Configure Internal Users through JSON or XML and API Calls in ISE 3.3 with Insominia

Contents

Introduction

This document describes the configuration of internal users in Cisco ISE by leveraging either JSON or XML data formats in conjunction with API calls.

Prerequisites

- ISE 3.0 or higher.
- API Client Software.

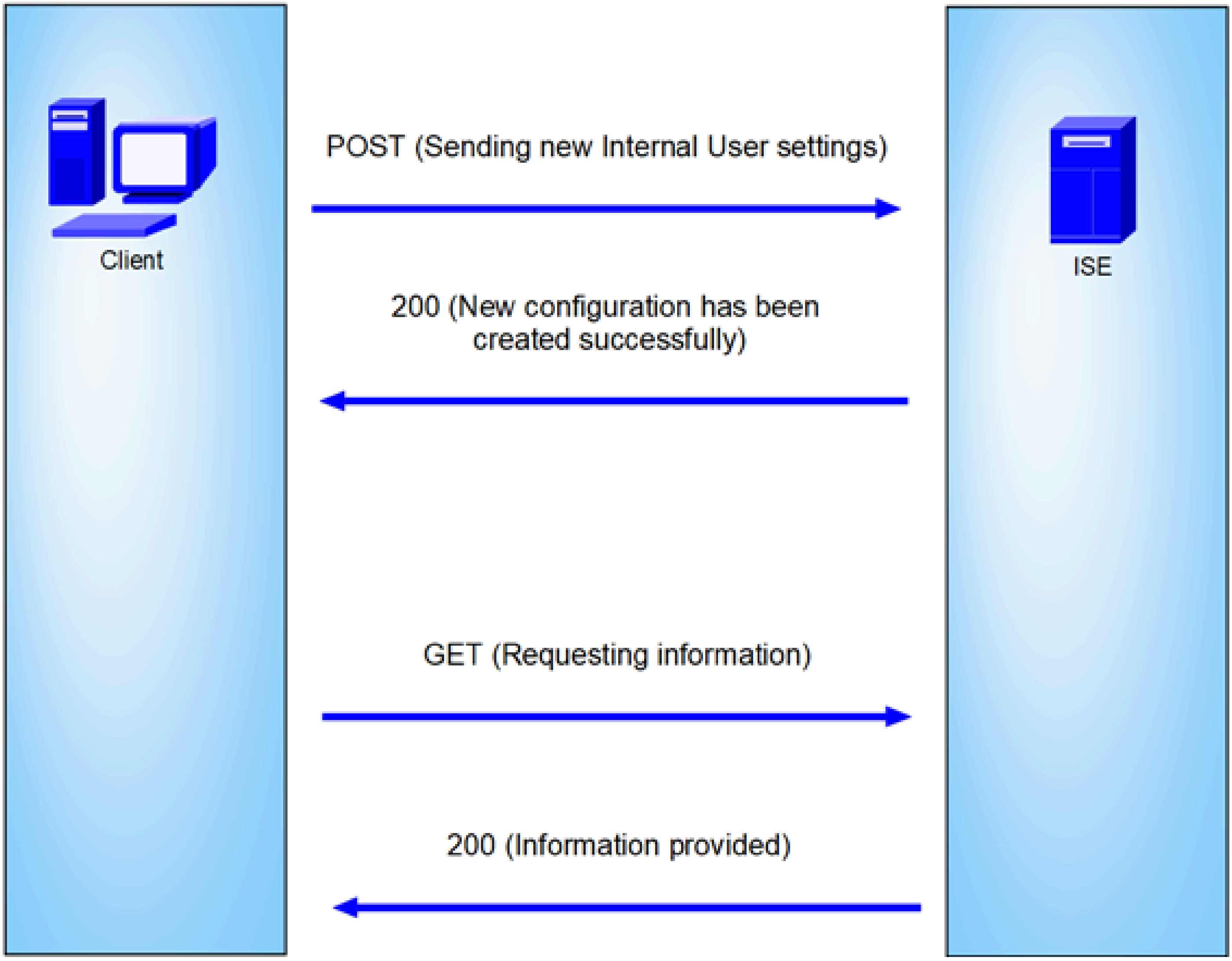
Components Used

- ISE 3.3

- Insominia 9.3.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Network Diagram


Client
ISE
POST (Sending new Internal User settings)
200 (New configuration has been created successfully)
GET (Requesting information)
200 (Information provided)

General topology

GET and POST are two of the most common HTTP methods used in API (Application Programming Interface) calls. They are used to interact with resources on a server, typically to retrieve data or to submit data for processing.

GET API Call

The GET method is used to request data from a specified resource. GET requests are the most common and widely used methods in APIs and websites. When you visit a webpage, your browser is making a GET request to the server hosting the webpage.

POST API Call

The POST method is used to send data to the server to create or update a resource. POST requests are often used when submitting form data or uploading a file.

Configurations

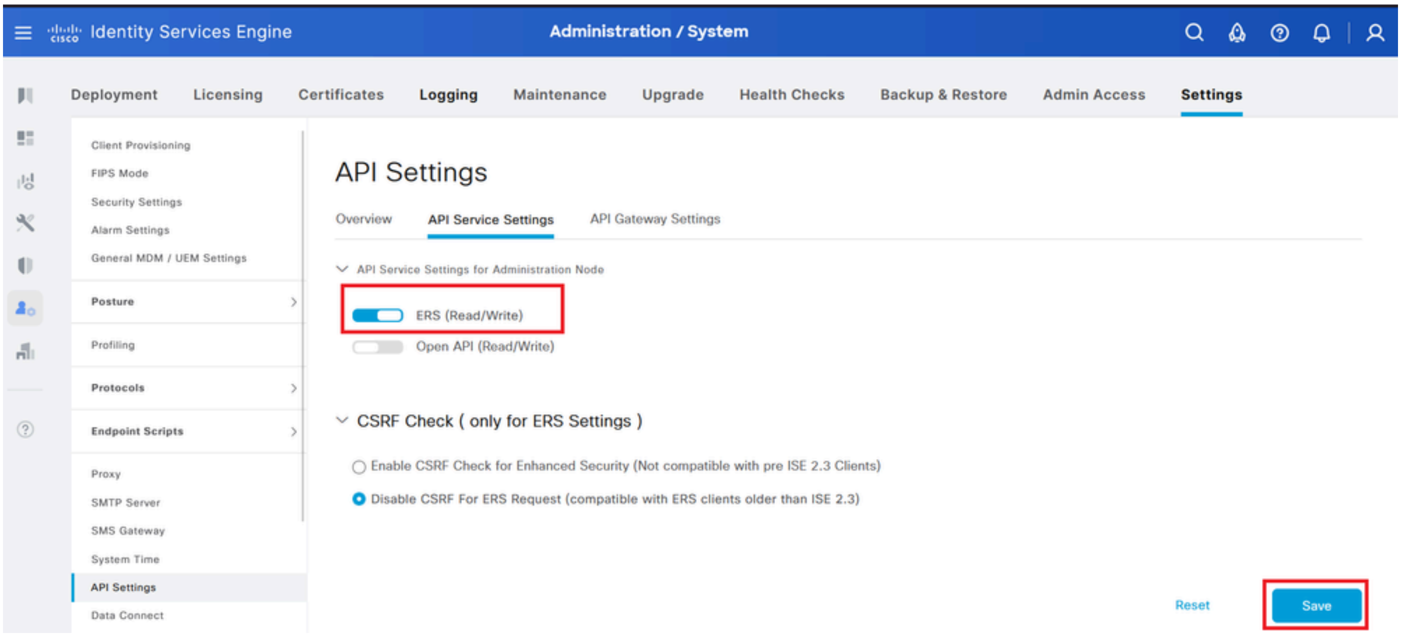
We need to send the exact information from the API Client Software to ISE node to create an Internal User.

ISE configurations

Enable the ERS feature.

1. Navigate to Administration > System > Settings > API Settings > API Service Settings.

2. Enable the ERS (Read/Write) option.



API Settings

API Service Settings for Administration Node

● ERS (Read/Write)

○ Open API (Read/Write)

CSRF Check (only for ERS Settings)

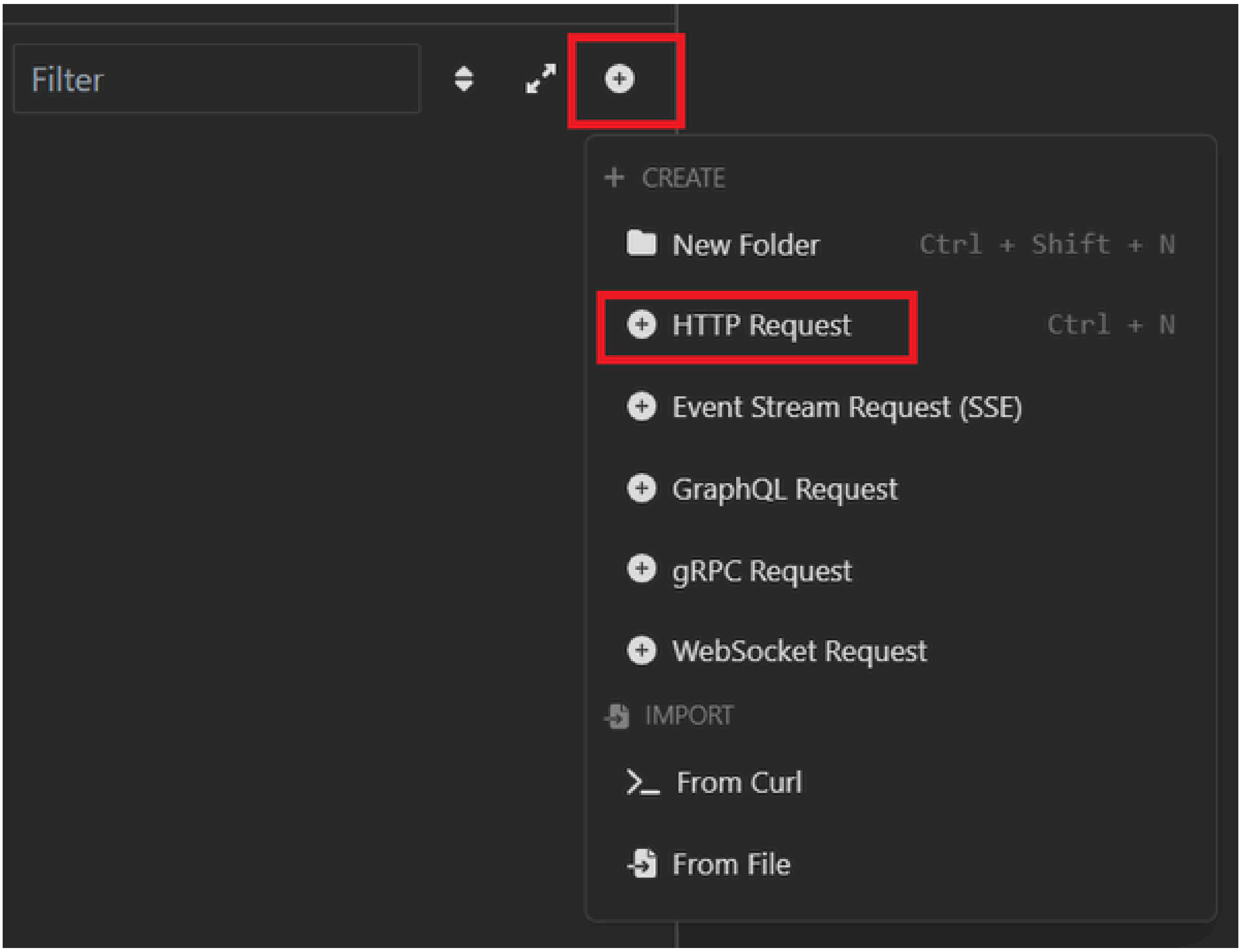
○ Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)

● Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)

API Settings

JSON request.

1. Open Insomnia.
2. Add a new HTTPS request on the left side.

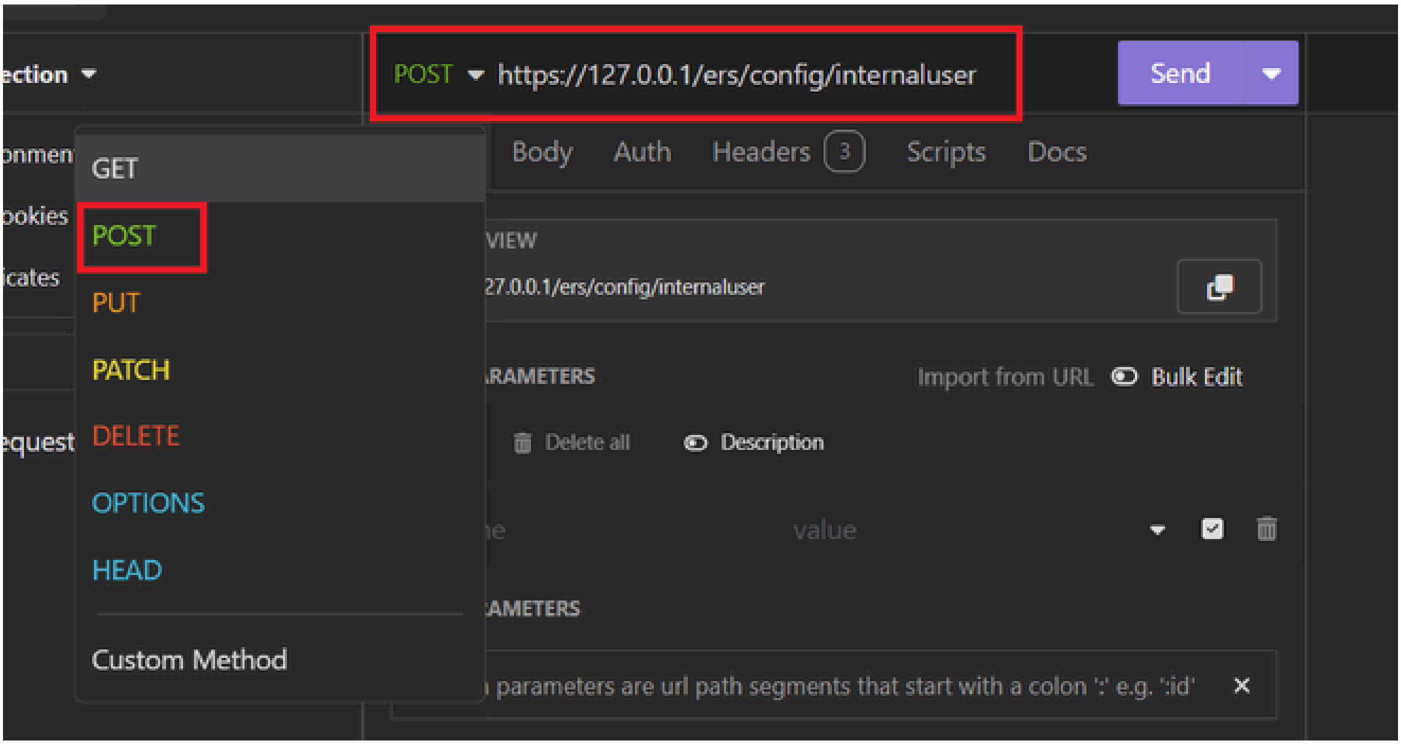


JSON Request

3. You need to choose POST to send the information to your ISE node.

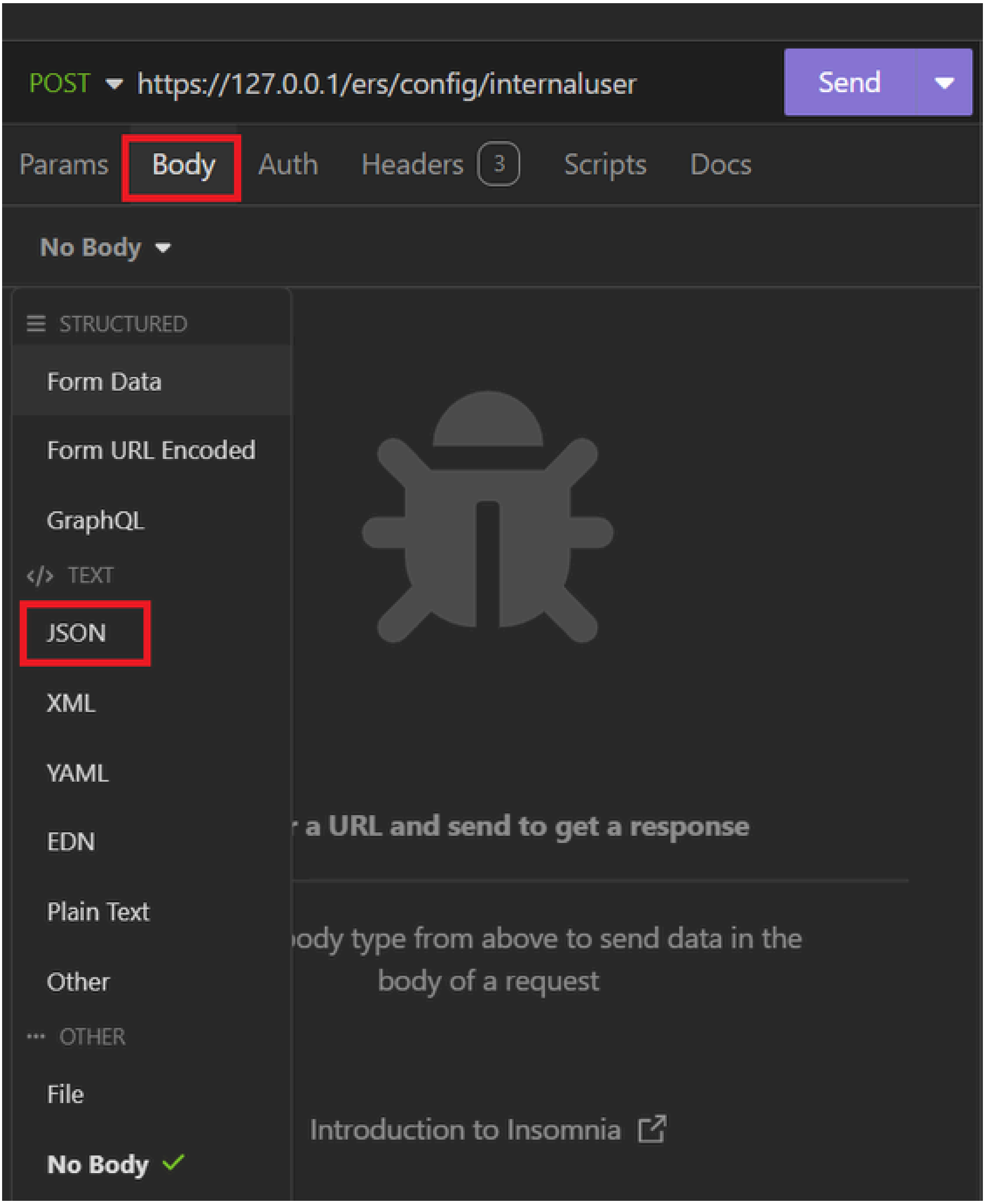
The URL that you need to enter depends on the IP address of you ISE node.

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



JSON POST

4. Then click Body and choose JSON



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

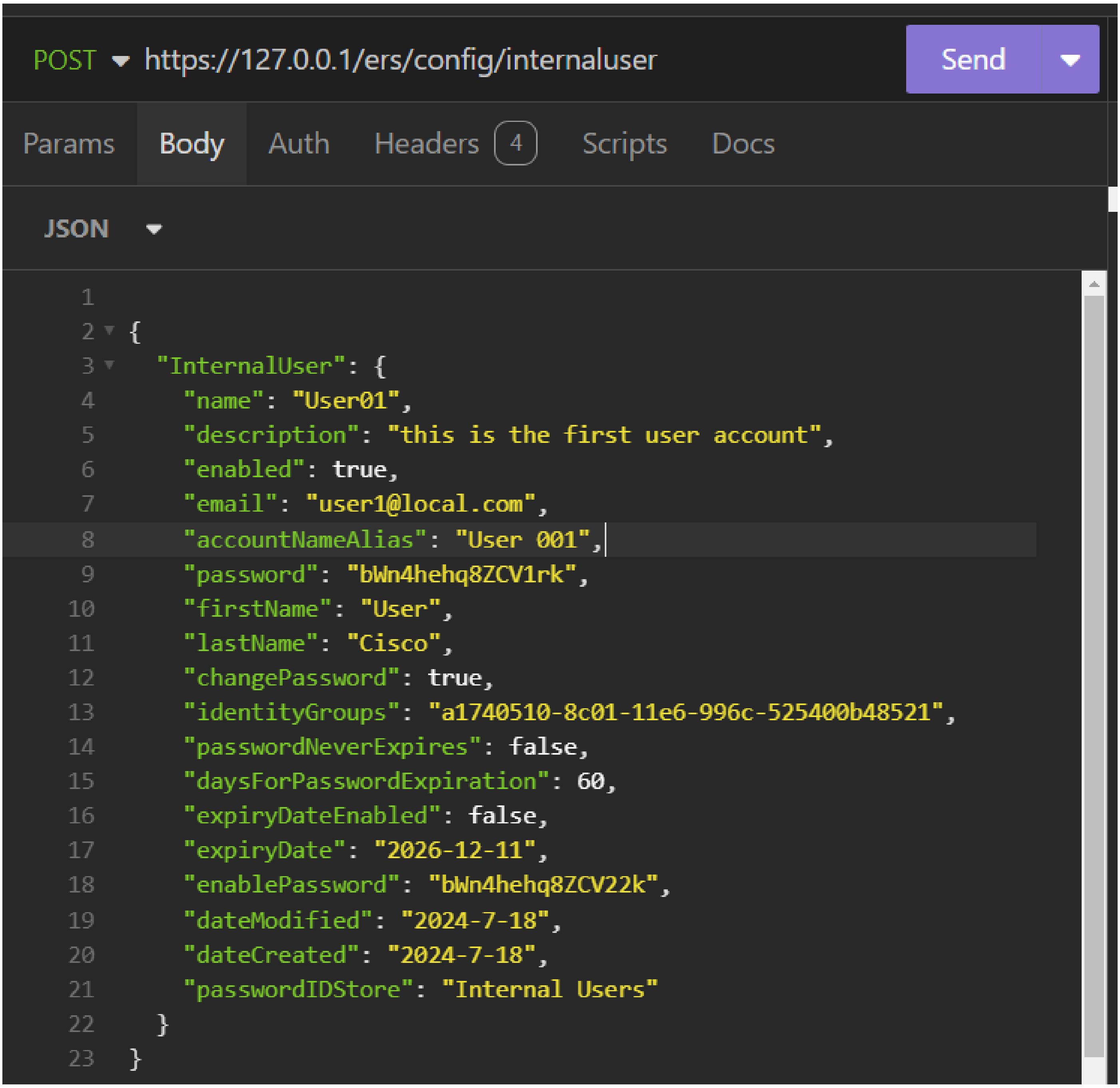
r a URL and send to get a response

body type from above to send data in the body of a request

Introduction to Insomnia

JSON Body

5. You can paste the syntax and change the parameters depending on what you want.



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

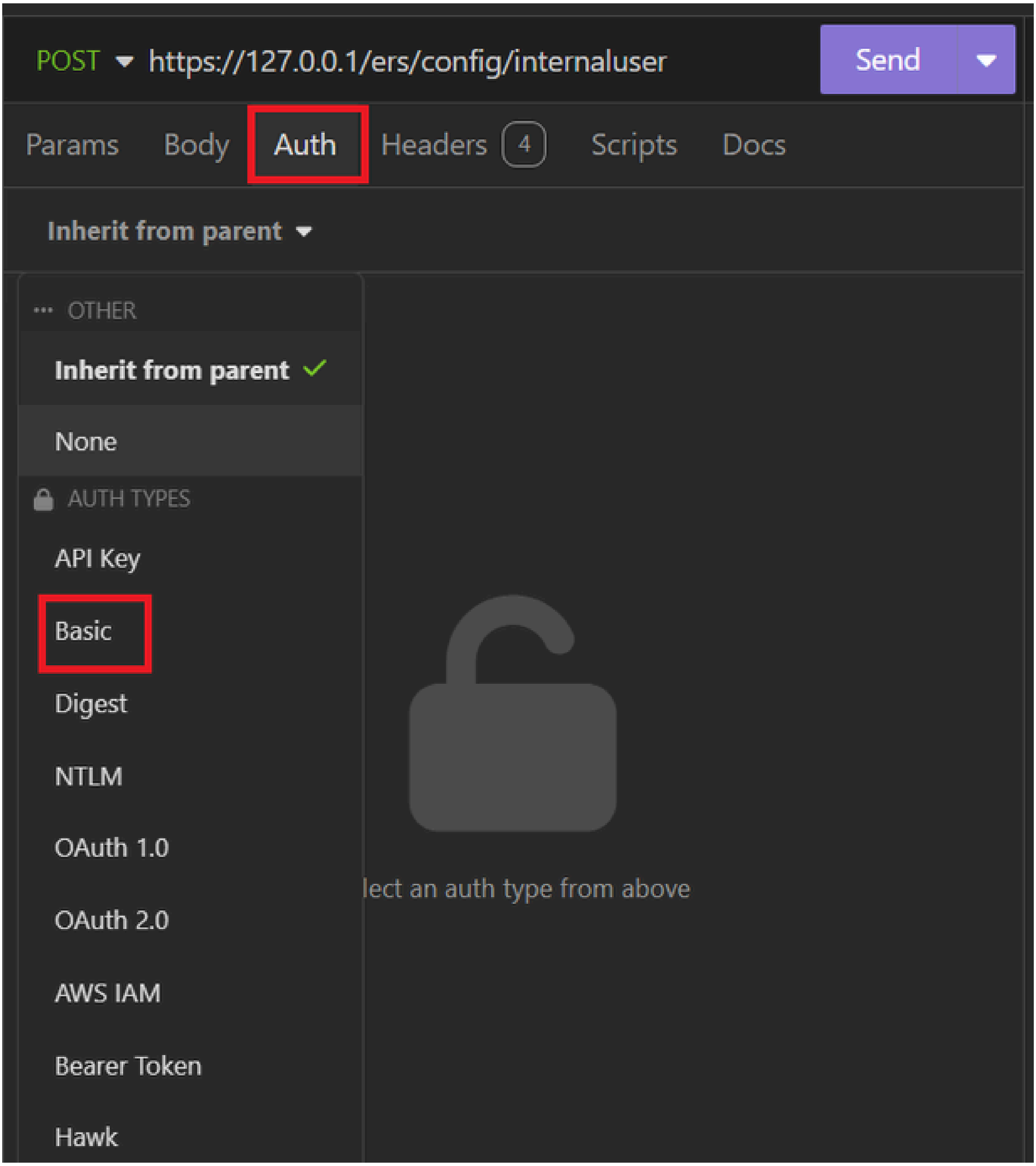
```json

{
  "InternalUser": {
    "name": "User01",
    "description": "this is the first user account",
    "enabled": true,
    "email": "user1@local.com",
    "accountNameAlias": "User 001",
    "password": "bWn4hehq8ZCV1rk",
    "firstName": "User",
    "lastName": "Cisco",
    "changePassword": true,
    "identityGroups": "a1740510-8c01-11e6-996c-525400b48521",
    "passwordNeverExpires": false,
    "daysForPasswordExpiration": 60,
    "expiryDateEnabled": false,
    "expiryDate": "2026-12-11",
    "enablePassword": "bWn4hehq8ZCV22k",
    "dateModified": "2024-7-18",
    "dateCreated": "2024-7-18",
    "passwordIDStore": "Internal Users"
  }
}
```

JSON Syntax

JSON syntax

```
{
  "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"
  }
}
```

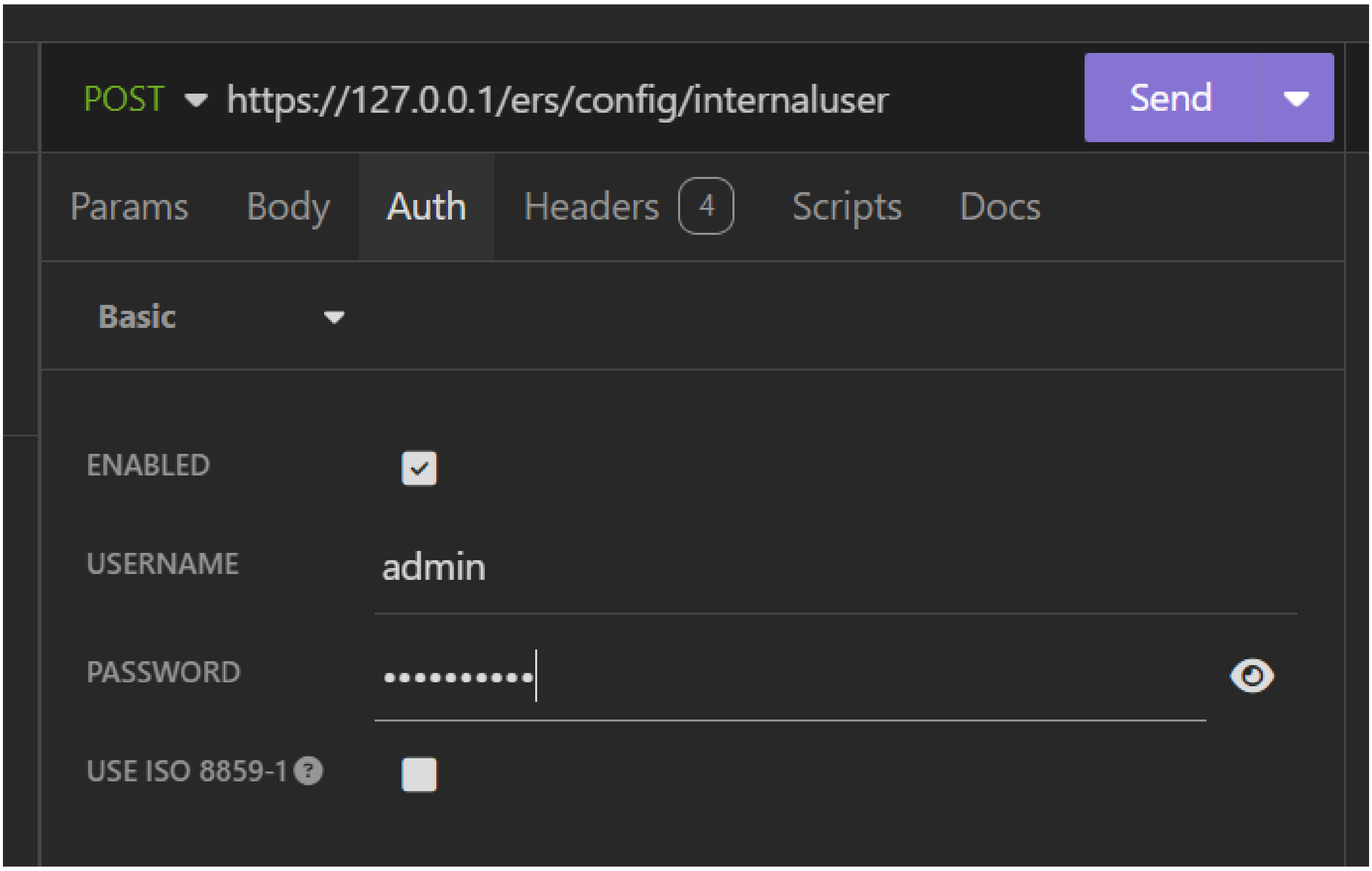
6. Click Auth and choose Basic.



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

JSON auth

7. Enter the ISE GUI credentials.



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

Basic

ENABLED ☑

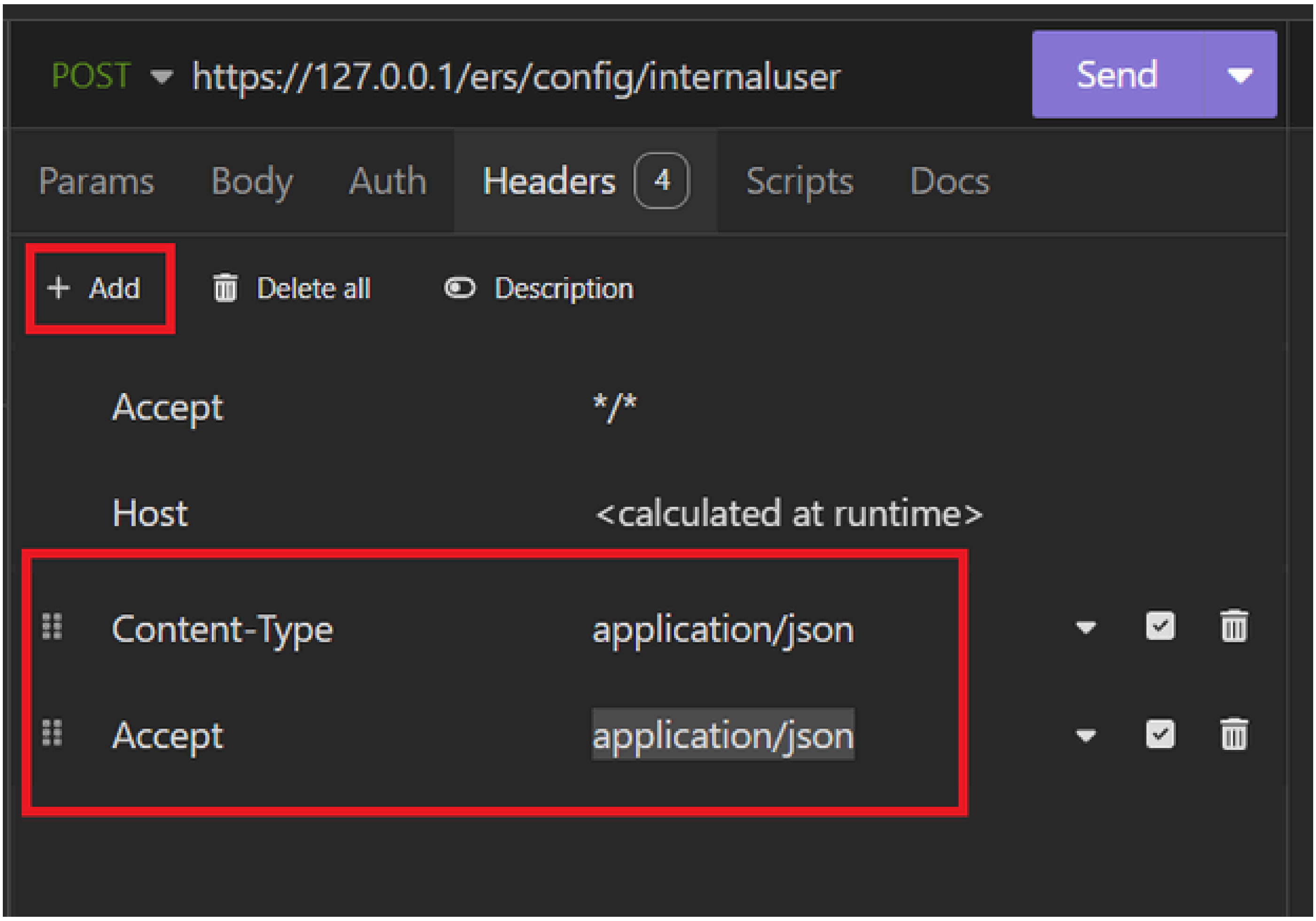
USERNAME admin

PASSWORD ••••••••••

USE ISO 8859-1 □

Admin JSON credentials

8. Click Headers to add the next methods:
    - Content-Type: application/json
    - Accept: application/json



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

Accept	*/*
Host	<calculated at runtime>
Content-Type	application/json
Accept	application/json

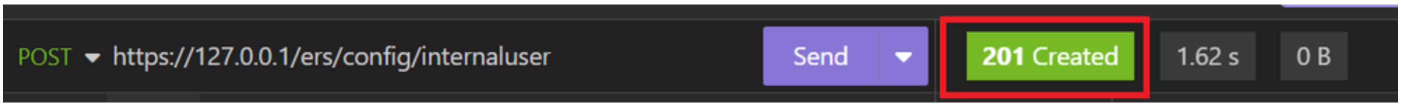
JSON Headers

9. Finally, click Send.

Note: If you want to assign an Identity Group to the new user account, you need to use the ID of the Identity Group. Check the **Troubleshooting section** for more information.

Validation

1. After sending the POST request you are going to see the status “201 Created”. It means that the process has been completed successfully.

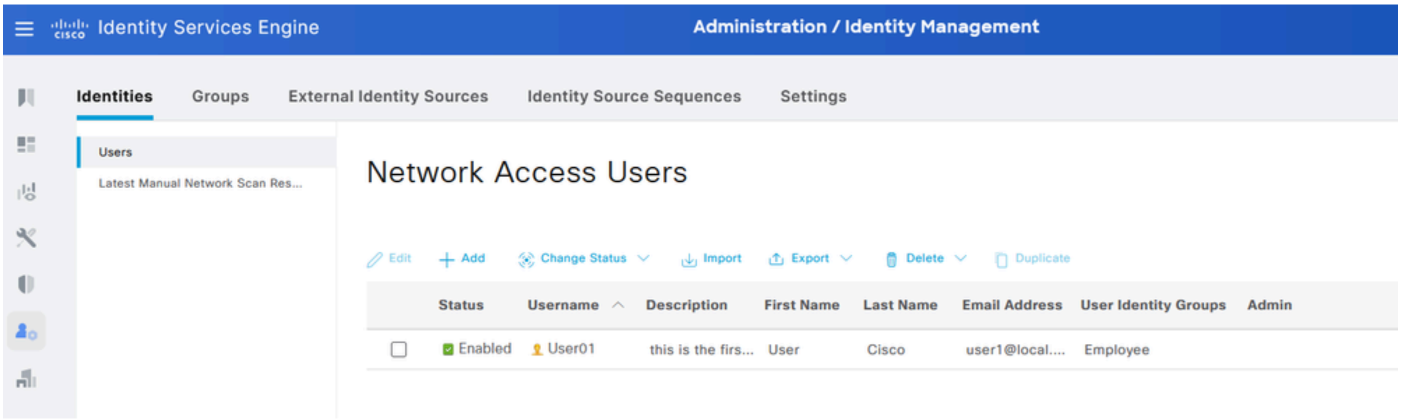


POST https://127.0.0.1/ers/config/internaluser

201 Created 1.62 s 0 B

Successful JSON request

2. Open the ISE GUI and navigate to Administration > Identity Management > Identities > Users > Network Access Users



Identity Services Engine — Administration / Identity Management

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Users

Latest Manual Network Scan Res...

Network Access Users

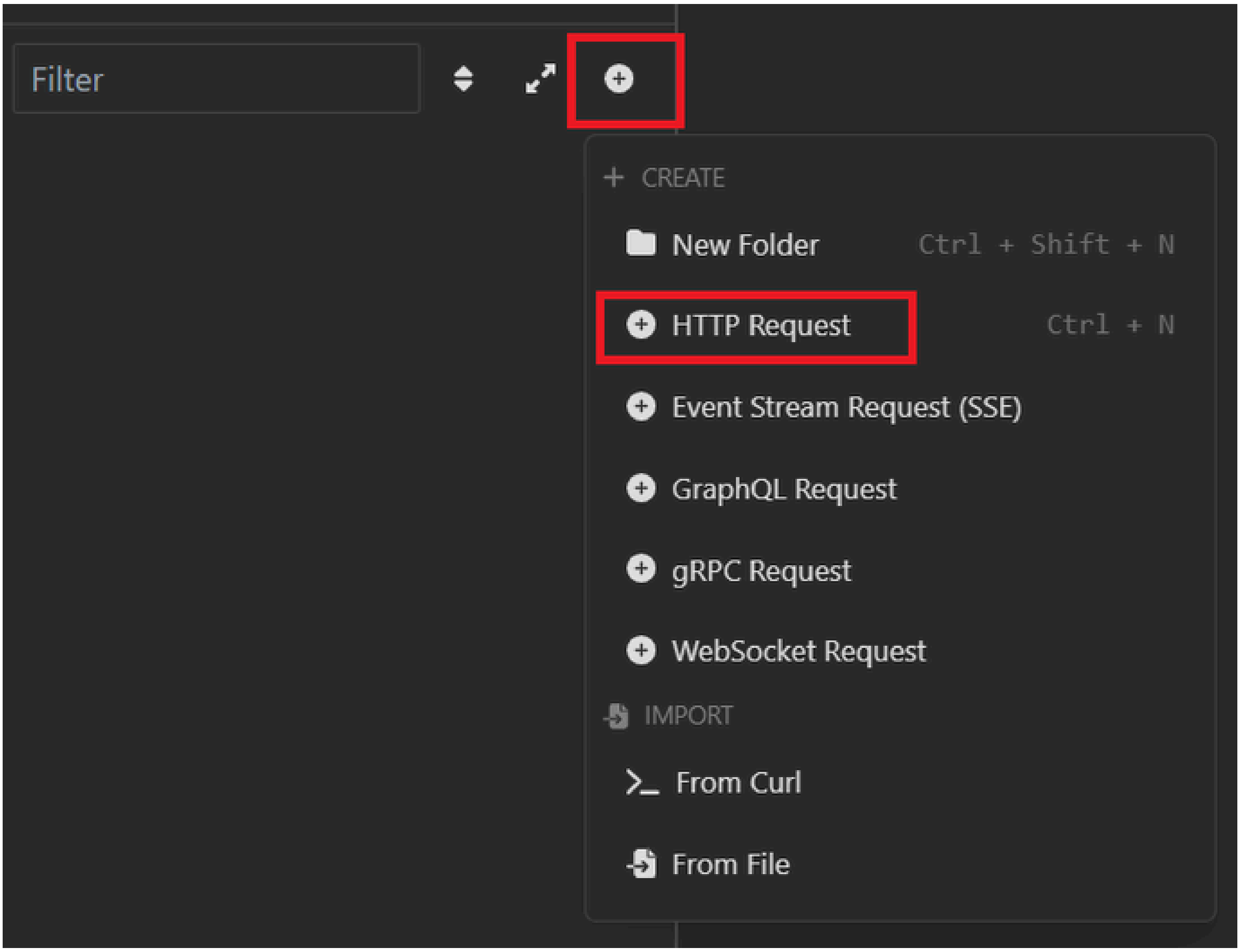
Edit | + Add | Change Status | Import | Export | Delete | Duplicate

	Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
□	Enabled	User01	this is the firs...	User	Cisco	user1@local....	Employee	

JSON User Account

XML request

1. Open Insomnia.
2. Add a new HTTPS request on the left side.

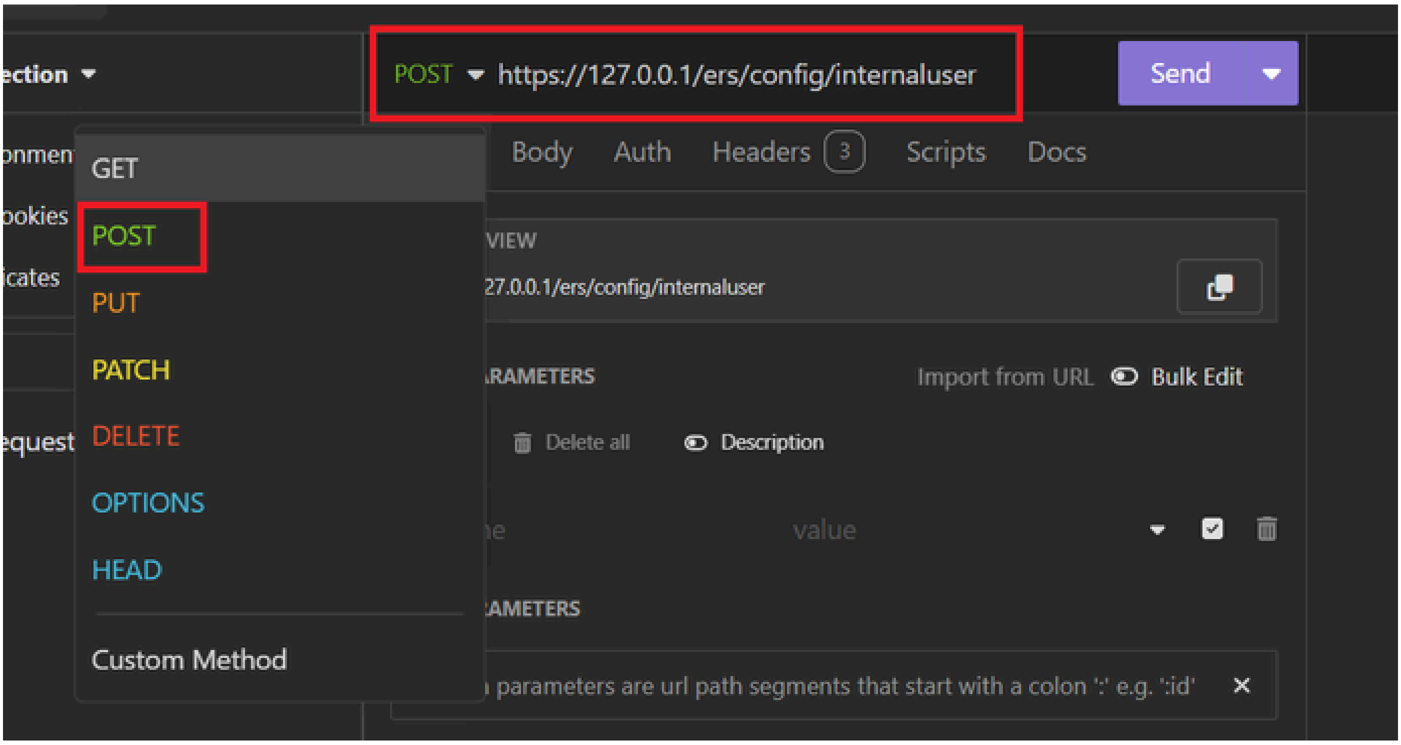


XML Request

3. You need to choose POST to send the information to your ISE node.

The URL that you need to enter depends on the IP address of you ISE node.

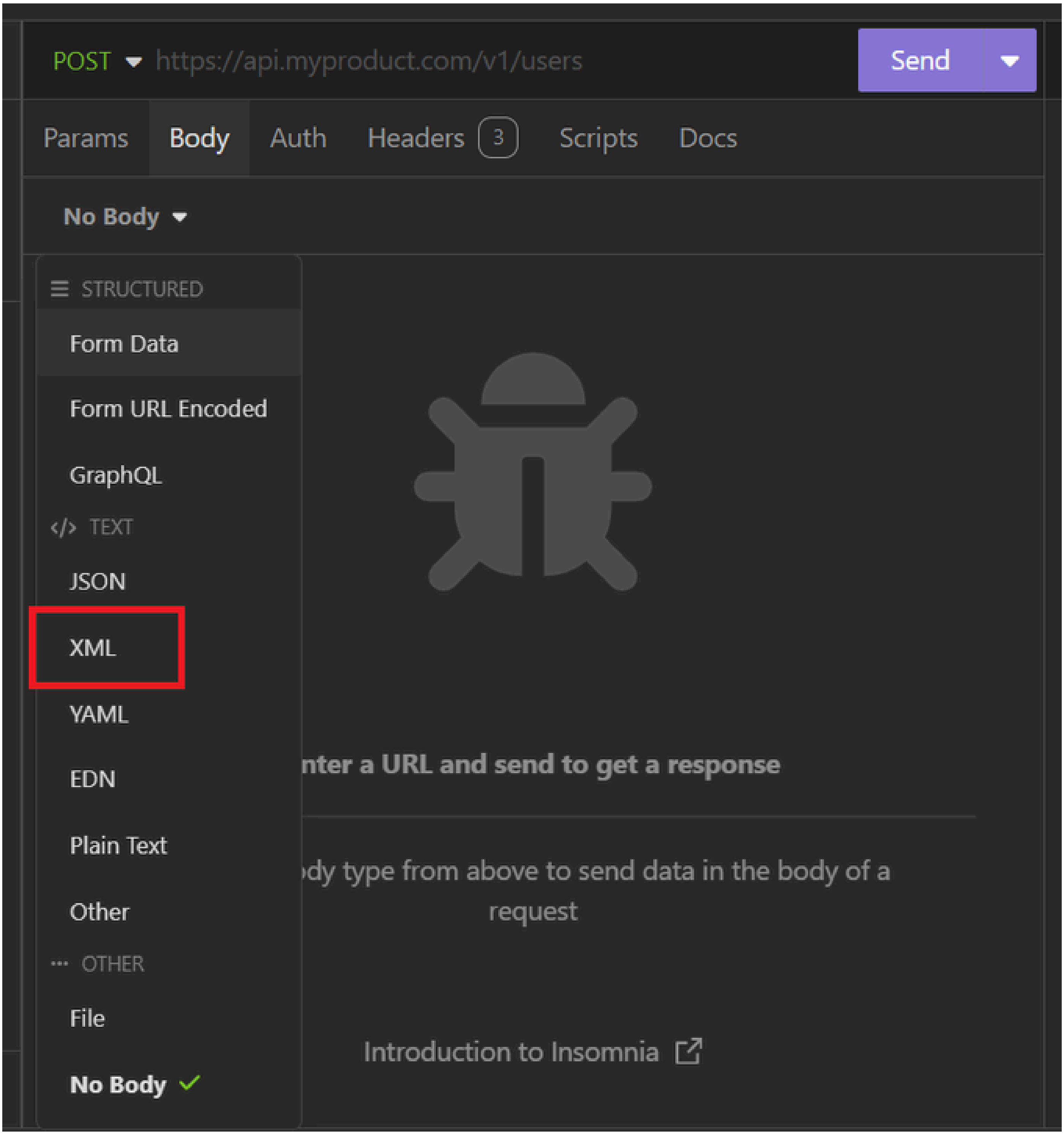
URL: https://x.x.x.x/ers/config/internaluser



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

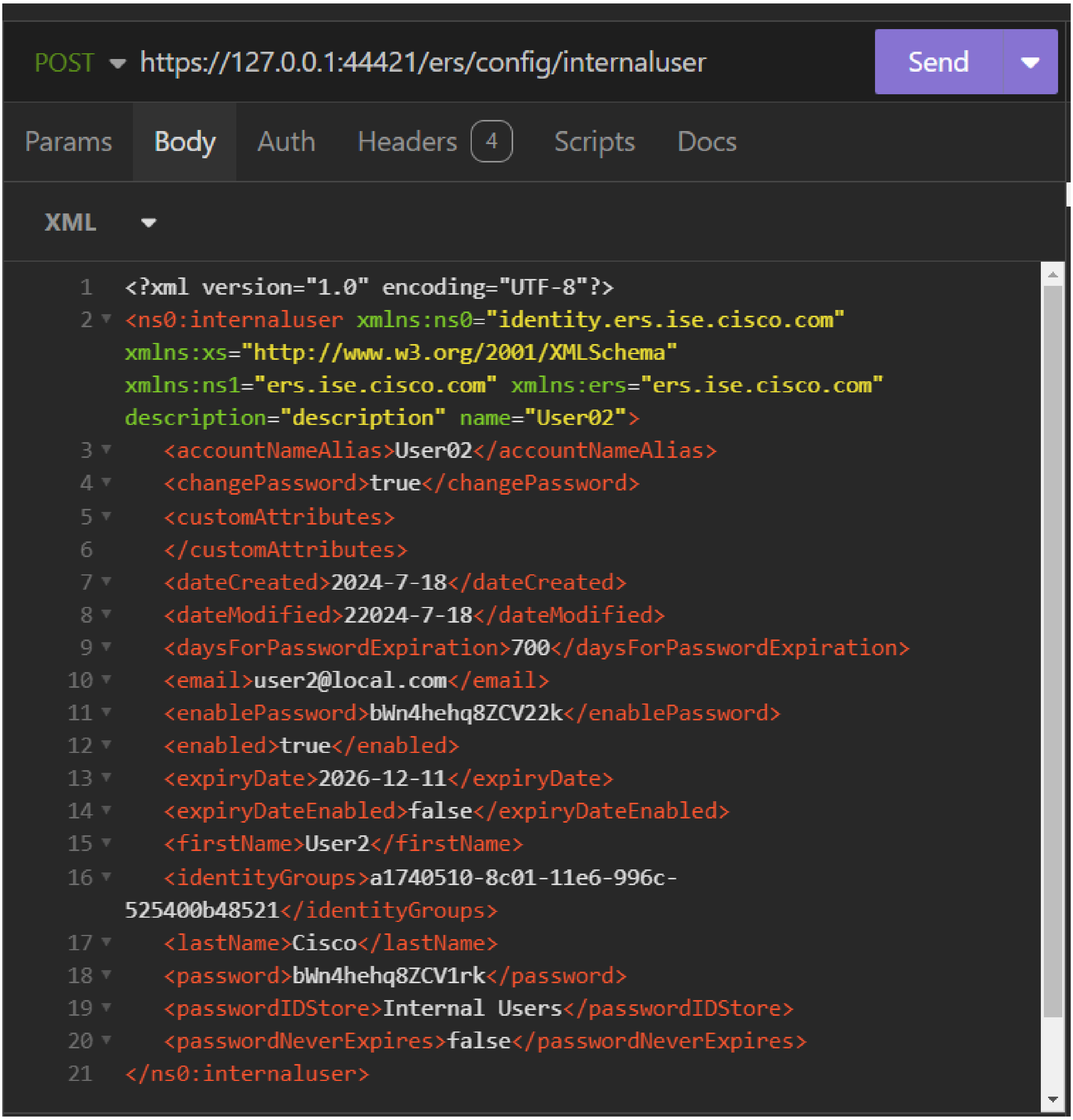
XML POST

4. Then click Body and choose XML.



XML Body

5. You can paste the syntax and change the parameters depending on what you want.



```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" xmlns:ns1="ers.ise.cisco.com" xmlns:ers="ers.ise.cisco.com" description="description" name="User02">
   <accountNameAlias>User02</accountNameAlias>
   <changePassword>true</changePassword>
   <customAttributes>
   </customAttributes>
   <dateCreated>2024-7-18</dateCreated>
   <dateModified>22024-7-18</dateModified>
   <daysForPasswordExpiration>700</daysForPasswordExpiration>
   <email>user2@local.com</email>
   <enablePassword>bWn4hehq8ZCV22k</enablePassword>
   <enabled>true</enabled>
   <expiryDate>2026-12-11</expiryDate>
   <expiryDateEnabled>false</expiryDateEnabled>
   <firstName>User2</firstName>
   <identityGroups>a1740510-8c01-11e6-996c-525400b48521</identityGroups>
   <lastName>Cisco</lastName>
   <password>bWn4hehq8ZCV1rk</password>
   <passwordIDStore>Internal Users</passwordIDStore>
   <passwordNeverExpires>false</passwordNeverExpires>
</ns0:internaluser>
```

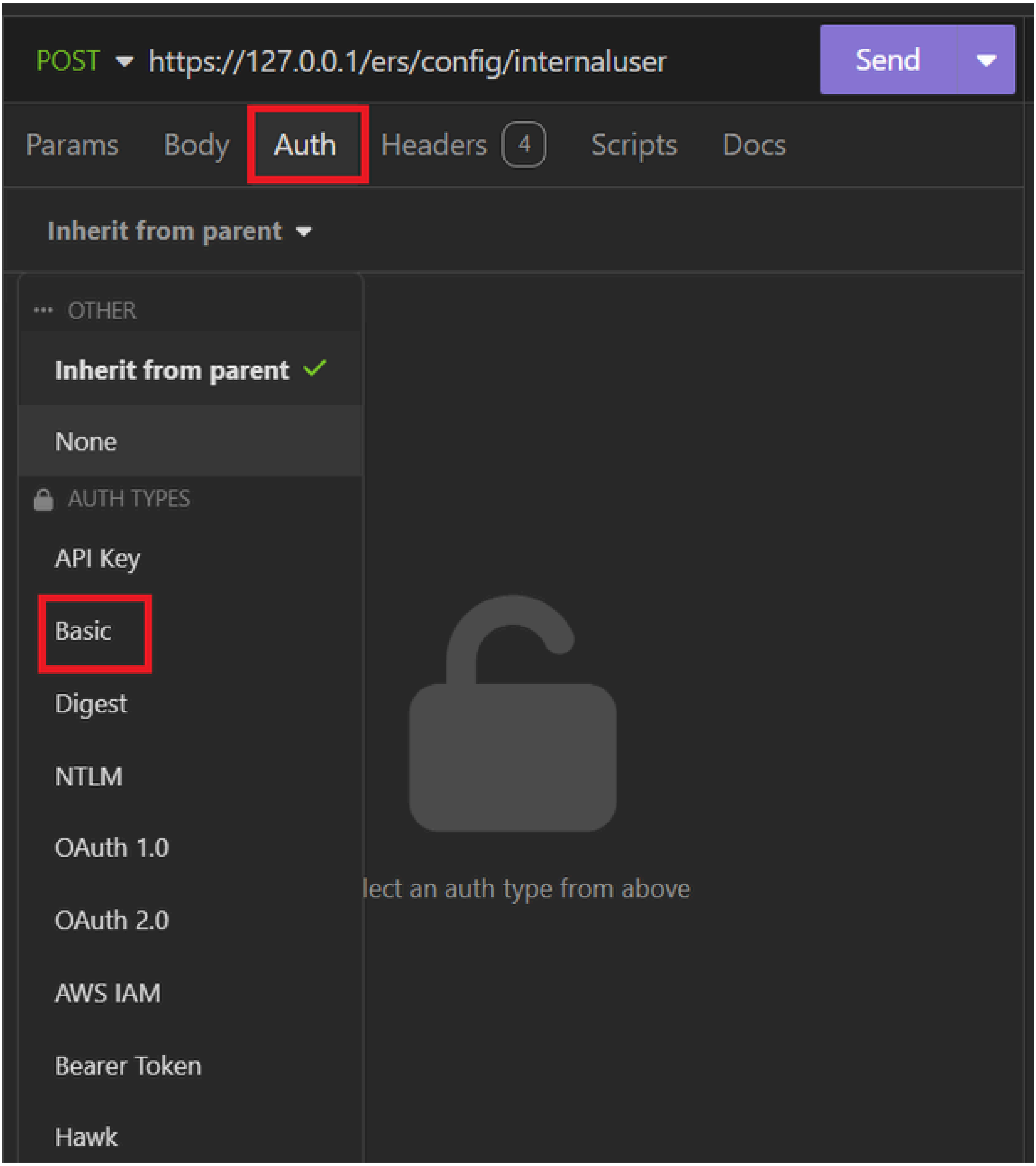
XML Post

XML syntax

```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>
```

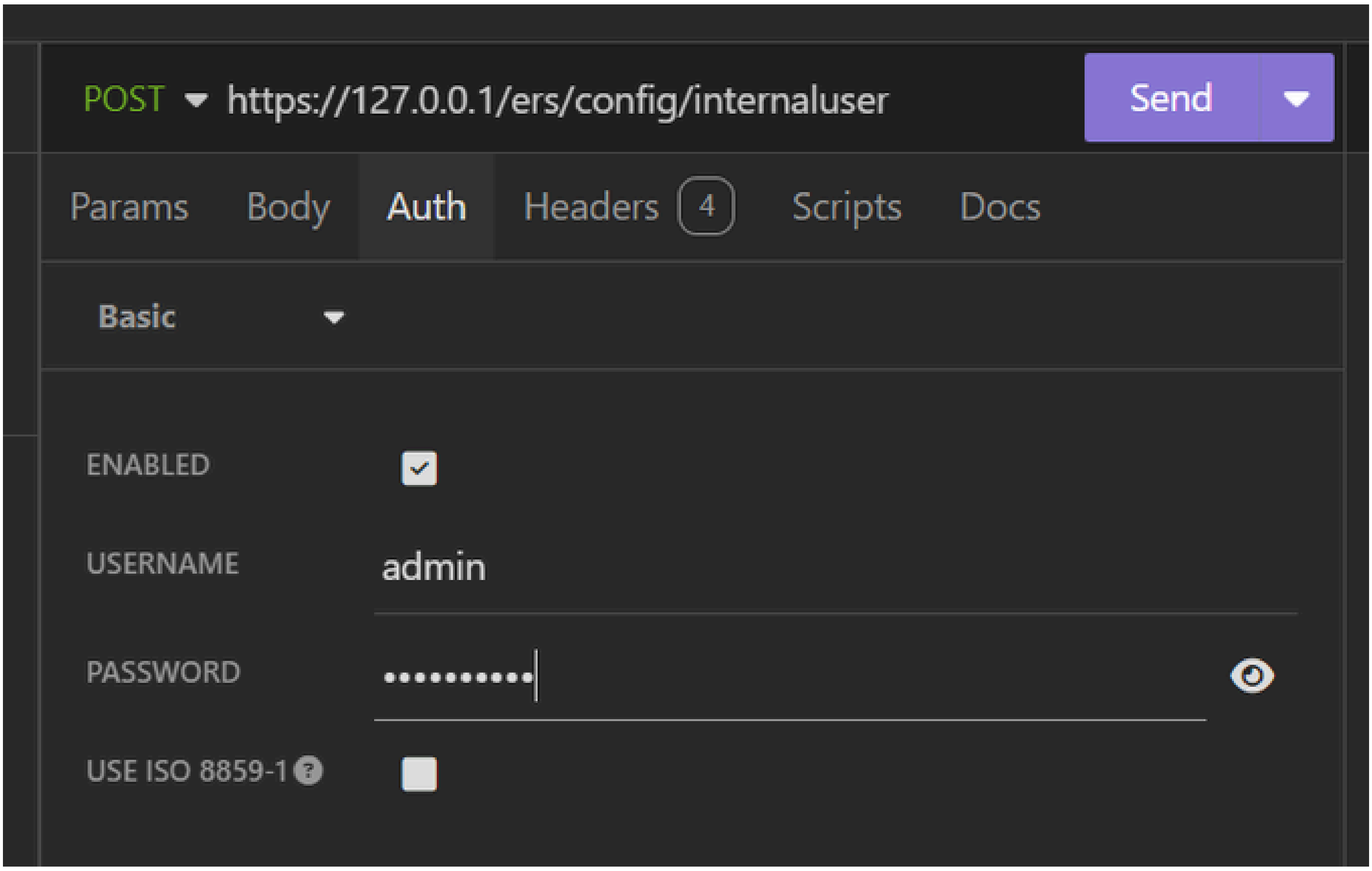
6. Click Auth and choose Basic



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

XML auth

7. Enter the ISE GUI credentials.



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

Basic

ENABLED ☑

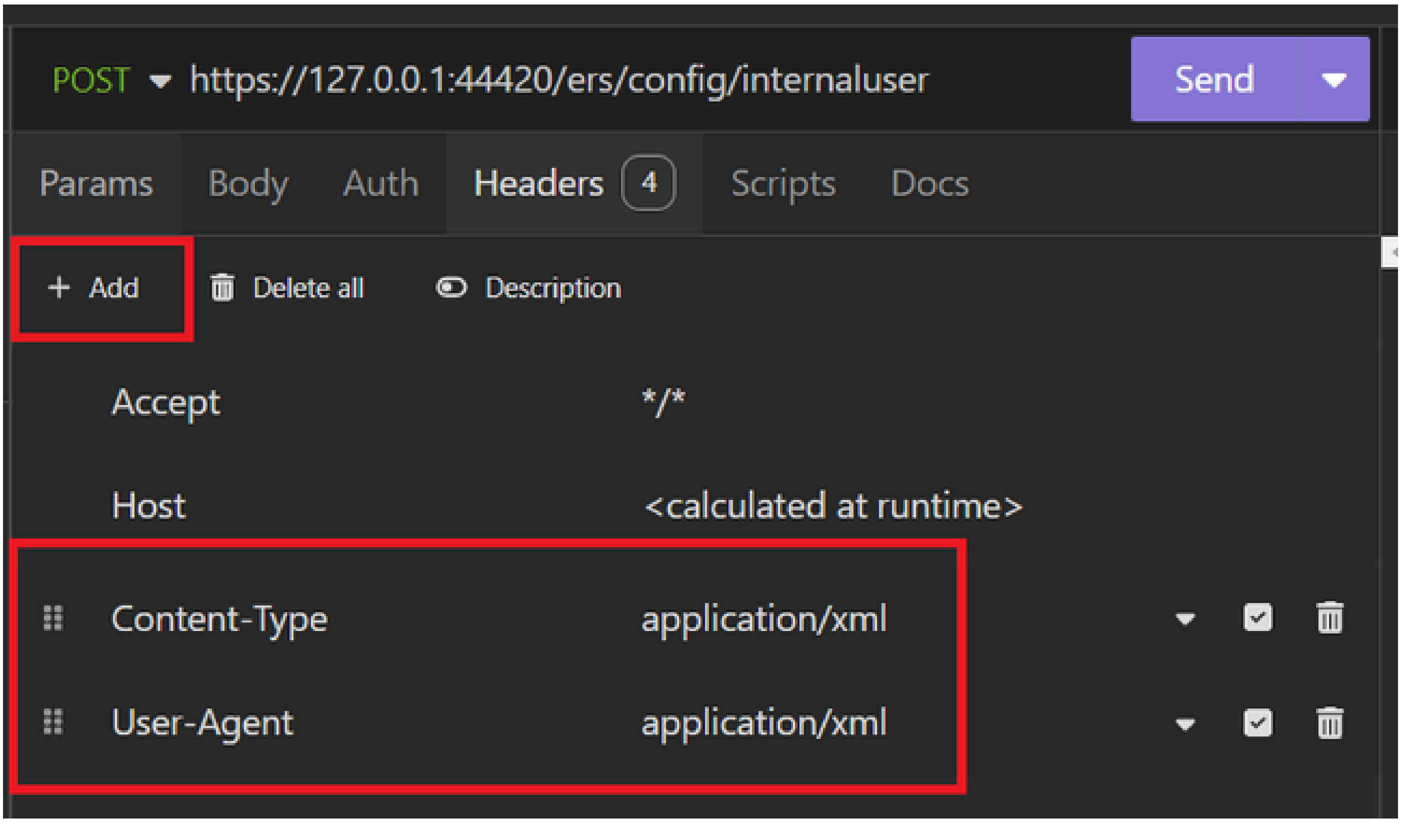
USERNAME admin

PASSWORD ••••••••••

USE ISO 8859-1 □

XML credentials

8. Click Headers to add the next methods:
   - Content-Type: application/xml
   - Accept: application/xml



POST https://127.0.0.1:44420/ers/config/internaluser

Accept	*/*
Host	<calculated at runtime>
Content-Type	application/xml
User-Agent	application/xml

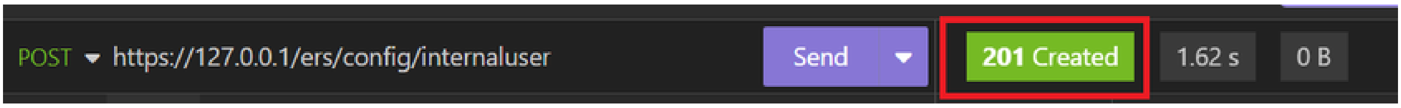
XML Headers

9. Finally, click Send.

Note: If you want to assign an Identity Group to the new user account, you need to use the ID of the Identity Group. Check the **Troubleshooting section** for more information.

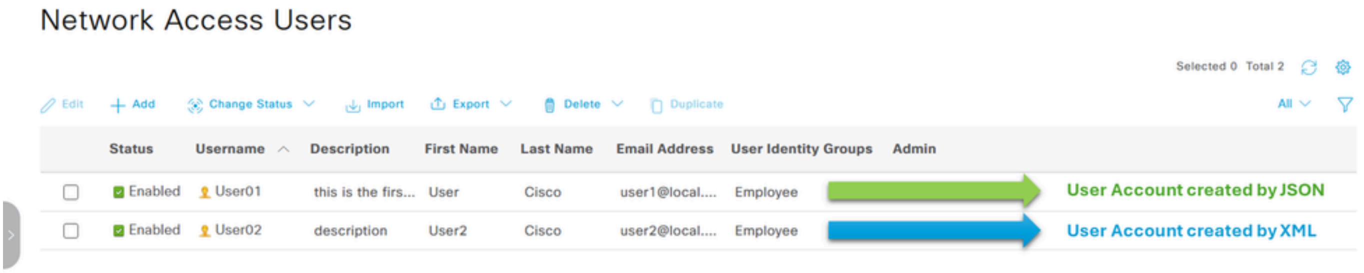
Validation

1. After sending the POST request you are going to see the status “201 Created”. It means that the process has been completed successfully.



Successful XML request

2. Open the ISE GUI and navigate to Administration > Identity Management > Identities > Users > Network Access Users



Network Access Users

	Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
□	Enabled	User01	this is the firs...	User	Cisco	user1@local....	Employee	
□	Enabled	User02	description	User2	Cisco	user2@local....	Employee	

User Account created by JSON

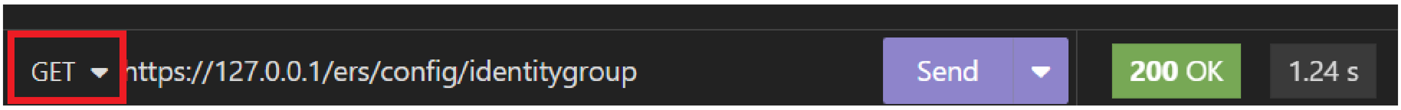
User Account created by XML

Validation of User Accounts

Troubleshoot

1. Identify the ID of the identity group.

Use GET and the https://X.X.X.X/ers/config/identitygroup query.

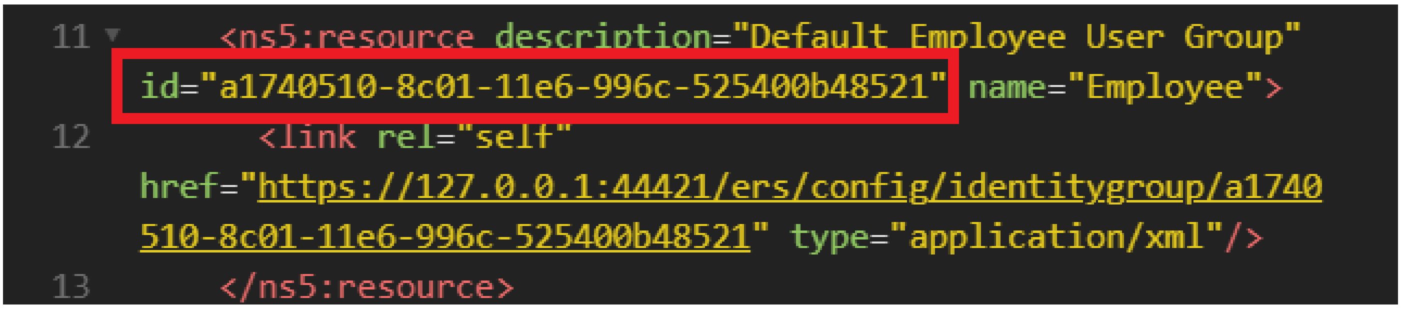


```
GET ▾  https://127.0.0.1/ers/config/identitygroup
```

GET option

JSON output.

Identify the ID next to the description.

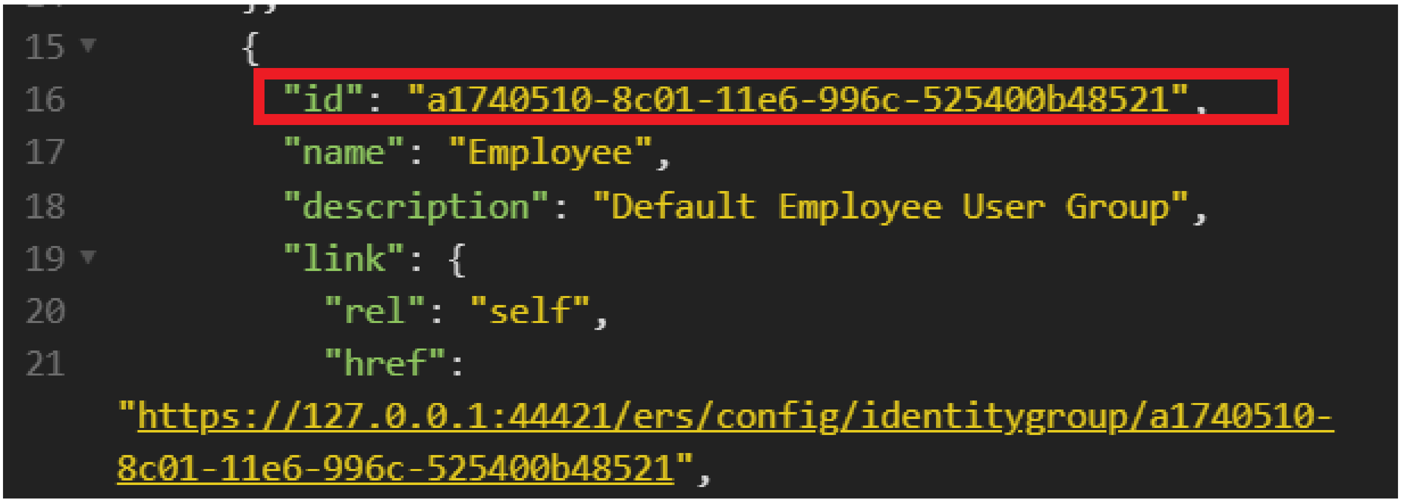


```
    <ns5:resource description="Default Employee User Group"
id="a1740510-8c01-11e6-996c-525400b48521" name="Employee">
        <link rel="self"
href="https://127.0.0.1:44421/ers/config/identitygroup/a1740510-8c01-11e6-996c-525400b48521" type="application/xml"/>
    </ns5:resource>
```

ID Identity Group 01

XML output.

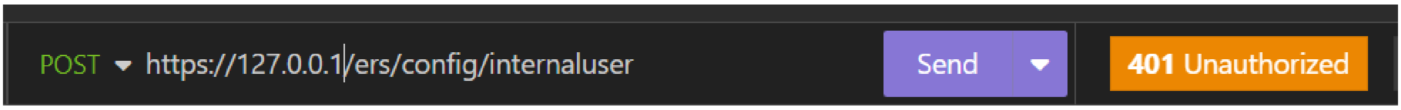
Identify the ID next to the description.



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

ID Identity Group 02

2. 401 Unauthorized error.

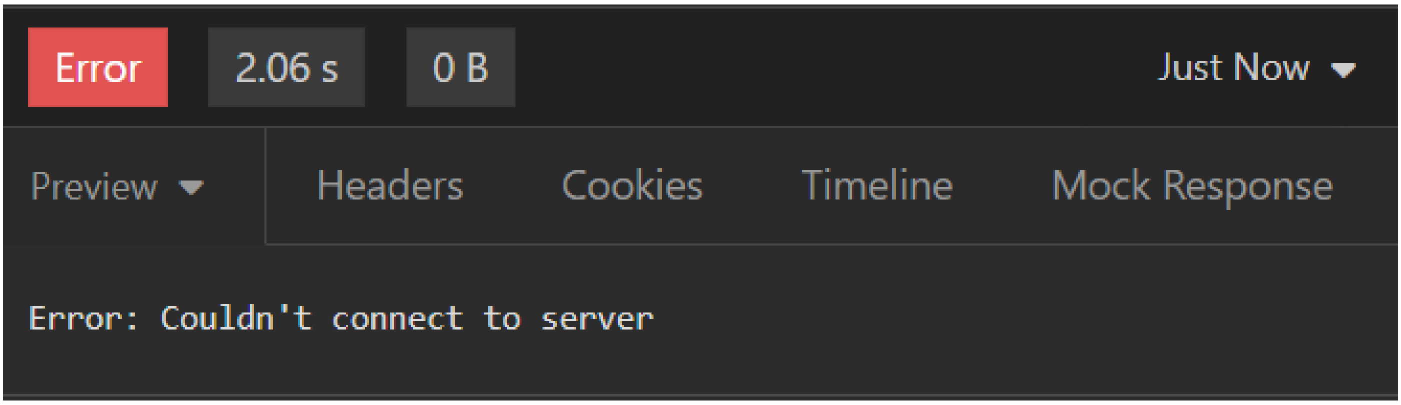


POST https://127.0.0.1/ers/config/internaluser

401 error

Solution: Check the access credentials configured in the Auth section

3. Error: Could not connect to server

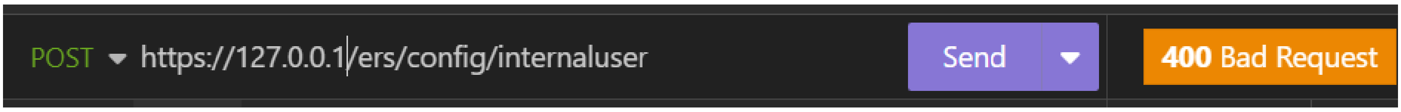


```
Error: Couldn't connect to server
```

Connection error

Solution: Check the IP address of the ISE node configured in Insomnia or validate the connectivity.

4. 400 Bad Request.



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

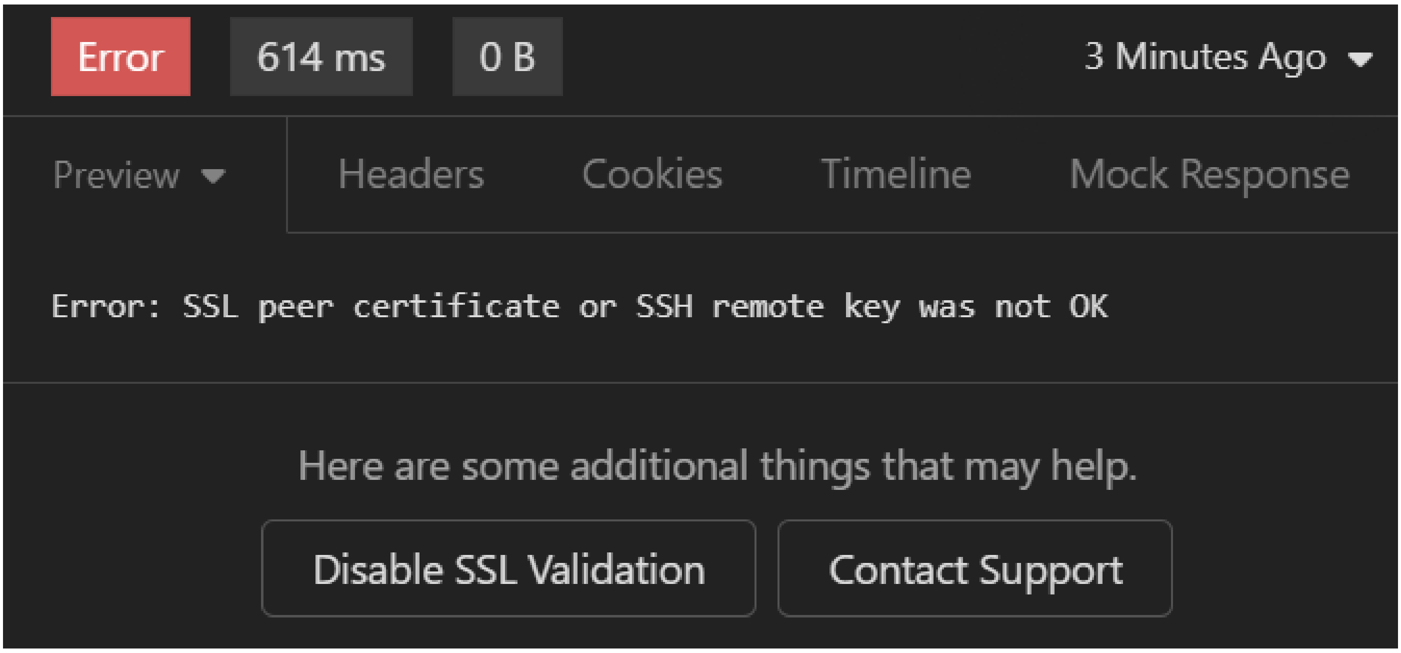
400 error

There are multiple reasons to face this error, the most common are:

- Mismatches with the security password policy

- Some parameters have been wrongly configured.
- Sintaxis error.
- Information duplicated.

5. Error: SSL peer certificate or SSH remote key was not OK



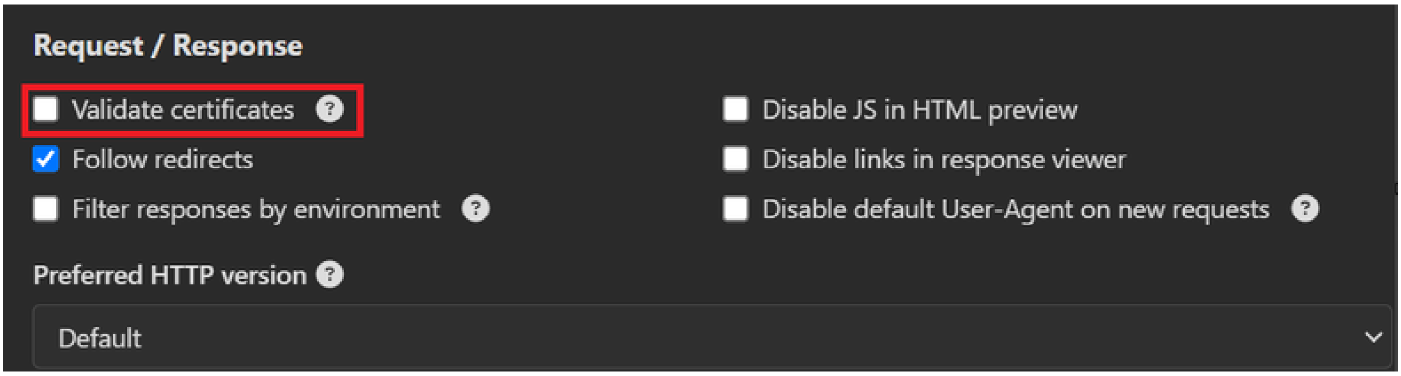
```
Error: SSL peer certificate or SSH remote key was not OK
```

Here are some additional things that may help.

SSL certificate error

Solution:

1. Click Disable SSL Validation.
2. Under Request / Response, disable the Validate Certificates option.



Request / Response

- □ Validate certificates ?
- ☑ Follow redirects
- □ Filter responses by environment ?
- □ Disable JS in HTML preview
- □ Disable links in response viewer
- □ Disable default User-Agent on new requests ?

Preferred HTTP version ?

Default

Validate certificates option

6. CSCwh71435

defect.

The enable password is configured randomly although you have not configured it. This behavior happens when the enable password syntax is removed or left empty as the value. Check the next link for more information:

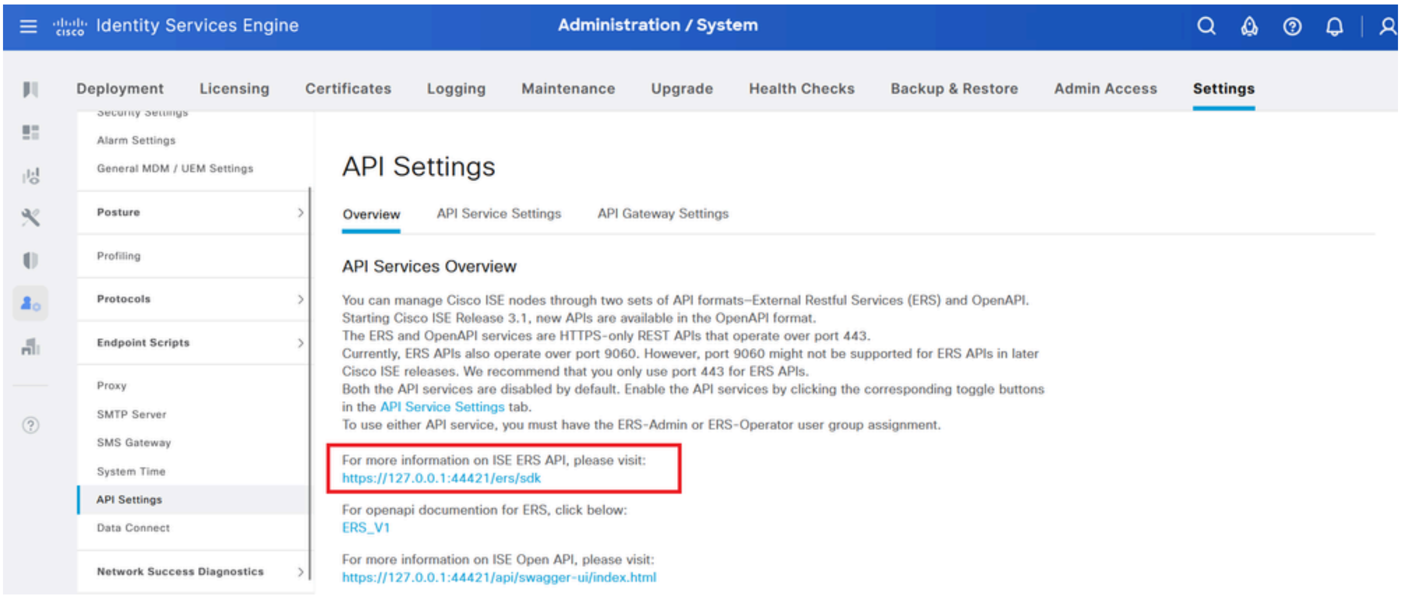
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh71435

API call references.

You can see all the information about the API calls that ISE supports.

1. Navigate to Administration > System > Settings > API Setting.

2. Click the ERS API information link.



API 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.

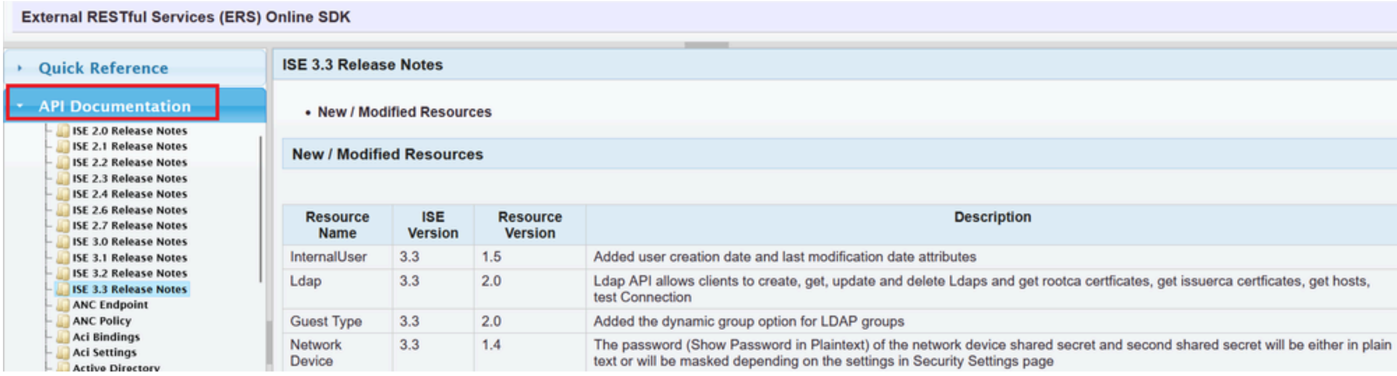
For more information on ISE ERS API, please visit:
https://127.0.0.1:44421/ers/sdk

For openapi documention 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 Settings

3. And click API documentation.



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 certficates, get issuerca certficates, 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 Documentation