Création de périphériques réseau ISE via l'API ERS

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Activer ERS (port 9060)
- Créer un administrateur ERS
- Configurer le facteur
- SDK ISE et autorisation postale de base
- Créer NAD en utilisant XML
- Créer NAD avec JSON

Vérifier

Dépannage

Introduction

Ce document décrit le processus de création de périphériques d'accès réseau (NAD) sur ISE via l'API ERS en utilisant PostMan comme client REST.

Conditions préalables

Exigences

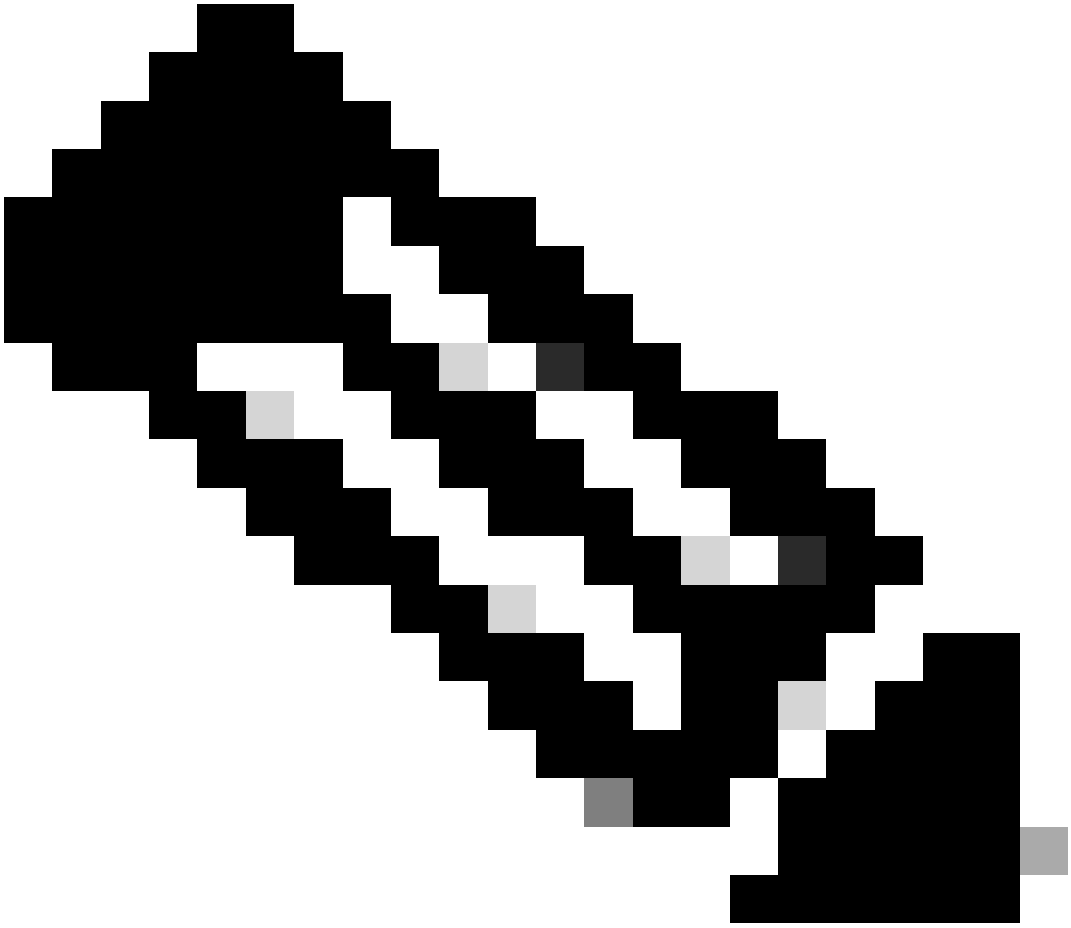
Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE (Identity Services Engine)
- ERS (External RESTful Services)
- Les clients REST comme Postman, RESTED, Insomnia, etc.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Cisco ISE (Identity Services Engine) 3.1 correctif 6
- Client REST Postman v10.17.4



Remarque : la procédure est similaire ou identique pour les autres versions d'ISE et les clients REST. Vous pouvez utiliser ces étapes sur toutes les versions du logiciel ISE 2.x et 3.x, sauf indication contraire.

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.

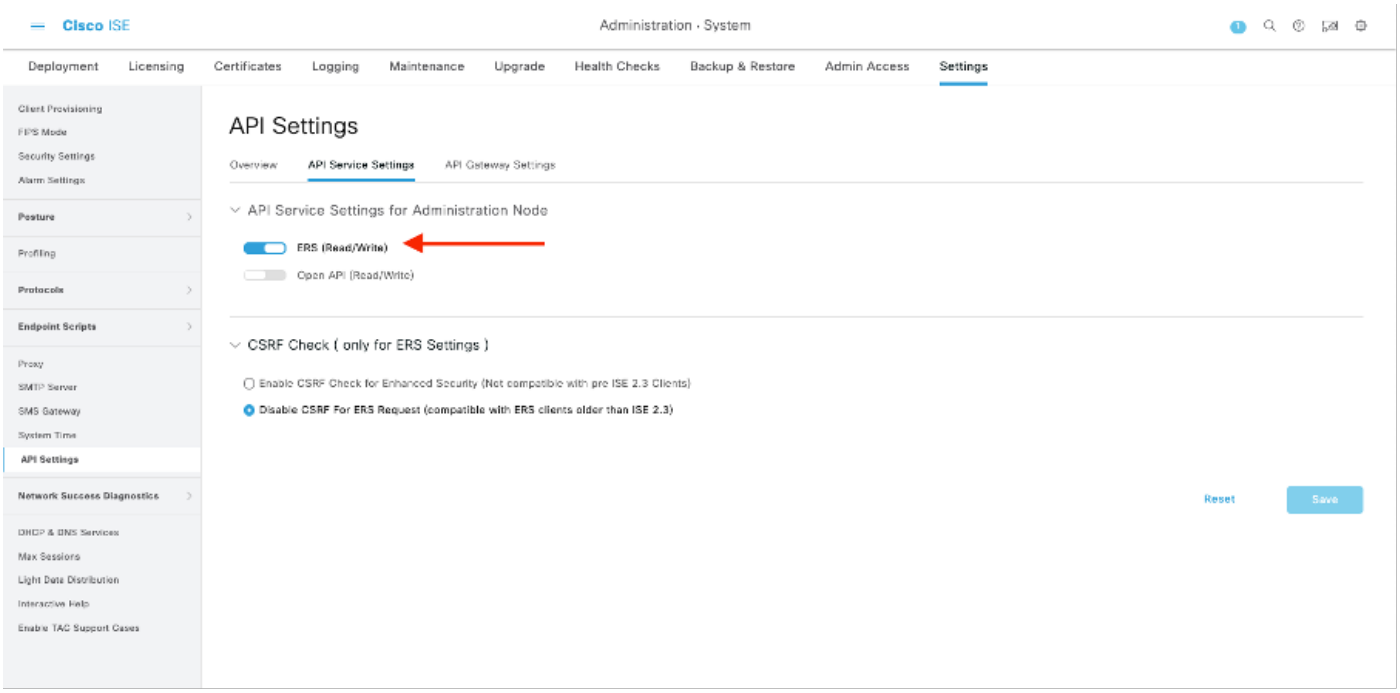
Configurer

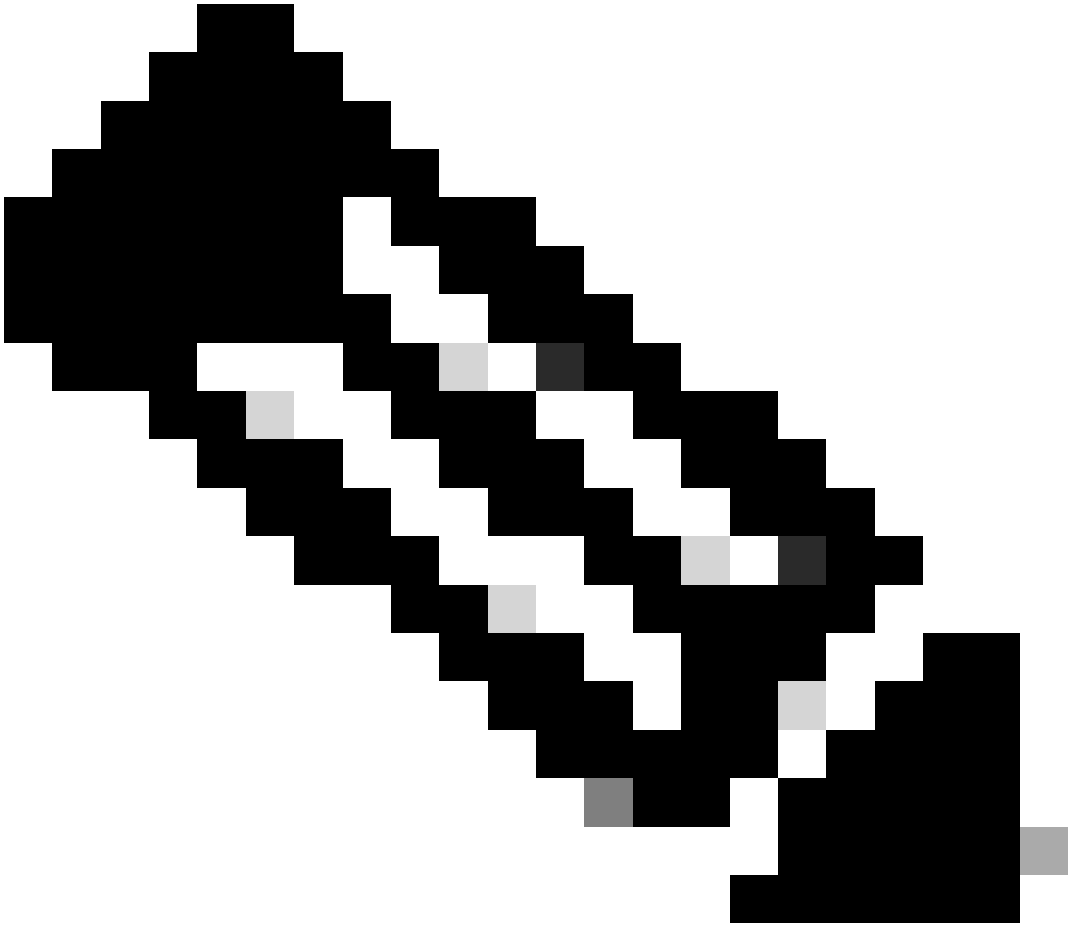
Activer ERS (port 9060)

Les API ERS sont des API REST HTTPS uniquement qui fonctionnent sur les ports 443 et 9060. Le port 9060 est fermé par défaut, il doit donc être ouvert en premier. Un délai d'attente à partir du serveur est présenté si les clients essayant d'accéder à ce port n'activent pas ERS en premier. Par conséquent, la première condition est d'activer ERS à partir de l'interface utilisateur

d'administration de Cisco ISE.

Accédez à Administration > Settings > API Settings et activez le bouton bascule ERS (Read/Write).

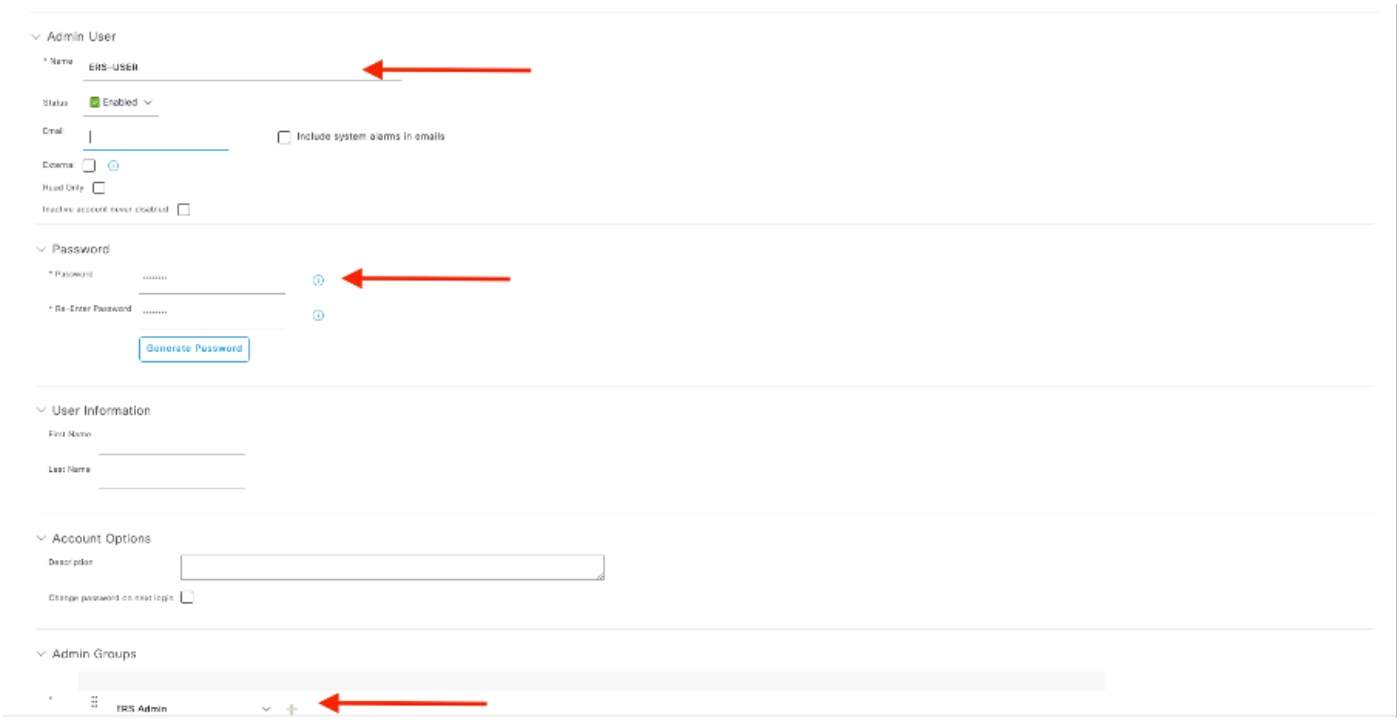




Remarque : les API ERS prennent en charge TLS 1.1 et TLS 1.2. Les API ERS ne prennent pas en charge TLS 1.0, quelle que soit l'activation de TLS 1.0 dans la fenêtre Security Settings de l'interface utilisateur graphique de Cisco ISE (Administration > System > Settings > Security Settings). L'activation de TLS 1.0 dans la fenêtre Paramètres de sécurité est liée au protocole EAP uniquement et n'a pas d'impact sur les API ERS.

Créer un administrateur ERS

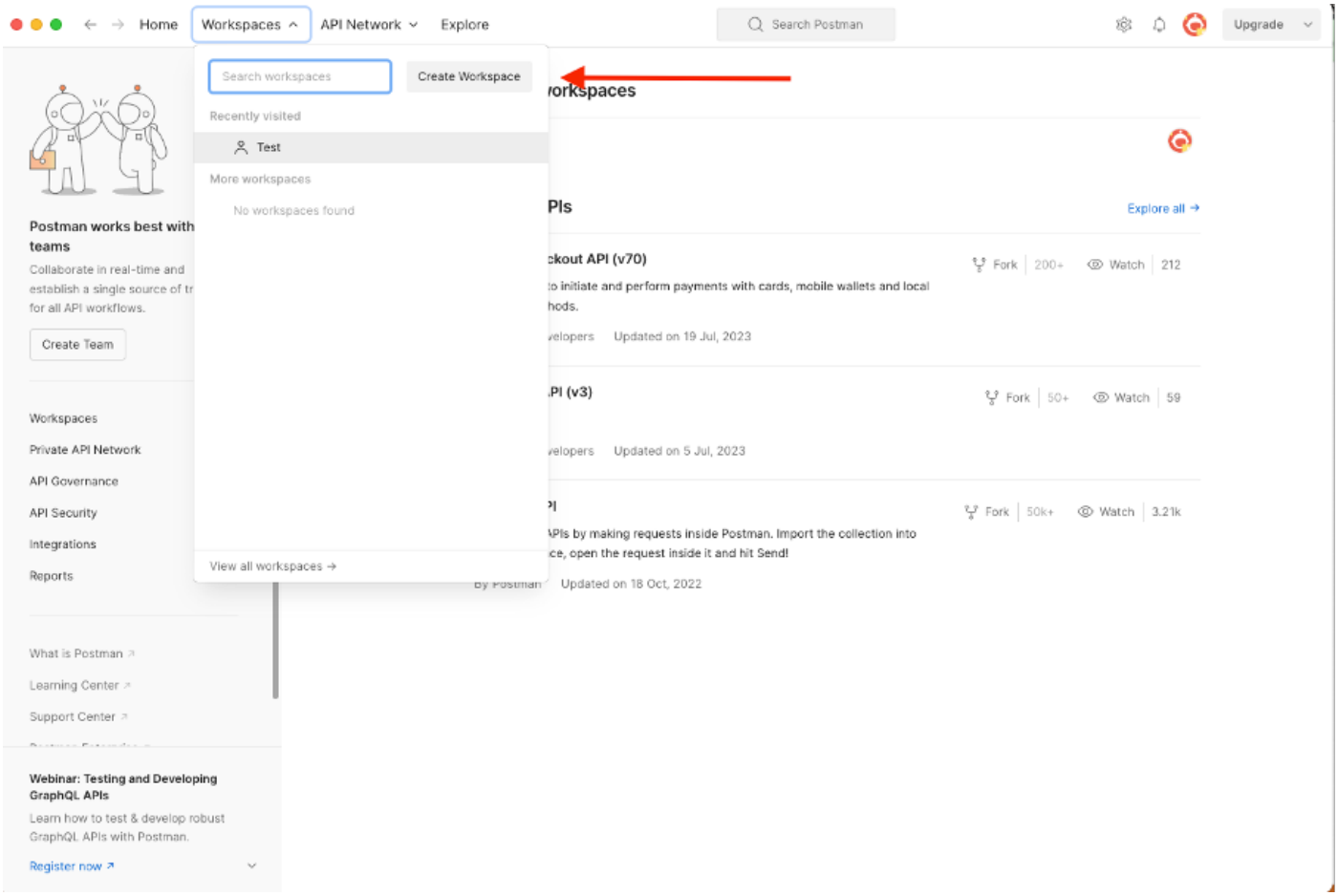
Créez un administrateur Cisco ISE, attribuez un mot de passe et ajoutez l'utilisateur au groupe admin en tant qu'administrateur ERS. Vous pouvez laisser le reste de la configuration vide.



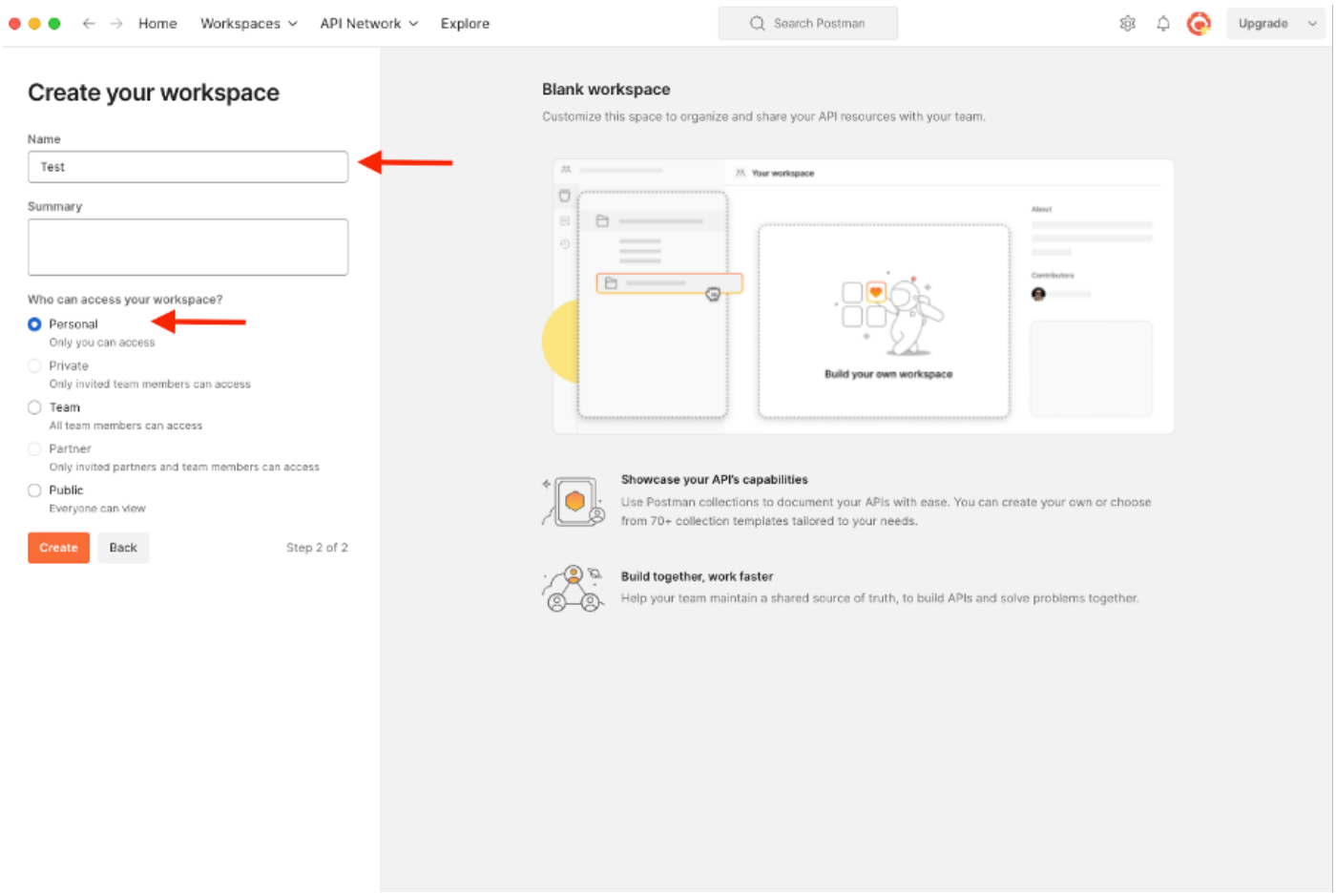
Configurer le facteur

Téléchargez ou utilisez la version en ligne de Postman.

1. Créez un utilisateur et un espace de travail en cliquant sur Créer un espace de travail sous l'onglet Espaces de travail.



2. Sélectionnez Espace de travail vide et attribuez un nom à l'espace de travail. Vous pouvez ajouter une description et la rendre publique. Pour cet exemple, Personalis est sélectionné.

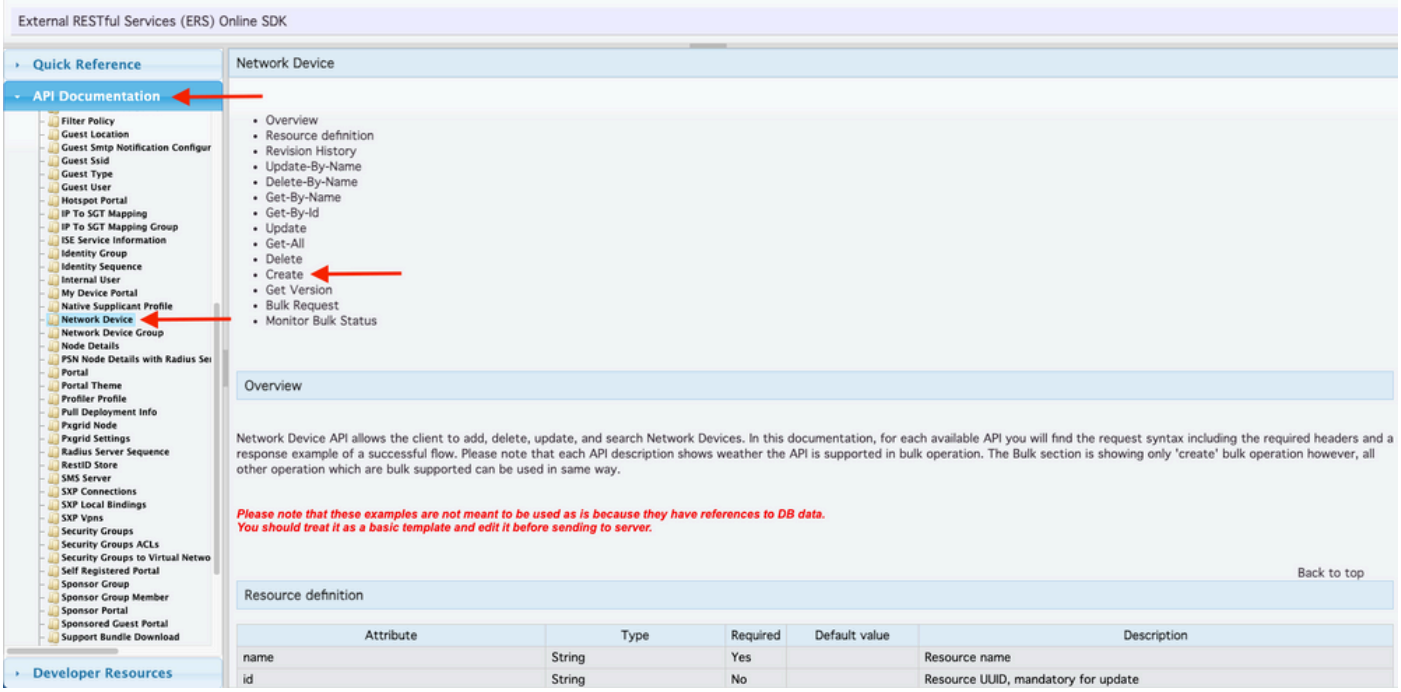


Une fois que vous avez créé l'espace de travail, vous pouvez maintenant configurer les appels d'API.

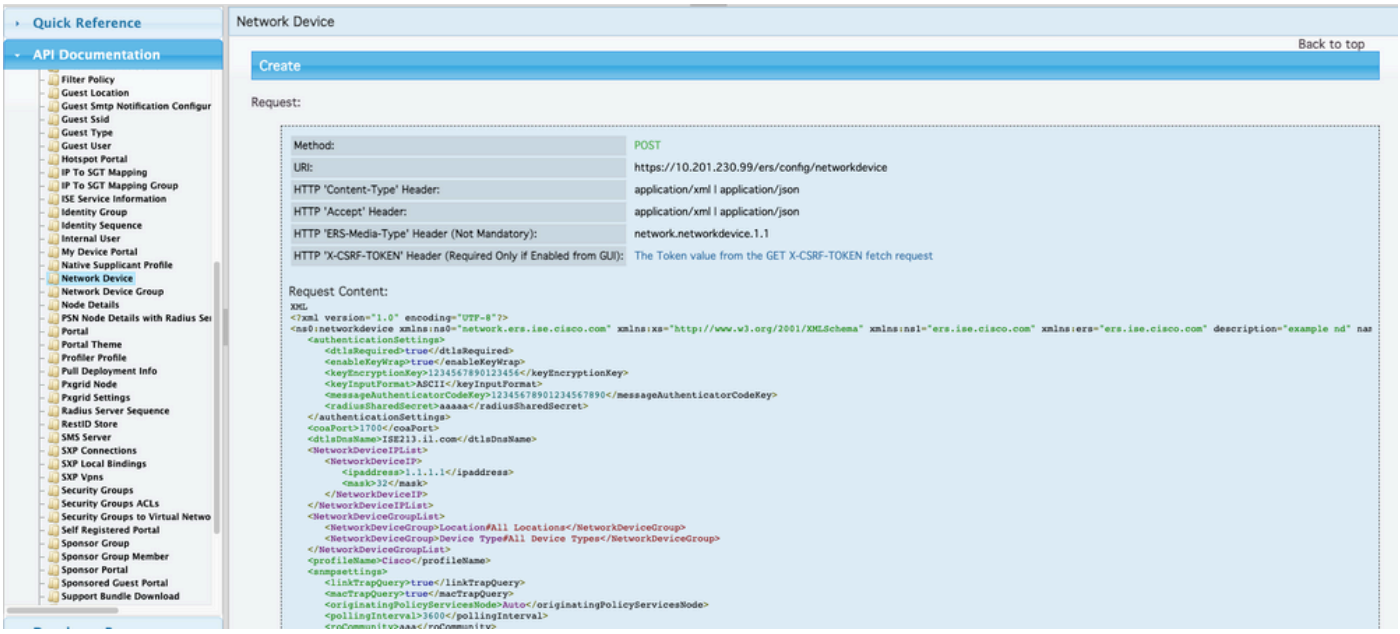
SDK ISE et autorisation postale de base

Pour configurer un appel, accédez d'abord au kit de développement logiciel ISE ERS SDK (Software Developer Kit). Cet outil compile la liste complète des appels d'API qu'ISE peut effectuer :

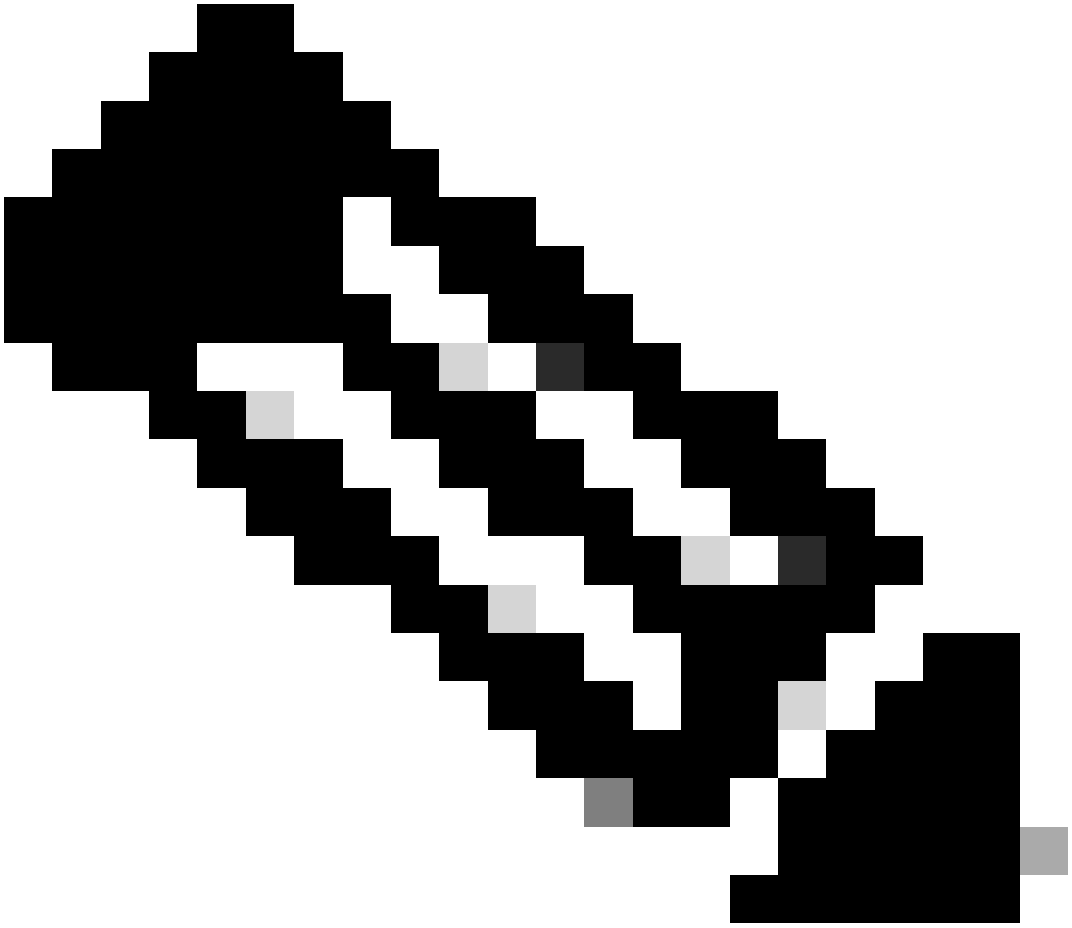
1. Accédez à https://{ise-ip}/ers/sdk.
2. Connectez-vous en utilisant vos identifiants d'administrateur ISE.
3. Développez la documentation API.
4. Faites défiler jusqu'à Network Device (Périphérique réseau) et cliquez dessus.
5. Avec cette option, vous pouvez désormais rechercher toutes les opérations disponibles que vous pouvez effectuer pour les périphériques réseau sur ISE. Sélectionnez Créer.



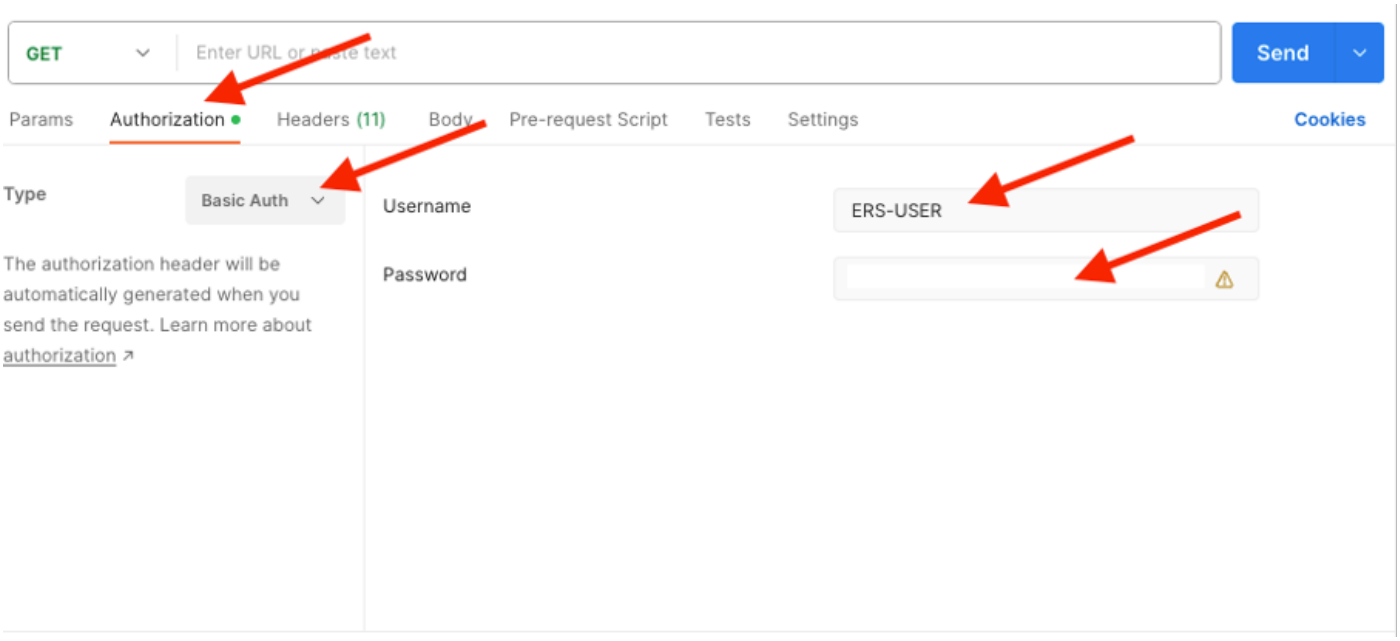
6. Vous pouvez maintenant voir la configuration requise pour effectuer l'appel d'API en utilisant XML ou JSON sur n'importe quel client de repos ainsi qu'un exemple de réponse attendue.



7.Retour à Postman configurer l'authentification de base à ISE. Sous l'onglet Authorization, sélectionnez Basic Auth comme type d'authentification et ajoutez les informations d'identification de l'utilisateur ISE ERS précédemment créées sur ISE.



Remarque : le mot de passe est affiché en texte clair sauf si des variables sont configurées sur Postman.

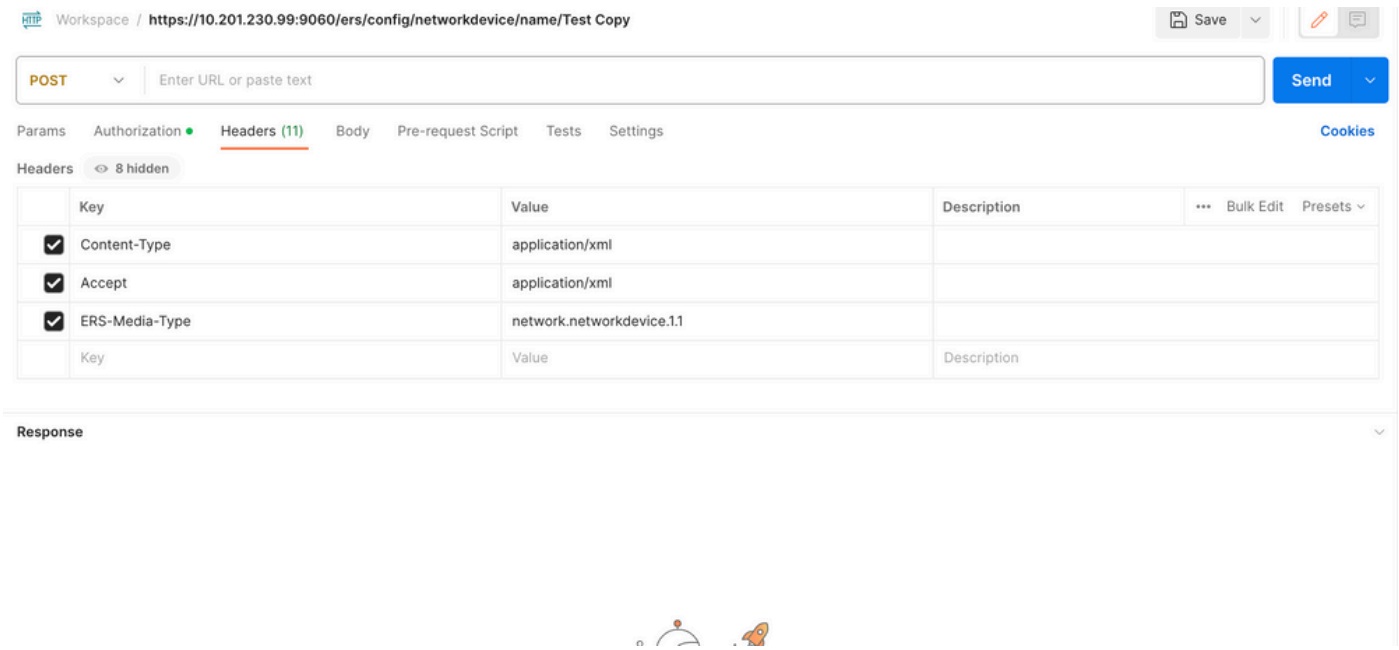


Créer NAD en utilisant XML

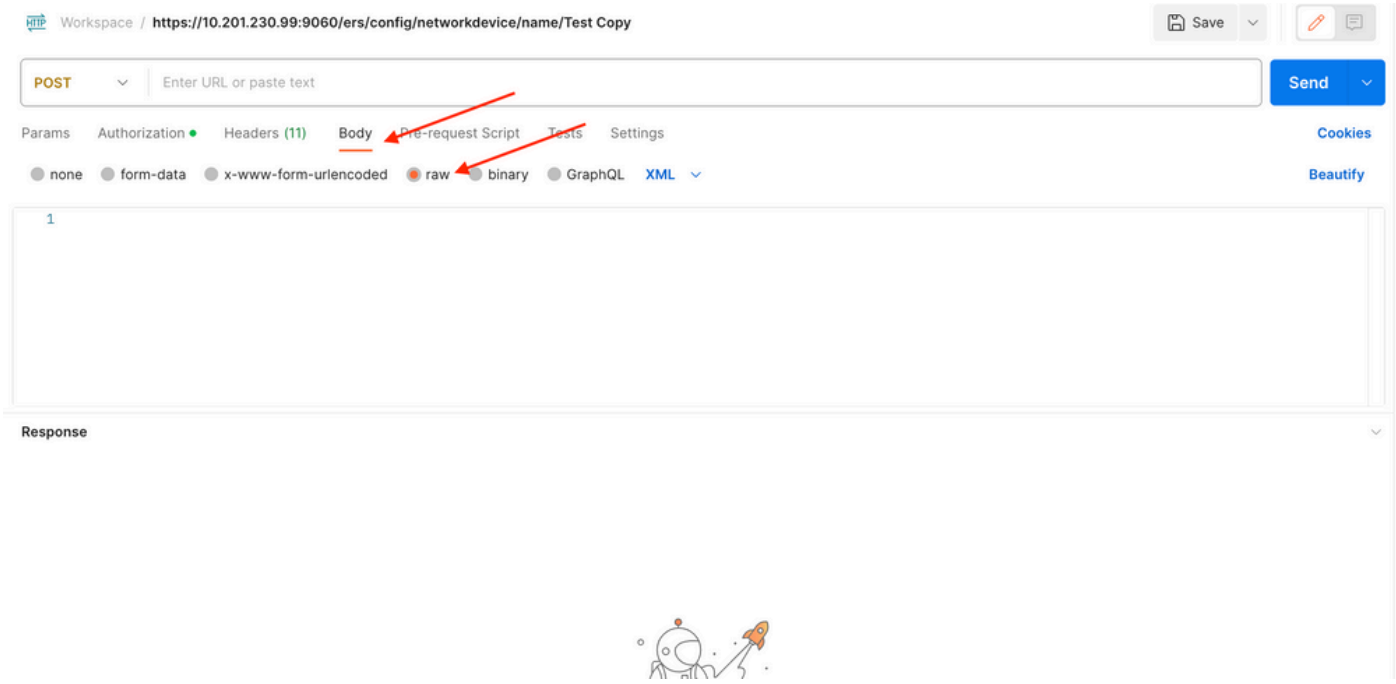
Créez TESTNAD1 avec les paramètres RADIUS TACACS, SNMP et TrustSec à l'aide de XML.

1. Sur le SDK, sous Créer, sont les en-têtes et les modèles requis pour effectuer l'appel ainsi que la réponse attendue.

2. Accédez à l'onglet En-têtes et configurez les en-têtes nécessaires pour l'appel API, comme indiqué dans le SDK. La configuration de l'en-tête doit ressembler à ceci :

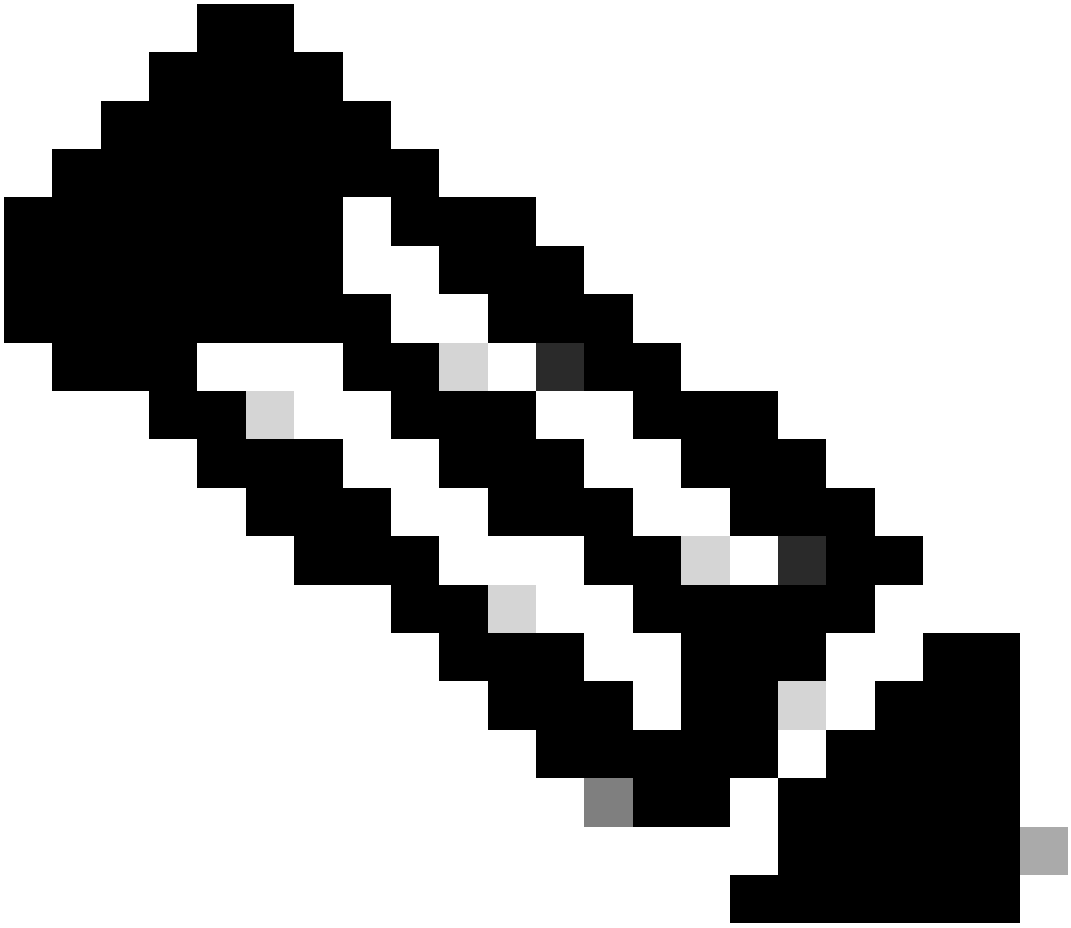


3. Accédez à l'en-tête Corps et sélectionnez Brut. Cela vous permet de coller le modèle XML nécessaire à la création du NAD.



4. Le modèle XML ressemble à ceci (modifiez les valeurs comme requis) :

<?xml version="1.0" encoding="UTF-8"?> <ns0:networkdevice xmlns:ns0="network.ers.ise.cisco.com" xmlns:xs="Schema XML File" xmlns:ns1="ers.ise.cisco.com" xmlns:ers="ers.ise.cisco.com" description="**This NAD was added via ERS API**" name="**TESTNAD1**"> <authenticationSettings> <dtlsRequired>true</dtlsRequired> <enableKeyWrap>**true**</enableKeyWrap> <keyEncryptionKey>**1234567890123456**</keyEncryptionKey> <keyInputFormat>**ASCII**</keyInputFormat> <messageAuthenticatorCodeKey>**12345678901234567890**</messageAuthenticatorCodeKey> <radiusSharedSecret>**cisco123**</radiusSharedSecret> </authenticationSettings> <coaPort>**1700**</coaPort> <dtlsDnsName>**Domain**</dtlsDnsName> <NetworkDeviceIPList> <NetworkDeviceIP> <ipaddress>**NAD IP Address**</ipaddress> <mask>32</mask> </NetworkDeviceIP> </NetworkDeviceIPList> <NetworkDeviceGroupList> <NetworkDeviceGroup>Location#All Locations#**LAB**</NetworkDeviceGroup> <NetworkDeviceGroup>Device Type#All Device Types#**Access-Layer**</NetworkDeviceGroup> </NetworkDeviceGroupList> <profileName>**Cisco**</profileName> <snmpsettings> <linkTrapQuery>**true**</linkTrapQuery> <macTrapQuery>**true**</macTrapQuery> <originatingPolicyServicesNode>**Auto**</originatingPolicyServicesNode> <pollingInterval>**3600**</pollingInterval> <roCommunity>**aaa**</roCommunity> <version>**ONE**</version> </snmpsettings> <tacacsSettings> <connectModeOptions>**ON_LEGACY**</connectModeOptions> <sharedSecret>**cisco123**</sharedSecret> </tacacsSettings> <trustsecsettings> <deviceAuthenticationSettings> <sgaDeviceId>**TESTNAD1**</sgaDeviceId> <sgaDevicePassword>**cisco123**</sgaDevicePassword> </deviceAuthenticationSettings> <deviceConfigurationDeployment> <enableModePassword>**cisco123**</enableModePassword> <execModePassword>**cisco123**</execModePassword> <execModeUsername>**Admin**</execModeUsername> <includeWhenDeployingSGTUpdates>**true**</includeWhenDeployingSGTUpdates> </deviceConfigurationDeployment> <pushIdSupport>**false**</pushIdSupport> <sgaNotificationAndUpdates> <coaSourceHost>**ise3-1test**</coaSourceHost> <downlaodEnvironmentDataEveryXSeconds>**86400**</downlaodEnvironmentDataEveryXSeconds> <downlaodPeerAuthorizationPolicyEveryXSeconds>**86400**</downlaodPeerAuthorizationPolicyEveryXSeconds> <downloadSGACLListsEveryXSeconds>**86400**</downloadSGACLListsEveryXSeconds> <otherSGADevicesToTrustThisDevice>**false**</otherSGADevicesToTrustThisDevice> <reAuthenticationEveryXSeconds>**86400**</reAuthenticationEveryXSeconds> <sendConfigurationToDevice>**false**</sendConfigurationToDevice> <sendConfigurationToDeviceUsing>**ENABLE_USING_COA**</sendConfigurationToDeviceUsing> </sgaNotificationAndUpdates> </trustsecsettings> </ns0:networkdevice>



Remarque : il est important de noter que les lignes suivantes ne sont requises que si **<enableKeyWrap>{false|true}</enableKeyWrap>** est défini sur **true**. Sinon, vous pouvez supprimer la même chose du modèle XML :

<keyEncryptionKey>**1234567890123456**</keyEncryptionKey> <keyInputFormat>**ASCII**</keyInputFormat>
<messageAuthenticatorCodeKey>**12345678901234567890**</messageAuthenticatorCodeKey>

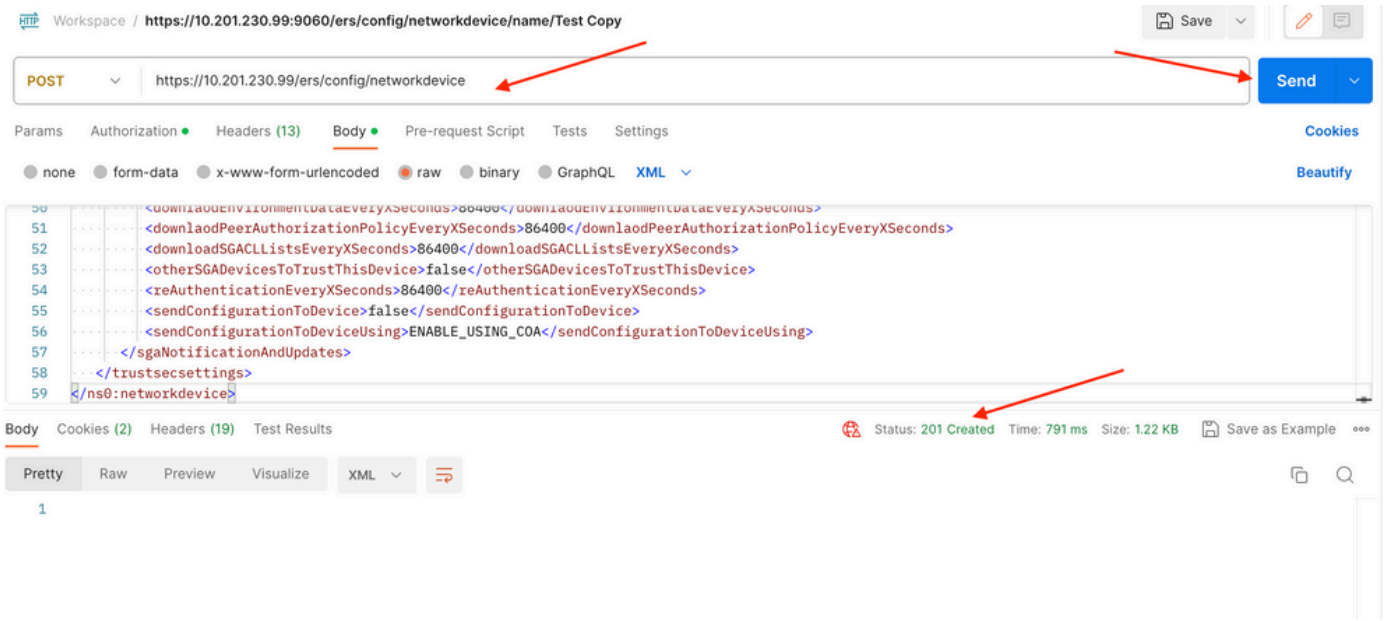
Vous pouvez supprimer la configuration dont vous n'avez pas besoin du modèle et simplement laisser les données que vous devez réellement ajouter lors de la création du NAD. Par exemple, voici le même modèle, mais uniquement avec la configuration TACACS. Quelle que soit la configuration requise, assurez-vous que le modèle se termine par **</ns0:networkdevice>.**

<?xml version="1.0" encoding="UTF-8"?> <ns0:networkdevice xmlns:ns0="network.ers.ise.cisco.com" xmlns:xs="Schema XML File"

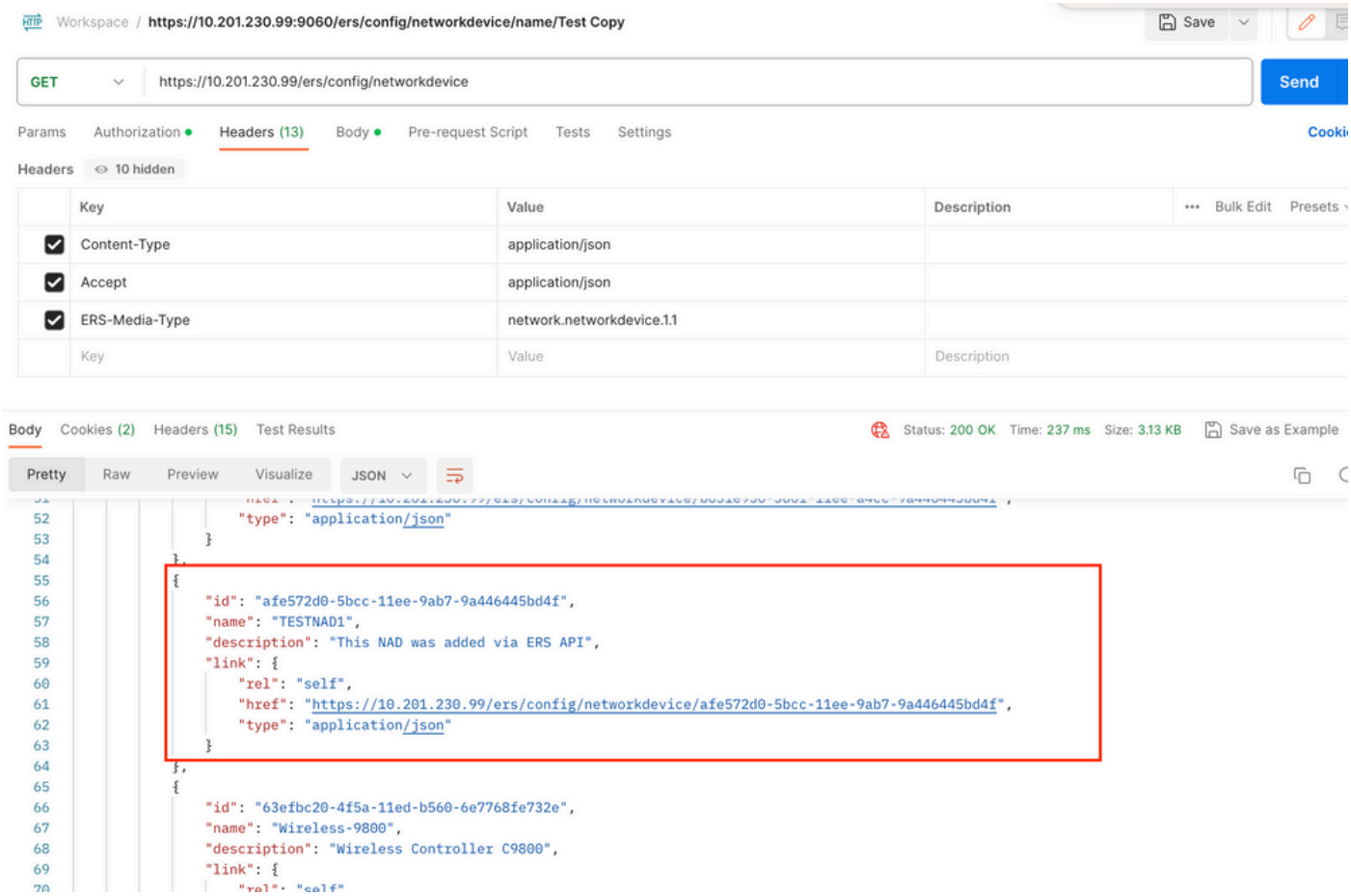
xmlns:ns1="ers.ise.cisco.com" xmlns:ers="ers.ise.cisco.com" description="**This NAD was added via ERS API**" name="**TESTNAD1**"> <NetworkDeviceIPList> <NetworkDeviceIP> <ipaddress>**NAD IP Address**</ipaddress> <mask>**32**</mask> </NetworkDeviceIP> </NetworkDeviceIPList> <NetworkDeviceGroupList> <NetworkDeviceGroup>Location#All Locations#**LAB**</NetworkDeviceGroup> <NetworkDeviceGroup>Device Type#All Device Types#**Access-Layer**</NetworkDeviceGroup> </NetworkDeviceGroupList> <profileName>Cisco</profileName> <tacacsSettings> <connectModeOptions>**ON_LEGACY**</connectModeOptions> <sharedSecret>**cisco123**</sharedSecret> </tacacsSettings> </ns0:networkdevice>

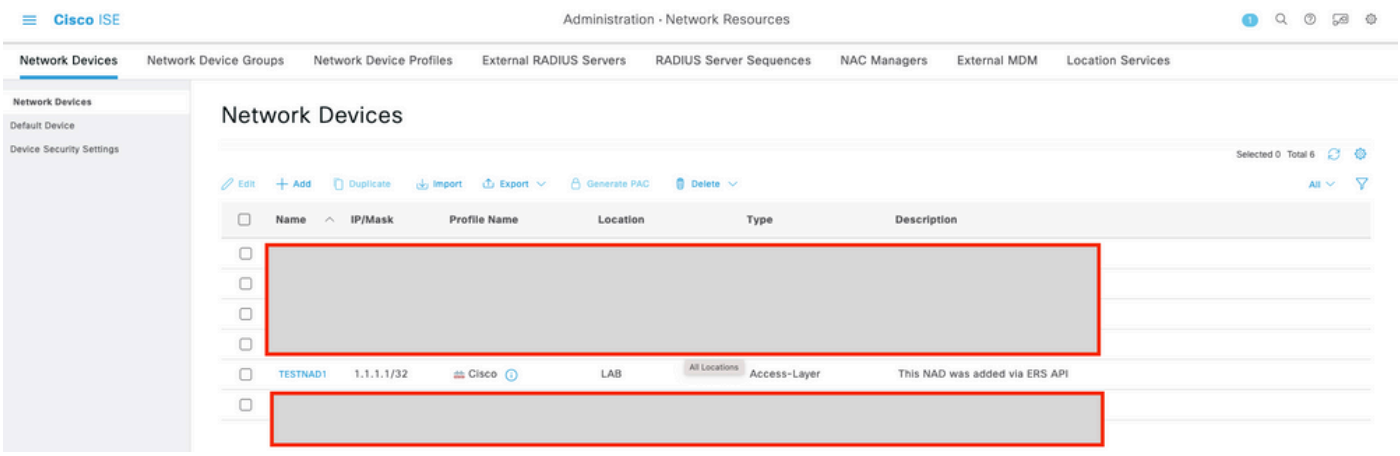
5. Collez le modèle XML pour **raw** sous l'en-tête **Body**.

6. Sélectionnez **POST** comme méthode, collez **https://{ISE-ip}/ers/config/networkdevice** et cliquez sur **Send. Si tout a été correctement configuré, vous devez voir un message 201 Created** et le résultat vide.



7. Vérifiez si le NAD a été créé en effectuant un appel **GET** pour le NAD ou en vérifiant la liste ISE NAD.



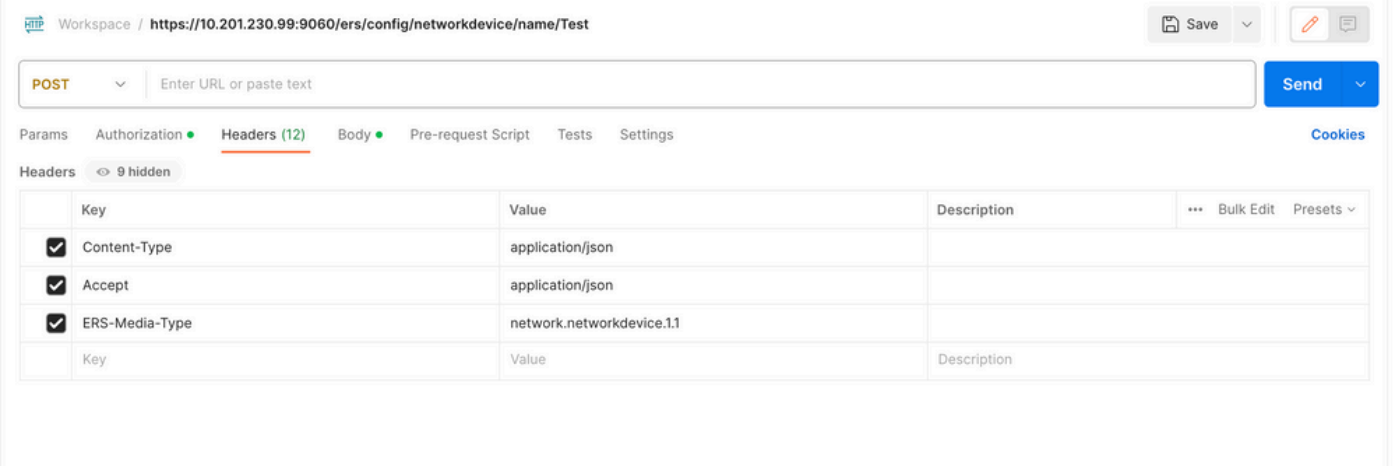


Créer NAD avec JSON

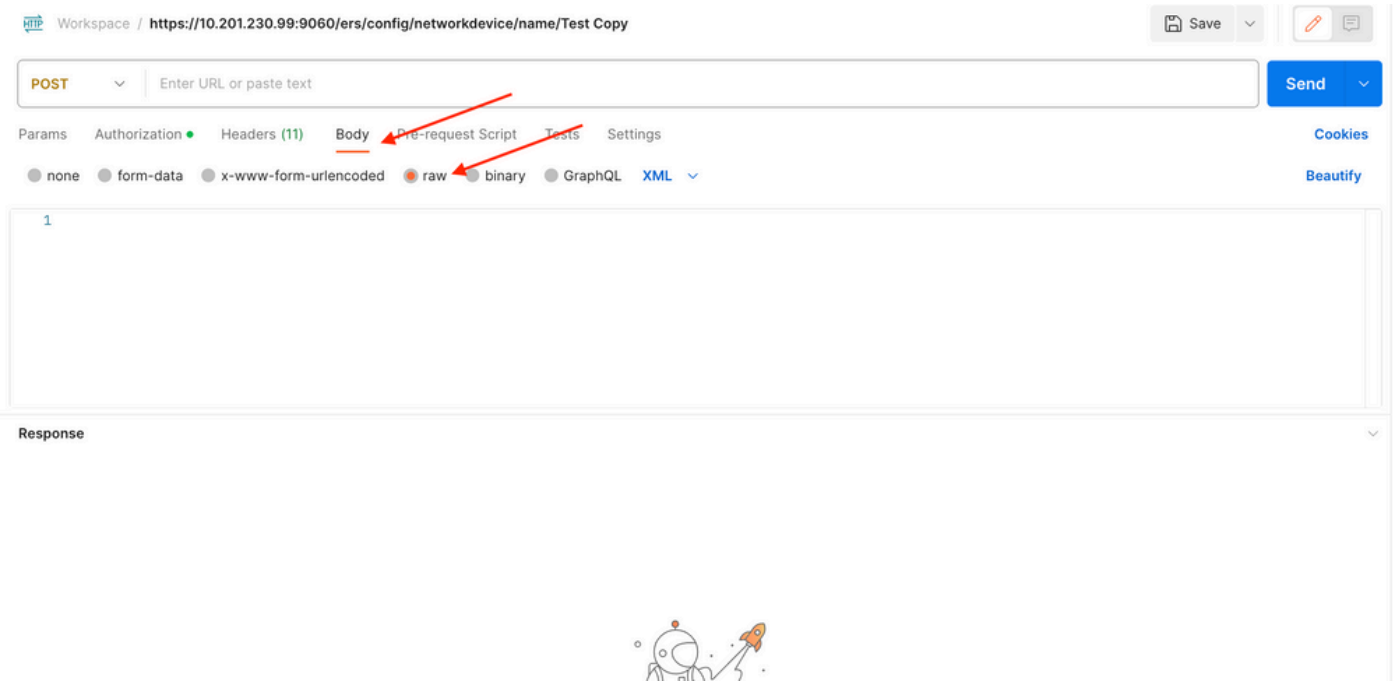
Créez TESTNAD2 avec les paramètres RADIUS TACACS, SNMP et TrustSec à l'aide de JSON.

1. Sur le SDK, sous **Créer,** sont les en-têtes et les modèles requis pour effectuer l'appel ainsi que la réponse attendue.

2. Accédez à l'onglet **En-têtes** et configurez les en-têtes nécessaires pour l'appel API, comme indiqué dans le SDK. La configuration de l'en-tête doit ressembler à ceci :

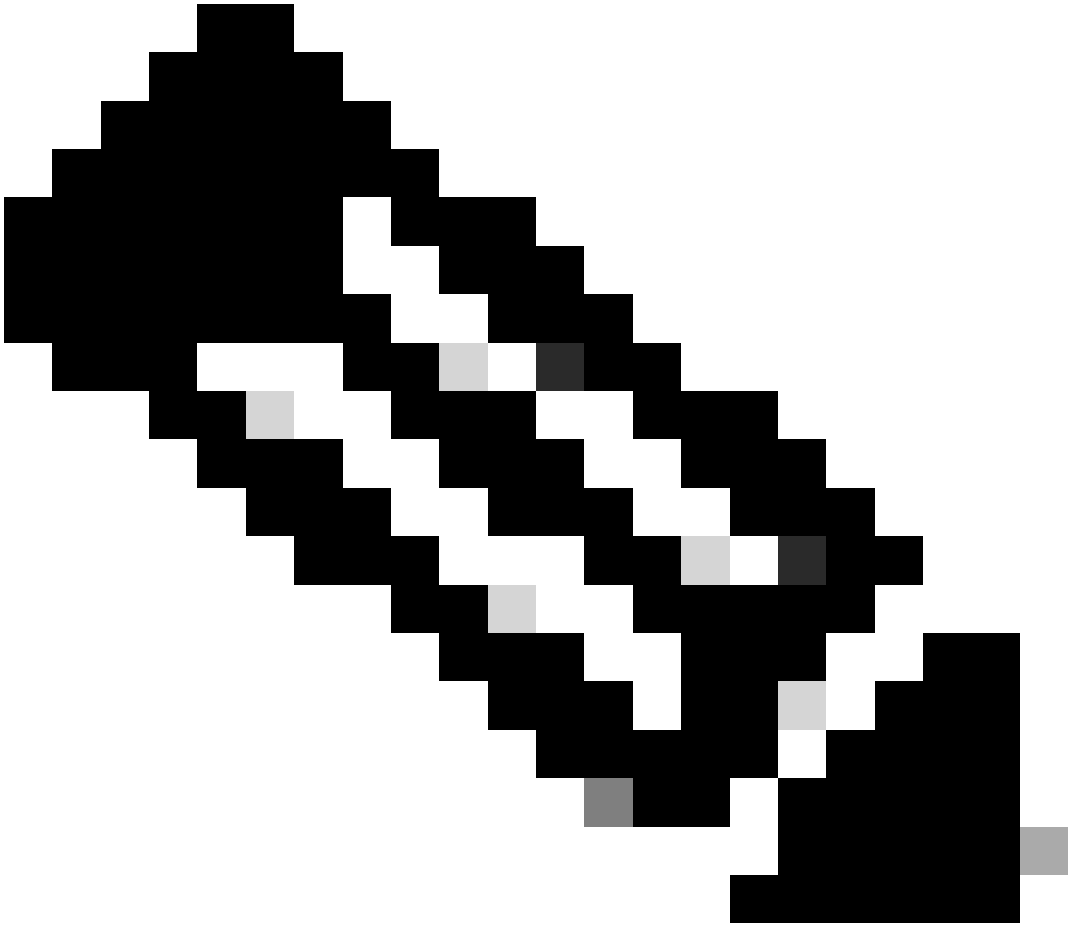


3. Accédez à l'en-tête **Corps** et sélectionnez **Brut**. Cela vous permet de coller le modèle JSON nécessaire à la création du NAD.



4. Le modèle JSON doit ressembler à ceci (modifiez les valeurs comme requis) :

{ "NetworkDevice": { "name": "**TESTNAD2**", "description": "**This NAD was added via ERS API**", "authenticationSettings": { "radiusSharedSecret": "**cisco123**", "enableKeyWrap": **true**, "dtlsRequired": **true**, "keyEncryptionKey": "**1234567890123456**", "messageAuthenticatorCodeKey": "**12345678901234567890**", "keyInputFormat": "**ASCII**" }, "snmpsettings": { "version": "ONE", "roCommunity": "**aaa**", "pollingInterval": **3600**, "linkTrapQuery": **true**, "macTrapQuery": **true**, "originatingPolicyServicesNode": "**Auto**" }, "trustsecsettings": { "deviceAuthenticationSettings": { "sgaDeviceId": "**TESTNAD2**", "sgaDevicePassword": "**cisco123**" }, "sgaNotificationAndUpdates": { "downlaodEnvironmentDataEveryXSeconds": **86400**, "downlaodPeerAuthorizationPolicyEveryXSeconds": **86400**, "reAuthenticationEveryXSeconds": **86400**, "downloadSGACLListsEveryXSeconds": **86400**, "otherSGADevicesToTrustThisDevice": **false**, "sendConfigurationToDevice": **false**, "sendConfigurationToDeviceUsing": "**ENABLE_USING_COA**", "coaSourceHost": "**ise3-1test**" }, "deviceConfigurationDeployment": { "includeWhenDeployingSGTUpdates": **true**, "enableModePassword": "**cisco123**", "execModePassword": "**cisco123**", "execModeUsername": "**Admin**" }, "pushIdSupport": "**false**" }, "tacacsSettings": { "sharedSecret": "**cisco123**", "connectModeOptions": "**ON_LEGACY**" }, "profileName": "**Cisco**", "coaPort": **1700**, "dtlsDnsName": "**Domain**", "NetworkDeviceIPList": [{ "ipaddress": "**NAD IP Adress**", "mask": **32** }], "NetworkDeviceGroupList": ["Location#All Locations", "Device Type#All Device Types"] } }

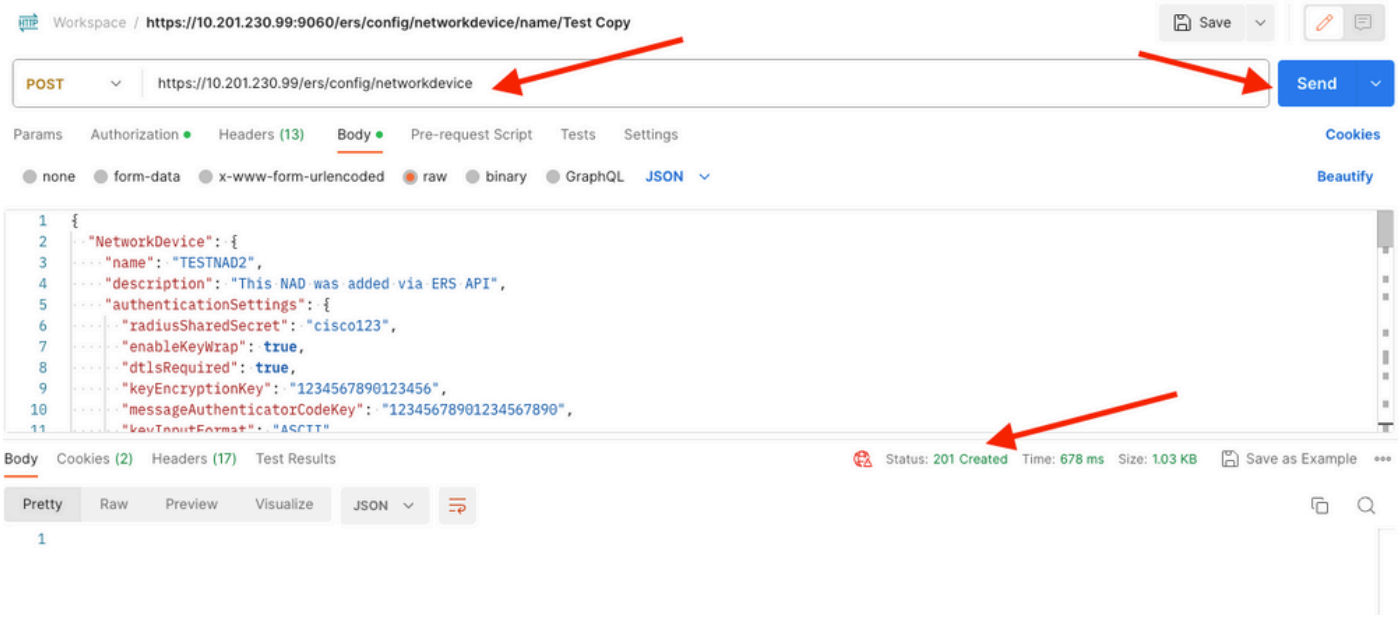


Remarque : il est important de noter que les lignes suivantes ne sont requises que si **enableKeyWrap":{false|true}**, est défini sur **true**. Sinon, vous pouvez supprimer la même chose du modèle JSON :

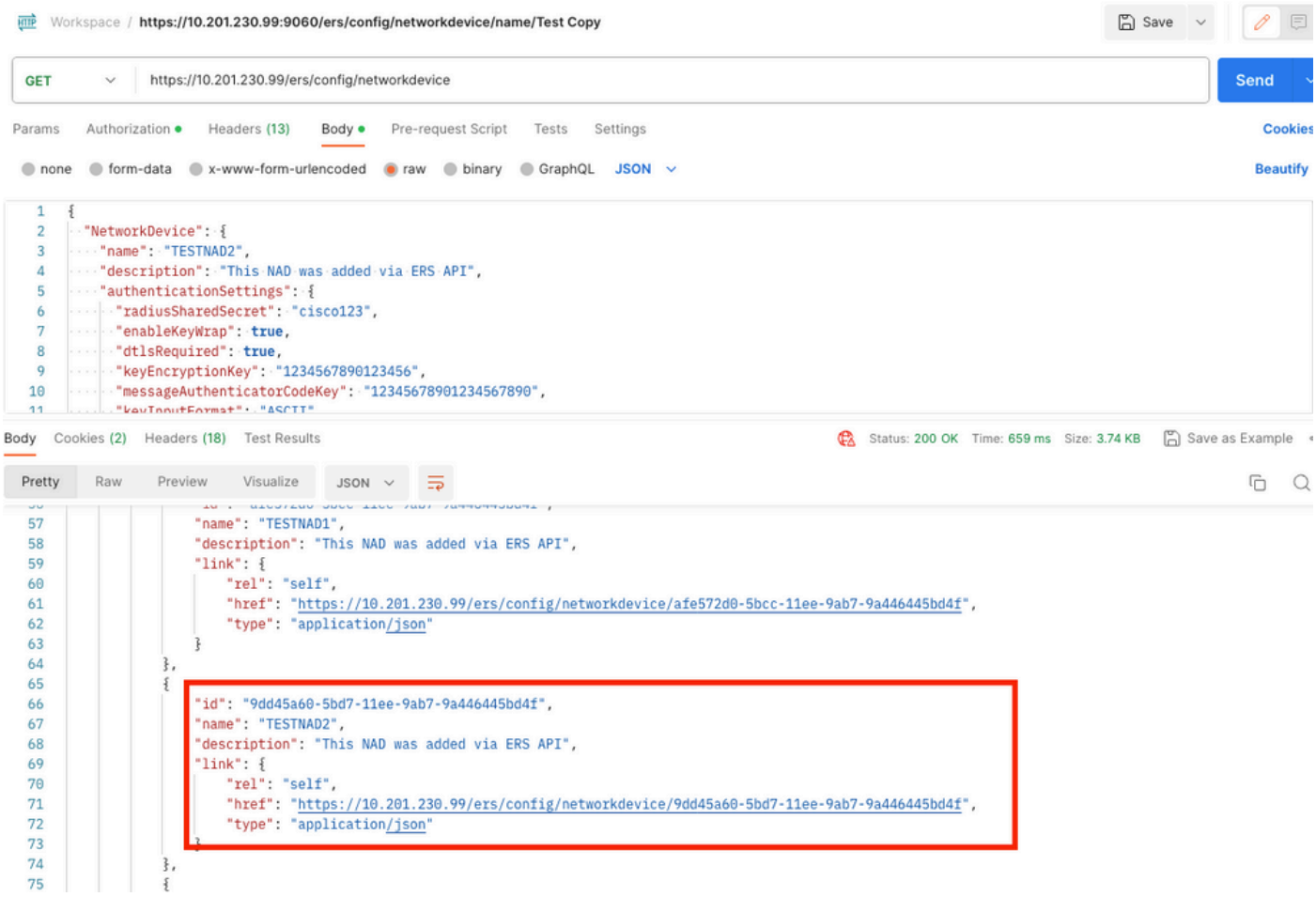
"keyEncryptionKey": "**1234567890123456**", "messageAuthenticatorCodeKey": "**12345678901234567890**", "keyInputFormat": "**ASCII**" Vous pouvez également supprimer la configuration dont vous n'avez pas besoin du modèle, et simplement laisser les données que vous avez réellement besoin d'être ajouté lors de la création du NAD.

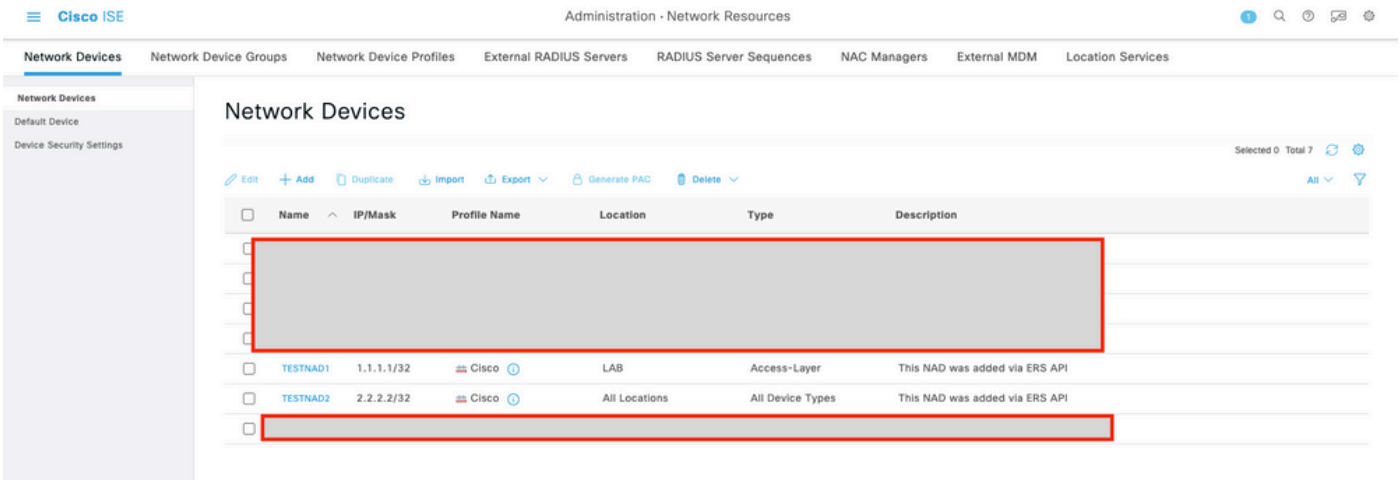
5. Collez le modèle JSON pour le **brut** sous l'en-tête **Body**.

6. Sélectionnez **POST** comme méthode, collez **https://{ISE-ip}/ers/config/networkdevice** et cliquez sur **Send. Si tout a été correctement configuré, vous devez voir un message 201 Created** et le résultat vide.



7. Vérifiez si le NAD a été créé en effectuant un appel GET pour le NAD ou en vérifiant la liste ISE NAD.





Vérifier

Si vous pouvez accéder à la page GUI du service API, par exemple, **https://*{iseip}*:*{port}*/api/swagger-ui/index.html** ou https://***{iseip}***:**9060/ers/sdk**, cela signifie que le service API fonctionne comme prévu.

Dépannage

- Toutes les opérations REST sont auditées et les journaux sont consignés dans les journaux système.
- Pour résoudre les problèmes liés aux API ouvertes, définissez le **niveau de journalisation** du composant **apiservice** sur **DEBUG** dans la fenêtre **Debug Log Configuration**.
- Pour résoudre les problèmes liés aux API ERS, définissez le **niveau de journalisation** du composant **ERS** sur **DEBUG** dans la fenêtre **Debug Log Configuration**. Pour afficher cette fenêtre, accédez à l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu et choisissez **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**.
- Vous pouvez télécharger les journaux à partir de la fenêtre **Download** Logs. Pour afficher cette fenêtre, accédez à l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône **Menu** et choisissez **Operations > Troubleshoot > Download Logs**.
- Vous pouvez choisir de télécharger un bundle de support à partir de l'onglet Support Bundle en cliquant sur le bouton **Download** sous l'onglet, ou de télécharger les journaux de débogage **api-service à** partir de l'onglet **Debug Logs** en cliquant sur la valeur du fichier de **journalisation** pour le journal de débogage api-service.

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.