

# Konfiguration und Fehlerbehebung von verbundenen Clustern für ILS

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Methode 1. Verwenden der Kennwortauthentifizierung zwischen Clustern](#)

[Methode 2. Verwenden der TLS-Authentifizierung zwischen Clustern](#)

[Methode 3: Verwenden Sie TLS mit Kennwortauthentifizierung zwischen Clustern.](#)

[Methode 4: Wechseln zur TLS-Authentifizierung, nachdem der Cluster mit der Kennwortauthentifizierung verbunden ist.](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Protokollanalyse für die ILS-Registrierung für Methode 1](#)

[Spoke-Registrierungen erfolgreich über Kennwortauthentifizierung zwischen Clustern im Hub](#)

[Spoke to Tries to Register to Hub \(Zu Hub anmelden\), schlägt aber aufgrund der Nichtübereinstimmung des Kennworts fehl](#)

[Protokollanalyse für die ILS-Registrierung für Methode 2](#)

[Spoke-Registrierungen erfolgreich über TLS-Authentifizierung am Hub](#)

[Verbindung schlägt fehl, da Tomcat-Zertifikat des Hub nicht in Spoke importiert wird](#)

[Verbindung schlägt fehl, da Tomcat-Zertifikat des Spokes nicht in Hub importiert wird](#)

[Protokollanalyse für die ILS-Registrierung für Methode 3](#)

[Spoke-Registrierungen erfolgreich über TLS mit Kennwortauthentifizierung zum Hub](#)

[Verbindung schlägt fehl, da Tomcat-Zertifikat des Spokes selbst signiert ist](#)

[Verbindung schlägt fehl, da Tomcat-Zertifikat des Hub selbst signiert ist](#)

[Protokollanalyse für die ILS-Registrierung für Methode 4](#)

[Spoke Registers Successfully to the Hub, wenn Sie von der eingerichteten Verbindung zur TLS-Authentifizierung unter Verwendung der Kennwortauthentifizierung wechseln.](#)

[Die Verbindung schlägt fehl, da der Hub über ein selbst signiertes Zertifikat verfügt, wenn von der etablierten Verbindung über die Kennwortauthentifizierung auf TLS-Authentifizierung umgeschaltet wird.](#)

[Die Verbindung schlägt fehl, da Spoke über ein selbst signiertes Zertifikat verfügt, wenn von der etablierten Verbindung über die Kennwortauthentifizierung auf TLS-Authentifizierung umgeschaltet wird.](#)

## Einführung

In diesem Dokument werden die möglichen Konfigurationsmethoden zum Verbinden von Clustern

für den Intercluster Lookup Service (ILS) beschrieben. Außerdem wird eine Protokollanalyse zur Fehlerbehebung bei den einzelnen Methoden erstellt.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

### Verwendete Komponenten

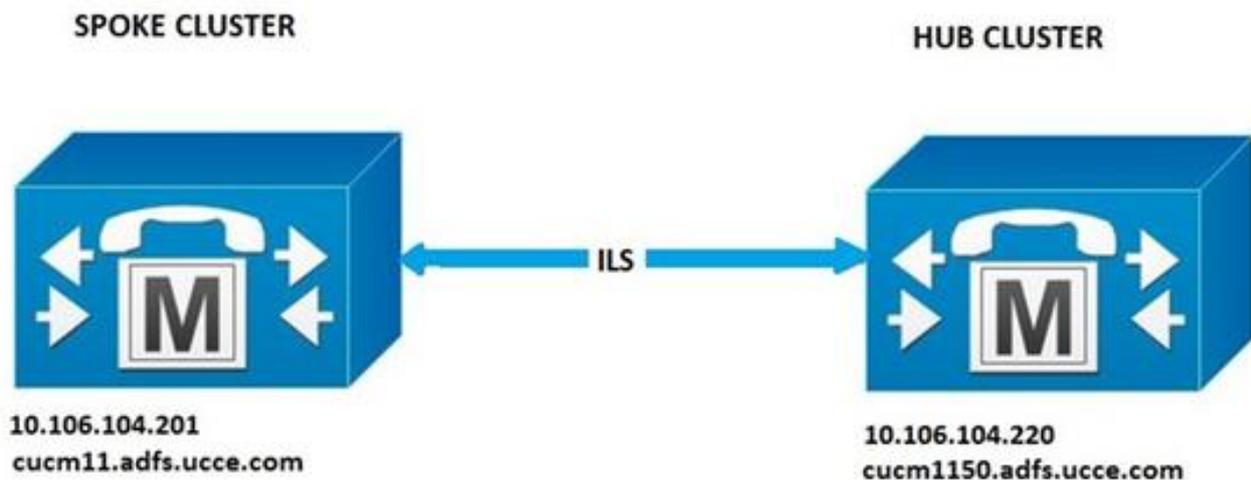
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Unified Communications Manager (CUCM) Version 11.5

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.

## Konfigurieren

### Netzwerkdiagramm



### Konfigurationen

#### Methode 1. Verwenden der Kennwortauthentifizierung zwischen Clustern

Melden Sie sich bei der CUCM-Verwaltungsseite an, und navigieren Sie zu **Erweiterte Funktionen > ILS-Konfiguration**.

Aktivieren Sie im Fenster ILS-Konfiguration das Kontrollkästchen **Kennwort verwenden**.

Verwalten Sie die Kennwörter, und klicken Sie dann auf **Speichern**. Das Kennwort muss für alle Cluster im ILS-Netzwerk identisch sein.

**ILS Authentication**

Use TLS Certificates

Use Password

Password \* [.....]

Confirm Password \* [.....]

Note: If you are using CA Signed Identified Certificates without exchanging certificates, the Password must be provisioned with "Use TLS Certificate"

## Method 2. Verwenden der TLS-Authentifizierung zwischen Clustern

Um diese Methode verwenden zu können, stellen Sie sicher, dass alle Cluster, die Teil des ILS-Netzwerks sein sollen, die entfernten Cluster Tomcat-Zertifikate in ihre tomcat-trust importiert haben.

Navigieren Sie in der CUCM-Verwaltung zu **Erweiterte Funktionen > ILS-Konfiguration**. Aktivieren Sie im Fenster ILS-Konfiguration das Kontrollkästchen **TLS-Zertifikate verwenden** unter ILS-Authentifizierung.

**ILS Authentication**

Use TLS Certificates

Use Password

Password \* [.....]

Confirm Password \* [.....]

Note: If you are using CA Signed Identified Certificates without exchanging certificates, the Password must be provisioned with "Use TLS Certificate"

## Method 3: TLS mit Kennwortauthentifizierung zwischen Clustern verwenden.

Der Vorteil dieser Methode besteht darin, dass die Tomcat-Zertifikate nicht zwischen den Clustern importiert werden müssen, um die TLS-Verbindung herzustellen, wenn sie von der External Certificate Authority (CA) signiert werden. Diese Methode ist ab CUCM 11.5 verfügbar.

Um diese Methode verwenden zu können, stellen Sie sicher, dass alle Cluster, die Teil des ILS-Netzwerks sein sollen, über die von einer externen Zertifizierungsstelle signierten Tomcat-Zertifikate verfügen und das Stammzertifikat dieser Zertifizierungsstelle in tomcat-trust vorhanden ist. Außerdem muss das Kennwort für alle Cluster im ILS-Netzwerk identisch sein.

Navigieren Sie in der CUCM-Verwaltung zu **Erweiterte Funktionen > ILS-Konfiguration** unter ILS-Authentifizierung, aktivieren Sie das Kontrollkästchen **TLS-Zertifikate verwenden** und **Kennwort verwenden**.

**ILS Authentication**

Use TLS Certificates

Use Password

Password \* [.....]

Confirm Password \* [.....]

Note: If you are using CA Signed Identified Certificates without exchanging certificates, the Password must be provisioned with "Use TLS Certificate"

## Method 4: Wechseln zur TLS-Authentifizierung, nachdem der Cluster mit der

## Kennwortauthentifizierung verbunden ist.

Dies ist eine andere Möglichkeit, TLS zu verwenden, ohne die Tomcat-Zertifikate zwischen den Clustern zu überschneiden, wenn sie von einer externen Zertifizierungsstelle signiert werden. Dies ist für CUCM-Versionen vor 11.5 nützlich, wenn Methode 3 nicht unterstützt wird.

Um diese Methode verwenden zu können, stellen Sie sicher, dass alle Cluster, die Teil des ILS-Netzwerks sein sollen, über die von einer externen Zertifizierungsstelle signierten Tomcat-Zertifikate verfügen und das Stammzertifikat dieser Zertifizierungsstelle in tomcat-trust vorhanden ist.

Treten Sie dem Cluster zuerst mit der Kennwortauthentifizierung bei. Navigieren Sie in der Cisco Unified CM-Verwaltung zu **Erweiterte Funktionen > ILS-Konfiguration**. Aktivieren Sie unter ILS-Authentifizierung das Kontrollkästchen **Kennwort verwenden**. Verwalten der Kennwörter Klicken Sie auf **Speichern**.

Das Kennwort muss beim Beitritt zum Cluster auf Client- und Serverseite identisch sein.



The screenshot shows the 'ILS Authentication' configuration window. The 'Use Password' checkbox is checked, while 'Use TLS Certificates' is unchecked. There are two password input fields, one for 'Password' and one for 'Confirm Password', both containing masked characters. A note at the bottom states: 'Note: If you are using CA Signed Identified Certificates without exchanging certificates, the Password must be provisioned with "Use TLS Certificate"'

Sobald die Verbindung hergestellt ist, ändern Sie die Authentifizierungsmethode in TLS. Navigieren Sie in der CUCM-Verwaltung zu **Erweiterte Funktionen > ILS-Konfiguration**. Aktivieren Sie im Fenster ILS-Konfiguration das Kontrollkästchen **TLS-Zertifikate verwenden** unter ILS-Authentifizierung.



The screenshot shows the 'ILS Authentication' configuration window. The 'Use TLS Certificates' checkbox is checked, while 'Use Password' is unchecked. There are two password input fields, one for 'Password' and one for 'Confirm Password', both containing masked characters. A note at the bottom states: 'Note: If you are using CA Signed Identified Certificates without exchanging certificates, the Password must be provisioned with "Use TLS Certificate"'

## Überprüfen

Die erfolgreiche Registrierung ist unter ILS-Clustern und unter Importierte globale Wählplan-Kataloge in

### Erweiterte Funktionen > ILS-Konfiguration



Cluster ID/Name	Last Contact Time	Role	Advertised Route String	Last USN Data Received	USN Data Synchronization Status	Action
2	-	Hub (Local Cluster)	cucm1150.adfs.uccoe.com	-	Up to date	Disconnect
1	8/26/16 5:06 PM	Spoke	cucm11.adfs.uccoe.com	8/26/16 5:06 PM	Up to date	Disconnect

Details des Remote-Clusters werden mit dem Befehl *run sql select \* aus remotecluster* aufgelistet.

```
admin:run sql select * from remotecluster
pkid                fullyqualifiedname  clusterid description version
-----
5edbbde9-d72b-4cd1-8f8e-93ab32cb58da cucm11.adfs.ucce.com 1                11.5.1.10000(4)
admin:
```

## Fehlerbehebung

Legen Sie für den Cisco Intercluster Lookup Service die Ablaufverfolgungsstufe für das Debuggen fest.

Ort der Spur: `activelog /cm/trace/ils/sdl/`

Die Protokollanalyse für Erfolgs- und Fehlerszenarien für jede ILS-Registrierungsmethode mit Beispiel wird erläutert.

### Protokollanalyse für die ILS-Registrierung für Methode 1

#### Spoke-Registrierungen erfolgreich über Kennwortauthentifizierung zwischen Clustern im Hub

Ausschnitt aus Hub protokollieren:

```
00154617.001 |16:58:42.888 |AppInfo |IlsD IlsHandler: Ils::wait_SdlConnectionInd(): New connection accepted. DeviceName=, TCPPIid = [1.600.13.5], IPAddr=10.106.104.201, Port=37816, Controller=[1,20,1]
```

```
00154617.002 |16:58:42.888 |AppInfo |IlsD Ils::ConnectInd TCPPIid([1, 600, 13, 5]), PeerIP/Port(10.106.104.201:37816), LocalIP/Port(10.106.104.220:7502) (10.106.104.201:37816)
```

```
00154618.012 |16:58:42.889 |AppInfo |IlsD ::ConnectIndInner Server Connection to PeerId(f7f885dcaca845f18f3b7e583ff6c457), TCPPIid([1, 600, 13, 5]), PeerIP/Port(10.106.104.201:37816), LocalIP/Port(10.106.104.220:7502) TLSReq(f) established
```

Snippet von Spoke protokollieren:

```
00145095.017 |16:58:42.878 |AppInfo |IlsD Ils::ConnectReq(): Requesting Connection to IpAddr(10.106.104.220), IpPort(7502), TLSReq(f)
```

```
00145095.018 |16:58:42.878 |AppInfo |IlsD Ils::ConnectReq() Pub IP/Port(10.106.104.220:7502) Pri IP/Port(:7502) TLSReq(false)
```

```
00145095.024 |16:58:42.879 |AppInfo |IlsD Ils::processConnectReq Initiating non-TLS Connection
```

```
00145096.001 |16:58:42.881 |AppInfo |IlsD Ils::ConnectRes() appCorr(1029) TCPPIid([1, 600, 13, 5]), PeerIP/Port(10.106.104.220:7502), LocalIP/Port(10.106.104.201:37816) TLSReq(f) found
```

```
00145096.002 |16:58:42.881 |AppInfo |IlsD DEBUG(0000FA0E): Client Connection to peerId(00000000000000000000000000000000) ipAddr(10.106.104.220) ipPort(7502) TLSReq(f) succeeded
```

```
00145097.010 |16:58:42.896 |AppInfo |IlsD ::ConnectIndInner starting to PeerId(77c59d0960cc4fdc959168a3d686a6de), TCPPIid([1, 600, 13, 5]), PeerIP/Port(10.106.104.220:7502), LocalIP/Port(10.106.104.201:37816) TLSReq(f) established
```

**Spoke to Tries to Register to Hub (Zu Hub anmelden), schlägt aber aufgrund der**

## Nichtübereinstimmung des Kennworts fehl

DecryptData ist fehlgeschlagen, und der ILSPwdAuthenticationFailed-Alarm in den Hub-Protokollen zeigt die Nichtübereinstimmung des Kennworts an.

Ausschnitt aus Hub protokollieren:

```
00155891.005 |17:25:26.197 |AppInfo |IlsD IlsHandler: wait_SdlDataInd EncrUtil::decryptData failed. DeviceName=, TCPPid = [1.600.13.7], IPAddr=10.106.104.201, Port=40592, Controller=[1,20,1]
```

```
00155891.006 |17:25:26.197 |AppInfo |IlsD wait_SdlDataInd sending ILSPwdAuthenticationFailed alarm with IPAddress= 10.106.104.201; mAlarmedConnections count= 1
```

**Hinweis:** Der Fehler ist in den anderen Methoden auch immer dann gleich, wenn die Verbindung aufgrund von Passwortfehlern nicht hergestellt werden kann.

## Protokollanalyse für die ILS-Registrierung für Methode 2

### Spoke-Registrierungen erfolgreich über TLS-Authentifizierung am Hub

Ausschnitt aus Hub protokollieren:

```
00000901.001 |15:46:27.238 |AppInfo |IlsD Ils::VerifyCertificateInfo(): peer certificates are in certificate store
```

```
00000902.008 |15:46:27.240 |AppInfo |IlsD ::ConnectIndInner Server Connection to PeerId(f7f885dcaca845f18f3b7e583ff6c457), TCPPid([1, 600, 17, 4]), PeerIP/Port(10.106.104.201:60938), LocalIP/Port(10.106.104.220:7501) TLSReq(t) established
```

Snippet von Spoke protokollieren:

```
00000646.001 |15:46:27.189 |AppInfo |IlsD Ils::VerifyCertificateInfo(): peer certificates are in certificate store
```

```
00000647.006 |15:46:27.199 |AppInfo |IlsD ::ConnectIndInner starting to PeerId(77c59d0960cc4fdc959168a3d686a6de), TCPPid([1, 600, 17, 3]), PeerIP/Port(10.106.104.220:7501), LocalIP/Port(10.106.104.201:36115) TLSReq(t) established
```

### Verbindung schlägt fehl, da Tomcat-Zertifikat des Hub nicht in Spoke importiert wird

Bei der Anmeldung von Spoke wird angezeigt, dass die Zertifikatsüberprüfung für den Hub fehlgeschlagen ist.

Snippet von Spoke protokollieren:

```
00001821.000 |16:34:01.765 |AppInfo |[1, 600, 17, 5]: HandleSSLERror - Certificate verification failed:(Verification error:18)- self signed certificate for 10.106.104.220:7501
```

```
00001822.000 |16:34:01.765 |AppInfo |[1, 600, 17, 5]: HandleSSLERror - Certificate verification failed for 10.106.104.220:7501
```

```
00001827.002 |16:34:01.766 |AppInfo |IlsD Ils::wait_SdlConnectErrRsp sending
```

ILSTLSAuthenticationFailed alarm with Cluster1 = 10.106.104.220; mAlarmedConnections count= 1

00001827.004 |16:34:01.770 |AppInfo |IlsD ERROR(000005C9): Connection to  
peerId(00000000000000000000000000000000) ipAddr(10.106.104.220) ipPort(7501) TLSReq(t) failed,  
ConnReason(1)

## Verbindung schlägt fehl, da Tomcat-Zertifikat des Spokes nicht in Hub importiert wird

Protokolle vom Hub weisen darauf hin, dass die Verbindung nicht geschlossen ist, da weder das Spoke-Zertifikat im lokalen Store noch der FQDN im Peer-Infovektor vorhanden sind.

Ausschnitt aus Hub protokollieren:

00003366.001 |17:06:30.877 |AppInfo |CertUtil Ils::isCertInLocalStore X509\_STORE\_get\_by\_subject  
failed.

00003366.002 |17:06:30.877 |AppInfo |IlsD Ils::VerifyCertificateInfo(): certificate is not in  
the local store and the FQDN (cucm11.adfs.ucce.com) is not in the peer info vector, closing the  
connection

00003366.003 |17:06:30.877 |AppInfo |IlsD Ils::VerifyCertificateInfo(): sending  
ILSTLSAuthenticationFailed alarm for Cluster1= cucm11.adfs.ucce.com; mAlarmedConnections count=  
1

00003366.004 |17:06:30.882 |AppInfo |IlsD IlsHandler: Close Req. DeviceName=, TCPPIid =  
[1.600.17.16], IPAddr=10.106.104.201, Port=39267, Controller=[1,20,1

## Protokollanalyse für die ILS-Registrierung für Methode 3

### Spoke-Registrierungen erfolgreich über TLS mit Kennwortauthentifizierung zum Hub

Ausschnitt aus Hub protokollieren:

00000211.001 |08:06:58.798 |AppInfo |CertUtil Ils::isCertInLocalStore X509\_STORE\_get\_by\_subject  
failed.

00000211.002 |08:06:58.798 |AppInfo |IlsD Ils::VerifyCertificateInfo(): peer certificates are  
not in certificate store but Root CA signed certs are uploaded locally

00000212.001 |08:06:58.803 |AppInfo |EncrUtil Function: decryptData at line 163 succeeded

00000212.002 |08:06:58.803 |AppInfo |EncrUtil Function: decryptData at line 165 succeeded

00000212.003 |08:06:58.803 |AppInfo |EncrUtil Function: decryptData at line 168 succeeded

00000212.004 |08:06:58.803 |AppInfo |EncrUtil decryptData: inlen 1956, outlen 1949 succeed

00000212.012 |08:06:58.804 |AppInfo |IlsD ::ConnectIndInner Server Connection to  
PeerId(f7f885dcaca845f18f3b7e583ff6c457), TCPPIid([1, 600, 17, 1]),  
PeerIP/Port(10.106.104.201:56181), LocalIP/Port(10.106.104.220:7501) TLSReq(t) established

Snippet von Spoke protokollieren:

00000064.000 |08:06:58.802 |SdlSig |SdlConnectRsp  
|wait |Ils(1,600,20,1)  
|SdlSSLTCPConnection(1,600,17,1) |1,600,16,1.1^\*\* |\*TraceFlagOverrode

00000064.001 |08:06:58.802 |AppInfo |CertUtil Ils::isCertInLocalStore X509\_STORE\_get\_by\_subject

failed.

```
00000064.002 |08:06:58.802 |AppInfo |IlsD Ils::VerifyCertificateInfo(): peer certificates are not in certificate store but Root CA signed certs are uploaded locally.
```

```
00000064.004 |08:06:58.802 |AppInfo |IlsD DEBUG(00000407): Client Connection to peerId(00000000000000000000000000000000) ipAddr(10.106.104.220) ipPort(7501) TLSReq(t) succeeded
```

```
00000065.010 |08:06:58.812 |AppInfo |IlsD ::ConnectIndInner starting to PeerId(77c59d0960cc4fdc959168a3d686a6de), TCPid([1, 600, 17, 1]), PeerIP/Port(10.106.104.220:7501), LocalIP/Port(10.106.104.201:56181) TLSReq(t) established
```

## Verbindung schlägt fehl, da Tomcat-Zertifikat des Spokes selbst signiert ist

Hub-Protokolle weisen auf Fehler bei der Zertifikatsüberprüfung für selbstsigniertes Zertifikat des Spokes hin.

Ausschnitt aus Hub protokollieren:

```
00000103.000 |09:44:16.896 |AppInfo |[1, 600, 17, 1]: HandleSSLError - Certificate verification failed:(Verification error:18)- self signed certificate for 10.106.104.201:52124
```

```
00000104.000 |09:44:16.896 |AppInfo |[1, 600, 17, 1]: HandleSSLError - Certificate verification failed for 10.106.104.201:52124
```

```
00000106.000 |09:44:16.896 |AppInfo |[1, 600, 17, 1]: HandleSSLError - TLS protocol error(ssl reason code=internal error [68]),lib=SSL routines [20],fun=SSL_clear [164], errno=0 for 10.106.104.201:52124
```

## Verbindung schlägt fehl, da Tomcat-Zertifikat des Hub selbst signiert ist

Die Protokolle von Spoke weisen auf einen Fehler bei der Zertifikatsüberprüfung für das selbst signierte Zertifikat des Hub hin.

Snippet von Spoke protokollieren:

```
00000064.000 |12:44:19.641 |AppInfo |[1, 600, 17, 1]: HandleSSLError - Certificate verification failed:(Verification error:18)- self signed certificate for 10.106.104.220:7501
```

```
00000065.000 |12:44:19.641 |AppInfo |[1, 600, 17, 1]: HandleSSLError - Certificate verification failed for 10.106.104.220:7501
```

```
00000067.000 |12:44:19.641 |AppInfo |[1, 600, 17, 1]: HandleSSLError - TLS protocol error(ssl reason code=bad message type [114]),lib=SSL routines [20],fun=ssl3_get_server_hello [146], errno=0 for 10.106.104.220:7501
```

**Hinweis:** Der in diesem Fall angezeigte Fehler ist auch dann gleich, wenn sowohl der Hub als auch die Spoke-Karte selbst signiert sind.

## Protokollanalyse für die ILS-Registrierung für Methode 4

Spoke Registers Successfully to the Hub, wenn Sie von der eingerichteten Verbindung zur TLS-Authentifizierung unter Verwendung der Kennwortauthentifizierung wechseln.

Der FQDN des Remote-Clusters wird im PeerInfoVector angezeigt, da die Verbindung bereits mit

der Kennwortauthentifizierungsmethode hergestellt wurde. Beim Wechsel von der Kennwortauthentifizierungsmethode zu TLS wird der Fehler "X509\_STORE\_get\_by\_subject failed" ausgegeben, da das Tomcat-Zertifikat nicht per Kreuz importiert wird. Die Verbindung wird jedoch weiterhin über TLS akzeptiert, da "FQDN ist in PeerInfoVector" vorhanden ist.

Ausschnitt aus Hub protokollieren:

```
00000169.001 |19:41:50.255 |AppInfo |CertUtil Ils::isCertInLocalStore X509_STORE_get_by_subject failed.
```

```
00000169.002 |19:41:50.255 |AppInfo |IlsD Ils::VerifyCertificateInfo(): FQDN is in PeerInfoVector
```

```
00000169.003 |19:41:50.255 |AppInfo |IlsD IlsHandler: Ils::wait_SdlConnectionInd(): New connection accepted. DeviceName=, TCPPIp = [1.600.17.1], IPAddr=10.106.104.201, Port=51887, Controller=[1,20,1]
```

Snippet von Spoke protokollieren:

```
00000072.001 |19:41:50.257 |AppInfo |CertUtil Ils::isCertInLocalStore X509_STORE_get_by_subject failed.
```

```
00000072.002 |19:41:50.257 |AppInfo |IlsD Ils::VerifyCertificateInfo(): FQDN is in PeerInfoVector
```

**Verbindung schlägt fehl, da Hub selbst signiertes Zertifikat hat, wenn auf TLS-Authentifizierung umgeschaltet wird über die festgelegte Verbindung mit der Kennwortauthentifizierung.**

Protokolle von Spoke weisen auf einen Fehler bei der Zertifikatverifizierung für das selbst signierte Zertifikat des Hub hin.

Snippet von Spoke protokollieren:

```
00000151.000 |12:29:18.600 |AppInfo |[1, 600, 17, 2]: HandleSSLERror - Certificate verification failed:(Verification error:18)- self signed certificate for 10.106.104.220:7501
```

```
00000152.000 |12:29:18.600 |AppInfo |[1, 600, 17, 2]: HandleSSLERror - Certificate verification failed for 10.106.104.220:7501
```

**Verbindung schlägt fehl, da Spoke beim Wechsel zur TLS-Authentifizierung ein selbst signiertes Zertifikat besitzt über die festgelegte Verbindung mit der Kennwortauthentifizierung.**

Hub-Protokolle weisen auf Fehler bei der Zertifikatsüberprüfung für selbstsigniertes Zertifikat des Spokes hin

Ausschnitt aus Hub protokollieren:

```
00000089.000 |09:32:27.365 |AppInfo |[1, 600, 17, 1]: HandleSSLERror - Certificate verification failed:(Verification error:18)- self signed certificate for 10.106.104.201:41295
```

```
00000090.000 |09:32:27.365 |AppInfo |[1, 600, 17, 1]: HandleSSLERror - Certificate verification failed for 10.106.104.201:41295
```