

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

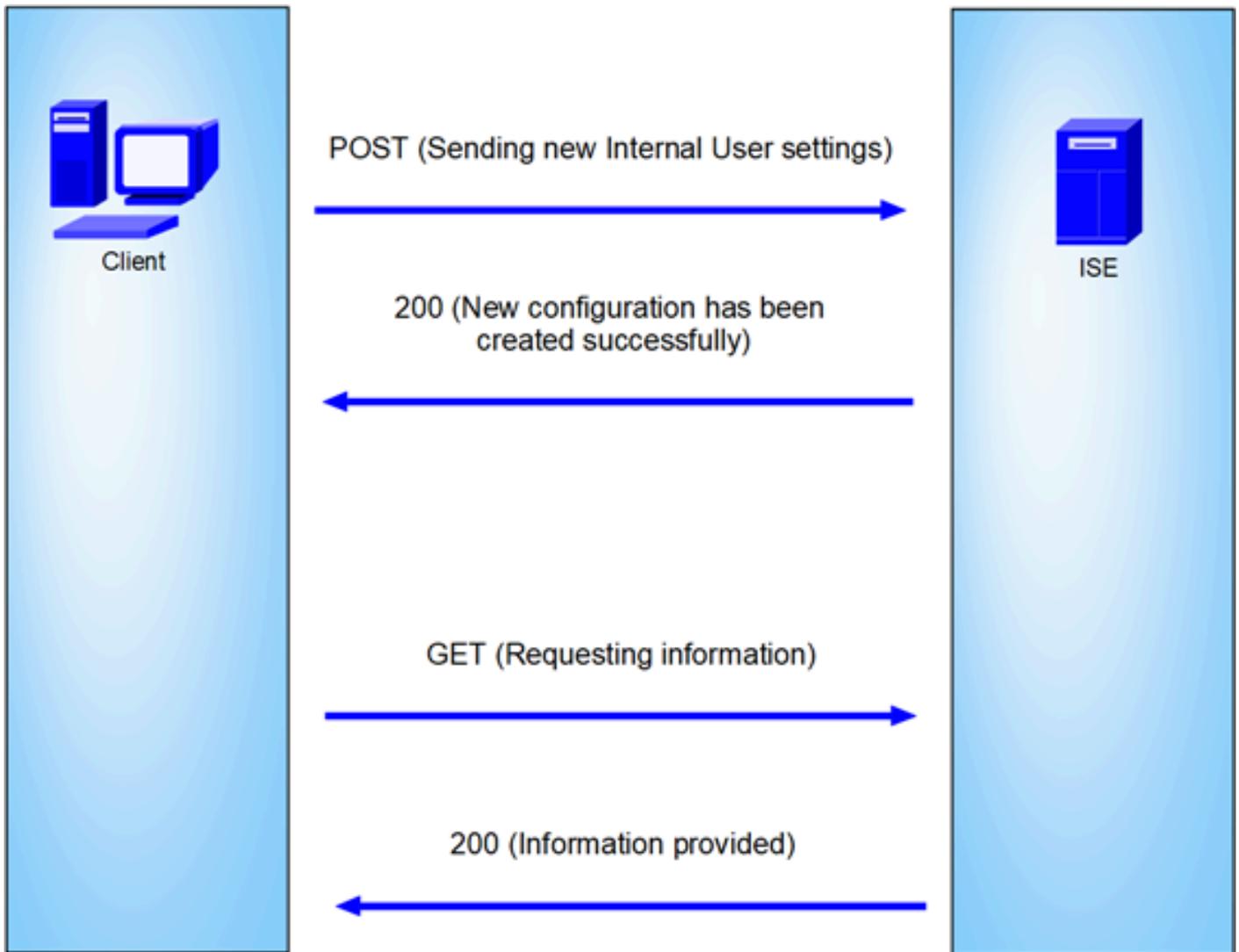
- ISE 3.0 o versione successiva.
- Software Client API.

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).

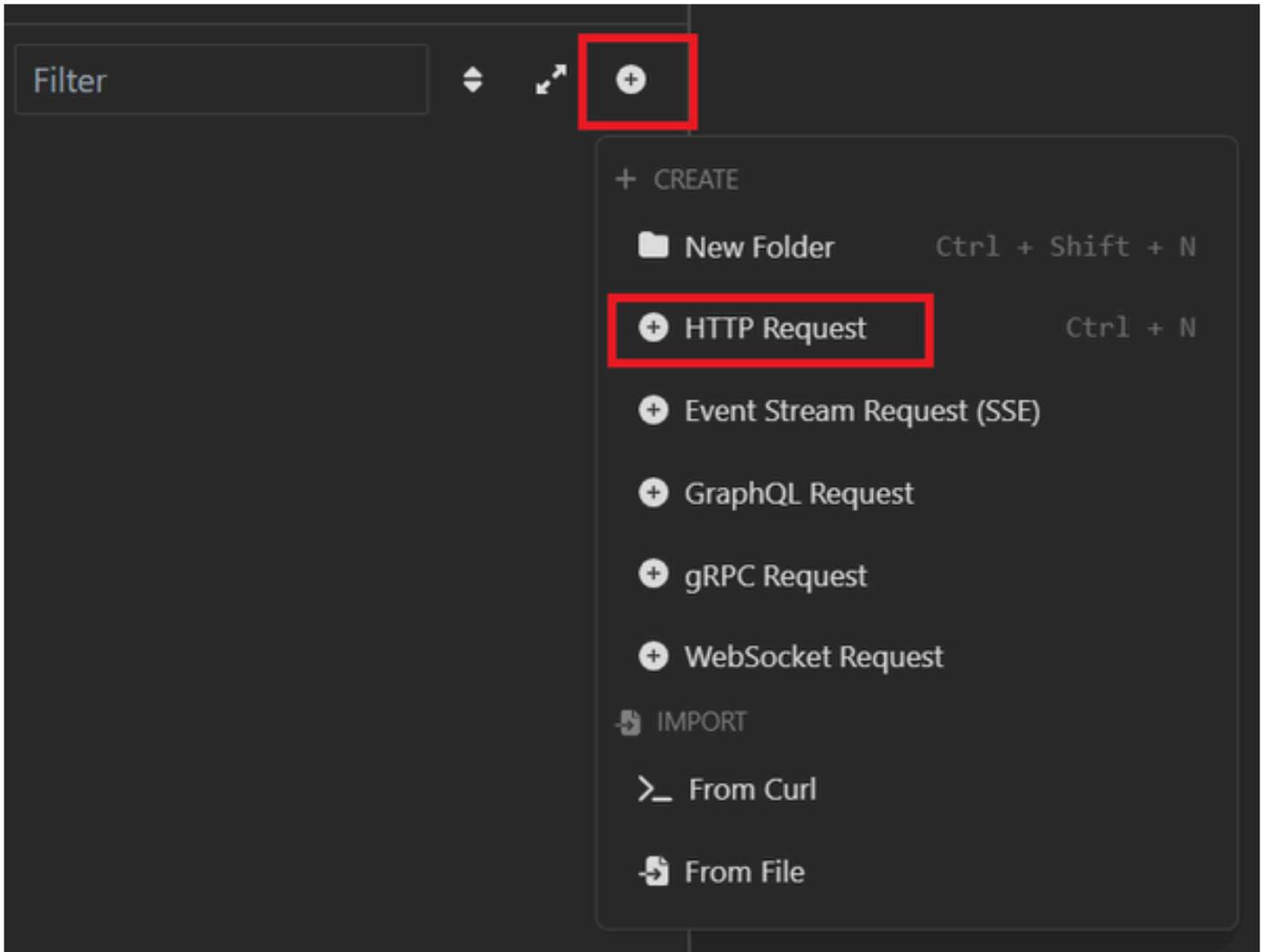
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Administration / System' and various utility icons. The main navigation menu on the left lists categories like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The 'Settings' menu is expanded, showing options such as 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 (selected), and Data Connect. The main content area displays the 'API Settings' page with three tabs: Overview, API Service Settings (active), 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.

Impostazioni API

Richiesta JSON.

1. Aprire Insonnia.

2. Aggiungere una nuova richiesta HTTPS sul lato sinistro.

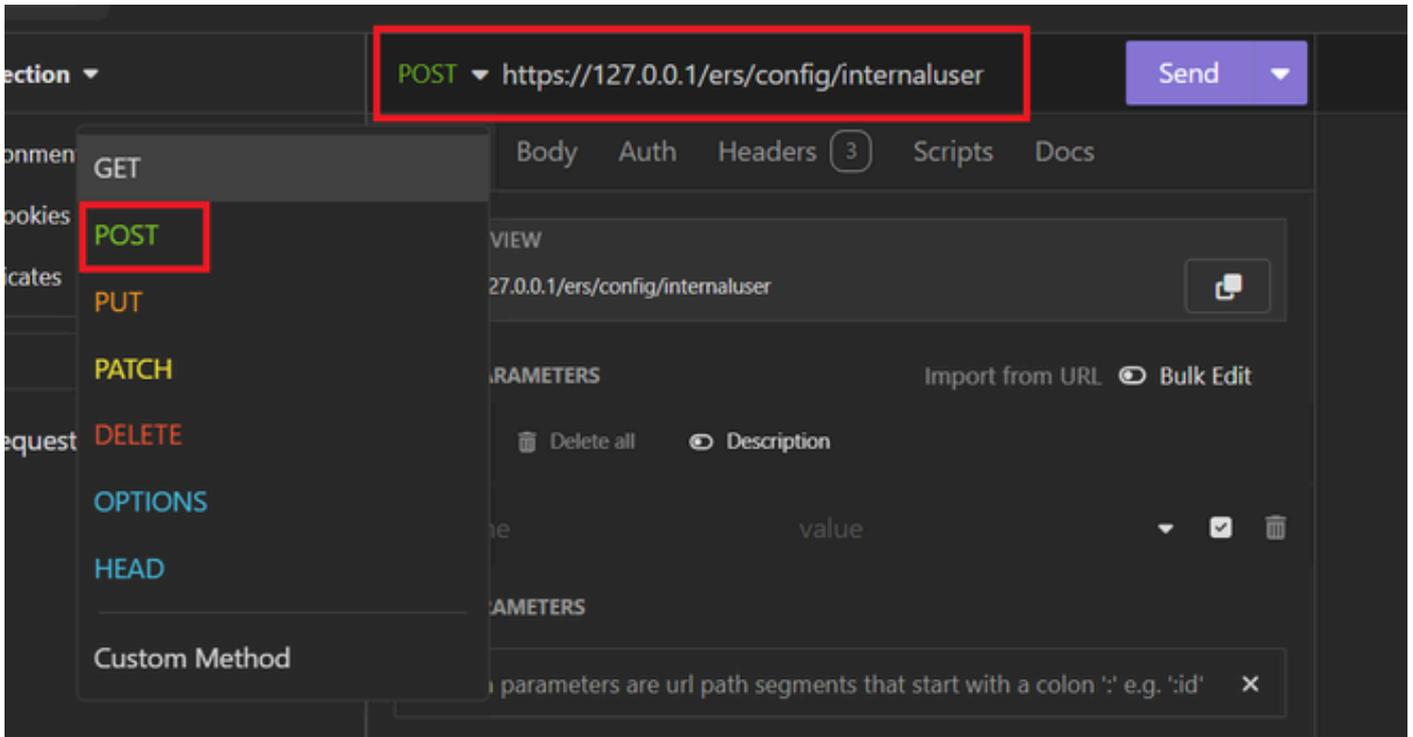


Richiesta JSON

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

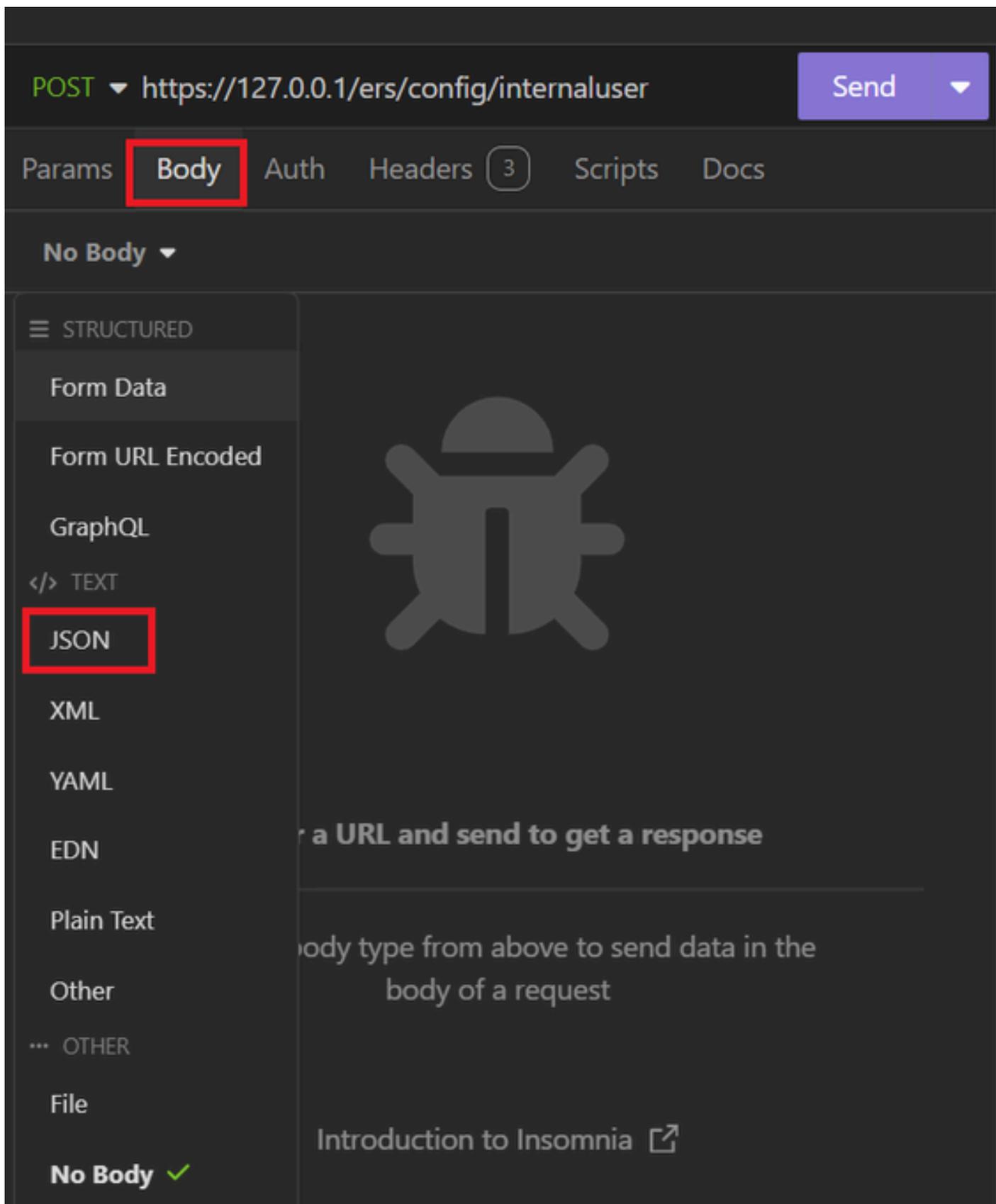
L'URL da immettere dipende dall'indirizzo IP del nodo ISE.

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.

```
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 }
```

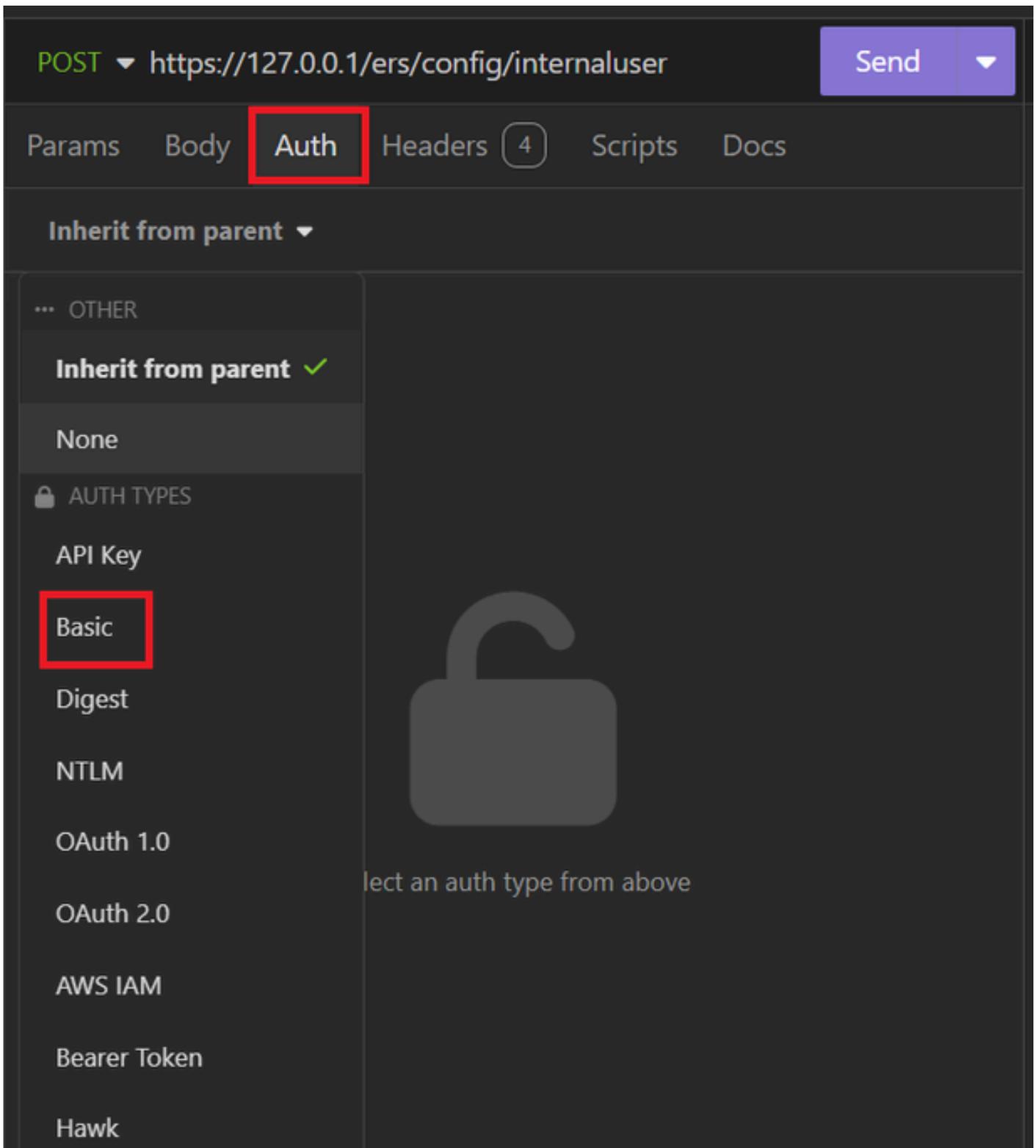
Sintassi JSON

Sintassi JSON

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

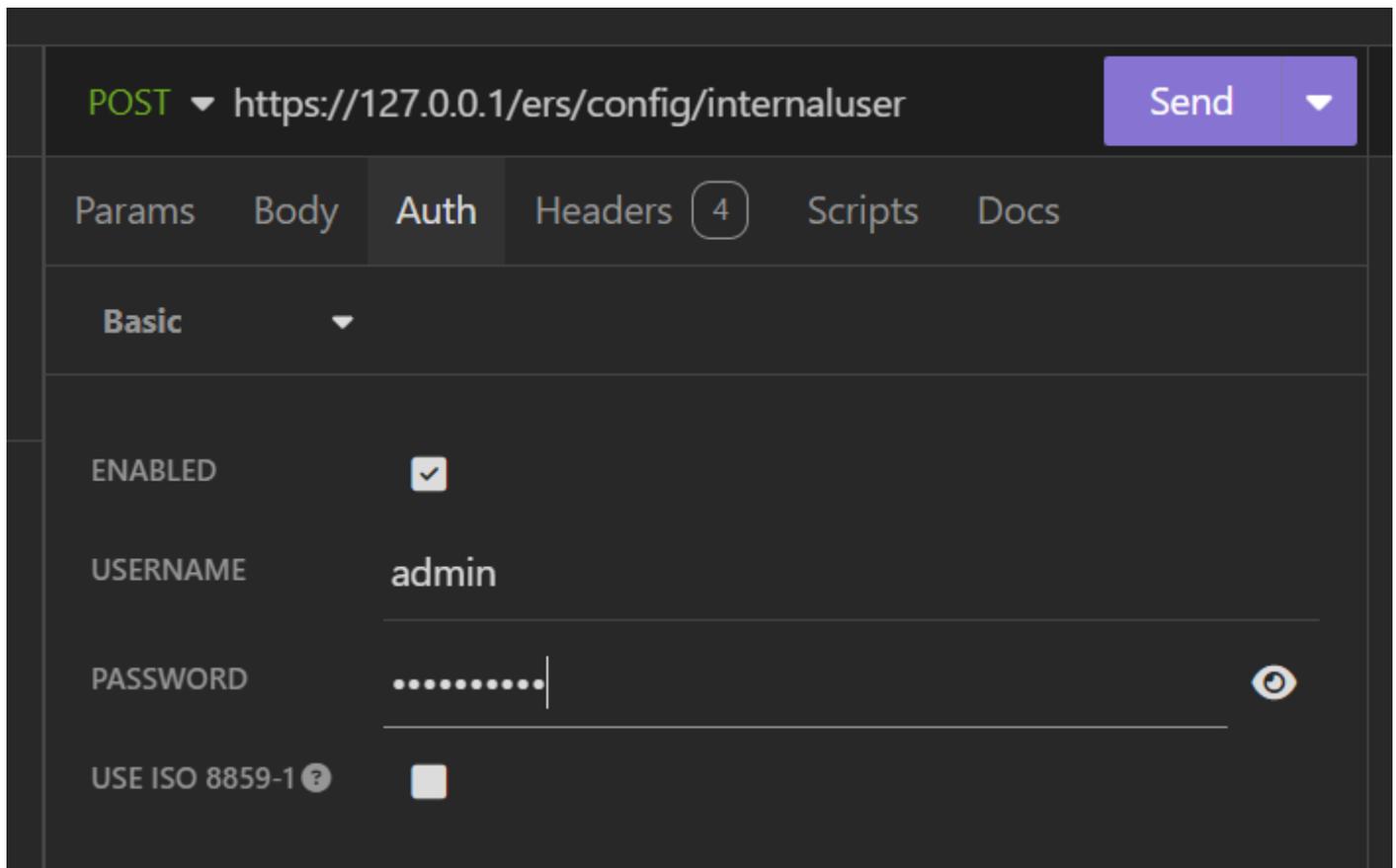
```
"password": "password",
"firstName": "firstName",
"lastName": "lastName",
"changePassword": true,
"identityGroups": "identityGroups",
"passwordNeverExpires": false,
"daysForPasswordExpiration": 60,
"expiryDateEnabled": false,
"expiryDate": "2016-12-11",
"enablePassword": "enablePassword",
"dateModified":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

6. Fare clic su Auth e scegliere Base.



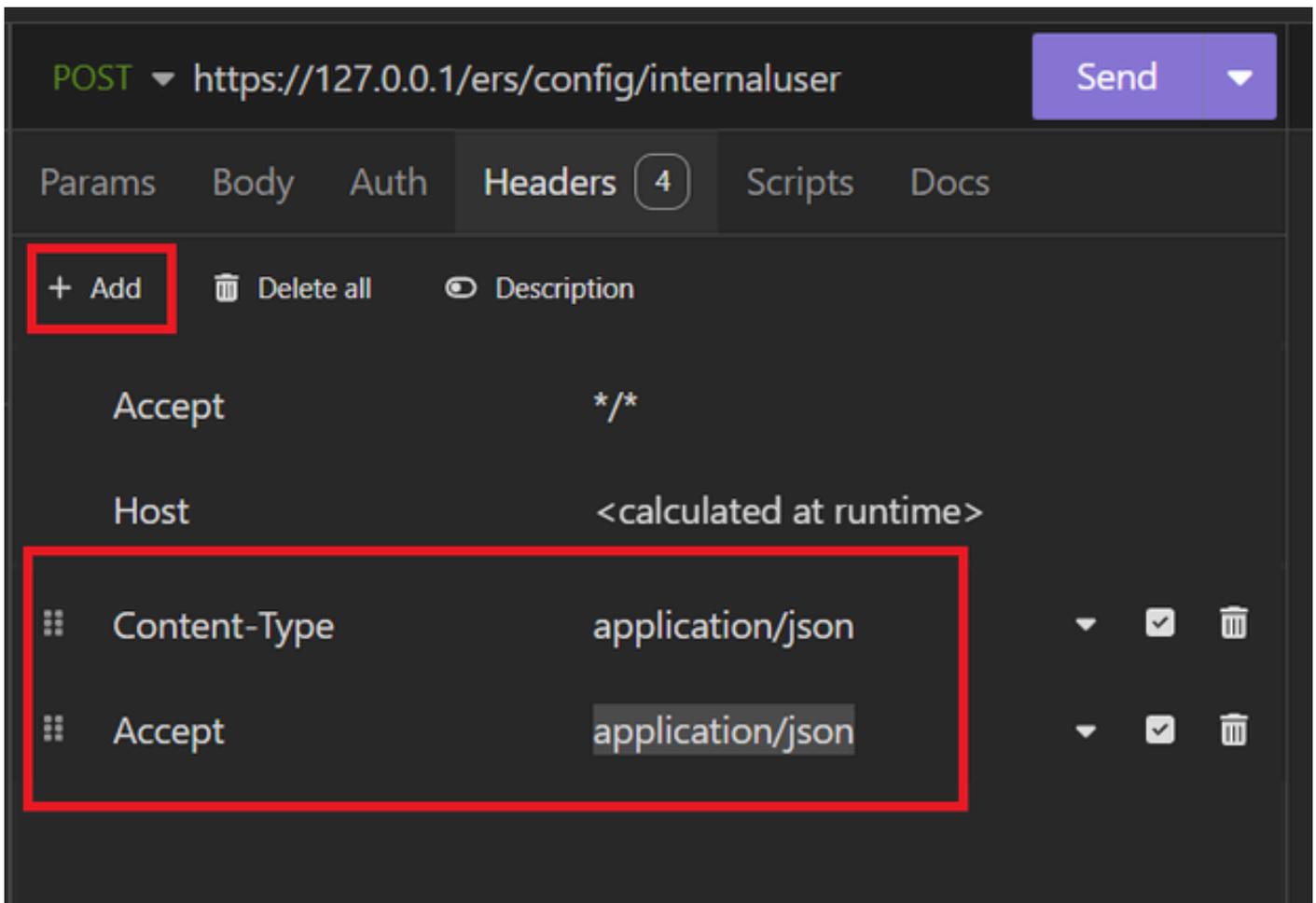
Autenticazione JSON

7. Immettere le credenziali dell'interfaccia grafica ISE.



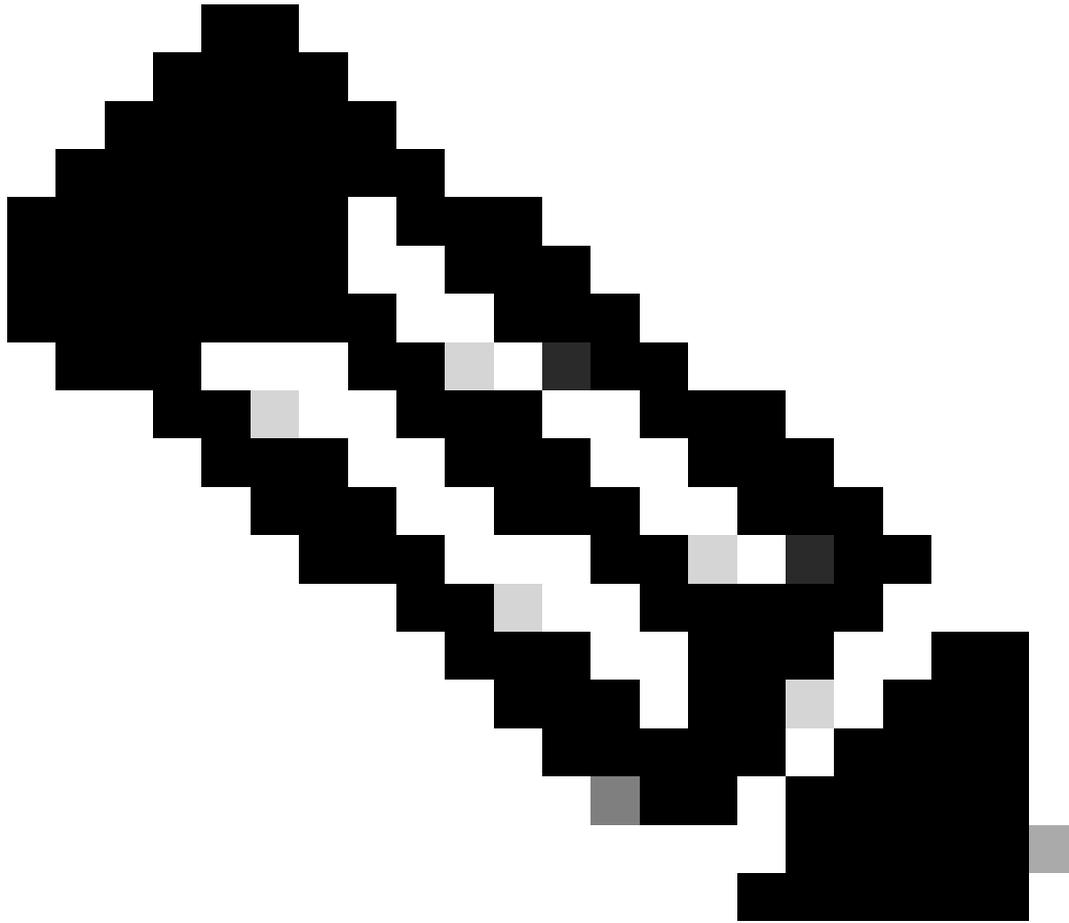
Credenziali JSON di amministrazione

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



Intestazioni JSON

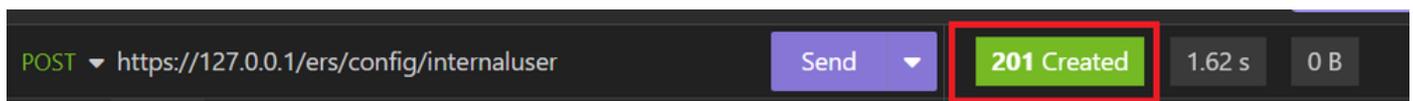
9. Infine, fare clic su Invia.



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**.

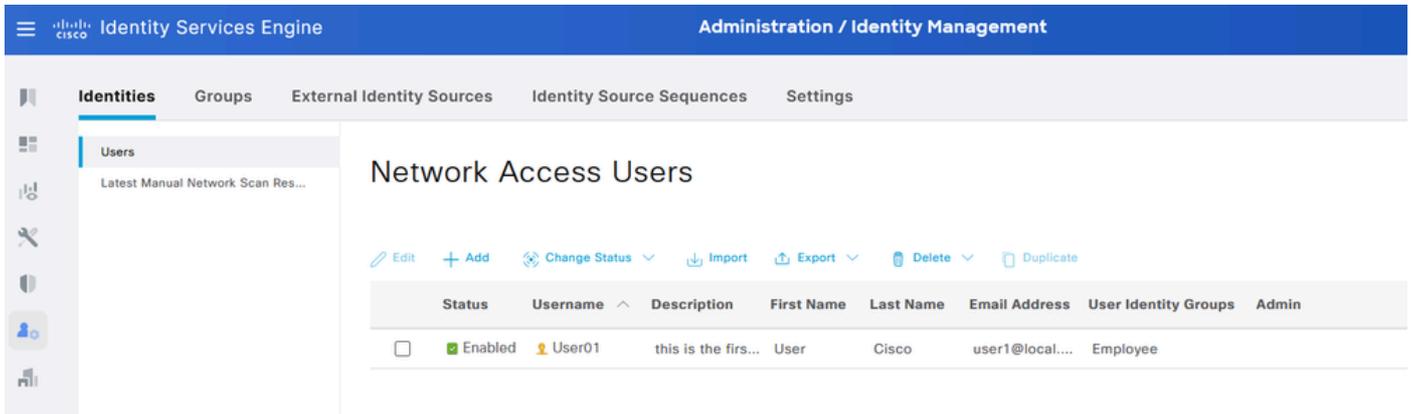
Convalida

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

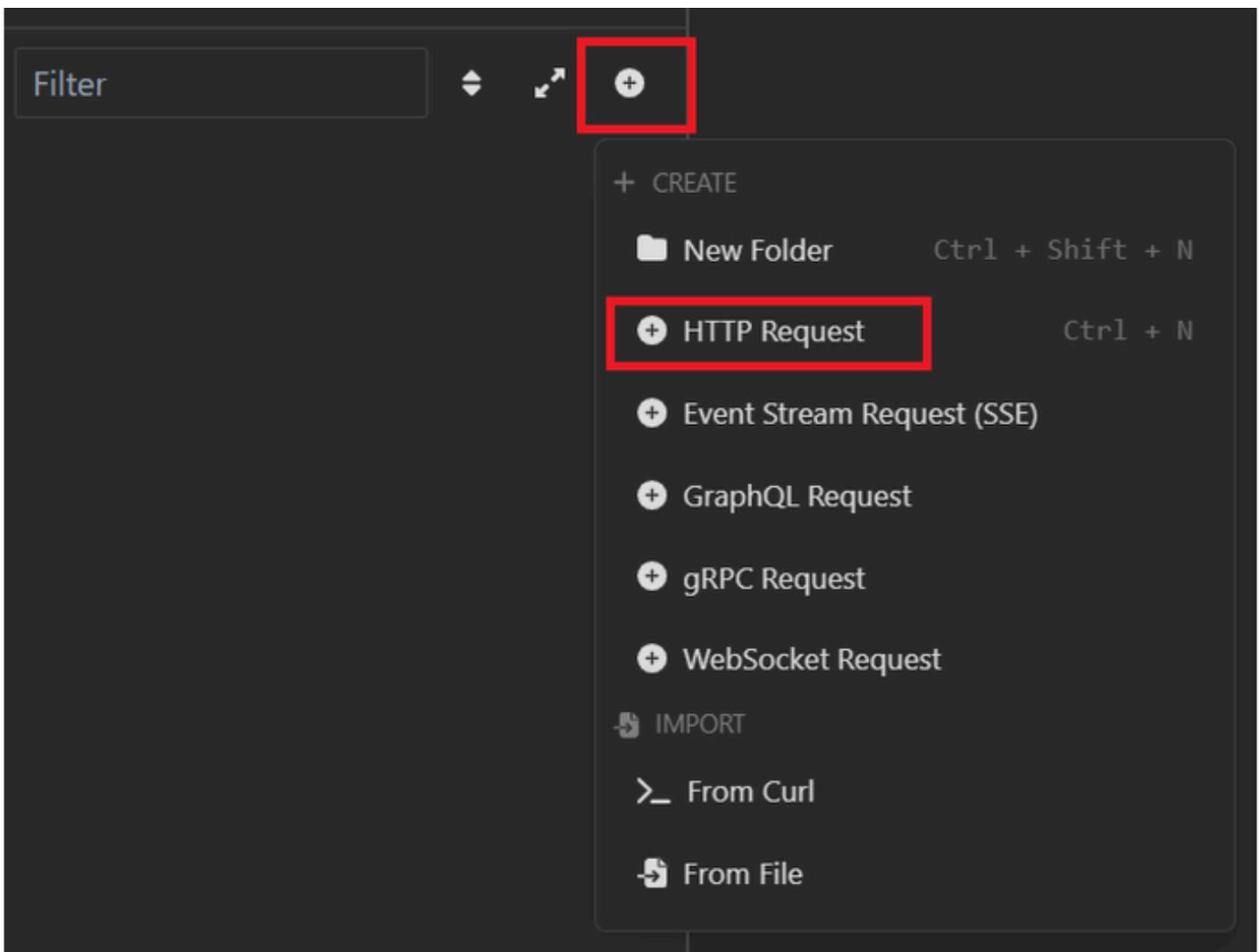
2. Aprire la GUI di ISE e selezionare Amministrazione > Gestione delle identità > Identità > Utenti > Utenti accesso alla rete



Account utente JSON

richiesta XML

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

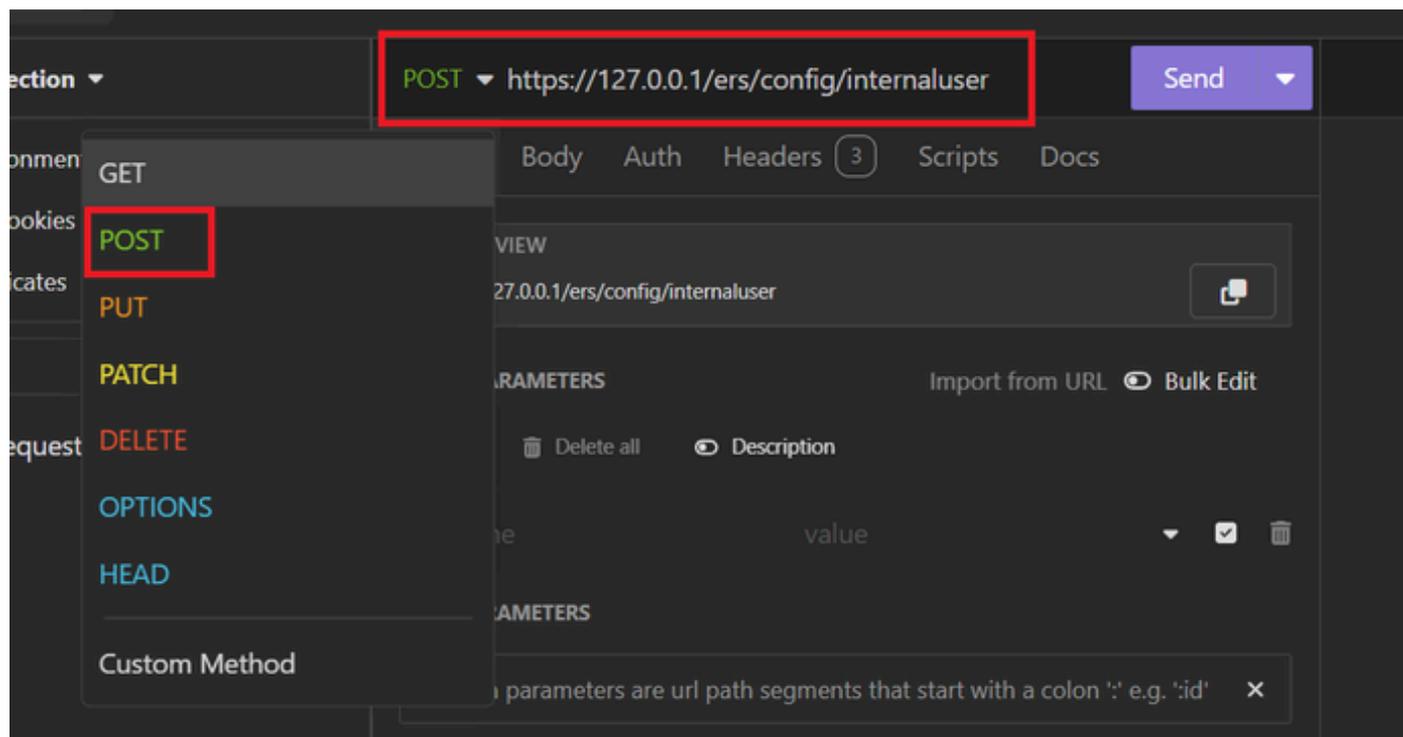


Richiesta XML

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

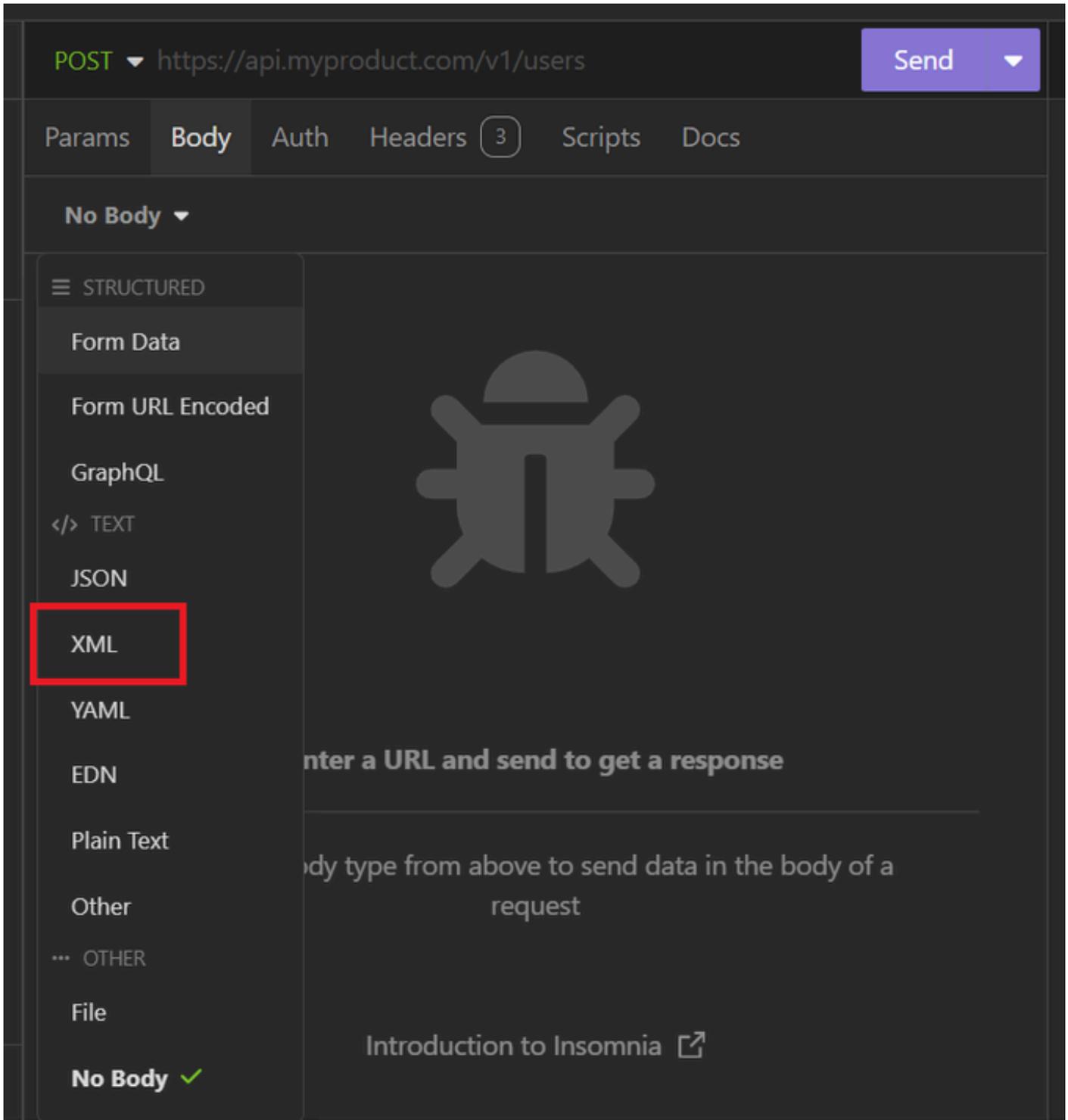
L'URL da immettere dipende dall'indirizzo IP del nodo ISE.

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 ▼ 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>

```

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
```

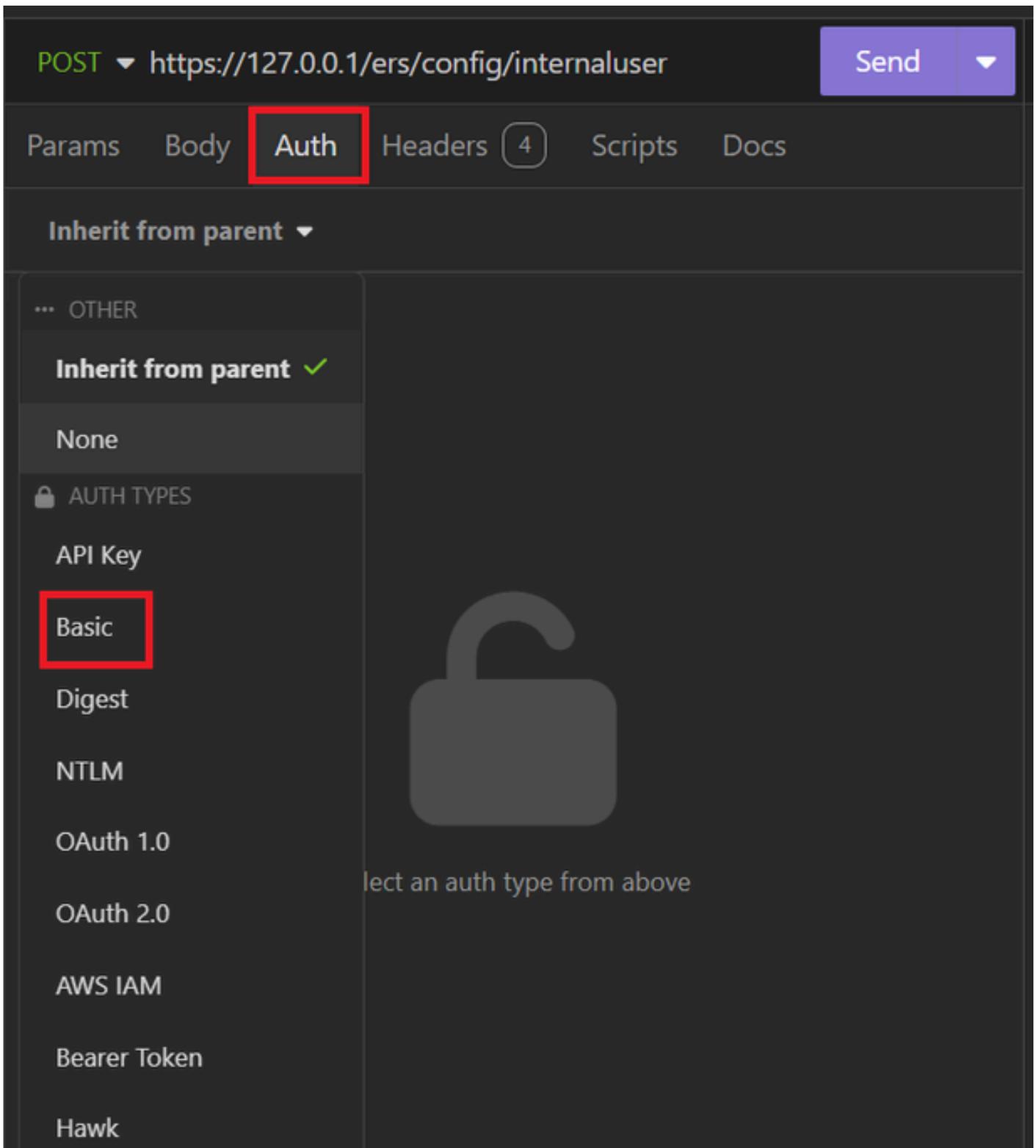
```
  <accountNameAlias>accountNameAlias</accountNameAlias>
```

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

```
  <customAttributes>
```

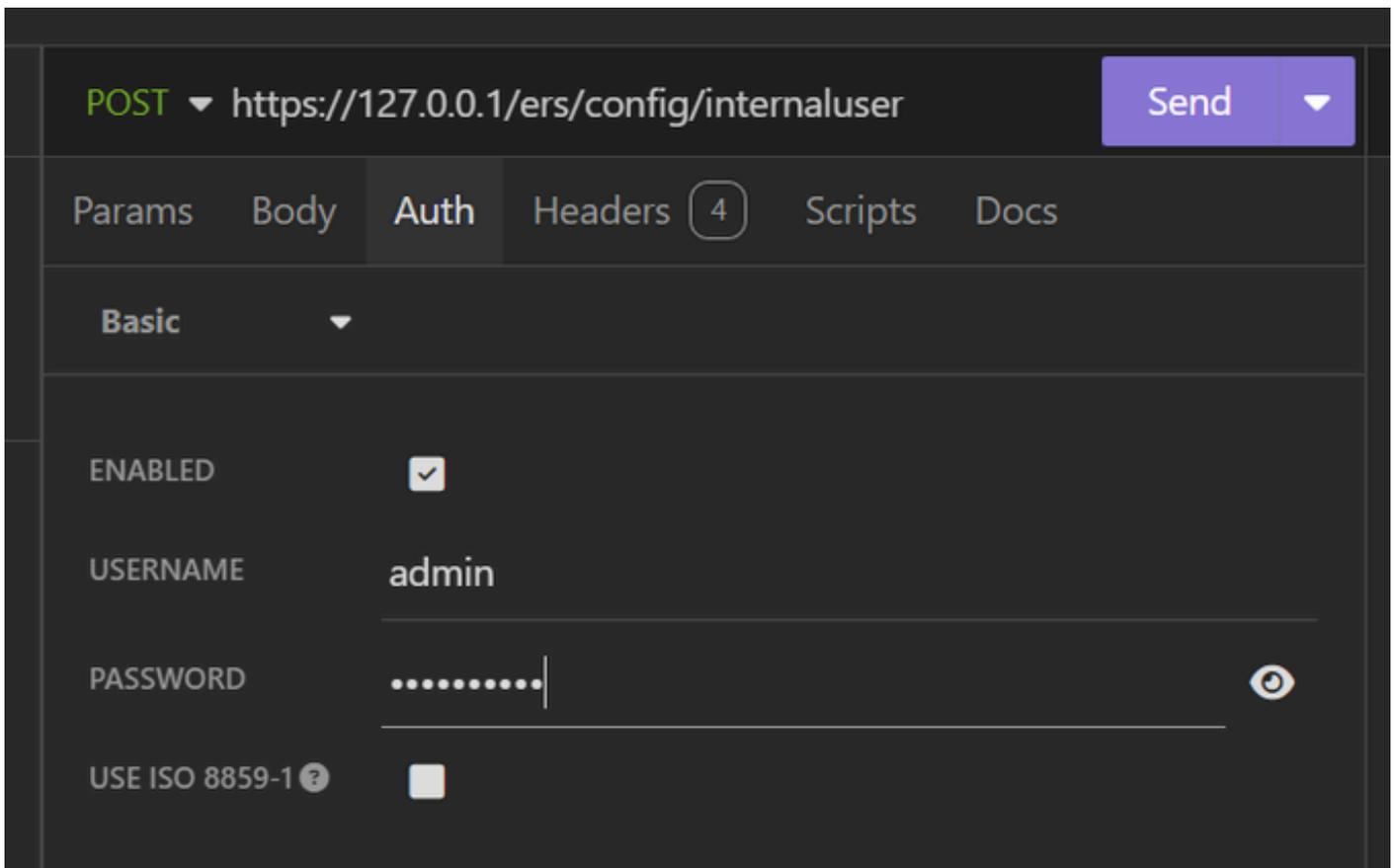
```
<entry>
  <key>key1</key>
  <value>value1</value>
</entry>
<entry>
  <key>key2</key>
  <value>value3</value>
</entry>
</customAttributes>
<dateCreated>2015-12-15</dateCreated>
<dateModified>2015-12-20</dateModified>
<daysForPasswordExpiration>60</daysForPasswordExpiration>
<email>email@domain.com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

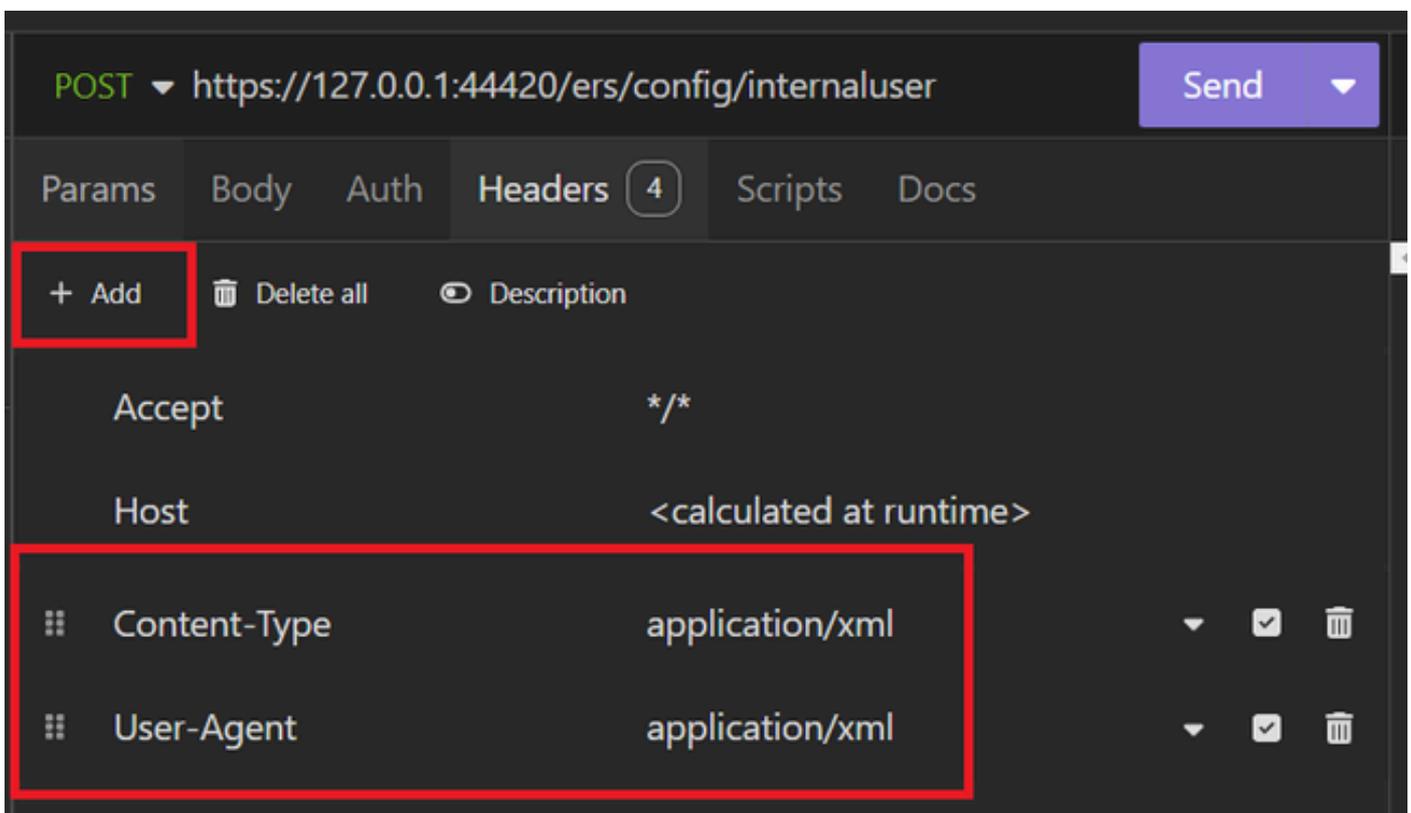
7. Immettere le credenziali dell'interfaccia grafica ISE.



Credenziali XML

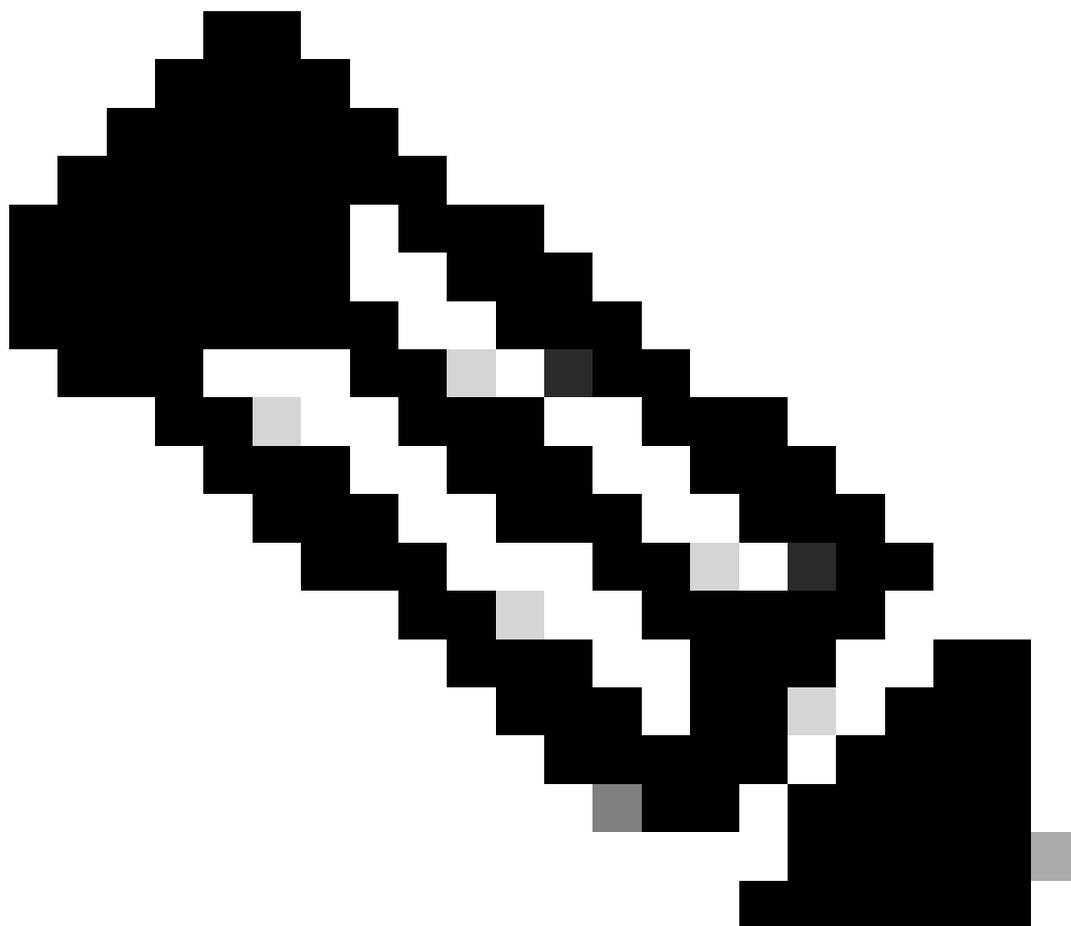
8. Fare clic su Intestazioni per aggiungere i metodi successivi:

- Content-Type: applicazione/xml
- Accetta: applicazione/xml



Intestazioni XML

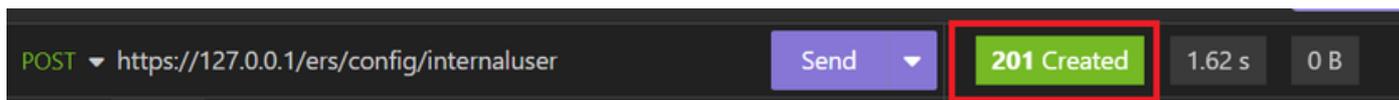
9. Infine, fare clic su Invia.



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

Network Access Users

Selected 0 Total 2  

 Edit  + Add  Change Status  Import  Export  Delete  Duplicate  All 

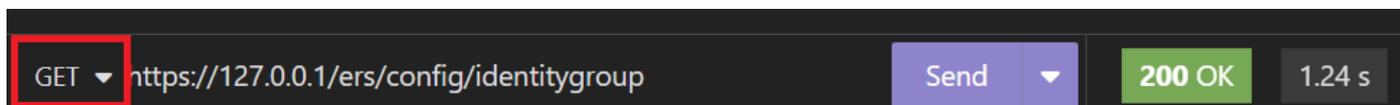
Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	Enabled  User01	this is the firs...	User	Cisco	user1@local...	Employee	 User Account created by JSON
<input type="checkbox"/>	Enabled  User02	description	User2	Cisco	user2@local...	Employee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

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.

```
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 gruppo di identità 01

Output XML.

Identificare l'ID accanto alla descrizione.

```
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 gruppo di identità 02

2. 401 Errore non autorizzato.

```
POST https://127.0.0.1/ers/config/internaluser Send 401 Unauthorized
```

Errore 401

Soluzione: verificare le credenziali di accesso configurate nella sezione Autenticazione

3. Errore: impossibile connettersi al server

```
Error 2.06 s 0 B Just Now
Preview Headers Cookies Timeline Mock Response
Error: Couldn't connect to server
```

Errore di connessione

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

4. 400 Richiesta non valida.

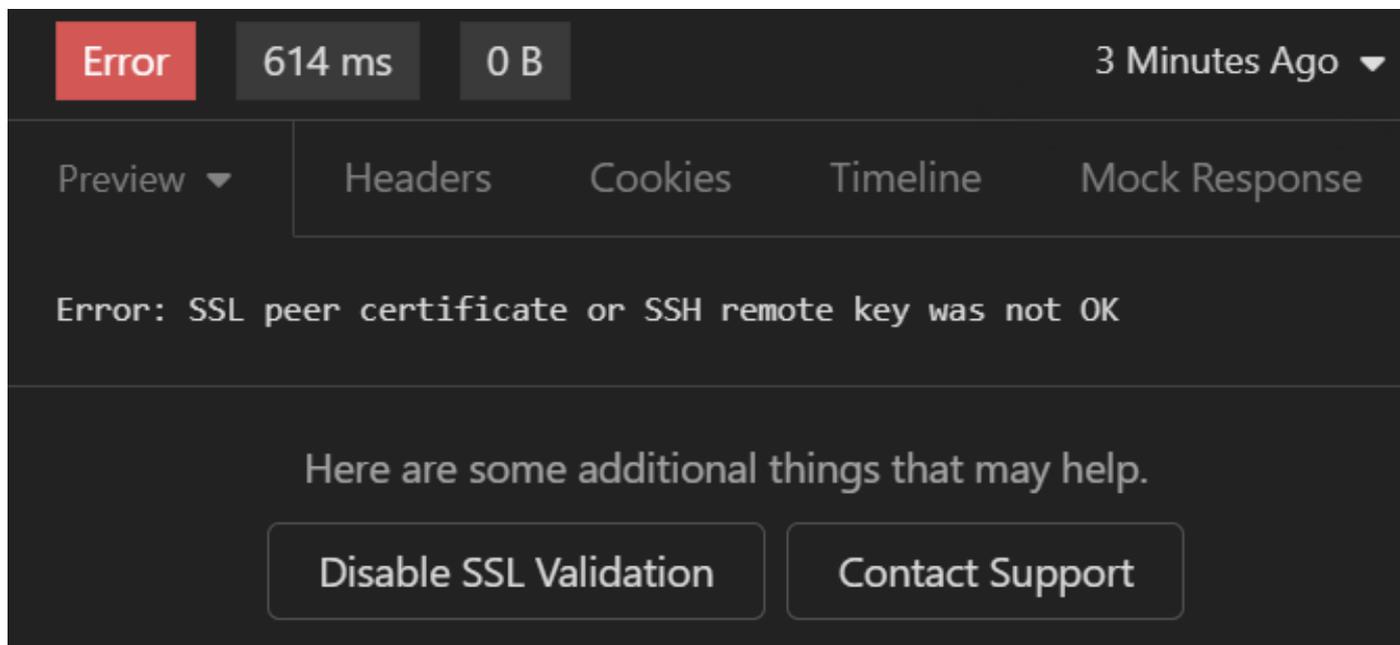
```
POST https://127.0.0.1/ers/config/internaluser Send 400 Bad Request
```

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.

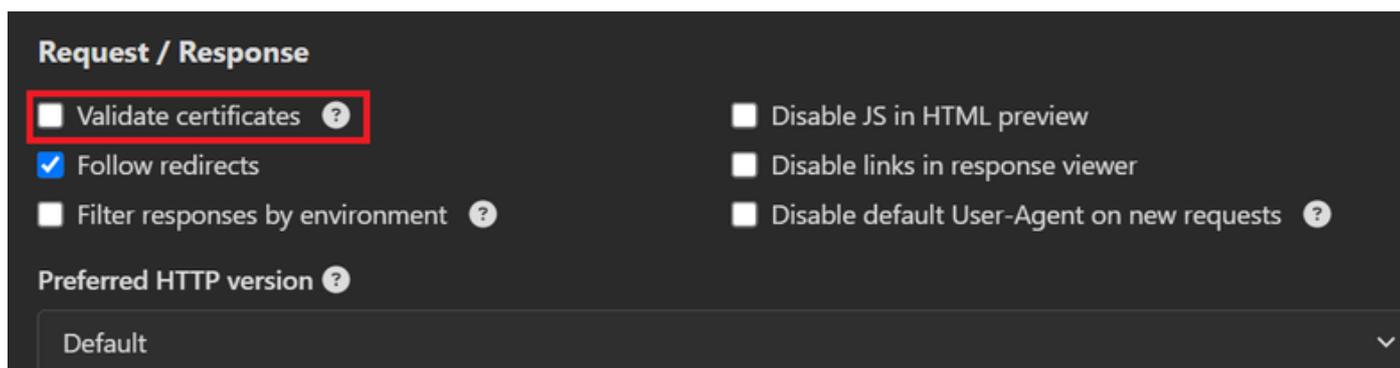
5. Errore: il certificato peer SSL o la chiave remota SSH non sono corretti



Errore certificato SSL

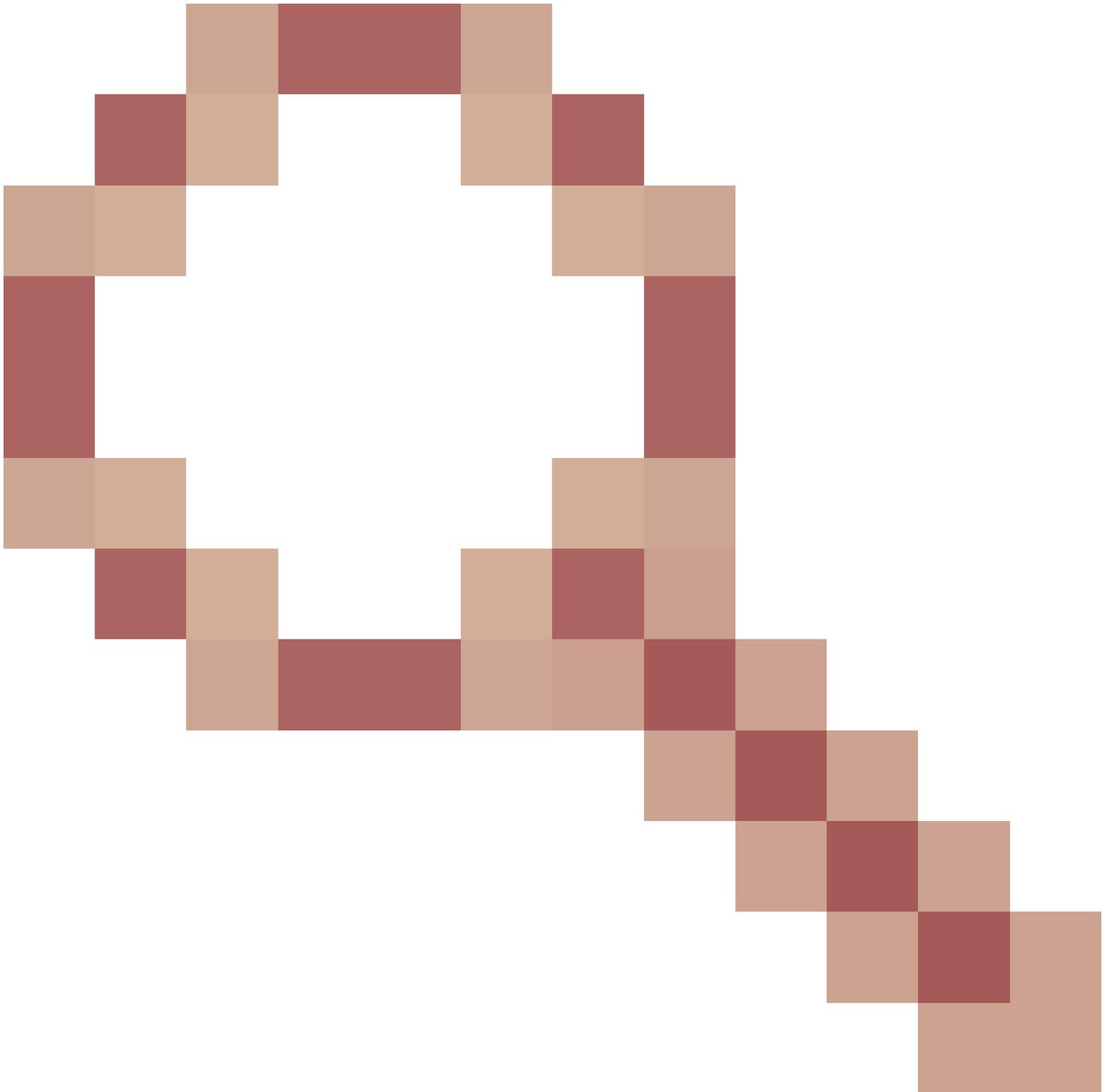
Soluzione:

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



Convalida certificati, opzione

6. [CSCwh71435](https://www.cscwh.com/71435)



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.

The screenshot shows the Cisco Identity Services Engine Administration / System interface. The left sidebar contains a navigation menu with categories like Security Settings, Alarm Settings, General MDM / UEM Settings, Posture, Profiling, Protocols, Endpoint Scripts, Proxy, SMTP Server, SMS Gateway, System Time, API Settings (highlighted), Data Connect, and Network Success Diagnostics. The main content area is titled 'API Settings' and has three tabs: Overview (selected), API Service Settings, and API Gateway Settings. The 'API Services Overview' section contains the following text:

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>

Impostazioni API

3. E fare clic su Documentazione API.

The screenshot shows the 'External RESTful Services (ERS) Online SDK' page. The left sidebar has a 'Quick Reference' section with 'API Documentation' highlighted. The main content area is titled 'ISE 3.3 Release Notes' and contains a table of '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

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).