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

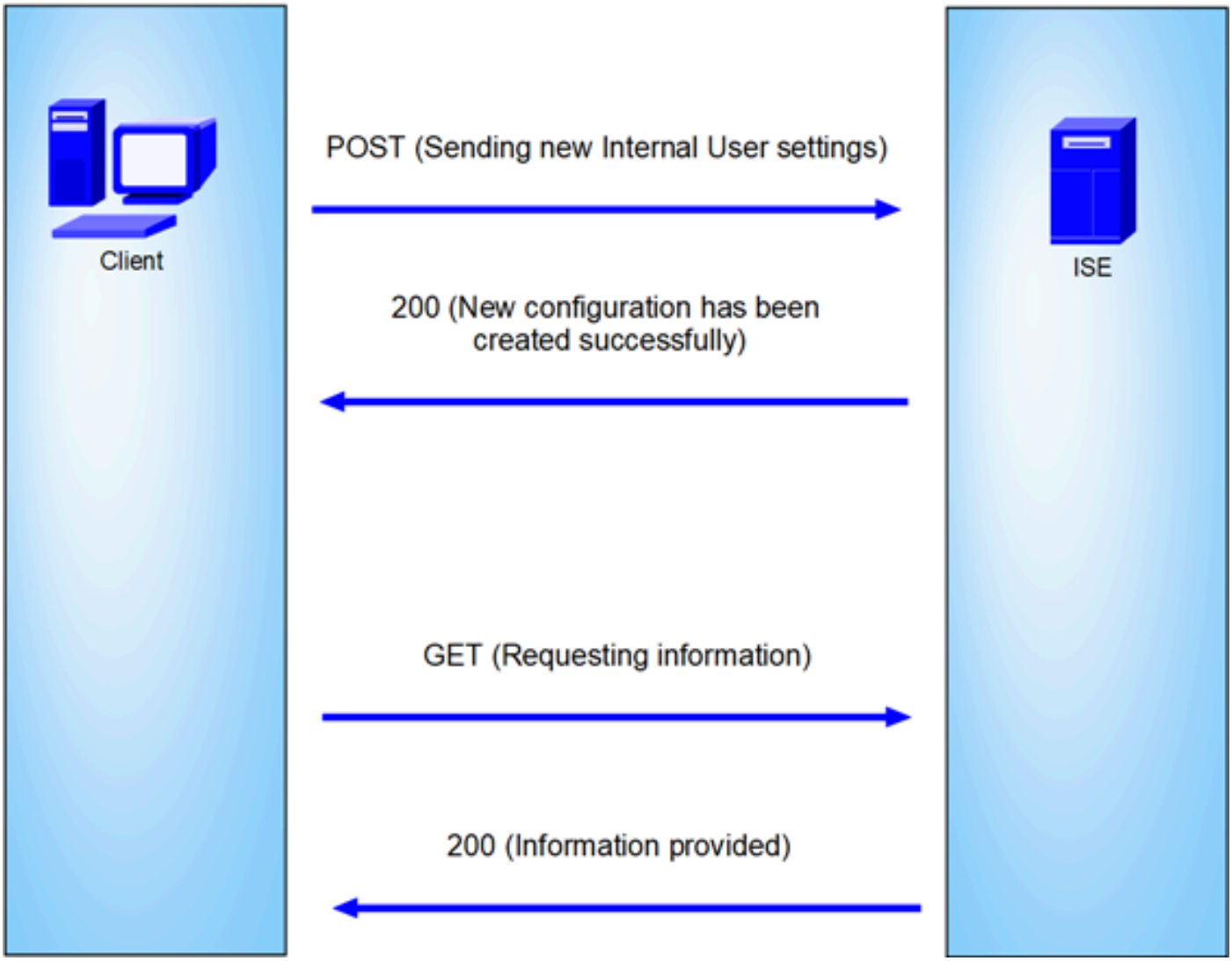
- ISE 3.0 o superior.
- Software cliente API.

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

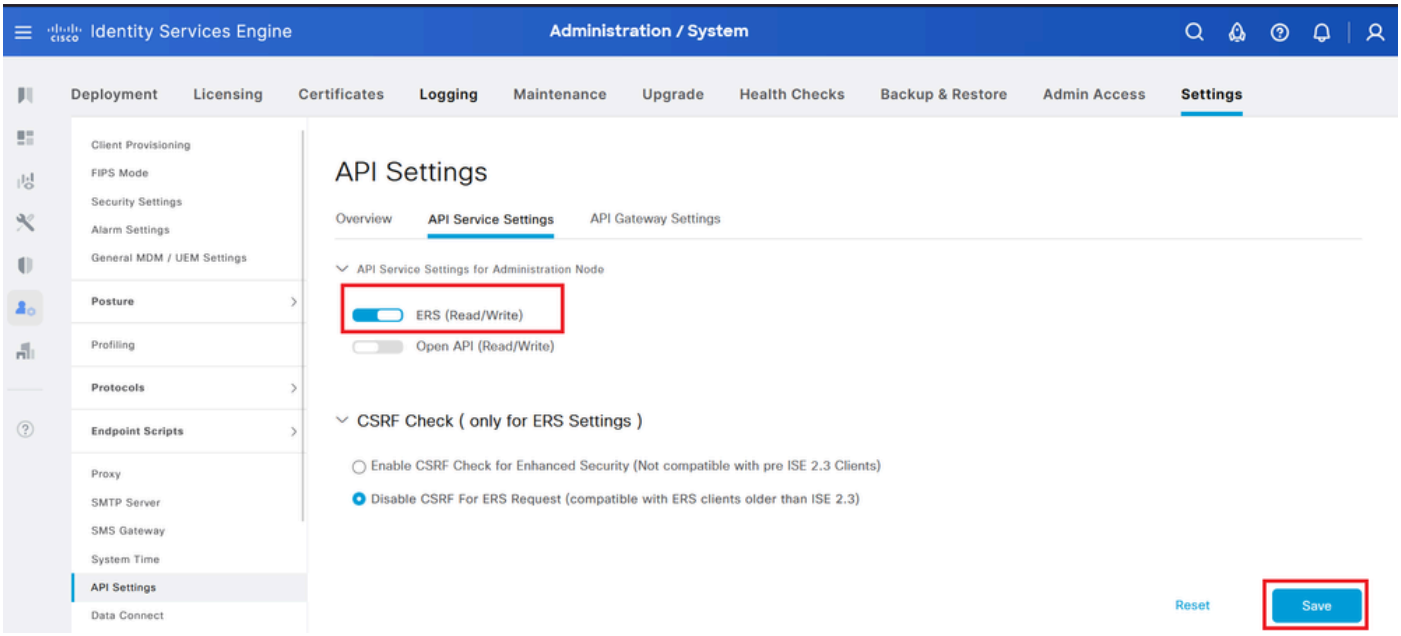
usuario interno.

Configuraciones de ISE

Active la función ERS.

1. Vaya a Administration > System > Settings > API Settings > API Service Settings.

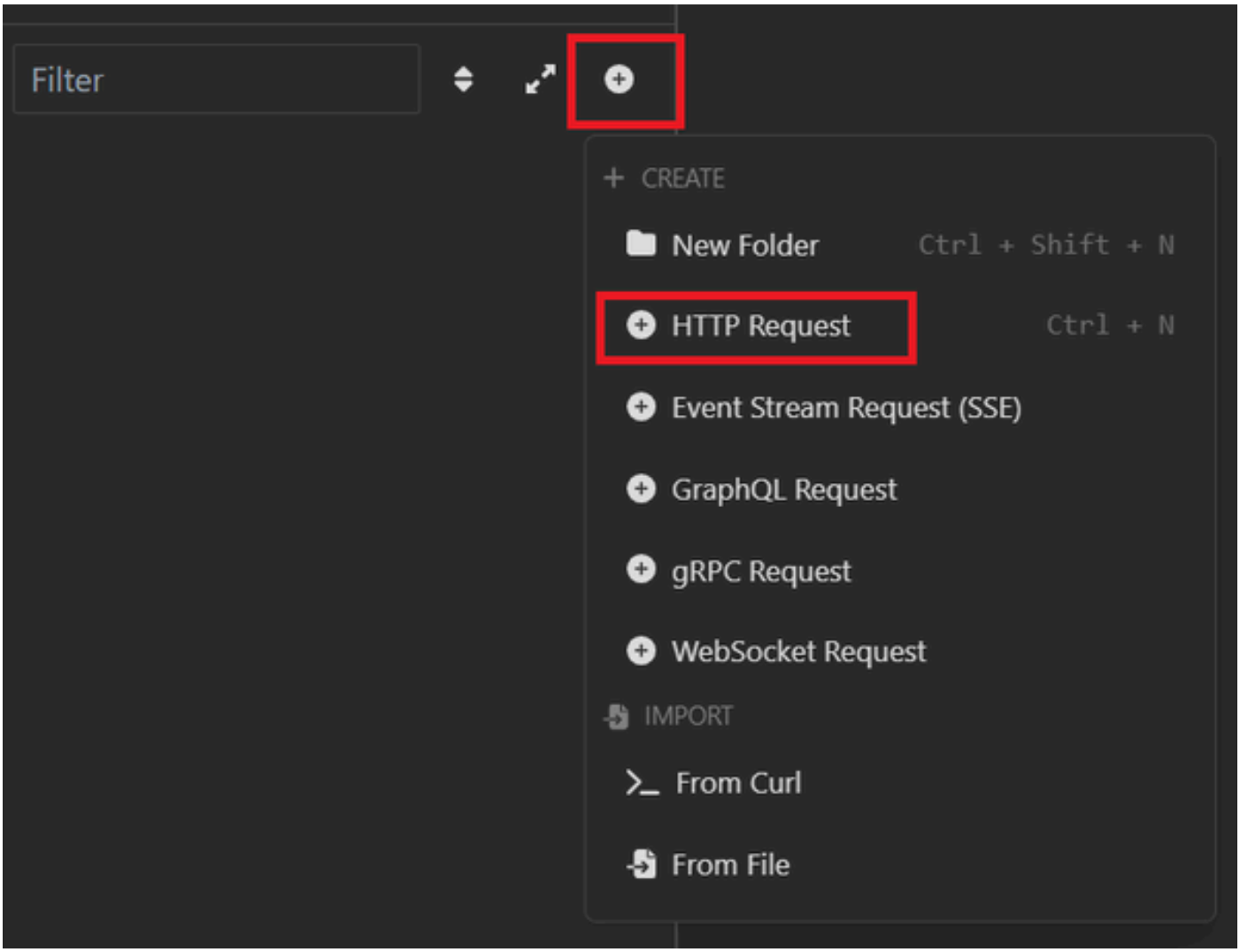
2. Active la opción ERS (lectura/escritura).



Configuración de API

Solicitud JSON.

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

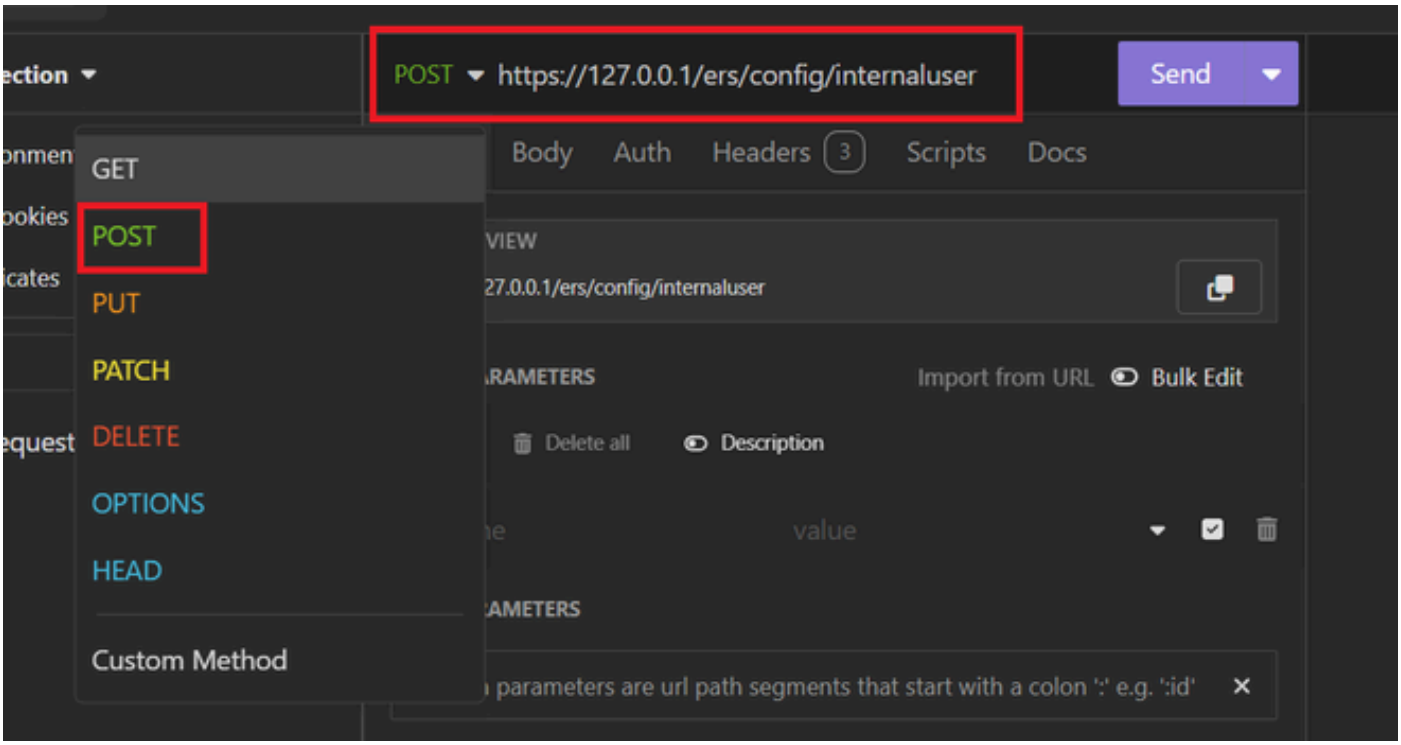


Solicitud JSON

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

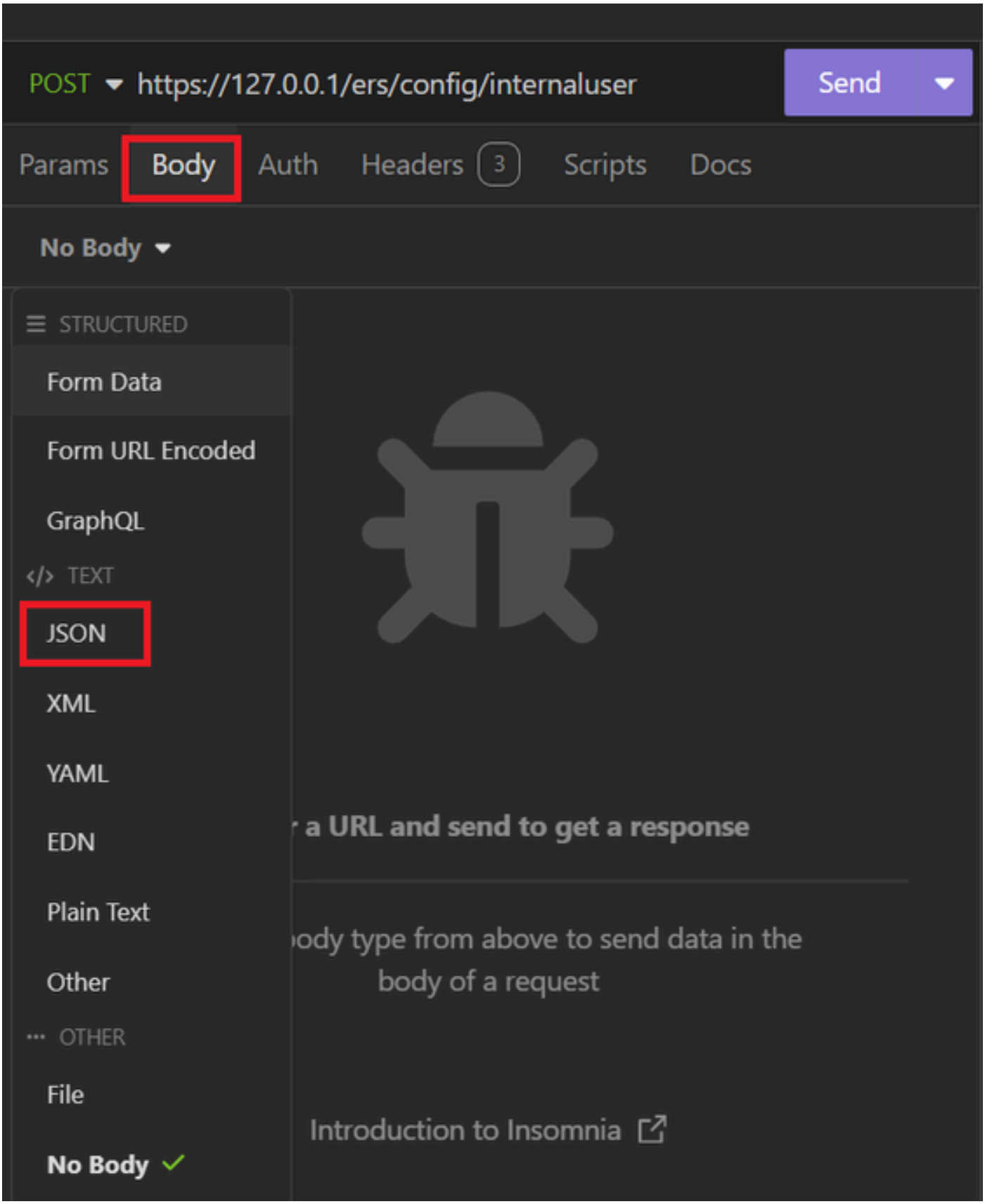
La URL que debe introducir depende de la dirección IP del nodo ISE.

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



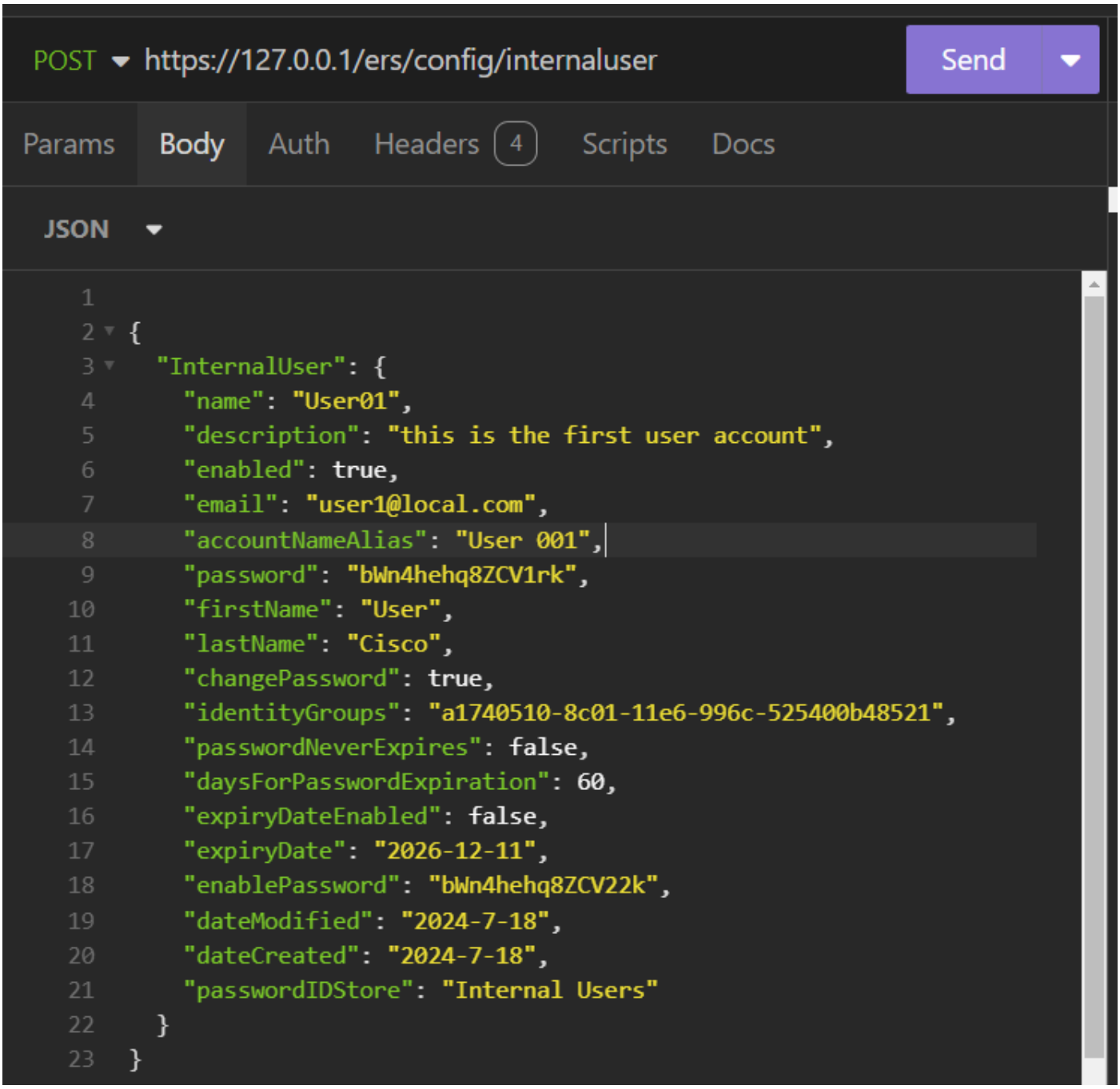
JSON POST

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.



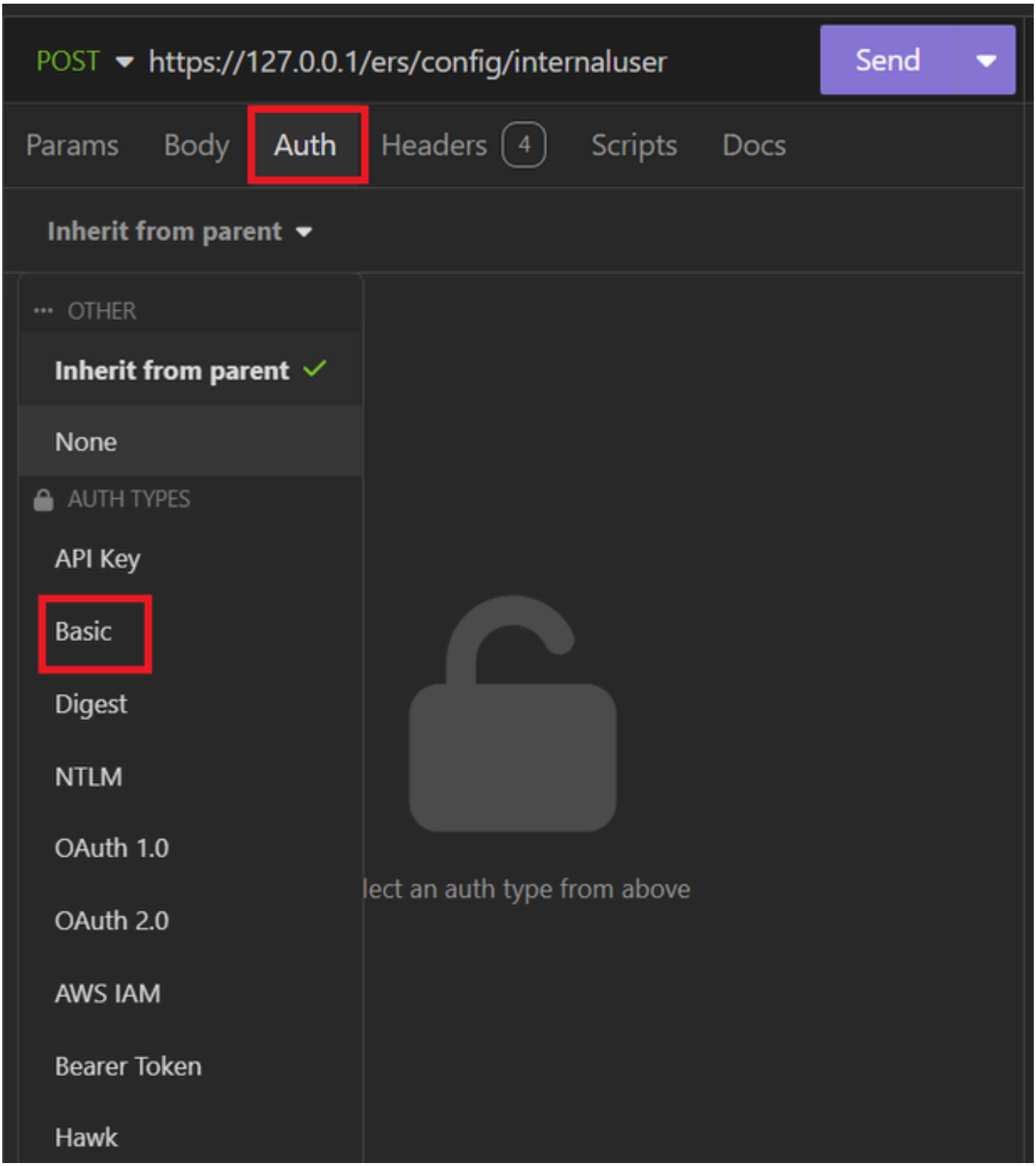
Sintaxis JSON

sintaxis JSON

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

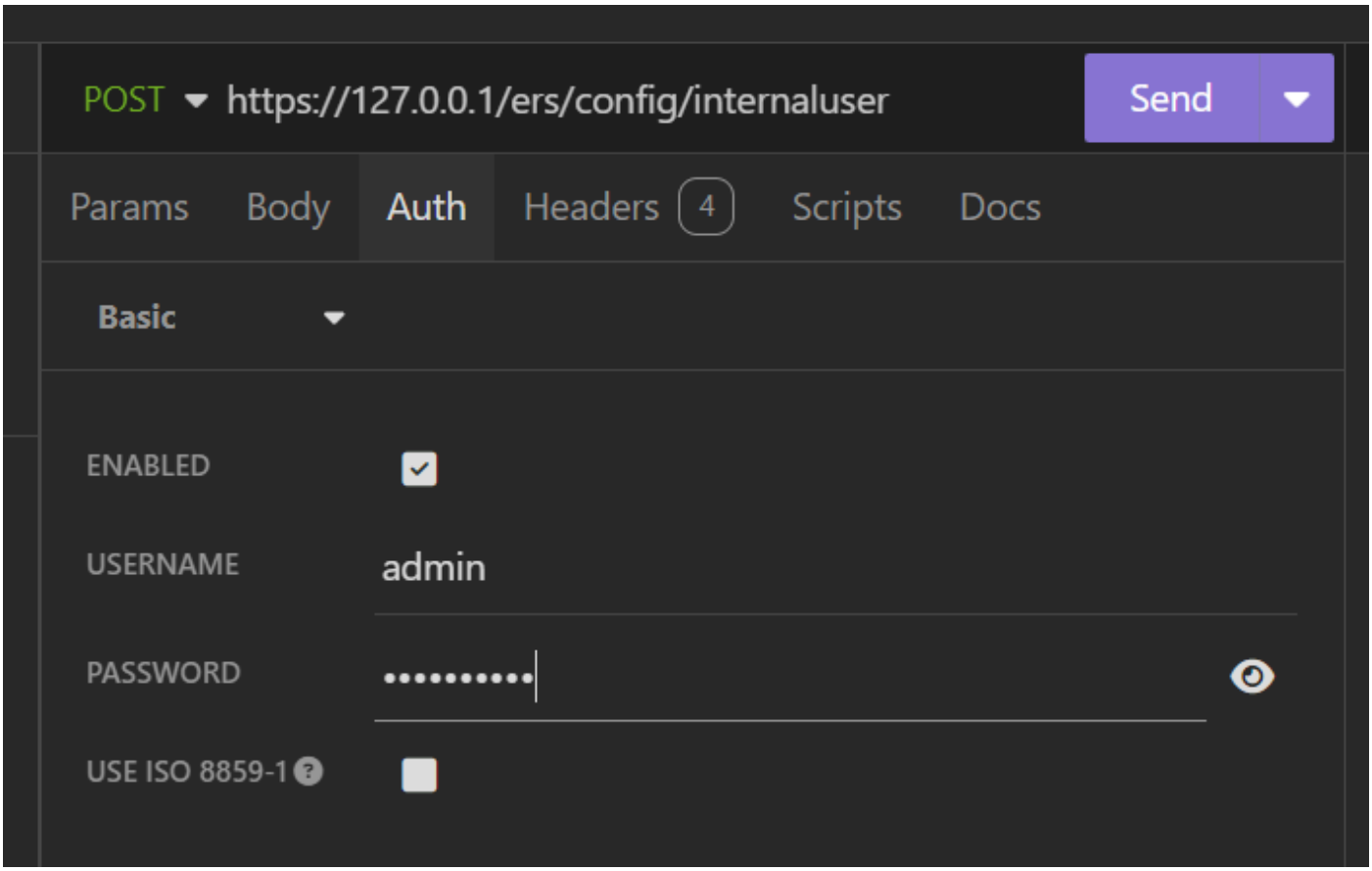
```
    "password": "password",
    "firstName": "firstName",
    "lastName": "lastName",
    "changePassword": true,
    "identityGroups": "identityGroups",
    "passwordNeverExpires": false,
    "daysForPasswordExpiration": 60,
    "expiryDateEnabled": false,
    "expiryDate": "2016-12-11",
    "enablePassword": "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.



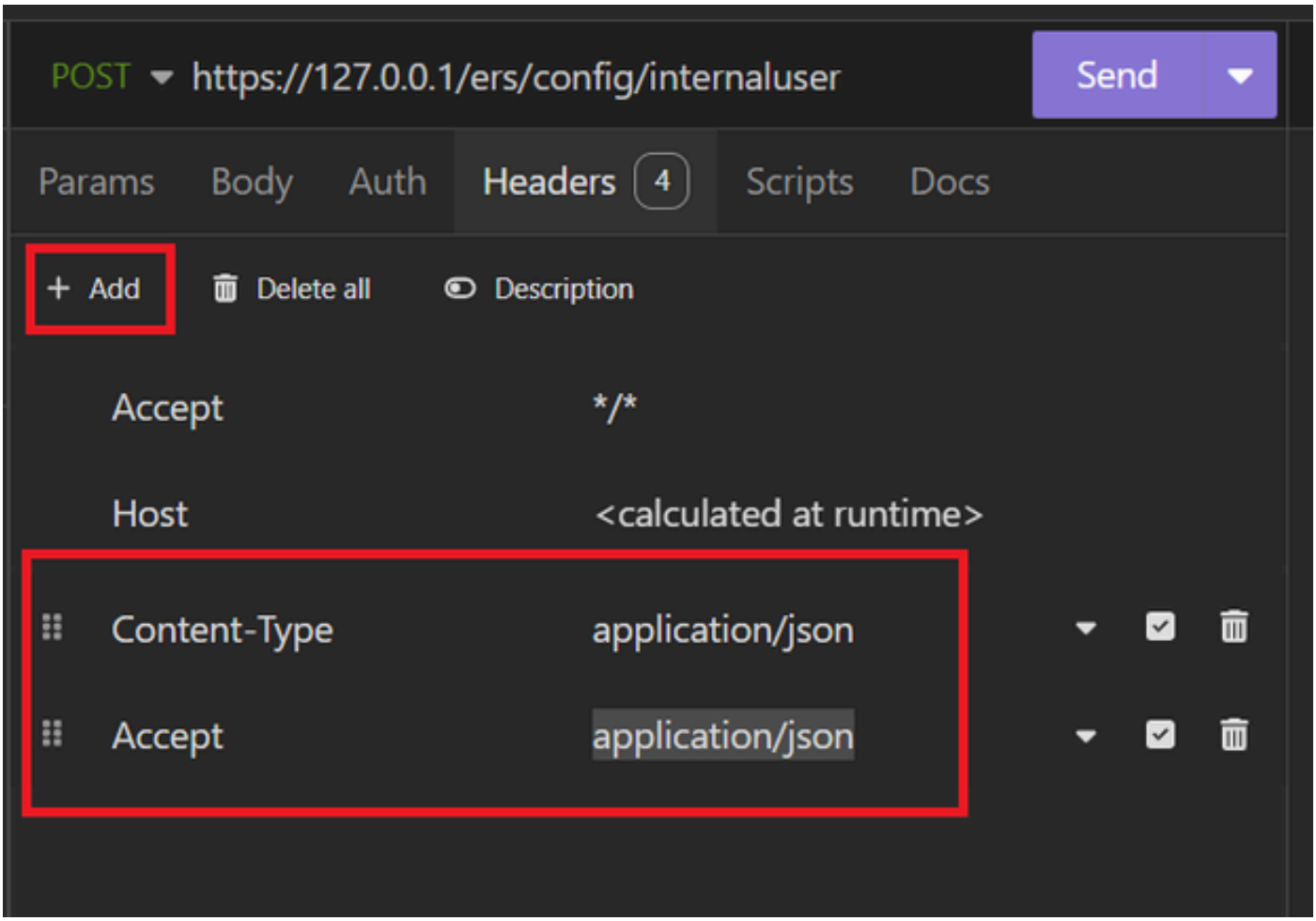
autenticación JSON

7. Introduzca las credenciales de la GUI de ISE.



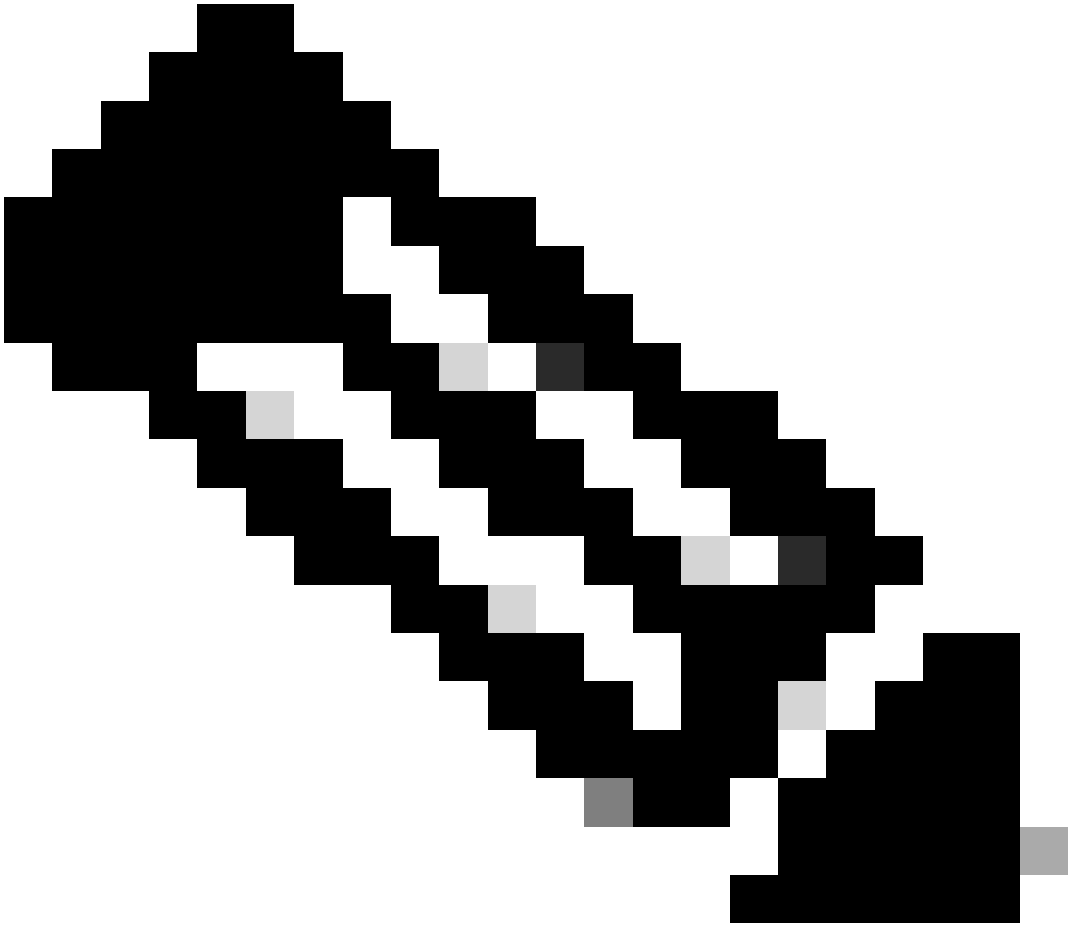
Credenciales JSON de administrador

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



Encabezados JSON

9. Por último, haga clic en Enviar.



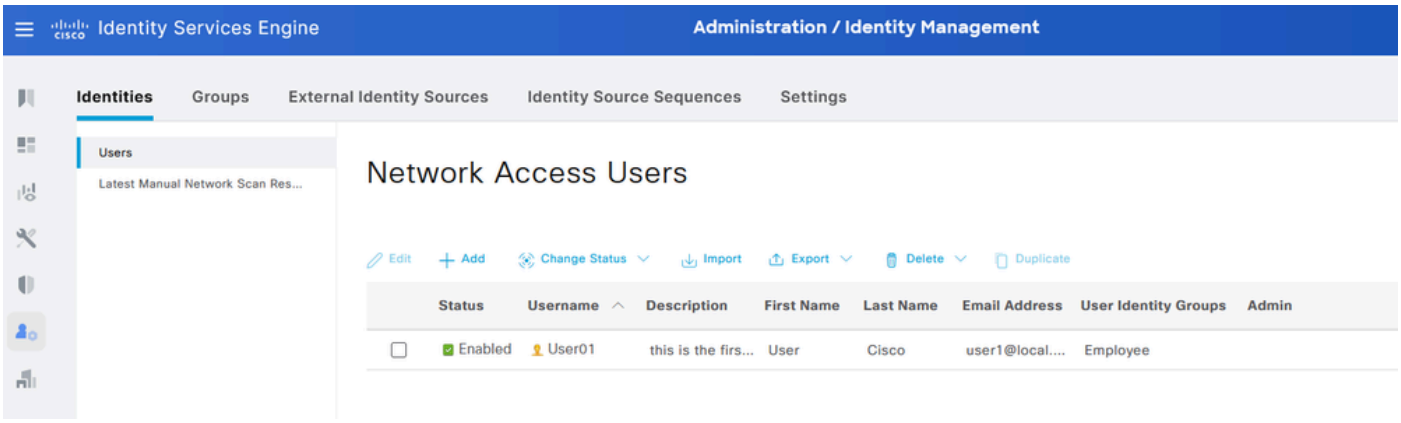
Nota: Si desea asignar un grupo de identidad a la nueva cuenta de usuario, debe utilizar el ID del grupo de identidad. Consulte la sección **Troubleshooting** para obtener más información.

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

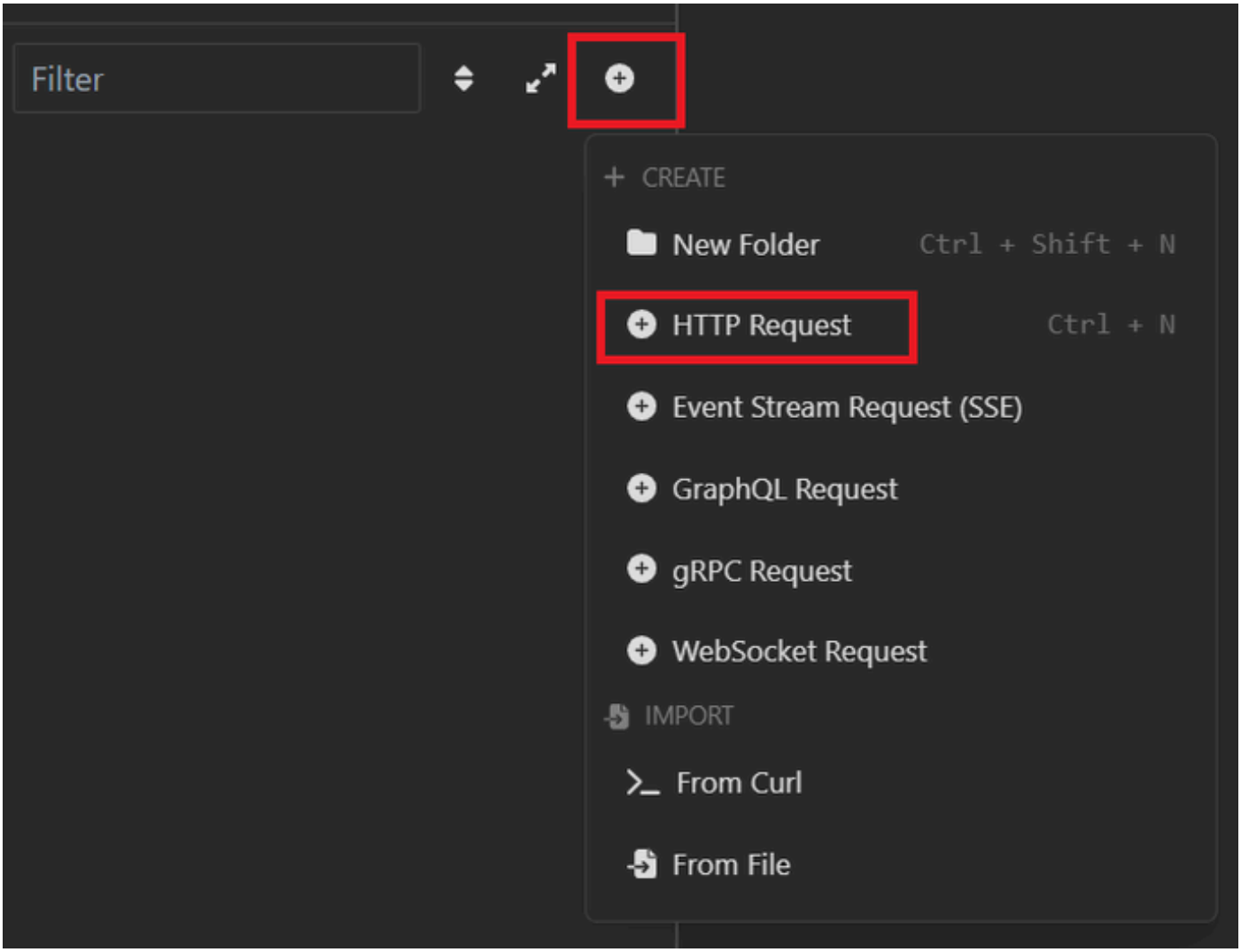
2. Abra la GUI de ISE y vaya a Administration > Identity Management > Identities > Users > Network Access Users



Cuenta de usuario JSON

solicitud XML

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

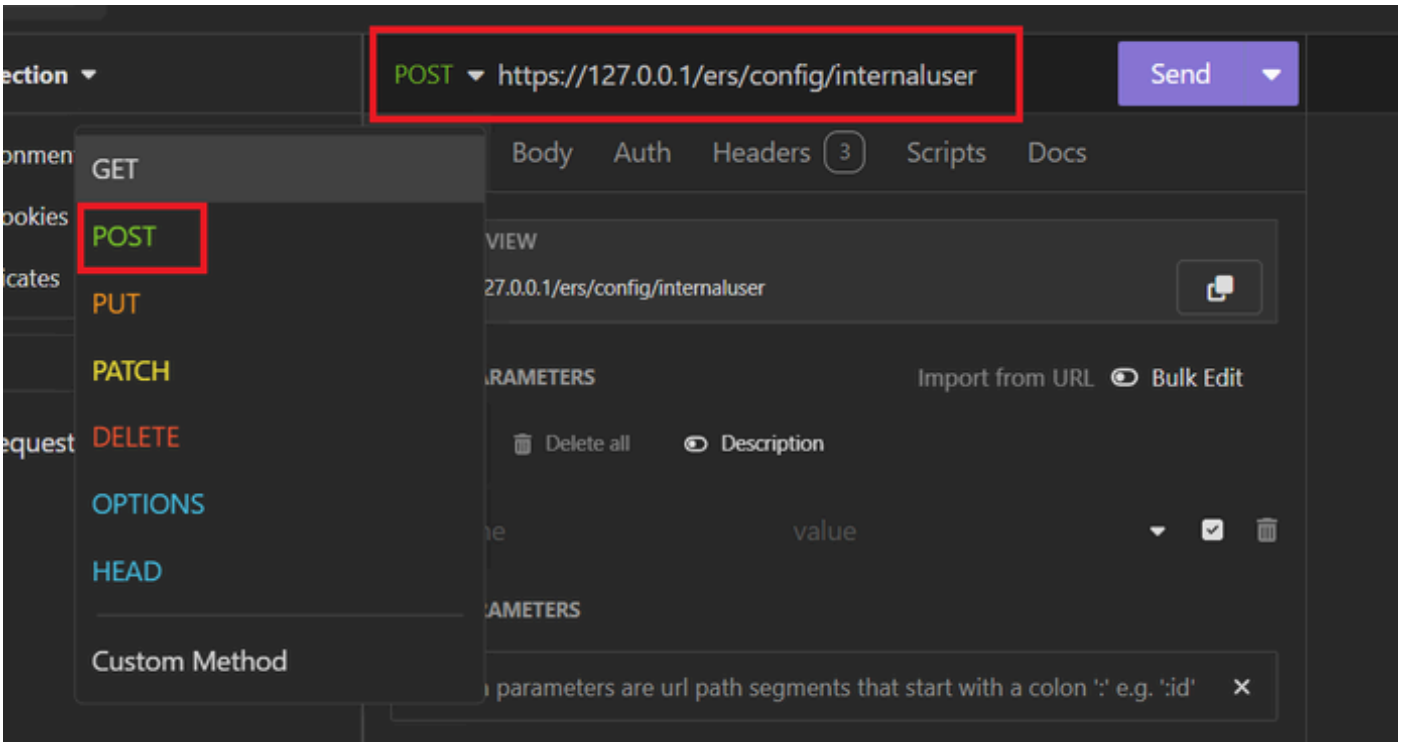


Solicitud XML

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

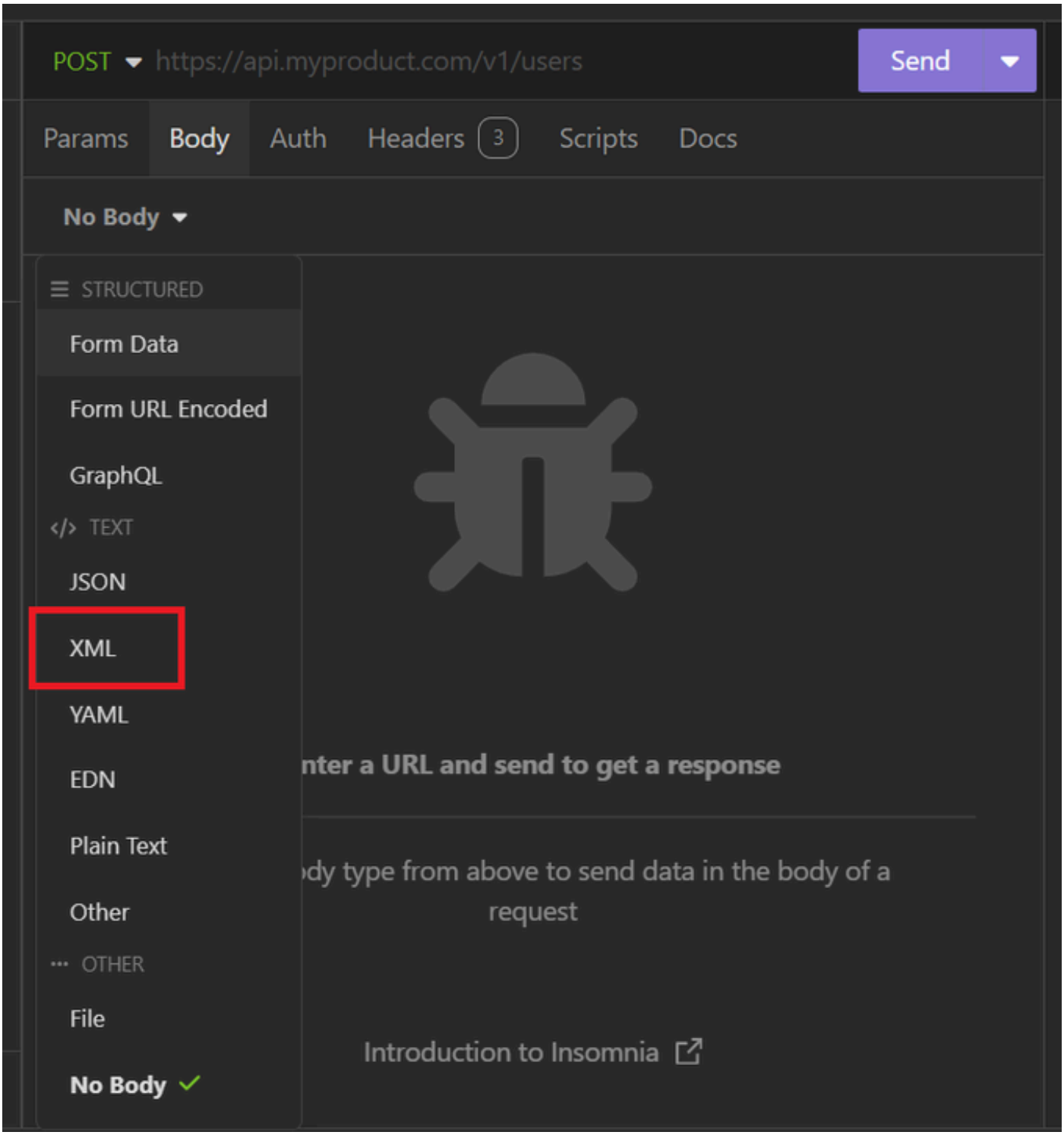
La URL que debe introducir depende de la dirección IP del nodo ISE.

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



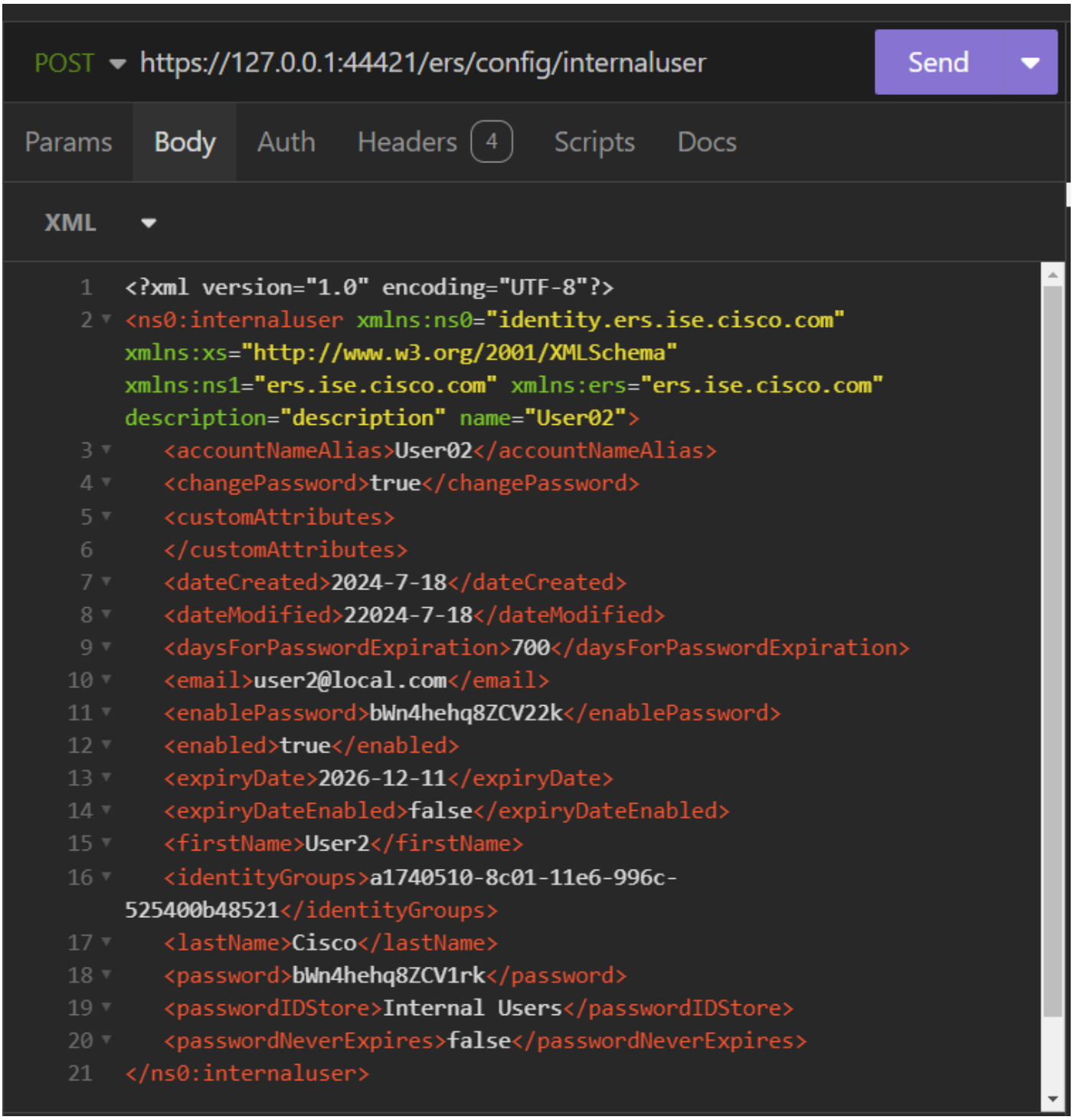
XML POST

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.



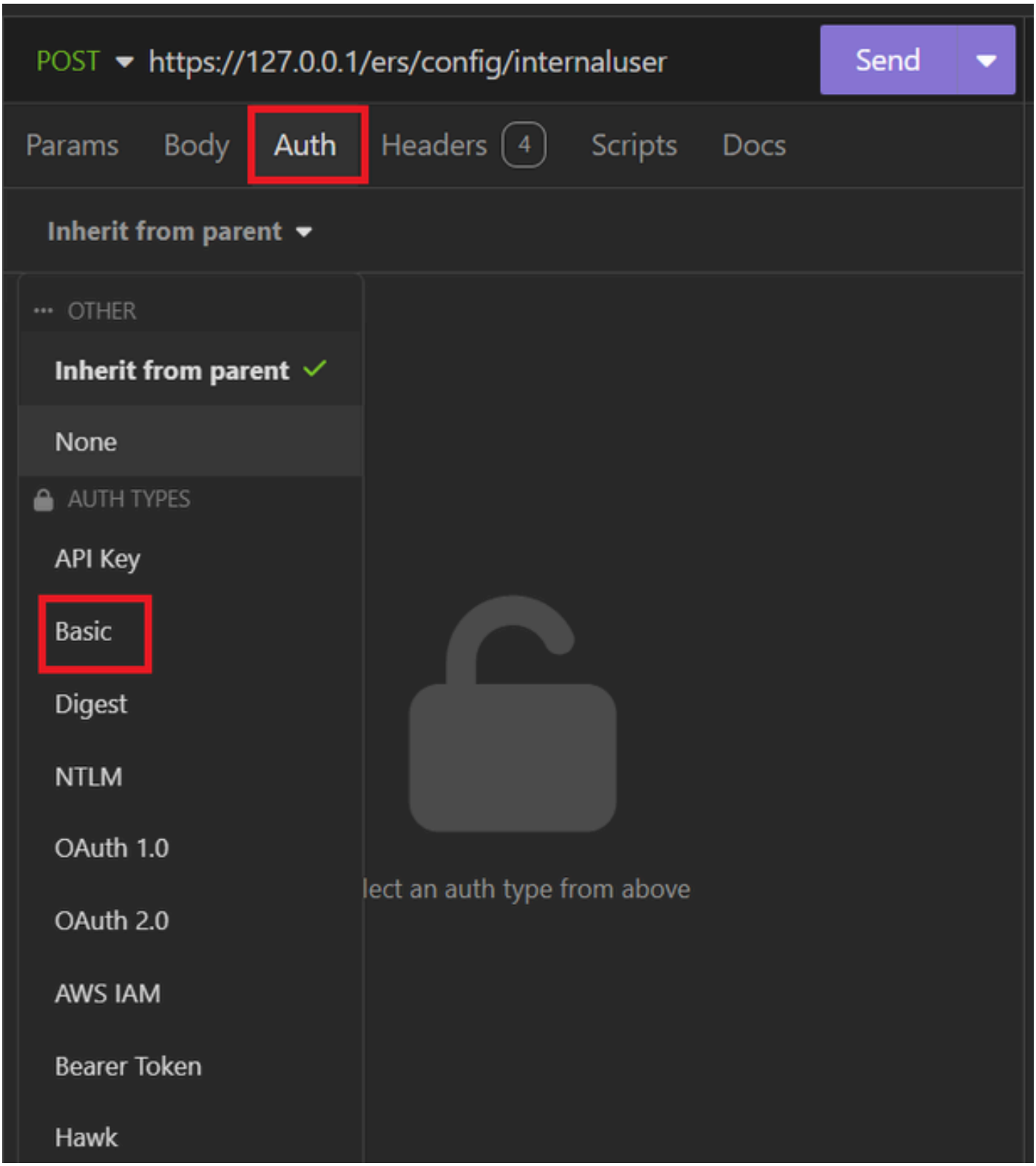
Publicación XML

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>
```

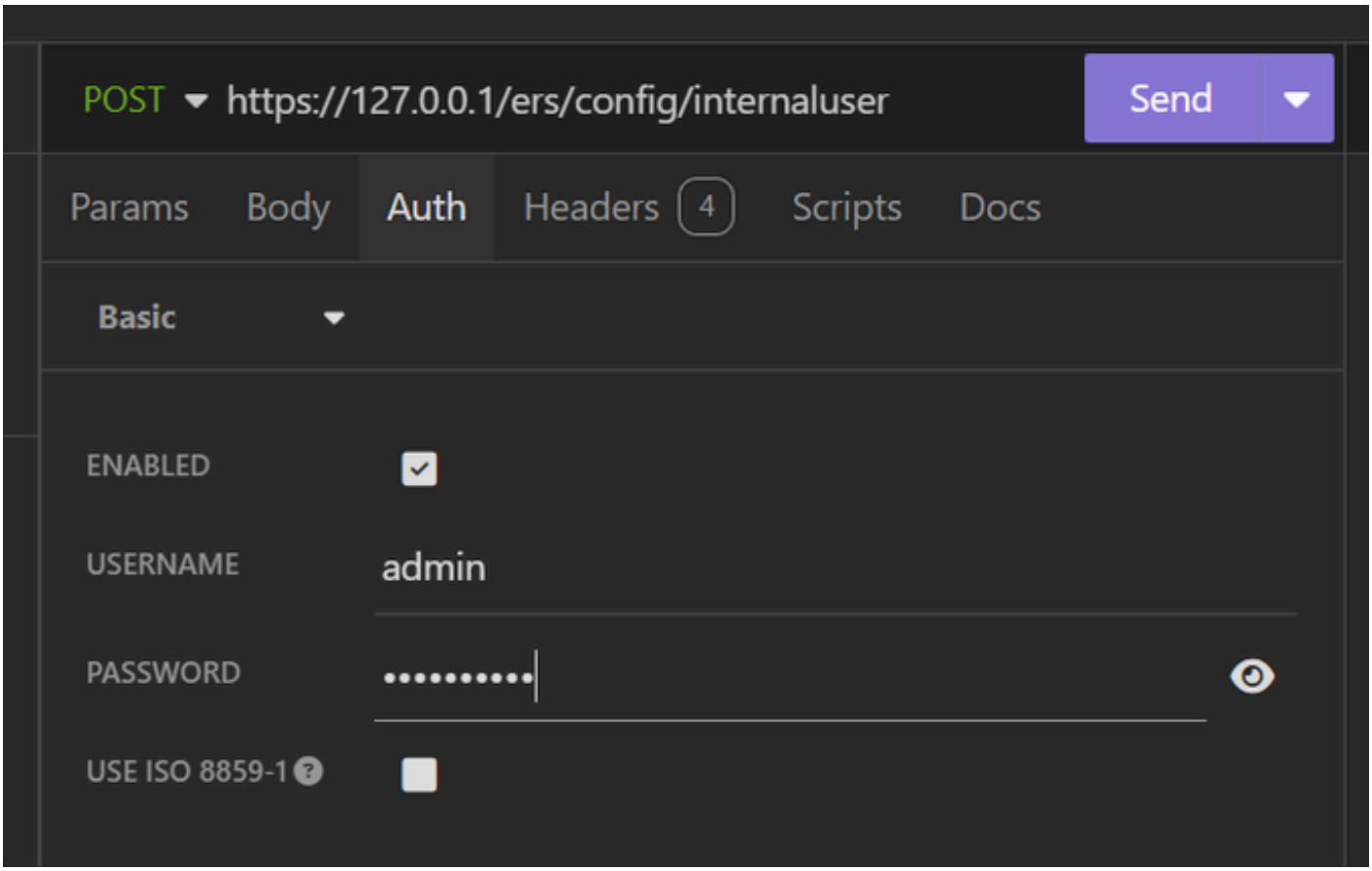
```
      <entry>
         <key>key1</key>
         <value>value1</value>
      </entry>
      <entry>
         <key>key2</key>
         <value>value3</value>
      </entry>
   </customAttributes>
   <dateCreated>2015-12-15</dateCreated>
   <dateModified>2015-12-20</dateModified>
   <daysForPasswordExpiration>60</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



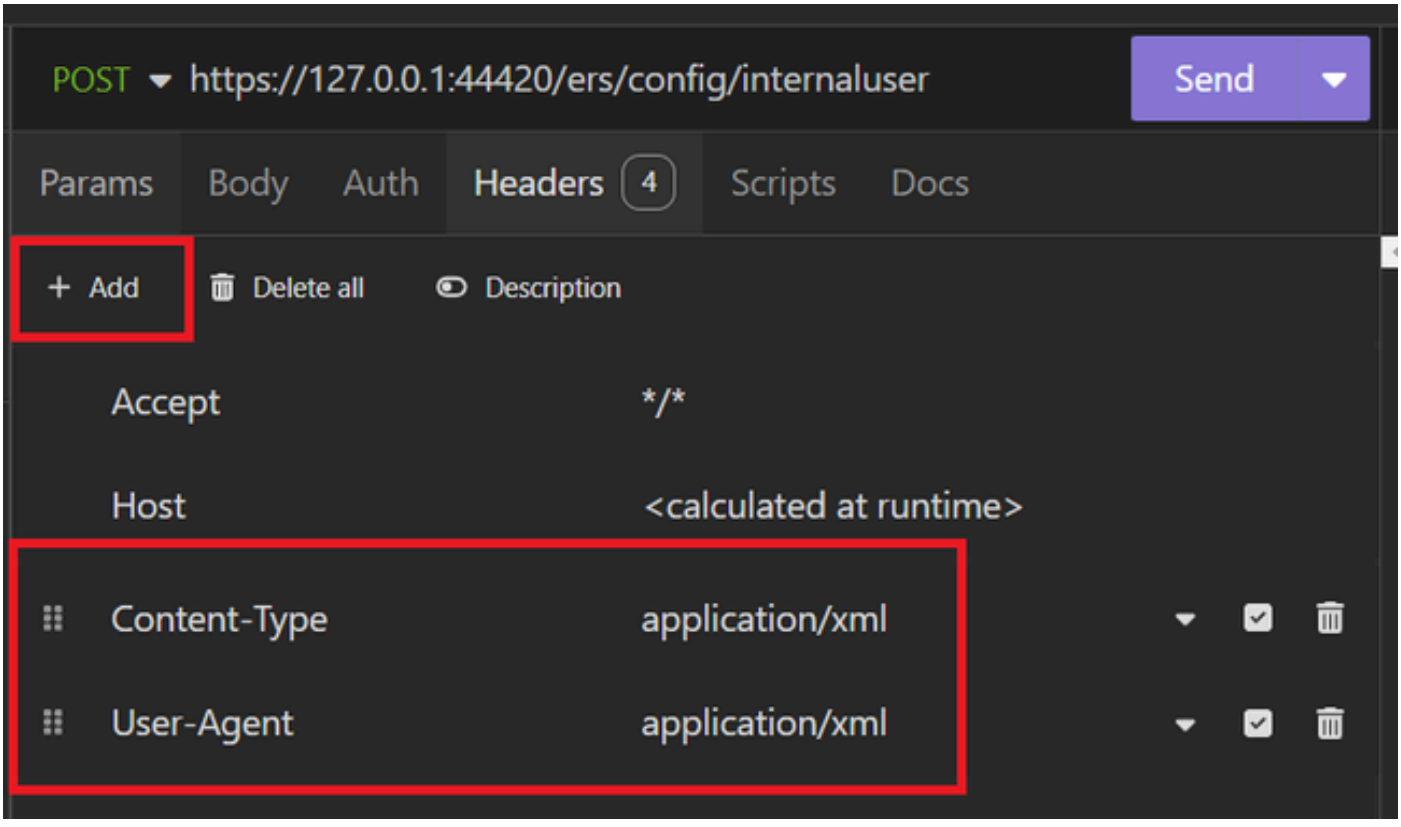
autenticación XML

7. Introduzca las credenciales de la GUI de ISE.



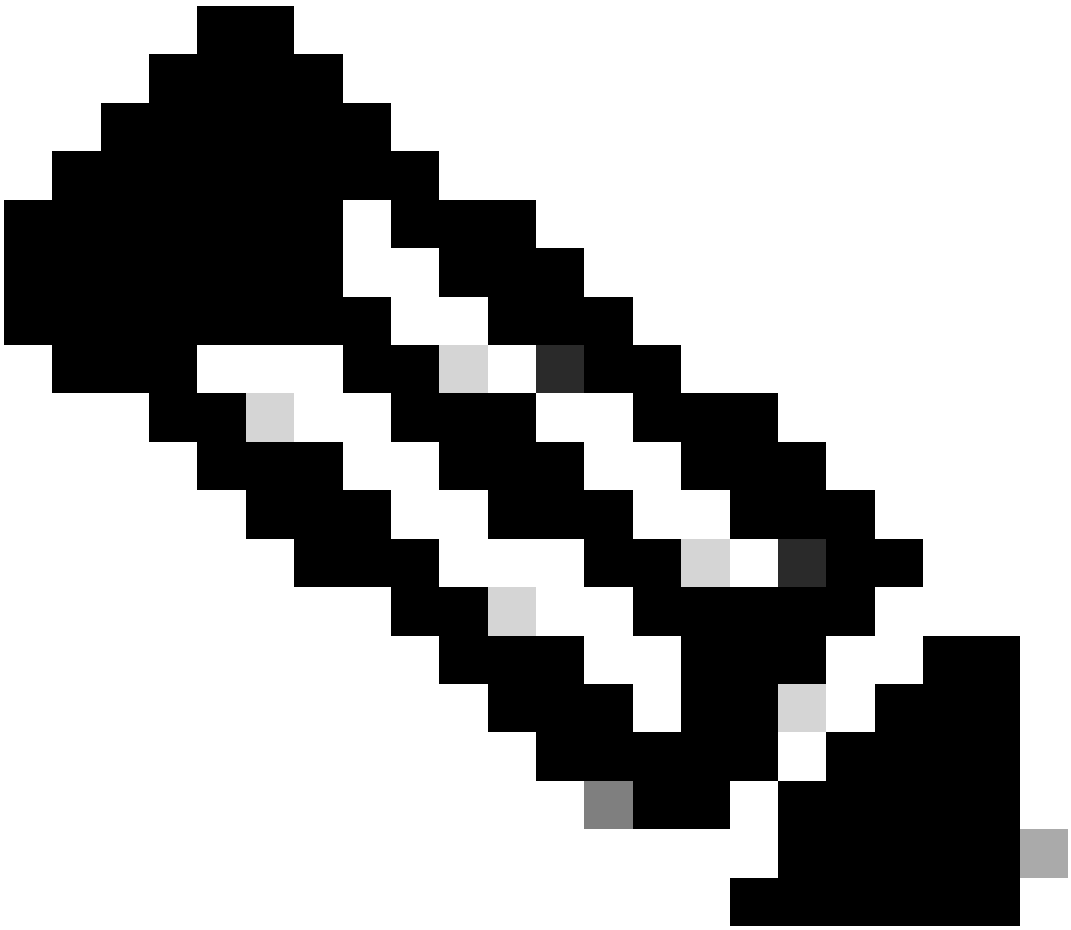
Credenciales XML

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.



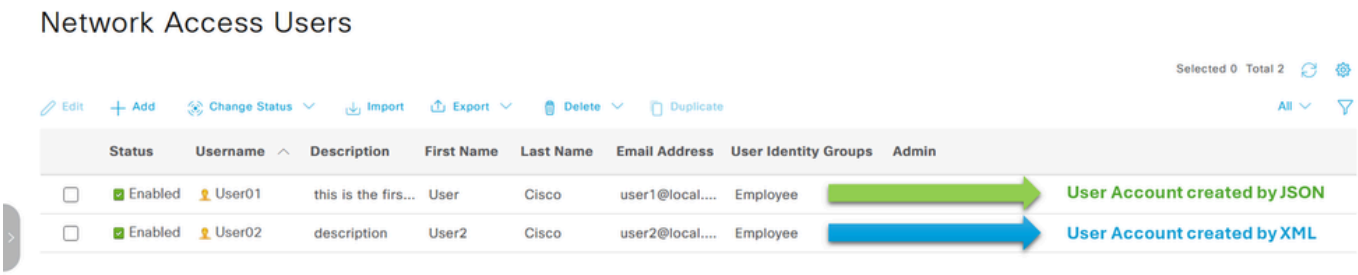
Nota: Si desea asignar un grupo de identidad a la nueva cuenta de usuario, debe utilizar el ID del grupo de identidad. Consulte la sección **Troubleshooting** para obtener más información.

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

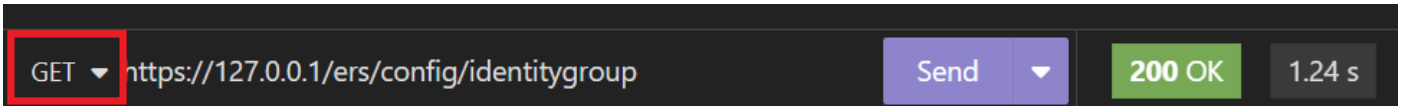


Validación de cuentas de usuario

Troubleshoot

1. Identifique la ID del grupo de identidad.

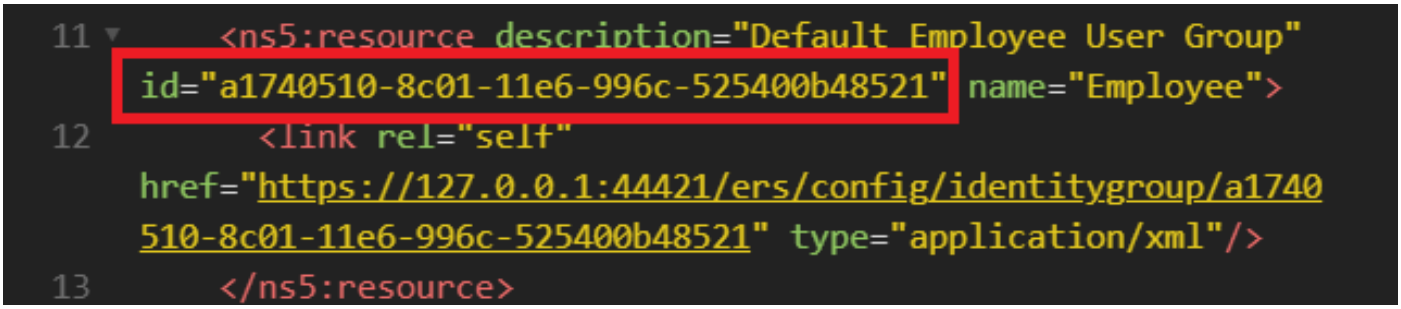
Utilice GET y la consulta https://X.X.X.X/ers/config/identitygroup.



opción GET

Salida JSON.

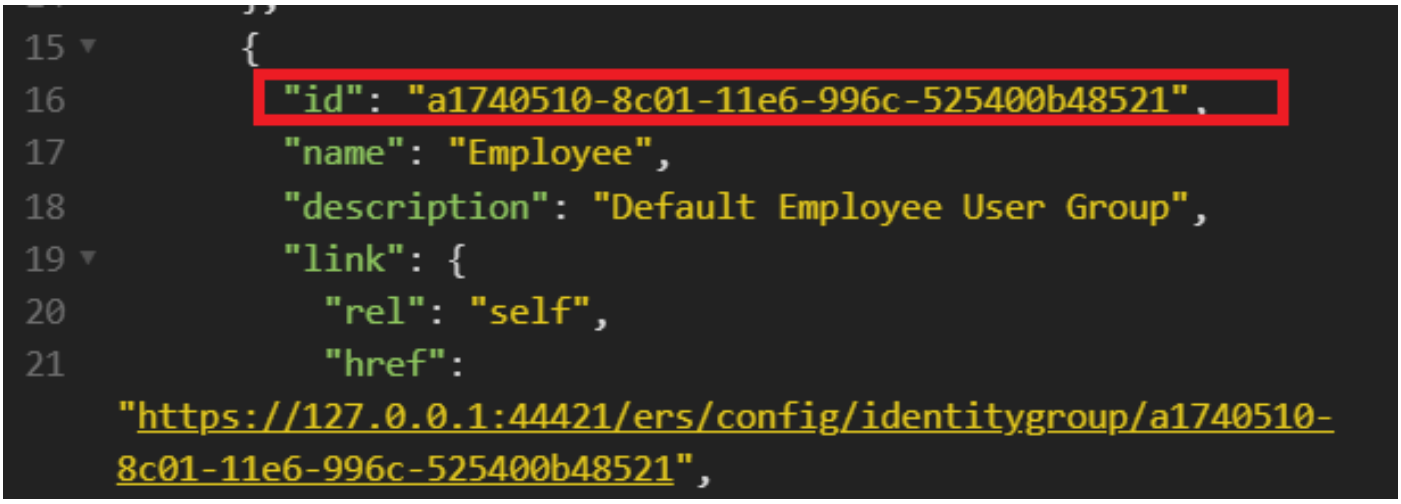
Identifique la ID junto a la descripción.



Grupo de Identidad de ID 01

Resultado XML.

Identifique la ID junto a la descripción.



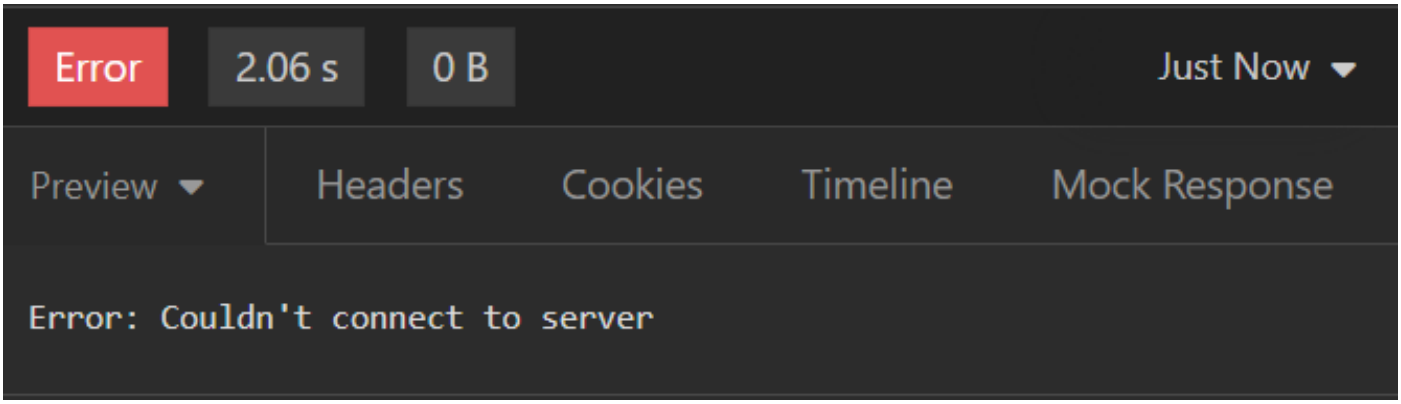
ID Grupo de Identidad 02

2. 401 Error no autorizado.

error 401

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

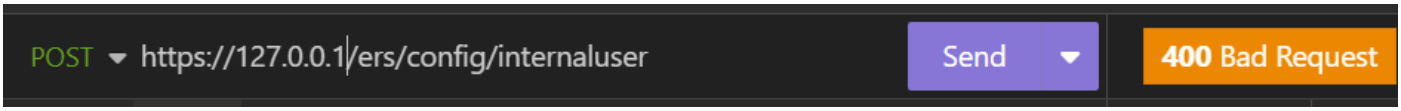
3. Error: no se pudo conectar al servidor



Error de conexión

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

4. 400 Solicitud incorrecta.

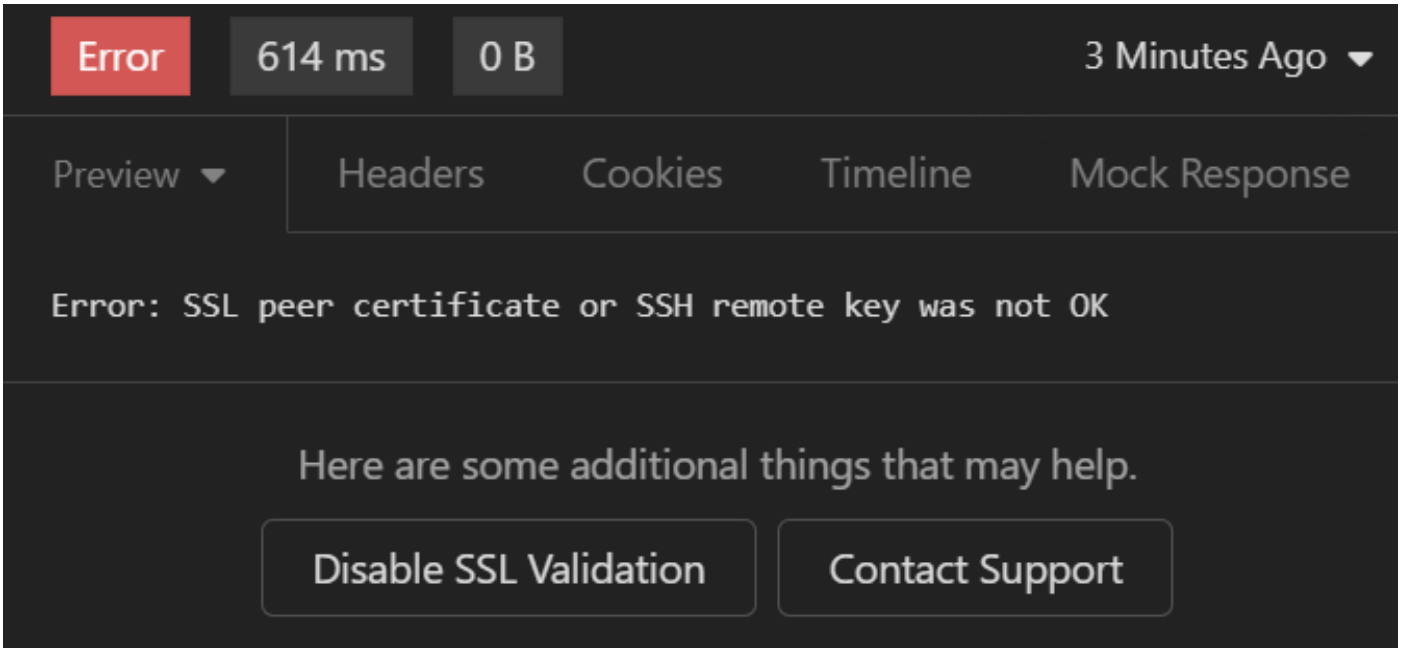


error 400

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.

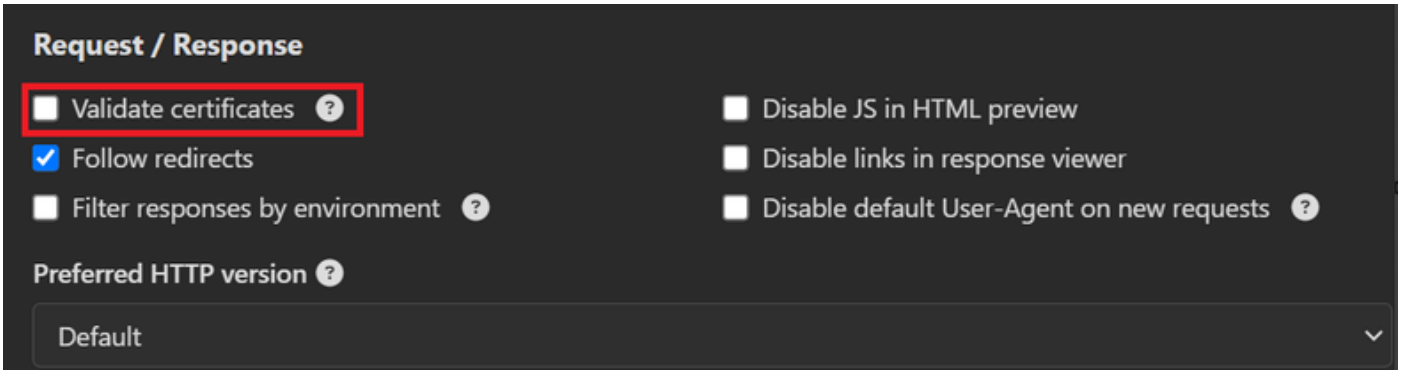
5. Error: el certificado de par SSL o la clave remota SSH no eran correctos



Error de certificado SSL

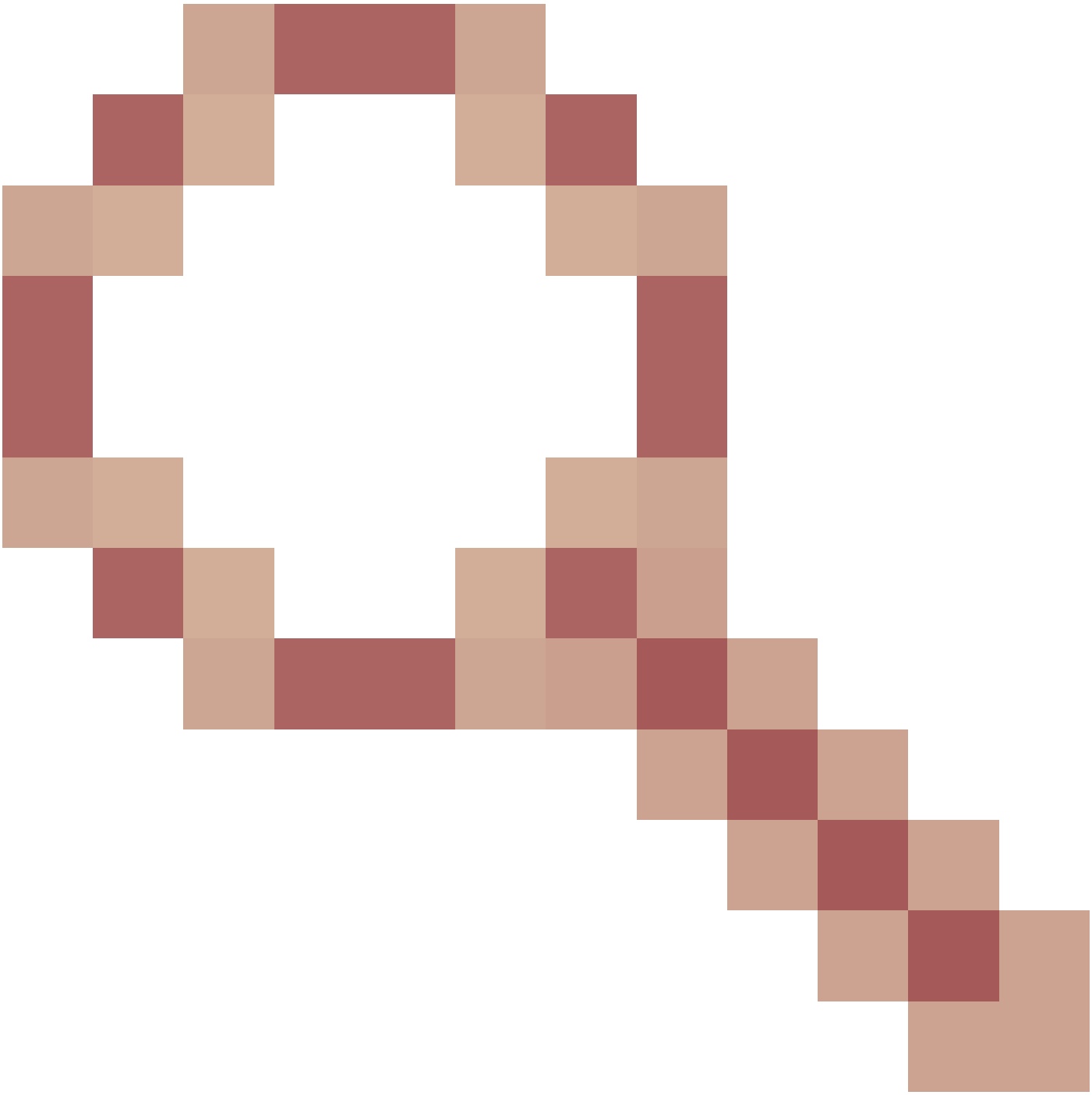
Solución:

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:

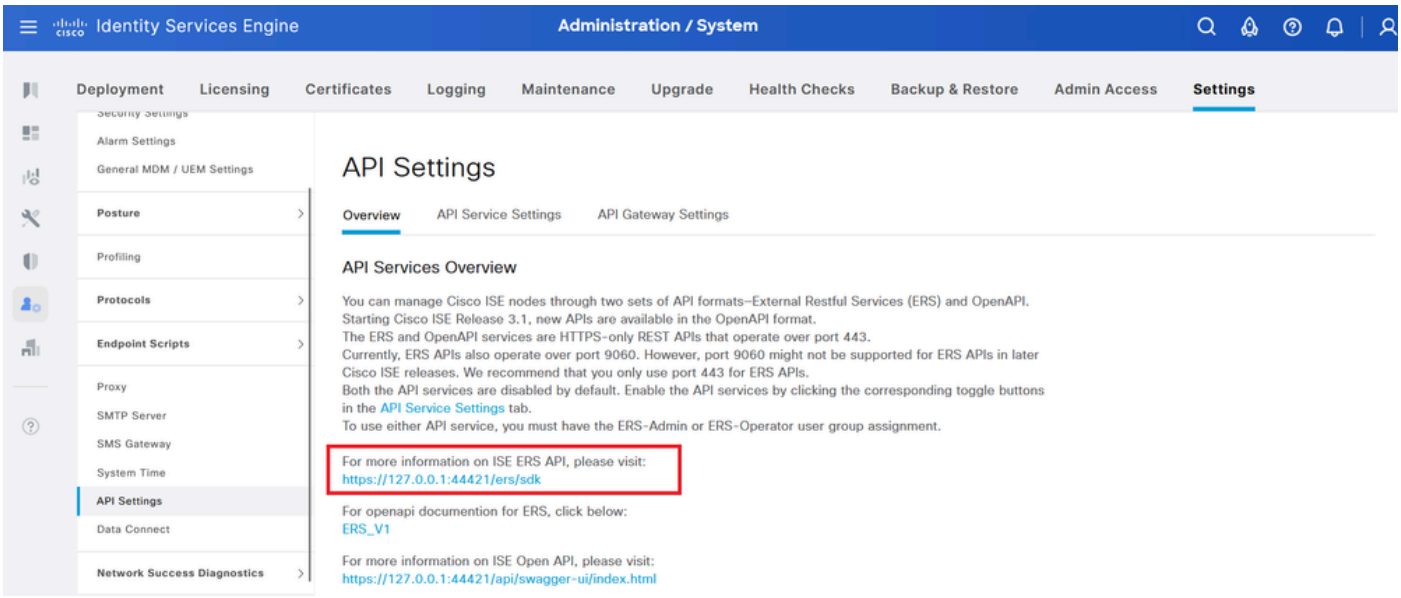
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh71435

Referencias de llamadas API.

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

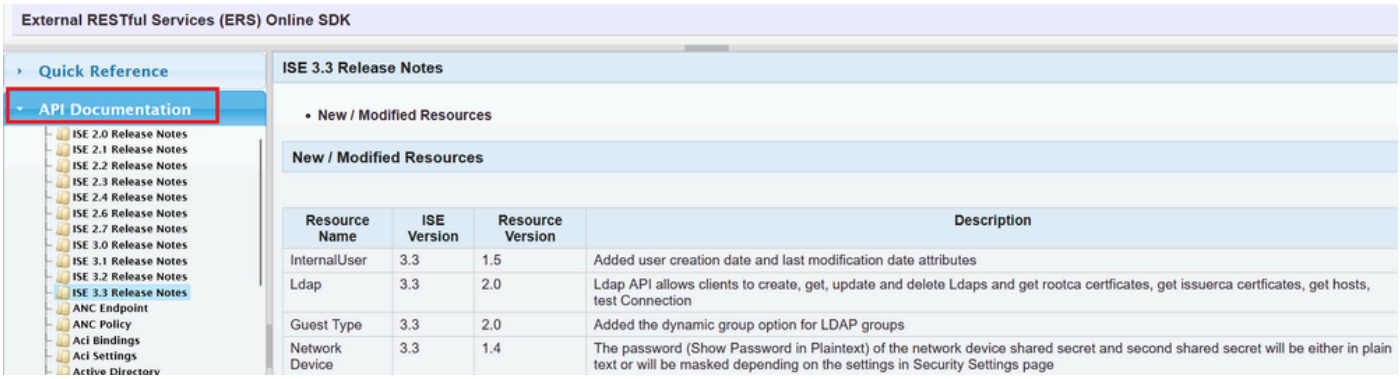
1. Vaya a Administración > Sistema > Configuración > Configuración de API.

2. Haga clic en el enlace de información de la API ERS.



Configuración de API

3. Y haga clic en documentación de API.



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).