

# Fehlerbehebung CAPF Online CA

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Übersicht über die Funktionskomponenten](#)

[Registrierungsstelle \(RA\)](#)

[Anmeldung für Secure Transport \(EST\)](#)

[libEST](#)

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

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

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

[Flussdiagramm](#)

[Erläuterung des Nachrichtenflusses](#)

[/.bekannt/est/SimpleSroll](#)

[/certsrv](#)

[/certsrv/certrqxt.asp](#)

[/certsrv/certifnsh.asp](#)

[/certsrv/certnew.cer](#)

[Relevante Spuren/Protokolle für die Fehlerbehebung](#)

[CAPF-Protokolle](#)

[CiscoRA-Protokolle](#)

[NGINX-Fehler.log](#)

[CA-Webserver-Protokolle](#)

[Speicherorte für Protokolldateien](#)

[CAPF-Protokolle:](#)

[Cisco RA:](#)

[Nginx-Fehlerprotokoll:](#)

[MS IIS-Protokoll:](#)

[Beispielprotokollanalyse](#)

[Normalerweise gestartete Services](#)

[CES Starting Up \(Wie im NGINX-Protokoll zu sehen\)](#)

[CES Starting Up \(Wie im NGINX error.log zu sehen\)](#)

[CES Starting Up \(Wie in den IIS-Protokollen zu sehen ist\)](#)

[CAPF-Start wie in den CAPF-Protokollen zu sehen](#)

[LSC-Installationsvorgang des Telefons](#)

[CAPF-Protokolle](#)

[IIS-Protokolle](#)

[Häufige Probleme](#)

[Fehlendes Zertifizierungsstellenzertifikat in der Ausstellerkette des IIS-Identitätszertifikats](#)

[Webserver, der ein selbstsigniertes Zertifikat anzeigt](#)

[Nicht übereinstimmend mit URL-Hostname und Common Name](#)

[Problem mit der DNS-Auflösung](#)

[Ausstellung mit Daten für die Gültigkeit von Zertifikaten](#)

[Falsche Konfiguration von Zertifikatsvorlagen](#)

[Timeout für CES-Authentifizierung](#)

[Timeout für CES-Registrierung](#)

[Bekannte Einwände](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird die Fehlerbehebung für die CAPF-Funktion (Certificate Authority Proxy Function) für die automatische Registrierung und Verlängerung beschrieben. Diese Funktion wird auch als CAPF Online CA bezeichnet.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Zertifikate
- Sicherheit von Cisco Unified Communications Manager (CUCM)

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der CUCM-Version 12.5, da die CAPF Online CA-Funktion in CUCM 12.5 eingeführt wurde.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Übersicht über die Funktionskomponenten

### Registrierungsstelle (RA)

RA ist eine Behörde in einem Netzwerk, die Benutzeranfragen für ein digitales Zertifikat prüft und die Zertifizierungsstelle (Certificate Authority, CA) anweist, das Zertifikat auszustellen. RAs sind Teil einer Public Key Infrastructure (PKI).

### Anmeldung für Secure Transport (EST)

EST ist ein Protokoll, das in Request for comment (RFC) 7030 für die Zertifikatsregistrierung für Clients definiert wird, die Zertifikatsmanagement-over-CMS (CMC)-Nachrichten über Transport Layer Security (TLS) und HyperText Transfer Protocol (HTTP) verwenden. EST verwendet ein

Client-/Servermodell, bei dem der EST-Client Registrierungsanfragen sendet und der EST-Server Antworten mit den Ergebnissen sendet.

## libEST

libEST ist die Bibliothek für die EST-Implementierung von Cisco. Mit libEST können X509-Zertifikate auf Endbenutzergeräten und Geräten der Netzwerkinfrastruktur bereitgestellt werden. Diese Bibliothek wird von CiscoEST und CiscoRA implementiert.

## Engine-X (NGINX)

NGINX ist ein Webserver und Reverse Proxy ähnlich dem Apache. NGINX wird für die HTTP-Kommunikation zwischen CAPF und CES sowie für die Kommunikation zwischen CES und dem CA Web Enrollment Service verwendet. Wenn libEST im Servermodus betrieben wird, muss ein Webserver TCP-Anfragen im Auftrag von libESTs bearbeiten.

## Certificate Enrollment Service (CES)

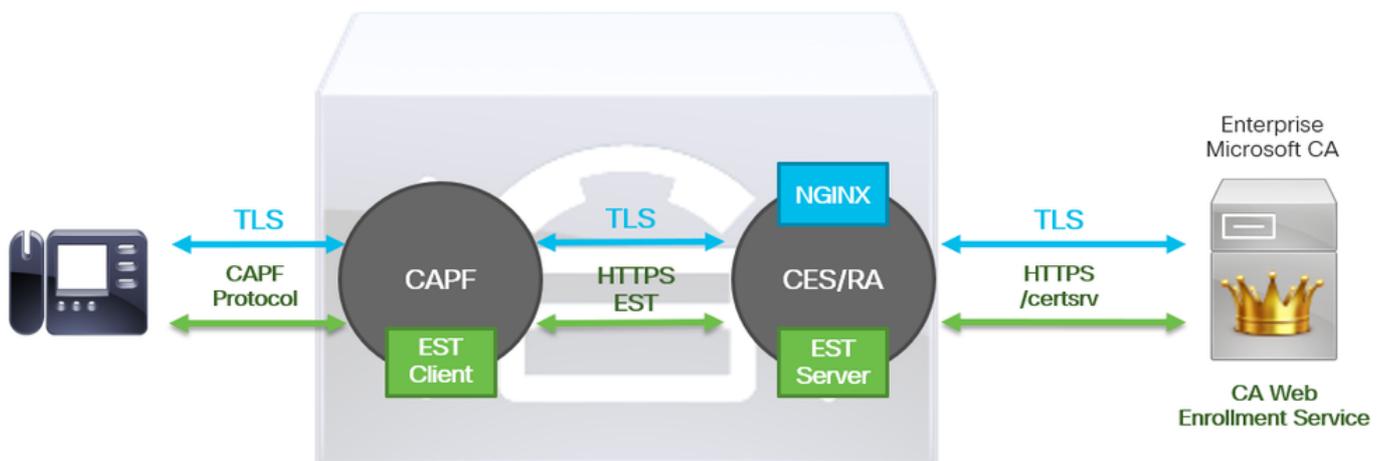
Der CES-Dienst auf dem CUCM fungiert als RA zwischen dem CAPF-Service und der CA. CES wird auch als CiscoRA oder einfach RA bezeichnet. CES verwendet NGINX als Webserver, da CES das libEST im Servermodus implementiert, um als RA zu agieren.

## CAPF (Certificate Authority Proxy Function)

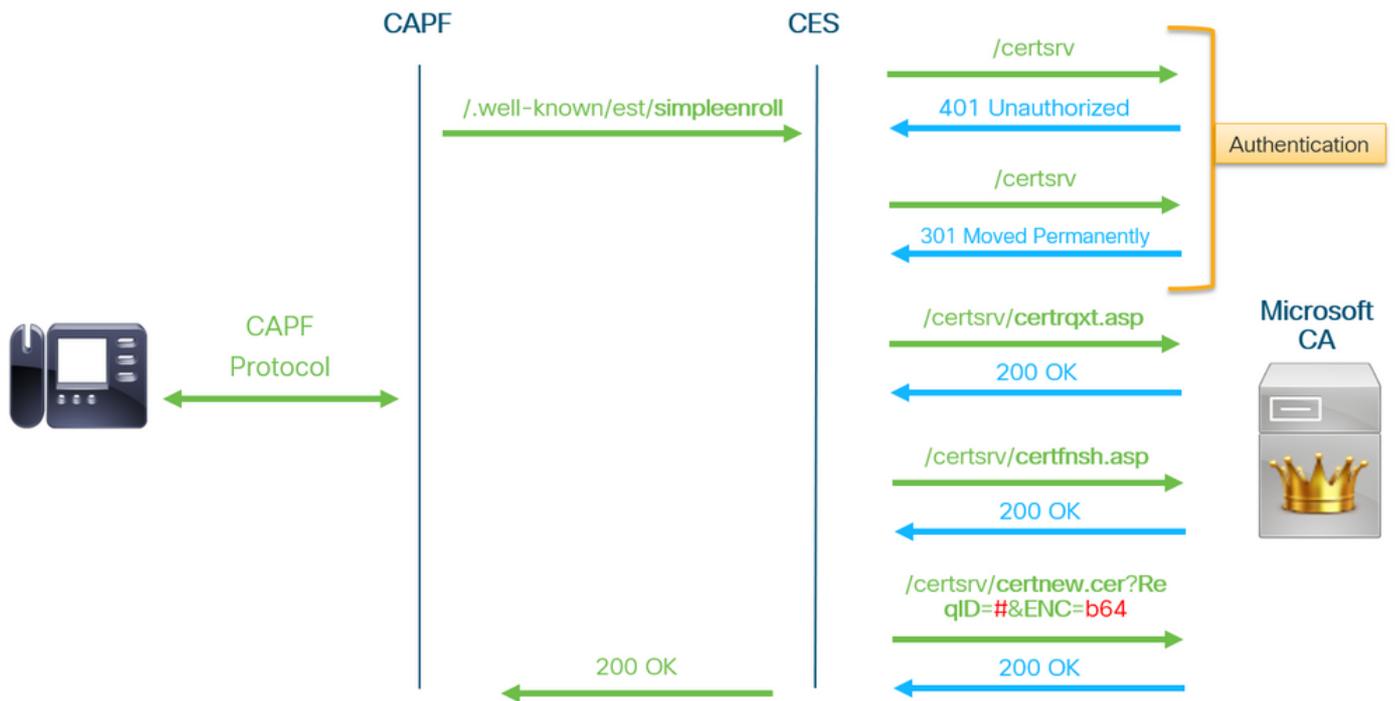
CAPF ist ein CUCM-Service, mit dem Telefone interagieren, wenn sie Zertifizierungsanforderungen erfüllen. CAPF interagiert mit dem CES für die Telefone. In diesem Funktionsmodell implementiert CAPF libEST im Clientmodus, um die Zertifikate der Telefone über CES zu registrieren.

Zusammenfassend lässt sich sagen, wie die einzelnen Komponenten implementiert werden:

1. Das Telefon sendet eine Zertifikatsanforderung an CAPF.
2. CAPF implementiert CiscoEST (Client-Modus) für die Kommunikation mit CES
3. CES implementiert CiscoRA (Servermodus) für die Verarbeitung und Beantwortung von Anfragen des EST-Clients
4. CES/CiscoRA kommuniziert über HTTPS mit dem Web Enrollment Service der CA.



# Flussdiagramm



## Erläuterung des Nachrichtenflusses

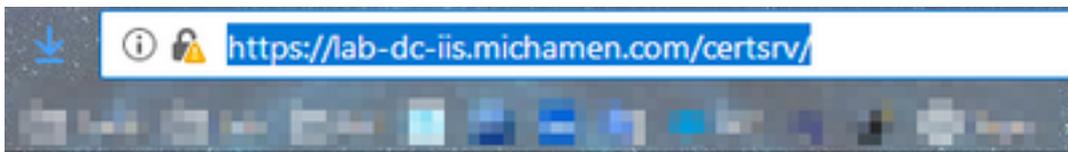
### `/.bekannt/est/SimpleSroll`

Der EST-Client verwendet diese URL, um einen API-Aufruf zu senden, der die Zertifikatregistrierung vom EST-Server anfordert. Sobald der EST-Server den API-Aufruf erhält, startet er den Zertifikatregistrierungsprozess, der HTTPS-Kommunikation mit dem Web Enrollment-Dienst der CA beinhaltet. Wenn der Registrierungsprozess erfolgreich verläuft und der EST-Server das neue Zertifikat erhält, lädt CAPF das Zertifikat und stellt es wieder an das IP-Telefon zurück.

### `/certsrv`

Die `/certsrv`-URL wird vom EST-Client für die Authentifizierung und das Starten einer Sitzung mit der CA verwendet.

Das Bild unten ist ein Beispiel für `/certsrv`-URL eines Webbrowsers. Dies ist die Landing Page für Zertifizierungsdienste.



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

Die `/certsrv/certrqxt.asp`-URL wird verwendet, um die Anforderung eines neuen Zertifikats zu initiieren. Der EST-Client verwendet `/certsrv/certrqxt.asp`, um den CSR, den Namen der Zertifikatsvorlage und alle gewünschten Attribute einzureichen.

Das Bild unten ist ein Beispiel für `/certsrv/certrqxt.asp` in einem Webbrowser.

↓ ⓘ https://lab-dc-iis.michamen.com/certsrv/certrqxt.asp

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:

Submit >

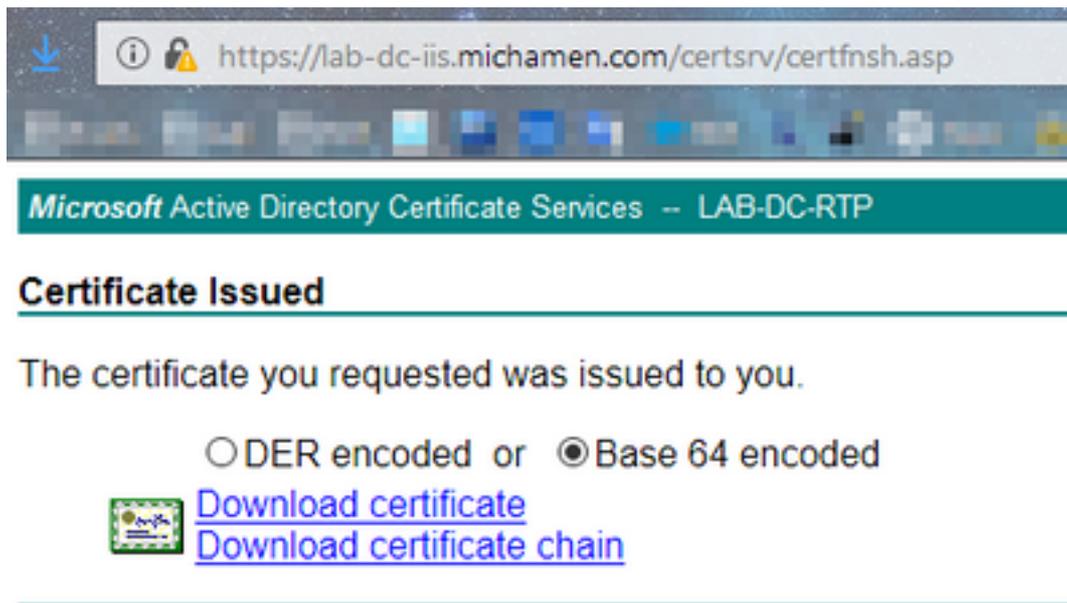
## /certsrv/certrqxt.asp

Die `/certsrv/certrqxt.asp`-URL wird verwendet, um Daten für die Zertifikatsanforderung zu übermitteln. Dazu gehören der CSR, der Name der Zertifikatsvorlage und alle gewünschten Attribute. Um die Übermittlung anzuzeigen, öffnen Sie mithilfe der **Developer Tools** des Browsers die Browserkonsole, bevor die Daten über die Seite `certrqxt.asp` übermittelt werden.

Das nachfolgende Bild zeigt ein Beispiel für die Daten, die in der Browserkonsole angezeigt werden.

```
POST https://lab-dc-iis.michamen.com/certsrv/certrqxt.asp
Headers  Cookies  Params  Response  Timings  Security
Filter request parameters
Form data
Mode: newreq
CertRequest: -----BEGIN+CERTIFICATE+REQUEST----- MIIC7TCCAdUCAQAwDELMAKGA1UEBHMVb3R0c2A3BGNVBAgTAKSI
EwNSVFh0dDwke283pT9YyB6E0NRmSG8T15339555x9cRvter4yr+/vMhAnIdaln oEP7GUv8dErnaxDRjd38HQ
IDAQABoEAnPgy3koZIHvCNAQKONTEwLzAd BGNVhSUEFjAUBgggr8gEFBQcDAQYIKoYB8QUHwIhwDgYDVRR0PAQH/I
CSqSSIb3DQEBcWUAA4IBAQBpHr5QmFQk8r1wdCE1P3DjSPqeYg8hY4h/vunM+49m ZfKlGUXJtxy03SPa9VAdR4
N/yIntaI7ewqXSpYHPSQHp1snxgDKjwf1xjLjTVdWfBod/w@yphn33S1bbWQdu1 6p46yFt0jUjx1ur3P1f0mH
rYfZ5XncgIY0hyRd1aBry0K0o3onfB1QLFqF6UBCW1/W3Me0TDSgKvLI9+S2WC2 y1grvVvqN/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
```

Die Antwort der `/certsrv/certifnsh.asp` enthält die Anfrage-ID des von der Zertifizierungsstelle ausgestellten Zertifikats. Die Anfrage-ID wird in einem Webbrowser angezeigt, wenn der Quellcode der Seite überprüft wird.



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

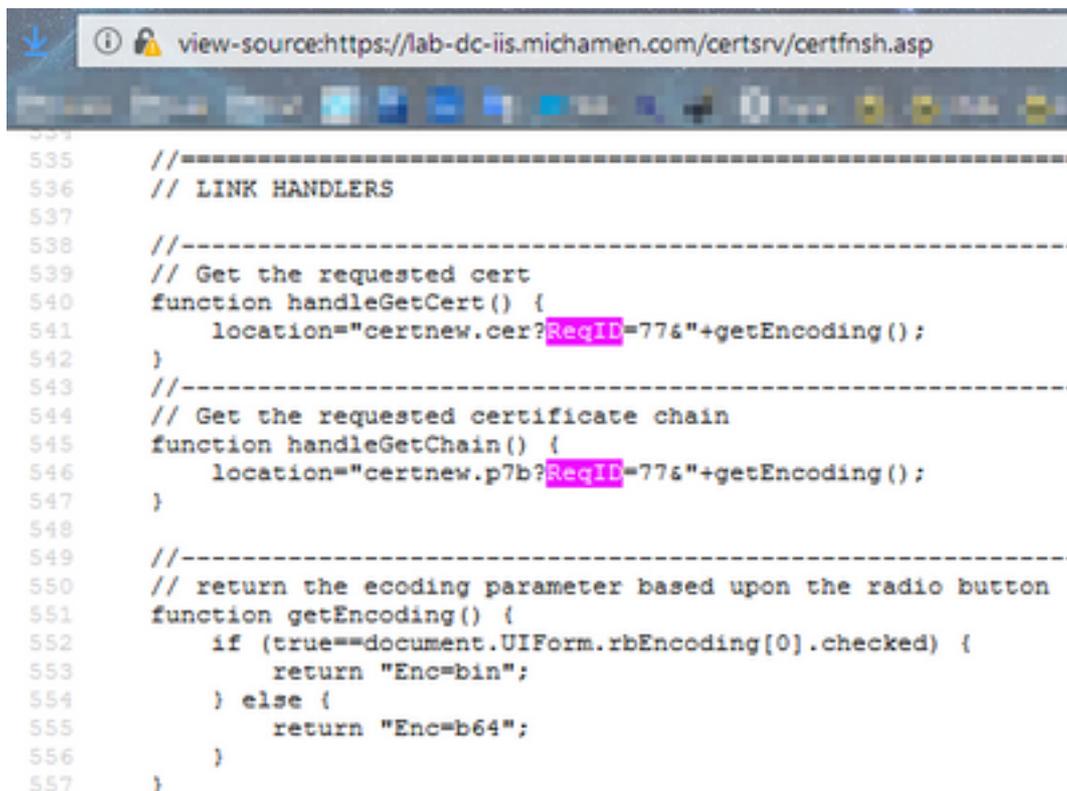
## Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

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

**Tip:** Durchsuchen Sie die Seitenquelle nach "ReqID".



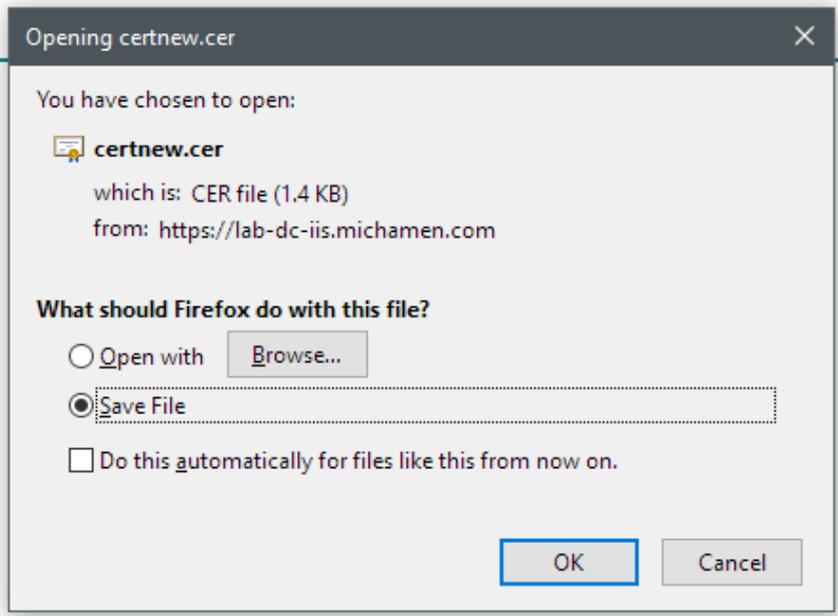
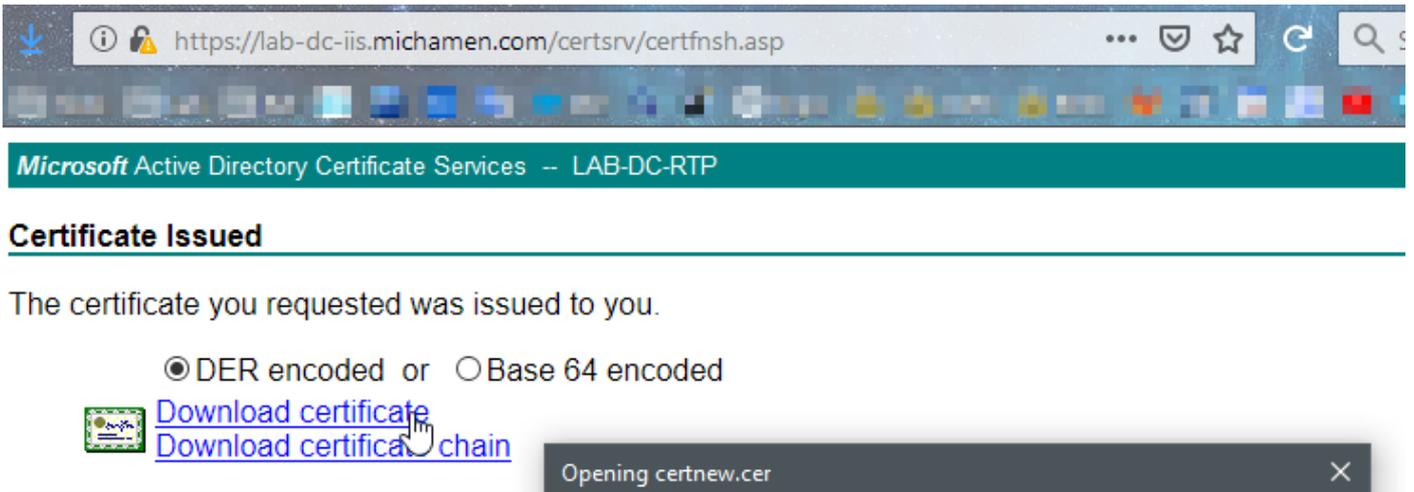
```
535 //-----  
536 // LINK HANDLERS  
537  
538 //-----  
539 // Get the requested cert  
540 function handleGetCert() {  
541     location="certnew.cer?ReqID=77&"+getEncoding();  
542 }  
543 //-----  
544 // Get the requested certificate chain  
545 function handleGetChain() {  
546     location="certnew.p7b?ReqID=77&"+getEncoding();  
547 }  
548  
549 //-----  
550 // return the encoding parameter based upon the radio button  
551 function getEncoding() {  
552     if (true==document.UIForm.rbEncoding[0].checked) {  
553         return "Enc=bin";  
554     } else {  
555         return "Enc=b64";  
556     }  
557 }
```

### `/certsrv/certnew.cer`

Zu diesem Zeitpunkt ist dem EST-Client die Anfrage-ID für das neue Zertifikat bekannt. Der EST-Client verwendet `/certsrv/certnew.cer`, um die Anforderungs-ID und die Dateicodierung als Parameter zu übergeben, um die Zertifikatsdatei mit der Erweiterung `.cer` herunterzuladen.

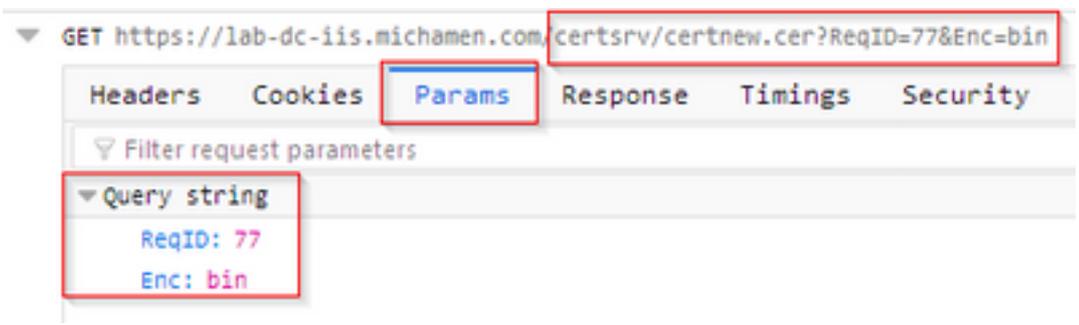
Dies entspricht dem, was in Ihrem Browser geschieht, wenn Sie auf den Link **Zertifikat**

herunterladen klicken.



Um die Anforderungs-URL und die Parameter anzuzeigen, verwenden Sie die Browserkonsole.

**Hinweis:** Der Browser gibt **bin** für den Kodierungsparameter an, wenn die DER-Codierung ausgewählt ist. Die Base64-Codierung wird jedoch als b64 angezeigt.



## Relevante Spuren/Protokolle für die Fehlerbehebung

Diese Protokolle helfen bei der Isolierung der meisten Probleme.

### CAPF-Protokolle

CAPF-Protokolle beinhalten die Interaktion mit Telefonen und die minimale Protokollierung der Cisco EST-Aktivität.

**Hinweis:** Diese Protokolle können über die Befehlszeilenschnittstelle (CLI) oder das Real Time Monitoring Tool (RTMT) erfasst werden. Aufgrund von [CSCvo28048](#) wird CAPF möglicherweise nicht in der Liste der Dienste in RTMT angezeigt.

## CiscoRA-Protokolle

CiscoRA-Protokolle werden häufig als CES-Protokolle bezeichnet. CiscoRA-Protokolle enthalten die erste Startaktivität des CES und zeigen Fehler an, die auftreten können, wenn die Authentifizierung mit der CA erfolgt. Wenn die erste Authentifizierung mit der CA erfolgreich ist, werden nachfolgende Aktivitäten für die Telefonregistrierung hier nicht protokolliert. CiscoRA-Protokolle dienen daher als Ausgangspunkt zur Fehlerbehebung.

**Hinweis:** Diese Protokolle können erst ab der Erstellung dieser Dokumente über die CLI erfasst werden.

## NGINX-Fehler.log

NGINX error.log ist das nützlichste Protokoll für diese Funktion, da es alle Aktivitäten beim Start sowie alle HTTP-Interaktionen zwischen NGINX und der CA-Seite protokolliert. Dazu gehören Fehlercodes, die von der CA zurückgegeben wurden, sowie Fehlercodes, die von CiscoRA nach Verarbeitung der Anfrage generiert wurden.

**Hinweis:** Zum Zeitpunkt der Erstellung dieses Dokuments ist es nicht möglich, diese Protokolle auch über die CLI zu erfassen. Diese Protokolle können nur über ein Remote-Support-Konto (root) heruntergeladen werden.

## CA-Webserver-Protokolle

Die Protokolle von CA Web Server sind wichtig, da sie alle HTTP-Aktivitäten anzeigen, einschließlich Anforderungs-URLs, Antwortcodes, Reaktionsdauer und Antwortgröße. Sie können diese Protokolle verwenden, um die Interaktionen zwischen CiscoRA und der CA zu korrelieren.

**Hinweis:** CA-Webserverprotokolle im Kontext dieses Dokuments sind die MS IIS-Protokolle. Wenn andere Web-CAs zukünftig unterstützt werden, verfügen sie möglicherweise über verschiedene Protokolldateien, die als Protokolle des CA-Webservers dienen.

## Speicherorte für Protokolldateien

### CAPF-Protokolle:

- Von Root: /var/log/active/cm/trace/capf/sdi/capf<number>.txt
- Von CLI: file get activelog cm/trace/capf/sdi/capf\*

**Hinweis:** Legen Sie die CAPF-Ablaufverfolgungsebene auf "Detailed" fest, und starten Sie den CAPF-Dienst neu, bevor Tests durchgeführt werden.

## Cisco RA:

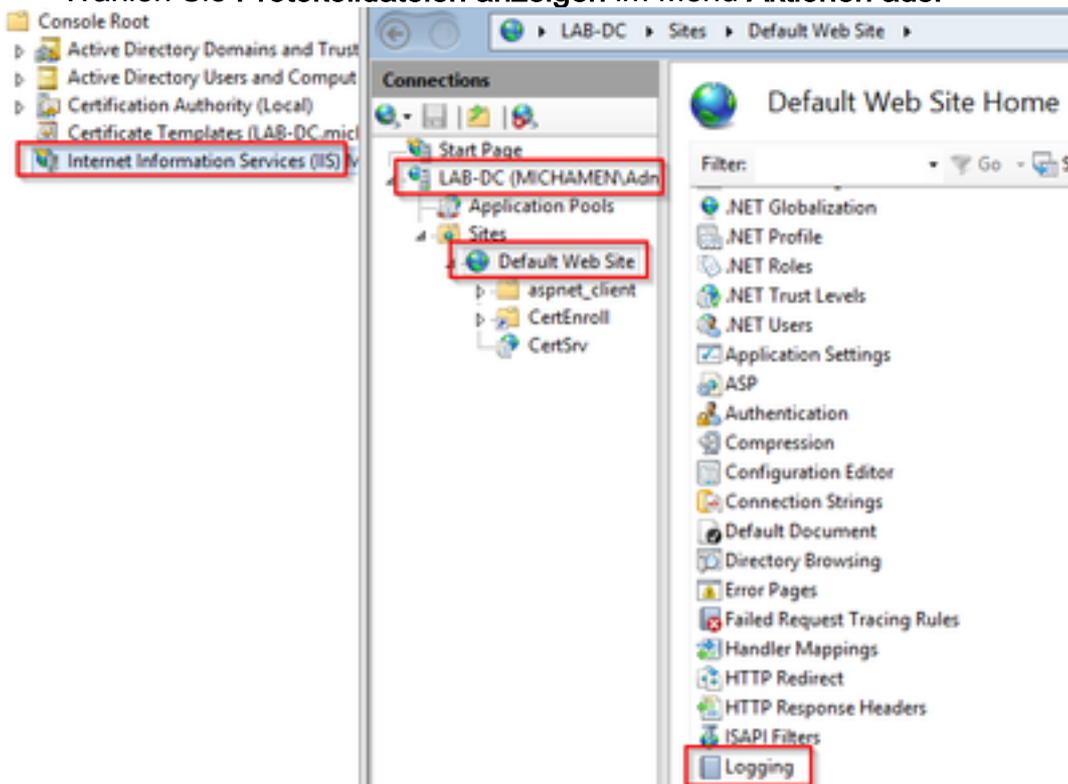
- Von Root: `/var/log/active/cm/trace/capf/sdi/nginx<number>.txt`
- Von CLI: `file get activelog cm/trace/capf/sdi/nginx*`

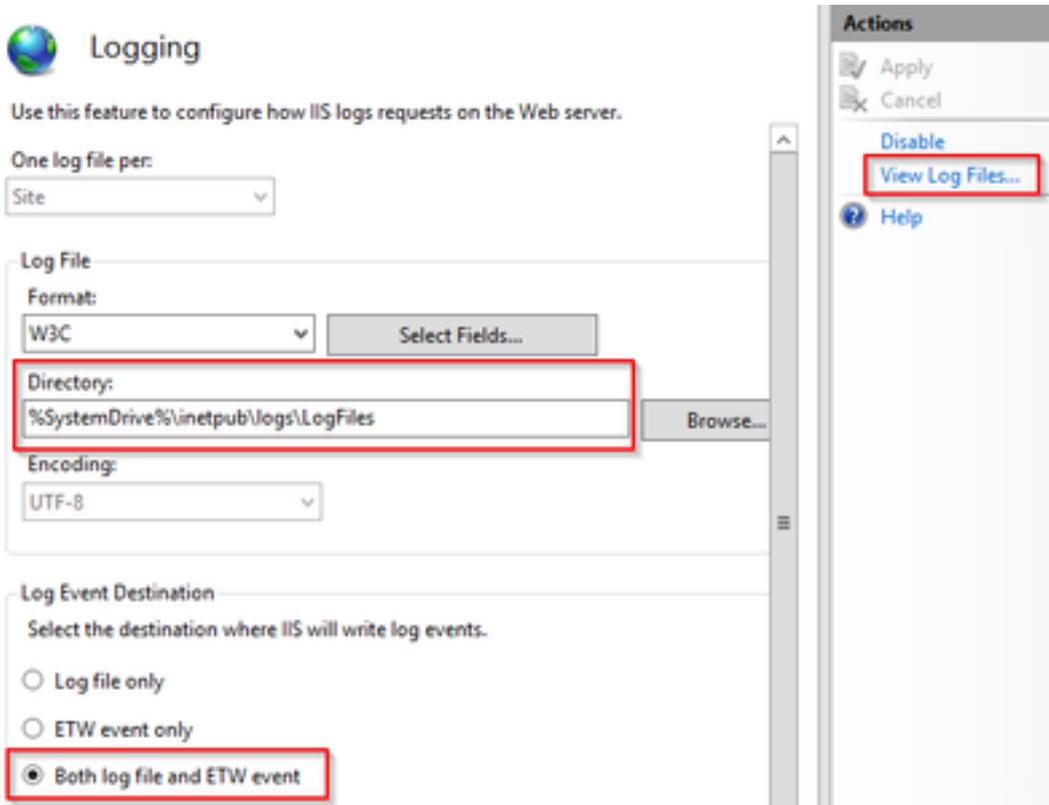
## Nginx-Fehlerprotokoll:

- Von Root: `/usr/local/thirdparty/nginx/install/logs/error.log`
- Von CLI nicht verfügbar

## MS IIS-Protokoll:

- MMC öffnen
- Wählen Sie das Snap-In **Internetinformationsdienste (IIS)** aus.
- Klicken Sie auf den Servernamen
- Klicken Sie auf **Standardwebsite**
- Doppelklicken Sie auf **Protokollierung**, um die Protokollierungsoptionen anzuzeigen.
- Wählen Sie **Protokolldateien anzeigen** im Menü **Aktionen** aus.





## Beispielprotokollanalyse

### Normalerweise gestartete Services

#### CES Starting Up (Wie im NGINX-Protokoll zu sehen)

Aus diesem Protokoll werden nur wenige Informationen gesammelt. Die vollständige Zertifikatkette, die in den Trust Store geladen wird, ist hier zu sehen. Eine davon ist für den Webcontainer, die andere für 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 wird gestartet, wie im NGINX error.log dargestellt.

Die Anmeldung mit der Zertifikatsvorlagenkonfiguration und den Zertifikatsanmeldeinformationen wird im Ausschnitt hier angezeigt:

```

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

```

Der Abruf der Zertifizierungsstellenkette der Zertifizierungsstelle wird im Ausschnitt hier beobachtet:

```

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

```

Wenn die Anfrage erfolgreich war, wird die Datei certnew.p7b abgerufen. Dieselbe URL mit den Anmeldeinformationen der Vorlage kann verwendet werden, um die neue.p7b-Datei von einem Webbrowser abzurufen.

## CES wird gestartet wie in IIS-Protokollen

Dieselben Ereignisse zum Starten des CES, die im NGINX error.log aufgeführt sind, werden auch in den IIS-Protokollen beobachtet. Die IIS-Protokolle enthalten jedoch zwei weitere HTTP GET-Anforderungen, da die erste Anforderung vom Webserver durch eine 401-Antwort herausgefordert wird. und nach der Authentifizierung wird eine angeforderte Nachricht mithilfe einer 301-Antwort umgeleitet:

```

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

```

## CAPF wird gestartet, wie in den CAPF-Protokollen zu sehen ist.

Das meiste, was in den CAPF-Protokollen für das Starten von CES auftritt, ähnelt dem in den anderen Protokollen. aber der CAPF-Dienst erkennt die Methode und Konfiguration für die 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
```

Die nächste wichtige Beobachtung aus den Protokollen ist, wenn der CAPF-Dienst den EST-Client initialisiert.

```
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!!
```

## LSC-Installationsvorgang des Telefons

### CAPF-Protokolle

Es wird empfohlen, alle erforderlichen Protokolle zu sammeln und die Analyse mit einer Überprüfung der CAPF-Protokolle zu starten. So können wir die Zeitreferenz für ein bestimmtes Telefon kennen.

Der erste Teil der Signalisierung sieht genauso aus wie bei anderen CAPF-Methoden. Der EST-

Client, der im CAPF-Dienst ausgeführt wird, führt die Registrierung mit CES zum Ende des Dialogs aus (nachdem der CSR vom Telefon bereitgestellt wurde).

```
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
```

Nachdem der CES das signierte Zertifikat des Telefons abgerufen hat, wird das Zertifikat in das DER-Format konvertiert, bevor es für das Telefon bereitgestellt wird.

```
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
```

Der CAPF-Dienst übernimmt wieder und lädt den CSR von dem Ort, an den er im obigen Ausschnitt geschrieben wurde (/tmp/capf/cert/). Der CAPF-Dienst stellt dann das signierte LSC für das Telefon bereit. Gleichzeitig wird die CSR-Nummer des Telefons gelöscht.

```
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-Protokolle

Der folgende Ausschnitt zeigt die Ereignisse in den IIS-Protokollen für die LSC-Installationsschritte eines Telefons, wie oben erläutert.

```
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
```

## Häufige Probleme

Wenn auf der CES-Seite ein Fehler auftritt, wird erwartet, dass die Ausgabe wie der folgende Ausschnitt in den CAPF-Protokollen angezeigt wird. Überprüfen Sie alle anderen Protokolle, um das Problem weiter zu reduzieren.

```
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
```

## Fehlendes Zertifizierungsstellenzertifikat in der Ausstellerkette des IIS-Identitätszertifikats

Wenn ein Stammzertifikat oder ein Zwischenzertifikat, das sich in der Zertifikatkette befindet, von CES nicht vertrauenswürdig ist, wird der Fehler "Nicht in der Lage, die Zertifizierungsstellenkette von CA abzurufen" in den Nginx-Protokollen ausgegeben.

```
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
```

## Webserver, der ein selbstsigniertes Zertifikat anzeigt

Die Verwendung eines selbstsignierten Zertifikats im IIS wird nicht unterstützt und funktioniert auch dann, wenn es als CAPF-trust auf den CUCM hochgeladen wird. Der folgende Ausschnitt stammt aus den Nginx-Protokollen und zeigt an, was beobachtet wird, wenn IIS ein selbstsigniertes Zertifikat verwendet.

```
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
```

## Nicht übereinstimmend mit URL-Hostname und Common Name

Der Common Name (lab-dc) des IIS-Zertifikats stimmt nicht mit dem FQDN im URL des Webanmeldungsdiens der CA überein. Damit die Zertifikatsvalidierung den FQDN innerhalb der URL ablöst, muss dieser dem Common Name des Zertifikats entsprechen, das von der CA verwendet wird.

```
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
```

## Problem mit der DNS-Auflösung

CiscoRA kann den Hostnamen der in den Dienstparametern konfigurierten Online-CA nicht auflösen.

```
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
```

## Ausstellung mit Daten für die Gültigkeit von Zertifikaten

Wenn NTP (Network Time Protocol) nicht ordnungsgemäß funktioniert, treten Probleme mit den Gültigkeitsdaten von Zertifikaten auf. Diese Überprüfung wird vom CES beim Start durchgeführt und wird in den NGINX-Protokollen beobachtet.

```
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
```

## Falsche Konfiguration von Zertifikatsvorlagen

Ein Typo im Namen innerhalb der Dienstparameter führt zu Fehlern. In den CAPF- und NGINX-Protokollen werden keine Fehler protokolliert. Daher muss NGINX error.log überprüft werden.

```
***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
```

## Timeout für CES-Authentifizierung

Die unten aufgeführten Ausschnitte zeigen das Timeout des CES EST-Clients nach dem Standard-Timer von 10 Sekunden während des ersten certsrv-Authentifizierungsprozesses.

```
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
```

**Hinweis:** [CSCvo58656](#) und [CSCvf83629](#) beziehen sich beide auf das Zeitlimit für die CES-Authentifizierung.

## Timeout für CES-Registrierung

Zeitüberschreitung des CES EST-Clients nach erfolgreicher Authentifizierung, jedoch während des Wartens auf eine Antwort auf eine Registrierungsanfrage.

```
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
```

## Bekannte Einwände

[CSCvo28048](#) CAPF-Dienst wird nicht mehr im Menü RTMT Collect Files (RTMT-Sammeldateien) aufgeführt

[Die CSCvo58656](#) CAPF Online CA benötigt eine Option, um die maximale Verbindungszeitüberschreitung zwischen RA und CA zu konfigurieren.

[CSCvf83629](#) EST-Server erhält während der Registrierung EST\_ERR\_HTTP\_WRITE

## Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)