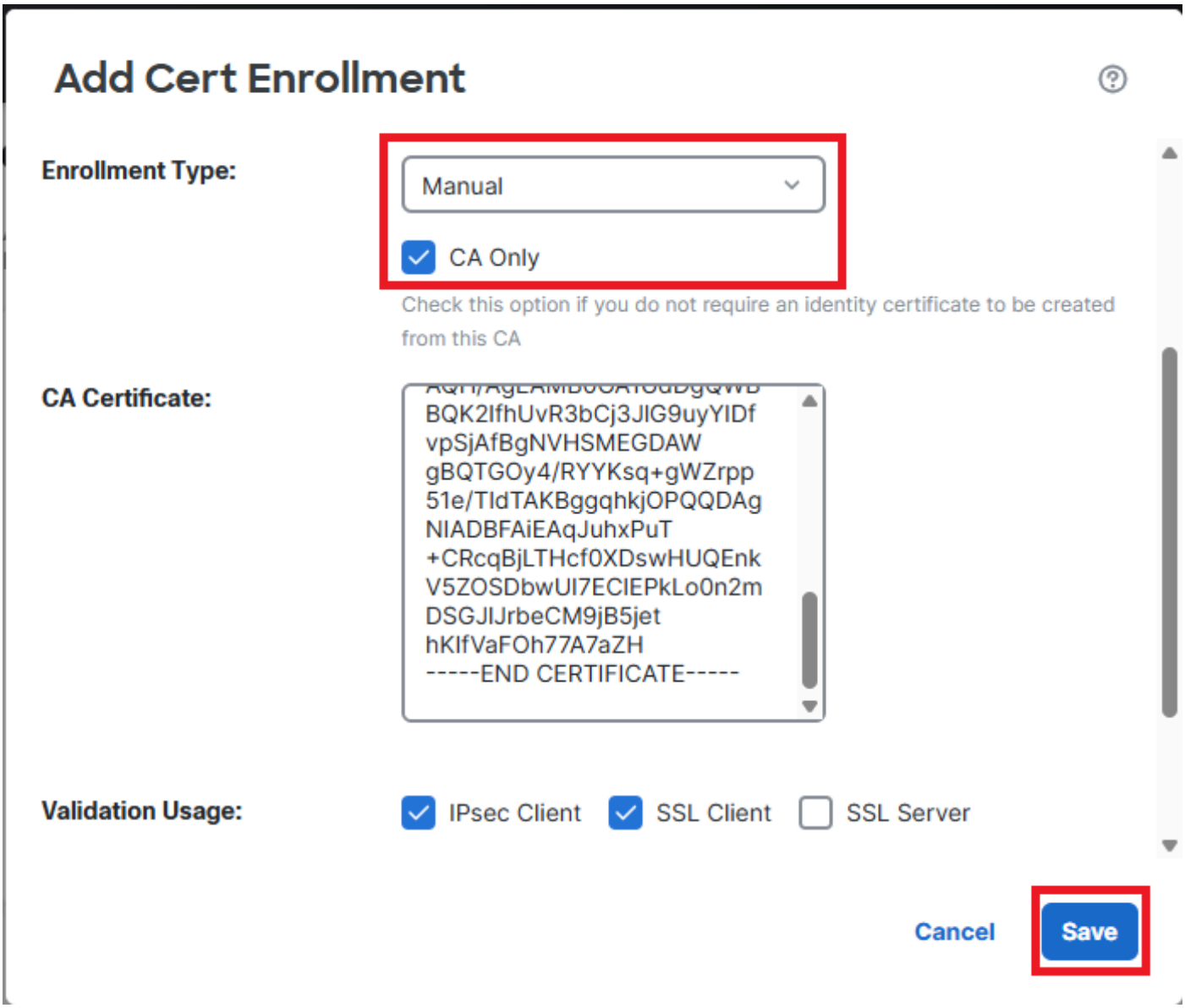
Nota: Per impostazione predefinita, fa riferimento all'URL pubblico del servizio Let's Encrypt: https://acme-v02.api.letsencrypt.org/directory.

---

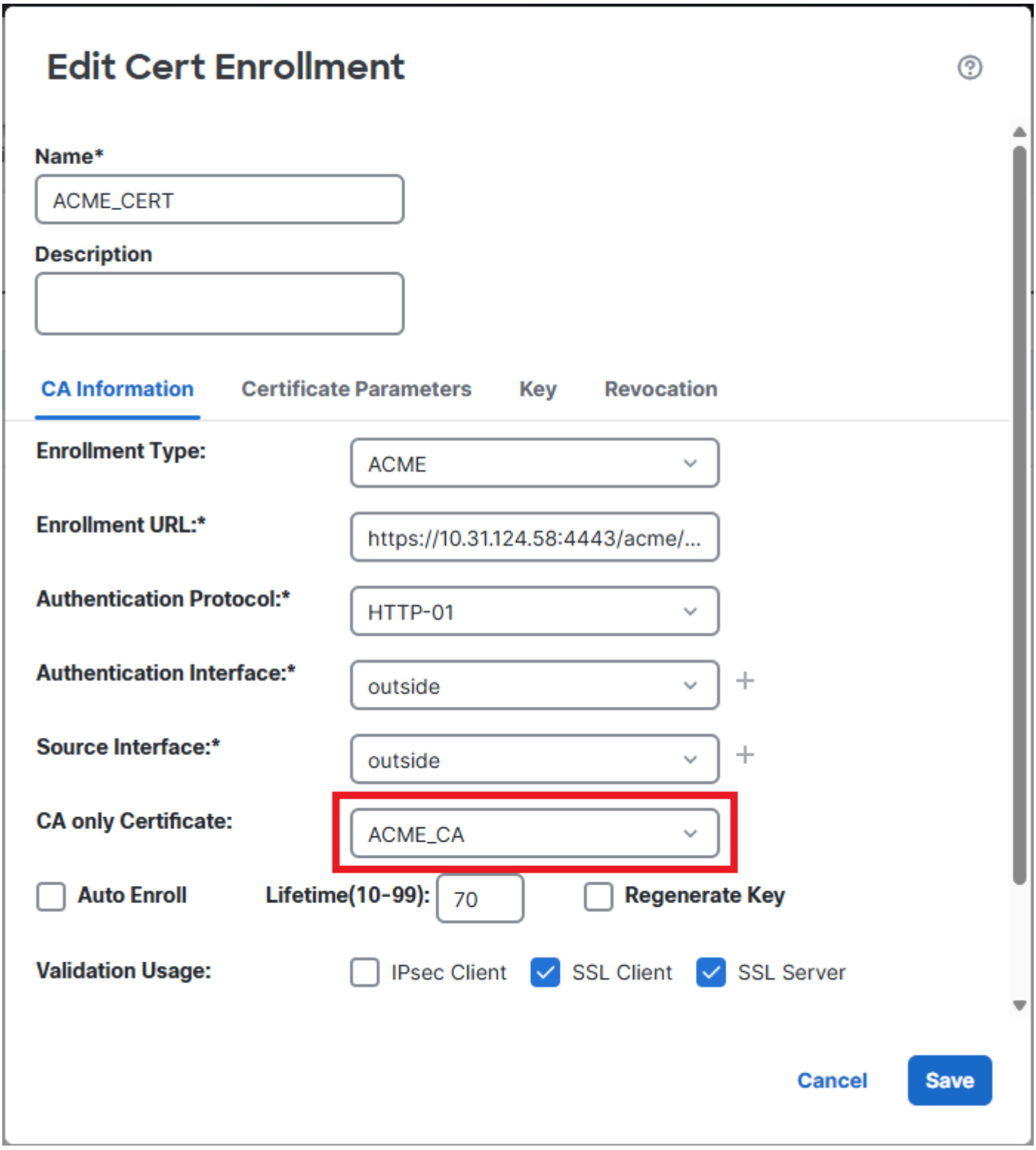
4. Se si utilizza un server ACME sconosciuto, è necessario aggiungere il certificato CA del server ACME. Passare a Oggetti > Iscrizione certificato e fare clic sul pulsante Aggiungi registrazione certificato.



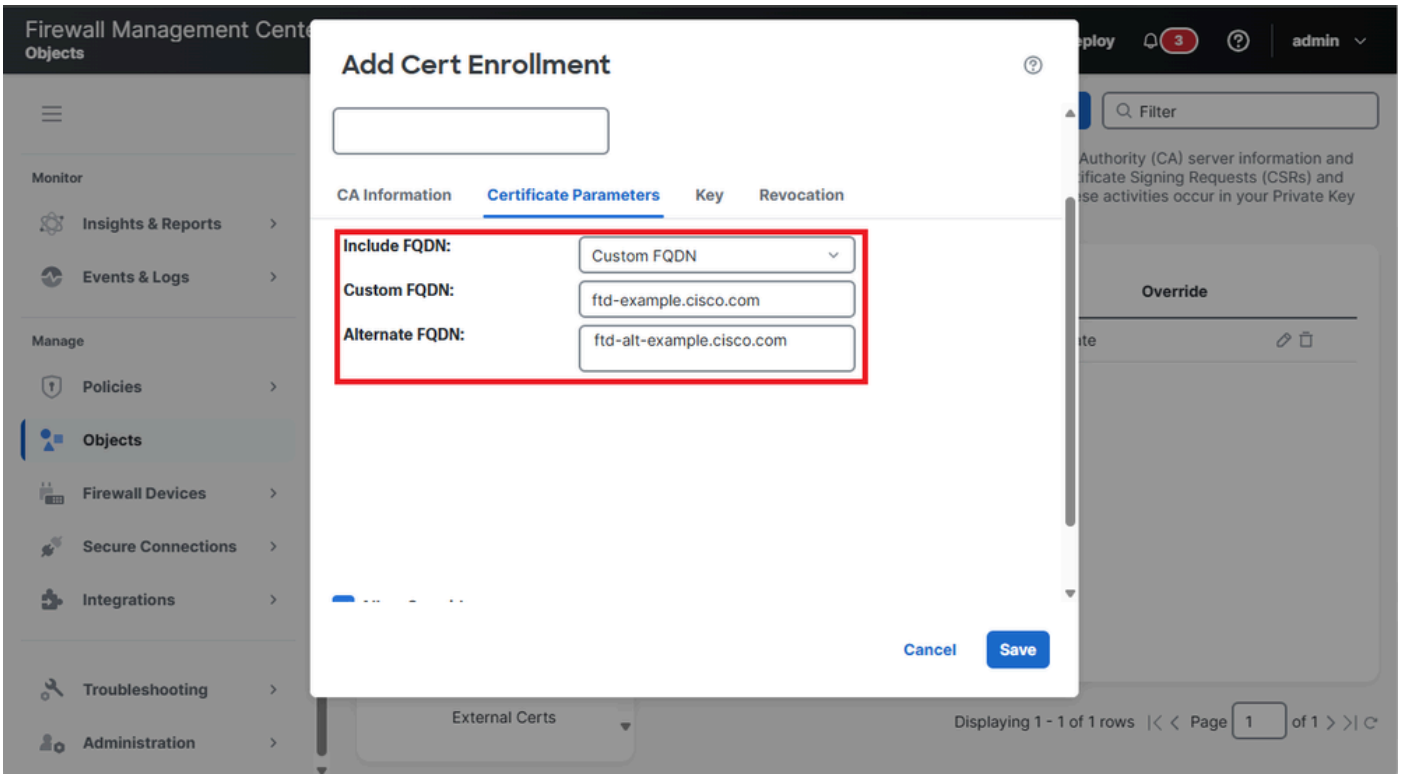
- Assegnare un nome al trust point e selezionare Tipo di iscrizione come Manuale. Selezionare quindi l'opzione Solo CA. Infine, incollare il certificato CA del server ACME e fare clic su Salva.



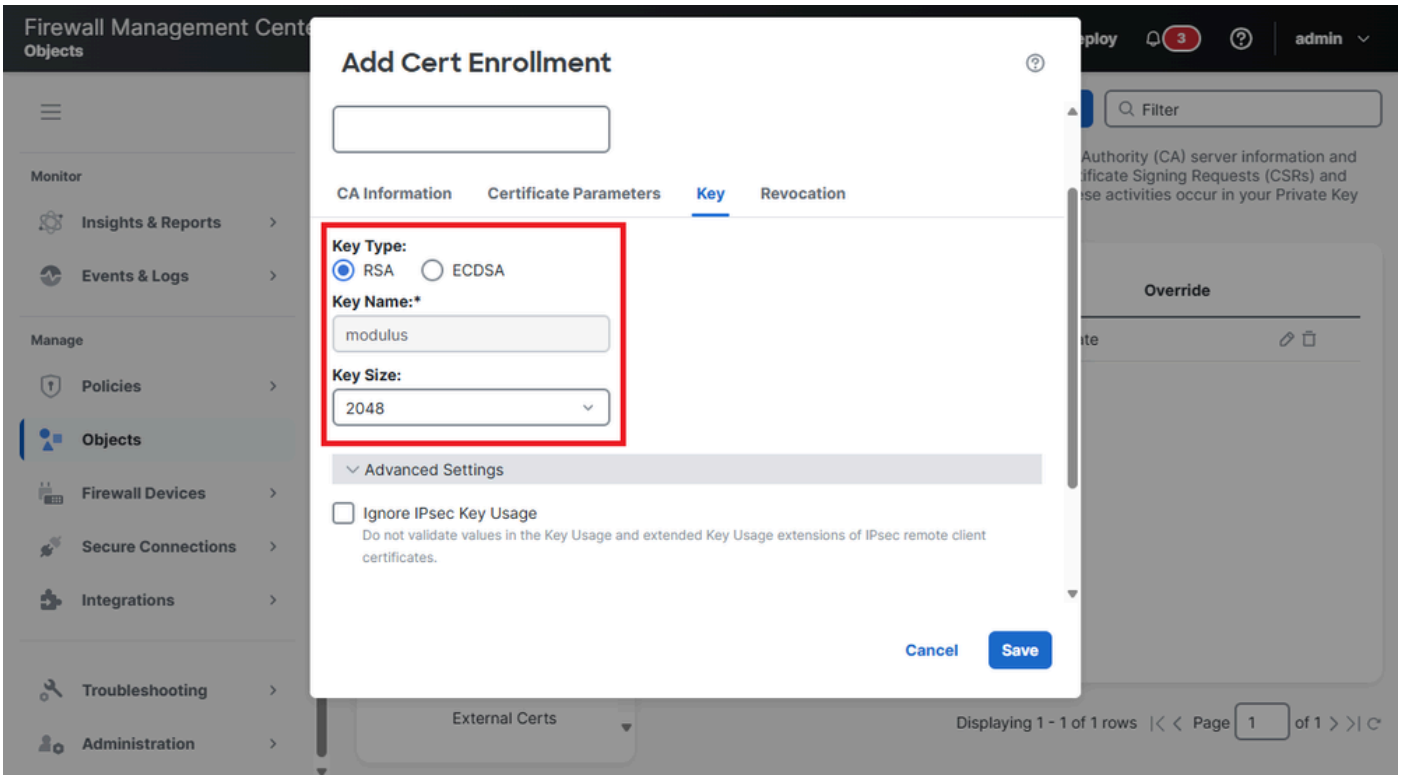
- Infine, selezionare il punto di attendibilità del server CA ACME nella sezione Certificato solo CA.



5. Passare a Parametri certificato, selezionare l'opzione FQDN personalizzato nella casella Includi FQDN e compilare i campi FQDN personalizzato e FQDN alternativo con il nome FQDN primario e gli eventuali nomi di dominio alternativi da includere nel certificato.



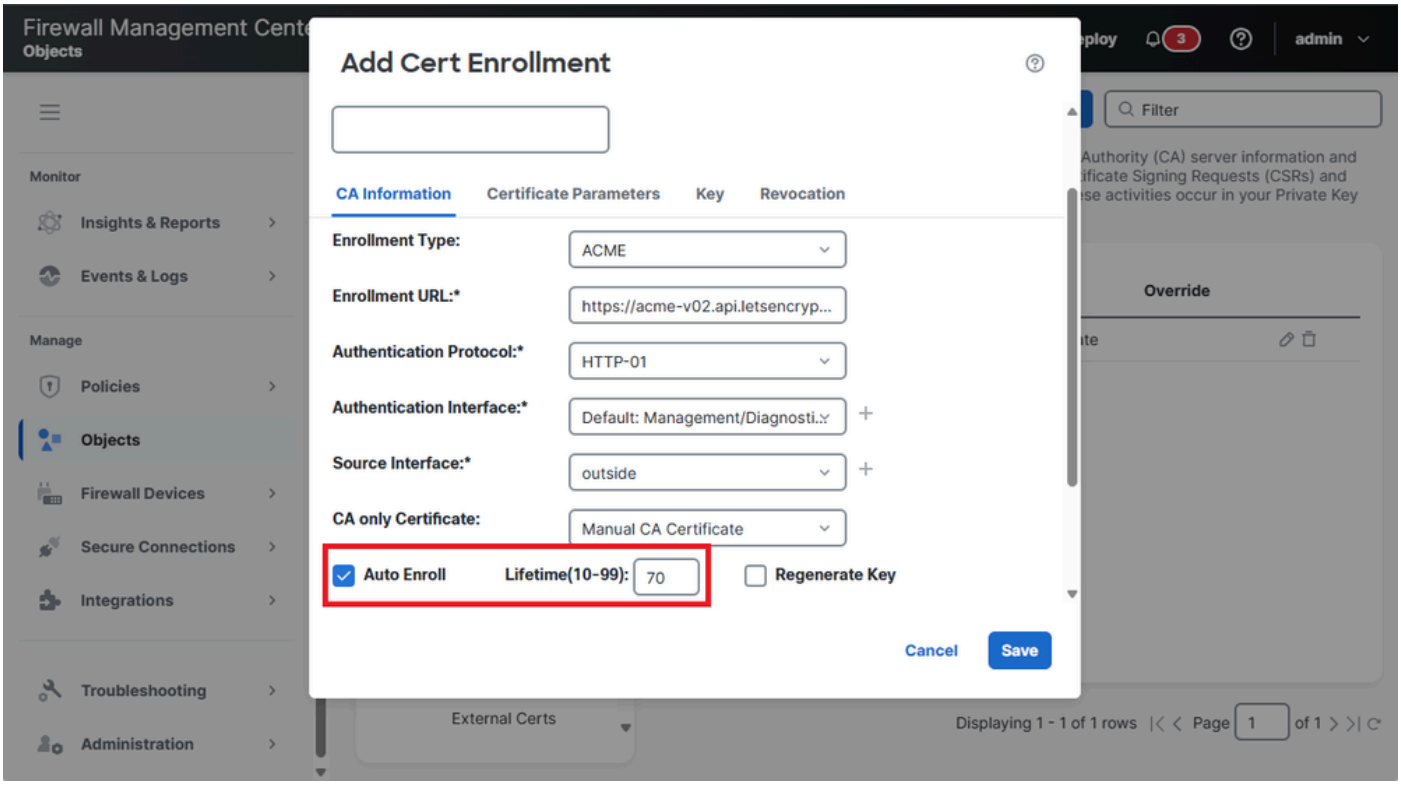
6. Passare a Chiave per modificare le impostazioni Tipo di chiave e Dimensione chiave.



7. (Facoltativo) Abilitare la registrazione automatica per il certificato di identità.

Selezionare la casella di controllo Iscrizione automatica e specificare la percentuale per la durata della registrazione automatica.

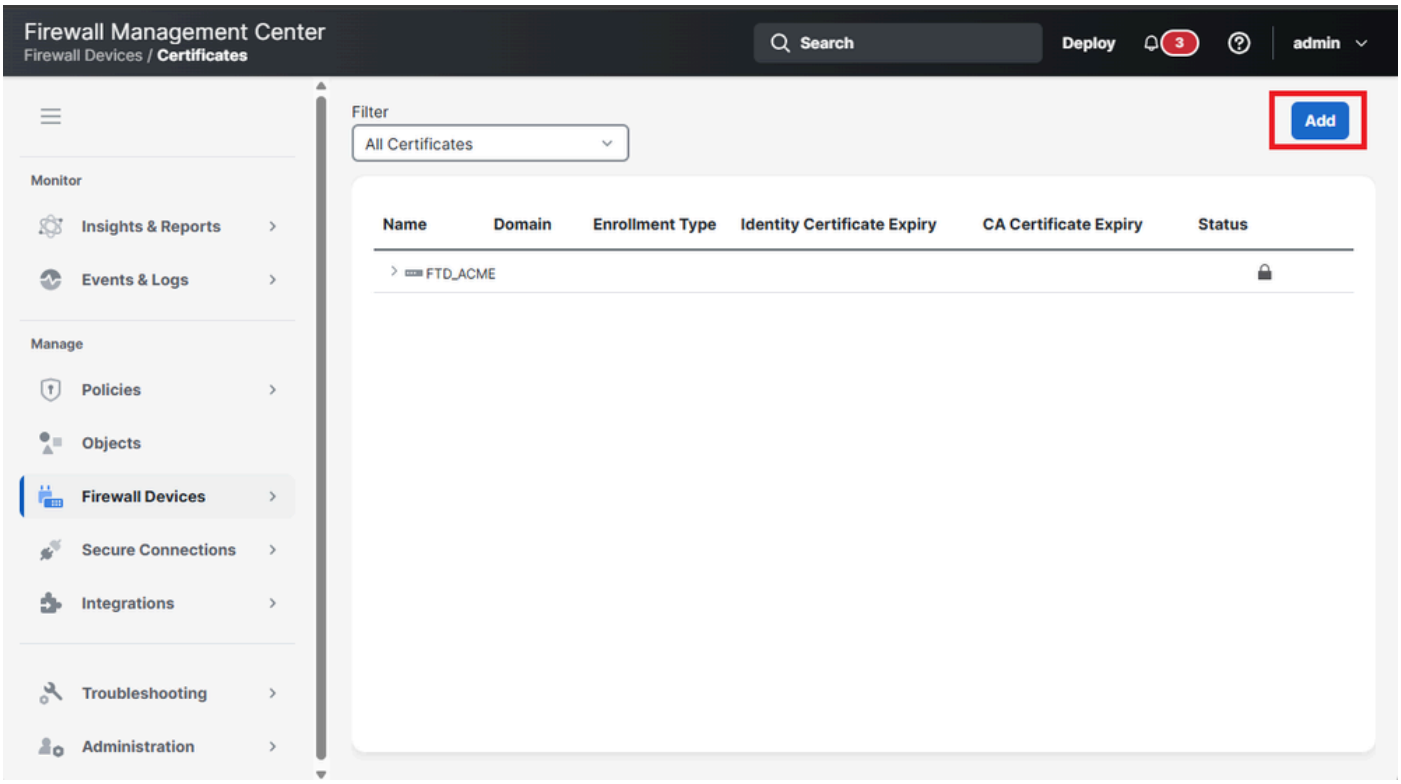
Questa funzionalità garantisce che il certificato venga rinnovato automaticamente prima della scadenza. La percentuale determina quanto tempo prima della scadenza del certificato inizia il processo di rinnovo. Se ad esempio è impostato su 80%, il processo di rinnovo inizia quando il certificato raggiunge l'80% del periodo di validità.



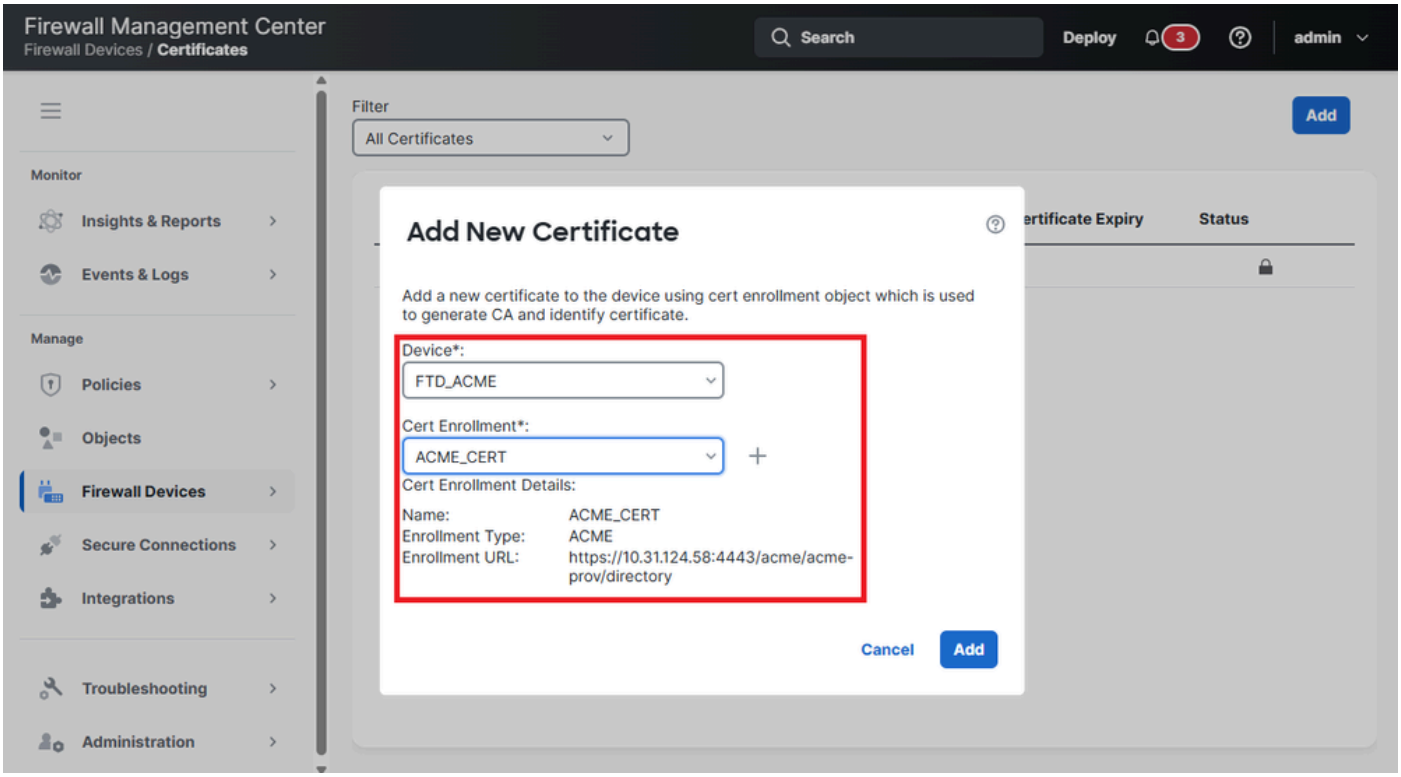
8. Fare clic su Save (Salva).

Registrazione certificato ACME sul dispositivo

1. Passare a Dispositivi firewall > Certificati e fare clic sul pulsante Aggiungi per registrare un nuovo certificato.



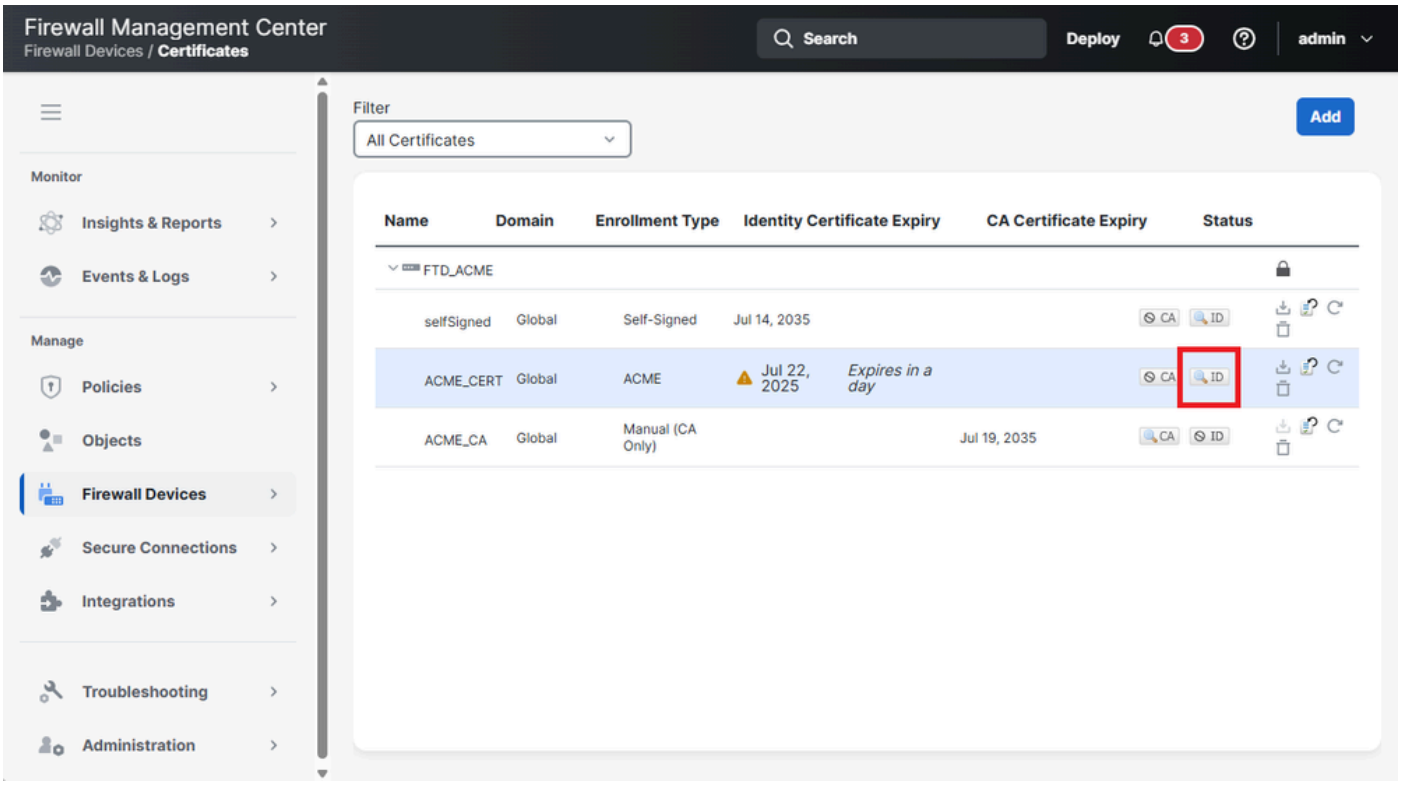
2. Selezionare il dispositivo FTD dall'elenco a discesa Dispositivo e l'oggetto certificato precedentemente creato in Registrazione certificato.



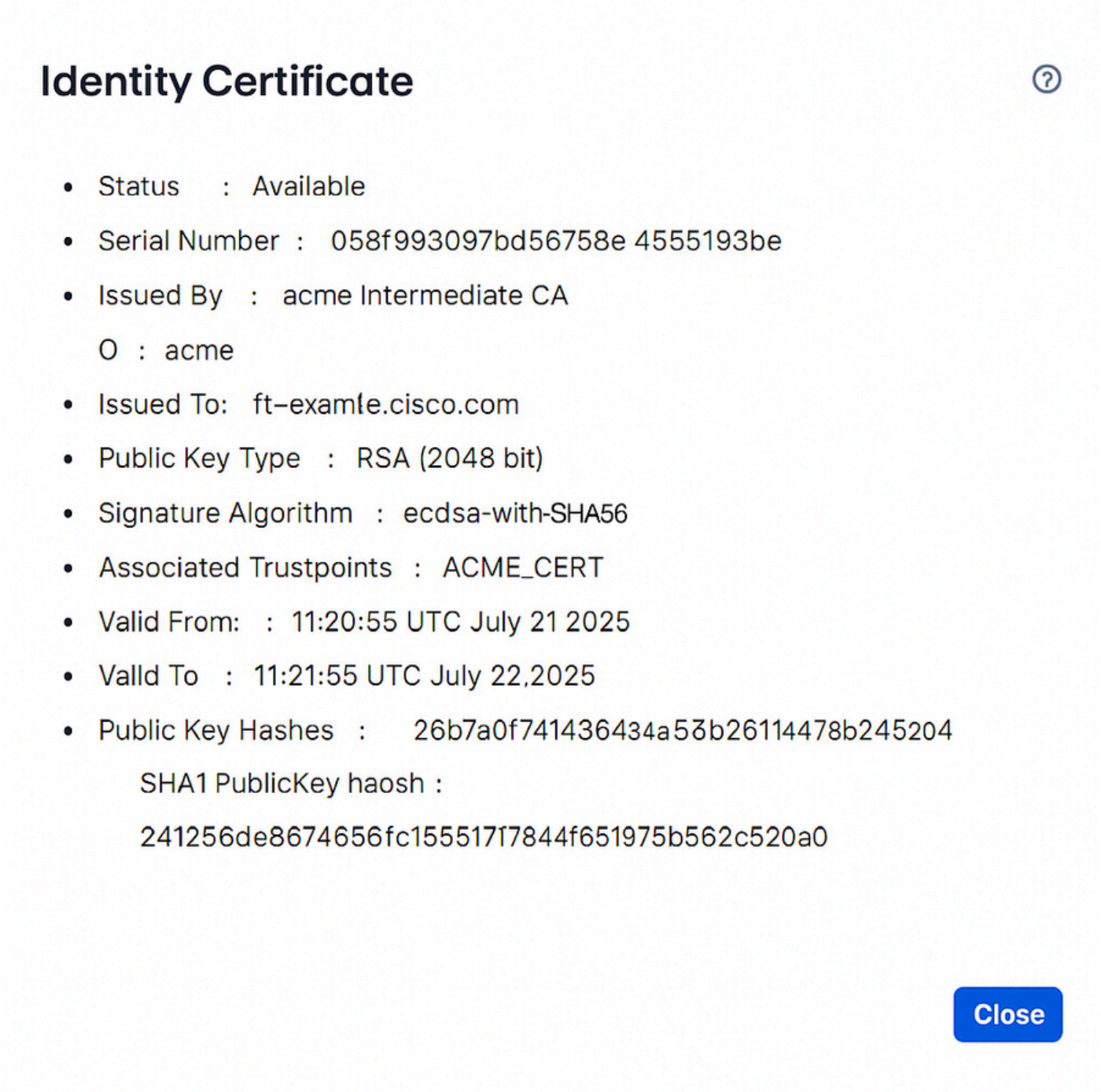
3. Fare clic su Add.

4. Una volta completata la distribuzione, nella colonna di stato viene visualizzato il pulsante ID

certificato.



5. Convalidare le informazioni sul certificato ID facendo clic sul pulsante ID.



Verifica

Visualizza certificato installato in FTD

Verificare che il certificato sia registrato con il comando show crypto ca certificates <nome punto di attendibilità>.

<#root>

```
firepower#
```

show crypto ca certificates

ACME_CERT

```
Certificate
Status: Available
Certificate Serial Number: 058f993097bd56758e44554194a953be
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=acme Intermediate CA
O=acme
Subject Name:
CN=ftd-example.cisco.com
Validity Date:
start date: 11:20:55 UTC Jul 21 2025
end date: 11:21:55 UTC Jul 22 2025
Storage: immediate
Associated Trustpoints: ACME_CERT
Public Key Hashes:
SHA1 PublicKey hash: 26b7a0f7414364a45b246114478bb74f432520c4
SHA1 PublicKeyInfo hash: 24125d6e8674566c1551784f651975b562c520a
```

Eventi Syslog

Nel FTD Secure Firewall sono presenti nuovi syslog per acquisire gli eventi correlati alla registrazione dei certificati tramite il protocollo ACME:

- 717067: Fornisce informazioni sull'avvio della registrazione dei certificati ACME.

```
%FTD-5-717067: Starting ACME certificate enrollment for the trustpoint <private_acme> with CA <ca-acme.
```

- 717068: Fornisce informazioni sull'esito della registrazione del certificato ACME.

```
%FTD-5-717068: ACME Certificate enrollment succeeded for trustpoint <private_acme> with CA <ca-acme.exa
```

- 717069: Fornisce informazioni su quando l'iscrizione ACME non riesce.

```
%FTD-3-717069: ACME Certificate enrollment failed for trustpoint <private_acme>
```

- 717070: Fornisce informazioni relative alla coppia di chiavi per la registrazione o il rinnovo del certificato.

```
%FTD-5-717070: Keypair <Auto.private_acme> in the trustpoint <private_acme> is regenerated for <manual>
```

Risoluzione dei problemi

Se la registrazione di un certificato ACME non riesce, considerare i passaggi successivi per identificare e risolvere il problema:

- Verificare la connettività al server:verificare che il firewall protetto disponga della connettività di rete al server ACME. Verificare che non vi siano problemi di rete o che le regole del firewall blocchino la comunicazione.
- Verificare che il nome di dominio del firewall protetto sia risolvibile:Verificare che il nome di dominio configurato nel FTD del firewall protetto sia risolvibile dal server ACME. Questa verifica è fondamentale per la convalida della richiesta da parte del server.
- Conferma proprietà dominio: verificare che tutti i nomi di dominio specificati nel trust point siano di proprietà dell'FTD del firewall protetto. In questo modo il server ACME può convalidare la proprietà del dominio.

Comandi per la risoluzione dei problemi

Per ulteriori informazioni, catturare l'output dei comandi di debug successivi:

- debug crypto ca acme <1-255>
- debug crypto ca <1-14>

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).