

# Troubleshooting CAPF Online CA

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Overview of Feature Components](#)

[Registration Authority \(RA\)](#)

[Enrollment over Secure Transport \(EST\)](#)

[libEST](#)

[Engine-X \(NGINX\)](#)

[Certificate Enrollment Service \(CES\)](#)

[Certificate Authority Proxy Function \(CAPF\)](#)

[Message Flow Diagram](#)

[Message Flow Explanation](#)

[/.well-known/est/simpleenroll](#)

[/certsrv](#)

[/certsrv/certrqxt.asp](#)

[/certsrv/certifnsh.asp](#)

[/certsrv/certnew.cer](#)

[Relevant Traces/Logs for Troubleshooting](#)

[CAPF Logs](#)

[CiscoRA Logs](#)

[NGINX error.log](#)

[CA Web Server's logs](#)

[Log File Locations](#)

[CAPF logs:](#)

[Cisco RA:](#)

[Nginx Error Log:](#)

[MS IIS log:](#)

[Example Log Analysis](#)

[Services Starting Up Normally](#)

[CES Starting Up as seen in the NGINX log](#)

[CES Starting Up as seen in the NGINX error.log](#)

[CES Starting Up as seen in the IIS Logs](#)

[CAPF Starting Up as seen in the CAPF logs](#)

[Phone LSC Install Operation](#)

[CAPF Logs](#)

[IIS Logs](#)

[Common Issues](#)

[Missing CA certificate in issuer chain of IIS identity certificate](#)

[Web Server presenting a Self-Signed certificate](#)

[Mismatch with URL hostname and Common Name](#)

[DNS Resolution Issue](#)

[Issue with Certificate Validity Dates](#)

[Certificate Template Misconfiguration](#)

[CES Authentication Timeout](#)

[CES Enrollment Timeout](#)

[Known Caveats](#)

[Related Information](#)

## Introduction

This document describes troubleshooting for the Certificate Authority Proxy Function (CAPF) Automatic Enrollment and Renewal feature. This feature is also referred to as CAPF Online CA.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Certificates
- Cisco Unified Communications Manager (CUCM) security

### Components Used

The information in this document is based on CUCM version 12.5 as the CAPF Online CA feature was introduced in CUCM 12.5.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Overview of Feature Components

### Registration Authority (RA)

RA is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue the certificate. RAs are part of a public key infrastructure (PKI).

### Enrollment over Secure Transport (EST)

EST is a protocol defined in request for comment (RFC) 7030 for certificate enrollment for clients which use Certificate Management over CMS (CMC) messages over Transport Layer Security (TLS) and HyperText Transfer Protocol (HTTP). EST uses a client/server model where the EST client sends enrollment requests and the EST server sends responses with the results.

### libEST

libEST is the library for Cisco's implementation of EST. libEST allows X509 certificates to be provisioned on end-user devices and network infrastructure devices. This library is implemented by CiscoEST and CiscoRA.

## Engine-X (NGINX)

NGINX is a web server and reverse proxy similar to Apache. NGINX is used for HTTP communication between CAPF and CES as well as communication between CES and the CA Web Enrollment Service. When libEST operates in server mode a web server is required to handle TCP requests on behalf of libEST's.

## Certificate Enrollment Service (CES)

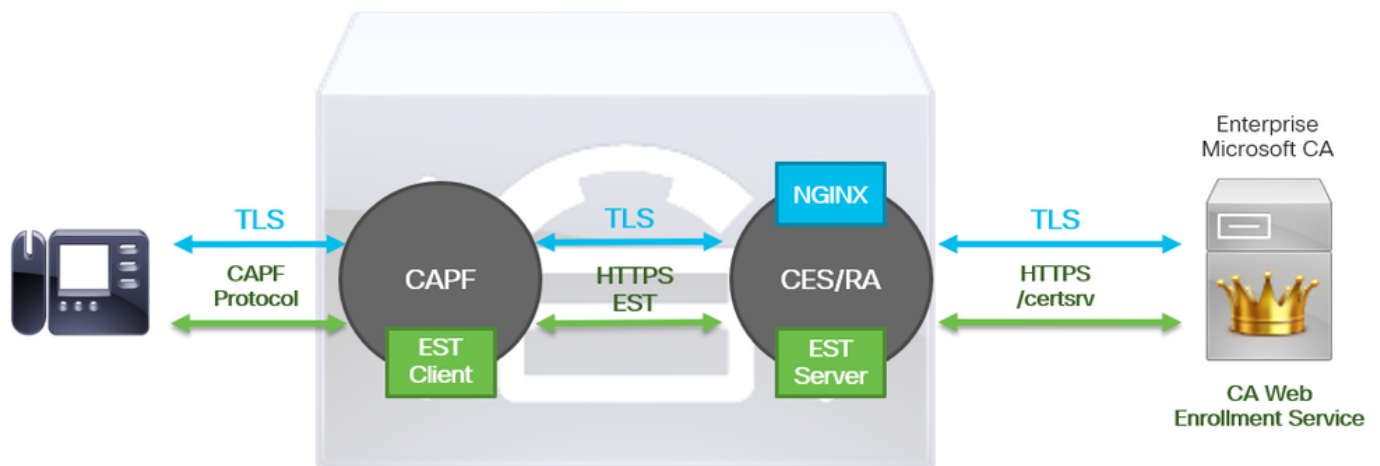
CES is the service on CUCM which acts as the RA between the CAPF service and the CA. CES is also referred to as CiscoRA, or simply RA. CES uses NGINX as it's Web server because CES implements the libEST in server mode in order to act as the RA.

## Certificate Authority Proxy Function (CAPF)

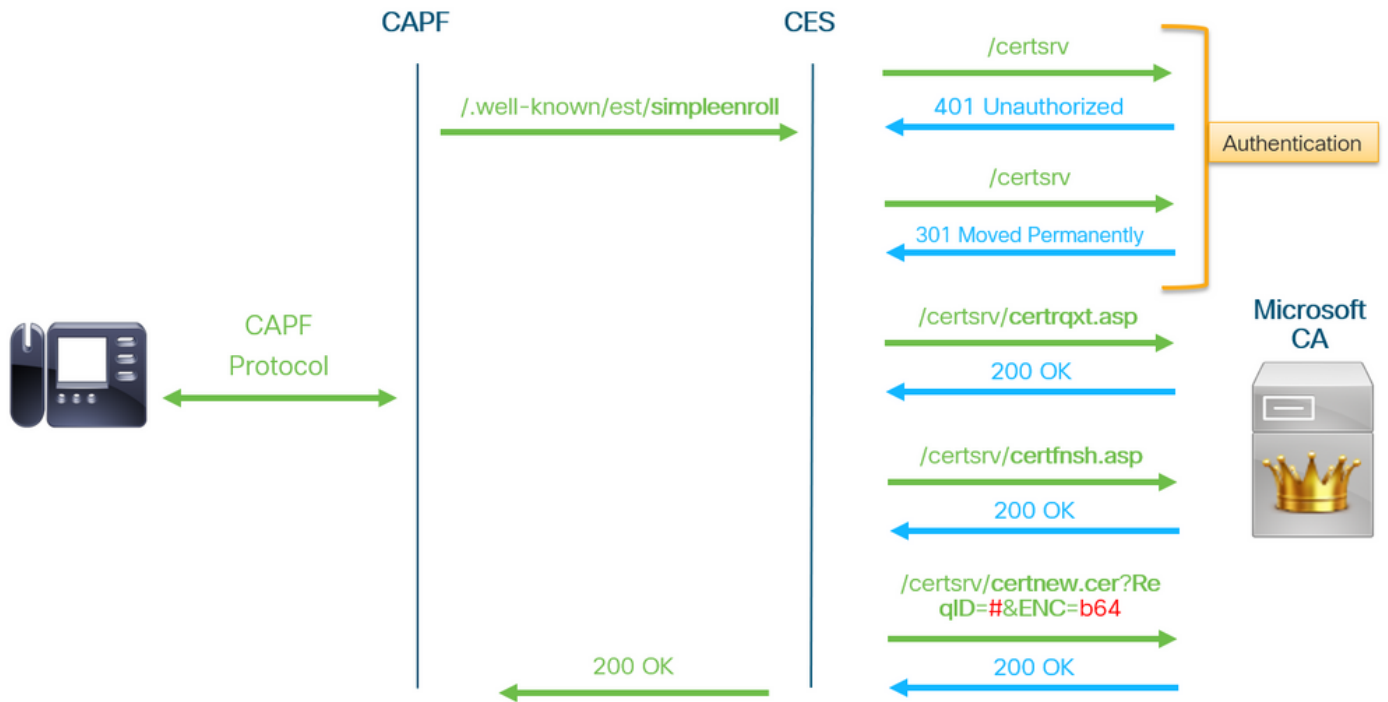
CAPF is a CUCM service which phones interact with when performing certificate enrollment requests. CAPF interacts with the CES on behalf of the phones. In this feature model CAPF implements libEST in client mode to enroll the phones' certificates through CES.

In summary, here's how each component is implemented:

1. The phone sends a certificate request to CAPF
2. CAPF implements CiscoEST (client mode) to communicate with CES
3. CES implements CiscoRA (server mode) to process and respond to the EST client's requests
4. CES/CiscoRA communicates with the CA's Web Enrollment Service via HTTPS



## Message Flow Diagram



## Message Flow Explanation

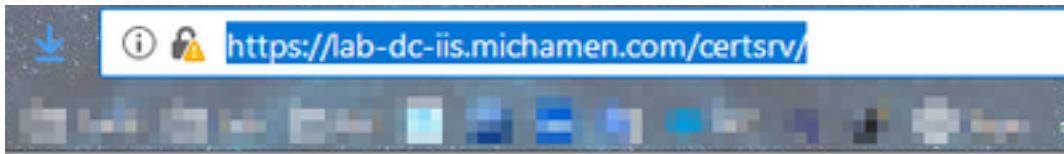
### `/.well-known/est/simpleenroll`

The EST client uses this URL to send an API call which requests the certificate enrollment from the EST server. Once the EST server receives the API call it will start the certificate enrollment process which includes HTTPS communication with the CA's Web Enrollment service. If the enrollment process is successful, and the EST server receives the new certificate, CAPF will proceed to load the certificate and serve it back to the IP phone.

### `/certsrv`

The `/certsrv` URL is used by the EST client to authenticate and start a session with the CA.

The image below is an example of `/certsrv` URL from a web browser. This is the Certificate Services landing page.



Microsoft Active Directory Certificate Services -- LAB-DC-RTP

## Welcome

---

Use this Web site to request a certificate for your Web browser, depending upon the type of certificate you request, perform other tasks.

You can also use this Web site to download a certificate authority certificate.

For more information about Active Directory Certificate Services, see the help topics.

### Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

---

## **/certsrv/certrqxt.asp**

The **/certsrv/certrqxt.asp** URL is used to initiate the request for a new certificate. The EST client uses **/certsrv/certrqxt.asp** to submit the CSR, certificate template name, and any desired attributes.

The image below is an example of **/certsrv/certrqxt.asp** from a web browser.

Browser address bar: <https://lab-dc-iis.michamen.com/certsrv/certrqxt.asp>

Page title: Microsoft Active Directory Certificate Services -- LAB-DC-RTP

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM (Web server) in the Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

**Certificate Template:**

CiscoRA

**Additional Attributes:**

Attributes:

## /certsrv/certfnsh.asp

The **/certsrv/certfnsh.asp** URL is used to submit data for the certificate request; which includes the CSR, the certificate template name and any desired attributes. To view the submission use the browser's **Developer Tools** to open the browser's console before the data is submitted via the *certrqxt.asp* page.

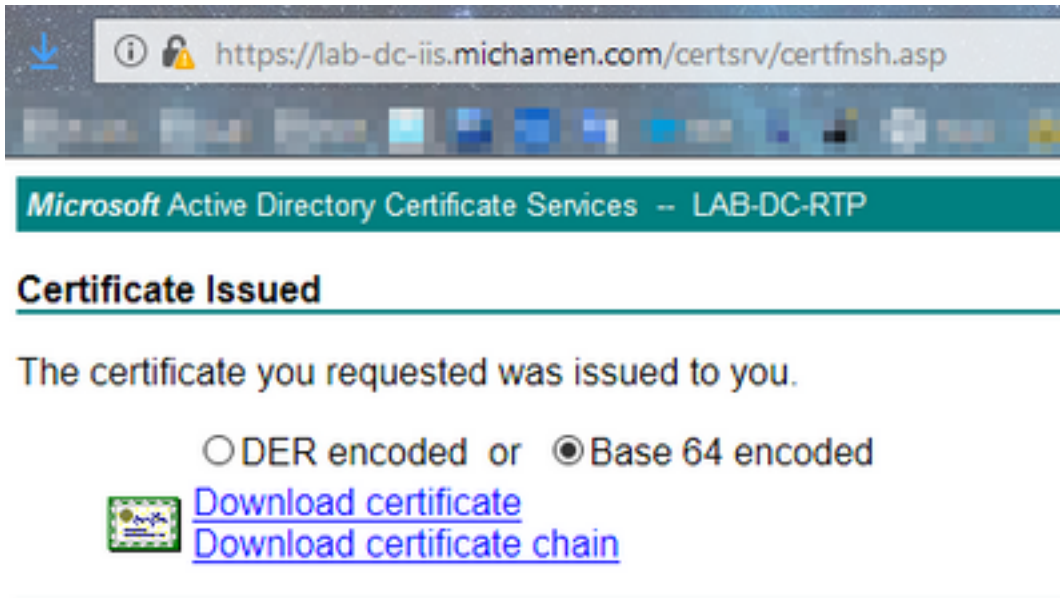
The image below is an example of the data displayed in the browser's console.

```

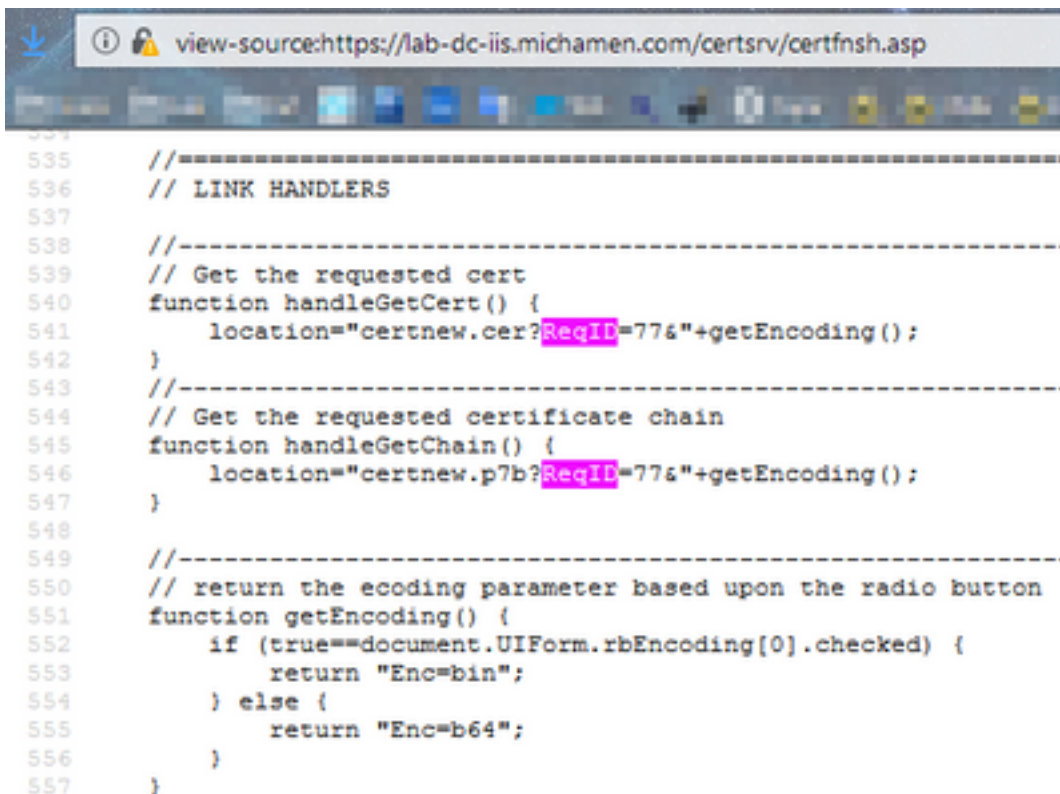
POST https://lab-dc-iis.michamen.com/certsrv/certfnsh.asp
Headers  Cookies  Params  Response  Timings  Security
Filter request parameters
Form data
  Mode: newreq
  CertRequest: -----BEGIN+CERTIFICATE+REQUEST----- MIIC7TCCAdUCAQAwBDELMAKGA1UEBHMwV9kCzA3BGNVBAgTAKSi
  EwNSVFh0ZjA0BGNVBAoTBUNpc2NvNkwiCgYDVQQLLEwNUQUPkIDAeBGNVBAHTF2N1 Y20xhVvdiIubk1jaSFTZi
  CgKCAQEAtk9AcGKcf5ht1Z18X9Iyke9p8sVW9wevUnn2N10K3PEqR8cTe2a+S3h0 D18rja5yM+Th3g0j4b/8Un
  09Pmzqlddw/ke283pT9YBEE0NRmsGT15339555x9cRvter4yr+/vM0N1da1n oEP7GUv8DErnAXDRj538HQ
  IDAQBoEAwPgy3ko2IhvcNAQkOHTeWlzAd BGNVH5UEFjAU8ggr8gEF8QcDAQYIKwYBBQUHwIwDgyDVR0PAQH/
  CSQGSIB3DQEBcUAA4IBAQBpHR5QmFQk8r1wdCElP3DjSPqeYg8hY4HvunM+49m ZfFKGUXJtxy03SPa9VAdR4I
  N/yintaI7ewqXspYhPSQhplsnxgDKjwf1xjLjTVdwfBod/w0rphn73S1bbWQdu1 6p46yFt0fujx1ur3P1f0mH
  rYfZSxrcgIY0hyrd1aBry0K00o2onf8IQLFqF6uBQw1/W2Me0tD5GkNLI9+S2WC2 y1grvWvqN/vwdrb5E+T79o
  CertAttrib: CertificateTemplate:CiscoRA userAgent:Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:65.0)
  FriendlyType: Saved-Request+Certificate+(3/14/2019,+10:09:02+AM)
  ThumbPrint:
  TargetStoreFlags: 0
  
```

The submission response from **/certsrv/certfnsh.asp** includes the request ID of the certificate

issued by the CA. The request ID is seen in a web browser when the page's source code is inspected.



**Tip:** Search the page source for “ReqID”



### **/certsrv/certnew.cer**

At this point the EST client is aware of the request ID for the new certificate. The EST client uses **/certsrv/certnew.cer** to pass the request ID and file encoding as parameters to download the certificate file with the **.cer** extension.


This is equivalent to what happens in your browser when you click the **Download Certificate** link.

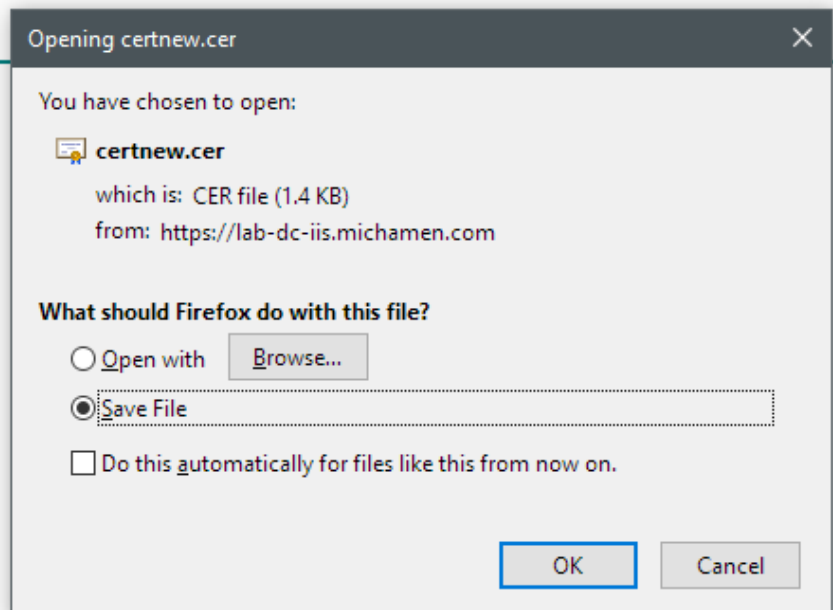


## Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

 [Download certificate](#)  
[Download certificate chain](#)



To view the request URL and parameters, use the browser's console.

**Note:** The browser specifies **bin** for the encoding parameter if DER encoding is selected; however, Base64 encoding will show as b64.



## Relevant Traces/Logs for Troubleshooting

These logs assist with the isolation of most issues.

### CAPF Logs

CAPF Logs include interactions with phones and minimal logging of CiscoEST activity.



**Note:** These logs are available for collection via the Command Line Interface (CLI) or the Real Time Monitoring Tool (RTMT). Due to [CSCvo28048](#) CAPF may not show among the list of services in RTMT.

## CiscoRA Logs

CiscoRA Logs are often referred to as the CES logs. CiscoRA logs contain the CES initial startup activity and displays errors which may arise while authentication with the CA occurs. If the initial authentication with the CA is successful, subsequent activity for phone enrollments is not logged in here. Therefore, CiscoRA logs serve as a good initial point to troubleshoot issues.

**Note:** These logs can only be collected via the CLI as of this document's creation.

## NGINX error.log

NGINX error.log is the most useful log for this feature as it logs all activity during start up as well as any HTTP interactions between NGINX and the CA side; which includes error codes returned from the CA as well as those generated by CiscoRA after processing the request.

**Note:** At the time of creating this document, there's no way to collect these logs even from CLI. These logs can only be downloaded using a remote support account (root).

## CA Web Server's logs

CA Web Server's logs are important as they display any HTTP activity including request URLs, response codes, response duration and response size. You can use these logs to correlate interactions between CiscoRA and the CA.

**Note:** CA Web Server logs in the context of this document are the MS IIS logs. If other web CAs are supported in the future, they may have different log files which serve as the CA Web Server's logs

## Log File Locations

### CAPF logs:

- From root: `/var/log/active/cm/trace/capf/sdi/capf<number>.txt`
- From CLI: `file get activelog cm/trace/capf/sdi/capf*`

**Note:** Set the CAPF trace level to "Detailed" and restart the CAPF service before testing is performed.

### Cisco RA:

- From root: `/var/log/active/cm/trace/capf/sdi/nginx<number>.txt`

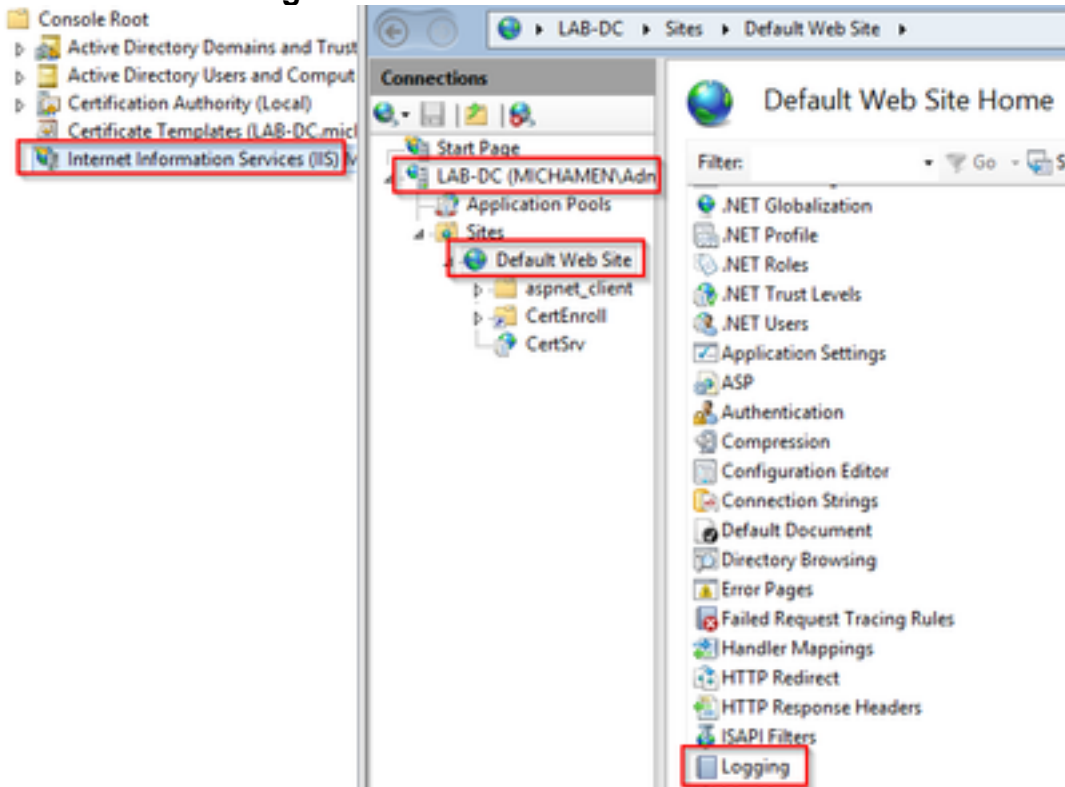
- From CLI: file get activelog cm/trace/capf/sdi/nginx\*

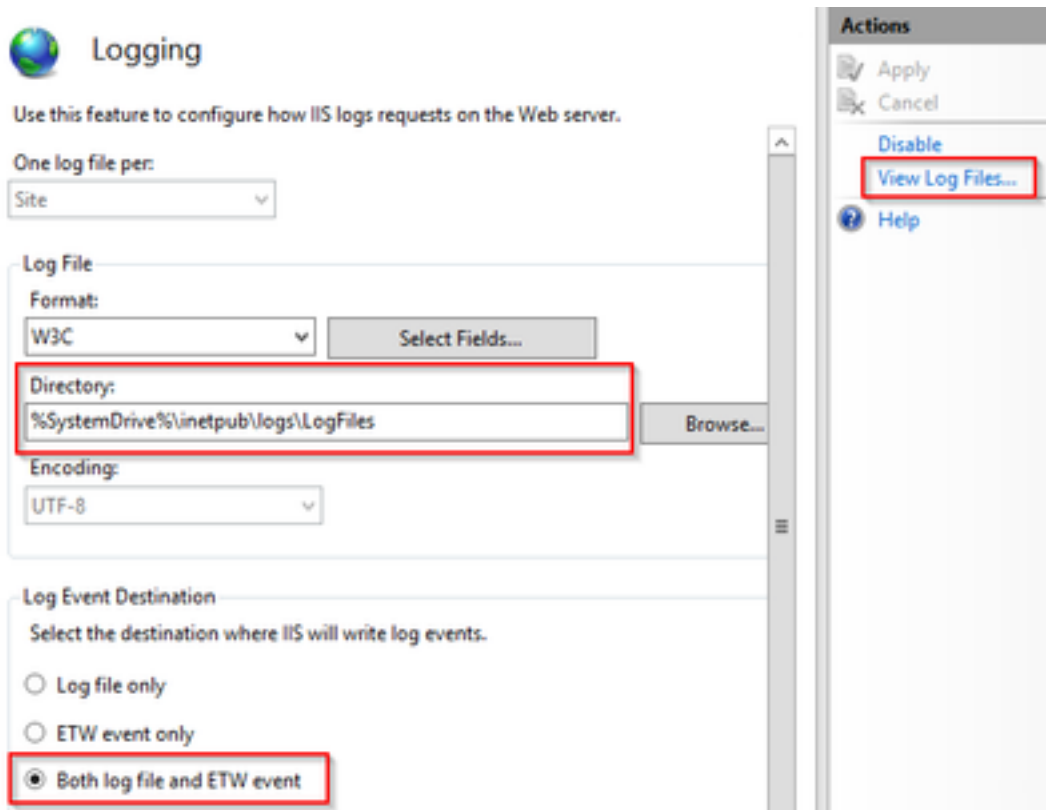
## Nginx Error Log:

- From root: /usr/local/thirdparty/nginx/install/logs/error.log
- Not available from CLI

## MS IIS log:

- Open MMC
- Select the **Internet Information Services (IIS)** snap-in
- Click the server name
- Click **Default Web Site**
- Double click **Logging** to see the logging options
- Select **View Log Files** in the **Actions** menu





## Example Log Analysis

### Services Starting Up Normally

#### CES Starting Up as seen in the NGINX log

Little information is gathered from this log. The full certificate chain that is loaded into its trust store is seen here and one is for the web container while the other is for 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] ssl_init_cert_store: Adding cert to store (/O=Cisco/CN=ACT2 SUDI CA)
nginx: [warn] ssl_init_cert_store: Adding cert to store (/C=US/O=cisco/OU=tac/CN=CAPF-
eb606ac0/ST=nc/L=rtp)
nginx: [warn] ssl_init_cert_store: Adding cert to store (/C=US/O=cisco/OU=tac/CN=CAPF-
eb606ac0/ST=nc/L=rtp)
nginx: [warn] ssl_init_cert_store: Adding cert to store (/O=Cisco Systems/CN=Cisco
Manufacturing CA)
nginx: [warn] ssl_init_cert_store: Adding cert to store (/O=Cisco/CN=Cisco Manufacturing CA
SHA2)
nginx: [warn] ssl_init_cert_store: Adding cert to store (/O=Cisco Systems/CN=Cisco Root CA
2048)
nginx: [warn] ssl_init_cert_store: Adding cert to store (/O=Cisco/CN=Cisco Root CA M2)
nginx: [warn] ssl_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][ssl_init_cert_store_from_raw:182]--> Adding cert to store (/O=Cisco/CN=ACT2 SUDI
CA)
***EST [INFO][ssl_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

```

## CES Starting Up as seen in the NGINX error.log

The login using the certificate template configuration and credentials is observed in the snippet here:

```

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

```

The retrieval of the CA certificate chain is observed in the snippet here:

```

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

```

When the request is successful the certnew.p7b file is obtained. The same URL with the template credentials can be used to get the certnew.p7b file from a web browser.

## CES Starting Up as seen in the IIS Logs

The same CES starting up events seen in the NGINX error.log are also observed on the IIS logs; however, the IIS logs include 2 more HTTP GET requests because the first request will be challenged by the Web server through a 401 response; and once authenticated a requested will be redirected using a 301 response:

```

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

```

## CAPF Starting Up as seen in the CAPF logs

Most of it what occurs in the CAPF logs for CES starting up looks the same as what occurs in the other logs; but you'll notice the CAPF service detecting the method and configuration for Online CA:

```
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
```

The next important observation from the logs is when the CAPF service initializes it's EST client.

```
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!!
```

## Phone LSC Install Operation

### CAPF Logs

It is recommended to collect all the necessary logs and start the analysis with a review of the CAPF logs. This allows us to know the time reference for a specific phone.

The initial part of the signaling looks the same as with other CAPF methods except the EST client running in the CAPF service will perform the enrollment with CES towards the end of the dialog (after the CSR has been provided by the phone).

```
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

```

Once the CES has retrieved the phone's signed certificate, the certificate is converted to DER format before it is provided to the phone.

```

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

```

The CAPF service takes over again and loads the CSR from the location it was written to in the snippet above (/tmp/capf/cert/). The CAPF service then provides the signed LSC to the phone. At the same time the phone's CSR is deleted.

```

14:05:05.289 |<--findAndPost
14:05:05.289 |-->debug
14:05:05.289 |   debug added 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

```

## IIS Logs

The snippet below displays the events in the IIS logs for a phone's LSC installation steps as explained above.

```

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/certifnsh.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

```

## Common Issues

Whenever there is an error in the CES side, it is expected to see output like the snippet below in the CAPF logs. Be sure to check other logs to continue narrowing down the issue.

```

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 added 10 to readset
12:38:04.779 |<--debug

```

## Missing CA certificate in issuer chain of IIS identity certificate

When a root certificate or intermediate certificate, which is in the certificate chain, is not trusted by CES the error "Unable to retrieve CA Cert chain from CA" is printed in the nginx logs.



```
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
```

## Web Server presenting a Self-Signed certificate

The use of a self-signed certificate on the IIS is not supported and will not work even if uploaded as CAPF-trust on the CUCM. The snippet below is from the nginx logs and it displays what is observed when the IIS is using a self-signed certificate.

```
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
```

## Mismatch with URL hostname and Common Name

The IIS certificate's Common Name (lab-dc) does not match the FQDN inside the URL of the CA's Web Enrollment service. For certificate validation to succeed the FQDN inside the URL must match the Common Name on the certificate used by the 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
```

## DNS Resolution Issue

CiscoRA is unable to resolve the hostname of the Online CA configured in service parameters.

```
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
```

## Issue with Certificate Validity Dates

When Network Time Protocol (NTP) not working properly issues with certificate validity dates occur. This check is performed by CES upon start up and it is observed in the NGINX logs.

```
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
```

## Certificate Template Misconfiguration

A typo in the name within service parameters will cause failures. No errors will be logged in the CAPF nor NGINX logs so it is required to check the NGINX error.log.

```
***EST [INFO][est_enroll_auth:356]--> TLS: no peer certificate
2019/02/27 16:53:28 [warn] 3187#0: *2 openssl_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
```

## CES Authentication Timeout

The snippet below shows the CES EST client time out after the default timer of 10 seconds during the initial certsrv authentication process.

```
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
```

**Note:** [CSCvo58656](#) and [CSCvf83629](#) both pertain to the CES authentication timeout.

## CES Enrollment Timeout

CES EST client time out after a successful authentication but while waiting for a response to an enrollment request.

```
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
```

## Known Caveats

[CSCvo28048](#) CAPF Service not listed in RTMT Collect Files menu anymore

[CSCvo58656](#) CAPF Online CA needs option to configure max connection timeout between RA and CA

[CSCvf83629](#) EST Server getting EST\_ERR\_HTTP\_WRITE during Enrollment

## Related Information

- [Technical Support & Documentation - Cisco Systems](#)