

Configurar usuários internos por meio de chamadas JSON ou XML e API no ISE 3.3 com Insominia

Contents

Introdução

Este documento descreve a configuração de usuários internos no Cisco ISE, aproveitando os formatos de dados JSON ou XML em conjunto com chamadas de API.

Pré-requisitos

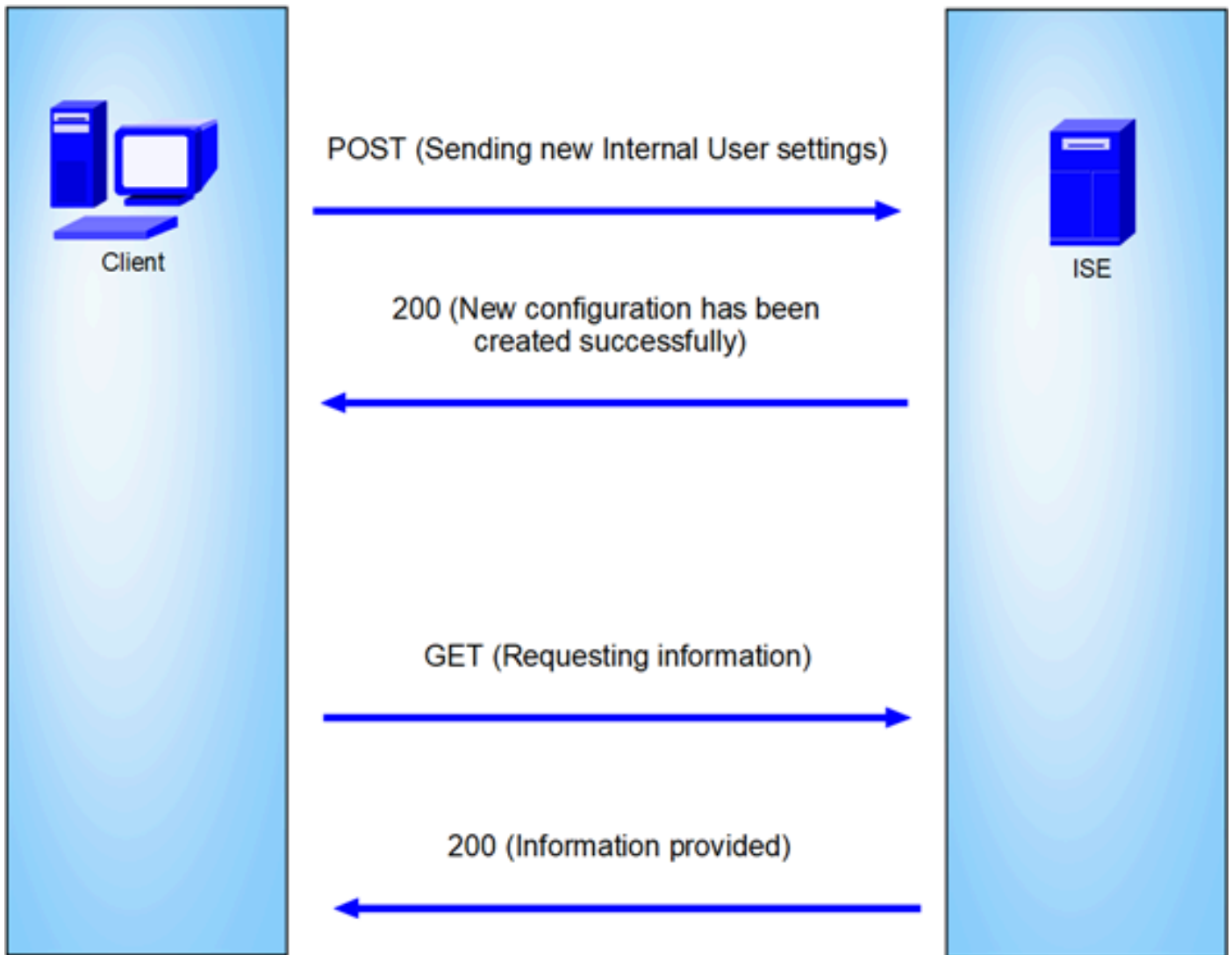
- ISE 3.0 ou posterior.
- Software de cliente API.

Componentes Utilizados

- ISE 3.3
- Insominia 9.3.2

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.

Diagrama de Rede



Topologia geral

GET e POST são dois dos métodos HTTP mais comuns usados em chamadas de API (Application Programming Interface). Eles são usados para interagir com recursos em um servidor, geralmente para recuperar dados ou enviar dados para processamento.

Chamada à API GET

O método GET é usado para solicitar dados de um recurso especificado. As solicitações GET são os métodos mais comuns e amplamente usados em APIs e sites. Quando você visita uma página da Web, o navegador faz uma solicitação GET ao servidor que hospeda a página da Web.

Chamada API POST

O método POST é usado para enviar dados ao servidor para criar ou atualizar um recurso. As solicitações POST são frequentemente usadas ao enviar dados de formulário ou ao carregar um arquivo.

Configurações

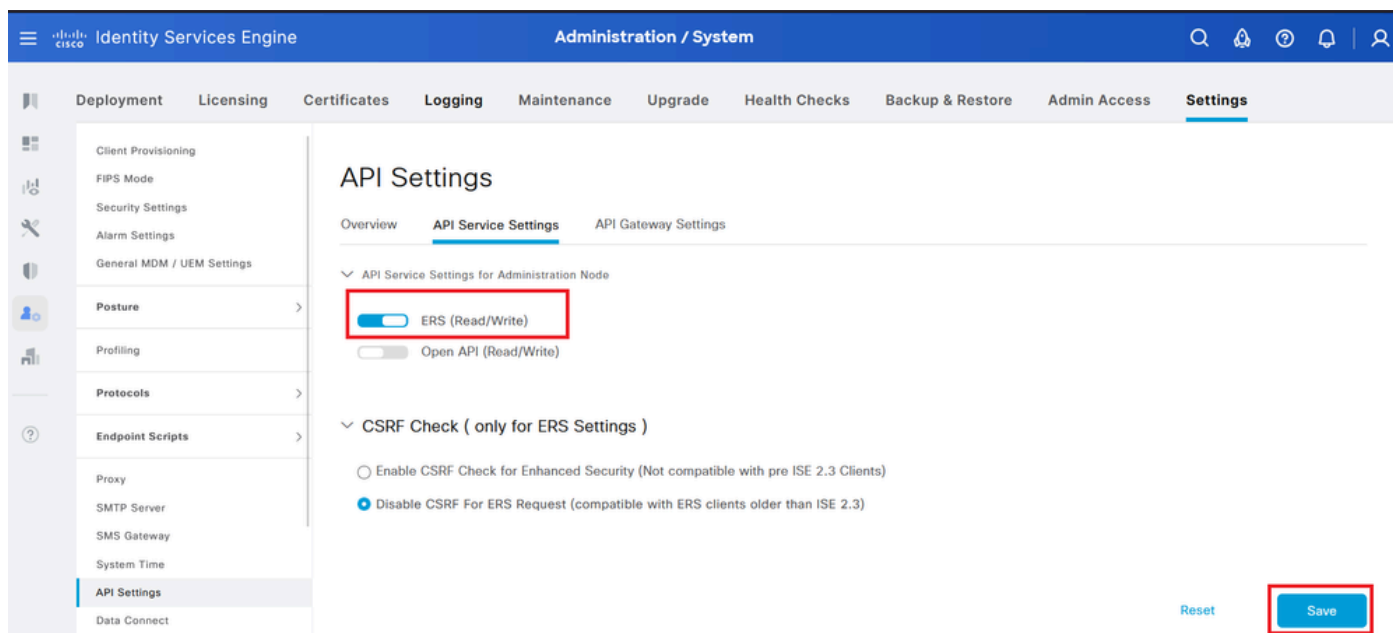
Precisamos enviar as informações exatas do software cliente API para o nó ISE para criar um usuário interno.

Configurações do ISE

Ativar a funcionalidade ERS.

1. Navegue até Administração > Sistema > Configurações > Configurações de API > Configurações de Serviço de API.

2. Ative a opção ERS (Read/Write).



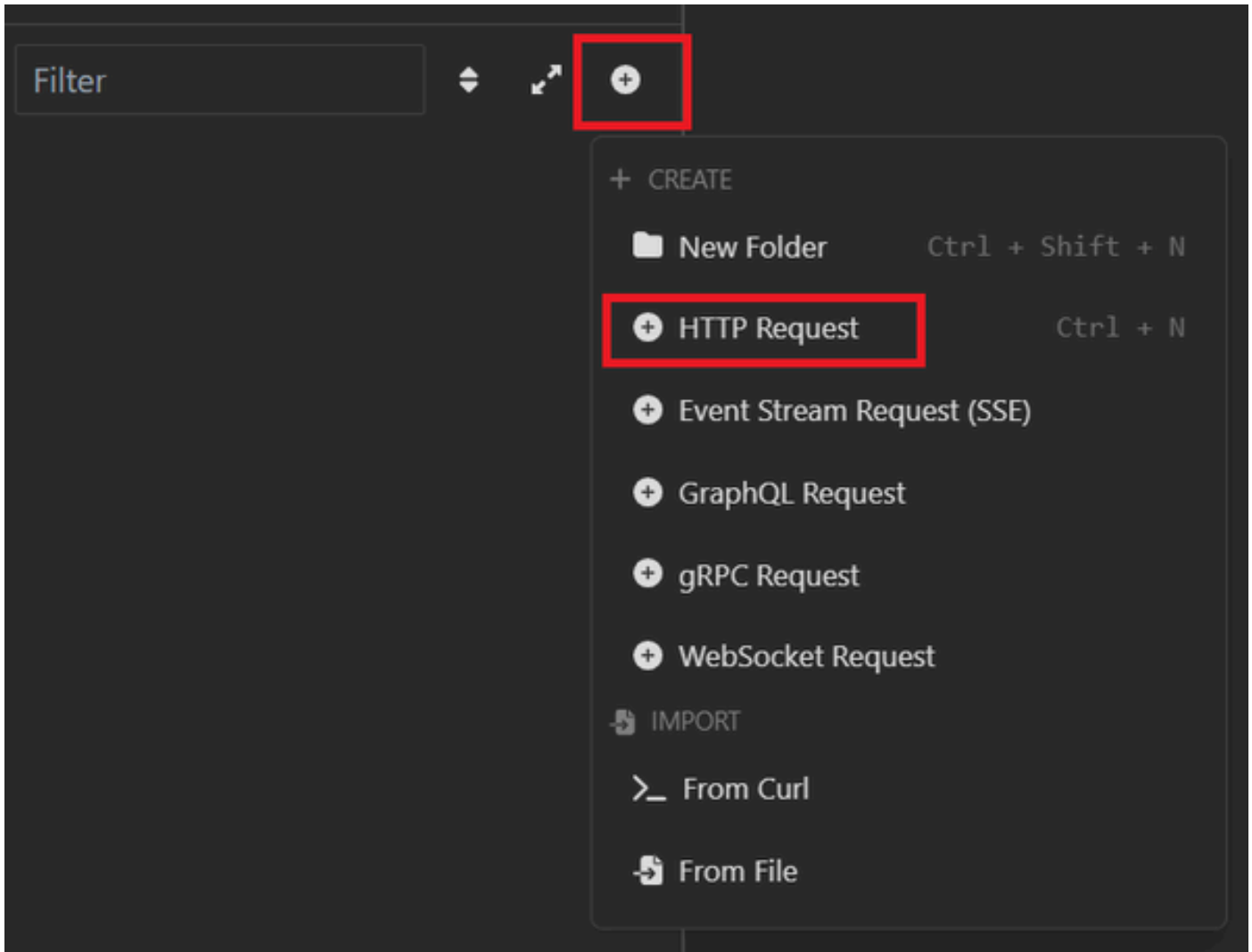
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Administration / System' and various utility icons. The main navigation menu on the left lists categories like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The 'Settings' menu is expanded, showing options such as Client Provisioning, FIPS Mode, Security Settings, Alarm Settings, General MDM / UEM Settings, Posture, Profiling, Protocols, Endpoint Scripts, Proxy, SMTP Server, SMS Gateway, System Time, API Settings, and Data Connect. The 'API Settings' page is displayed, with tabs for Overview, API Service Settings, and API Gateway Settings. Under 'API Service Settings for Administration Node', the 'ERS (Read/Write)' toggle is turned on and highlighted with a red box. Below it, the 'Open API (Read/Write)' toggle is turned off. Under 'CSRF Check (only for ERS Settings)', the 'Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)' radio button is selected. At the bottom right, there are 'Reset' and 'Save' buttons, with the 'Save' button highlighted by a red box.

Configurações de API

solicitação JSON.

1. Insônia Aberta.

2. Adicione uma nova solicitação HTTPS no lado esquerdo.

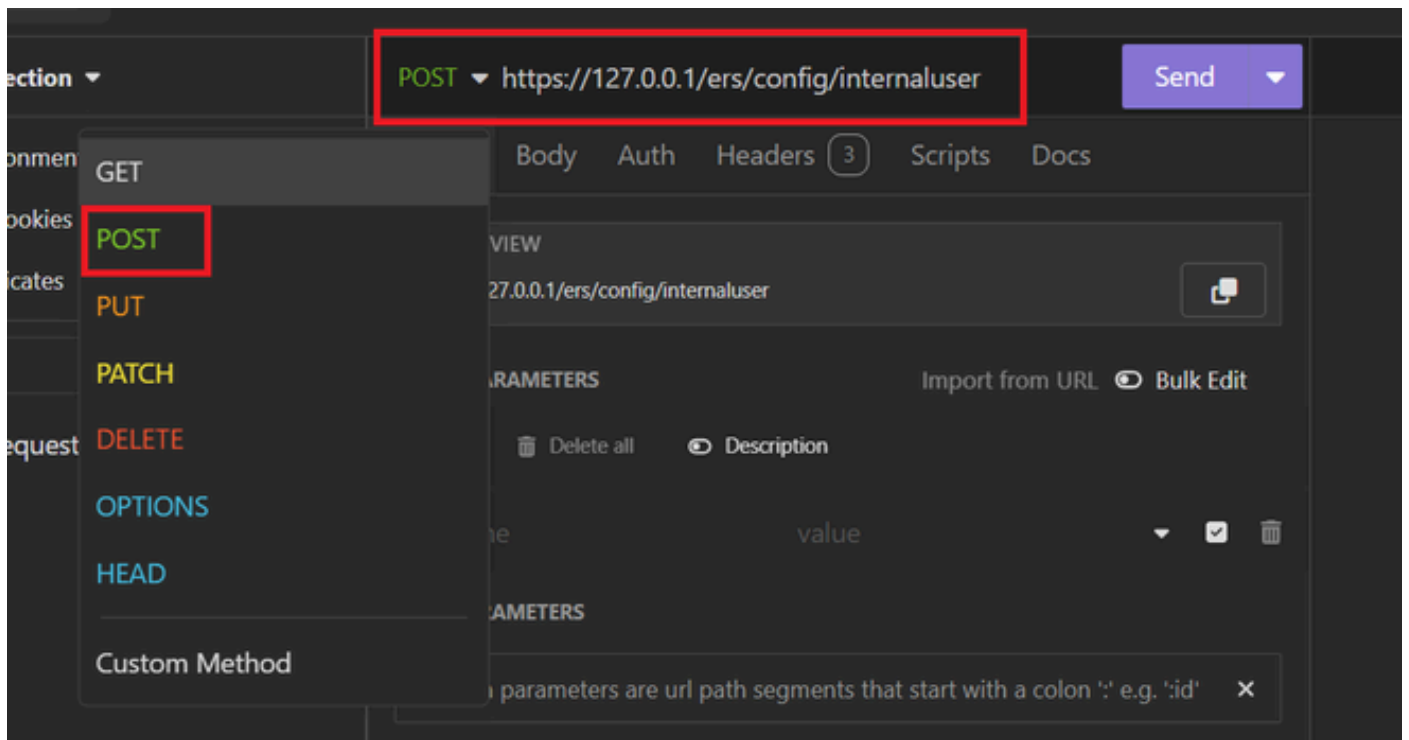


Solicitação JSON

3. Você precisa escolher POST para enviar as informações ao nó ISE.

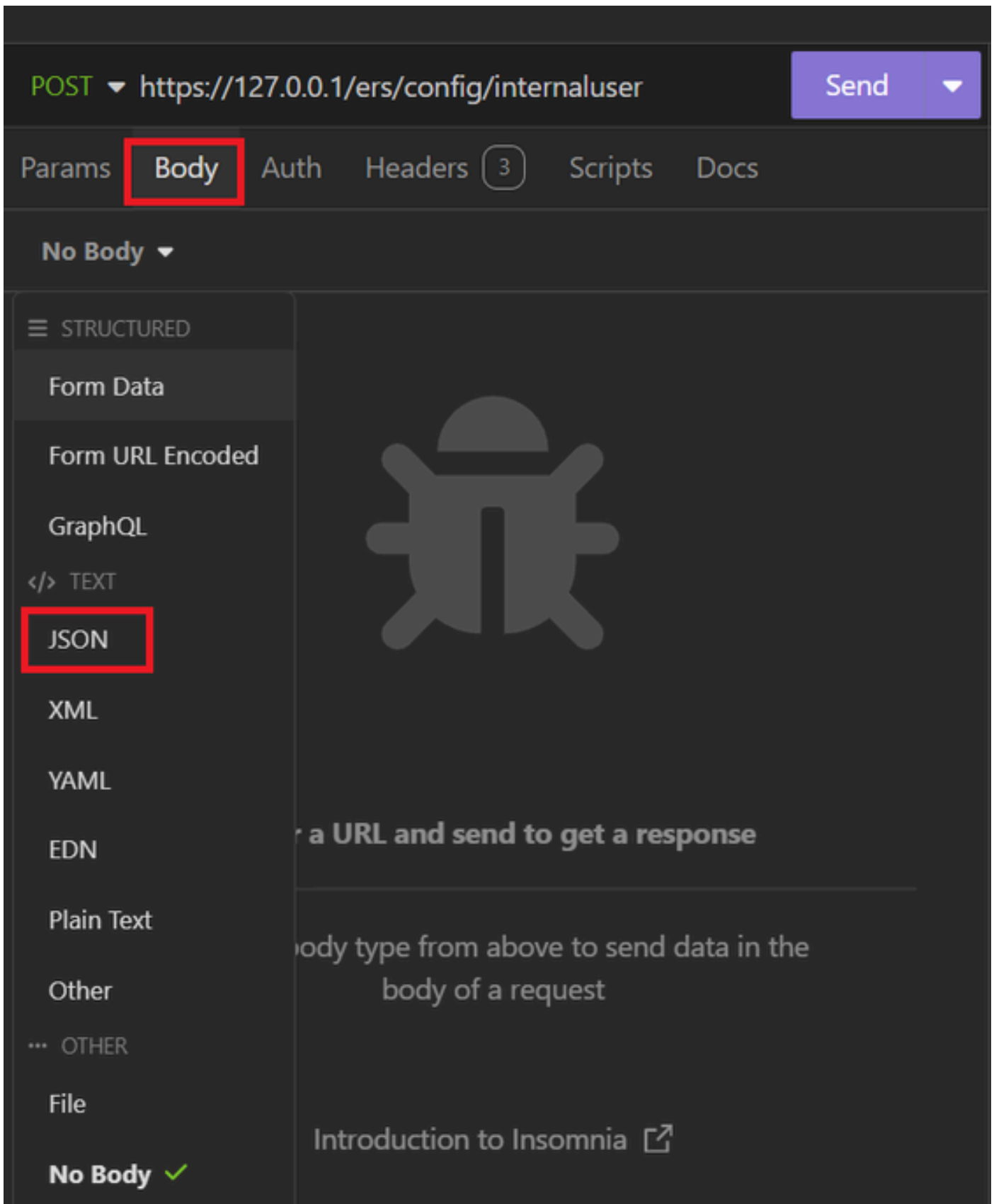
O URL que você precisa inserir depende do endereço IP do nó do ISE.

URL: <https://x.x.x.x/ers/config/internaluser>



POSTAGEM JSON

4. Em seguida, clique em Corpo e escolha JSON



Corpo JSON

5. Você pode colar a sintaxe e alterar os parâmetros dependendo do que deseja.

```
POST https://127.0.0.1/ers/config/internaluser Send
Params Body Auth Headers 4 Scripts Docs
JSON
1
2 {
3   "InternalUser": {
4     "name": "User01",
5     "description": "this is the first user account",
6     "enabled": true,
7     "email": "user1@local.com",
8     "accountNameAlias": "User 001",
9     "password": "bWn4hehq8ZCV1rk",
10    "firstName": "User",
11    "lastName": "Cisco",
12    "changePassword": true,
13    "identityGroups": "a1740510-8c01-11e6-996c-525400b48521",
14    "passwordNeverExpires": false,
15    "daysForPasswordExpiration": 60,
16    "expiryDateEnabled": false,
17    "expiryDate": "2026-12-11",
18    "enablePassword": "bWn4hehq8ZCV22k",
19    "dateModified": "2024-7-18",
20    "dateCreated": "2024-7-18",
21    "passwordIDStore": "Internal Users"
22  }
23 }
```

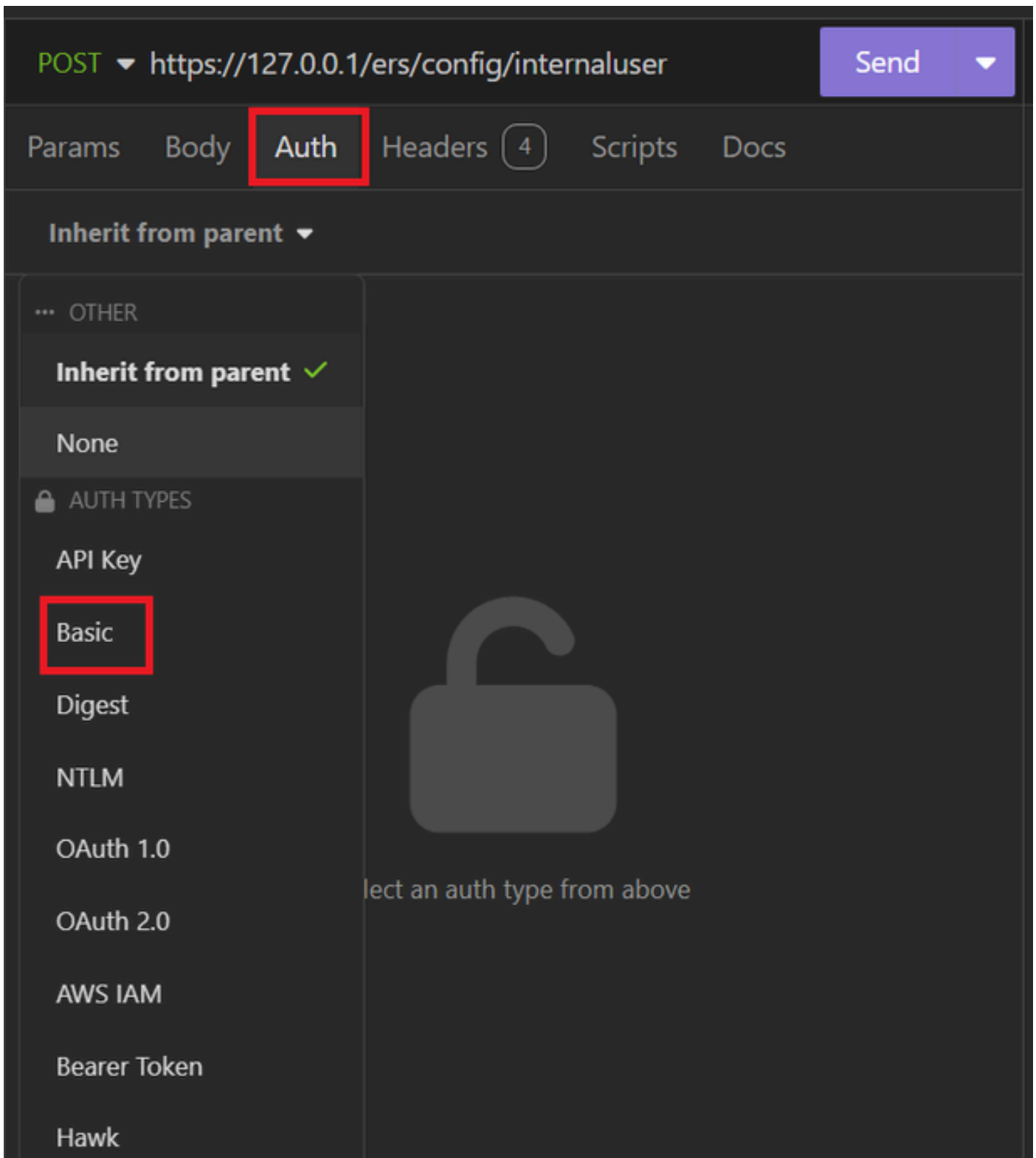
Sintaxe JSON

sintaxe JSON

```
{
  "InternalUser": {
    "name": "name",
    "description": "description",
    "enabled": true,
    "email": "email@domain.com",
    "accountNameAlias": "accountNameAlias",
```

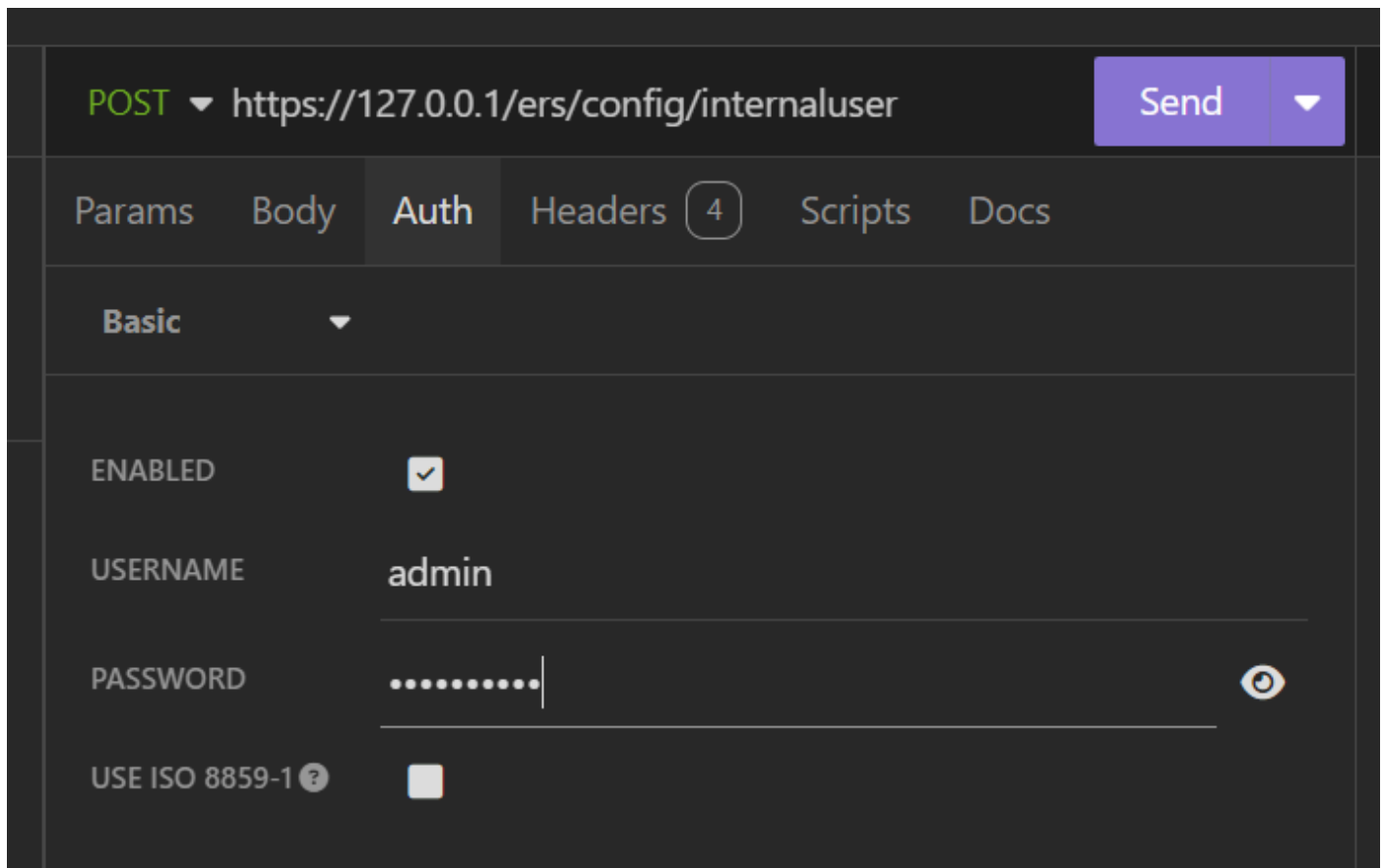
```
"password": "password",
"firstName": "firstName",
"lastName": "lastName",
"changePassword": true,
"identityGroups": "identityGroups",
"passwordNeverExpires": false,
"daysForPasswordExpiration": 60,
"expiryDateEnabled": false,
"expiryDate": "2016-12-11",
"enablePassword": "enablePassword",
"dateModified": "2015-12-20",
"dateCreated": "2015-12-15",
"customAttributes": {
  "key1": "value1",
  "key2": "value3"
},
"passwordIDStore": "Internal Users"
}
}
```

6. Clique em Auth e escolha Basic.



autenticação JSON

7. Insira as credenciais da GUI do ISE.



Credenciais JSON de administração

8. Clique em Cabeçalhos para adicionar os próximos métodos:
- Tipo de conteúdo: aplicativo/json
 - Aceitar: application/json

POST ▼ https://127.0.0.1/ers/config/internaluser Send ▼

Params Body Auth **Headers** 4 Scripts Docs

+ Add 🗑 Delete all 👁 Description

Accept */*

Host <calculated at runtime>

☰	Content-Type	application/json	▼	☑	🗑
☰	Accept	application/json	▼	☑	🗑

Cabeçalhos JSON

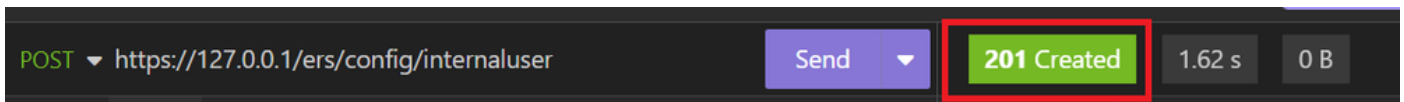
9. Finalmente, clique em Enviar.



Observação: se quiser atribuir um Grupo de Identidade à nova conta de usuário, você precisará usar o ID do Grupo de Identidade. Verifique a **seção Solução de problemas** para obter mais informações.

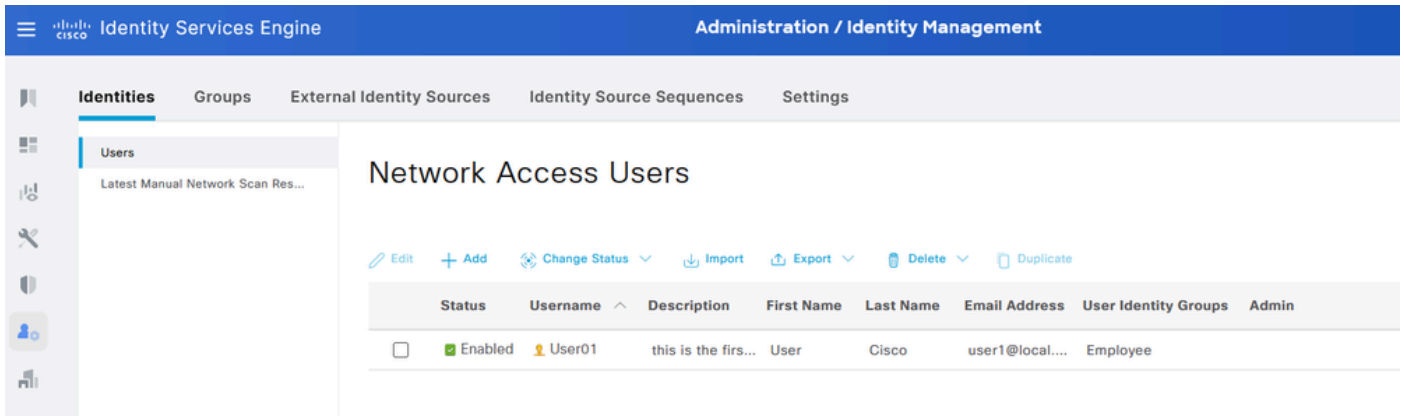
Validação

1. Após enviar a solicitação POST você verá o status "201 Criado". Isso significa que o processo foi concluído com êxito.



Solicitação JSON bem-sucedida

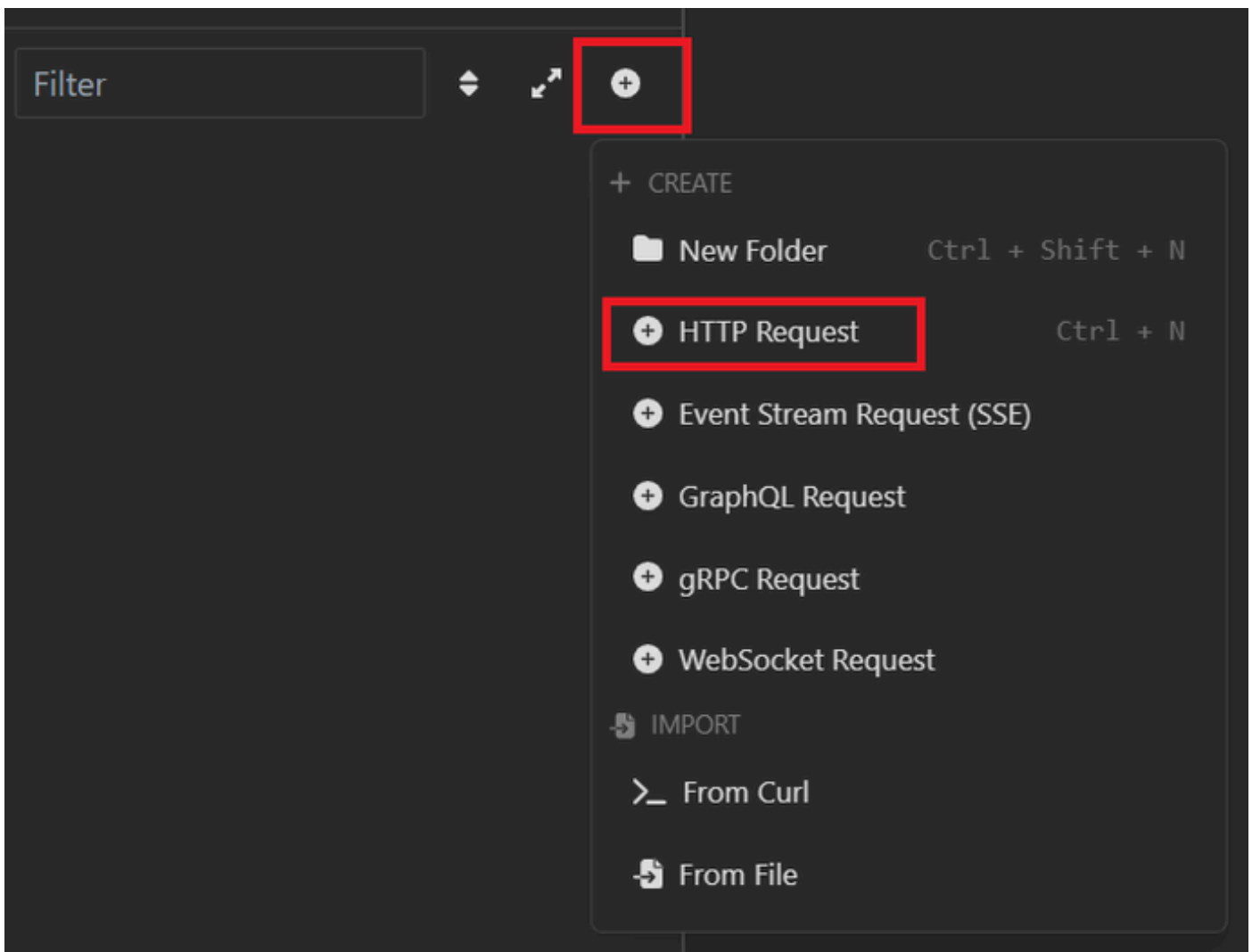
2. Abra a GUI do ISE e navegue até Administração > Gerenciamento de identidades > Identidades > Usuários > Usuários de acesso à rede



Conta de usuário JSON

solicitação XML

1. Insônia Aberta.
2. Adicione uma nova solicitação HTTPS no lado esquerdo.

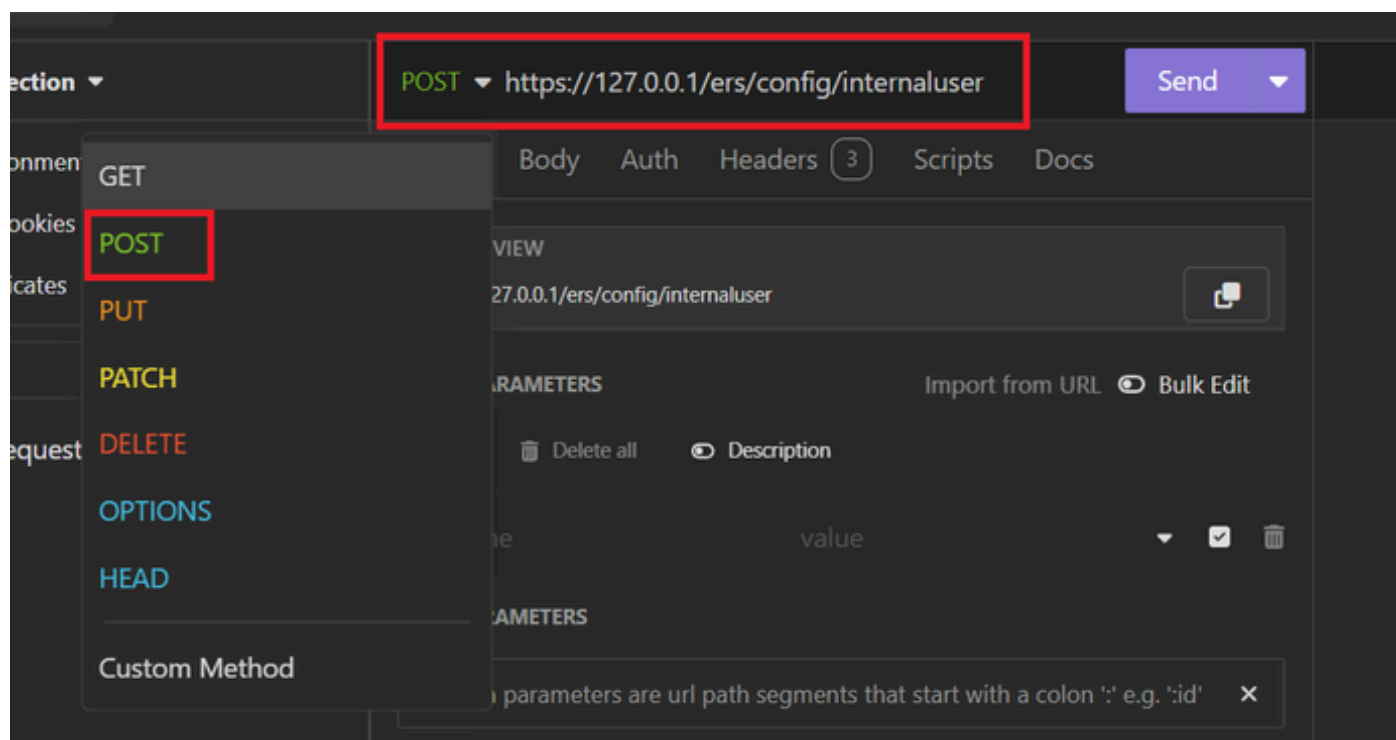


Solicitação XML

3. Você precisa escolher POST para enviar as informações ao nó ISE.

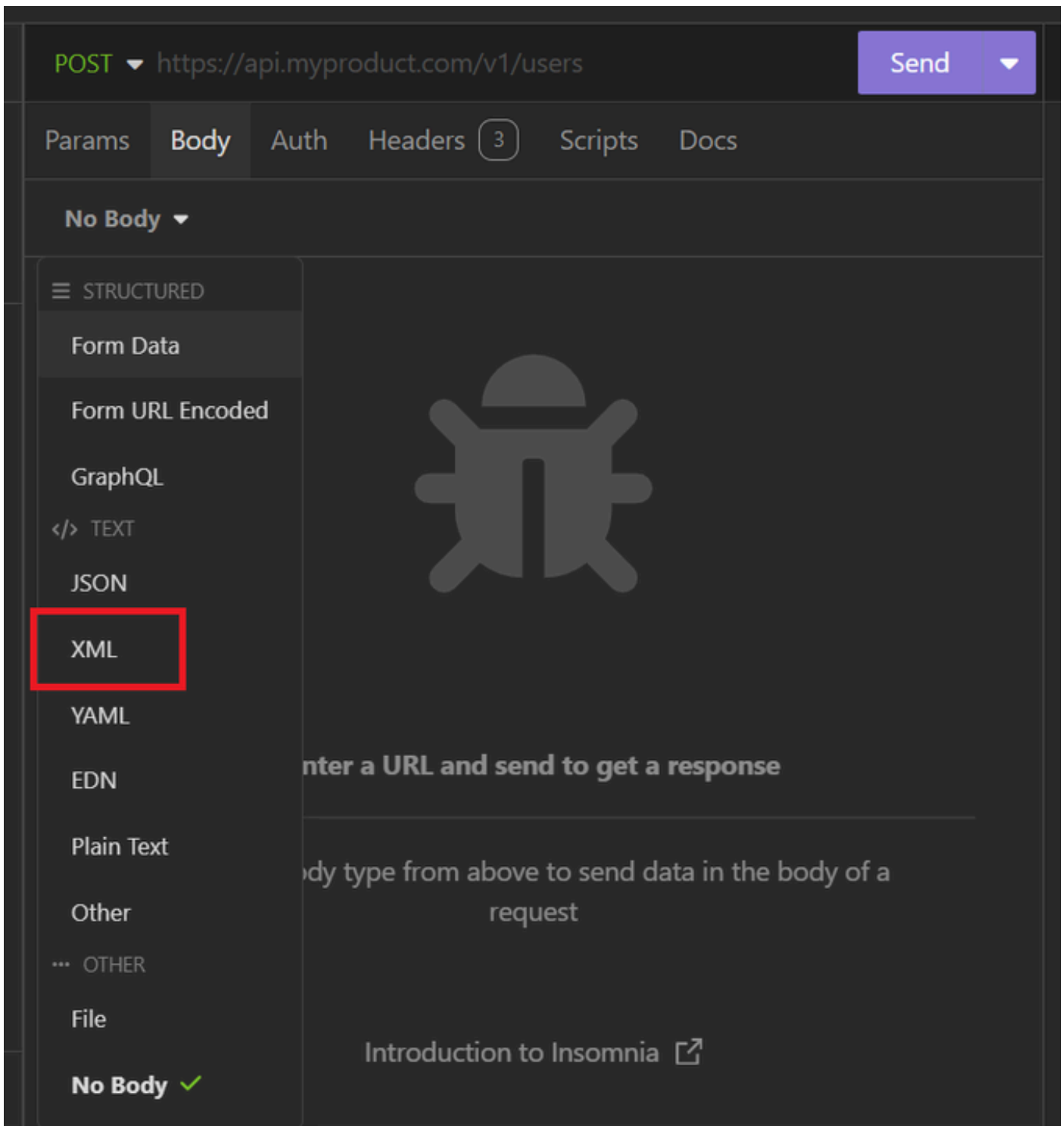
O URL que você precisa inserir depende do endereço IP do nó do ISE.

URL: <https://x.x.x.x/ers/config/internaluser>



POSTAGEM XML

4. Em seguida, clique em Corpo e escolha XML.



Corpo XML

5. Você pode colar a sintaxe e alterar os parâmetros dependendo do que deseja.

POST ▼ https://127.0.0.1:44421/ers/config/internaluser Send ▼

Params **Body** Auth Headers 4 Scripts Docs

XML ▼

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ns0:internaluser xmlns:ns0="identity.ers.ise.cisco.com"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:ns1="ers.ise.cisco.com" xmlns:ers="ers.ise.cisco.com"
  description="description" name="User02">
3   <accountNameAlias>User02</accountNameAlias>
4   <changePassword>true</changePassword>
5   <customAttributes>
6   </customAttributes>
7   <dateCreated>2024-7-18</dateCreated>
8   <dateModified>2024-7-18</dateModified>
9   <daysForPasswordExpiration>700</daysForPasswordExpiration>
10  <email>user2@local.com</email>
11  <enablePassword>bWn4hehq8ZCV22k</enablePassword>
12  <enabled>true</enabled>
13  <expiryDate>2026-12-11</expiryDate>
14  <expiryDateEnabled>false</expiryDateEnabled>
15  <firstName>User2</firstName>
16  <identityGroups>a1740510-8c01-11e6-996c-
    525400b48521</identityGroups>
17  <lastName>Cisco</lastName>
18  <password>bWn4hehq8ZCV1rk</password>
19  <passwordIDStore>Internal Users</passwordIDStore>
20  <passwordNeverExpires>false</passwordNeverExpires>
21 </ns0:internaluser>

```

Postagem XML

sintaxe XML

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<ns0:internaluser xmlns:ns0="identity.ers.ise.cisco.com" xmlns:xs="http://www.w3.org/2001/XMLSchema" xm
```

```
  <accountNameAlias>accountNameAlias</accountNameAlias>
```

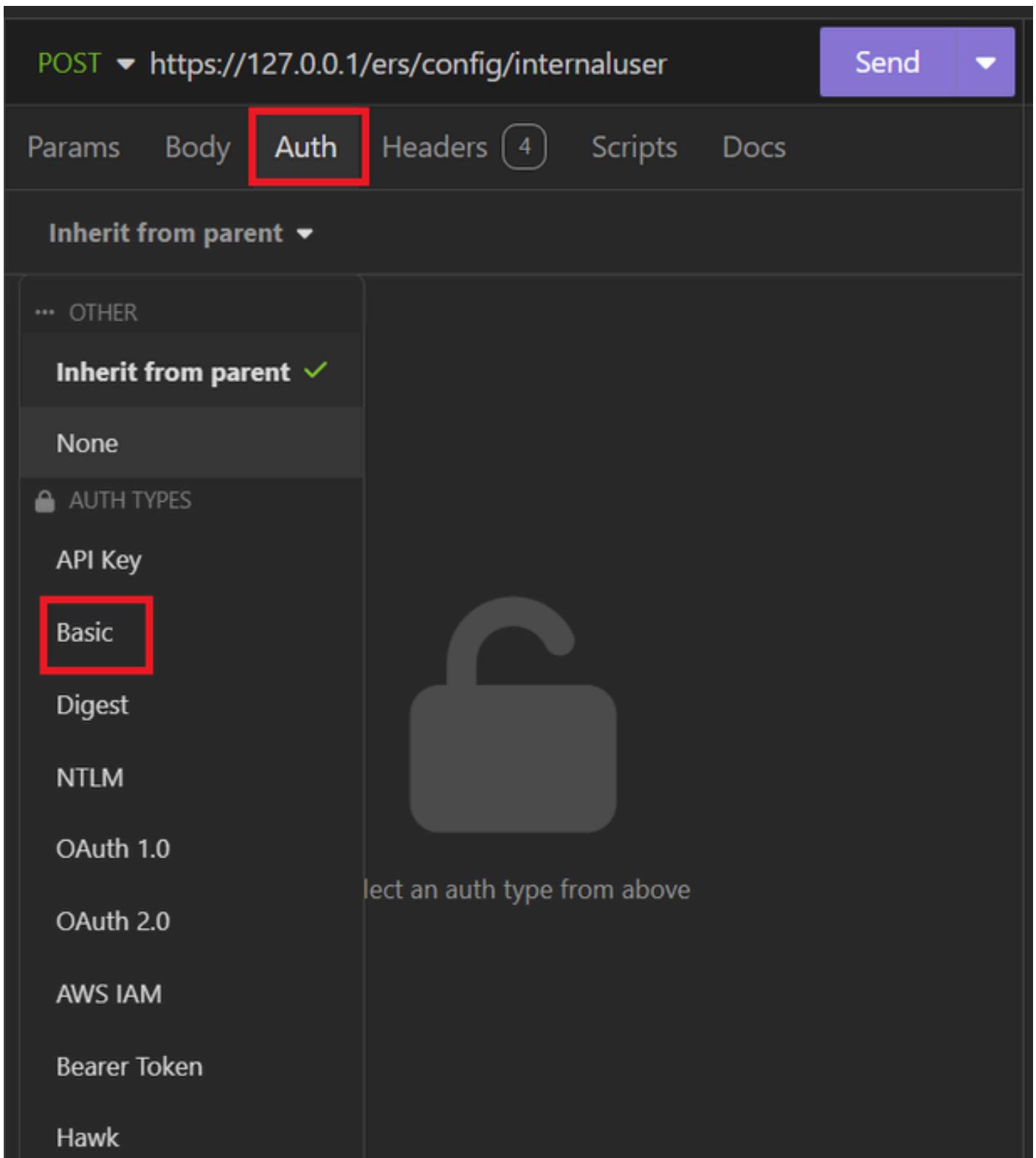
```
  <changePassword>true</changePassword>
```

```
  <customAttributes>
```



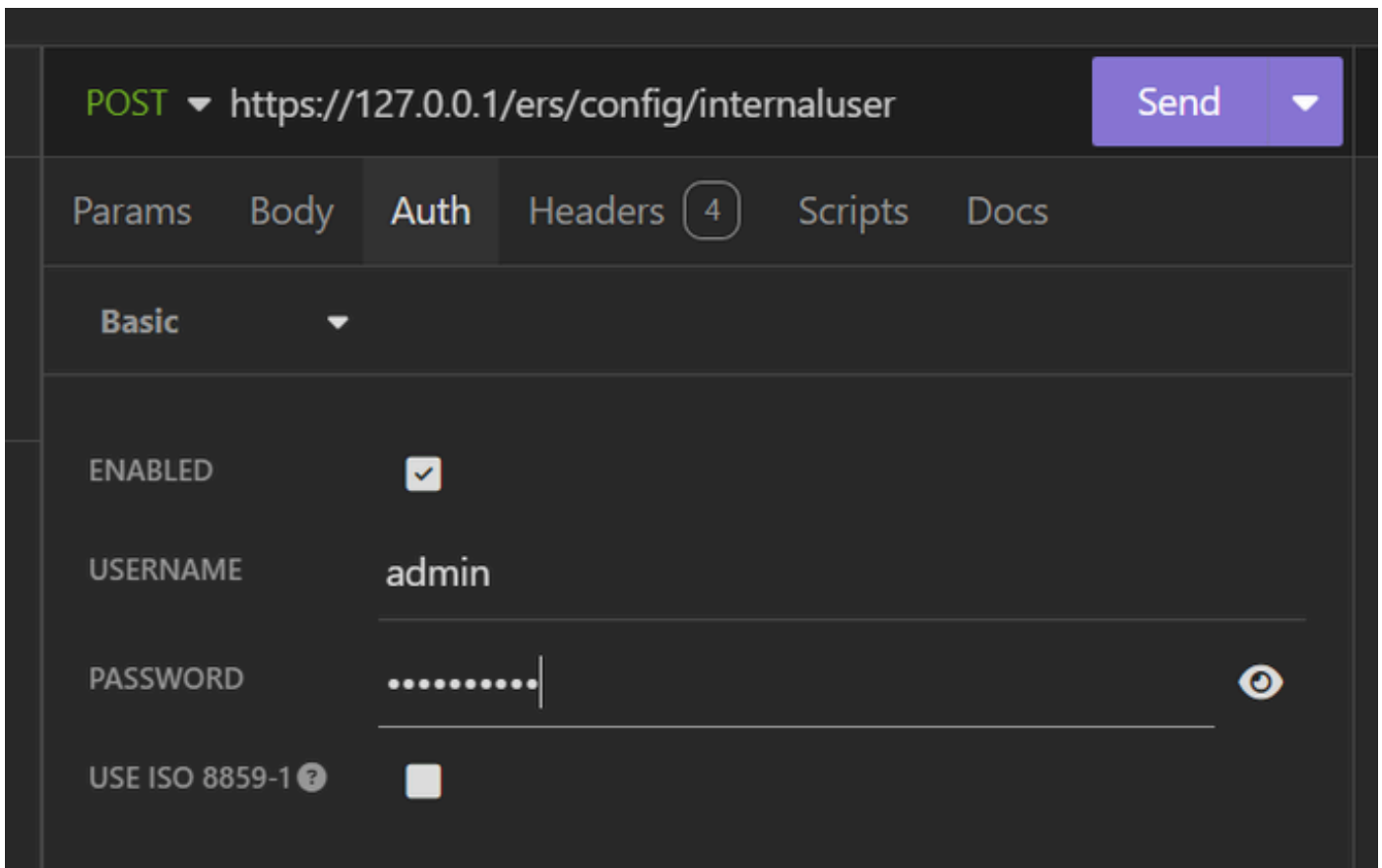
```
<entry>
  <key>key1</key>
  <value>value1</value>
</entry>
<entry>
  <key>key2</key>
  <value>value3</value>
</entry>
</customAttributes>
<dateCreated>2015-12-15</dateCreated>
<dateModified>2015-12-20</dateModified>
<daysForPasswordExpiration>60</daysForPasswordExpiration>
<email>email@domain.com</email>
<enablePassword>enablePassword</enablePassword>
<enabled>true</enabled>
<expiryDate>2016-12-11</expiryDate>
<expiryDateEnabled>>false</expiryDateEnabled>
<firstName>firstName</firstName>
<identityGroups>identityGroups</identityGroups>
<lastName>lastName</lastName>
<password>password</password>
<passwordIDStore>Internal Users</passwordIDStore>
<passwordNeverExpires>>false</passwordNeverExpires>
</ns0:internaluser>
```

6. Clique em Auth e selecione Basic



Autenticação XML

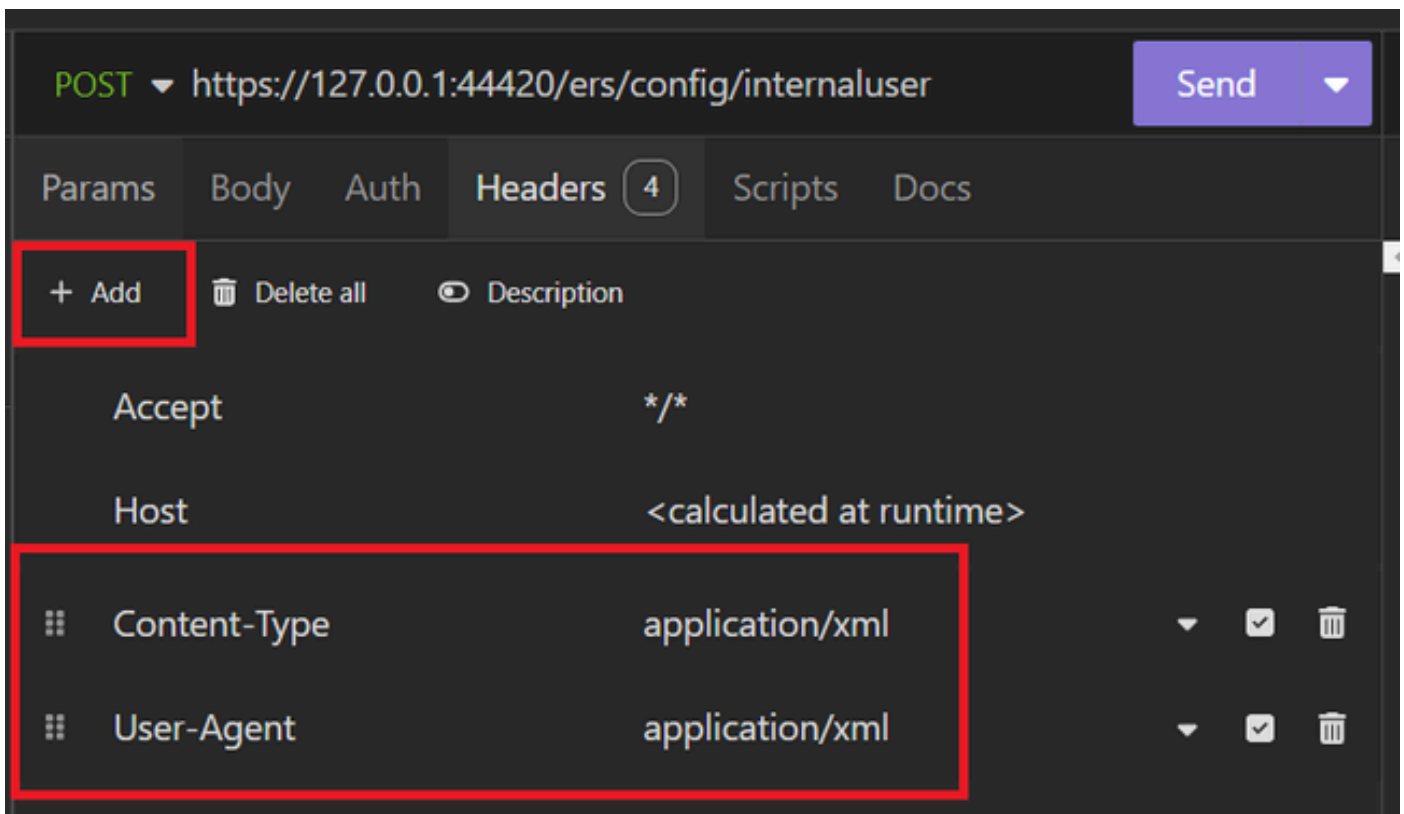
7. Insira as credenciais da GUI do ISE.



Credenciais XML

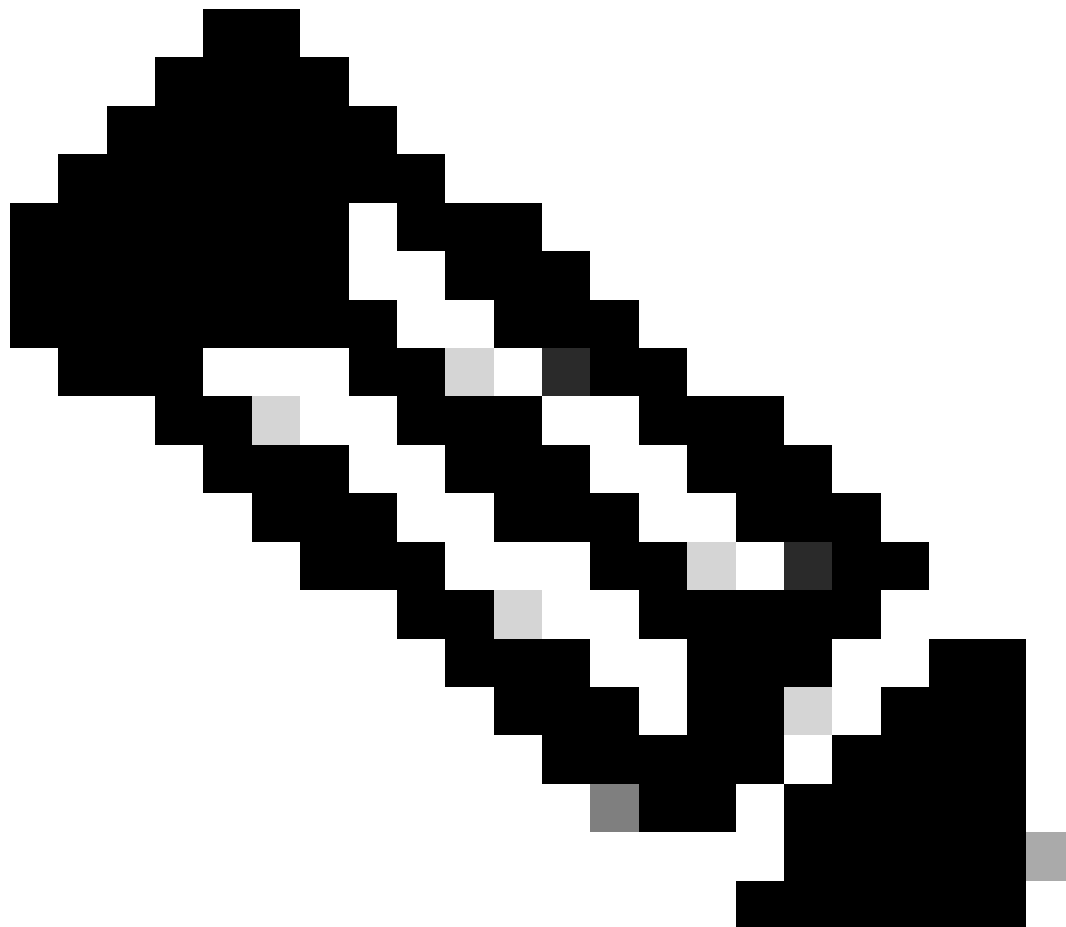
8. Clique em Cabeçalhos para adicionar os próximos métodos:

- Tipo de conteúdo: aplicativo/xml
- Aceitar: aplicativo/xml



Cabeçalhos XML

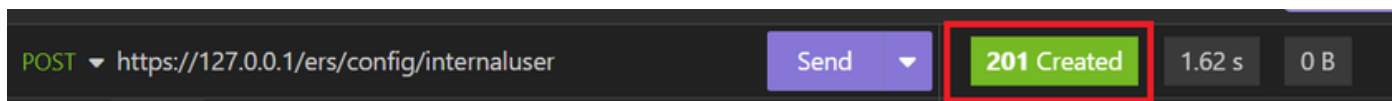
9. Finalmente, clique em Enviar.



Observação: se quiser atribuir um Grupo de Identidade à nova conta de usuário, você precisará usar o ID do Grupo de Identidade. Verifique a **seção Solução de problemas** para obter mais informações.

Validação



1. Após enviar a solicitação POST você verá o status "201 Criado". Isso significa que o processo foi concluído com êxito.
















Solicitação XML bem-sucedida

2. Abra a GUI do ISE e navegue até Administração > Gerenciamento de identidades > Identidades > Usuários > Usuários de acesso à rede

Network Access Users

Selected 0 Total 2  

 Edit  + Add  Change Status  Import  Export  Delete  Duplicate  All 

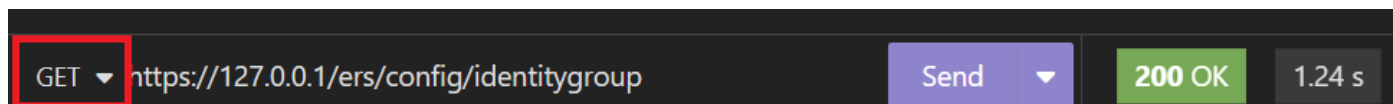
Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	Enabled  User01	this is the firs...	User	Cisco	user1@local...	Employee	 User Account created by JSON
<input type="checkbox"/>	Enabled  User02	description	User2	Cisco	user2@local...	Employee	 User Account created by XML

Validação de Contas de Usuário

Troubleshooting

1. Identifique o ID do grupo de identidade.

Use GET e a consulta <https://X.X.X.X/ers/config/identitygroup>.



opção GET

Saída JSON.

Identifique a ID ao lado da descrição.

```
11 <ns5:resource description="Default Employee User Group"
12   id="a1740510-8c01-11e6-996c-525400b48521" name="Employee">
13   <link rel="self"
14     href="https://127.0.0.1:44421/ers/config/identitygroup/a1740
15     510-8c01-11e6-996c-525400b48521" type="application/xml"/>
16 </ns5:resource>
```

Grupo de Identidade de Identificação 01

Saída XML.

Identifique a ID ao lado da descrição.

```
15 }
16   "id": "a1740510-8c01-11e6-996c-525400b48521",
17   "name": "Employee",
18   "description": "Default Employee User Group",
19   "link": {
20     "rel": "self",
21     "href":
22     "https://127.0.0.1:44421/ers/config/identitygroup/a1740510-8c01-11e6-996c-525400b48521",
```

Grupo de Identidade de Identificação 02

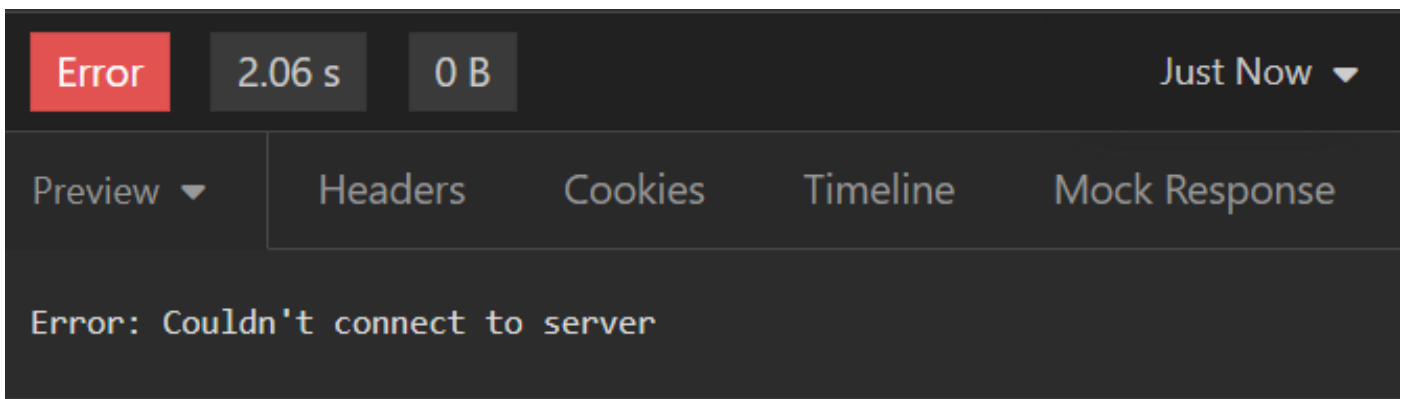
2. 401 Erro não autorizado.



erro 401

Solução: verifique as credenciais de acesso configuradas na seção Auth

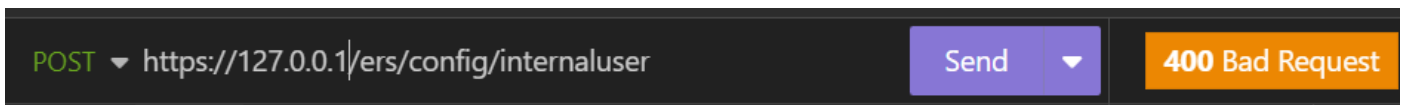
3. Erro: Não foi possível conectar ao servidor



Erro de conexão

Solução: verifique o endereço IP do nó ISE configurado em Insomnia ou valide a conectividade.

4. 400 Solicitação Incorreta.

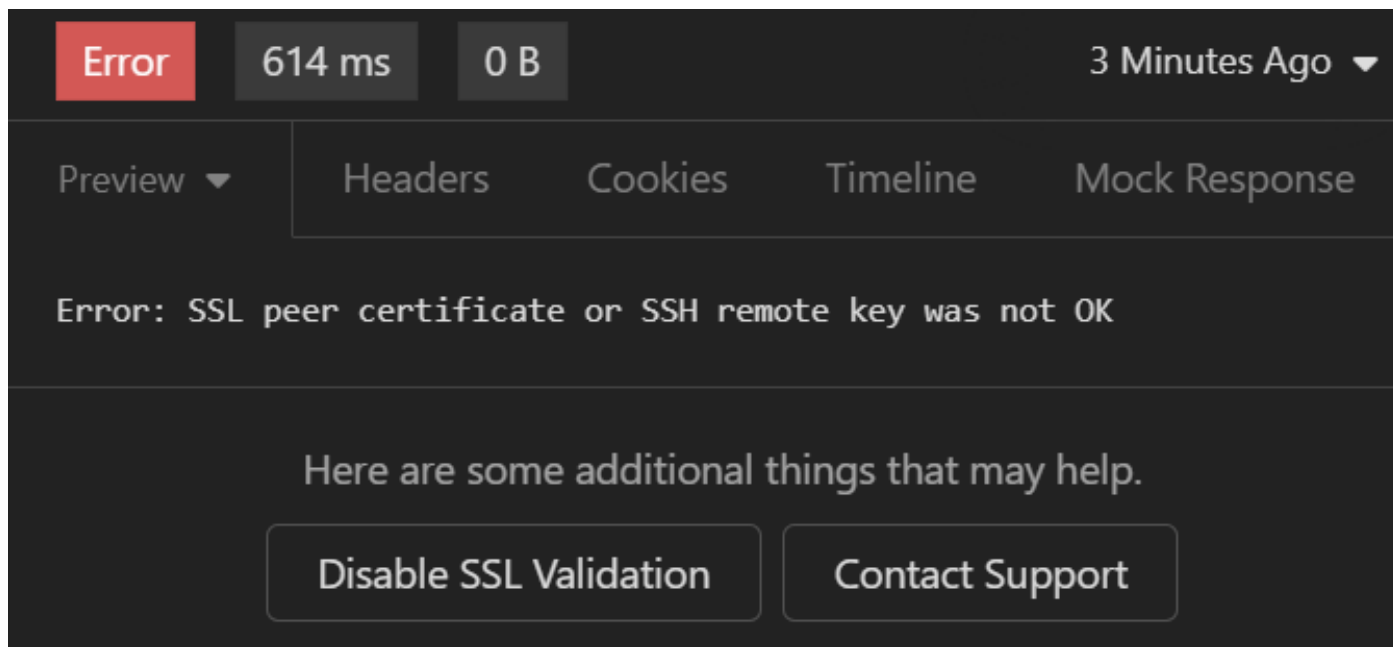


erro 400

Há várias razões para enfrentar esse erro, as mais comuns são:

- Incompatibilidade com a política de senha de segurança
- Alguns parâmetros foram configurados incorretamente.
- Erro Sintaxis.
- Informações duplicadas.

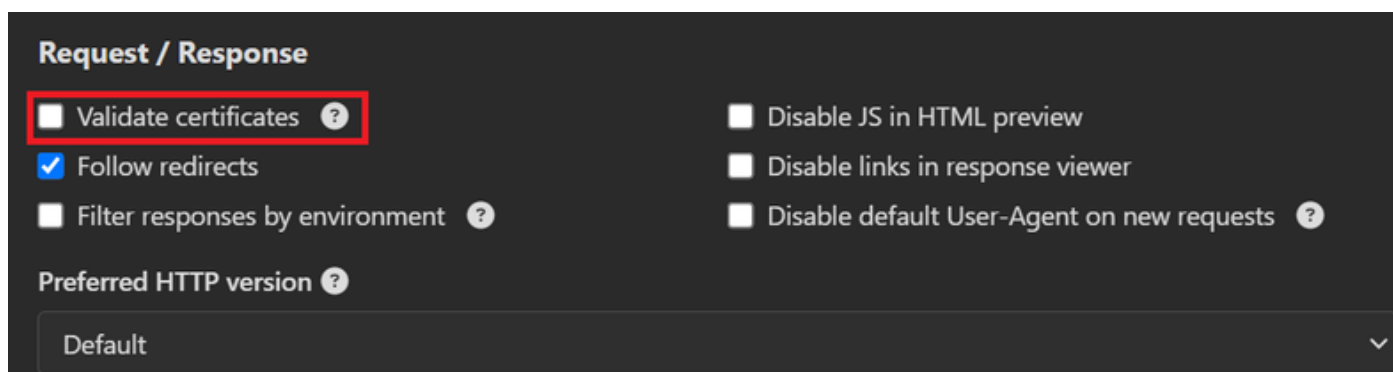
5. Erro: o certificado de par SSL ou a chave remota SSH não estava OK



erro de certificado SSL

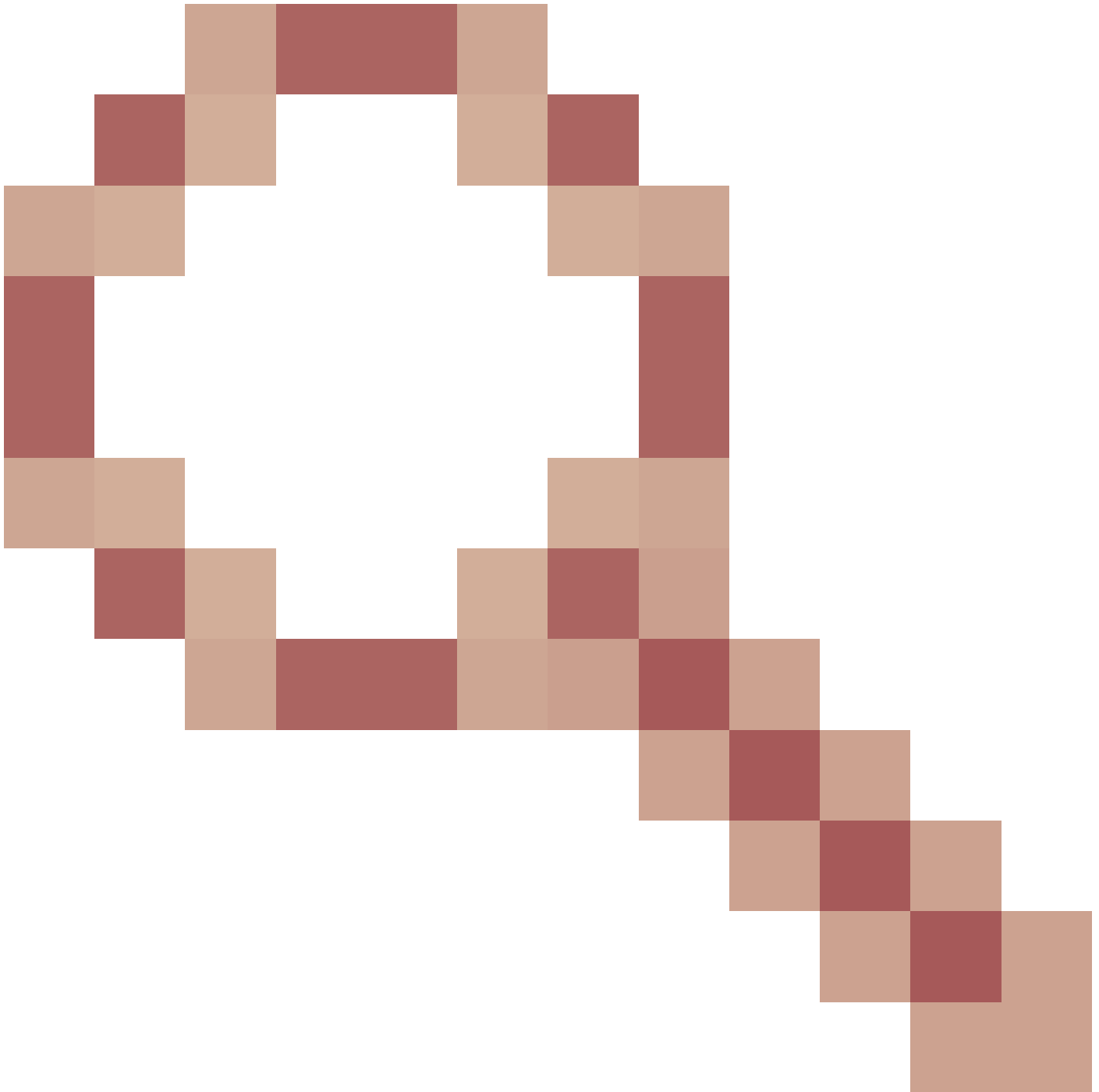
Solução:

1. Clique em Desativar validação SSL.
2. Em Solicitação/Resposta, desative a opção Validar certificados.



Opção Validar certificados

6. [CSCwh71435](https://www.cscwh.com/71435)



defeito.

A senha de ativação é configurada aleatoriamente, embora você não a tenha configurado. Esse comportamento acontece quando a sintaxe de habilitação de senha é removida ou deixada em branco como valor. Verifique o próximo link para obter mais informações:

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh71435>

Referências de chamada de API.

Você pode ver todas as informações sobre as chamadas de API suportadas pelo ISE.

1. Navegue até Administração > Sistema > Configurações > Configuração de API.

2. Clique no link de informações da API ERS.

Identity Services Engine Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access **Settings**

Security Settings
Alarm Settings
General MDM / UEM Settings
Posture
Profiling
Protocols
Endpoint Scripts
Proxy
SMTP Server
SMS Gateway
System Time
API Settings
Data Connect
Network Success Diagnostics

API Settings

Overview API Service Settings API Gateway Settings

API Services Overview

You can manage Cisco ISE nodes through two sets of API formats—External Restful Services (ERS) and OpenAPI. Starting Cisco ISE Release 3.1, new APIs are available in the OpenAPI format. The ERS and OpenAPI services are HTTPS-only REST APIs that operate over port 443. Currently, ERS APIs also operate over port 9060. However, port 9060 might not be supported for ERS APIs in later Cisco ISE releases. We recommend that you only use port 443 for ERS APIs. Both the API services are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the [API Service Settings](#) tab. To use either API service, you must have the ERS-Admin or ERS-Operator user group assignment.

For more information on ISE ERS API, please visit:
<https://127.0.0.1:44421/ers/sdk>

For openapi documentation for ERS, click below:
[ERS_V1](#)

For more information on ISE Open API, please visit:
<https://127.0.0.1:44421/api/swagger-ui/index.html>

Configurações de API

3. E clique em documentação da API.

External RESTful Services (ERS) Online SDK

Quick Reference
API Documentation

- ISE 2.0 Release Notes
- ISE 2.1 Release Notes
- ISE 2.2 Release Notes
- ISE 2.3 Release Notes
- ISE 2.4 Release Notes
- ISE 2.6 Release Notes
- ISE 2.7 Release Notes
- ISE 3.0 Release Notes
- ISE 3.1 Release Notes
- ISE 3.2 Release Notes
- ISE 3.3 Release Notes**
- ANC Endpoint
- ANC Policy
- AcI bindings
- AcI Settings
- Active Directory

ISE 3.3 Release Notes

• New / Modified Resources

New / Modified Resources

Resource Name	ISE Version	Resource Version	Description
InternalUser	3.3	1.5	Added user creation date and last modification date attributes
Ldap	3.3	2.0	Ldap API allows clients to create, get, update and delete Ldaps and get rootca certificates, get issuerca certificates, get hosts, test Connection
Guest Type	3.3	2.0	Added the dynamic group option for LDAP groups
Network Device	3.3	1.4	The password (Show Password in Plaintext) of the network device shared secret and second shared secret will be either in plain text or will be masked depending on the settings in Security Settings page

Documentação de API

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.