

# Configurazione di VCS con CAC e lettore di smart card

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Che cos'è una smart card?](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

## Introduzione

Questo documento descrive una guida dettagliata all'installazione e all'utilizzo di un lettore di smart card e di una scheda di accesso comune da utilizzare con Cisco Video Communication Server (VCS) per le organizzazioni che richiedono l'autenticazione a due fattori per l'ambiente VCS, ad esempio banche, ospedali o enti pubblici con strutture protette.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Expressway Administrator (X14.0.2).

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.

## Premesse

Il CAC fornisce l'autenticazione necessaria in modo che i "sistemi" sappiano chi ha avuto accesso al proprio ambiente e quale parte dell'infrastruttura sia fisica o elettronica. Negli ambienti governativi classificati, e in altre reti sicure, prevalgono le regole dell'"accesso meno privilegiato" o della "necessità di sapere". Un accesso può essere utilizzato da chiunque, l'autenticazione richiede qualcosa che l'utente ha, ergo il CAC, anche noto come Common Access Card, è nato

nel 2006 in modo che l'individuo non ha bisogno di avere più dispositivi, che siano i piedini, carte d'identità o dongle per accedere al loro luogo di lavoro o sistemi.

## Che cos'è una smart card?

Le smart card sono un componente chiave dell'infrastruttura a chiave pubblica (PKI, Public Key Infrastructure) utilizzata da Microsoft per l'integrazione nella piattaforma Windows, in quanto le smart card consentono di migliorare le soluzioni basate esclusivamente su software, ad esempio l'autenticazione dei client, l'accesso e la protezione della posta elettronica. Le smart card rappresentano un punto di convergenza per i certificati a chiave pubblica e le chiavi associate in quanto:

- Archiviazione a prova di manomissione per la protezione di chiavi private e altre forme di informazioni personali.
- Isolare i calcoli critici per la sicurezza, che implicano l'autenticazione, le firme digitali e lo scambio di chiavi da altre parti del sistema che non hanno necessità di conoscere.
- Consente la portabilità delle credenziali e di altre informazioni private tra computer al lavoro, a casa o in viaggio.

La smart card è diventata parte integrante della piattaforma Windows, in quanto offre funzionalità nuove e interessanti, rivoluzionarie per il settore informatico come l'introduzione del mouse o del CD-ROM. Se al momento non si dispone di un'infrastruttura PKI interna, è necessario assicurarsi di eseguire questa operazione. Il presente documento non descrive l'installazione di questo ruolo in questo particolare articolo, ma per informazioni su come implementarlo, fare clic qui:

<http://technet.microsoft.com/en-us/library/hh831740.aspx>.

## Configurazione

In questa esercitazione si presume che il protocollo LDAP sia già stato integrato con VCS e che gli utenti possano eseguire l'accesso con le credenziali LDAP.

1. [Apparecchiature di laboratorio](#)
2. [Installazione della smart card](#)
3. [Configura modelli Autorità di certificazione](#)
4. [Registra il certificato Agente di registrazione](#)
5. [Registra per conto di....](#)
6. [Configurazione di VCS per Common Access Card](#)

Attrezzatura richiesta:

Server di dominio Windows 2012R2 con i seguenti ruoli/software installato:

- Autorità di certificazione
- Active Directory
- DNS
- PC Windows con smart card collegata
- vSEC Software di gestione CMS serie K per la gestione della smart card:



Software Versa Card Reader

## Installazione della smart card

I lettori di smart card in genere includono istruzioni su come collegare i cavi necessari. Di seguito è riportato un esempio di installazione per questa configurazione.

## Installazione del driver di un lettore di smart card

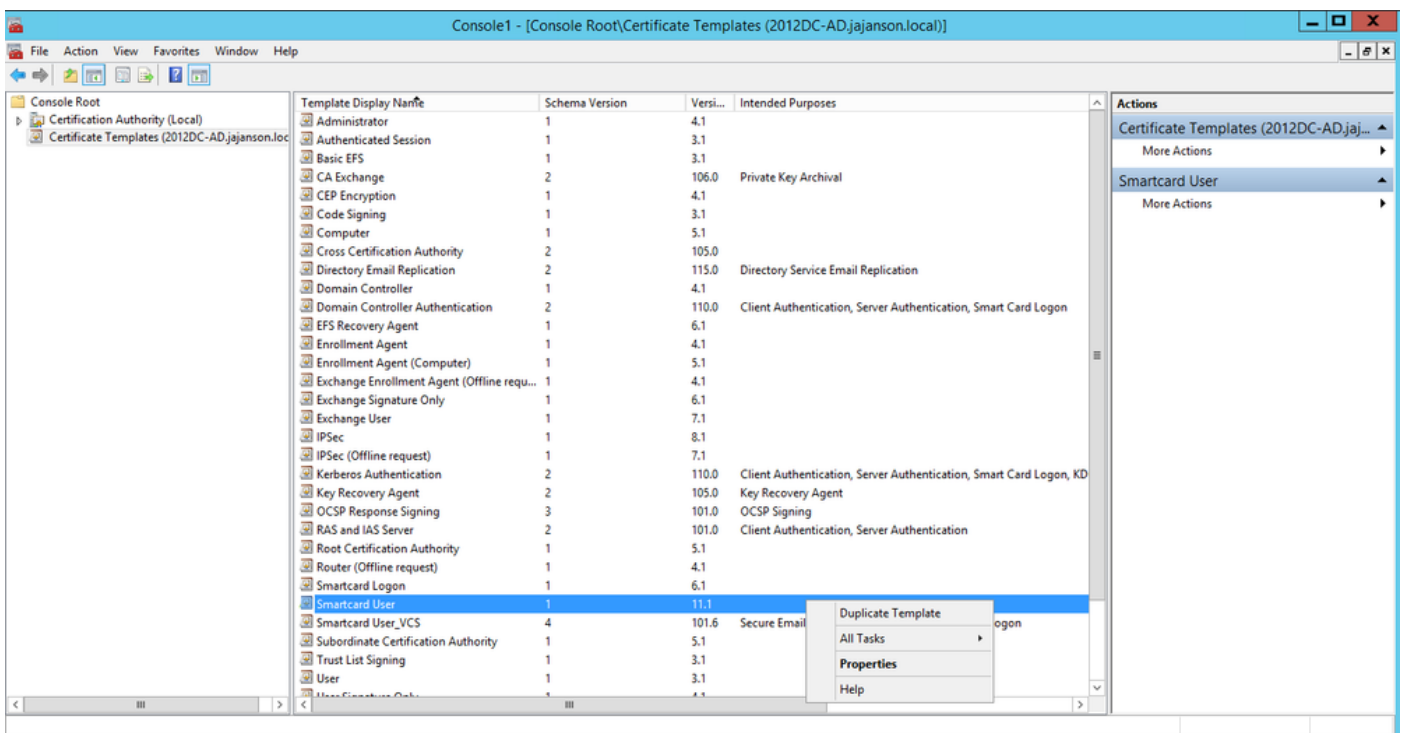
Se il lettore di smart card è stato rilevato e installato, la schermata di accesso di Windows riconosce questa condizione. In caso contrario:

1. Collegare la smart card alla porta USB del PC Windows
2. Seguire le istruzioni visualizzate sullo schermo per l'installazione del driver di periferica. È quindi necessario che il supporto del driver utilizzato dal produttore della smart card o del driver sia individuato in Windows. Nel mio caso ho utilizzato il driver di Manufactures dal loro sito di download. **NON CONSIDERARE ATTENDIBILE WINDOWS.**
3. Fare clic con il pulsante destro del mouse sull'icona **Risorse del computer** sul desktop e scegliere **Gestisci** dal sottomenu.

4. Espandere il nodo **Servizi e applicazioni** e fare clic su **Servizi**.
5. Nel riquadro destro fare clic con il pulsante destro del mouse su **Smart Card**. Scegliere **Proprietà** dal sottomenu.
6. Nella scheda **General** (Generale), selezionare **Automatic** (Automatico) nell'elenco a discesa **Startup Type** (Tipo di avvio). Fare clic su **OK**.
7. Riavviare il computer se richiesto dall'Installazione guidata hardware.

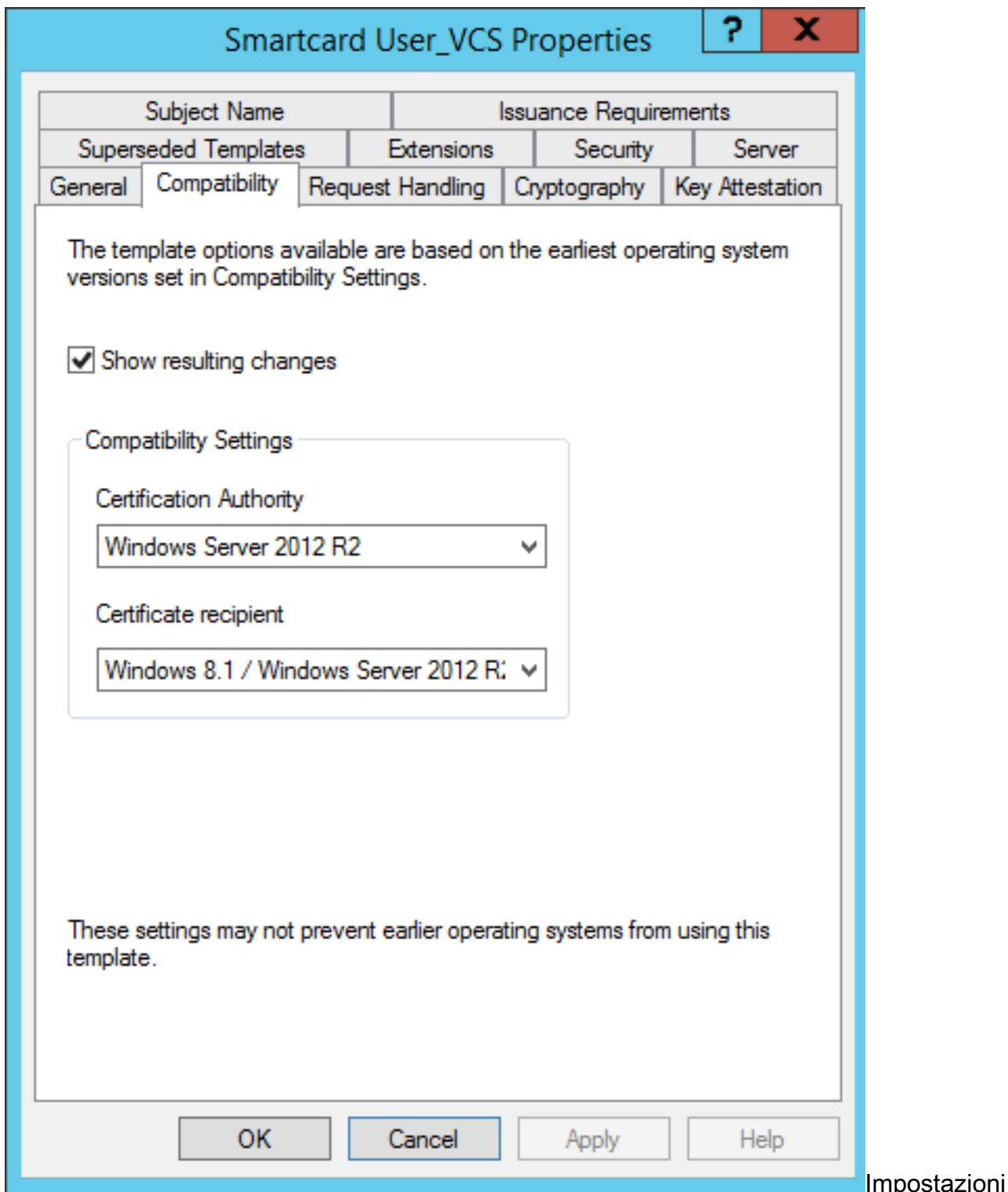
### Configura modelli Autorità di certificazione

1. Avviare MMC Autorità di certificazione da Strumenti di amministrazione.
2. Fare clic sul nodo **Modelli di certificato** o selezionarlo e selezionare **Gestisci**.
3. Fare clic con il pulsante destro del mouse o selezionare il modello di certificato **utente smart card** e quindi selezionare **Duplica** come illustrato nell'immagine.



### Modelli di certificato controller di dominio

4. Nella scheda **Compatibilità**, in **Autorità di certificazione**, rivedere la selezione e modificarla se necessario.



compatibilità smart card

5. Nella scheda **Generale**:

r. Specificare un nome, ad esempio **User\_VCS** della smart card.

b. Impostare il periodo di validità sul valore desiderato. Fare clic su **Apply** (Applica).

Smartcard User\_VCS Properties

Subject Name Issuance Requirements

Superseded Templates Extensions Security Server

General Compatibility Request Handling Cryptography Key Attestation

Template display name:  
Smartcard User\_VCS

Template name:  
Smartcard User\_VCS

Validity period: 10 years

Renewal period: 6 weeks

Publish certificate in Active Directory

Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

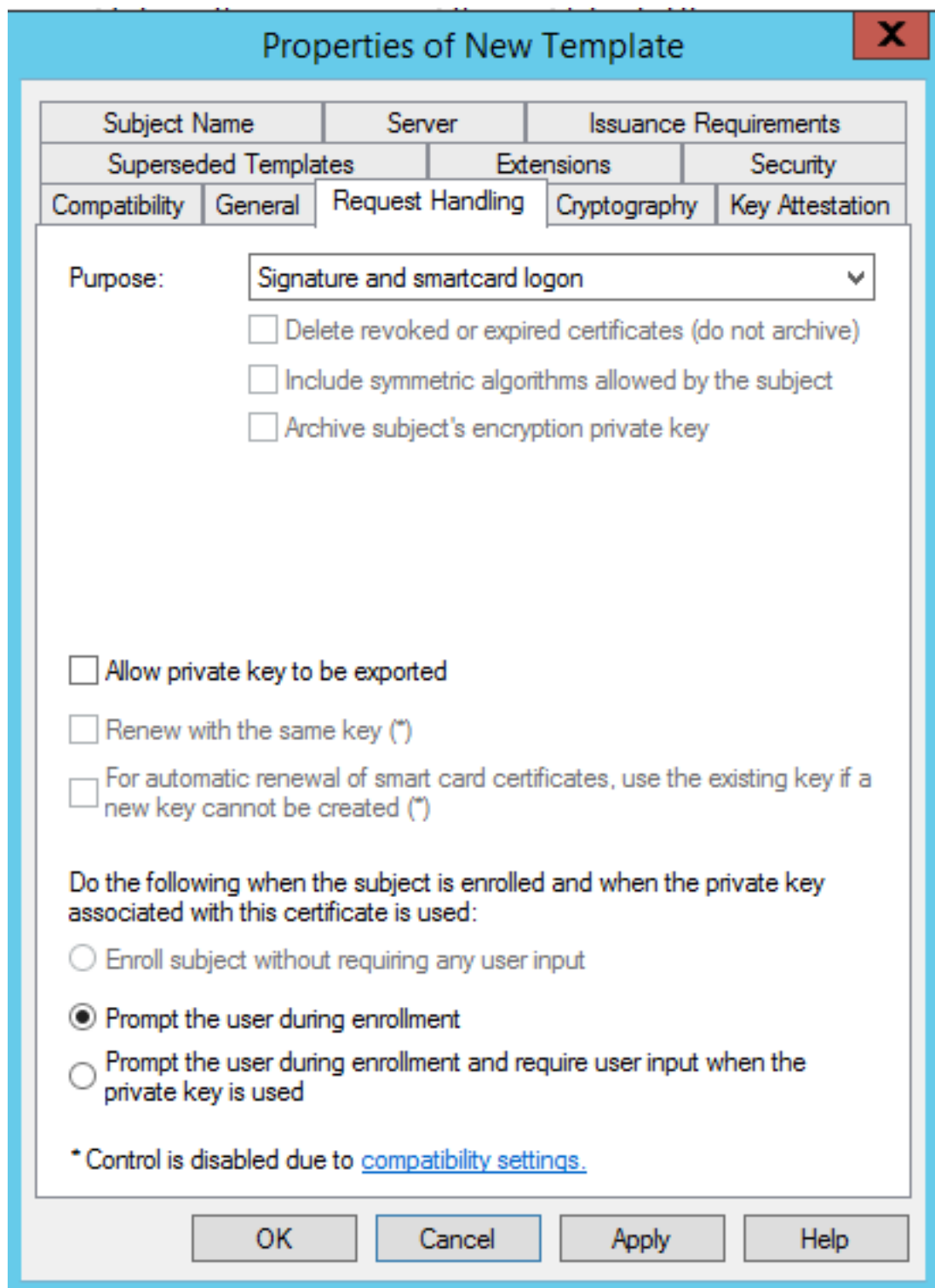
Scadenza ora

generale smart card

6. Nella scheda **Gestione richieste**:

r. Impostare **Scopo** su **Firma e accesso smart card**.

b. Fare clic su **Chiedi conferma all'utente durante la registrazione**. Fare clic su **Apply** (Applica).



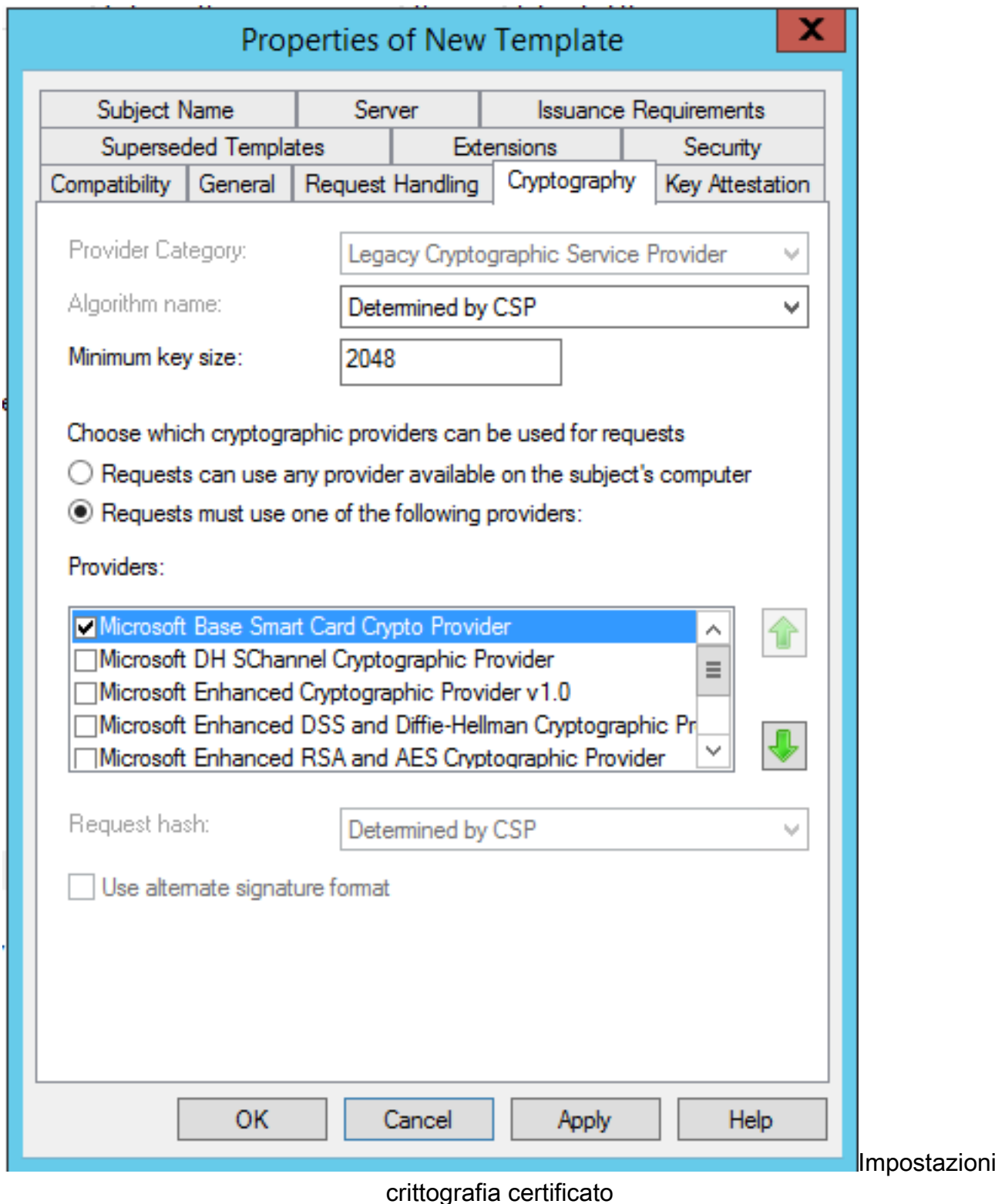
Gestione richieste

smart card

7. Nella scheda **Crittografia** impostare le dimensioni minime della chiave su 2048.

r. Fare clic su **Le richieste devono utilizzare uno dei provider seguenti**, quindi selezionare **Microsoft Base Smart Card Crypto Provider**.

b. Fare clic su **Apply (Applica)**.

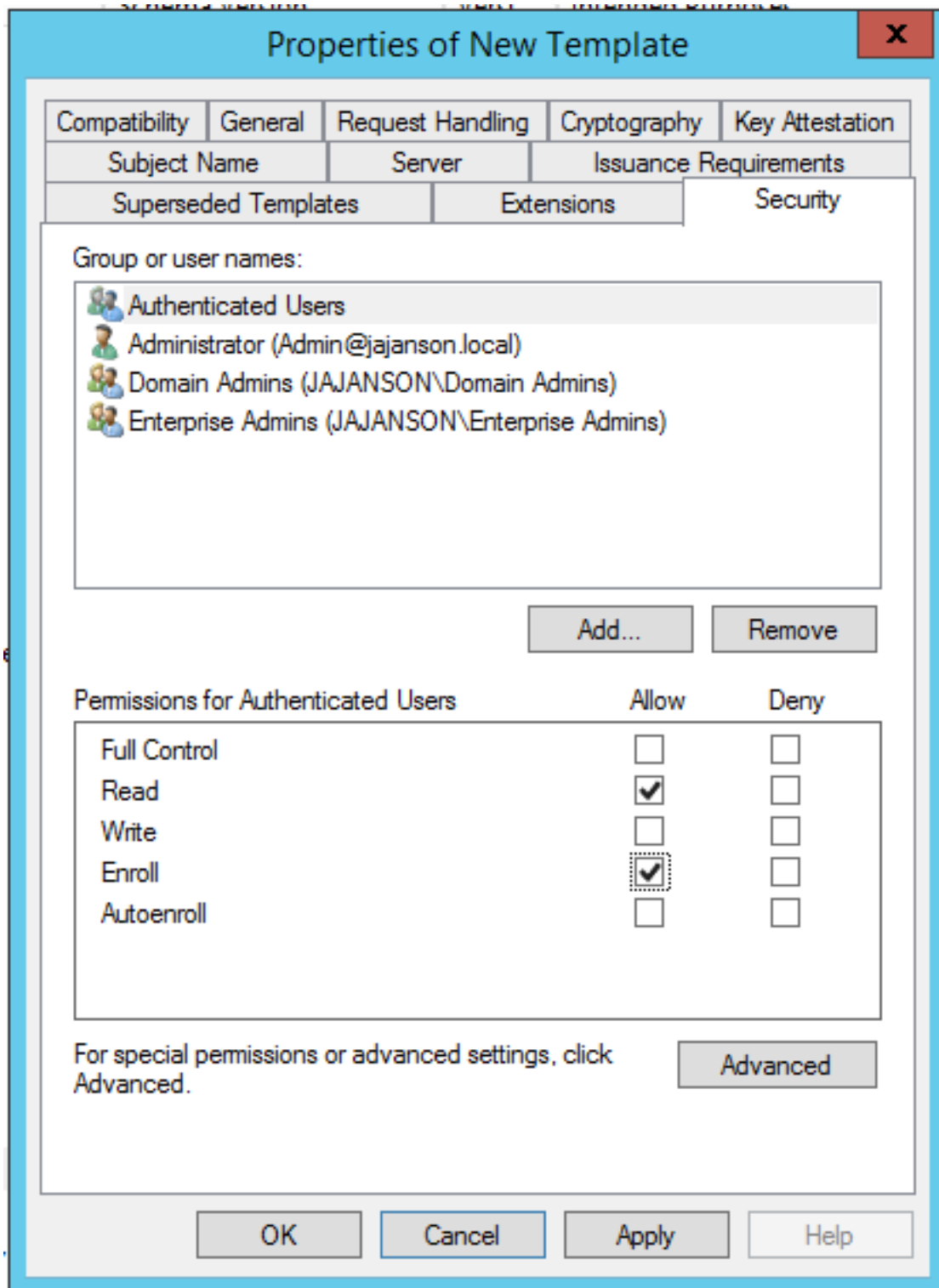


Impostazioni

crittografia certificato

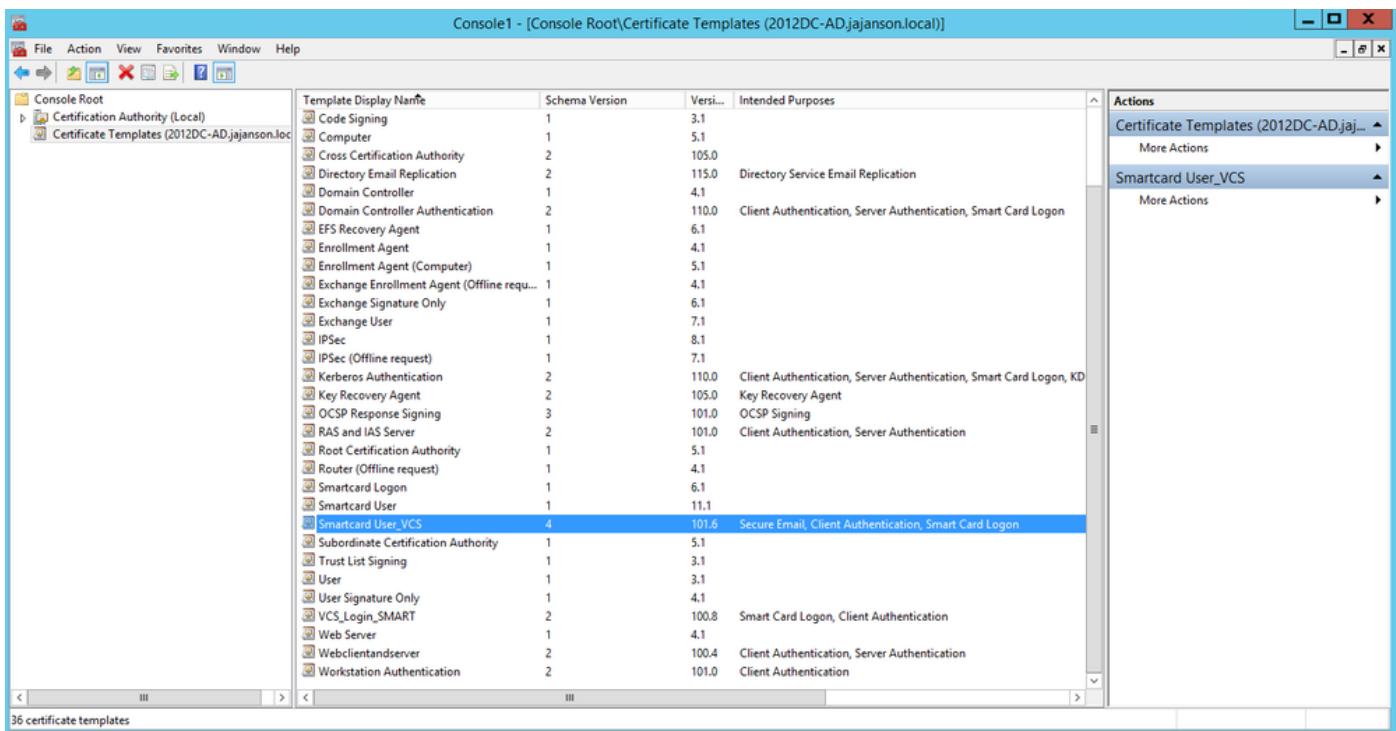
8. Nella scheda Protezione aggiungere il gruppo di protezione a cui si desidera concedere l'accesso Registrazione. Ad esempio, se si desidera concedere l'accesso a tutti gli utenti, selezionare il gruppo Utenti autenticati e quindi selezionare **Registra** autorizzazioni per tali utenti.





Sicurezza modello

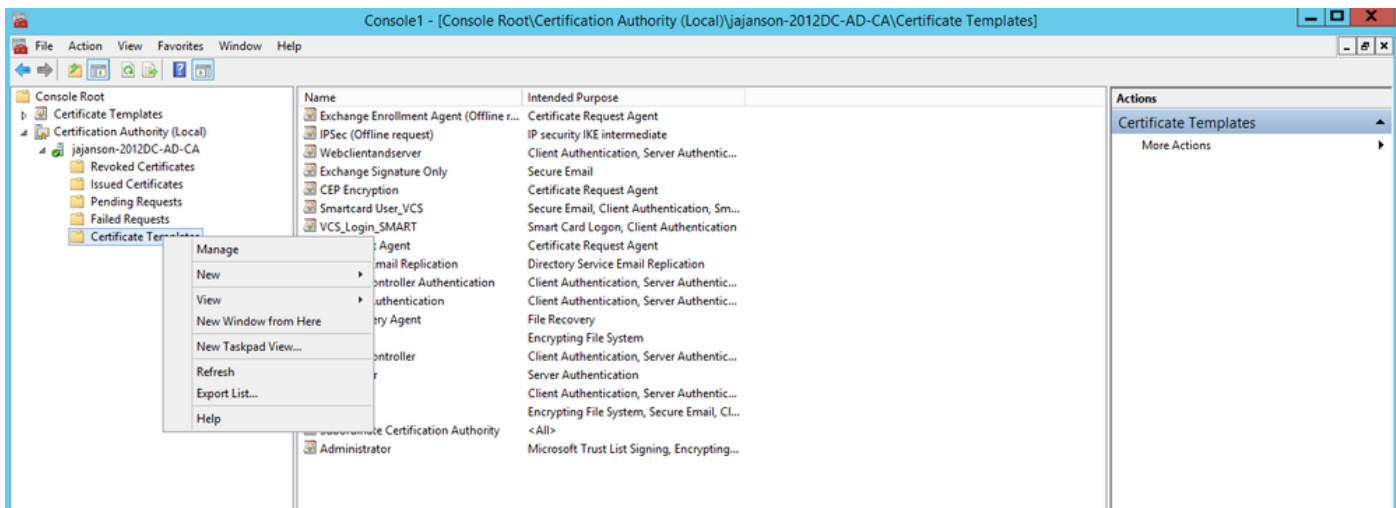
9. Fare clic su **OK** per finalizzare le modifiche e creare il nuovo modello. Il nuovo modello deve essere visualizzato nell'elenco dei modelli di certificato.



Modello visualizzato nel controllo del dominio

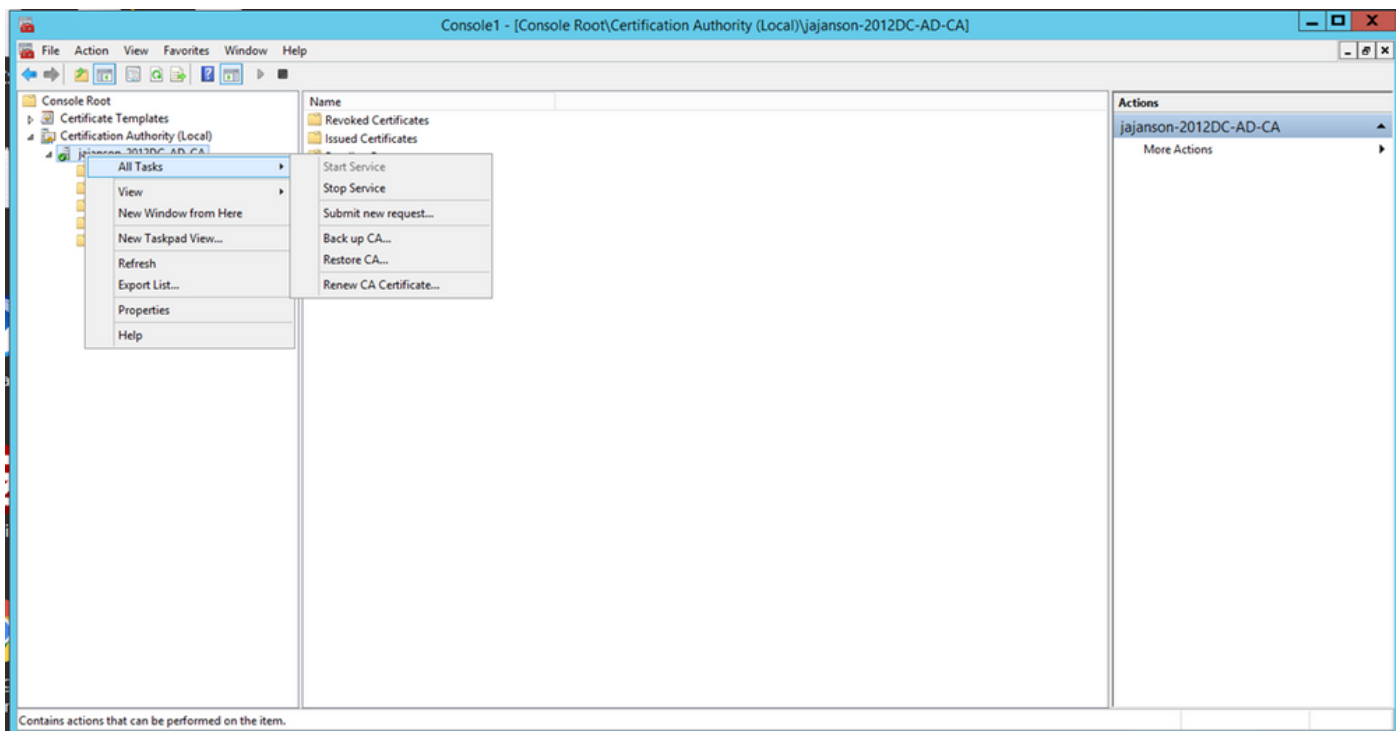
10. Nel riquadro sinistro di MMC espandere Autorità di certificazione (locale), quindi l'Autorità di certificazione nell'elenco Autorità di certificazione.

Fare clic con il pulsante destro del mouse su Modelli di certificato, scegliere **Nuovo** e quindi fare clic su **Modello di certificato** da rilasciare. Scegliere quindi il modello di smart card appena creato.



Rilascia nuovo modello

11. Una volta replicato il modello, in MMC fare clic con il pulsante destro del mouse o selezionare l'elenco Autorità di certificazione, scegliere **Tutte le attività**, quindi **Arresta servizio**. Fare quindi nuovamente clic con il pulsante destro del mouse sul nome della CA, scegliere **Tutte le attività**, quindi **Avvia servizio**.

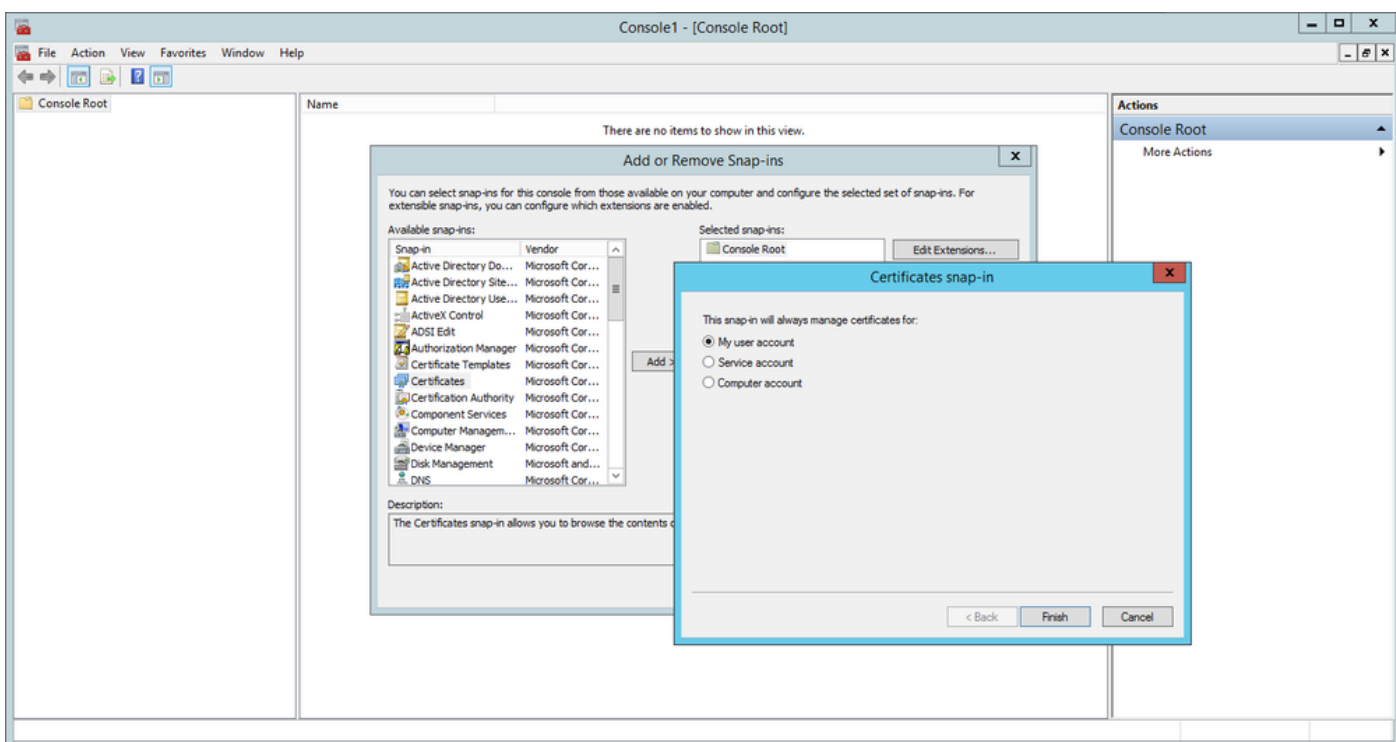


Arresta e avvia i servizi certificati

## Registra nel certificato Agente di registrazione

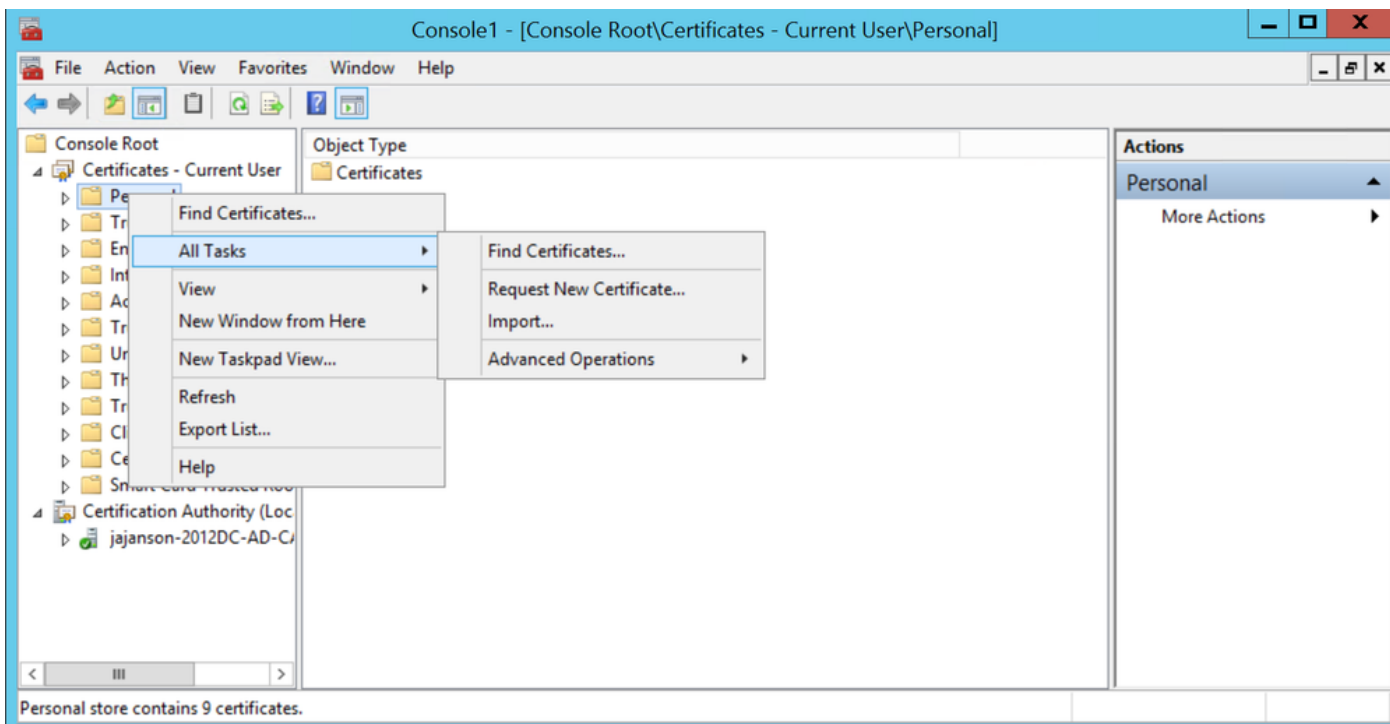
Si consiglia di eseguire questa operazione su un computer client (desktop amministratori IT).

1. Avviare MMC. Scegliere **Certificati**, fare clic su **Aggiungi**, quindi su **Certificati per Account utente**.



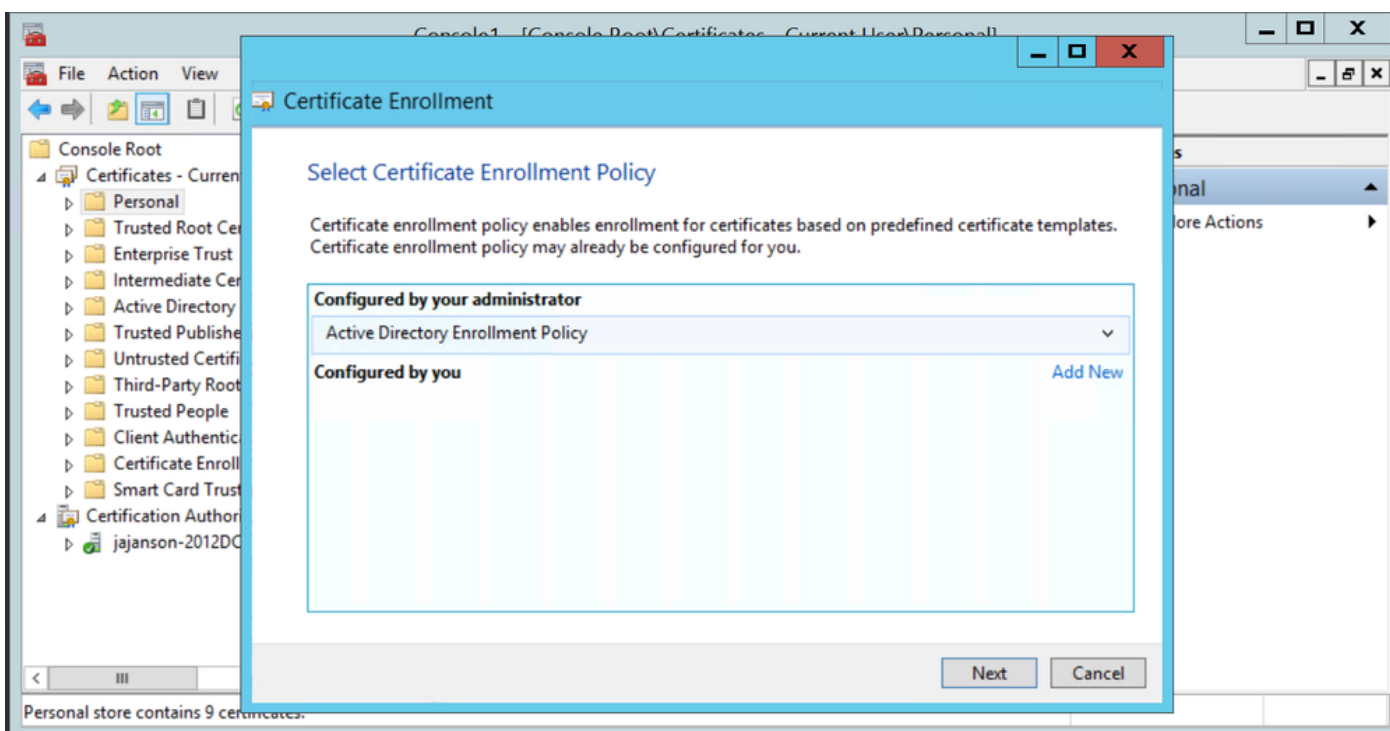
Aggiungi certificati

2. Fare clic con il pulsante destro del mouse o selezionare il **nodo personale**, selezionare **Tutte le attività** e quindi **Richiedi nuovo certificato**.



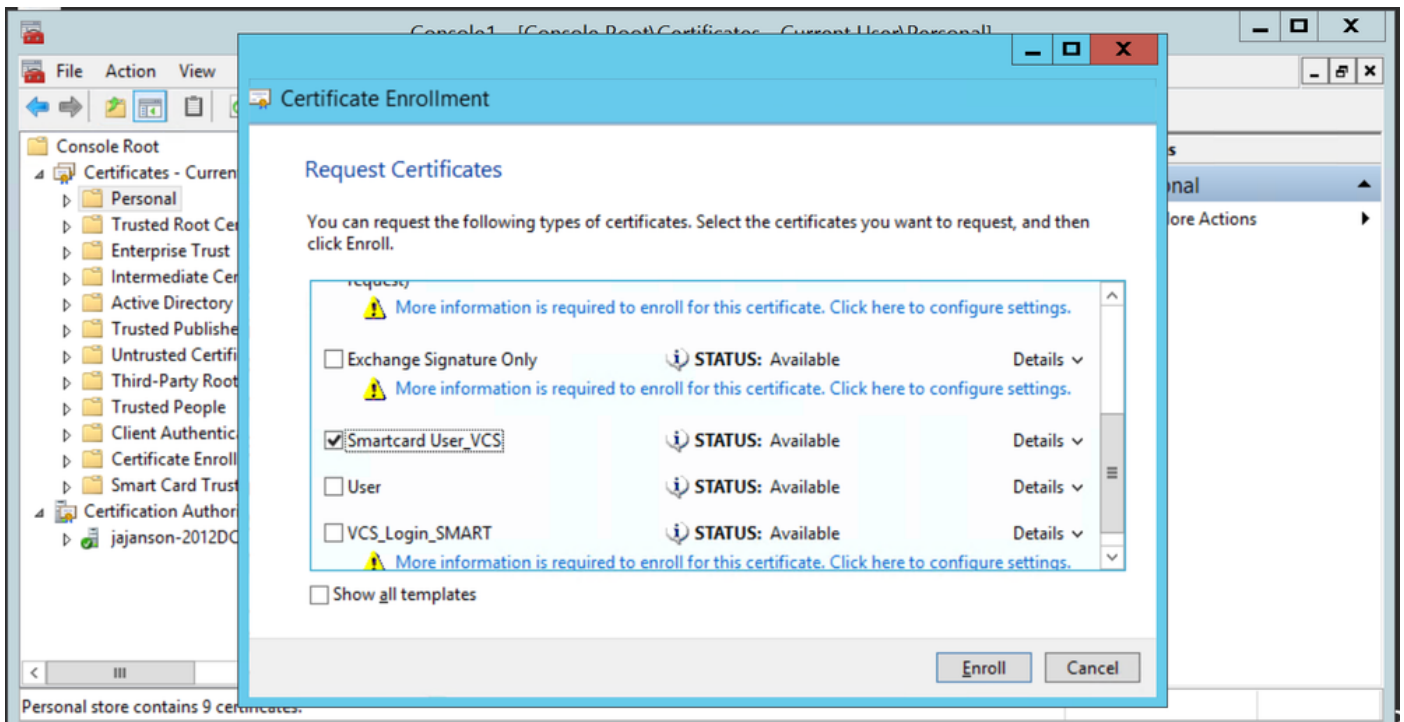
Richiedi nuovi certificati

3. Fare clic su **Avanti** nella procedura guidata e quindi selezionare **Criteri di registrazione di Active Directory**. Quindi fare di nuovo clic su **Avanti**.



Registrazione Active Directory

4. Selezionare il certificato **Agente di registrazione**, in questo caso **Smart Card User\_VCS**, quindi fare clic su **Registra**.

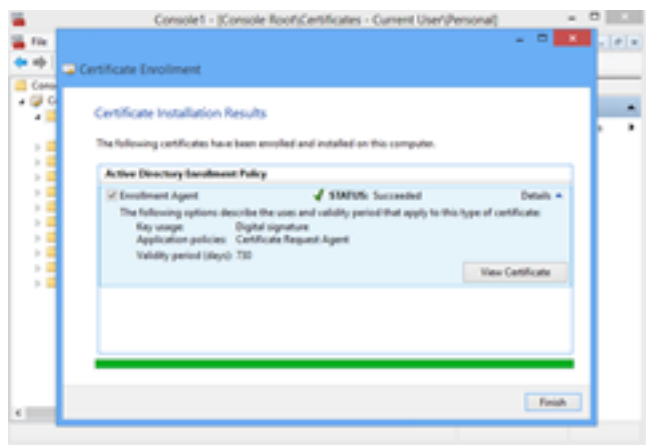


Agente certificato di registrazione

Il desktop degli amministratori IT è ora configurato come stazione di registrazione, consentendo di registrare nuove smart card per conto di altri utenti.

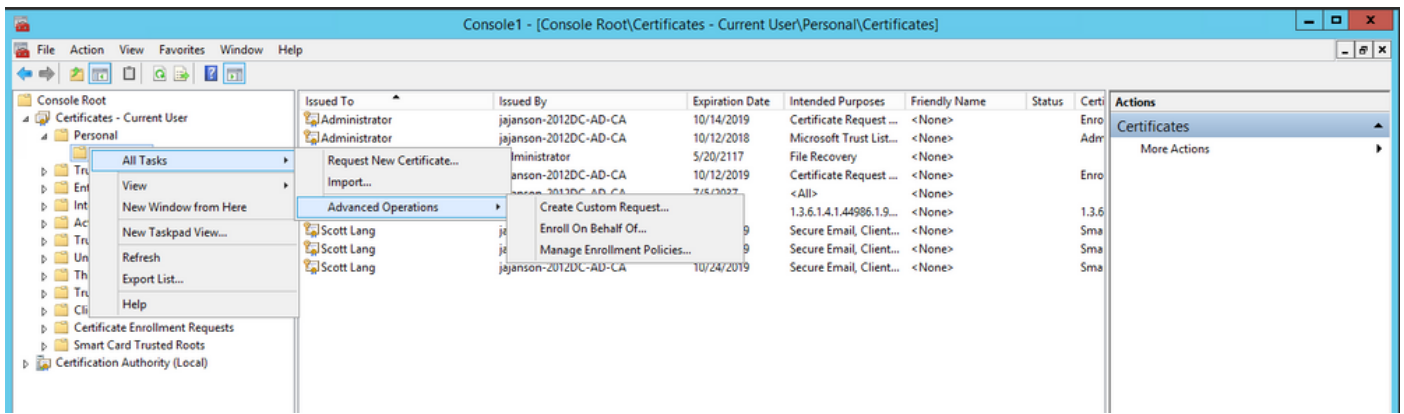
### Registra per conto di....

Per fornire ai dipendenti le smart card per l'autenticazione, è necessario registrarle e generare il certificato che verrà quindi importato nella smart card.

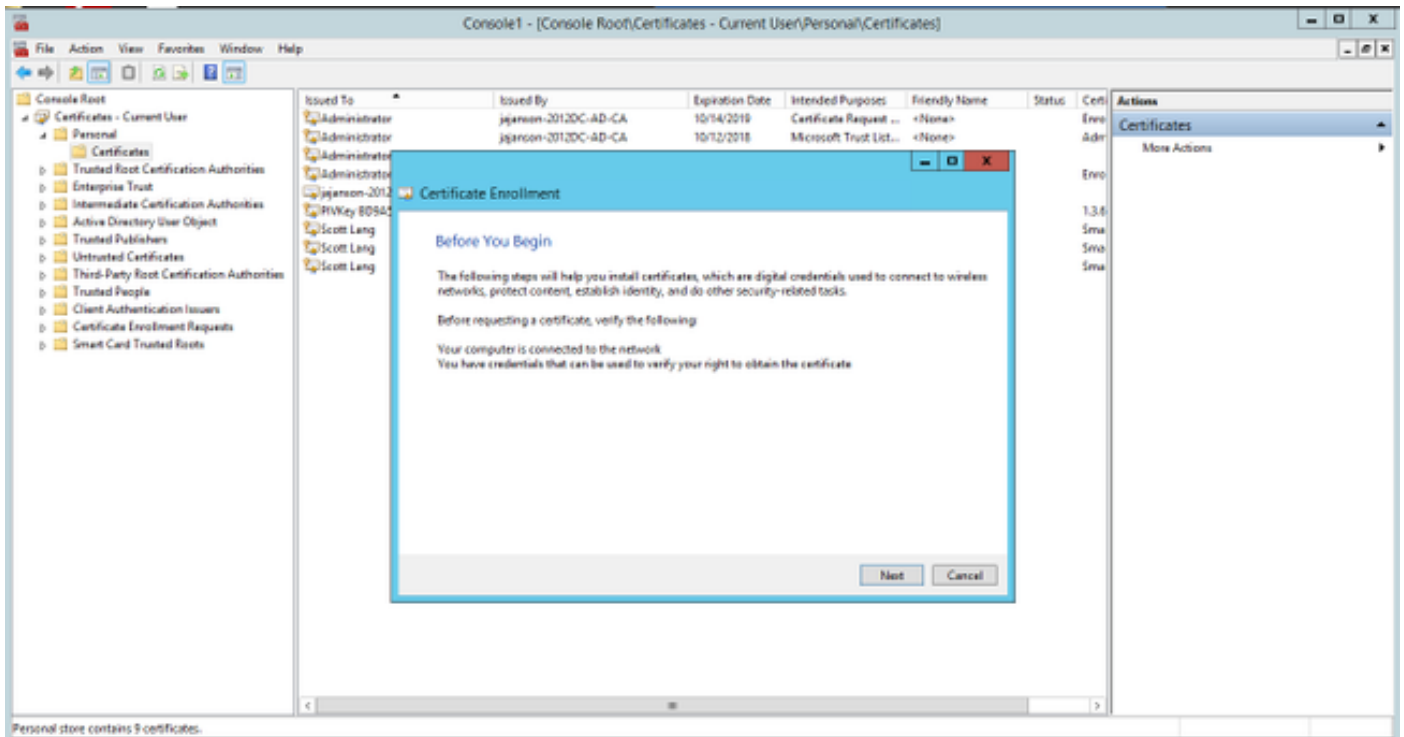


Registra per conto di

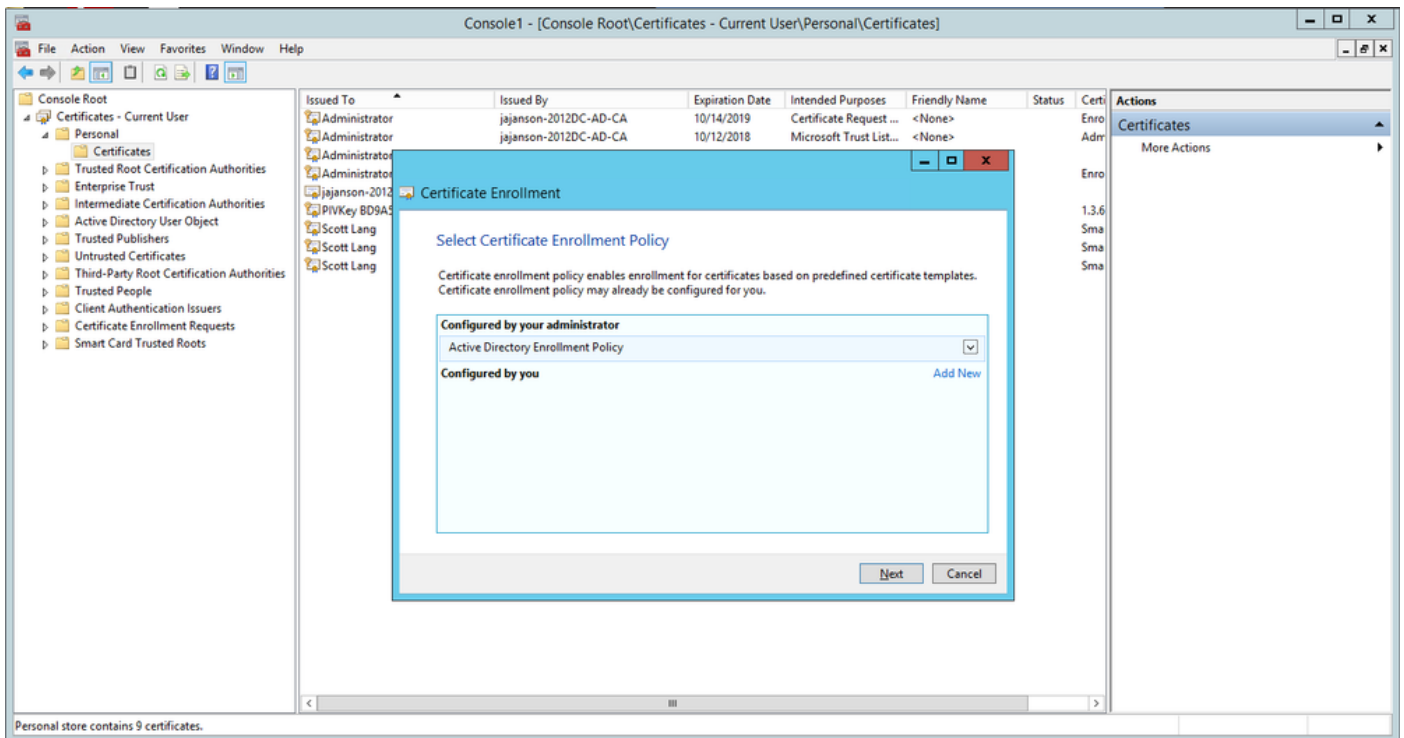
1. Avviare MMC e importare i certificati **Modulo certificati e manager** per Il mio account utente.
2. Fare clic con il pulsante destro del mouse o selezionare **Personale > Certificati** e selezionare **Tutte le attività > Operazioni avanzate** e fare clic su **Registra per conto di...**
3. Nella procedura guidata, scegliere il criterio di registrazione di Active Directory, quindi fare clic su **Avanti**.



## Registrazione per conto di utenti avanzati

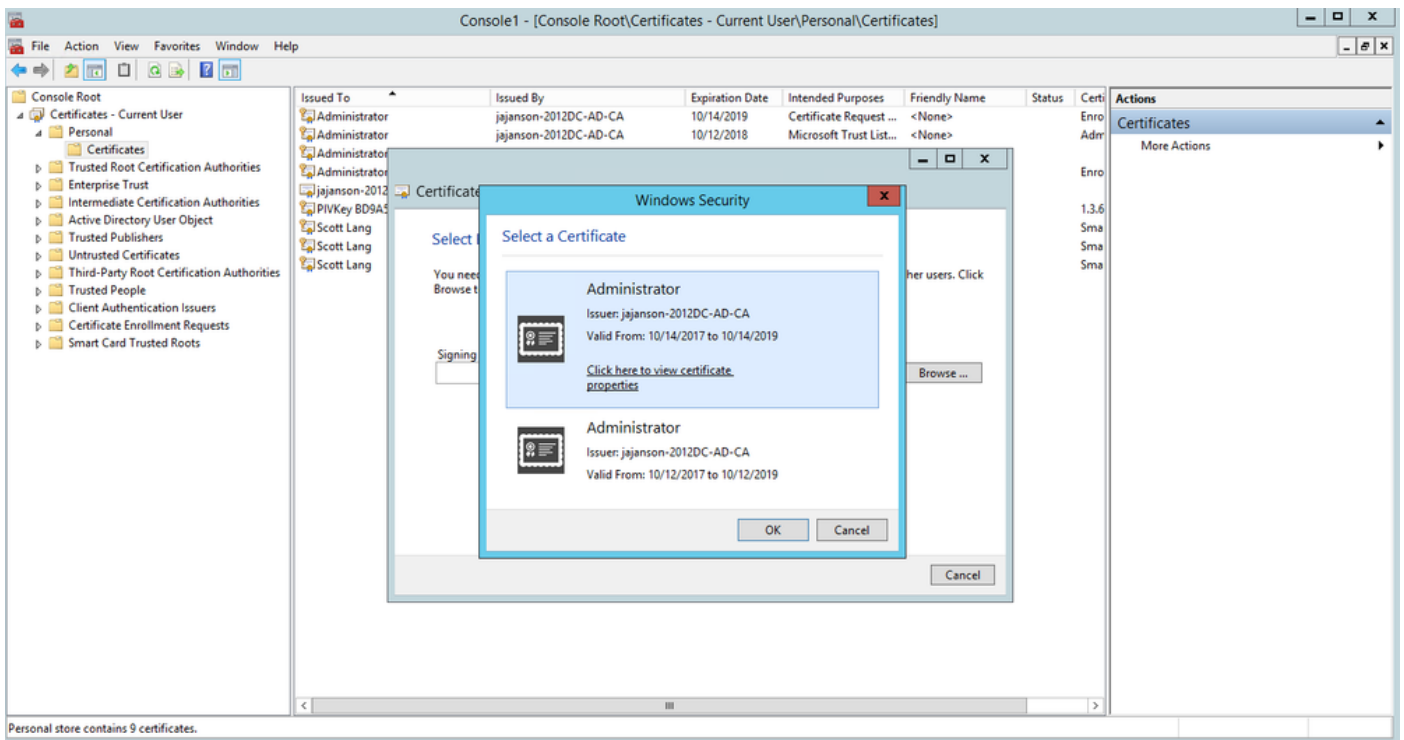


4. Selezionare Criteri di registrazione certificati, quindi fare clic su **Avanti**.



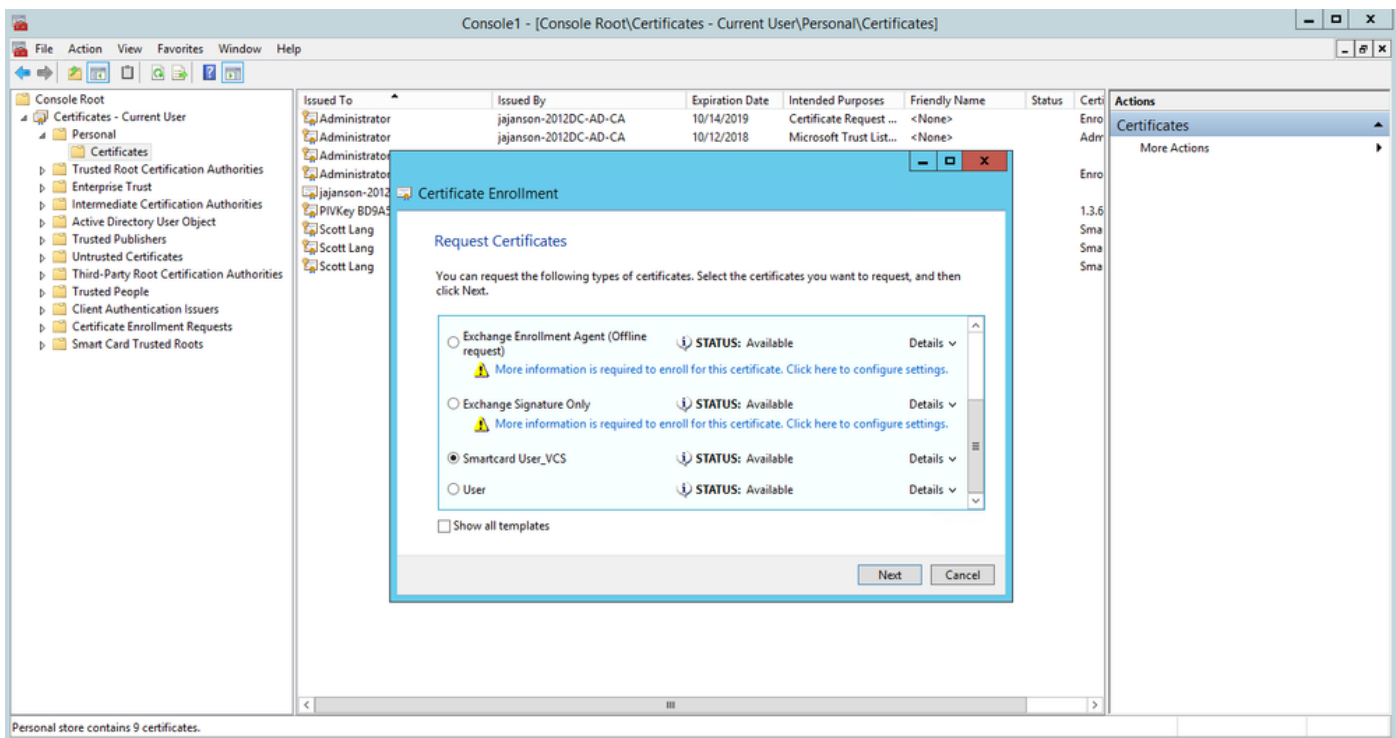
## Criteri di registrazione

5. Verrà richiesto di selezionare il **certificato di firma**. Si tratta del certificato di registrazione richiesto in precedenza.



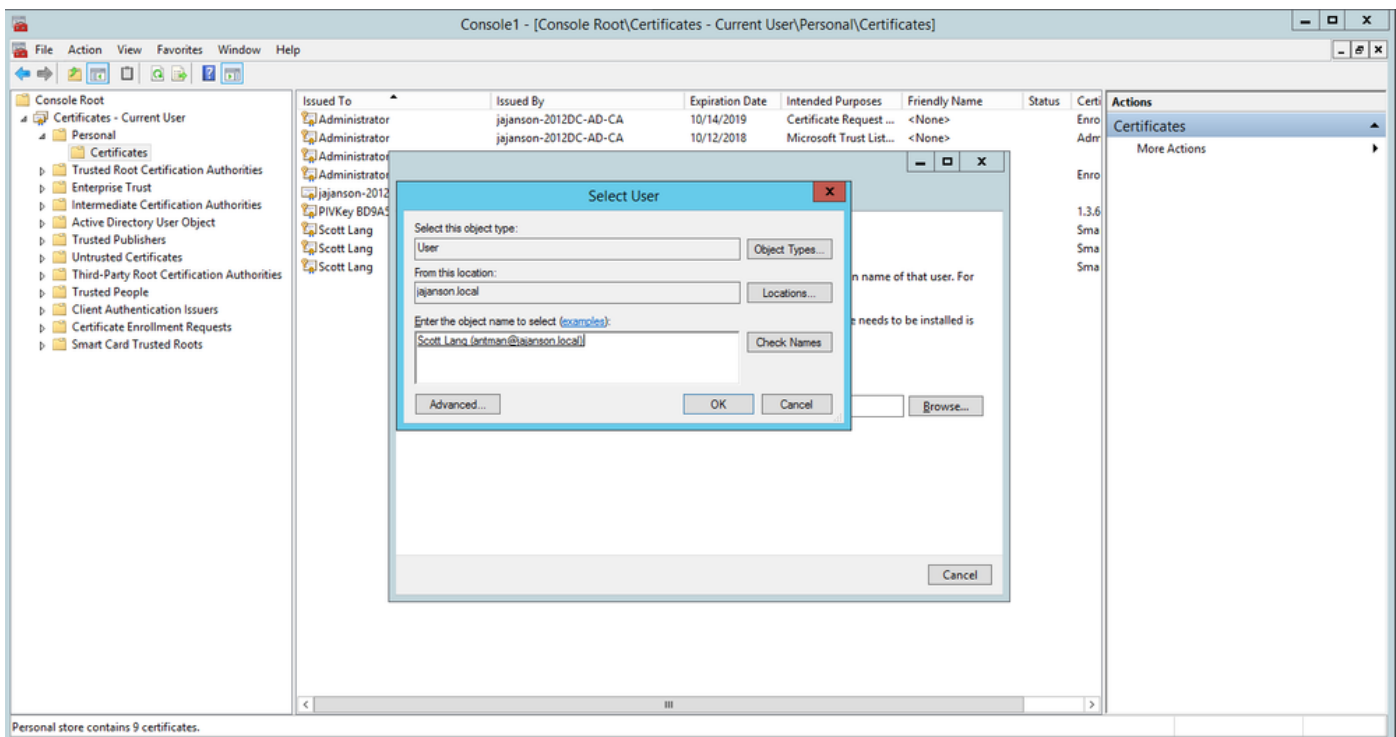
## Seleziona certificato di firma

6. Nella schermata successiva, è necessario selezionare il certificato che si desidera richiedere e, in questo caso, è **Smartcard User\_VCS** il modello creato in precedenza.



Scelta della smart card VCS

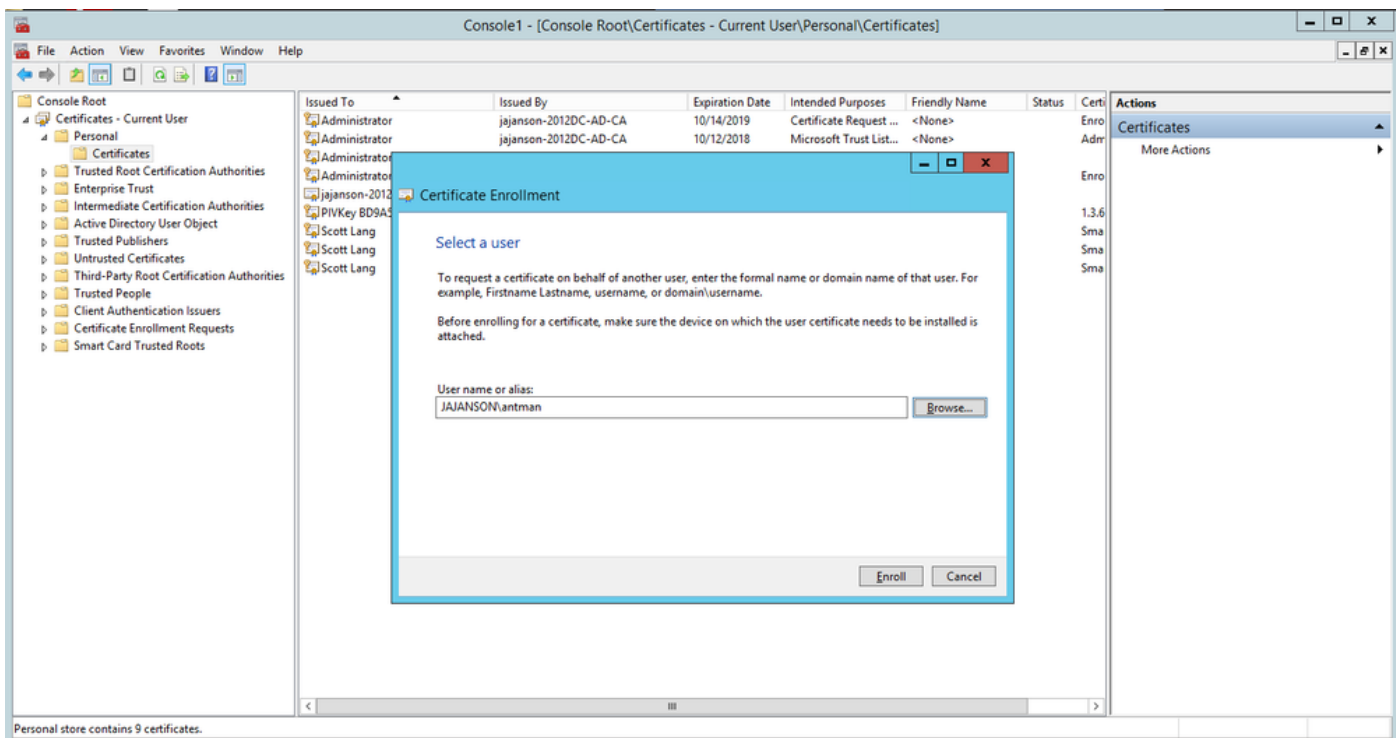
7. Quindi, è necessario selezionare l'utente che si desidera iscrivere per conto di. Fare clic su **Sfoglia** e digitare il nome utente del dipendente che si desidera iscrivere. In questo caso viene utilizzato l'account 'antman@jajanson.local' di Scott Lang.



Scegli l'utente

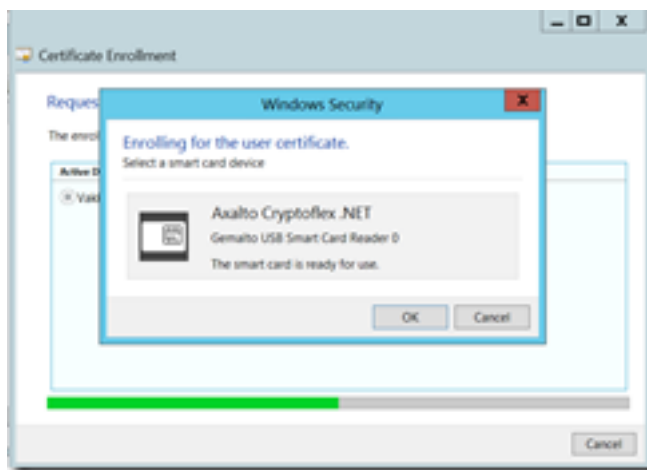
8. Nella schermata successiva, procedere con la registrazione facendo clic su **Enroll**. Inserire una smart card nel lettore.





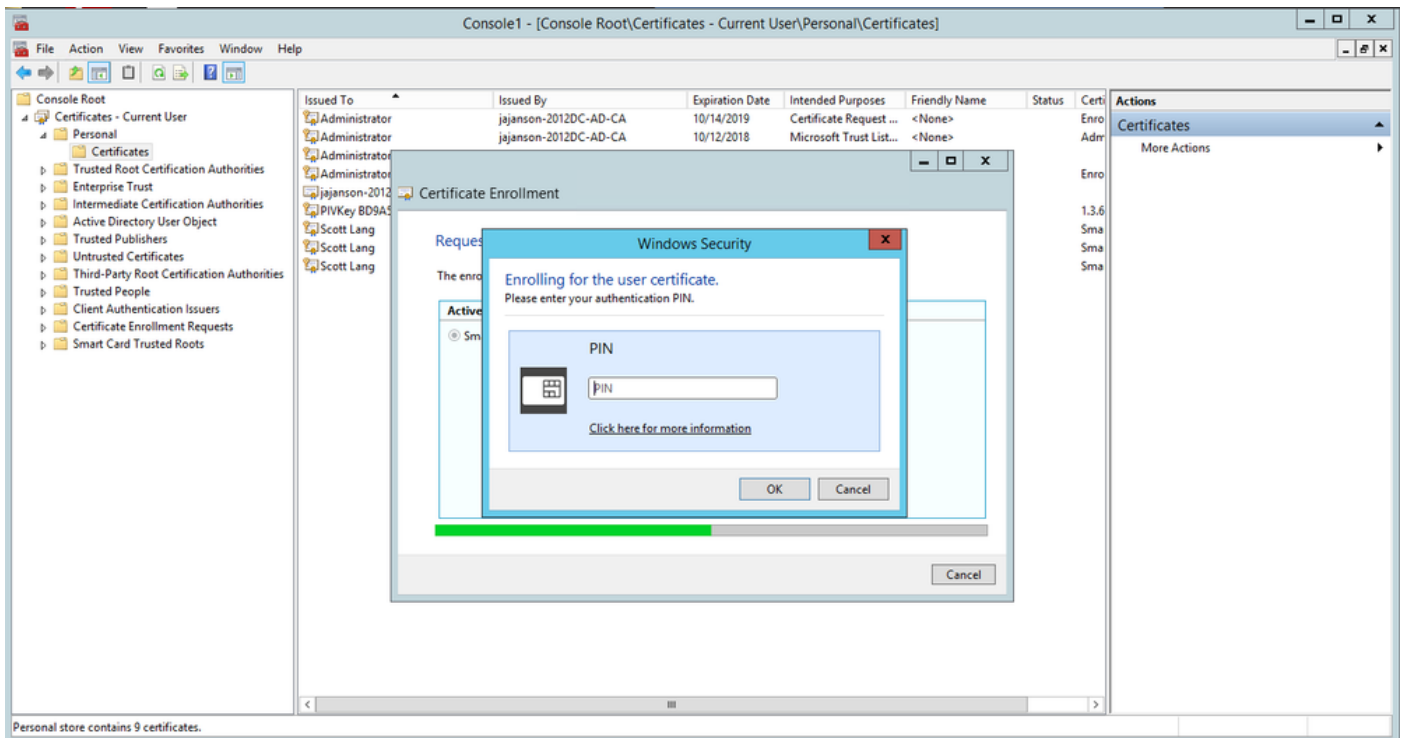
## Registrati

9. Una volta inserita la smart card, viene rilevata come segue:



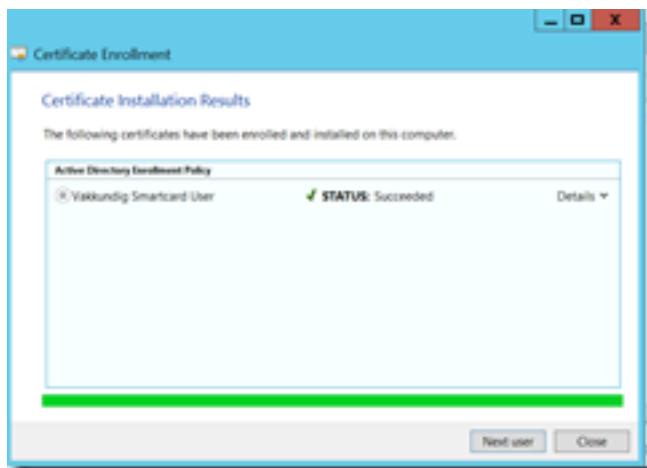
Inserire la smart card

10. Viene quindi richiesto di immettere un numero PIN della smart card (PIN predefinito: 0000).



Immettere il pin

11. Infine, una volta visualizzata la schermata **Iscrizione riuscita**, è possibile utilizzare questa smart card per accedere a un server aggiunto al dominio, come il VCS con solo la scheda e un pin noto. Tuttavia, non è stato fatto sì, è comunque necessario preparare il VCS per reindirizzare le richieste di autenticazione alla smart card e utilizzare la smart card Common Access Card per rilasciare il certificato della smart card archiviato nella smart card per l'autenticazione.



Registrazione completata

## Configurazione di VCS per Common Access Card

Caricare la CA radice nell'elenco dei certificati CA attendibili nel software VCS selezionando **Manutenzione > Sicurezza > Certificato CA attendibile**.

2. Caricare nel software VCS l'elenco di revocche di certificati firmato dalla CA radice. Passare a **Manutenzione > Sicurezza > Gestione CRL**.

3. Verificare il certificato client con il regex che estrae il nome utente dal certificato da utilizzare per l'autenticazione con il protocollo LDAP o l'utente locale. Il regex verrà confrontato con il **soggetto** del certificato. Può essere il tuo UPN, email e così via. In questa esercitazione è stato utilizzato il messaggio di posta elettronica corrispondente al certificato client per il certificato client.

# Certificate



General Details Certification Path

Show: <All>

| Field                       | Value                            |
|-----------------------------|----------------------------------|
| Signature hash algorithm    | sha512                           |
| Issuer                      | jajanson-2012DC-AD-CA, jaja...   |
| Valid from                  | Tuesday, October 17, 2017 5:...  |
| Valid to                    | Thursday, October 17, 2019 5...  |
| Subject                     | antman@jajanson.local, Scott ... |
| Public key                  | RSA (1024 Bits)                  |
| Public key parameters       | 05 00                            |
| Certificate Template Inform | Template=1 3 6 1 4 1 311 21      |

E = antman@jajanson.local  
CN = Scott Lang  
OU = Heroes  
DC = jajanson  
DC = local

Edit Properties...

Copy to File...

OK

Oggetto del certificato client

4. Passare a **Manutenzione > Sicurezza > Test certificati client**. Selezionare il certificato client da testare, in My lab era antman.pem, caricarlo nell'area di test. Nella sezione **Modello di autenticazione basato su certificato** in **Regex** incollare il regex da verificare. Non modificare il campo **Formato nome utente**.

My Regex: /Subject:. \*emailAddress=(? .\* )@jajanson.local/m

The screenshot shows the Cisco TelePresence Video Communication Server Expressway configuration page. The page title is "Client certificate testing". The "Certificate source" section shows a file named "antman.pem" is currently uploaded. The "Certificate-based authentication pattern" section has a "Regex to match against certificates" field containing the regex: "/Subject:.\*emailAddress=(? .\* )@jajanson.local/m". The "Username format" field is empty. A "Make these settings permanent" button is visible at the bottom of the form.

Prova regex in VCS

**Check certificate**

| Certificate test results         |   |
|----------------------------------|---|
| Valid certificate:               | OK  |
| Source:                          | Uploaded test file (PEM format)                               |
| Filename:                        | antman.pem  |
| Test pattern (as entered above): |   |
| Regex:                           | /Subject: "emailAddress={captureCommonName}";@bjackson.localm |
| Template:                        | #captureCommonName#   |
| Resulting string (username):     | antman  |

← This is our test source client certificate and the regex we are testing. We see the resulting string username is antman which is in our Active Directory to be used with authentication. Antman was issued the smartcard certificate on his CAC card.

**Stored pattern (current VCS configuration):**

|                              |  |
|------------------------------|--|
| Regex:                       | /Subject: "CN={captureCommonName}";@(\w+)\.m |
| Template:                    | #captureCommonName#                          |
| Resulting string (username): | ** Regex Invalid **                          |

**Certificate in plain text:**

```

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2410000001173f460b3102511a4651370000000000017
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=Antman,OU=DOE,OU=CA,OU=BJackson,DC=local
        Validity
            Not Before: Oct 17 21:39:55 2017 GMT
            Not After: Oct 17 21:39:55 2017 GMT
        Subject: emailAddress={captureCommonName}";@bjackson.local
        Subject Public Key Algorithm: rsaEncryption
        Public-Key: (4096 bit)
        Modulus:
            009f46d09f5a12815a1517b46810246b1131d0771
            0c19a1981841374219917516412d0f11391d91c041
            611631d01f81761081c16412416f8016a1f51451
            681f1c10816d1f017a13112710a14110811711d11f1f01
            91132191f21610c10d10f10a115c14211a13610f1
            a01441121718816d18416d1981f21f71f413619c1911
            041101161a17417141f16f16b112810b10b11711a1
            c413217f14813614210419c13c16a1851f016718912b1
    
```


← Here we see the uploaded certificate and the current configuration of the regex on the server. Once you have verified that the regex is working then you can permanently change the Regex. So do not worry that this section shows a failure because this is the current configuration not your test configuration above.

## Risultati test


5. Se il test fornisce i risultati desiderati, è possibile fare clic sul pulsante **Rendi permanenti le modifiche**. In questo modo viene modificato il regex per la **configurazione dell'autenticazione basata su certificati** del server. Per verificare la modifica, passare alla configurazione **Manutenzione > Protezione > Autenticazione basata su certificati**.


6. Abilitare l'autenticazione basata su client passando a **Sistema > Amministratore** e quindi selezionare o fare clic sulla casella a discesa per scegliere **Protezione basata su certificati client = Autenticazione basata su client**. Con questa impostazione, l'utente digita il nome di dominio completo (FQDN) del server VCS nel browser e gli viene richiesto di scegliere l'account client e immettere il PIN assegnato alla scheda di accesso comune. Il certificato viene quindi rilasciato e l'utente riceve la GUI Web del server VCS e deve solo fare clic o selezionare il pulsante **Administrator (Amministratore)**. Poi viene ammesso nel server. Se si seleziona l'opzione **Protezione basata su certificati client = Convalida basata su client**, il processo è lo stesso, con l'eccezione che quando l'utente fa clic sul pulsante **Amministratore**, ha richiesto nuovamente la password amministratore. Di solito, quest'ultimo non è quello che l'organizzazione sta cercando di ottenere con CAC.


### System administration

Ephemeral port range end \* 49999 


#### Services


Serial port / console On 


SSH service On 

Web interface (over HTTPS) On 


#### Session limits


Session time out (minutes) \* 30 

Per-account session limit \* 0 


System session limit \* 0 


#### System protection


Automated protection service On 


Automatic discovery protection On 

#### Web server configuration

Redirect HTTP requests to HTTPS On 

HTTP Strict Transport Security (HSTS) On 

Web administrator port 443 

Client certificate-based security Not required 

Save

Drop down the above box and choose Client-Based Authentication

#### Related tasks

[Upload a CA certificate file for HTTPS](#)

[Test client certificates](#)

Abilita autenticazione basata su client

Aiuto! Sono bloccato!!!

Se si abilita l'autenticazione basata sul client e il VCS rifiuta il certificato per qualsiasi motivo, non sarà più possibile accedere alla GUI Web nel modo tradizionale. Ma, non preoccuparti, c'è un modo per tornare nel tuo sistema. Il documento allegato è disponibile sul sito Web Cisco e fornisce informazioni su come disabilitare l'autenticazione basata su client dall'accesso alla radice.

## Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.