

# Integre ISE 3.3 con JAMF como servidor MDM

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Preparación de JAMF PRO para la conexión MDM](#)

[Preparación de ISE para la conexión MDM](#)

[Verifique la conectividad inicial de la integración con la instancia de JAMF PRO.](#)

[Solución de problemas de servidor MDM inalcanzable](#)

[Situación 1. Se ha agotado el tiempo de espera de conexión](#)

[Situación 2. Error de conexión: 404](#)

[Situación 3. Error de conexión: 401](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe los procedimientos necesarios para implementar Identity Services Engine v3.3 con la instancia 10.48.X de JAMF PRO.

## Prerequisites

### Requirements

Cisco recomienda conocimientos sobre los siguientes temas:

- Identity Services Engine (ISE)
- JAMF como solución de MDM

### Componentes Utilizados

La información de este documento se basa en estas versiones y software:

- Cisco Identity Services Engine (ISE) v3.3
- JAMF PRO v10.48.1-t1689600654

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

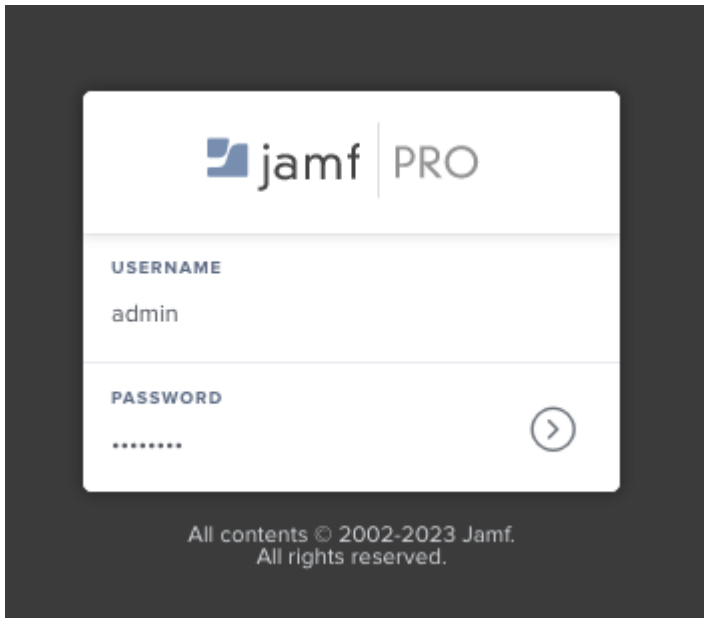
Cisco ISE admite JAMF como servidor MDM para administrar equipos con Windows. Cuando estos ordenadores (gestionados por JAMF) están conectados y autenticados, ISE recupera información de conformidad de los servidores JAMF para recuperar información adicional para la condición en materia de seguridad de dichos dispositivos.

Utiliza la información para aplicar la seguridad de acceso seguro al permitir o denegar dichos equipos, en función de los criterios y condiciones configurados en ISE. Por lo tanto, esta implementación ayuda a identificar las posibles vulnerabilidades y debilidades de seguridad que podrían aprovechar los atacantes.

## Configurar

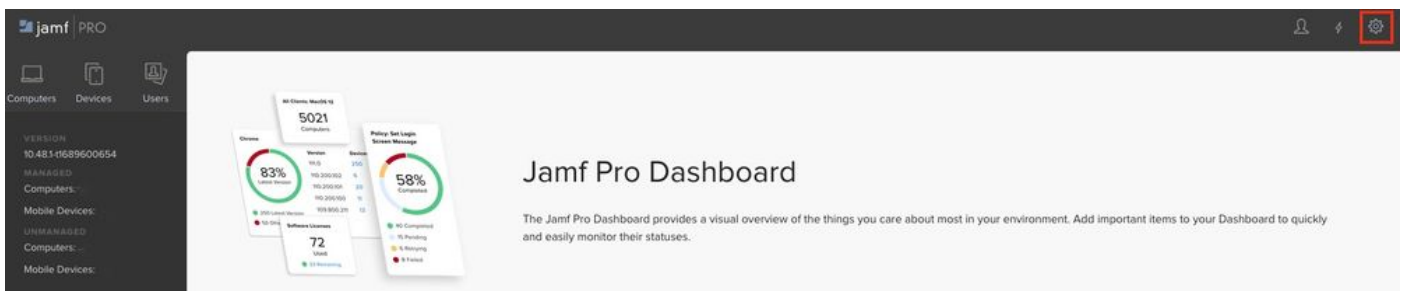
### Preparación de JAMF PRO para la conexión MDM

Paso 1. Inicie sesión con su nube JAMF con la cuenta para privilegios de administrador en: [https://YOUR\\_ACCOUNT.jamfcloud.com/index.html](https://YOUR_ACCOUNT.jamfcloud.com/index.html).



Página de inicio de sesión de JAMF PRO

Paso 2. En el menú principal, seleccione el icono de engranaje.



Panel de JAMF PRO

Paso 3. En el menú principal, elija Sistema > Cuentas de usuario y grupos.

## Settings

[All](#) [System](#) [Global](#) [Jamf Apps](#) [Self Service](#) [Server](#) [Network](#) [Com](#)

### System 11 settings

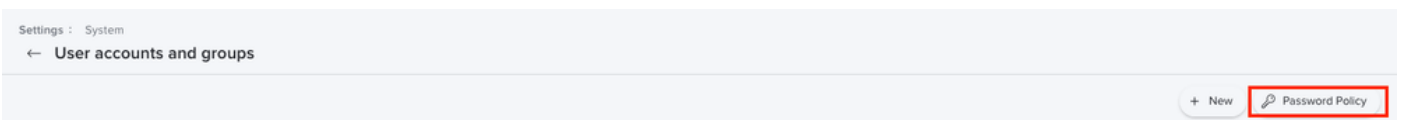


#### User accounts and groups

Set Jamf Pro user privileges, Directory Service accounts, and password policies

Configuración del sistema JAMF PRO

Paso 4. Seleccione la opción Política de contraseñas.



Cuentas y grupos de usuarios de JAMF PRO

Paso 5. En esta sección, confirme que tiene la opción Allow Basic Authentication además de Bearer Token Authentication.



Nota: A partir de JAMF PRO v10.35, la autenticación básica para la API no está habilitada de forma predeterminada. Por lo tanto, debe activar estas funciones para asegurarse de que la integración de MDM funciona correctamente.

Para obtener más información, revise los [cambios de autenticación de API clásicas](#).

Paso 6. Una vez que haya habilitado la última función, vaya a Menu Settings (Configuración de menú) descrito en el Paso 3, busque el Network IntegrationMenu y selecciónelo.

## Settings

[Clear](#)

[All](#) [System](#) [Global](#) [Jamf Apps](#) [Self Service](#) [Server](#) [Network](#)

## Network 1 result found for "network integration"



### Network integration

Integrate with a network access management service

Integración de red JAMF PRO

Paso 7. Vaya a select + New para agregar una nueva instancia para ISE 3.3.

Settings : Network

← Network integration

+ New

NAME

No Network integration

Parámetros de integración de red JAMF PRO

Paso 8. En el menú desplegable bajo Servicio de administración de acceso a la red, deje la opción marcada como Cisco ISE.

- A continuación, proporcione un nombre en el menú Display Name tal como se muestra en este ejemplo.
- Para los parámetros iniciales y la conexión para ISE, la configuración se puede dejar con estas configuraciones estándar.
- Vaya a Guardar la configuración.

**Network Access Management Service** Network access management service to use for the network integration

Cisco ISE

**Display Name** Display name for the network integration  
isev33

**Advanced Computer Search For Compliance Verification** Select the saved search for Cisco ISE to use to verify computers compliant to organizational standards  
None

**Computer Compliance Verification Failure Message** Optional message to display to the user via Cisco ISE when the computer is not compliant

**Computer Compliance Remediation Message** Optional message to display to the user via Cisco ISE about how to become compliant

**Advanced Mobile Device Search For Compliance Verification** Select the saved search for Cisco ISE to use to verify mobile devices compliant to organizational standards  
None

**Mobile Device Compliance Verification Failure Message** Optional message to display to the user via Cisco ISE when the mobile device is not compliant

**Mobile Device Compliance Remediation Message** Optional message to display to the user via Cisco ISE about how to become compliant

**Remote Lock And Wipe Passcode Assignment Method For Computers** Method to use to assign the passcode when locking or wiping computers via Cisco ISE  
Create Random Passcode

Cancel Save

Ejemplo de configuración Integración de red con ISE

Paso 9. La integración genera una URL de integración de red con este formato:

https://YOUR\_ACCOUNT.jamfcloud.com/networkIntegrationEndpoint/ID. Guarde esta URL porque debe utilizarla más adelante para conectarse con ISE.

## Preparación de ISE para la conexión MDM

Paso 1. Seleccione el Menú > Administración > Recursos de red > MDM externa, y luego haga clic en Agregar.

Identity Services Engine Administration / Network Resources

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

### MDM / UEM Integrations

Unified Endpoint Management (UEM) and Mobile Device Management (MDM) integrations enable you to secure, monitor, and manage the endpoints on your network. Integrate UEM and MDM platforms with Cisco ISE to allow Cisco ISE to query the integrations for endpoint attributes. You can then use these attributes to create and apply necessary access control policies. Also, you can configure [General MDM Settings](#).

Add Duplicate Edit Delete Change Timeout Filter Download

MDM / UEM Integration Name	Status	Service Provider	Hostname / IP Address	Description	Timeout (msec)
No data found.					

Menú de integración de ISE MDM

Paso 2. Asigne un nombre a la instalación dentro del segmento MDM / UEM Integration Name.

- En la sección Hostname / IP Address, seleccione YOUR\_ACCOUNT.jamfcloud.com de la URL generada en los pasos anteriores.

- En Puerto, seleccione el 443 para la conexión HTTPS con la instancia de JAMF PRO.
- En la sección Nombre de instancia, continúe introduciendo los valores en los que falta la sección de la URL creada (en este caso: /networkIntegrationEndpoint/ID).
- Introduzca un nombre de usuario con acceso completo a la instancia de JAMF PRO junto con la contraseña correspondiente.
- Cambie el estado del servidor MDM a Enabled.

Identity Services Engine Administration / Network Resources

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

MDM / UEM Integrations > New

## New Server

Cisco ISE supports mobile device management and Microsoft configuration management servers. Click [here](#) to view the list of MDM servers supported by Cisco ISE.

MDM / UEM Integration Name\*  
JAMF\_PRO

Description

Server Type  
Mobile Device Manager

Authentication Type  
Basic

Hostname / IP Address\*  
YOUR\_ACCOUNT.jamfcloud.com

Port\*  
443 (max length: 5)

Instance Name  
/networkIntegrationEndpoint/ID

Username\*  
admin

Password\*  
.....

Polling Interval\*  
240

MDM/UEM Device Compliance Timeout\*  
30000  
1 to 30000 (milliseconds)

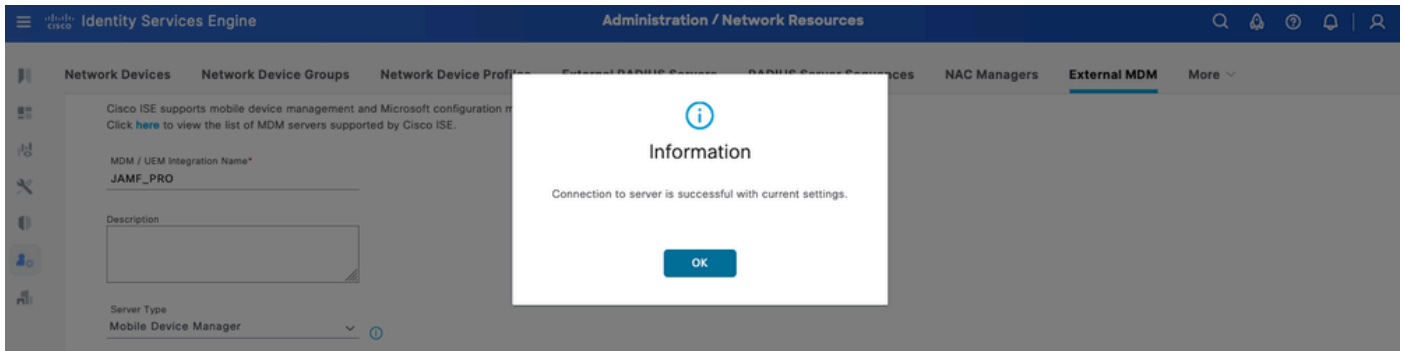
When re-authenticating an endpoint into the network Cisco ISE refers to cached MDM attributes of the endpoint. If the age of the cached MDM attributes is greater than the interval configured, Cisco ISE sends a fresh query to the MDM server for the endpoint's attributes. If there is a change in compliance status, Cisco ISE issues a Change of Authorization.

Compliance Cache Expiration Time\*  
1  
1 to 10080 (minutes)

Status  
Enabled

Ejemplo de configuración de ISE MDM JAMF PRO

Paso 3. Desplácese hacia abajo y vaya a Probar conexión. Si la conexión es exitosa, se muestra esta imagen. Si no recibe el mismo resultado, consulte la sección Resolución de problemas de este documento.



Conexión correcta con la cuenta JAMF de MDM





Paso 4. Seleccione Aceptar en la opción anterior. En la parte inferior de la página, busque el identificador de dispositivo donde se asocia ISE de la sesión del terminal.

- Dependiendo de su situación, puede seleccionar la dirección MAC del dispositivo o los atributos del certificado.
- Una vez que haya personalizado esta sección, guarde la configuración.

 This MDM or UEM server supports Cisco ISE API Version 3.

### Device Identifier

Configure Cisco ISE to identify endpoints through variables other than MAC addresses. This allows accurate identification of endpoints even the MAC address presented Cisco ISE is not necessarily the MAC address of the physical network interface card (for example, when MAC address randomisation is enabled). Check the check boxes next to the device identifiers to be used. Drag and drop the device identifiers to define the sequence of verification. If the first device identifier on the list is not available for an endpoint, then Cisco ISE checks for the second identifier on the list, and so on.

Device Identifier 	Enabled
 1. Legacy MAC Address	<input checked="" type="checkbox"/>
 2. Cert - SAN URI, GUID	<input type="checkbox"/>
 3. Cert - CN, GUID	<input type="checkbox"/>

Cancel

Save

Configuración adicional para el servidor MDM

# Verifique la conectividad inicial de la integración con la instancia de JAMF PRO.

Captura de paquete: En caso de que la conectividad se realice correctamente, puede ver el tráfico HTTPS que se envía desde el servidor ISE PAN a la instancia JAMF PRO:

Protocol	Length	Info
TCP	74	47386 → 3128 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=211264130 TSecr=0 WS=128
TCP	74	3128 → 47386 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=503104063 TSecr=211264130 WS=128
TCP	66	47386 → 3128 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=211264131 TSecr=503104063
HTTP	183	CONNECT → 443 HTTP/1.1
TCP	66	3128 → 47386 [ACK] Seq=1 Ack=118 Win=65152 Len=0 TSval=503104064 TSecr=211264131
HTTP	105	HTTP/1.1 200 Connection established
TCP	66	47386 → 3128 [ACK] Seq=118 Ack=40 Win=29312 Len=0 TSval=211264384 TSecr=503104317
TLsv1...	387	Client Hello
TCP	66	3128 → 47386 [ACK] Seq=40 Ack=439 Win=64896 Len=0 TSval=503104318 TSecr=211264385
TLsv1...	166	Server Hello
TCP	1254	3128 → 47386 [PSH, ACK] Seq=140 Ack=439 Win=64896 Len=1188 TSval=503104457 TSecr=211264385 [TCP segment of a reassembled PDU]
TCP	66	47386 → 3128 [ACK] Seq=439 Ack=1328 Win=32128 Len=0 TSval=211264524 TSecr=503104457
TCP	1254	3128 → 47386 [PSH, ACK] Seq=1328 Ack=439 Win=64896 Len=1188 TSval=503104457 TSecr=211264385 [TCP segment of a reassembled PDU]
TLsv1...	2641	Certificate
TCP	66	47386 → 3128 [ACK] Seq=439 Ack=5091 Win=40192 Len=0 TSval=211264525 TSecr=503104457
TLsv1...	413	Server Key Exchange, Server Hello Done
TLsv1...	141	Client Key Exchange
TCP	66	3128 → 47386 [ACK] Seq=5438 Ack=514 Win=64896 Len=0 TSval=503104459 TSecr=211264526
TLsv1...	72	Change Cipher Spec
TLsv1...	111	Encrypted Handshake Message
TCP	66	3128 → 47386 [ACK] Seq=5438 Ack=520 Win=64896 Len=0 TSval=503104462 TSecr=211264529
TCP	66	3128 → 47386 [ACK] Seq=5438 Ack=565 Win=64896 Len=0 TSval=503104463 TSecr=211264529
TLsv1...	117	Change Cipher Spec, Encrypted Handshake Message
TLsv1...	360	Application Data
TCP	66	3128 → 47386 [ACK] Seq=5489 Ack=859 Win=64640 Len=0 TSval=503104601 TSecr=211264668
TLsv1...	1617	Application Data, Application Data
TCP	66	47386 → 3128 [ACK] Seq=859 Ack=7040 Win=46208 Len=0 TSval=211264922 TSecr=503104855

Ejemplo de captura de paquetes de conectividad con la instancia de JAMF

Registros en ISE: ISE procesa y analiza los datos según se muestra en ise-psc.log:

```
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.api.MdmServerInfoApi -:::- inside the method : callMdmServerInfo
TRACE [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::- Inside MDMVerifyServer.verifyMdmServerInfo
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::- apiVersionSb : 3, mdmApiVersion : 3
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::- MDM Rest API Server Query Success
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::- MDM Rest API Server Query Success
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::- 1. Connecting to the MDM server
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDom: start HTTP request
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDomNonComp: start HTTP request
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- ===mdmFlowInfo===null,====serve
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- QueryType is heartbeatQuery
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- using httpClient for http query
INFO [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- GET: MDM Server URL: https://YOURISEIP:443/
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- Proxy Config in request = [PROXY]
.
.
INFO [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- MDM Server Response Code: 200
TRACE [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -:::-
Response data received from the MDM server : <?xml version="1.0" encoding="UTF-8"?><ise_api><name>mdminfo
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDom: end HTTP request
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDomNonComp: end HTTP request
TRACE [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::- isMdmSettingsIdNotNull flag is true
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.api.MdmServerInfoApi -:::- returning from the method : callMdmServerInfo
apiPath: /ID/ciscoise/v3
```

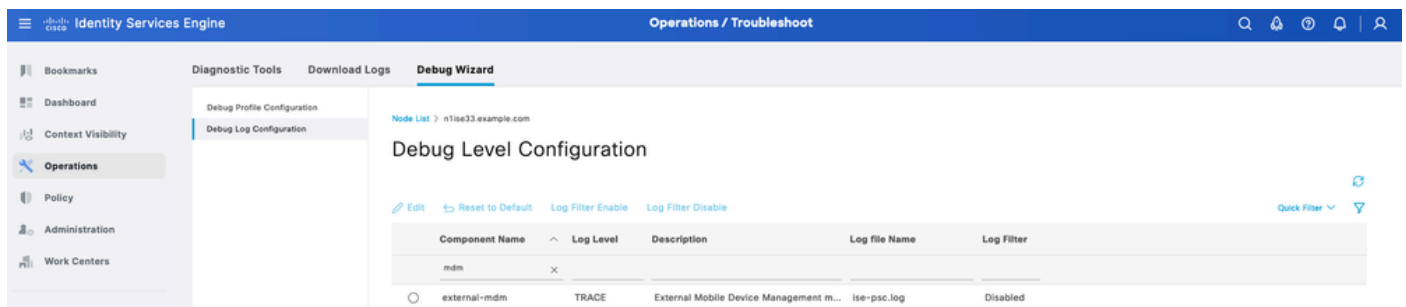
```
redirectUrl: https://YOUR_ACCOUNT.jamfcloud.com/enroll
queryMaxSize: 1000
apiVersion: 3
vendor: JAMF Software
productName: JSS
productVersion: 10.48.1-t1689600654
COMMA: ,
errorMsg: null
errorOccurred: false
}
```

## Solución de problemas de servidor MDM inalcanzable

La base de esta integración consta de consultas que ISE realiza periódicamente a la instancia de JAMF-PRO. El punto de referencia en el que se realiza la resolución de problemas (en este caso) es el nodo de administración principal (PAN). El nodo PAN es donde se configura el método de conectividad para alcanzar el servidor MDM. Este mismo método se replica en todos los nodos para la implementación.

Los siguientes pasos se pueden aplicar para la resolución de problemas de disponibilidad.

Paso 1. Habilite el componente external-mdm en el nivel TRACE en el nodo PAN.

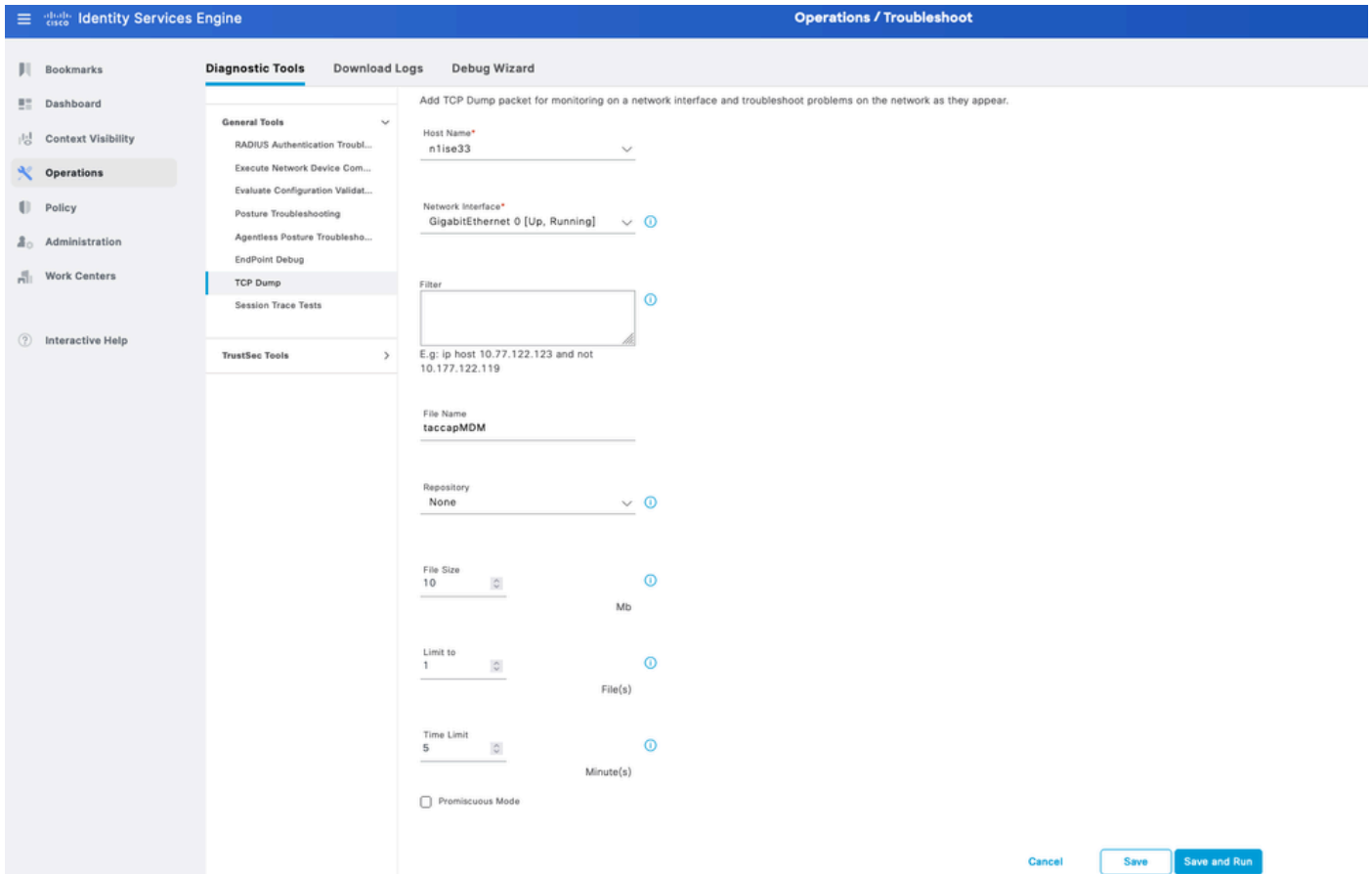


The screenshot shows the Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Operations / Troubleshoot'. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations (selected), Policy, Administration, and Work Centers. The main content area is titled 'Debug Wizard' and shows 'Debug Level Configuration' for the component 'external-mdm'. The configuration table is as follows:

Component Name	Log Level	Description	Log File Name	Log Filter
external-mdm	TRACE	External Mobile Device Management m...	ise-psc.log	Disabled

Componente externo de MDM en el nivel TRACE para solucionar problemas

Paso 2. Configure una captura desde el nodo PAN y guarde su configuración.



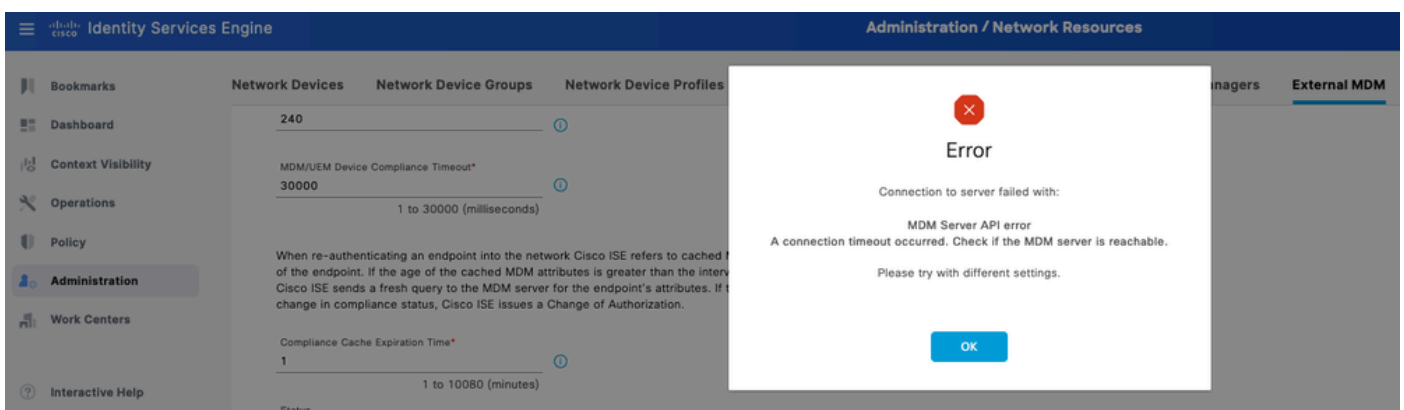
Ejemplo de captura de paquetes para recopilar información de la conexión MDM

Paso 3. Desplácese por el menú MDM externo. Ejecute la captura desde el paso 2 y seleccione el botón Probar Conexión. Espere a que aparezca el error.

Paso 4. Detenga la captura en el Paso 2. Revise los registros correspondientes a ise-psc.log para analizar el comportamiento.

Situación 1. Se ha agotado el tiempo de espera de conexión

En este escenario, cuando recibe este error en ISE mientras prueba la conexión con JAMF:



Los registros relacionados con la MDM externa revelan esta información:

```
TRACE [admin-http-pool26][[]] cisco.cpm.mdm.apiimp].MDMVerifyServer -:::- Inside MDMVerifyServer.verify
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimp].MDMVerifyServer -:::- API version retrieved from MDM
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimp].MDMVerifyServer -:::- apiVersionSb : 3, mdmApiVersion: 3
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimp].MDMVerifyServer -:::- MDM Rest API Server Query Success
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimp].MDMVerifyServer -:::- MDM Rest API Server Query Partial
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimp].MDMVerifyServer -:::- 1. Connecting to the MDM server
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDom: start HTTP request
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDomNonComp: start HTTP request
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- ===mdmFlowInfo===null,=====serverInfo=====
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- QueryType is heartbeatQuery
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- using httpClient for http query
INFO [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- GET: MDM Server URL: https://YOUR_ACCOUNT.jamfcloud.com
INFO [Timer-12][[]] cisco.mnt.common.utility.AlarmMessageDiskQueue -:::- Inside dequeue
INFO [Timer-12][[]] cisco.mnt.common.utility.AlarmMessageDiskQueue -:::- root exists
INFO [Timer-12][[]] cisco.mnt.common.utility.AlarmMessageDiskQueue -:::- alarm.1692086243915 deleted
INFO [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmServersCache -:::- MDM server - Status : Active, MDM server host - YOUR_ACCOUNT.jamfcloud.com, and port - 443
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- Error message while connecting to MDM server host - YOUR_ACCOUNT.jamfcloud.com, and port - 443 : Connection timed out
Connection Failed to the MDM server host - YOUR_ACCOUNT.jamfcloud.com, and port - 443 : Connection timed out
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDom: end HTTP request
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDomNonComp: end HTTP request
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.apiimp].MDMVerifyServer -:::- Exception occurred while connecting to MDM server host - YOUR_ACCOUNT.jamfcloud.com, and port - 443
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.api.MdmClient -:::- A connection timeout occurred. Check the MDM server host - YOUR_ACCOUNT.jamfcloud.com, and port - 443
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.api.MdmServerInfoApi -:::- returning from the method : callMdmServerInfo
    apiPath: null
    redirectUrl: null
    queryMaxSize: null
    apiVersion: null
    vendor: null
    productName: null
    productVersion: null
    COMMA: ,
    errorMsg: null
    errorOccurred: true
}
```

En la captura de paquetes, revise la siguiente información:

Tráfico DNS: ISE realiza una consulta a la instancia relacionada con JAMF si introduce el nombre de host en la parte de configuración de la integración. Si no ve la resolución del nombre de host, intente utilizar la dirección IP. Esta opción está disponible para configurar en lugar del nombre de host.

Source	Destination	Protocol	Length	Info
10.88.240.21	10.88.240.59	DNS	85	Standard query 0x5a75 A
10.88.240.21	10.88.240.59	DNS	85	Standard query 0x9f69 A
10.88.240.59	10.88.240.21	DNS	206	Standard query response
10.88.240.59	10.88.240.21	DNS	158	Standard query response

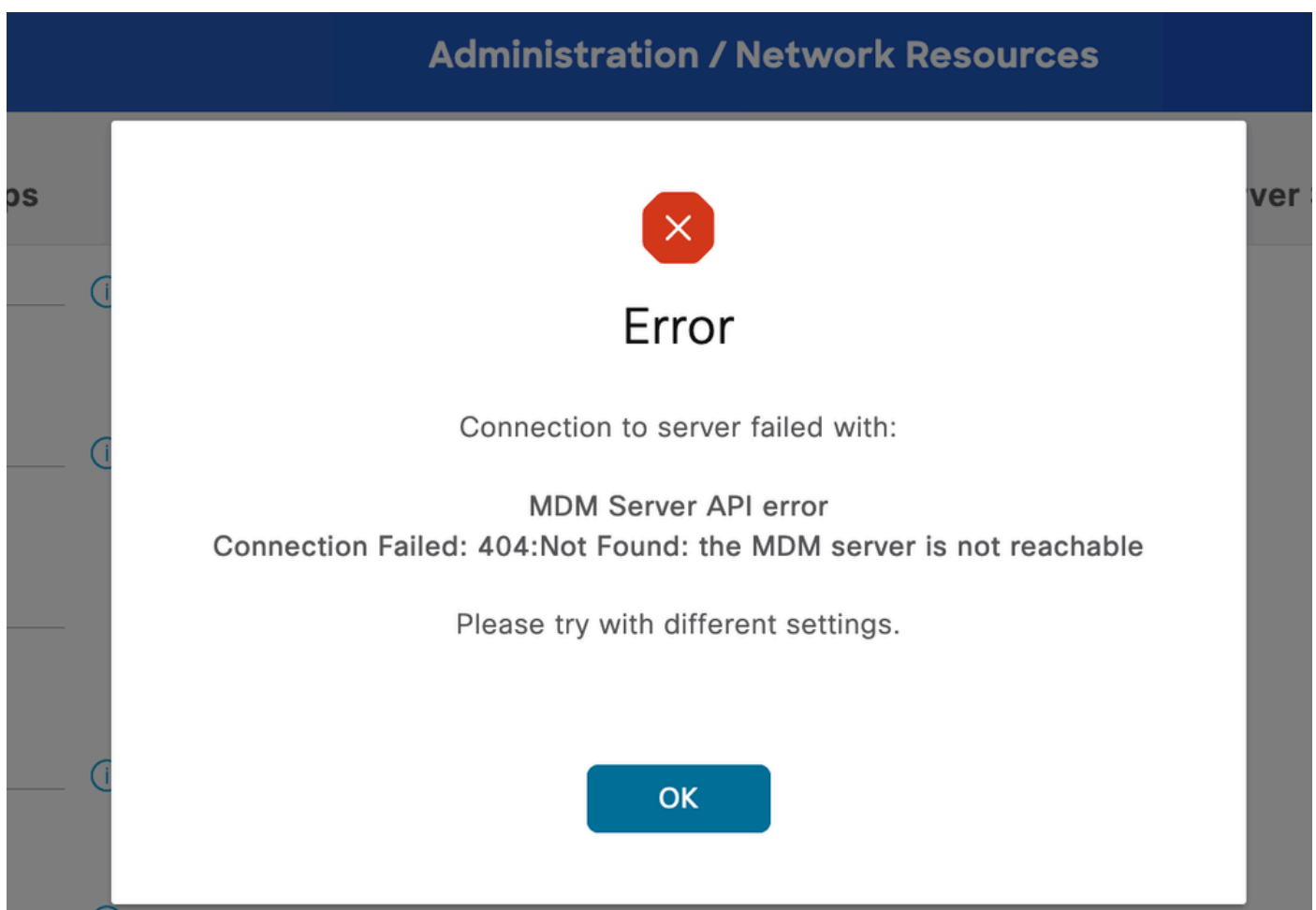
Retransmisiones en el Puerto de Conexión MDM - Si consulta la dirección IP directamente (proporcionada en la consulta DNS o en la configuración MDM), posiblemente puede ver los paquetes SYN repetidos. Esto indica que no hay una ruta directa a la instancia de JAMF o a un dispositivo externo que interfiera con las comunicaciones en el puerto 443.

Source	Protocol	Length	Info
10.88.240.21	TCP	74	22432 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=272773814 TSecr=0 WS=128
10.88.240.21	TCP	74	[TCP Retransmission] 22432 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=272774846 TSecr=0 WS=128
10.88.240.21	TCP	74	[TCP Retransmission] 22432 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=272776894 TSecr=0 WS=128

Ejemplo de conexión al tiempo de espera de MDM

## Situación 2. Error de conexión: 404

Este evento indica que tiene conectividad con la cuenta JAMF que ha configurado al configurar el servidor MDM. Sin embargo, la instancia indicada para la conexión no existe o contiene un error, ya que no se encuentra.



Ejemplo de error 404 de MDM

Se muestran los registros correspondientes a este evento:

```

DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmServerInfoApi -:::::- inside the method : callMdmServerInfo
TRACE [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::::- Inside MDMVerifyServer.verifyServerInfo
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::::- API version retrieved from MDM Rest API Server Query Parameters
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::::- apiVersionSb : 3, mdmApiVersion : 1.0
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::::- MDM Rest API Server Query Parameters
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::::- MDM Rest API Server Query Parameters
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -:::::- 1. Connecting to the MDM server
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -:::::- sendGETRequestDom: start HTTP request
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -:::::- sendGETRequestDomNonComp: start HTTP request
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -:::::- ===mdmFlowInfo===null,=====serverInfo=====
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -:::::- QueryType is heartbeatQuery
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -:::::- using httpClient for http query
INFO [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -:::::- GET: MDM Server URL: https://YOUR_IP_HERE:443/MDMRestAPI/MDMRestAPI
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -:::::- Proxy Config in request = [PROXY_HOST, PROXY_PORT]
INFO [admin-http-pool37][[]] cpm.admin.infra.spring.ISEAdminControllerUtils -::admin::- mapping path /MDMRestAPI/MDMRestAPI
INFO [admin-http-pool37][[]] cpm.admin.infra.spring.ISEAdminControllerUtils -::admin::- mapping path /MDMRestAPI/MDMRestAPI
INFO [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmServersCache -:::::- MDM server - Status : Active, MDM Version : 1.0
ERROR [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -:::::- Error message while connecting to MDM server
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -:::::- sendGETRequestDom: end HTTP request
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -:::::- sendGETRequestDomNonComp: end HTTP request
ERROR [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::::- Exception occurred while connecting to MDM server
ERROR [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmClient -:::::- Connection Failed: 404:: the MDM server is not available
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmServerInfoApi -:::::- returning from the method : callMdmServerInfo
    apiPath: null
    redirectUrl: null
    queryMaxSize: null
    apiVersion: null
    vendor: null
    productName: null
    productVersion: null
    COMMA: ,
    errorMsg: null
    errorOccurred: true
}
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmServersCache -:::::- mdm Guid: GUID is found in cache

```

La captura de paquetes en este momento proporciona una conexión HTTPS que contiene los datos de la aplicación que se transfieren entre el sitio JAMF y el servidor ISE.

Source	Protocol	Length	Info
10.88.240.21	HTTP	183	CONNECT :443 HTTP/1.1
10.31.104.78	HTTP	105	HTTP/1.1 200 Connection established
10.88.240.21	TLSv1.2	419	Client Hello
10.31.104.78	TLSv1.2	213	Server Hello, Change Cipher Spec, Encrypted Handshake Message
10.88.240.21	TLSv1.2	72	Change Cipher Spec
10.88.240.21	TLSv1.2	111	Encrypted Handshake Message
10.88.240.21	TLSv1.2	349	Application Data
10.31.104.78	TLSv1.2	1024	Application Data

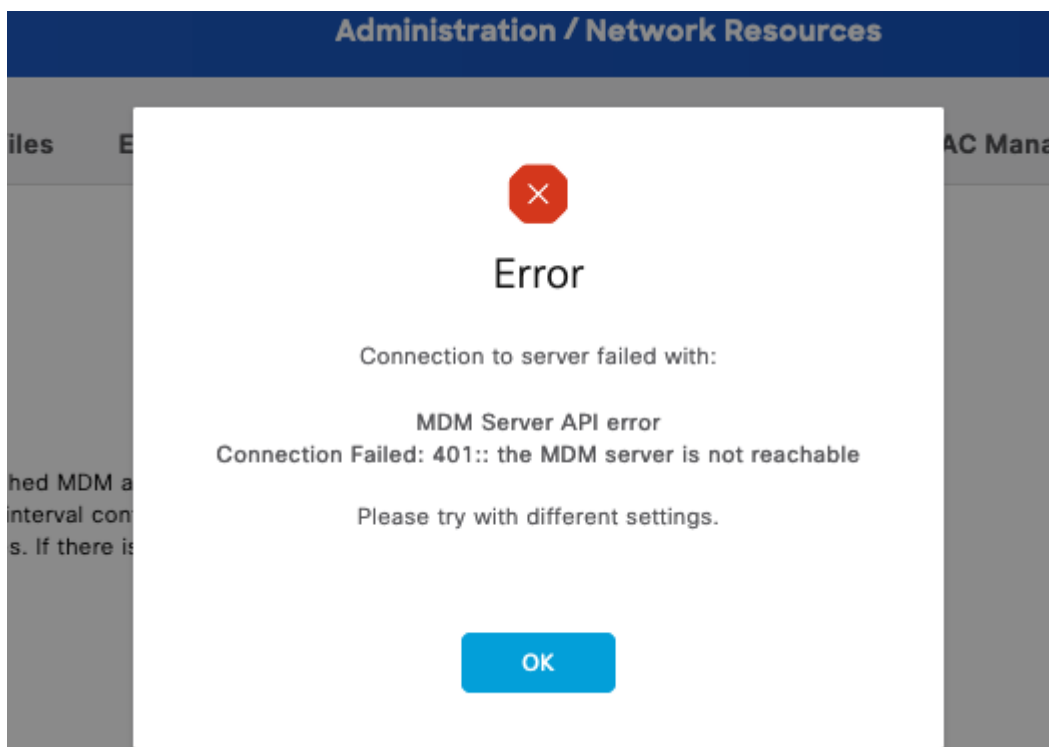
Paquetes involucrados en el error 404 MDM

### Situación 3. Error de conexión: 401

Este error en la conexión indica un problema con el usuario que está implementando en la configuración de MDM para integrar.

Verifique que el usuario:

- Existe en la cuenta JAMF.
- Dispone de los privilegios adecuados para completar la integración con ISE.
- Y se puede utilizar para realizar la autenticación de API (como se ha descrito anteriormente en esta guía).



código de error de conexión MDM 401

Los registros de ISE indican este comportamiento:

```
INFO [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- GET: MDM Server URL: https://YOUR
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- Proxy Config in request = [,PROX
ERROR [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- Error message while connecting to
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDom: end HTTP requ
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDomNonComp: end HT
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::- retry connecting using api v
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::- MDM Rest API Server Query St
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::- MDM Rest API Server Query PA
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::- 2. On Error : re-connecting
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDom: start HTTP re
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDomNonComp: start
```

```

DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- ===mdmFlowInfo===null,=====server
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- QueryType is heartbeatQuery
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- using httpClient for http query -
INFO [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- GET: MDM Server URL: https://YOUR
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- Proxy Config in request = [,PROX
ERROR [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- Error message while connecting to
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDom: end HTTP requ
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -:::- sendGETRequestDomNonComp: end HT
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::- retry connecting using api v

```

La captura de paquetes revela un comportamiento similar al de esta imagen:

Source	Protocol	Length	Info
10.88.240.21	HTTP	183	CONNECT :443 HTTP/1.1
10.31.104.78	HTTP	105	HTTP/1.1 200 Connection established
10.88.240.21	TLSv1.2	419	Client Hello
10.31.104.78	TLSv1.2	213	Server Hello, Change Cipher Spec, Encrypted Handshake Message
10.88.240.21	TLSv1.2	72	Change Cipher Spec
10.88.240.21	TLSv1.2	111	Encrypted Handshake Message
10.88.240.21	TLSv1.2	349	Application Data
10.31.104.78	TLSv1.2	1071	Application Data
10.88.240.21	TLSv1.2	349	Application Data
10.31.104.78	TLSv1.2	1071	Application Data

Paquetes MDM involucrados en el error 401

## Información Relacionada

- [Integración de JAMF con ISE 2.X como MDM](#)
- [Solucionar problemas y habilitar depuraciones en ISE](#)
- [Cómo habilitar las depuraciones en las versiones de ISE 3.x.](#)

## 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).