Configurazione degli utenti interni tramite chiamate JSON o XML e API in ISE 3.3 con Insominia

Sommario

Introduzione

Questo documento descrive la configurazione degli utenti interni in Cisco ISE usando i formati di dati JSON o XML insieme alle chiamate API.

Prerequisiti

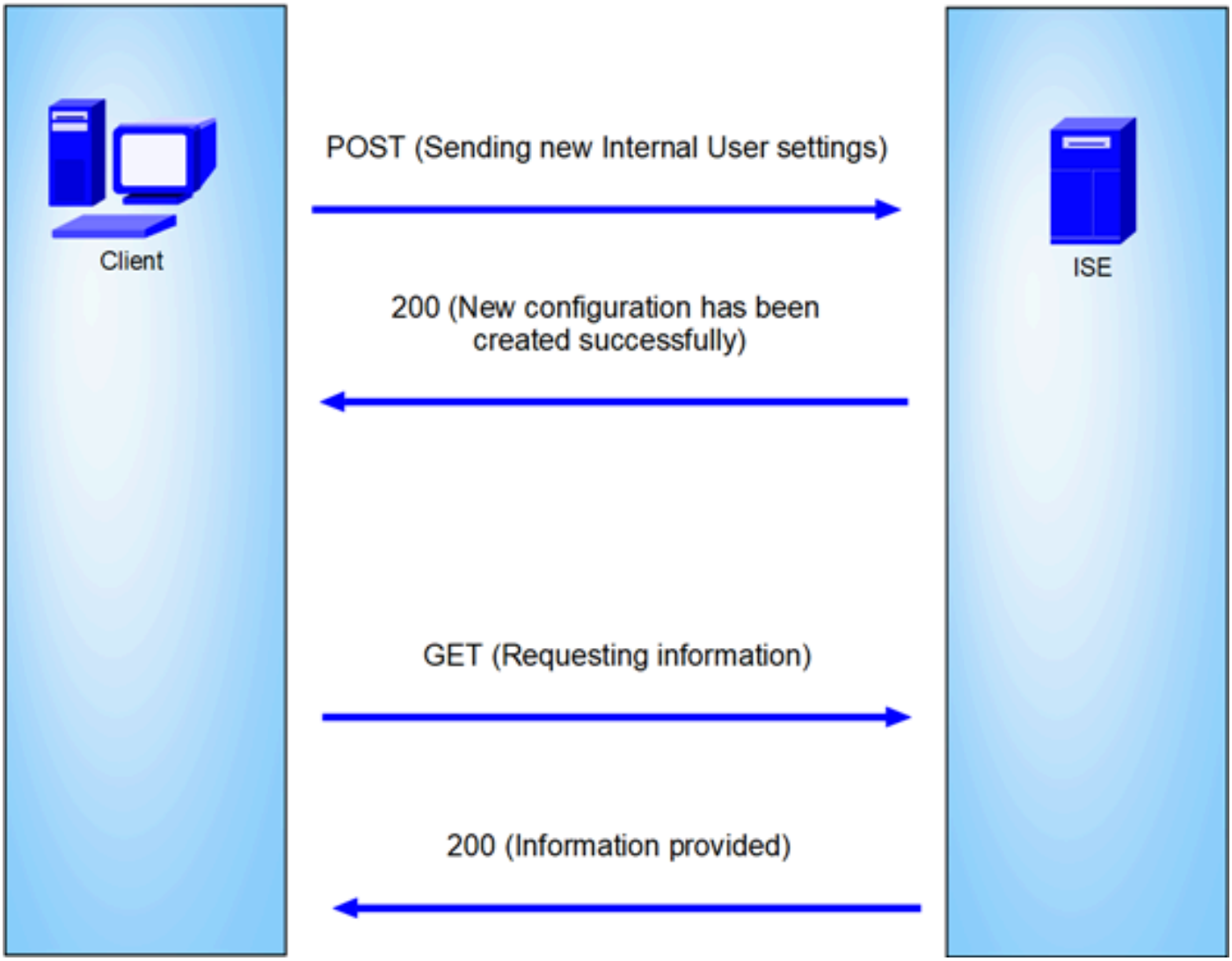
- ISE 3.0 o versione successiva.
- Software Client API.

Componenti usati

- ISE 3.3
- Insominia 9.3.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete



Topologia generale

GET e POST sono due dei metodi HTTP più comuni utilizzati nelle chiamate API (Application Programming Interface). Vengono utilizzati per interagire con le risorse di un server, in genere per recuperare dati o inviarli per l'elaborazione.

OTTIENI chiamata API

Il metodo GET viene utilizzato per richiedere dati a una risorsa specificata. Le richieste GET sono i metodi più comuni e ampiamente utilizzati nelle API e nei siti Web. Quando si visita una pagina Web, il browser invia una richiesta GET al server che ospita la pagina Web.

POST API Call

Il metodo POST viene utilizzato per inviare dati al server per creare o aggiornare una risorsa. Le richieste POST vengono spesso utilizzate quando si inviano i dati del modulo o si carica un file.

Configurazioni

Per creare un utente interno, è necessario inviare le informazioni esatte dal software client API al

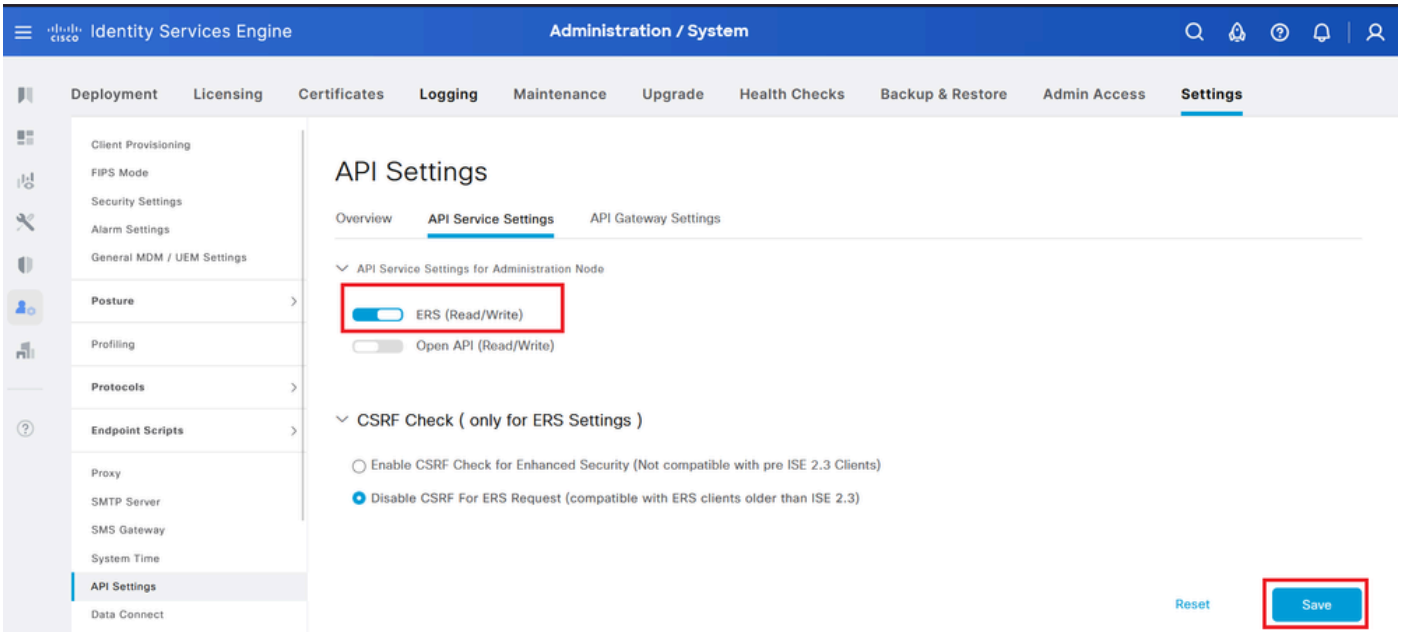
nodo ISE.

Configurazioni ISE

Attivare la funzione ERS.

1. Passare a Amministrazione > Sistema > Impostazioni > Impostazioni API > Impostazioni servizio API.

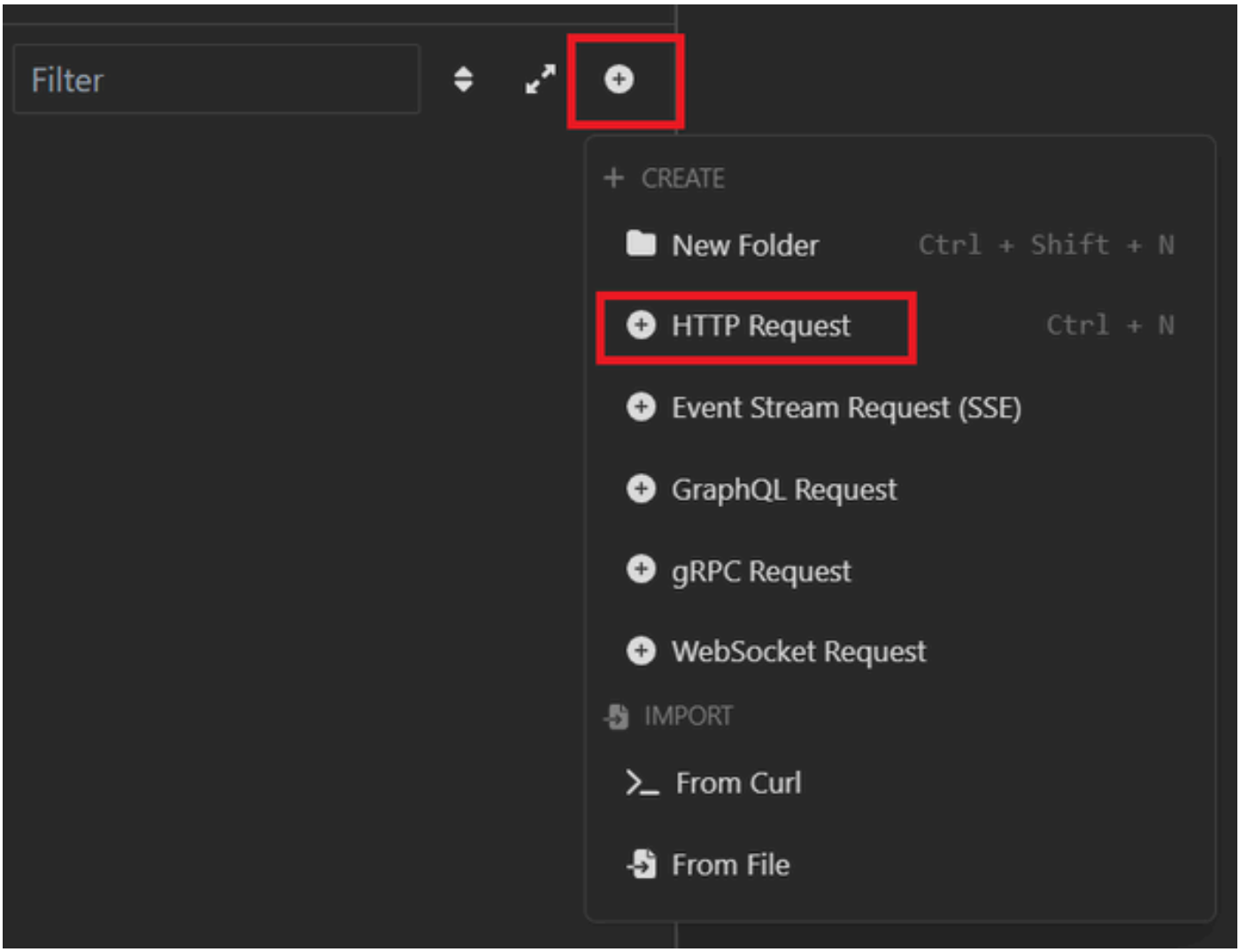
2. Abilitare l'opzione ERS (Read/Write).



Impostazioni API

Richiesta JSON.

1. Aprire Insonnia.
2. Aggiungere una nuova richiesta HTTPS sul lato sinistro.

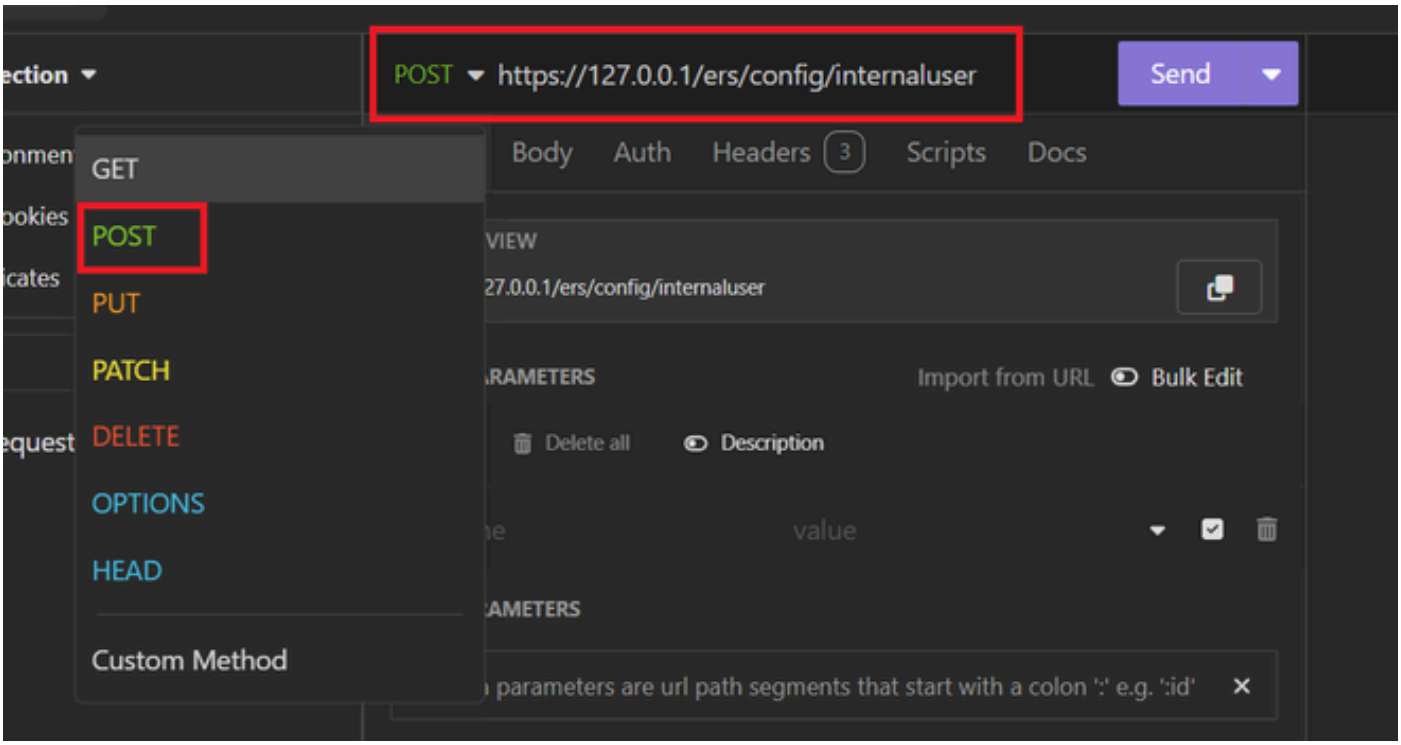


Richiesta JSON

3. Per inviare le informazioni al nodo ISE, è necessario scegliere POST.

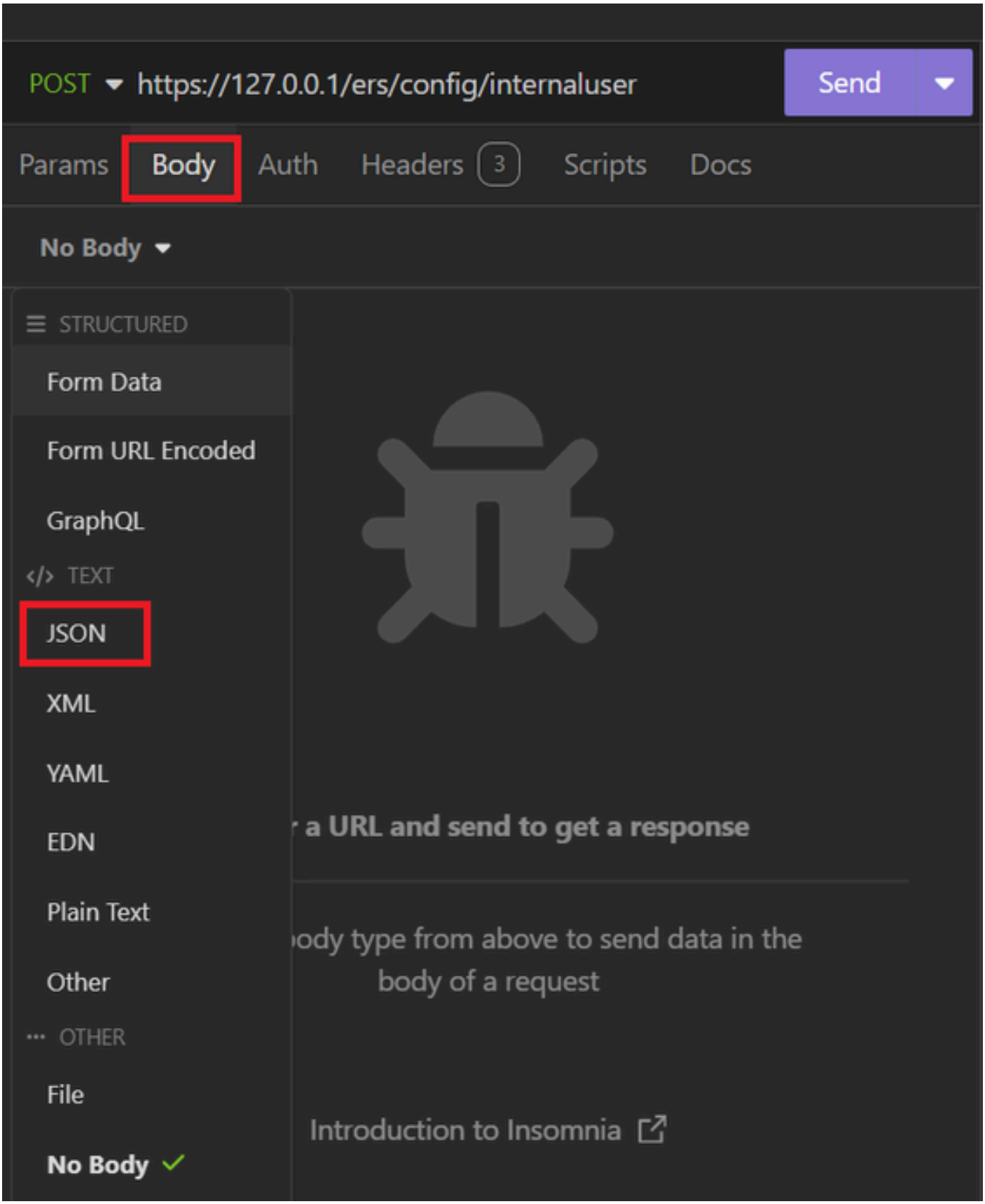
L'URL da immettere dipende dall'indirizzo IP del nodo ISE.

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



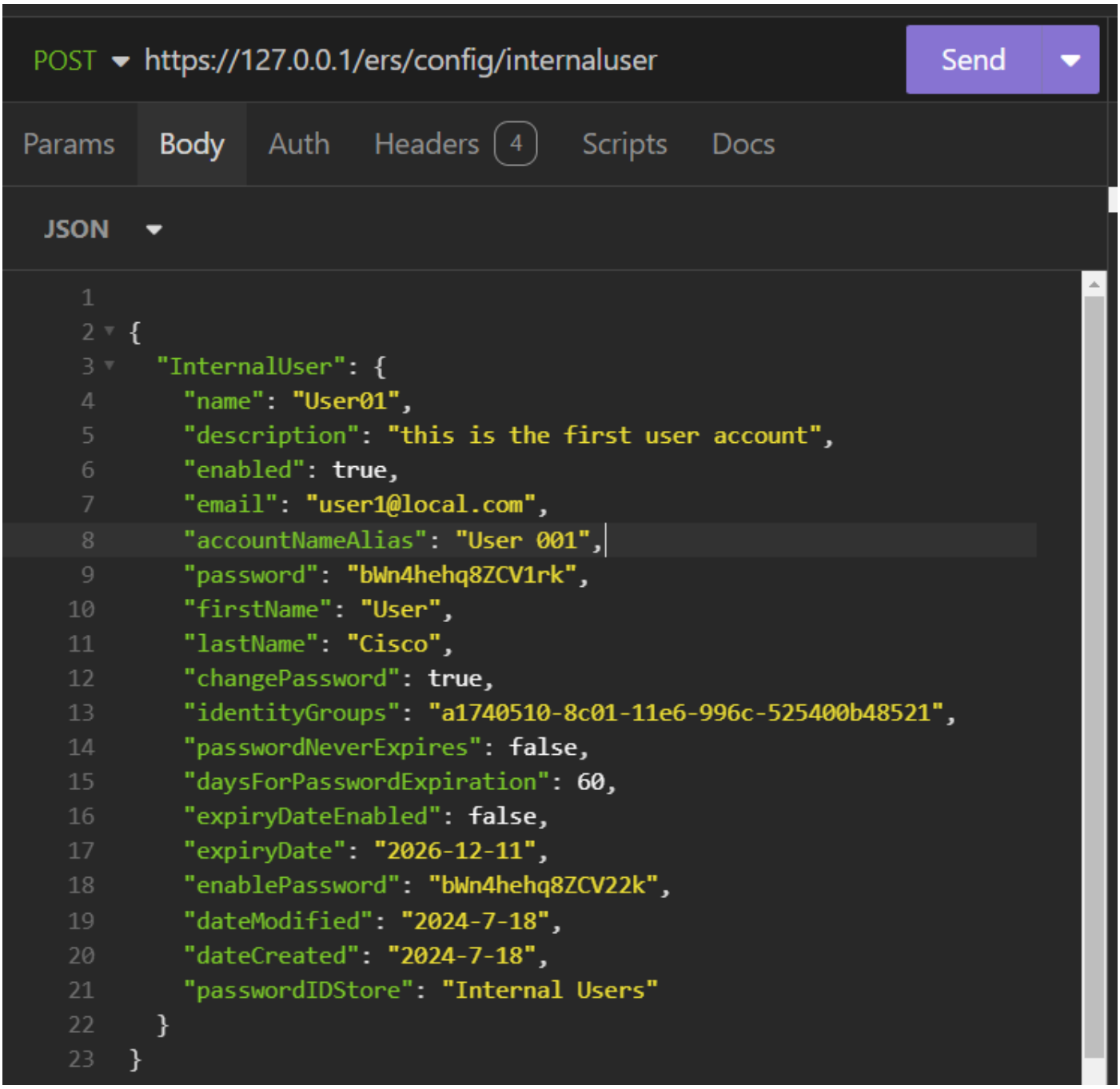
POST JSON

4. Quindi fare clic su Body e scegliere JSON



Corpo JSON

5. È possibile incollare la sintassi e modificare i parametri in base alle esigenze.



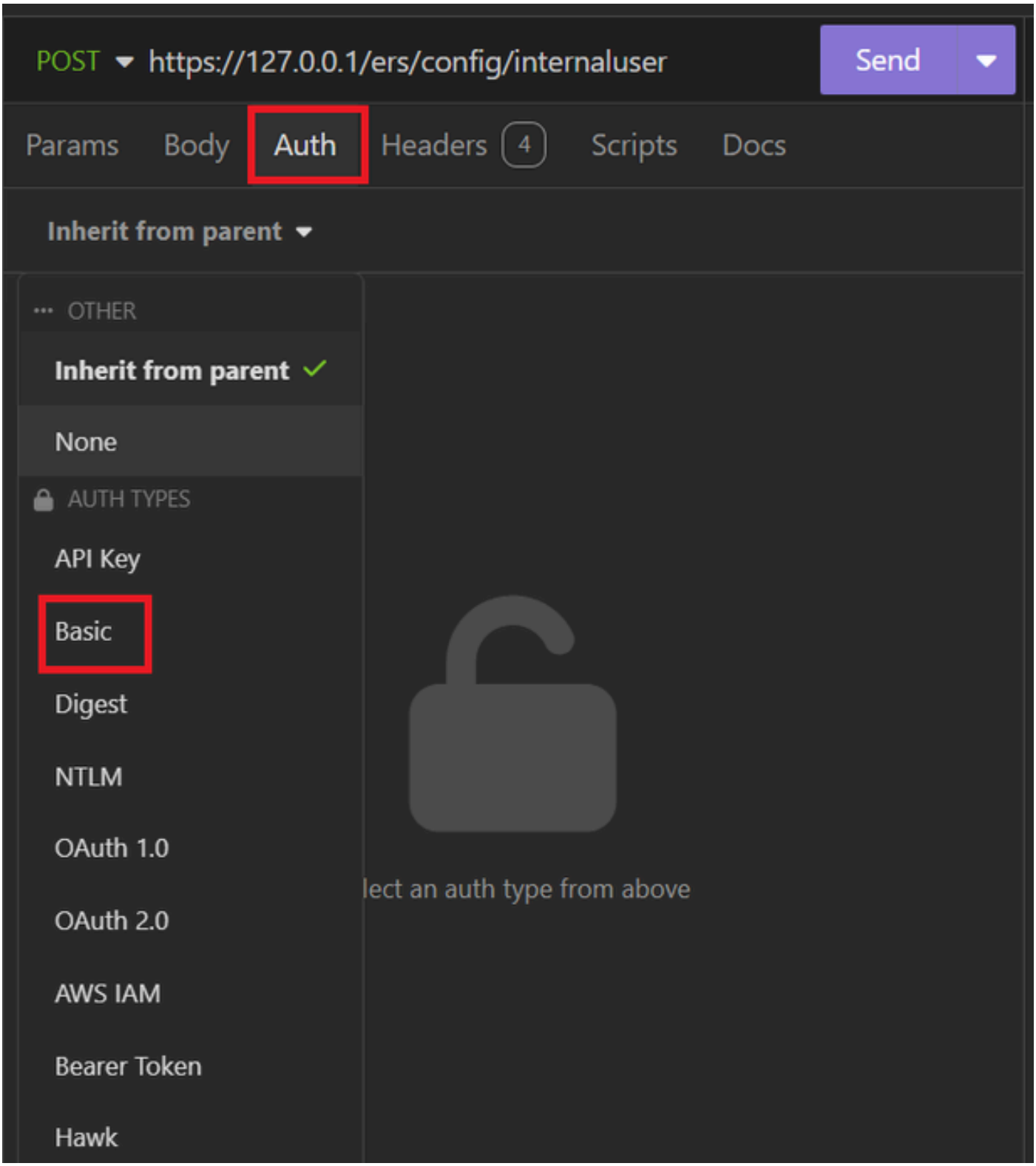
Sintassi JSON

Sintassi JSON

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

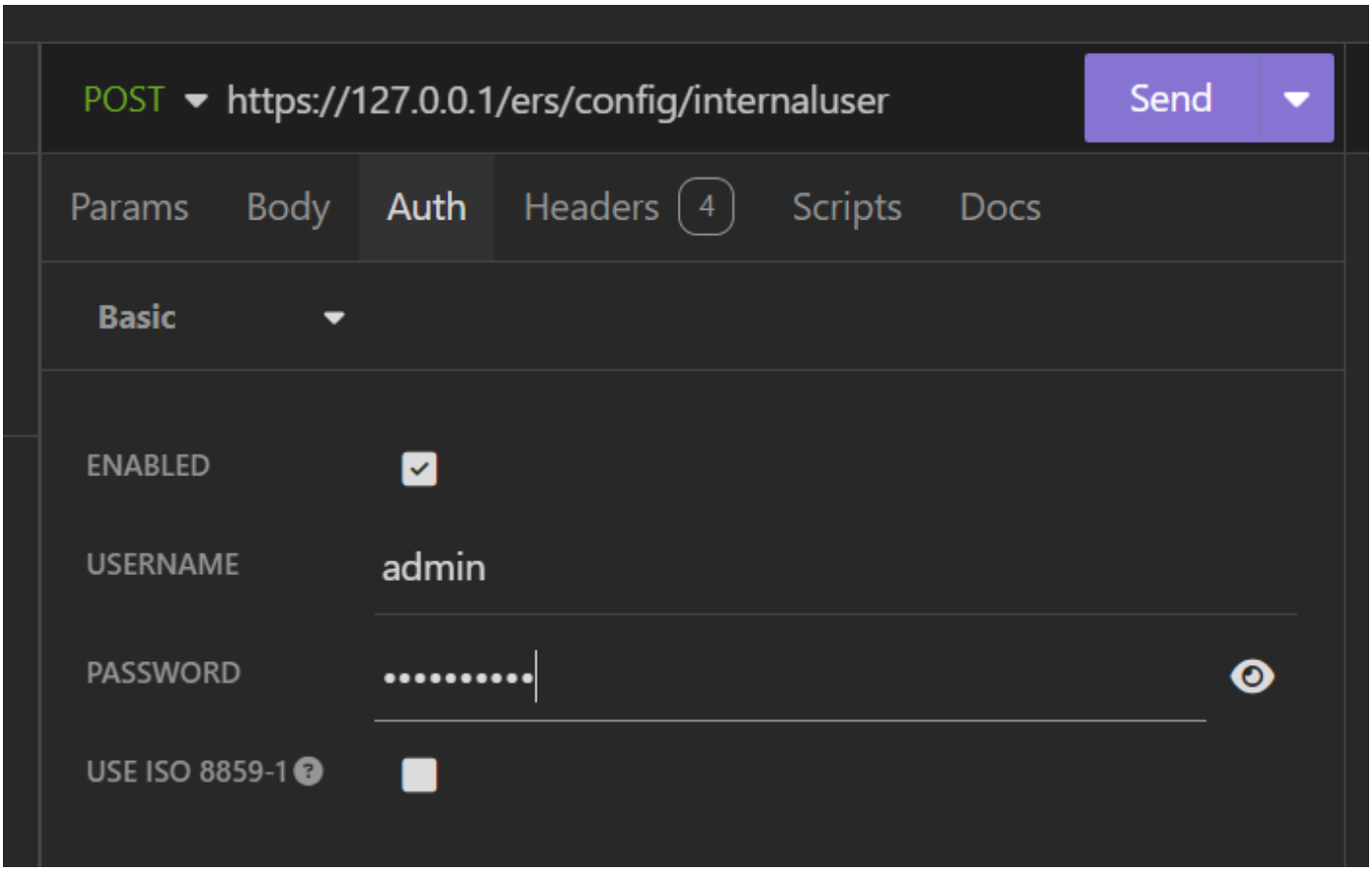
```
    "password": "password",
    "firstName": "firstName",
    "lastName": "lastName",
    "changePassword": true,
    "identityGroups": "identityGroups",
    "passwordNeverExpires": false,
    "daysForPasswordExpiration": 60,
    "expiryDateEnabled": false,
    "expiryDate": "2016-12-11",
    "enablePassword":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


6. Fare clic su Auth e scegliere Base.



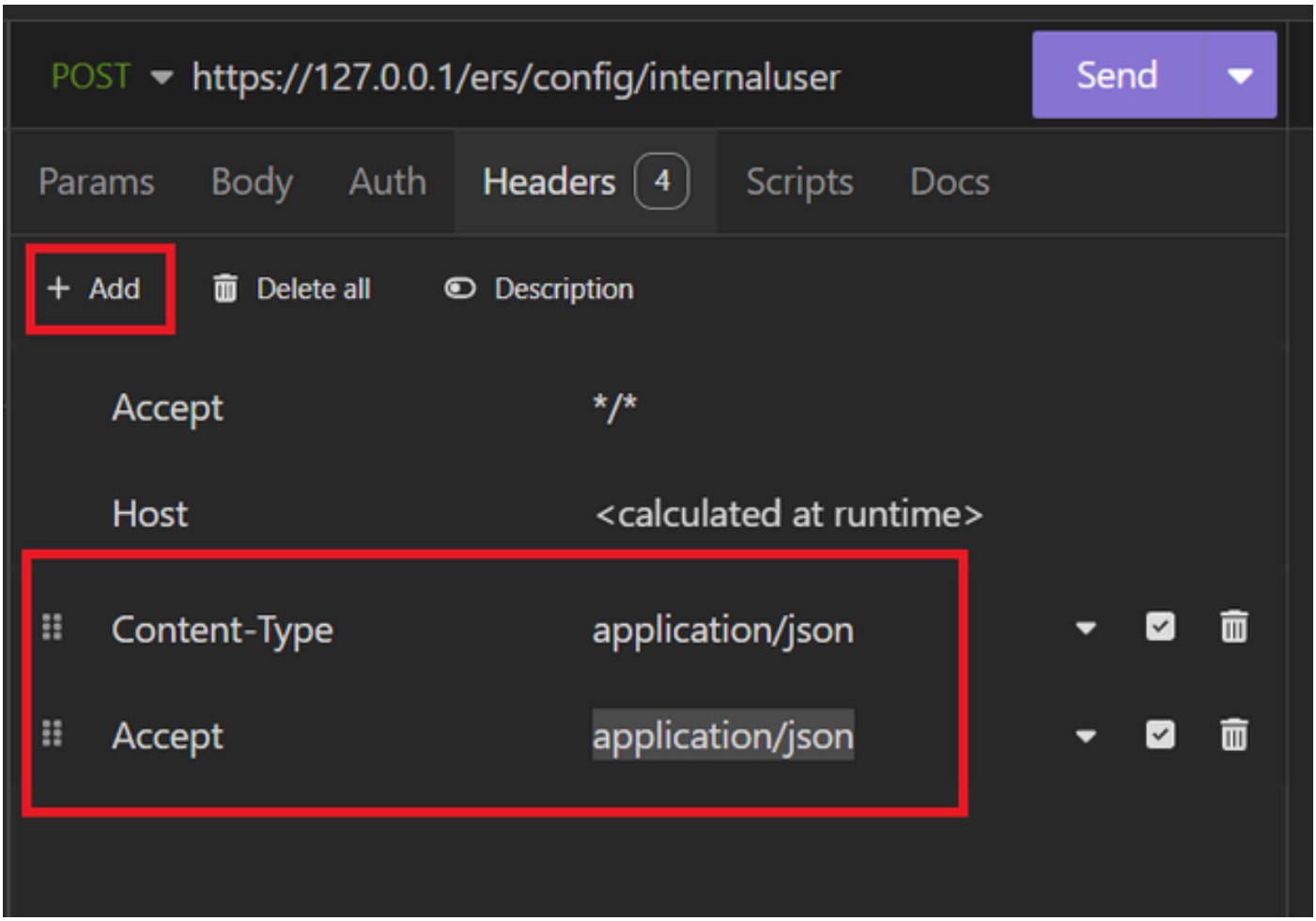
Autenticazione JSON

7. Immettere le credenziali dell'interfaccia grafica ISE.



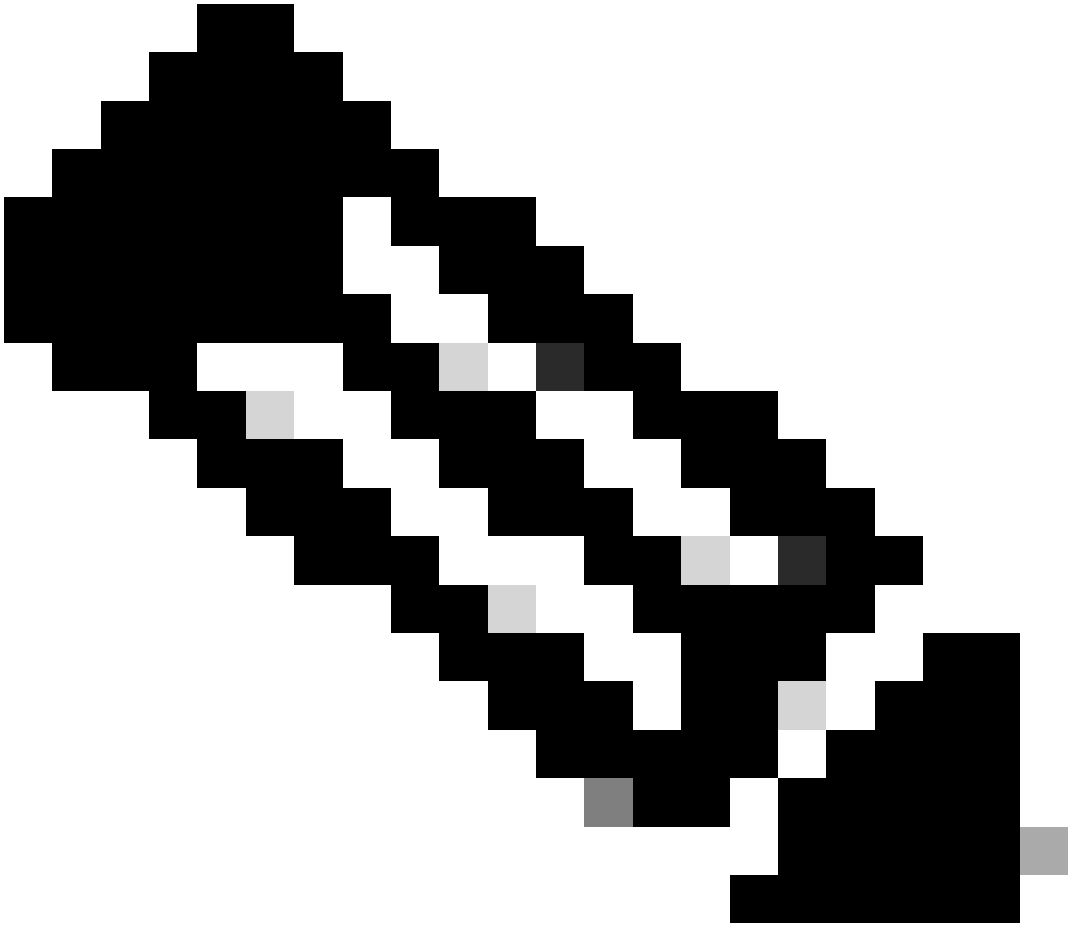
Credenziali JSON di amministrazione

8. Fare clic su Intestazioni per aggiungere i metodi successivi:
    - Content-Type: applicazione/json
    - Accetta: application/json



Intestazioni JSON

9. Infine, fare clic su Invia.



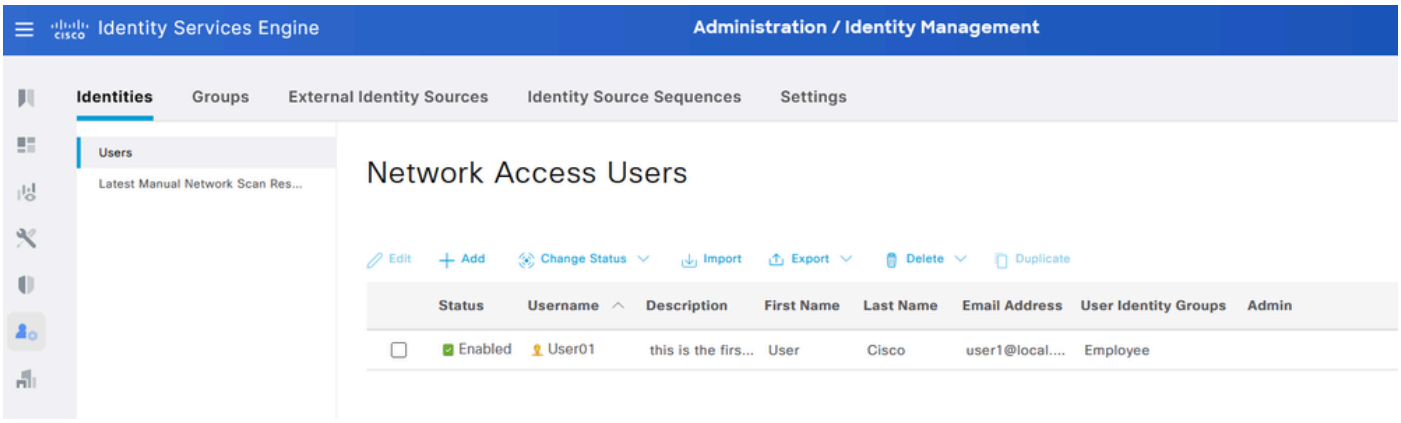
Nota: per assegnare un gruppo di identità al nuovo account utente, è necessario utilizzare l'ID del gruppo di identità. Per ulteriori informazioni, vedere la **sezione Risoluzione dei problemi**.

Convalida

1. Dopo l'invio della richiesta POST, verrà visualizzato lo stato "201 Creato". Significa che il processo è stato completato con successo.

Richiesta JSON riuscita

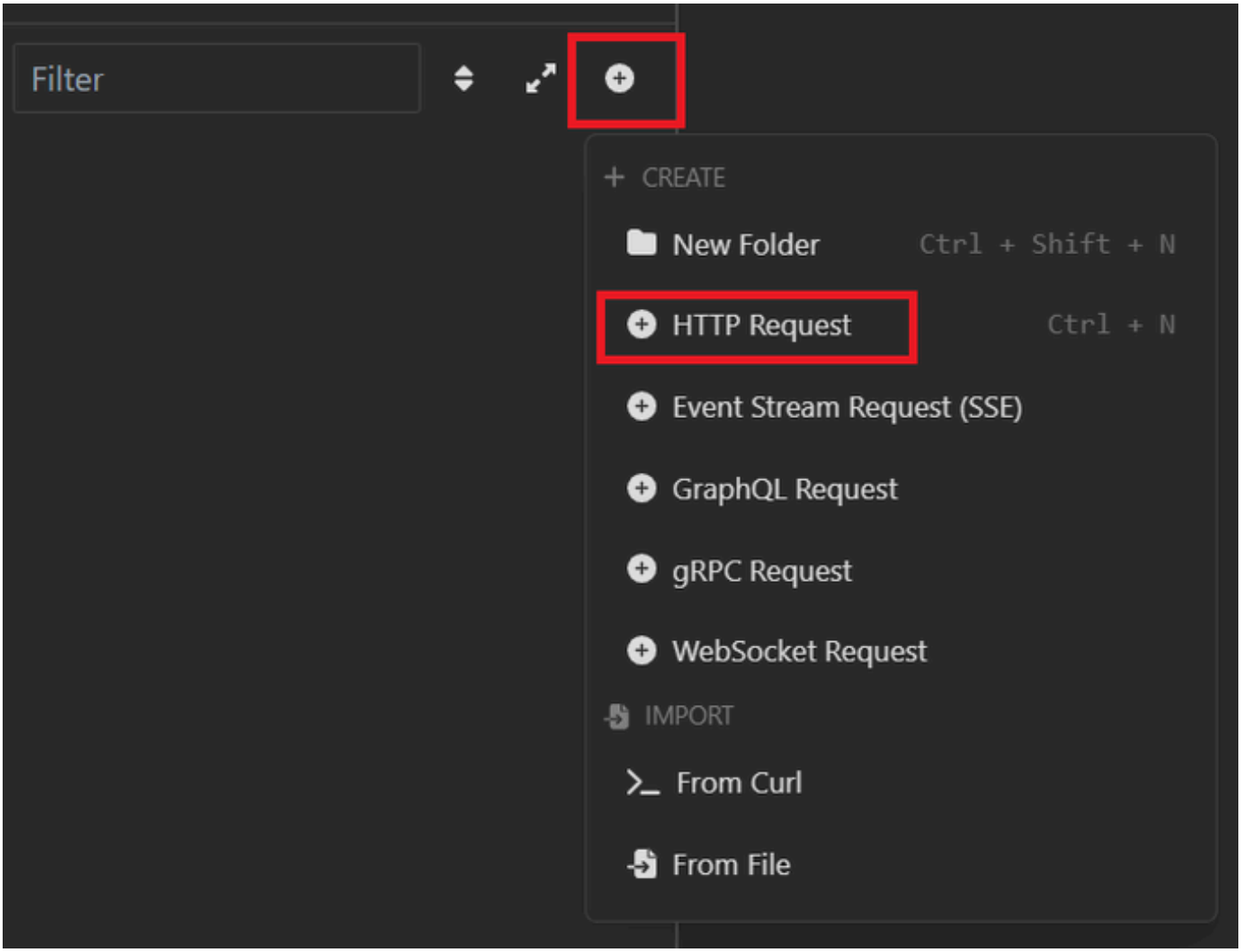
2. Aprire la GUI di ISE e selezionare Amministrazione > Gestione delle identità > Identità > Utenti > Utenti accesso alla rete



Account utente JSON

richiesta XML

1. Aprire Insonnia.
2. Aggiungere una nuova richiesta HTTPS sul lato sinistro.

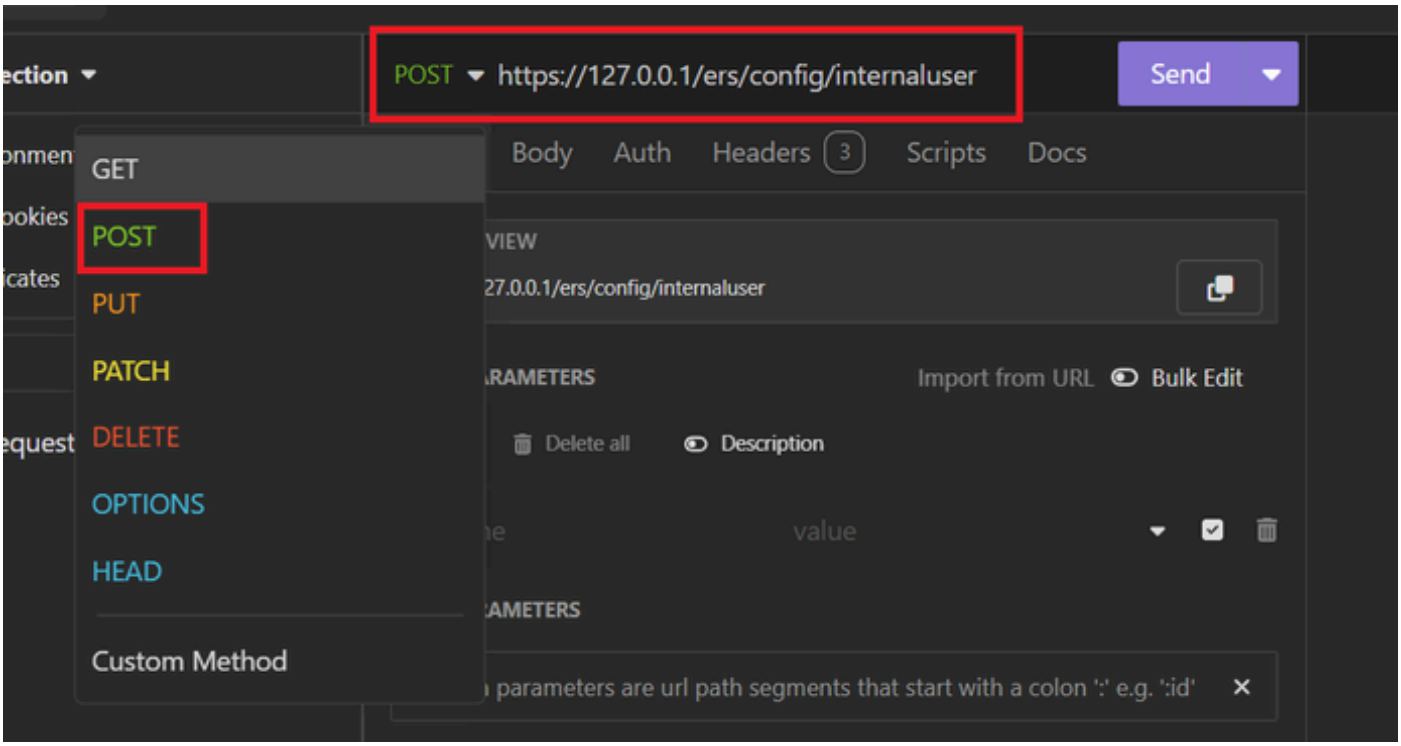


Richiesta XML

3. Per inviare le informazioni al nodo ISE, è necessario scegliere POST.

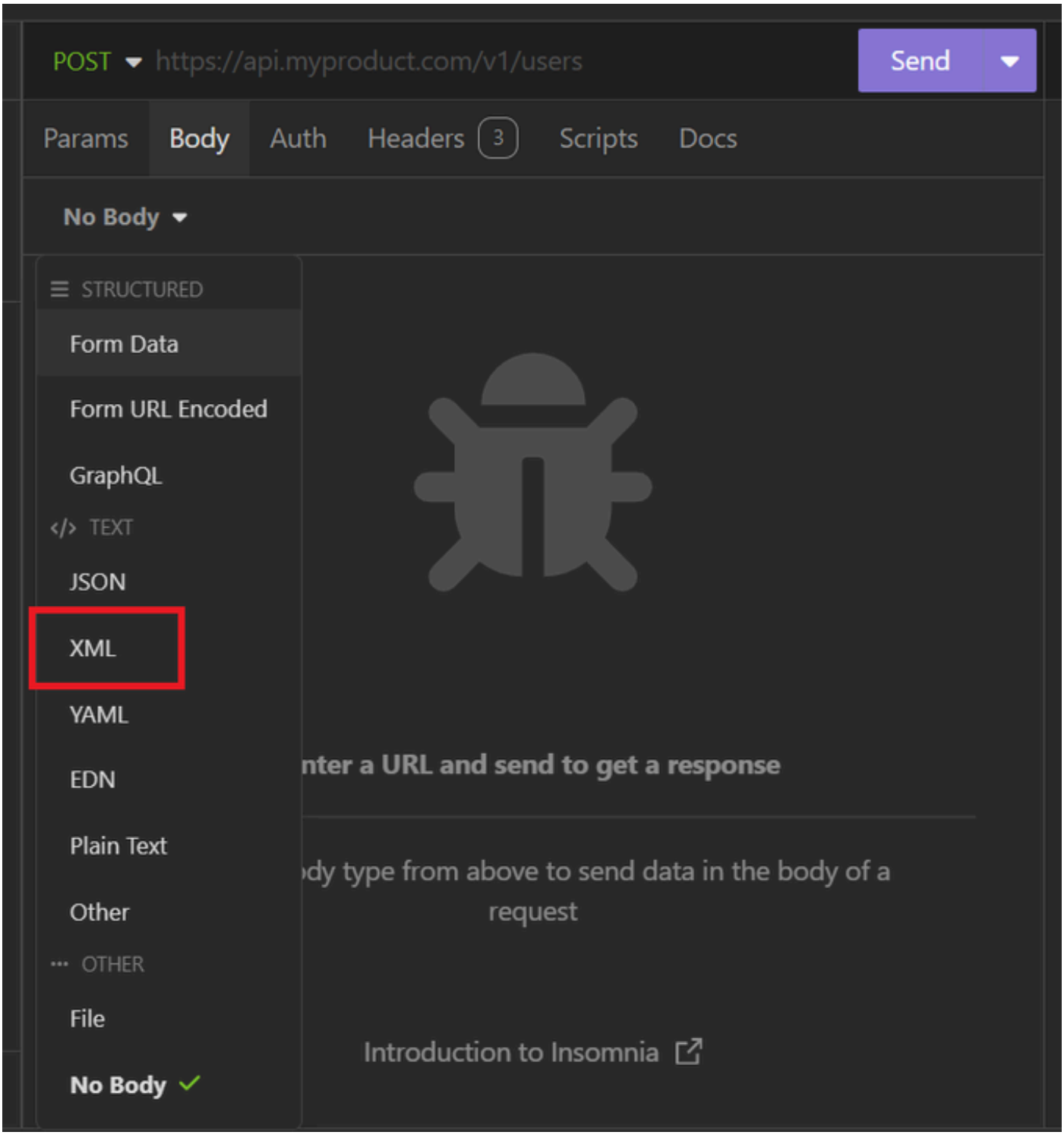
L'URL da immettere dipende dall'indirizzo IP del nodo ISE.

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



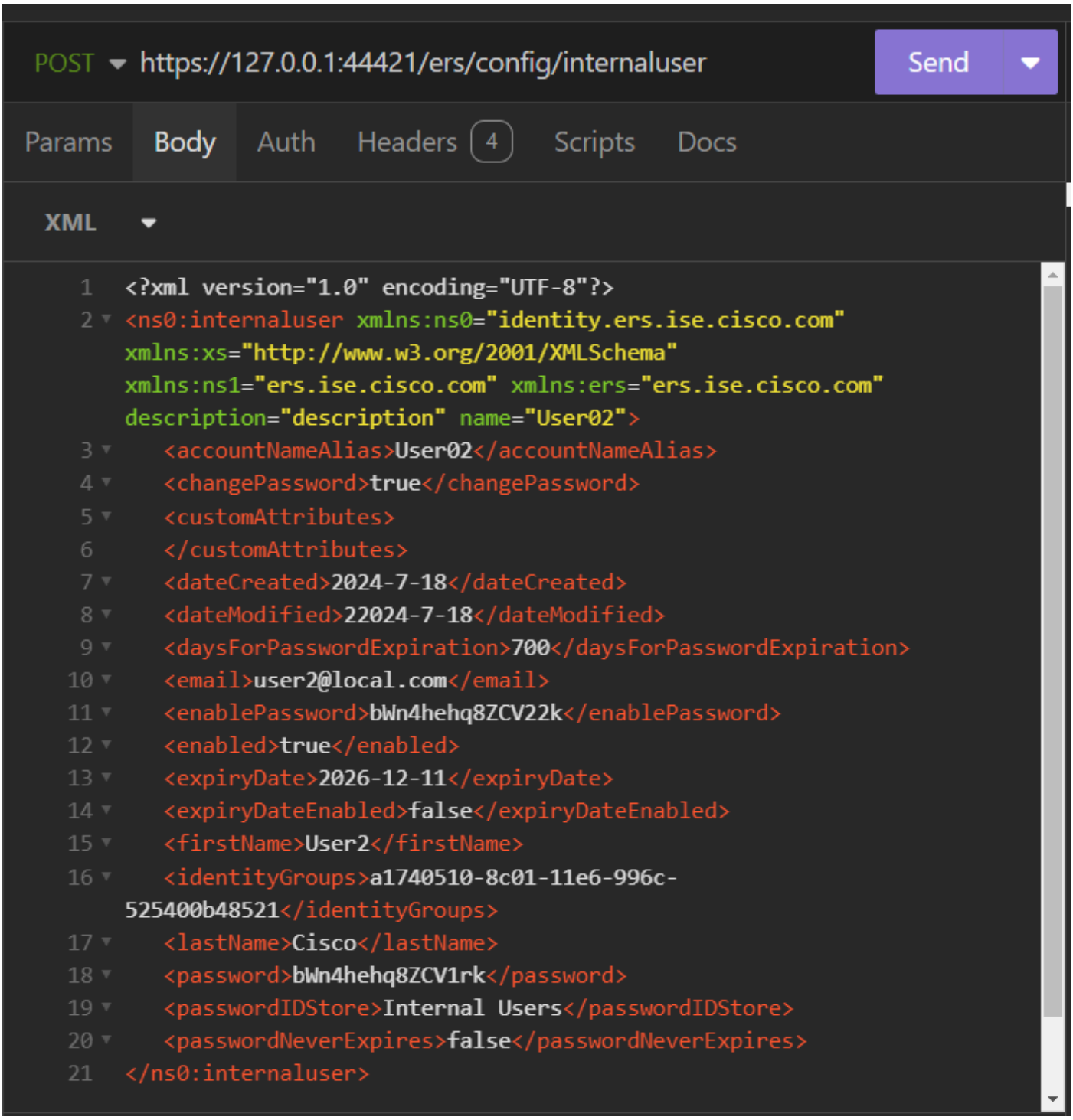
POST XML

4. Quindi fate clic su Corpo (Body) e scegliete XML.



Corpo XML

5. È possibile incollare la sintassi e modificare i parametri in base alle esigenze.



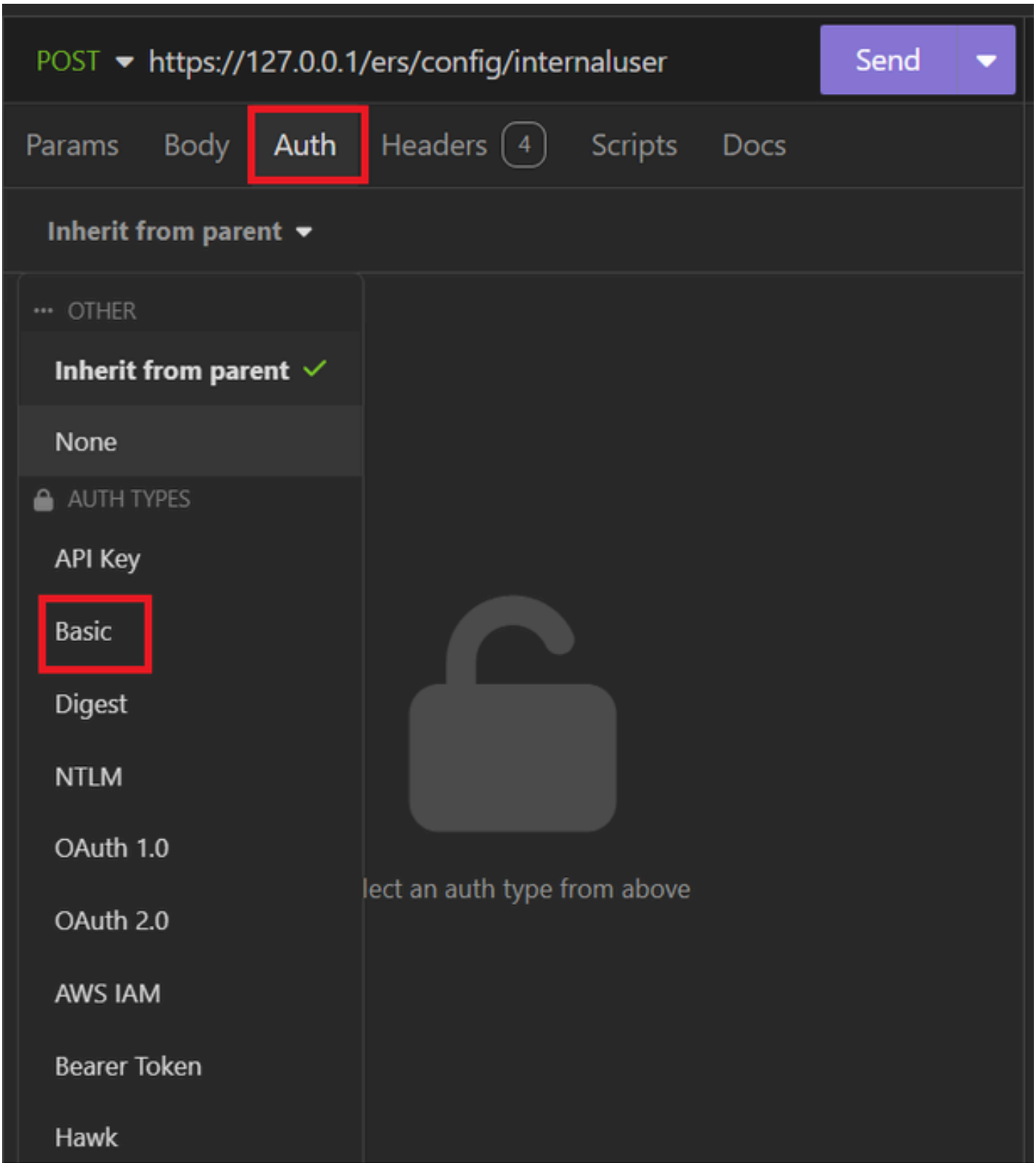
Post XML

Sintassi 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>
```

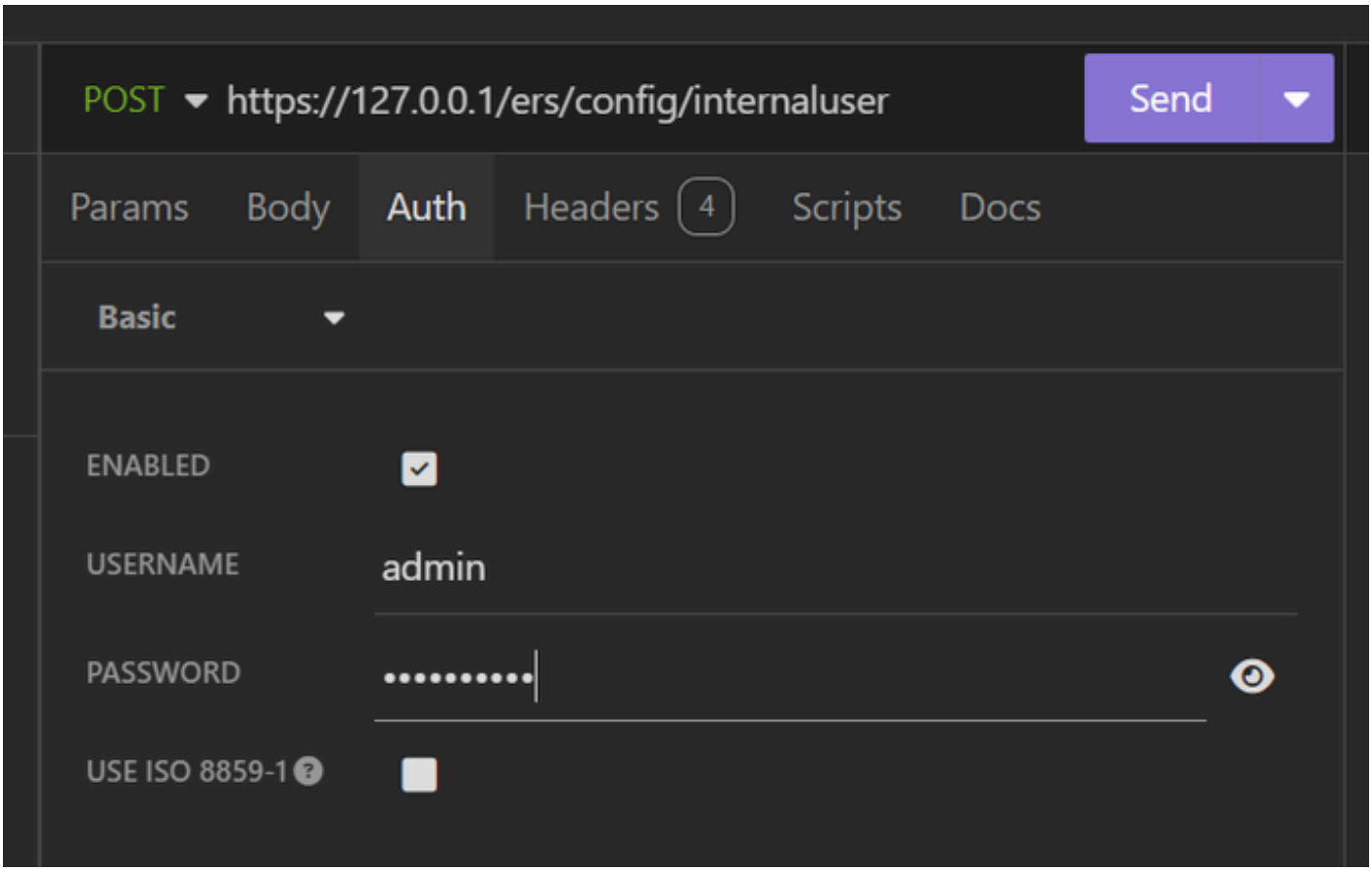
```
      <entry>
         <key>key1</key>
         <value>value1</value>
      </entry>
      <entry>
         <key>key2</key>
         <value>value3</value>
      </entry>
   </customAttributes>
   <dateCreated>2015-12-15</dateCreated>
   <dateModified>2015-12-20</dateModified>
   <daysForPasswordExpiration>60</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. Fare clic su Auth e scegliere Basic



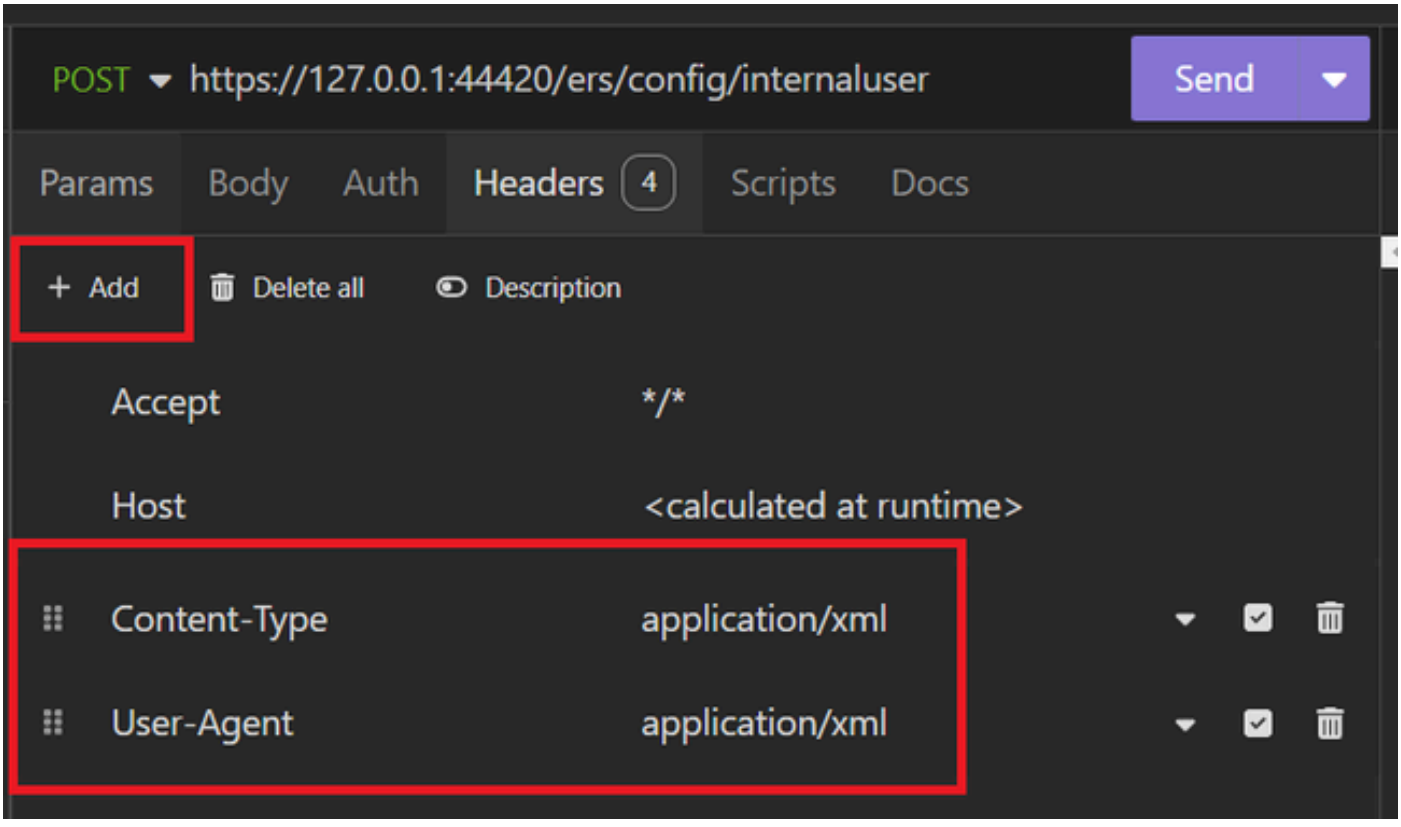
Autenticazione XML

7. Immettere le credenziali dell'interfaccia grafica ISE.



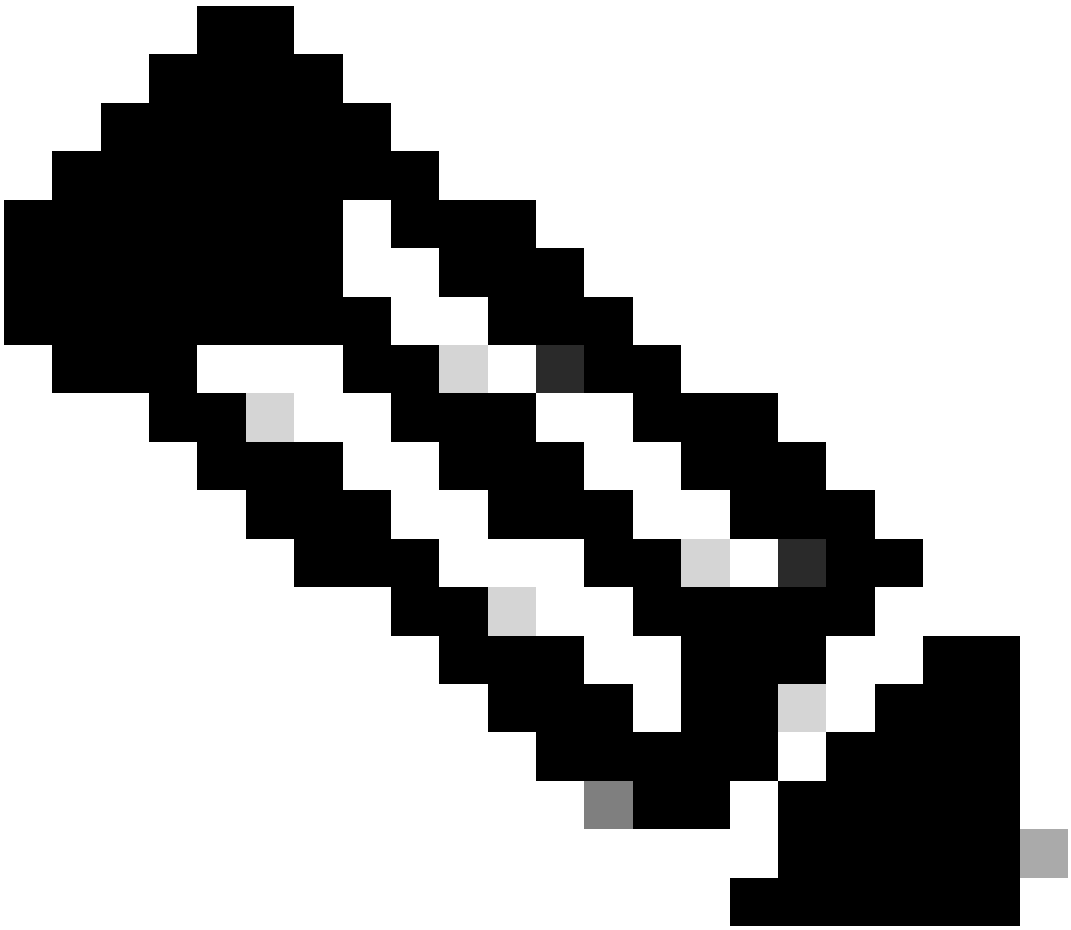
Credenziali XML

8. Fare clic su Intestazioni per aggiungere i metodi successivi:
    - Content-Type: applicazione/xml
    - Accetta: applicazione/xml



Intestazioni XML

9. Infine, fare clic su Invia.



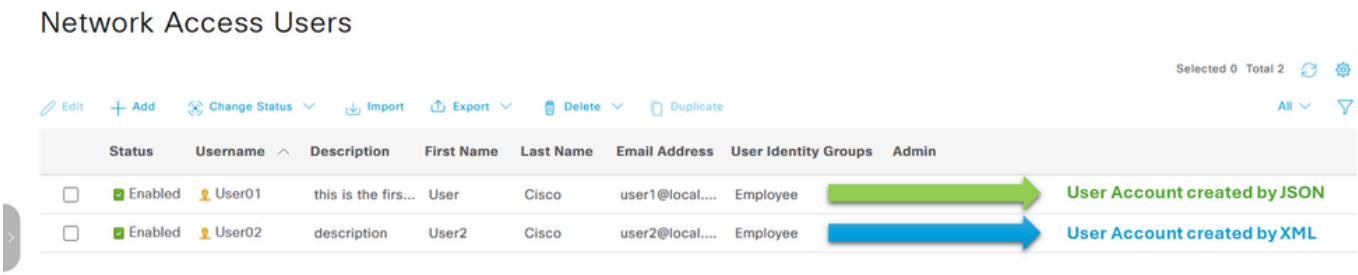
Nota: per assegnare un gruppo di identità al nuovo account utente, è necessario utilizzare l'ID del gruppo di identità. Per ulteriori informazioni, vedere la **sezione Risoluzione dei problemi**.

Convalida

1. Dopo l'invio della richiesta POST, verrà visualizzato lo stato "201 Creato". Significa che il processo è stato completato con successo.

Richiesta XML riuscita

2. Aprire la GUI di ISE e selezionare Amministrazione > Gestione delle identità > Identità > Utenti > Utenti accesso alla rete

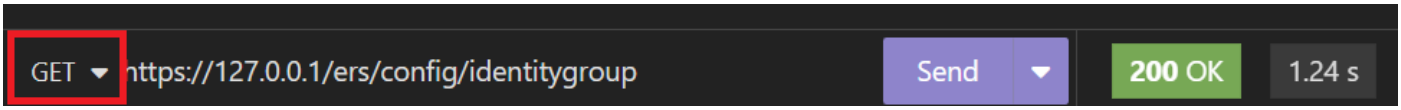


Convalida degli account utente

Risoluzione dei problemi

1. Identificare l'ID del gruppo di identità.

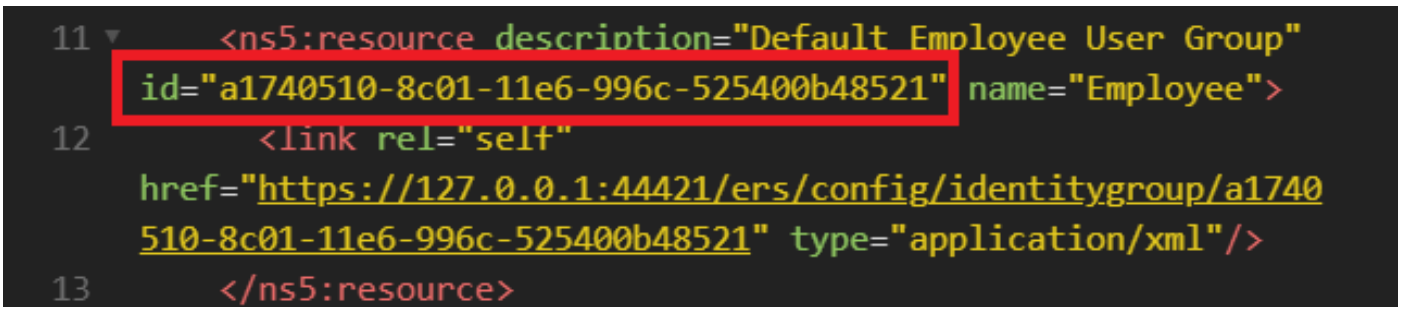
Utilizzare GET e la query https://X.X.X.X/ers/config/identitygroup.



opzione GET

Output JSON.

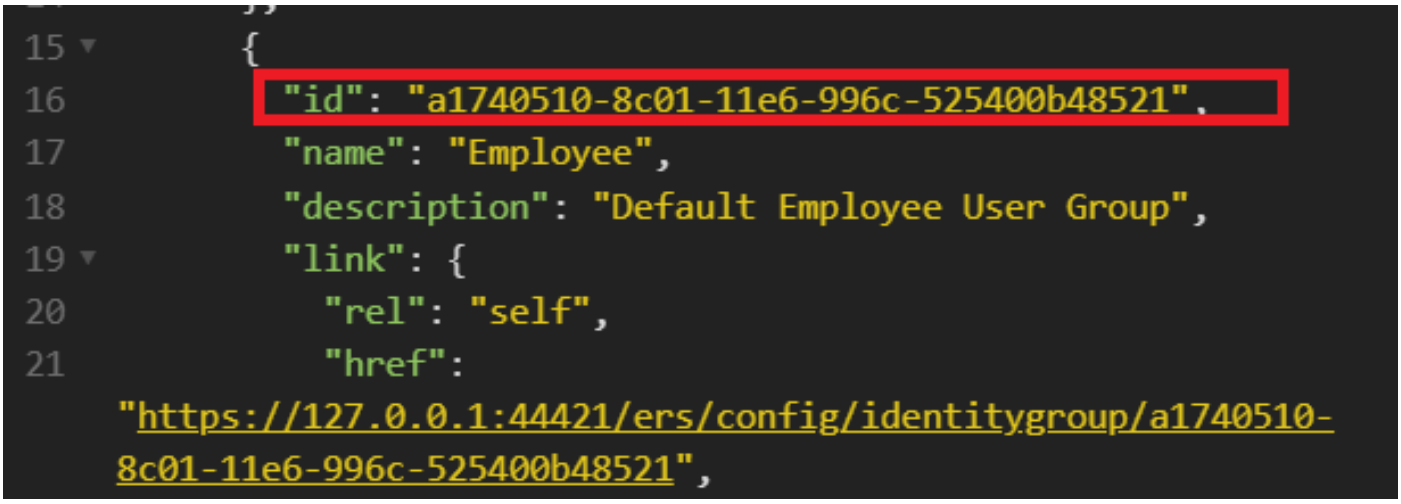
Identificare l'ID accanto alla descrizione.



ID gruppo di identità 01

Output XML.

Identificare l'ID accanto alla descrizione.



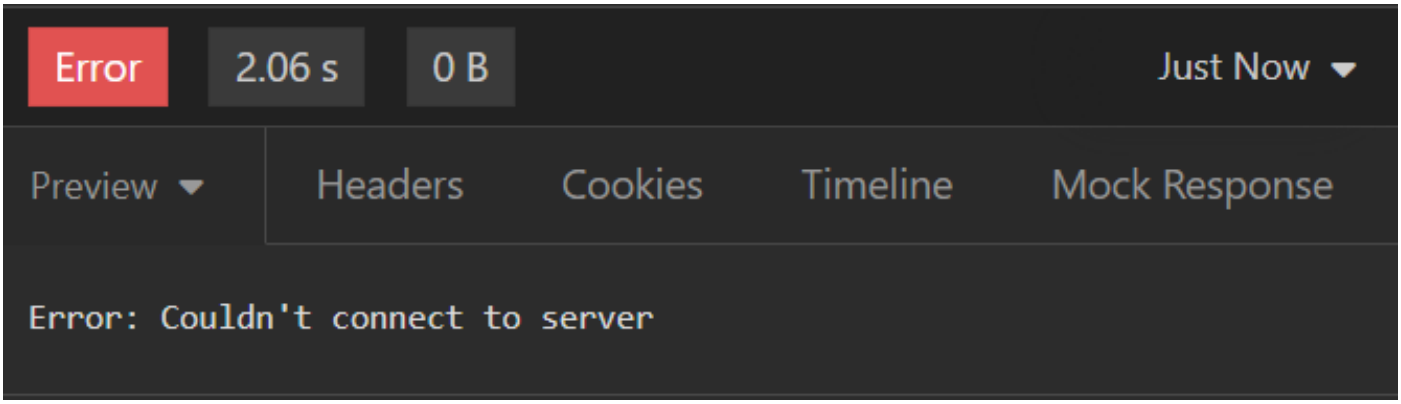
ID gruppo di identità 02

2. 401 Errore non autorizzato.

Errore 401

Soluzione: verificare le credenziali di accesso configurate nella sezione Autenticazione

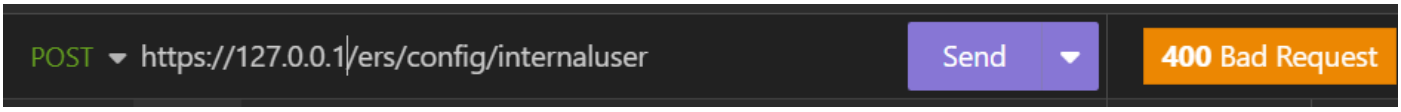
3. Errore: impossibile connettersi al server



Errore di connessione

Soluzione: controllare l'indirizzo IP del nodo ISE configurato in Insonnia o convalidare la connettività.

4. 400 Richiesta non valida.

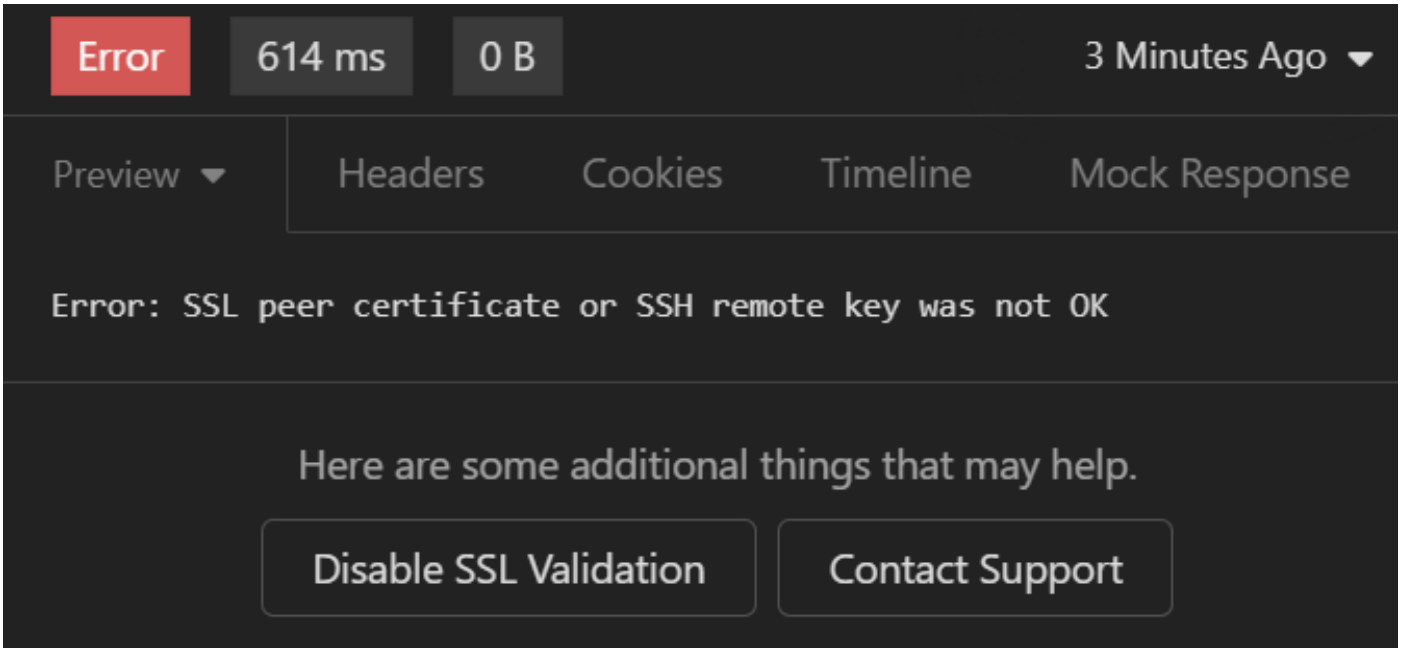


Errore 400

Ci sono diversi motivi per affrontare questo errore, i più comuni sono:

- Mancata corrispondenza con i criteri password di sicurezza
- Alcuni parametri non sono stati configurati correttamente.
- Errore di Sintaxis.
- Informazioni duplicate.

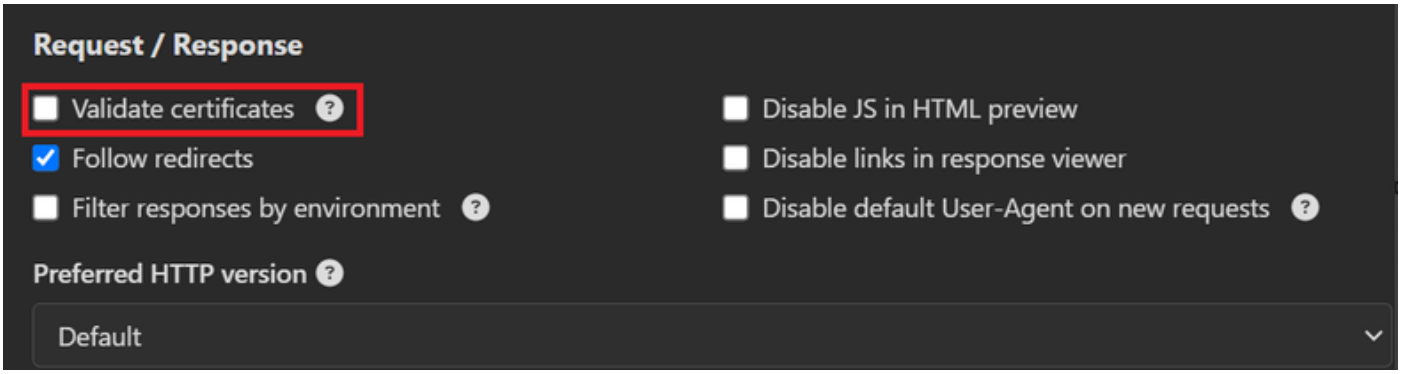
5. Errore: il certificato peer SSL o la chiave remota SSH non sono corretti



Errore certificato SSL

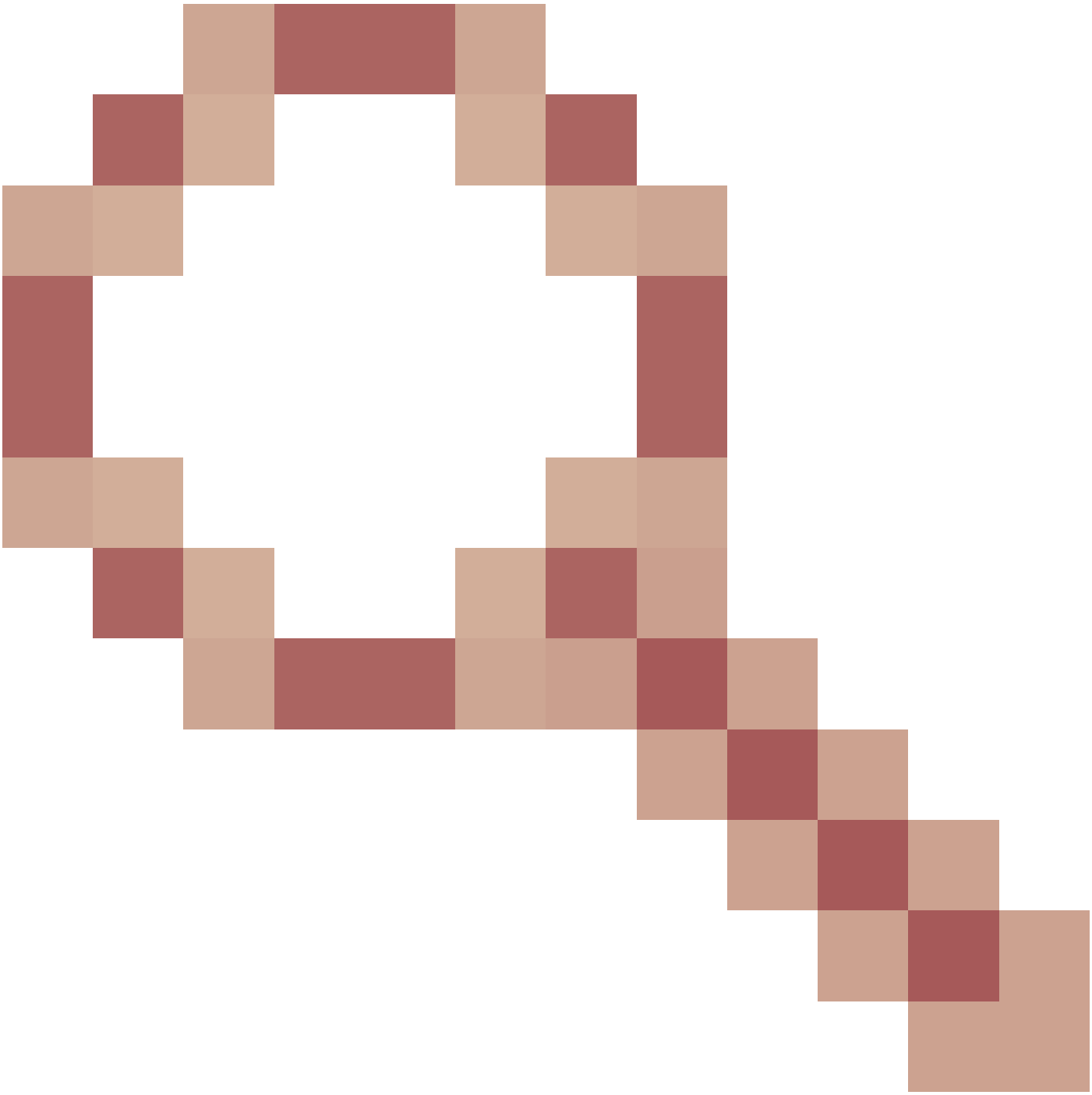
Soluzione:

1. Fare clic su Disabilita convalida SSL.
2. In Richiesta/risposta disabilitare l'opzione Convalida certificati.



Convalida certificati, opzione

6. CSCwh71435



difetto.

La password enable viene configurata in modo casuale anche se non è stata ancora configurata. Questo comportamento si verifica quando la sintassi enable password viene rimossa o lasciata vuota come valore. Per ulteriori informazioni, vedere il collegamento successivo:

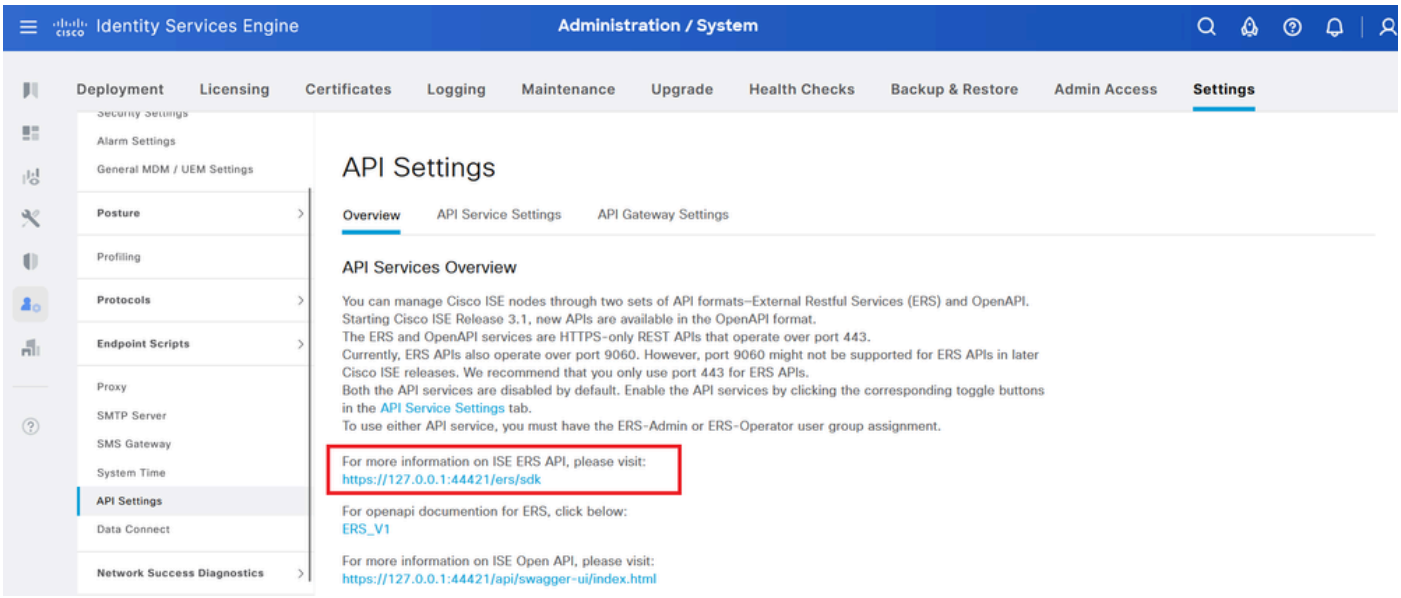
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh71435

Riferimenti alla chiamata API.

Puoi visualizzare tutte le informazioni sulle chiamate API supportate da ISE.

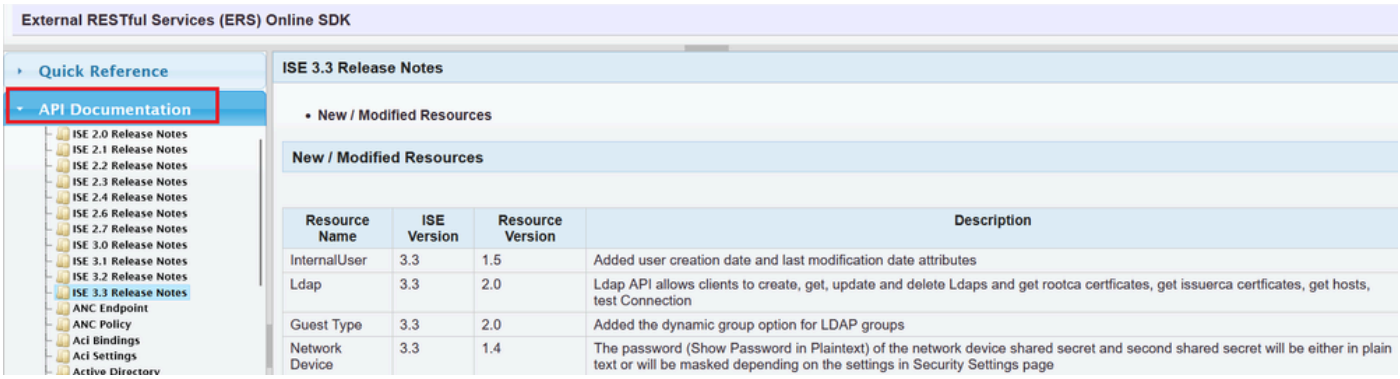
1. Passare a Amministrazione > Sistema > Impostazioni > Impostazione API.

2. Fare clic sul collegamento Informazioni API ERS.



Impostazioni API

3. E fare clic su Documentazione API.



Documentazione API

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).