

# Configurazione del supporto HTTPS per l'integrazione ISE SCEP

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazione certificato server NDES](#)

[Configurazione binding IIS NDES Server](#)

[Configurazione server ISE](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritto come configurare il supporto HTTPS (Hypertext Transfer Protocol Secure) per l'integrazione SCEP (Secure Certificate Enrollment Protocol) con ISE (Identity Services Engine).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base del server Web Microsoft Internet Information Services (IIS)
- Esperienza nella configurazione di SCEP e certificati su ISE

### Componenti usati

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

- ISE release 11.1.x

- Windows Server 2008 R2 Enterprise con aggiornamenti rapidi per [KB2483564](#) e [KB2633200](#) installati

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.

Le informazioni relative ai servizi certificati Microsoft sono fornite come guida specifica per Cisco Bring Your Own Device (BYOD). Per informazioni dettagliate sulle configurazioni dei server relative a Microsoft, NDES (Network Device Enrollment Service) e SCEP, vedere il sito Web TechNet di Microsoft.

## Premesse

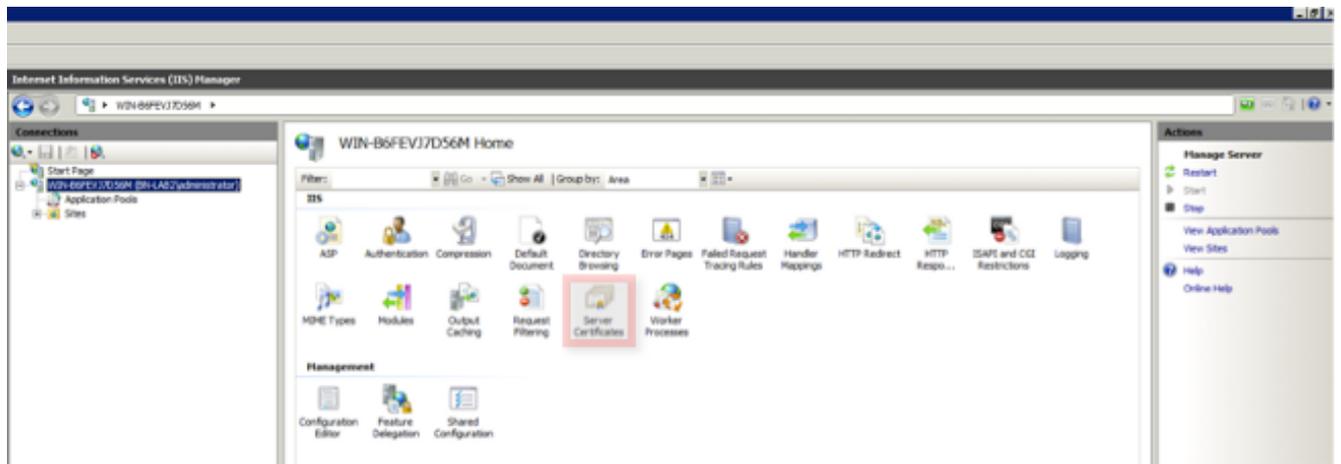
In una distribuzione BYOD, uno dei componenti principali è un server Microsoft 2008 R2 Enterprise con il ruolo NDES installato. Il server è un membro della foresta di Active Directory (AD). Durante l'installazione iniziale di NDES, il server Web IIS di Microsoft viene installato e configurato automaticamente per supportare la terminazione HTTP di SCEP. In alcune implementazioni BYOD, i clienti potrebbero voler proteggere ulteriormente le comunicazioni tra ISE e NDES utilizzando HTTPS. In questa procedura vengono descritti in dettaglio i passaggi necessari per richiedere e installare un certificato SSL (Secure Sockets Layer) per il sito Web SCEP.

## Configurazione

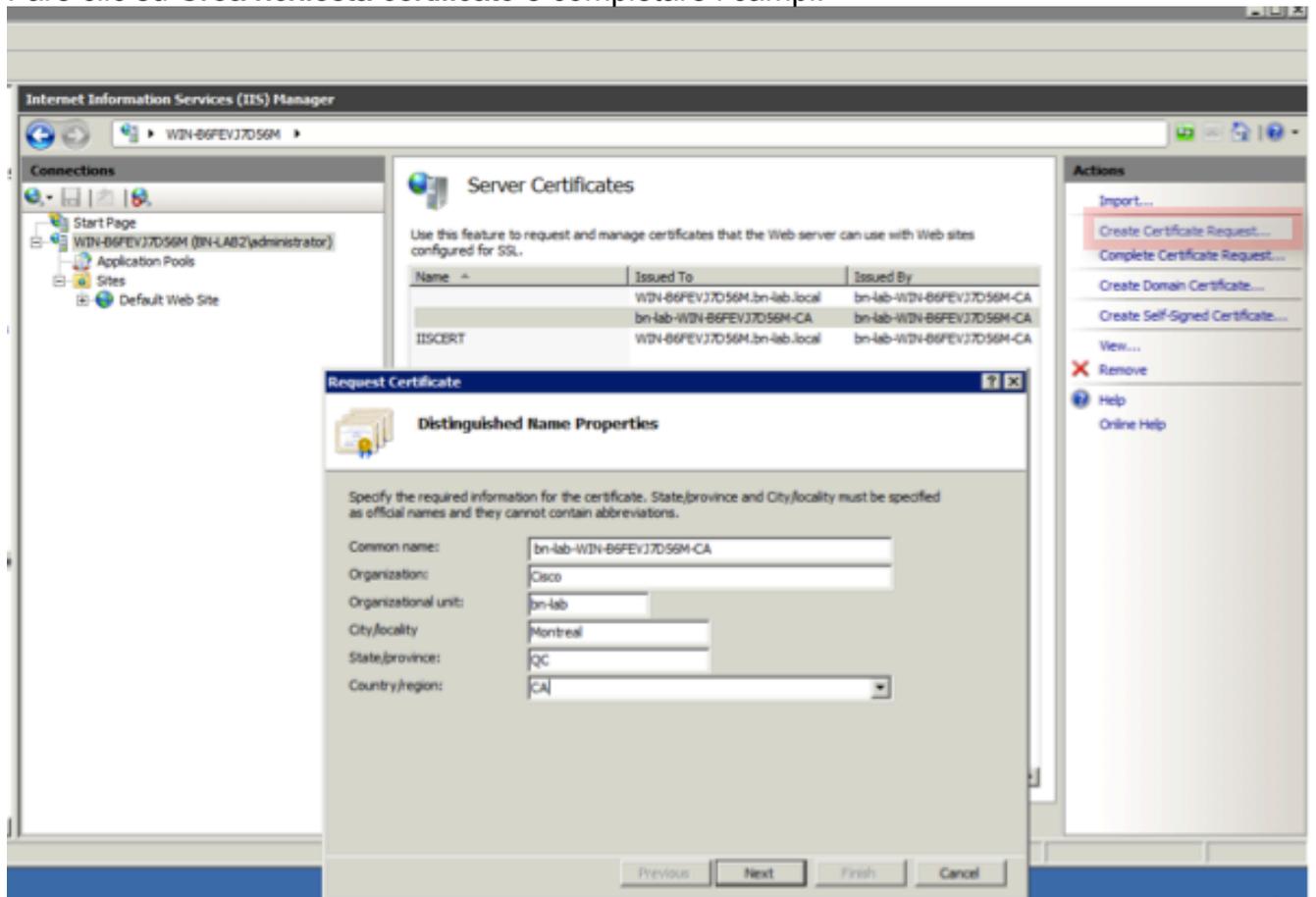
### Configurazione certificato server NDES

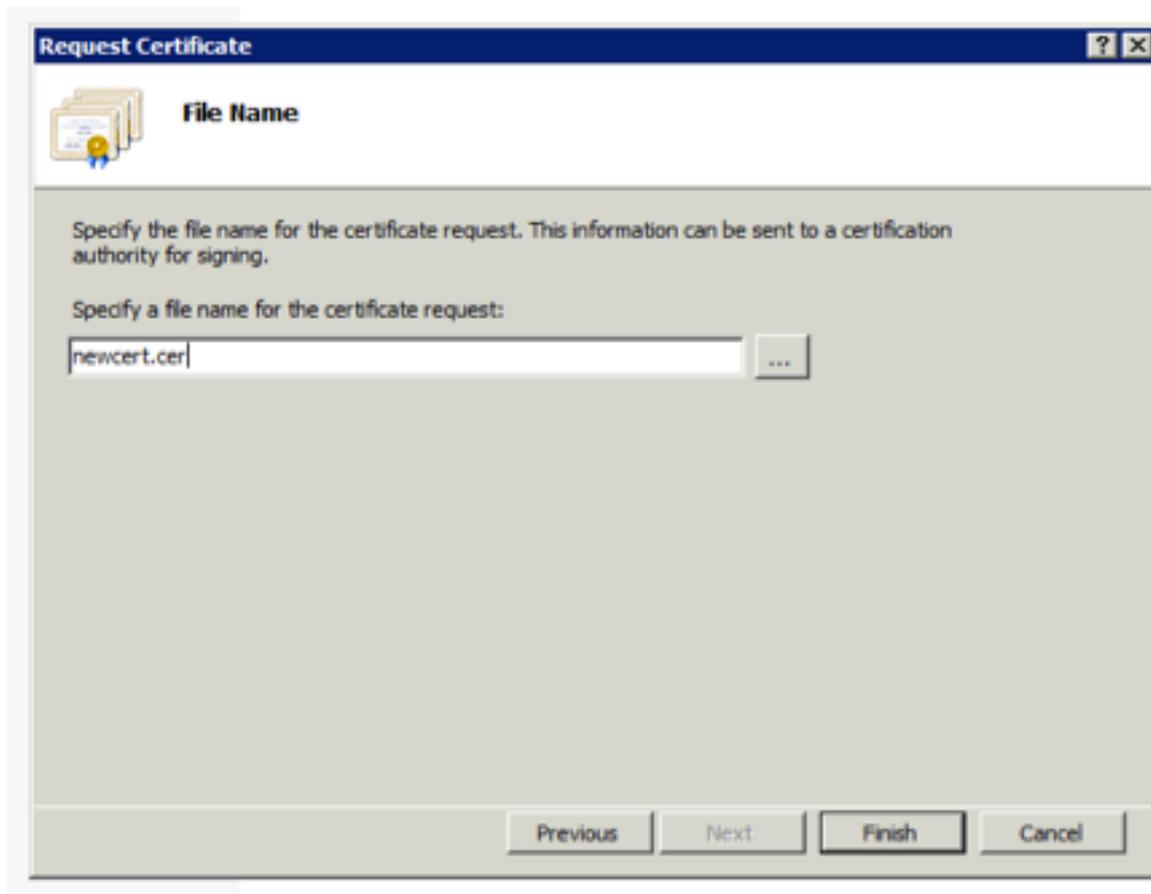
**Nota:** È necessario configurare un nuovo certificato per IIS (richiesto solo quando IIS è integrato con una PKI di terze parti, ad esempio Verisign o quando i ruoli dell'Autorità di certificazione (CA) e del server NDES sono separati in server separati). Durante l'installazione, se il ruolo NDES si trova su un server CA Microsoft corrente, IIS utilizza il certificato di identità del server creato durante l'installazione della CA. Per configurazioni autonome come questa, passare direttamente alla sezione **Configurazione binding IIS di NDES Server** in questo documento.

1. Connettersi al server NDES tramite console o RDP.
2. Fare clic su **Start -> Strumenti di amministrazione -> Gestione Internet Information Services (IIS)**.
3. Evidenziare il nome del server IIS e fare clic sull'icona **Certificati server**.

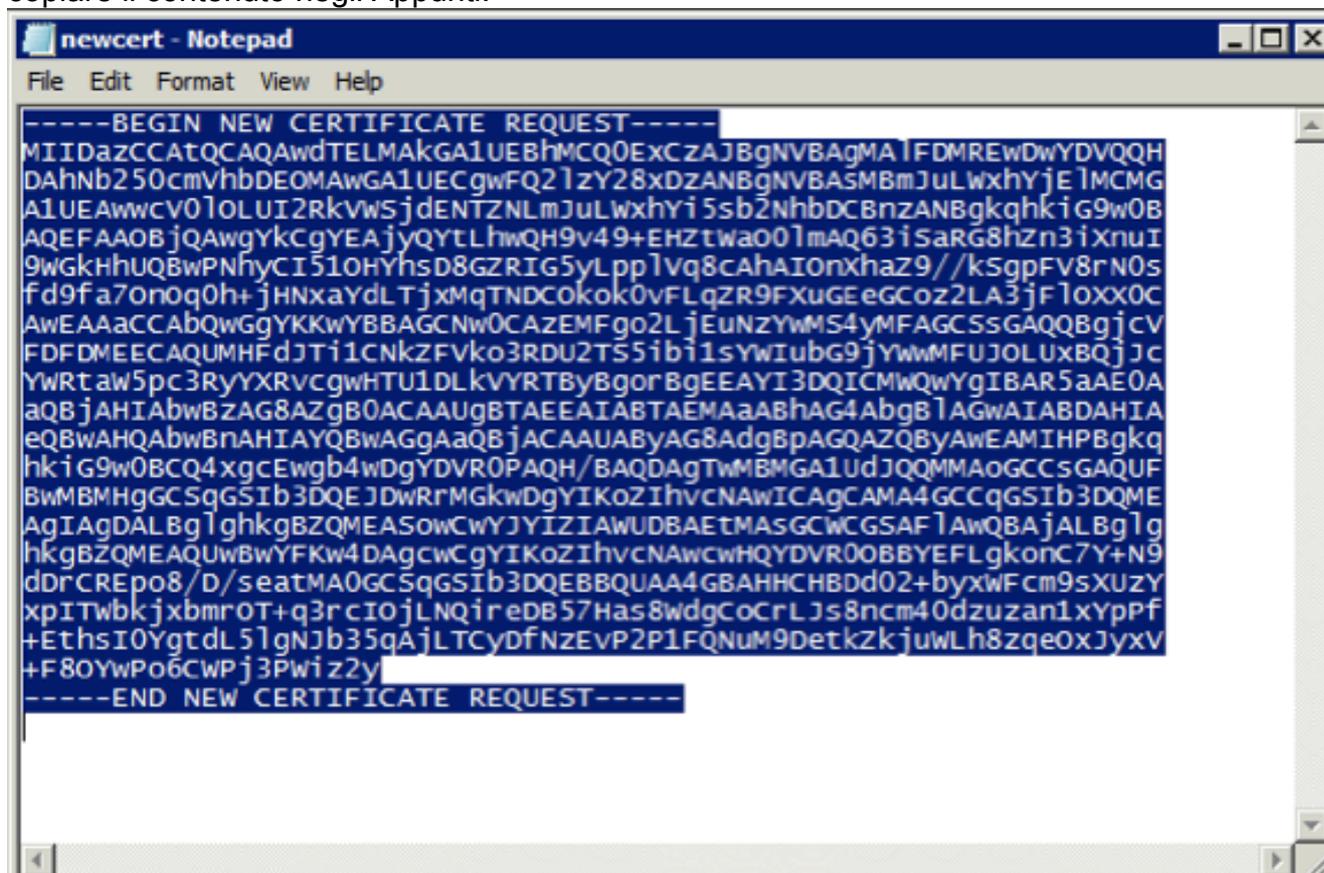


4. Fare clic su **Crea richiesta certificato** e completare i campi.

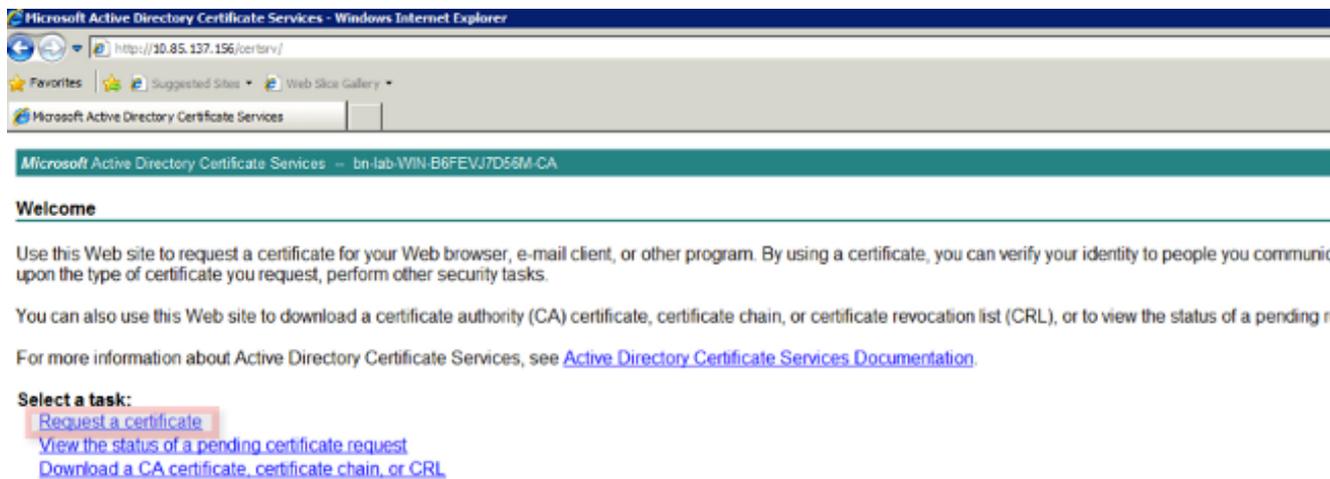




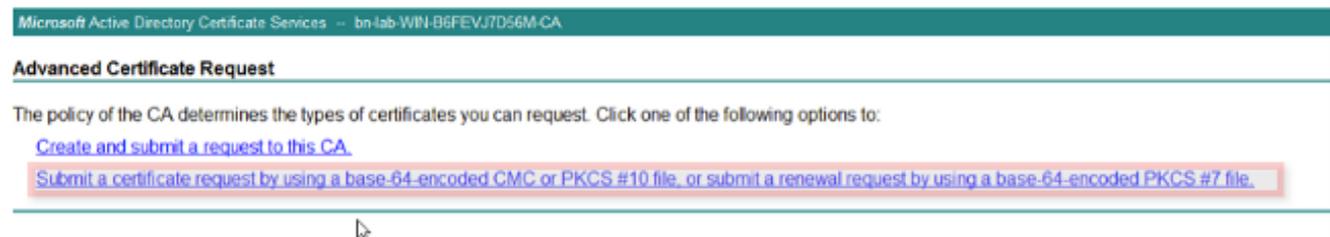
5. Aprire il file con estensione cer creato nel passaggio precedente con un editor di testo e copiare il contenuto negli Appunti.



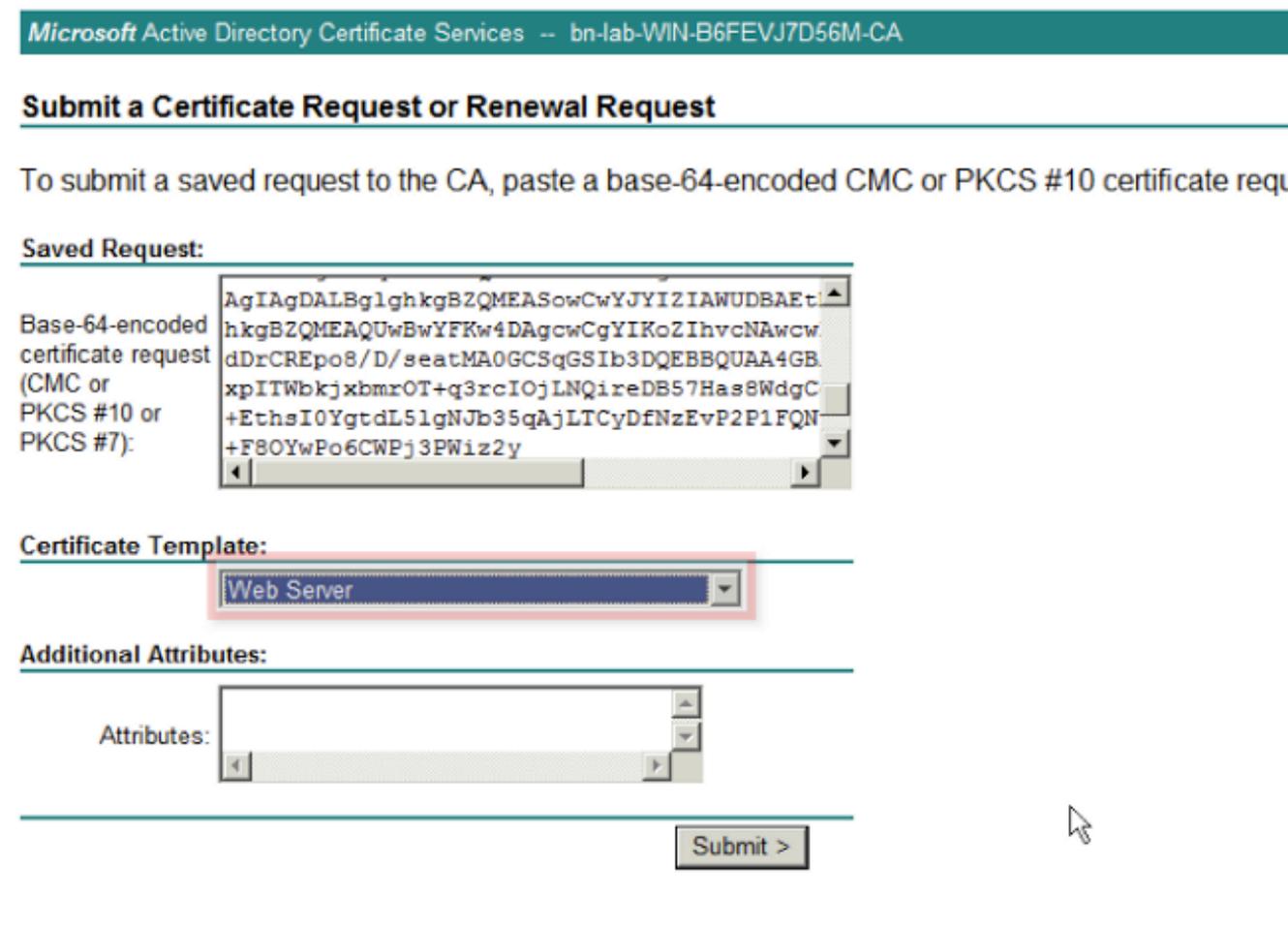
6. Accedere al sito Web di registrazione della CA Microsoft e fare clic su **Richiedi certificato**. URL di esempio: <http://yourCAIP/certsrv>



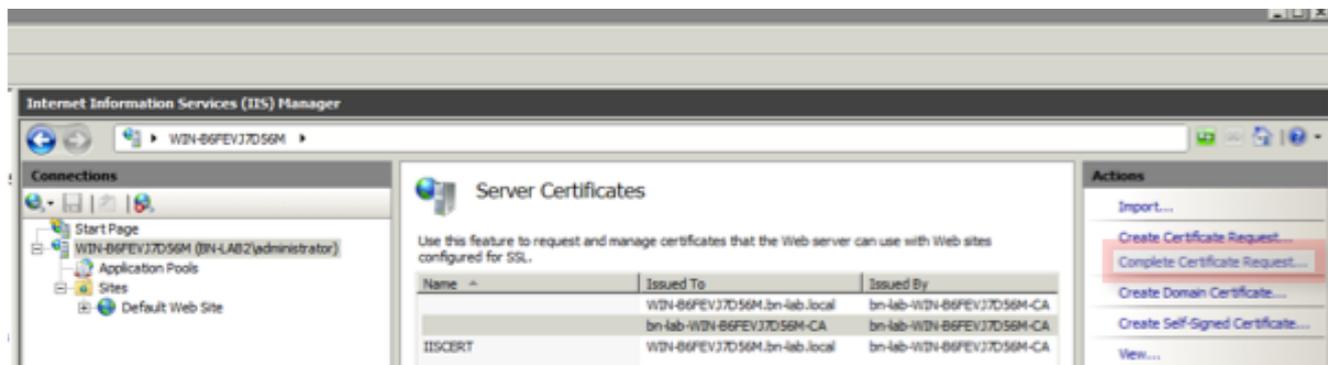
7. Fare clic su **Invia una richiesta di certificato utilizzando...**. Incollare il contenuto del certificato dagli Appunti e scegliere il modello **Server Web**.



8. Fare clic su **Invia**, quindi salvare il file del certificato sul desktop.

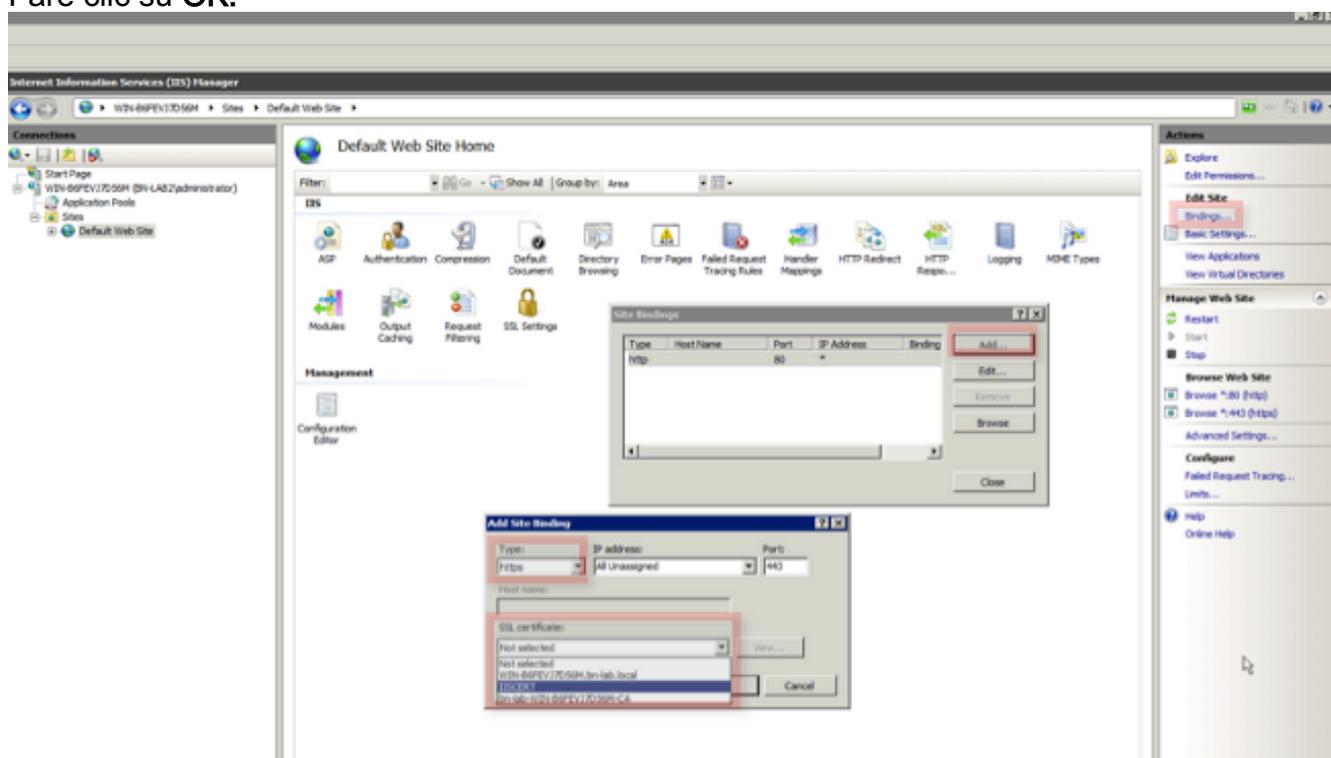


9. Tornare al server NDES e aprire l'utilità Gestione IIS. Per importare il certificato server appena creato, fare clic sul nome del server e quindi su **Completa richiesta certificato**.



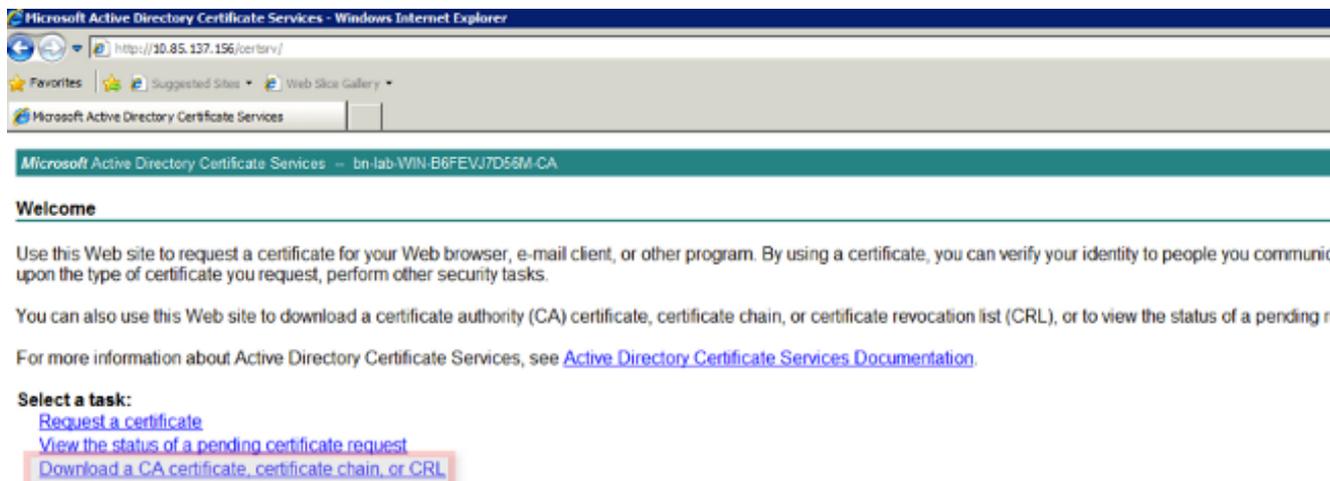
## Configurazione binding IIS NDES Server

1. Espandere il nome del server, Siti, quindi fare clic su **Sito Web** predefinito.
2. Fare clic su **Binding** nell'angolo superiore destro.
3. Fare clic su **Add** (Aggiungi), impostare Type (Tipo) su HTTPS e scegliere il certificato dall'elenco a discesa.
4. Fare clic su **OK**.

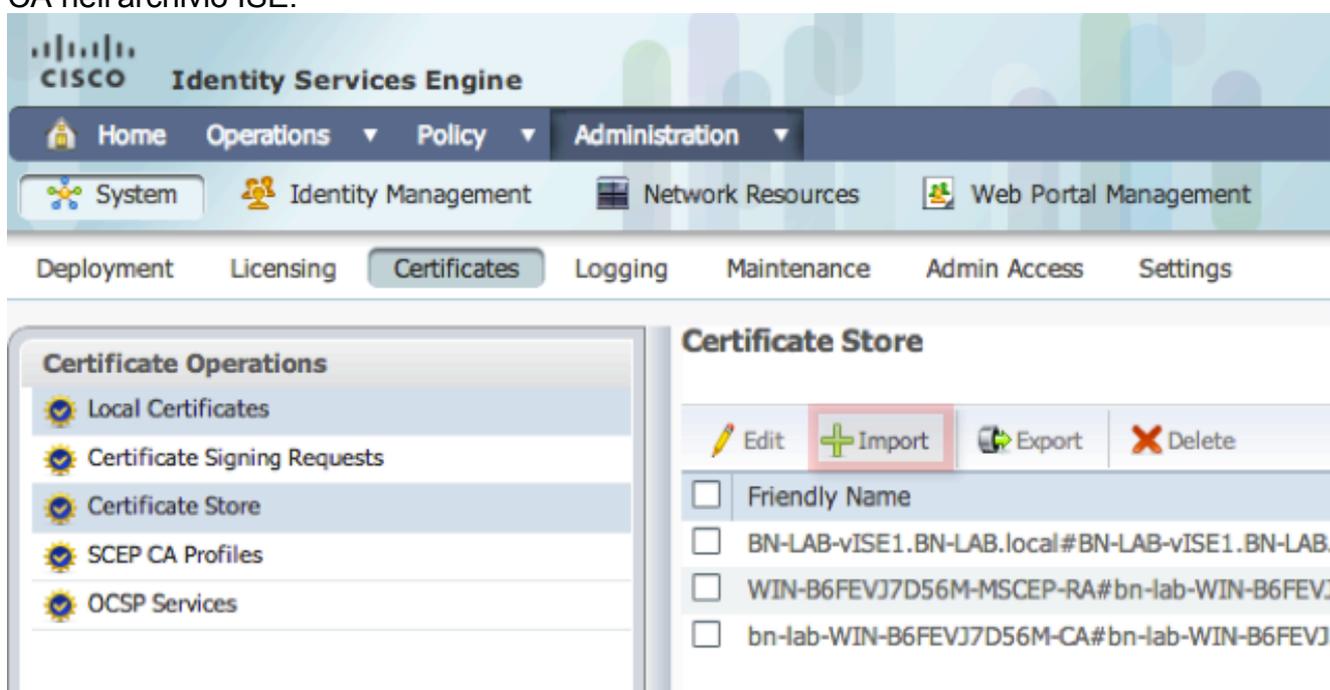


## Configurazione server ISE

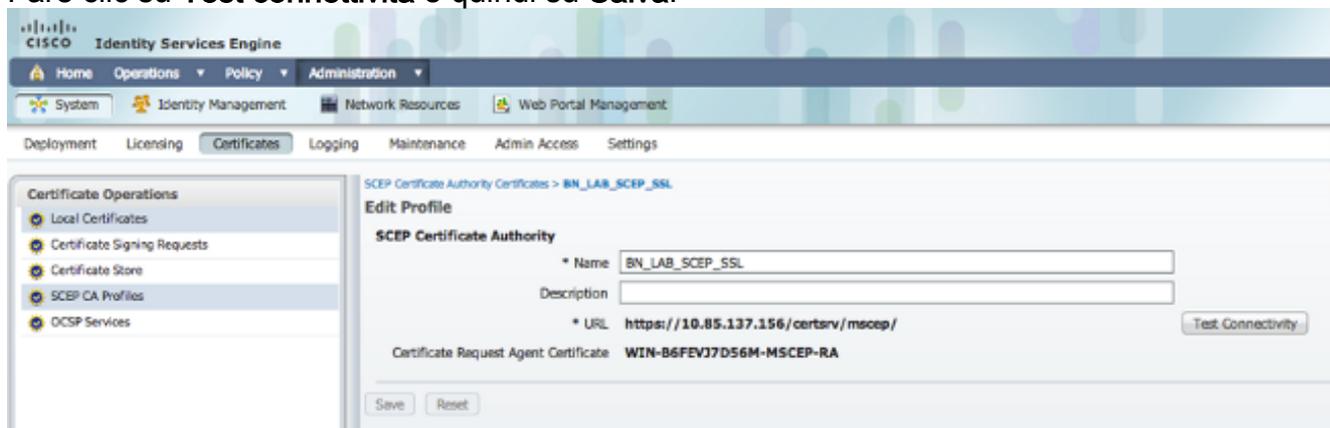
1. Connettersi all'interfaccia di registrazione Web del server CA e scaricare la catena di certificati CA.



2. Dalla GUI di ISE, selezionare **Administration > Certificates > Certificate Store** (Amministrazione > Certificati > Archivio certificati), quindi importare la catena di certificati CA nell'archivio ISE.



3. Passare a **Amministrazione -> Certificati -> Profili CA SCEP** e configurare l'URL per HTTPS. Fare clic su **Test connettività** e quindi su **Salva**.



## Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

- Passare a **Amministrazione** -> **Certificati** -> Archivio **certificati** e verificare che la catena di certificati CA e il certificato RA (Registration Authority) del server NDES siano presenti.
- Usare Wireshark o TCP Dump per monitorare lo scambio SSL iniziale tra il nodo di amministrazione ISE e il server NDES.

Lo [strumento Output Interpreter \(solo utenti registrati\) supporta alcuni comandi show](#). Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show**.

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

- Suddividere la topologia di rete BYOD in punti di riferimento logici per identificare i punti di debug e di acquisizione sul percorso tra questi endpoint, ISE, NDES e CA.
- Verificare che TCP 443 sia consentito in modo bidirezionale tra ISE e il server NDES.
- Monitorare i registri delle applicazioni server CA e NDES per individuare eventuali errori di registrazione e utilizzare Google o TechNet per ricercarli.
- Usare l'utility TCP Dump sul PSN ISE e monitorare il traffico da e verso il server NDES. È disponibile in **Operazioni > Strumenti diagnostici > Strumenti generali**.
- Installare Wireshark sul server NDES o usare SPAN sugli switch intermedi per acquisire il traffico SCEP da e verso il PSN su ISE.

Lo [strumento Output Interpreter \(solo utenti registrati\) supporta alcuni comandi show](#). Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show**.

**Nota:** consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di debug.

## Informazioni correlate

- [Configurazione del supporto SCEP per BYOD](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)