

# オンプレミスのレポートモードを使用した Catalyst SD-WAN Managerでのライセンス同期のトラブルシューティング

## 内容

---

[はじめに](#)

[要件](#)

[エラー](#)

[トラブルシューティング手順](#)

[回避策](#)

---

## はじめに

このドキュメントでは、オンプレミスレポートモードでCatalyst SD-WAN Manager(CSM)のライセンスを同期しているときに発生するエラーのトラブルシューティング方法について説明します。

## 要件

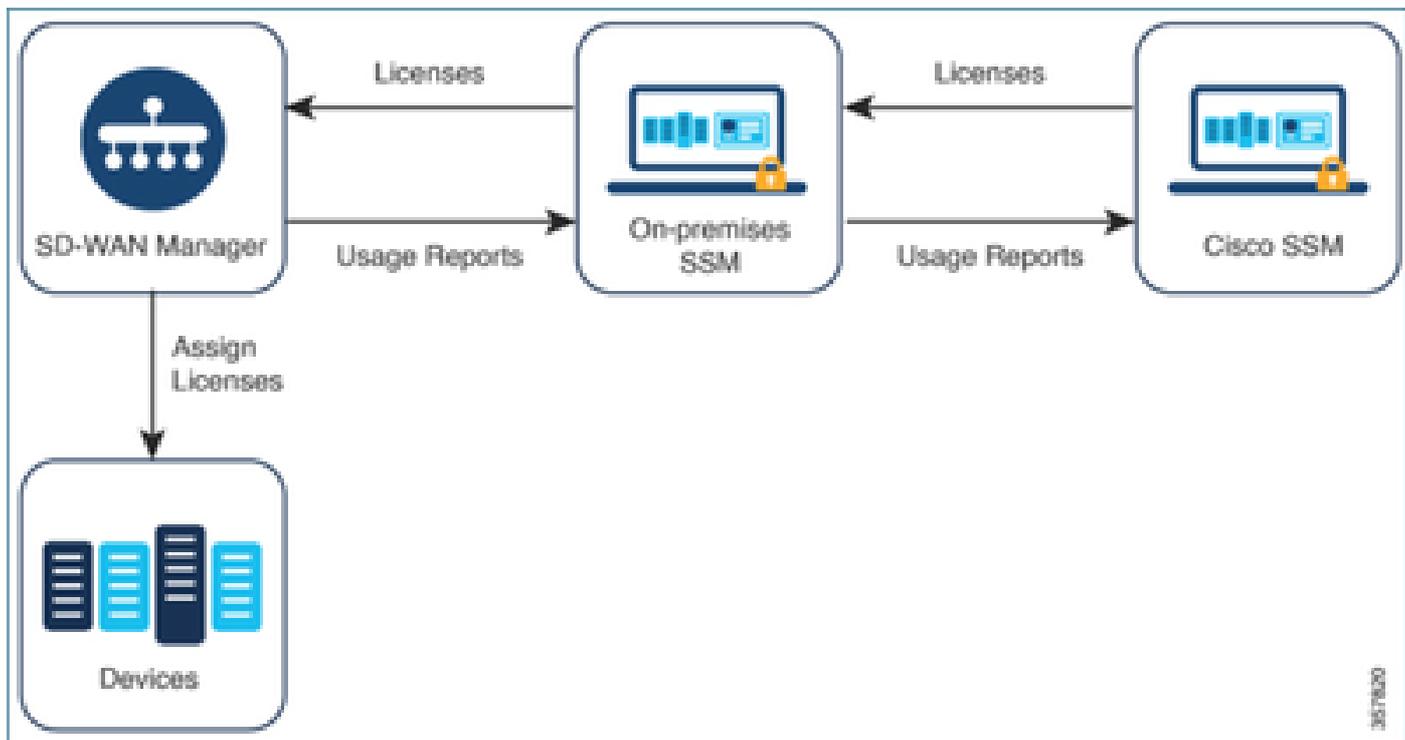
Catalyst SD-WAN Managerがインターネットに直接接続されていないシナリオでは、プロキシサーバーを使用して、Cisco SSMなどのインターネットベースのサービスやローカルのオンプレミスSSMへのアクセスを提供できます。

最小リリース：Catalyst SD-WAN Managerリリース20.9.1

Cisco Smart Software Manager on-prem(SSM on-prem)は、Cisco Smart Licensingソリューションです。Cisco SSMに直接接続しなくても、オンプレミスのサーバからライセンスを管理できます。このソリューションには、Cisco SSMオンプレミスライセンスサーバのセットアップが含まれます。このサーバは、ローカルで動作している間に、ライセンスデータベースをCisco SSMと定期的に同期させ、Cisco SSMと同様に機能します。

Catalyst SD-WAN Managerは、オンプレミスと呼ばれるモードを使用して、Cisco SSMオンプレミスサーバを使用したライセンス管理をサポートします。オンプレミスモードは、ネットワークデバイスがインターネットへの直接接続によってCisco SSMと通信することを許可しない厳格なセキュリティポリシーに対応するためにCisco SSMをオンプレミスで使用する組織に役立ちます。

Catalyst SD-WAN Managerをオンプレミスモードで稼働させると、24時間ごとにライセンス情報がCisco SSMオンプレミスライセンスサーバと同期されます。この同期の間、Catalyst SD-WAN Managerは使用可能なライセンスの更新を受信し、ライセンス使用状況レポートをCisco SSMオンプレミスライセンスサーバに送信します。ライセンスはいつでも同期できます。



## Cisco Smart Software Managerをオンプレミスで使用する利点

セキュリティポリシーやその他の状況により、Catalyst SD-WAN Managerをインターネットに接続しないようにする必要がある組織では、ポリシーを使用してスマートライセンスのライセンスを管理する方法が2つあります。

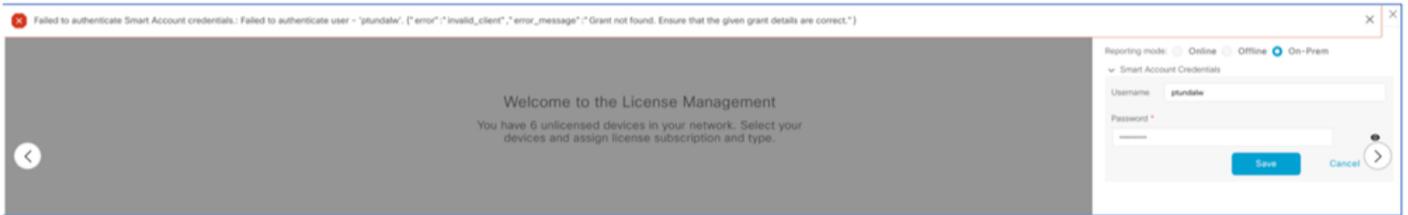
- オフラインモードを使用します。このモードでは、Catalyst SD-WAN ManagerとCisco SSMの間でファイルを手動で転送する必要があります。
- ローカルエリア接続を介してCatalyst SD-WAN Managerにアクセス可能なCisco SSMオンプレミスサーバを使用します。

これらの方法は両方とも、Cisco SSMとCatalyst SD-WAN Managerの間でライセンス情報を転送する必要性に対処するものです。オンプレミスモードを使用できる場合は常に、このモードを使用すると、オフラインモードで必要なCatalyst SD-WAN ManagerとCisco SSMの間でのファイルの手動転送によるメンテナンスオーバーヘッドを削減できるという大きなメリットがあります。

## エラー

Catalyst SD-WAN Manager GUIからスマートクレデンシャルを同期しているときに、次のエラーが表示されます。

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



## トラブルシューティング手順

- vManageはコード20.9.1以降である必要があります。
- Catalyst SD-WAN Manager License Managementセクションにスマートアカウント資格情報を入力しながら、Catalyst SD-WAN Manager(vmanage-server.logs)のログを確認します。
- オンプレミスのSSMチームによって共有される正しいクライアントIDと秘密キーを確認します。
- CSSMサーバIP用vManageのTCPDUMP
- Catalyst SD-WAN ManagerでDNSが正しく設定されており、cloudsso.cisco.comにpingできることを確認します。
- オンプレミスのSSMチームを関与させ、オンプレミスのサーバ側でデバッグを行うようSSMチームに要求します。

Catalyst SD-WANマネージャIP:10.66.76.81 / 192.168.10.1

CSSMサーバIP:10.106.66.55

SSMサーバIP用のvManageのTCPDump:

```
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
```

## オンプレミスのサーバログ :

```
[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
```

vManageライセンス管理セクションにスマートアカウントの詳細を入力して、vManageにログインします。

```
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 pr
13-Jan-2023 17:29:02,793 IST INFO [um8_vManage] [RestAPIClient] (default task-24) |default| RestAPI pr
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
```

注：vManage GUIからスマートアカウントを同期中にエラー403が表示されます。これは、サーバが要求を理解しているが承認を拒否していることを示します。

## 回避策

1. Prem Serverにログインします。
2. API Tool Kitに移動します。
3. 「リソース所有者権限」を選択し、詳細を名前として入力して保存します。

## Smart Software Manager On-Prem



### API Tool Kit

API Console

Event Log

Client Credentials Grant



Available

Resource Owner Grant



### Resource Owner Grant



Name \*

Test5

Description

Expiration Date

Client ID \*

z92Dss3\_SVnlhUXURJV97gdf03ukxSE5\_shD3vB7llyl2YKAaJkGh8nbYSRWYCzN

Client Secret \*

.....



Regenerate Client Secret

Save

Cancel

4. 保存したレコード（前のスナップショットで説明）を選択し、Client IDとClient Secretにチェックマークを付けます。

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. Catalyst SD-WAN Managerポータルで、共有クライアントIDとクライアントシークレットを共有して入力します。
6. vManageの「Sync Licenses and Refresh Devices」に移動し、ログインしたオンプレミスのクレデンシャルを使用して、クライアントIDとクライアントシークレットを生成します。

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。