

# Solucionar problemas de sincronização de licença no Catalyst SD-WAN Manager por meio do modo de relatório local

## Contents

---

[Introdução](#)

[Requisitos](#)

[Erro](#)

[Abordagem de solução de problemas](#)

[Solução](#)

---

## Introdução

Este documento descreve como solucionar um erro encontrado durante a sincronização da licença no Catalyst SD-WAN Manager através do modo de relatório local.

## Requisitos

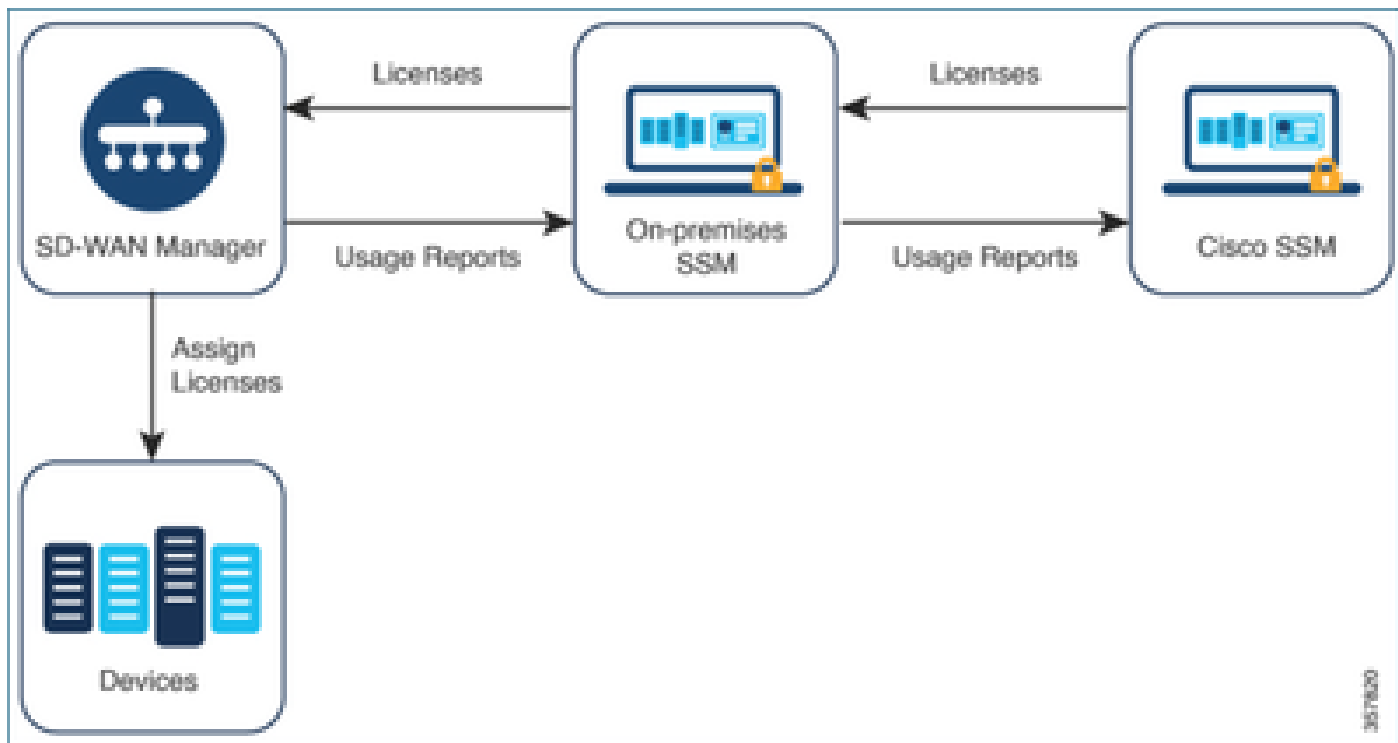
Para cenários em que o Catalyst SD-WAN Manager não está conectado diretamente à Internet, o uso de um servidor proxy pode fornecer acesso a serviços baseados na Internet, como o Cisco SSM, ou a um SSM local.

Versão mínima: Catalyst SD-WAN Manager versão 20.9.1

O Cisco Smart Software Manager no local (SSM no local) é uma solução Cisco Smart Licensing que permite administrar licenças de um servidor no local, em vez de ter que se conectar diretamente ao Cisco SSM. A solução envolve a configuração de um servidor de licença local do Cisco SSM, que sincroniza seu banco de dados de licença com o Cisco SSM periodicamente e funciona de forma semelhante ao Cisco SSM, enquanto opera localmente.

O Catalyst SD-WAN Manager suporta o gerenciamento de licenças usando um servidor local Cisco SSM, usando um modo chamado local. O modo no local é útil para organizações que usam o Cisco SSM no local para acomodar uma política de segurança rígida que não permite que os dispositivos de rede se comuniquem com o Cisco SSM por conexão direta com a Internet.

Ao operar no modo local, o Catalyst SD-WAN Manager sincroniza as informações de licença com o servidor de licença local do Cisco SSM a cada 24 horas. Durante essa sincronização, o Catalyst SD-WAN Manager recebe todas as atualizações para licenças disponíveis e envia relatórios de uso de licença para o servidor de licença local do Cisco SSM. Você pode sincronizar licenças a qualquer momento.



## Benefícios do uso do Cisco Smart Software Manager no local

As organizações cujas políticas de segurança, ou outras circunstâncias, exigem que o Catalyst SD-WAN Manager não esteja conectado à Internet têm duas opções para gerenciar licenças para Licença inteligente usando política:

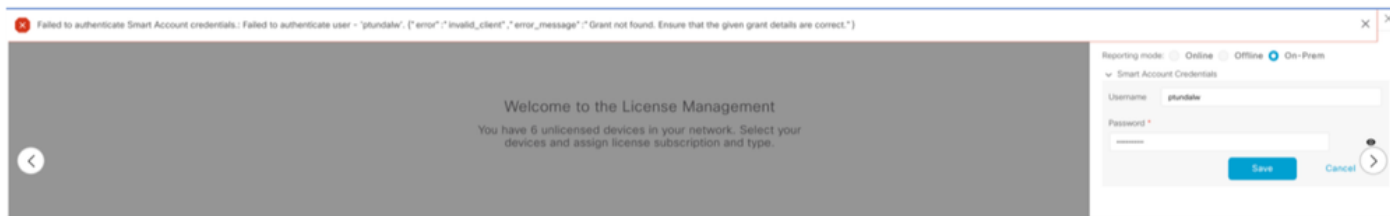
- Use o modo off-line, que requer a transferência manual de arquivos entre o Catalyst SD-WAN Manager e o Cisco SSM.
- Use um servidor local do Cisco SSM que seja acessível por meio de uma conexão local com o Catalyst SD-WAN Manager.

Ambos os métodos atendem à necessidade de transferir informações de licença entre o Cisco SSM e o Catalyst SD-WAN Manager. Sempre que for possível usar o modo local, este modo oferece o benefício significativo de reduzir a sobrecarga de manutenção da transferência manual de arquivos entre o Catalyst SD-WAN Manager e o Cisco SSM, conforme necessário para o modo off-line.

## Erro

Ao sincronizar as credenciais Smart da GUI do Catalyst SD-WAN Manager, obtemos este erro:

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



## Abordagem de solução de problemas

- O vManage deve estar no código 20.9.1 ou posterior.
- Verifique os logs no Catalyst SD-WAN Manager (vmanage-server.logs) enquanto coloca as Credenciais de Conta Inteligente na Seção Gerenciamento de Licenças do Catalyst SD-WAN Manager.
- Verifique se a ID do cliente e a chave secreta foram compartilhadas pela equipe SSM local.
- TCPDUMP no vManage para o IP do servidor CSSM
- Verifique se o DNS está configurado corretamente no Catalyst SD-WAN Manager e se é possível fazer ping em cloudssso.cisco.com
- Envolver a equipe SSM local e solicitar que a equipe SSM depure no servidor local.

IP do Catalyst SD-WAN Manager: 10.66.76.81 / 192.168.10.1

IP do servidor CSSM: 10.106.66.55

TCPDump no vManage para o IP do servidor SSM:

```
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 [P.], 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
```

### Logs de servidor no local:

```
[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 172.20.226.229
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 1:M 13 Jan 2023 11:14:09.049 * 100 changes in 300 seconds. Saving
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 1:M 13 Jan 2023 11:14:09.050 * Background saving started by process
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 disk
Jan 13 11:14:09 SSM-On-Prem b09c1e3b5d81: 1:M 13 Jan 2023 11:14:09.150 * Background saving terminated with success
Jan 13 11:14:46 SSM-On-Prem 1a1fca641d0a: Redis#exists(key) will return an Integer in redis-rb 4.3. exists
Jan 13 11:14:46 SSM-On-Prem 1a1fca641d0a: [active_model_serializers] Rendered UserSerializer with ActiveModelSerializers
Jan 13 11:14:46 SSM-On-Prem 1a1fca641d0a: method=GET path=/sessions/get_user format=json controller=SessionsController
Jan 13 11:14:46 SSM-On-Prem 504f06c0d581: 10.110.35.124https://10.110.35.124 - - [13/Jan/2023:11:14:46 +0000]
Jan 13 11:17:01 SSM-On-Prem 504f06c0d581: 2023/07/13 11:17:01 [error] 47#47: *1576 connect() failed (111: Connection refused)
Jan 13 11:17:01 SSM-On-Prem 504f06c0d581: 2023/07/13 11:17:01 [warn] 47#47: *1576 upstream server temporarily disabled
Jan 13 11:17:01 SSM-On-Prem 1a1fca641d0a: [active_model_serializers] Rendered ActiveModel::Serializer::UserSerializer
Jan 13 11:17:01 SSM-On-Prem 1a1fca641d0a: method=POST path=/oauth/token format=json controller=Doorkeeper::SessionsController
Jan 13 11:17:01 SSM-On-Prem 504f06c0d581: 10.66.76.85https://10.66.76.85 - - [13/Jan/2023:11:17:01 +0000]
Jan 13 11:17:14 SSM-On-Prem 1a1fca641d0a: [INFO] Session expiring outcome=success
```

Efetua logon no vManage, colocando os detalhes das Smart Accounts na seção Gerenciamento

de licenças do vManage:

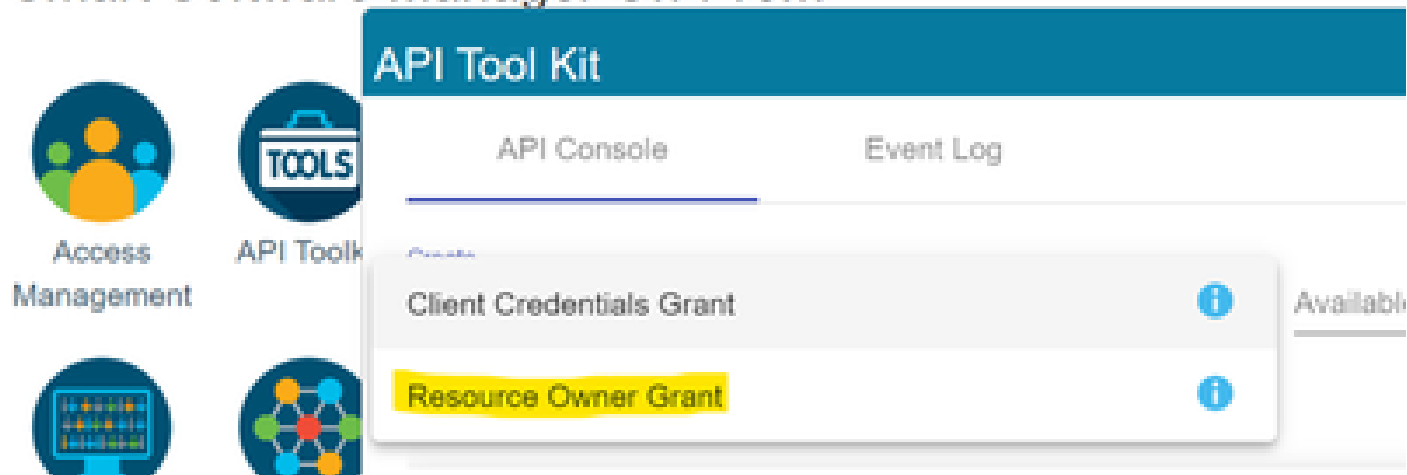
```
13-Jan-2023 17:29:02,775 IST INFO [um8_vManage] [SmartLicensingIntegrationManager] (default task-24) |
13-Jan-2023 17:29:02,776 IST INFO [um8_vManage] [SmartLicensingIntegrationManager] (default task-24) |
13-Jan-2023 17:29:02,780 IST INFO [um8_vManage] [AbstractSettingsManager] (default task-24) |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| Faile
13-Jan-2023 17:29:03,491 IST ERROR [um8_vManage] [SmartLicensingIntegrationRestfulResource] (default ta
```

Observação: estamos recebendo o erro 403 ao sincronizar a Smart Account na GUI do vManage, que indica que o servidor compreende a solicitação, mas se recusa a autorizá-la.

## Solução

1. Faça login no servidor local.
2. Navegue até API Tool Kit (Kit de ferramentas de API).
3. Selecione "Concessão do Proprietário do Recurso", Insira os detalhes como Nome e salve.

## Smart Software Manager On-Prem



The screenshot shows the 'API Tool Kit' interface. It has a dark blue header with the title 'API Tool Kit'. Below the header are two tabs: 'API Console' (selected) and 'Event Log'. The main content area displays a list of grants. The first grant is 'Client Credentials Grant' with an information icon and the status 'Available'. The second grant is 'Resource Owner Grant', which is highlighted in yellow, with an information icon.

### Resource Owner Grant ✕

Name \*

Test5

Description

Expiration Date

Client ID \*

z92Dss3\_SVnlhUXURJV97gdf03ukxSE5\_shD3vB7llyl2YKAaJkGh8nbYSRWYCzN

Client Secret \*

.....



Regenerate Client Secret

Save

Cancel

4. Selecione o registro salvo (mencionado no instantâneo anterior) e marque ID do cliente e Segredo do cliente.

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_SVnlhUXJ...

5. Compartilhe e insira a ID do cliente compartilhada e o Segredo do cliente no portal do Catalyst SD-WAN Manager.
6. Vá para "Sincronizar licenças e atualizar dispositivos" no vManage e use as mesmas credenciais locais com as quais você fez logon para gerar ID de cliente e segredo de cliente.

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.