

Integrar o ISE 3.3 com JAMF como um servidor MDM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Preparação do JAMF PRO para a conexão MDM](#)

[Preparando o ISE para a conexão MDM](#)

[Verifique a conectividade inicial da integração com a instância JAMF PRO.](#)

[Troubleshooting de Servidor MDM Inacessível](#)

[Cenário 1. Tempo Limite de Conexão Excedido](#)

[Cenário 2. Falha na Conexão: 404](#)

[Cenário 3. Falha na Conexão: 401](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve os procedimentos necessários para implementar o Identity Services Engine v3.3 com a instância JAMF PRO 10.48.X.

Pré-requisitos

Requisitos

A Cisco recomenda conhecimento sobre estes tópicos:

- Identity services engine (ISE)
- JAMF como uma solução MDM

Componentes Utilizados

As informações neste documento são baseadas nestes softwares e versões:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

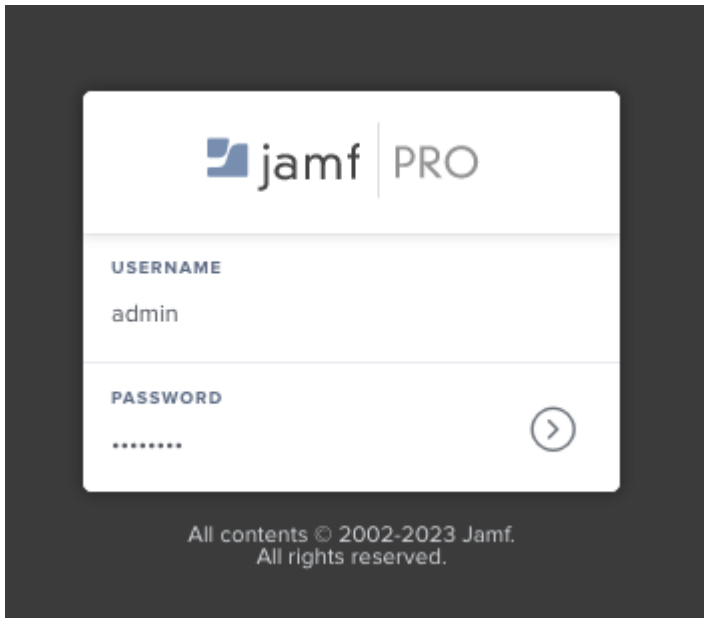
O Cisco ISE suporta JAMF como um servidor MDM para gerenciar computadores Windows. Quando esses computadores (gerenciados pelo JAMF) são conectados e autenticados, o ISE recupera informações de conformidade dos servidores JAMF para recuperar mais informações sobre a postura de segurança desses dispositivos.

Ele usa as informações para reforçar a segurança de acesso seguro permitindo/negando esses computadores, dependendo dos critérios e condições configurados no ISE. Portanto, essa implementação ajuda a identificar possíveis vulnerabilidades e pontos fracos na segurança que podem ser explorados pelos invasores.

Configurar

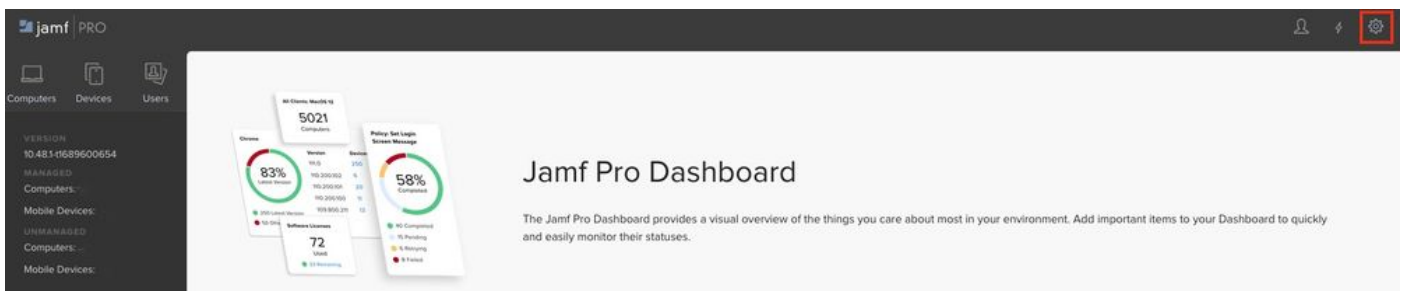
Preparação do JAMF PRO para a conexão MDM

Etapa 1. Faça login com sua nuvem JAMF com a conta para privilégios de administrador em: https://YOUR_ACCOUNT.jamfcloud.com/index.html.



Página de login do JAMF PRO

Etapa 2. No menu principal, selecione o ícone da engrenagem.



Painel JAMF PRO

Etapa 3. No menu principal, escolha Sistema > Contas de usuário e grupos.

Settings

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

System 11 settings

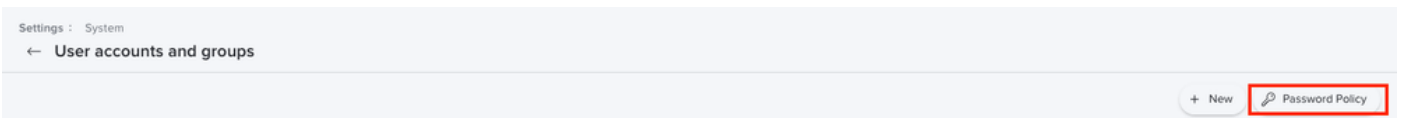


User accounts and groups

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

Configurações do sistema JAMF PRO

Etapa 4. Selecione a opção Password Policy.



Contas e grupos de usuários do JAMF PRO

Etapa 5. Nesta seção, confirme se você tem a opção Allow Basic Authentication além de Bearer Token Authentication.



Note: Começando com JAMF PRO v10.35, a autenticação básica para a API não é habilitada por padrão. Portanto, você deve habilitar esses recursos para garantir que a integração de MDM esteja funcionando.

Para obter mais informações, reveja as [Alterações da Autenticação de API Clássica](#).

Etapa 6. Depois que o último recurso estiver habilitado, vá para o menu Configurações descrito na Etapa 3, procure por Rede IntegrationMenu e selecione-o.

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

Integração de rede JAMF PRO

Etapa 7. Continue para selecionar + Novo para adicionar uma nova instância ao ISE 3.3.

Settings : Network

← Network integration

+ New

NAME

No Network integration

Configurações de integração de rede JAMF PRO

Etapa 8. No menu suspenso em Network Access Management Service, deixe a opção marcada como Cisco ISE.

- Em seguida, forneça um nome no menu Display Name, conforme mostrado neste exemplo.
- Para as configurações iniciais e a conexão para o ISE, a configuração pode ser deixada com essas configurações padrão.
- Continue em Save the configuration.

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

Exemplo de configuração Integração de rede com ISE

Etapa 9. A integração gera um URL de integração de rede com este formato:

https://YOUR_ACCOUNT.jamfcloud.com/networkIntegrationEndpoint/ID. Salvar esta URL porque você deve usá-la posteriormente para se conectar ao ISE.

Preparando o ISE para a conexão MDM

Etapa 1. Selecione o Menu > Administração > Recursos de rede > MDM externo e clique em Adicionar.

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.					

menu de integração de MDM do ISE

Etapa 2. Nomeie a instalação no segmento MDM / UEM Integration Name.

- Na seção Nome de host/Endereço IP, selecione YOUR_ACCOUNT.jamfcloud.com no URL gerado nas etapas anteriores.

- Em Port, selecione o 443 para a conexão HTTPS com sua instância JAMF PRO.
- Na seção Instance Name, prossiga para inserir os valores com a seção ausente do URL criado (neste caso: /networkIntegrationEndpoint/ID).
- Insira um nome de usuário com acesso total à instância do JAMF PRO junto com a senha correspondente.
- Altere o Status do servidor MDM para 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)

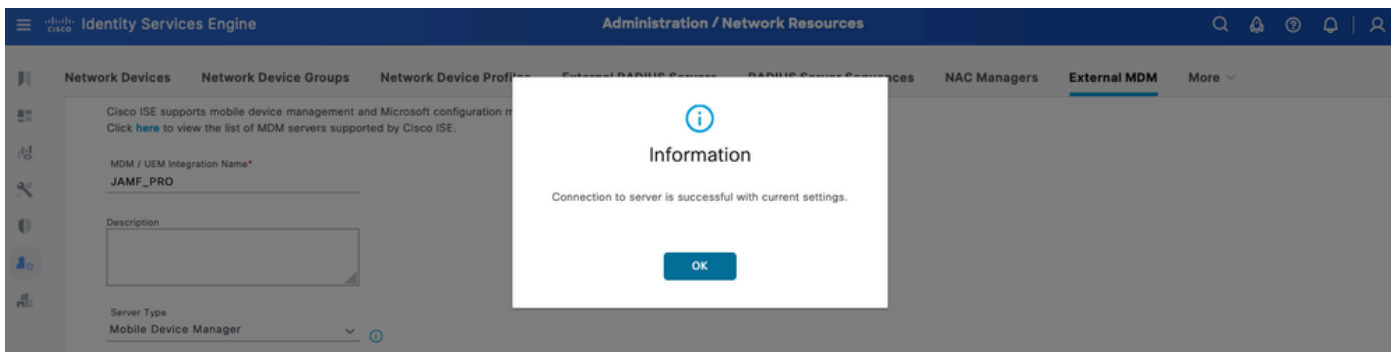
When re-authenticating an endpoint into the network Cisco ISE refers to cached MDM attributes of the endpoint. If the age of the cached MDM attributes is greater than the interval configured, Cisco ISE sends a fresh query to the MDM server for the endpoint's attributes. If there is a change in compliance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

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

Status
Enabled

Exemplo de configuração do ISE MDM JAMF PRO

Etapa 3. Role para baixo e continue até Testar conexão. Se a conexão for bem-sucedida, esta imagem será exibida. Se você não receber a mesma saída, consulte a Seção Troubleshooting neste documento.



Conexão bem-sucedida com a conta MDM JAMF





Etapa 4. Selecione OK na opção anterior. Na parte inferior da página, localize o Identificador de dispositivo onde o ISE se associa à sessão do endpoint.

- Dependendo do cenário, você pode selecionar o endereço MAC do dispositivo ou os atributos do certificado.
- Depois de personalizar esta seção, salve a configuração.

 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

Configuração adicional para o servidor MDM

Verifique a conectividade inicial da integração com a instância JAMF PRO.

Captura do pacote: No caso de uma conectividade bem-sucedida, você pode visualizar o tráfego HTTPS que é enviado do servidor PAN ISE para a instância 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

Exemplo de captura de pacote de conectividade com a instância JAMF

Logs no ISE: O ISE processa e analisa os dados de forma correspondente, conforme mostrado no 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.verifyServer
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::- apiVersionSb : 3, mdmApiVersion : 1
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 Parameters
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,=====serverInfo=====
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/MDM/ServerInfo
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
```

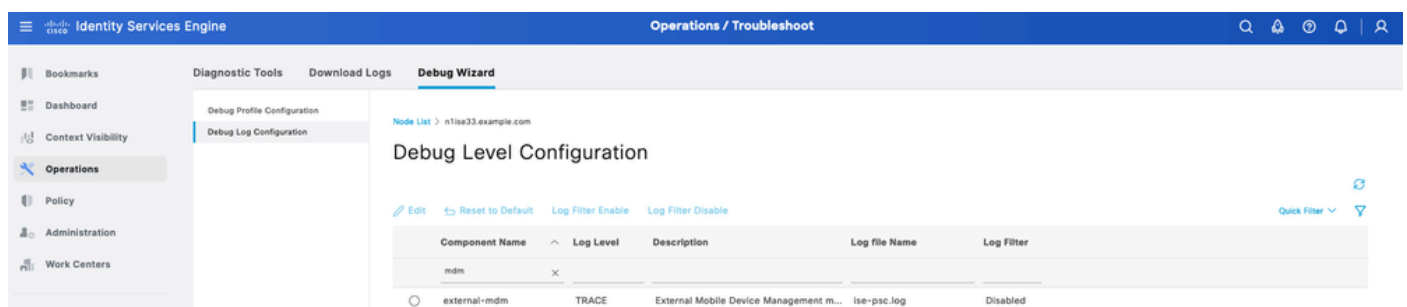
```
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.api.MdmServerInfoApi -:::- returning from the method : ca
  apiPath: /ID/ciscoise/v3
  redirectUrl: https://YOUR_ACCOUNT.jamfcloud.com/enroll
  queryMaxSize: 1000
  apiVersion: 3
  vendor: JAMF Software
  productName: JSS
  productVersion: 10.48.1-t1689600654
  COMMA: ,
  errorMsg: null
  errorOccurred: false
}
```

Troubleshooting de Servidor MDM Inacessível

A base dessa integração consiste em consultas que o ISE executa periodicamente para a instância JAMF-PRO. O ponto de referência onde a solução de problemas é executada (nessa instância) é o Nó de Administração Principal (PAN). O nó PAN é onde o método de conectividade é configurado para acessar o servidor MDM. Esse mesmo método é replicado em todos os nós para a implementação.

As próximas etapas podem ser aplicadas para solucionar problemas de acessibilidade.

Etapa 1. Ative o componente external-mdm no nível TRACE no nó PAN.

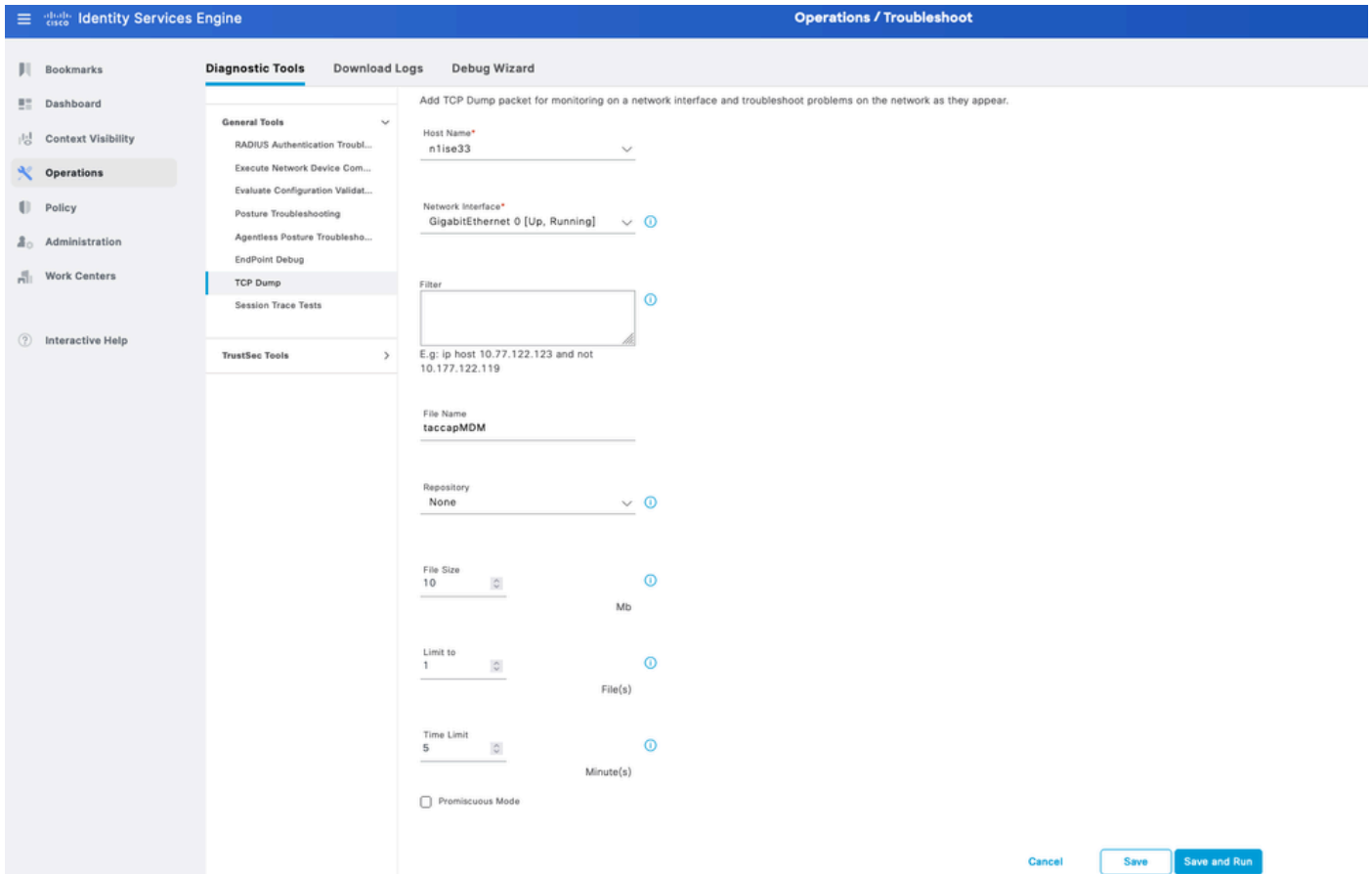


The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Operations / Troubleshoot'. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations (selected), Policy, Administration, and Work Centers. The main content area is titled 'Debug Wizard' and shows 'Debug Level Configuration' for a node named 'n1se33.example.com'. There are buttons for 'Edit', 'Reset to Default', 'Log Filter Enable', and 'Log Filter Disable'. A table below lists the configuration for the 'external-mdm' component.

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

Componente MDM externo no nível TRACE para solução de problemas

Etapa 2. Configure uma captura do nó PAN e Salve sua configuração.



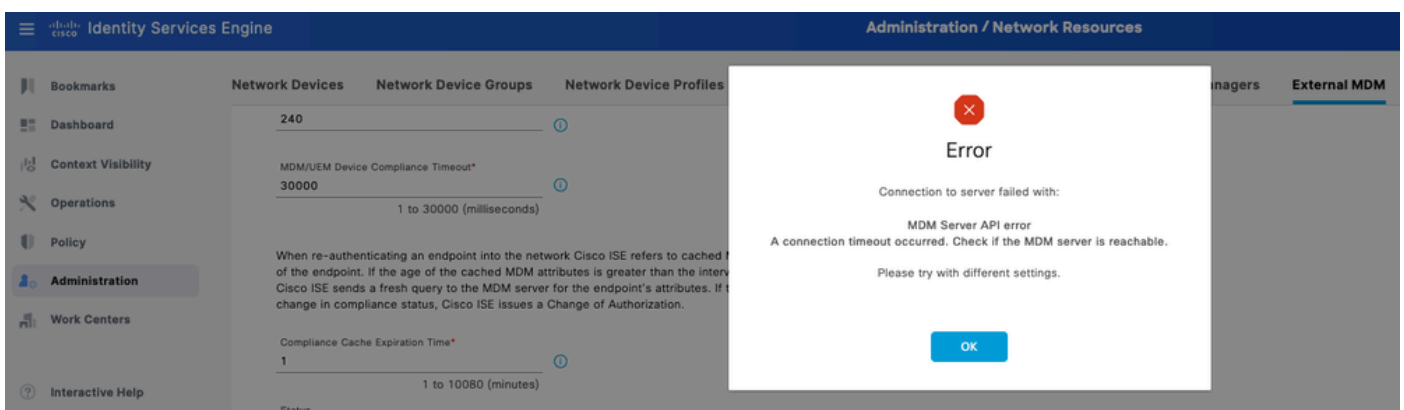
Exemplo de captura de pacote para coletar informações de conexão MDM

Etapa 3. Navegue pelo menu External MDM. Execute a captura na Etapa 2 e selecione o botão Test Connection. Aguarde até que o erro seja exibido.

Etapa 4. Interrompa a captura da Etapa 2. Revise os logs correspondentes ao ise-psc.log para analisar o comportamento.

Cenário 1. Tempo Limite de Conexão Excedido

No cenário, quando você recebe esse erro no ISE ao testar a conexão com JAMF:



Os logs relacionados ao MDM externo revelam estas informações:

```
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 Parameters
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 URL: https://YOUR_ACCOUNT.jamfcloud.com
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
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.api.MdmClient -:::::- A connection timeout occurred. Check the MDM server URL and port
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
}
```

Na captura de pacotes, revise as próximas informações:

Tráfego DNS - O ISE executa uma consulta em relação à instância relacionada ao JAMF se você inserir o nome de host na parte de configuração da integração. Se você não vir a resolução do nome do host, tente usar o endereço IP. Esta opção está disponível para configurar em vez do nome do 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

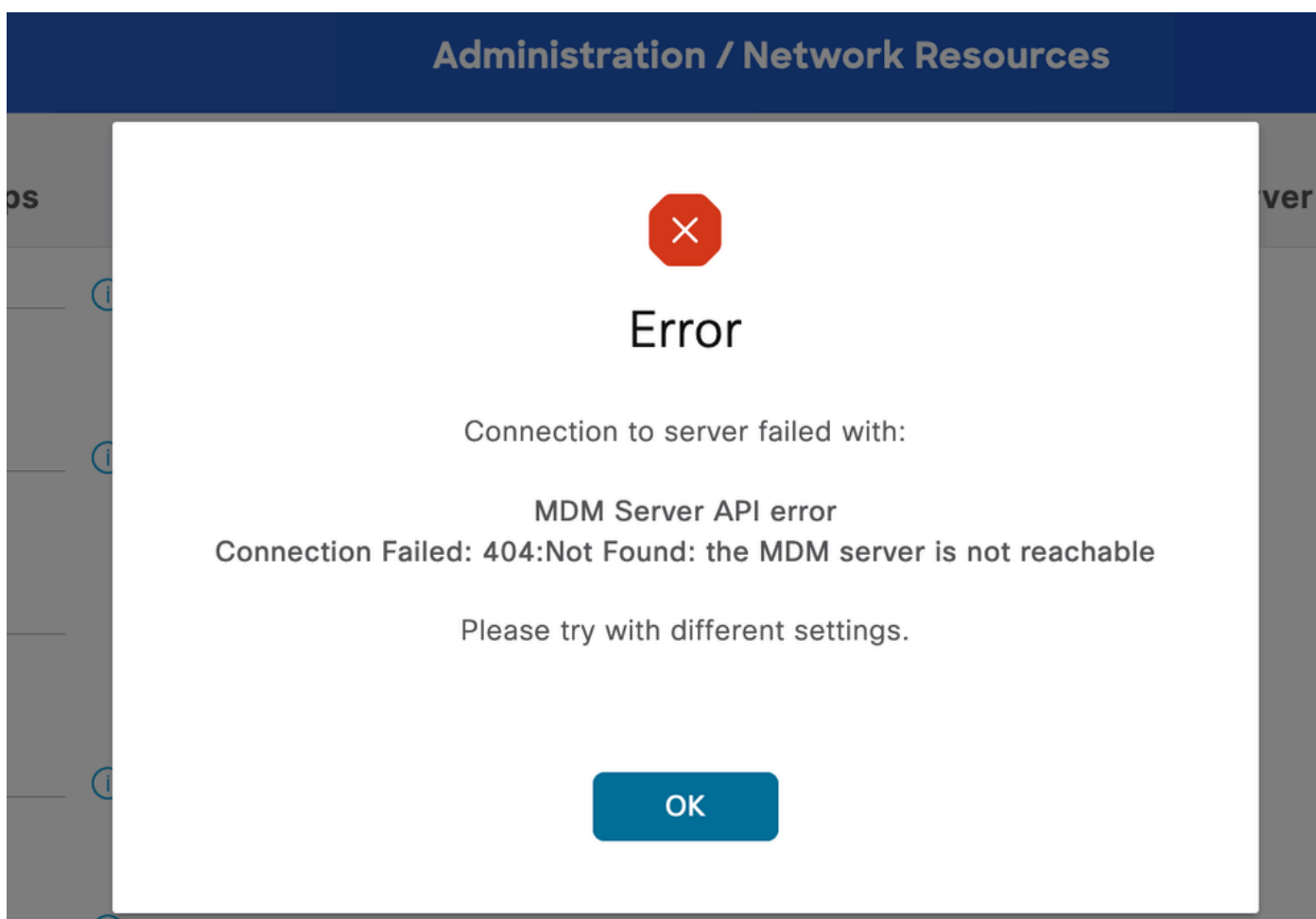
Retransmissões na porta de conexão MDM - Se você consultar o endereço IP diretamente (fornecido na consulta DNS ou na configuração MDM), poderá ver os pacotes SYN repetidos. Isso indica que não há rota direta para a instância JAMF ou para um dispositivo externo interferindo nas comunicações na porta 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

Exemplo de conexão com o tempo limite de MDM

Cenário 2. Falha na Conexão: 404

Este evento indica que você tem conectividade com sua conta JAMF configurada ao configurar o servidor MDM. No entanto, a instância que você indicou para conexão não existe ou contém um erro, pois não foi encontrada.



Exemplo de erro 404 de MDM

Os logs correspondentes a este evento são exibidos:

```

DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmServerInfoApi -:::::- inside the method : callMdmServerInfo
TRACE [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -:::::- Inside MDMVerifyServer.verifyServer
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 : 3
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
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 /mdm-server-info to /mdm-server-info
INFO [admin-http-pool37][[]] cpm.admin.infra.spring.ISEAdminControllerUtils -::admin::- mapping path /mdm-server-info to /mdm-server-info
INFO [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmServersCache -:::::- MDM server - Status : Active, MDM Version : 3.0.0
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

```

A captura de pacote neste momento fornece uma conexão HTTPS que contém dados de aplicativo que estão sendo transferidos entre o site JAMF e o 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

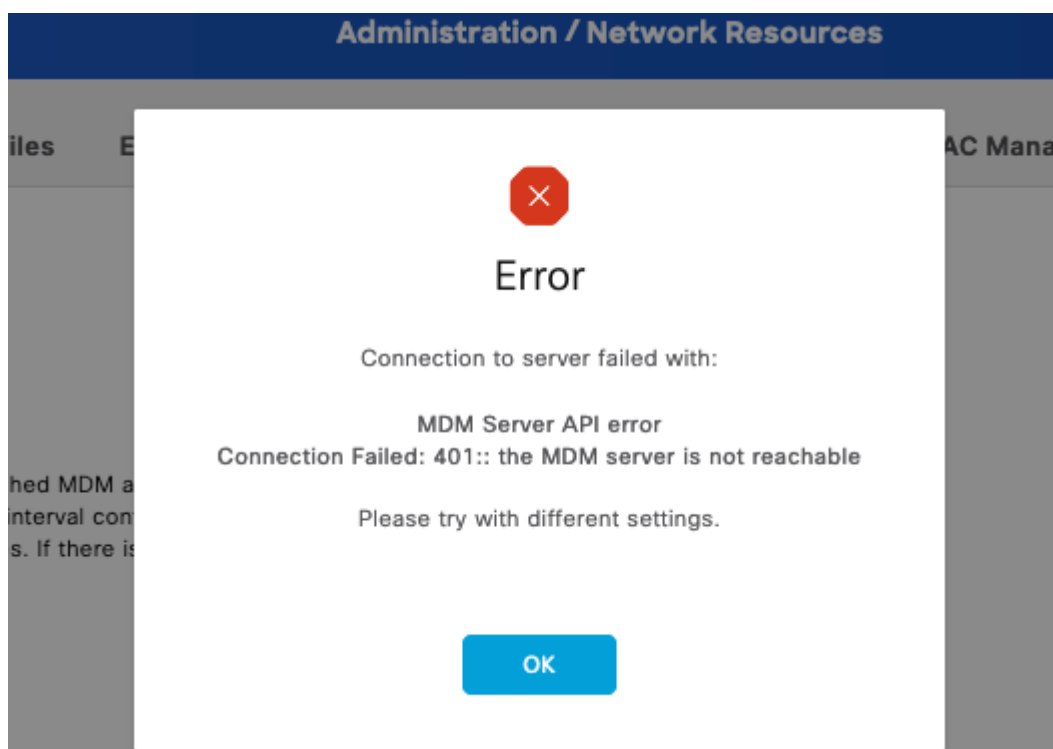
Pacotes envolvidos no erro 404 MDM

Cenário 3. Falha na Conexão: 401

Esse erro na conexão indica um problema com o usuário que você está implantando na configuração do MDM para integrar.

Verifique se o usuário:

- Existe na conta JAMF.
- Tem os privilégios apropriados para concluir a integração com o ISE.
- E pode ser usado para executar a autenticação da API (conforme descrito anteriormente neste guia).



Código de erro de conexão MDM 401

Os logs no ISE indicam este comportamento:

```
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

```

A captura de pacotes revela um comportamento semelhante ao desta imagem:

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

Pacotes MDM envolvidos no erro 401

Informações Relacionadas

- [Integração JAMF com ISE 2.X como MDM](#)
- [Solucionar problemas e ativar depurações no ISE](#)
- [Como habilitar depurações em versões do ISE 3.x.](#)

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.