Creación de dispositivos de red ISE mediante la API ERS

Contenido

Introducción

Este documento describe el proceso para crear dispositivos de acceso a la red (NAD) en ISE a través de la API ERS utilizando PostMan como cliente REST.

Prerequisites

Requirements

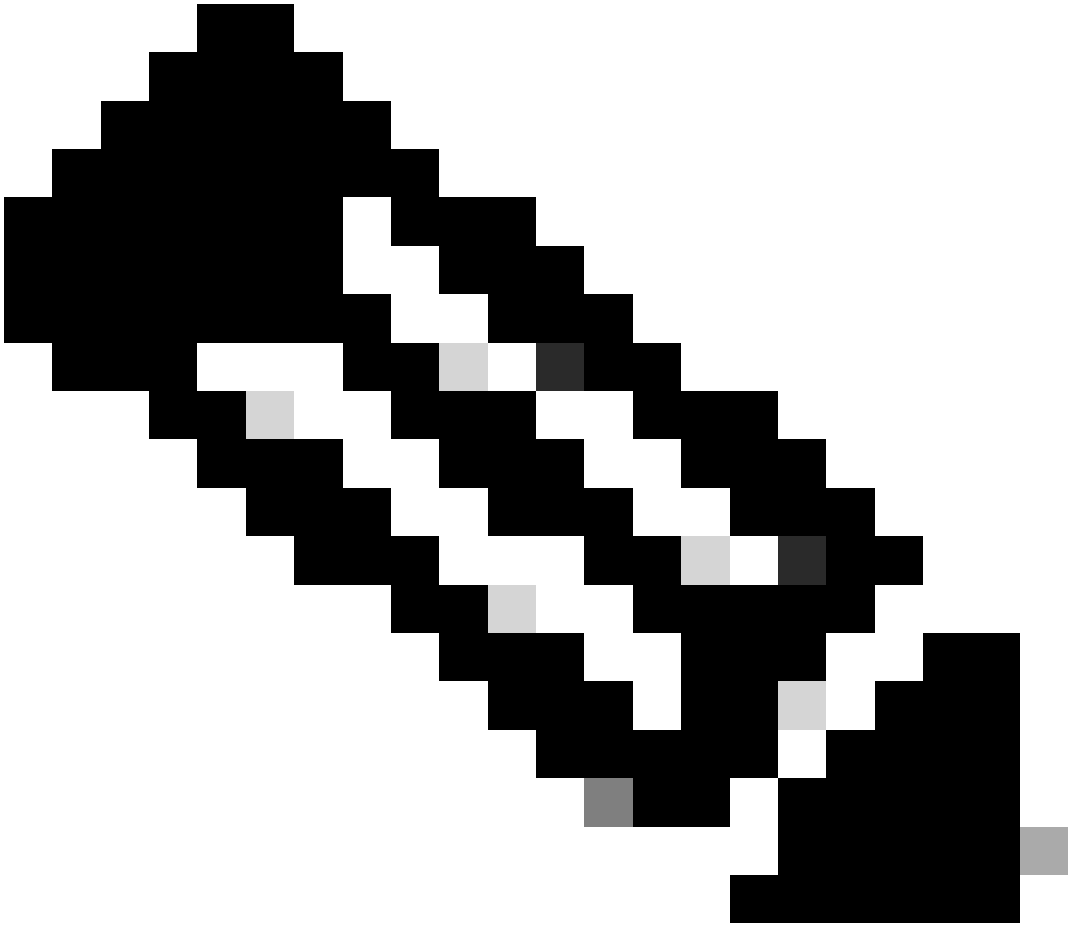
Cisco recomienda que tenga conocimiento sobre estos temas:

- ISE (Identity Services Engine)
- ERS (servicios RESTful externos)
- Clientes de REST como Postman, RESTED, Insomnio, etc.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

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



Nota: el procedimiento es similar o idéntico para otras versiones de ISE y clientes REST. Puede seguir estos pasos en todas las versiones de software 2.x y 3.x ISE, a menos que se indique lo contrario.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

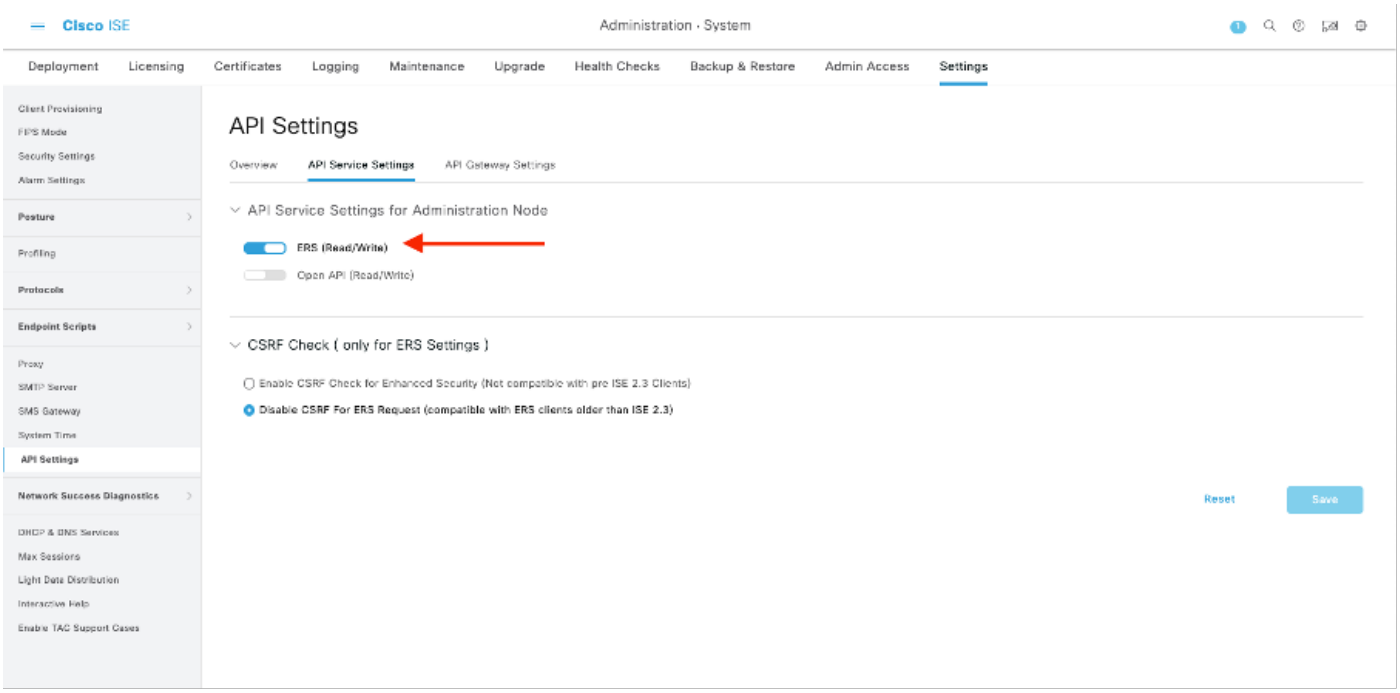
Configurar

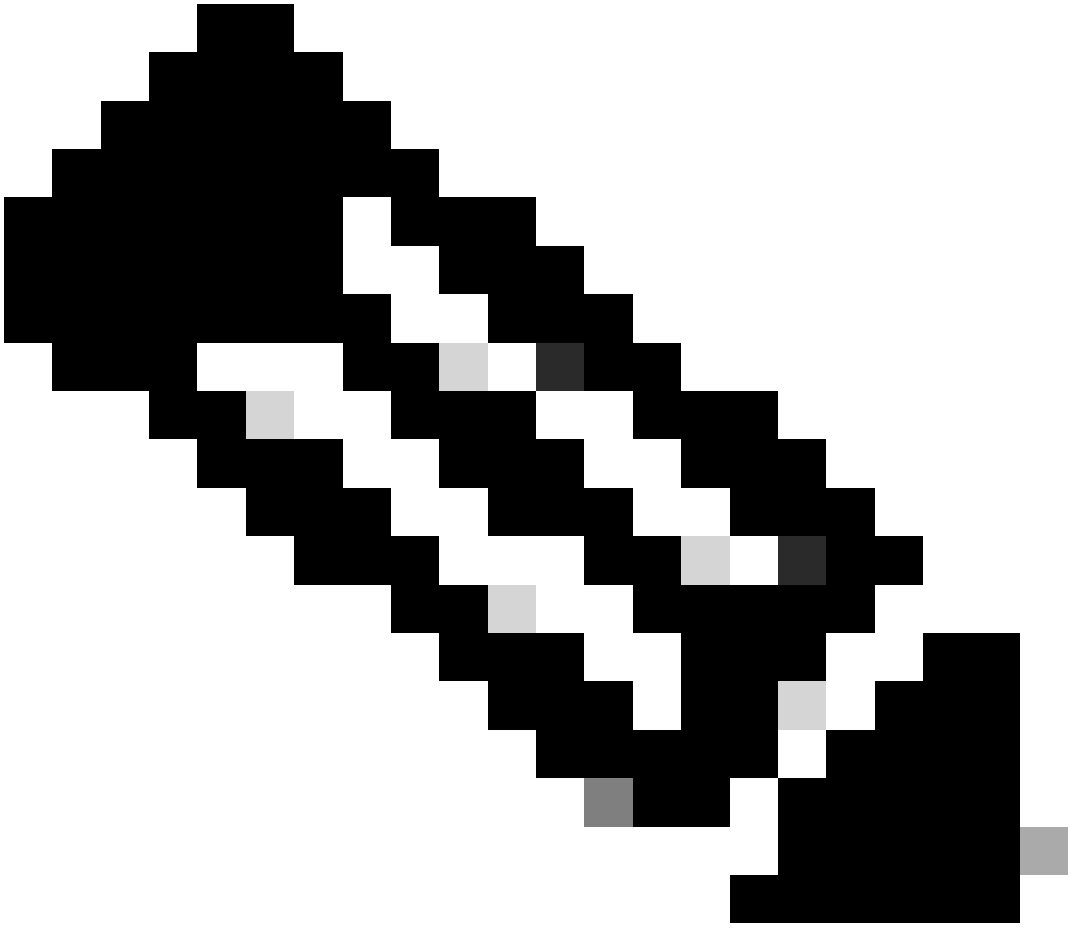
Activar ERS (puerto 9060)

Las API ERS son API REST solo HTTPS que funcionan a través de los puertos 443 y 9060. El puerto 9060 está cerrado de forma predeterminada, por lo que debe abrirse primero. Se presenta un tiempo de espera del servidor si los clientes que intentan acceder a este puerto no habilitan

ERS primero. Por lo tanto, el primer requisito es habilitar ERS desde la interfaz de usuario de administración de Cisco ISE.

Vaya a Administration > Settings > API Settings y active el botón de alternancia ERS (lectura/escritura).

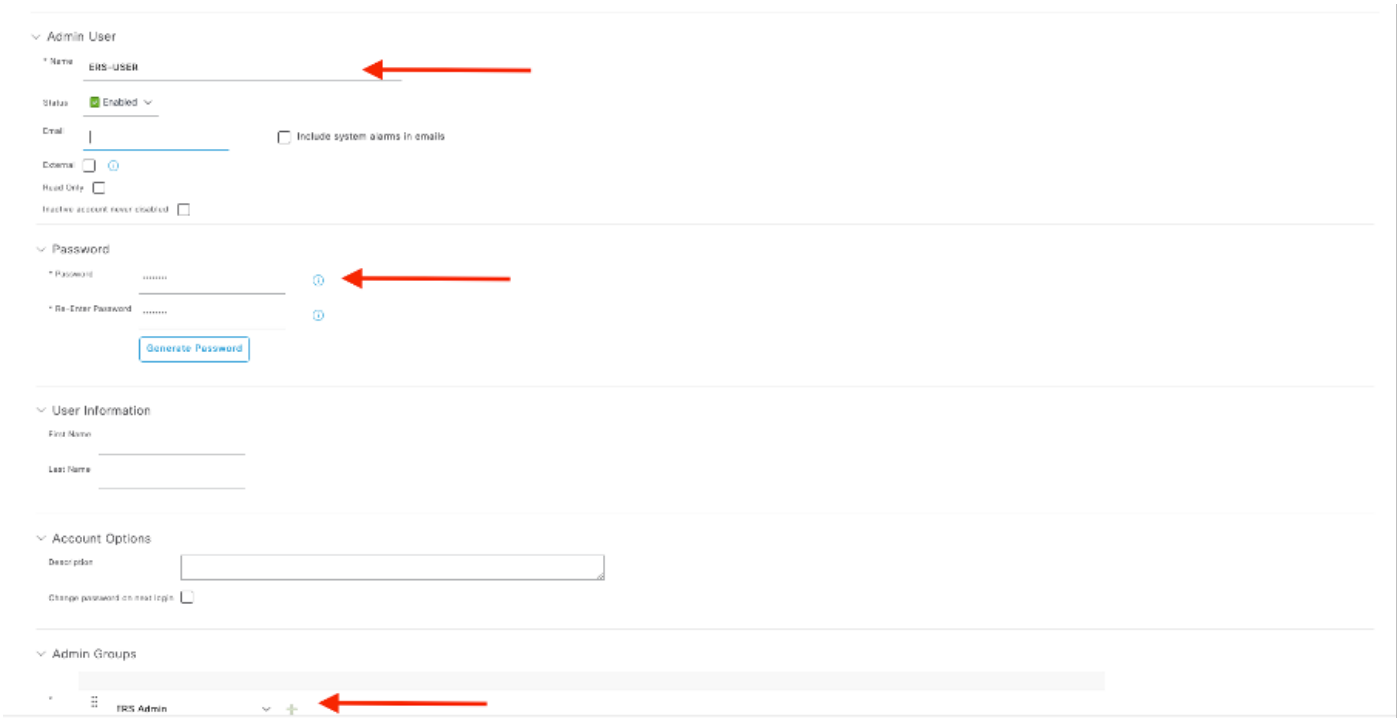




Nota: Las API ERS admiten TLS 1.1 y TLS 1.2. Las API ERS no admiten TLS 1.0 independientemente de que se habilite TLS 1.0 en la ventana Security Settings (Parámetros de seguridad) de la GUI de Cisco ISE (Administración > Sistema > Settings > Security Settings). La habilitación de TLS 1.0 en la ventana Security Settings está relacionada solamente con el protocolo EAP y no afecta a las API ERS.

Crear administrador ERS

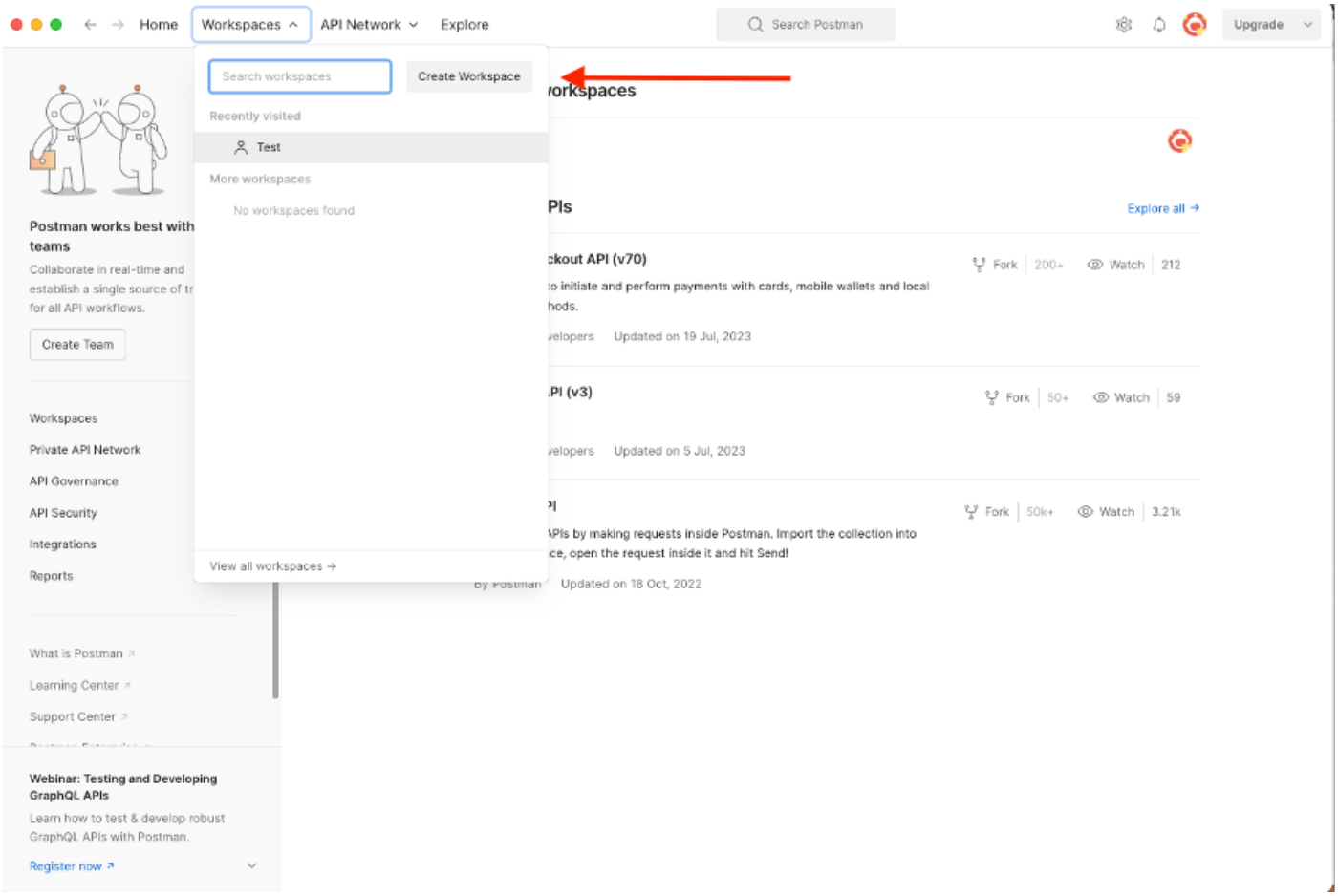
Cree un administrador de Cisco ISE, asigne una contraseña y agregue el usuario al grupo de administradores como administrador de ERS. Puede dejar el resto de la configuración vacía.



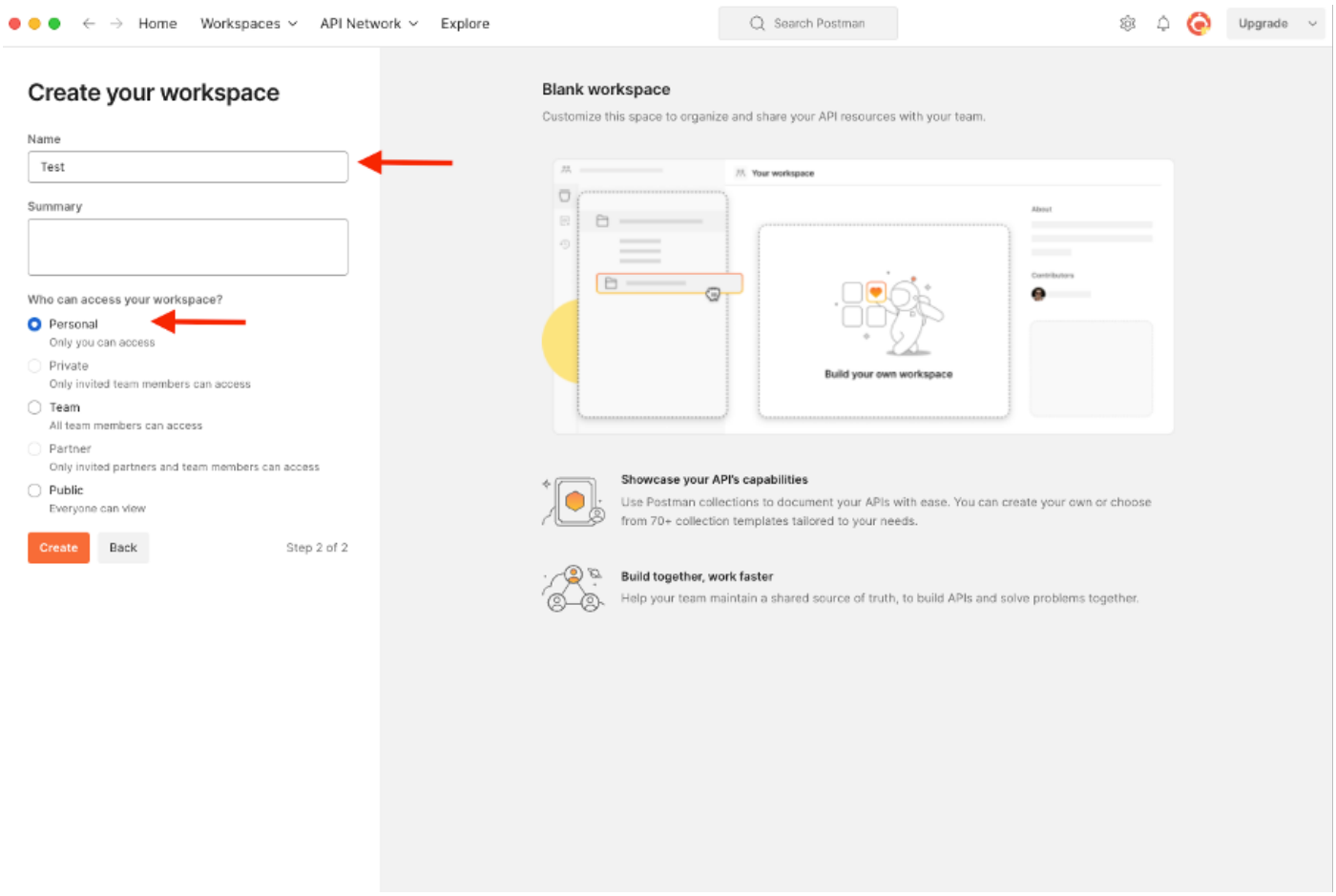
Configuración de Postman

Descargue o utilice la versión en línea de Postman.

1. Cree un usuario y un espacio de trabajo haciendo clic en Create Workspace en la pestaña Workspaces.



2. Seleccione Espacio de Trabajo en Blanco y asígnele un nombre. Puede agregar una descripción y hacerla pública. En este ejemplo, Personalis está seleccionado.

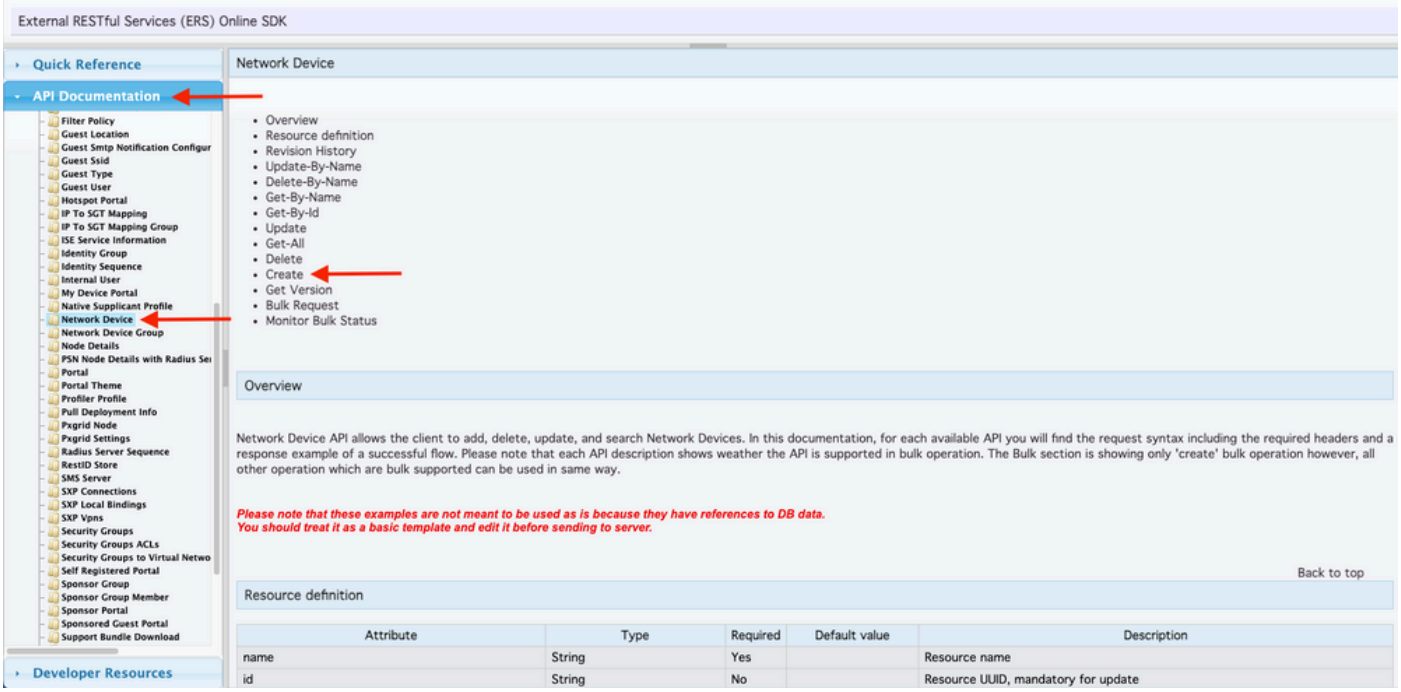


Una vez creado el espacio de trabajo, podrá configurar las llamadas API.

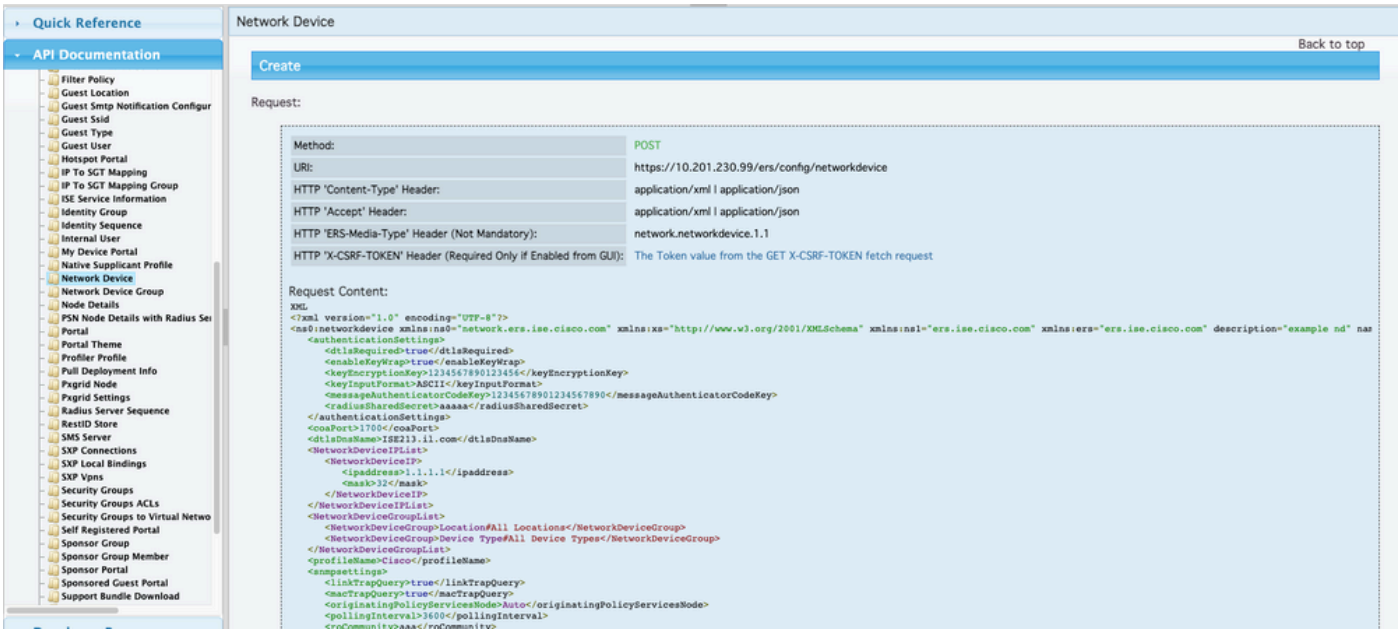
ISE SDK y autorización básica de postman

Para configurar cualquier llamada, acceda primero a ISE ERS SDK (Software Developer Kit). Esta herramienta recopila la lista completa de llamadas API que ISE puede realizar:

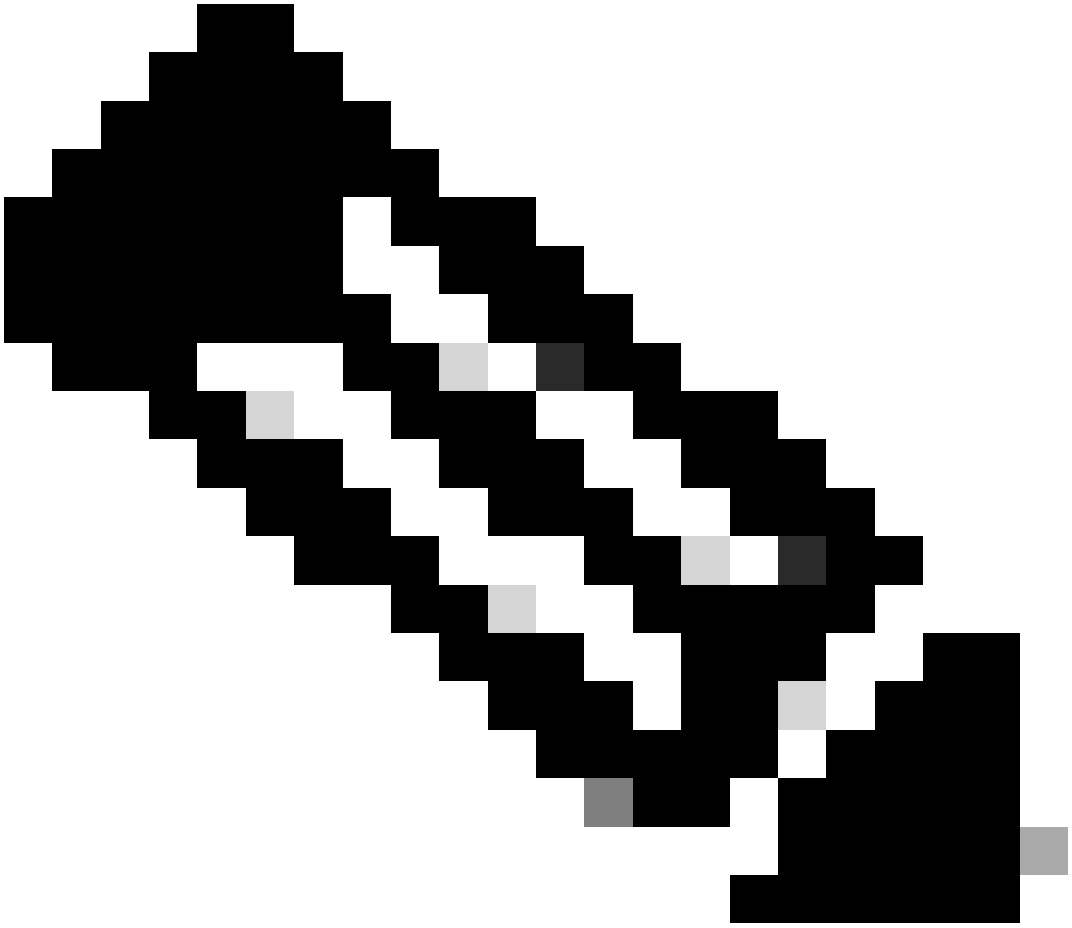
1. Vaya a https://{ise-ip}/ers/sdk.
2. Inicie sesión con sus credenciales de administrador de ISE.
3. Expanda la documentación de la API.
4. Desplácese hacia abajo hasta que encuentre Network Device y haga clic en él.
5. Con esta opción, ahora puede encontrar todas las operaciones disponibles que puede realizar para los dispositivos de red en ISE. Seleccione Create.



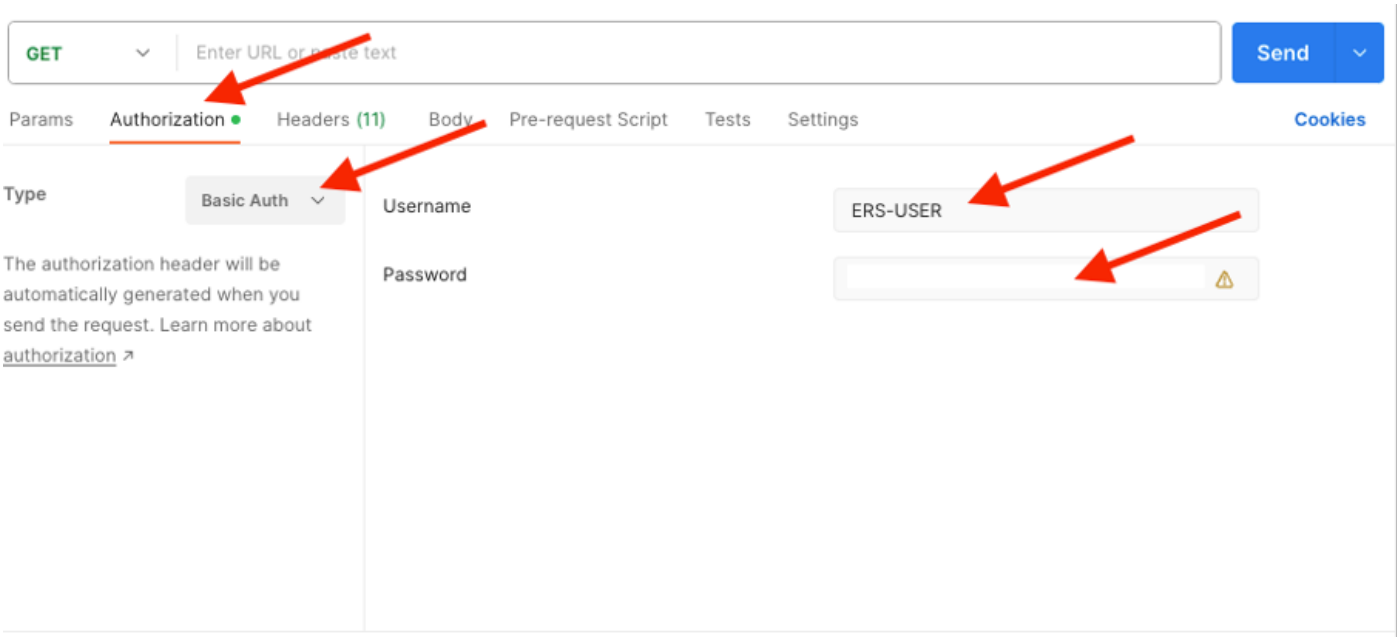
6. Ahora puede ver la configuración necesaria para realizar la llamada API mediante XML o JSON en cualquier cliente Rest, así como un ejemplo de respuesta esperada.



7.Volver a Postman configurar la autenticación básica para ISE. En la pestaña Authorization, seleccione Basic Auth como tipo de autenticación y agregue las credenciales de usuario ERS de ISE creadas anteriormente en ISE.



Nota: La contraseña se muestra como texto sin cifrar a menos que se configuren variables en Postman.

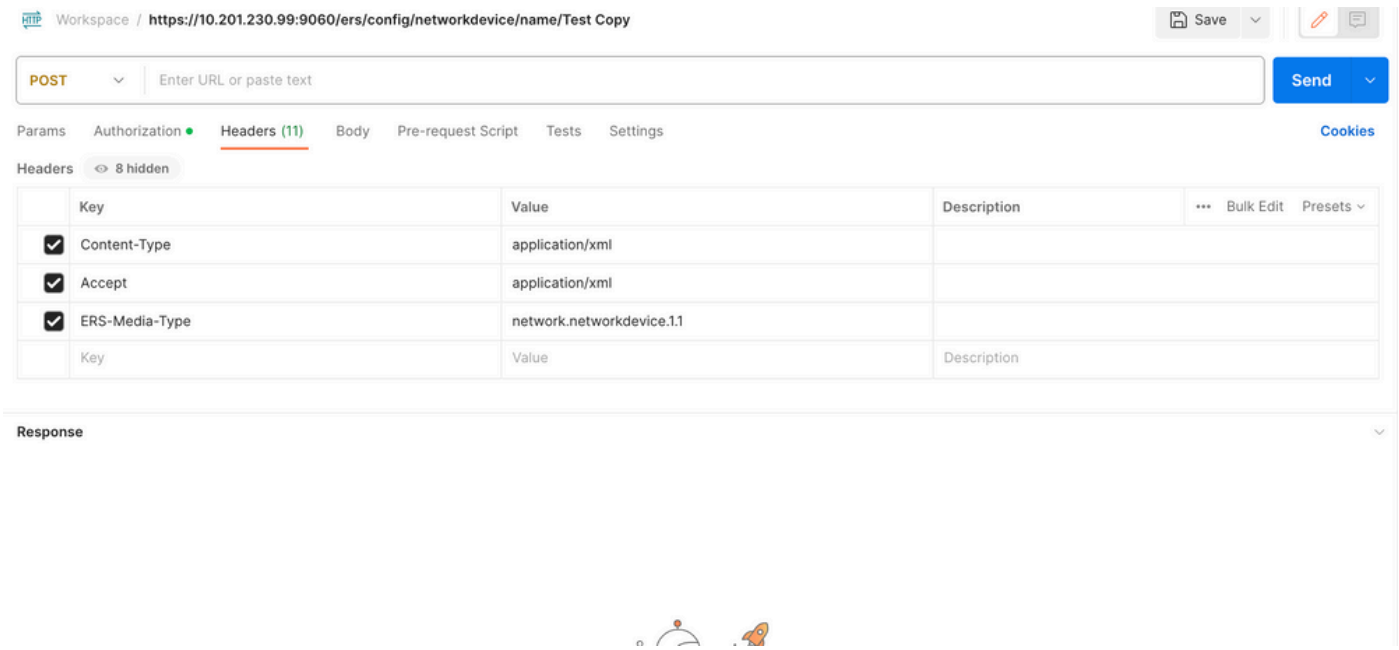


Crear y utilizar XML

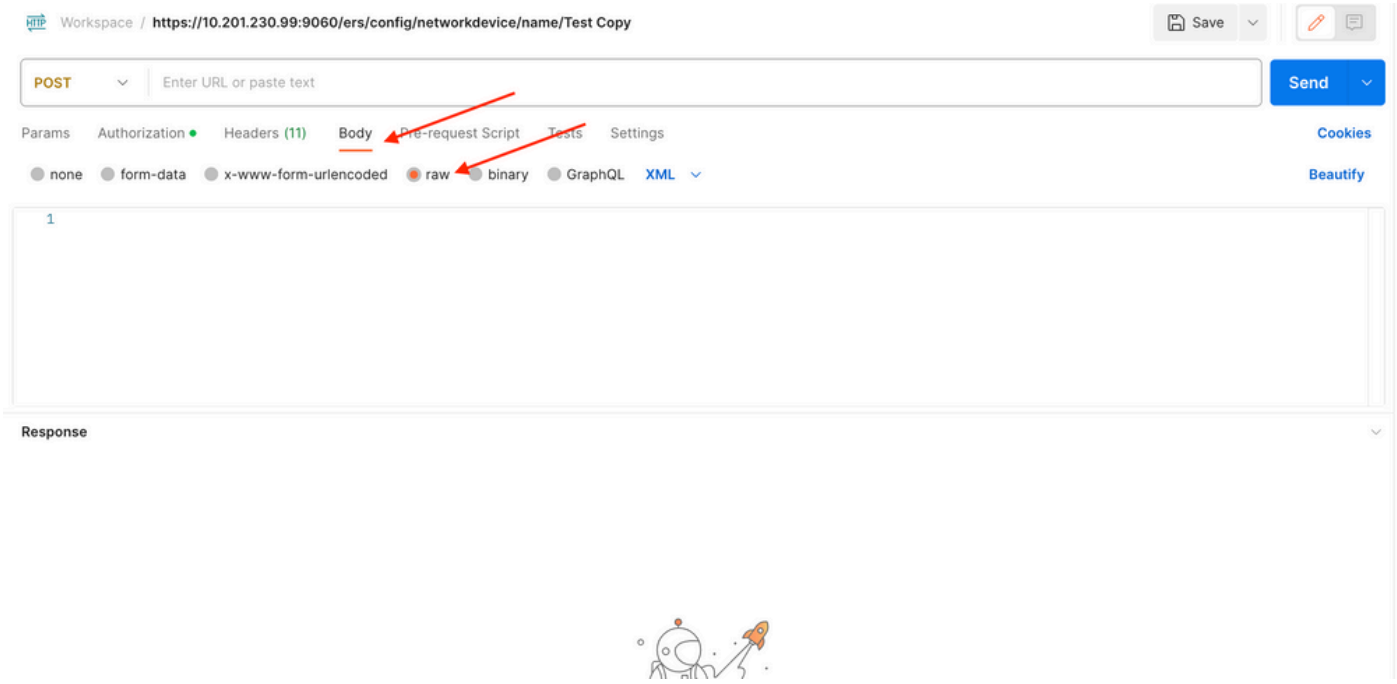
Cree TESTNAD1 con RADIUS TACACS, SNMP y configuraciones TrustSec usando XML.

1. En el SDK, en Crear, se encuentran los encabezados y las plantillas necesarias para realizar la llamada, así como la respuesta esperada.

2. Vaya a la pestaña Headers y configure los encabezados necesarios para la llamada API tal como se ve en el SDK. La configuración del encabezado debe ser similar a la siguiente:

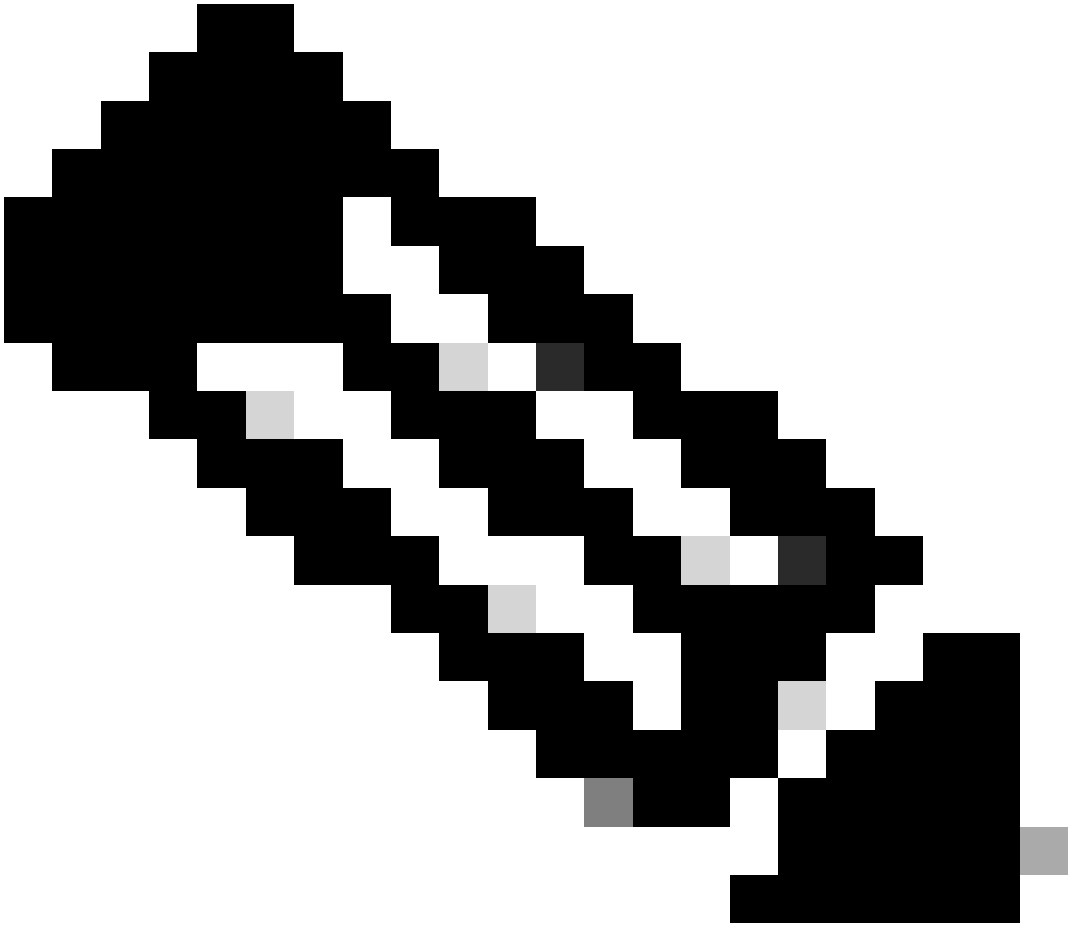


3. Desplácese hasta la cabecera Body y seleccione raw. Esto le permite pegar la plantilla XML necesaria para crear el NAD.



4. La plantilla XML tiene el siguiente aspecto (cambie los valores según sea necesario):

<?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: Es importante tener en cuenta que las líneas siguientes solo son necesarias si **<enableKeyWrap>{false|true}</enableKeyWrap>** se establece en **true**. De lo contrario, se puede eliminar lo mismo de la plantilla XML:

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

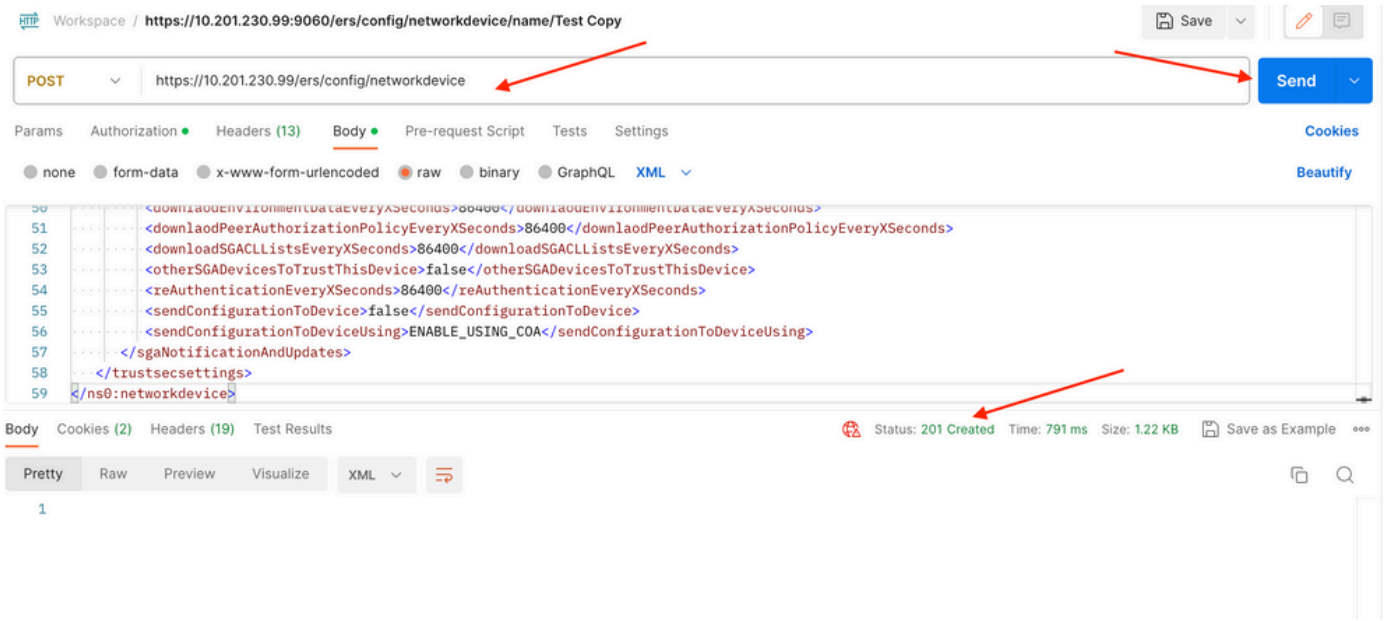
Puede quitar la configuración que no necesite de la plantilla y dejar los datos que realmente necesite agregar durante la creación del NAD. A modo de ejemplo, aquí está la misma plantilla pero solo con la configuración TACACS. Independientemente de la configuración requerida, asegúrese de que la plantilla termine con **</ns0:networkdevice>.**

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

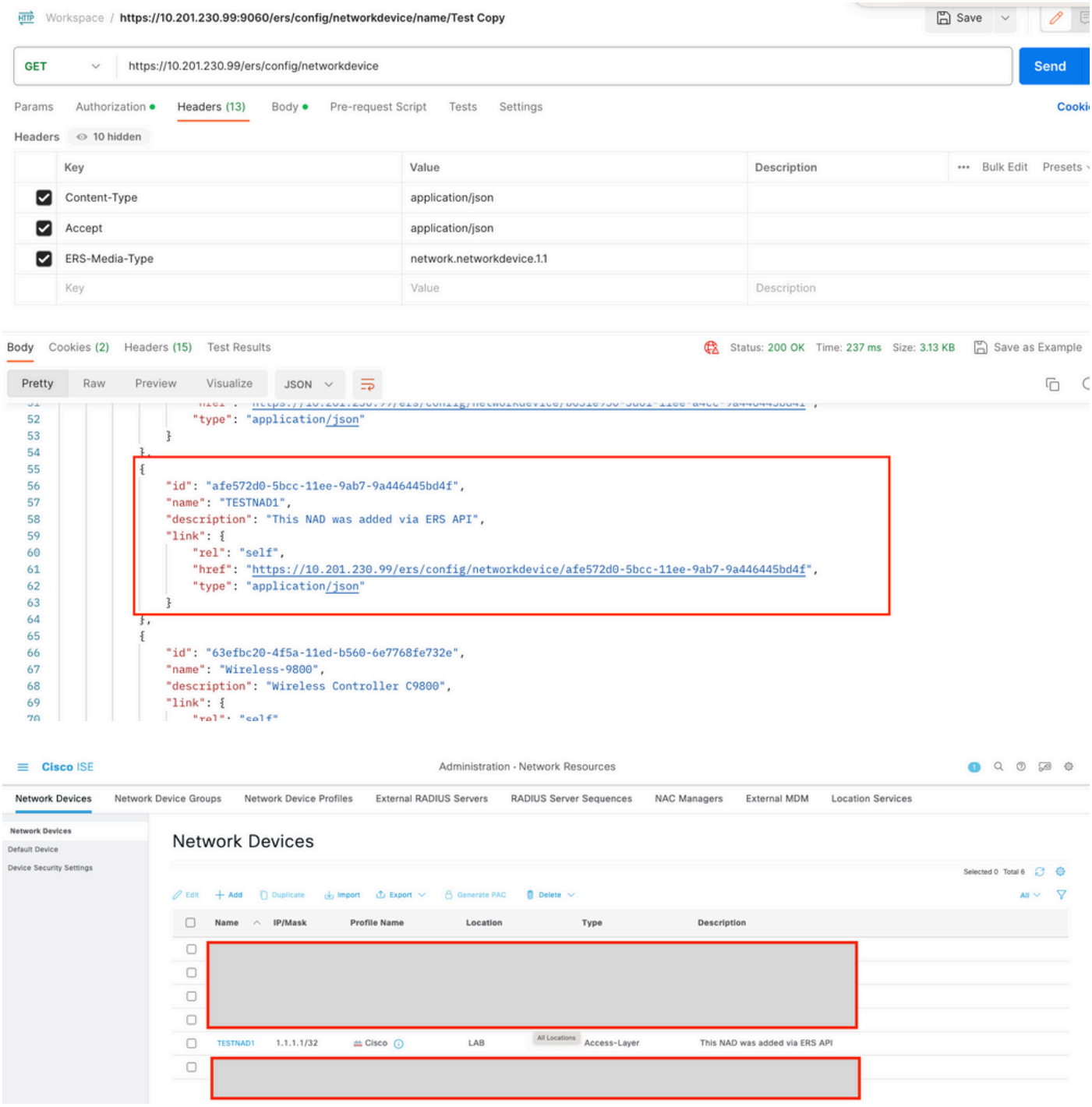
xmlns:ns1="ers.ise.cisco.com" xmlns:ers="ers.ise.cisco.com" description="**This NAD was added via ERS API**" name="**TESTNAD1**"> <NetworkDeviceIPList> <NetworkDeviceIP> <ipaddress>**NAD IP Address**</ipaddress> <mask>**32**</mask> </NetworkDeviceIP> </NetworkDeviceIPList> <NetworkDeviceGroupList> <NetworkDeviceGroup>Location#All 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. Pegue la plantilla XML para **raw** bajo el encabezado **Body**.

6. Seleccione **POST** como método, pegue **https://{ISE-ip}/ers/config/networkdevice** y haga clic en Send. **Si todo se configuró correctamente, debe ver un mensaje 201 Created** y el resultado estará vacío.



7. Confirme si el NAD se creó realizando una llamada **GET** para el NAD o comprobando la lista de ISE NAD.

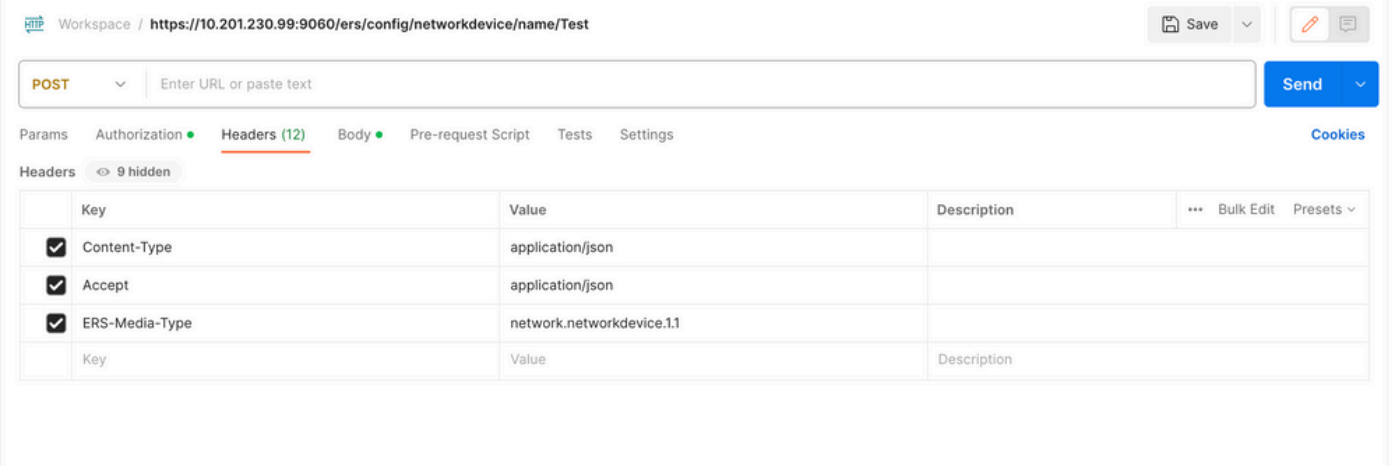


Crear y utilizar JSON

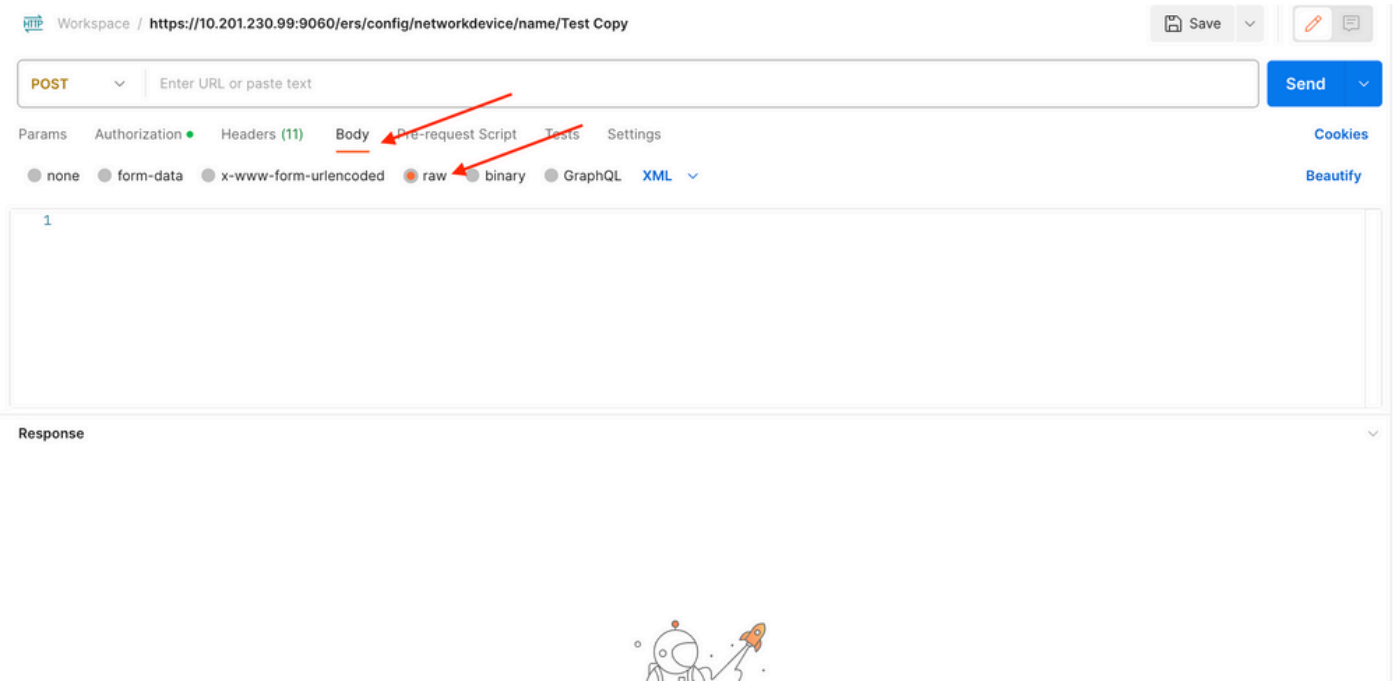
Cree TESTNAD2 con RADIUS TACACS, SNMP y configuraciones TrustSec usando JSON.

1. En el SDK, en **Crear,** se encuentran los encabezados y las plantillas necesarias para realizar la llamada, así como la respuesta esperada.

2. Vaya a la pestaña **Headers** y configure los encabezados necesarios para la llamada API tal como se ve en el SDK. La configuración del encabezado debe ser similar a la siguiente:

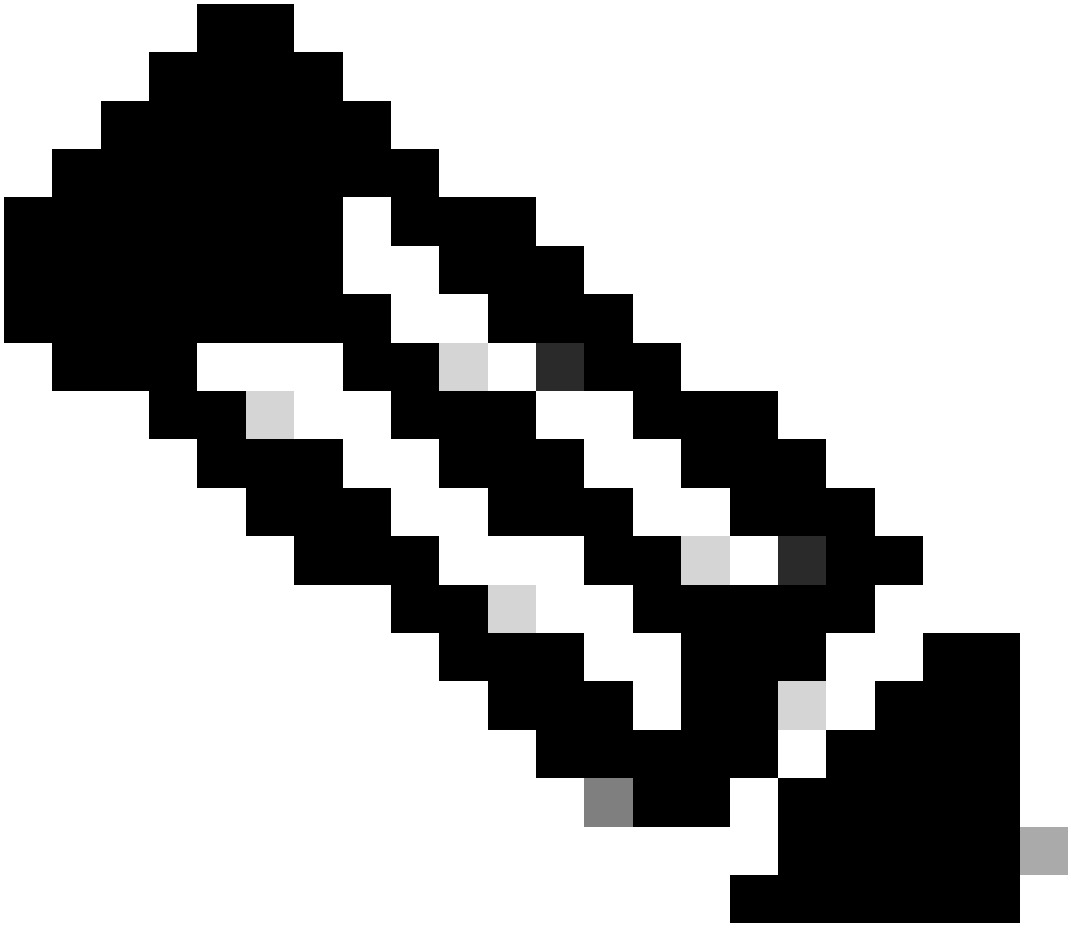


3. Desplácese hasta la cabecera **Body** y seleccione **raw**. Esto le permite pegar la plantilla JSON necesaria para crear el NAD.



4. La plantilla JSON debe tener el siguiente aspecto (cambie los valores según sea necesario):

{ "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"] } }

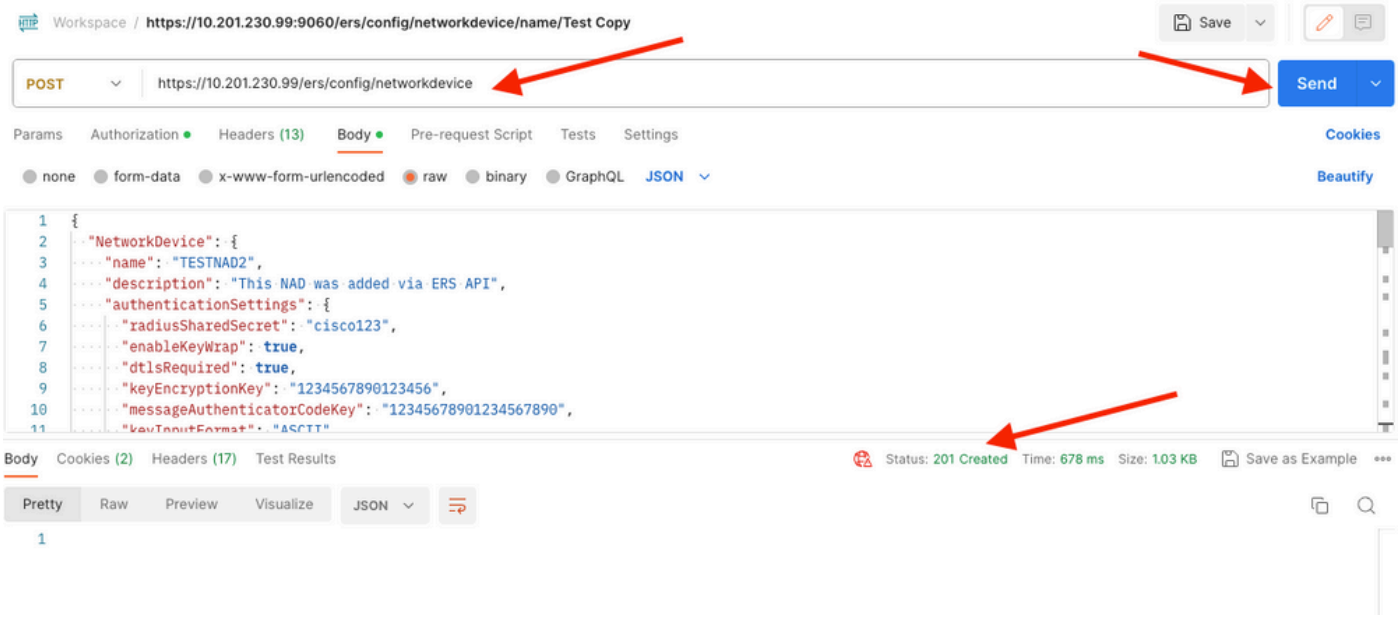


Nota: Es importante tener en cuenta que las líneas siguientes solo son necesarias si **enableKeyWrap":{false|true}**, se establece en **true**. De lo contrario, se puede eliminar lo mismo de la plantilla JSON:

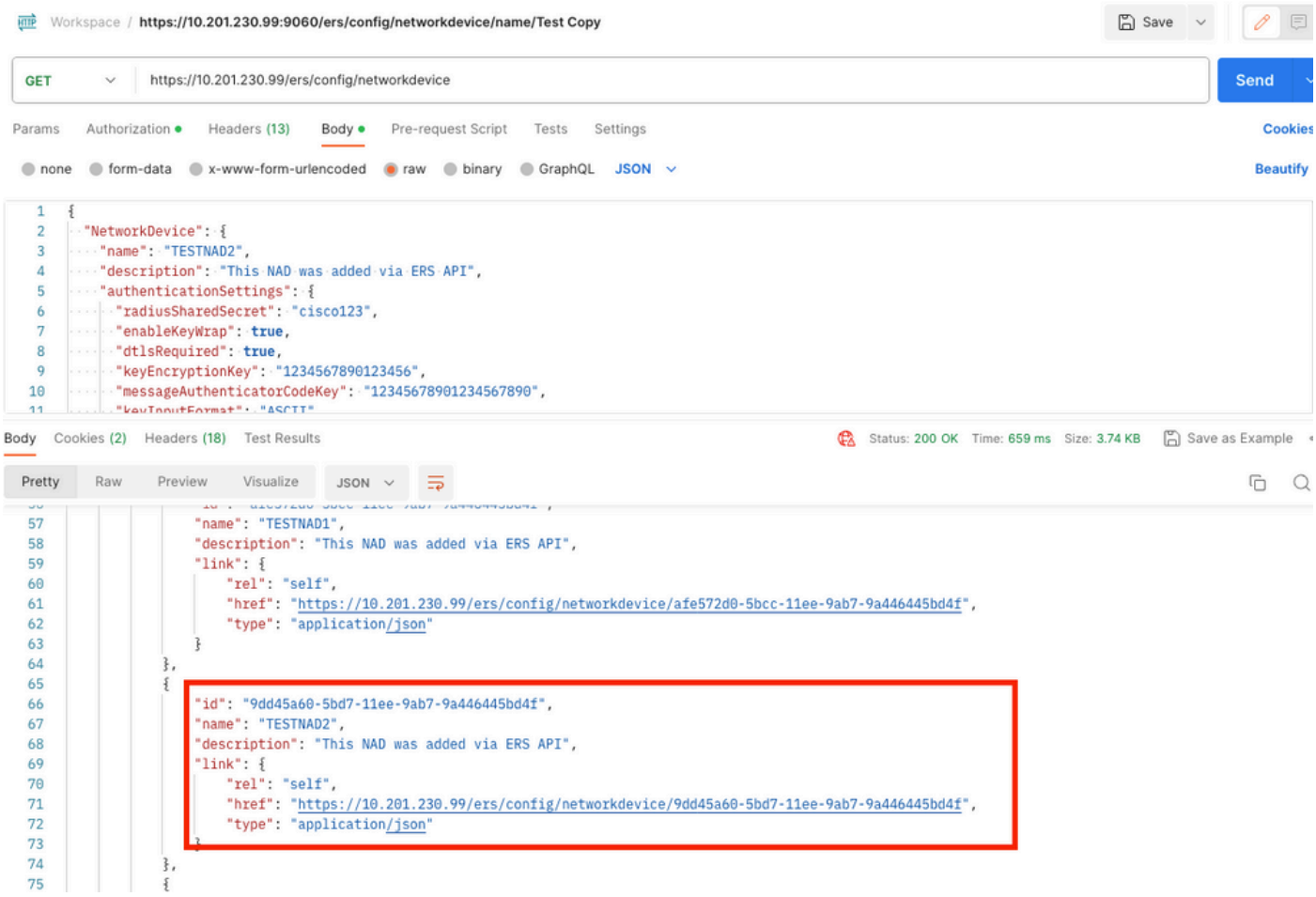
"keyEncryptionKey": "**1234567890123456**", "messageAuthenticatorCodeKey": "**12345678901234567890**", "keyInputFormat": "**ASCII**" También puede quitar la configuración que no necesite de la plantilla y dejar los datos que realmente necesita agregar durante la creación del NAD.

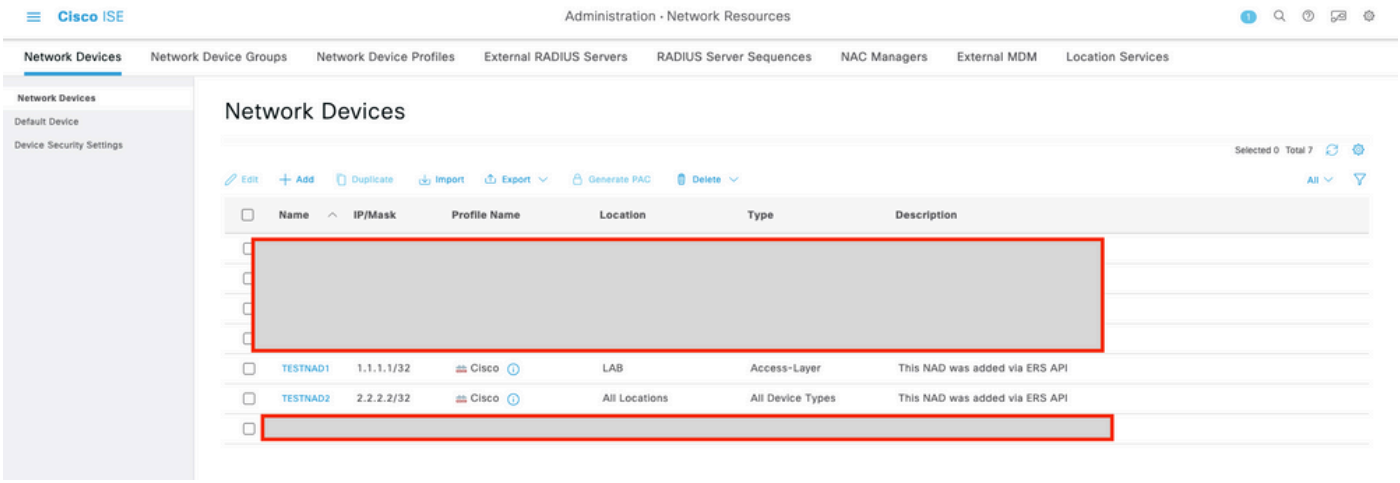
5. Pegue la plantilla JSON para **raw** bajo el encabezado **Body**.

6. Seleccione **POST** como método, pegue **https://{ISE-ip}/ers/config/networkdevice** y haga clic en Send. **Si todo se configuró correctamente, debe ver un mensaje 201 Created** y el resultado estará vacío.



7. Confirme si el NAD se creó realizando una llamada GET para el NAD o comprobando la lista de ISE NAD.





Verificación

Si puede acceder a la página GUI del servicio API, por ejemplo, **https://**{iseip}:{port}**/api/swagger-ui/index.html** o **https://**{iseip}**:9060/ers/sdk**, significa que el servicio API está funcionando como se esperaba.

Troubleshoot

- Todas las operaciones REST se auditan y los registros se registran en los registros del sistema.
- Para resolver problemas relacionados con las API abiertas, establezca el **Nivel de registro** para el componente **apiservice** en **DEBUG** en la ventana **Debug Log Configuration**.
- Para resolver problemas relacionados con las API ERS, establezca el **Nivel de registro** para el componente **ers** en **DEBUG** en la ventana **Debug Log Configuration**. Para ver esta ventana, navegue hasta la GUI de Cisco ISE, haga clic en el icono Menú y elija **Operaciones > Solución de problemas > Asistente de depuración > Configuración del registro de depuración**.
- Puede descargar los registros desde la ventana **Download** Logs (**Descargar** registros). Para ver esta ventana, navegue hasta la GUI de Cisco ISE, haga clic en el icono **Menu** y elija **Operations > Troubleshoot > Download Logs**.
- Puede descargar un paquete de soporte de la pestaña Paquete de soporte haciendo clic en el botón **Descargar** debajo de la pestaña, o descargar los registros de depuración **api-service** de la pestaña **Registros de depuración** haciendo clic en el valor de Archivo de registro para el registro de depuración api-service.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).