Intégrer ISE 3.3 à JAMF en tant que serveur MDM

Table des matières

Introduction

Ce document décrit les procédures nécessaires à l'implémentation d'Identity Services Engine v3.3 avec l'instance 10.48.X de JAMF PRO.

Conditions préalables

Exigences

Cisco recommande des connaissances sur les sujets suivants :

- Moteur du service de vérification des identités (ISE)
- JAMF en tant que solution MDM

Composants utilisés

Les informations contenues dans ce document sont basées sur les logiciels et versions suivants :

- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

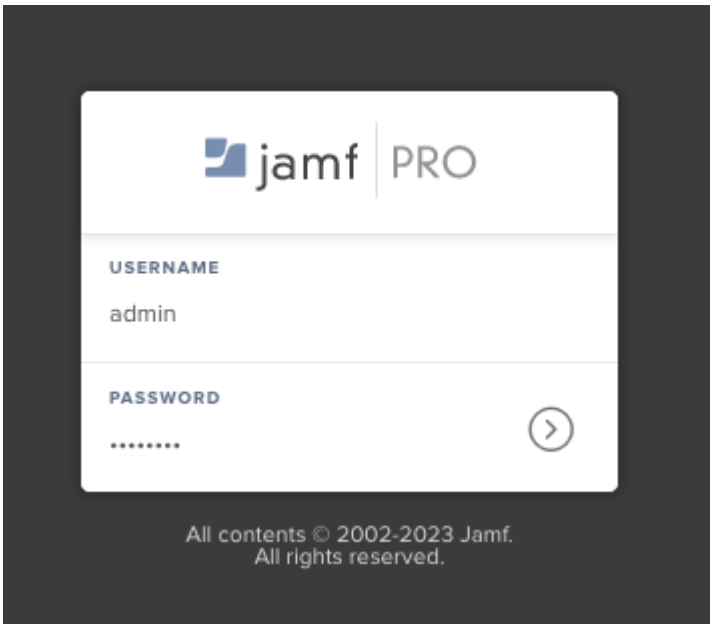
Cisco ISE prend en charge JAMF en tant que serveur MDM pour la gestion des ordinateurs Windows. Lorsque ces ordinateurs (gérés par JAMF) sont connectés et authentifiés, ISE récupère les informations de conformité à partir des serveurs JAMF pour récupérer des informations supplémentaires sur la position de sécurité de ces périphériques.

Il utilise les informations pour appliquer la sécurité d'accès sécurisée en autorisant/refusant ces ordinateurs, en fonction des critères et des conditions configurés dans ISE. Par conséquent, cette mise en oeuvre permet d'identifier les vulnérabilités potentielles et les failles de sécurité susceptibles d'être exploitées par les pirates.

Configurer

Préparation de JAMF PRO pour la connexion MDM

Étape 1. Connectez-vous avec votre cloud JAMF avec le compte pour les privilèges d'administrateur à l'adresse : https://YOUR_ACCOUNT.jamfcloud.com/index.html.



Page de connexion JAMF PRO

Étape 2. Dans le menu principal, sélectionnez l'icône de l'engrenage.

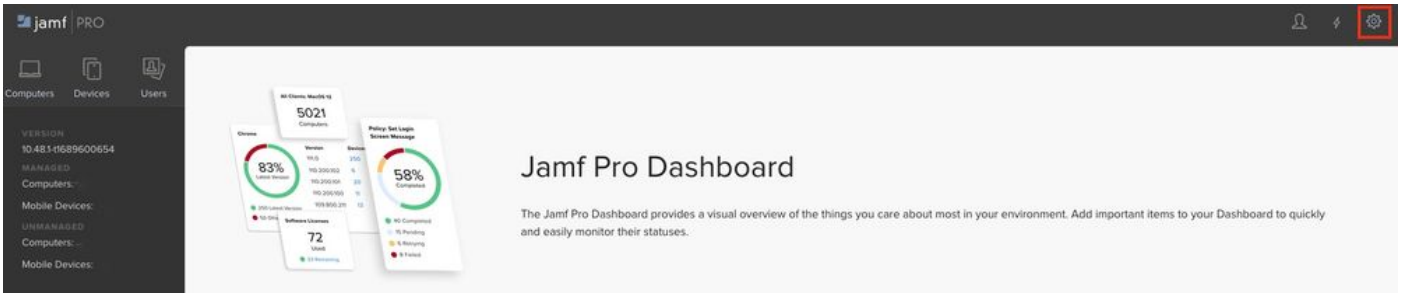
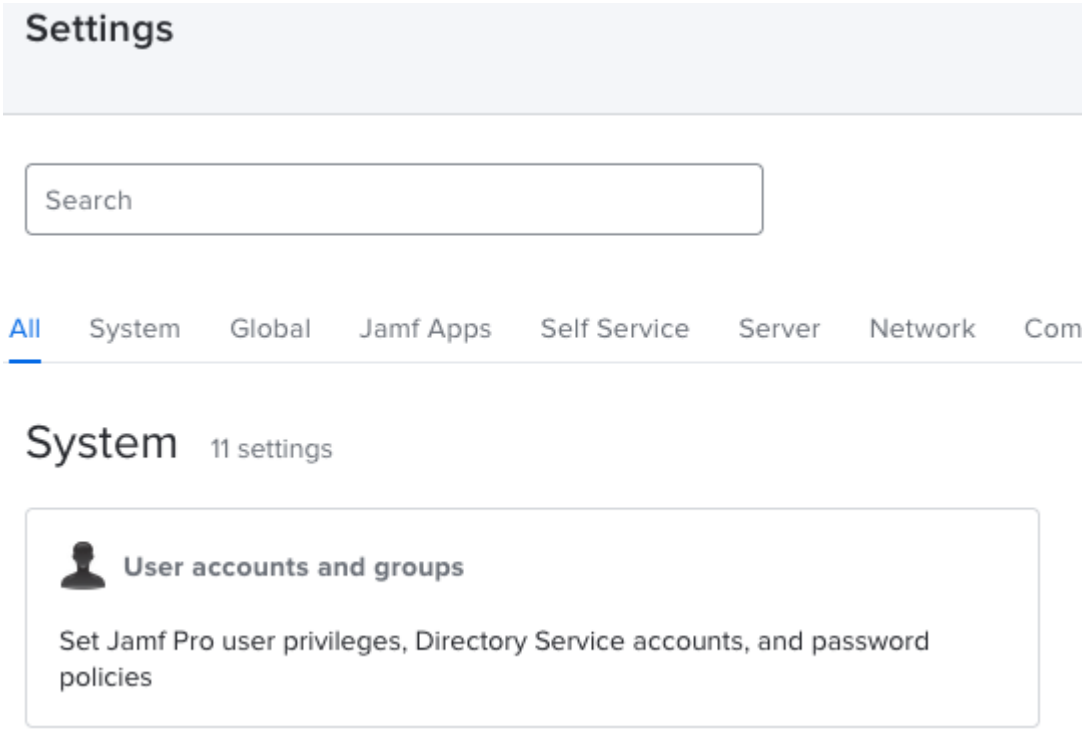


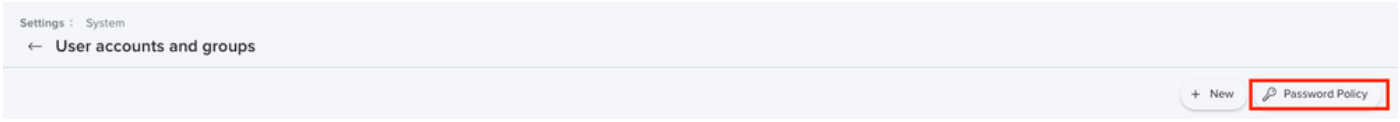
Tableau de bord JAMF PRO

Étape 3. Dans le menu principal, sélectionnez Système > Comptes d'utilisateurs et groupes.



Paramètres système de JAMF PRO

Étape 4. Sélectionnez l’option Stratégie de mot de passe.



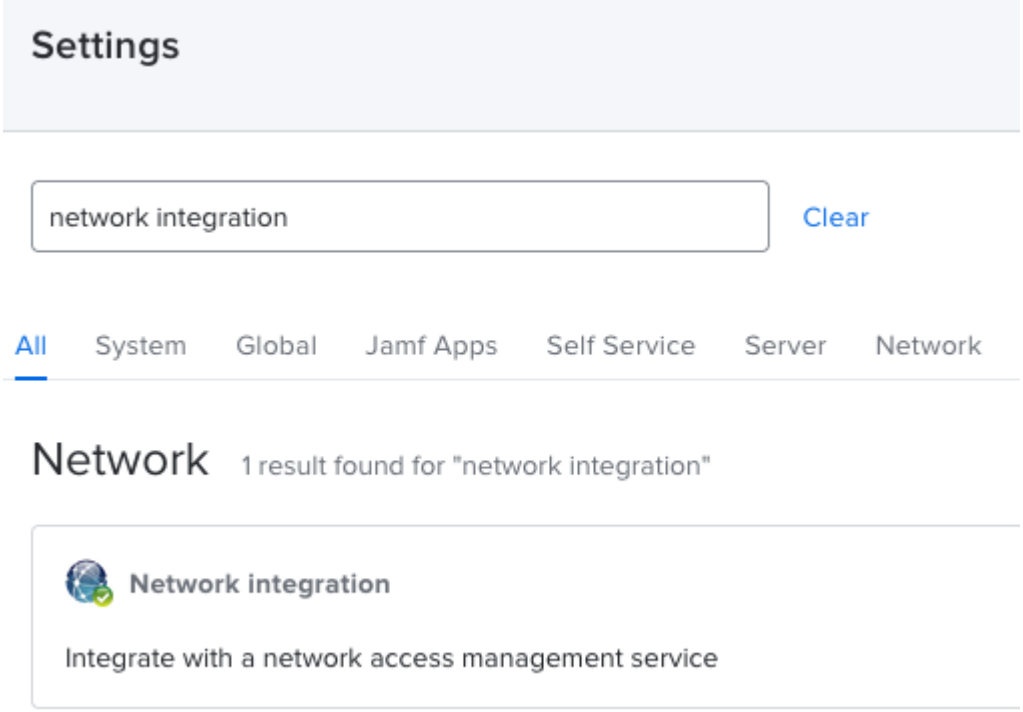
Comptes et groupes d'utilisateurs JAMF PRO

Étape 5. Dans cette section, vérifiez que vous disposez de l’option Allow Basic Authentication en plus de Bearer Token Authentication.

Remarque : À partir de JAMF PRO v10.35, l'authentification de base pour l'API n'est pas activée par défaut. Par conséquent, vous devez activer ces fonctions pour garantir le bon fonctionnement de l'intégration MDM.

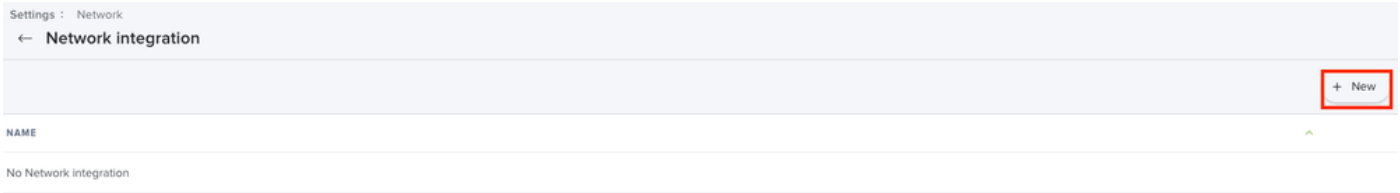
Pour plus d'informations, consultez Changements d'authentification API classique.

Étape 6. Une fois la dernière fonction activée, accédez aux paramètres de menu décrits à l’étape 3, puis recherchez le menu Network IntegrationMenu et sélectionnez-le.



Intégration réseau JAMF PRO

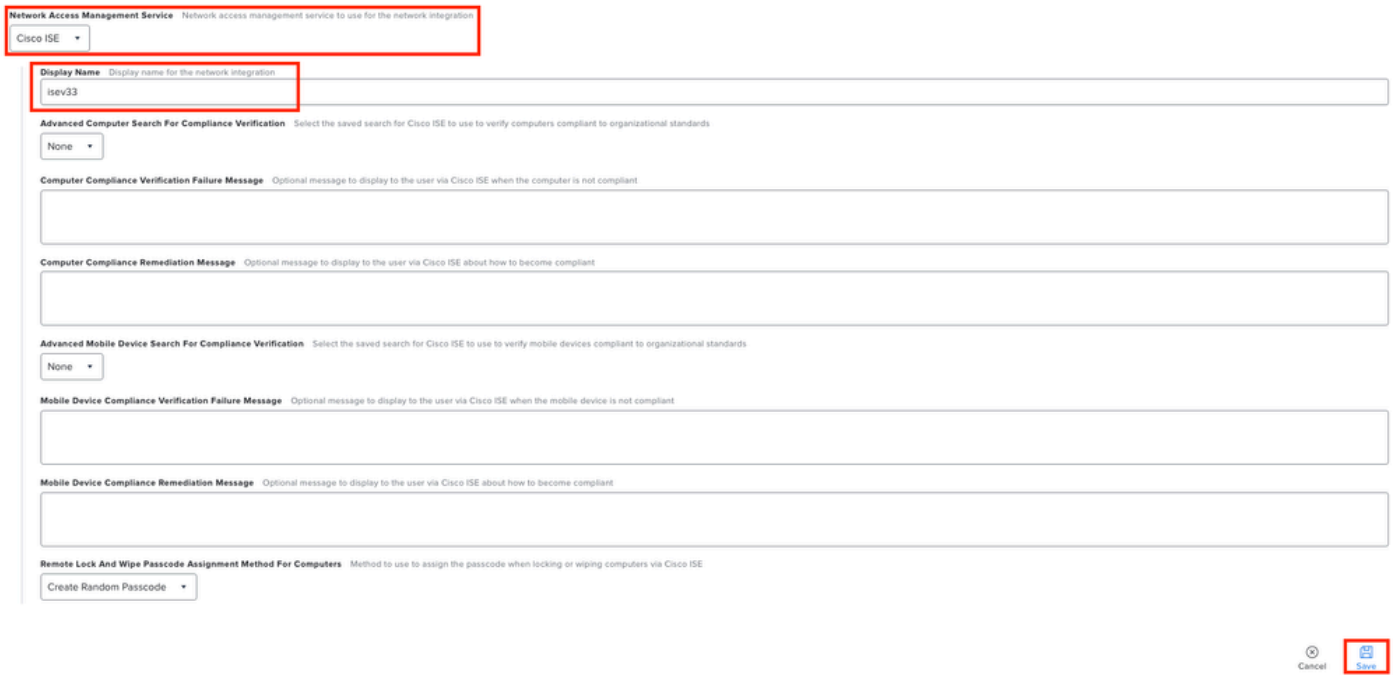
Étape 7. Passez à l'étape + New pour ajouter une nouvelle instance pour ISE 3.3.



Paramètres d'intégration réseau JAMF PRO

Étape 8. Dans le menu déroulant sous Network Access Management Service, laissez l'option marquée comme Cisco ISE.

- Entrez ensuite un nom dans le menu Display Name comme il est montré dans cet exemple.
- Pour les paramètres initiaux et la connexion pour ISE, la configuration peut être conservée avec ces configurations standard.
- Passez à la section Enregistrement de la configuration.

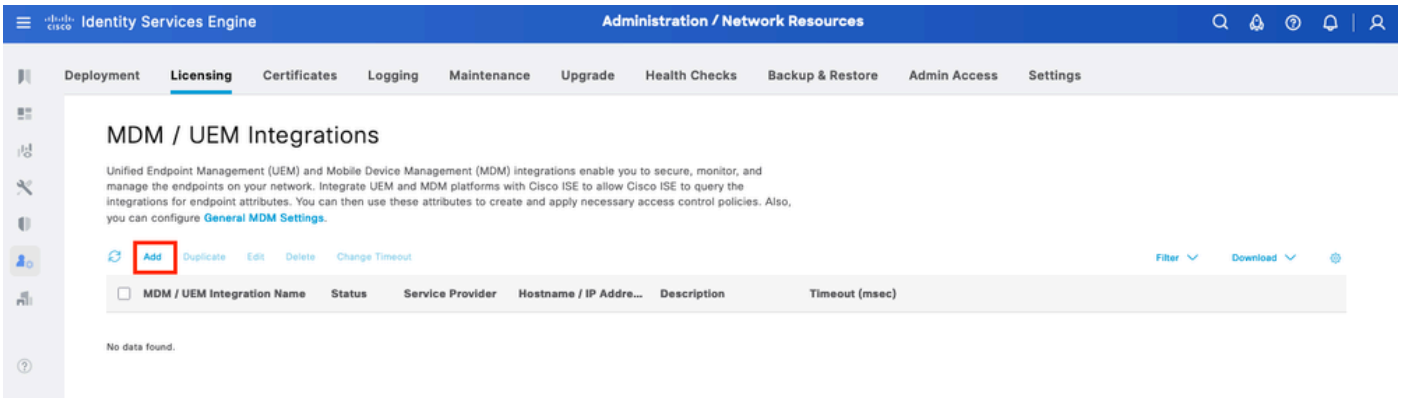


Exemple de configuration Intégration réseau avec ISE

Étape 9. L'intégration génère une URL d'intégration réseau au format suivant : https://YOUR_ACCOUNT.jamfcloud.com/networkIntegrationEndpoint/ID. Enregistrez cette URL car vous devrez l'utiliser ultérieurement pour vous connecter à ISE.

Préparation d'ISE pour la connexion MDM

Étape 1. Sélectionnez Menu > Administration > Network Resources > External MDM, puis cliquez sur Add.

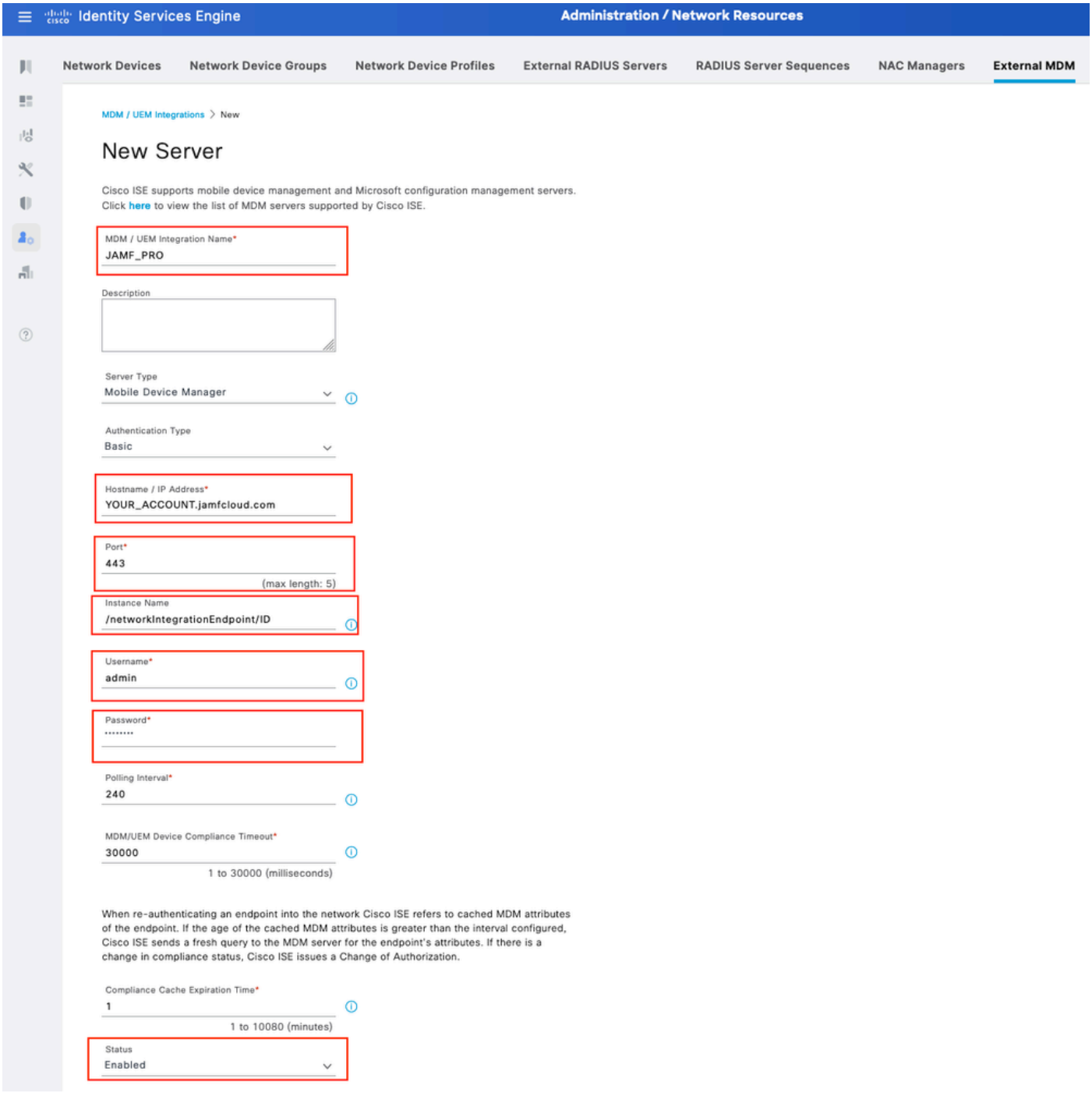


Menu d'intégration ISE MDM

Étape 2. Attribuez un nom à l'installation dans le segment Nom de l'intégration MDM / UEM.

- Dans la section Hostname / IP Address, sélectionnez YOUR_ACCOUNT.jamfcloud.com à partir de l'URL générée dans les étapes précédentes.

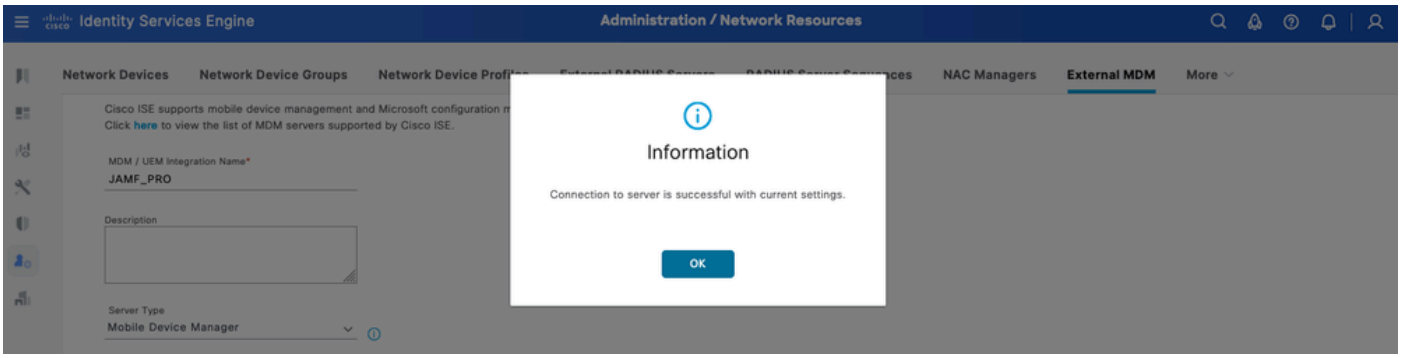
- Dans Port, sélectionnez la valeur 443 pour la connexion HTTPS avec votre instance JAMF PRO.
- Dans la section Nom d'instance, entrez les valeurs dont la section est absente de l'URL créée (dans ce cas : /networkIntegrationEndpoint/ID).
- Saisissez un nom d'utilisateur avec un accès complet à l'instance de JAMF PRO avec le mot de passe correspondant.
- Modifiez l'état du serveur MDM sur Activé.



Exemple de configuration de ISE MDM JAMF PRO

Étape 3. Faites défiler la page vers le bas et passez à l'étape Test de la connexion. Si la connexion réussit, cette image s'affiche. Si vous ne recevez pas le même résultat, reportez-vous à

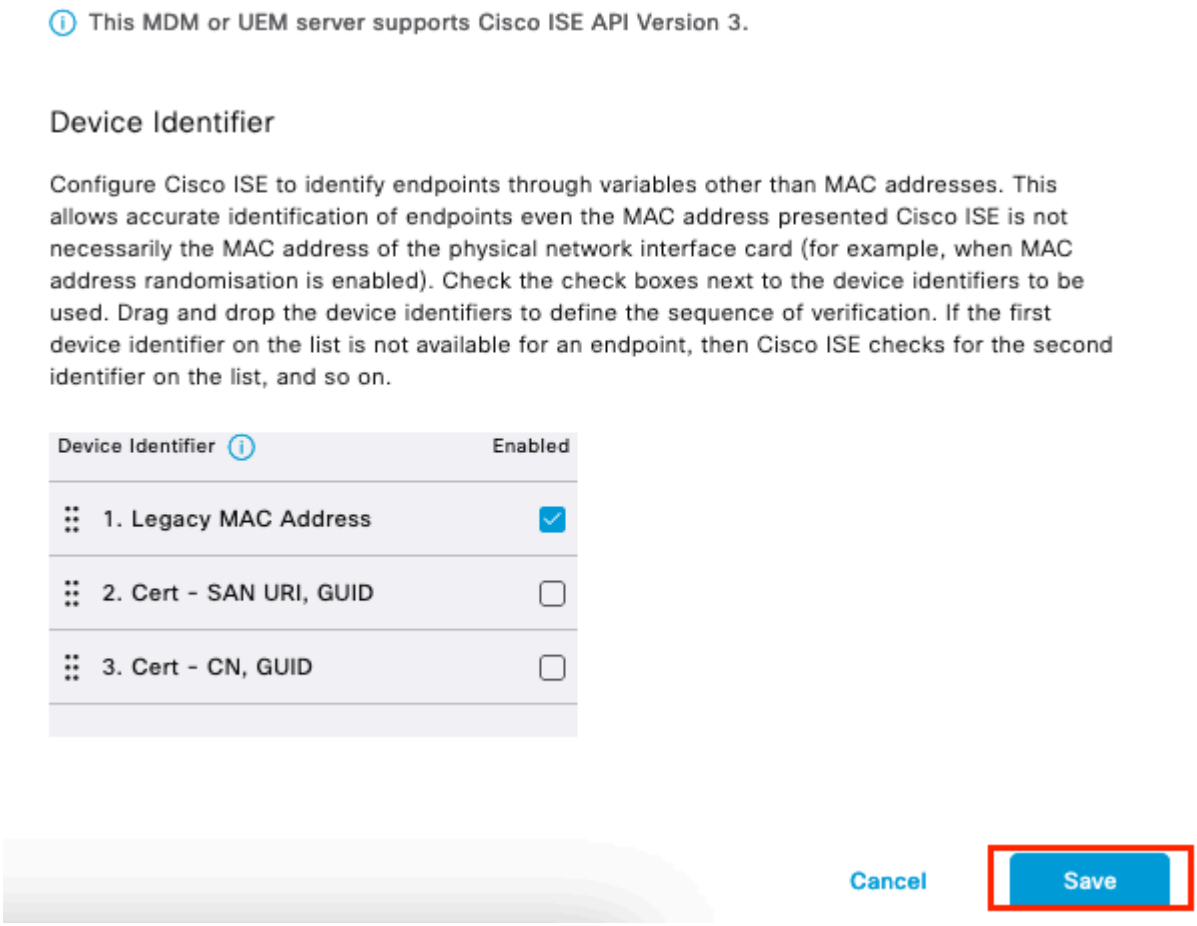
la section Dépannage de ce document.



Connexion réussie avec le compte MDM JAMF

Étape 4. Sélectionnez OK dans l'option précédente. Au bas de la page, recherchez l'identifiant de périphérique où l'ISE s'associe à la session du point d'extrémité.

- Selon votre scénario, vous pouvez sélectionner l'adresse MAC du périphérique ou les attributs du certificat.
- Une fois que vous avez personnalisé cette section, enregistrez la configuration.



Configuration supplémentaire du serveur MDM

Vérifiez la connectivité initiale de l'intégration avec l'instance de JAMF PRO.

Capture de paquets: Dans le cas d'une connectivité réussie, vous pouvez afficher le trafic HTTPS qui est envoyé du serveur PAN ISE à l'instance 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 [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

Exemple de capture de paquets avec une instance JAMF

Journaux sur ISE : L'ISE traite et analyse les données en conséquence, comme indiqué dans le fichier 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
```

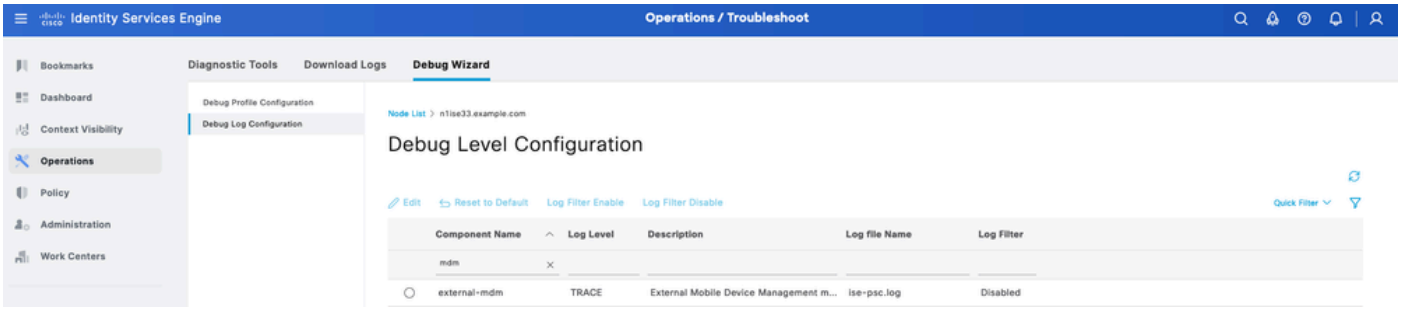
```
DEBUG [admin-http-pool16][[]] cisco.cpm.mdm.api.MdmServerInfoApi -::::- returning from the method : ca
  apiPath: /ID/ciscoise/v3
  redirectUrl: https://YOUR_ACCOUNT.jamfcloud.com/enroll
  queryMaxSize: 1000
  apiVersion: 3
  vendor: JAMF Software
  productName: JSS
  productVersion: 10.48.1-t1689600654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

Dépannage du serveur MDM inaccessible

La base de cette intégration consiste en des requêtes qu'ISE effectue périodiquement vers l'instance JAMF-PRO. Le point de référence où le dépannage est effectué (dans cette instance) est le noeud d'administration principal (PAN). Le noeud PAN est l'emplacement où la méthode de connectivité est configurée pour atteindre le serveur MDM. Cette même méthode est répliquée dans tous les noeuds pour la mise en oeuvre.

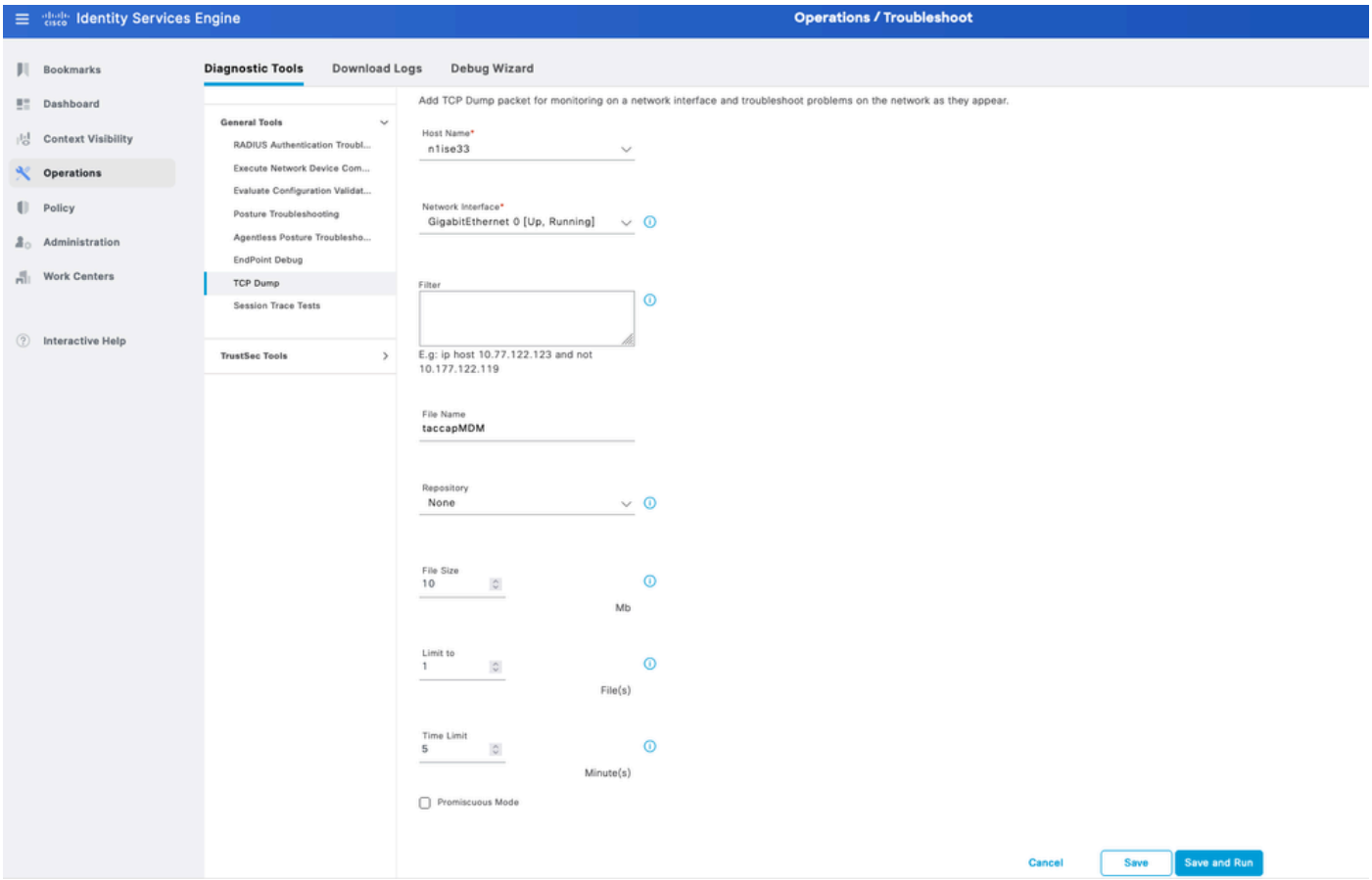
Les étapes suivantes peuvent être appliquées pour le dépannage des problèmes d'accessibilité.

Étape 1. Activer le composant external-mdm au niveau TRACE sur le noeud PAN



Composant MDM externe au niveau TRACE pour le dépannage

Étape 2. Configurer une capture à partir du noeud PAN et enregistrer votre configuration



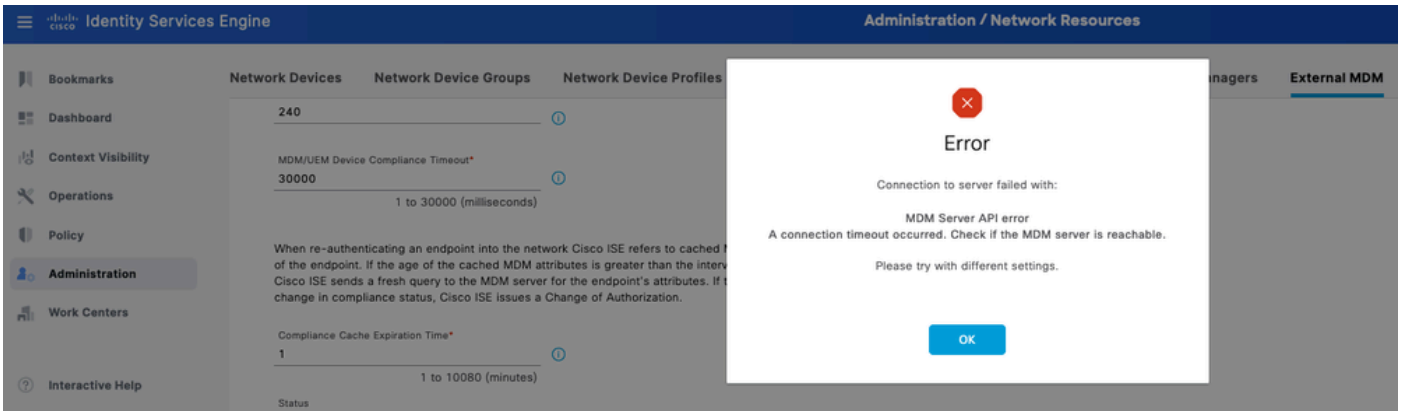
Exemple de capture de paquets pour collecter des informations de connexion MDM

Étape 3. Parcourez le menu MDM externe. Exécutez la capture de l'étape 2 et sélectionnez le bouton Test Connection. Attendez que l'erreur apparaisse.

Étape 4. Arrêtez la capture de l'étape 2. Examinez les journaux correspondant à ise-psc.log pour analyser le comportement.

Scénario 1. Expiration du délai de connexion

Dans le scénario, lorsque vous recevez cette erreur dans ISE lors du test de la connexion avec JAMF :



Délai de connexion d'erreur MDM

Les journaux associés au MDM externe révèlent ces informations :

```
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
}
```

À partir de la capture de paquets, passez en revue les informations suivantes :

Trafic DNS - L'ISE effectue une requête vers votre instance liée à JAMF si vous entrez le nom d'hôte dans la partie configuration de l'intégration. Si vous ne voyez pas la résolution du nom d'hôte, essayez d'utiliser l'adresse IP. Cette option peut être configurée à la place du nom d'hôte.

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

Trafic DNS dans un flux MDM

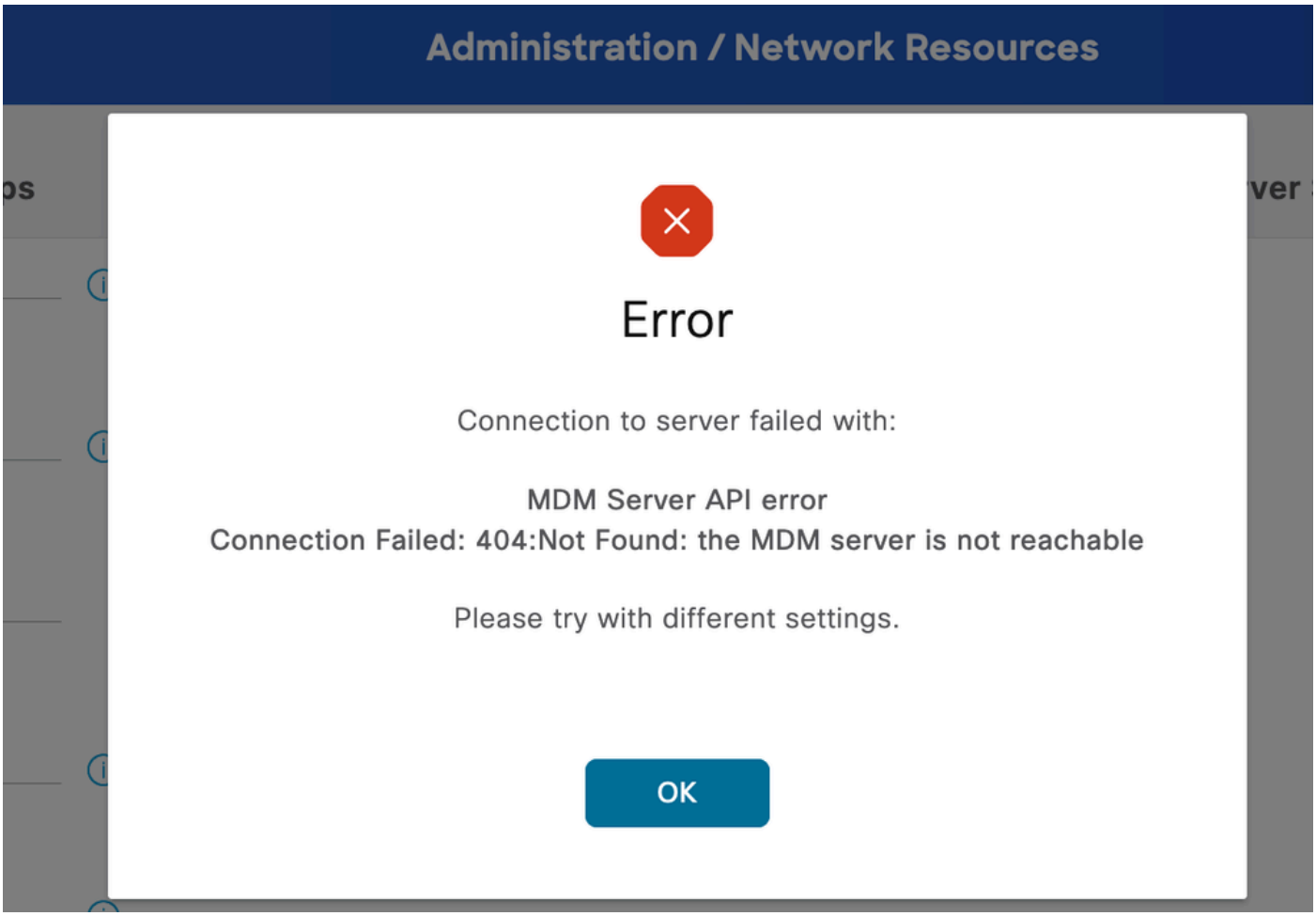
Retransmissions dans le port de connexion MDM - Si vous interrogez directement l'adresse IP (fournie dans la requête DNS ou dans la configuration MDM), vous pouvez voir les paquets SYN répétés. Cela indique qu'aucune route directe vers l'instance JAMF ou qu'un périphérique externe interfère avec les communications sur le port 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

Exemple de délai de connexion à MDM

Scénario 2. Échec de la connexion : 404

Cet événement indique que vous disposez d'une connectivité à votre compte JAMF que vous avez configurée lors de la configuration du serveur MDM. Cependant, l'instance que vous avez indiquée pour la connexion n'existe pas ou contient une erreur car elle est introuvable.



Exemple d'erreur MDM 404

Les journaux correspondant à cet événement s'affichent :

```
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
```

À ce stade, la capture de paquets fournit une connexion HTTPS qui contient les données d'application transférées entre le site JAMF et le serveur 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

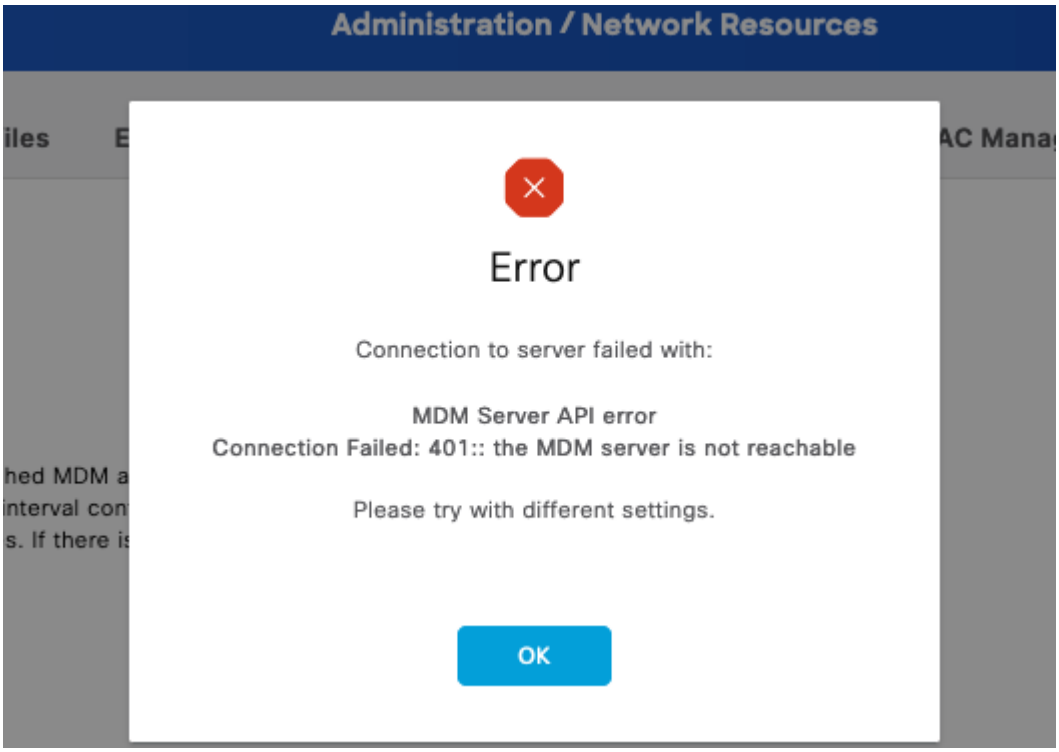
Paquets impliqués dans l'erreur 404 MDM

Scénario 3. Échec de la connexion : 401

Cette erreur dans la connexion indique un problème avec l'utilisateur que vous déployez dans la configuration MDM à intégrer.

Vérifiez que l'utilisateur :

- Existe dans le compte JAMF.
- Dispose des privilèges appropriés pour effectuer l'intégration avec ISE.
- Et peut être utilisé pour effectuer l'authentification API (comme décrit précédemment dans ce guide).



Code d'erreur de connexion MDM 401

Les journaux sur ISE indiquent ce comportement :

```
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 capture de paquets révèle un comportement similaire à celui de cette 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

Paquets MDM impliqués dans l'erreur 401

Informations connexes

- Intégration de JAMF avec ISE 2.X en tant que MDM
- Dépannage et activation des débogages sur ISE
- Comment activer les débogages sur les versions ISE 3.x.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.