Integrate ISE 3.3 with JAMF as an MDM Server

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Preparing JAMF PRO for the MDM Connection
- Preparing ISE for the MDM connection

Verify the Initial Connectivity of the integration with JAMF PRO instance.

Troubleshooting MDM Server is not Reachable

- Scenario 1. A Connection Timeout Occurred
- Scenario 2. Connection Failed: 404
- Scenario 3. Connection Failed: 401

Related information

Introduction

This document describes procedures that are necessary to implement Identity Services Engine v3.3 with JAMF PRO instance 10.48.X.

Prerequisites

Requirements

Cisco recommends knowledge in these topics:

- Identity Services Engine (ISE)
- JAMF as an MDM Solution

Components Used

The information in this document is based on these software and versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

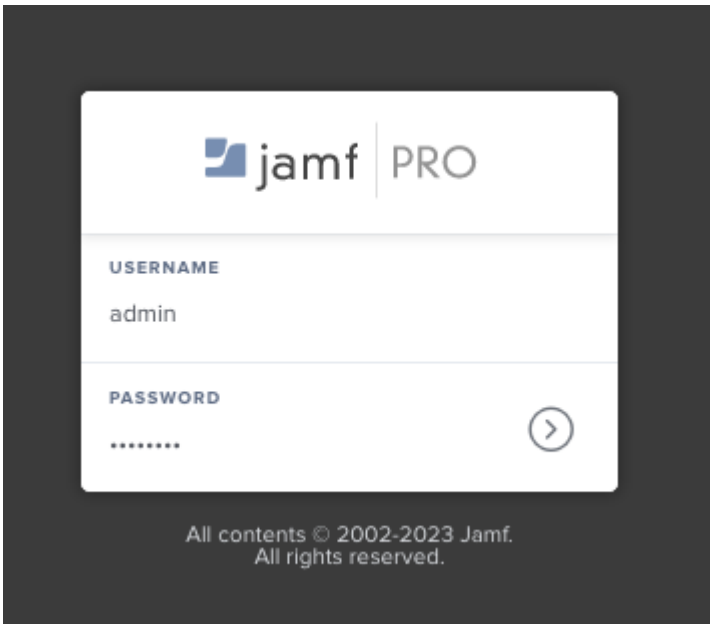
Cisco ISE supports JAMF as an MDM Server for managing Windows computers. When these computers (managed by JAMF) they are connected and authenticated, ISE retrieves compliance information from JAMF Servers to retrieve further information for the security posture of those devices.

It uses the information to enforce secure access security by allowing/denying those computers, depending on the criteria and conditions configured in ISE. Therefore, this implementation helps to identify potential vulnerabilities and security weaknesses that could be exploited by attackers.

Configure

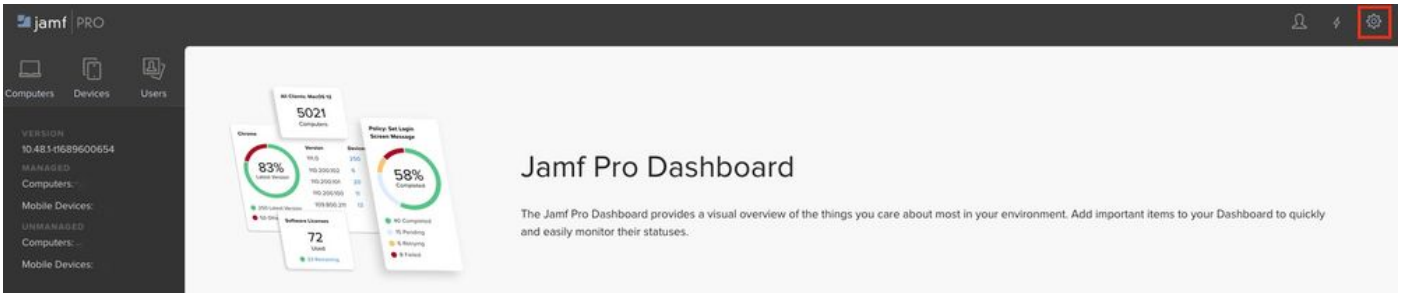
Preparing JAMF PRO for the MDM Connection

Step 1. Log in with your JAMF cloud with the account for admin privileges at: https://YOUR_ACCOUNT.jamfcloud.com/index.html.



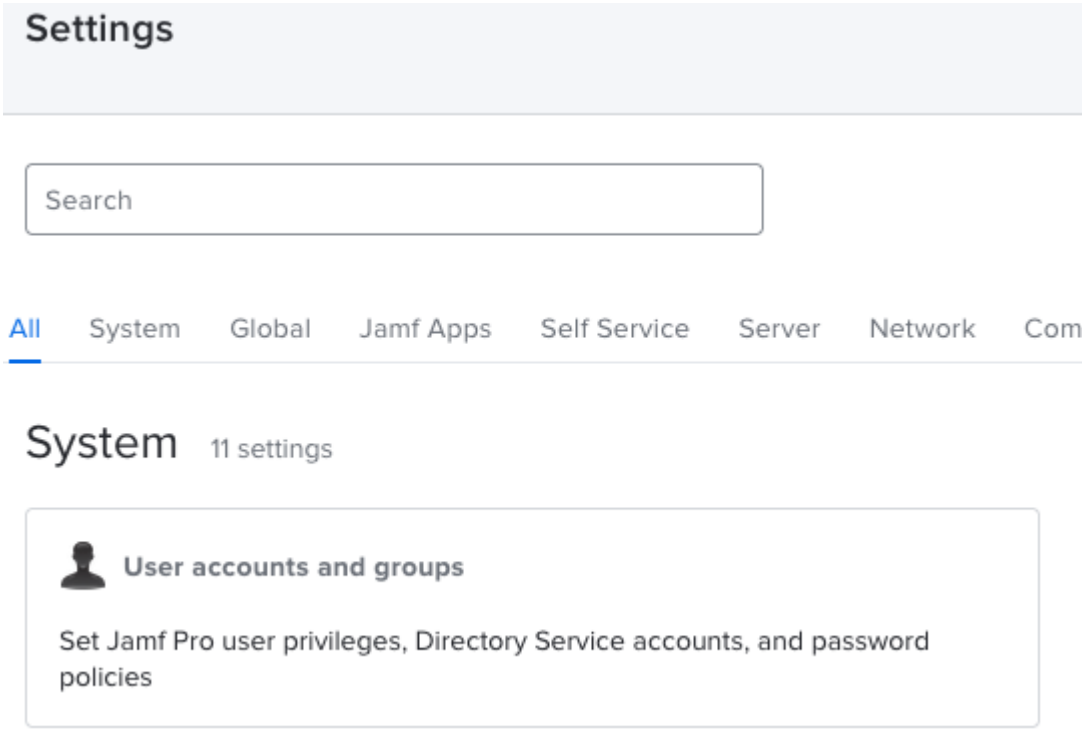
JAMF PRO login page

Step 2. From the Main Menu, select the gear icon.



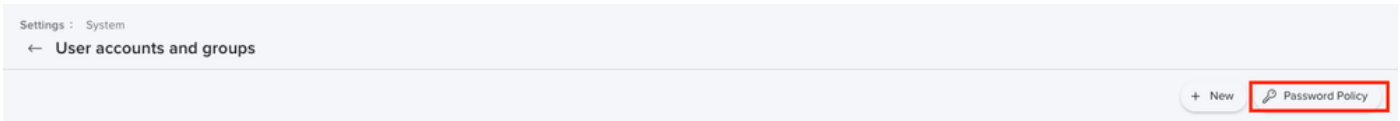
JAMF PRO Dashboard

Step 3. On the Main Menu, choose **System** > **Useraccounts and groups**.



JAMF PRO System Settings

Step 4. Select the option **Password Policy**.



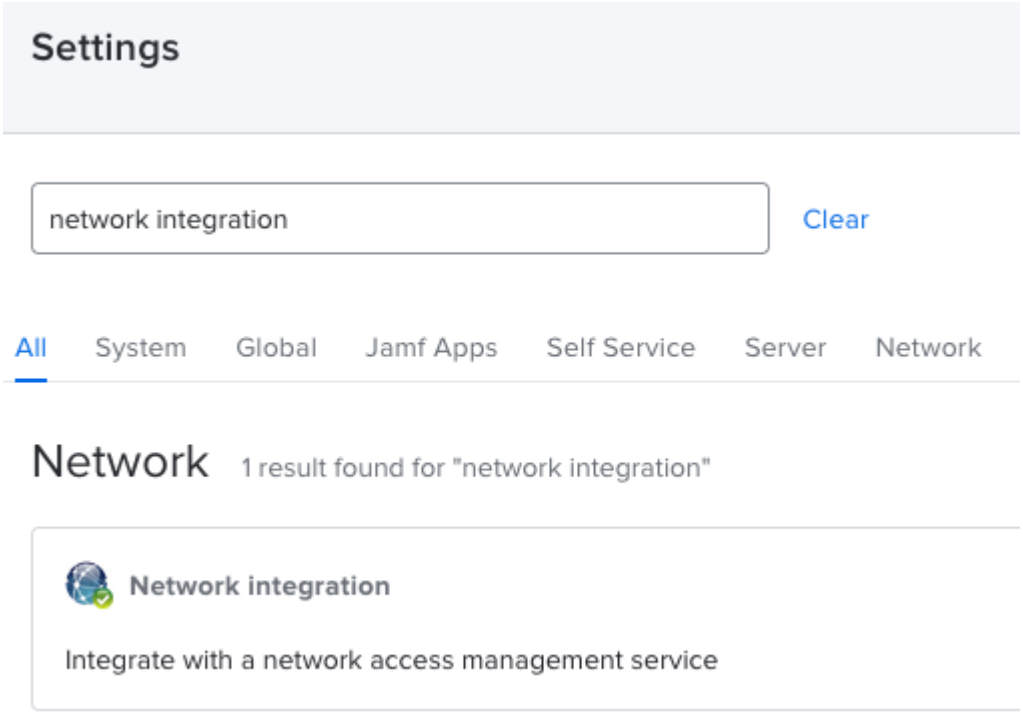
JAMF PRO Users accounts and groups

Step 5. In this section, confirm you have the option **Allow Basic Authentication in addition to Bearer Token Authentication**.

Note: Starting with JAMF PRO v10.35, the basic authentication for the API is not enabled by default. Therefore, you must enable these features to ensure the MDM integration is working.

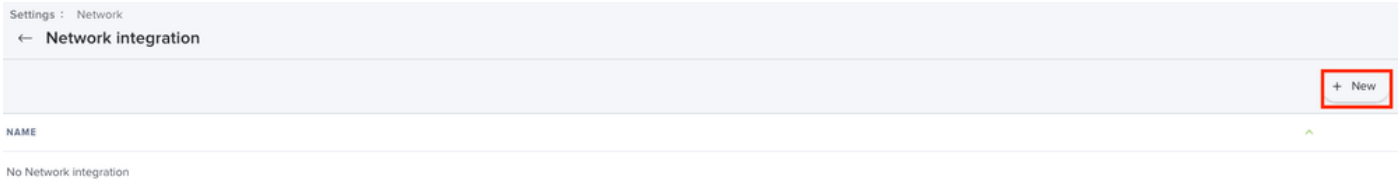
For more information please review Classic API Authentication Changes.

Step 6. Once you have the last feature enabled, go to the Menu **Settings** described in Step 3, then look for the **Network IntegrationMenu**, and select it.



JAMF PRO Network integration

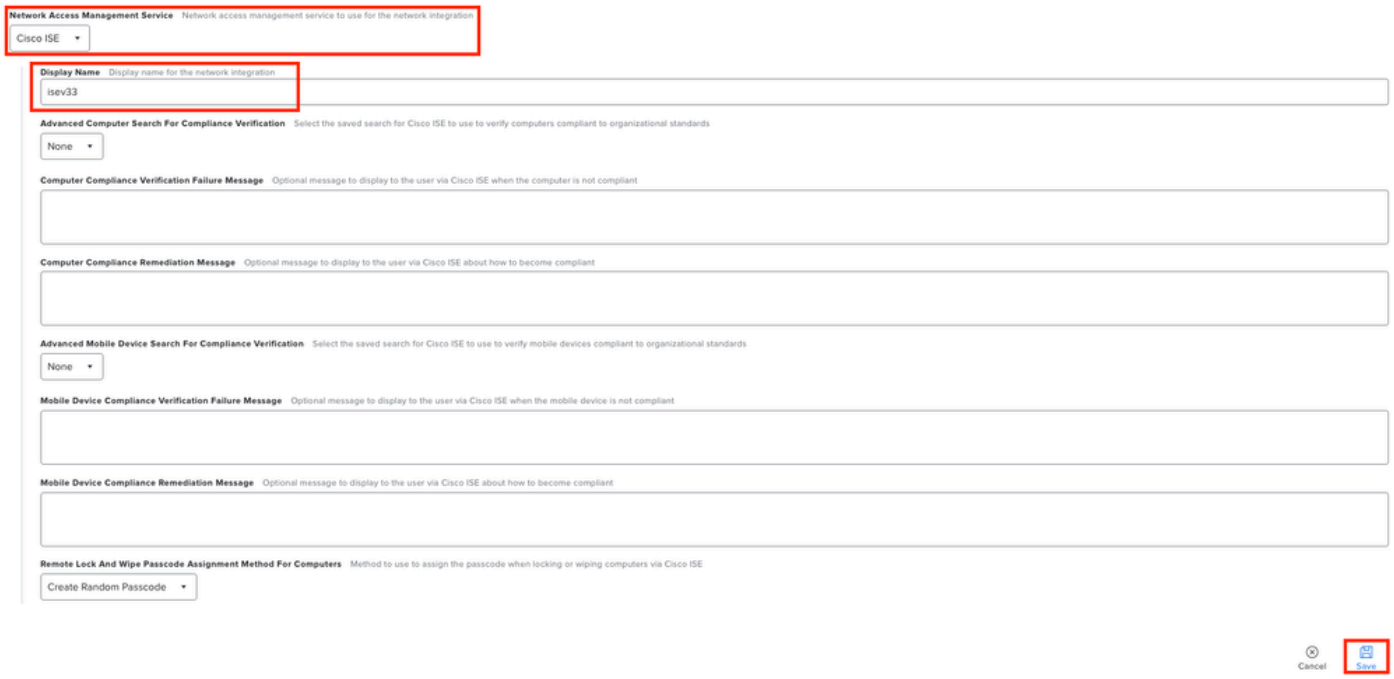
Step 7. Proceed to select **+ New** to add a new instance for ISE 3.3.



JAMF PRO Network integration settings

Step 8. In the drop-down menu under **Network Access Management Service**, leave the option marked as **Cisco ISE**.

- Next provide a name in the menu **Display Name** as it is shown in this example.
- For the initial settings and the connection for ISE, the configuration can be left with these standard configurations.
- Proceed to **Save** the configuration.

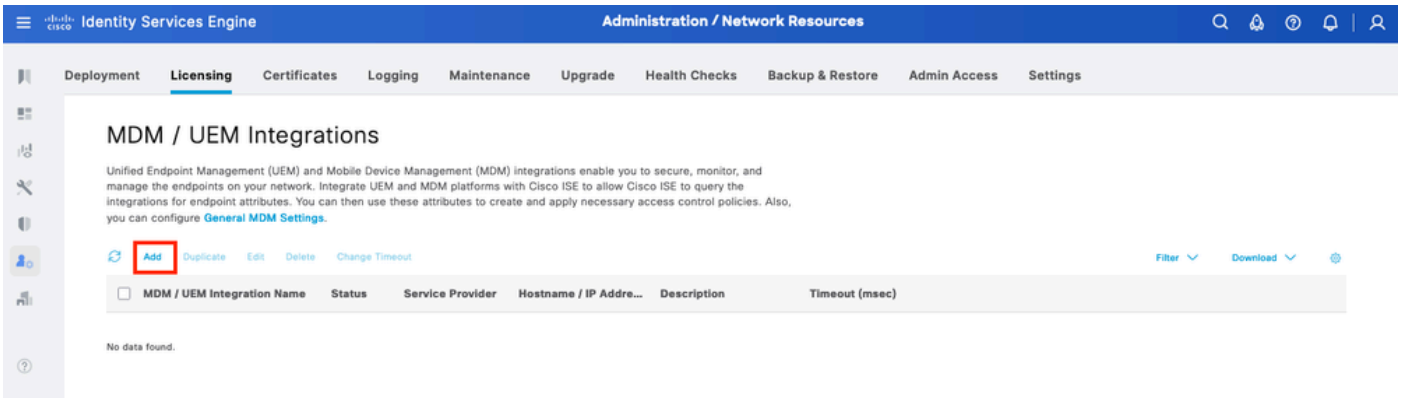


Configuration sample Network integration with ISE

Step 9. The integration generates a **Network Integration URL** with this format: https://YOUR_ACCOUNT.jamfcloud.com/networkIntegrationEndpoint/ID. Save this URL because you must use it later to connect with ISE.

Preparing ISE for the MDM connection

Step 1. Select the **Menu** > **Administration** > **Network Resources** > **External MDM**, and then click **Add**.



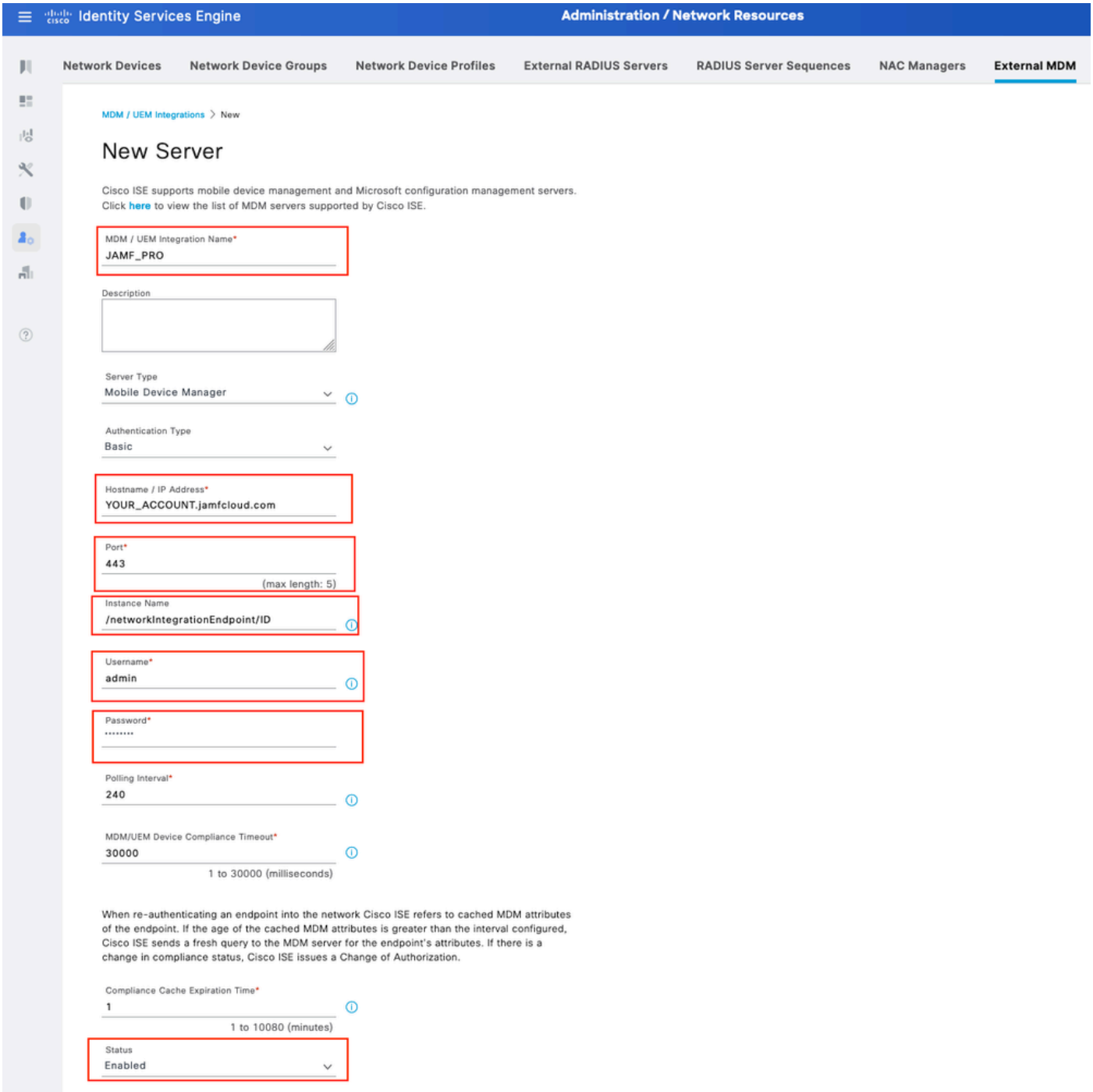
ISE MDM integration menu

Step 2. Name the installation within the **MDM / UEM Integration Name** segment.

- In the section **Hostname / IP Address,** select **YOUR_ACCOUNT.jamfcloud.com** from the URL generated in previous steps.
- In **Port,** select the 443 for the HTTPS connection with your JAMF PRO instance.
- In the section **Instance Name**, proceed to enter the values with the section missing from the URL

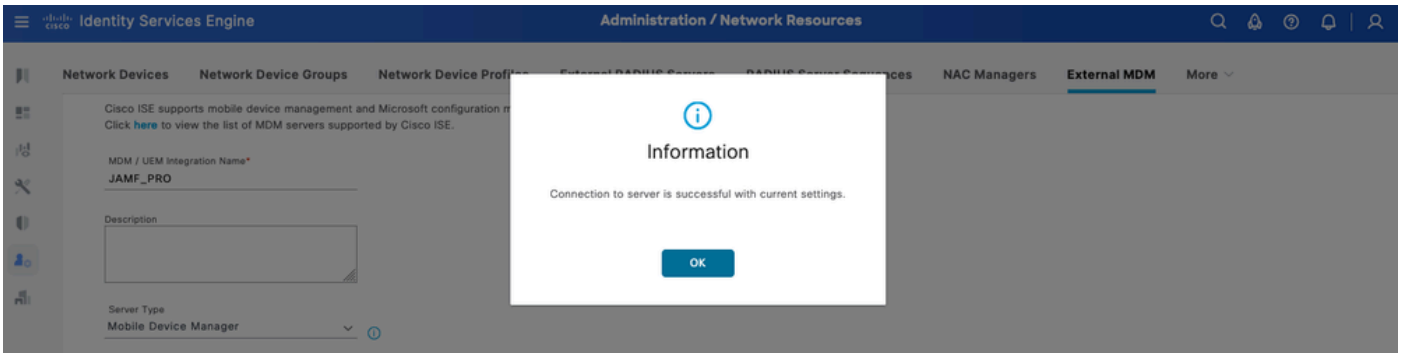
created (in this case: /networkIntegrationEndpoint/ID).

- Input a **Username** with full access to the JAMF PRO instance alongside the corresponding **Password**.
- Change the **Status** of the MDM server to **Enabled**.



ISE MDM JAMF PRO configuration example

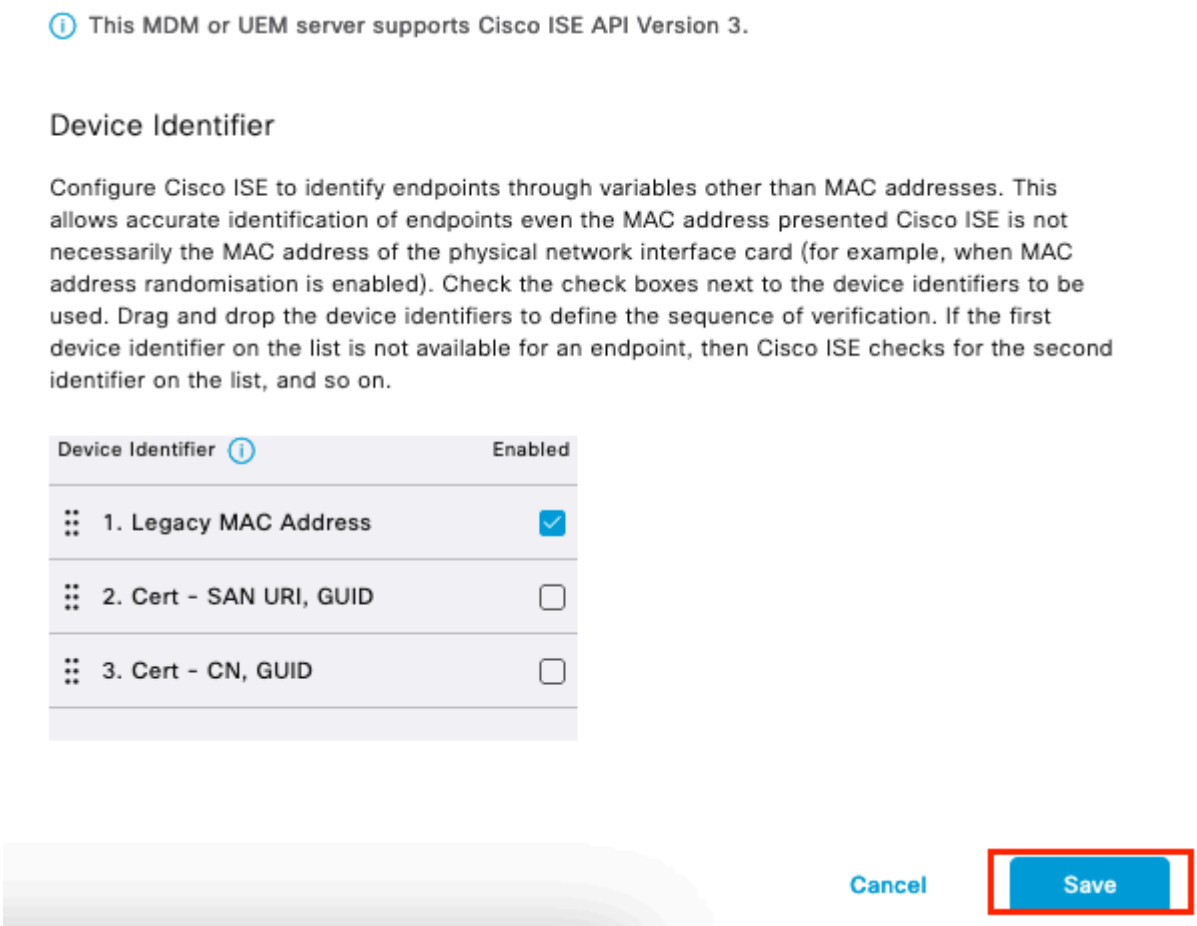
Step 3. Scroll down and proceed to **Test Connection**. If the connection is successful, this image is displayed. If you do not receive the same output, please refer to the Troubleshooting Section in this document.



Successful connection with the MDM JAMF account

Step 4. Select **OK** in the option previously. At the bottom of the page, find the **Device Identifier** where the ISE associate of the session of the endpoint.

- Depending on your scenario, you can select the MAC address of the device or the attributes of the certificate.
- Once you have customized this section, **Save** the configuration.



Additional configuration for MDM server

Verify the Initial Connectivity of the integration with JAMF PRO

instance.

Packet Capture: In the case of a successful connectivity, you can view the HTTPS traffic that is sent from the ISE PAN server to the JAMF PRO instance:

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 [redacted] 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

Packet capture example of connectivity with JAMF instance

Logs on ISE: The ISE processes and analyzes the data correspondingly as shown in the ise-psc.log:

```
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::- inside the method : callMdmSer
TRACE [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- Inside MDMVerifyServer.veri
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- apiVersionSb : 3, mdmApiVer
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- MDM Rest API Server Query S
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- MDM Rest API Server Query P
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- 1. Connecting to the MDM se
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDom: start  HTTP r
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDomNonComp: start
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://YOU
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- Proxy Config in request  = [,PRO
.
.
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>mdmin
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDom: end  HTTP req
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDomNonComp: end  H
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
```

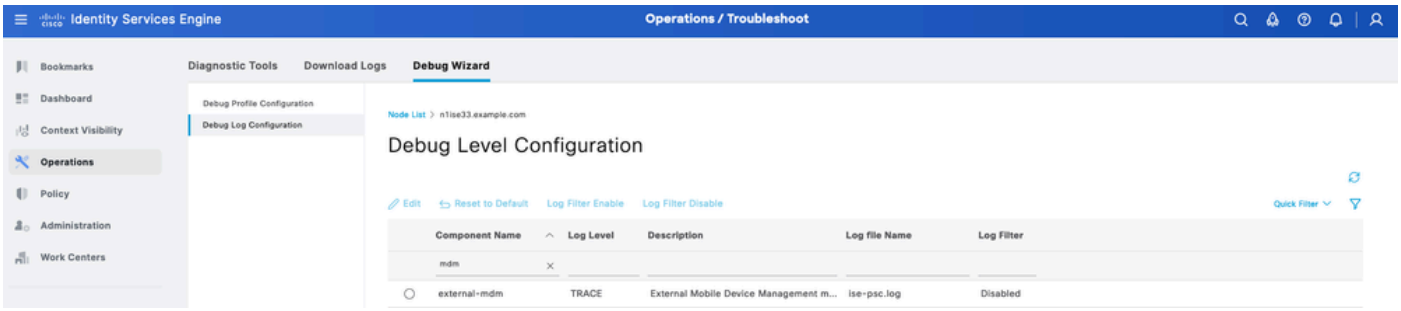
```
  vendor: JAMF Software
  productName: JSS
  productVersion: 10.48.1-t1689600654
  COMMA: ,
  errorMsg: null
  errorOccurred: false
}
```

Troubleshooting MDM Server is not Reachable

The base of this integration consists of queries that ISE performs periodically to the JAMF-PRO instance. The point of reference where troubleshooting is performed (in this instance) is the Primary Administration Node (PAN). The PAN node is where the connectivity method is configured to reach the MDM server. This same method is replicated in all nodes for the implementation.

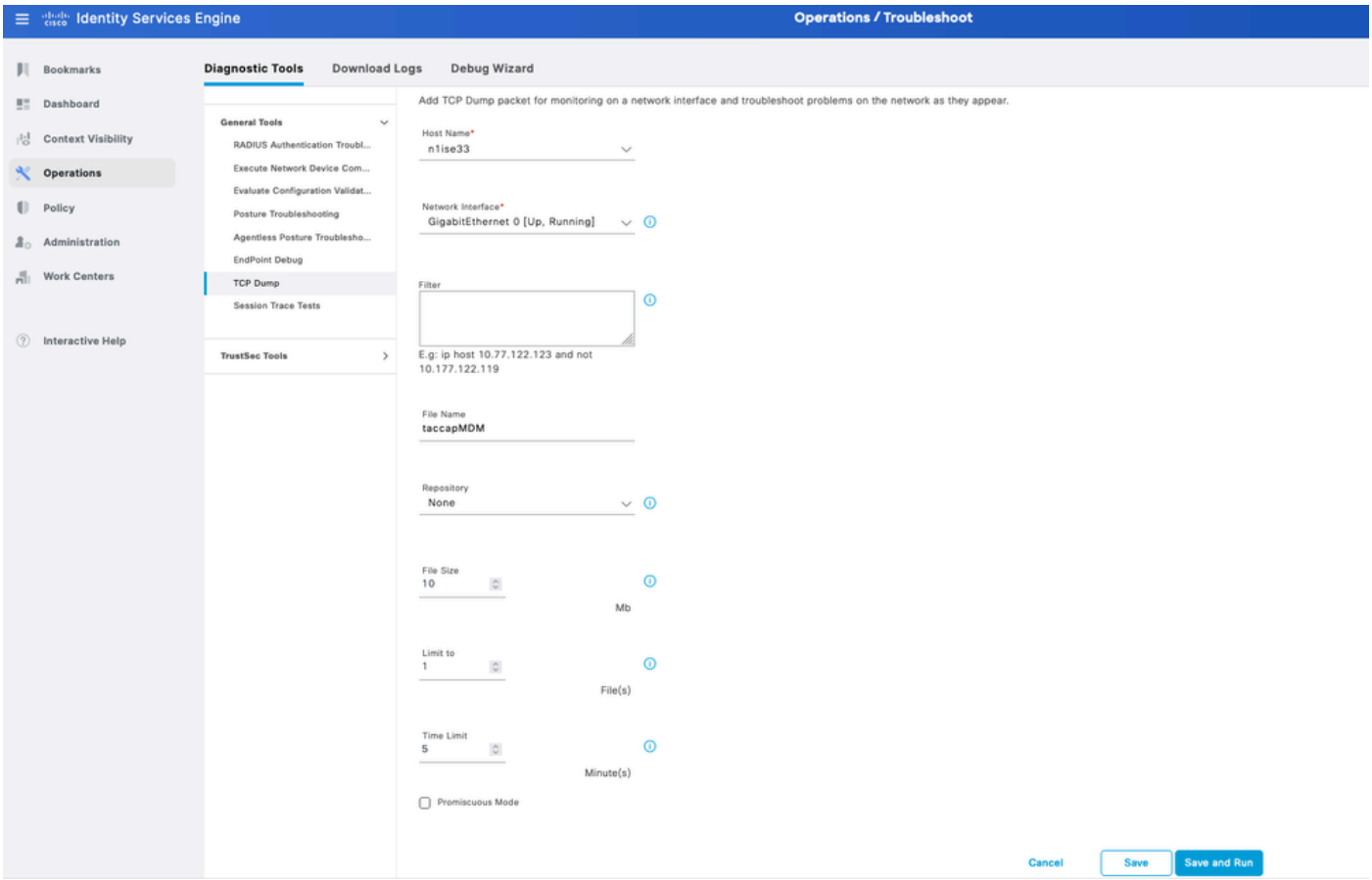
The next steps can be applied for troubleshooting reachability problems.

Step 1. Enable the component **external-mdm** at the **TRACE** level on the PAN node.



External MDM component in TRACE level to troubleshoot

Step 2. Setup a capture from the PAN node and **Save** your configuration.



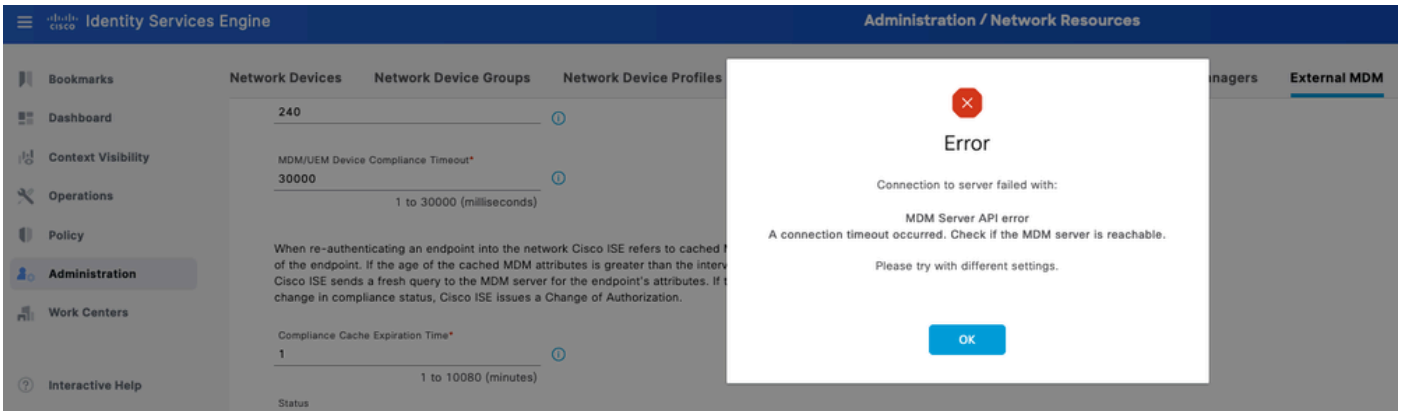
Packet capture example to collect information of MDM connection

Step 3. Navigate through the **External MDM** Menu. **Run** the capture from **Step 2** and select the button **Test Connection.** Wait for the error to appear.

Step 4. Stop the capture from **Step 2.** Review the logs corresponding ise-psc.log to analyze the behavior.

Scenario 1. A Connection Timeout Occurred

In the scenario, when you receive this error in ISE while testing the connection with JAMF:



MDM error connection timeout

The logs related to external MDM reveal this information:

```
TRACE [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- Inside MDMVerifyServer.veri
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- API version retrieved from
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- apiVersionSb : 3, mdmApiVer
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- MDM Rest API Server Query S
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- MDM Rest API Server Query P
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- 1. Connecting to the MDM se
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDom: start  HTTP r
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDomNonComp: start
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- ===mdmFlowInfo===null,=====serve
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://YOU
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,
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- Error message while connecting t
Connection Failed to the MDM server host - YOUR_ACCOUNT.jamfcloud.com, and port - 443 : Connection time
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDom: end  HTTP req
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDomNonComp: end  H
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- Exception occurred while co
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.api.MdmClient -::::- A connection timeout occurred. Check
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::- returning from the method : ca
  apiPath: null
  redirectUrl: null
  queryMaxSize: null
  apiVersion: null
  vendor: null
  productName: null
  productVersion: null
  COMMA: ,
  errorMsg: null
  errorOccurred: true
}
```

From the packet capture, review the next information:

DNS Traffic - The ISE performs a query towards your JAMF related instance if you input the hostname in the setup portion of the integration. If you do not see the resolution of the hostname, attempt to use the IP address. This option is available to configure instead of the hostname.

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

DNS traffic in a MDM flow

Retransmissions in the MDM Connection Port - If you query the IP address directly (provided either in the DNS query or the MDM setup), you can possibly see the repeated SYN packets. This indicates no direct

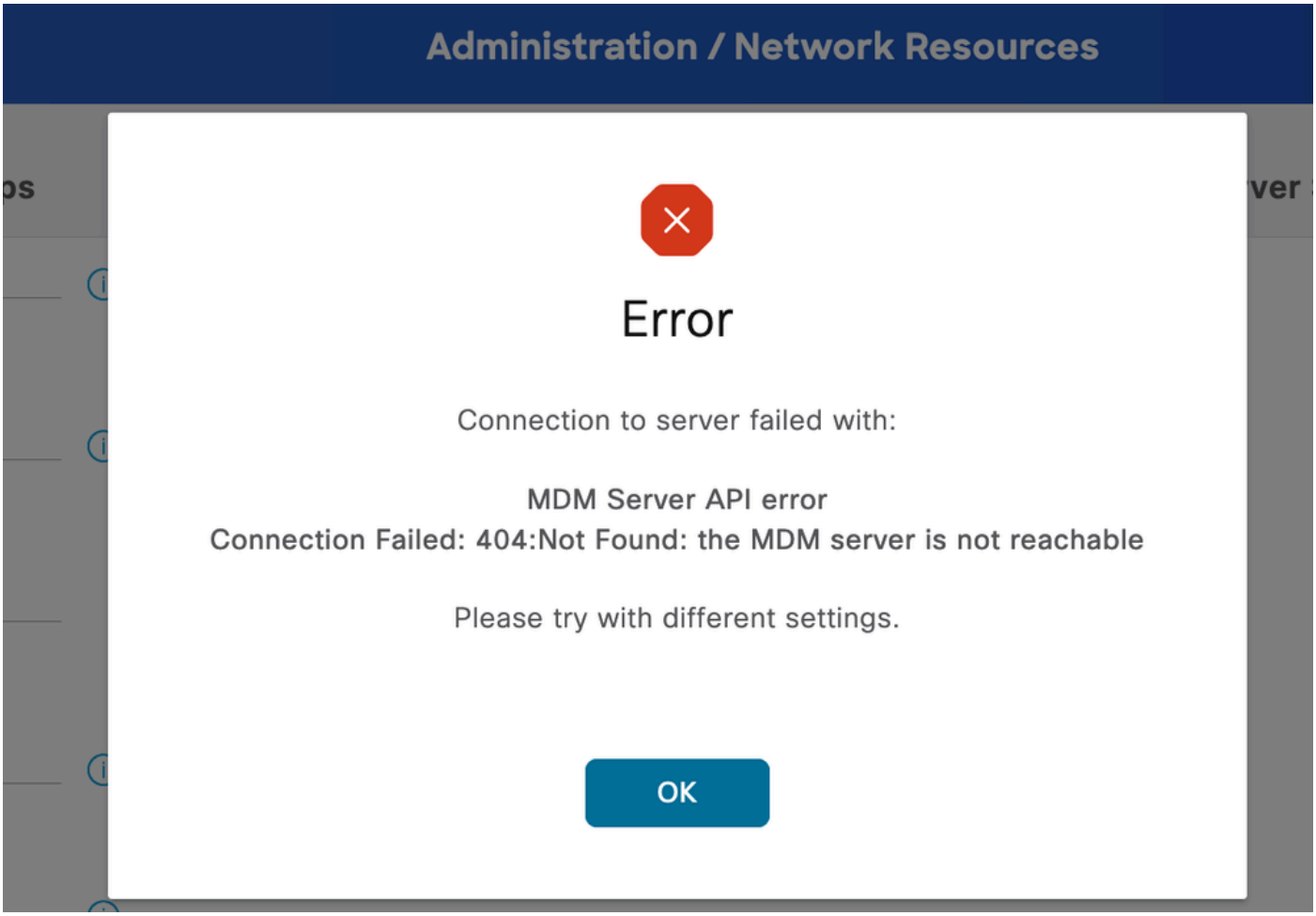
route to the JAMF instance or an external device interfering with communications on the 443 port.

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

Connection to MDM timeout example

Scenario 2. Connection Failed: 404

This event indicates you have connectivity to your JAMF account that you configured while setting up the MDM server. However, the instance you indicated to connect does not exist or contains an error as it is not found.



MDM error 404 example

The logs corresponding to this event are displayed:

```
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::- inside the method : callMdmSer
TRACE [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- Inside MDMVerifyServer.veri
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- API version retrieved from
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- apiVersionSb : 3, mdmApiVer
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- MDM Rest API Server Query S
```

```
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- MDM Rest API Server Query PA
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- 1. Connecting to the MDM se
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDom: start  HTTP r
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDomNonComp: start
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- ===mdmFlowInfo===null,=====serve
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://YOU
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- Proxy Config in request  = [,PRO
INFO  [admin-http-pool37][[]] cpm.admin.infra.spring.ISEAdminControllerUtils -::admin:::- mapping path
INFO  [admin-http-pool37][[]] cpm.admin.infra.spring.ISEAdminControllerUtils -::admin:::- mapping path
INFO  [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmServersCache -::::- MDM server - Status : Active,
ERROR [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- Error message while connecting t
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDom: end  HTTP req
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::- sendGETRequestDomNonComp: end  H
ERROR [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::- Exception occurred while co
ERROR [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmClient -::::- Connection Failed: 404:: the MDM serv
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::- returning from the method : ca
  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 cac
```

The packet capture at this time provides an HTTPS connection that contains application data that is being transferred between the JAMF site and the ISE server.

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

Packets involved in error 404 MDM

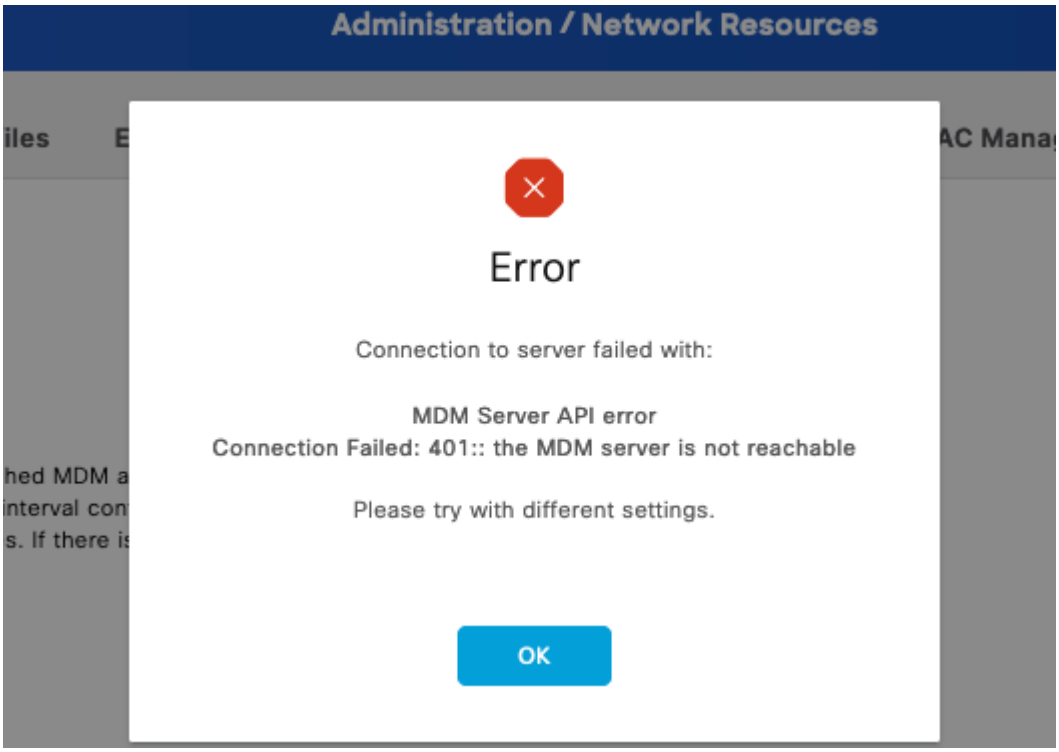
Scenario 3. Connection Failed: 401

This error in the connection indicates a problem with the user that you are deploying in the MDM setup to integrate.

Verify that the user:

- Exists within the JAMF account.

- Has the appropriate privileges to complete the integration with ISE.
- And can be used to perform API authentication (as described earlier in this guide).



MDM connection error code 401

The logs on ISE indicate this behavior:

```
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
```

The packet capture reveals a similar behavior like in this image:

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

MDM packets involved in error 401

Related information

- JAMF Integration with ISE 2.X as MDM
- Troubleshoot and Enable Debugs on ISE
- How to Enable Debugs on ISE 3.x Versions.