

Configuración de usuarios internos a través de llamadas JSON o XML y API en ISE 3.3 con Insominia

Contenido

Introducción

Este documento describe la configuración de los usuarios internos en Cisco ISE mediante el aprovechamiento de los formatos de datos JSON o XML junto con las llamadas API.

Prerequisites

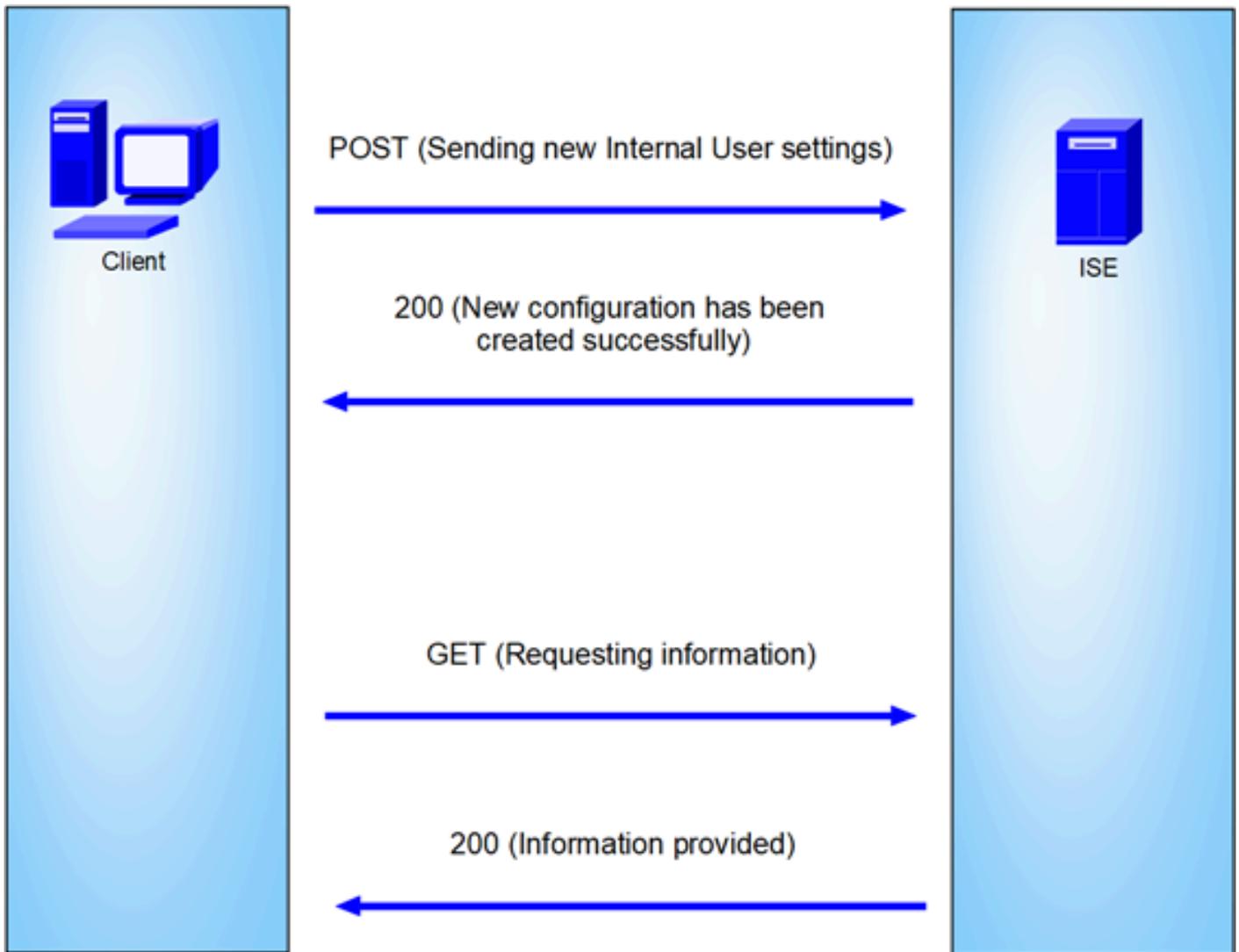
- ISE 3.0 o superior.
- Software cliente API.

Componentes Utilizados

- ISE 3.3
- Insominia 9 3 2

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.

Diagrama de la red



Topología general

GET y POST son dos de los métodos HTTP más comunes que se utilizan en las llamadas de la API (interfaz de programación de aplicaciones). Se utilizan para interactuar con los recursos de un servidor, normalmente para recuperar datos o enviar datos para su procesamiento.

Llamada API GET

El método GET se utiliza para solicitar datos de un recurso especificado. Las solicitudes GET son los métodos más comunes y ampliamente utilizados en API y sitios web. Al visitar una página web, el explorador realiza una solicitud GET al servidor que aloja la página web.

Llamada API POST

El método POST se utiliza para enviar datos al servidor para crear o actualizar un recurso. Las solicitudes POST se utilizan a menudo al enviar datos de formulario o cargar un archivo.

Configuraciones

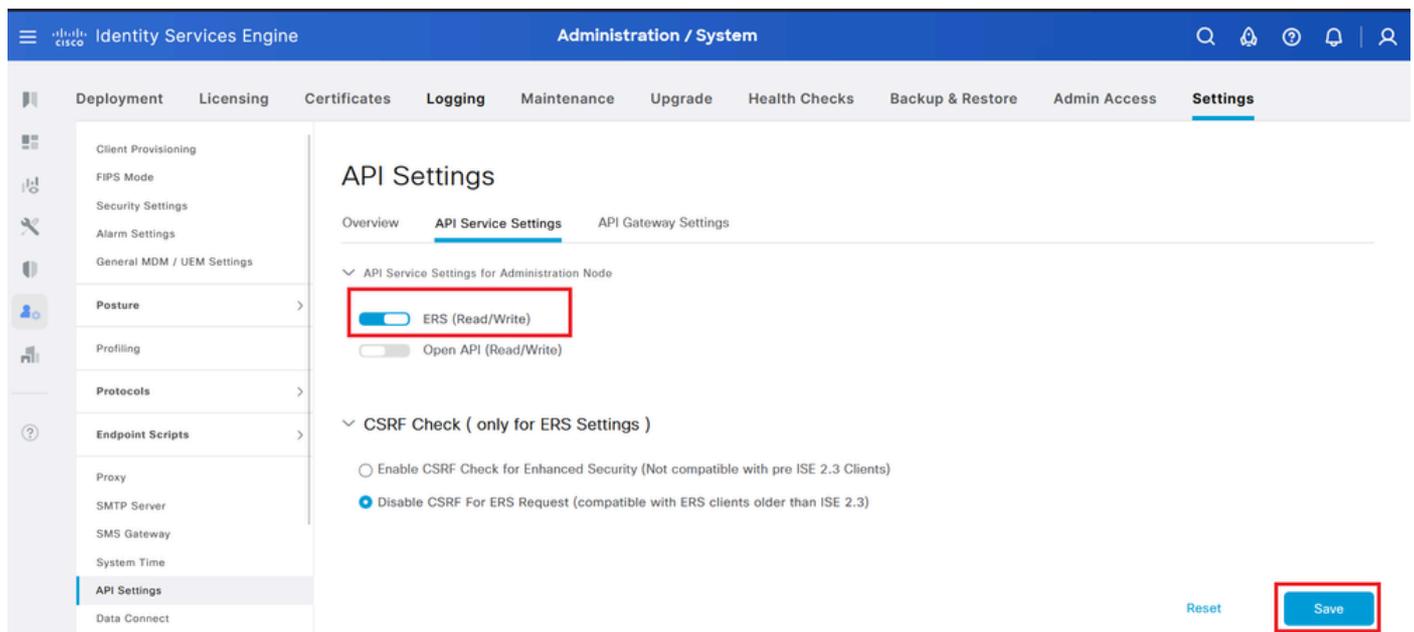
Necesitamos enviar la información exacta desde el software cliente API al nodo ISE para crear un

usuario interno.

Configuraciones de ISE

Active la función ERS.

1. Vaya a Administration > System > Settings > API Settings > API Service Settings.
2. Active la opción ERS (lectura/escritura).

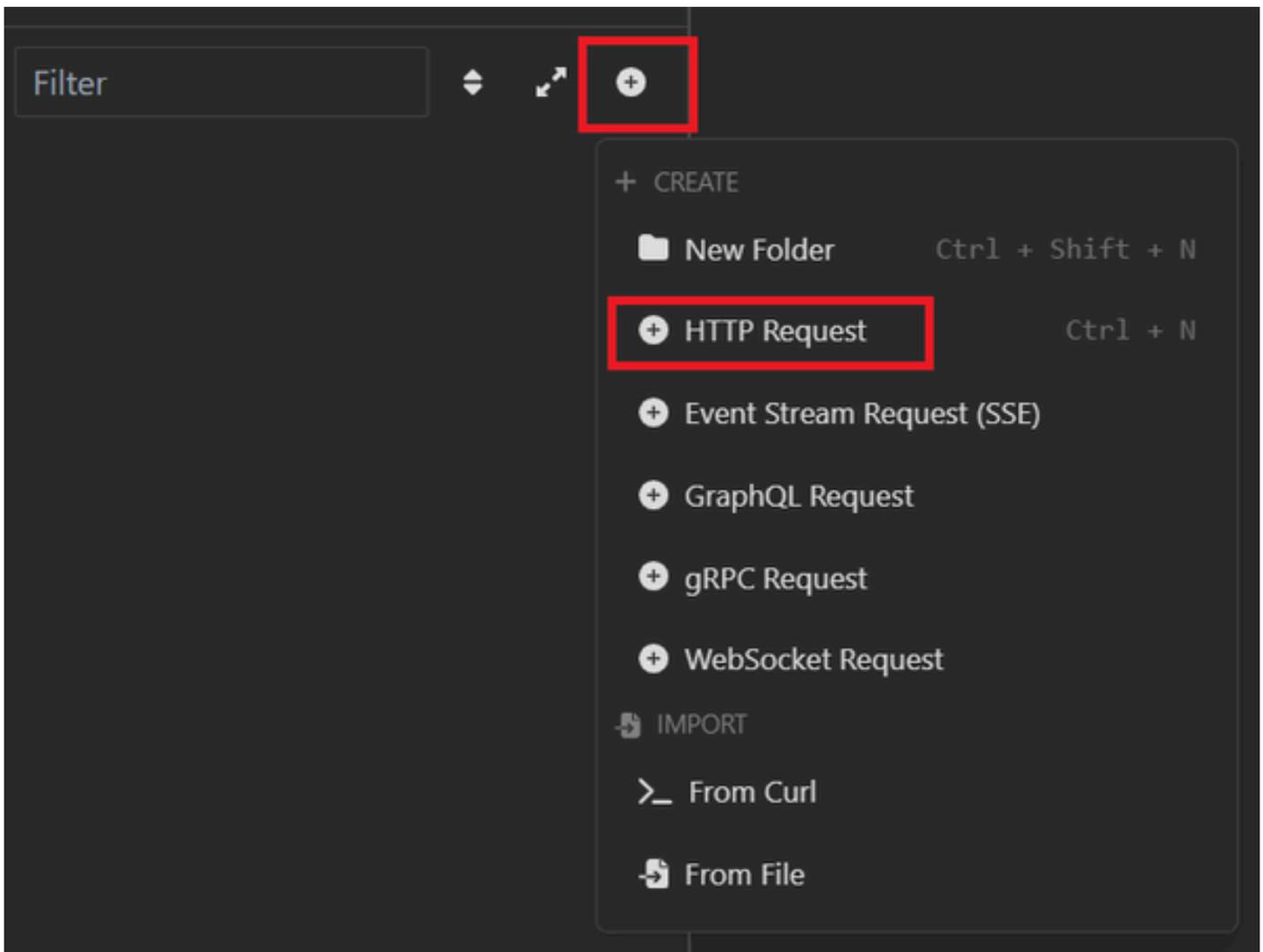


The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Administration / System' and various utility icons. The main navigation menu on the left lists categories like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The 'Settings' section is expanded, showing sub-sections: 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 (selected), 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)' option is selected. At the bottom right, there are 'Reset' and 'Save' buttons, with the 'Save' button highlighted by a red box.

Configuración de API

Solicitud JSON.

1. Insomnio abierto.
2. Agregue una nueva solicitud HTTPS en el lado izquierdo.

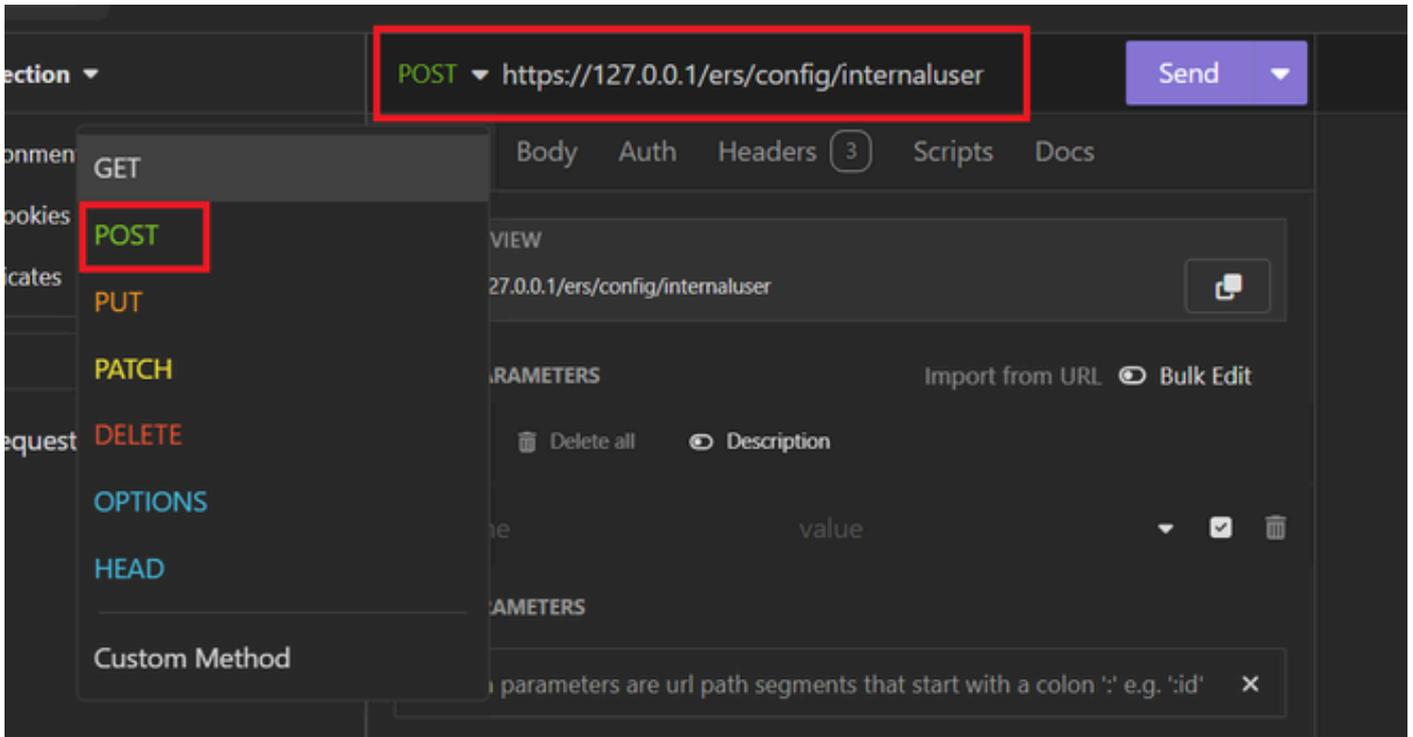


Solicitud JSON

3. Debe seleccionar POST (autoprueba de encendido) para enviar la información al nodo ISE.

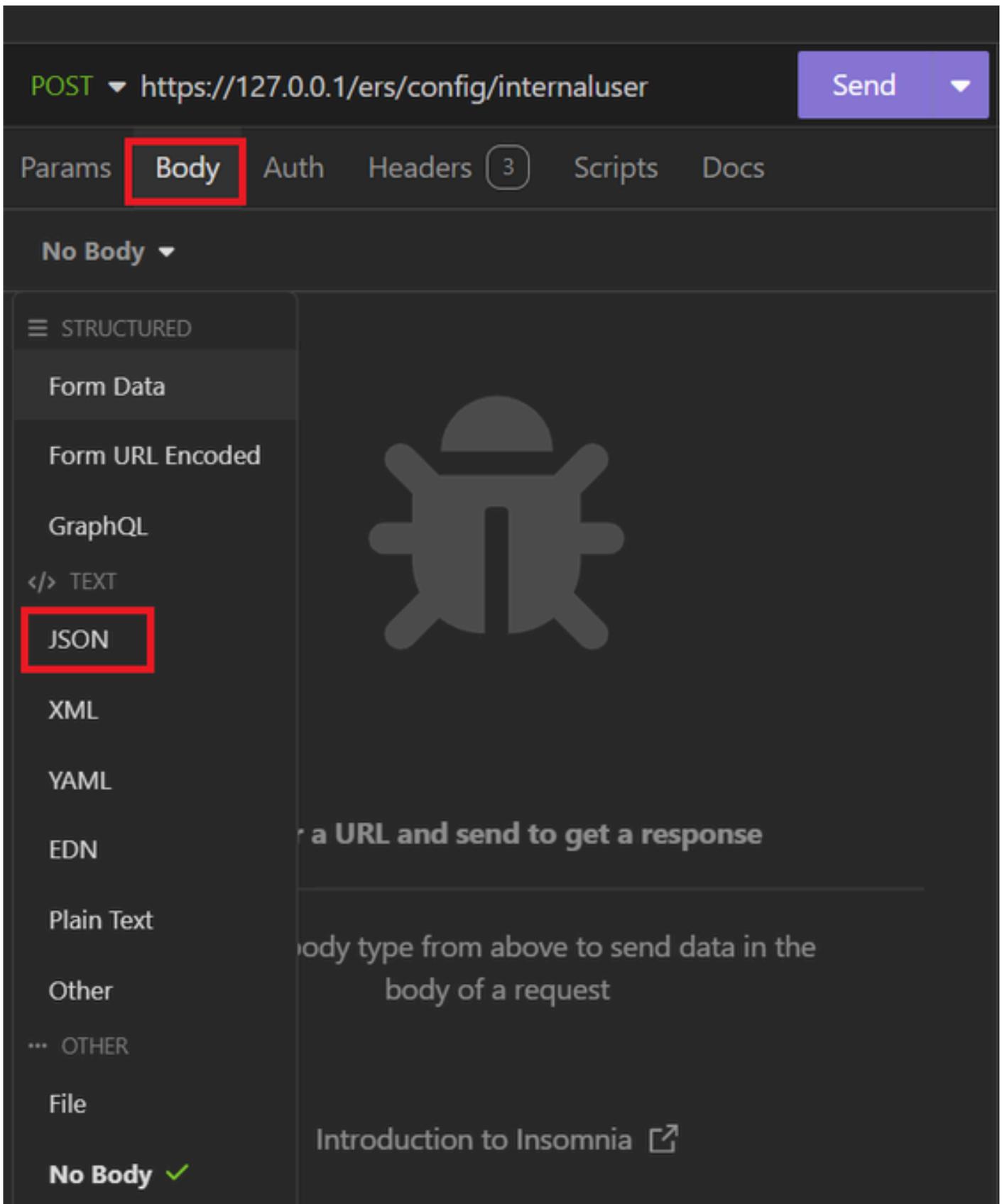
La URL que debe introducir depende de la dirección IP del nodo ISE.

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



JSON POST

4. A continuación, haga clic en Cuerpo y seleccione JSON



Cuerpo JSON

5. Puede pegar la sintaxis y cambiar los parámetros según lo que desee.

```
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 }
```

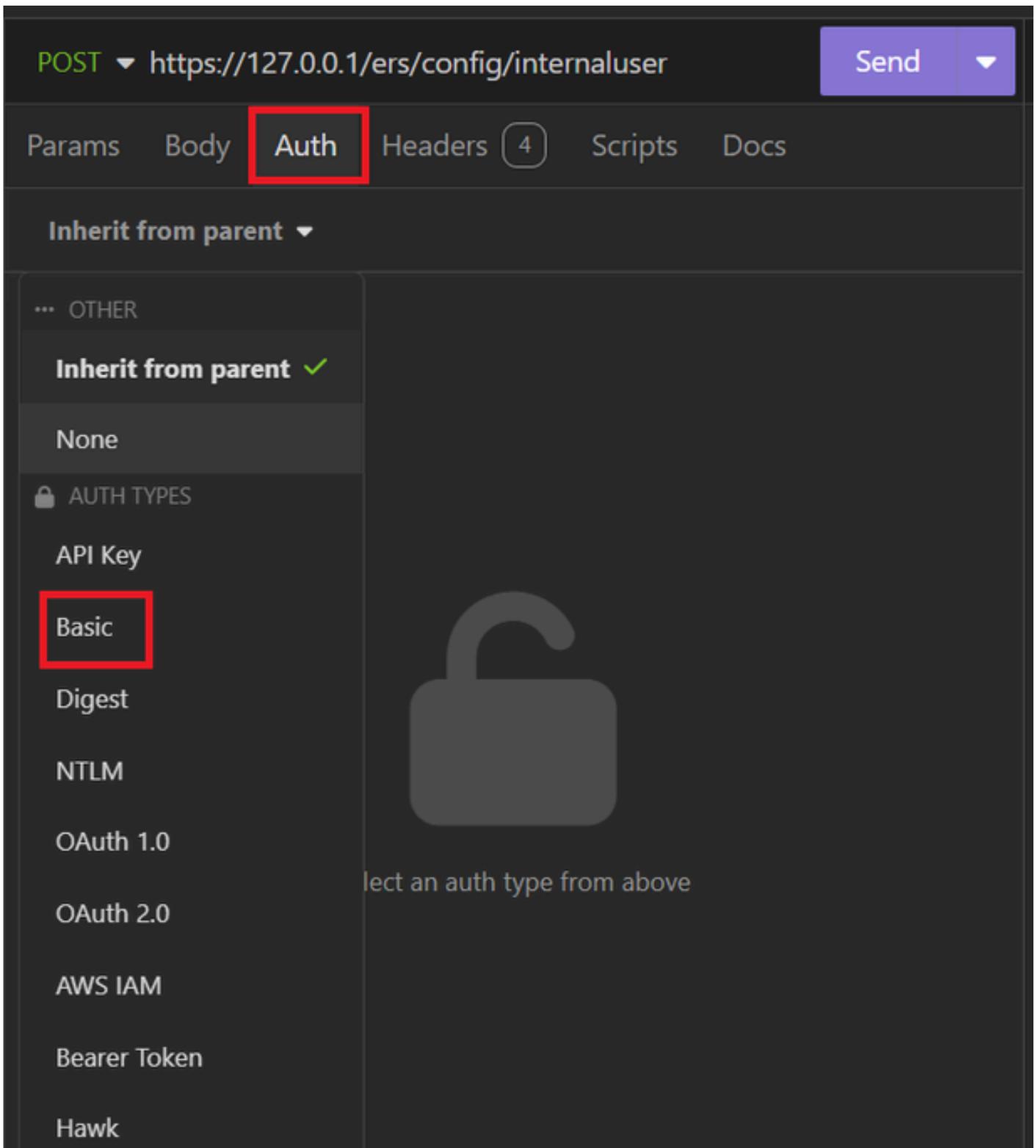
Sintaxis JSON

sintaxis JSON

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

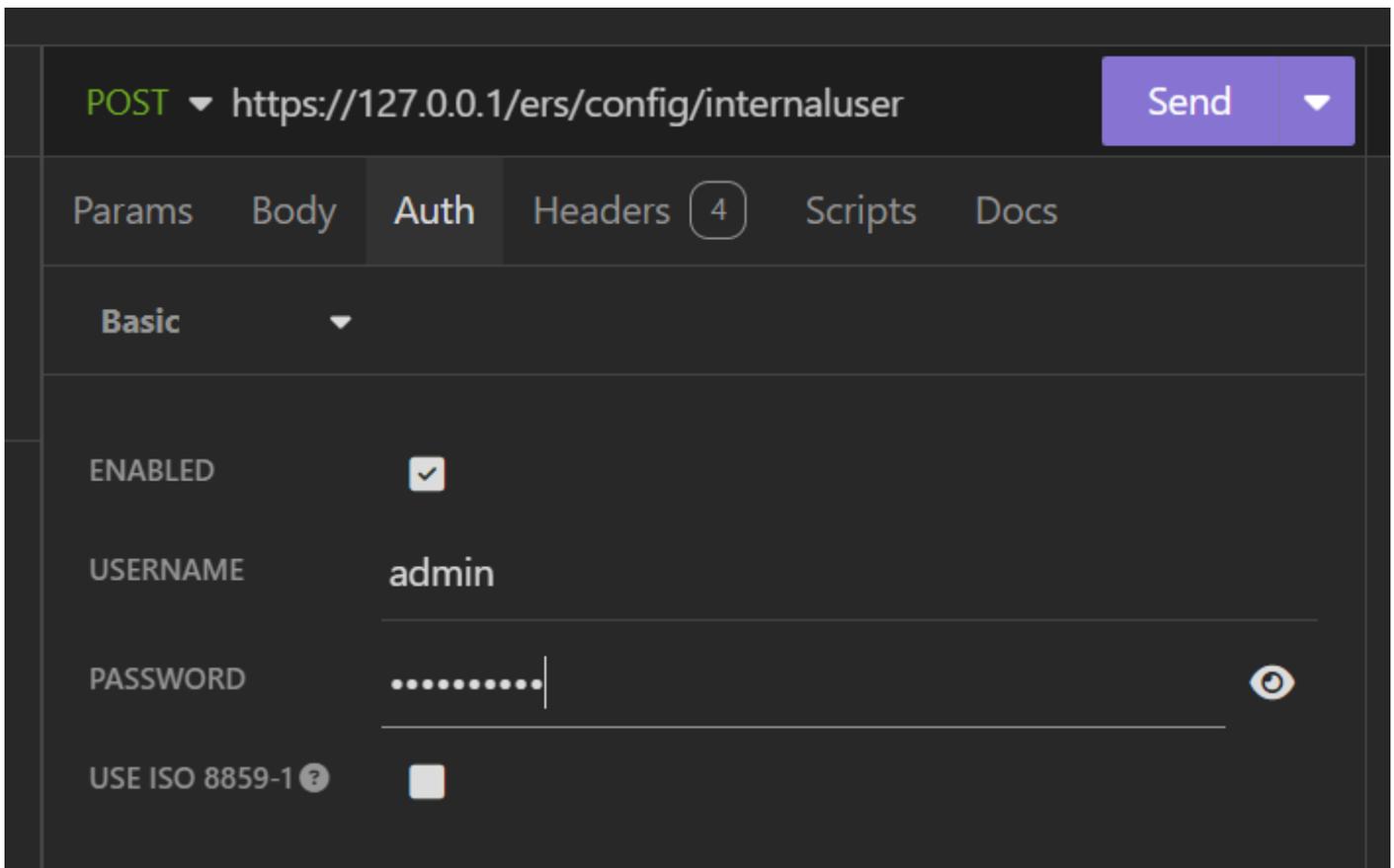
```
"password": "password",
"firstName": "firstName",
"lastName": "lastName",
"changePassword": true,
"identityGroups": "identityGroups",
"passwordNeverExpires": false,
"daysForPasswordExpiration": 60,
"expiryDateEnabled": false,
"expiryDate": "2016-12-11",
"enablePassword": "enablePassword",
"dateModified":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

6. Haga clic en Auth y elija Basic.



autenticación JSON

7. Introduzca las credenciales de la GUI de ISE.



Credenciales JSON de administrador

8. Haga clic en Encabezados para agregar los siguientes métodos:
- Tipo de contenido: application/json
 - Aceptar: aplicación/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	▼	☑	🗑

Encabezados JSON

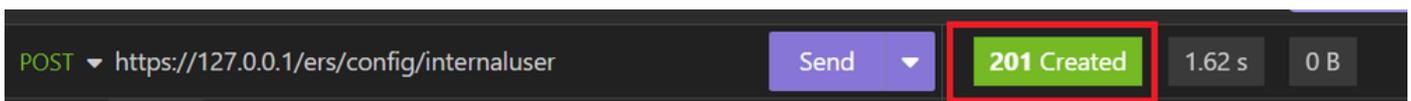
9. Por último, haga clic en Enviar.



Nota: Si desea asignar un grupo de identidad a la nueva cuenta de usuario, debe utilizar el ID del grupo de identidad. Consulte la sección **Troubleshooting** para obtener más información.

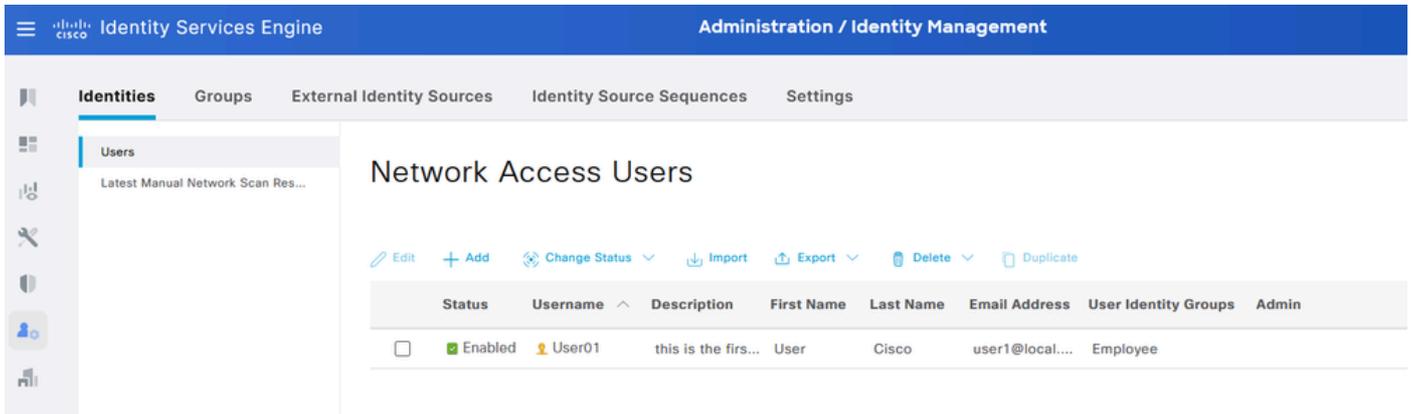
Validación

1. Después de enviar la solicitud POST, verá el estado "201 Created" (201 Creado). Esto significa que el proceso se ha completado con éxito.



Solicitud JSON correcta

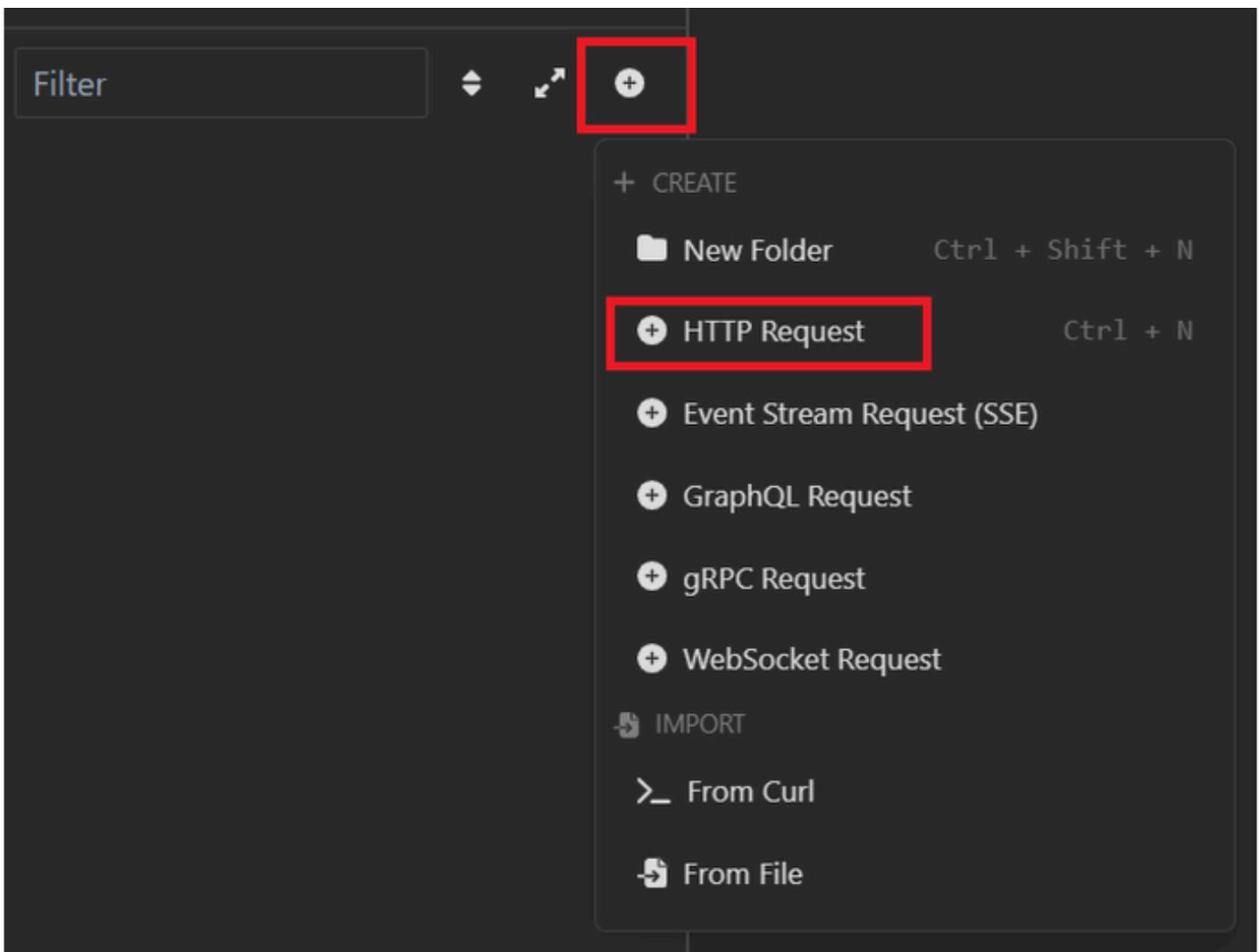
2. Abra la GUI de ISE y vaya a Administration > Identity Management > Identities > Users > Network Access Users



Cuenta de usuario JSON

solicitud XML

1. Insomnio abierto.
2. Agregue una nueva solicitud HTTPS en el lado izquierdo.

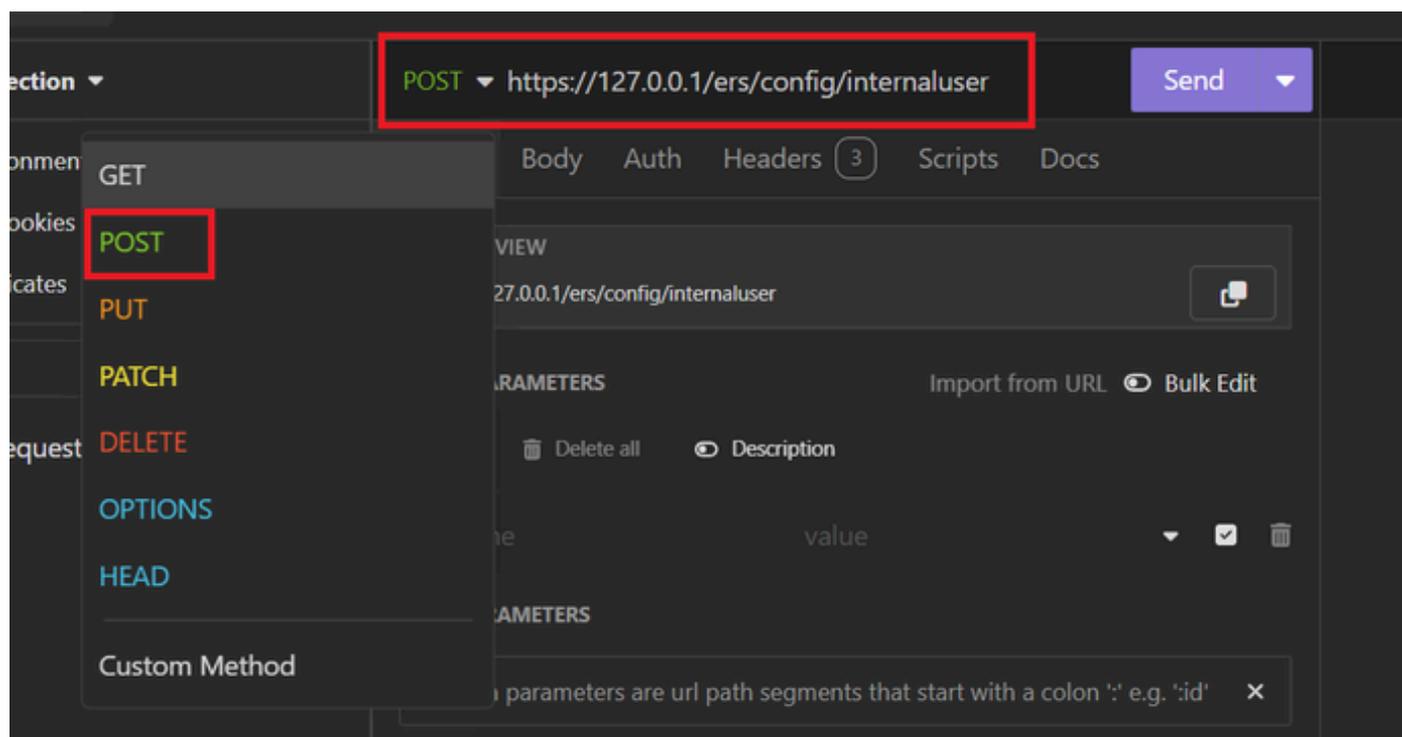


Solicitud XML

3. Debe seleccionar POST (autoprueba de encendido) para enviar la información al nodo ISE.

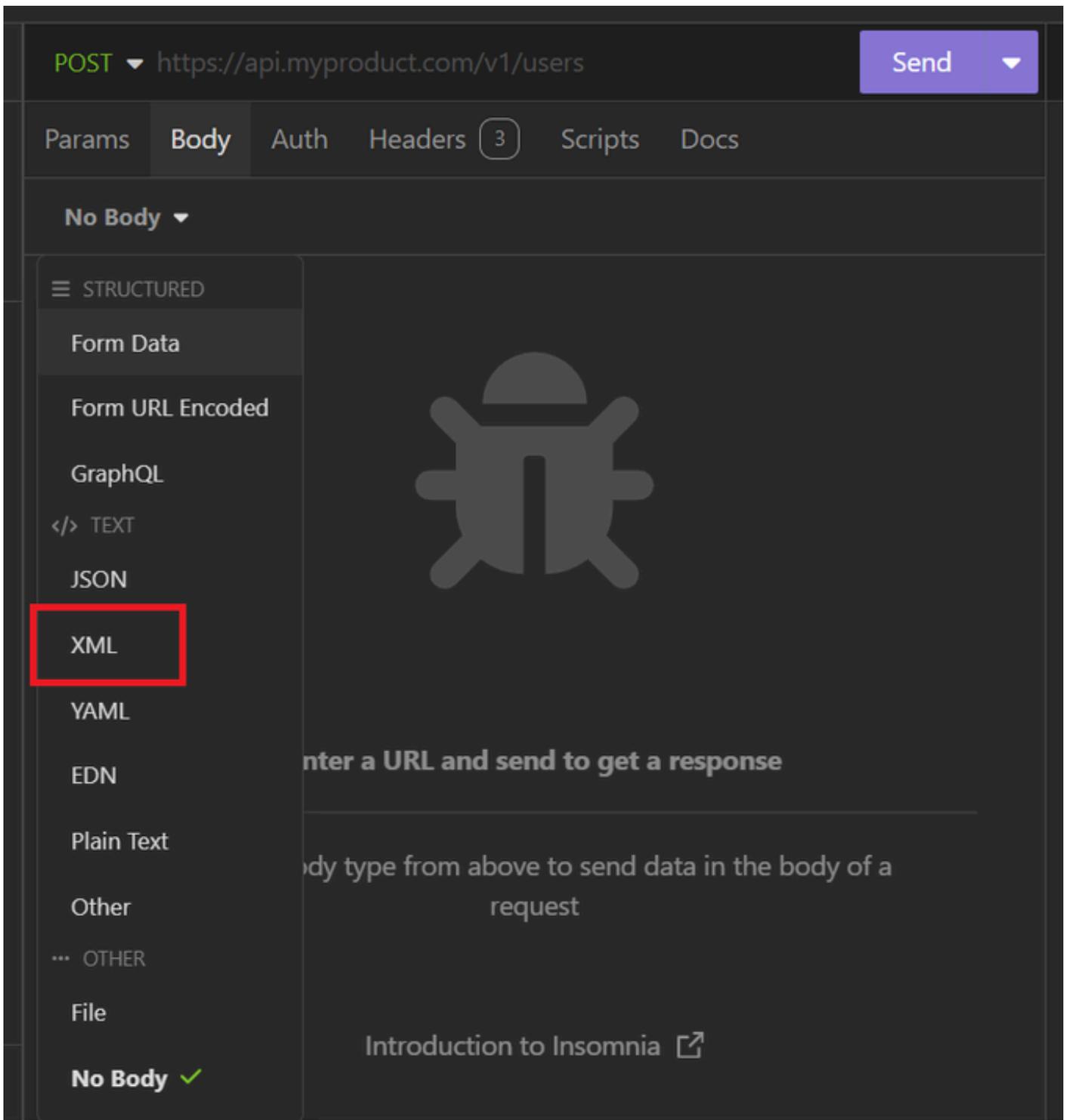
La URL que debe introducir depende de la dirección IP del nodo ISE.

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



XML POST

4. A continuación, haga clic en Cuerpo y seleccione XML.



Cuerpo XML

5. Puede pegar la sintaxis y cambiar los parámetros según lo que desee.

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>

```

Publicación XML

Sintaxis 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
```

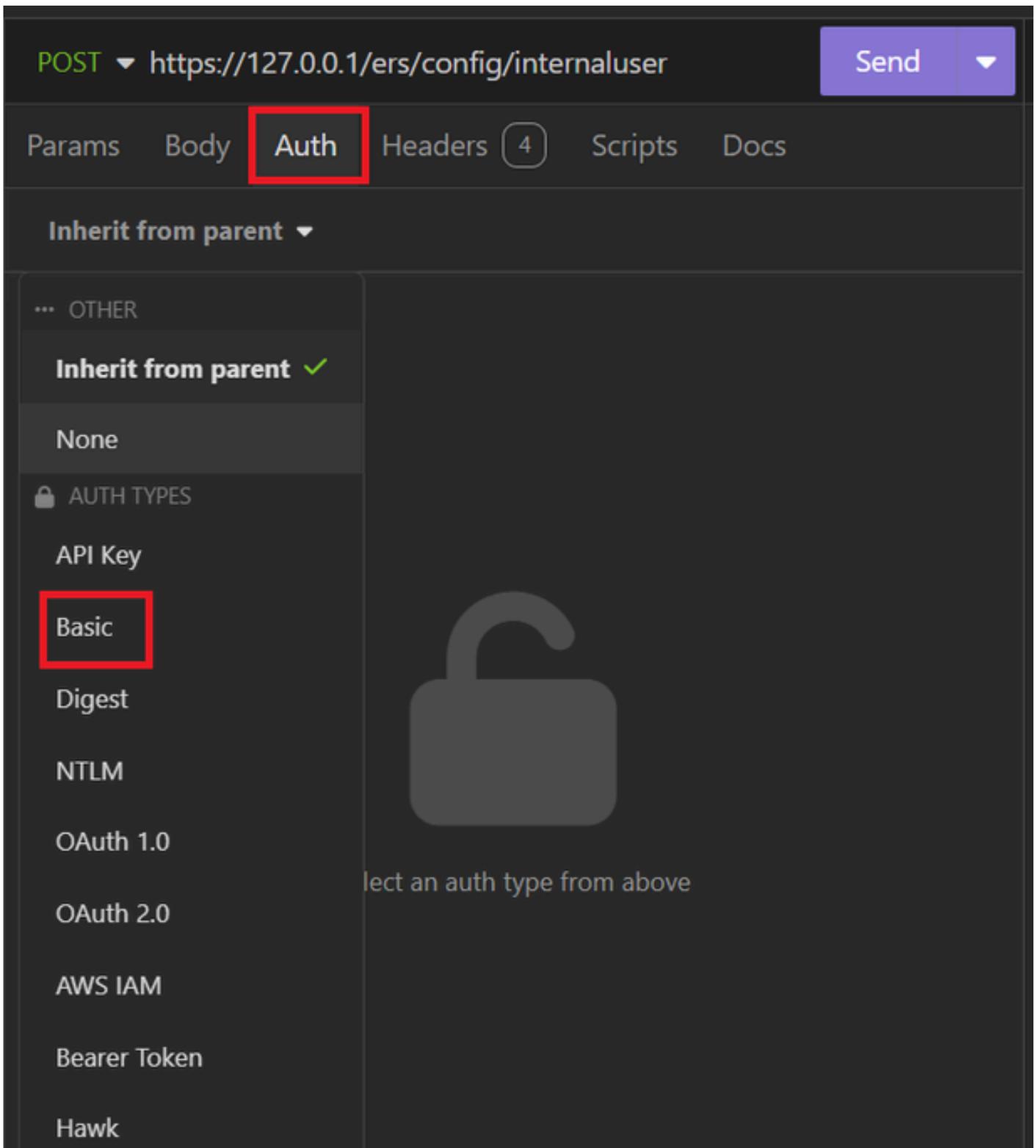
```
  <accountNameAlias>accountNameAlias</accountNameAlias>
```

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

```
  <customAttributes>
```

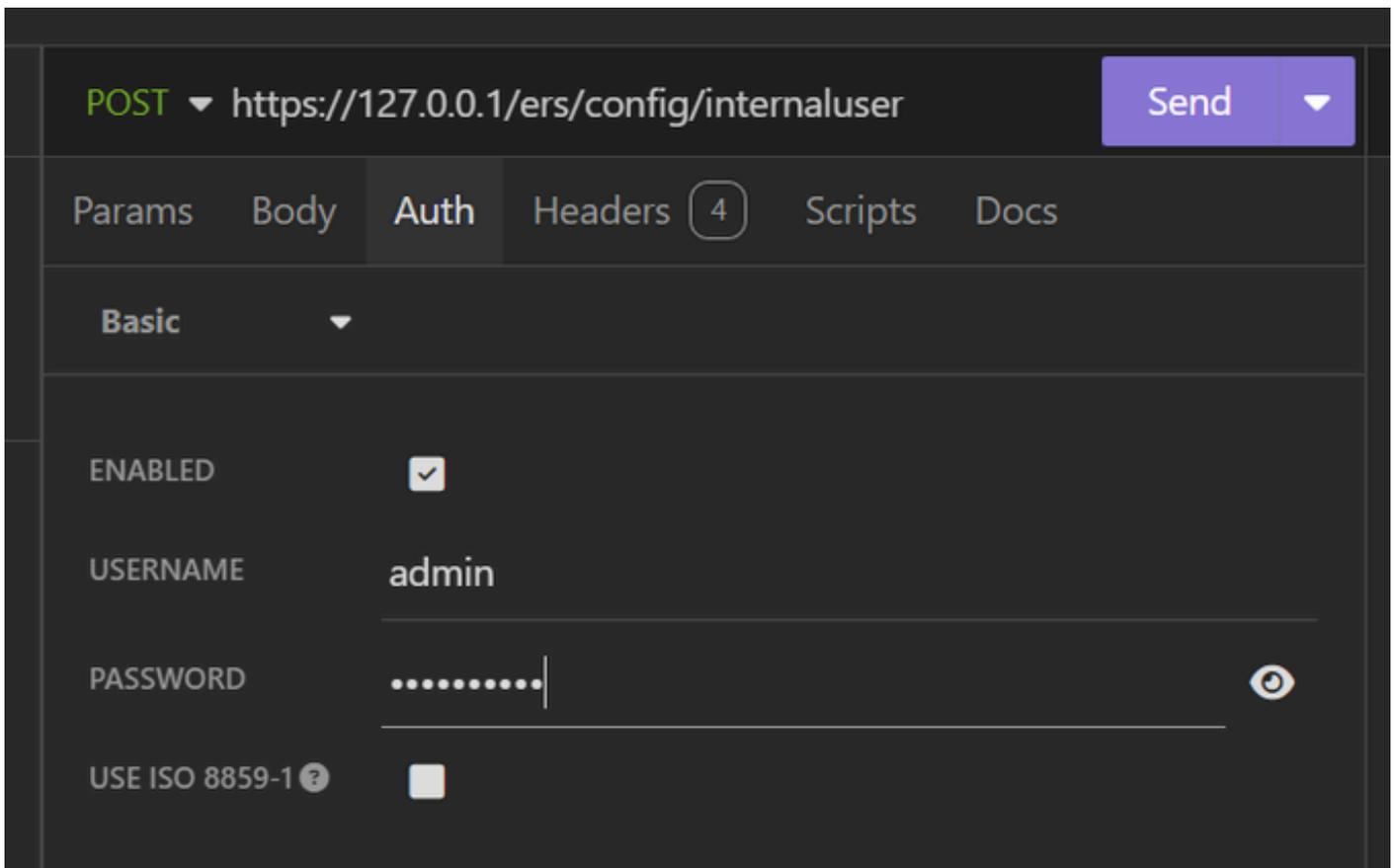
```
<entry>
  <key>key1</key>
  <value>value1</value>
</entry>
<entry>
  <key>key2</key>
  <value>value3</value>
</entry>
</customAttributes>
<dateCreated>2015-12-15</dateCreated>
<dateModified>2015-12-20</dateModified>
<daysForPasswordExpiration>60</daysForPasswordExpiration>
<email>email@domain.com</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. Haga clic en Auth y elija Basic



autenticación XML

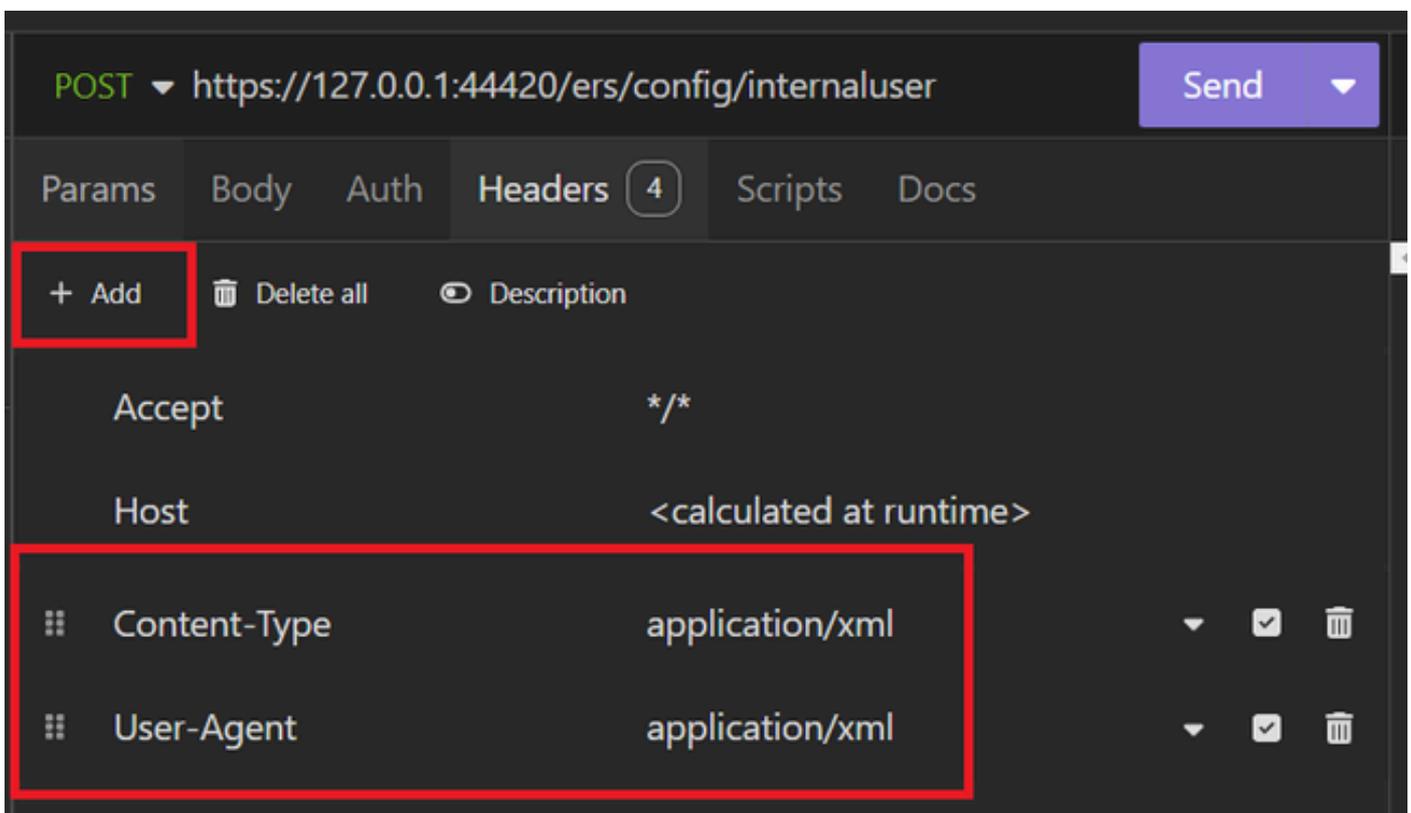
7. Introduzca las credenciales de la GUI de ISE.



Credenciales XML

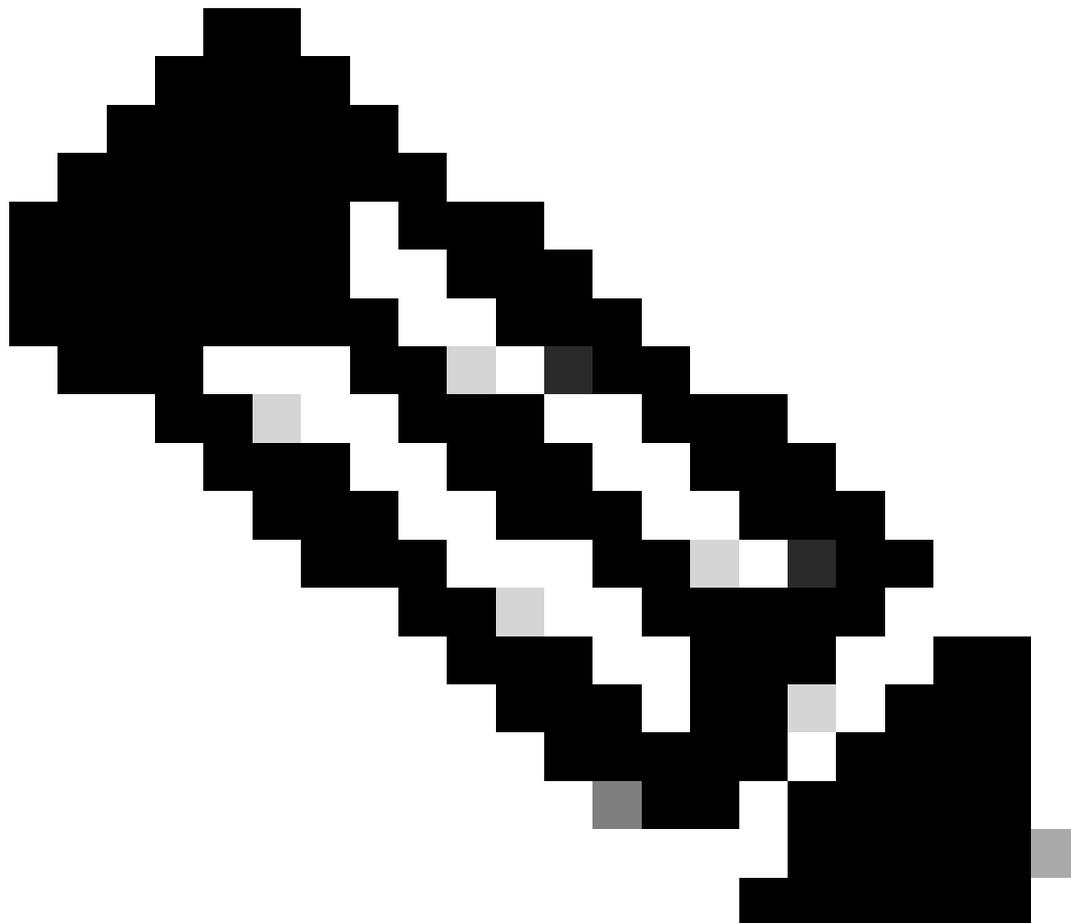
8. Haga clic en Encabezados para agregar los siguientes métodos:

- Tipo de contenido: application/xml
- Aceptar: application/xml



Encabezados XML

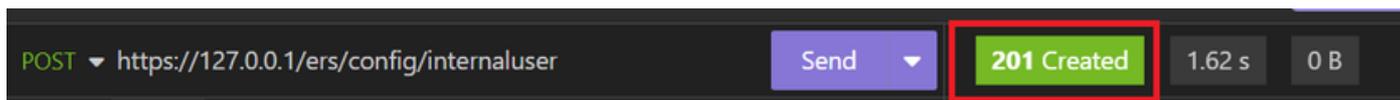
9. Por último, haga clic en Enviar.



Nota: Si desea asignar un grupo de identidad a la nueva cuenta de usuario, debe utilizar el ID del grupo de identidad. Consulte la sección **Troubleshooting** para obtener más información.

Validación

1. Después de enviar la solicitud POST, verá el estado "201 Created" (201 Creado). Esto significa que el proceso se ha completado con éxito.



Solicitud XML correcta

2. Abra la GUI de ISE y vaya a Administration > Identity Management > Identities > Users > Network Access Users

Network Access Users

Selected 0 Total 2  

 Edit  + Add  Change Status  Import  Export  Delete  Duplicate  All 

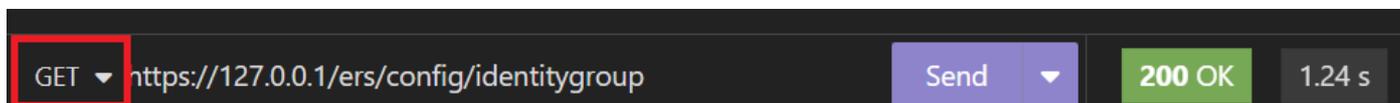
Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	 Enabled  User01	this is the firs...	User	Cisco	user1@local...	Employee	 User Account created by JSON
<input type="checkbox"/>	 Enabled  User02	description	User2	Cisco	user2@local...	Employee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

Validación de cuentas de usuario

Troubleshoot

1. Identifique la ID del grupo de identidad.

Utilice GET y la consulta <https://X.X.X.X/ers/config/identitygroup>.



opción GET

Salida JSON.

Identifique la ID junto a la descripción.

```
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 Identidad de ID 01

Resultado XML.

Identifique la ID junto a la descripción.

```
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",
```

ID Grupo de Identidad 02

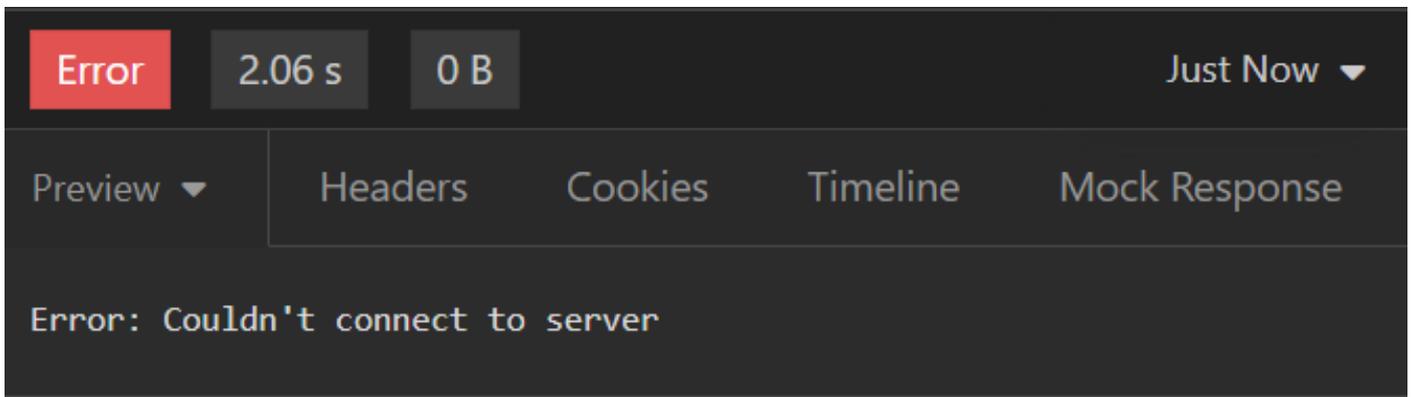
2. 401 Error no autorizado.



error 401

Solución: compruebe las credenciales de acceso configuradas en la sección Auth

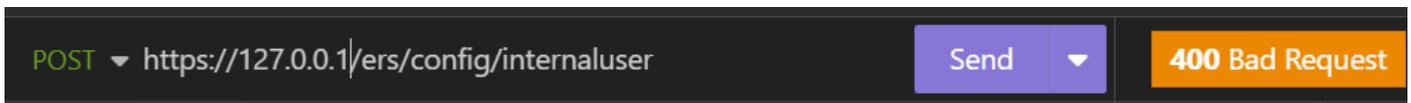
3. Error: no se pudo conectar al servidor



Error de conexión

Solución: compruebe la dirección IP del nodo ISE configurado en Insomnia o valide la conectividad.

4. 400 Solicitud incorrecta.

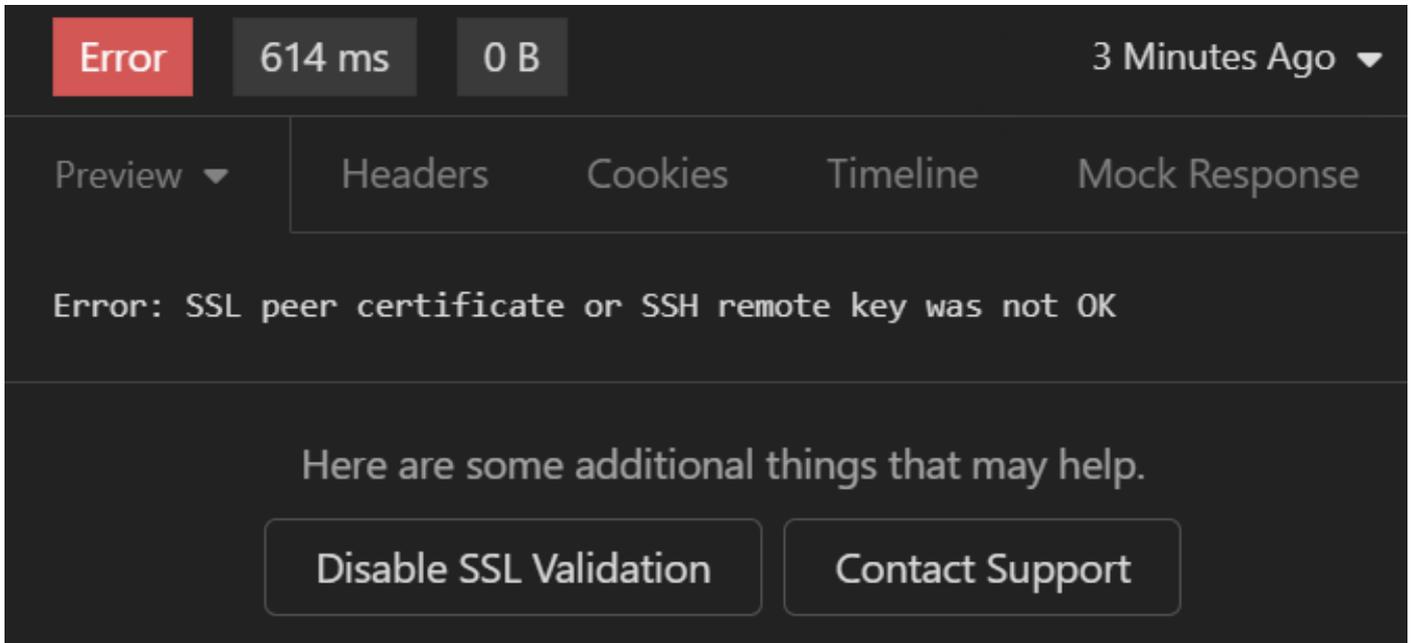


error 400

Existen múltiples razones para enfrentar este error, las más comunes son:

- No coincide con la directiva de contraseñas de seguridad
- Algunos parámetros se han configurado incorrectamente.
- Error de Sintaxis.
- Información duplicada.

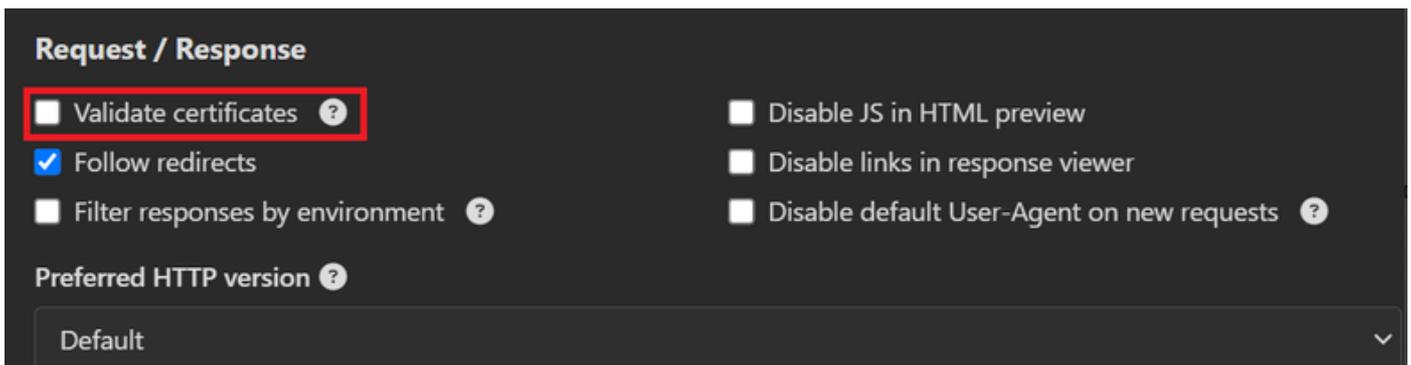
5. Error: el certificado de par SSL o la clave remota SSH no eran correctos



Error de certificado SSL

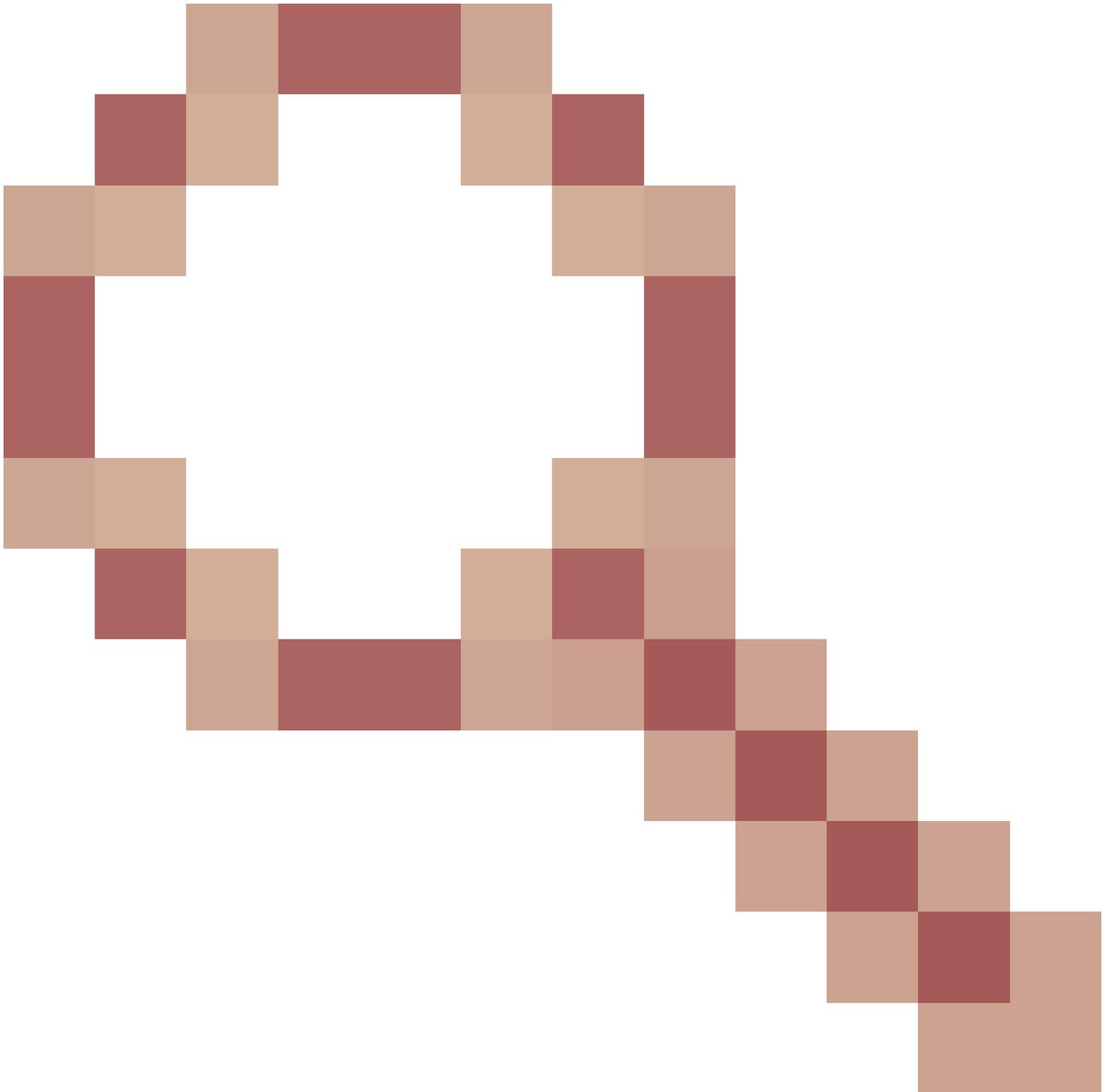
Solución:

1. Haga clic en Deshabilitar validación SSL.
2. En Solicitud o respuesta, desactive la opción Validar certificados.



Opción Validar certificados

6. [CSCwh71435](#)



defecto.

La contraseña de habilitación se configura aleatoriamente aunque no la haya configurado. Este comportamiento se produce cuando la sintaxis de habilitación de contraseña se elimina o se deja vacía como valor. Consulte el siguiente enlace para obtener más información:

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

Referencias de llamadas API.

Puede ver toda la información sobre las llamadas de API que admite ISE.

1. Vaya a Administración > Sistema > Configuración > Configuración de API.

2. Haga clic en el enlace de información de la 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>

Configuración de API

3. Y haga clic en documentación de 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

Documentación de API

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).