

Resolución de problemas de sincronización de licencias en Catalyst SD-WAN Manager a través del modo de informes en las instalaciones

Contenido

[Introducción](#)

[Requirements](#)

[Error](#)

[Enfoque de solución de problemas](#)

[Solución Aternativa](#)

Introducción

Este documento describe cómo resolver un error encontrado al sincronizar la licencia en el Catalyst SD-WAN Manager a través del modo de informes en las instalaciones.

Requirements

En los escenarios en los que Catalyst SD-WAN Manager no está conectado directamente a Internet, el uso de un servidor proxy puede proporcionar acceso a servicios basados en Internet, como Cisco SSM, o a un SSM local en las instalaciones.

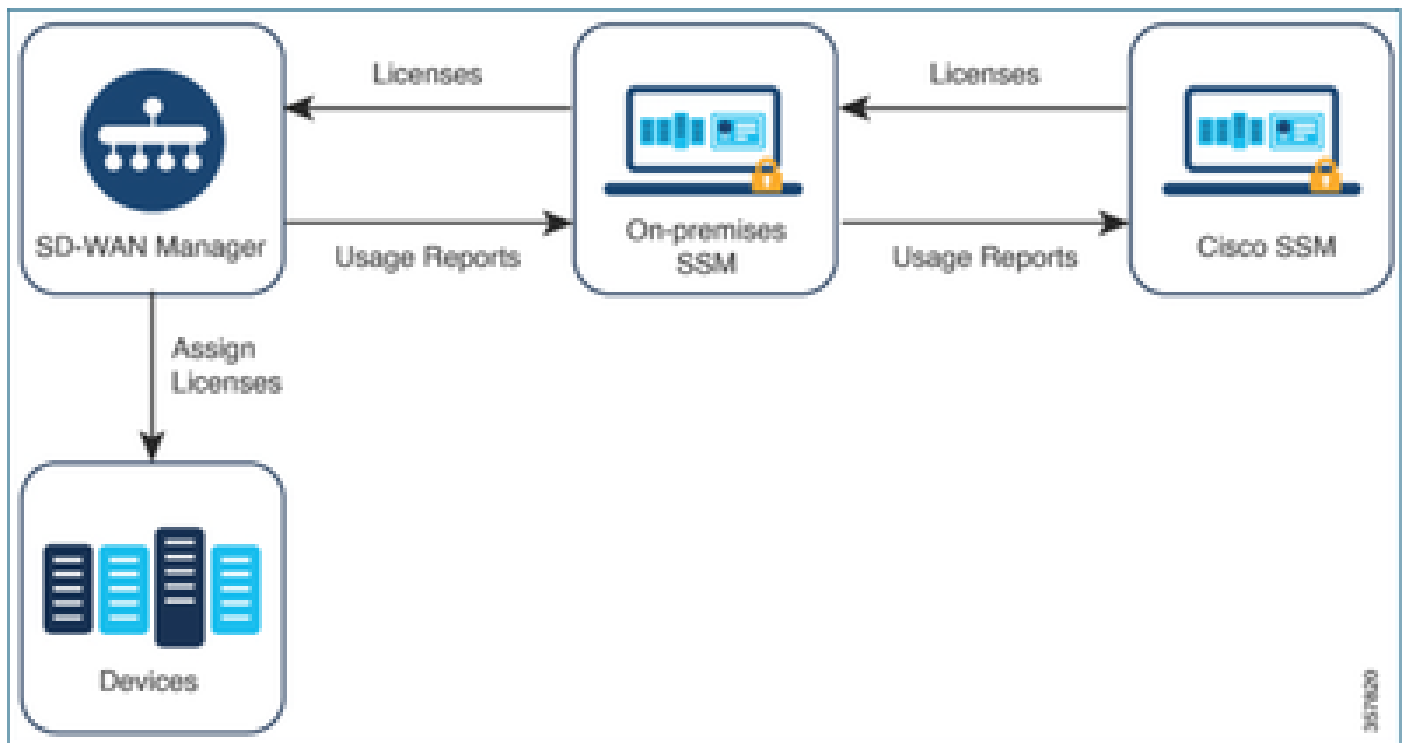
Versión mínima: Catalyst SD-WAN Manager versión 20.9.1

Cisco Smart Software Manager en las instalaciones (SSM en las instalaciones) es una solución de Cisco Smart Licensing que le permite administrar licencias desde un servidor en sus instalaciones, en lugar de tener que conectarse directamente a Cisco SSM. La solución implica la configuración de un servidor de licencias en las instalaciones de Cisco SSM, que sincroniza periódicamente su base de datos de licencias con Cisco SSM y funciona de forma similar a Cisco SSM, mientras funciona localmente.

Catalyst SD-WAN Manager admite la gestión de licencias mediante un servidor Cisco SSM en las instalaciones, mediante un modo denominado en las instalaciones. El modo en las instalaciones resulta útil para las organizaciones que utilizan Cisco SSM en las instalaciones para adaptarse a una política de seguridad estricta que no permite que los dispositivos de red se comuniquen con Cisco SSM mediante una conexión directa a Internet.

Cuando funciona en modo in situ, Catalyst SD-WAN Manager sincroniza la información de licencia con el servidor de licencias in situ de Cisco SSM cada 24 horas. Durante esta sincronización, Catalyst SD-WAN Manager recibe cualquier actualización de las licencias disponibles y envía informes de uso de licencias al servidor de licencias en las instalaciones de

Cisco SSM. Puede sincronizar licencias en cualquier momento.



Ventajas del uso in situ de Cisco Smart Software Manager

Las organizaciones cuyas políticas de seguridad, u otras circunstancias, requieren que Catalyst SD-WAN Manager no esté conectado a Internet tienen dos opciones para administrar las licencias de Smart License Using Policy:

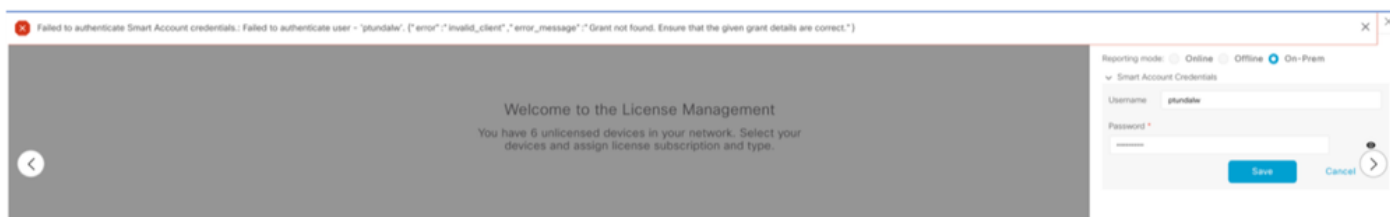
- Utilice el modo sin conexión, que requiere la transferencia manual de archivos entre Catalyst SD-WAN Manager y Cisco SSM.
- Utilice un servidor Cisco SSM en las instalaciones al que se pueda acceder a través de una conexión de área local con el administrador Catalyst SD-WAN.

Ambos métodos abordan la necesidad de transferir información de licencia entre Cisco SSM y Catalyst SD-WAN Manager. Siempre que sea posible utilizar el modo en las instalaciones, este modo proporciona la ventaja significativa de reducir la sobrecarga de mantenimiento de la transferencia manual de archivos entre Catalyst SD-WAN Manager y Cisco SSM, como es necesario para el modo sin conexión.

Error

Al sincronizar las credenciales inteligentes desde la GUI de Catalyst SD-WAN Manager, se obtiene este error:

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



Enfoque de solución de problemas

- vManage debe estar en el código 20.9.1 o posterior.
- Verifique los registros en el administrador Catalyst SD-WAN (vmanage-server.logs) mientras coloca las credenciales de la cuenta inteligente en la sección de administración de licencias del administrador Catalyst SD-WAN.
- Asegúrese de que el equipo SSM local comparte la ID de cliente y la clave secreta correctas.
- TCPDUMP en vManage para IP de servidor CSSM
- Verifique que el DNS esté configurado correctamente en el Catalyst SD-WAN Manager y que pueda hacer ping a cloudssso.cisco.com
- Involucrar al equipo SSM en las instalaciones y solicitar al equipo SSM que depure en el extremo del servidor en las instalaciones.

IP de Catalyst SD-WAN Manager: 10.66.76.81 / 192.168.10.1

IP del servidor CSSM: 10.106.66.55

TCPDump en vManage para la IP del 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 [S.], 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 [S.], 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
```

Registros del servidor en las instalaciones:

```
[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
```

Inicia sesión en vManage mientras se colocan los detalles de las cuentas inteligentes en la sección de administración de licencias de vManage:

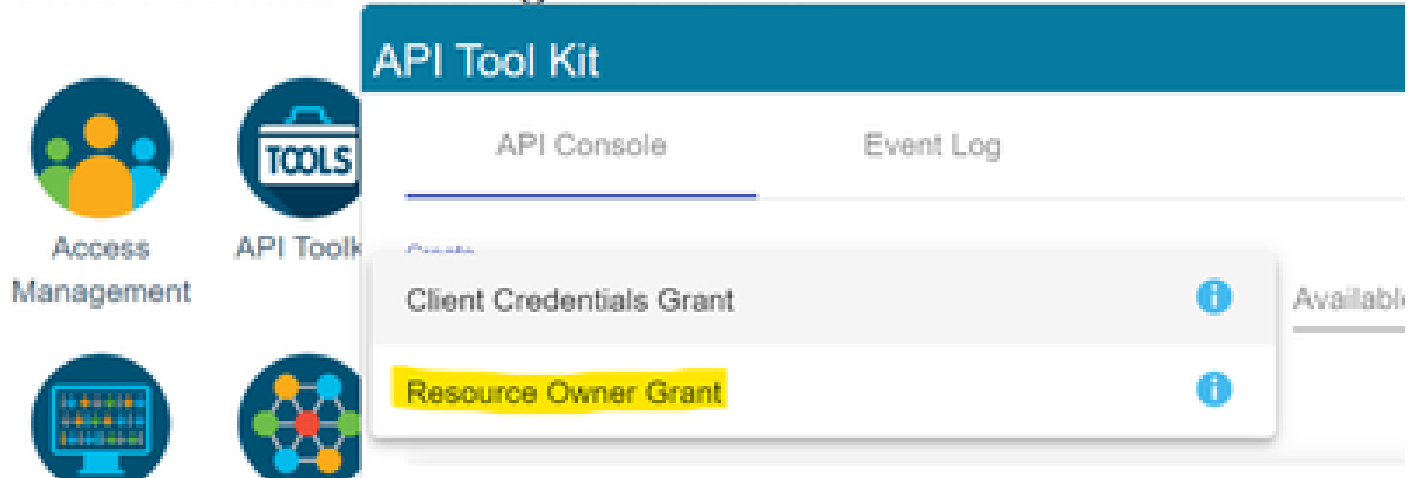
```
13-Jan-2023 17:29:02,775 IST INFO [um8_vManage] [SmartLicensingIntegrationManager] (default task-24) |
13-Jan-2023 17:29:02,776 IST INFO [um8_vManage] [SmartLicensingIntegrationManager] (default task-24) |
13-Jan-2023 17:29:02,780 IST INFO [um8_vManage] [AbstractSettingsManager] (default task-24)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

Nota: Aparece el error 403 al sincronizar la cuenta inteligente desde la GUI de vManage, lo que indica que el servidor entiende la solicitud pero se niega a autorizarla.

Solución Aternativa

1. Inicie sesión en el servidor local.
2. Vaya a API Tool Kit.
3. Seleccione "Concesión de propietario de recurso", introduzca los detalles como Nombre y guárdelo.

Smart Software Manager On-Prem



The screenshot shows the 'API Tool Kit' interface. It has a top navigation bar with 'API Console' and 'Event Log'. Below the navigation bar, there are four icons: 'Access Management', 'API Tool Kit', 'Access Management', and 'API Tool Kit'. A dropdown menu is open over the 'API Tool Kit' icon, showing a list of grants. The 'Resource Owner Grant' is highlighted in yellow. To the right of the list, there is a column labeled 'Availability'.

Resource Owner Grant

Name *

Test5

Description

Expiration Date

Client ID *

z92Dss3_SVnlhUXURJV97gdf03ukxSE5_shD3vB7tllyl2YKAaJkGh8nbYSRWYCzN

Client Secret *

.....

 Regenerate Client Secret

Save

Cancel

4. Seleccione el registro guardado (mencionado en la instantánea anterior) y marque Client ID (ID de cliente) y Client Secret (Secreto de 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_SVnIhUXJ...

5. Comparta e introduzca la ID de cliente y la clave secreta de cliente compartidas en el portal del administrador Catalyst SD-WAN.
6. Vaya a "Sincronizar licencias y actualizar dispositivos" en vManage y utilice las mismas credenciales en las instalaciones con las que inició sesión para generar la ID de cliente y el secreto de cliente.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).