

# Fehlerbehebung bei Jabber-Anmeldeproblemen

## Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[So erfassen Sie Protokolle](#)

[Schlüsselwörter für die Suche in Protokollen](#)

[Phasen der Fehlerbehebung](#)

[Phase 1: CUCM-Serviceerkennung](#)

[Phase 2: CUCM-Benutzerauthentifizierung](#)

[Phase 3: SOAP-Anmeldung \(IM- und Presence-Anmeldung\)](#)

[Phase 4: XMPP-Anmeldung \(IM- und Presence-Anmeldung\)](#)

[Obligatorische Prüfungen](#)

[So legen Sie Protokolle auf DEBUG fest](#)

[Zu erfassende Protokolle](#)

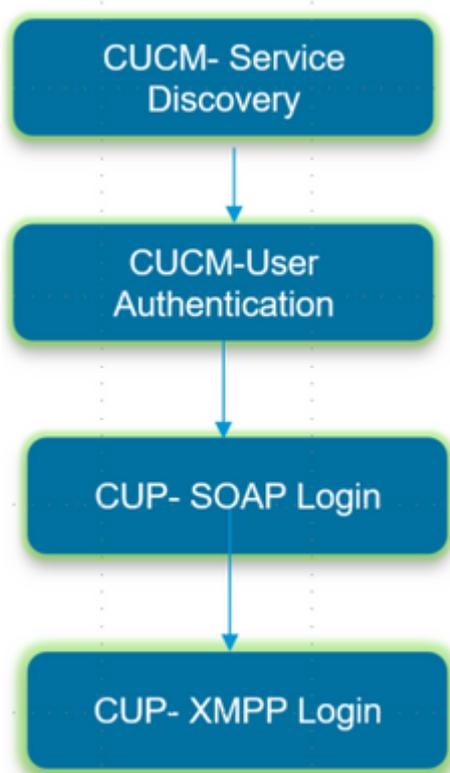
[Erfassen von Protokollen von RTMT](#)

## Einleitung

In diesem Dokument wird die Fehlerbehebung bei Jabber Log-in beschrieben, wenn dieses in einem internen oder Unternehmensnetzwerk ausfällt.

## Hintergrundinformationen

Die Anmeldung bei Jabber erfolgt in zwei Phasen: Anmeldung beim Cisco Unified Communications Manager-Server (CUCM) und Anmeldung beim IM und Presence-Server (IM&P).



- Die CUCM-Anmeldung beinhaltet eine Serviceerkennung, um den CUCM-Server zu identifizieren, bei dem sich Jabber anmelden muss.
- Jabber nutzt die Authentifizierung mit CUCM, um die Serviceprofildetails abzurufen, die den IMP-Server, Voicemail, Konferenzen, CTI-Serverdetails sowie eine Gerätekonfigurationsdatei für Telefondienste enthalten.
- Nach erfolgreicher CUCM-Anmeldung meldet sich Jabber beim IMP-Server an, um die Kontaktliste und andere IM-Dienste zu authentifizieren und abzurufen.
- Das IMP-Log-in besteht aus zwei Phasen: SOAP-Log-in, das die Benutzerauthentifizierung behandelt, und dann XMPP-Log-in, das die Erstellung von XMPP-Sitzungen und das Stream-Management behandelt.

## So erfassen Sie Protokolle

Löschen Sie den Cache auf dem PC, und sammeln Sie den sauberen Jabber-Problembenachrichtigung (PRT).

Schritt 1: Melden Sie sich ab und beenden Sie die Jabber-Anwendung.

Schritt 2: Löschen Sie alle vorhandenen Protokolle unter

```
%AppData%\Local\Cisco\Unified Communications\Jabber\  
%AppData%\Roaming\Cisco\Unified Communications\Jabber\  

```

Schritt 3: Starten Sie Jabber neu und reproduzieren Sie das Problem, indem Sie sich anmelden.

Schritt 4: Sammeln Sie den Problembenachrichtigung. (Wählen Sie im Jabber-Menü Hilfe die Option **Problem melden**, um das Problembenachrichtigungs-Tool zu starten. Die Anleitung finden Sie hier.)

Link zu diesen Ressourcen:

- [So sammeln Sie ein Jabber-Problem](#)
- [So erfassen Sie Protokolle von Expressway \(wenn Jabber über MRA läuft\)](#)

## Schlüsselwörter für die Suche in Protokollen

<#root>

```
IMPStackCap::Log in::OnLog inError  
ServiceDiscoveryHandlerResult  
@CupSoapCli: log in cup succeeds -
```

shows when the SOAP log in was successful.

```
[CTriTPConnectionClient::OnConnectSuccess] - @XmppSDK: -
```

shows when the XMPP log in was successful.

LERR -

shows the Log in Errors when the Jabber fails to log in to the IM&P Server.

# Phasen der Fehlerbehebung

## Phase 1: CUCM-Serviceerkennung

Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Cannot find your services automatically. Click advanced settings to set up manually (Ihre Services können nicht automatisch gefunden werden. Klicken Sie auf <b>Advanced Settings</b> (Erweiterte Einstellungen), um sie manuell einzurichten.)	Dieser Fehler tritt auf, wenn der SRV-Eintrag <b>_cisco-uds</b> oder <b>_cuplogin</b> nicht auf dem DNS-Server konfiguriert ist.	csf::dns::mapFromWindowsDNSResult

### Beispiel für einen Protokollausschnitt

<#root>

```
017-03-19 17:55:00,422 WARN [0x000050ac] [src\dnsutils\win32\win32DnsUtils.cpp(52)] [csf.dns] [csf::dns::mapFromWindowsDNSResult] - *-----*
```

```
DNS query _cisco-uds._tcp.applab has failed
```

```
:
```

```
DNS name does not exist. (9003).
```

```
2017-03-19 17:55:00,438 WARN [0x000050ac] [src\dnsutils\win32\win32DnsUtils.cpp(52)] [csf.dns] [csf::
```

```
DNS query _cuplogin._tcp.applab has failed
```

```
: DNS name does not exist. (9003).
```

### Schritte zur Problembhebung

Schritt 1: Starten Sie zuerst die Eingabeaufforderung (auf einem Windows-Client) und geben Sie dann **nslookup** ein.

Schritt 2: Legen Sie den Abfragetyp auf SRV fest  
**set type = SRV**

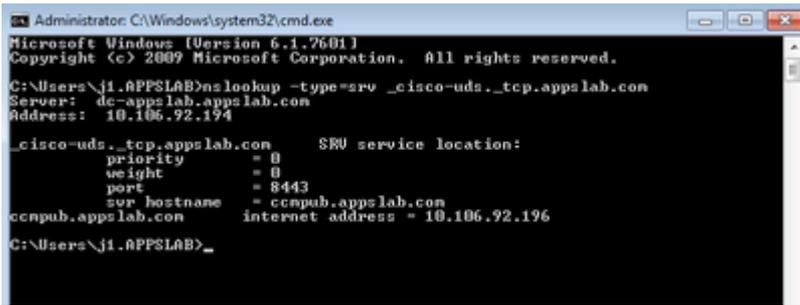
Schritt 3: SRV-Eintrag einfügen, den wir überprüfen müssen  
**\_cisco-uds.\_tcp.example.com**

Schritt 4: Dadurch werden die DNS-A-Einträge zurückgegeben, die auf die CUCM-Server verweisen.

Dies ist ein Beispiel für den SRV-Eintrag **Successful\_cisco-uds**.

Wenn keine Einträge zurückgegeben werden, wenden Sie sich an Ihren DNS-Administrator, um [SRV-](#)

[Einträge zu konfigurieren.](#)



Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Cannot find your services automatically. Click advanced settings to set up manually (Ihre Services können nicht automatisch gefunden werden. Klicken Sie auf "Advanced Settings" (Erweiterte Einstellungen), um sie manuell einzurichten.)	Dieser Fehler wird angezeigt, wenn <b>Jabber</b> die UDS- oder TFTP-Server nicht abrufen kann, um seine Anmeldeinformationen und Konfigurationseinstellungen zu erfassen.	HTTP-Antwortcode 503 für Anfrage Nr. 29 an <a href="https://cucm.domain:8443/cucm-uds/">https://cucm.domain:8443/cucm-uds/</a> HTTP-Antwortcode 503 für Anfrage Nr. 29 an <a href="https://cucm.domain:6972/">https://cucm.domain:6972/</a>

**Schritte zur Problembhebung**

Schritt 1: Überprüfen Sie, ob die als TFTP-Server konfigurierten CUCM-Knoten betriebsbereit sind.

Schritt 2: **Führen Sie auf allen CUCM-Knoten einen Neustart dieser Services durch.**

- Cisco TFTP
- Cisco UDS-Service

**Phase 2: CUCM-Benutzerauthentifizierung**

Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Ihr Benutzername oder Kennwort ist falsch.	Dieser Fehler tritt auf, wenn die eingegebenen Anmeldeinformationen falsch sind oder der Benutzer in CUCM/LDAP gesperrt ist.	"FAILED_UCM90_AUTHENTICATION"

**Beispiel für einen Protokollausschnitt**

<#root>

2017-01-09 08:59:10.652 INFO [0x00001740] [vices\impl\DiscoveryHandlerImpl.cpp(460)] [service-discovery] [CSFUnified::DiscoveryHandlerImpl::ev

FAILED\_UCM90\_AUTHENTICATION

## Schritte zur Problembhebung

Schritt 1: Stellen Sie sicher, dass der Benutzer in CUCM als **Endbenutzer** konfiguriert ist. Navigieren Sie zur Seite **CUCM Administration > End-user** (CUCM-Administration > Endbenutzer).

Schritt 2: Überprüfen Sie, ob die Anmeldeinformationen korrekt sind und der Benutzer aktiv ist. Melden Sie sich beim CUCM-Selbsthilfeportal an.

Dieses Bild bezieht sich auf ein Szenario, in dem LDAP den Benutzer nicht authentifizieren kann, weil entweder der Benutzer kein gültiger Benutzer ist oder das angegebene Kennwort falsch ist.



Schritt 3: Wenn dieses Problem bei allen Benutzern auftritt, überprüfen Sie, ob die Einstellungen für die LDAP-Synchronisierung und die LDAP-Authentifizierung unter **CUCM Administration > System > LDAP** korrekt sind.

**Tipp:** Stellen Sie aus Sicht des LDAP-Servers sicher, dass das **Konto nicht gesperrt ist**, dass die **Kennwörter nicht abgelaufen sind** und dass alle **Benutzer mit dem CUCM-Server synchronisiert sind**.

Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Kommunikation mit dem Server nicht möglich	Jabber kann den bei der Serviceerkennung empfangenen CUCM-FQDN/HOSTNAME nicht auflösen/erreichen.	â€žFAILED_UCM90_CONNECTIONâ€œ

## Beispiel für einen Protokollauschnitt

```
<#root>
```

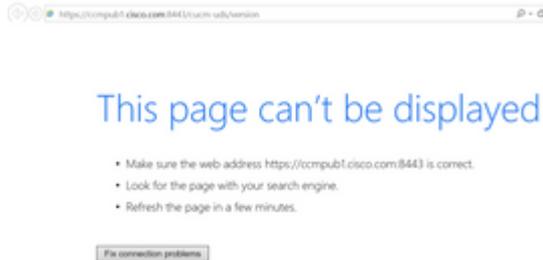
```
2017-08-28 12:04:00,282 INFO [0x00004290] [vices\impl\DiscoveryHandlerImpl.cpp(452)] [service-discovery] [CSFUnified::DiscoveryHandlerImpl::ev
```

```
FAILED_UCM90_CONNECTION
```

## Schritte zur Problembhebung

Schritt 1: Testen Sie, ob Sie diese URL im Browser auf dem PC öffnen können: <https://<CUCM IP/FQDN>:8443/cucm-uds/version>

### Fehlgeschlagen



### Erfolgreich



Schritt 2: Wenn die Antwort nicht erfolgreich ist, überprüfen Sie, ob der DNS für die Auflösung richtig konfiguriert ist und ob Netzwerkelemente wie Firewall/ASA den Port 8443 blockieren.

Schritt 3: Diese URL muss für alle CUCM-Server im Cluster getestet werden. Eine Liste der Server finden Sie unter **CUCM Administration > System > Server**.

Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Kommunikation mit dem Server nicht möglich	Dieser Fehler tritt auf, wenn die in Jabber eingegebene Benutzer-ID nicht mit der in CUCM konfigurierten Benutzer-ID übereinstimmt.	â€žFAILED_USER_LOOKUPâ€œ

### Beispiel für einen Protokollauschnitt

<#root>

2016-08-18 13:14:49,943 INFO [0x000036e4] [vices\impl\DiscoveryHandlerImpl.cpp(367)] [service-discovery] [DiscoveryHandlerImpl::evaluateService

FAILED\_USER\_LOOKUP

## Schritte zur Problembhebung

Schritt 1: Vergewissern Sie sich, dass Sie diese URL im Browser des PCs öffnen können:  
<https://CUCM:8443/cucm-uds/clusterUser?username=<userid>>

Schritt 2: Überprüfen Sie, ob die in Jabber eingegebene Benutzer-ID mit der Benutzer-ID auf der CUCM-Endbenutzerseite übereinstimmt.

---

**Tip:** Bei Jabber ist die UPN-Erkennung standardmäßig aktiviert, und die **Benutzer-ID** wird daher aus dem LDAP-UPN-Feld übernommen. Überprüfen Sie, ob UPN mit der Konfiguration in CUCM übereinstimmt. Wenn Sie die UPN-Erkennung deaktivieren müssen, **stellen Sie** UPN\_DISCOVERY\_ENABLED=false während der [Installation ein](#).

---

### Phase 3: SOAP-Anmeldung (IM- und Presence-Anmeldung)

Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Ihr Benutzername oder Kennwort ist falsch.	Dieser Fehler wird durch einen Fehler bei der Benutzerauthentifizierung verursacht.	â€žLERR_CUP_AUTHâ€œ

#### Beispiel für einen Protokollausschnitt

<#root>

```
2017-01-14 15:55:09,615 INFO [0x00000dc0] [ts\adapters\imp\components>Login.cpp(99)] [imp.service] [IMPStackCap::Login::OnLoginError] - *****
2017-01-14 15:55:09,615 INFO [0x00000dc0] [s\adapters\imp\components>Login.cpp(100)] [imp.service] [IMPStackCap::Login::OnLoginError] - OnLog
```

LERR\_CUP\_AUTH <12>:

```
201-01-14 15:55:09,615 INFO [0x00000dc0] [s\adapters\imp\components>Login.cpp(101)] [imp.service] [IMPS
```

#### Schritte zur Problembhebung

Schritt 1: Vergewissern Sie sich, dass der Benutzer einem Presence-Knoten zugewiesen ist und keine Duplikate für den Benutzer vorhanden sind (**IM und Presence-Administration > Diagnostics > System troubleshooter**).

Schritt 2: Vergewissern Sie sich, dass der Hochverfügbarkeitsstatus Normal lautet und kein Failover stattgefunden hat.

Wenn Sie versucht haben, den Benutzer während eines abnormalen HA-Zustands zuzuweisen, werden die Benutzer keinem IMP-Knoten zugewiesen, und die Anmeldung schlägt fehl.

Stellen Sie zunächst den HA-Status wieder her, und weisen Sie den Benutzer neu zu.

Schritt 3: Überprüfen Sie die Gültigkeit der Anmeldeinformationen.

1. Im Falle eines LDAP-Benutzers: Überprüfen Sie, ob sich der Benutzer beim CUCM-Selbsthilfeportal anmelden kann.

2. Wenn die Anmeldung auf der **ccmenduser**-Seite fehlschlägt, überprüfen Sie die LDAP-Authentifizierungseinstellungen in CUCM, und vergewissern Sie sich, dass dieselben Einstellungen auf IMP repliziert werden.

**Führen Sie über ldapauthentication den Befehl `sql select *` aus.  
Führen Sie über ldapauthenticationhost den Befehl `sql select *` aus.**

3. Vergewissern Sie sich, dass das Konto nicht in LDAP gesperrt ist.
4. Wenn der Benutzer kürzlich für Presence aktiviert wurde, starten Sie den Cisco Sync-Agent-Service auf IMP Publisher neu.

Schritt 4: Überprüfen Sie, ob der Server eine hohe TOMCAT-CPU-Auslastung hat.

- **show process load**
- **utils diagnose test**

Schritt 5: Legen Sie für diese Services das Protokoll DEBUG fest, reproduzieren Sie das Anmeldeproblem, und erfassen Sie die Protokolle.

- Client Profile Agent
- Cisco Tomcat
- Ereignisanzeige `“Anwendungsprotokoll`
- Ereignisanzeige `“Systemprotokoll`

Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Ungültige Anmeldeinformationen	Dieser Fehler wird verursacht, wenn der Benutzer nicht aktiv ist oder sich in der Datenbank befindet.	<code>LERR_CUP_AUTH &lt;10&gt;</code>

### Beispiel für einen Protokollausschnitt

```
[IMPServices] [CSFUnified::IMPStackCap::Log in::OnLog inError] - *****
[IMPServices] [CSFUnified::IMPStackCap::Log in::OnLog inError] - OnLog inError: LERR_CUP_AUTH <10>:
[IMPServices] [CSFUnified::IMPStackCap::Log in::OnLog inError] - *****
[http-bio-443-exec-15] handlers.Log inHandlerAbstract - preLog in:PRELOGIN reasoncode=FAILURE. User eith
```

---

**Tip:** Für diesen Fehler wird außerdem empfohlen, die Cisco Tomcat-Protokolle von den CUCM- und IM&P-Servern abzurufen.

---

Aus den Cisco Tomcat-Protokollen

<#root>

```
2019-10-27 18:33:40,373 DEBUG [http-bio-443-exec-5] impl.LDAPHostnameVerifier - check : inside check with
2019-10-27 18:33:40,373 DEBUG [http-bio-443-exec-5] impl.Certificates - getCNs :
```

```

2019-10-27 18:33:40,373 DEBUG [http-bio-443-exec-5] impl.LDAPHostnameVerifier - check : cns = [ldap.cisco.com]
2019-10-27 18:33:40,373 DEBUG [http-bio-443-exec-5] impl.Certificates - getDNSSubjectAlts :
2019-10-27 18:33:40,374 DEBUG [http-bio-443-exec-5] impl.LDAPHostnameVerifier - check : subjectAlts = [
2019-10-27 18:33:40,374 ERROR [http-bio-443-exec-5] impl.AuthenticationLDAP - verifyHostName:Exception: java.lang.IllegalArgumentException: Invalid DN: ldap.cisco.com
2019-10-27 18:33:40,374 DEBUG [http-bio-443-exec-5] impl.AuthenticationLDAP - value of hostnameverified: ldap.cisco.com
2019-10-27 18:33:40,374 INFO [http-bio-443-exec-5] impl.AuthenticationLDAP - verifyHostName: Closing LDAP connection

```

## Schritte zur Problembhebung

Wenn in den Cisco Tomcat-Protokollen kein Zertifikatfehler angezeigt wird, ist in zwei Fällen eine Validierung erforderlich.

Schritt 1: Validieren Sie, ob der Benutzer einem IM&P-Server zugeordnet ist.

- Navigieren Sie zu **Webseite [CUCM-Administration](#) > User Management > Assign Presence Users** (Benutzerverwaltung > Anwesende Benutzer zuweisen) > Suchen Sie nach der **Benutzer-ID** und klicken Sie auf **Find** (Suchen).

Schritt 2: Wenn der Benutzer einem IM&P-Server zugeordnet ist, wird er vom Home Node-Cluster abgemeldet.

- Navigieren Sie zu **Webseite [CUCM-Administration](#) > User Management > End User (Benutzerverwaltung > Endbenutzer)** > Suchen Sie nach dem **Endbenutzer** und **klicken Sie auf Find (Suchen)** > **Deaktivieren Sie unter Service Settings (Serviceeinstellungen) das Kontrollkästchen Home Cluster** > **Klicken Sie auf Save (Speichern)** > **Aktivieren Sie das Kontrollkästchen Home Cluster und klicken Sie auf Save (Speichern).**

Führen Sie die folgenden Schritte aus, wenn in den Cisco Tomcat-Protokollen der Fehler aus dem zuvor angezeigten Snippet angezeigt wird:

Schritt 1: Bestätigen Sie, ob Cisco Jabber für die Verwendung von Secure LDAP konfiguriert ist.

Schritt 2: Wenn Secure LDAP verwendet wird, bestätigen Sie die zugehörigen Zertifikatsinformationen wie den vollqualifizierten Domain-Namen (Fully Qualified Domain Name, FQDN), den Hostnamen und den allgemeinen Namen (Common Name, CN).

Schritt 3: Validieren Sie die Konfiguration von CUCM und IM&P, falls mit IP-Adresse oder FQDN, und vergleichen Sie diese mit den Informationen im Zertifikat.

- Navigieren Sie zu **Webseite [CUCM-Administration](#) > System > Server (System > Server).**

Schritt 4: Wenn die Server mit IP-Adresse konfiguriert sind und die LDAP-Zertifikate mit FQDN konfiguriert sind, muss der nächste Befehl auf allen CUCM- und IM&P-Knoten ausgeführt werden.

- **utils ldap config ipaddr**
- Alternativ muss die Definition der Server als FQDN geändert werden. Weitere Informationen finden Sie unter. [Ändern der CUCM-Serverdefinition von IP-Adresse oder Hostname in FQDN-Leitfaden](#)

Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Kommunikation mit dem Server nicht	Dieser Fehler wird durch Probleme mit der IMDB- oder	â€ŽLERR_CUP_UNREACHABLEâ€œ , â€ŽLERR_CUP_TIMEOUTâ€œ

möglich	TCP-Verbindung zu IMP verursacht.	
---------	-----------------------------------	--

## Beispiel für einen Protokollausschnitt

```
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(127)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLog
2017-11-08 16:03:20,051 INFO [0x00003a0c] [s\adapters\imp\components\Login.cpp(128)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLogin
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(129)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLog
```

## Schritte zur Problembhebung

Schritt 1: Stellen Sie sicher, dass IMP-FQDN-/Hostnamen vom Client-PC aufgelöst werden können.

Schritt 2: Vergewissern Sie sich, dass Sie diese URL im Browser öffnen können: **https://<IMP SERVER FQDN/IP>:8443/EPASSoap/service/v105**

## Erfolgreich

This XML file does not appear to have any style information associated with it. The document tree is shown below.

<error>This is a SOAP service. Send a POST request!</error>

## Fehlgeschlagen



Schritt 3: Vergewissern Sie sich, dass keine Firewall/kein VPN die Verbindung zum IMP-Server (Port 8443, 5222) blockiert.

Schritt 4: Überprüfen Sie, ob dieser Service auf dem IMP-Server ausgeführt wird: Cisco Client Profile Agent

Schritt 5: Wenn die obigen Schritte das Problem nicht beheben, legen Sie für diese Services das Protokoll DEBUG fest, reproduzieren Sie das Anmeldeproblem und erfassen Sie die Protokolle.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP-Authentifizierungsservice
- Client Profile Agent

---

**Tip:** Wenn das Problem bei nur einem Benutzer weiterhin besteht, heben Sie die Zuweisung auf, und weisen Sie den Benutzer erneut zu, damit er in CUCM präsent ist. Wenn es sich um ein systemweites Problem handelt, sammeln Sie die Protokolle, und überprüfen Sie den Status der Services.

---

Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Kommunikation mit dem Server nicht möglich	In der Regel wird dieser Fehler durch Probleme mit IMDB verursacht.	â€žLERR_CUP_INTERNAL_ERRORâ€œ

### Beispiel für einen Protokollausschnitt

```
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(127)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLog
2017-11-08 16:03:20,051 INFO [0x00003a0c] [s\adapters\imp\components\Login.cpp(128)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLogin
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(129)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLog
```

### Schritte zur Problembhebung

Schritt 1: Führen Sie die [obligatorischen Prüfungen durch](#).

Schritt 2: Stellen Sie sicher, dass diese Services auf dem IM&P-Server ausgeführt werden.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP-Authentifizierungsservice
- Cisco Anmeldungsdatenspeicher

Schritt 3: Überprüfen Sie, ob dieser Problemhinweis zutreffend ist.

### Problemhinweis: FN - 64267 - Cisco Unified Communications Manager IM & Presence verursacht Cisco Jabber-Anmeldefehler - Software-Upgrade empfohlen

Schritt 4: Wenn die obigen Schritte das Problem nicht beheben, legen Sie für diese Services das Protokoll DEBUG fest, reproduzieren Sie das Anmeldeproblem und erfassen Sie die Protokolle.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP-Authentifizierungsservice
- Client Profile Agent
- Cisco Anmeldungsdatenspeicher
- Ereignisanzeige â€œ Anwendungsprotokoll
- Ereignisanzeige â€œ Systemprotokoll

Schritt 5: Starten Sie das Cluster neu, um die Situation wiederherzustellen.

### Phase 4: XMPP-Anmeldung (IM- und Presence-Anmeldung)

Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Kommunikation mit dem Server nicht möglich	Wird häufig angezeigt, wenn Jabber keine Verbindung über MRA und keine TLS-Sitzung mit dem IM&P herstellen kann	LERR_JABBER_AUTH <14>: Authentifizierungsfehler beim Server, z. B. Ressourcenbindung, TLS, Sitzungserstellung oder SASL-Fehler

## Beispiel für einen Protokollausschnitt

```
2019-05-03 15:19:32,225 DEBUG [0x0000000109732f80] [s/adapters/imp/components/Log in.cpp(128)] [IMP Servi
2019-05-03 15:19:32,225 INFO [0x0000000109732f80] [s/adapters/imp/components/Log in.cpp(129)] [IMP Servi
2019-05-03 15:19:32,225 DEBUG [0x0000000109732f80] [s/adapters/imp/components/Log in.cpp(130)] [IMP Servi
```

## Schritte zur Problembhebung

Schritt 1: Stellen Sie sicher, dass der Port 5222 zwischen den IM&P-Servern und den Expressways geöffnet ist.

Schritt 2: Stellen Sie sicher, dass diese Dienste auf dem IM&P-Server ausgeführt werden, und starten Sie sie einmal neu.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP-Authentifizierungsservice

Schritt 3: Deaktivieren Sie die Hochverfügbarkeit aus den CUCM Presence Redundancy Groups.

Schritt 4: Starten Sie den **Cisco XCP Router-Service** auf allen IM&P-Knoten neu, zuerst mit dem IM&P-Publisher und dann mit den Abonnenten.

- **utils service restart Cisco XCP Router Service**

Schritt 5: Aktivieren Sie die Hochverfügbarkeit über die CUCM Presence Redundancy Groups erneut.

Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Kommunikation mit dem Server nicht möglich	Wird häufig angezeigt, wenn Jabber keine Sitzung erstellen und sich nicht im IMP-Server binden kann.	LERR_JABBER_AUTH <17>: Authentifizierungsfehler beim Server, z. B. Ressourcenbindung, TLS, Sitzung erstellen oder SASL-Fehler"

## Beispiel für einen Protokollausschnitt

```
2017-10-27 10:56:47,396 DEBUG [0x00007fff8b3d7340] [s/adapters/imp/components/Login.cpp(127)] [IMP Services] [OnLoginError] - *****
2017-10-27 10:56:47,396 INFO [0x00007fff8b3d7340] [s/adapters/imp/components/Login.cpp(128)] [IMP Services] [OnLoginError] - OnLoginError: LEI
2017-10-27 10:56:47,396 DEBUG [0x00007fff8b3d7340] [s/adapters/imp/components/Login.cpp(129)] [IMP Services] [OnLoginError] - *****
```

## Schritte zur Problembhebung

Schritt 1: Überprüfen Sie, ob die cup-xmpp-Zertifikate gültig sind.

Schritt 2: Stellen Sie sicher, dass Port 5222 offen ist.

Schritt 3: Setzen Sie diese Dienste auf DEBUG, erstellen Sie das Problem mit der Anmeldung neu, und

sammeln Sie die Protokolle vor Schritt 4.

Wenn die Ursache als Neustart des Servers identifiziert werden, ist die einzige bekannte Lösung.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP-Authentifizierungsservice
- Client Profile Agent
- Ereignisanzeige â€œ Anwendungsprotokoll
- Ereignisanzeige â€œ Systemprotokoll

Schritt 4: Starten Sie den Server neu, um das Problem zu beheben.

Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Kommunikation mit dem Server nicht möglich	Tritt auf, wenn IMP aufgrund von Netzwerkproblemen wie der Firewall nicht auflösbar oder erreichbar ist.	â€œLERR_JABBER_UNREACHABLEâ€œ

### Beispiel für einen Protokollausschnitt

```
2014-12-15 12:07:31,600 INFO [0x00001670] [ts\adapters\imp\components>Login.cpp(96)] [imp.service] [IMPStackCap::Login::OnLoginError] - *****
2014-12-15 12:07:31,600 INFO [0x00001670] [ts\adapters\imp\components>Login.cpp(97)] [imp.service] [IMPStackCap::Login::OnLoginError] - OnLog
2014-12-15 12:07:31,600 INFO [0x00001670] [ts\adapters\imp\components>Login.cpp(98)] [imp.service] [IMPStackCap::Login::OnLoginError] - *****
```

### Schritte zur Problembhebung

Schritt 1: Überprüfen Sie, ob IMP-FQDN/Hostnamen aufgelöst werden können.

Schritt 2: Vergewissern Sie sich, dass keine Firewall/kein VPN die Verbindung zum IMP-Server (Port 8443, 5222) blockiert.

Schritt 3: Vergewissern Sie sich, dass diese Services auf dem IM&P-Server ausgeführt werden, und starten Sie sie einmal neu.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP-Authentifizierungsservice

Schritt 4: Führen Sie die [obligatorischen Prüfungen](#) durch.

Schritt 5: Wenn die obigen Schritte das Problem nicht beheben, legen Sie für diese Services das Protokoll DEBUG fest, reproduzieren Sie das Anmeldeproblem und erfassen Sie die Protokolle.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP-Authentifizierungsservice
- Client Profile Agent
- Ereignisanzeige â€œ Anwendungsprotokoll

- Ereignisanzeige â€œ Systemprotokoll

Schritt 6: Wenn bei allen Benutzern derselbe Fehler auftritt, kann für eine schnelle Wiederherstellung ein Serverneustart durchgeführt werden.

Fehler auf dem Bildschirm	Ursache	Was sollten Sie im Jabber-Protokoll überprüfen?
Anmeldung in Ihrem Konto nicht möglich. Wenden Sie sich an den Administrator.	Wird häufig angezeigt, wenn sich Jabber mit SSO entweder lokal oder über Expressways (Mobile Remote Access, MRA) anmeldet.	"Log inError to ErrorCode: 27 mapped to: UnknownLog inError"

### Beispiel für einen Protokollauschnitt

```
2020-03-12 19:55:01,283 DEBUG [0x000000010b71d800][apters/imp/components/Log inUtils.cpp(96)][IMPService
2020-03-12 19:55:01,283 DEBUG [0x000000010b71d800][listeners/Log inEventListenerImpl.cpp(148)][IMPService
2020-03-12 19:55:01,283 INFO [0x000000016b61f000][ers/imp/lifecycle/Log inExecutor.cpp(314)][IMPService
2020-03-12 19:55:01,478 INFO [0x000000010b71d800][pp/tahi/tahi/ui/log in/YLCLog inBaseVC.m(500)][UI.Action
```

### Schritte zur Problembhebung

Schritt 1: Validieren Sie, ob der Benutzer dem IM&P zugewiesen ist.

Schritt 2: Überprüfen Sie, ob die Zertifikate korrekt zwischen den Knoten und dem Jabber ausgetauscht wurden.

Schritt 3: Validieren Sie, ob die OAuth-Signatur- und Verschlüsselungsschlüssel auf allen Knoten korrekt konfiguriert sind. [Weitere Informationen finden Sie in diesem Dokument im Abschnitt â€žÜberprüfenâ€œ.](#)

Schritt 4: Führen Sie die [obligatorischen Prüfungen](#) durch.

Schritt 5: Wenn die obigen Schritte das Problem nicht beheben, legen Sie für diese Services das Protokoll DEBUG fest, reproduzieren Sie das Anmeldeproblem und erfassen Sie die Protokolle.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP-Authentifizierungsservice
- Client Profile Agent
- Ereignisanzeige â€œ Anwendungsprotokoll
- Ereignisanzeige â€œ Systemprotokoll
- Cisco SSO
- Cisco Tomcat
- Cisco Tomcat-Sicherheit

## Obligatorische Prüfungen

Schritt 1: Vergewissern Sie sich, dass der Benutzer einem Presence-Knoten zugewiesen ist (navigieren Sie zu **IM und Presence-Administration > System > Topologie**) und dass keine Duplikate für den Benutzer vorhanden sind (navigieren Sie zu **IM und Presence-Administration > Diagnostics > System**

## Troubleshooter)

Schritt 2: Wenn Hochverfügbarkeit aktiviert ist, navigieren Sie zu **CUCM Administration > Server > Presence Redundancy Group** (CUCM-Administration > Server > Presence Redundancy Group) und überprüfen Sie, ob diese den **Status "Normal"** aufweisen. Hier sehen Sie, wie der normale Status aussieht. Weitere Informationen zur Hochverfügbarkeit finden Sie [hier](#).

### Anormaler Status

High Availability				
<input checked="" type="checkbox"/> Enable High Availability				
Monitored Server	Assigned Users	Active Users	Server State	
192.168.100.95	0	0	Running in Backup Mode	
192.168.100.96	0	0	Failed Over	

**Hinweis:** Diese Dienste werden vom Jabber zur Anmeldung verwendet: Cisco Tomcat, Cisco Tomcat Security, Cisco Client Profile Agent, Cisco XCP Connection Manager, Cisco XCP Router und Cisco XCP Authentication.

### Normaler Status

High Availability				
<input checked="" type="checkbox"/> Enable High Availability				
Monitored Server	Assigned Users	Active Users	Server State	
192.168.100.95	0	0	Normal	
192.168.100.96	0	0	Normal	

Schritt 3: Überprüfen Sie den Status der Hochverfügbarkeitsreplikation.

#### a.utils dbreplication runtimestate

```
DB Version: ccm10_5_1_13900_2
Repltimeout set to: 300s
PROCESS option set to: 1

Cluster Detailed View from IMPSUB-1051SU3 (2 Servers):

SERVER-NAME          IP ADDRESS          PING          DB/RPC/          REPL.          Replication
-----            -
IMPPUB-1051SU3      192.168.100.85      6.163         Y/Y/Y            0              (g_4)
IMPSUB-1051SU3      192.168.100.86      0.025         Y/Y/Y            0              (g_5)
```

Wenn bei der Datenbankreplikation Probleme auftreten, [navigieren Sie zu diesem Link](#).

#### b.run pe sql ttlogin select count(\*) from typesysreplication

```

admin:run pe sql ttlogin select count(*) from typesysreplication
sqlRv(t) sqlstmt(select count(*) from typesysreplication;)
***result set start***
count(0), success(t)
***result set end***

```

### Oder utils imdb\_Replication status (10.5.2 SU2a und höher)

```

admin:utils imdb_replication status
Running IMDB DSN (ttsoft, ttlogin, ttreg) replication checks on all nodes in cluster
NOTE: For diagnostic test to run, ports 6603, 6604 & 6605 must be open on any fire

Sub Cluster Name / Id :: galacticRepublic / 1000
  Checking connectivity & removing old data prior to running diagnostic
  Cisco Presence Datastore Replication
    10.3.85.23 -> 10.3.85.24      Passed
    10.3.85.24 -> 10.3.85.23      Passed
  Cisco Login Datastore Replication
    10.3.85.23 -> 10.3.85.24      Passed
    10.3.85.24 -> 10.3.85.23      Passed
  Cisco SIP Registration Datastore Replication
    10.3.85.23 -> 10.3.85.24      Passed
    10.3.85.24 -> 10.3.85.23      Passed

Sub Cluster Name / Id :: rebelAllianceCluster / 3000
  rebelAllianceCluster has a single node, IMDB replication not required

SUCCESS :: IMDB DSN Replication is correctly configured across cluster
Log file for the test can be gathered as follows:
  file get activelog epas/trace/imdb/sdi/imdb_state-20210705-1851.log
admin:

```

Die drei Datenspeicher müssen **PASSED** anzeigen und der Befehl muss auf allen IM&P-Knoten ausgeführt werden, da manchmal auf einem Knoten bei der Replikation sämtlicher Datenspeicher **Passed** angezeigt wird, auf einem anderen Knoten jedoch **â€žFailedâ€œ** angezeigt wird.

Wenn die IMDB-Replikation (In-Memory-Datenbank) nicht korrekt ist, kann dies bedeuten, dass sich einige oder alle Benutzer nicht anmelden können oder ihr Anwesenheitsstatus nicht korrekt angezeigt werden kann.

Die Schritte zum Beheben der IMDB-Replikationsprobleme lauten wie folgt:

Schritt 1: Deaktivieren Sie die Hochverfügbarkeit für das betroffene IM&P-Subcluster.

Schritt 2: Stoppen Sie die Cisco Presence Engine auf allen Knoten.

**utils service stop *Cisco Presence Engine***

Schritt 3: Vergewissern Sie sich, dass alle Datenspeicher-Services ausgeführt werden: Cisco Log in Datastore, Cisco Route Datastore, Cisco Presence Datastore, Cisco SIP Registration Datastore.

**utils service list**

Schritt 4: Starten Sie Cisco Config Agent auf jedem Knoten einzeln neu.

## utils service restart Cisco Config Agent

Schritt 5: Starten Sie die Cisco Presence Engine.

## utils service start Cisco Presence Engine

Schritt 6: Aktivieren Sie Hochverfügbarkeit für das Subcluster.

## So legen Sie Protokolle auf DEBUG fest

Schritt 1: Wählen Sie **Navigation > Unified serviceability > Trace > Configuration** (Navigation > Unified Serviceability > Verfolgung) aus.

Schritt 2 Wählen Sie in der Dropdown-Liste Server den Server (d. h. den IMP-Knoten) aus, auf dem der Dienst zum Konfigurieren der Ablaufverfolgung ausgeführt wird, und klicken Sie auf **Go (Los)**.

Schritt 3 Wählen Sie aus dem Dropdown-Listenfeld "Service Group" (Servicegruppe) die Servicegruppe aus, für die die Ablaufverfolgung konfiguriert werden soll, und klicken Sie dann auf **Go**.

Schritt 4 Wählen Sie aus dem Dropdown-Listenfeld "Service" den Service aus, für den Sie die Ablaufverfolgung konfigurieren möchten, und klicken Sie dann auf **Go**.

Schritt 5: Aktivieren Sie das Kontrollkästchen **Apply to All Nodes** (Auf alle Knoten anwenden) und wählen Sie als Verfolgungsstufe **DEBUG** aus.

Schritt 6: Um die Konfiguration der Verfolgungsparameter zu speichern, klicken Sie auf die Schaltfläche **Save** (Speichern).

Weitere Informationen zum Festlegen von Verfolgungsstufen finden Sie im [Cisco Unified Serviceability-Administrationshandbuch](#).

Hilfreiche Videos:

- [Erfassen von Protokollen von RTMT](#)

**Trace Configuration**

Save Set Default

**Status:**  
Ready

**Select Server, Service Group and Service**

Server\* 192.168.100.85--CUCM IM and Presence Go

Service Group\* IM and Presence Services Go

Service\* Cisco XCP Connection Manager (Active) Go

Apply to All Nodes

Trace On

**Trace Filter Settings**

Debug Trace Level Debug

Enable All Trace

**Trace Output Settings**

Maximum No. of Files\* 250

Maximum File Size (MB)\* 2

**Trace Configuration**

Save Set Default

**Status:**  
Ready

**Select Server, Service Group and Service**

Server\* 192.168.100.85--CUCM IM and Presence Go

Service Group\* IM and Presence Services Go

Service\* Cisco Client Profile Agent (Active) Go

Apply to All Nodes

Trace On

**Trace Filter Settings**

Debug Trace Level Debug

Enable All Trace

**Trace Output Settings**

Maximum No. of Files\* 250

Maximum File Size (MB)\* 1

**Trace Configuration**

Save Set Default

**Status:**  
Ready

**Select Server, Service Group and Service**

Server\* 192.168.100.85--CUCM IM and Presence Go

Service Group\* IM and Presence Services Go

Service\* Cisco Login Datastore (Active) Go

Apply to All Nodes

Trace On

**Trace Filter Settings**

Debug Trace Level Debug

Enable All Trace

**Trace Output Settings**

Maximum No. of Files\* 250

Maximum File Size (MB)\* 1

**Trace Configuration**

Save Set Default

**Status:**  
Ready

**Select Server, Service Group and Service**

Server\* 192.168.100.85--CUCM IM and Presence Go

Service Group\* IM and Presence Services Go

Service\* Cisco XCP Authentication Service (Active) Go

Apply to All Nodes

Trace On

**Trace Filter Settings**

Debug Trace Level Debug

Enable All Trace

**Trace Output Settings**

Maximum No. of Files\* 250

Maximum File Size (MB)\* 2

**Trace Configuration**

Save Set Default

**Status:**  
Ready

**Select Server, Service Group and Service**

Server\* 192.168.100.85--CUCM IM and Presence Go

Service Group\* IM and Presence Services Go

Service\* Cisco XCP Router (Active) Go

Apply to All Nodes

Trace On

**Trace Filter Settings**

Debug Trace Level Debug

Enable All Trace

**Trace Output Settings**

Maximum No. of Files\* 250

Maximum File Size (MB)\* 2

## Zu erfassende Protokolle

RTMT	Admin-CLI
Cisco Client Profile Agent	file get activelog tomcat/logs/epassoap/log4j/*
Cisco Anmeldungsdatenspeicher	file get activelog epas/trace/imdb/sdi/ttlog in/
Cisco Tomcat-Sicherheitsprotokolle	file get activelog tomcat/logs/security/log4j/*
Cisco XCP-Authentifizierungsservice	file get activelog epas/trace/xcp/log/auth*
Cisco XCP Connection Manager	file get activelog epas/trace/xcp/log/client-cm-1*.log
Cisco XCP Router	file get activelog epas/trace/xcp/log/rtr-jsm-1
Ereignisanzeige â€œ Anwendungsprotokoll	file get activelog syslog/CiscoSyslog*
Ereignisanzeige â€œ Systemprotokoll	file get activelog syslog/messages*

## Erfassen von Protokollen von RTMT

# Real Time Monitoring Tool For Cisco Unified Communications Solutions

**System**

- System Summary
  - System Summary
- Server
  - CPU and Memory
  - Process
  - Disk Usage
  - Critical Services
- Performance
  - Performance
  - Performance Log Viewer
- Tools
  - Alert Control
  - Trace & Log Central**
  - Job Status
  - SysLog Viewer
  - VLT
  - AuditLog Viewer

**Trace & Log Central**

- Trace & Log Central
  - Remote Browse
  - Collect Files**
  - Query Wizard
  - Schedule Collection
  - Local Browse
  - Real Time Trace
    - Collect Crash Dump
    - Collect Install Logs
    - Audit Logs

## Collect Files

Select System Services/Applications  Select all Services on all

Name	All Servers
Cisco Role-based Security	<input type="checkbox"/>
Cisco Row Information Spooling	<input type="checkbox"/>
Cisco SOAP Web Service	<input type="checkbox"/>
Cisco SOAPMessage Service	<input type="checkbox"/>
Cisco SSO	<input type="checkbox"/>
Cisco Serviceability Reporter	<input type="checkbox"/>
Cisco Serviceability Reporter AlertReport	<input type="checkbox"/>
Cisco Serviceability Reporter CallActivitiesR...	<input type="checkbox"/>
Cisco Serviceability Reporter DeviceReport	<input type="checkbox"/>
Cisco Serviceability Reporter PRRReport	<input type="checkbox"/>
Cisco Serviceability Reporter ServerReport	<input type="checkbox"/>
Cisco Serviceability Reporter ServiceReport	<input type="checkbox"/>
Cisco Stored Procedure Trace	<input type="checkbox"/>
Cisco Syslog Agent	<input type="checkbox"/>
Cisco Tomcat	<input type="checkbox"/>
<b>Cisco Tomcat Security Logs</b>	<input checked="" type="checkbox"/>
Cisco Tomcat Stats Servlet	<input type="checkbox"/>
Cisco Trace Collection Service	<input type="checkbox"/>
Cisco Unified OS Admin Web Service	<input type="checkbox"/>
Cisco Unified OS Platform API	<input type="checkbox"/>
Cisco Unified Reporting Web Service	<input type="checkbox"/>
Cisco WebDialerRedirector Web Service	<input type="checkbox"/>
Cron Logs	<input type="checkbox"/>
Event Viewer-Application Log	<input type="checkbox"/>
Event Viewer-System Log	<input type="checkbox"/>
FIPS Logs	<input type="checkbox"/>

< Back   Next >   Finish

Voice/Video

AnalysisManager

IM and Presence

Trace&LogCentral

**System**

System Summary

- System Summary

Server

- CPU and Memory
- Process
- Disk Usage
- Critical Services

Performance

- Performance
- Performance Log Viewer

Tools

- Alert Central
- Trace & Log Central**
- Job Status
- SysLog Viewer
- VLT
- AuditLog Viewer

---

**Voice/Video**

**AnalysisManager**

**IM and Presence**

---

**Trace & Log Central**

- Trace & Log Central
  - Remote Browse
  - Collect Files**
  - Query Wizard
  - Schedule Collector
  - Local Browse
  - Real Time Trace
  - Collect Crash Dump
  - Collect Install Logs
  - Audit Logs

---

**Collect Files**

Select IM\_AND\_PRESENCE Services/Applications

Select all Services on all Servers

Name	All Servers
Cisco AXL Web Service	<input type="checkbox"/>
Cisco Bulk Provisioning Service	<input type="checkbox"/>
<b>Cisco Client Profile Agent</b>	<input checked="" type="checkbox"/>
Cisco Config Agent	<input type="checkbox"/>
Cisco IM and Presence Admin	<input type="checkbox"/>
Cisco IM and Presence Data Monitor	<input type="checkbox"/>
Cisco Intercluster Sync Agent	<input type="checkbox"/>
<b>Cisco Login Datastore</b>	<input checked="" type="checkbox"/>
Cisco OAM Agent	<input type="checkbox"/>
Cisco Presence Datastore	<input type="checkbox"/>
Cisco Presence Engine	<input type="checkbox"/>
Cisco RCC Device Selection Service	<input type="checkbox"/>
Cisco Route Datastore	<input type="checkbox"/>
Cisco SIP Proxy	<input type="checkbox"/>
Cisco SIP Registration Datastore	<input type="checkbox"/>
Cisco Server Recovery Manager	<input type="checkbox"/>
Cisco Sync Agent	<input type="checkbox"/>
<b>Cisco XCP Authentication Service</b>	<input checked="" type="checkbox"/>
Cisco XCP Config Manager	<input type="checkbox"/>
<b>Cisco XCP Connection Manager</b>	<input checked="" type="checkbox"/>
Cisco XCP Directory Service	<input type="checkbox"/>
Cisco XCP File Transfer Manager	<input type="checkbox"/>
Cisco XCP Message Archiver	<input type="checkbox"/>
<b>Cisco XCP Router</b>	<input checked="" type="checkbox"/>
Cisco XCP SIP Federation Connection Man...	<input type="checkbox"/>
Cisco XCP Text Conference Manager	<input type="checkbox"/>

< Back    **Next >**    Finish

---

Trace&LogCentral

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.