

Fehlerbehebung bei Lizenz-Synchronisierung auf dem Catalyst SD-WAN Manager im standortbasierten Berichtsmodus

Inhalt

[Einleitung](#)

[Anforderungen](#)

[Fehler](#)

[Ansatz zur Fehlerbehebung](#)

[Probleumgehung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie einen Fehler beheben, der beim Synchronisieren der Lizenz für den Catalyst SD-WAN Manager im standortbasierten Berichtsmodus aufgetreten ist.

Anforderungen

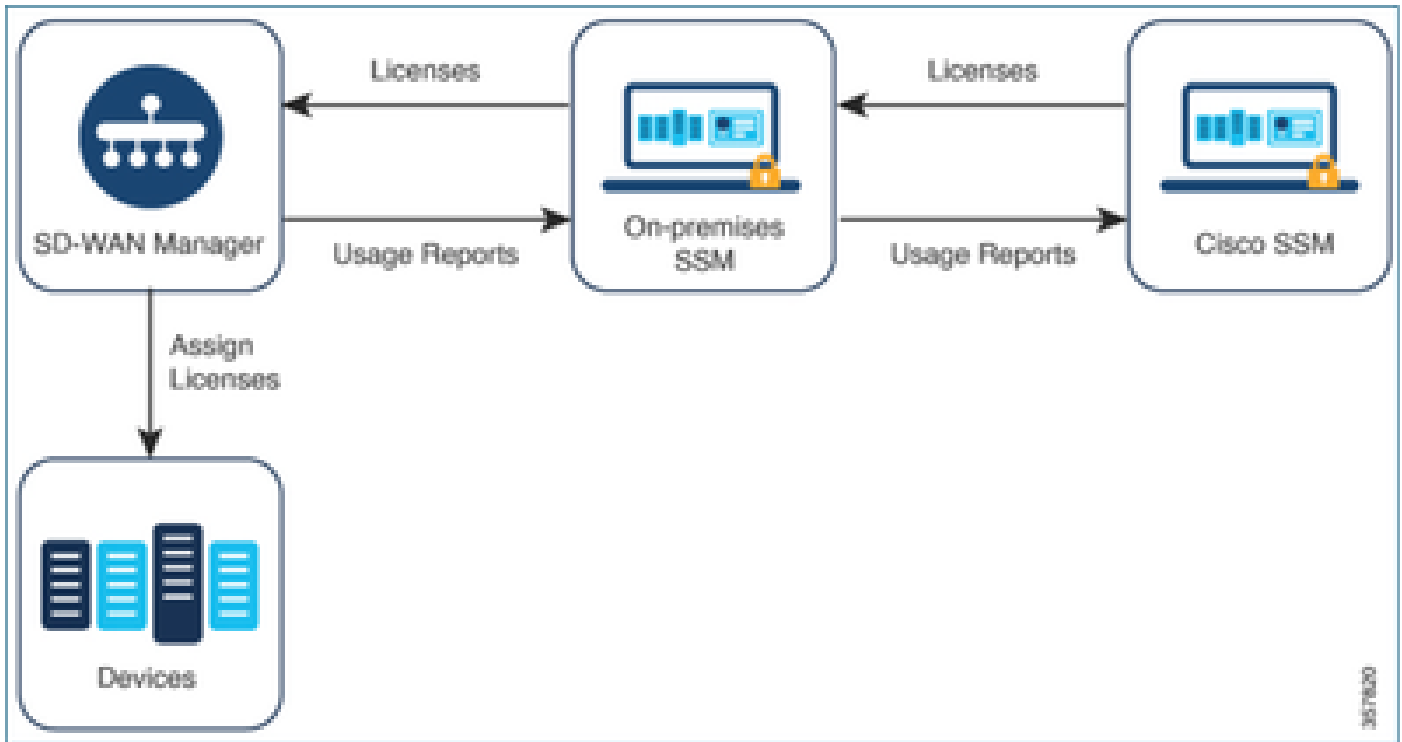
In Szenarien, in denen der Catalyst SD-WAN Manager nicht direkt mit dem Internet verbunden ist, kann die Verwendung eines Proxyserver den Zugriff auf internetbasierte Services wie Cisco SSM oder ein lokales SSM am Standort ermöglichen.

Mindestversion: Catalyst SD-WAN Manager Version 20.9.1

Cisco Smart Software Manager vor Ort (SSM vor Ort) ist eine Cisco Smart Licensing-Lösung, mit der Sie Lizenzen von einem Server an Ihrem Standort aus verwalten können, anstatt eine direkte Verbindung zu Cisco SSM herstellen zu müssen. Die Lösung umfasst die Einrichtung eines Cisco SSM-On-Prem-Lizenzservers, der seine Lizenzdatenbank regelmäßig mit Cisco SSM synchronisiert und im lokalen Betrieb ähnlich wie Cisco SSM funktioniert.

Der Catalyst SD-WAN Manager unterstützt die Verwaltung von Lizenzen über einen Cisco SSM Server vor Ort im so genannten On-Prem-Modus. Der standortbasierte Modus ist für Unternehmen nützlich, die Cisco SSM vor Ort verwenden, um eine strenge Sicherheitsrichtlinie einzuhalten, die es Netzwerkgeräten nicht erlaubt, über eine direkte Internetverbindung mit Cisco SSM zu kommunizieren.

Im standortbasierten Modus synchronisiert der Catalyst SD-WAN Manager alle 24 Stunden die Lizenzinformationen mit dem standortbasierten Cisco SSM-Lizenzserver. Während dieser Synchronisierung erhält der Catalyst SD-WAN Manager alle Aktualisierungen für verfügbare Lizenzen und sendet Berichte zur Lizenznutzung an den lokalen Cisco SSM-Lizenzserver. Sie können die Lizenzen jederzeit synchronisieren.



Vorteile von Cisco Smart Software Manager vor Ort

Unternehmen, deren Sicherheitsrichtlinien oder andere Umstände erfordern, dass der Catalyst SD-WAN Manager nicht mit dem Internet verbunden ist, haben zwei Optionen für die Verwaltung von Lizenzen für Smart License Using Policy:

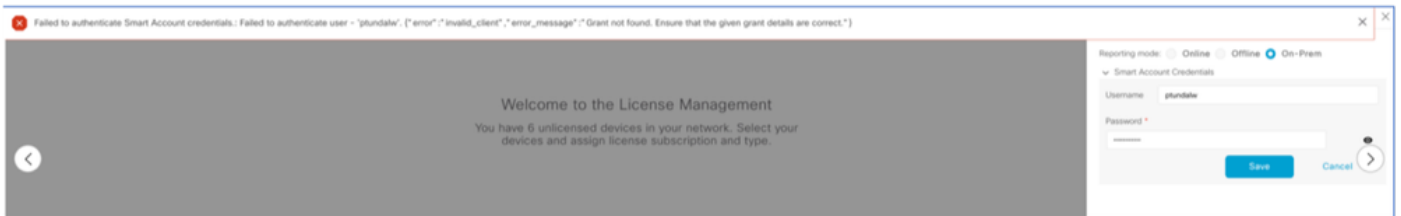
- Offline-Modus verwenden, bei dem Dateien manuell zwischen Catalyst SD-WAN Manager und Cisco SSM übertragen werden müssen
- Verwenden Sie einen Cisco SSM-Server vor Ort, der über eine LAN-Verbindung mit dem Catalyst SD-WAN Manager zugänglich ist.

Beide Methoden dienen der Übertragung von Lizenzinformationen zwischen Cisco SSM und Catalyst SD-WAN Manager. Wo immer der standortbasierte Modus verwendet werden kann, bietet dieser Modus den entscheidenden Vorteil, dass der Wartungsaufwand für die manuelle Übertragung von Dateien zwischen Catalyst SD-WAN Manager und Cisco SSM reduziert wird, wie dies für den Offline-Modus erforderlich ist.

Fehler

Beim Synchronisieren der Smart-Anmeldedaten der Benutzeroberfläche des Catalyst SD-WAN Manager wird folgender Fehler angezeigt:

```
Failed to authenticate Smart Account credentials.: Failed to authenticate user - 'admin'. {"error": "inv
```



Ansatz zur Fehlerbehebung

- vManage muss sich in Code 20.9.1 oder höher befinden.
- Überprüfen Sie die Protokolle auf dem Catalyst SD-WAN-Manager (vmanage-server.logs), während Sie die Smart Account-Anmeldedaten im Abschnitt zum Catalyst SD-WAN-Manager-Lizenzmanagement eingeben.
- Stellen Sie sicher, dass die richtige Client-ID und der vom lokalen SSM-Team freigegebene geheime Schlüssel vorhanden sind.
- TCPDUMP auf dem vManage für CSSM Server-IP
- Vergewissern Sie sich, dass DNS auf dem Catalyst SD-WAN Manager richtig konfiguriert ist und einen Ping an cloudsso.cisco.com senden kann.
- Beziehen Sie das SSM-Team vor Ort ein, und fordern Sie das SSM-Team an, das Debugging am Ende des lokalen Servers durchzuführen.

Catalyst SD-WAN Manager IP: 10.66.76.81 / 192.168.10.1

CSSM-Server-IP: 10.106.66.55

TCPDump auf dem vManage für SSM-Server-IP:

```
um8_vManage# tcpdump vpn 0 interface eth0 options "host 10.106.66.55 -nn -vv"
```

```
tcpdump -p -i eth0 -s 128 host 10.106.66.55 -nn -vv in VPN 0
```

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 128 bytes
```

```
12:15:06.407513 IP (tos 0x0, ttl 64, id 24618, offset 0, flags [DF], proto TCP (6), length 52)
```

```
192.168.10.1.57886 > 10.106.66.55.8443: Flags [S], cksum 0xfadb (incorrect -> 0xdf91), seq 74638621
```

```
12:15:06.651698 IP (tos 0x20, ttl 44, id 0, offset 0, flags [DF], proto TCP (6), length 52)
```

```
10.106.66.55.8443 > 192.168.10.1.57886: Flags [S.], cksum 0x1b34 (correct), seq 2758352947, ack 746
```

```
12:15:06.651768 IP (tos 0x0, ttl 64, id 24619, offset 0, flags [DF], proto TCP (6), length 40)
```

```
192.168.10.1.57886 > 10.106.66.55.8443: Flags [.], cksum 0xfacf (incorrect -> 0xcce1), seq 1, ack 1
```

```
12:15:06.654592 IP (tos 0x0, ttl 64, id 24620, offset 0, flags [DF], proto TCP (6), length 212)
```

```
192.168.10.1.57886 > 10.106.66.55.8443: Flags [P.], seq 1:173, ack 1, win 229, length 172
```

```
12:15:06.899695 IP (tos 0x0, ttl 41, id 44470, offset 0, flags [DF], proto TCP (6), length 40)
```

```
10.106.66.55.8443 > 192.168.10.1.57886: Flags [.], cksum 0xcc2d (correct), seq 1, ack 173, win 237,
```

```
12:15:06.911484 IP (tos 0x0, ttl 41, id 44471, offset 0, flags [DF], proto TCP (6), length 1420)
    10.106.66.55.8443 > 192.168.10.1.57886: Flags [.], seq 1:1381, ack 173, win 237, length 1380
12:15:06.911542 IP (tos 0x0, ttl 41, id 44472, offset 0, flags [DF], proto TCP (6), length 254)
    10.106.66.55.8443 > 192.168.10.1.57886: Flags [P.], seq 1381:1595, ack 173, win 237, length 214
12:15:06.911573 IP (tos 0x0, ttl 64, id 24621, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.10.1.57886 > 10.106.66.55.8443: Flags [.], cksum 0xfacf (incorrect -> 0xc6bb), seq 173, ack
12:15:06.911598 IP (tos 0x0, ttl 64, id 24622, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.10.1.57886 > 10.106.66.55.8443: Flags [.], cksum 0xfacf (incorrect -> 0xc5cf), seq 173, ack
12:15:06.923929 IP (tos 0x0, ttl 64, id 24623, offset 0, flags [DF], proto TCP (6), length 234)
    192.168.10.1.57886 > 10.106.66.55.8443: Flags [P.], seq 173:367, ack 1595, win 273, length 194
```

Protokolle des lokalen Servers:

```
[root@SSM-On-Prem log]# tail -f messages
Jan 13 11:13:36 SSM-On-Prem chronyd[1319]: Source 172.20.226.229https://172.20.226.229 replaced with 17
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 1:M 13 Jan 2023 11:14:09.049 * 100 changes in 300 seconds. Sa
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 1:M 13 Jan 2023 11:14:09.050 * Background saving started by p
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 4617:C 13 Jan 2023 11:14:09.052 * DB saved on disk
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 4617:C 13 Jan 2023 11:14:09.053 * RDB: 0 MB of memory used by
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 1:M 13 Jan 2023 11:14:09.150 * Background saving terminated w
Jan 13 11:14:46 SSM-On-Prem 1a1fca641d0a: Redis#exists(key) will return an Integer in redis-rb 4.3. exi
Jan 13 11:14:46 SSM-On-Prem 1a1fca641d0a: [active_model_serializers] Rendered UserSerializer with Activ
Jan 13 11:14:46 SSM-On-Prem 1a1fca641d0a: method=GET path=/sessions/get_user format=json controller=Ses
Jan 13 11:14:46 SSM-On-Prem 504f06c0d581: 10.110.35.124https://10.110.35.124 - - [13/Jan/2023:11:14:46
Jan 13 11:17:01 SSM-On-Prem 504f06c0d581: 2023/07/13 11:17:01 [error] 47#47: *1576 connect() failed (11
Jan 13 11:17:01 SSM-On-Prem 504f06c0d581: 2023/07/13 11:17:01 [warn] 47#47: *1576 upstream server tempo
Jan 13 11:17:01 SSM-On-Prem 1a1fca641d0a: [active_model_serializers] Rendered ActiveModel::Serializer::
Jan 13 11:17:01 SSM-On-Prem 1a1fca641d0a: method=POST path=/oauth/token format=json controller=Doorkeep
Jan 13 11:17:01 SSM-On-Prem 504f06c0d581: 10.66.76.85https://10.66.76.85 - - [13/Jan/2023:11:17:01 +000
Jan 13 11:17:14 SSM-On-Prem 1a1fca641d0a: [INFO] Session expiring outcome=success
```

Meldet sich bei vManage an, während Smart Accounts-Details im vManage License Management-Abschnitt gespeichert werden:

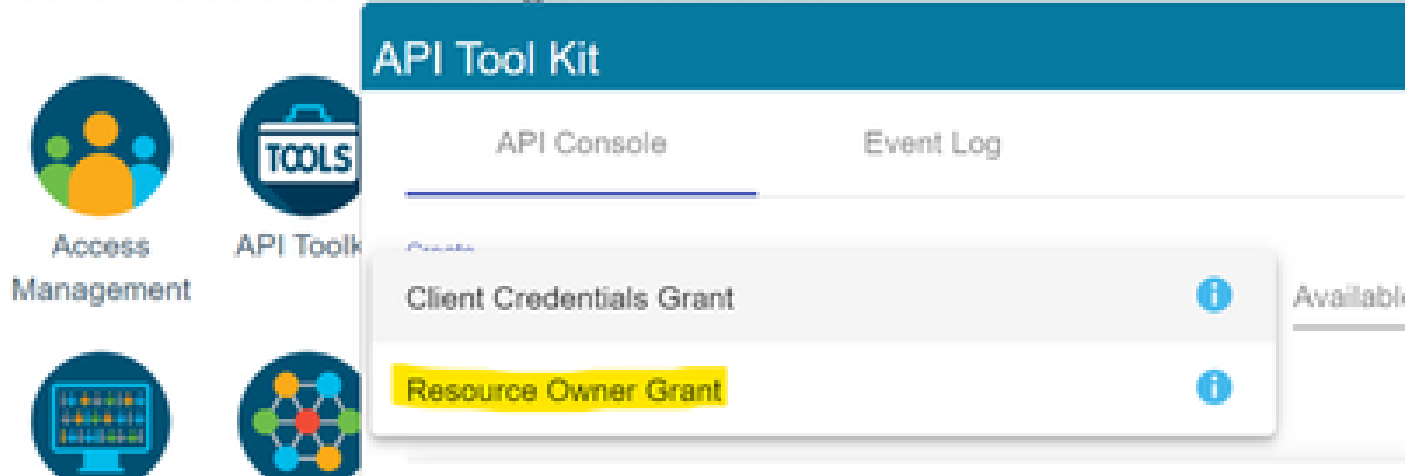
```
13-Jan-2023 17:29:02,775 IST INFO [um8_vManage] [SmartLicensingIntegrationManager] (default task-24) |
13-Jan-2023 17:29:02,776 IST INFO [um8_vManage] [SmartLicensingIntegrationManager] (default task-24) |
13-Jan-2023 17:29:02,780 IST INFO [um8_vManage] [AbstractSettingsManager] (default task-24) |default|
13-Jan-2023 17:29:02,781 IST INFO [um8_vManage] [SmartLicensingUtil] (default task-24) |default| initia
13-Jan-2023 17:29:02,781 IST INFO [um8_vManage] [SmartLicensingUtil] (default task-24) |default| Getti
13-Jan-2023 17:29:02,793 IST INFO [um8_vManage] [RestAPIClient] (default task-24) |default| RestAPI pro
13-Jan-2023 17:29:02,793 IST INFO [um8_vManage] [RestAPIClient] (default task-24) |default| RestAPI pro
13-Jan-2023 17:29:02,798 IST INFO [um8_vManage] [SmartLicensingUtil] (default task-24) |default| URL b
13-Jan-2023 17:29:02,798 IST INFO [um8_vManage] [SmartLicensingUtil] (default task-24) |default| Query
13-Jan-2023 17:29:03,490 IST ERROR [um8_vManage] [RestAPIClient] (default task-24) |default| Failed to
13-Jan-2023 17:29:03,491 IST ERROR [um8_vManage] [SmartLicensingUtil] (default task-24) |default| Failed
13-Jan-2023 17:29:03,491 IST ERROR [um8_vManage] [SmartLicensingIntegrationRestfulResource] (default ta
```

Hinweis: Beim Synchronisieren des Smart Accounts aus der vManage-GUI wird der Fehler 403 angezeigt. Dieser weist darauf hin, dass der Server die Anforderung versteht, sich jedoch weigert, sie zu autorisieren.

Problemumgehung

1. Melden Sie sich am lokalen Server an.
2. Navigieren Sie zum API-Toolkit.
3. Wählen Sie "Ressourceneigentümer gewähren", geben Sie die Details als Name ein und speichern.

Smart Software Manager On-Prem



The screenshot shows the 'API Tool Kit' interface. On the left, there are four icons: 'Access Management' (a group of people), 'API Tool Kit' (a toolbox), 'Access Management' (a computer monitor), and 'API Tool Kit' (a network diagram). The main area is titled 'API Tool Kit' and has two tabs: 'API Console' (selected) and 'Event Log'. Below the tabs, there is a list of grants. The 'Resource Owner Grant' is highlighted in yellow. To the right of the list, there is a 'Available' label.

Resource Owner Grant

Name *

Test5

Description


Expiration Date

Client ID *

z92Dss3_SVnlhUXURJV97gdf03ukxSE5_shD3vB7tllyl2YKAaJkGh8nbYSRWYCzN

Client Secret *

.....

 Regenerate Client Secret

Save

Cancel

4. Wählen Sie den gespeicherten Datensatz aus (siehe vorherigen Schnappschuss) und aktivieren Sie Client ID und Client Secret.

API Console Enabled 

Create

Available Actions

Search by Name

Showing All Records

<input type="checkbox"/>	Name	Creation Date	Type	Description	Client ID
<input type="checkbox"/>	Test5	Aug 04 2023	Resource Owner Grant		z92Dss3_SVnIhUXJ...

5. Geben Sie die freigegebene Client-ID und den Client-Schlüssel im Catalyst SD-WAN Manager-Portal ein.
6. Gehen Sie zu "Sync Licenses and Refresh Devices" in vManage, und verwenden Sie die gleichen Anmeldeinformationen vor Ort, mit denen Sie sich angemeldet haben, um Client-ID und Client-Schlüssel zu generieren.

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.