Erstellen von ISE-Netzwerkgeräten mit ERS API

Inhalt

Einleitung

In diesem Dokument wird der Prozess zum Erstellen von Netzwerkzugriffsgeräten (Network Access Devices, NADs) auf der ISE über die ERS-API mit PostMan als REST-Client beschrieben.

Voraussetzungen

Anforderungen

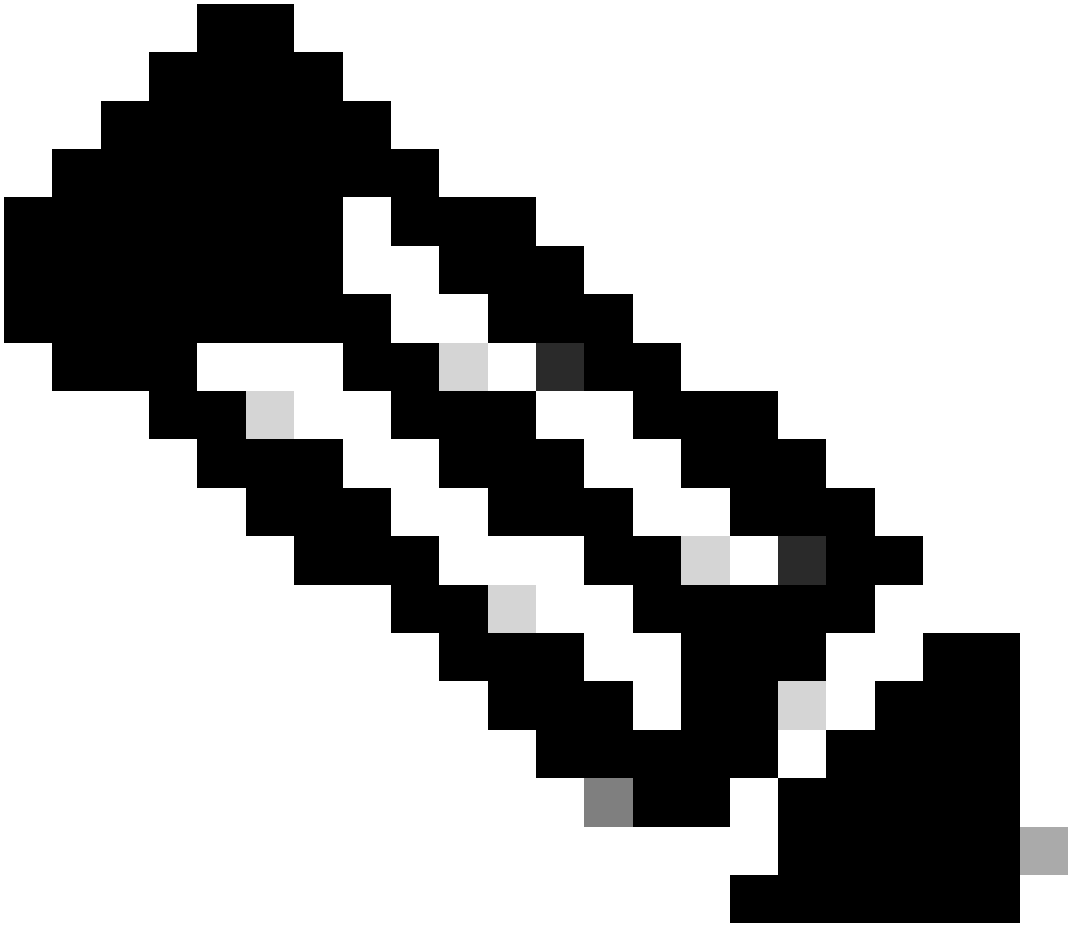
Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ISE (Identity Services Engine)
- ERS (externe RESTful-Services)
- REST-Clients wie Postman, RESTED, Insomnia usw.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

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



Hinweis: Das Verfahren ist für andere ISE-Versionen und REST-Clients ähnlich oder identisch. Sofern nicht anders angegeben, können Sie diese Schritte für alle ISE-Softwareversionen der Versionen 2.x und 3.x ausführen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

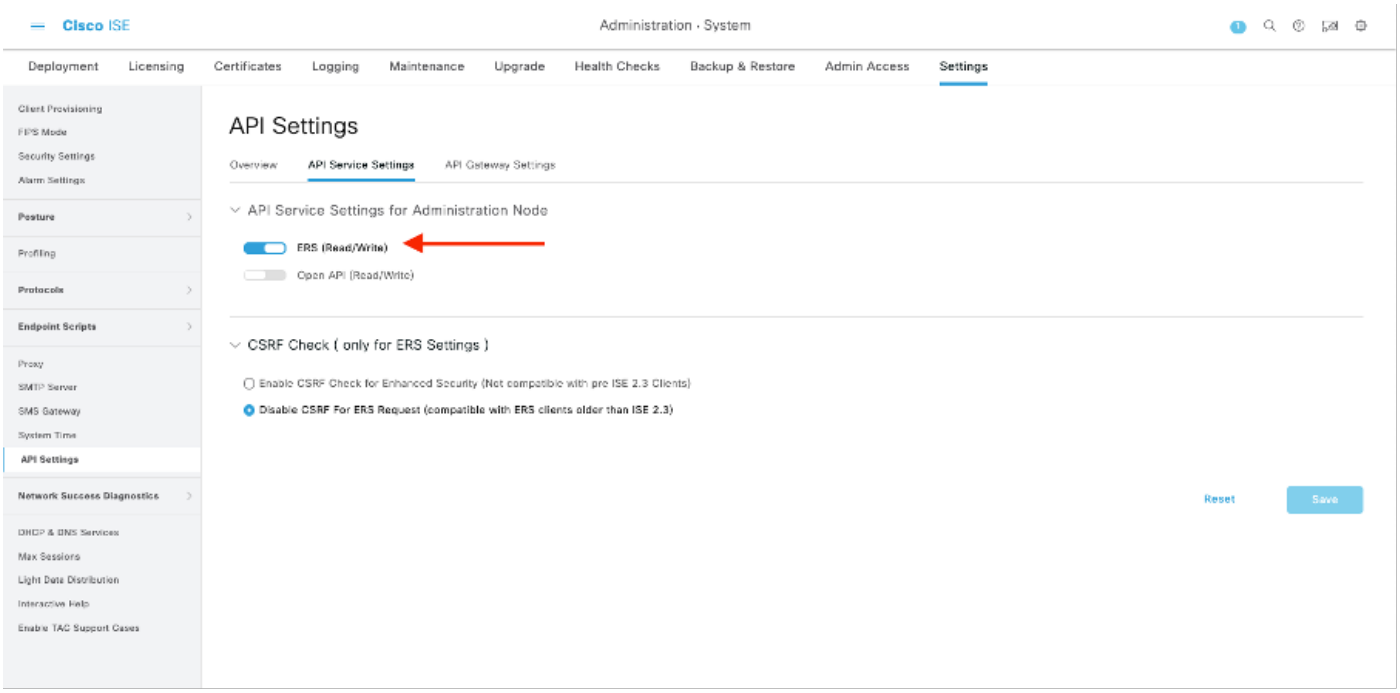
Konfigurieren

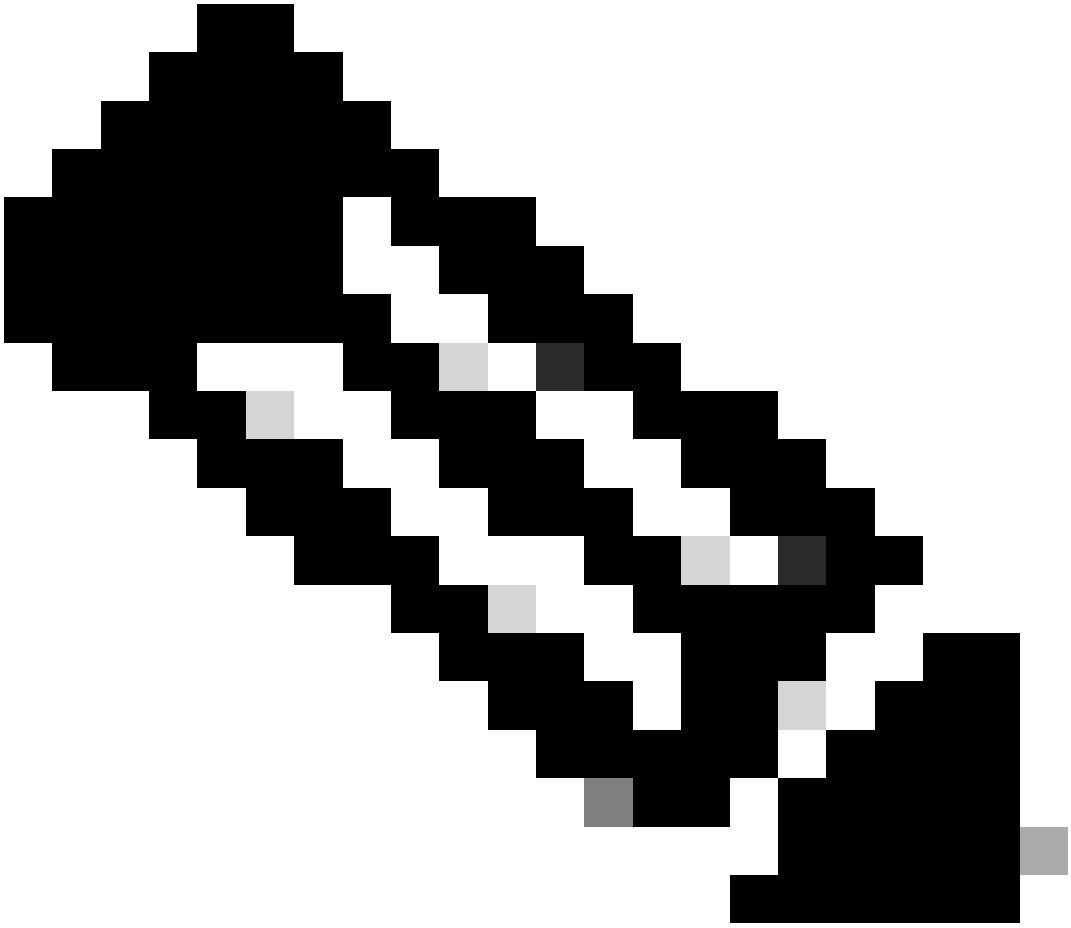
ERS aktivieren (Port 9060)

ERS-APIs sind reine HTTPS-REST-APIs, die über Port 443 und Port 9060 betrieben werden. Port 9060 ist standardmäßig geschlossen, daher muss er zuerst geöffnet werden. Wenn Clients, die versuchen, auf diesen Port zuzugreifen, ERS nicht zuerst aktivieren, wird eine Zeitüberschreitung

vom Server angezeigt. Daher muss ERS zuerst über die Cisco ISE-Administrations-Benutzeroberfläche aktiviert werden.

Navigieren Sie zu Administration > Settings > API Settings, und aktivieren Sie die Umschaltfläche ERS (Read/Write).

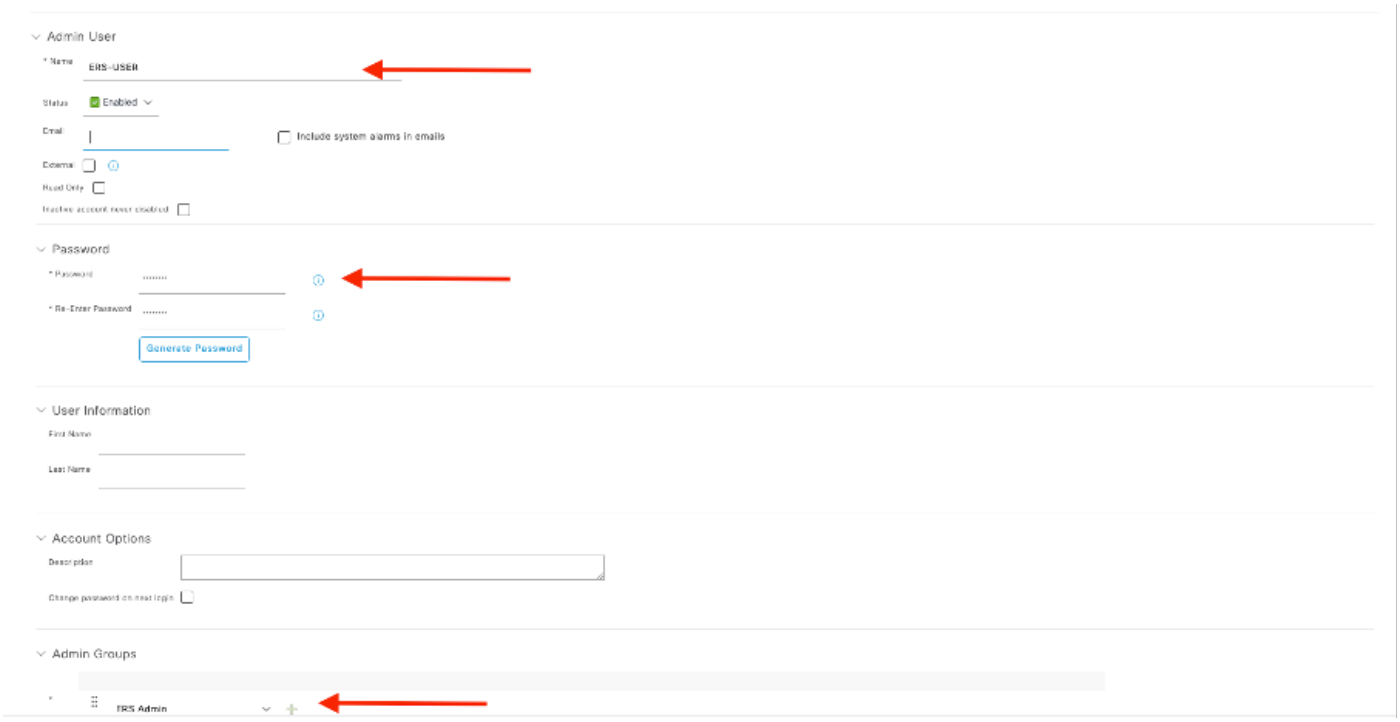




Hinweis: Die ERS-APIs unterstützen TLS 1.1 und TLS 1.2. ERS-APIs unterstützen TLS 1.0 nicht, unabhängig davon, ob TLS 1.0 im Fenster Sicherheitseinstellungen der Cisco ISE-GUI aktiviert wurde (Administration > System > Settings > Security Settings). Die Aktivierung von TLS 1.0 im Fenster "Security Settings" (Sicherheitseinstellungen) bezieht sich nur auf das EAP-Protokoll und hat keine Auswirkungen auf ERS APIs.

ERS-Administrator erstellen

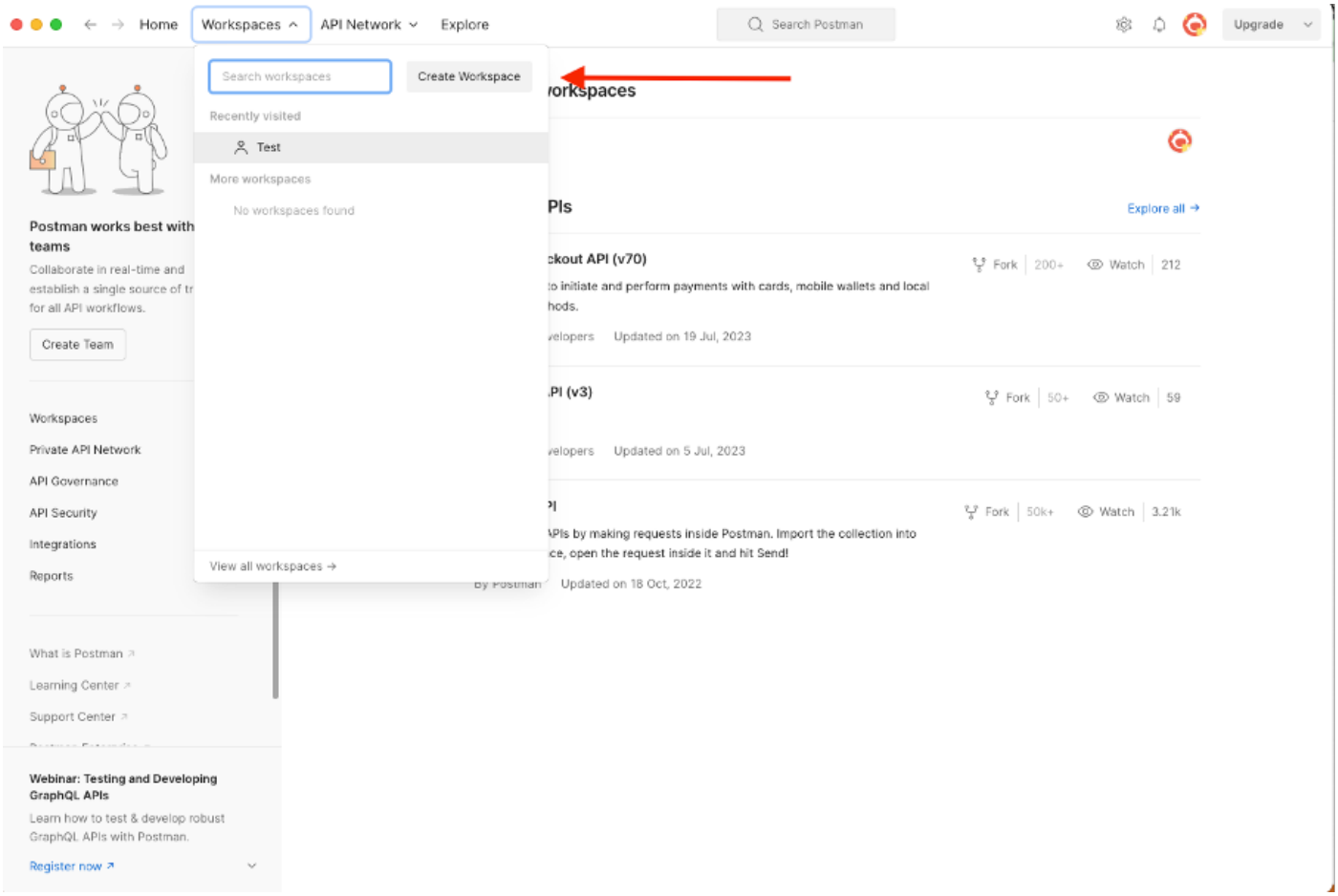
Erstellen Sie einen Cisco ISE-Administrator, weisen Sie ein Kennwort zu, und fügen Sie den Benutzer als ERS-Administrator zur Admin-Gruppe hinzu. Sie können den Rest der Konfiguration leer lassen.



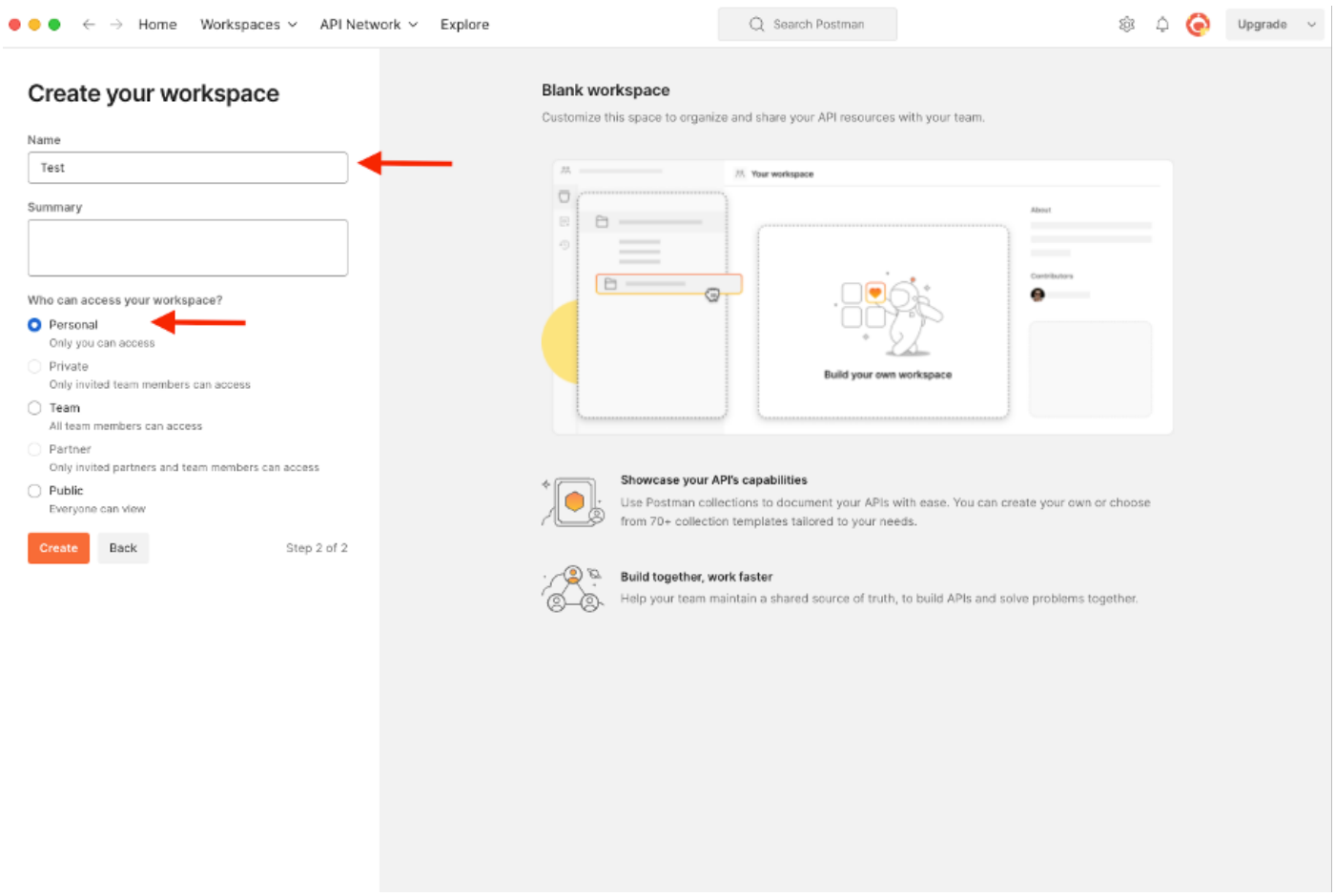
Postbote einrichten

Laden Sie die Online-Version von Postman herunter oder verwenden Sie sie.

1. Erstellen Sie einen Benutzer, und erstellen Sie einen Arbeitsbereich, indem Sie auf der Registerkarte Arbeitsbereiche auf Arbeitsbereich erstellen klicken.



2. Wählen Sie Leerer Arbeitsbereich und weisen Sie dem Arbeitsbereich einen Namen zu. Sie können eine Beschreibung hinzufügen und veröffentlichen. Für dieses Beispiel ist Personalis ausgewählt.

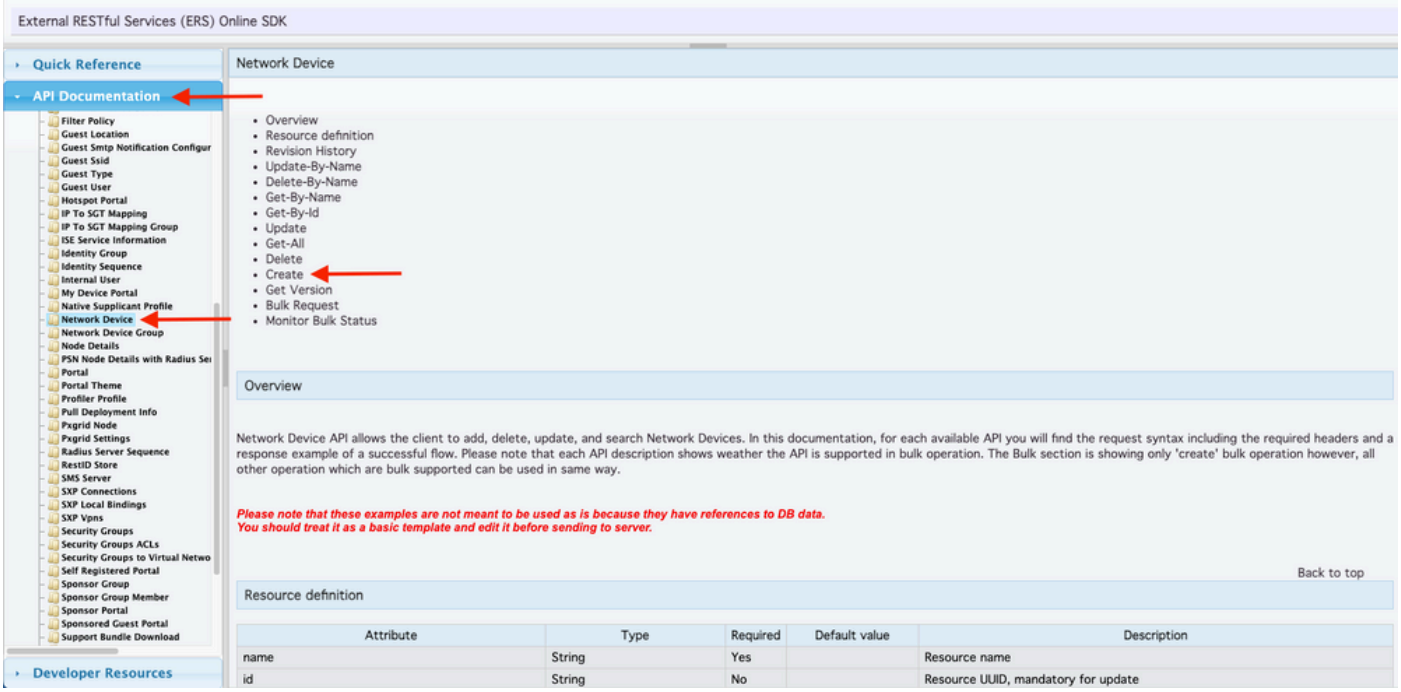


Nachdem Sie den Arbeitsbereich erstellt haben, können Sie API-Aufrufe konfigurieren.

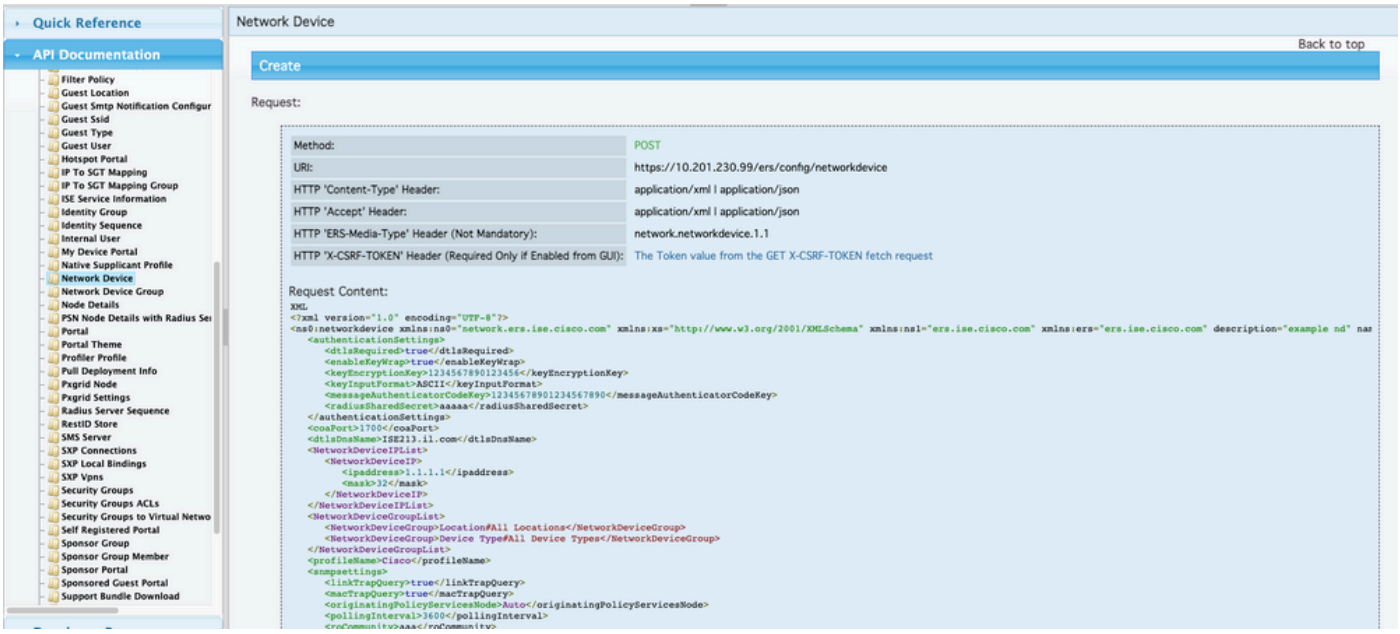
ISE SDK und grundlegende Postman-Autorisierung

Um einen Anruf zu konfigurieren, greifen Sie zunächst auf das ISE ERS SDK (Software Developer Kit) zu. Dieses Tool erstellt die gesamte Liste der API-Aufrufe, die die ISE ausführen kann:

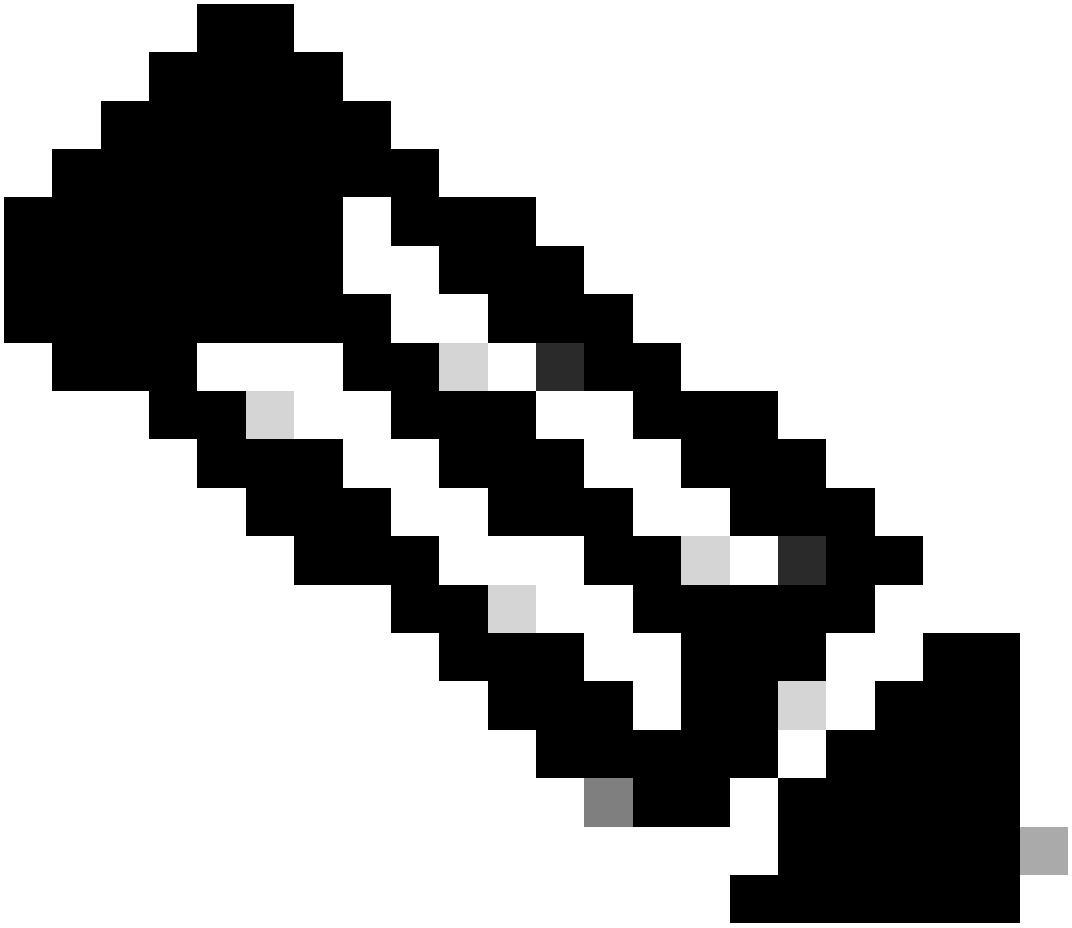
1. Navigieren Sie zu https://{ise-ip}/ers/sdk.
2. Melden Sie sich mit Ihren ISE-Administratorrechten an.
3. Erweitern Sie die API-Dokumentation.
4. Blättern Sie nach unten, bis Sie Netzwerkgerät gefunden haben, und klicken Sie darauf.
5. Unter dieser Option finden Sie jetzt alle verfügbaren Vorgänge, die Sie für Netzwerkgeräte auf der ISE ausführen können. Wählen Sie Erstellen aus.



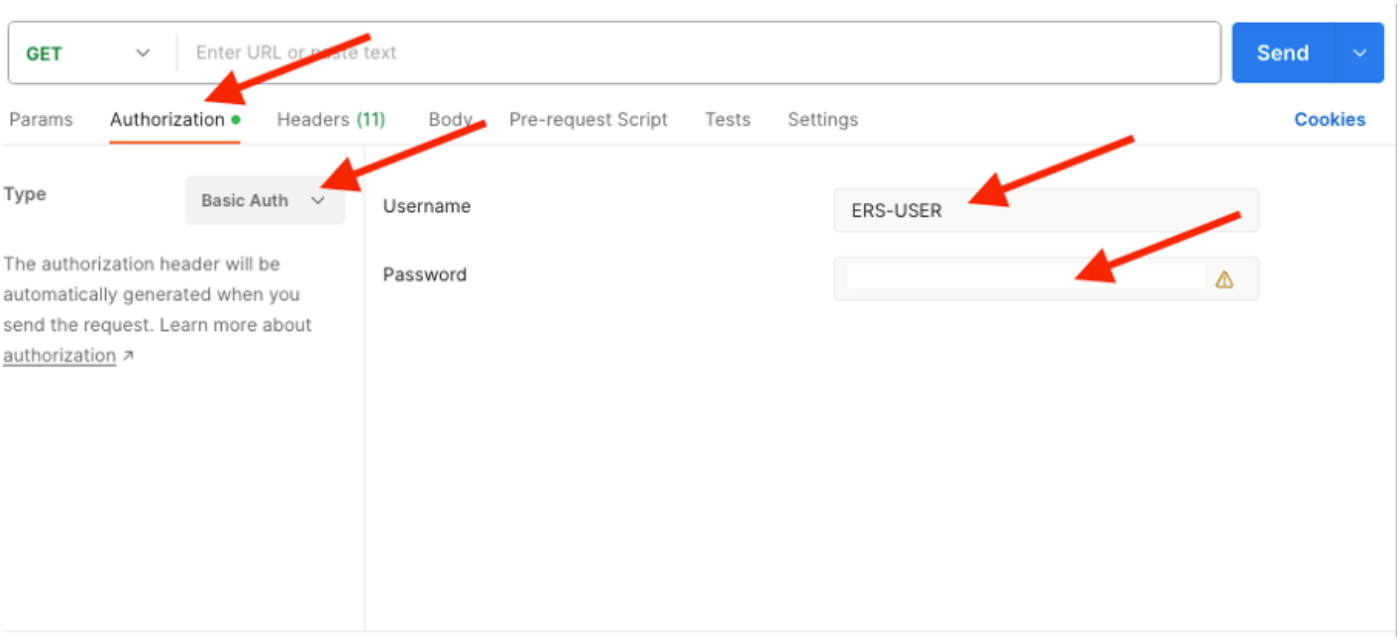
6. Sie können nun die erforderliche Konfiguration zum Durchführen des API-Aufrufs mit XML oder JSON auf einem beliebigen REST-Client sowie ein erwartetes Antwortbeispiel sehen.



7. Zurück zu Postman konfigurieren Sie die grundlegende Authentifizierung zu ISE. Wählen Sie auf der Registerkarte Autorisierung die Option Einfache Authentifizierung als Authentifizierungstyp aus, und fügen Sie die zuvor auf der ISE erstellten ISE ERS-Benutzeranmeldeinformationen hinzu.



Hinweis: Das Passwort wird als Klartext angezeigt, es sei denn, es wurden Variablen für Postman konfiguriert.

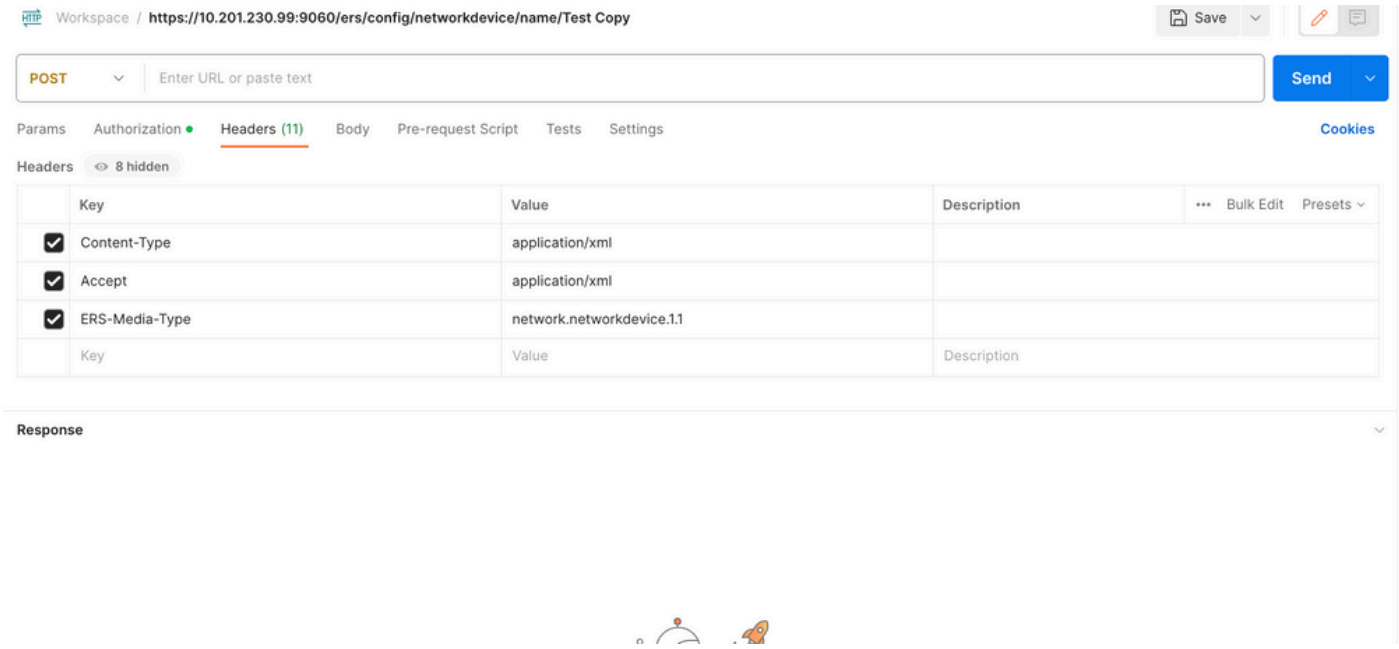


Erstellen von NAD mithilfe von XML

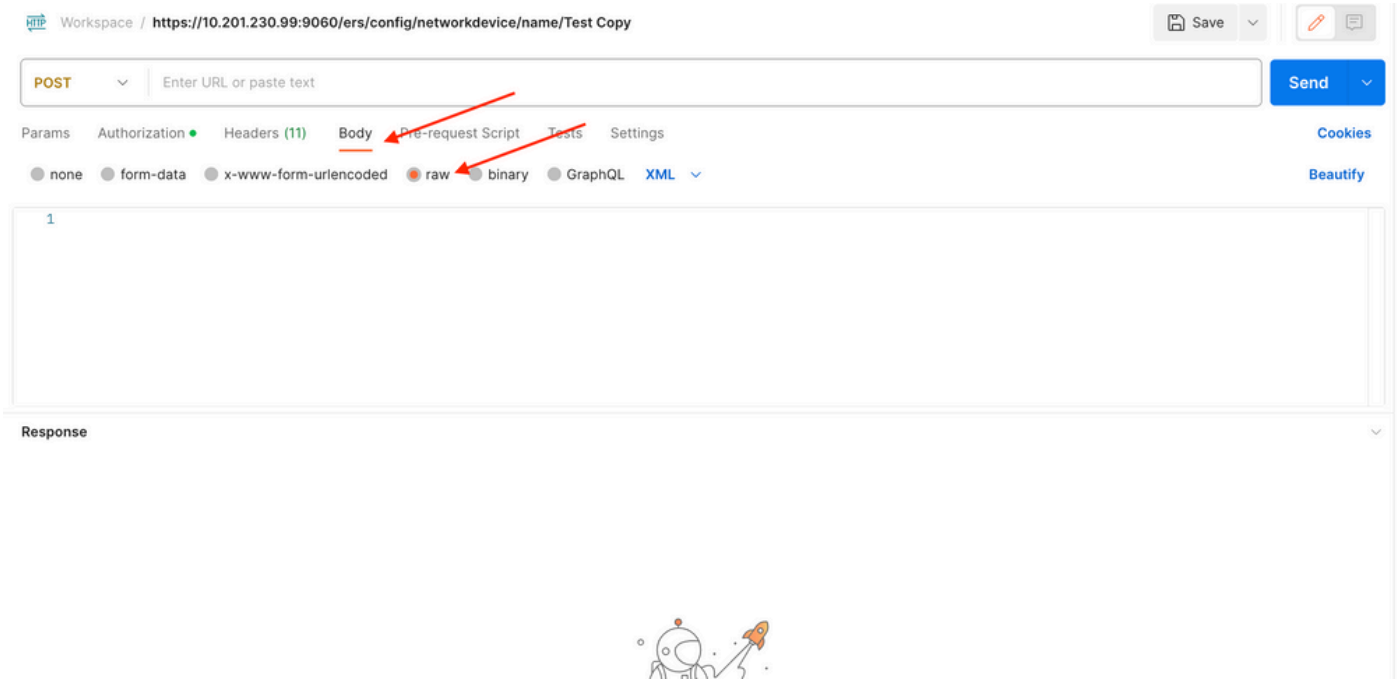
Erstellen Sie TESTNAD1 mit RADIUS TACACS-, SNMP- und TrustSec-Einstellungen unter Verwendung von XML.

1. Auf dem SDK befinden sich unter Erstellen die Header und Vorlagen, die für den Anruf sowie die erwartete Antwort erforderlich sind.

2. Wechseln Sie zur Registerkarte Headers, und konfigurieren Sie die erforderlichen Header für den API-Aufruf, wie im SDK dargestellt. Die Header-Konfiguration muss wie folgt aussehen:

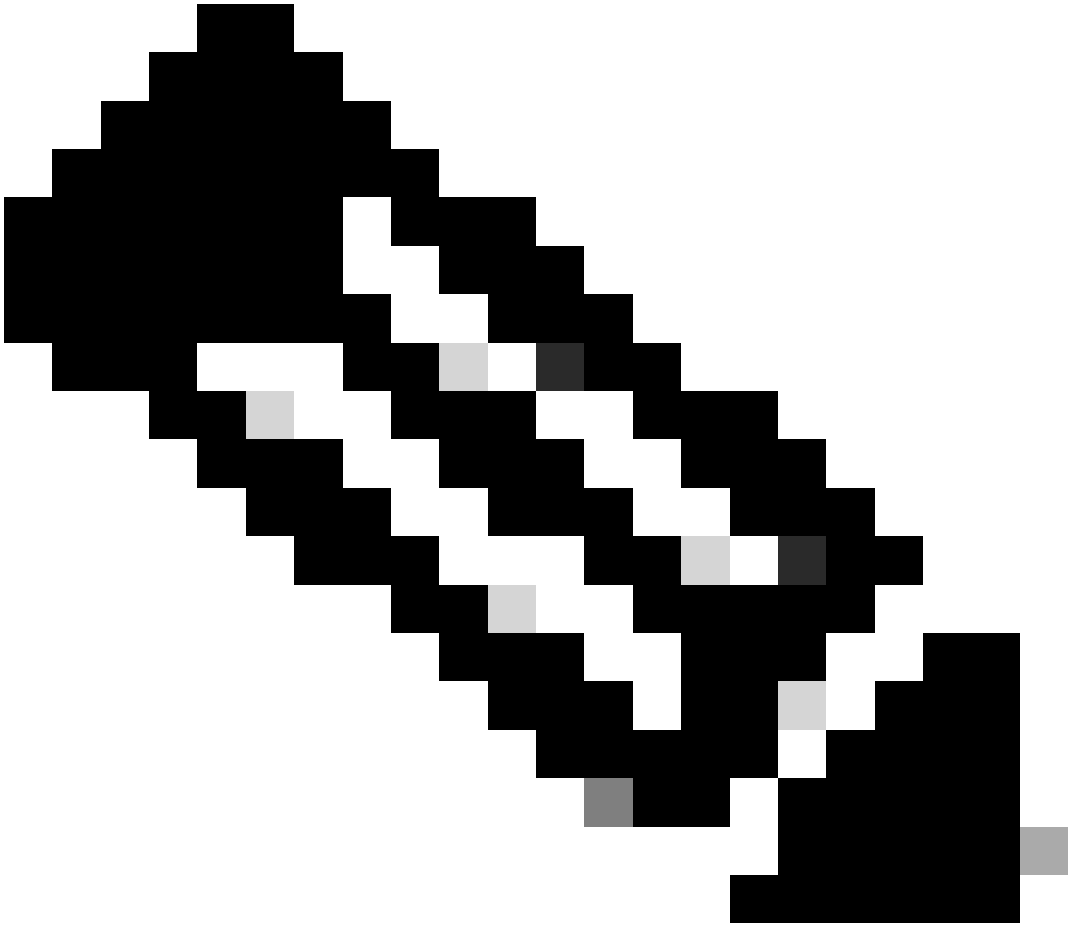


3. Navigieren Sie zur Kopfzeile des Hauptteils, und wählen Sie unformatiert aus. Auf diese Weise können Sie die XML-Vorlage einfügen, die zum Erstellen der NAD erforderlich ist.



4. Die XML-Vorlage sieht wie folgt aus (ändern Sie die Werte nach Bedarf):

<?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>



Hinweis: Beachten Sie, dass die nächsten Zeilen nur erforderlich sind, wenn **<enableKeyWrap>{false|true}</enableKeyWrap>** auf **true** festgelegt ist. Andernfalls kann dasselbe aus der XML-Vorlage gelöscht werden:

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

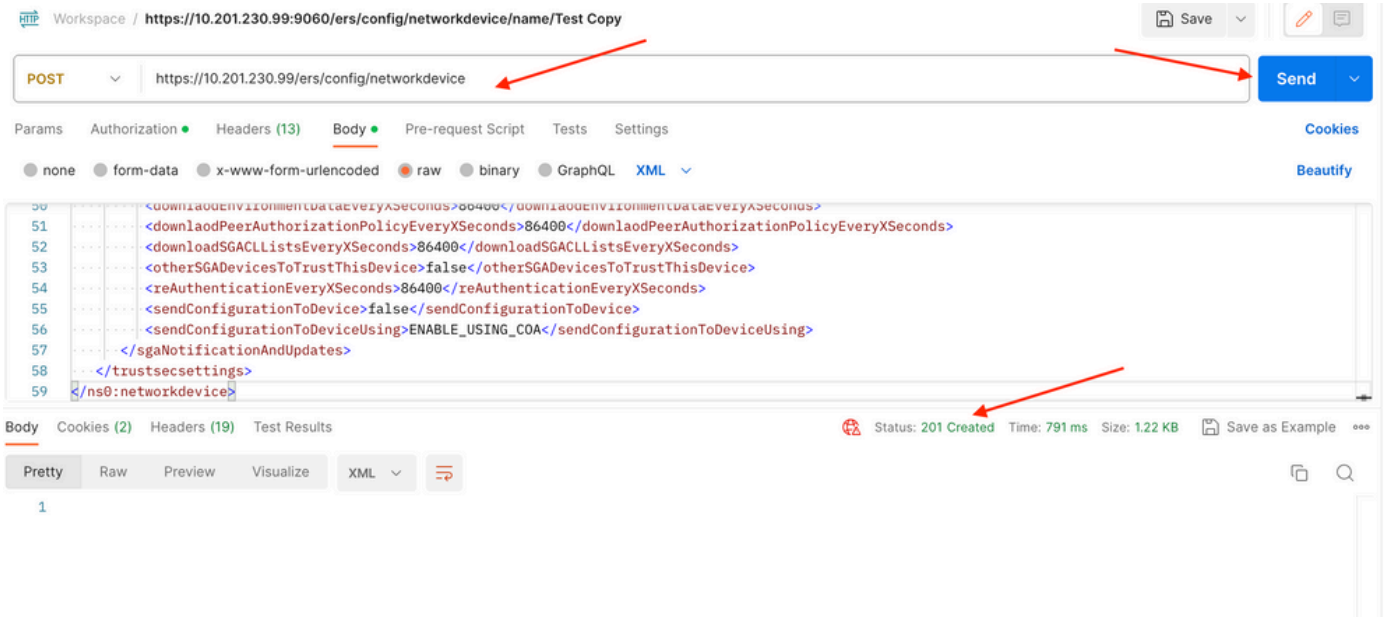
Sie können die Konfiguration, die Sie nicht benötigen, aus der Vorlage entfernen und die Daten, die Sie tatsächlich während der Erstellung der NAD hinzufügen müssen, belassen. Als Beispiel wird hier dieselbe Vorlage verwendet, jedoch nur für die TACACS-Konfiguration. Stellen Sie unabhängig von der erforderlichen Konfiguration sicher, dass die Vorlage mit **</ns0:network**device**> endet.**

<?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**">

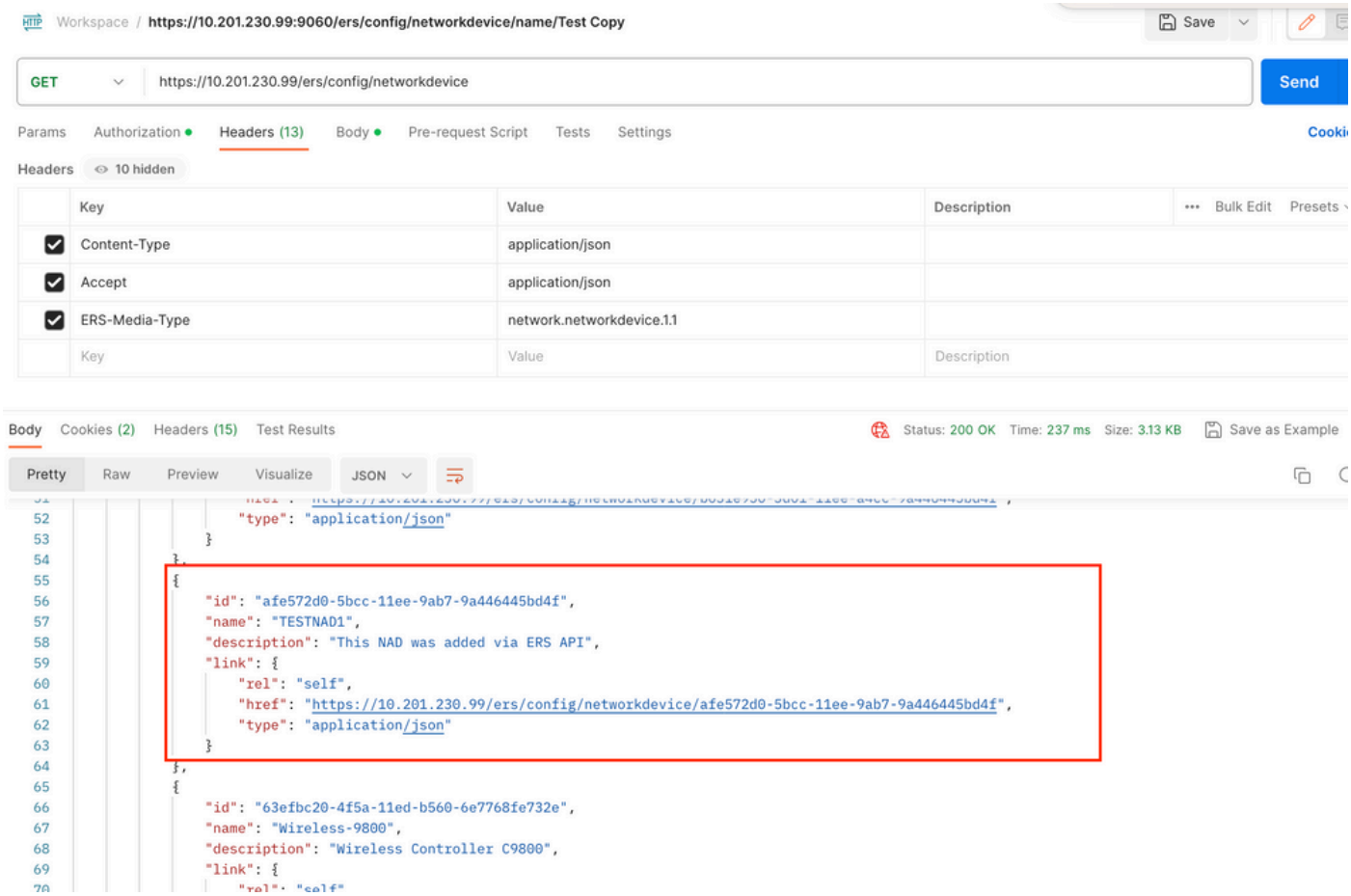
<NetworkDeviceIPList> <NetworkDeviceIP> <ipaddress>**NAD IP Address**</ipaddress> <mask>**32**</mask> </NetworkDeviceIP> </NetworkDeviceIPList> <NetworkDeviceGroupList> <NetworkDeviceGroup>Location#All Locations#**LAB**</NetworkDeviceGroup> <NetworkDeviceGroup>Device Type#All Device Types#**Access-Layer**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

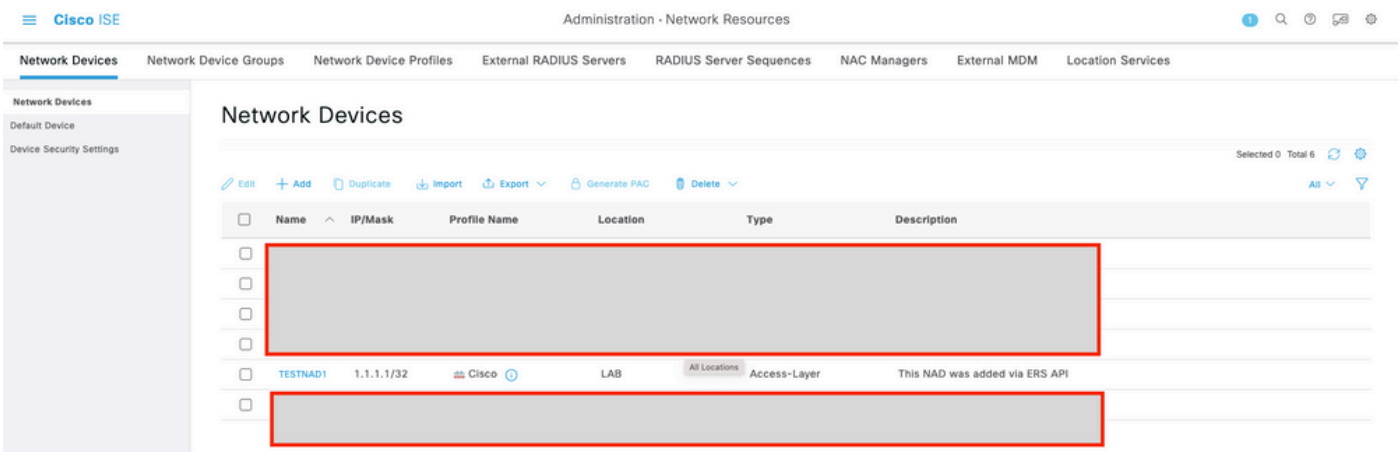
5. Fügen Sie die XML-Vorlage für **raw** unter den **Body**-Header ein.

6. Wählen Sie **POST** als Methode, fügen Sie **https://{ISE-ip}/ers/config/network-device ein,** und klicken Sie auf **Senden.** Wenn alles korrekt konfiguriert wurde, müssen Sie eine Meldung **201 Erstellt** sehen und das Ergebnis leer lassen.



7. Bestätigen Sie, ob die NAD erstellt wurde, indem Sie einen **GET**-Aufruf für die NAD durchführen oder die ISE-NAD-Liste überprüfen.



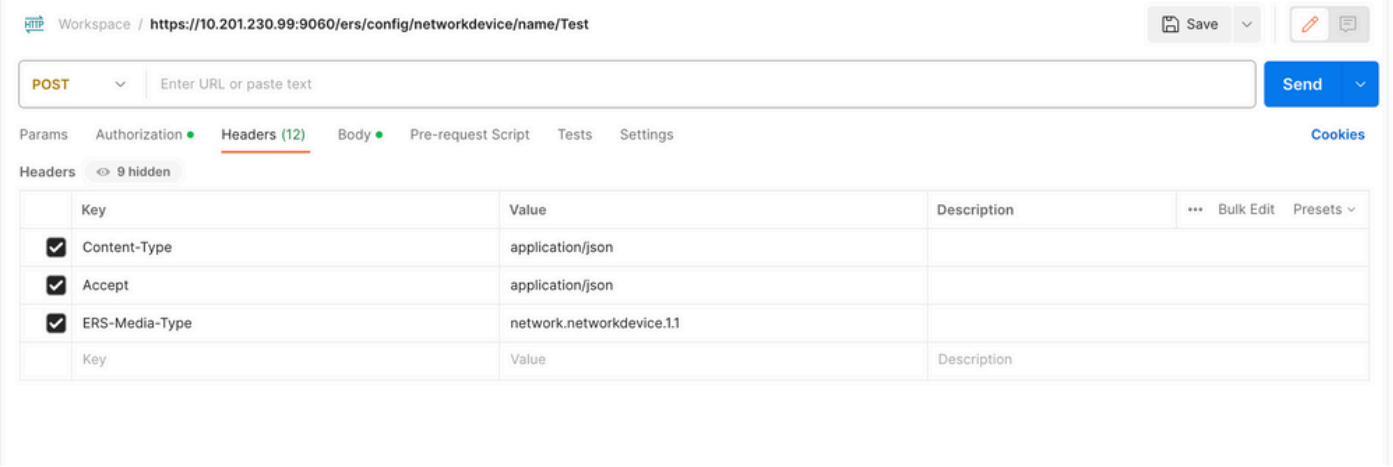


Erstellen von NAD mithilfe von JSON

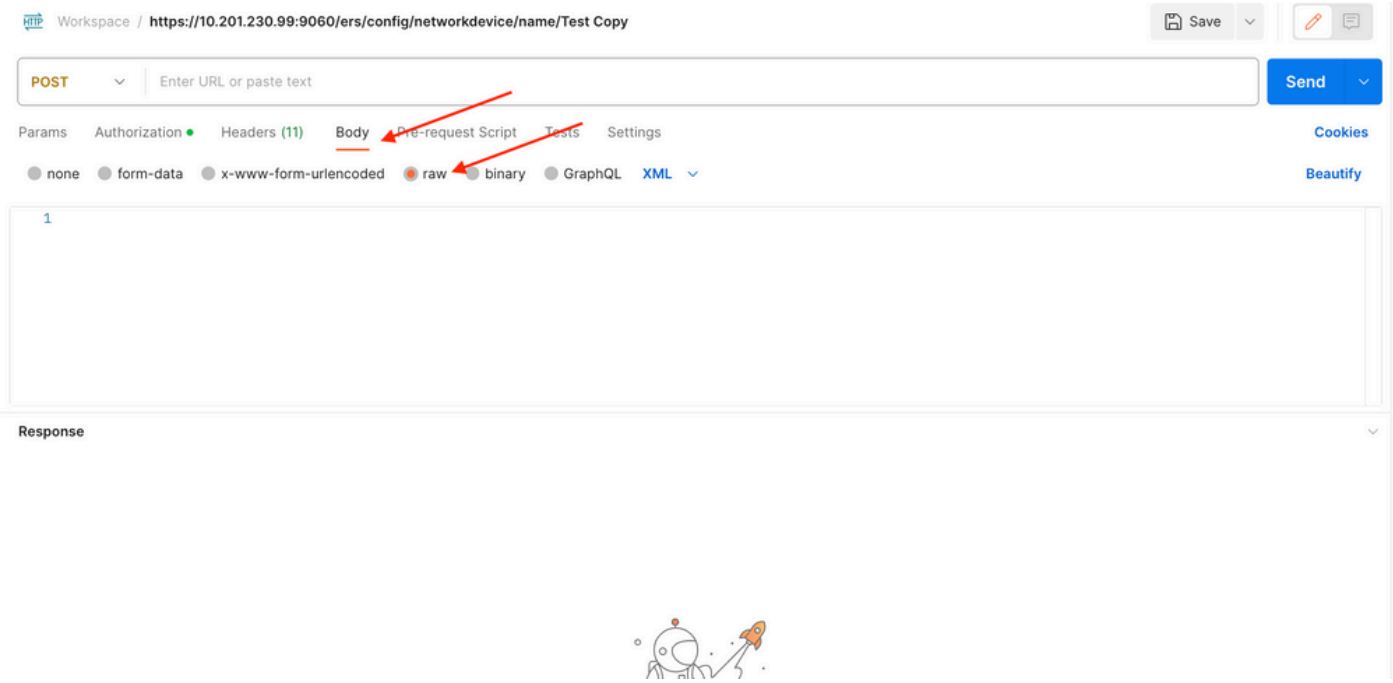
Erstellen Sie TESTNAD2mit RADIUS TACACS-, SNMP- und TrustSec-Einstellungen mit JSON.

1. Auf dem SDK befinden sich unter **Erstellen** die Header und Vorlagen, die für den Anruf sowie die erwartete Antwort erforderlich sind.

2. Wechseln Sie zur Registerkarte **Headers**, und konfigurieren Sie die erforderlichen Header für den API-Aufruf, wie im SDK dargestellt. Die Header-Konfiguration muss wie folgt aussehen:

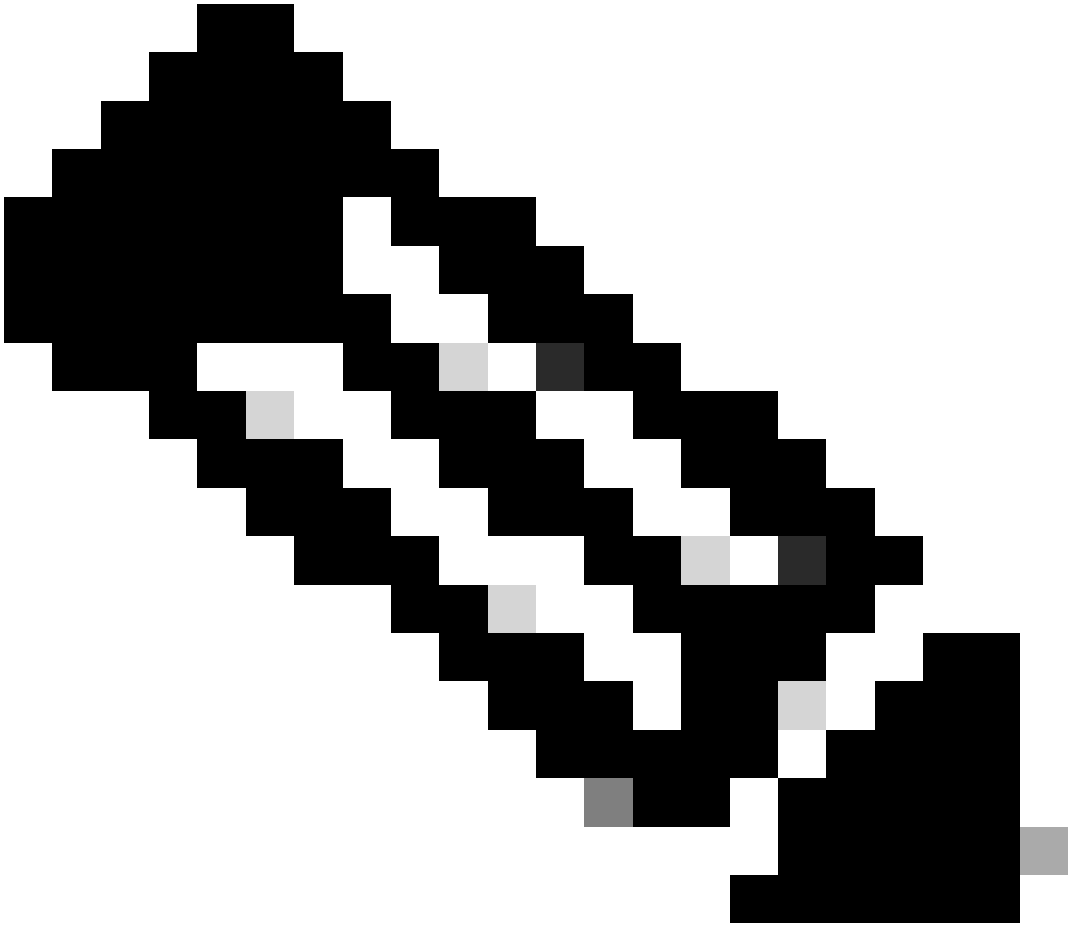


3. Navigieren Sie zur Kopfzeile des **Hauptteils**, und wählen Sie **unformatiert** aus. Auf diese Weise können Sie die JSON-Vorlage einfügen, die zum Erstellen der NAD erforderlich ist.



4. Die JSON-Vorlage muss wie folgt aussehen (ändern Sie die Werte nach Bedarf):

{ "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"] } }

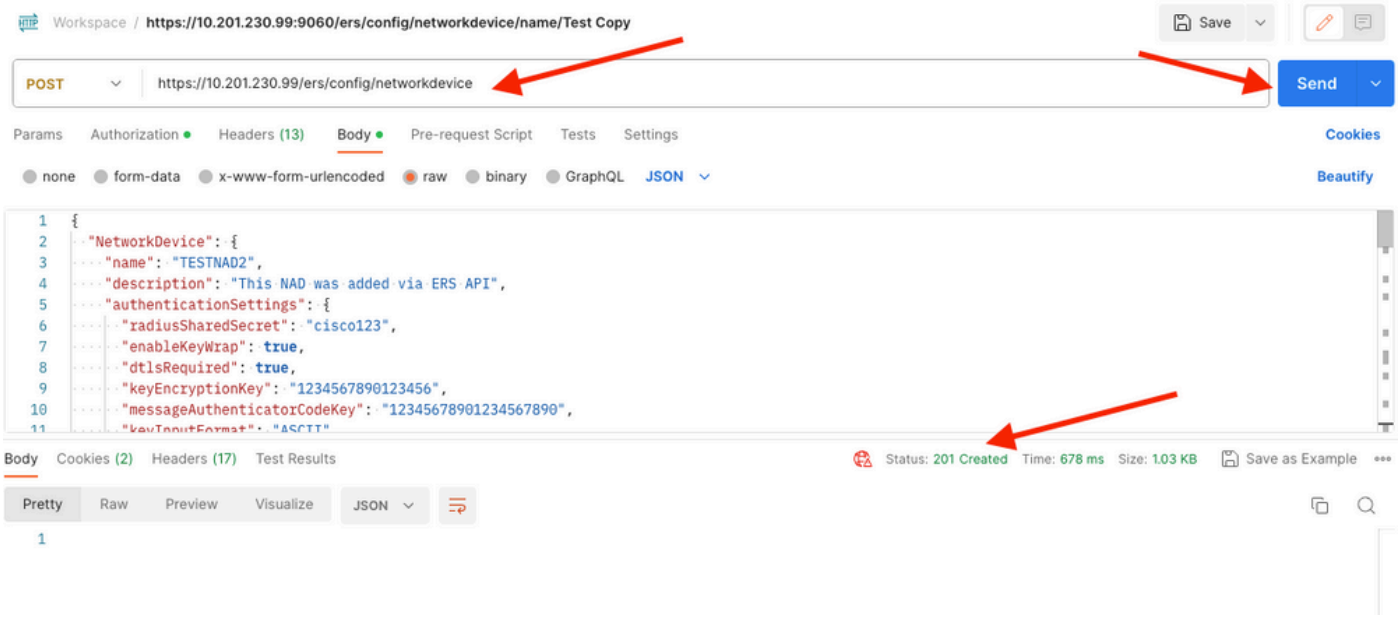


Hinweis: Beachten Sie, dass die nächsten Zeilen nur erforderlich sind, wenn "**enableKeyWrap":{false|true}** auf "**true**" festgelegt ist. Andernfalls kann dasselbe aus der JSON-Vorlage gelöscht werden:

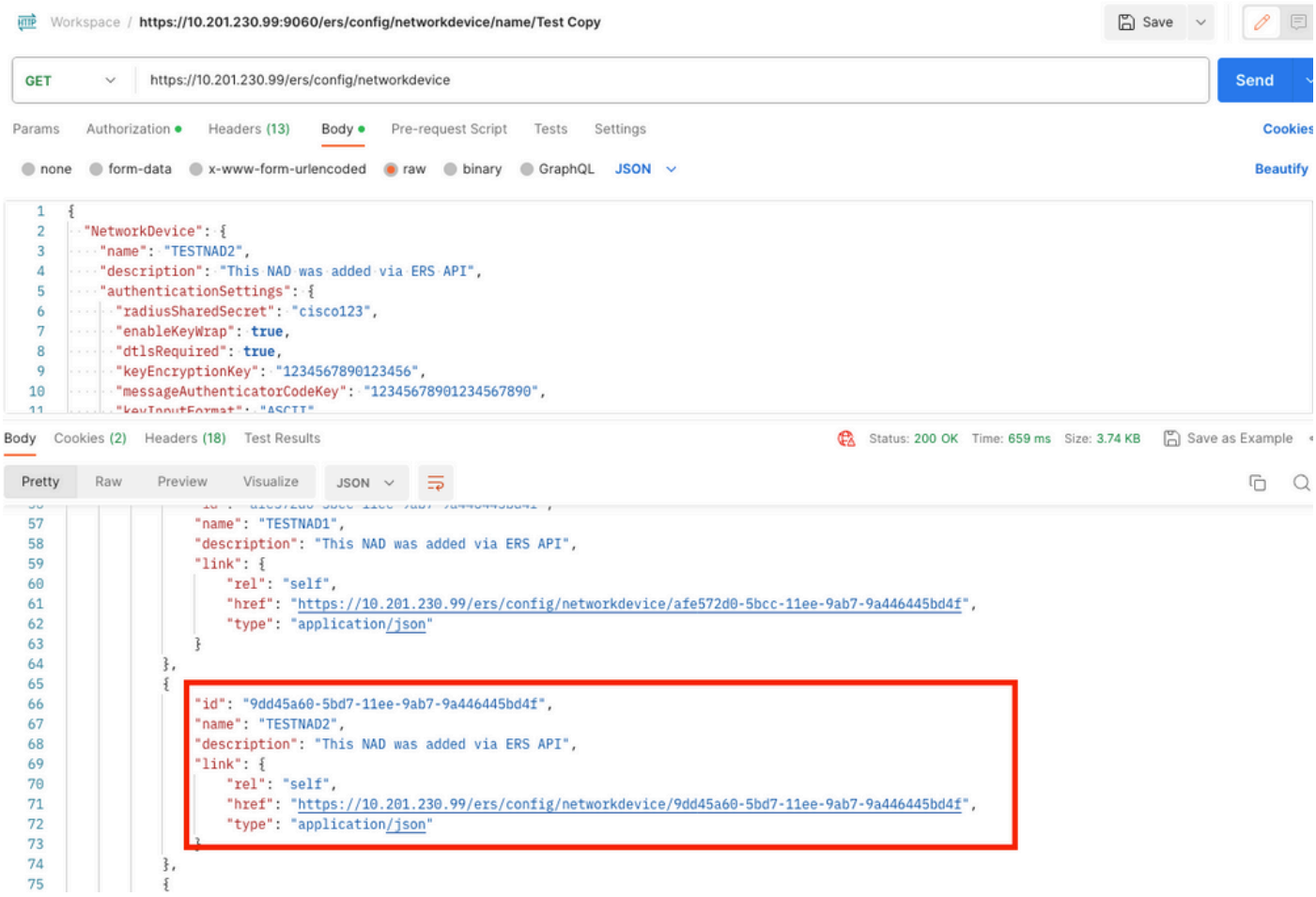
"keyEncryptionKey": "**1234567890123456**", "messageAuthenticatorCodeKey": "**12345678901234567890**", "keyInputFormat": "**ASCII**" Sie können auch die Konfiguration, die Sie nicht benötigen, aus der Vorlage entfernen und die Daten, die Sie tatsächlich während der Erstellung der NAD hinzufügen müssen, belassen.

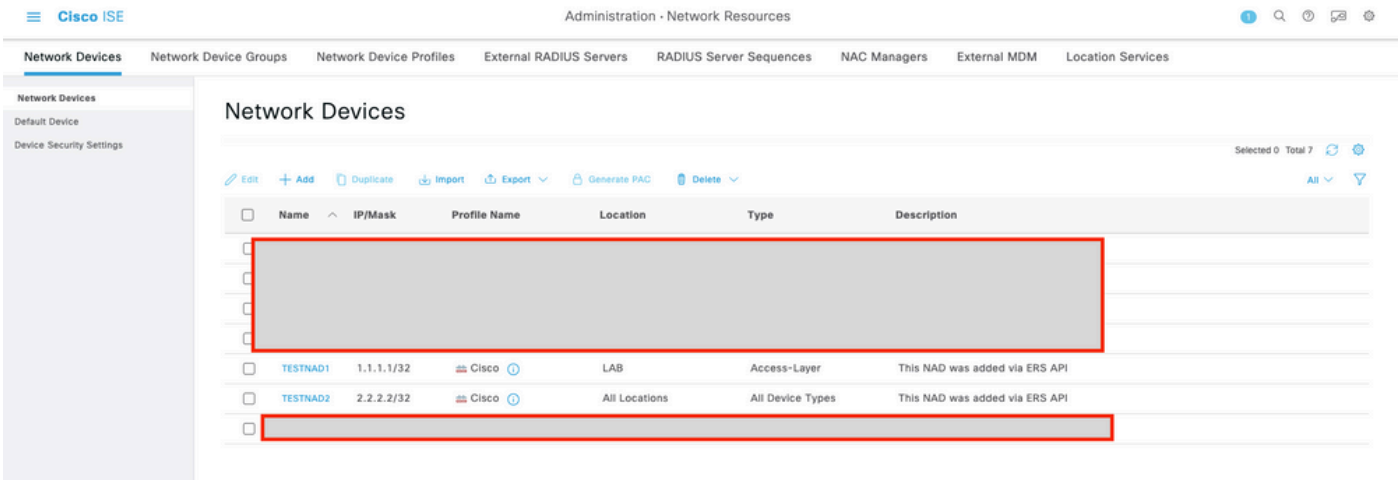
5. Fügen Sie die JSON-Vorlage für **raw** unter den **Body**-Header ein.

6. Wählen Sie **POST** als Methode, fügen Sie **https://{ISE-ip}/ers/config/network-device ein,** und klicken Sie auf **Senden.** Wenn alles korrekt konfiguriert wurde, müssen Sie eine Meldung **201 Erstellt** sehen und das Ergebnis leer lassen.



7. Bestätigen Sie, ob die NAD erstellt wurde, indem Sie einen GET-Aufruf für die NAD durchführen oder die ISE-NAD-Liste überprüfen.





Überprüfung

Wenn Sie auf die GUI-Seite des API-Diensts zugreifen können, z. B. **https://*{iseip}*:*{port}*/api/swagger-ui/index.html** oder **https://*{iseip}*:9060/ers/sdk,** bedeutet dies, dass der API-Dienst wie erwartet funktioniert.

Fehlerbehebung

- Alle REST-Vorgänge werden überwacht, und die Protokolle werden in den Systemprotokollen protokolliert.

- Um Probleme zu beheben, die sich auf die offenen APIs beziehen, legen Sie die **Protokollstufe** für die **apiservice**-Komponente im Fenster Konfiguration des **Debug-Protokolls** auf **DEBUG fest**.

- Um Probleme im Zusammenhang mit den ERS APIs zu beheben, legen Sie die **Protokollstufe** für die **ers**-Komponente im Fenster zur Konfiguration des **Debug-Protokolls** auf **DEBUG fest**. Um dieses Fenster anzuzeigen, navigieren Sie zur Cisco ISE-Benutzeroberfläche, klicken Sie auf das Menüsymbol und wählen Sie **Vorgänge > Fehlerbehebung > Debug-Assistent > Debug-Protokollkonfiguration aus**.

- Sie können die Protokolle aus dem Fenster **Download** Logs (Protokolle **herunterladen**) herunterladen. Um dieses Fenster anzuzeigen, navigieren Sie zur Cisco ISE-Benutzeroberfläche, klicken Sie auf das **Menü**-Symbol, und wählen Sie **Operations > Troubleshoot > Download Logs**.

- Sie können entweder ein Support-Paket von der Registerkarte Support Bundle herunterladen, indem Sie auf die Schaltfläche **Download** unter der Registerkarte klicken, oder Sie laden die **api-service**-Debug-Protokolle von der Registerkarte **Debug Logs herunter,** indem Sie auf den Wert **Log File (Protokolldatei)** für das api-service-Debug-Protokoll klicken.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.