Configuration des utilisateurs internes via JSON ou XML et des appels API dans ISE 3.3 avec Insominia

Table des matières

Introduction

Ce document décrit la configuration des utilisateurs internes dans Cisco ISE en exploitant les formats de données JSON ou XML en conjonction avec les appels d'API.

Conditions préalables

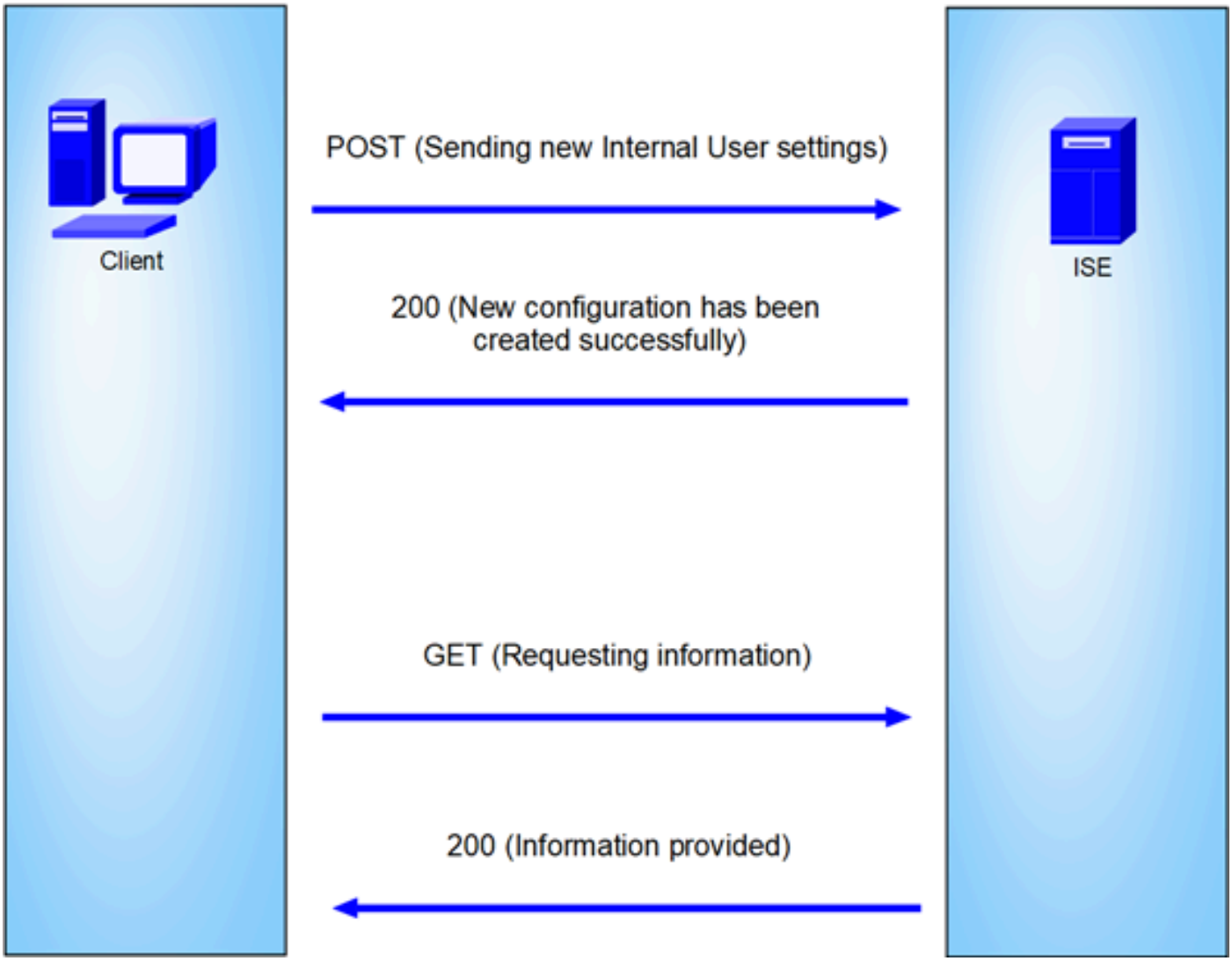
- ISE 3.0 ou supérieur.
- Logiciel client API.

Composants utilisés

- ISE 3.3
- Insomnie 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Diagramme du réseau



Topologie générale

GET et POST sont deux des méthodes HTTP les plus courantes utilisées dans les appels API (Application Programming Interface). Ils sont utilisés pour interagir avec les ressources d'un serveur, généralement pour récupérer des données ou les envoyer pour traitement.

Appel API GET

La méthode GET est utilisée pour demander des données à une ressource spécifiée. Les requêtes GET sont les méthodes les plus courantes et les plus utilisées dans les API et les sites Web. Lorsque vous visitez une page Web, votre navigateur envoie une requête GET au serveur hébergeant la page Web.

Appel API POST

La méthode POST est utilisée pour envoyer des données au serveur afin de créer ou de mettre à jour une ressource. Les requêtes POST sont souvent utilisées lors de l'envoi de données de formulaire ou du téléchargement d'un fichier.

Configurations

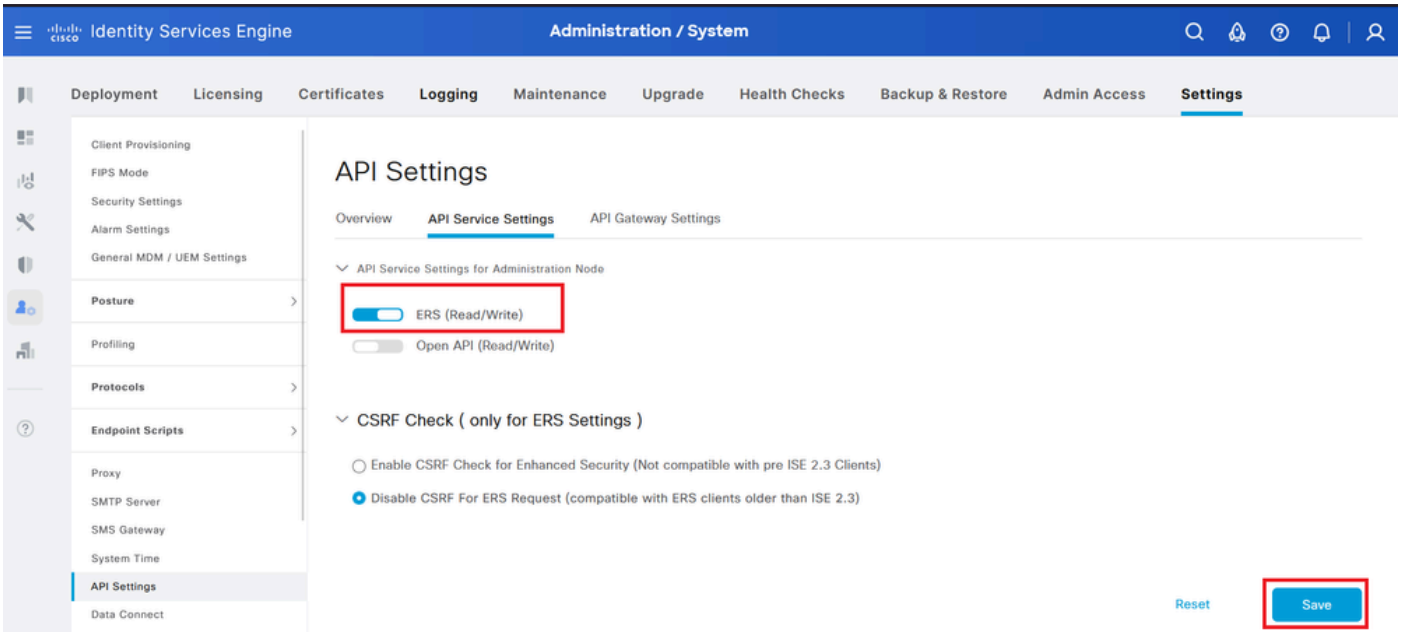
Nous devons envoyer les informations exactes du logiciel client API au noeud ISE pour créer un utilisateur interne.

Configurations ISE

Activez la fonctionnalité ERS.

1. Accédez à Administration > System > Settings > API Settings > API Service Settings.

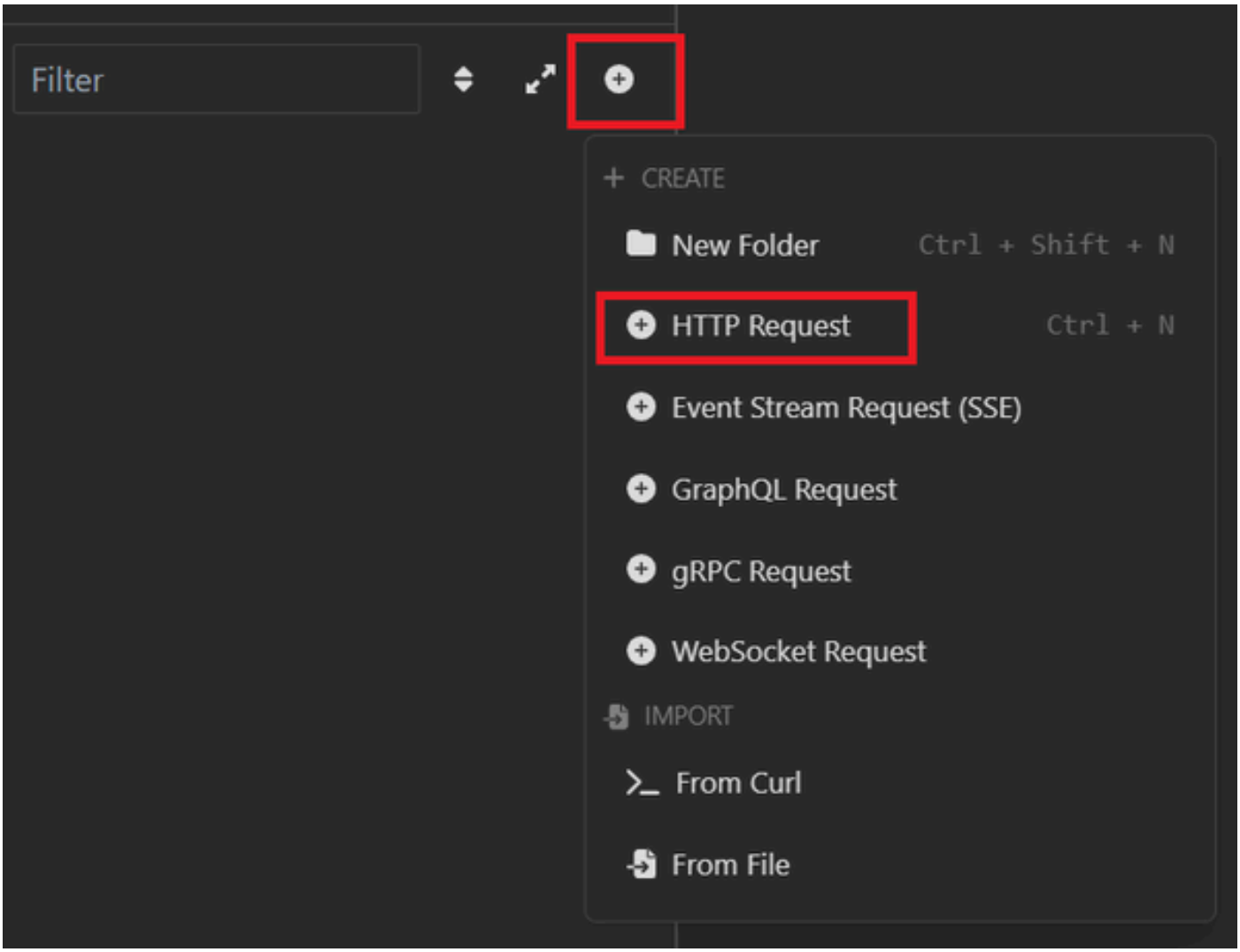
2. Activez l'option ERS (Read/Write).



Paramètres API

Demande JSON.

1. Insomnie ouverte.
2. Ajoutez une nouvelle requête HTTPS sur le côté gauche.

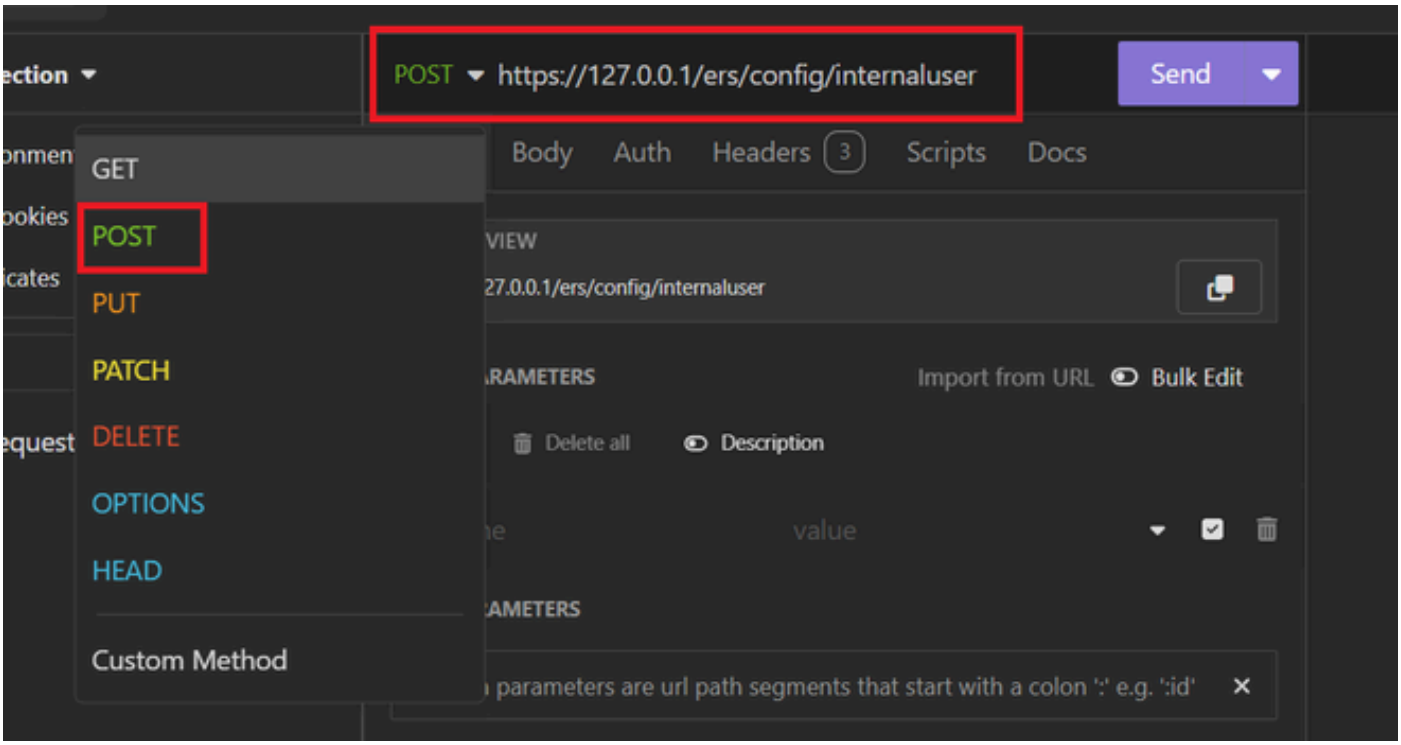


Demande JSON

3. Vous devez choisir POST pour envoyer les informations à votre noeud ISE.

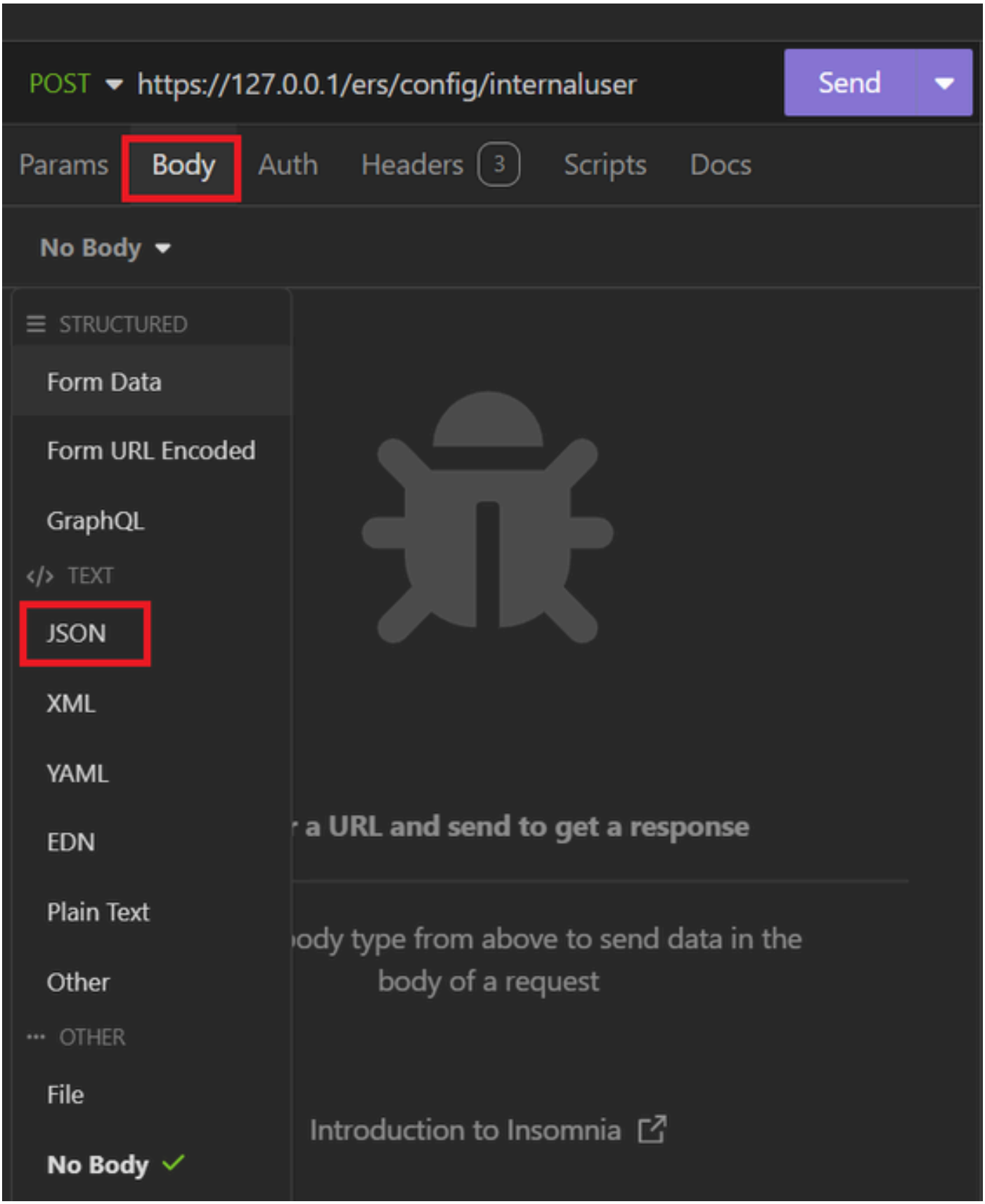
L'URL que vous devez entrer dépend de l'adresse IP de votre noeud ISE.

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



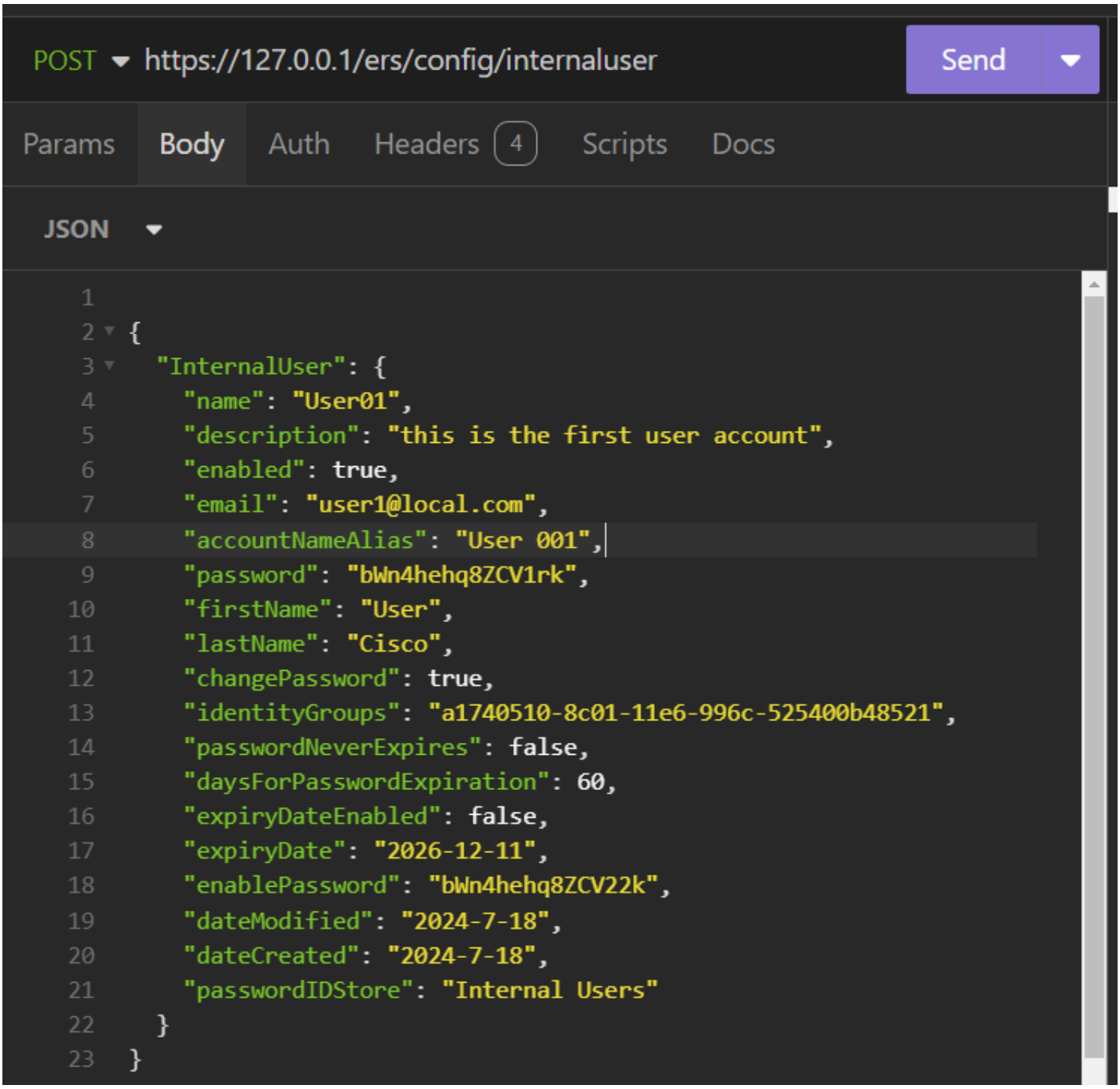
POSTE JSON

4. Cliquez ensuite sur Body et choisissez JSON



Corps JSON

5. Vous pouvez coller la syntaxe et modifier les paramètres en fonction de ce que vous voulez.



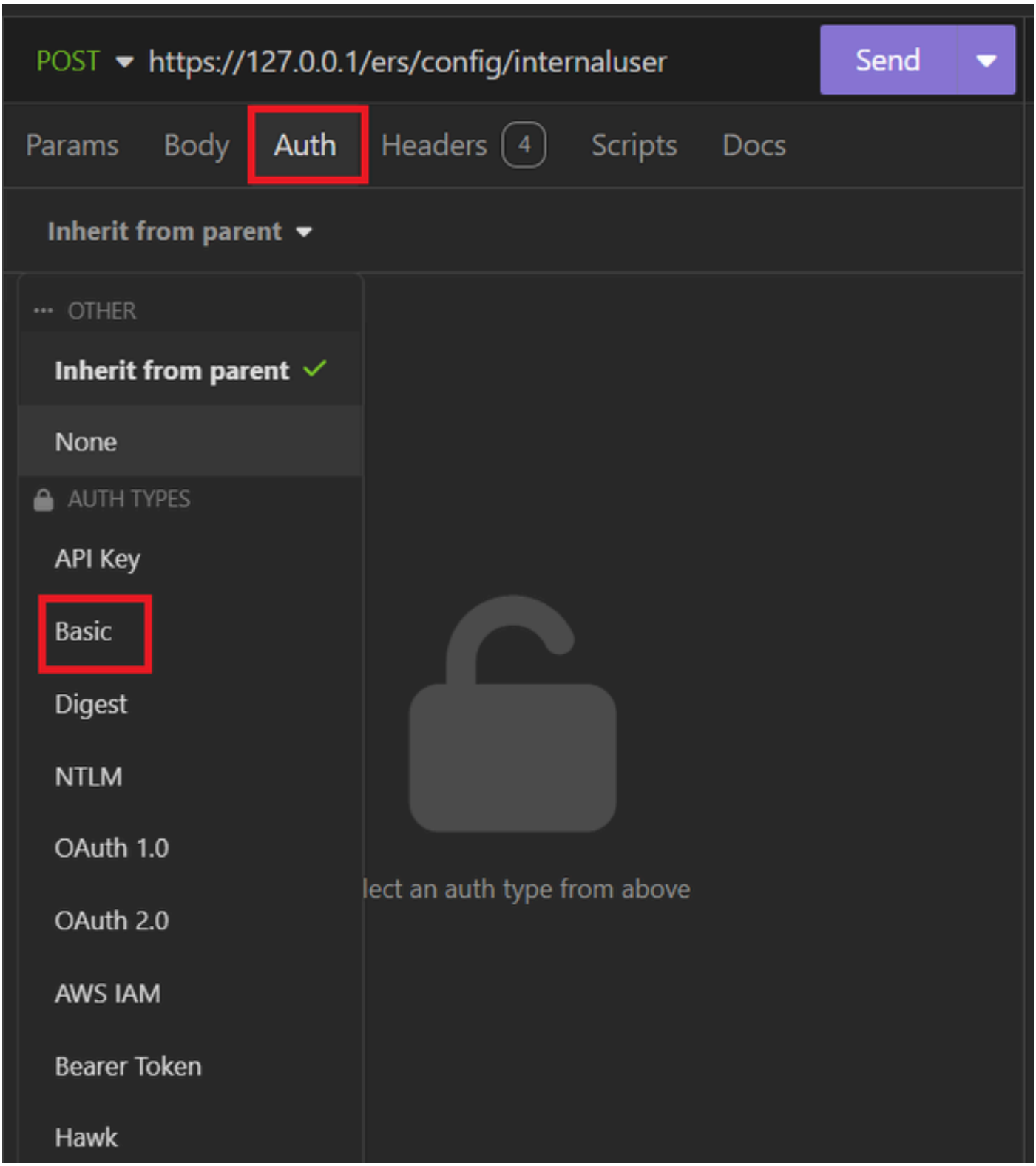
Syntaxe JSON

syntaxe JSON

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

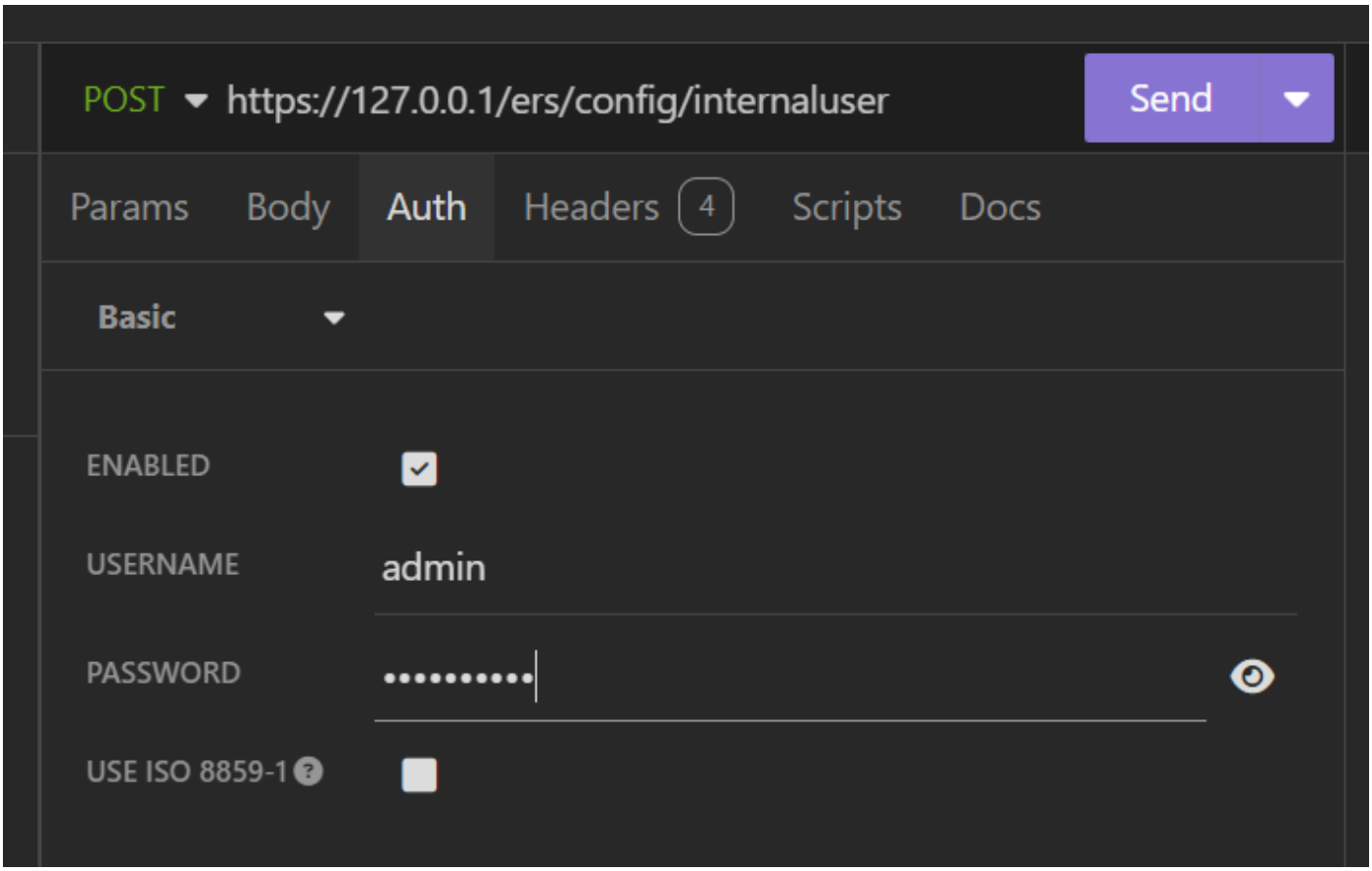
```
    "password": "password",
    "firstName": "firstName",
    "lastName": "lastName",
    "changePassword": true,
    "identityGroups": "identityGroups",
    "passwordNeverExpires": false,
    "daysForPasswordExpiration": 60,
    "expiryDateEnabled": false,
    "expiryDate": "2016-12-11",
    "enablePassword":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

6. Cliquez sur Auth et choisissez Basic.



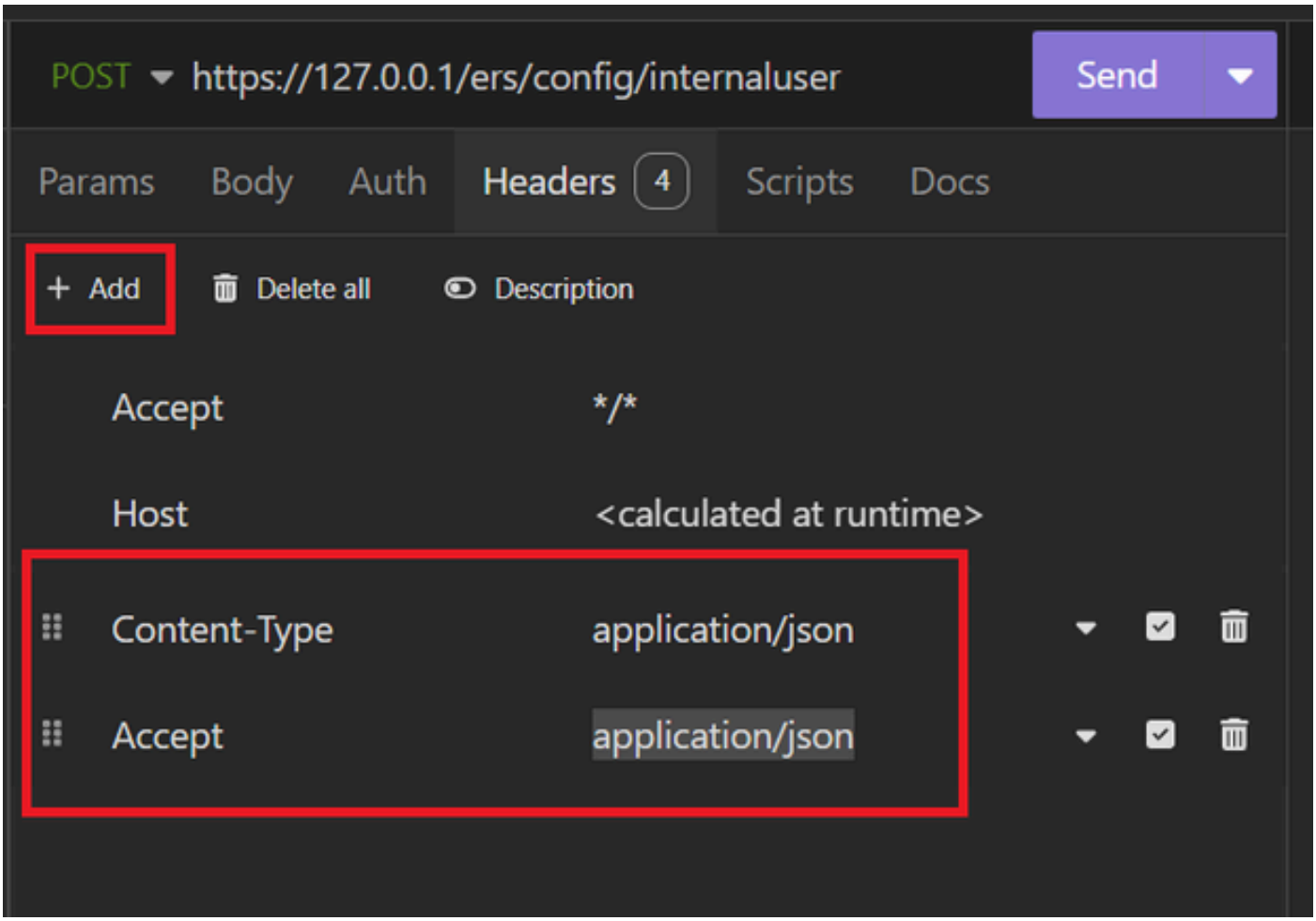
Authentification JSON

7. Saisissez les informations d'identification de l'interface ISE.



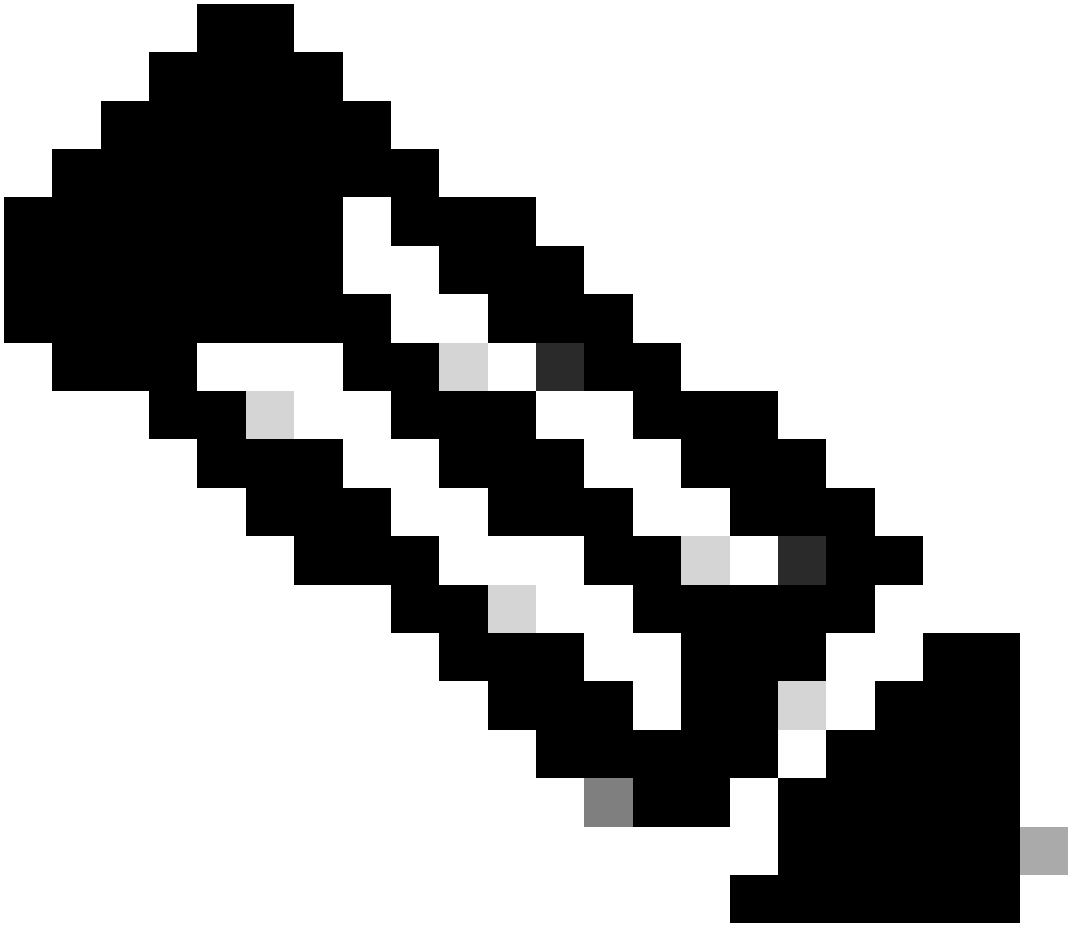
Informations d'identification JSON administrateur

8. Cliquez sur En-têtes pour ajouter les méthodes suivantes :
    - Content-Type : application/json
    - Accepter : application/json



En-têtes JSON

9. Enfin, cliquez sur Envoyer.



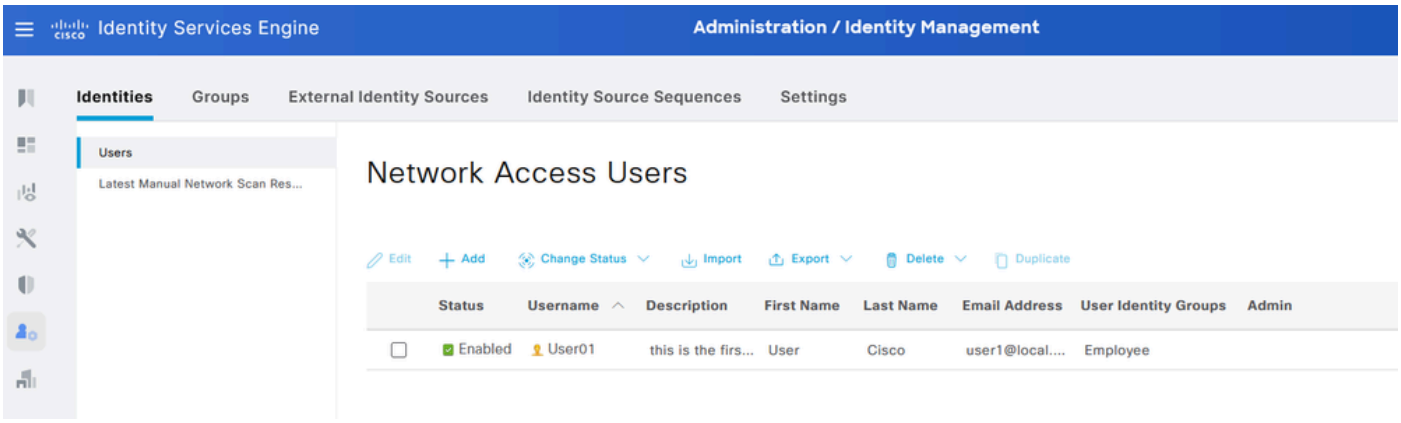
Remarque : si vous souhaitez affecter un groupe d'identités au nouveau compte d'utilisateur, vous devez utiliser l'ID du groupe d'identités. Consultez la **section Dépannage** pour plus d'informations.

Validation

1. Après l'envoi de la requête POST, vous allez voir l'état « 201 Créé ». Cela signifie que le processus s'est terminé avec succès.

Demande JSON réussie

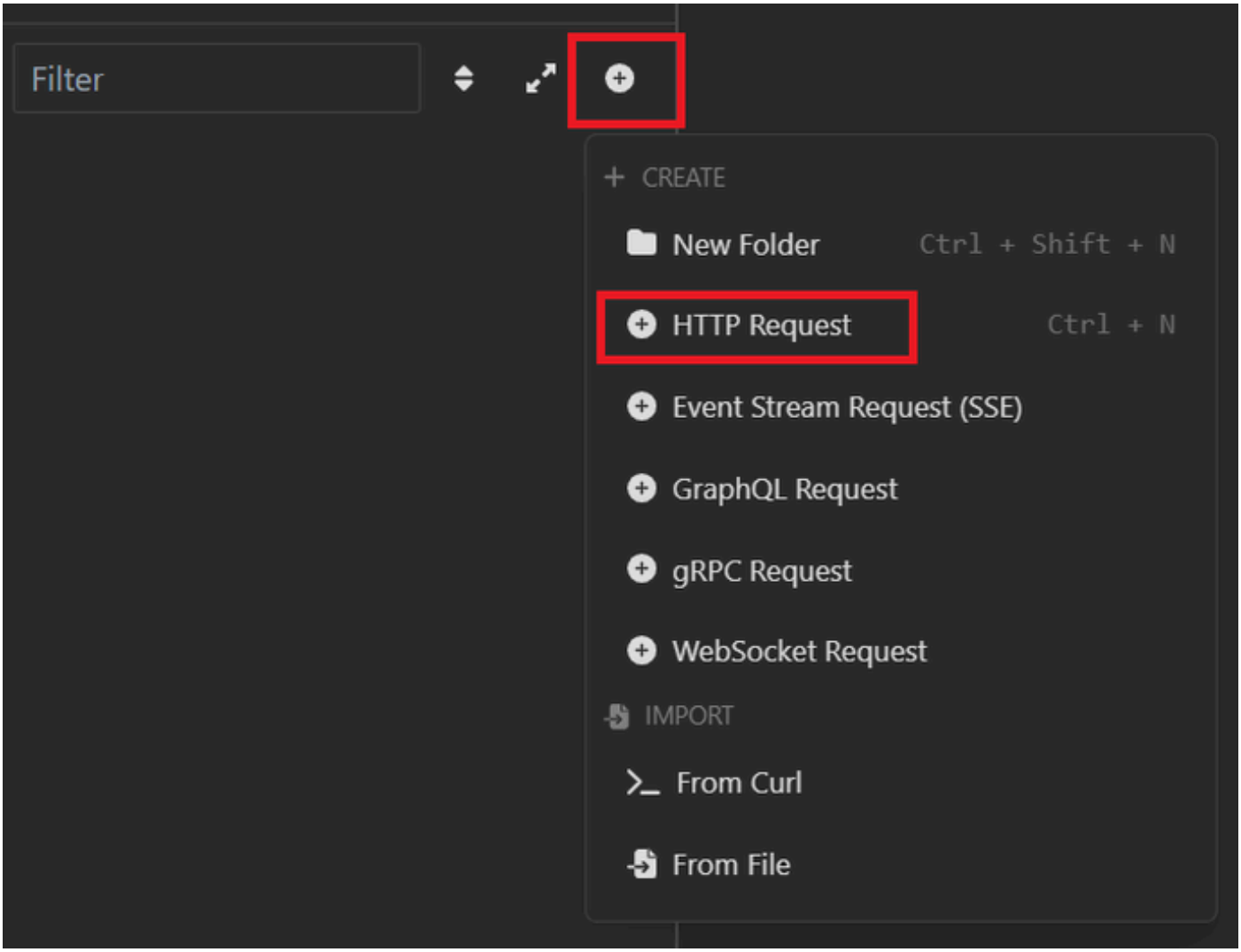
2. Ouvrez l'interface utilisateur graphique ISE et accédez à Administration > Identity Management > Identities > Users > Network Access Users



Compte d'utilisateur JSON

Requête XML

1. Insomnie ouverte.
2. Ajoutez une nouvelle requête HTTPS sur le côté gauche.

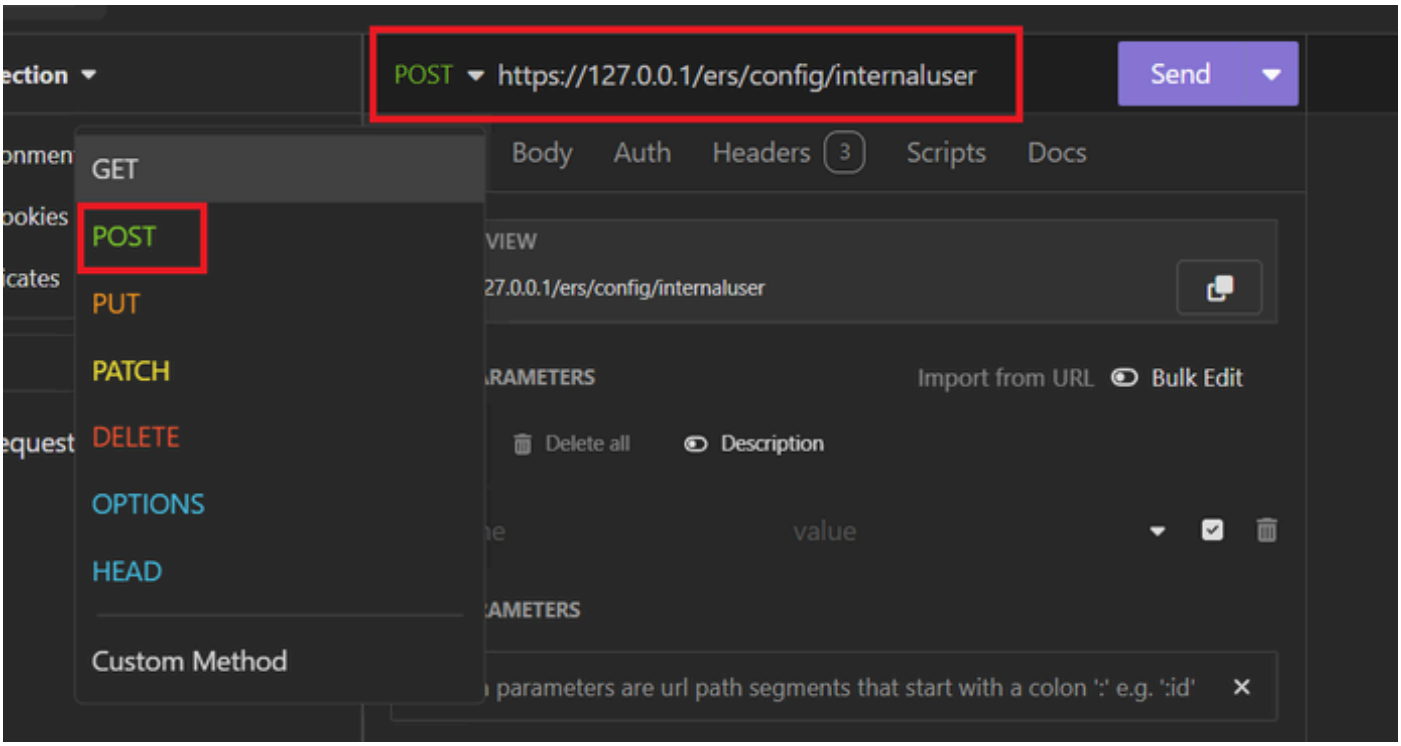


Requête XML

3. Vous devez choisir POST pour envoyer les informations à votre noeud ISE.

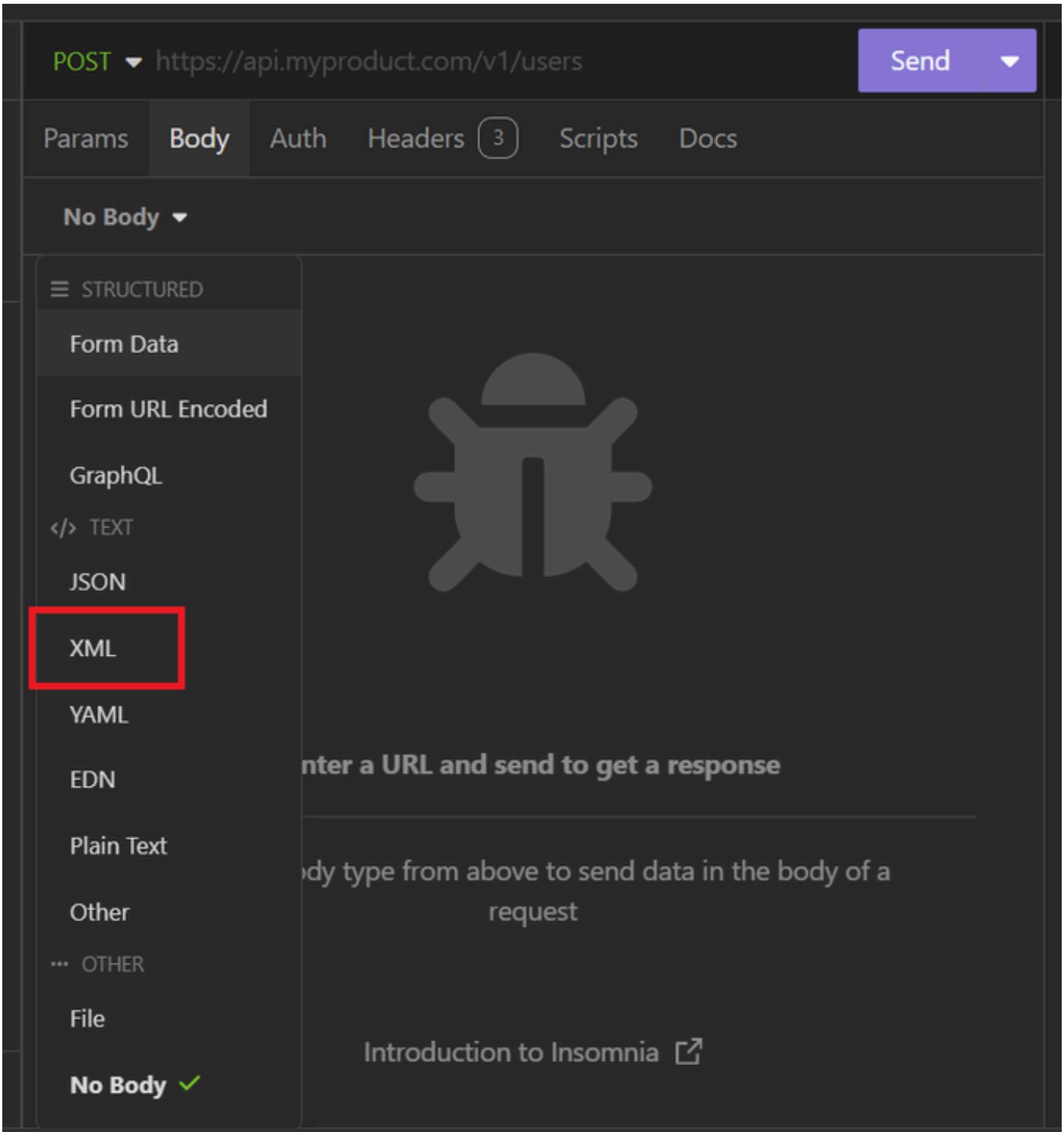
L'URL que vous devez entrer dépend de l'adresse IP de votre noeud ISE.

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



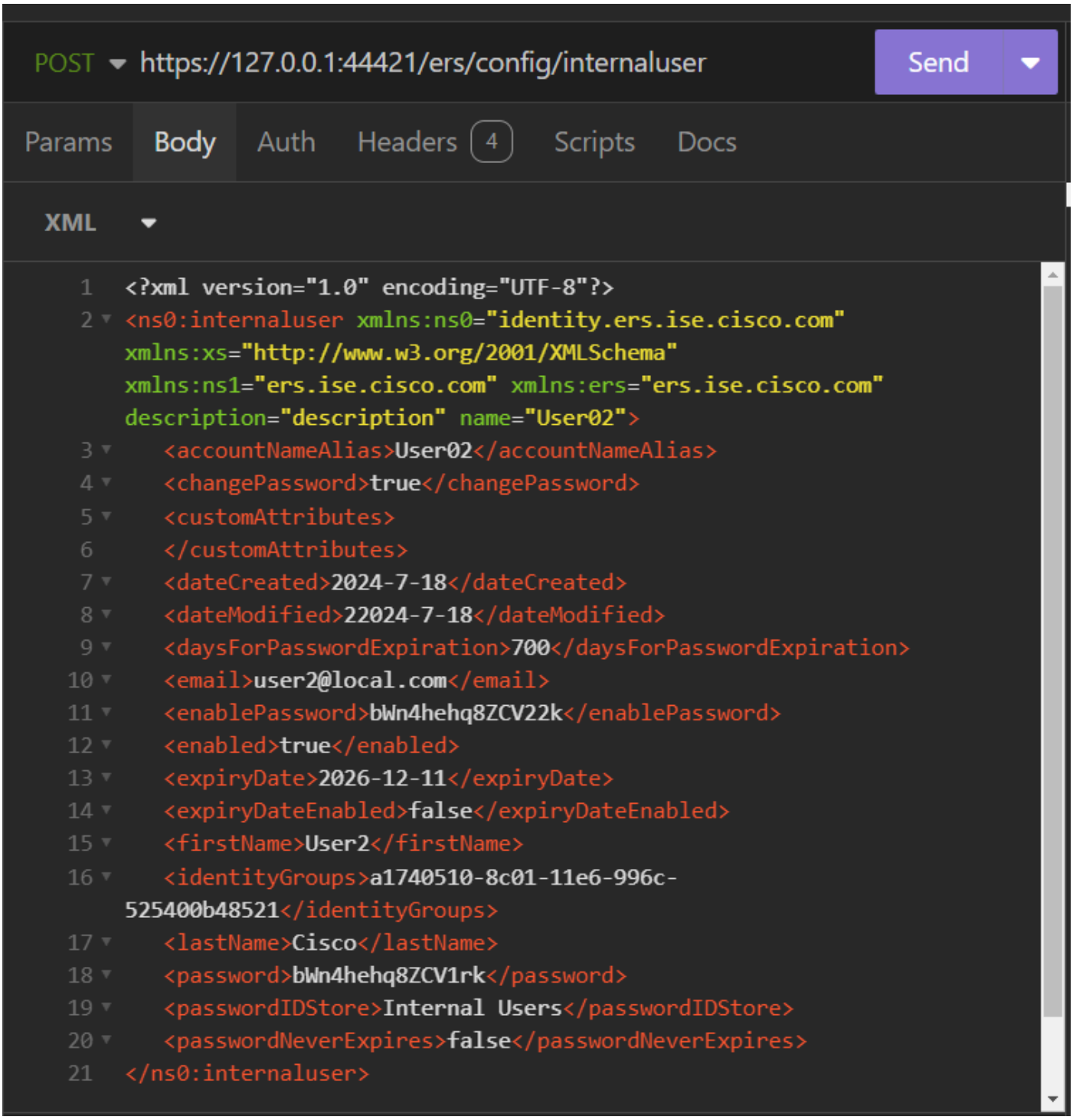
POST XML

4. Cliquez ensuite sur Corps et choisissez XML.



Corps XML

5. Vous pouvez coller la syntaxe et modifier les paramètres en fonction de ce que vous voulez.



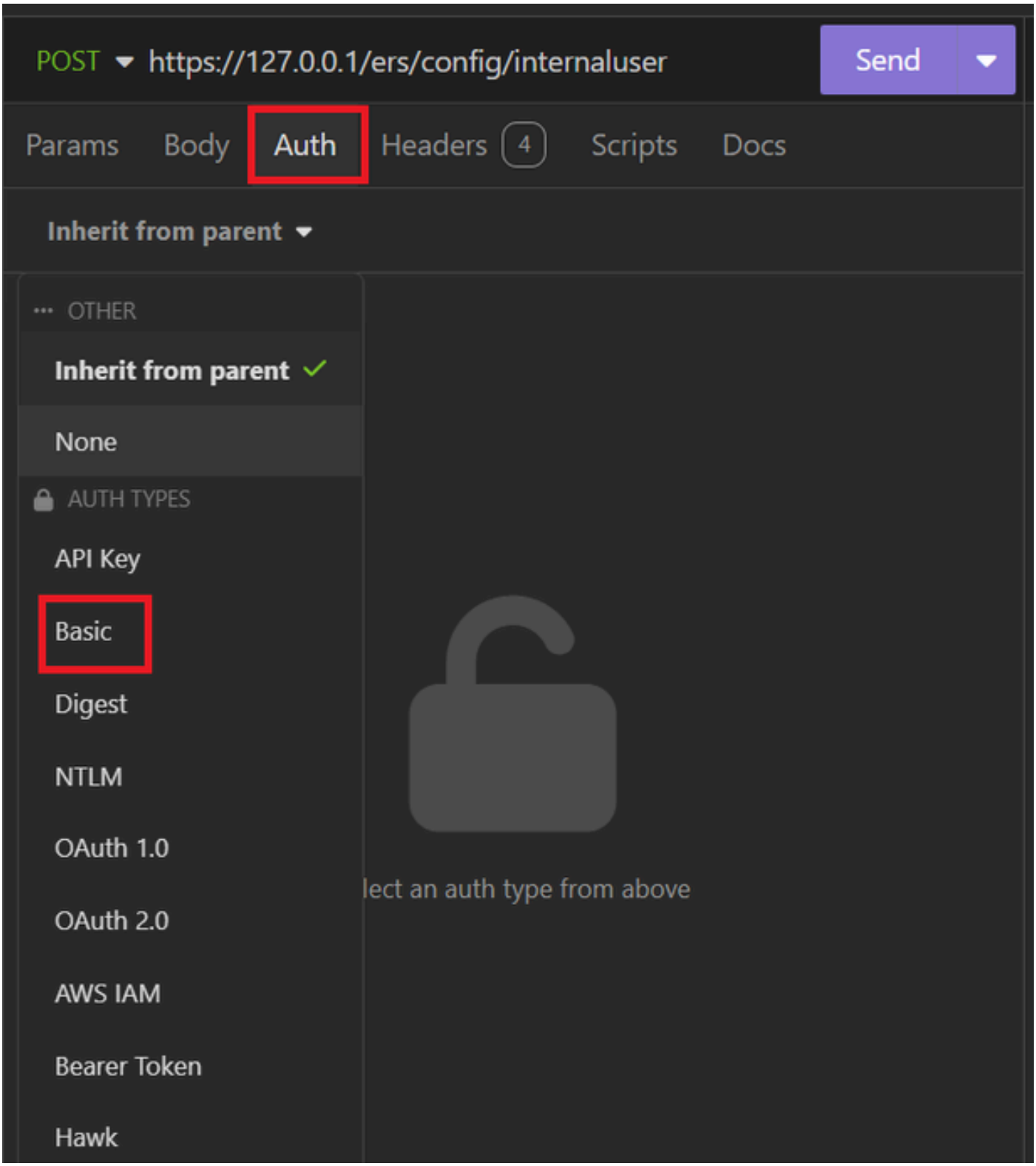
Publication XML

syntaxe 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>
```

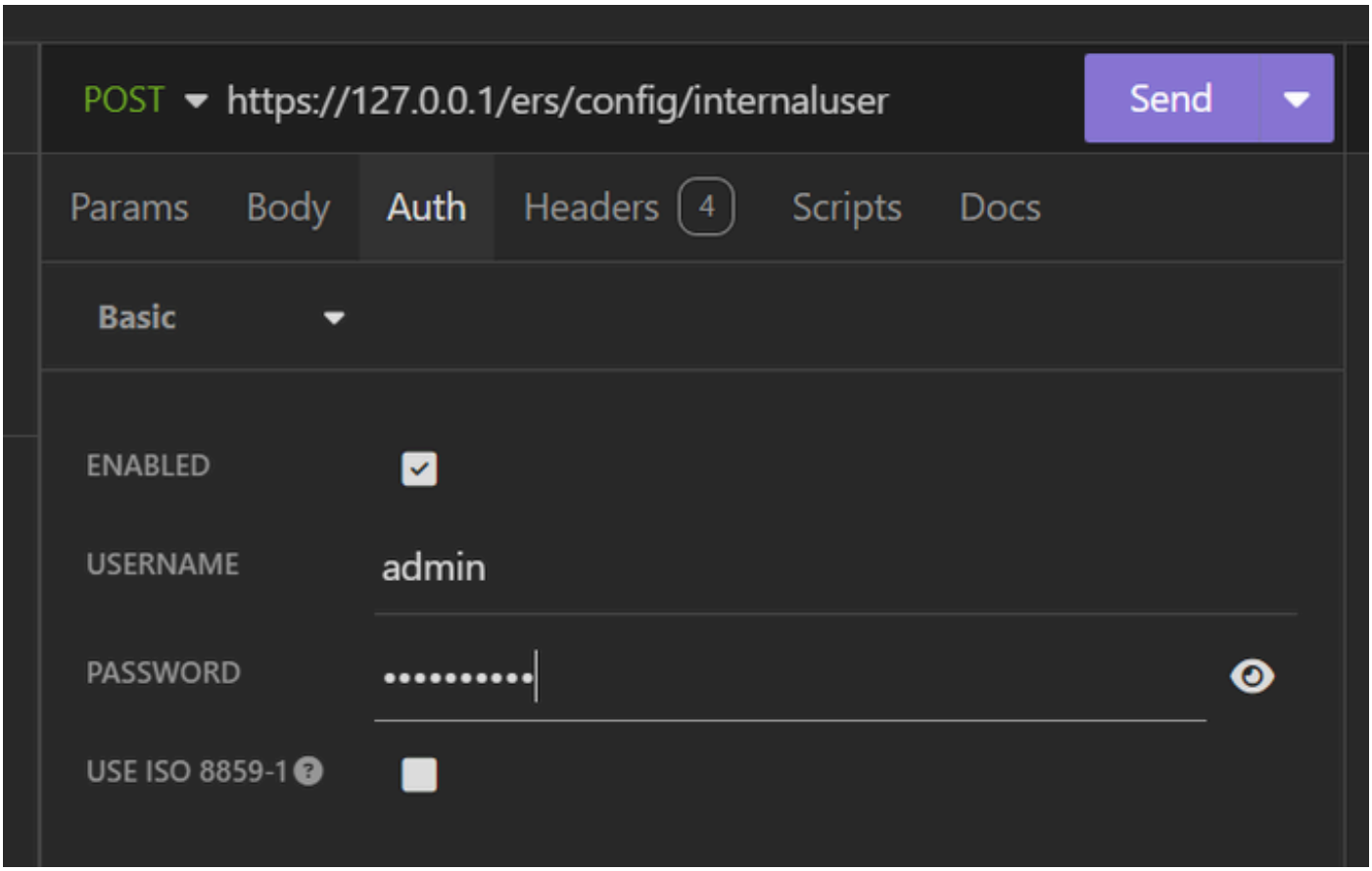
```
        <entry>
            <key>key1</key>
            <value>value1</value>
        </entry>
        <entry>
            <key>key2</key>
            <value>value3</value>
        </entry>
    </customAttributes>
    <dateCreated>2015-12-15</dateCreated>
    <dateModified>2015-12-20</dateModified>
    <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. Cliquez sur Auth et choisissez Basic



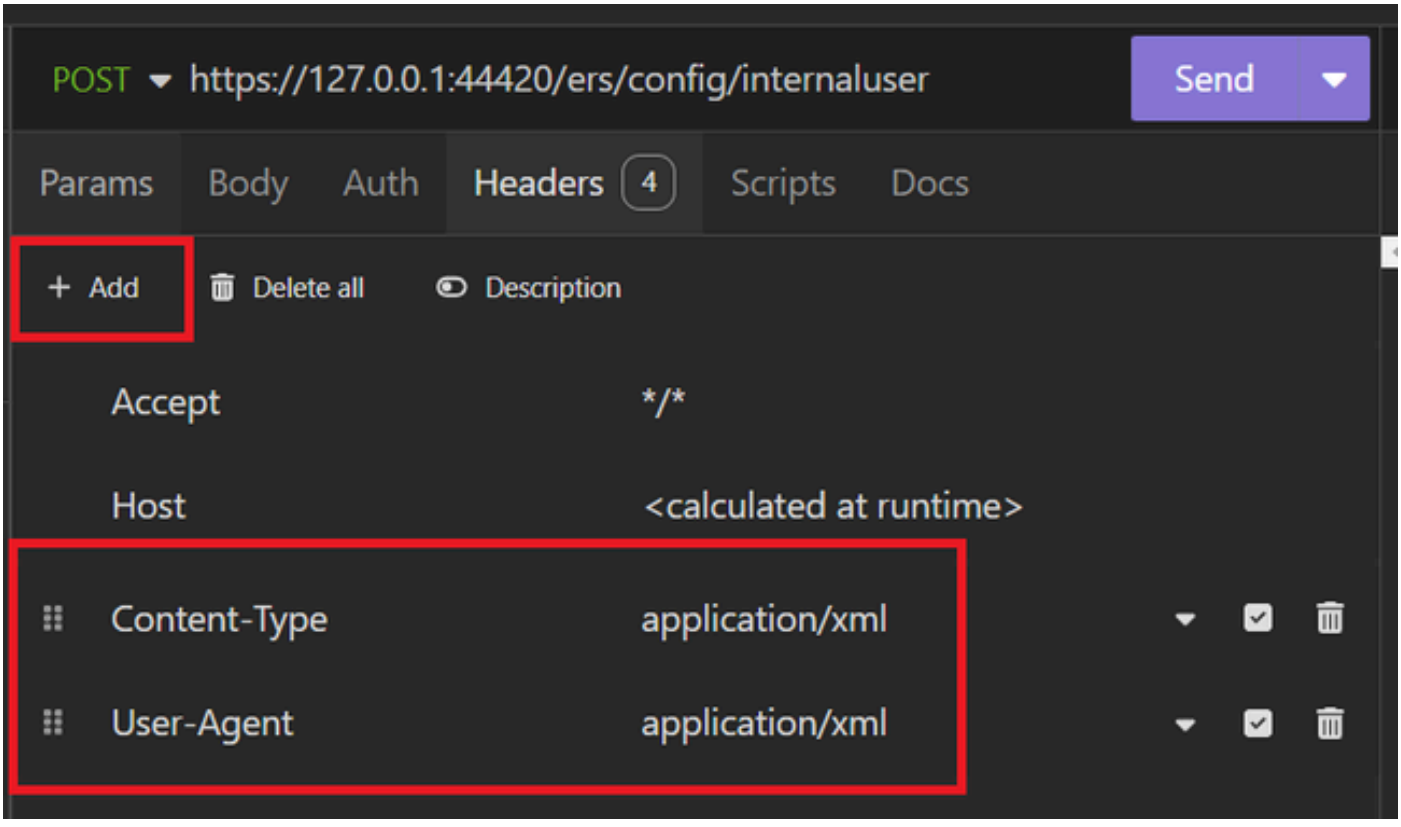
Authentification XML

7. Saisissez les informations d'identification de l'interface ISE.



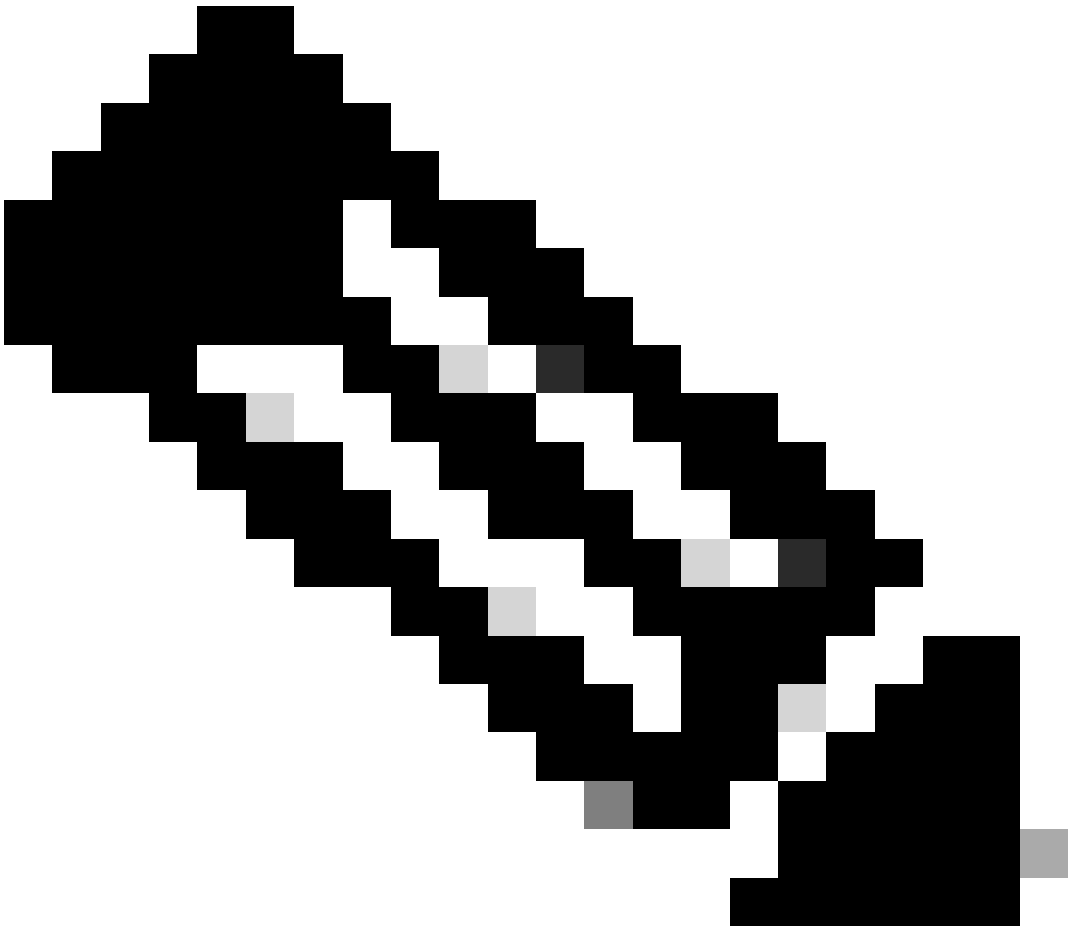
Informations d'identification XML

8. Cliquez sur En-têtes pour ajouter les méthodes suivantes :
    - Content-Type : application/xml
    - Accepter : application/xml



En-têtes XML

9. Enfin, cliquez sur Envoyer.



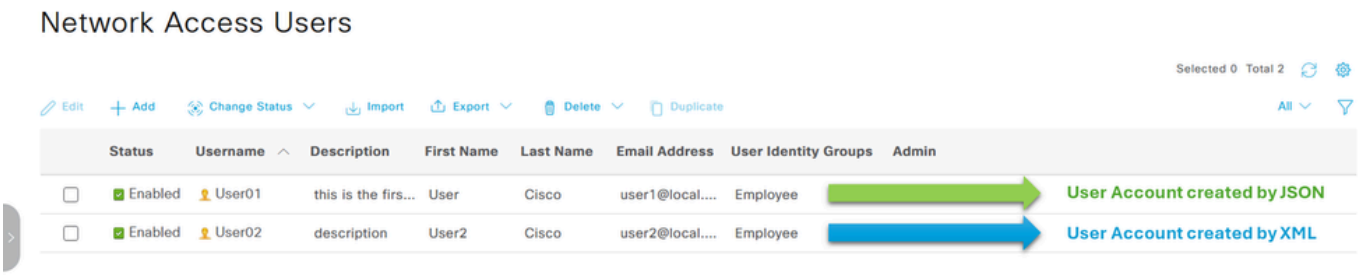
Remarque : si vous souhaitez affecter un groupe d'identités au nouveau compte d'utilisateur, vous devez utiliser l'ID du groupe d'identités. Consultez la **section Dépannage** pour plus d'informations.

Validation

1. Après l'envoi de la requête POST, vous allez voir l'état « 201 Créé ». Cela signifie que le processus s'est terminé avec succès.

Demande XML réussie

2. Ouvrez l'interface utilisateur graphique ISE et accédez à Administration > Identity Management > Identities > Users > Network Access Users

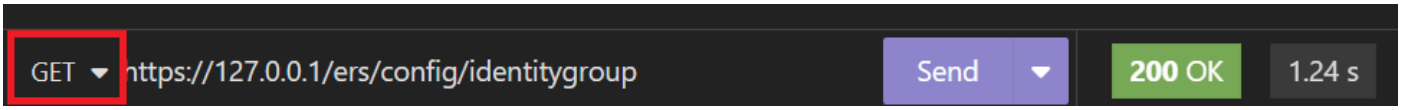


Validation des comptes d'utilisateurs

Dépannage

1. Identifiez l'ID du groupe d'identités.

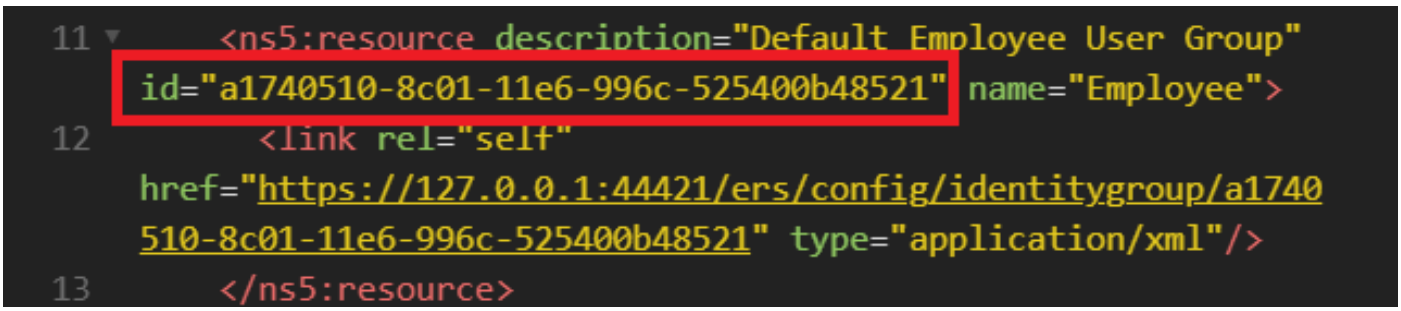
Utilisez GET et la requête https://X.X.X.X/ers/config/identitygroup.



option GET

Sortie JSON.

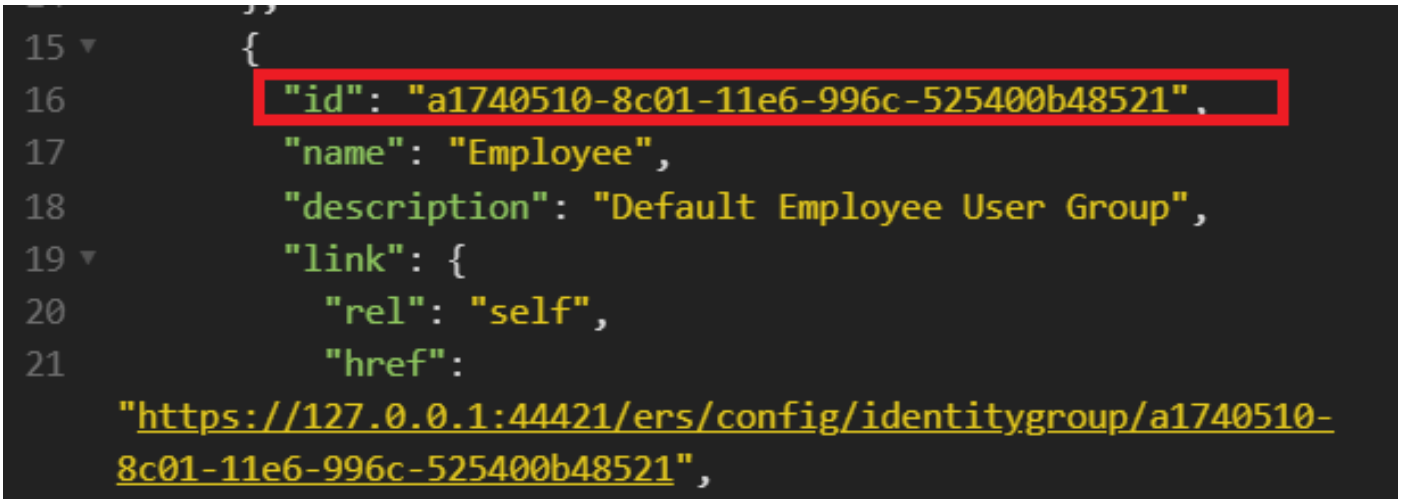
Identifiez l'ID en regard de la description.



ID groupe d'identité 01

Sortie XML.

Identifiez l'ID en regard de la description.



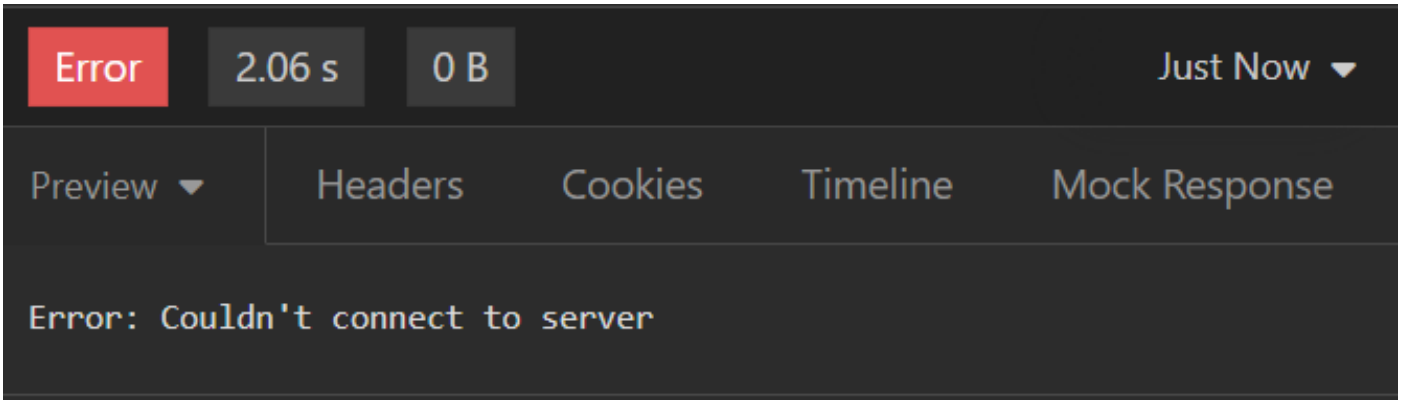
ID Identity Group 02

2. 401 Erreur non autorisée.

erreur 401

Solution : vérifiez les informations d'identification d'accès configurées dans la section Auth

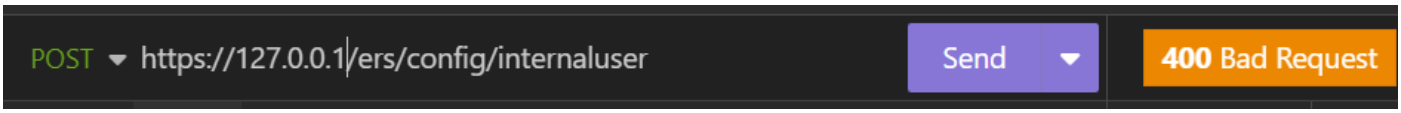
3. Erreur : Impossible de se connecter au serveur



Erreur de connexion

Solution : vérifiez l'adresse IP du noeud ISE configuré dans Insomnia ou validez la connectivité.

4. 400 Requête incorrecte.

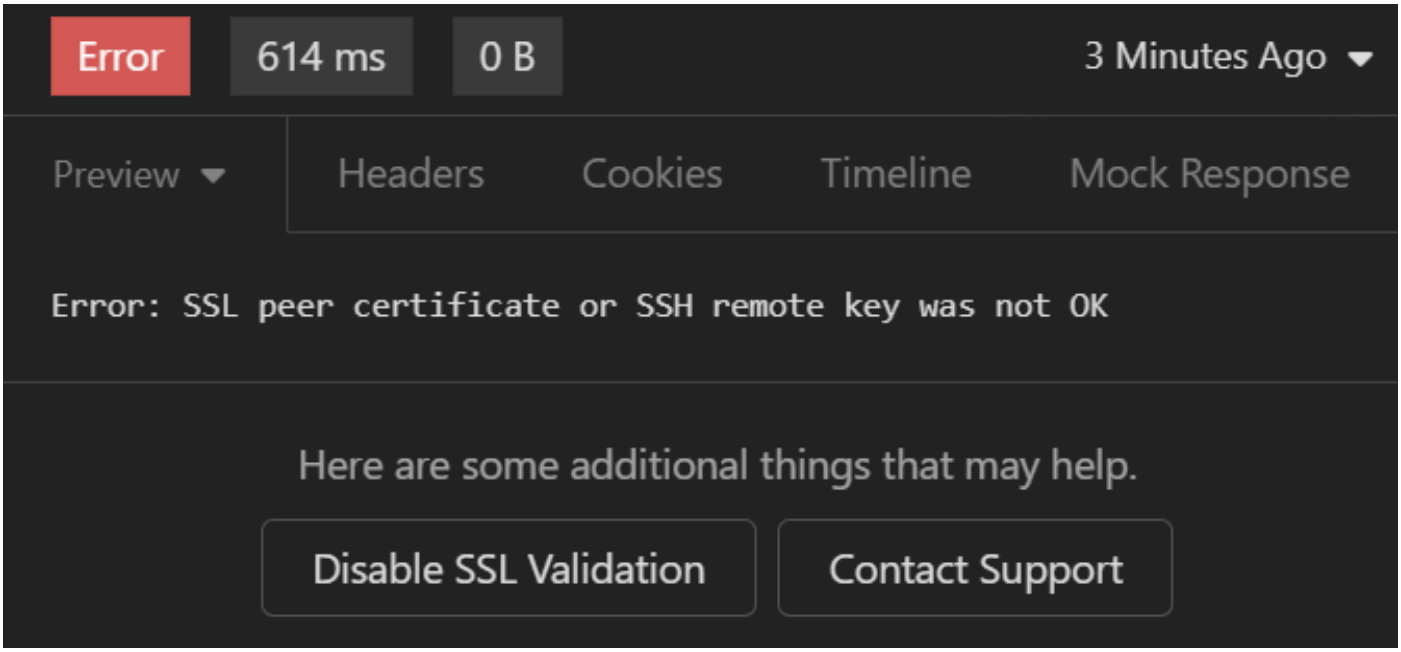


Erreur 400

Il existe plusieurs raisons de faire face à cette erreur, les plus courantes sont :

- Incompatibilité avec la stratégie de mot de passe de sécurité
- Certains paramètres ont été mal configurés.
- Erreur Sintaxis.
- Informations dupliquées.

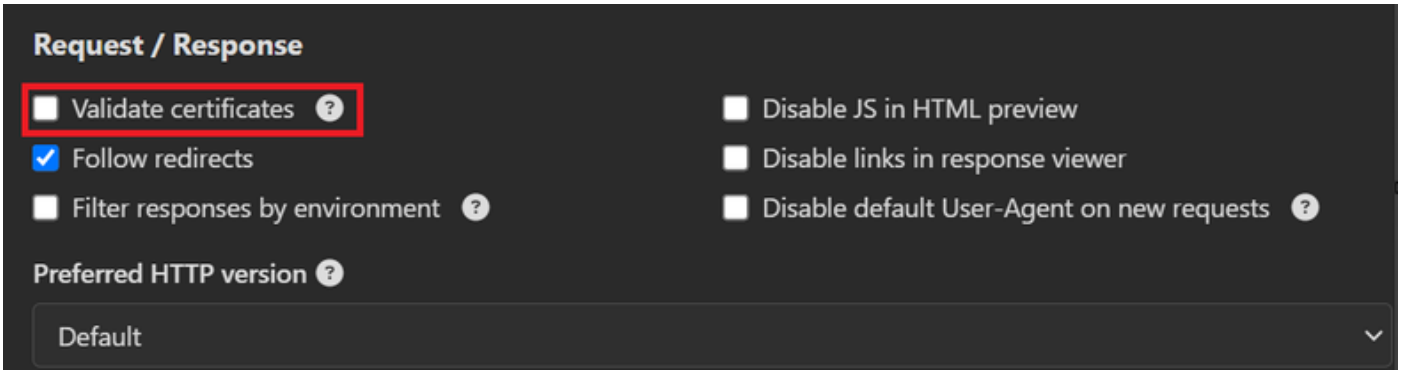
5. Erreur : le certificat d'homologue SSL ou la clé distante SSH n'était pas correct



Erreur de certificat SSL

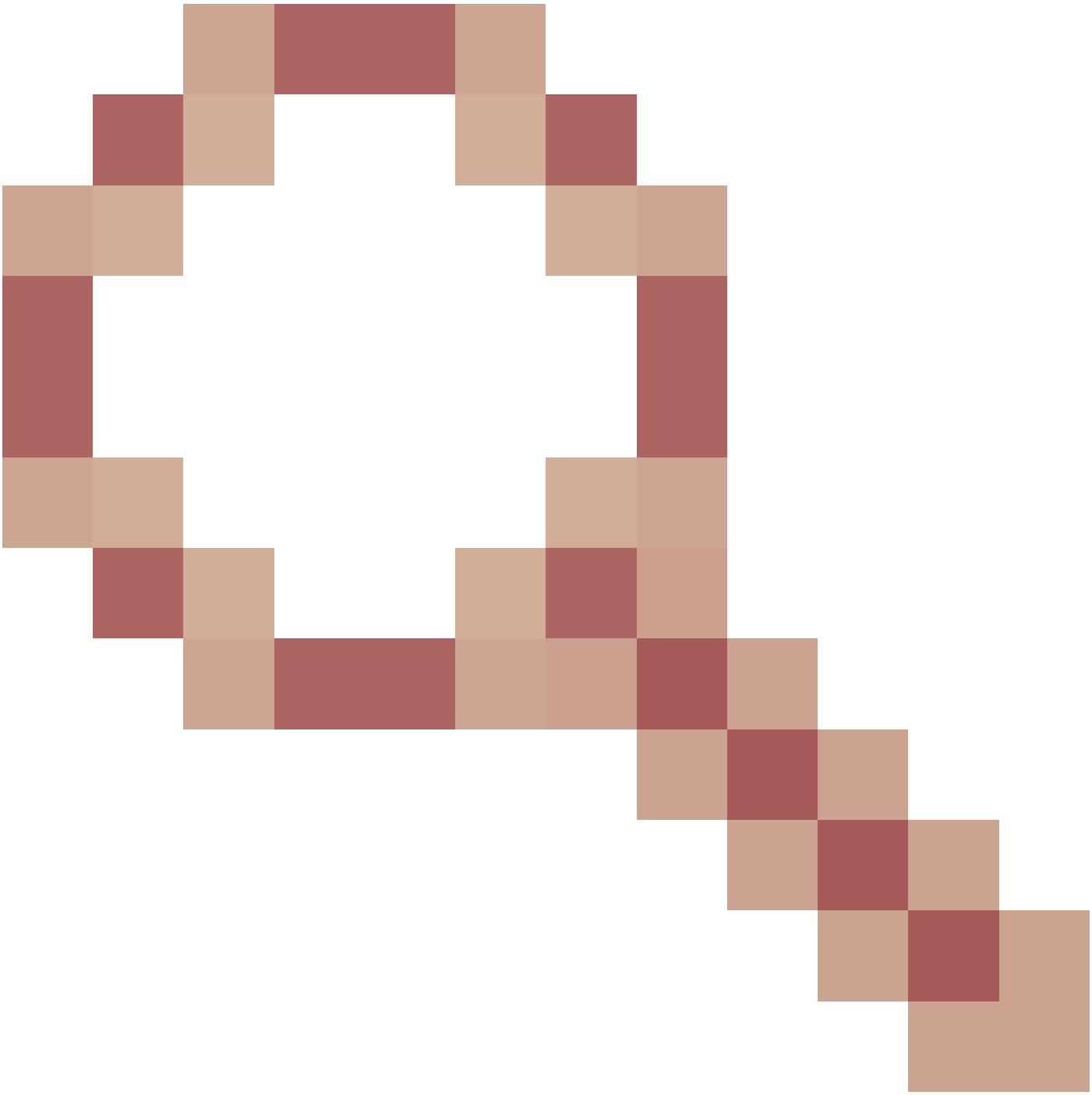
Solution :

1. Cliquez sur Désactiver la validation SSL.
2. Sous Request / Response, désactivez l'option Validate Certificates.



Option Valider les certificats

6.



défaut CSCwh71435.

Le mot de passe enable est configuré de manière aléatoire, bien que vous ne l'ayez pas configuré. Ce comportement se produit lorsque la syntaxe enable password est supprimée ou laissée vide comme valeur. Pour plus d'informations, cliquez sur le lien suivant :

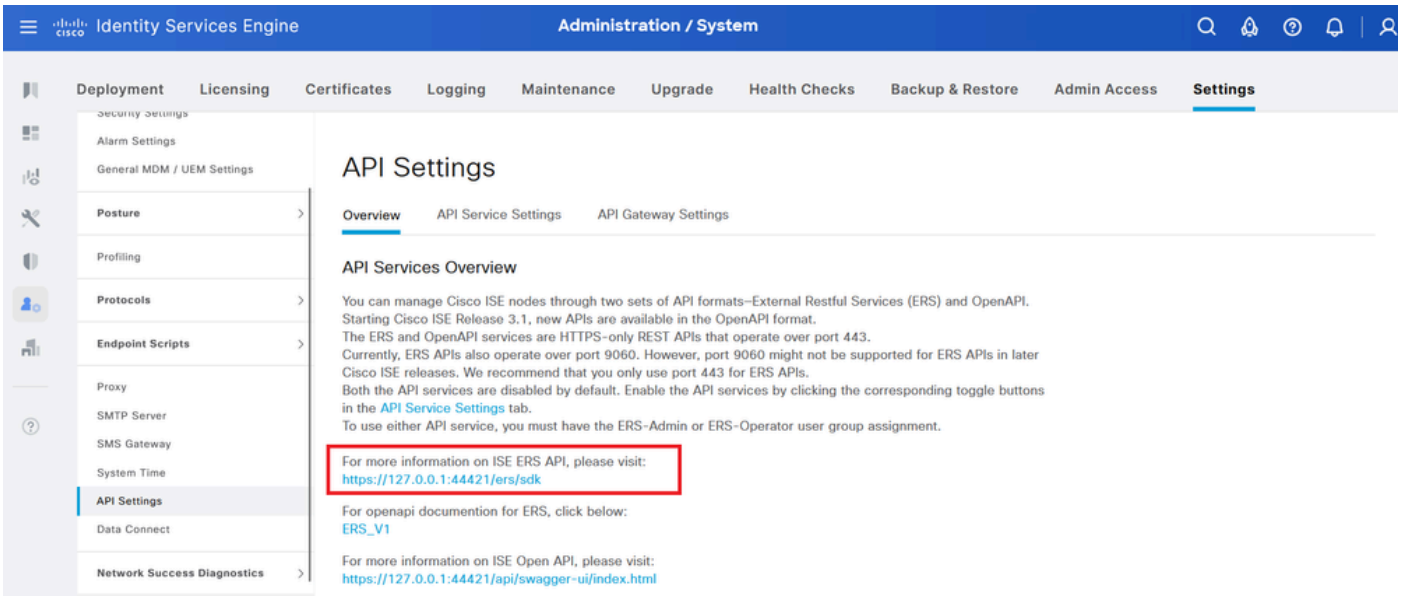
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh71435

Références d'appel API.

Vous pouvez voir toutes les informations sur les appels d'API pris en charge par ISE.

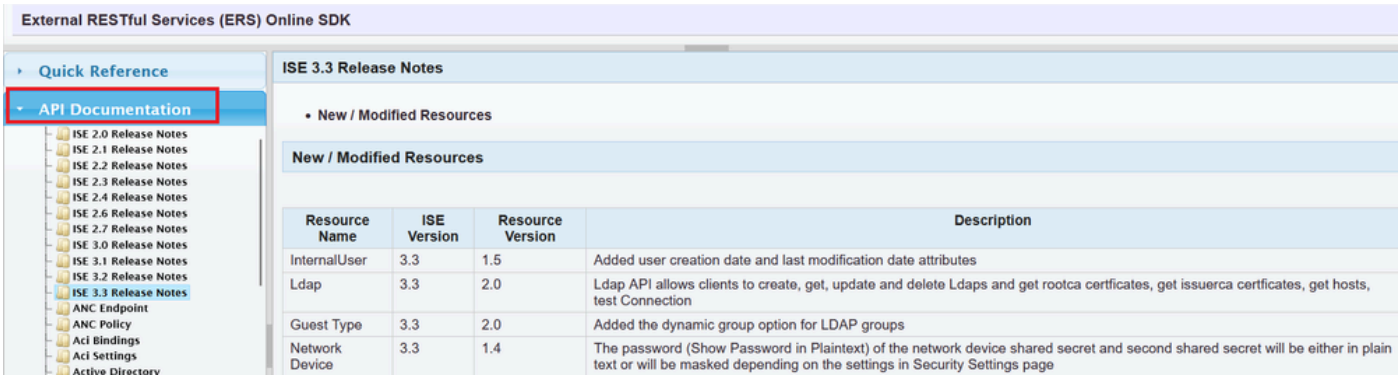
1. Accédez à Administration > System > Settings > API Setting.

2. Cliquez sur le lien d'informations de l'API ERS.



Paramètres API

3. Et cliquez sur la documentation de l'API.



Documentation API

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.