Criar dispositivos de rede do ISE usando a API ERS

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Configurar
  - Ativar ERS (Porta 9060)
  - Criar ERS Admin
  - Configurar Postman
  - SDK do ISE e autorização de carteiro básico
  - Criar NAD usando XML
  - Criar NAD usando JSON
- Verificar
- Troubleshooting

Introdução

Este documento descreve o processo para criar dispositivos de acesso à rede (NADs) no ISE através da API ERS usando PostMan como o cliente REST.

Pré-requisitos

Requisitos

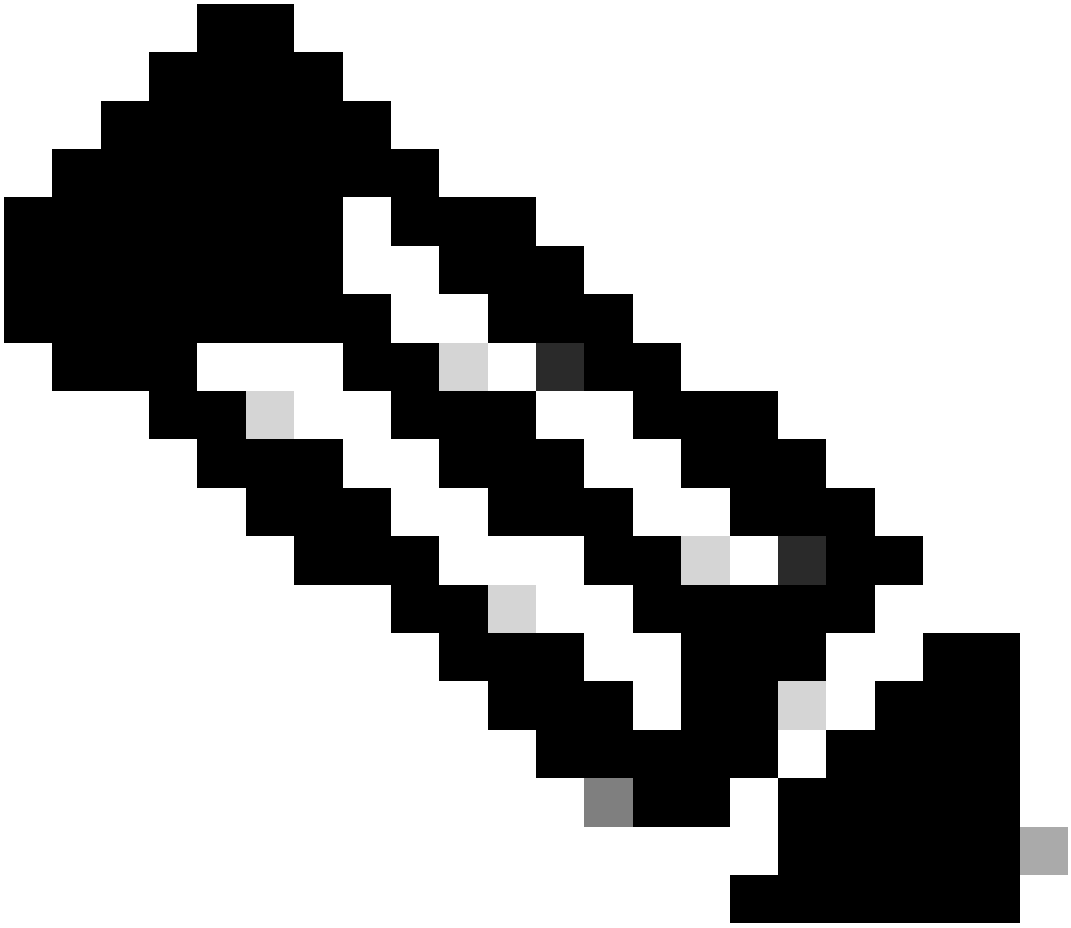
A Cisco recomenda que você tenha conhecimento destes tópicos:

- ISE (Identity Services Engine, mecanismo de serviços de identidade)
- ERS (External RESTful Services, Serviços RESTful externos)
- Clientes do REST como Postman, RESTED, Insomnia, etc.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

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



Observação: o procedimento é semelhante ou idêntico para outras versões do ISE e Clientes REST. Você pode usar essas etapas em todas as versões 2.x e 3.x do software ISE, a menos que declarado o contrário.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

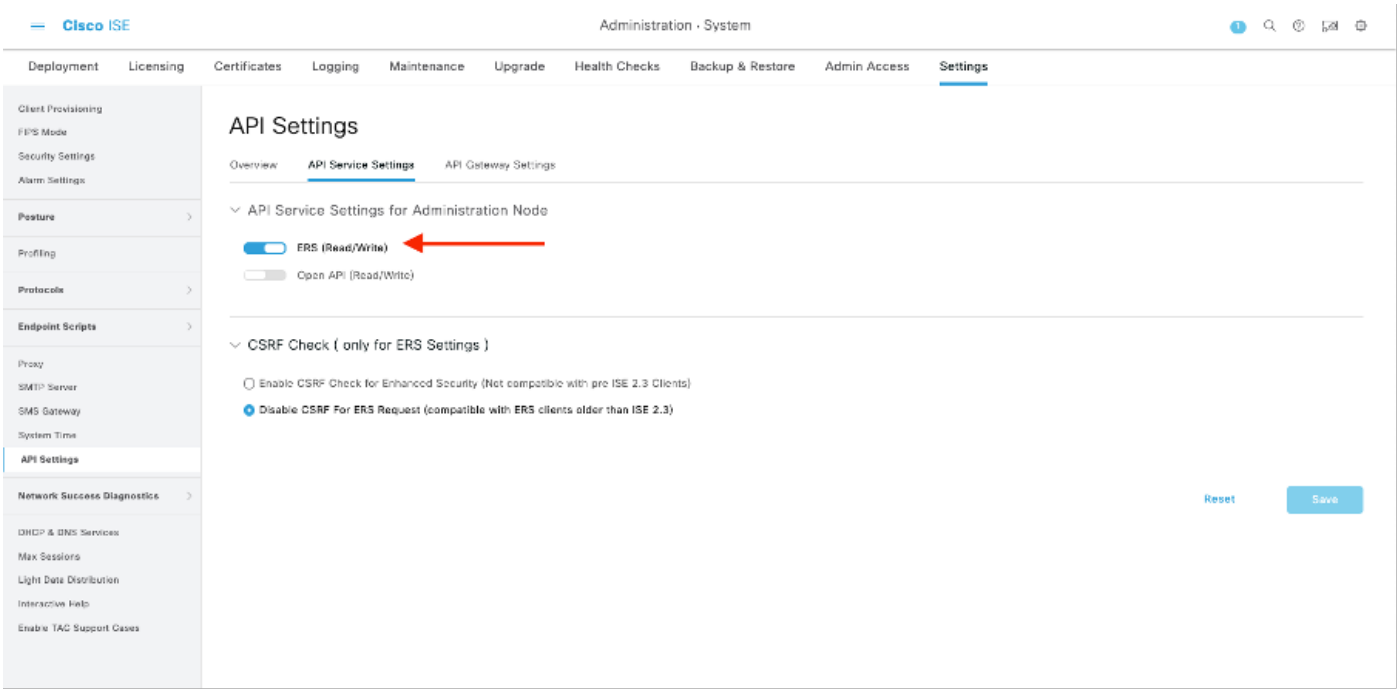
Configurar

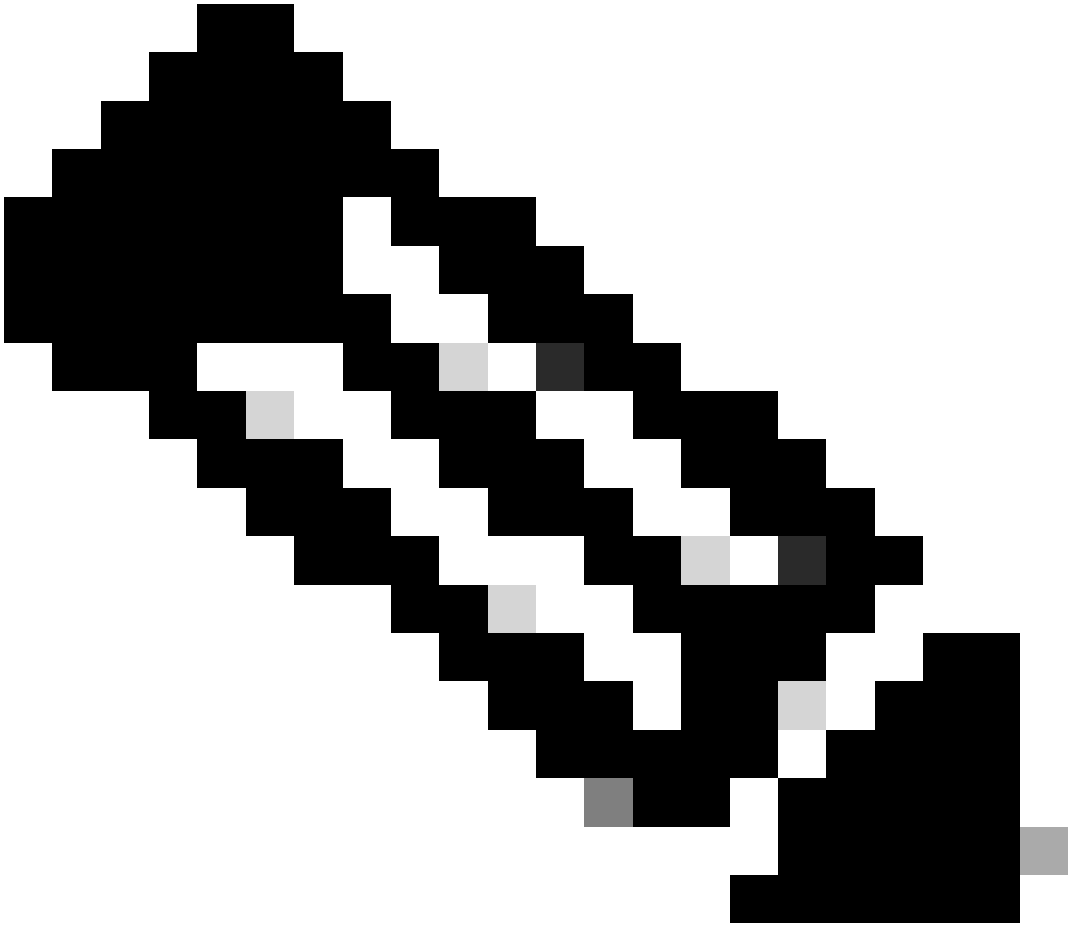
Ativar ERS (Porta 9060)

As APIs ERS são APIs REST somente HTTPS que operam nas portas 443 e 9060. A porta 9060 é fechada por padrão, por isso precisa ser aberta primeiro. Um tempo limite do servidor será apresentado se os clientes que tentarem acessar essa porta não ativarem o ERS primeiro.

Portanto, o primeiro requisito é ativar o ERS na interface do usuário do administrador do Cisco ISE.

Navegue até Administration > Settings > API Settings e ative o botão de alternância ERS (Read/Write).

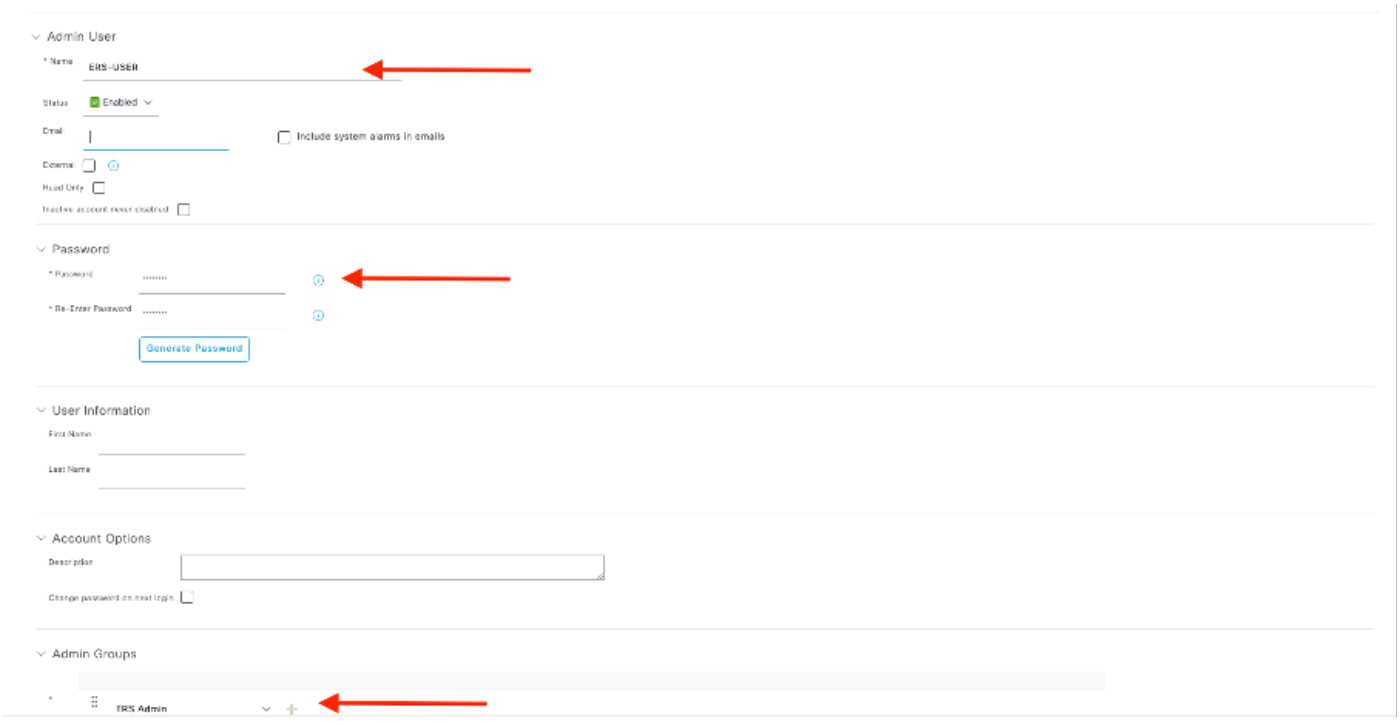




Observação: as APIs ERS suportam TLS 1.1 e TLS 1.2. As APIs ERS não suportam TLS 1.0, independentemente da ativação do TLS 1.0 na janela Configurações de segurança da GUI do Cisco ISE (Administração > Sistema > Configurações > Configurações de segurança). A habilitação do TLS 1.0 na janela Configurações de segurança está relacionada apenas ao protocolo EAP e não afeta as APIs ERS.

Criar ERS Admin

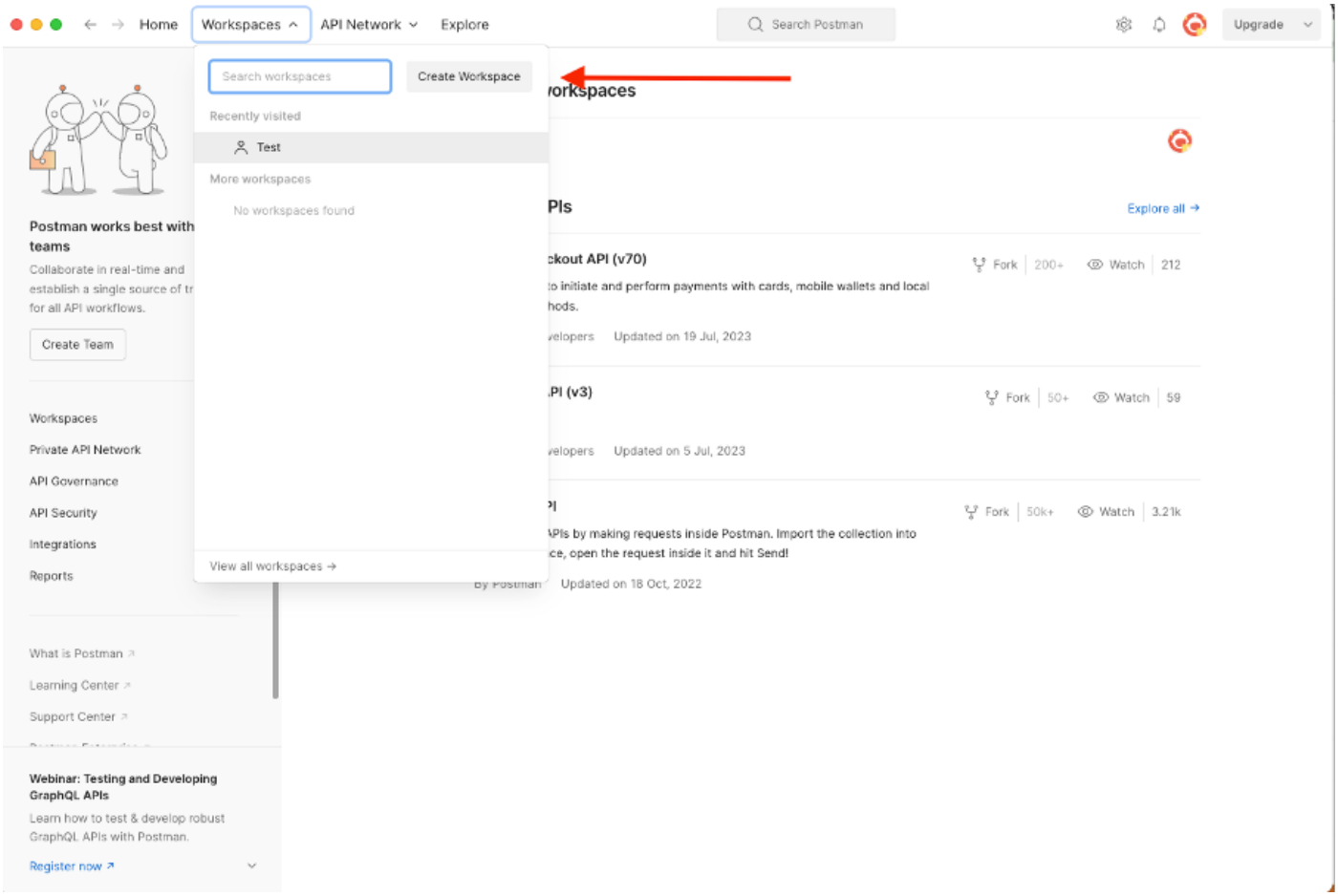
Crie um administrador do Cisco ISE, atribua uma senha e adicione o usuário ao grupo admin como ERS Admin. Você pode deixar o restante da configuração vazio.



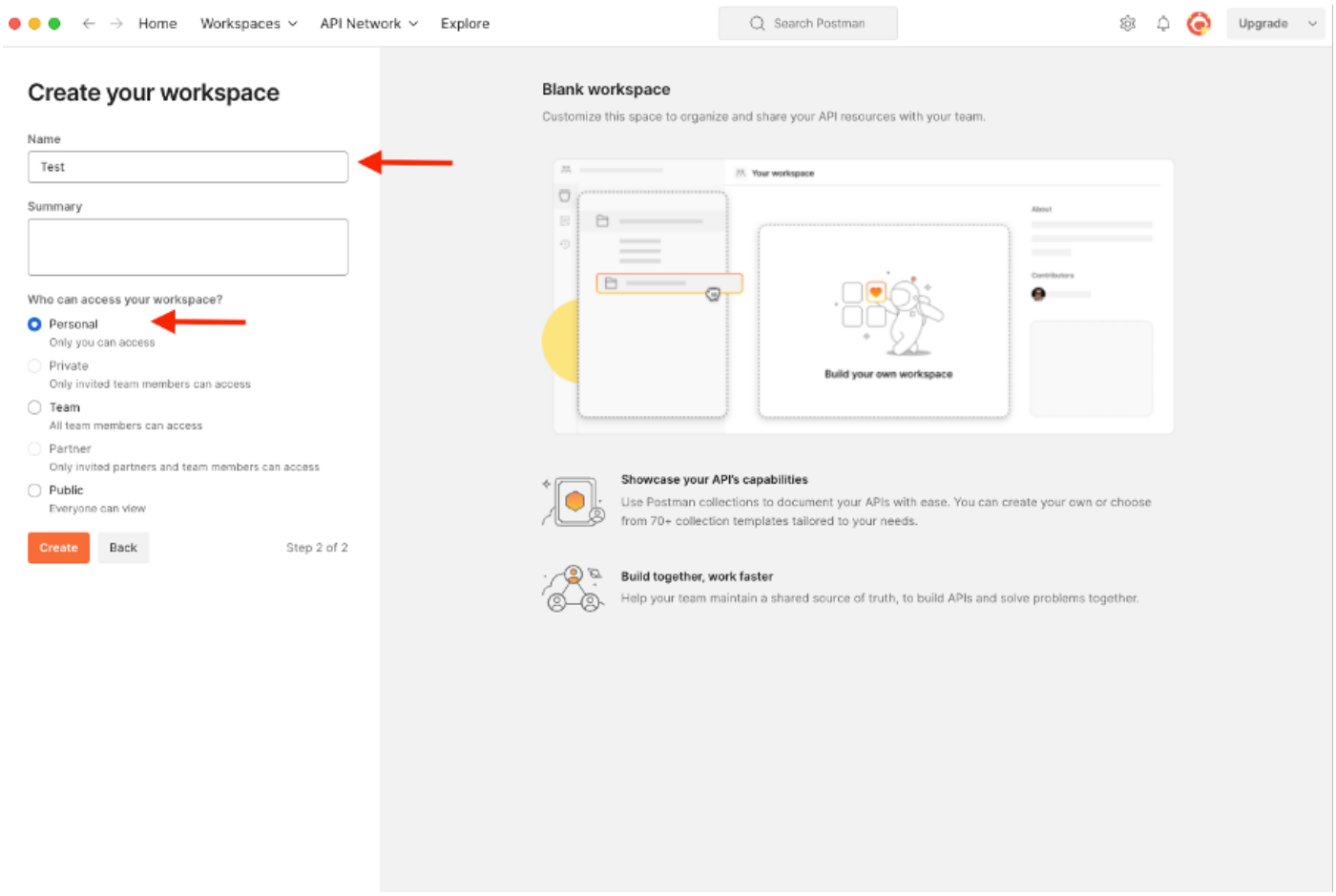
Configurar Postman

Faça o download ou use a versão online do Postman.

1. Crie um usuário e um espaço de trabalho clicando em Criar espaço de trabalho na guia Espaços de trabalho.



2. Selecione Espaço de Trabalho em Branco e atribua um nome ao espaço de trabalho. Você pode adicionar uma descrição e torná-la pública. Para este exemplo, Personalis foi selecionado.

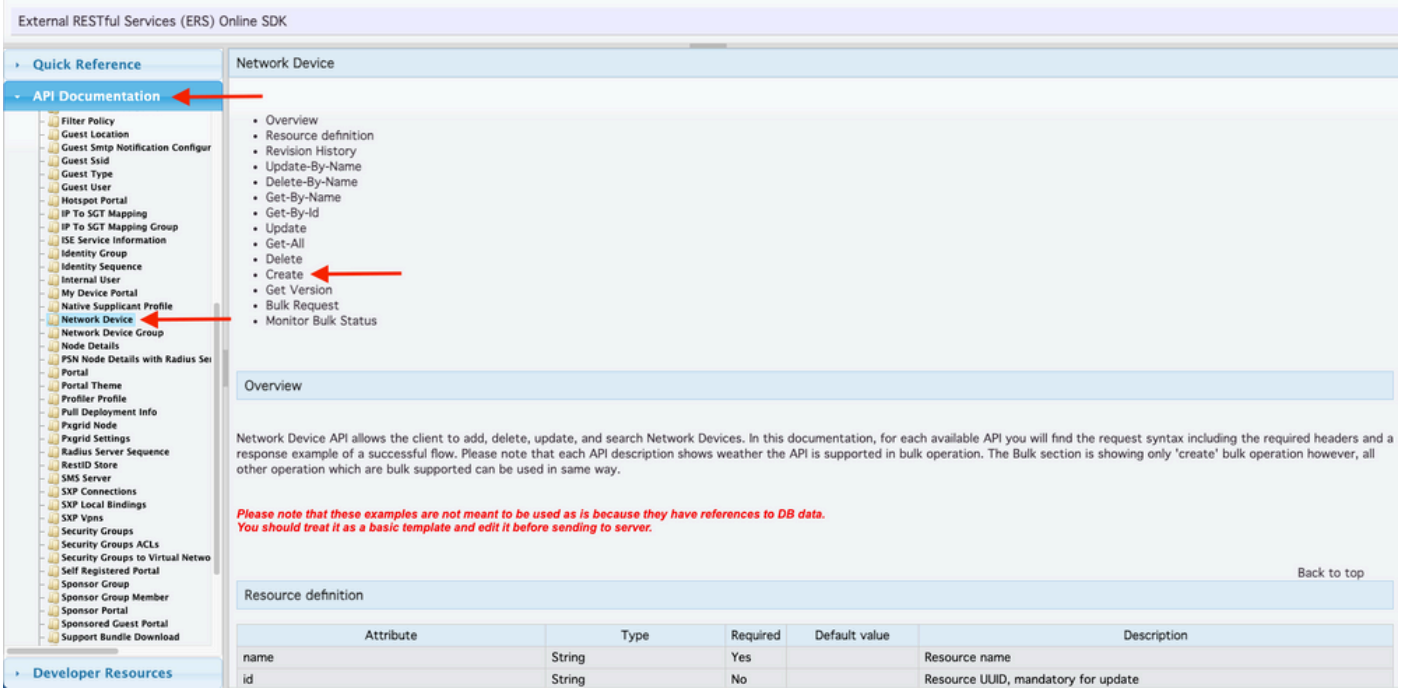


Depois de criar o espaço de trabalho, você pode configurar as chamadas à API.

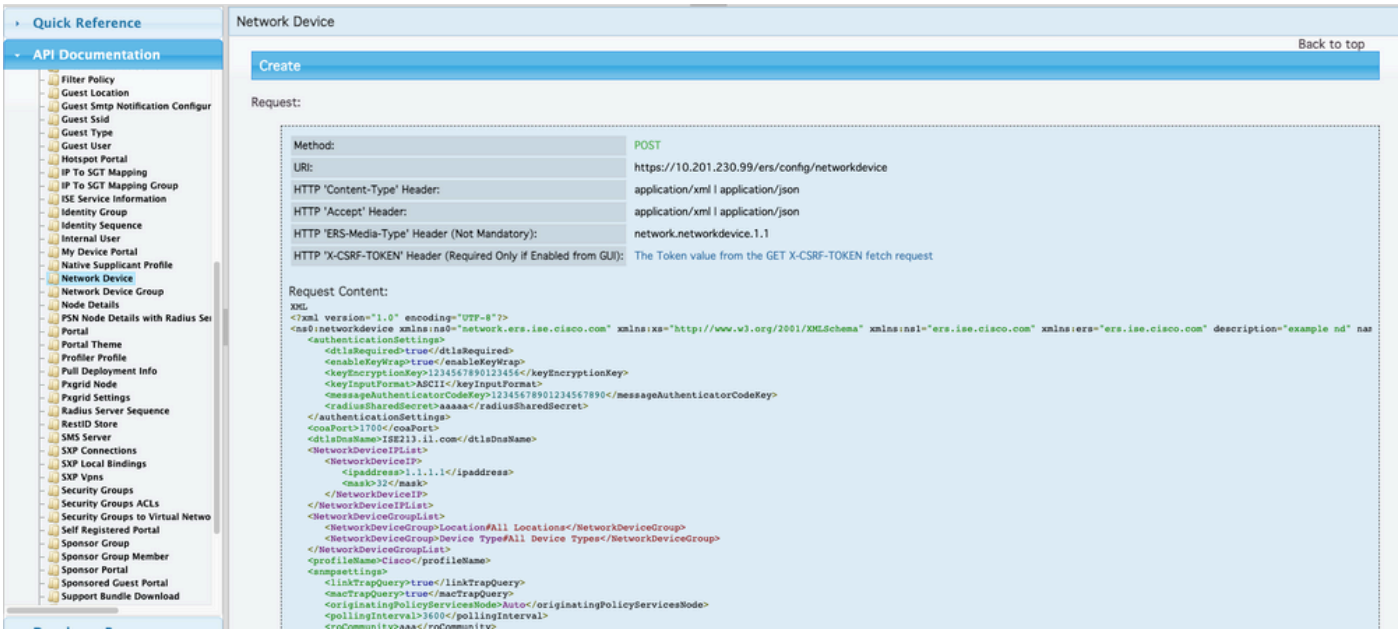
SDK do ISE e autorização de carteiro básico

Para configurar qualquer chamada, acesse primeiro o ISE ERS SDK (Software Developer Kit). Esta ferramenta compila toda a lista de chamadas de API que o ISE pode executar:

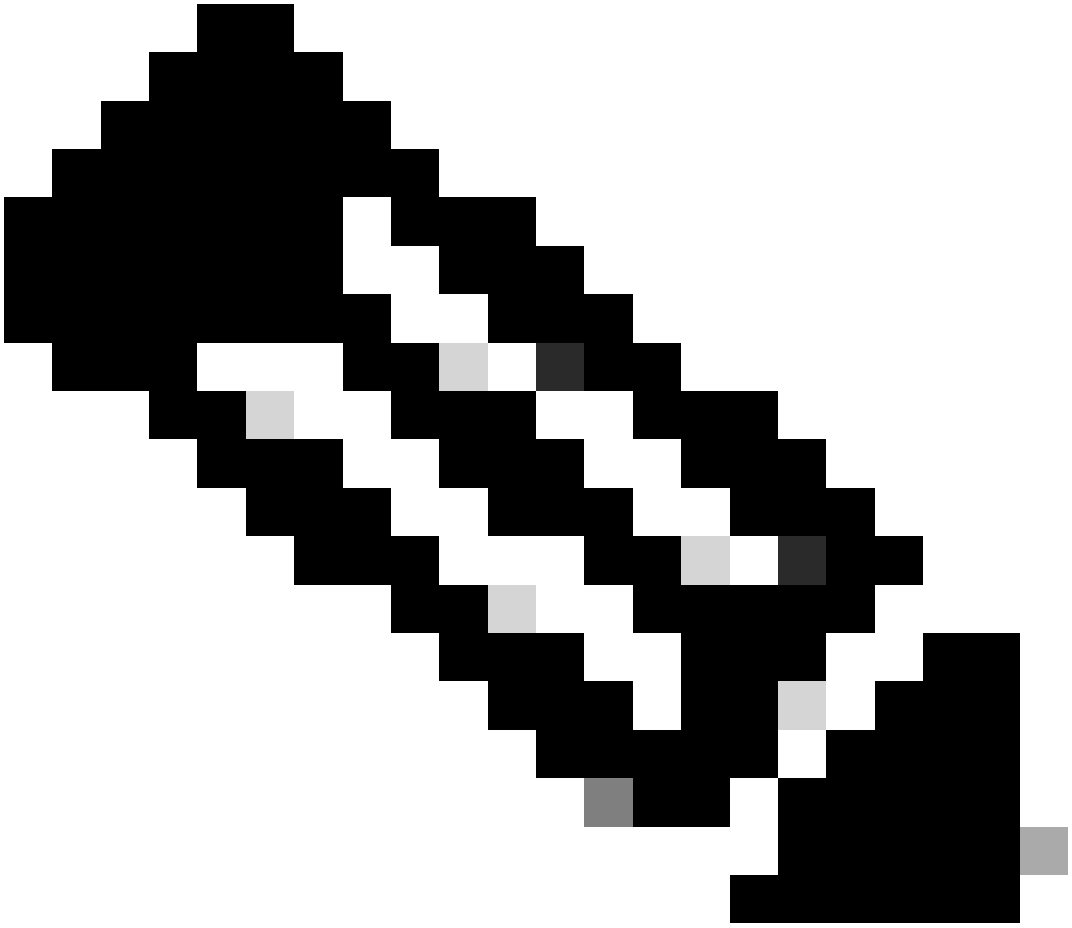
1. Navegue até https://{ise-ip}/ers/sdk.
2. Faça login usando suas credenciais de administrador do ISE.
3. Expanda a Documentação da API.
4. Role para baixo até encontrar Network Device e clique nele.
5. Nessa opção, você pode encontrar todas as operações disponíveis que pode executar para dispositivos de rede no ISE. Selecione Criar.



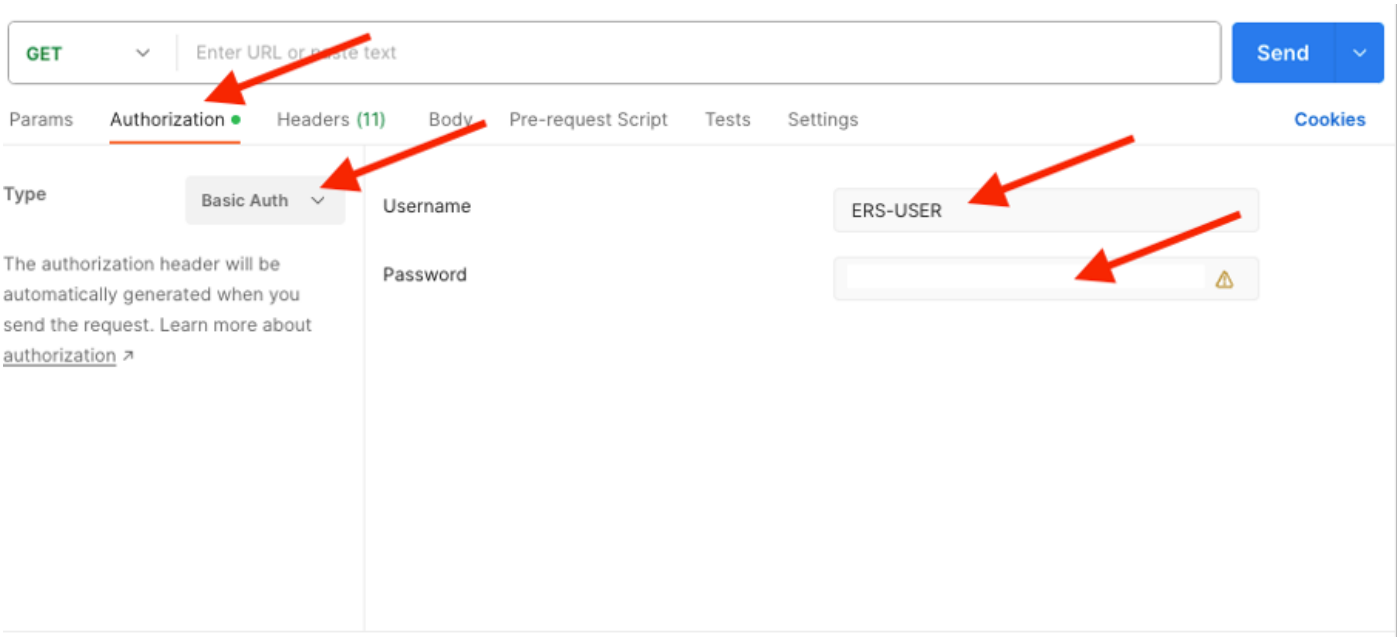
6. Agora você pode ver a configuração necessária para executar a chamada de API usando XML ou JSON em qualquer Cliente Rest, bem como um exemplo de resposta esperada.



7. Voltar para Postman configurar a autenticação básica para ISE. Na guia Authorization, selecione Basic Auth como o tipo de autenticação e adicione as credenciais do usuário do ISE ERS criadas anteriormente no ISE.



Observação: a senha é mostrada como texto claro, a menos que as variáveis sejam configuradas no Postman.

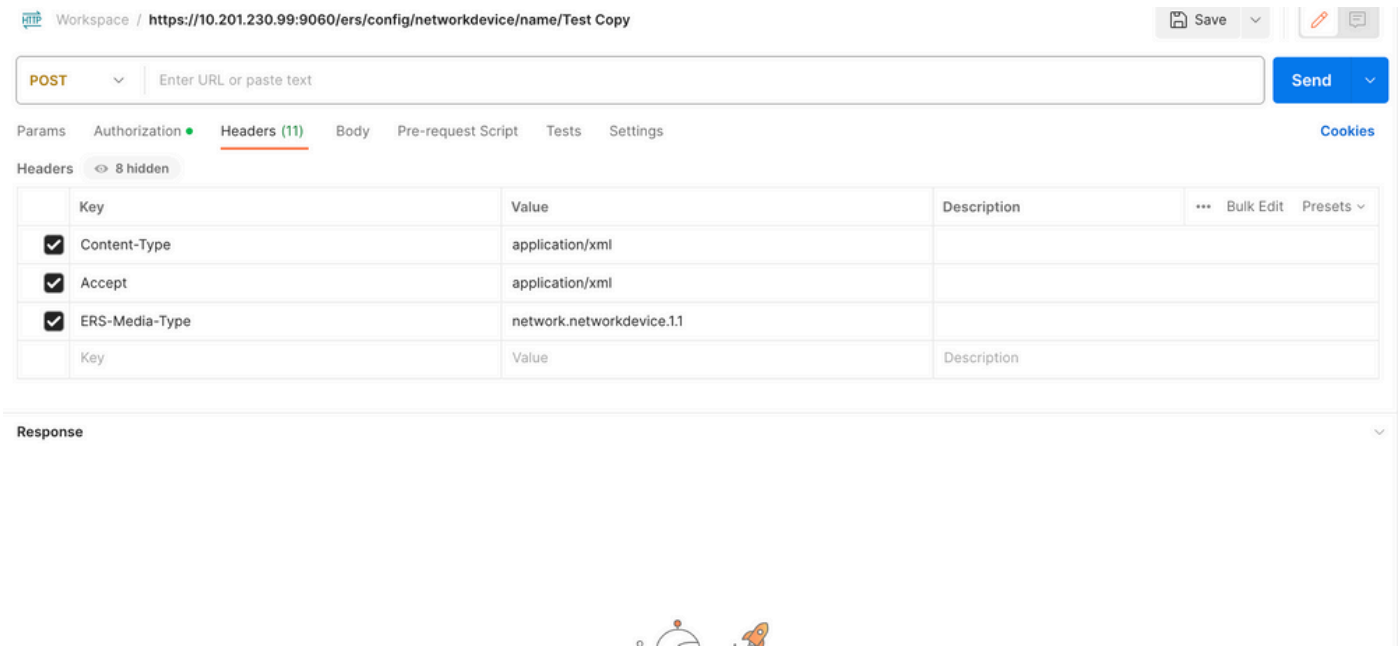


Criar NAD usando XML

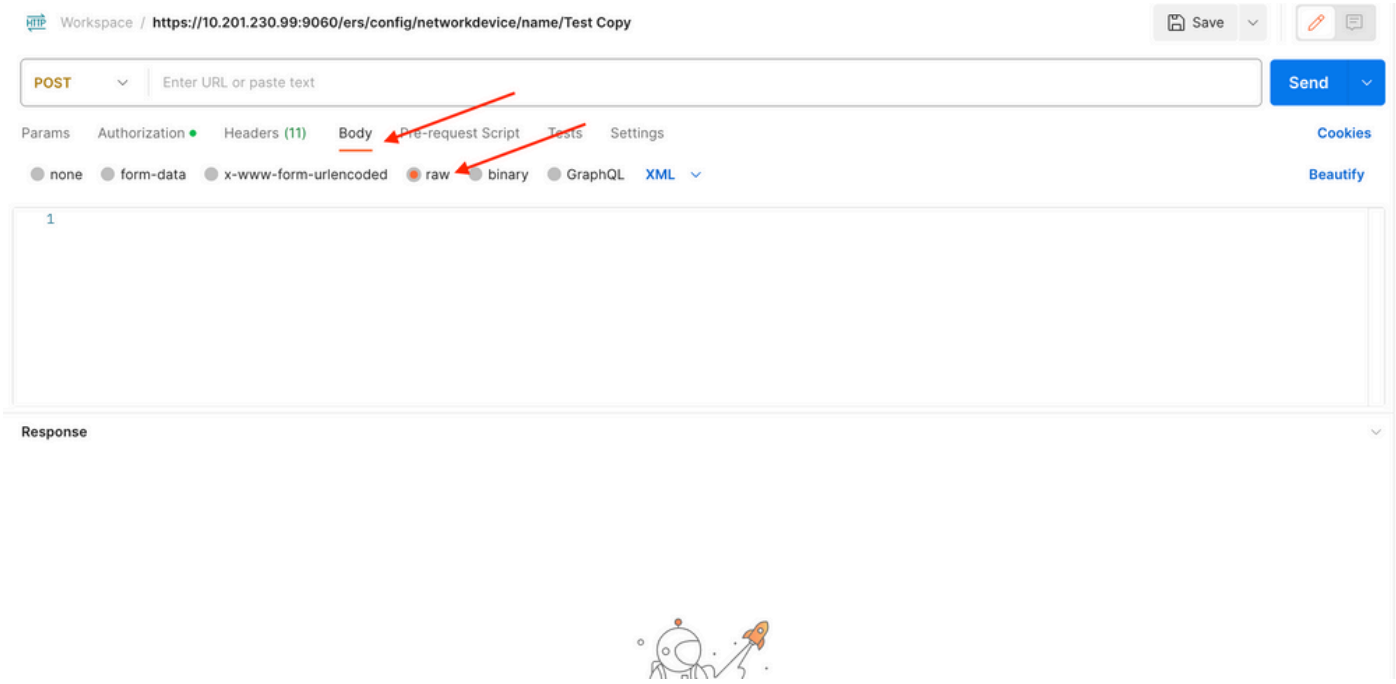
Crie TESTNAD1 com as configurações RADIUS TACACS, SNMP e TrustSec usando XML.

1. No SDK, em Criar, estão os cabeçalhos e modelos necessários para executar a chamada, bem como a resposta esperada.

2. Vá até a guia Cabeçalhos e configure os cabeçalhos necessários para a chamada de API conforme visto no SDK. A configuração do cabeçalho deve ser semelhante a esta:

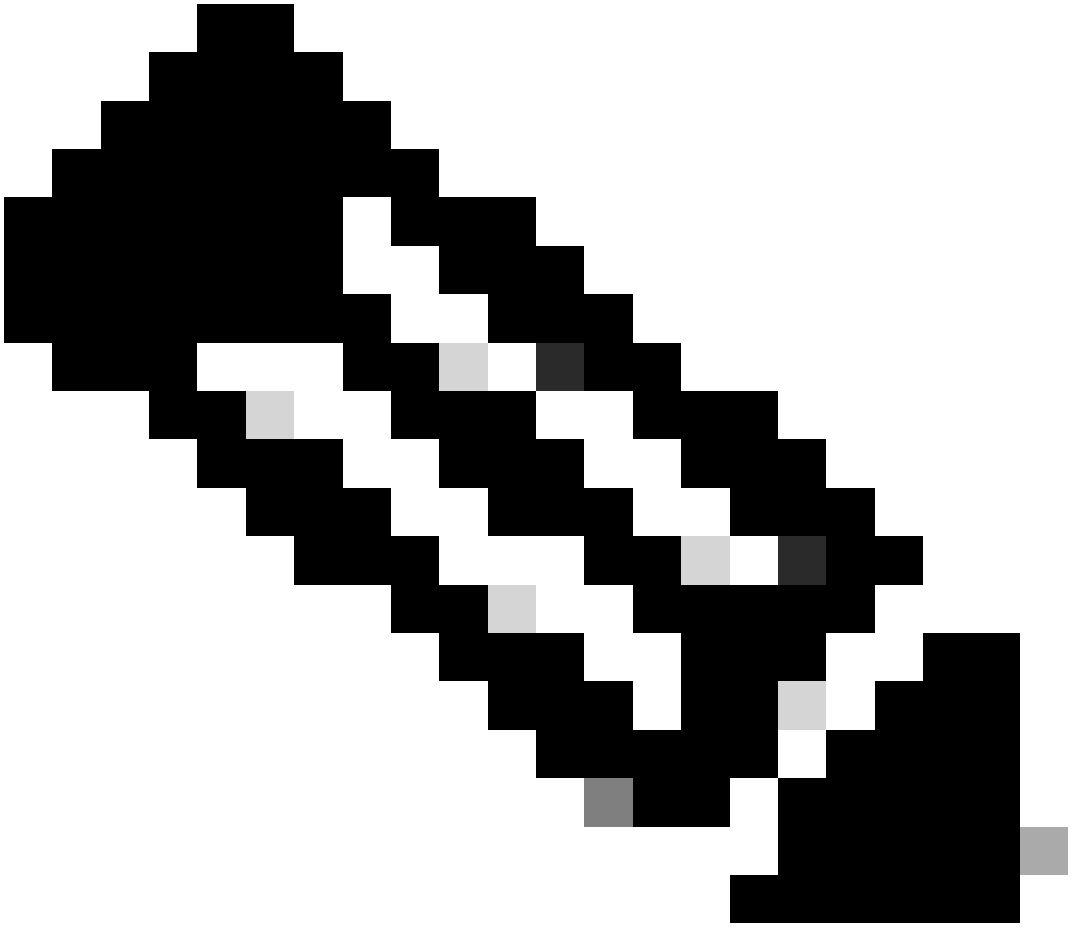


3. Vá até o cabeçalho Body e selecione raw. Isso permite colar o modelo XML necessário para criar o NAD.



4. O modelo XML é semelhante a este (altere os valores conforme necessário):

<?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>



Observação: é importante observar que as próximas linhas serão necessárias somente se **<enableKeyWrap>{false|true}</enableKeyWrap> for definido como true.** Caso contrário, o mesmo pode ser excluído do modelo XML:

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

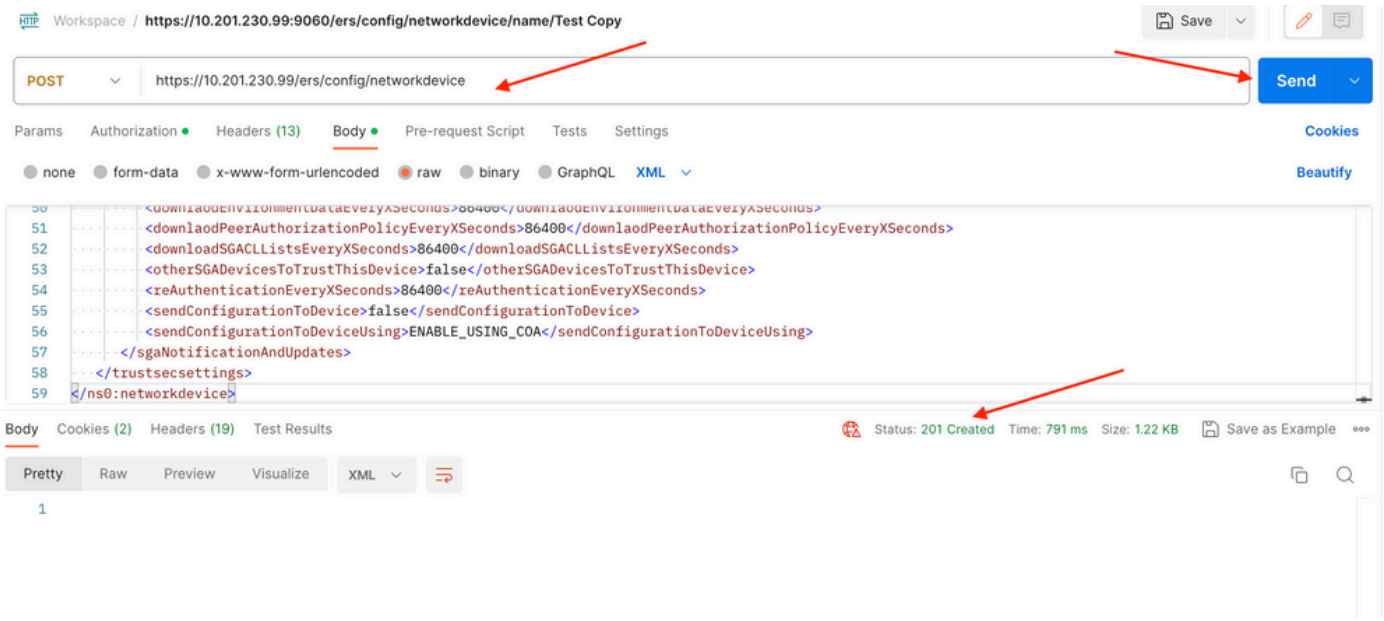
Você pode remover a configuração que não precisa do modelo e apenas deixar os dados que realmente precisam ser adicionados durante a criação do NAD. Como exemplo, aqui está o mesmo modelo, mas somente com a configuração TACACS. Independentemente da configuração necessária, certifique-se de que o modelo termine com **</ns0:networkdevice>.**

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

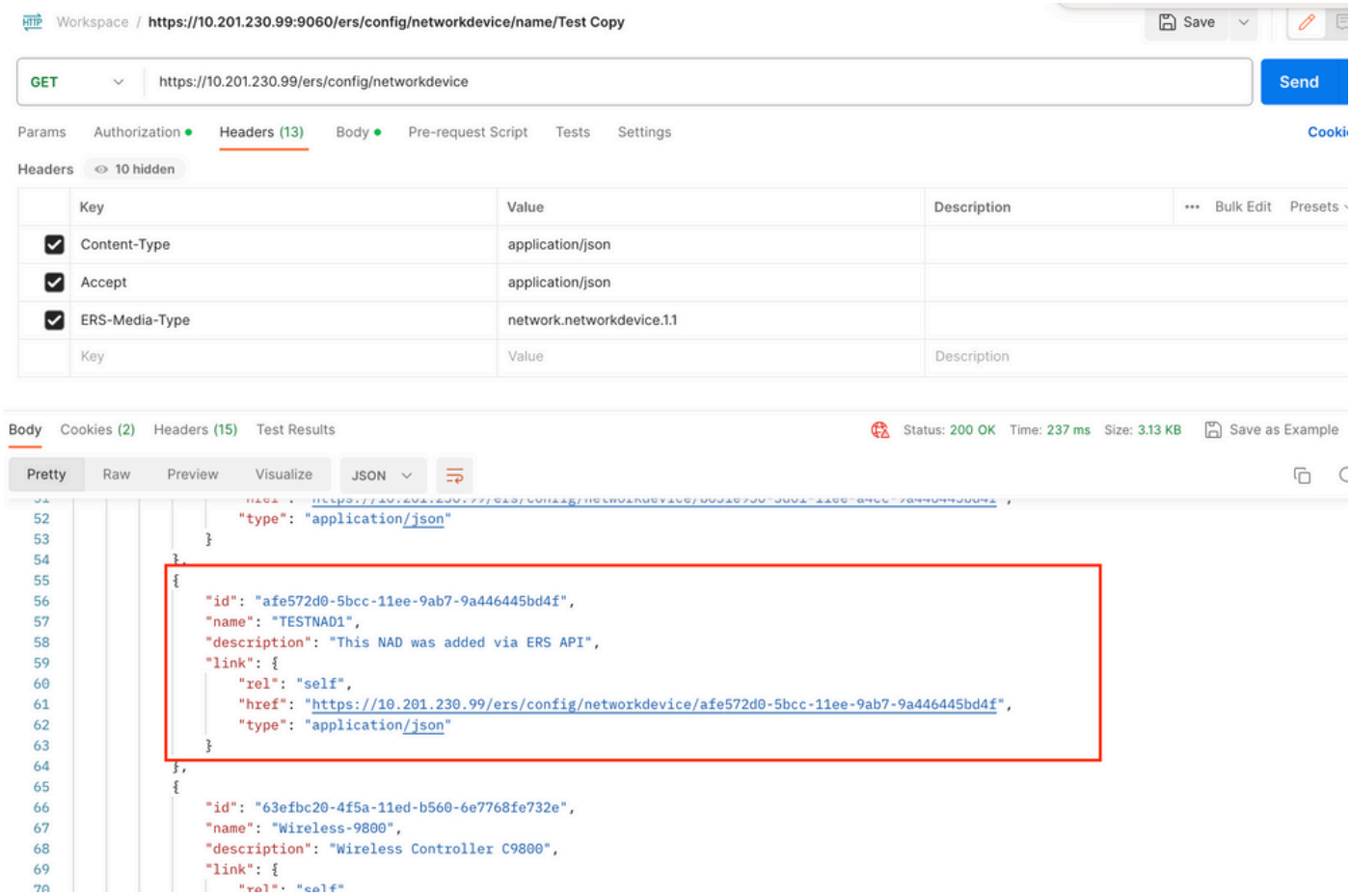
xmlns:ns1="ers.ise.cisco.com" xmlns:ers="ers.ise.cisco.com" description="**This NAD was added via ERS API**" name="**TESTNAD1**"> <NetworkDeviceIPList> <NetworkDeviceIP> <ipaddress>**NAD IP Address**</ipaddress> <mask>**32**</mask> </NetworkDeviceIP> </NetworkDeviceIPList> <NetworkDeviceGroupList> <NetworkDeviceGroup>Location#All 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>

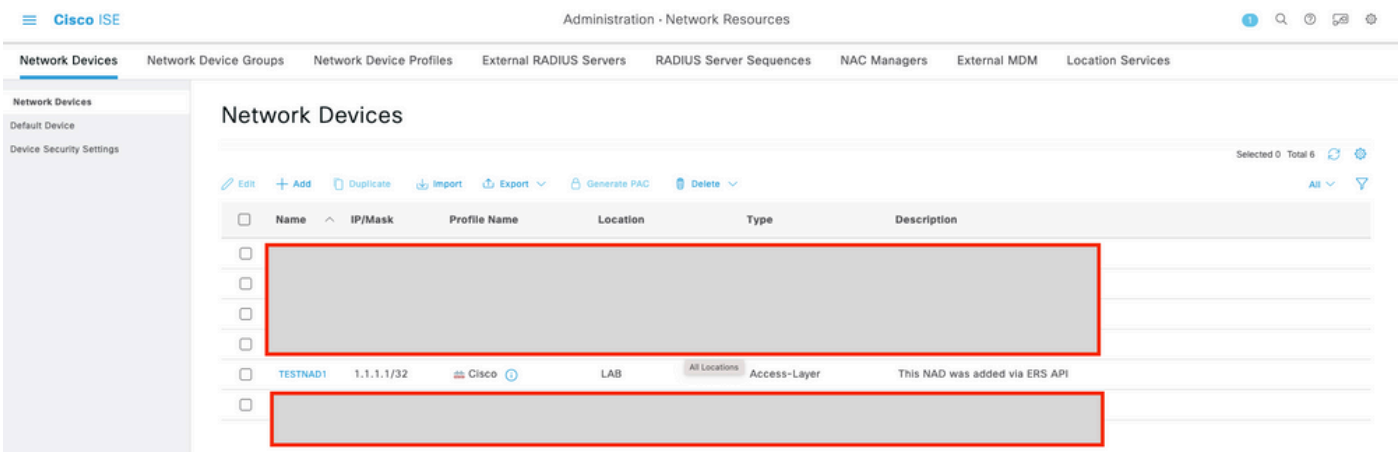
5. Cole o modelo XML para **raw** no cabeçalho **Body**.

6. Selecione **POST** como o método, cole https://{ISE-ip}/ers/config/networkdevice e clique em Send. **Se tudo tiver sido configurado corretamente, você deverá ver uma mensagem 201 Created** e o resultado vazio.



7. Confirme se o NAD foi criado executando uma **chamada GET** para o NAD ou verificando a lista ISE NAD.



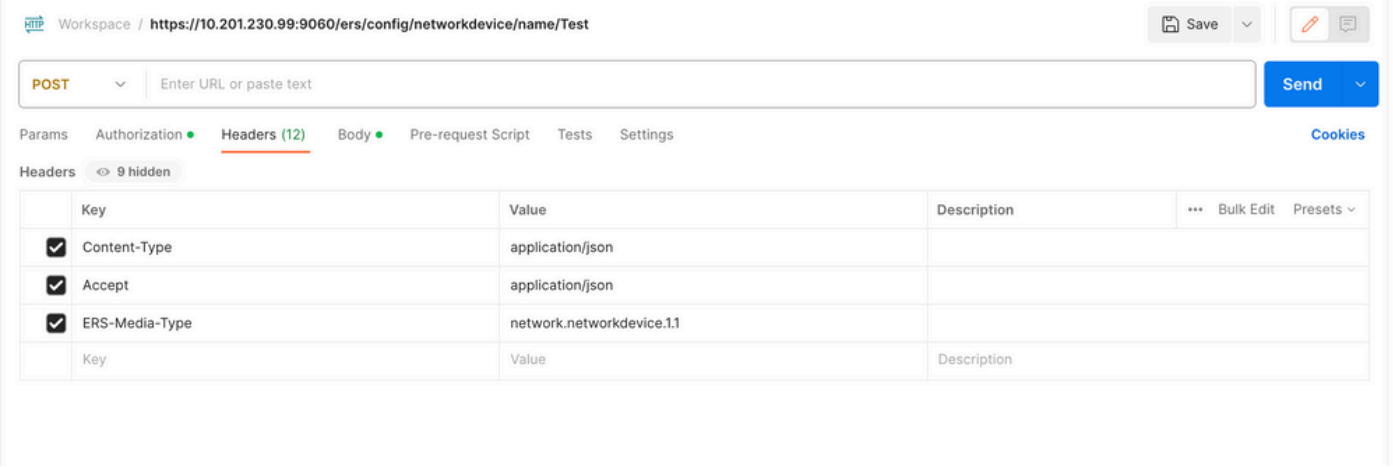


Criar NAD usando JSON

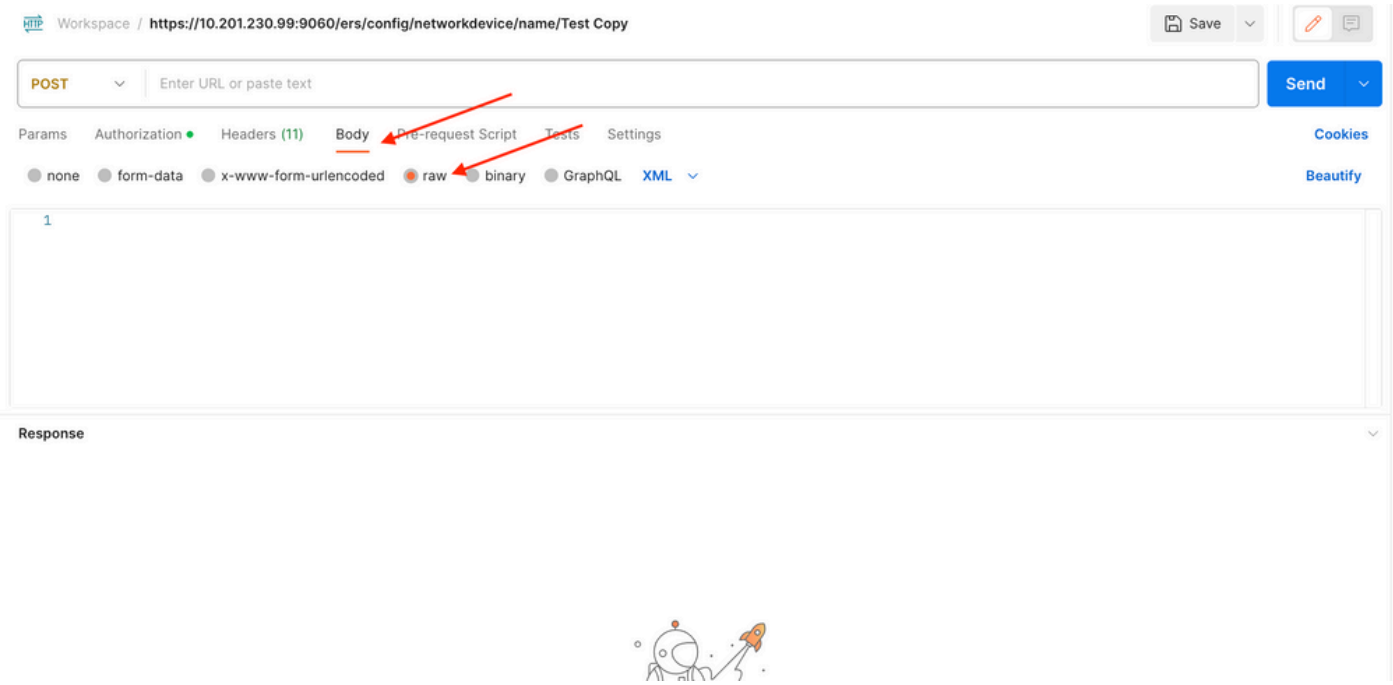
Crie TESTNAD2com as configurações RADIUS TACACS, SNMP e TrustSec usando JSON.

1. No SDK, em **Criar,** estão os cabeçalhos e modelos necessários para executar a chamada, bem como a resposta esperada.

2. Vá até a guia **Cabeçalhos** e configure os cabeçalhos necessários para a chamada de API conforme visto no SDK. A configuração do cabeçalho deve ser semelhante a esta:

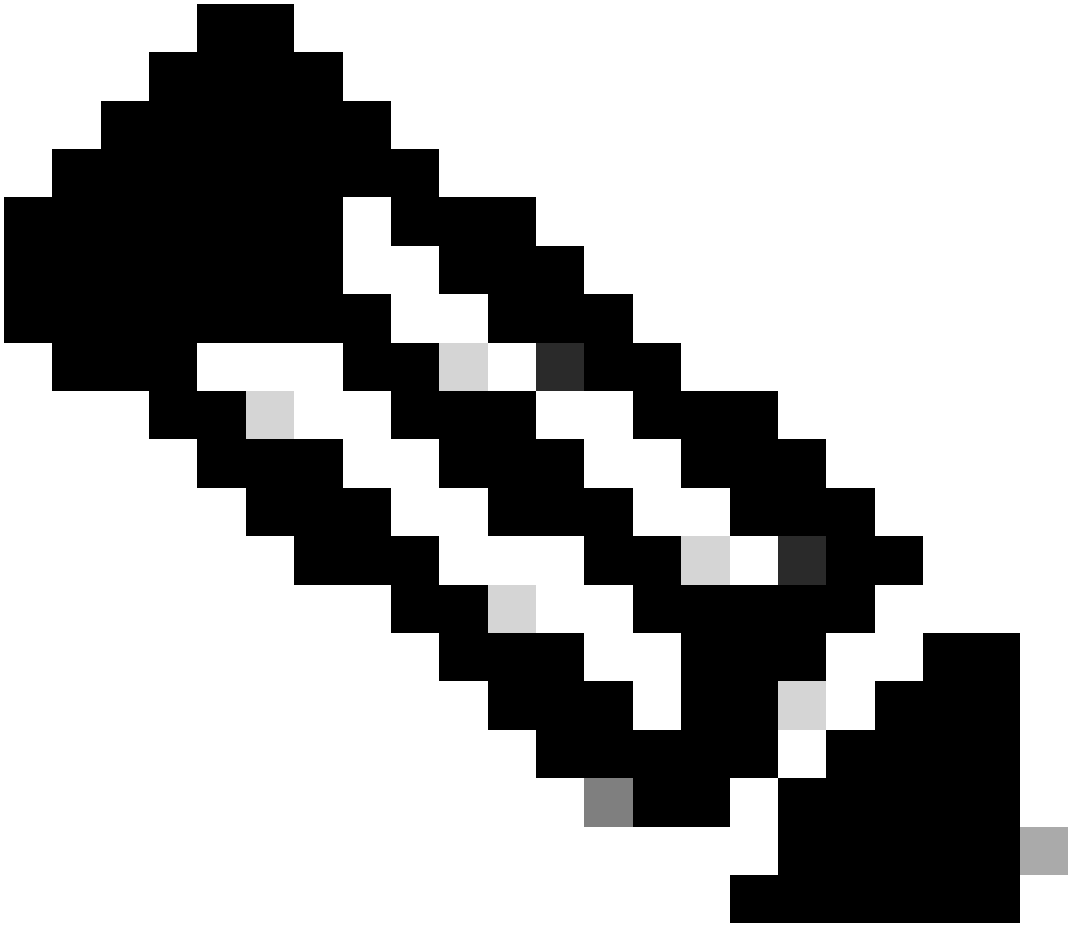


3. Vá até o cabeçalho **Body** e selecione **raw**. Isso permite colar o modelo JSON necessário para criar o NAD.



4. O modelo JSON deve ter esta aparência (altere os valores conforme necessário):

{ "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"] } }

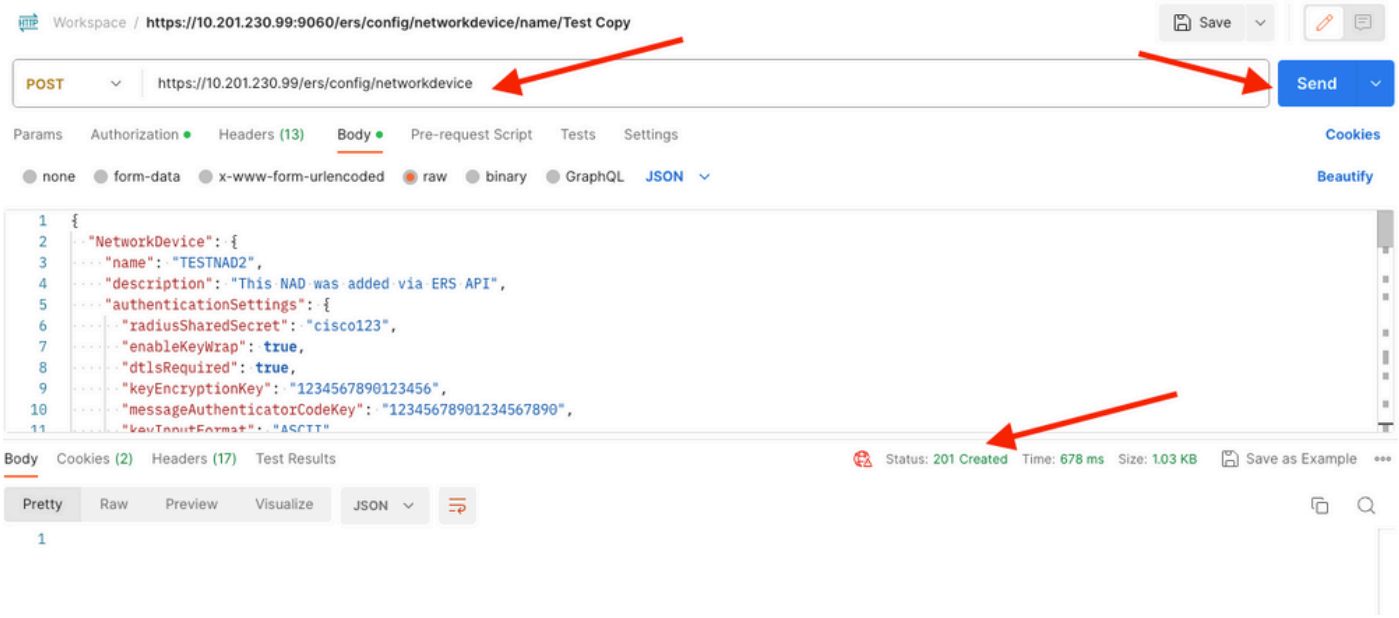


Observação: é importante observar que as próximas linhas serão necessárias somente se **enableKeyWrap":{false|true}**, for definido como **true**. Caso contrário, o mesmo pode ser excluído do modelo JSON:

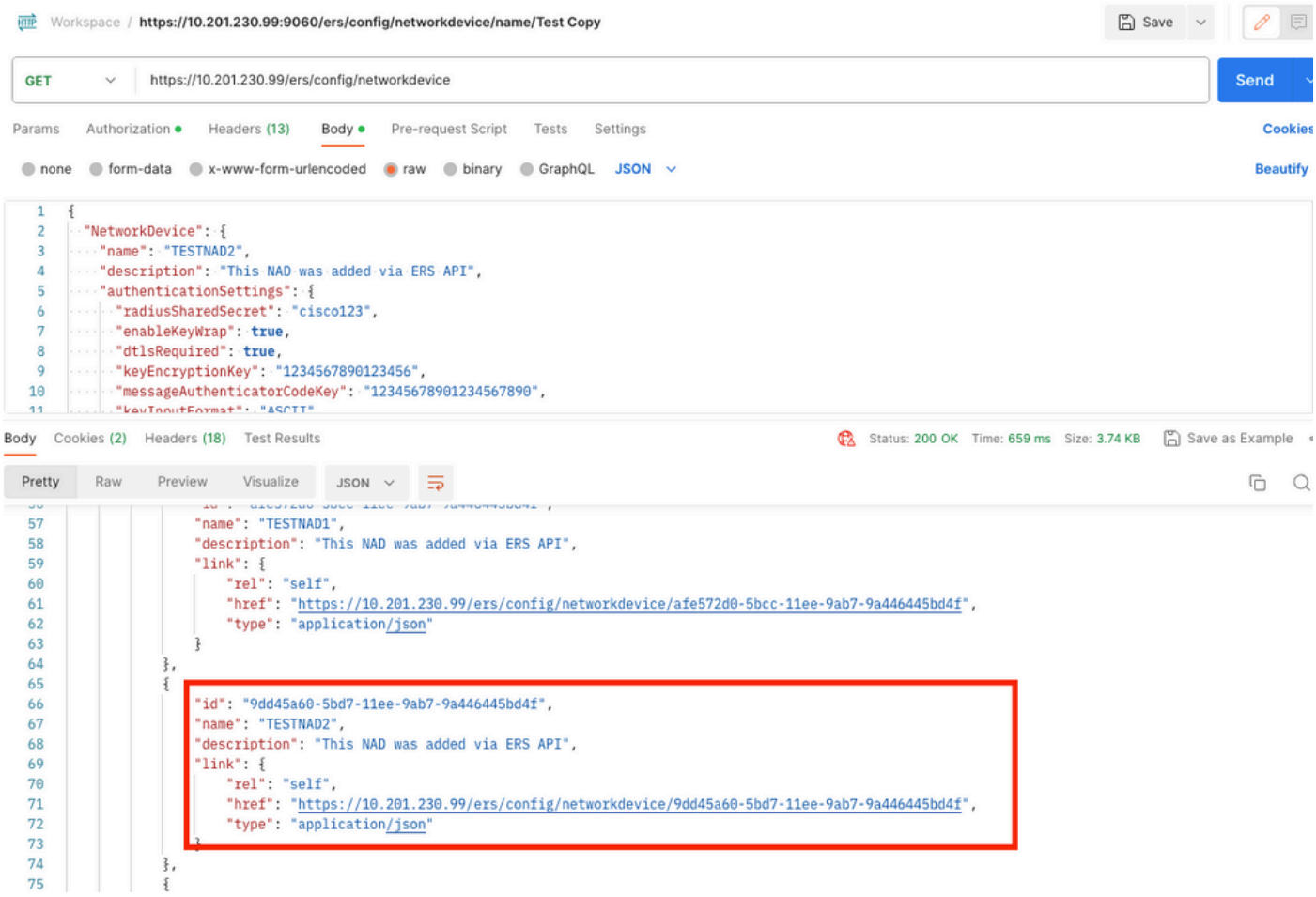
"keyEncryptionKey": "**1234567890123456**", "messageAuthenticatorCodeKey": "**12345678901234567890**", "keyInputFormat": "**ASCII**" Você também pode remover a configuração que não precisa do modelo e apenas deixar os dados que realmente precisam ser adicionados durante a criação do NAD.

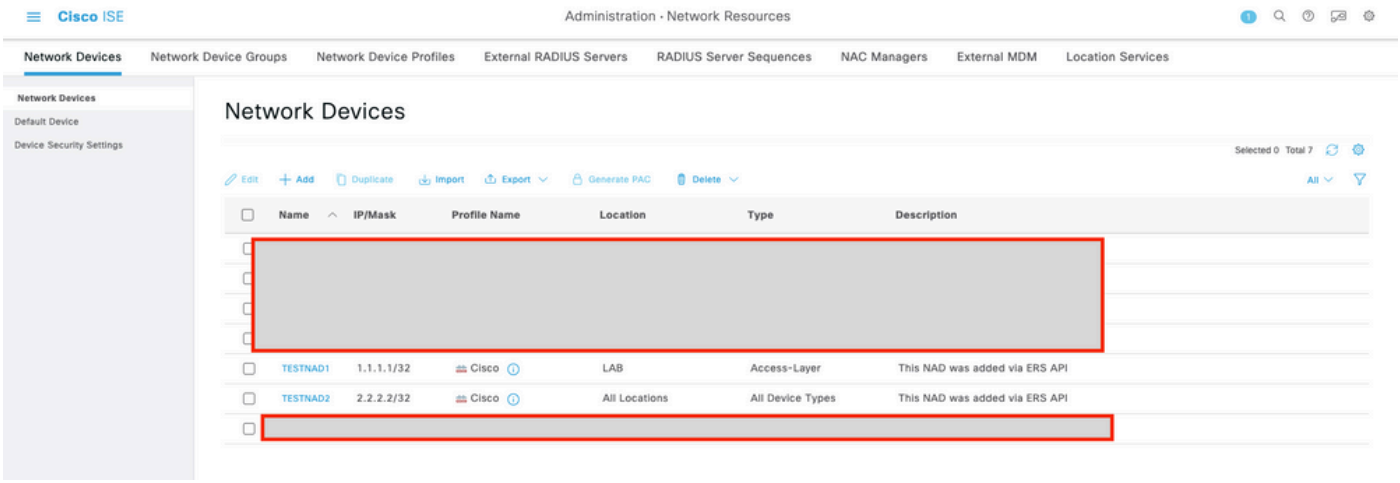
5. Cole o modelo JSON para **raw** no cabeçalho **Body**.

6. Selecione **POST** como o método, cole https://{ISE-ip}/ers/config/networkdevice e clique em Send. **Se tudo tiver sido configurado corretamente, você deverá ver uma mensagem 201 Created** e o resultado vazio.



7. Confirme se o NAD foi criado executando uma chamada GET para o NAD ou verificando a lista ISE NAD.





Verificar

Se você puder acessar a página da GUI do serviço de API, por exemplo, **https://*{iseip}*:*{port}*/api/swagger-ui/index.html** ou **https://**{iseip}**:9060/ers/sdk**, isso significa que o serviço de API está funcionando conforme esperado.

Troubleshooting

- Todas as operações REST são auditadas e os registros são registrados nos registros do sistema.

- Para solucionar problemas relacionados às APIs abertas, defina o **Nível de Log** do componente **apiservice** como **DEBUG** na janela **Configuração do Log de Depuração**.

- Para solucionar problemas relacionados às APIs ERS, defina o **Nível de Log** do componente **ers** como **DEBUG** na janela **Debug Log Configuration**. Para visualizar essa janela, navegue até a GUI do Cisco ISE, clique no ícone Menu e escolha **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**.

- Você pode fazer o download dos logs na janela **Download** Logs. Para visualizar essa janela, navegue até a GUI do Cisco ISE, clique no ícone **Menu** e escolha **Operações > Solução de problemas > Logs de download**.

- Você pode optar por fazer download de um pacote de suporte na guia Pacote de suporte clicando no botão **Download** na guia, ou fazer download dos logs de depuração do api-service na guia Logs de depuração clicando no valor do Arquivo de log para o log de depuração do api-service.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.