Integrate ISE 3.3 with JAMF as MDM Server.

Contents

Introduction

This document describes procedures that are necessary to implement successfully Identity Services Engine version 3.3 with JAMF PRO instance 10.48.X

Prerequisites

Requirements

Cisco recommends knowledge in these topics:

- Identity Services Engine.
- JAMF as MDM solution.

Components Used

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

- Cisco Identity Services Engine (ISE) version 3.3
- JAMF PRO version 10.48.1-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 a MDM server for managing Windows computers. Once these computers managed by JAMF are connected the network and authenticated, in order to retrieve further information for the security posture of those devices, ISE retrieves compliance information from JAMF server.

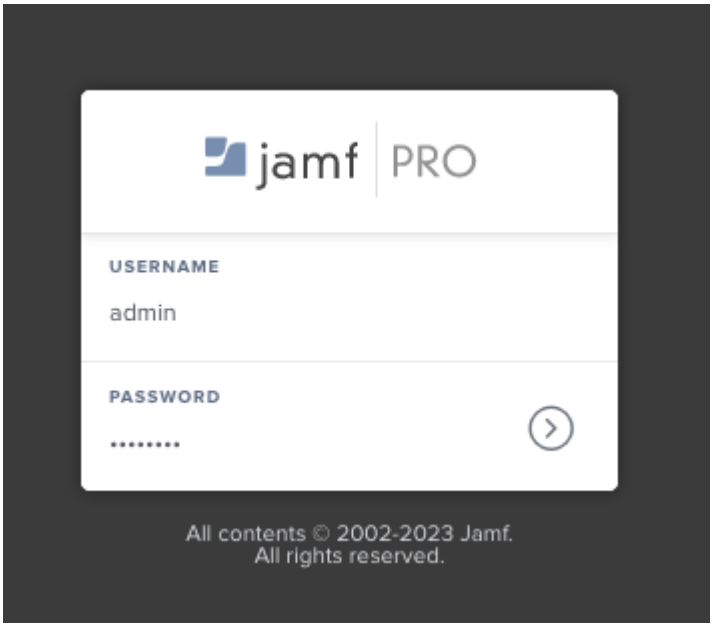
It uses this information to enforce secure access security by allowing/denying those computers depending on the criteria and conditions configured in ISE.

Therefore, this implementation helps to identify potential vulnerabilities and security weakness 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.

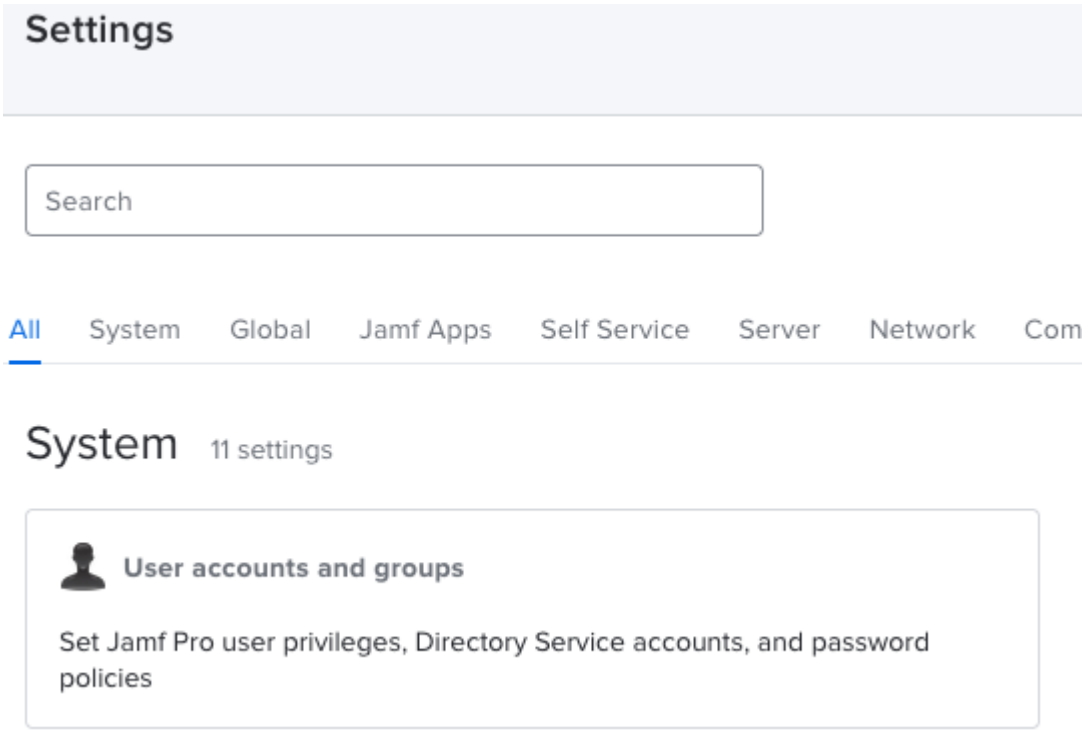


JAMF PRO login page

Step 2. From the main menu, select the gear that is displayed over this icon.

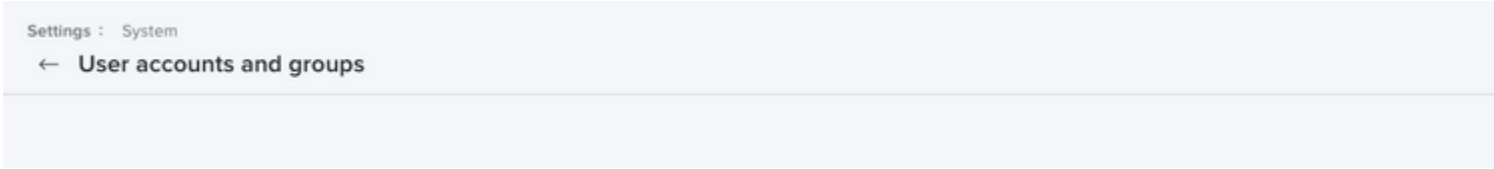
JAMF PRO Dashboard

Step 3. In the main menu, select the option named **System > User** accounts and groups.



JAMF PRO System Settings

Step 4. Select the section Password Policies.



JAMF PRO Users accounts and groups

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

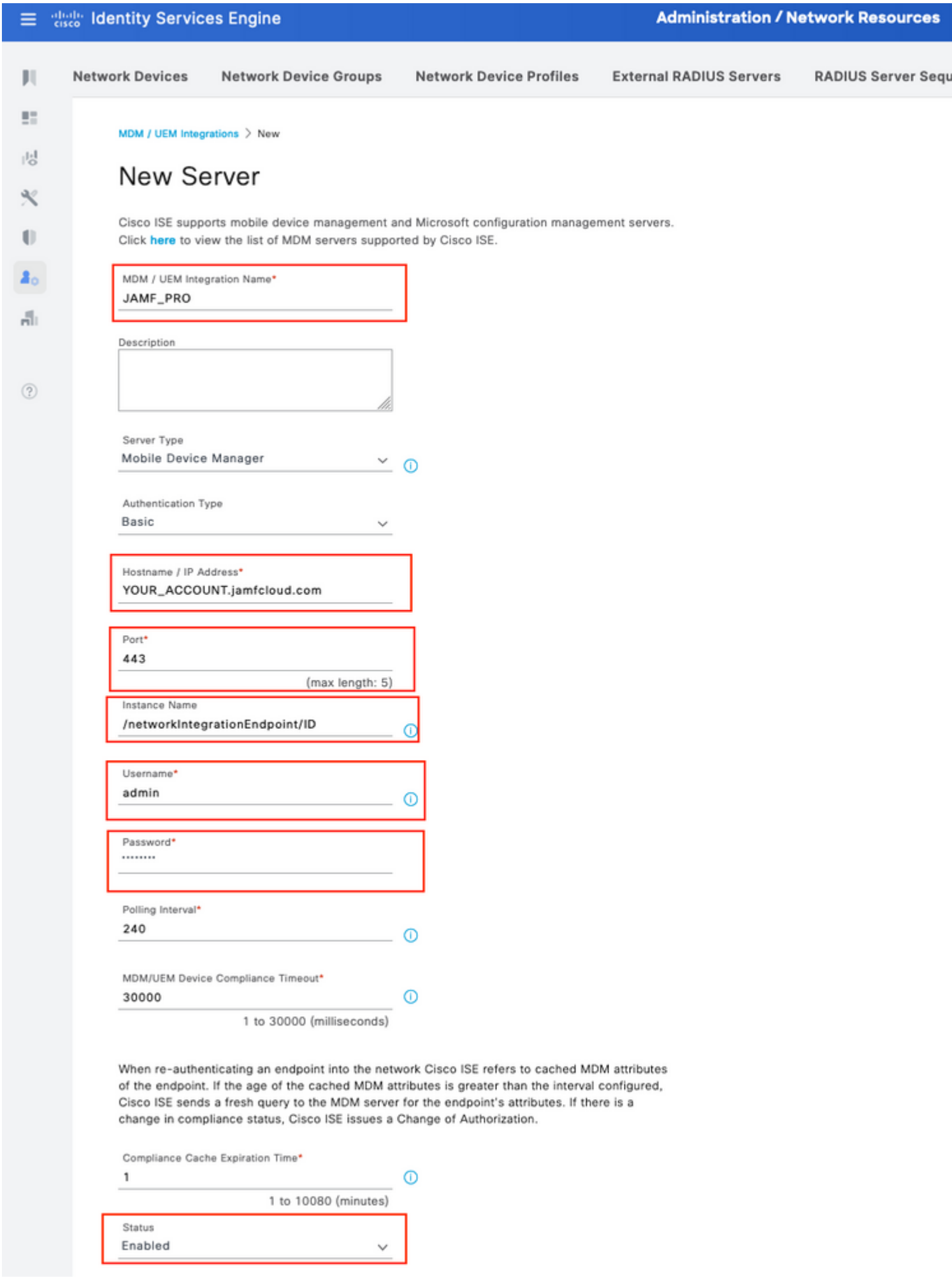
> **Note**: Starting JAMF PRO version 10.35 and upper version the basic authentication for API is not enabled by default, hence you need to enable such feature to get the MDM integration working, for more information please
> review https://developer.jamf.com/jamf-pro/docs/classic-api-authentication-changes

---

Step 6. Return once you have the last feature enabled to the menu **Settings**.

proceed to fill this information 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**.

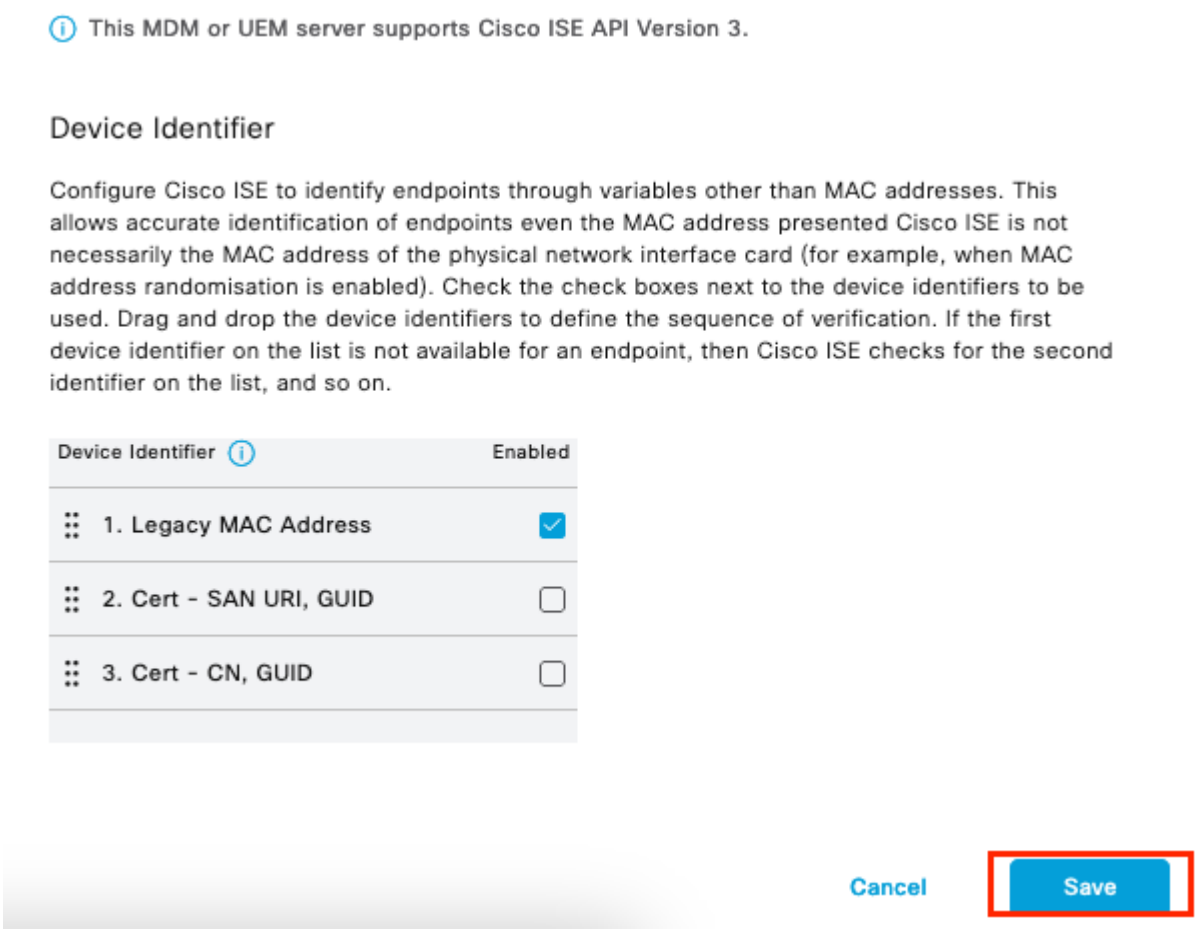


ISE MDM JAMF PRO configuration example

Step 3. Scroll down and proceed to **Test**

epending upon your scenario, you can select the MAC address of the device or attributes of certificates as it is displayed.

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 successful connectivity, we see the HTTPS traffic that is sent from the ISE PAN server towards 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 TSec
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	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
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 for ise-psc.log.

```
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::::- inside the method : callMdmServ
TRACE [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- Inside MDMVerifyServer.verif
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- apiVersionSb : 3, mdmApiVers
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- MDM Rest API Server Query St
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- MDM Rest API Server Query PA
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- 1. Connecting to the MDM ser
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDom: start  HTTP re
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: start
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- ===mdmFlowInfo===null,=====server
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://YOUR
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- Proxy Config in request  = [,PROX
.
.
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>mdminf
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDom: end  HTTP requ
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: end  HT
TRACE [admin-http-pool16][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- isMdmSettingsIdNotNull flag
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::::- returning from the method : cal
  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 the queries that ISE performs periodically towards the JAMF-PRO instance.

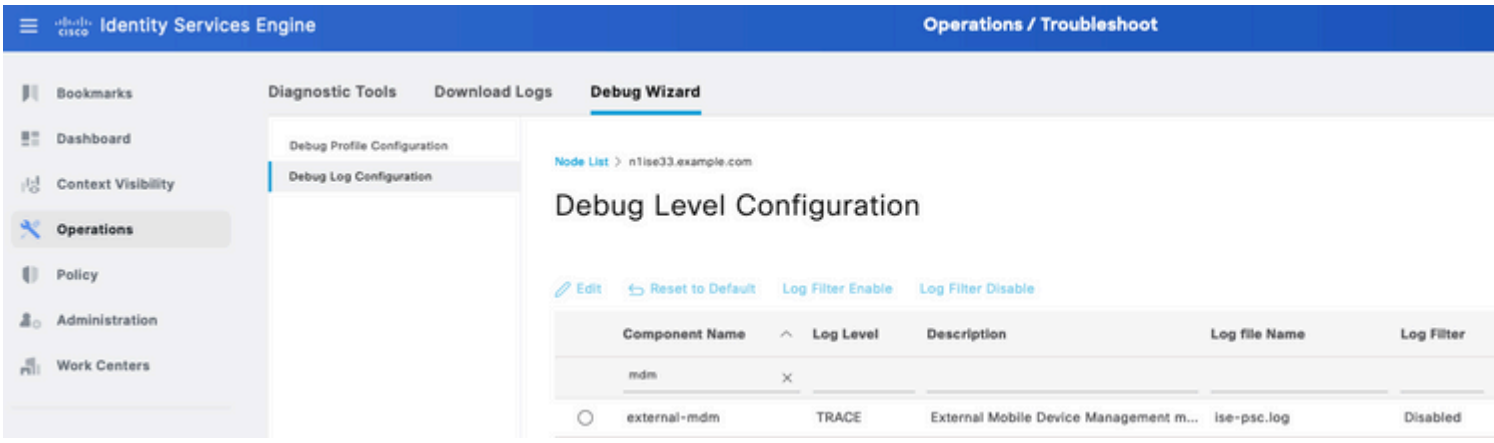
The point of reference where the troubleshooting is performed (in this instance) is the Primary Administration Node (PAN).

The PAN node is from where the connectivity method is configured to reach the MDM server.

This same method is replicated in all the nodes for the implementation.

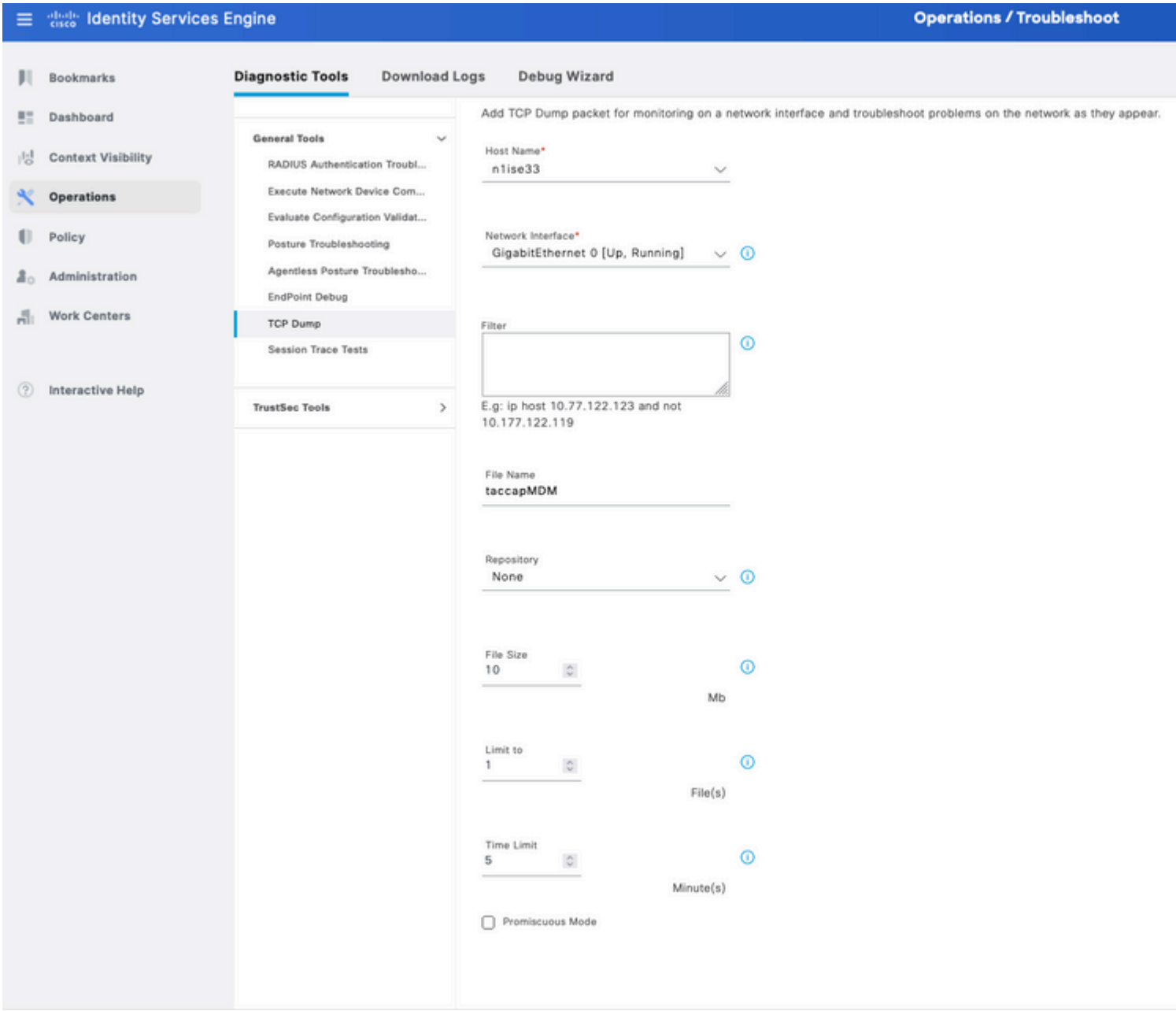
The next steps can be applied for troubleshooting reachability problems.

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



External MDM component in TRACE level to troubleshoot

Step 2. Setup a capture from the PAN node, **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** then 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.

```
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- API version retrieved from M
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- apiVersionSb : 3, mdmApiVers
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- MDM Rest API Server Query St
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- MDM Rest API Server Query PA
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- 1. Connecting to the MDM ser
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDom: start  HTTP re
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: start
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- ===mdmFlowInfo===null,=====server
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
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, m
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- Error message while connecting to
Connection Failed to the MDM server host â€“ YOUR_ACCOUNT.jamfcloud.com, and port - 443 : Connection tim
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDom: end  HTTP requ
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: end  HT
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- Exception occurred while con
ERROR [admin-http-pool26][[]] cisco.cpm.mdm.api.MdmClient -::::::- A connection timeout occurred. Check i
DEBUG [admin-http-pool26][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::::- returning from the method : cal
  apiPath: null
  redirectUrl: null
  queryMaxSize: null
  apiVersion: null
  vendor: null
  productName: null
  productVersion: null
  COMMA: ,
  errorMsg: null
  errorOccurred: true
}
```

From the packet capture, the next information can be reviewed.

DNS traffic. The ISE performs a query towards your JAMF related instance if you input the hostname in the setup part 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 MDM connection port. After this, if you query the IP address directly provided either in the DNS query or the MDM setup, you possibly see repeated SYN packets.

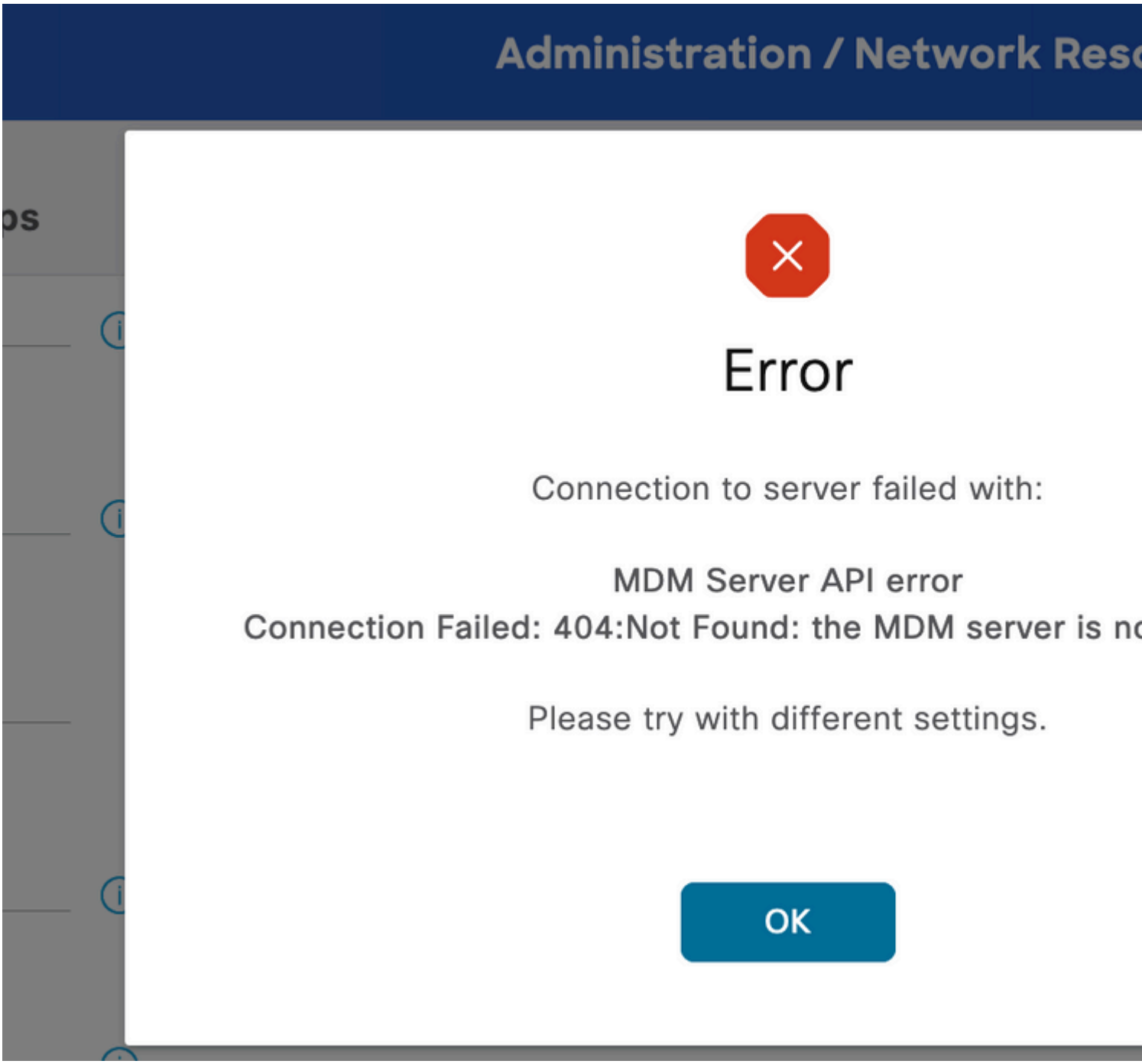
This indicates no direct route to the JAMF instance or an external device interfering with communications on the 443 port.

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
10.88.240.21	TCP	74	[TCP Retransmission] 22432 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK
10.88.240.21	TCP	74	[TCP Retransmission] 22432 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK

Connection to MDM timeout example

Scenario 2. Connection Failed: 404.

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



MDM error 404 example

The logs corresponding this event are displayed:

```
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::- inside the method : callMdmServ
```

```
TRACE [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- Inside MDMVerifyServer.verif
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- API version retrieved from M
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- apiVersionSb : 3, mdmApiVers
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- MDM Rest API Server Query St
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 ser
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDom: start  HTTP re
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: start
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- ===mdmFlowInfo===null,=====server
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
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- Proxy Config in request  = [,PROX
INFO  [admin-http-pool37][[]] cpm.admin.infra.spring.ISEAdminControllerUtils -::admin:::- mapping path f
INFO  [admin-http-pool37][[]] cpm.admin.infra.spring.ISEAdminControllerUtils -::admin:::- mapping path f
INFO  [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmServersCache -::::::- MDM server - Status : Active, m
ERROR [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- Error message while connecting to
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDom: end  HTTP requ
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: end  HT
ERROR [admin-http-pool32][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- Exception occurred while con
ERROR [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmClient -::::::- Connection Failed: 404:: the MDM serve
DEBUG [admin-http-pool32][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::::- returning from the method : cal
  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 cach
```

The packet capture in this time provides a 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 Me
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

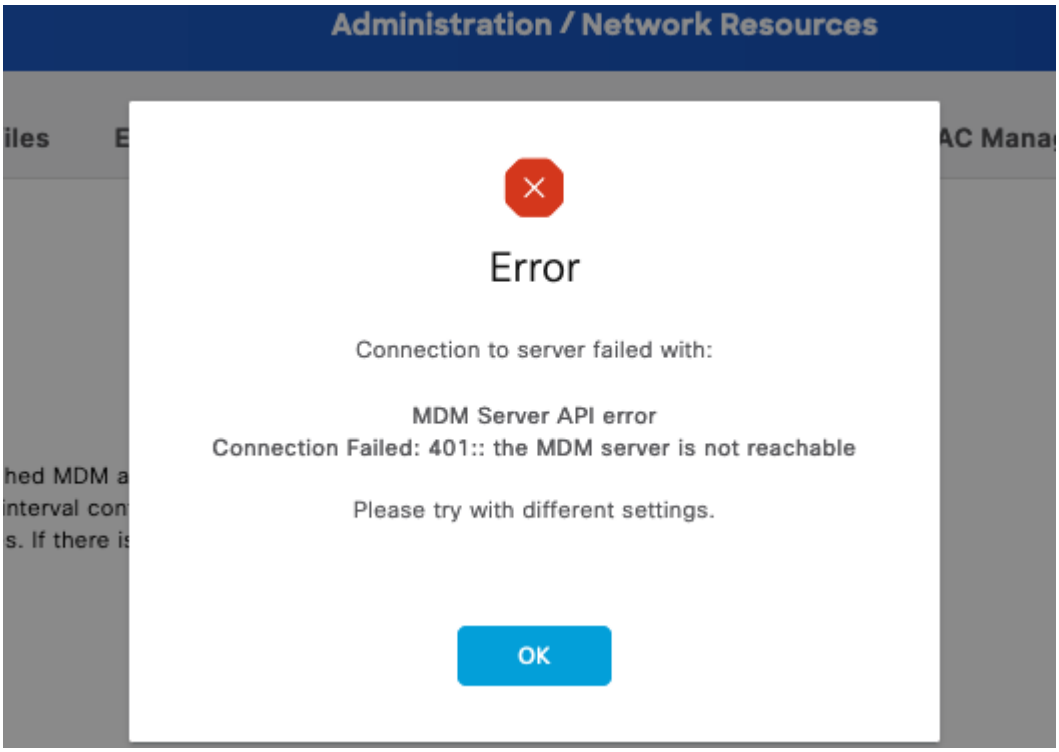
Packets involved in error 404 MDM

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 right privileges to do the integration with ISE,
- and can be used to perform API authentication (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  = [,PROXY
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 reque
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: end  HTT
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- retry connecting using api v2
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- MDM Rest API Server Query Str
```

```
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- MDM Rest API Server Query PAT
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- 2. On Error : re-connecting t
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDom: start  HTTP req
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: start  H
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- ===mdmFlowInfo===null,=====serverT
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  = [,PROXY
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 reque
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.util.MdmRESTClient -::::::- sendGETRequestDomNonComp: end  HTT
DEBUG [admin-http-pool8][[]] cisco.cpm.mdm.apiimpl.MDMVerifyServer -::::::- retry connecting using api v1
```

The packet capture reveals a similar behavior like the one shown here.

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 Mes
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.