Creazione di dispositivi di rete ISE con l'API ERS

Sommario

Introduzione

Questo documento descrive il processo di creazione di dispositivi di accesso alla rete (NAD) su ISE tramite l'API ERS con PostMan come client REST.

Prerequisiti

Requisiti

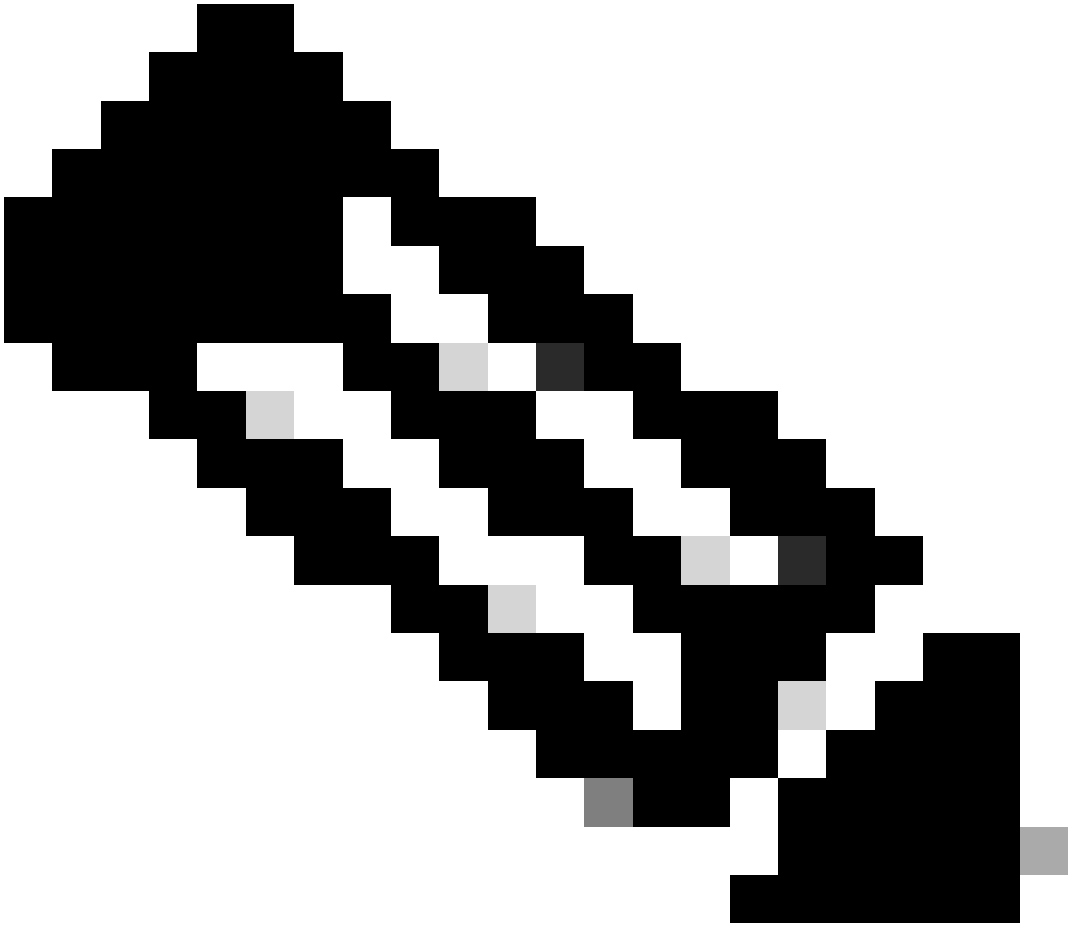
Cisco raccomanda la conoscenza dei seguenti argomenti:

- ISE (Identity Services Engine)
- ERS (Servizi esterni di assistenza a terra)
- I clienti REST come Postman, RESTED, Insonnia, e così via.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Patch 6 per Cisco ISE (Identity Services Engine) 3.1
- Postman REST client v10.17.4



Nota: la procedura è simile o identica per altre versioni ISE e client REST. Se non specificato diversamente, è possibile eseguire la procedura seguente su tutte le versioni software ISE 2.x e 3.x.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

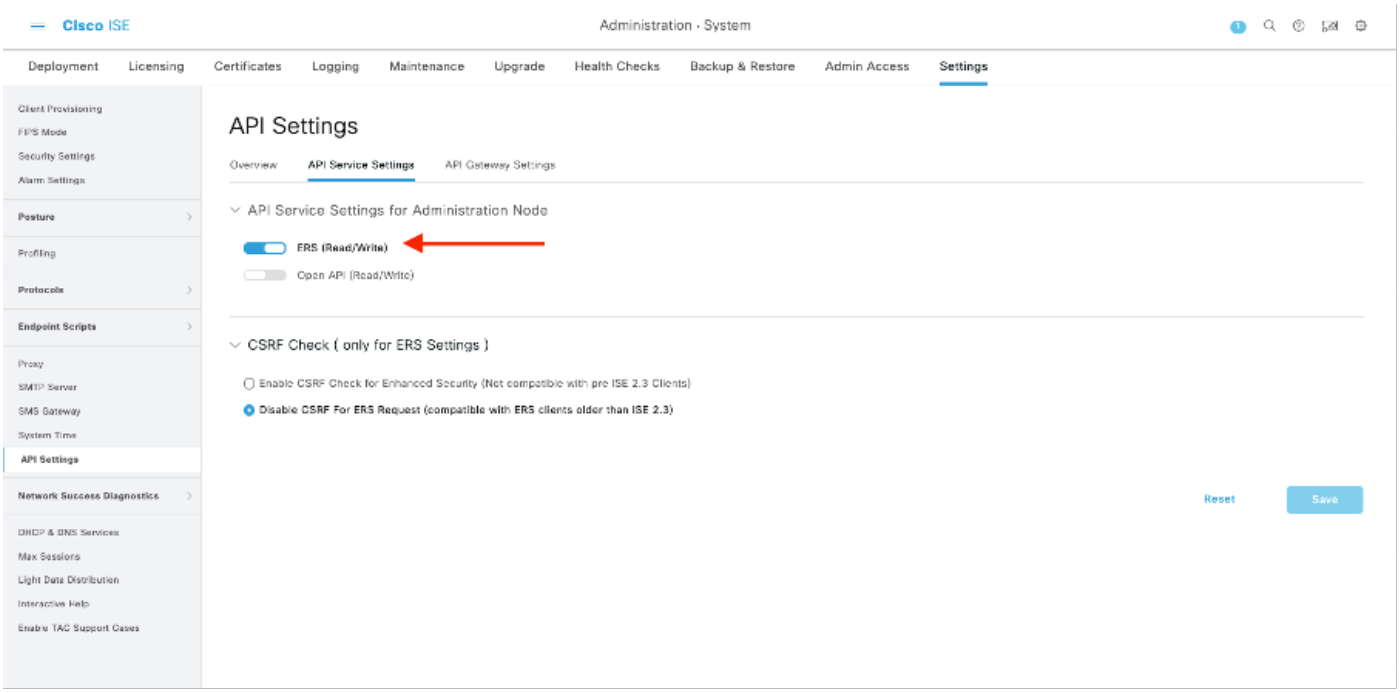
Configurazione

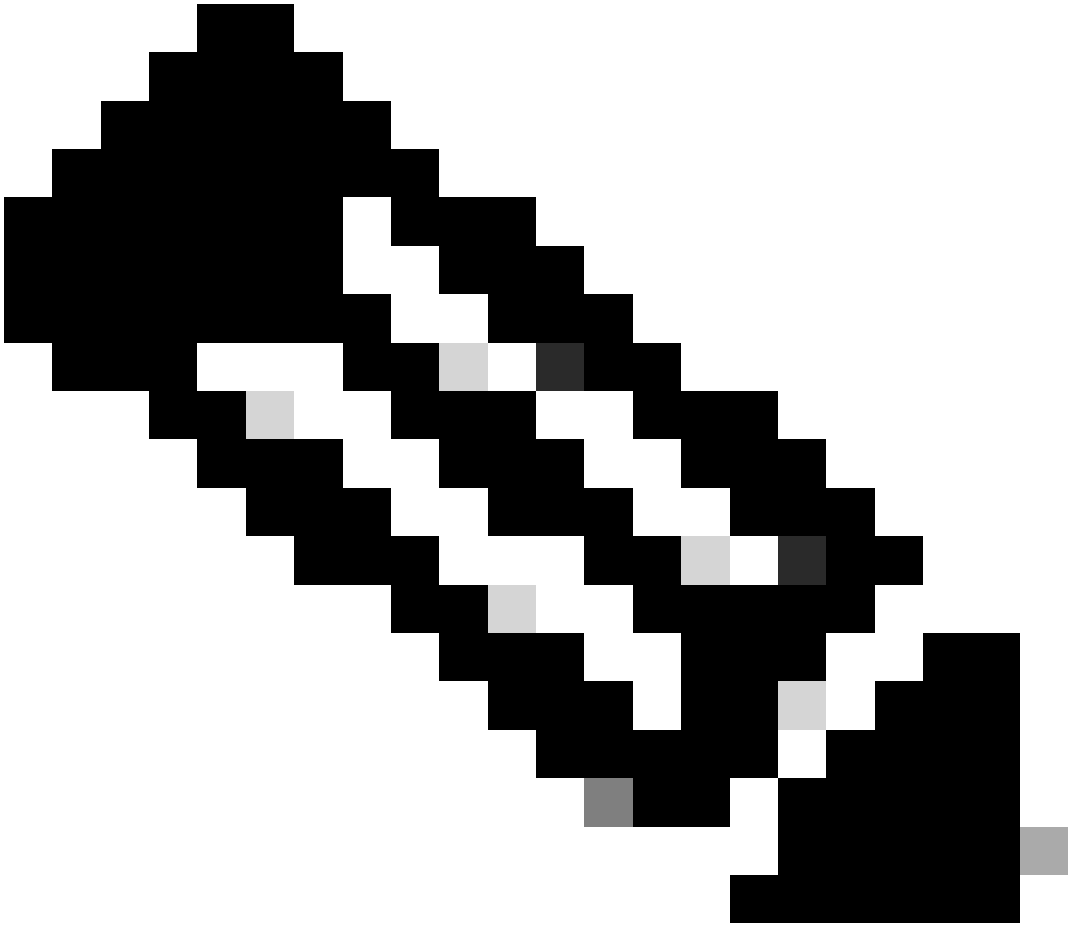
Abilita ERS (porta 9060)

Le API ERS sono API REST solo HTTPS che operano sulla porta 443 e sulla porta 9060. La porta 9060 è chiusa per impostazione predefinita, quindi deve essere aperta per prima. Se i client che tentano di accedere a questa porta non attivano prima ERS, viene visualizzato un timeout del

server. Pertanto, il primo requisito è abilitare ERS dall'interfaccia utente di amministrazione di Cisco ISE.

Passare a Amministrazione > Impostazioni > Impostazioni API e abilitare l'interruttore ERS (Read/Write).

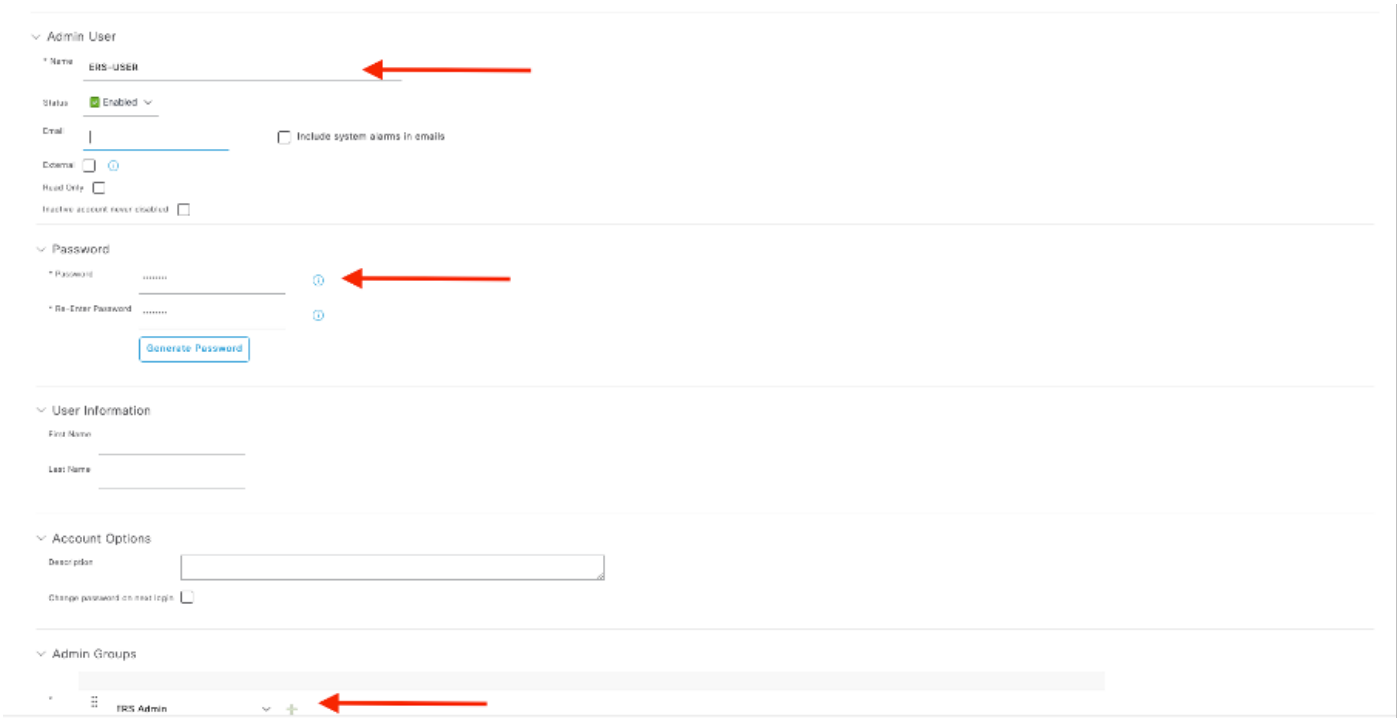




Nota: le API ERS supportano TLS 1.1 e TLS 1.2. Le API ERS non supportano TLS 1.0, a prescindere dall'abilitazione di TLS 1.0 nella finestra Security Settings (Impostazioni protezione) dell'interfaccia utente di Cisco ISE (Amministrazione > Sistema > Impostazioni > Impostazioni protezione). L'attivazione di TLS 1.0 nella finestra Impostazioni protezione è correlata solo al protocollo EAP e non influisce sulle API ERS.

Crea amministratore ERS

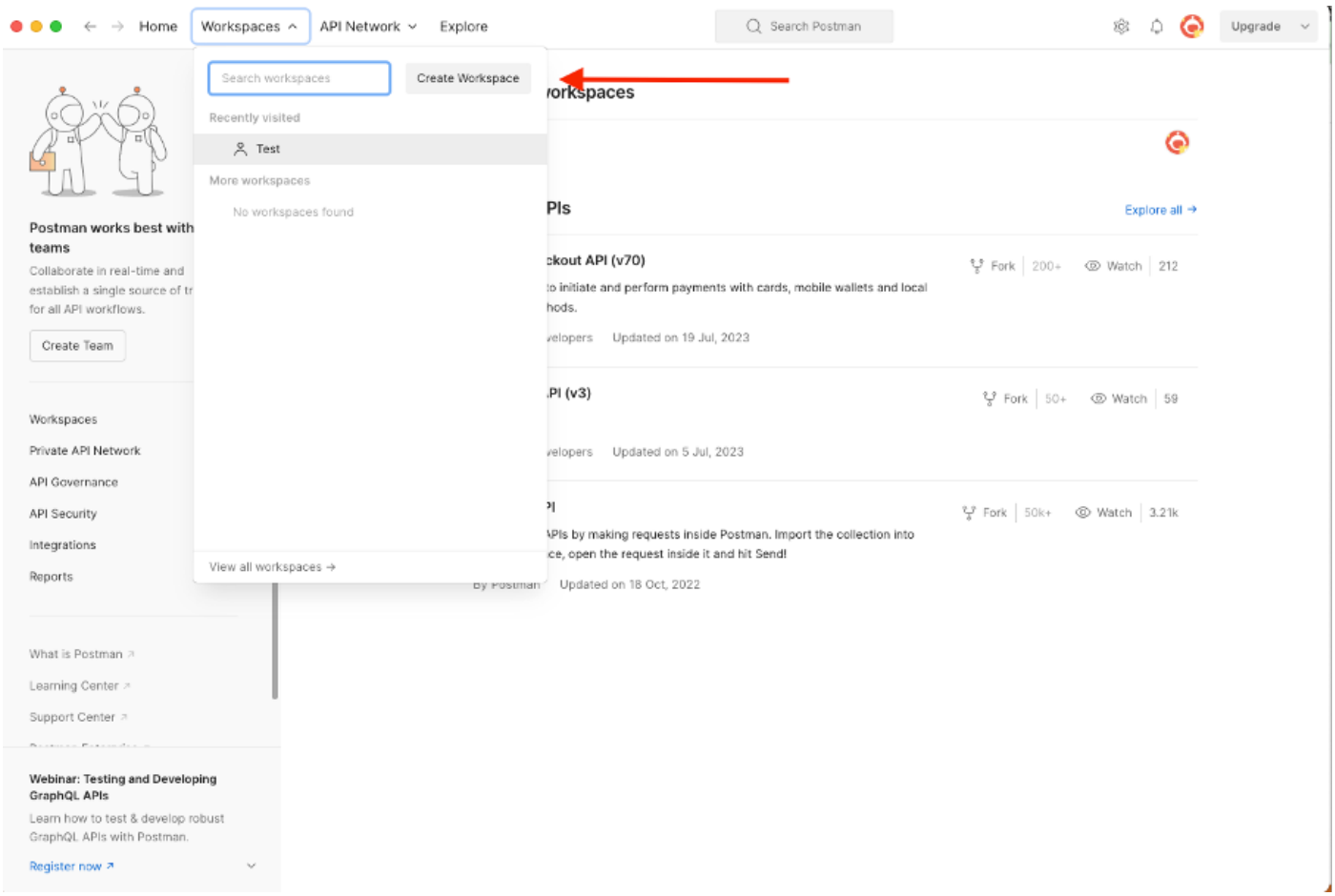
Creare un Cisco ISE Administrator, assegnare una password e aggiungere l'utente al gruppo admin come Amministratore ERS. È possibile lasciare vuota la parte restante della configurazione.



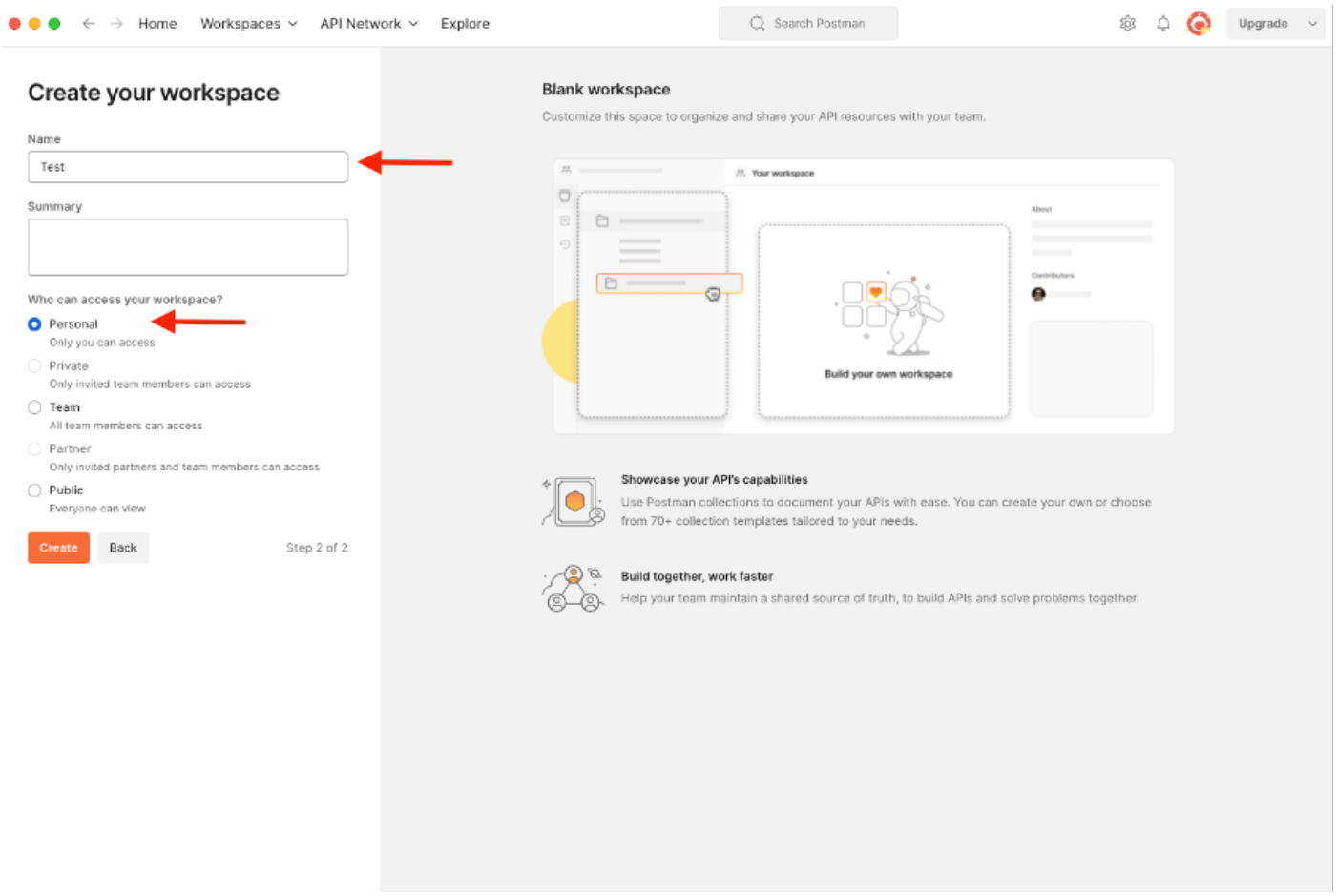
Imposta postino

Scarica o utilizza la versione online di Postman.

1. Creare un utente e un workspace facendo clic su Crea workspace nella scheda Workspace.



2. Selezionare Spazio di lavoro vuoto e assegnare un nome al workspace. È possibile aggiungere una descrizione e renderla pubblica. Per questo esempio, Personalis ha selezionato.

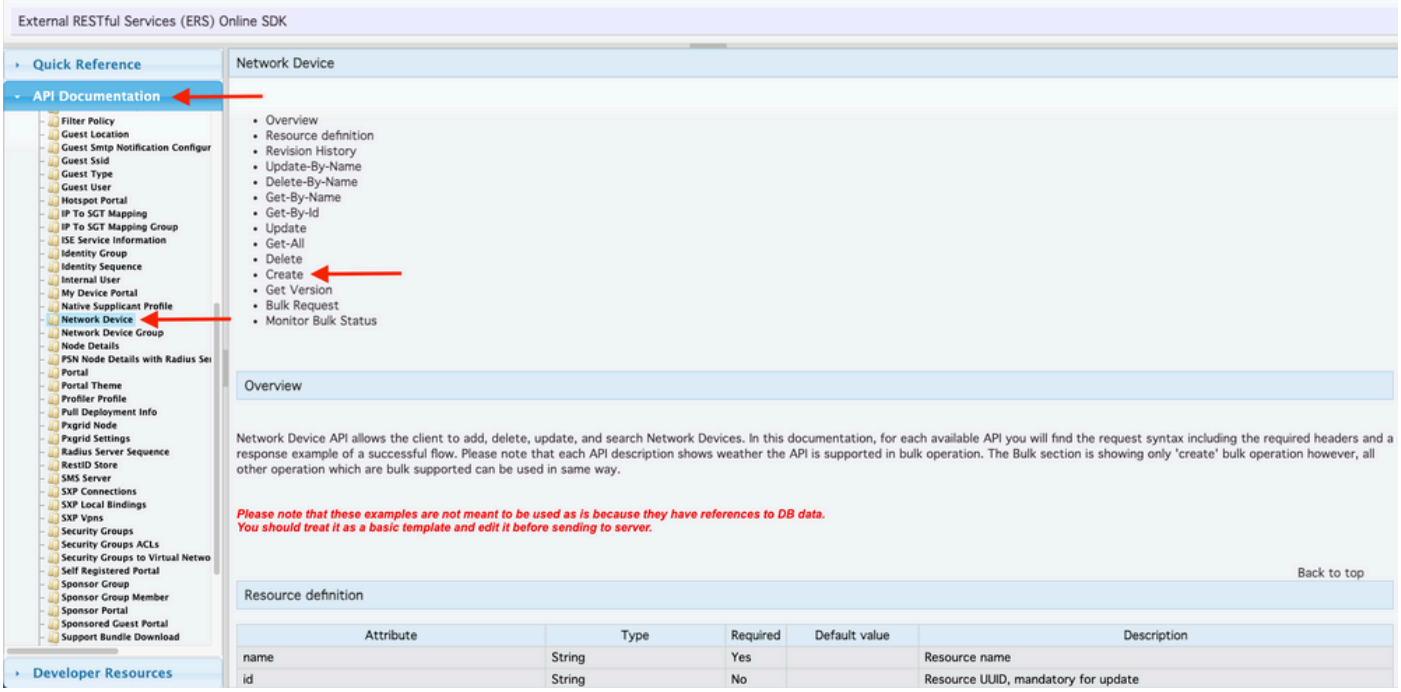


Una volta creata l'area di lavoro, è ora possibile configurare le chiamate API.

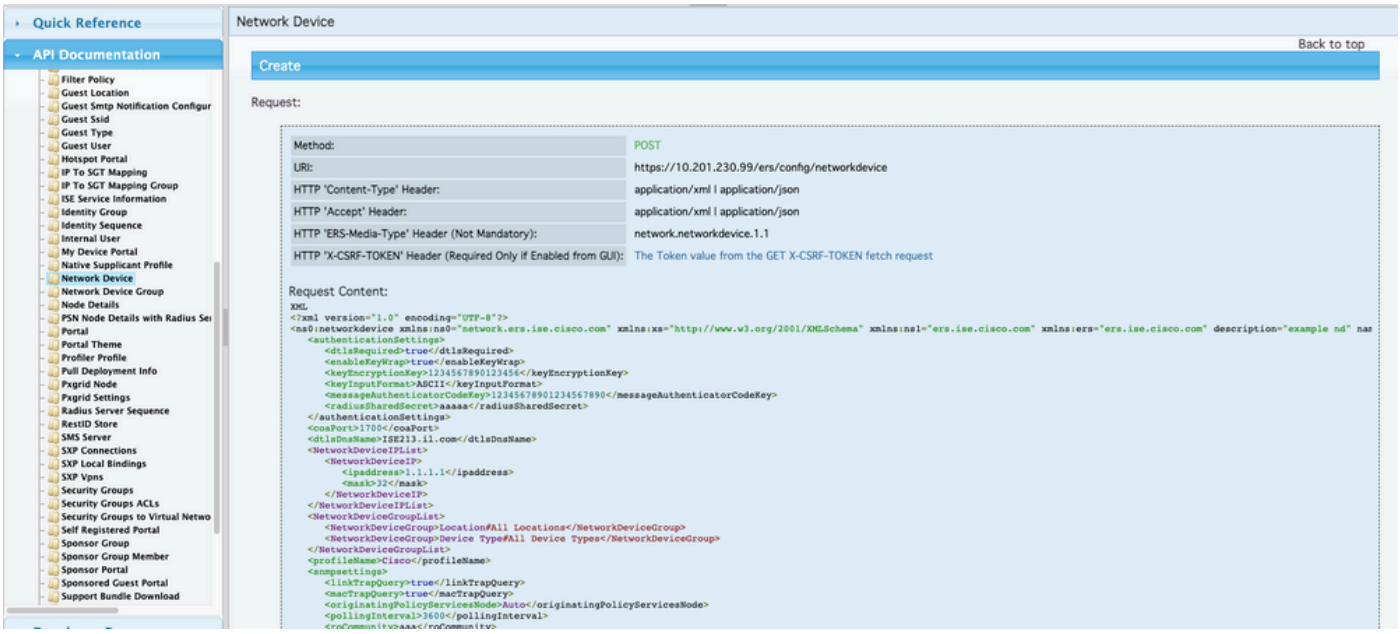
ISE SDK e autorizzazione Basic Postman

Per configurare una chiamata, accedere prima a ISE ERS SDK (Software Developer Kit). Questo strumento compila l'intero elenco di chiamate API che ISE può eseguire:

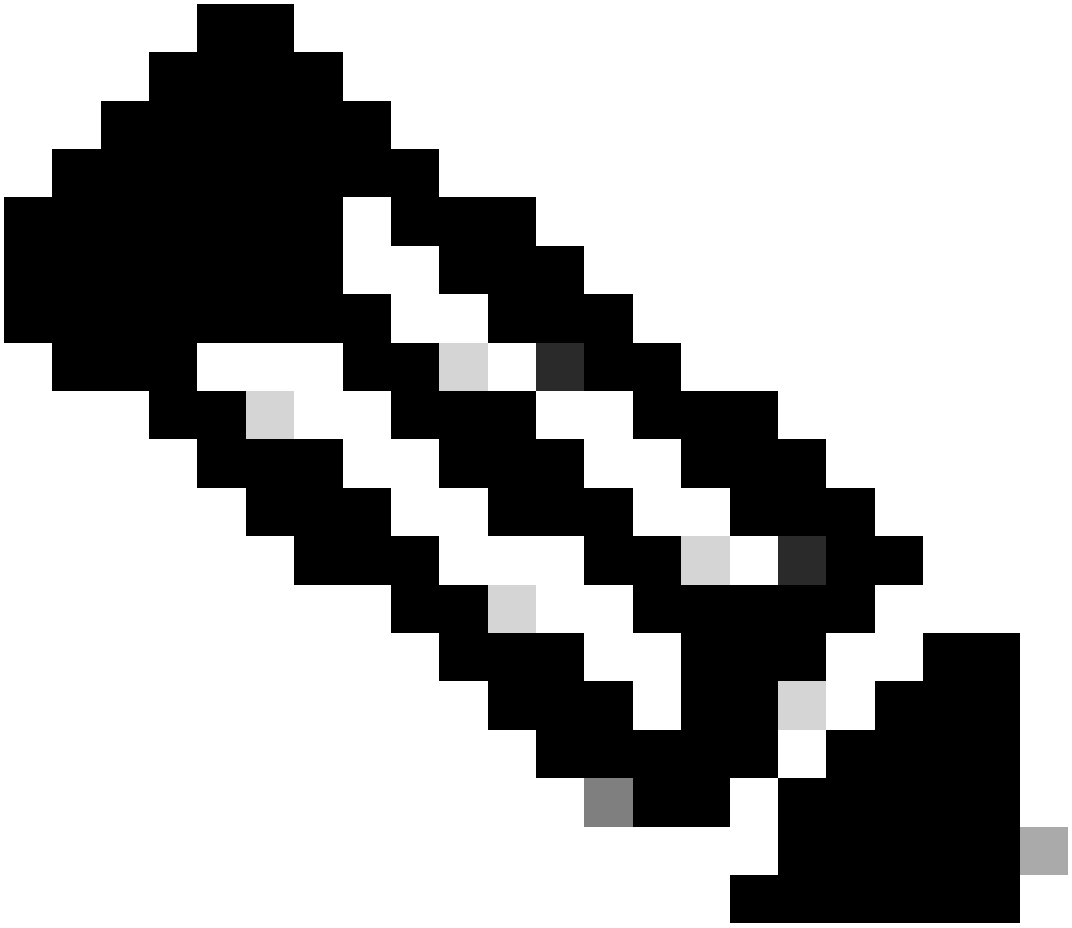
1. Passare a https://{ise-ip}/ers/sdk.
2. Accedere usando le credenziali ISE Admin.
3. Espandere la documentazione API.
4. Scorrere verso il basso fino a individuare Periferica di rete e fare clic su di essa.
5. Sotto questa opzione, è ora possibile trovare tutte le operazioni disponibili che è possibile eseguire per i dispositivi di rete su ISE. Selezionare Crea.



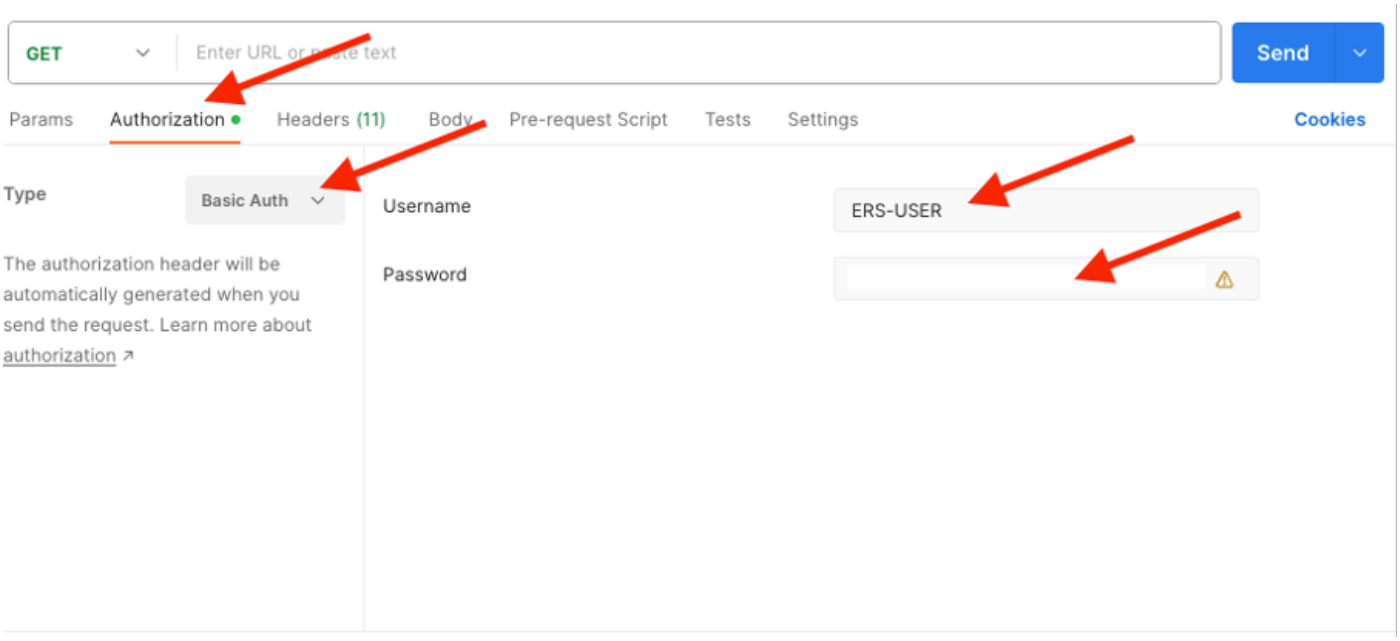
6. È ora possibile visualizzare la configurazione richiesta per eseguire la chiamata API utilizzando XML o JSON su qualsiasi client REST, nonché un esempio di risposta prevista.



7.Back to Postman configurare l'autenticazione di base per ISE. Nella scheda Authorization (Autorizzazione), selezionare Basic Auth (Autenticazione di base) come tipo di autenticazione, quindi aggiungere le credenziali utente ISE ERS precedentemente create su ISE.



Nota: la password viene visualizzata come testo non crittografato a meno che non siano configurate variabili in Postman.

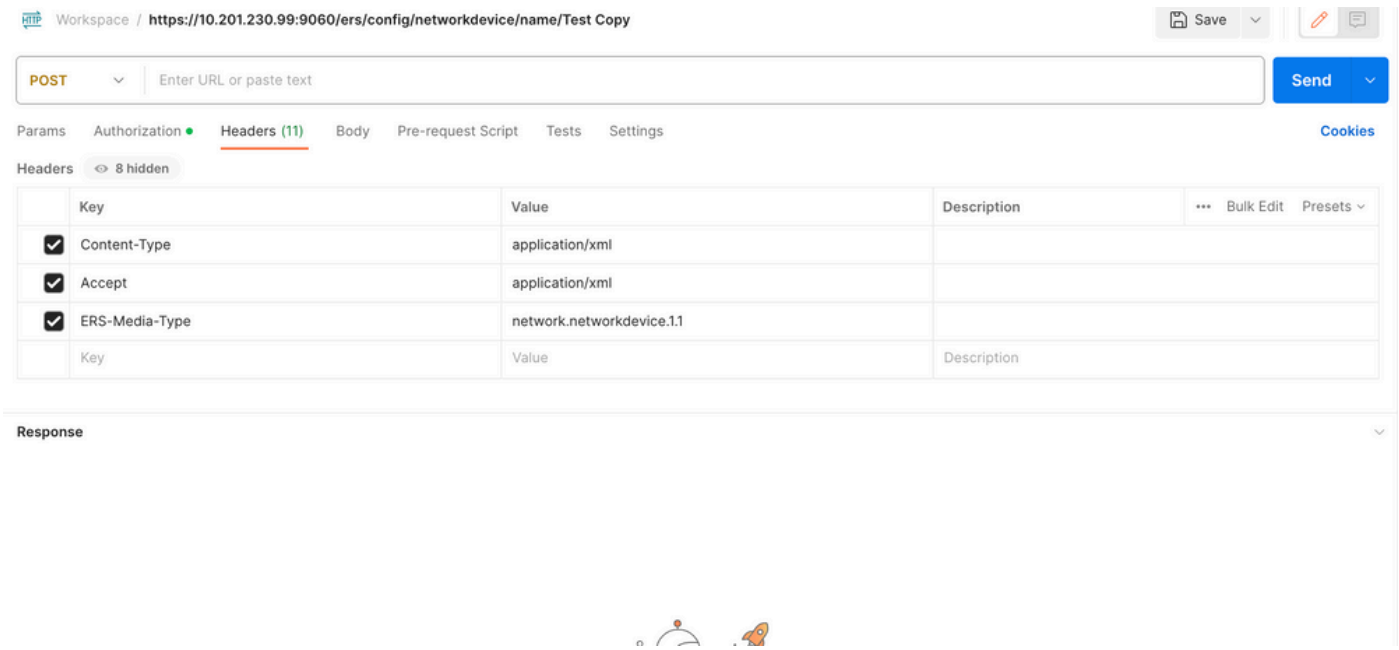


Creazione e utilizzo di XML

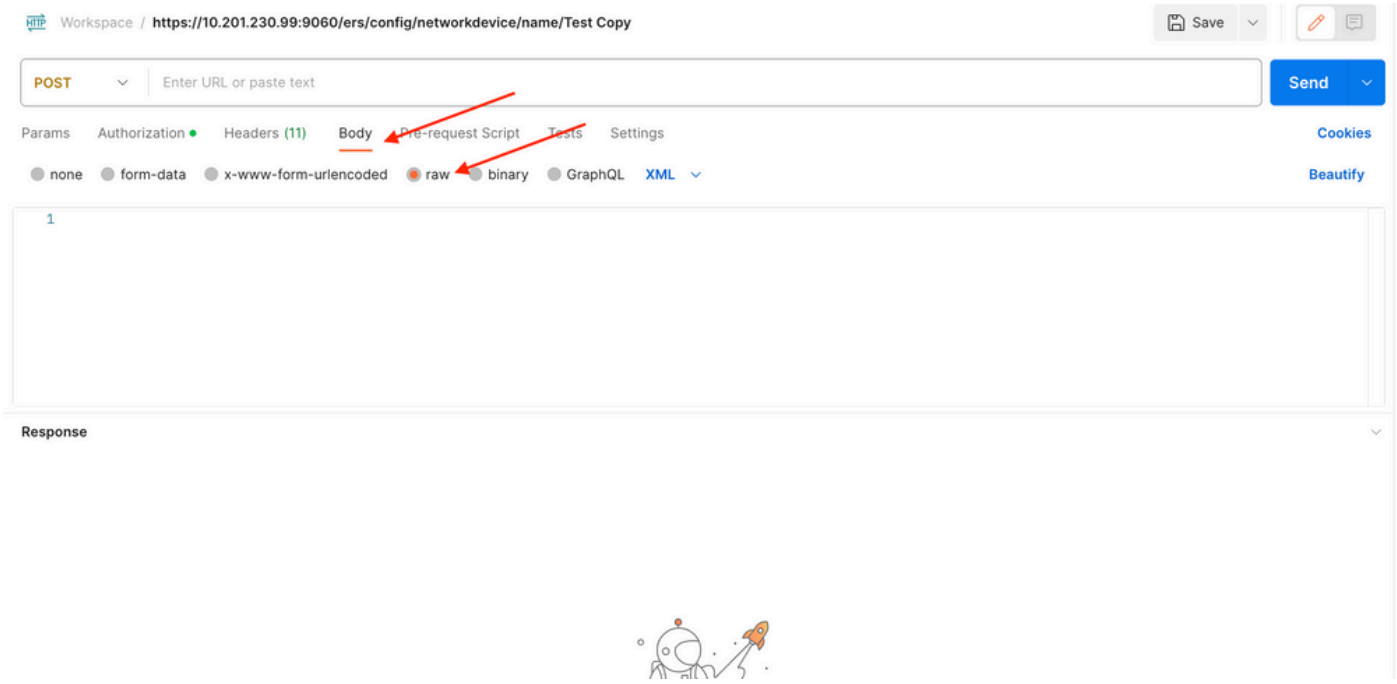
Creare TESTNAD1 con le impostazioni RADIUS TACACS, SNMP e TrustSec utilizzando XML.

1. Nell'SDK, in Crea, sono presenti le intestazioni e i modelli necessari per eseguire la chiamata, nonché la risposta prevista.

2. Passare alla scheda Intestazioni e configurare le intestazioni necessarie per la chiamata API come mostrato nell'SDK. La configurazione dell'intestazione deve essere simile alla seguente:

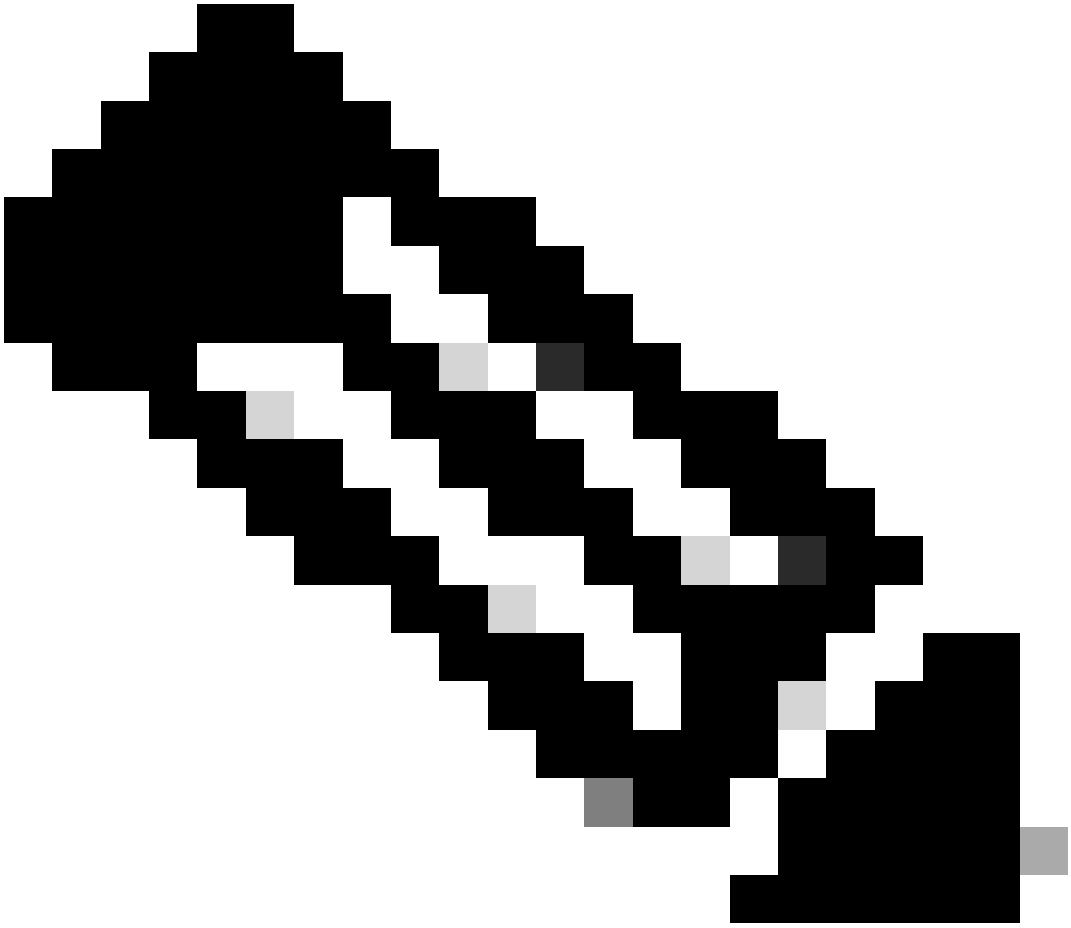


3. Spostarsi sull'intestazione Body e selezionare raw. In questo modo è possibile incollare il modello XML necessario per la creazione di NAD.



4. Il modello XML ha il seguente aspetto (modificare i valori in base alle esigenze):

<?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>



Nota: è importante notare che le righe successive sono obbligatorie solo se **<enableKeyWrap>{false|true}</enableKeyWrap>** è impostato su **true**. In caso contrario, è possibile eliminare lo stesso dal modello XML:

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

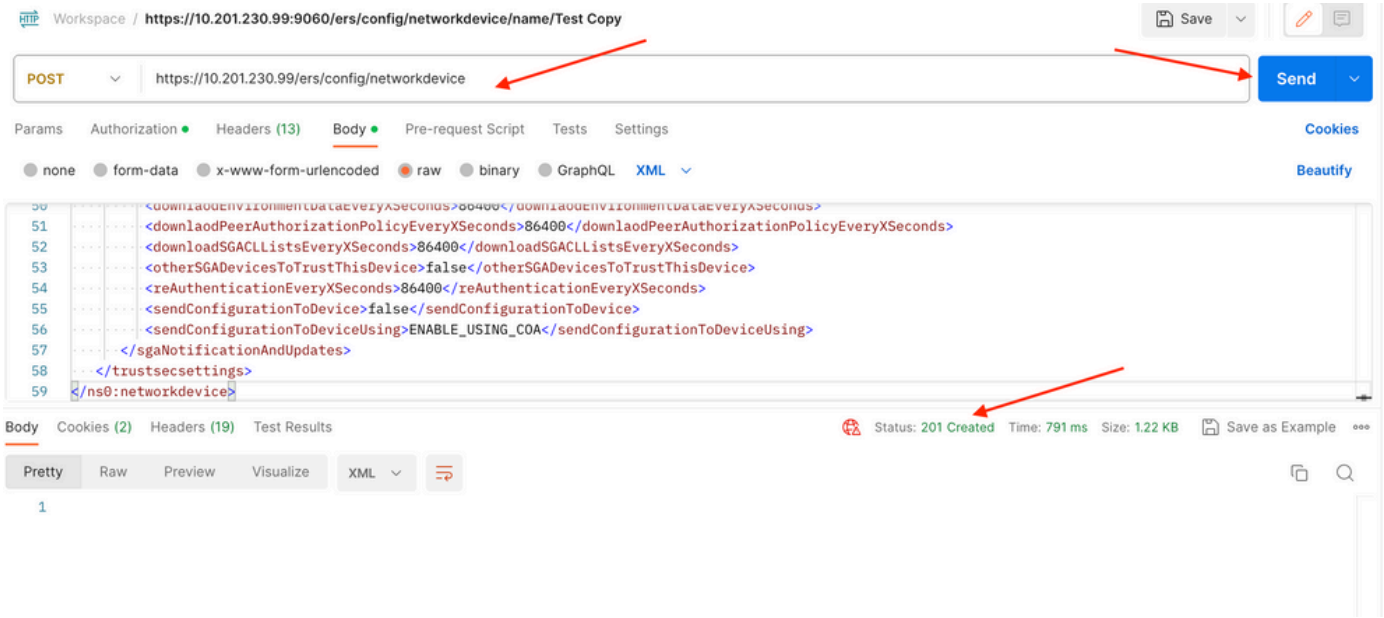
È possibile rimuovere la configurazione non necessaria dal modello e lasciare semplicemente i dati effettivamente necessari da aggiungere durante la creazione del NAD. Ad esempio, questo è lo stesso modello, ma solo con la configurazione TACACS. Indipendentemente dalla configurazione richiesta, assicurarsi che il modello termini con **</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**">

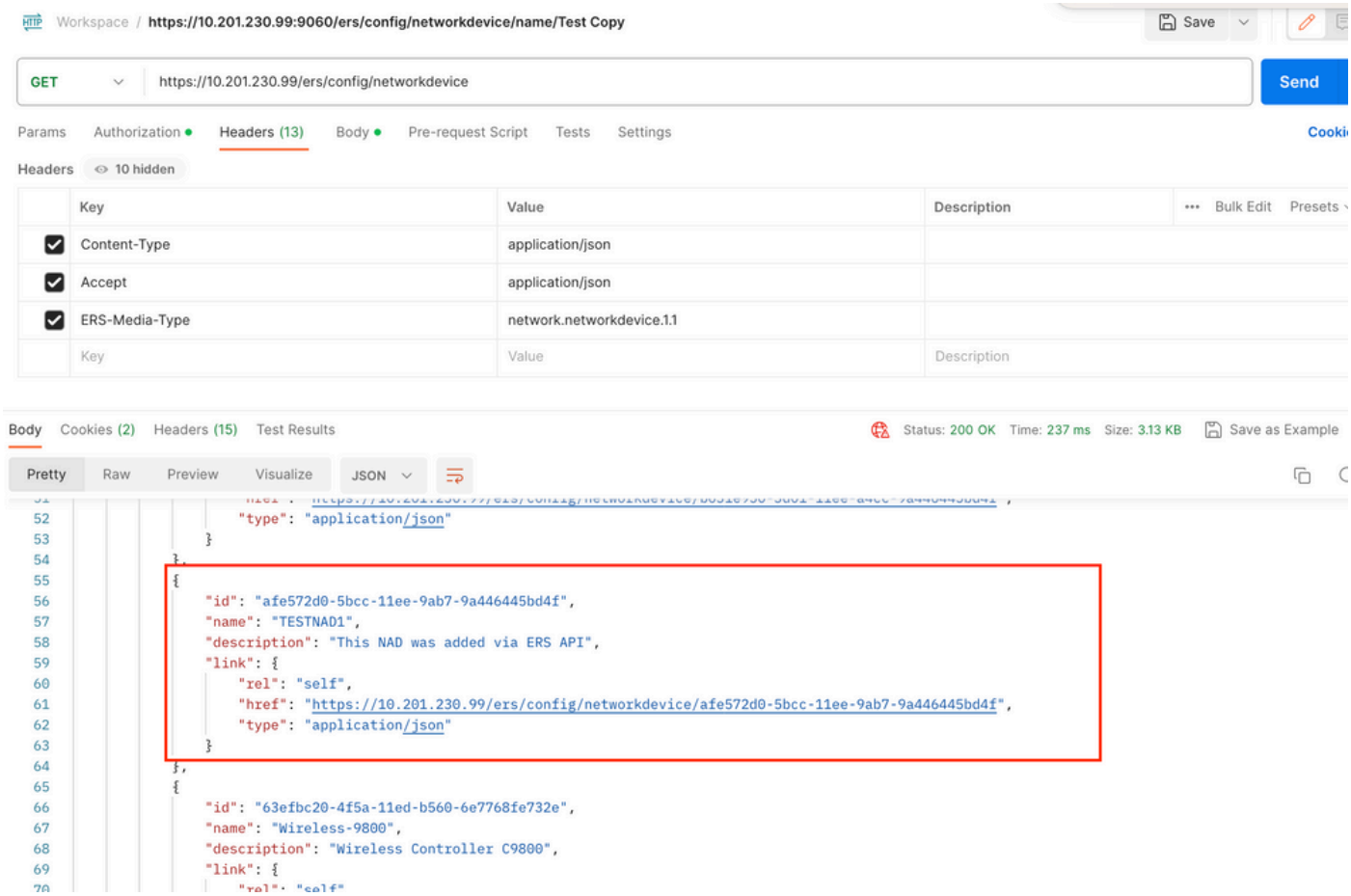
<NetworkDeviceIPList> <NetworkDeviceIP> <ipaddress>**NAD IP Address**</ipaddress> <mask>**32**</mask> </NetworkDeviceIP> </NetworkDeviceIPList> <NetworkDeviceGroupList> <NetworkDeviceGroup>Location#All Locations#**LAB**</NetworkDeviceGroup> <NetworkDeviceGroup>Device Type#All Device Types#**Access-Layer**</NetworkDeviceGroup> </NetworkDeviceGroupList> <profileName>Cisco</profileName> <tacacsSettings> <connectModeOptions>**ON_LEGACY**</connectModeOptions> <sharedSecret>**cisco123**</sharedSecret> </tacacsSettings> </ns0:networkdevice>

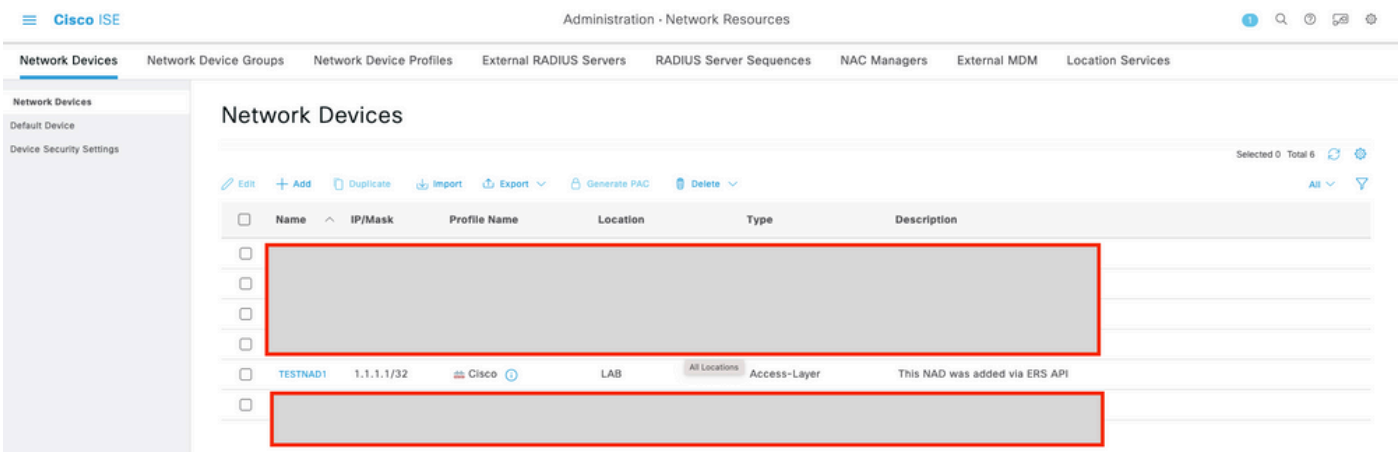
5. Incollare il modello XML per **raw** sotto l'intestazione **Body**.

6. Selezionare **POST** come metodo, incollare **https://{ISE-ip}/ers/config/networkdevice** e fare clic su **Send. Se tutti gli elementi sono stati configurati correttamente, è necessario visualizzare un messaggio 201 Created** (Creato) e il risultato è vuoto.



7. Confermare se il NAD è stato creato eseguendo una chiamata **GET** per il NAD o controllando l'elenco ISE NAD.



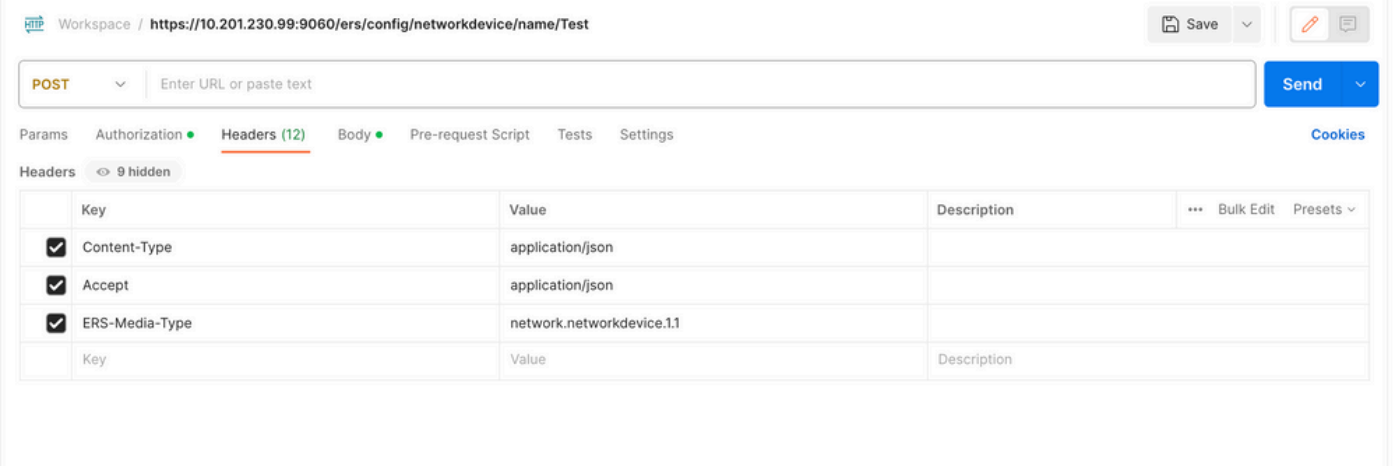


Crea e utilizza JSON

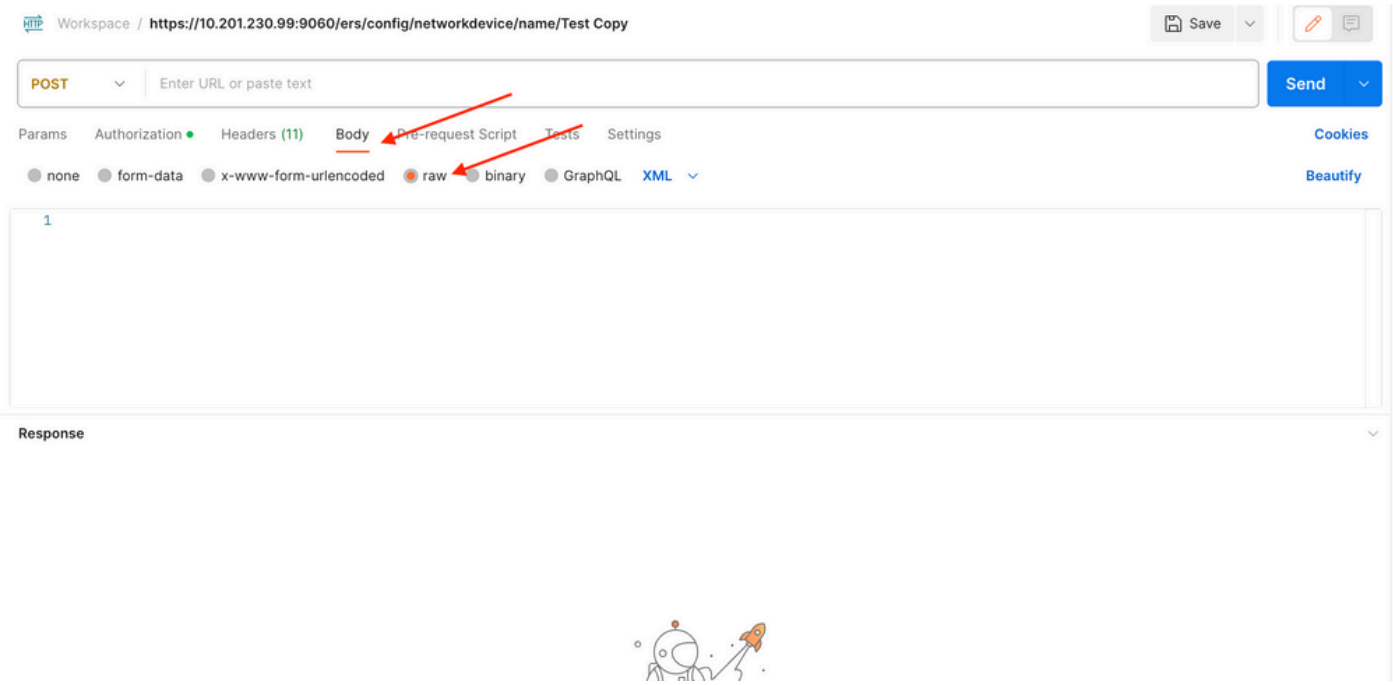
Creare TESTAND2con le impostazioni RADIUS TACACS, SNMP e TrustSec utilizzando JSON.

1. Nell'SDK, in **Crea,** sono presenti le intestazioni e i modelli necessari per eseguire la chiamata, nonché la risposta prevista.

2. Passare alla scheda **Intestazioni** e configurare le intestazioni necessarie per la chiamata API come mostrato nell'SDK. La configurazione dell'intestazione deve essere simile alla seguente:

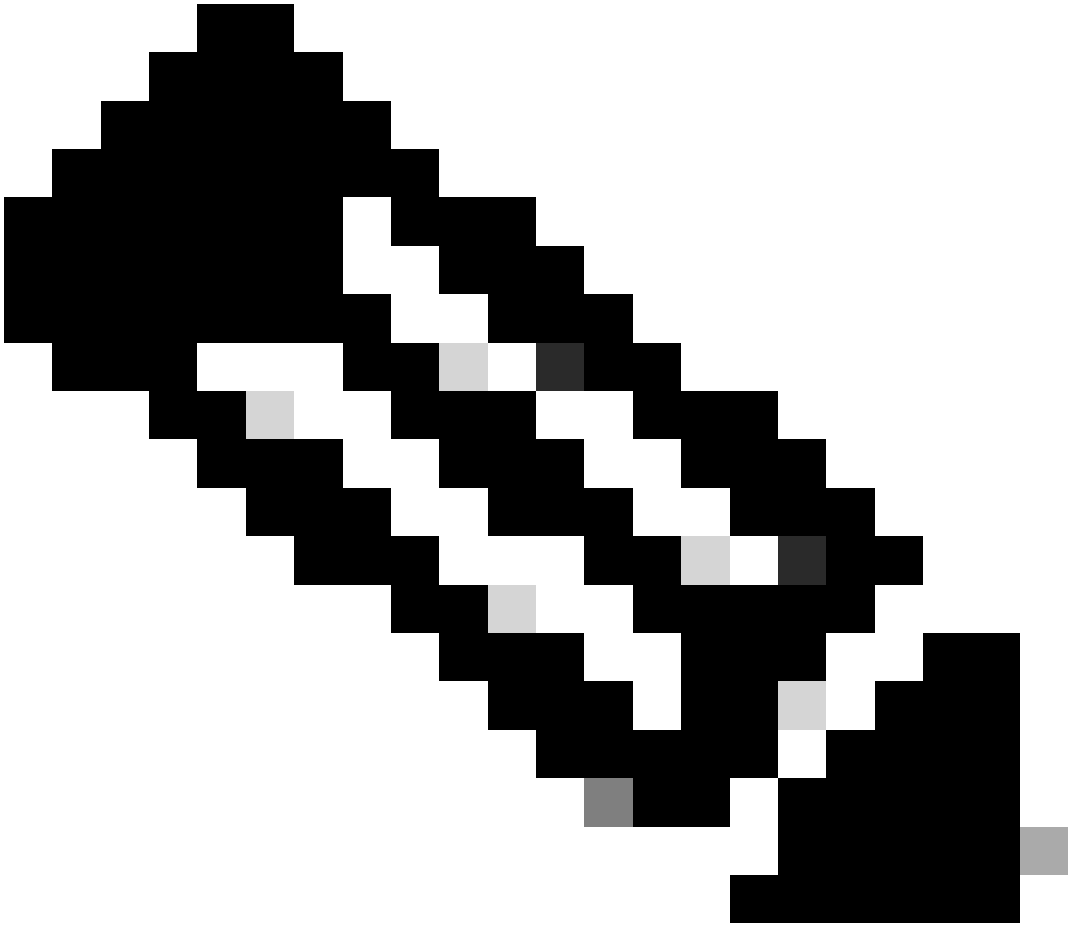


3. Spostarsi sull'intestazione **Body** e selezionare **raw**. In questo modo è possibile incollare il modello JSON necessario per la creazione di NAD.



4. Il modello JSON deve avere il seguente aspetto (modificare i valori in base alle esigenze):

{ "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"] } }

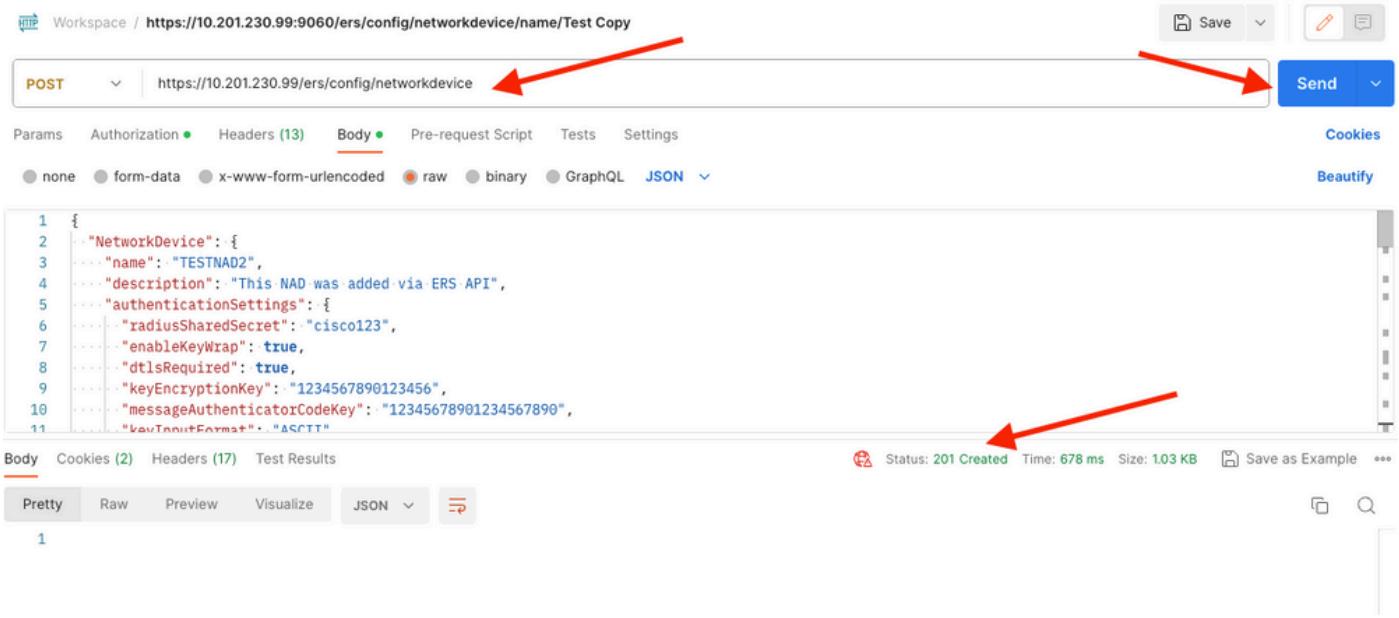


Nota: è importante notare che le righe successive sono obbligatorie solo se **enableKeyWrap":{false|true}**, è impostato su **true**. In caso contrario, è possibile eliminare lo stesso dal modello JSON:

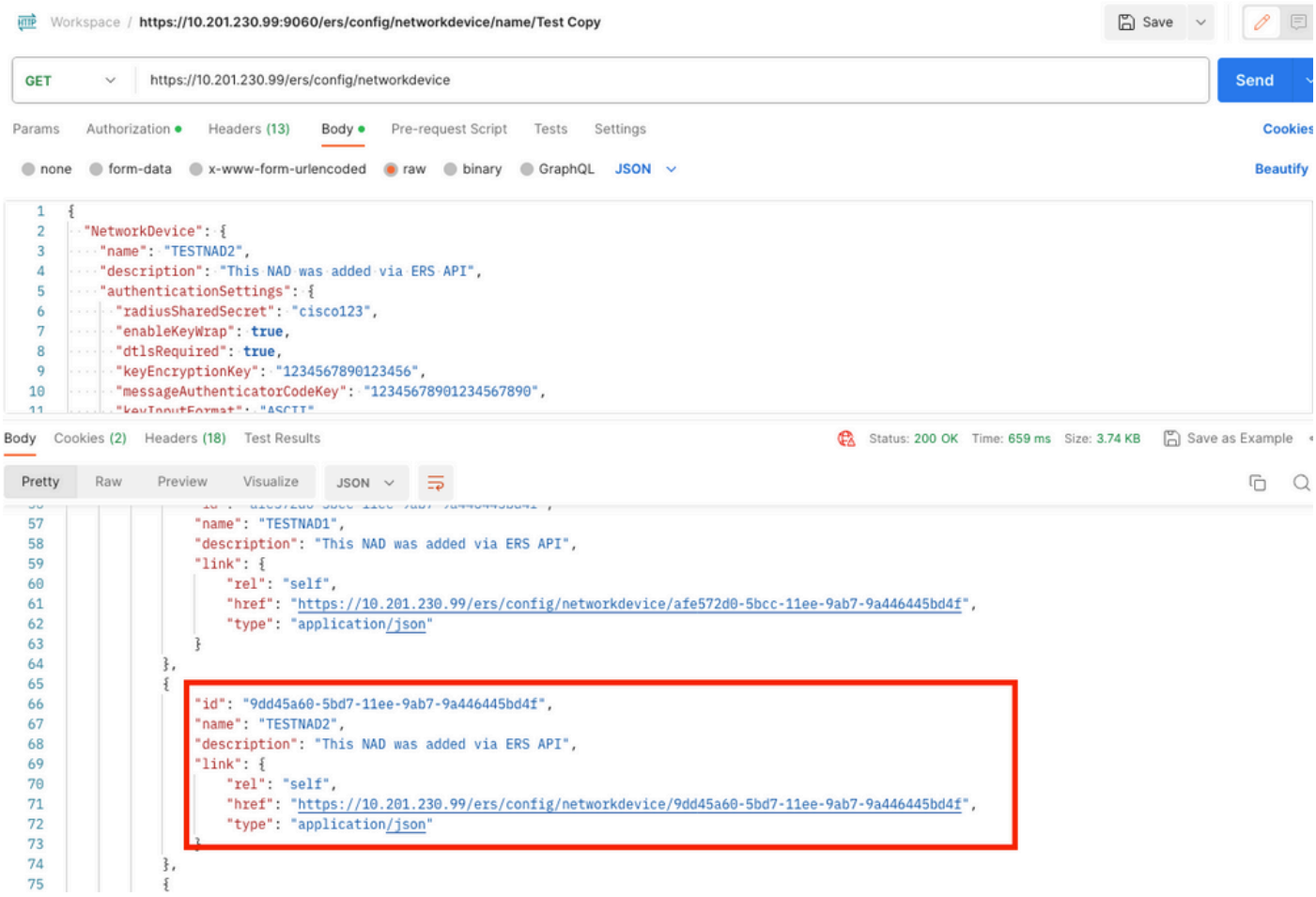
"keyEncryptionKey": "**1234567890123456**", "messageAuthenticatorCodeKey": "**12345678901234567890**", "keyInputFormat": "**ASCII**" È inoltre possibile rimuovere la configurazione non necessaria dal modello e lasciare semplicemente i dati effettivamente necessari da aggiungere durante la creazione del NAD.

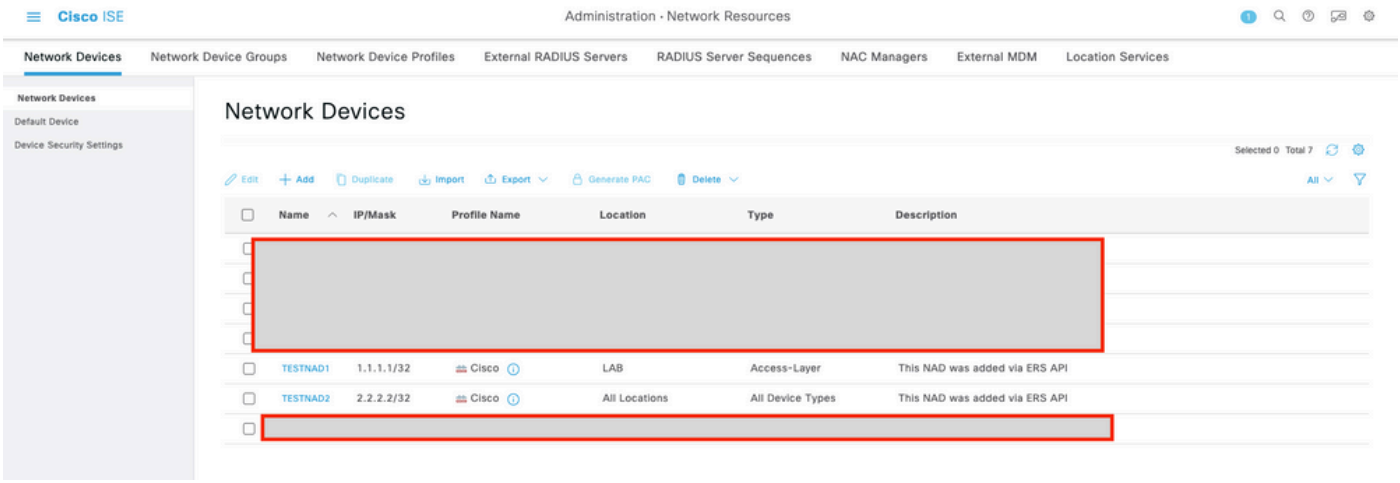
5. Incollare il modello JSON per **raw** sotto l'intestazione **Body**.

6. Selezionare **POST** come metodo, incollare **https://{ISE-ip}/ers/config/networkdevice** e fare clic su **Send.** Se tutti gli elementi sono stati configurati correttamente, è necessario visualizzare un messaggio **201 Created** e il risultato è vuoto.



7. Confermare se il NAD è stato creato eseguendo una chiamata GET per il NAD o controllando l'elenco ISE NAD.





Verifica

Se è possibile accedere alla pagina dell'interfaccia utente del servizio API, ad esempio **https://*{iseip}*:*{port}*/api/swagger-ui/index.html** o **https://*{iseip}*:9060/ers/sdk**, significa che il servizio API funziona come previsto.

Risoluzione dei problemi

- Tutte le operazioni REST vengono controllate e i log vengono registrati nei log di sistema.
- Per risolvere i problemi relativi alle API aperte, impostare il **livello di log** per il componente **apiservice** su **DEBUG** nella finestra **Configurazione log di debug**.
- Per risolvere i problemi relativi alle API ERS, impostare il **livello di log** per il componente **ers** su **DEBUG** nella finestra **Configurazione log di debug**. Per visualizzare questa finestra, passare all'interfaccia grafica di Cisco ISE, fare clic sull'icona Menu e scegliere **Operazioni > Risoluzione dei problemi > Debug guidato > Debug Log Configuration**.
- È possibile scaricare i log dalla finestra **Scarica** log. Per visualizzare questa finestra, passare all'interfaccia utente di Cisco ISE, fare clic sull'icona **Menu** e scegliere **Operazioni > Risoluzione dei problemi > Log di download**.
- È possibile scegliere di scaricare un bundle di supporto dalla scheda Support Bundle facendo clic sul pulsante **Download** nella scheda, oppure scaricare i log di debug **api-service** dalla scheda **Debug Logs** facendo clic sul **valore Log File** per il log di debug api-service.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).