

# 使用Insomnia通过ISE 3.3中的JSON或XML和API调用配置内部用户

## 目录

---

---

## 简介

本文档介绍通过结合使用JSON或XML数据格式和API调用，在Cisco ISE中配置内部用户。

## 先决条件

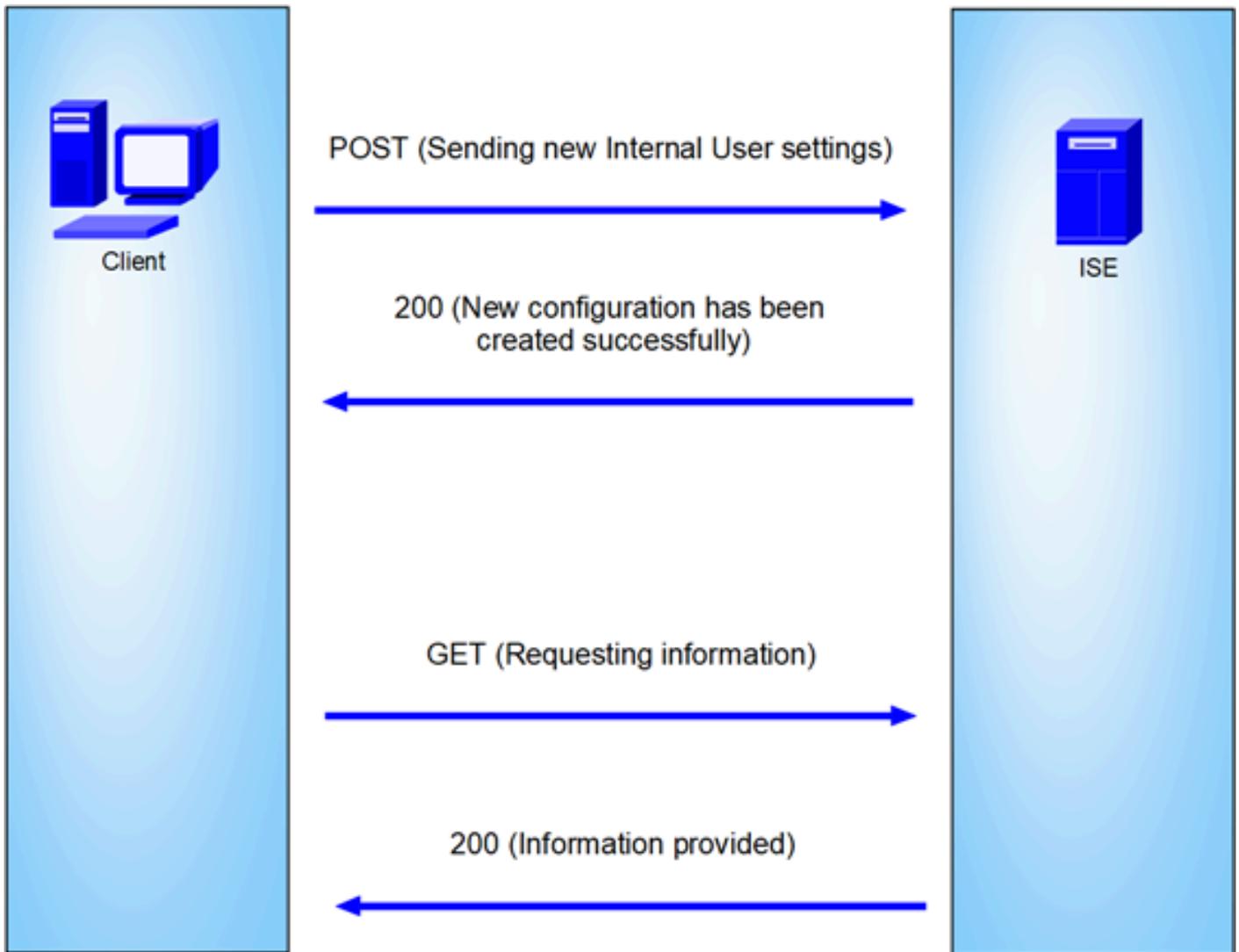
- ISE 3.0或更高版本。
- API客户端软件。

## 使用的组件

- ISE 3.3
- Insomnia 9.3.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 网络图



常规拓扑

GET和POST是API (应用编程接口) 调用中最常用的两种HTTP方法。它们用于与服务器上的资源交互，通常用于检索数据或提交数据以进行处理。

## 获取API调用

GET方法用于从指定资源请求数据。GET请求是API和网站中最常见且最广泛使用的方法。当您访问网页时，您的浏览器向托管网页的服务器发出GET请求。

## POST API调用

POST方法用于将数据发送到服务器以创建或更新资源。POST请求通常用于提交表单数据或上传文件。

## 配置

我们需要将来自API客户端软件的确切信息发送到ISE节点以创建内部用户。

## ISE配置

启用ERS功能。

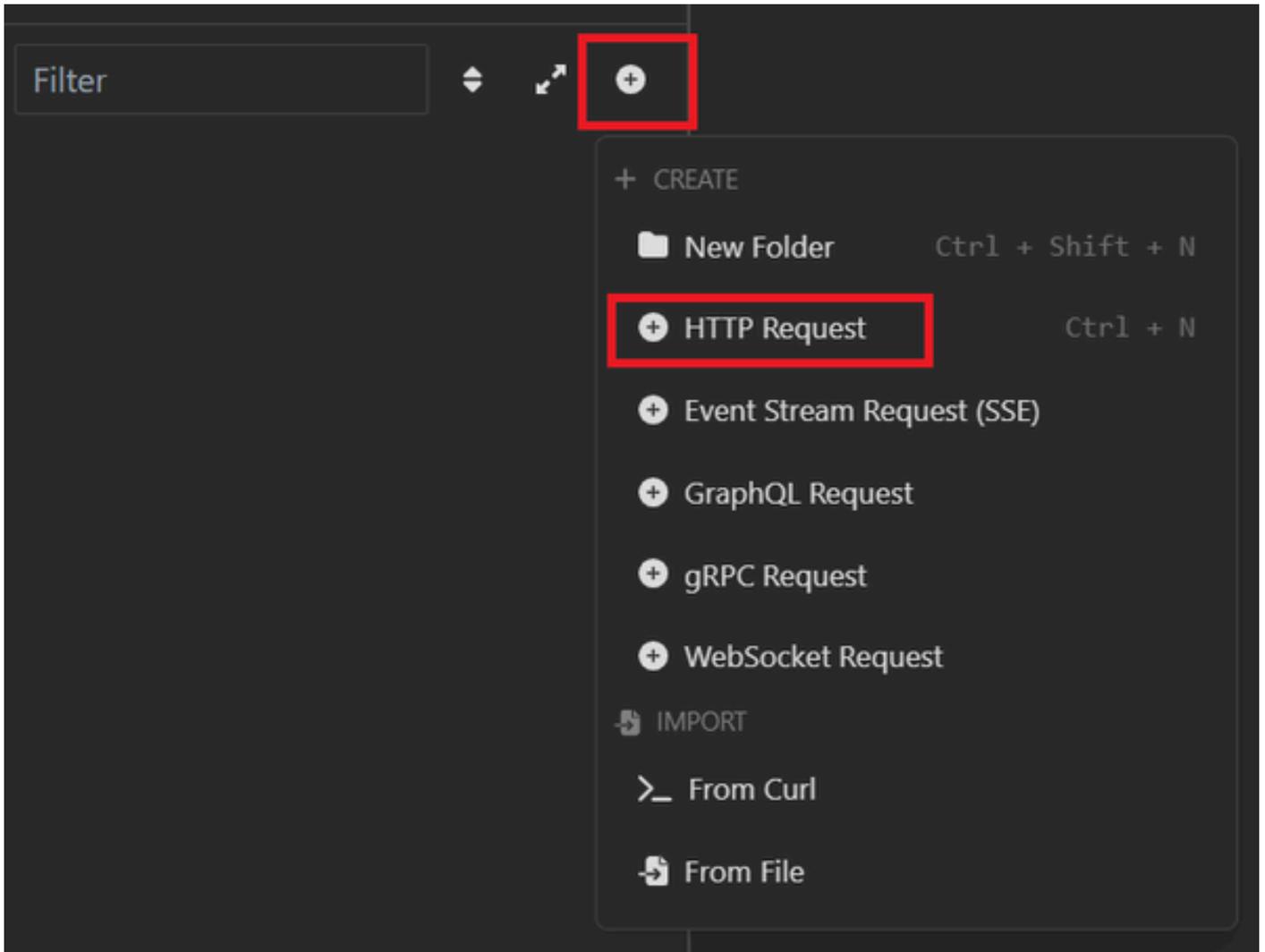
1. 导航至“管理”>“系统”>“设置”>“API设置”>“API服务设置”。
2. 启用ERS ( 读/写 ) 选项。

The screenshot shows the Cisco Identity Services Engine Administration / System interface. The left sidebar contains a navigation menu with categories like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The main content area is titled 'API Settings' and has three tabs: Overview, API Service Settings (selected), and API Gateway Settings. Under 'API Service Settings for Administration Node', there are two toggle switches: 'ERS (Read/Write)' (which is turned on and highlighted with a red box) and 'Open API (Read/Write)' (which is turned off). Below this, there is a section for 'CSRF Check ( only for ERS Settings )' with two radio button options: 'Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)' and 'Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)'. At the bottom right, there are 'Reset' and 'Save' buttons, with the 'Save' button highlighted by a red box.

API设置

## JSON请求。

1. 开放式失眠。
2. 在左侧添加新的HTTPS请求。

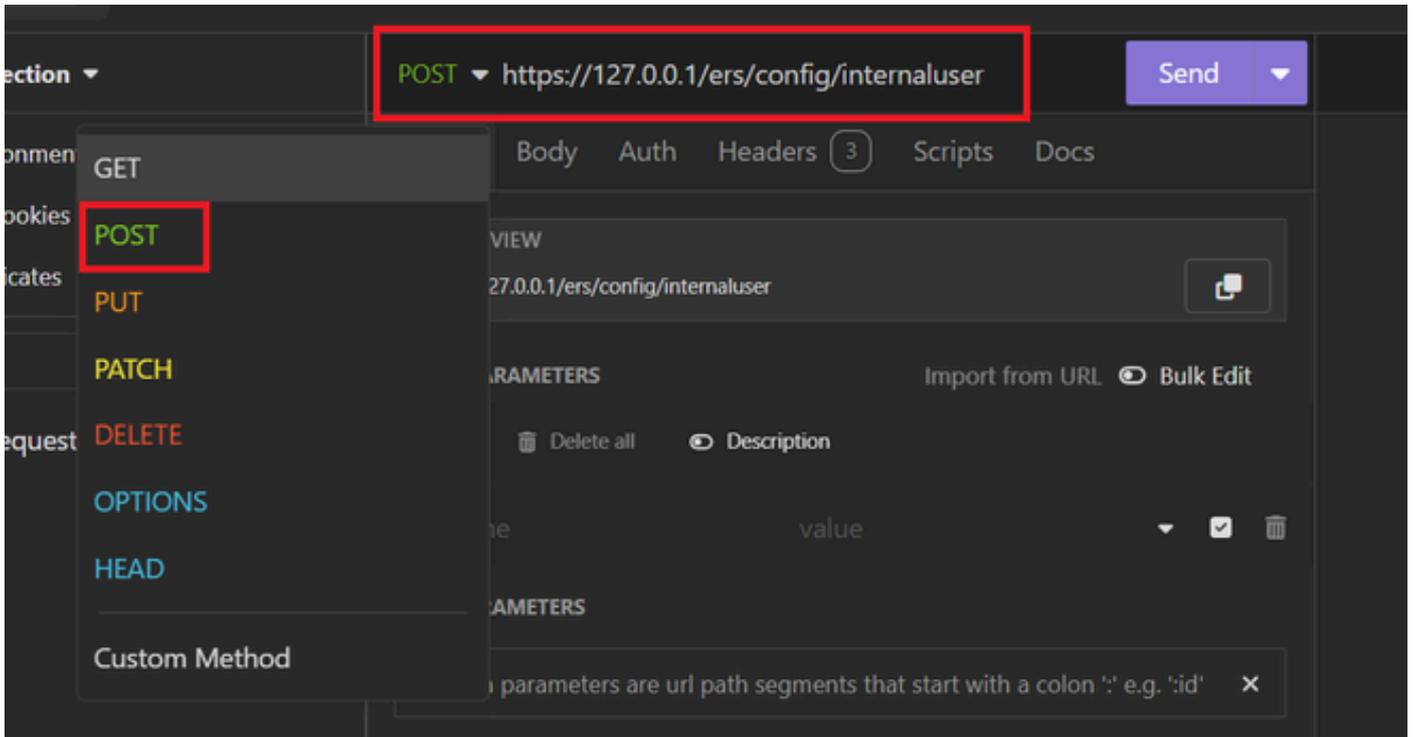


JSON请求

3. 您需要选择POST以将信息发送到ISE节点。

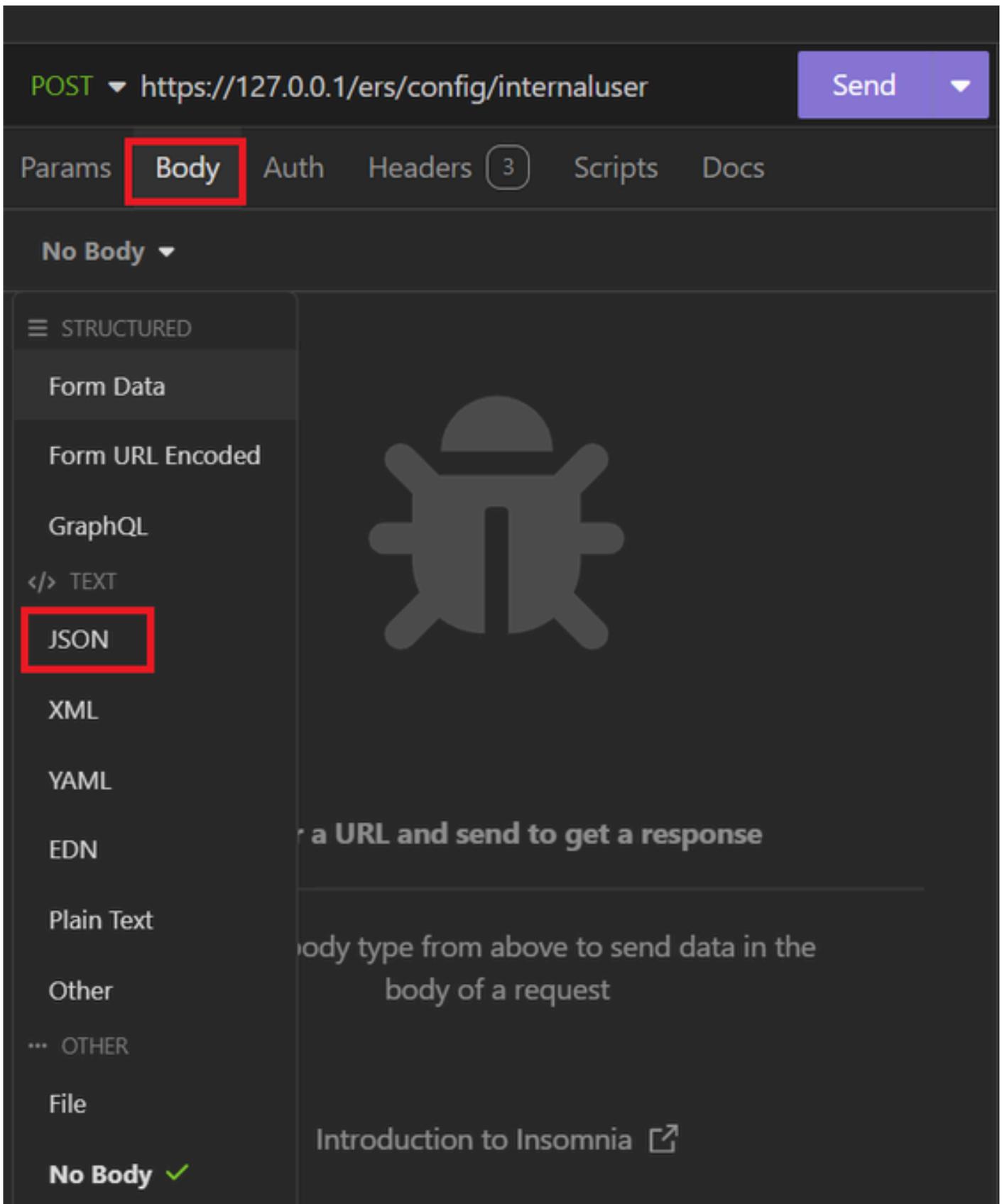
您需要输入的URL取决于ISE节点的IP地址。

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



JSON发布

4. 然后点击Body并选择JSON



JSON正文

5. 您可以粘贴语法并根据需要更改参数。

```
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 }
```

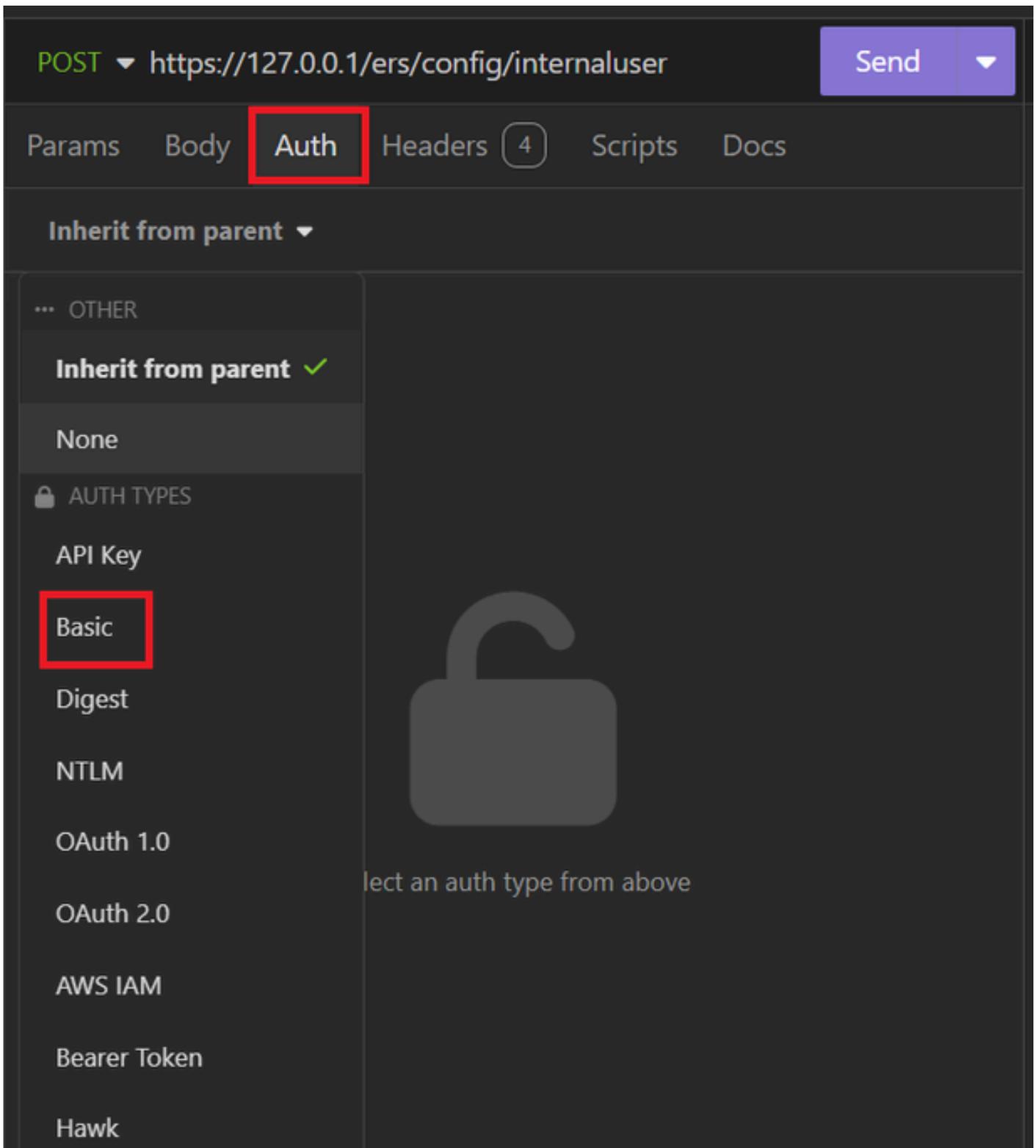
JSON语法

## JSON语法

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

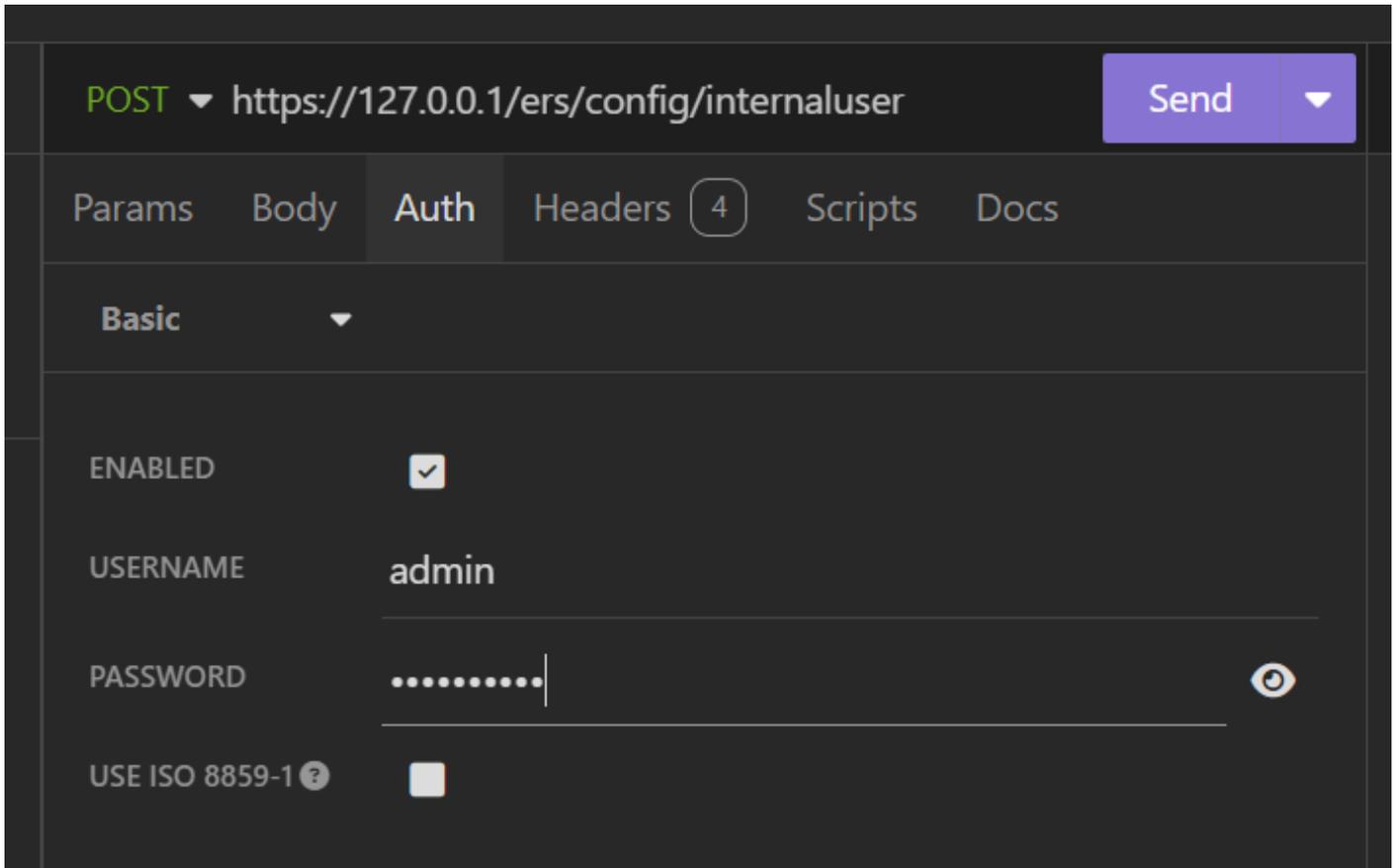
```
"password": "password",
"firstName": "firstName",
"lastName": "lastName",
"changePassword": true,
"identityGroups": "identityGroups",
"passwordNeverExpires": false,
"daysForPasswordExpiration": 60,
"expiryDateEnabled": false,
"expiryDate": "2016-12-11",
"enablePassword": "enablePassword",
"dateModified":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

6. 点击Auth并选择Basic。



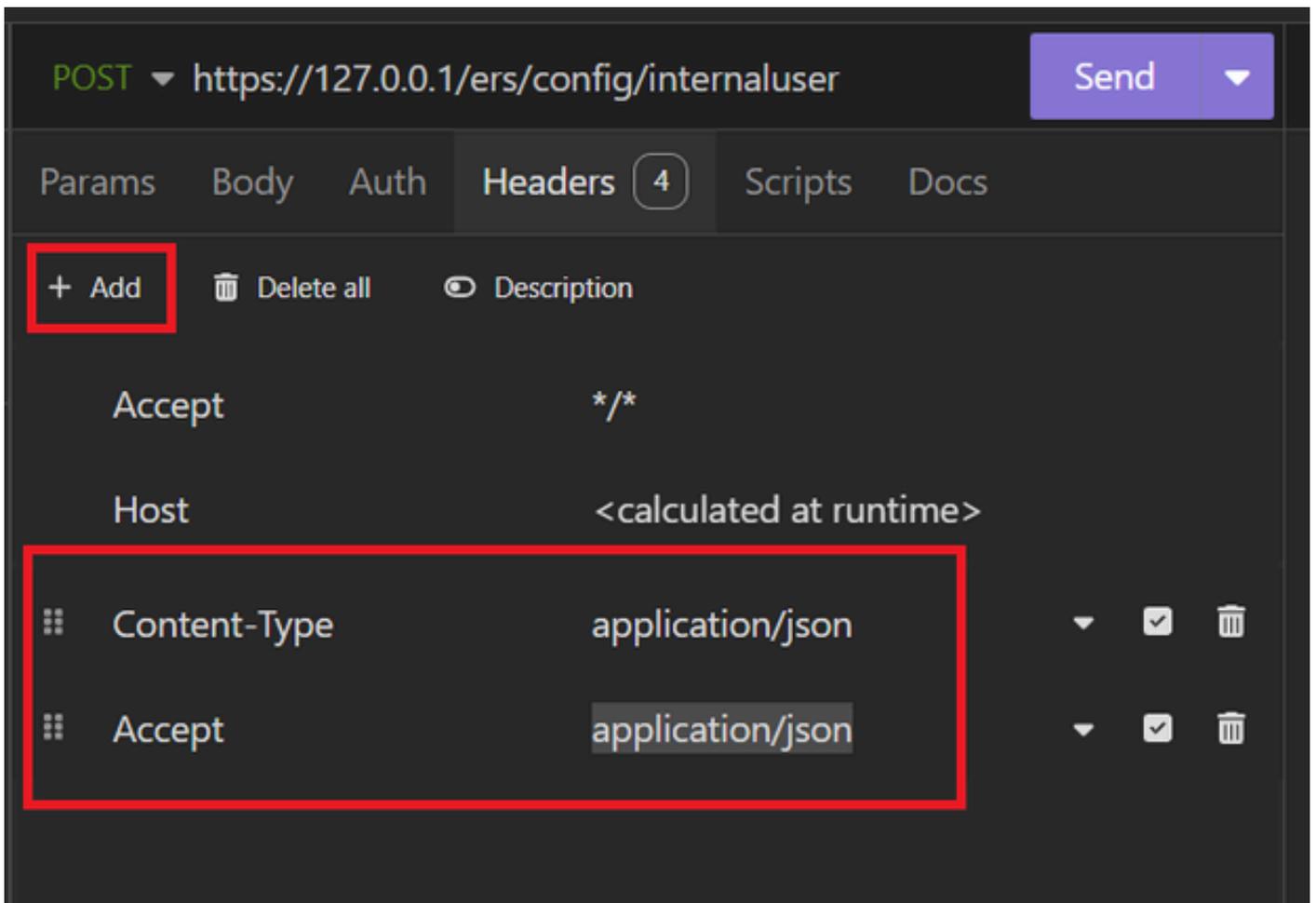
JSON身份验证

7. 输入ISE GUI凭证。



管理员JSON凭证

8. 点击Headers以添加以下方法：
- 内容类型：application/json
  - 接受：application/json



JSON报头

9. 最后，单击“发送”。

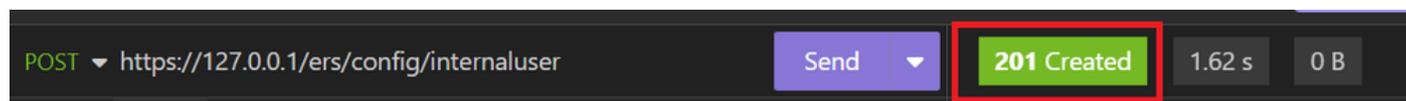
---

注意：如果要身份组分配给新用户帐户，需要使用身份组的ID。有关详细信息，请查看故障排除部分。

---

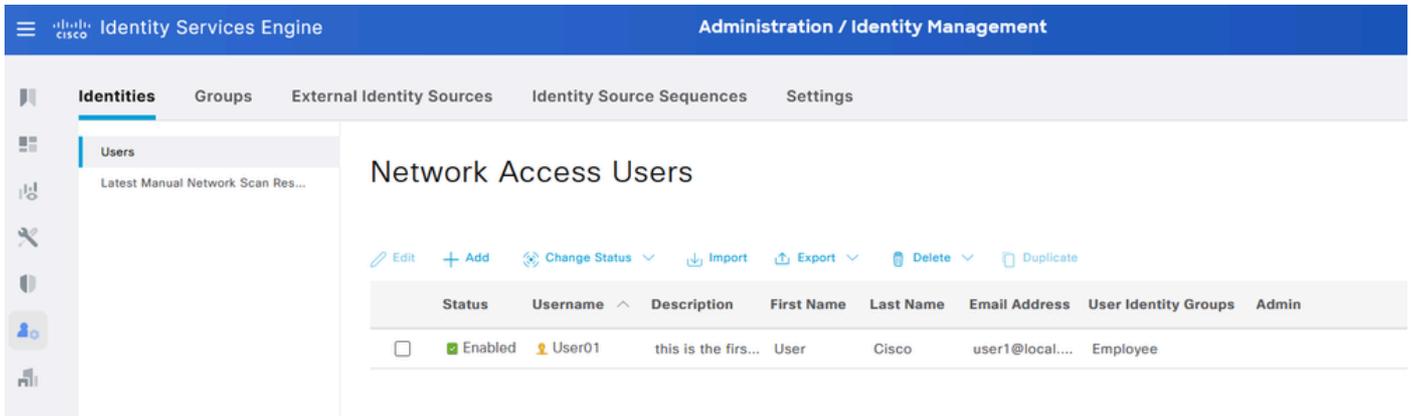
## 验证

1. 发送POST请求后，您将看到状态“201 Created”。这表示该过程已成功完成。



成功的JSON请求

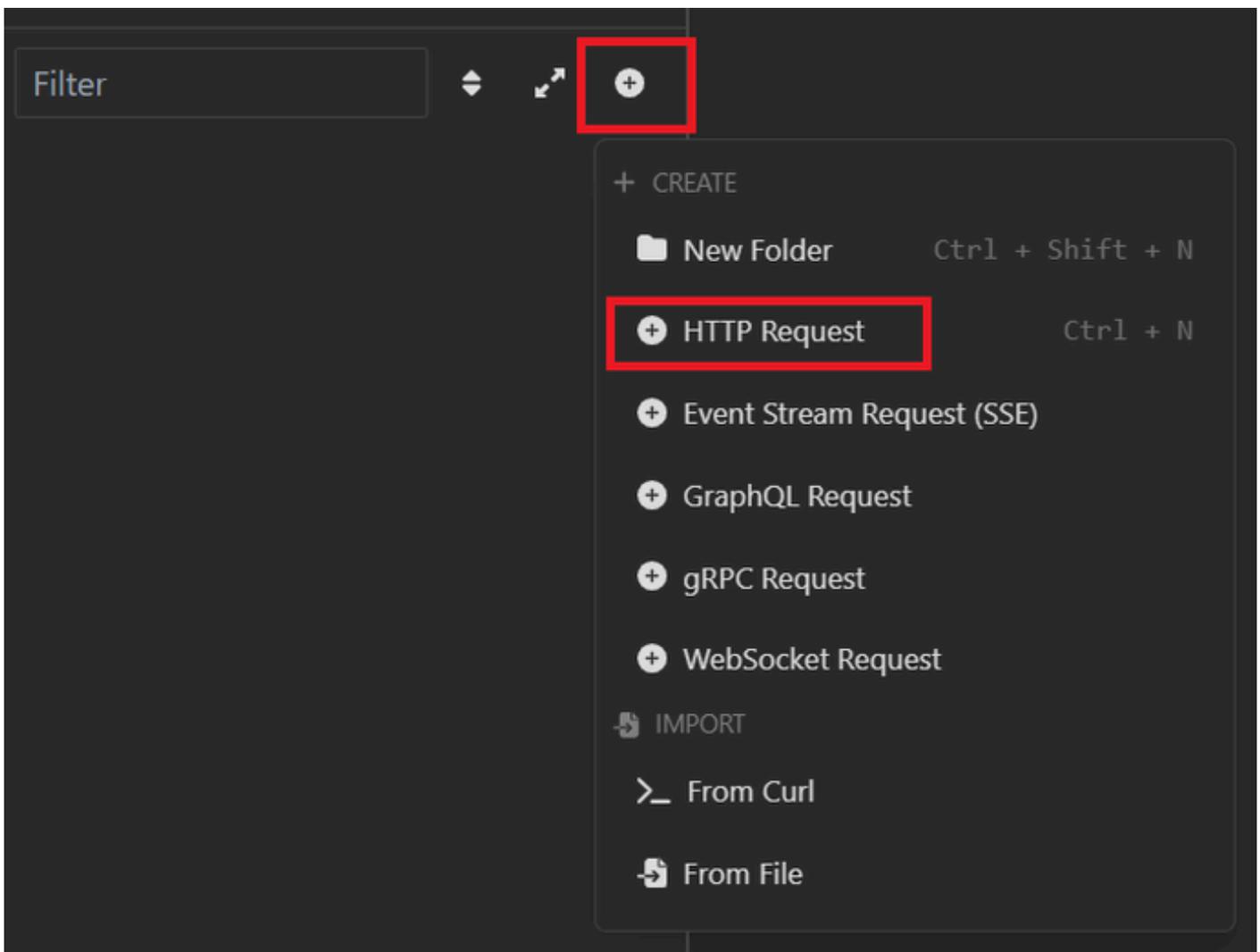
2. 打开ISE GUI并导航到管理>身份管理>身份>用户>网络访问用户



JSON用户帐户

## XML请求

1. 开放式失眠。
2. 在左侧添加新的HTTPS请求。

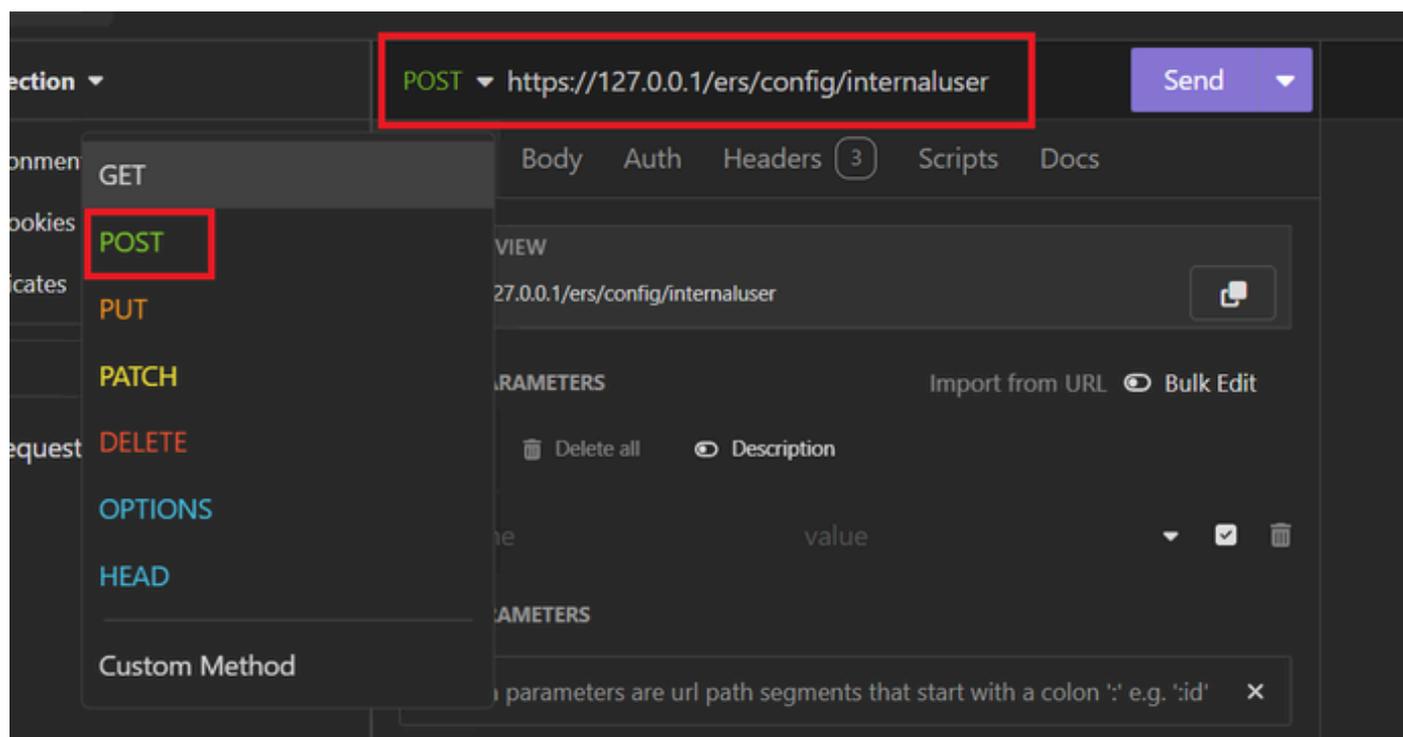


XML请求

3. 您需要选择POST以将信息发送到ISE节点。

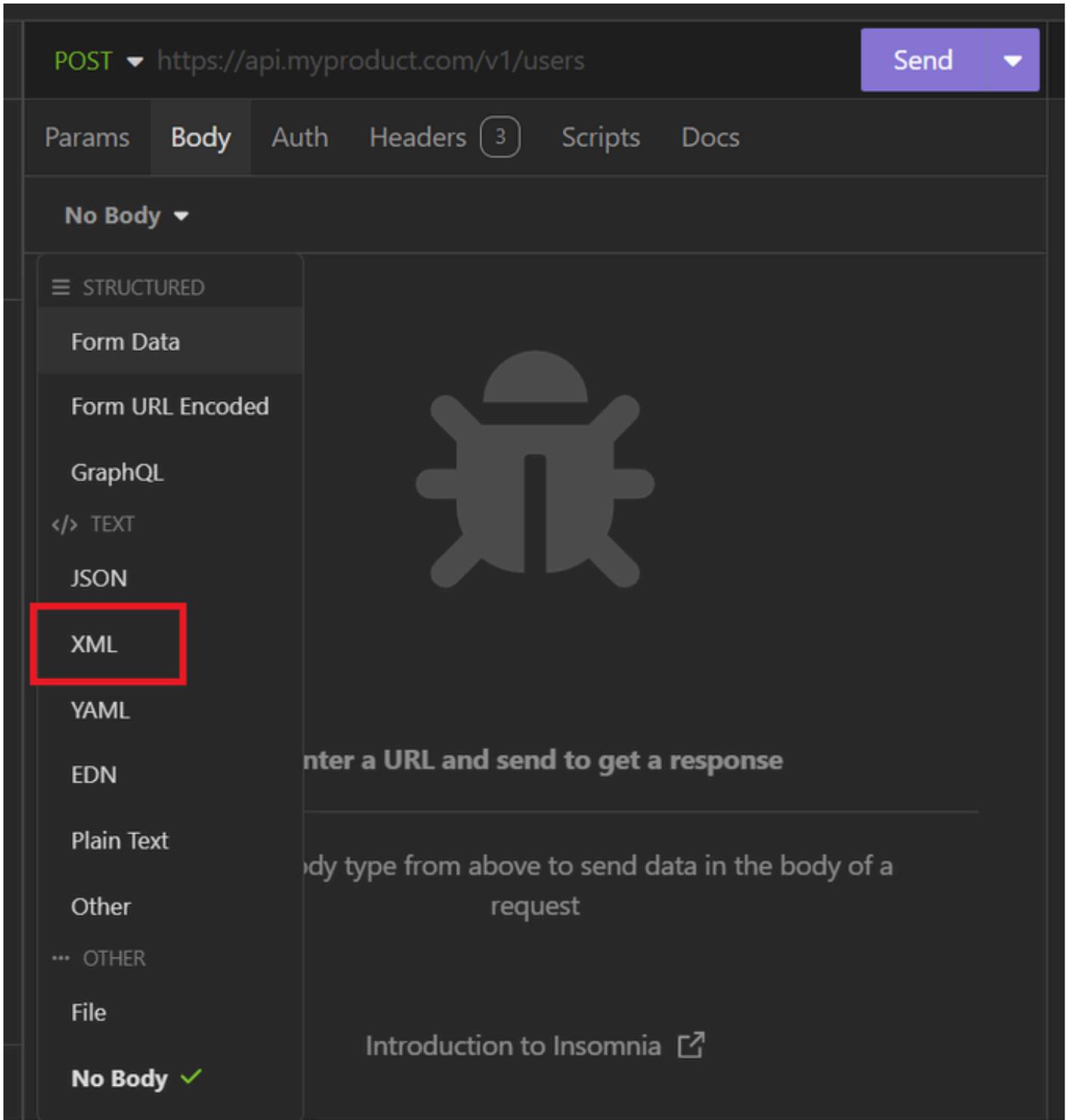
您需要输入的URL取决于ISE节点的IP地址。

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



XML文章

4. 然后单击“正文”，然后选择“XML”。



XML正文

5. 您可以粘贴语法并根据需要更改参数。

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>
```

XML文章

## XML语法

```
<?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
```

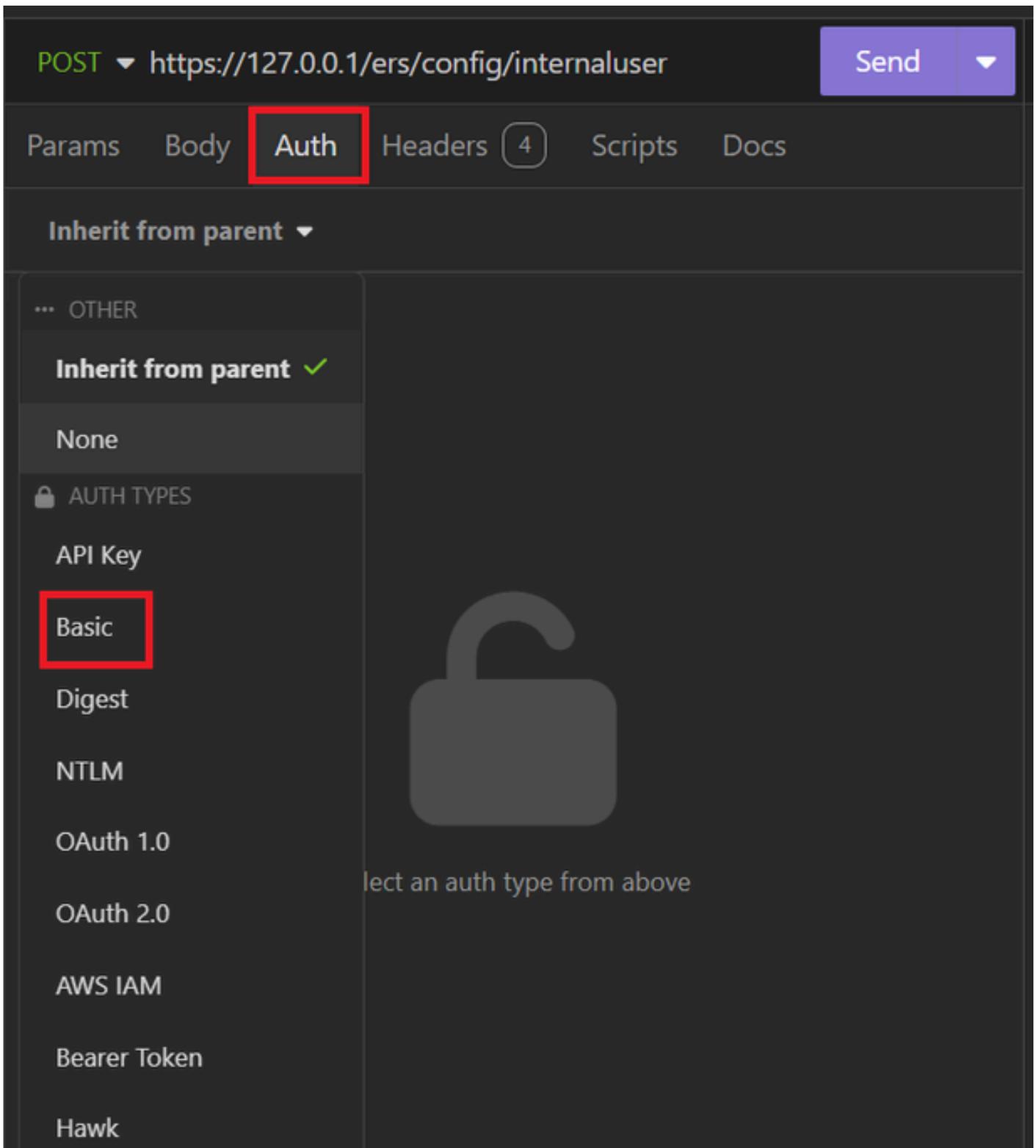
```
  <accountNameAlias>accountNameAlias</accountNameAlias>
```

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

```
  <customAttributes>
```

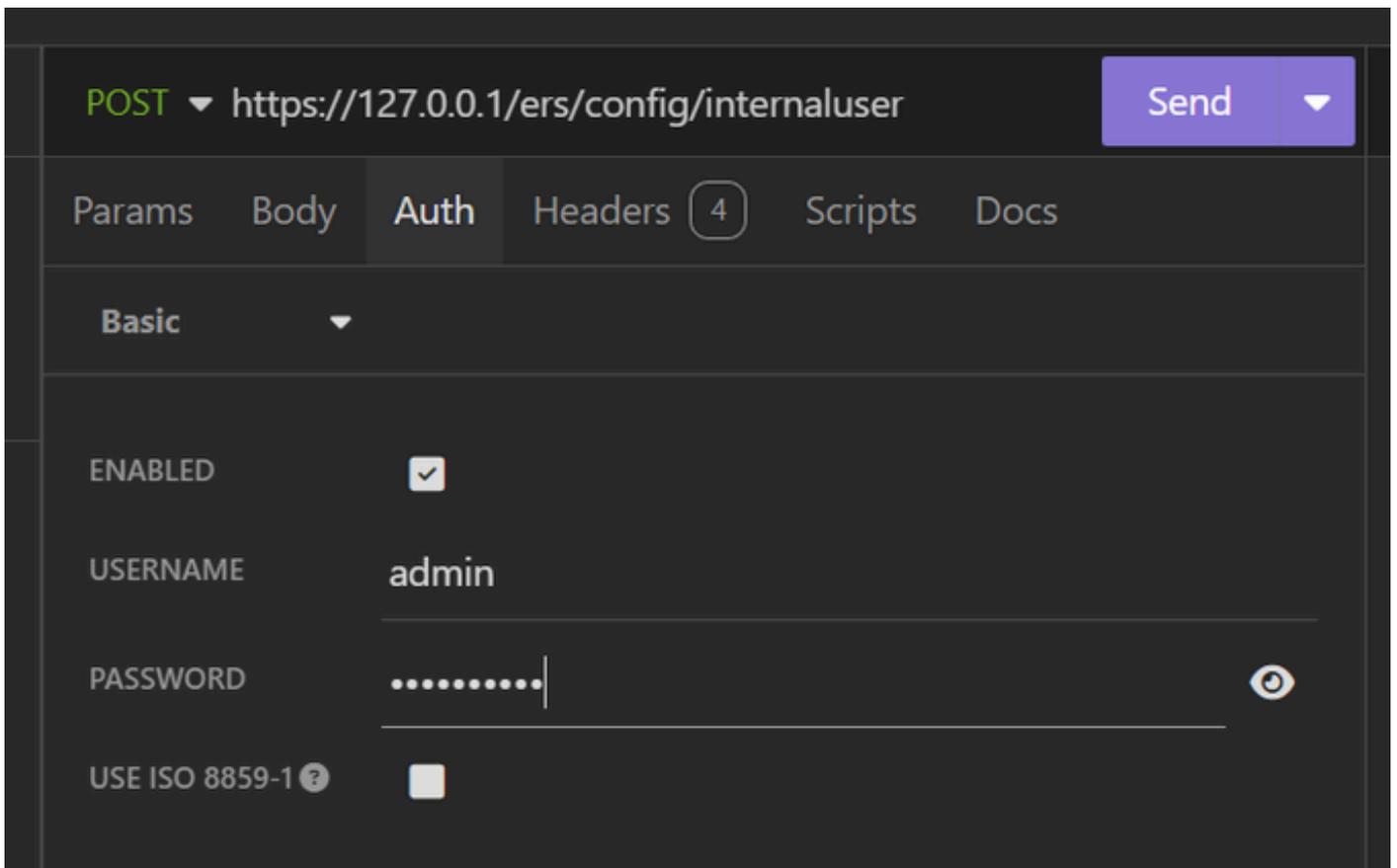
```
<entry>
  <key>key1</key>
  <value>value1</value>
</entry>
<entry>
  <key>key2</key>
  <value>value3</value>
</entry>
</customAttributes>
<dateCreated>2015-12-15</dateCreated>
<dateModified>2015-12-20</dateModified>
<daysForPasswordExpiration>60</daysForPasswordExpiration>
<email>email@domain.com</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. 点击Auth并选择Basic



XML身份验证

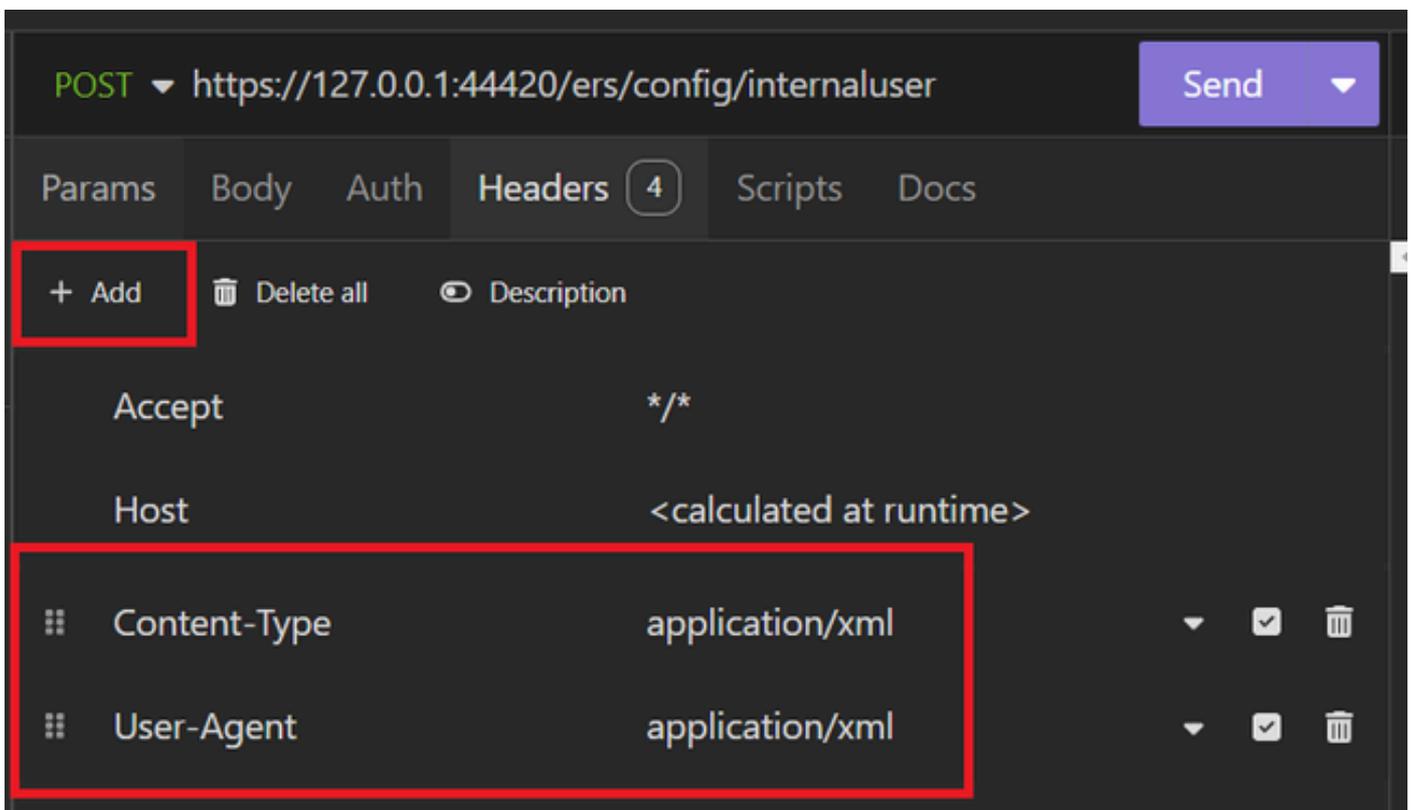
7. 输入ISE GUI凭证。



XML凭证

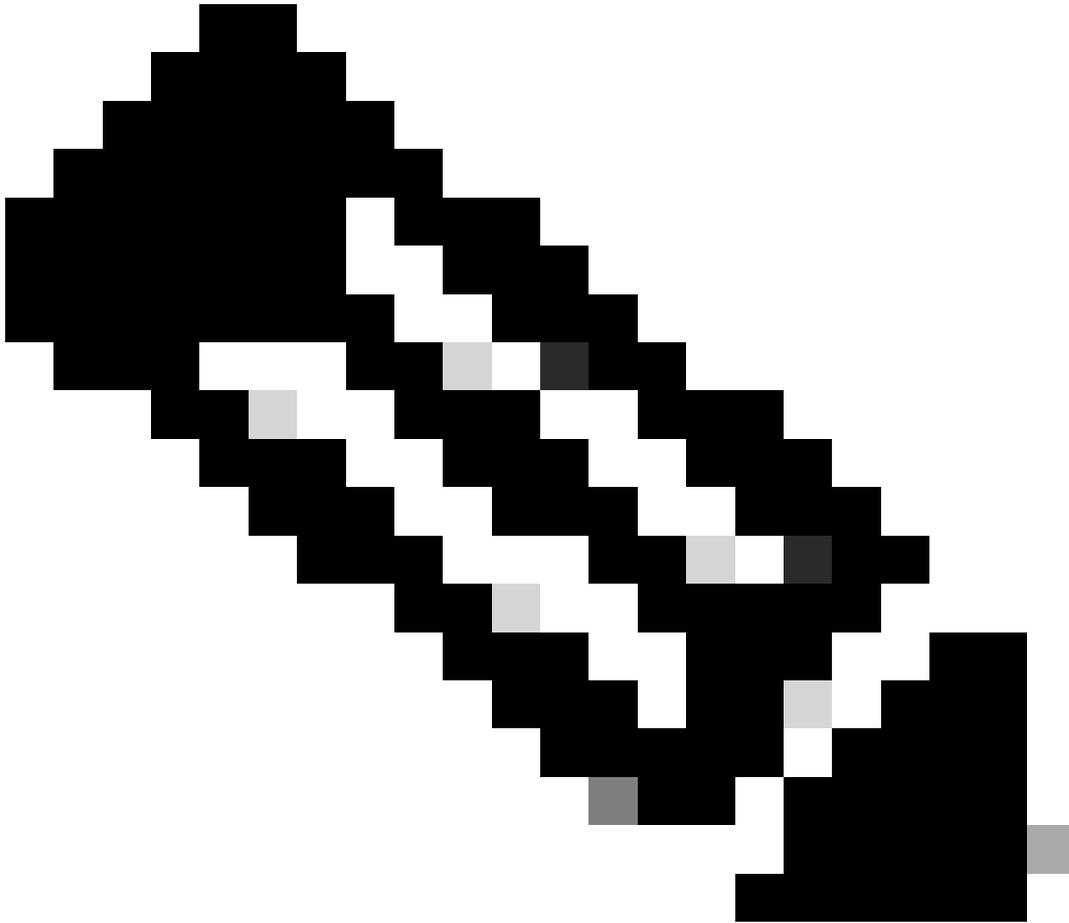
8. 点击Headers以添加以下方法：

- 内容类型：应用/xml
- 接受：application/xml



XML标头

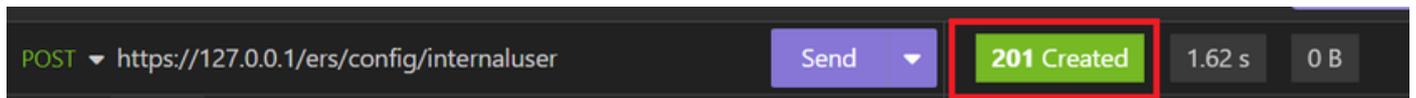
9. 最后，单击“发送”。



注意：如果要身份组分配给新用户帐户，需要使用身份组的ID。有关详细信息，请查看故障排除部分。

## 验证

1. 发送POST请求后，您将看到状态“201 Created”。这表示该过程已成功完成。



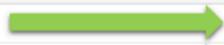
成功的XML请求

2. 打开ISE GUI并导航到管理>身份管理>身份>用户>网络访问用户

## Network Access Users

Selected 0 Total 2  

 Edit  + Add  Change Status  Import  Export  Delete  Duplicate  All 

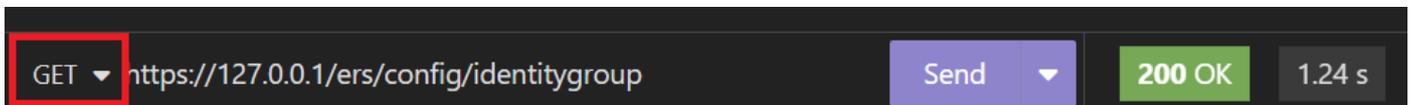
Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	Enabled  User01	this is the firs...	User	Cisco	user1@local...	Employee	 User Account created by JSON
<input type="checkbox"/>	Enabled  User02	description	User2	Cisco	user2@local...	Employee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

验证用户帐户

## 故障排除

### 1. 标识身份组的ID。

使用GET和<https://X.X.X.X/ers/config/identitygroup>查询。



GET选项

JSON输出。

确定描述旁边的ID。

```
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>
```

ID身份组01

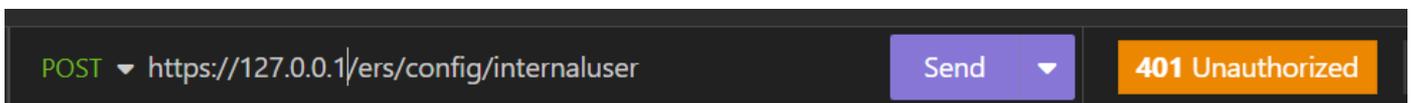
XML输出。

确定描述旁边的ID。

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

ID身份组02

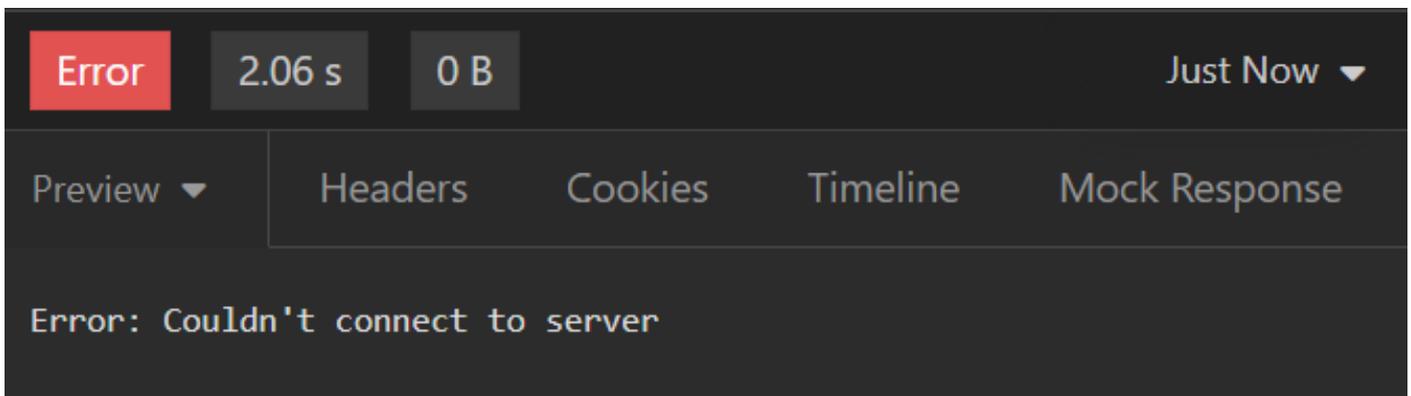
## 2. 401未经授权的错误。



401 个错误

解决方案：检查在Auth部分中配置的访问凭据

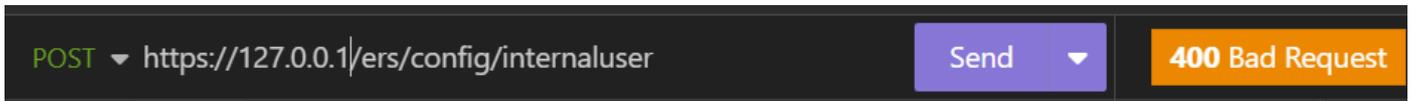
## 3. 错误：无法连接到服务器



连接错误

解决方案：检查在Insomnia中配置的ISE节点的IP地址或验证连接。

## 4. 400错误请求。

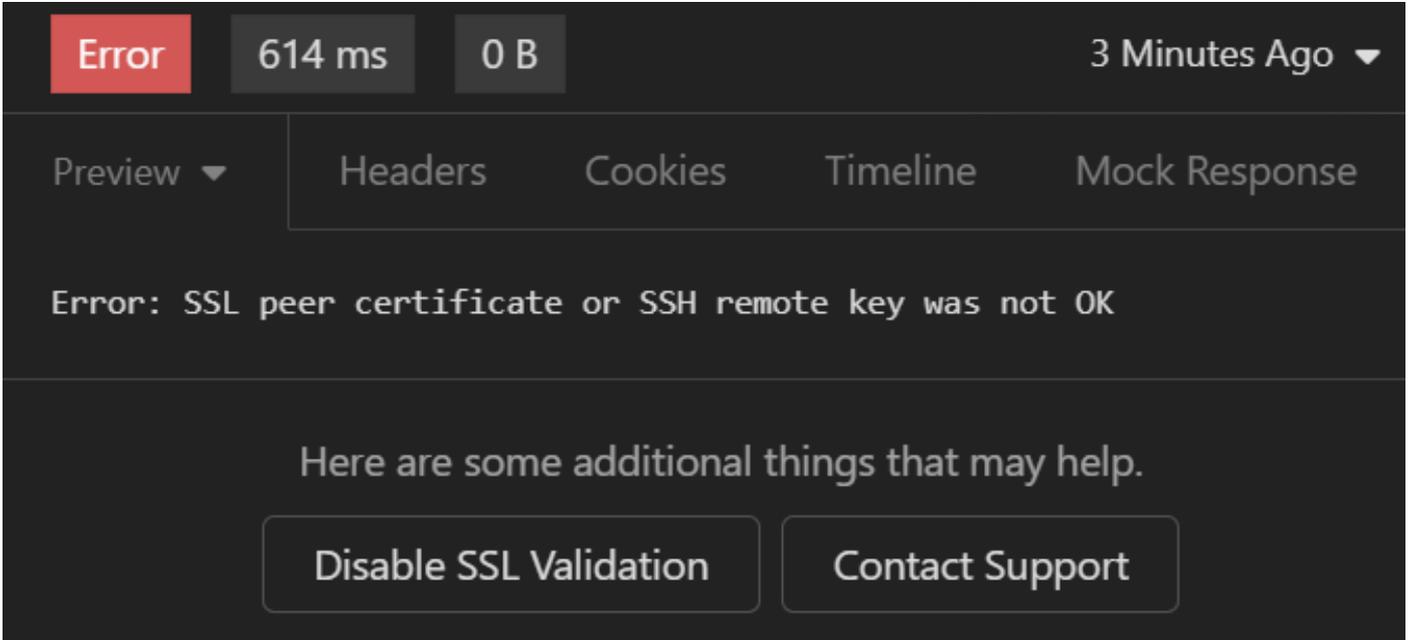


400 个错误

面临此错误的原因有多种，最常见的原因包括：

- 与安全密码策略不匹配
- 某些参数配置错误。
- Sintaxis错误。
- 信息重复。

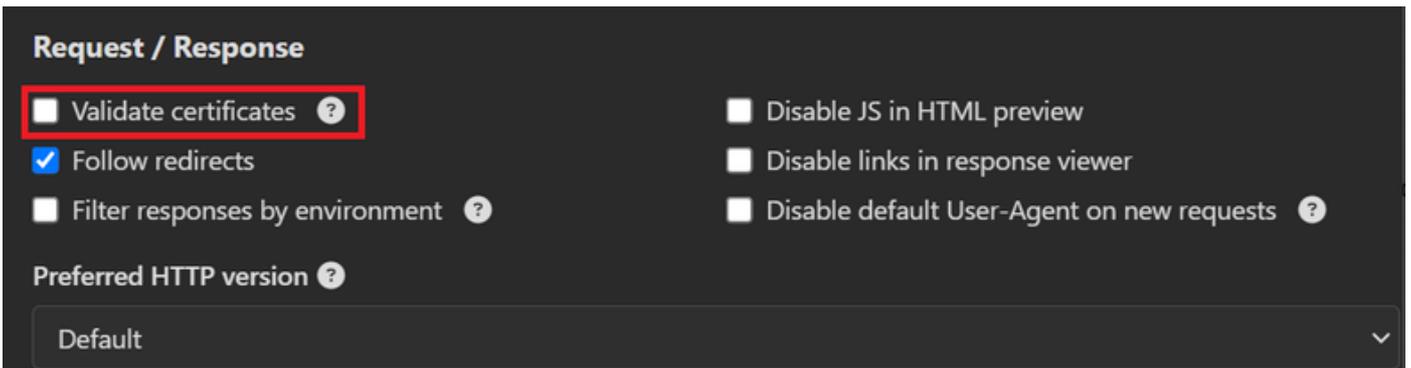
5. 错误：SSL对等证书或SSH远程密钥不正常



SSL证书错误

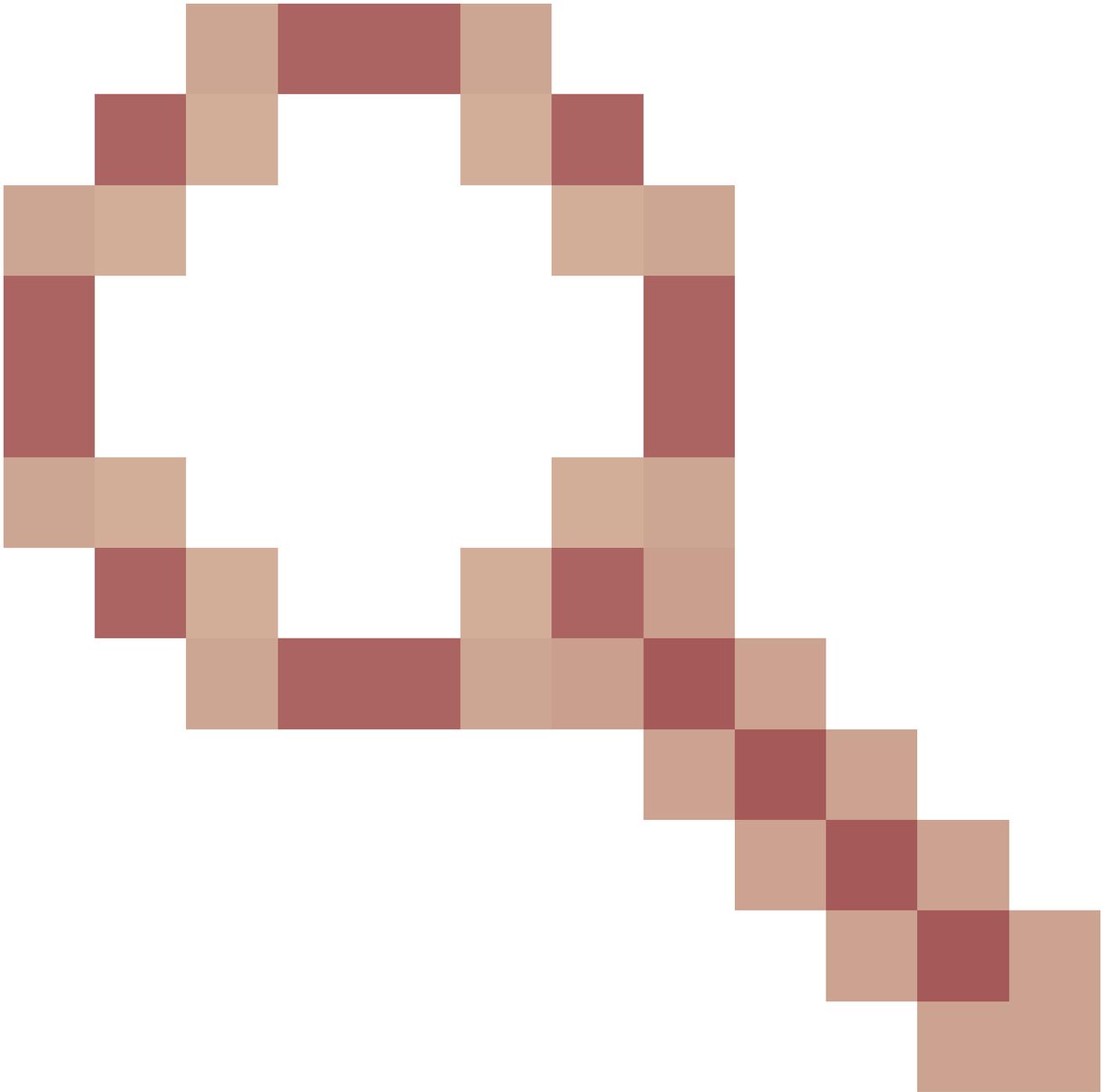
解决方案：

1. 点击禁用SSL验证(Disable SSL Validation)。
2. 在Request / Response下，禁用Validate Certificates选项。



Validate certificates选项

6. [CSCwh71435](#)



缺陷。

使能口令是随机配置的，但您尚未配置它。当启用密码语法删除或保留为空值时会发生此行为。有关详细信息，请查看下一个链接：

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

## API调用引用。

您可以查看有关ISE支持的API调用的所有信息。

1. 导航至“管理”>“系统”>“设置”>“API设置”。
2. 单击ERS API信息链接。

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>

API设置

### 3. 然后单击API文档。

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

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

API文档

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。