# Risoluzione dei problemi relativi a CAPF Online CA

## Sommario


[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Panoramica dei componenti delle feature](#)
[Autorità di registrazione (RA)](#)
[Iscrizione su trasporto sicuro (EST)](#)
[libEST](#)
[Engine-X (NGINX)](#)
[Servizio di registrazione certificati](#)
[Funzione CAPF (Certification Authority Proxy Function)](#)
[Diagramma flusso messaggi](#)
[Spiegazione flusso messaggi](#)
[/.well-known/est/simpleenroll](#)
[/certsrv](#)
[/certsrv/certrqxt.asp](#)
[/certsrv/certfnsh.asp](#)
[/certsrv/certnew.cer](#)
[Tracce/registri rilevanti per la risoluzione dei problemi](#)
[Log CAPF](#)
[Registri CiscoRA](#)
[Errore NGINX.log](#)
[Registri del server Web CA](#)
[Posizioni file di log](#)
[Log CAPF:](#)
[Cisco ASR:](#)
[Registro errori Nginx:](#)
[Registro di MS IIS:](#)
[Esempio di analisi del log](#)
[Avvio normale dei servizi](#)
[Avvio CES come indicato nel registro NGINX](#)
[Avvio di CES come indicato nel file error.log di NGINX](#)
[Avvio di CES come indicato nei log di IIS](#)
[Avvio di CAPF come nei registri CAPF](#)
[Operazione di installazione LSC telefono](#)
[Log CAPF](#)
[Registri IIS](#)
[Problemi comuni](#)

Certificato CA mancante nella catena emittente del certificato di identità IIS
Server Web che presenta un certificato autofirmato
Mancata corrispondenza con il nome host e il nome comune dell'URL
Problema di risoluzione DNS
Rilascio con date di validità del certificato
Configurazione errata del modello di certificato
Timeout autenticazione CES
Timeout registrazione CES
Avvertenze note
Informazioni correlate

# Introduzione

In questo documento viene descritta la risoluzione dei problemi relativi alla funzionalità di registrazione e rinnovo automatici CAPF (Certificate Authority Proxy Function). Questa funzione è nota anche come CAPF Online CA.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Certificati
- Sicurezza di Cisco Unified Communications Manager (CUCM)

## Componenti usati

Le informazioni fornite in questo documento si basano sulla versione 12.5 di CUCM, in quanto la funzione CAPF Online CA è stata introdotta in CUCM 12.5.

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.

# Panoramica dei componenti delle feature

## Autorità di registrazione (RA)

RA è un'autorità di una rete che verifica le richieste degli utenti per un certificato digitale e comunica all'autorità di certificazione (CA) di rilasciare il certificato. Gli RA fanno parte di un'infrastruttura a chiave pubblica (PKI).

## Iscrizione su trasporto sicuro (EST)

EST è un protocollo definito in RFC (Request for Comment) 7030 per la registrazione dei certificati per i client che utilizzano messaggi CMS (Certificate Management over CMS) su TLS (Transport Layer Security) e HTTP (HyperText Transfer Protocol). Il sistema EST utilizza un modello client/server in cui il client EST invia le richieste di registrazione e il server EST invia le risposte con i risultati.

## libEST

libEST è la libreria per l'implementazione di EST da parte di Cisco. libEST consente il provisioning dei certificati X509 sui dispositivi dell'utente finale e sull'infrastruttura di rete. Questa libreria è implementata da CiscoEST e CiscoRA.

## Engine-X (NGINX)

NGINX è un server Web e un proxy inverso simile ad Apache. NGINX viene utilizzato per la comunicazione HTTP tra CAPF e CES, nonché per la comunicazione tra CES e il servizio di registrazione Web CA. Quando libEST funziona in modalità server, è necessario un server Web per gestire le richieste TCP per conto di libEST.

## Servizio di registrazione certificati

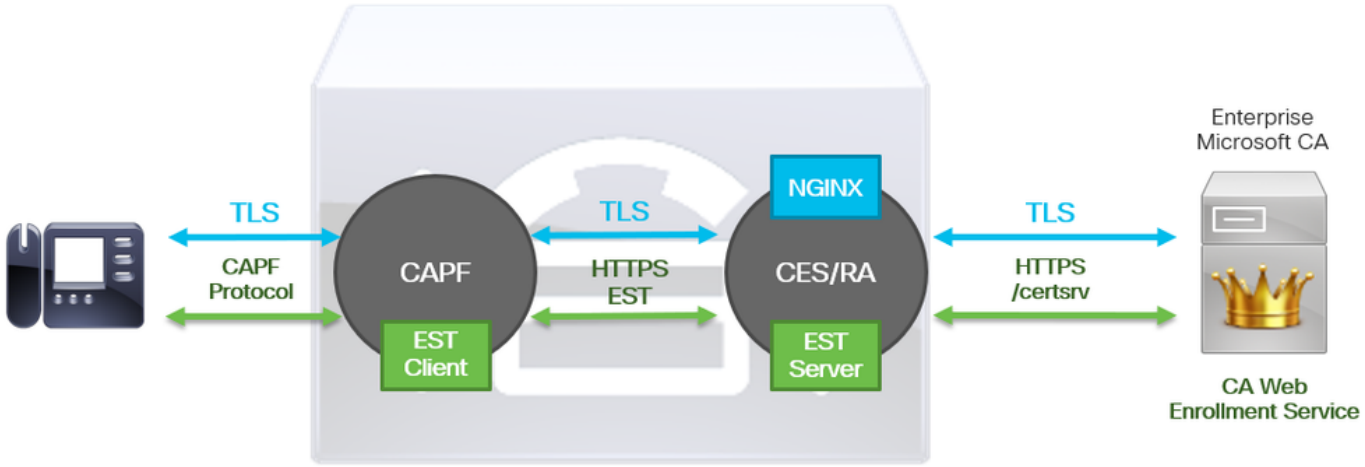
CES è il servizio su CUCM che funge da RA tra il servizio CAPF e la CA. Il termine CES viene anche definito CiscoRA o semplicemente RA. Il CES utilizza NGINX come server Web perché implementa libEST in modalità server per fungere da server di registrazione.

## Funzione CAPF (Certification Authority Proxy Function)

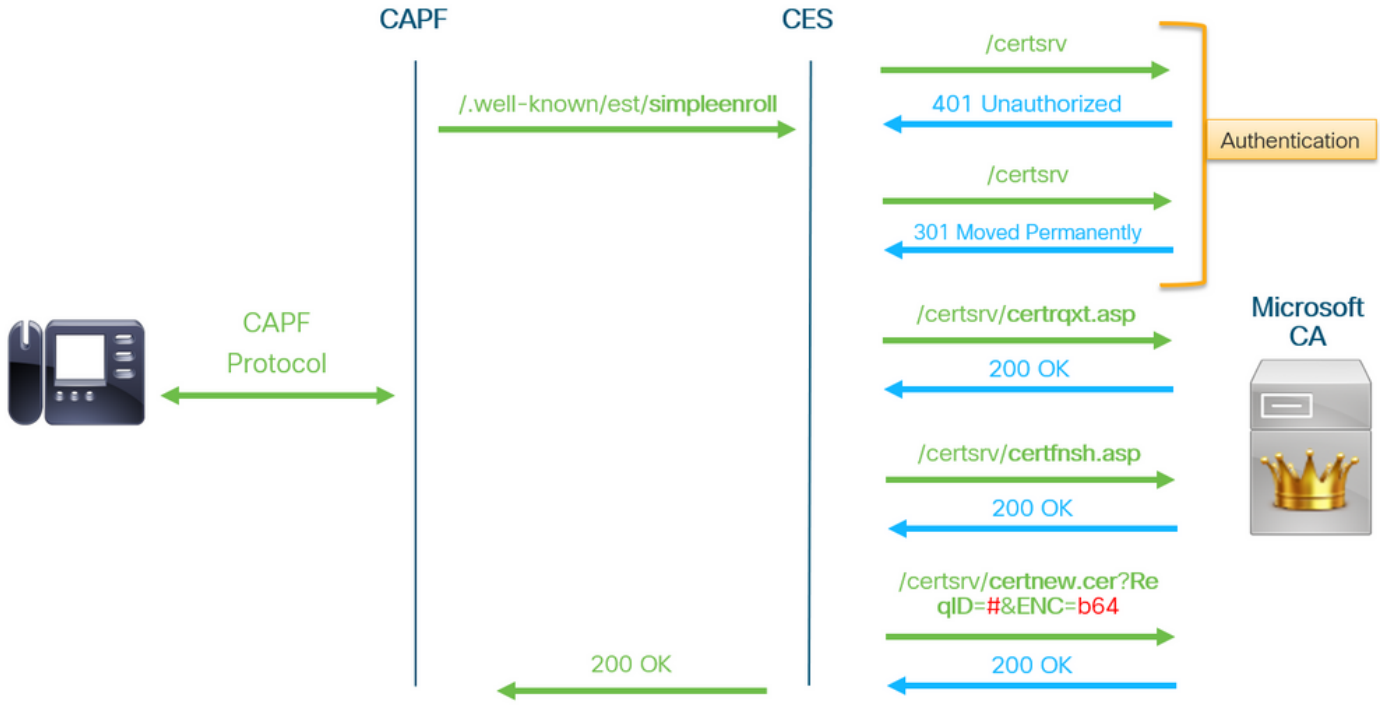
CAPF è un servizio CUCM con cui i telefoni interagiscono quando si eseguono richieste di registrazione di certificati. Il CAPF interagisce con il CES per conto dei telefoni. In questo modello di funzionalità CAPF implementa libEST in modalità client per registrare i certificati dei telefoni tramite CES.

In sintesi, ecco come viene implementato ciascun componente:

1. Il telefono invia una richiesta di certificato a CAPF
2. CAPF implementa CiscoEST (modalità client) per comunicare con CES
3. Il CES implementa CiscoRA (modalità server) per elaborare e rispondere alle richieste del client EST
4. CES/CiscoRA comunica con il servizio di registrazione Web della CA tramite HTTPS




## Diagramma flusso messaggi




## Spiegazione flusso messaggi

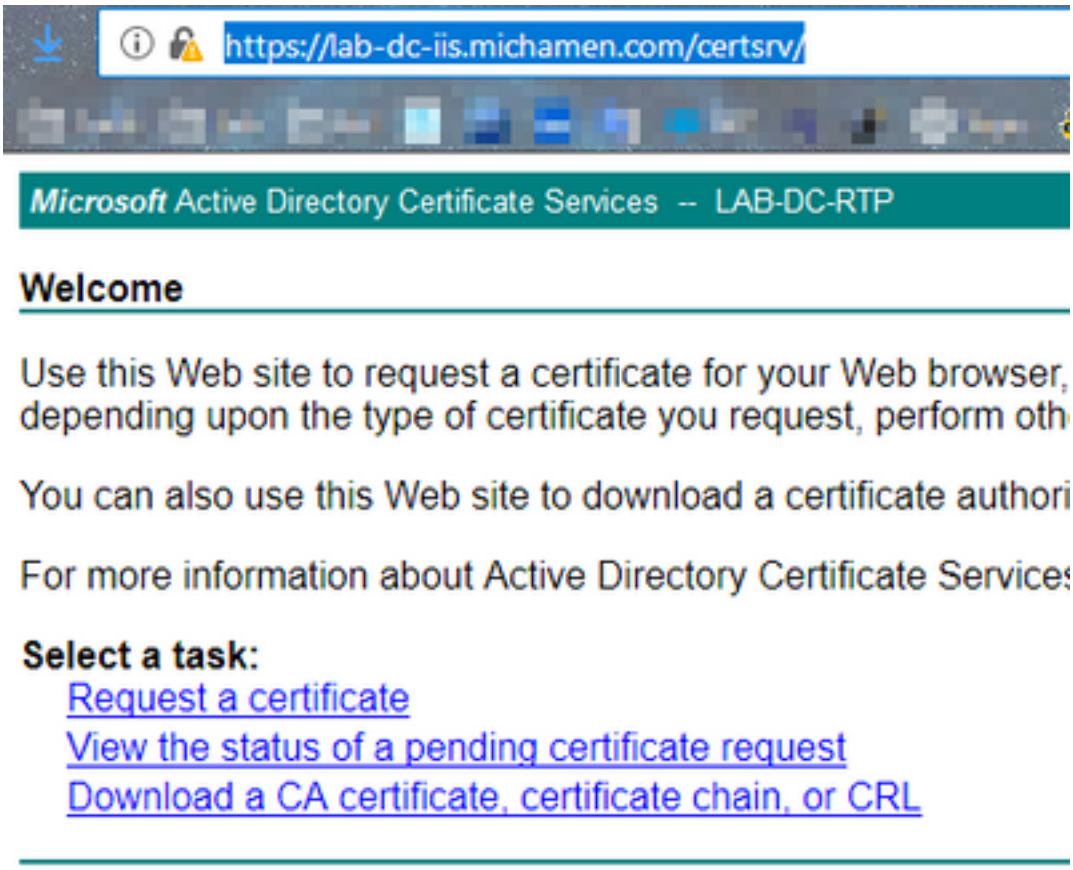
### /.well-known/est/simpleenroll

Il client EST utilizza questo URL per inviare una chiamata API che richiede la registrazione del certificato al server EST. Una volta ricevuta la chiamata API, il server EST avvierà il processo di registrazione dei certificati che include la comunicazione HTTPS con il servizio di registrazione Web della CA. Se il processo di registrazione ha esito positivo e il server EST riceve il nuovo certificato, CAPF procederà a caricare il certificato e a restituirlo al telefono IP.

### /certsrv

L'URL **/certsrv** viene utilizzato dal client EST per autenticare e avviare una sessione con la CA.

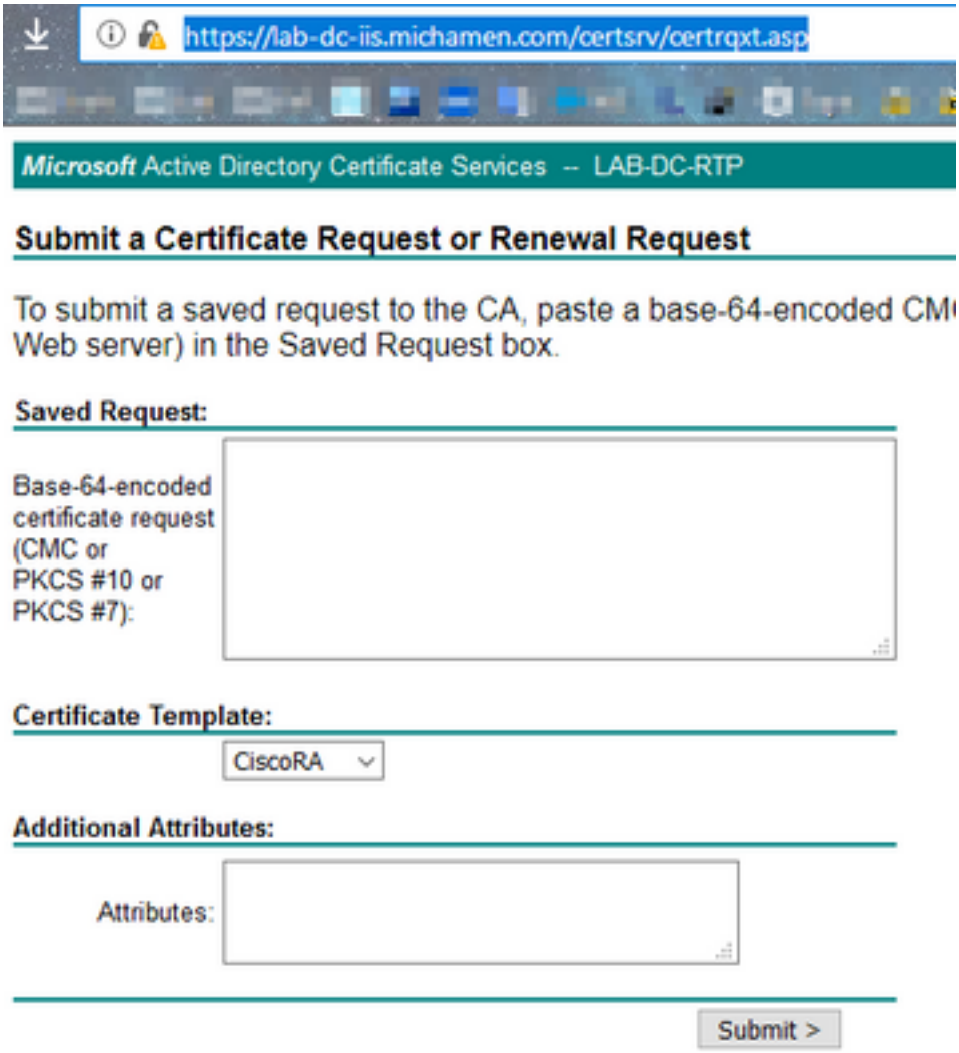
L'immagine seguente è un esempio di URL **/certsrv** da un browser Web. Pagina iniziale dedicata a Servizi certificati.




## /certsrv/certrqxt.asp

L'URL **/certsrv/certrqxt.asp** viene utilizzato per avviare la richiesta di un nuovo certificato. Il client EST utilizza **/certsrv/certrqxt.asp** per inviare il CSR, il nome del modello di certificato e qualsiasi attributo desiderato.

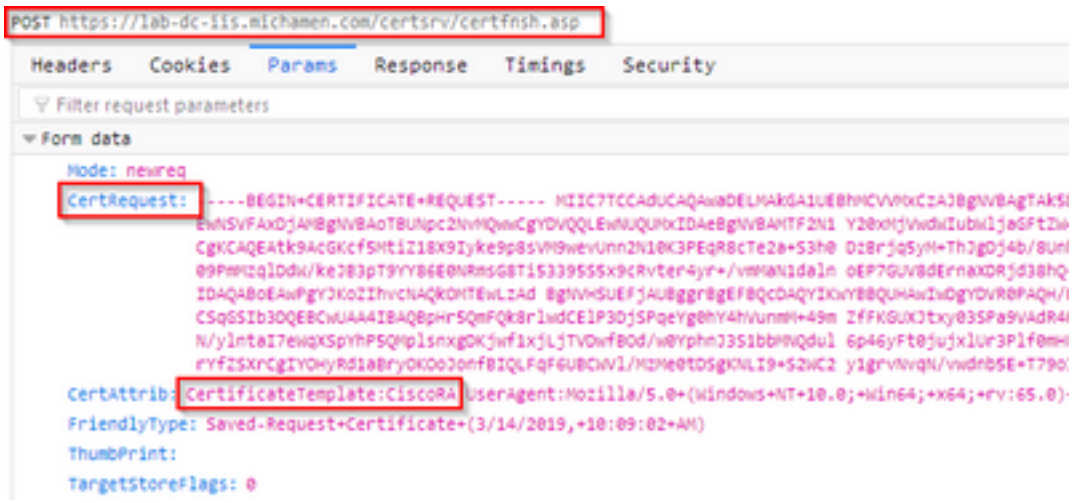
L'immagine seguente è un esempio di **/certsrv/certrqxt.asp** da un browser Web.




## /certsrv/certfnsh.asp

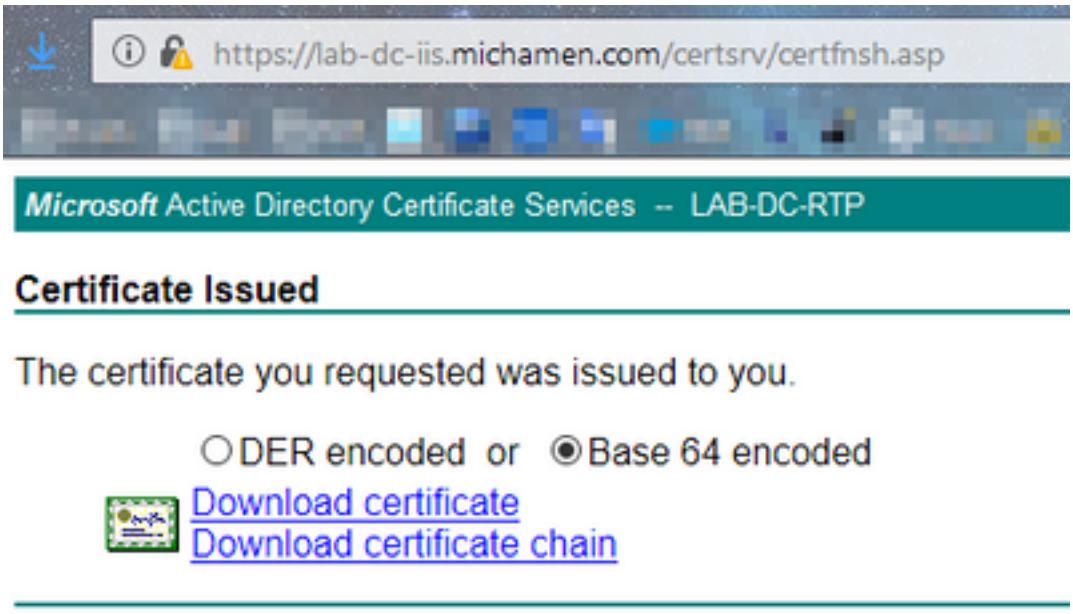
L'URL **/certsrv/certfnsh.asp** viene utilizzato per inviare i dati per la richiesta di certificato; che include il CSR, il nome del modello di certificato ed eventuali attributi desiderati. Per visualizzare l'inoltro, utilizzare gli **Strumenti di sviluppo** del browser per aprire la console del browser prima di inviare i dati tramite la pagina *certrqxt.asp*.

L'immagine seguente è un esempio dei dati visualizzati nella console del browser.

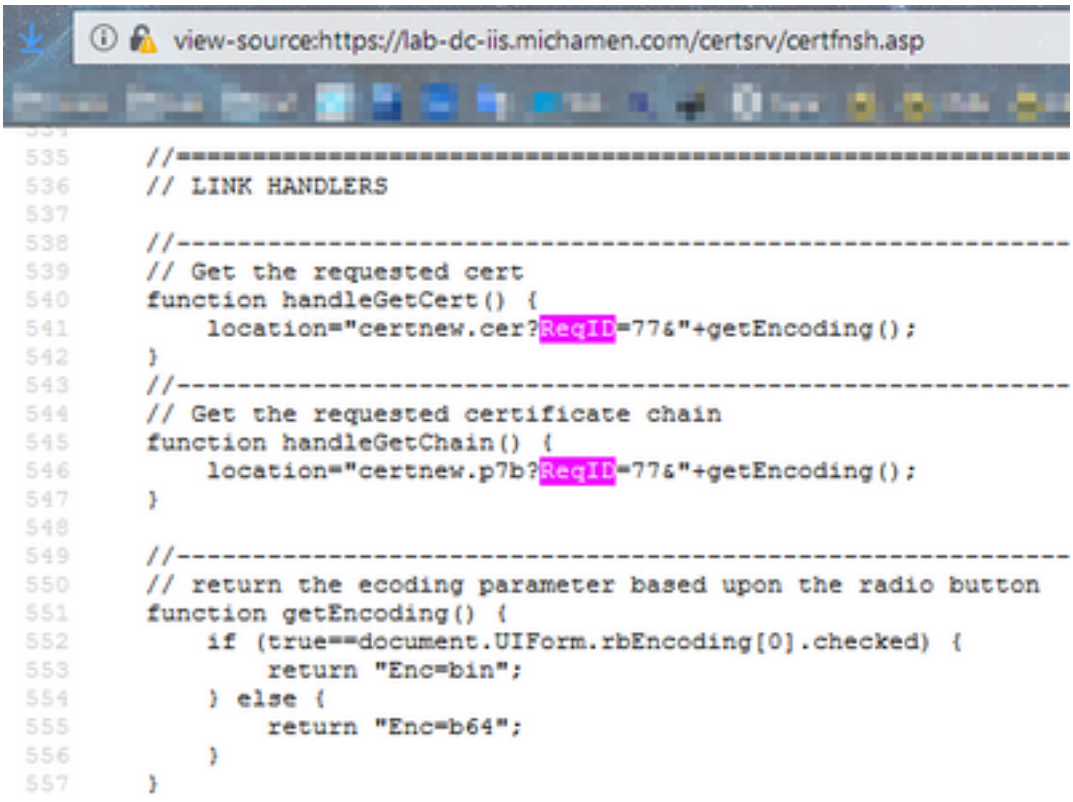



La risposta di invio da **/certsrv/certfnsh.asp** include l'ID richiesta del certificato rilasciato dalla CA.

L'ID della richiesta viene visualizzato in un browser Web quando si controlla il codice sorgente della pagina.



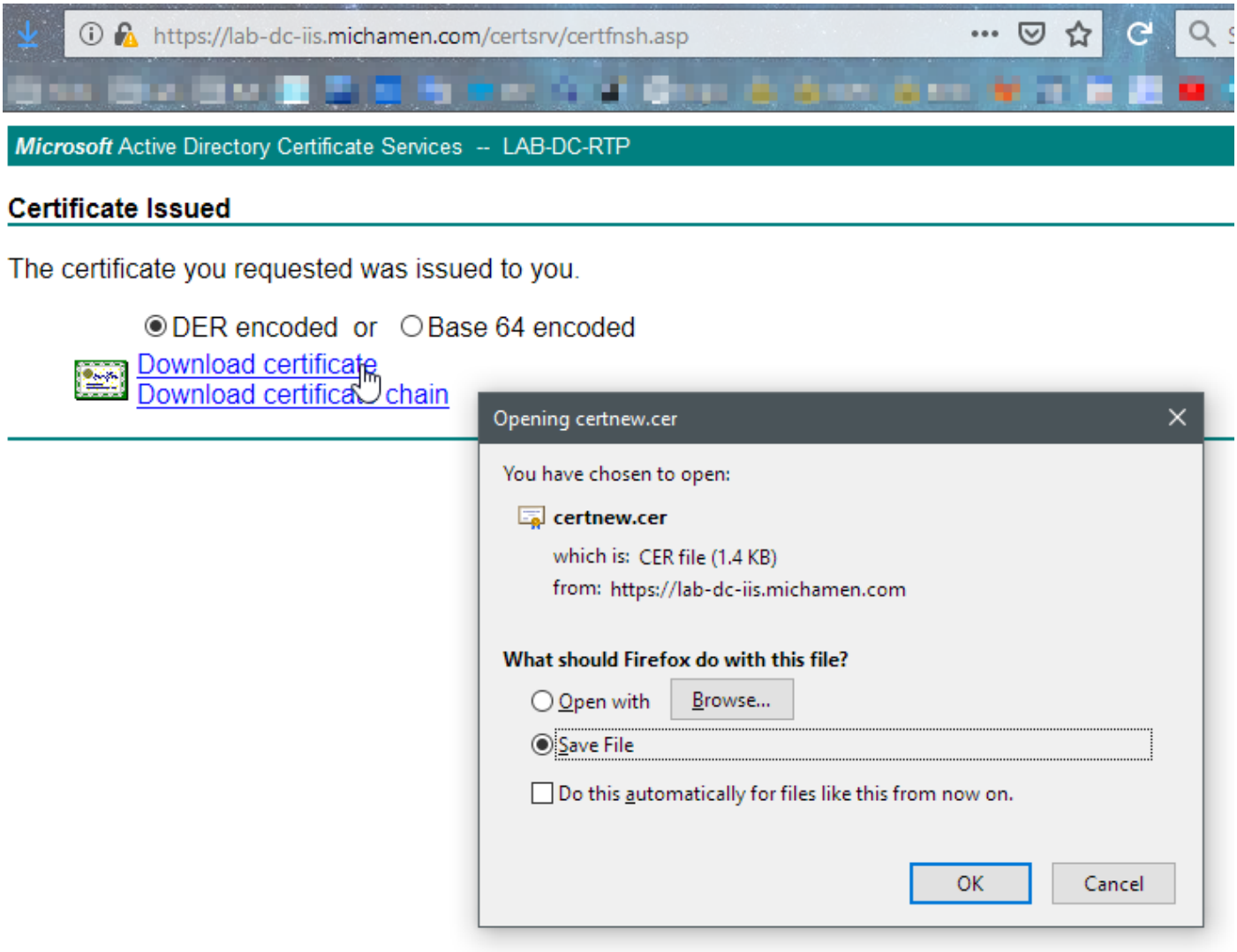

**Suggerimento**: Cerca "ReqID" nell'origine della pagina




## /certsrv/certnew.cer

A questo punto il client EST è a conoscenza dell'ID richiesta per il nuovo certificato. Il client EST utilizza **/certsrv/certnew.cer** per passare l'ID richiesta e la codifica del file come parametri per scaricare il file di certificato con estensione **.cer**.

Equivale a quanto accade nel browser quando si fa clic sul collegamento **Scarica certificato**.




Per visualizzare l'URL e i parametri della richiesta, utilizzare la console del browser.

> **Nota:** Il browser specifica **bin** per il parametro di codifica se è selezionata la codifica DER; tuttavia, la codifica Base64 verrà visualizzata come b64.


# Tracce/registri rilevanti per la risoluzione dei problemi

Questi registri consentono di isolare la maggior parte dei problemi.

## Log CAPF

I registri CAPF includono le interazioni con i telefoni e la registrazione minima delle attività di CiscoEST.

**Nota:** Questi log sono disponibili per la raccolta mediante l'interfaccia della riga di comando (CLI) o lo strumento di monitoraggio in tempo reale (RTMT). A causa di CSCvo28048 CAPF potrebbe non apparire tra l'elenco dei servizi in RTMT.

### Registri CiscoRA

I registri CiscoRA vengono spesso definiti registri CES. I registri CiscoRA contengono l'attività di avvio iniziale del servizio Web di registrazione certificati e visualizzano gli errori che possono verificarsi durante l'autenticazione con l'autorità di certificazione.Se l'autenticazione iniziale con l'autorità di certificazione ha esito positivo, l'attività successiva per le registrazioni telefoniche non viene registrata in questa posizione. Pertanto, i registri CiscoRA rappresentano un buon punto di partenza per la risoluzione dei problemi.

**Nota:** questi log possono essere raccolti solo dalla CLI a partire dalla creazione di questo documento.

### Errore NGINX.log

NGINX error.log è il log più utile per questa funzione, in quanto registra tutte le attività durante l'avvio e tutte le interazioni HTTP tra NGINX e il lato CA; che include i codici di errore restituiti dalla CA e quelli generati da CiscoRA dopo l'elaborazione della richiesta.

**Nota:** Al momento della creazione di questo documento, non è possibile raccogliere questi log neanche dalla CLI. Questi registri possono essere scaricati solo utilizzando un account di supporto remoto (root).

### Registri del server Web CA

I registri del server Web CA sono importanti in quanto visualizzano qualsiasi attività HTTP, inclusi URL di richieste, codici di risposta, durata della risposta e dimensioni della risposta. È possibile utilizzare questi registri per correlare le interazioni tra CiscoRA e la CA.

**Nota:** I registri del server Web CA nel contesto di questo documento sono i registri di MS IIS. Se in futuro saranno supportate altre CA Web, è possibile che dispongano di file di log diversi che fungono da log del server Web della CA

## Posizioni file di log

### Log CAPF:

- Dalla radice: /var/log/active/cm/trace/capf/sdi/capf<*numero*>.txt
- Dalla CLI: file get activelog cm/trace/capf/sdi/capf*

**Nota:** Impostare il livello di traccia CAPF su "Dettagliato" e riavviare il servizio CAPF prima di eseguire il test.

## Cisco ASR:

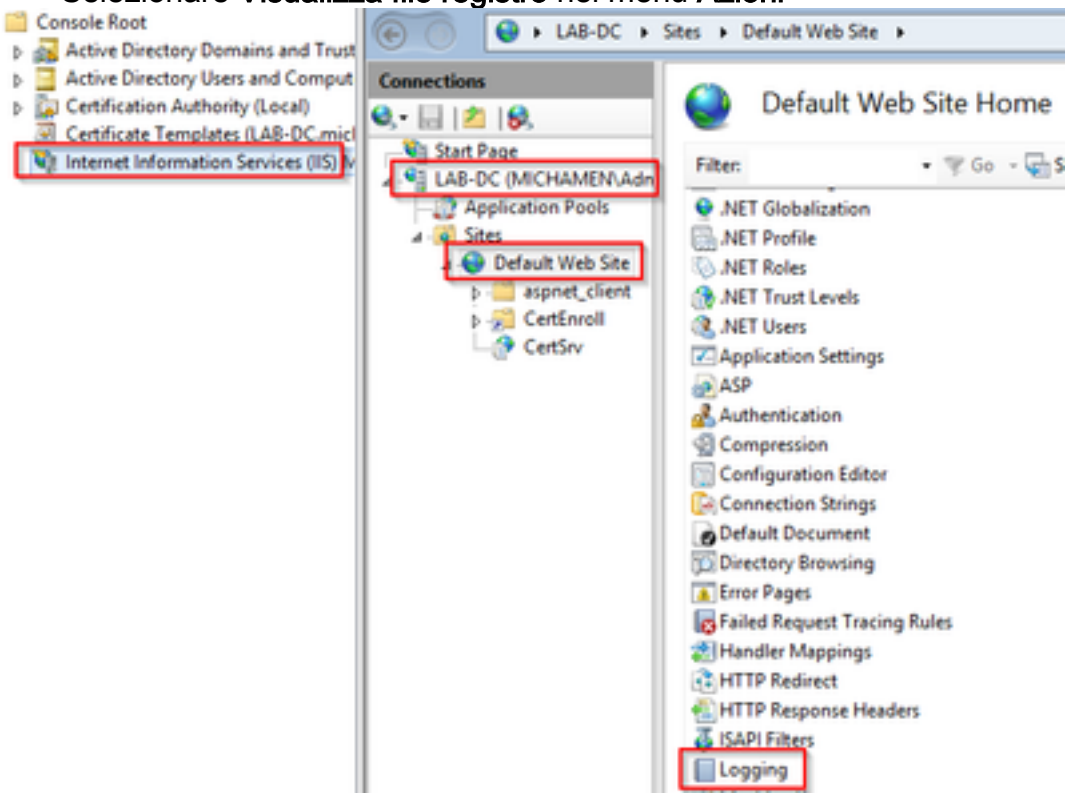
- Dalla radice: /var/log/active/cm/trace/capf/sdi/ginx<*numero*>.txt
- Dalla CLI: file get activelog cm/trace/capf/sdi/ginx*

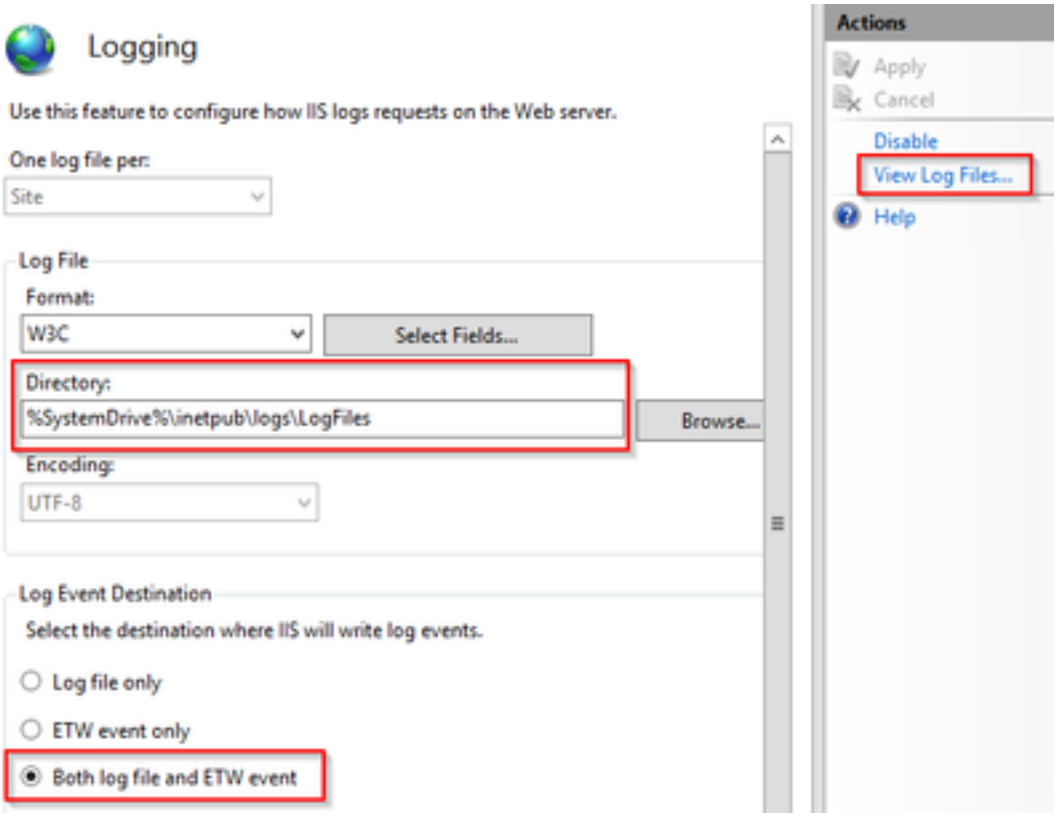
## Registro errori Nginx:

- Dalla radice: /usr/local/thirdparty/nginx/install/logs/error.log
- Non disponibile dalla CLI

## Registro di MS IIS:

- Aprire MMC
- Selezionare lo snap-in **Internet Information Services (IIS)**
- Fare clic sul nome del server
- Fare clic su **Sito Web predefinito**
- Fare doppio clic su **Log** per visualizzare le opzioni di log
- Selezionare **Visualizza file registro** nel menu **Azioni**






# Esempio di analisi del log

## Avvio normale dei servizi

### Avvio CES come indicato nel registro NGINX

Da questo registro vengono raccolte poche informazioni. La catena di certificati completa caricata nell'archivio di certificati attendibili è visualizzata qui e una è per il contenitore Web mentre l'altra è per EST:

```
nginx: [warn] CA Chain requested but this value has not yet been set
nginx: [warn] CA Cert response requested but this value has not yet been set
nginx: [warn] ossl_init_cert_store: Adding cert to store (/O=Cisco/CN=ACT2 SUDI CA)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/C=US/O=cisco/OU=tac/CN=CAPF-
eb606ac0/ST=nc/L=rtp)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/C=US/O=cisco/OU=tac/CN=CAPF-
eb606ac0/ST=nc/L=rtp)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/O=Cisco Systems/CN=Cisco
Manufacturing CA)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/O=Cisco/CN=Cisco Manufacturing CA
SHA2)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/O=Cisco Systems/CN=Cisco Root CA
2048)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/O=Cisco/CN=Cisco Root CA M2)
nginx: [warn] ossl_init_cert_store: Adding cert to store (/DC=com/DC=michamen/CN=lab-
ca.michamen.com)
***EST [INFO][est_log_version:216]--> libest 2.2.0 (API level 4)
***EST [INFO][est_log_version:220]--> Compiled against CiscoSSL 1.0.2n.6.2.194-fips
***EST [INFO][est_log_version:221]--> Linking to CiscoSSL 1.0.2n.6.2.194-fips
***EST [INFO][ossl_init_cert_store_from_raw:182]--> Adding cert to store (/O=Cisco/CN=ACT2 SUDI
CA)
***EST [INFO][ossl_init_cert_store_from_raw:182]--> Adding cert to store
```

```
(/C=US/O=cisco/OU=tac/CN=CAPF-eb606ac0/ST=nc/L=rtp)
***EST [INFO][ossl_init_cert_store_from_raw:182]--> Adding cert to store
(/C=US/O=cisco/OU=tac/CN=CAPF-eb606ac0/ST=nc/L=rtp)
***EST [INFO][ossl_init_cert_store_from_raw:182]--> Adding cert to store (/O=Cisco
Systems/CN=Cisco Manufacturing CA)
***EST [INFO][ossl_init_cert_store_from_raw:182]--> Adding cert to store (/O=Cisco/CN=Cisco
Manufacturing CA SHA2)
***EST [INFO][ossl_init_cert_store_from_raw:182]--> Adding cert to store (/O=Cisco
Systems/CN=Cisco Root CA 2048)
***EST [INFO][ossl_init_cert_store_from_raw:182]--> Adding cert to store (/O=Cisco/CN=Cisco Root
CA M2)
***EST [INFO][ossl_init_cert_store_from_raw:182]--> Adding cert to store
(/DC=com/DC=michamen/CN=lab-ca.michamen.com)
nginx: [warn] pop_enabled off in nginx.conf. Disabling EST Proof of Possession
***EST [INFO][set_ssl_option:1378]--> Using non-default ECDHE curve (nid=415)
***EST [INFO][set_ssl_option:1432]--> TLS SRP not enabled
EnrollmentService.sh : nginx server PID value =  31070
```

## Avvio CES come mostrato nel file error.log NGINX

L'accesso con la configurazione e le credenziali del modello di certificato viene osservato nel frammento di codice:

```
2019/03/05 12:31:21 [info] 31067#0: login_to_certsrv_ca: Secure connection to MS CertServ
completed successfully using the following URL
https://lab-dc.michamen.com:443/certsrv
```

Il recupero della catena di certificati CA viene osservato nel frammento di codice:

```
2019/03/05 12:31:21 [info] 31067#0: retrieve_cacerts: Secure connection to MS CertServ completed
successfully using the following URL
https://lab-dc.michamen.com:443/certsrv/certnew.p7b?ReqID=CACert&Renewal=0&Enc=bin
[…]
2019/03/05 12:31:21 [info] 31067#0: ra_certsrv_ca_plugin_postconf: CA Cert chain retrieved from
CA, will be passed to EST
```

Quando la richiesta ha esito positivo, viene ottenuto il file certnew.p7b. Lo stesso URL con le credenziali del modello può essere utilizzato per ottenere il file certnew.p7b da un browser Web.

## Avvio CES come visualizzato nei registri IIS

Gli stessi eventi di avvio CES rilevati nel file error.log di NGINX sono osservati anche nei log di IIS; tuttavia, i log di IIS includono altre 2 richieste HTTP GET perché la prima richiesta verrà contestata dal server Web tramite una risposta 401; e una volta autenticata, una richiesta verrà reindirizzata utilizzando una risposta 301:

```
2019-03-05 17:31:15 14.48.31.152 GET /certsrv - 443 - 14.48.31.128 CiscoRA+1.0 - 401 1
2148074254 0
2019-03-05 17:31:15 14.48.31.152 GET /certsrv - 443 MICHAMEN\ciscora 14.48.31.128 CiscoRA+1.0 -
301 0 0 16
2019-03-05 17:31:15 14.48.31.152 GET /certsrv/certnew.p7b ReqID=CACert&Renewal=0&Enc=bin 443
MICHAMEN\ciscora 14.48.31.128 CiscoRA+1.0 - 200 0 0 2
```

### Avvio di CAPF come indicato nei registri CAPF

La maggior parte di ciò che si verifica nei log CAPF per l'avvio del CES ha lo stesso aspetto di quello che si verifica negli altri log; ma il servizio CAPF rileva il metodo e la configurazione per la CA online:

```
12:31:03.354 |   CServiceParameters::Init() Certificate Generation Method=OnlineCA:4
12:31:03.358 |   CServiceParameters::Init() TAM password already exists, no need to create.
12:31:03.358 |-->CServiceParameters::OnlineCAInit()
12:31:03.388 |   CServiceParameters::OnlineCAInit() Online CA hostname is lab-dc.michamen.com
12:31:03.389 |   CServiceParameters::OnlineCAInit() Online CA Port : 443
12:31:03.390 |   CServiceParameters::OnlineCAInit() Online CA Template is  CiscoRA
12:31:03.546 |   CServiceParameters::OnlineCAInit() nginx.conf Updated and Credential.txt file
is created
12:31:03.546 |   CServiceParameters::OnlineCAInit() Reading CAPF Service Parameters done
12:31:03.546 |<--CServiceParameters::OnlineCAInit()
12:31:03.547 |   CServiceParameters::Init() OnlineCA Initialized
12:32:09.172 |   CServiceParameters::Init() Cisco RA Service Start Initiated. Please check NGINX
logs for further details
```

La successiva osservazione importante dai log è quando il servizio CAPF inizializza il client EST.

```
12:32:09.231 |   debug CA Type is Online CA, setting up EST Connection
12:32:09.231 |<--debug
12:32:09.231 |-->debug
12:32:09.231 |   debug Inside setUpESTClient
[…]
12:32:09.231 |-->debug
12:32:09.231 |   debug cacert read success. cacert length : 1367
12:32:09.231 |<--debug
12:32:09.232 |-->debug
12:32:09.232 |   debug EST context ectx initialized
12:32:09.232 |<--debug
12:32:09.661 |-->debug
12:32:09.661 |   debug CA Credentials retrieved
12:32:09.661 |<--debug
12:32:09.661 |-->debug
12:32:09.661 |   debug est_client_set_auth() Successful!!
12:32:09.661 |<--debug
12:32:09.661 |-->debug
12:32:09.661 |   debug EST set server details success!!
```

## Operazione di installazione LSC telefono

### Log CAPF

Si consiglia di raccogliere tutti i registri necessari e avviare l'analisi con una revisione dei registri CAPF. Questo ci permette di conoscere il riferimento orario per un telefono specifico.

La parte iniziale della segnalazione è simile a quella di altri metodi CAPF, con la differenza che il client EST in esecuzione nel servizio CAPF eseguirà l'iscrizione con CES verso la fine della finestra di dialogo (dopo che il CSR è stato fornito dal telefono).

```
14:05:04.628 |-->debug
14:05:04.628 |   debug 2:SEP74A02FC0A675:CA Mode is OnlineCA, Initiating Automatic Certificate
Enrollment
14:05:04.628 |<--debug
14:05:04.628 |-->debug
14:05:04.628 |   debug 2:SEP74A02FC0A675:Calling enrollCertUsingEST()
csr_file=/tmp/capf/csr/SEP74A02FC0A675.csr
14:05:04.628 |<--debug
14:05:04.628 |-->debug
14:05:04.628 |   debug 2:SEP74A02FC0A675:Inside  X509_REQ *read_csr()
14:05:04.628 |<--debug
14:05:04.628 |-->debug
14:05:04.628 |   debug 2:SEP74A02FC0A675:Completed action in X509_REQ *read_csr()
14:05:04.628 |<--debug
```

Una volta che il CES ha recuperato il certificato firmato del telefono, il certificato viene convertito in formato DER prima di essere fornito al telefono.

```
14:05:05.236 |-->debug
14:05:05.236 |   debug 2:SEP74A02FC0A675:Enrollment rv = 0 (EST_ERR_NONE) with pkcs7 length =
1963
14:05:05.236 |<--debug
14:05:05.236 |-->debug
14:05:05.236 |   debug 2:SEP74A02FC0A675:Signed Cert written to /tmp/capf/cert/ location...
14:05:05.236 |<--debug
14:05:05.236 |-->debug
14:05:05.236 |   debug 2:SEP74A02FC0A675:Inside write_binary_file()
14:05:05.236 |<--debug
14:05:05.236 |-->debug
14:05:05.236 |   debug 2:SEP74A02FC0A675:Completed action in write_binary_file()
14:05:05.236 |<--debug
14:05:05.236 |-->debug
14:05:05.236 |   debug 2:SEP74A02FC0A675:Converting PKCS7 file to PEM format and PEM to DER
14:05:05.236 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug 2:SEP74A02FC0A675:Return value from enrollCertUsingEST() : 0
14:05:05.289 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug 2:SEP74A02FC0A675:Online Cert Signing successful
14:05:05.289 |<--debug
14:05:05.289 |-->findAndPost
14:05:05.289 |   findAndPost Device found in the cache map SEP74A02FC0A675
```

Il servizio CAPF riprende il controllo e carica il CSR dal punto in cui è stato scritto nel frammento precedente (/tmp/capf/cert/). Il servizio CAPF fornisce quindi al telefono il LSC firmato. Allo stesso tempo il CSR del telefono viene eliminato.

```
14:05:05.289 |<--findAndPost
14:05:05.289 |-->debug
14:05:05.289 |   debug addded 6 to readset
14:05:05.289 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug Recd event
14:05:05.289 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug 2:SEP74A02FC0A675:CA CERT RES certificate ready .
14:05:05.289 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug 2:SEP74A02FC0A675:CAPF CORE: Rcvd Event: CAPF_EV_CA_CERT_REP in State:
```

```
CAPF_STATE_AWAIT_CA_CERT_RESP
14:05:05.289 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug 2:SEP74A02FC0A675:CAPF got device certificate
14:05:05.289 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug loadFile('/tmp/capf/cert/SEP74A02FC0A675.der')
14:05:05.289 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug loadFile() successfully loaded file: '/tmp/capf/cert/SEP74A02FC0A675.der'
14:05:05.289 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug 2:SEP74A02FC0A675:Read certificate for device
14:05:05.289 |<--debug
14:05:05.289 |-->debug
14:05:05.289 |   debug LSC is verified. removing CSR at /tmp/capf/csr/SEP74A02FC0A675.csr
14:05:05.289 |<--debug
14:05:05.290 |-->debug
14:05:05.290 |   debug 2:SEP74A02FC0A675:Sending STORE_CERT_REQ msg

14:05:05.419 |<--Select(SEP74A02FC0A675)
14:05:05.419 |-->SetOperationStatus(Success:CAPF_OP_SUCCESS):0
14:05:05.419 |   SetOperationStatus(Success:CAPF_OP_SUCCESS):0 Operation status Value is '0'

14:05:05.419 |-->CAPFDevice::MapCapf_OpStatusToDBLTypeCertificateStatus(OPERATION_UPGRADE, Suc
14:05:05.419 |   CAPFDevice::MapCapf_OpStatusToDBLTypeCertificateStatus(OPERATION_UPGRADE, Suc
=>DbStatus=CERT_STATUS_UPGRADE_SUCCESS
14:05:05.419 |<--CAPFDevice::MapCapf_OpStatusToDBLTypeCertificateStatus(OPERATION_UPGRADE, Suc
14:05:05.419 |   SetOperationStatus(Success:CAPF_OP_SUCCESS):0 Operation status is set to 1
14:05:05.419 |   SetOperationStatus(Success:CAPF_OP_SUCCESS):0 Operation status is set to
Success:CAPF_OP_SUCCESS
14:05:05.419 |   SetOperationStatus(Success:CAPF_OP_SUCCESS):0 sql query - (UPDATE Device SET
tkCertificateOperation=1, tkcertificatestatus='3' WHERE
my_lower(name)=my_lower('SEP74A02FC0A675'))
14:05:05.503 |<--SetOperationStatus(Success:CAPF_OP_SUCCESS):0
14:05:05.503 |-->debug
14:05:05.503 |   debug 2:SEP74A02FC0A675:In capf_ui_set_ph_public_key()
14:05:05.503 |<--debug
14:05:05.503 |-->debug
14:05:05.503 |   debug 2:SEP74A02FC0A675:pubKey: 0,
[…]
14:05:05.503 |<--debug
14:05:05.503 |-->debug
14:05:05.503 |   debug 2:SEP74A02FC0A675:pubKey length: 270
14:05:05.503 |<--debug
14:05:05.503 |-->Select(SEP74A02FC0A675)
14:05:05.511 |   Select(SEP74A02FC0A675) device exists
14:05:05.511 |   Select(SEP74A02FC0A675) BEFORE DB query Authentication Mode=AUTH_BY_STR:1
14:05:05.511 |   Select(SEP74A02FC0A675) KeySize=KEY_SIZE_2048:3
14:05:05.511 |   Select(SEP74A02FC0A675) ECKeySize=INVALID:0
14:05:05.511 |   Select(SEP74A02FC0A675) KeyOrder=KEYORDER_RSA_ONLY:1
14:05:05.511 |   Select(SEP74A02FC0A675) Operation=OPERATION_NONE:1
14:05:05.511 |   Select(SEP74A02FC0A675) Operation Status =CERT_STATUS_UPGRADE_SUCCESS:3
14:05:05.511 |   Select(SEP74A02FC0A675) Authentication Mode=AUTH_BY_NULL_STR:2
14:05:05.511 |   Select(SEP74A02FC0A675) Operation Should Finish By=2019:01:20:12:00
[…]
14:05:05.971 |-->debug
14:05:05.971 |   debug     MsgType              : CAPF_MSG_END_SESSION
```

## Registri IIS

Lo snippet di codice seguente visualizza gli eventi nei registri di IIS relativi alla procedura di

installazione LSC di un telefono, come spiegato in precedenza.

```
2019-01-16 14:05:02 14.48.31.152 GET /certsrv - 443 - 14.48.31.125 CiscoRA+1.0 - 401 1
2148074254 0
2019-01-16 14:05:02 14.48.31.152 GET /certsrv - 443 MICHAMEN\ciscora 14.48.31.125 CiscoRA+1.0 -
301 0 0 0
2019-01-16 14:05:02 14.48.31.152 GET /certsrv/certrqxt.asp - 443 MICHAMEN\ciscora 14.48.31.125
CiscoRA+1.0 - 200 0 0 220
2019-01-16 14:05:02 14.48.31.152 GET /certsrv - 443 - 14.48.31.125 CiscoRA+1.0 - 401 1
2148074254 0
2019-01-16 14:05:02 14.48.31.152 GET /certsrv - 443 MICHAMEN\ciscora 14.48.31.125 CiscoRA+1.0 -
301 0 0 0
2019-01-16 14:05:02 14.48.31.152 POST /certsrv/certfnsh.asp - 443 MICHAMEN\ciscora 14.48.31.125
CiscoRA+1.0 https://lab-dc.michamen.com:443/certsrv/certrqxt.asp 200 0 0 15
2019-01-16 14:05:02 14.48.31.152 GET /certsrv/certnew.cer ReqID=10&ENC=b64 443 MICHAMEN\ciscora
14.48.31.125 CiscoRA+1.0 - 200 0 0 0
```

# Problemi comuni

Quando si verifica un errore sul lato CES, nei log CAPF dovrebbe essere visualizzato un output simile al frammento di codice riportato di seguito. Accertarsi di controllare altri registri per continuare a ridurre il problema.

```
12:37:54.741 |-->debug
12:37:54.741 |   debug 2:SEP001F6C81118B:CA Mode is OnlineCA, Initiating Automatic Certificate
Enrollment
12:37:54.741 |<--debug
12:37:54.741 |-->debug
12:37:54.741 |   debug 2:SEP001F6C81118B:Calling enrollCertUsingEST()
csr_file=/tmp/capf/csr/SEP001F6C81118B.csr
12:37:54.741 |<--debug
12:37:54.741 |-->debug
12:37:54.742 |   debug 2:SEP001F6C81118B:Inside  X509_REQ *read_csr()
12:37:54.742 |<--debug
12:37:54.742 |-->debug
12:37:54.742 |   debug 2:SEP001F6C81118B:Completed action in X509_REQ *read_csr()
12:37:54.742 |<--debug
12:38:04.779 |-->debug
12:38:04.779 |   debug 2:SEP001F6C81118B:Enrollment rv = 35 (EST_ERR_SSL_READ) with pkcs7 length
= 0
12:38:04.779 |<--debug
12:38:04.779 |-->debug
12:38:04.779 |   debug 2:SEP001F6C81118B:est_client_enroll_csr() Failed! Could not obtain new
certificate. Aborting.
12:38:04.779 |<--debug
12:38:04.779 |-->debug
12:38:04.779 |   debug 2:SEP001F6C81118B:Return value from enrollCertUsingEST() : 35
12:38:04.779 |<--debug
12:38:04.779 |-->debug
12:38:04.779 |   debug 2:SEP001F6C81118B:Online Cert Signing Failed
12:38:04.779 |<--debug
12:38:04.779 |-->debug
12:38:04.779 |   debug addded 10 to readset
12:38:04.779 |<--debug
```

## Certificato CA mancante nella catena emittente del certificato di identità IIS

Quando un certificato radice o intermedio che si trova nella catena di certificati non è considerato attendibile dal servizio di certificazione esterna, nei registri Inginx viene visualizzato il messaggio di errore "Unable to retrieve CA Cert chain from CA" (Impossibile recuperare la catena di certificati CA da CA).

```
nginx: [warn] login_to_certsrv_ca: Curl call for MS CA login failed with return code 60 (SSL
certificate problem: unable to get local issuer certificate)

nginx: [warn] login_to_certsrv_ca: URL used: https://lab-dc.michamen.com:443/certsrv

nginx: [error] retrieve_cacerts: Unable to execute login to certsrv with curl
nginx: [warn] ra_certsrv_ca_plugin_postconf: Unable to retrieve CA Cert chain from CA
```

## Server Web che presenta un certificato autofirmato

L'utilizzo di un certificato autofirmato in IIS non è supportato e funzionerà anche se caricato come CAPF-trust in CUCM. Lo snippet di codice seguente proviene dai log di Index e visualizza ciò che viene osservato quando IIS utilizza un certificato autofirmato.

```
nginx: [warn] login_to_certsrv_ca: Curl call for MS CA login failed with return code 60 (SSL
certificate problem: unable to get local issuer certificate)

nginx: [warn] login_to_certsrv_ca: URL used: https://lab-dc.michamen.com:443/certsrv

nginx: [error] retrieve_cacerts: Unable to execute login to certsrv with curl
nginx: [warn] ra_certsrv_ca_plugin_postconf: Unable to retrieve CA Cert chain from CA
```

## Mancata corrispondenza con il nome host e il nome comune dell'URL

Il nome comune (lab-dc) del certificato IIS non corrisponde all'FQDN all'interno dell'URL del servizio di registrazione Web della CA. Affinché la convalida del certificato riesca, il nome di dominio completo (FQDN) all'interno dell'URL deve corrispondere al nome comune nel certificato utilizzato dalla CA.

```
nginx: [warn] login_to_certsrv_ca: Curl call for MS CA login failed with return code 51 (SSL:
certificate subject name 'lab-dc' does not match target host name 'lab-dc.michamen.com')

nginx: [warn] login_to_certsrv_ca: URL used: https://lab-dc.michamen.com:443/certsrv

nginx: [error] retrieve_cacerts: Unable to execute login to certsrv with curl
```

## Problema di risoluzione DNS

CiscoRA non è in grado di risolvere il nome host della CA online configurata nei parametri del servizio.

```
nginx: [warn] CA Chain requested but this value has not yet been set
nginx: [warn] CA Cert response requested but this value has not yet been set
nginx: [warn] login_to_certsrv_ca: Curl call for MS CA login failed with return code 6 (Could
not resolve: lab-dcc.michamen.com (Domain name not found))
```

```
nginx: [warn] login_to_certsrv_ca: URL used: https://lab-dcc.michamen.com:443/certsrv

nginx: [error] retrieve_cacerts: Unable to execute login to certsrv with curl
nginx: [warn] ra_certsrv_ca_plugin_postconf: Unable to retrieve CA Cert chain from CA
```

## Rilascio con date di validità del certificato

Quando il protocollo NTP (Network Time Protocol) non funziona correttamente si verificano problemi con le date di validità dei certificati. Questo controllo viene eseguito dal CES all'avvio e viene osservato nei registri NGINX.

```
nginx: [warn] login_to_certsrv_ca: Curl call for MS CA login failed with return code 60 (SSL
certificate problem: certificate is not yet valid)

nginx: [warn] login_to_certsrv_ca: URL used: https://lab-dc-iis.michamen.com:443/certsrv

nginx: [error] retrieve_cacerts: Unable to execute login to certsrv with curl
nginx: [warn] ra_certsrv_ca_plugin_postconf: Unable to retrieve CA Cert chain from CA
```

## Configurazione errata del modello di certificato

Un errore causato da un errore nel nome nei parametri del servizio. Poiché nei registri CAPF e NGINX non vengono registrati errori, è necessario controllare il file error.log di NGINX.

```
***EST [INFO][est_enroll_auth:356]--> TLS: no peer certificate
2019/02/27 16:53:28 [warn] 3187#0: *2 ossl_init_cert_store: Adding cert to store
(/DC=com/DC=michamen/CN=LAB-DC-RTP) while SSL EST handshaking, client: 14.48.31.128, server:
0.0.0.0:8084
2019/02/27 16:53:28 [info] 3187#0: *2 ra_certsrv_auth_curl_data_cb: Rcvd data len: 163
 while SSL EST handshaking, client: 14.48.31.128, server: 0.0.0.0:8084
2019/02/27 16:53:28 [info] 3187#0: *2 login_to_certsrv_ca: Secure connection to MS CertServ
completed successfully using the following URL
https://lab-dc-iis.michamen.com:443/certsrv
 while SSL EST handshaking, client: 14.48.31.128, server: 0.0.0.0:8084
2019/02/27 16:53:28 [info] 3187#0: *2 ra_certsrv_auth_curl_data_cb: Rcvd data len: 11771
 while SSL EST handshaking, client: 14.48.31.128, server: 0.0.0.0:8084
2019/02/27 16:53:28 [info] 3187#0: *2 navigate_to_certsrv_page: Secure connection to MS CertServ
completed successfully using the following URL
https://lab-dc-iis.michamen.com:443/certsrv/certrqxt.asp
 while SSL EST handshaking, client: 14.48.31.128, server: 0.0.0.0:8084
***EST [WARNING][est_enroll_auth:394]--> HTTP authentication failed. Auth type=1
***EST [WARNING][est_http_request:1435]--> Enrollment failed with rc=22 (EST_ERR_AUTH_FAIL)

***EST [INFO][mg_send_http_error:389]--> [Error 401: Unauthorized
The server was unable to authorize the request.
]
***EST [ERROR][est_mg_handler:1234]--> EST error response code: 22 (EST_ERR_AUTH_FAIL)

***EST [WARNING][handle_request:1267]--> Incoming request failed rv=22 (EST_ERR_AUTH_FAIL)
***EST [INFO][log_access:1298]--> 14.48.31.128 [27/Feb/2019:16:53:28 -0500] "POST /.well-
known/est/simpleenroll HTTP/1.1" 401 0
***EST [INFO][log_header:1276]-->  -
***EST [INFO][log_header:1278]-->  "Cisco EST client 1.0"
***EST [WARNING][est_server_handle_request:1716]--> SSL_shutdown failed
```

## Timeout autenticazione CES

L'istantanea seguente mostra il timeout del client CES EST dopo il timer predefinito di 10 secondi durante il processo di autenticazione certsrv iniziale.

```
nginx: [warn] login_to_certsrv_ca: Curl call for MS CA login failed with return code 28
(Operation timed out after 10000 milliseconds with 0 bytes received)

nginx: [warn] login_to_certsrv_ca: URL used: https://lab-dc.michamen.com:443/certsrv

nginx: [error] retrieve_cacerts: Unable to execute login to certsrv with curl
nginx: [warn] ra_certsrv_ca_plugin_postconf: Unable to retrieve CA Cert chain from CA
```

> **Nota:** CSCvo58656 e CSCvf83629 riguardano entrambi il timeout di autenticazione CES.

### Timeout registrazione CES

Timeout del client CES EST dopo un'autenticazione riuscita in attesa di una risposta a una richiesta di registrazione.

```
nginx: [warn] retrieve_cacerts: Curl request failed with return code 28 (Operation timed out
after 10001 milliseconds with 0 bytes received)


nginx: [warn] retrieve_cacerts: URL used: https://lab-
dc.michamen.com:443/certsrv/certnew.p7b?ReqID=CACert&Renewal=0&Enc=bin


nginx: [warn] ra_certsrv_ca_plugin_postconf: Unable to retrieve CA Cert chain from CA
```

## Avvertenze note

Servizio CSCvo28048 CAPF non più elencato nel menu Raccogli file RTMT

CSCvo58656 CAPF Online CA richiede l'opzione per configurare il timeout massimo della connessione tra RA e CA

CSCvf83629 EST Server che ottiene EST_ERR_HTTP_WRITE durante la registrazione

## Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems