

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

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

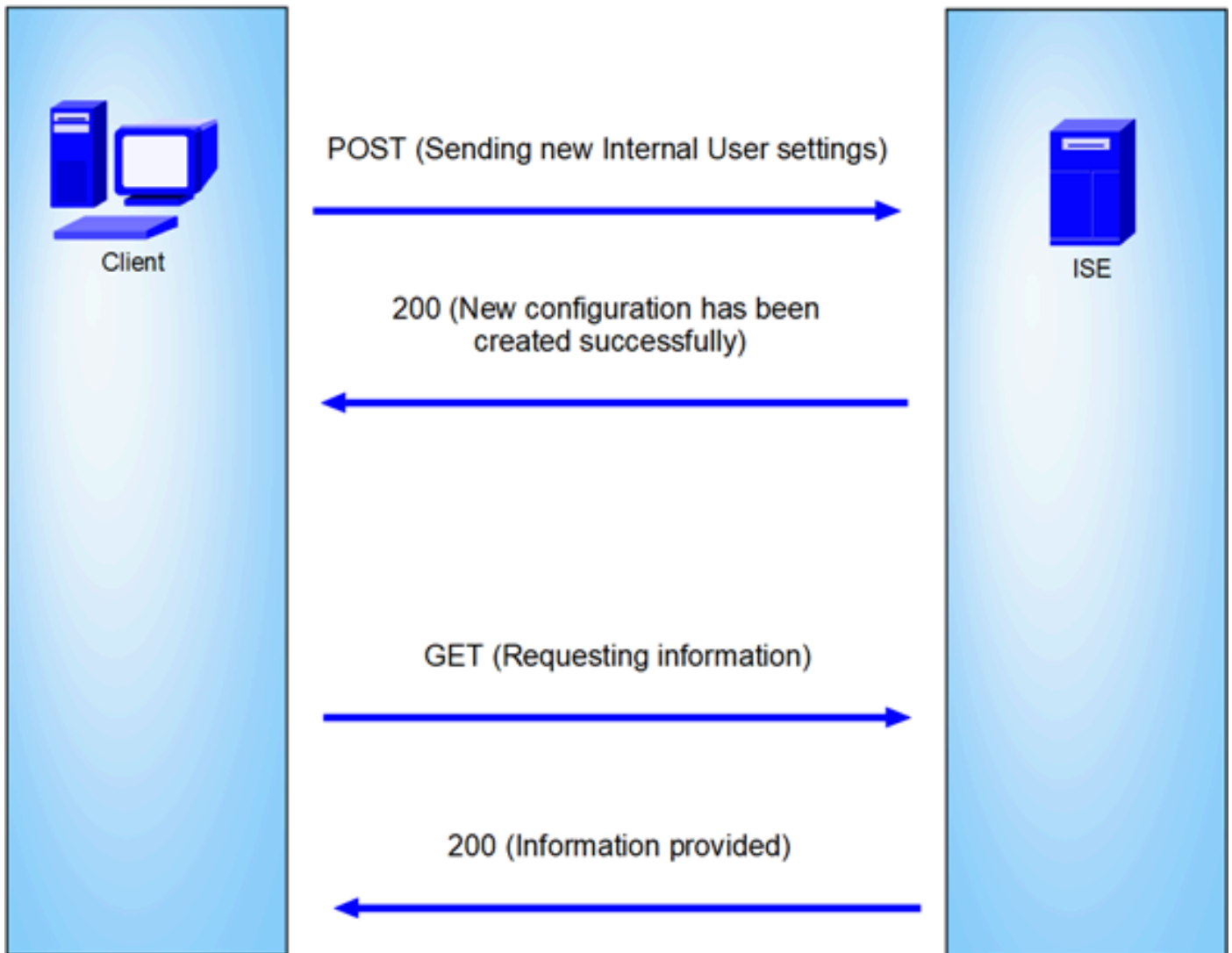
- ISE 3.0 ou supérieur.
- Logiciel client API.

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.

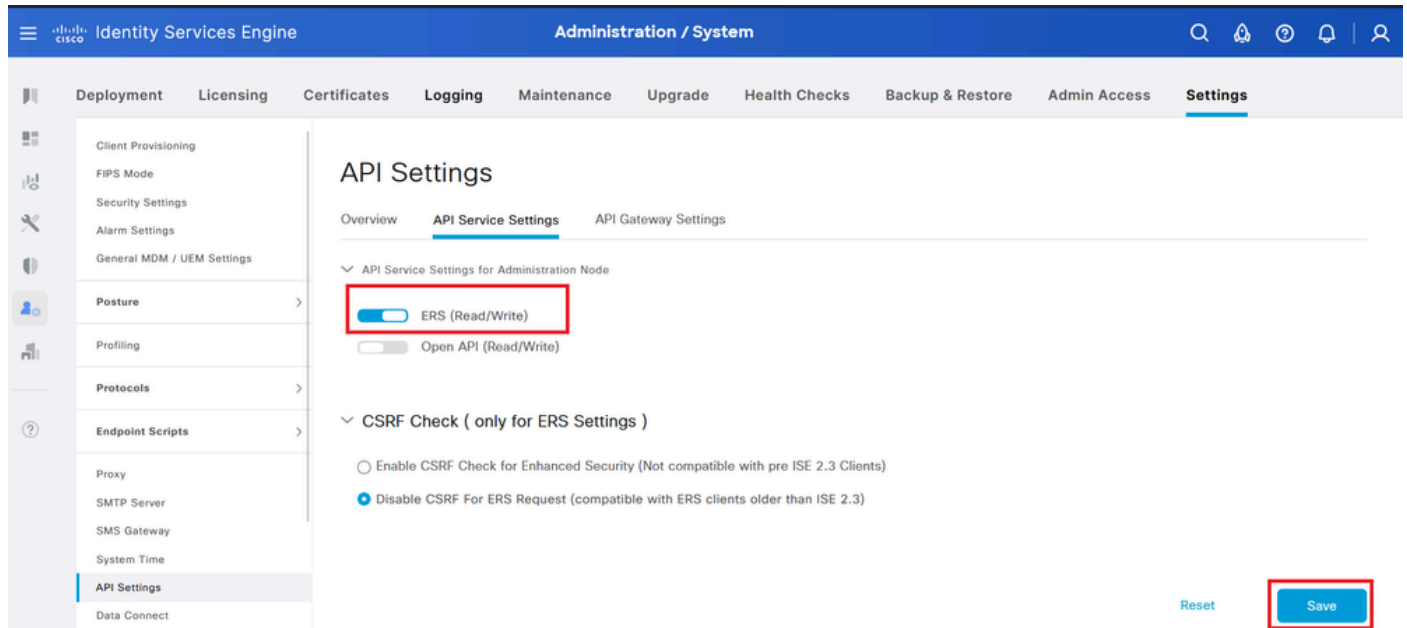
Configurations

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).

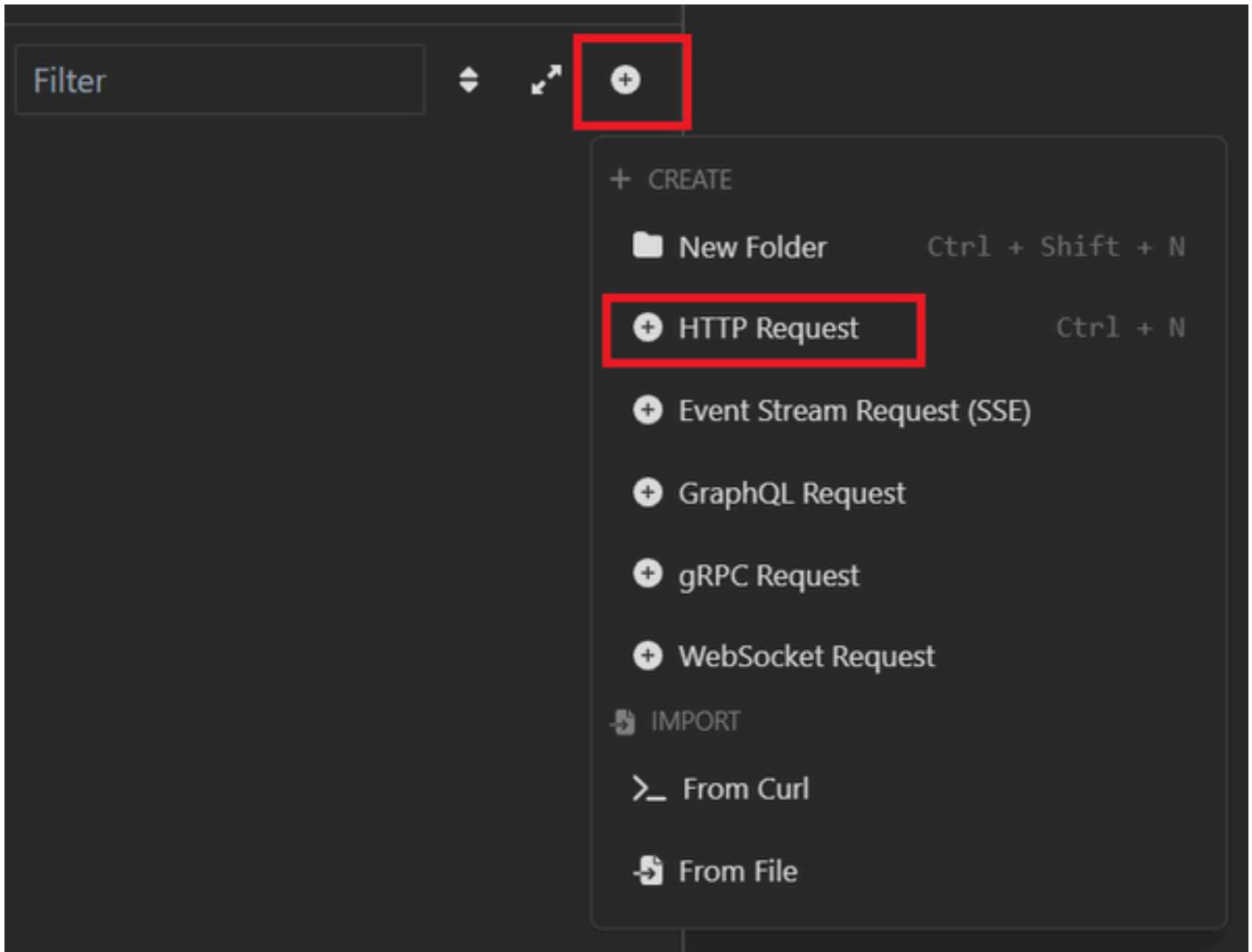


The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Administration / System' and various utility icons. The main menu on the left lists categories like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The 'Settings' section is expanded, showing a list of configuration areas including 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 (highlighted), 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.

Paramètres API

Demande JSON.

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

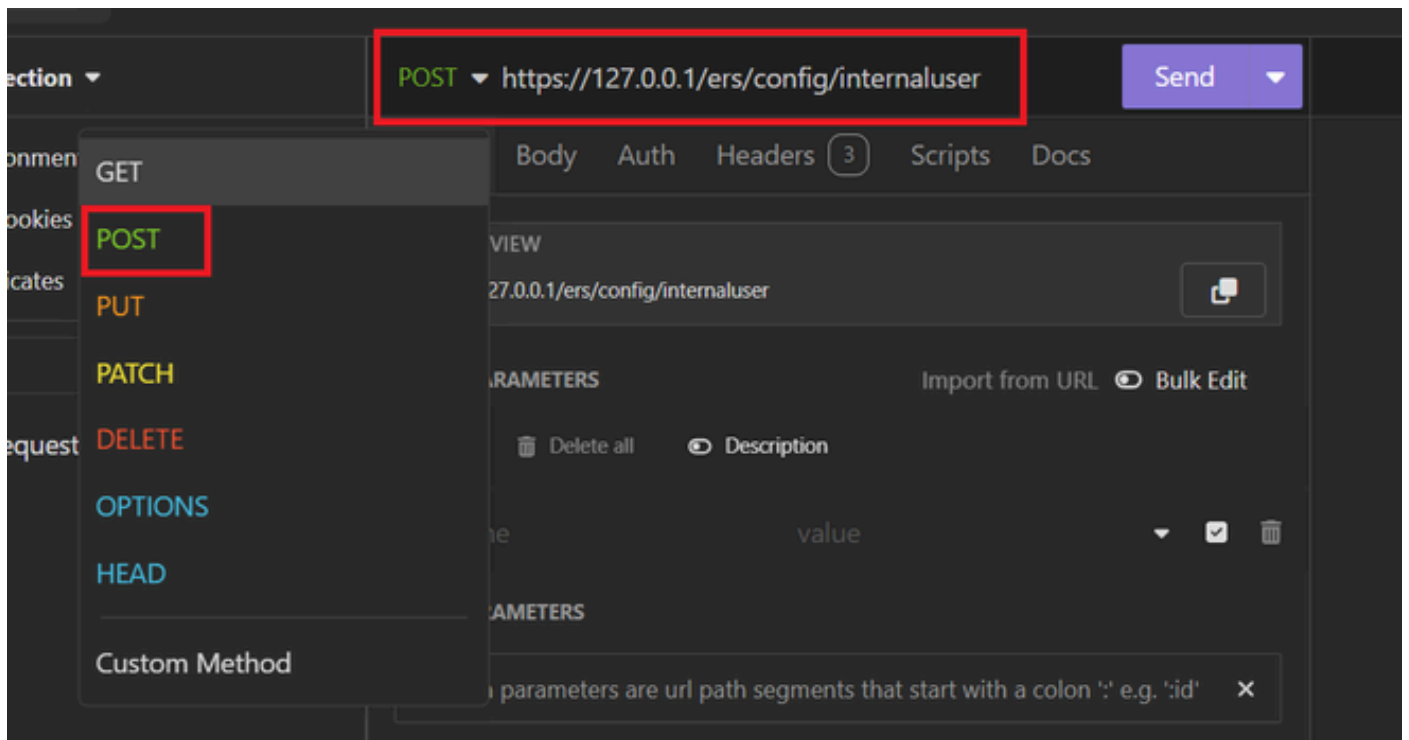


Demande JSON

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

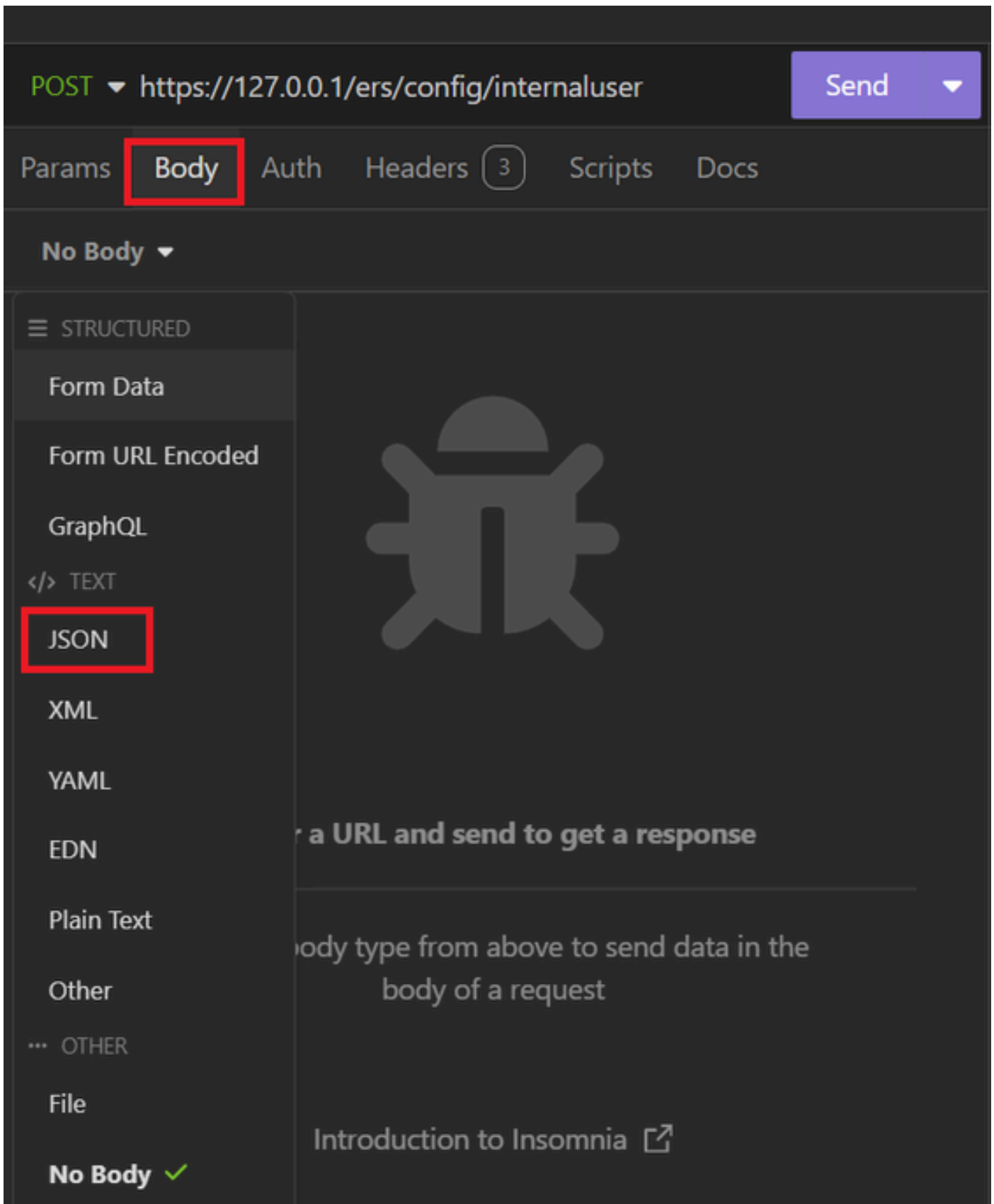
L'URL que vous devez entrer dépend de l'adresse IP de votre noeud ISE.

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.

```
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 }
```

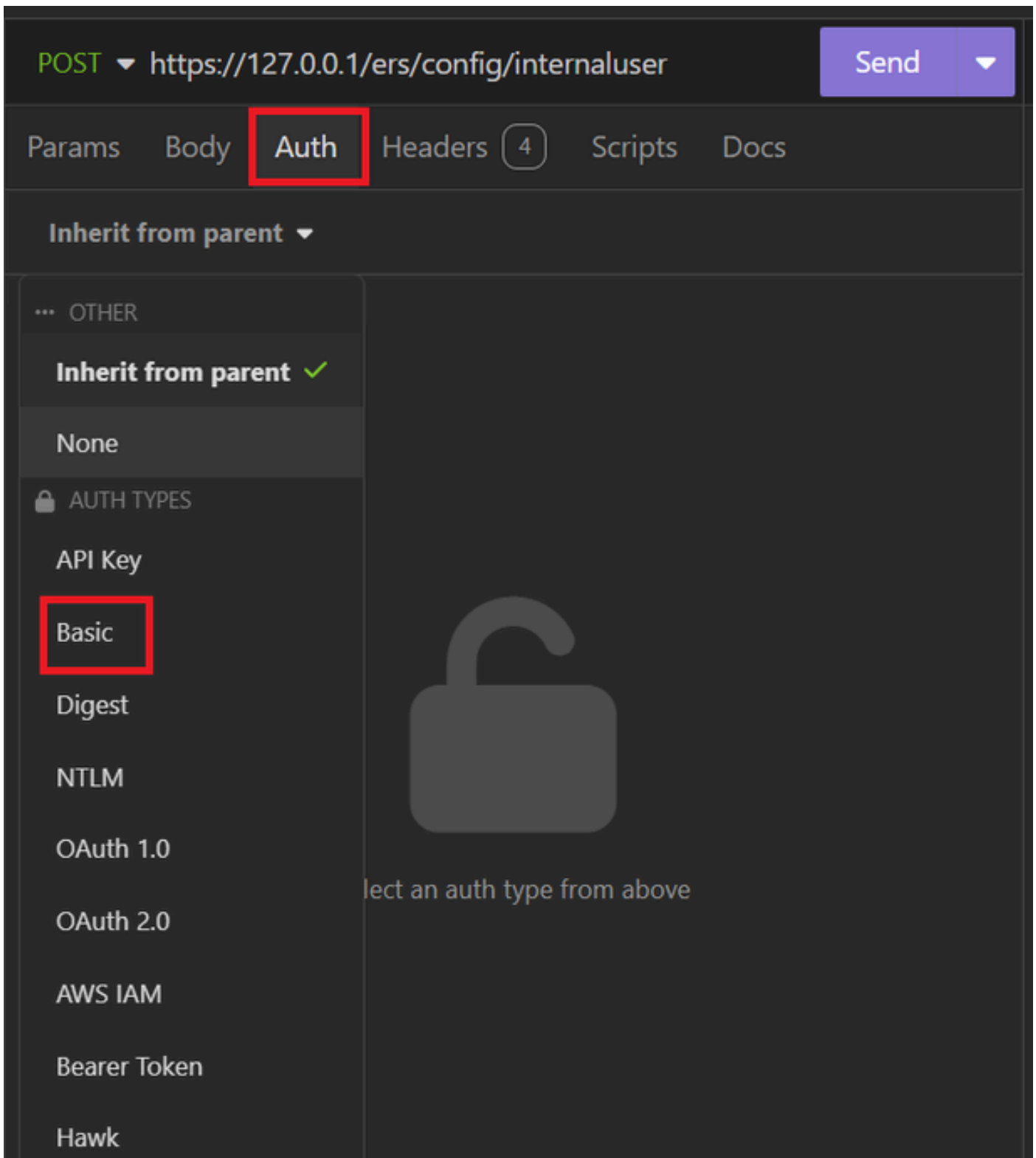
Syntaxe JSON

syntaxe JSON

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

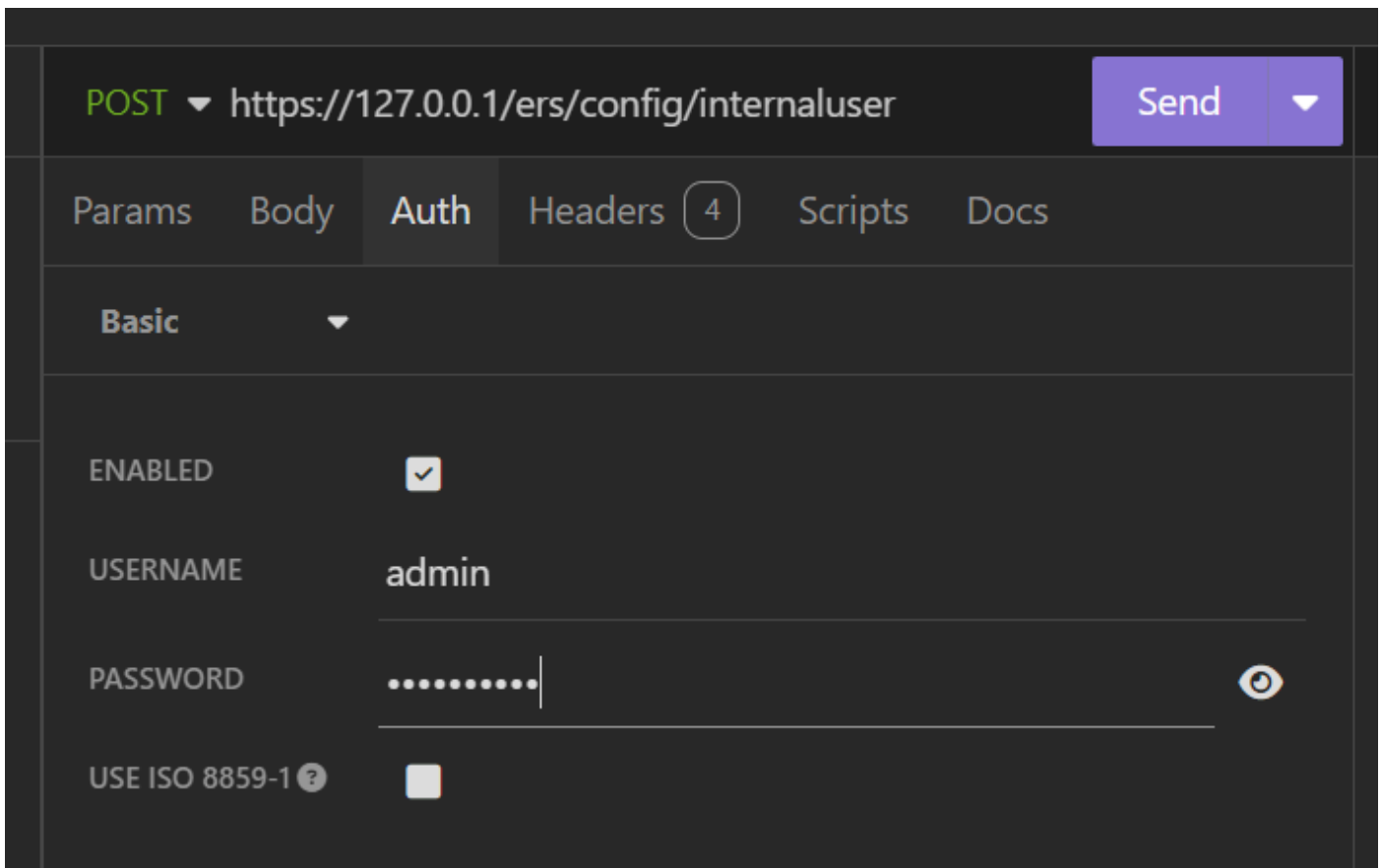
```
"password": "password",
"firstName": "firstName",
"lastName": "lastName",
"changePassword": true,
"identityGroups": "identityGroups",
"passwordNeverExpires": false,
"daysForPasswordExpiration": 60,
"expiryDateEnabled": false,
"expiryDate": "2016-12-11",
"enablePassword": "enablePassword",
"dateModified":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

6. Cliquez sur Auth et choisissez Basic.



Authentication 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

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	▼	☑	🗑

En-têtes JSON

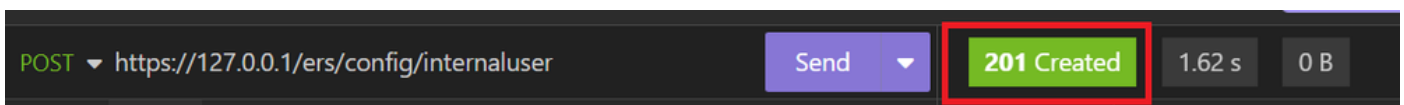
9. Enfin, cliquez sur Envoyer.



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

Administration / Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Res...

Edit Add Change Status Import Export Delete Duplicate

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
Enabled	User01	this is the firs...	User	Cisco	user1@local...	Employee	

Compte d'utilisateur JSON

Requête XML

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

Filter

+ CREATE

- New Folder Ctrl + Shift + N
- HTTP Request Ctrl + N**
- Event Stream Request (SSE)
- GraphQL Request
- gRPC Request
- WebSocket Request

IMPORT

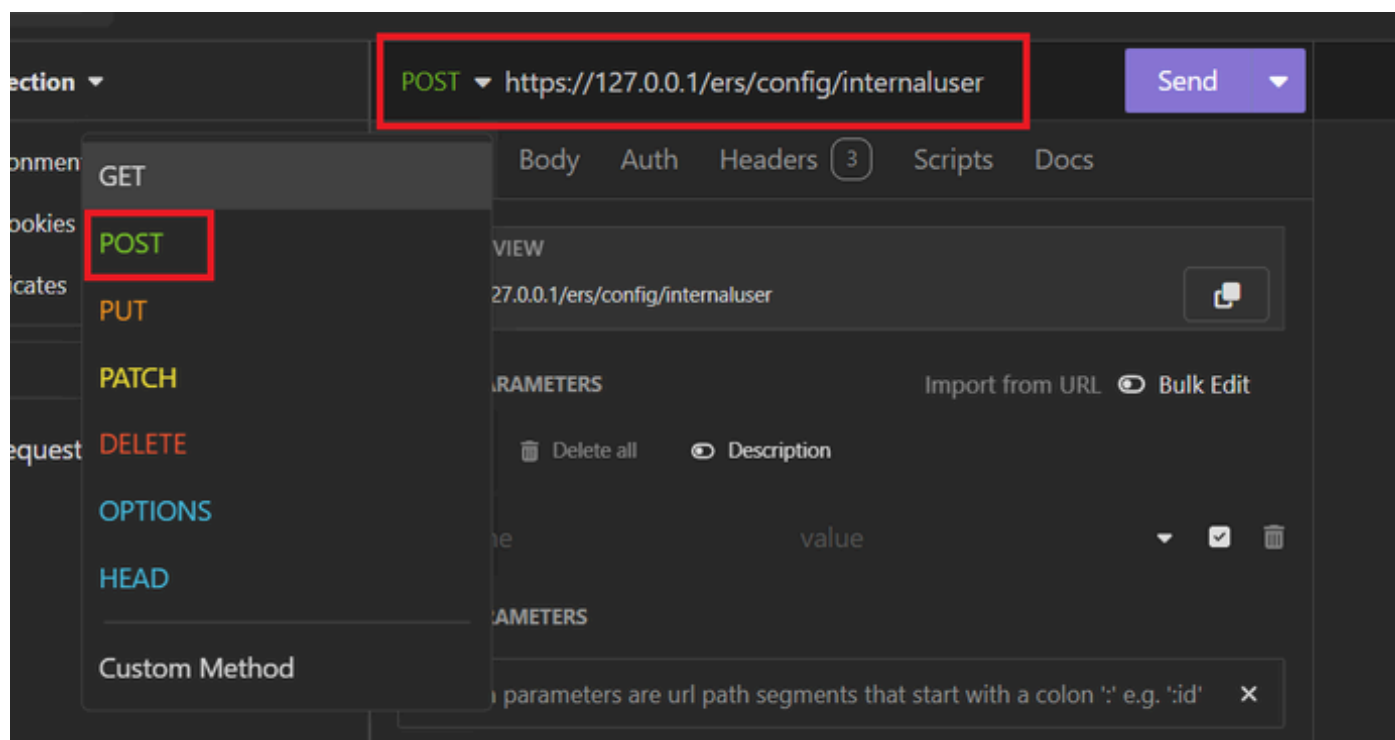
- From Curl
- From File

Requête XML

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

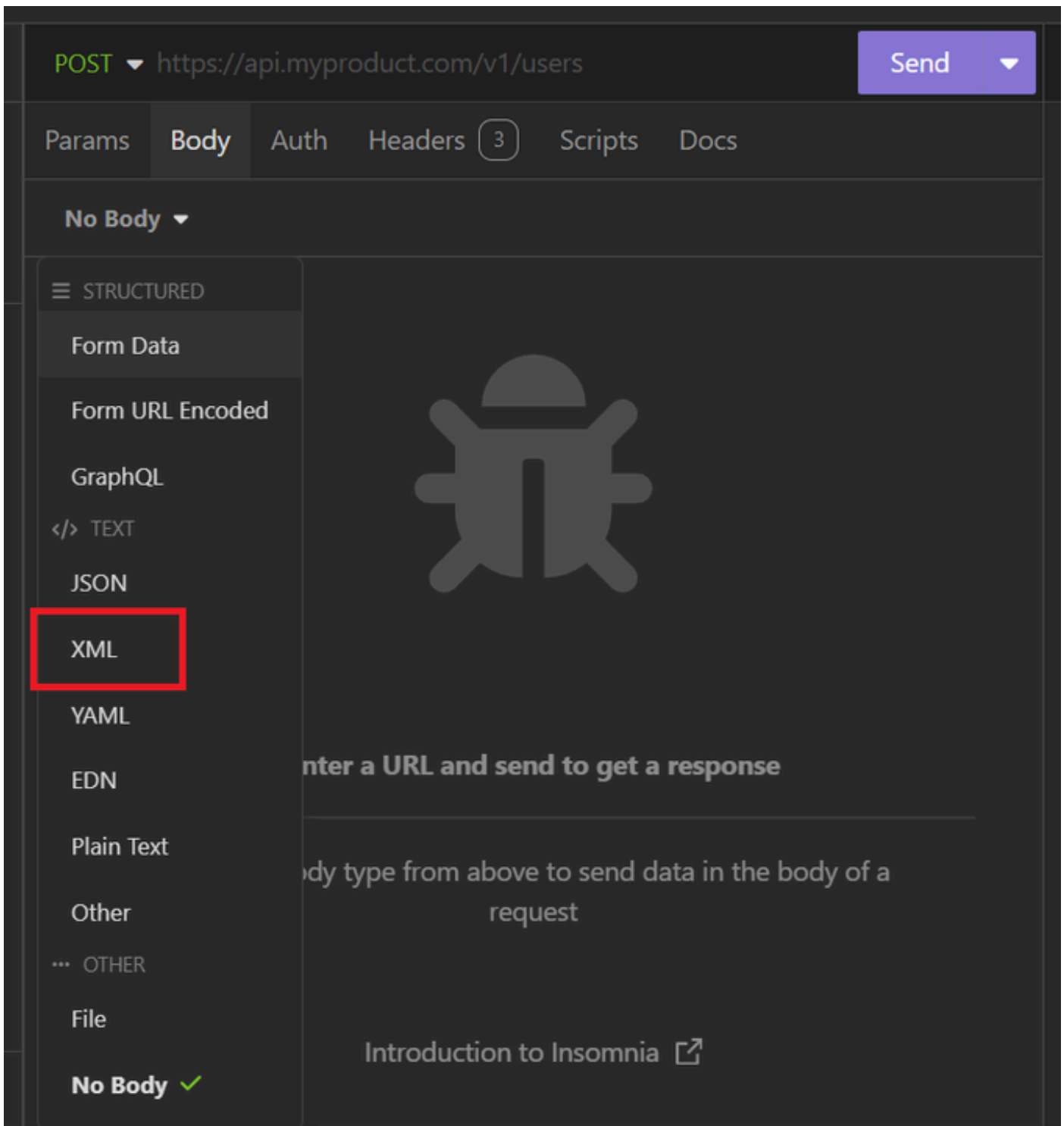
L'URL que vous devez entrer dépend de l'adresse IP de votre nœud ISE.

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.

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>

```

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>
```

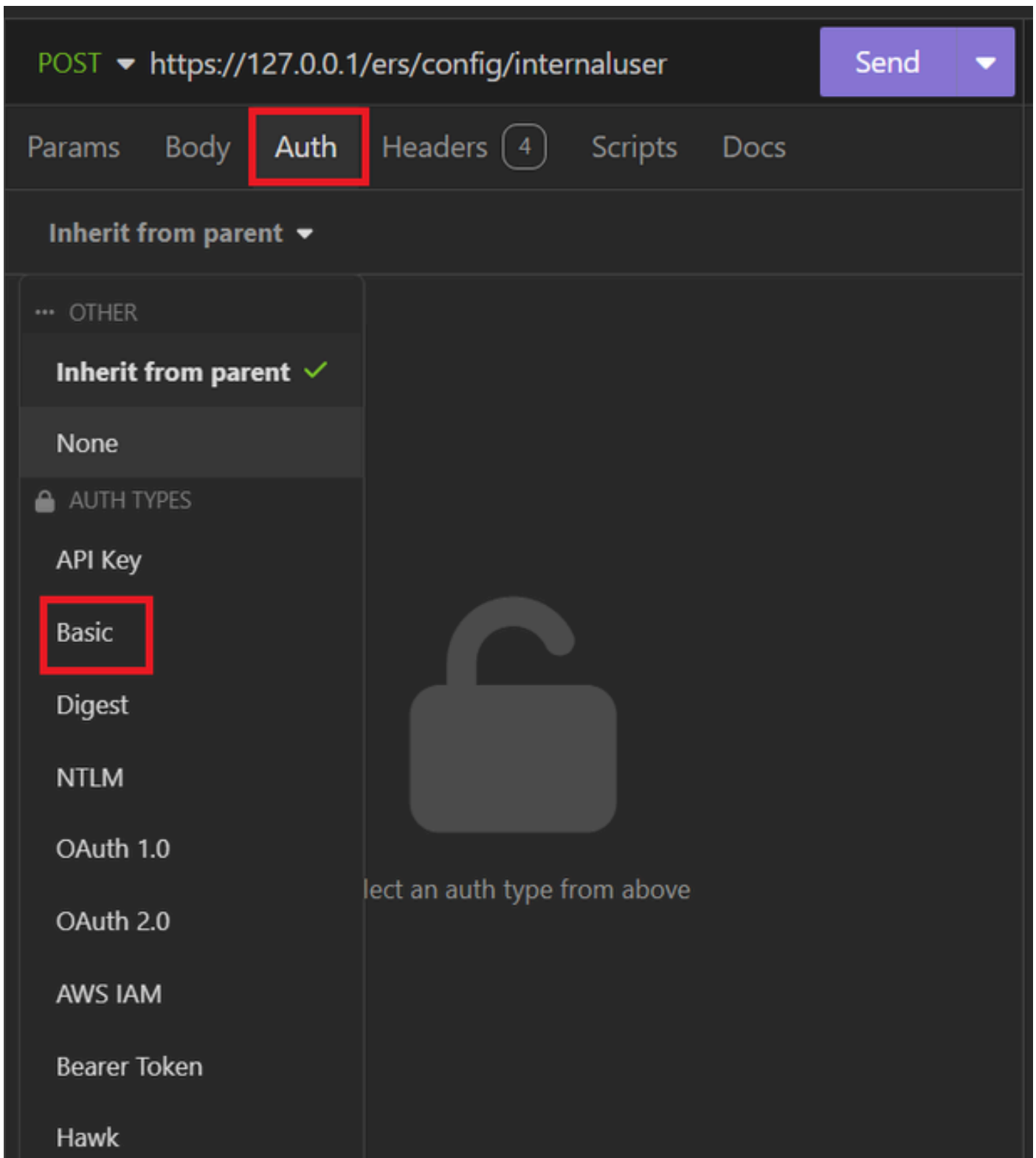
```
  <changePassword>true</changePassword>
```

```
  <customAttributes>
```



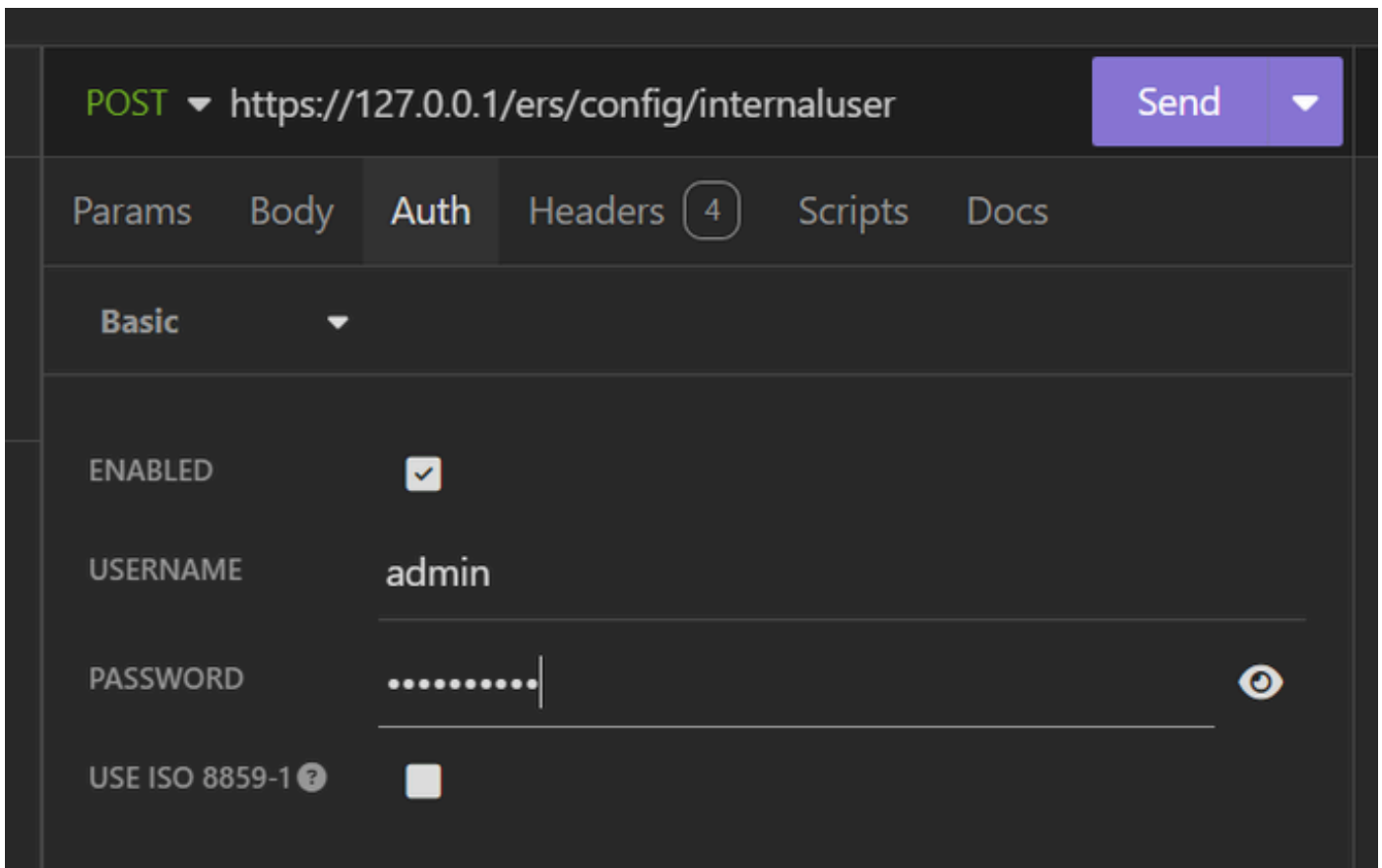
```
<entry>
  <key>key1</key>
  <value>value1</value>
</entry>
<entry>
  <key>key2</key>
  <value>value3</value>
</entry>
</customAttributes>
<dateCreated>2015-12-15</dateCreated>
<dateModified>2015-12-20</dateModified>
<daysForPasswordExpiration>60</daysForPasswordExpiration>
<email>email@domain.com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



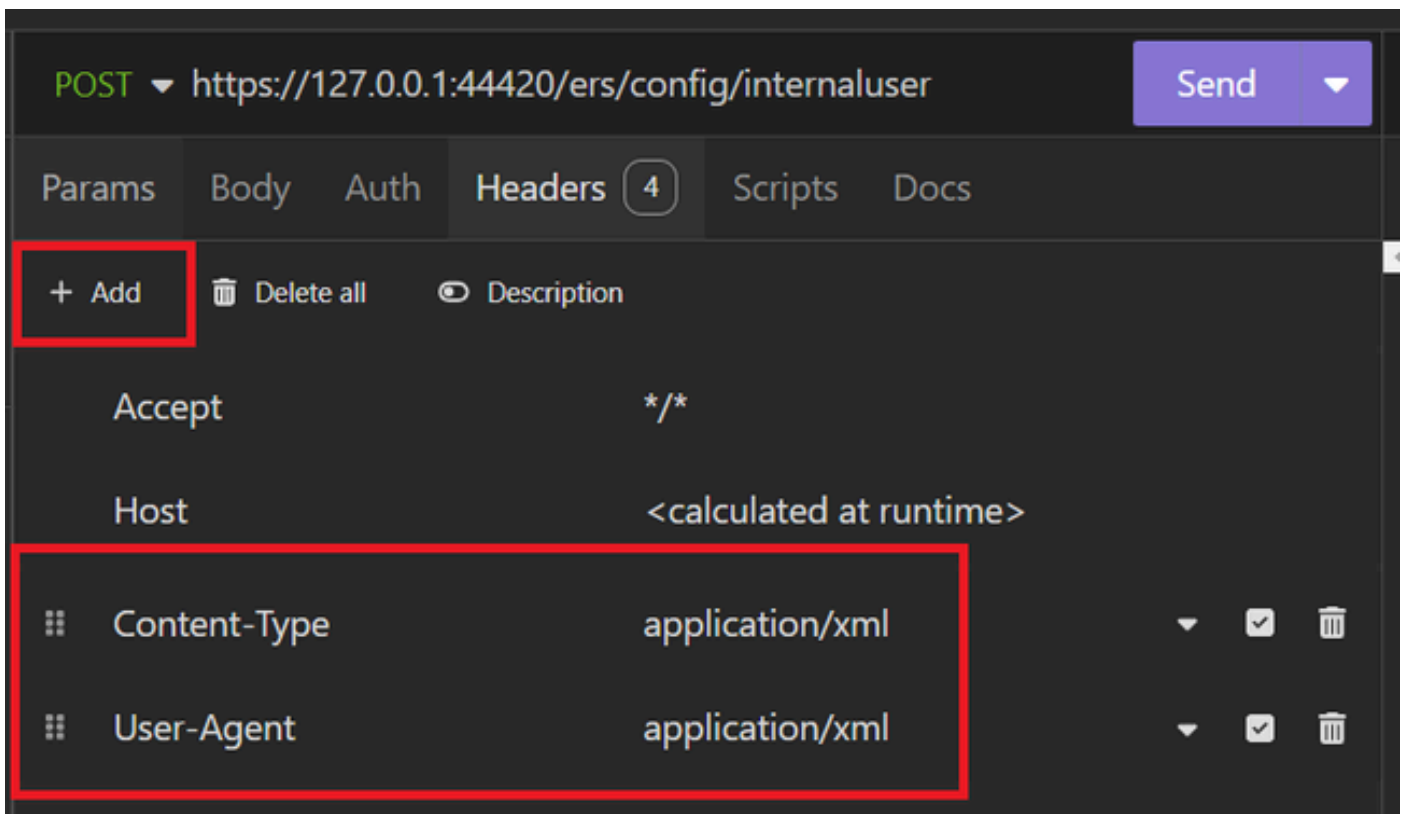
Authentication XML

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



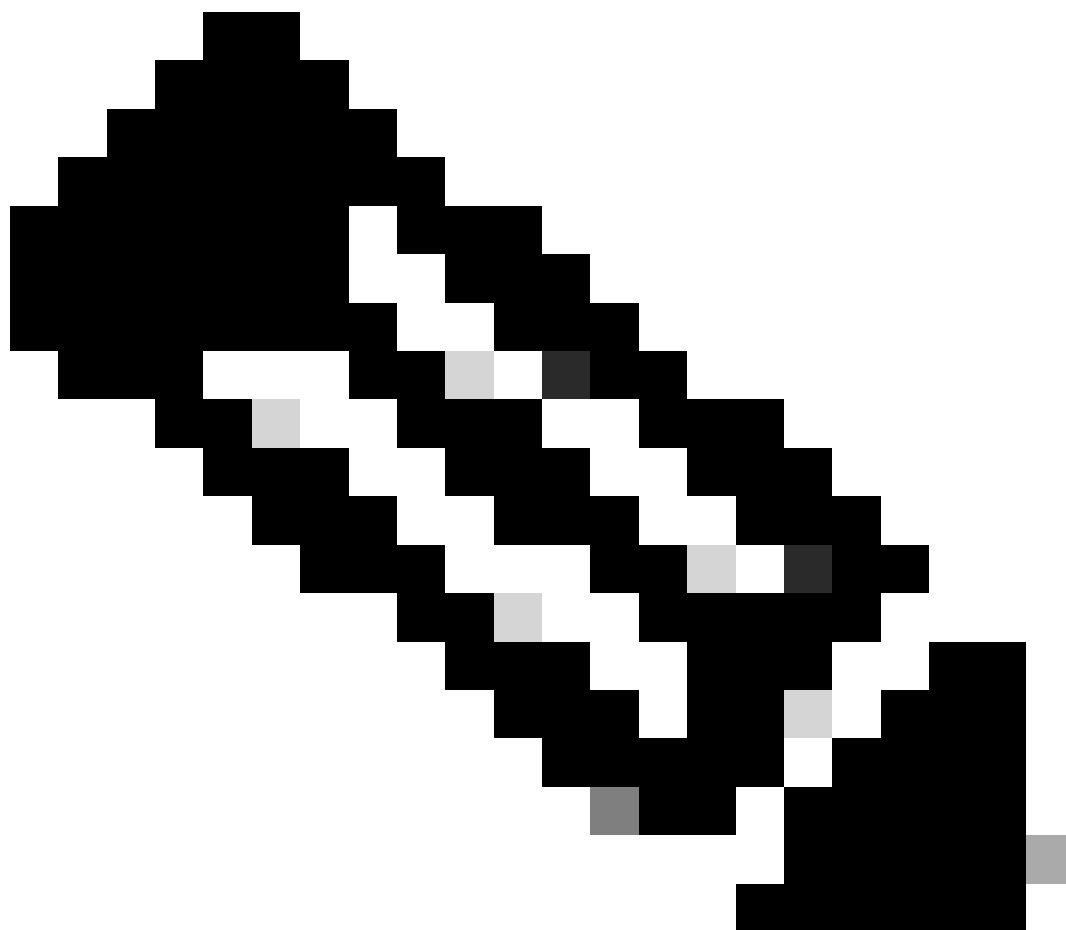
Informations d'identification XML

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



En-têtes XML

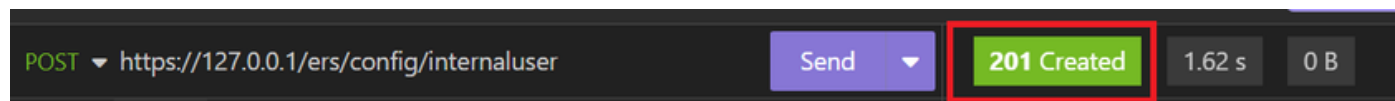
9. Enfin, cliquez sur Envoyer.



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

Network Access Users

Selected 0 Total 2  

 Edit  + Add  Change Status  Import  Export  Delete  Duplicate  All 

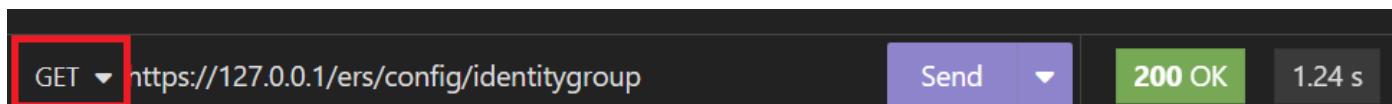
Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	 Enabled  User01	this is the firs...	User	Cisco	user1@local...	Employee	 User Account created by JSON
<input type="checkbox"/>	 Enabled  User02	description	User2	Cisco	user2@local...	Employee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

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.

```
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 groupe d'identité 01

Sortie XML.

Identifiez l'ID en regard de la description.

```
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 Identity Group 02

2. 401 Erreur non autorisée.

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

erreur 401

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

3. Erreur : Impossible de se connecter au serveur

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

Erreur de connexion

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

4. 400 Requête incorrecte.

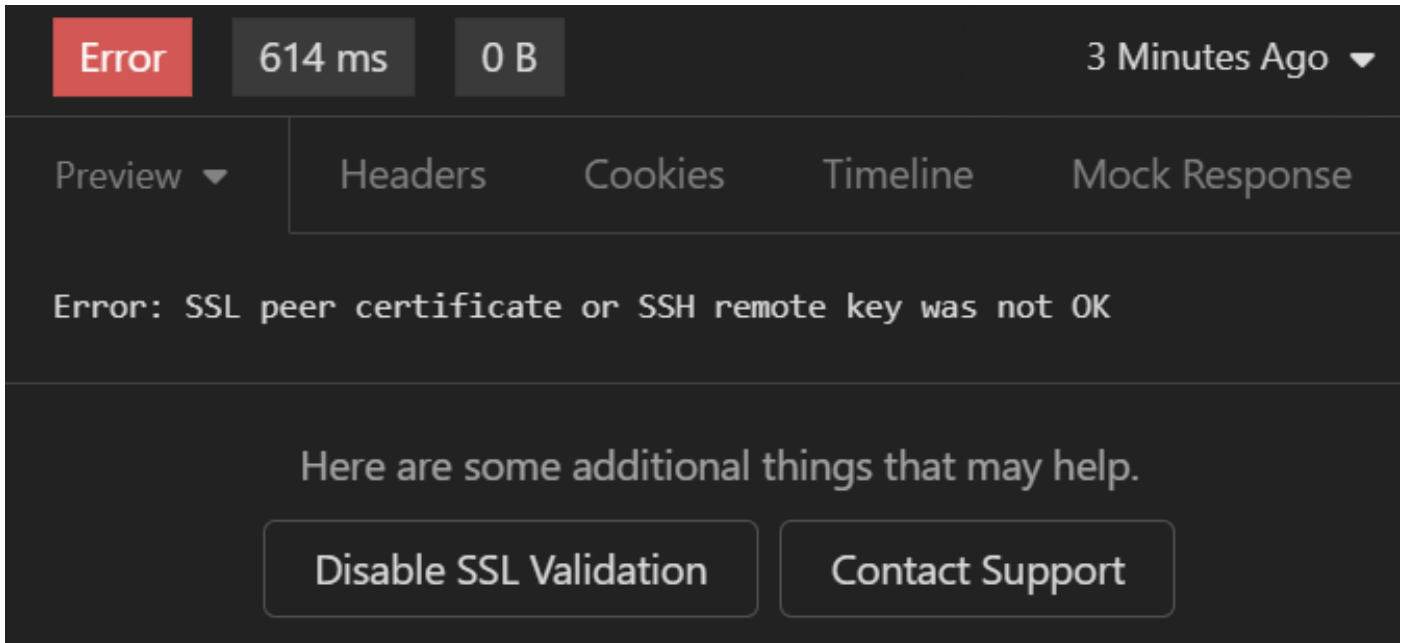
```
POST https://127.0.0.1/ers/config/internaluser Send 400 Bad Request
```

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 Syntaxis.
- Informations dupliquées.

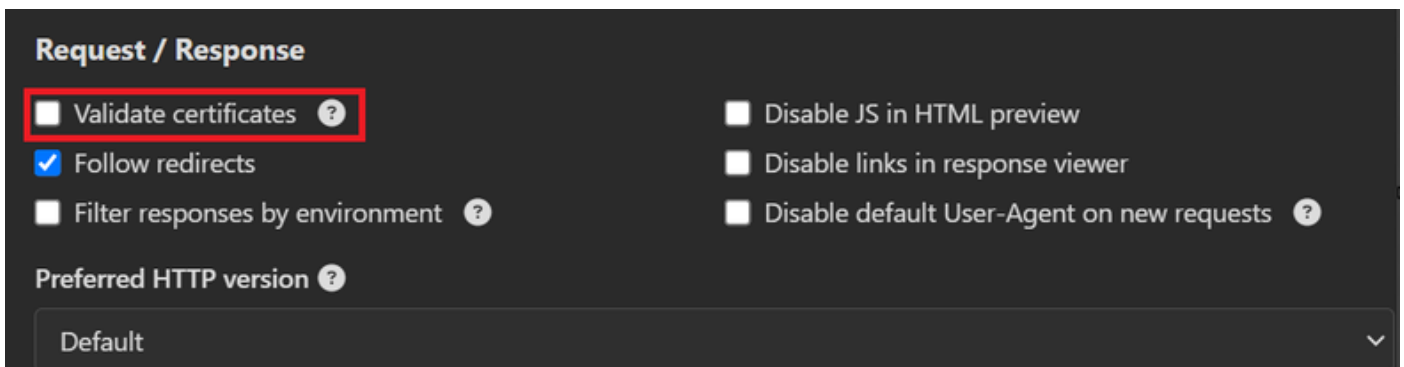
5. Erreur : le certificat d'homologue SSL ou la clé distante SSH n'était pas correct



Erreur de certificat SSL

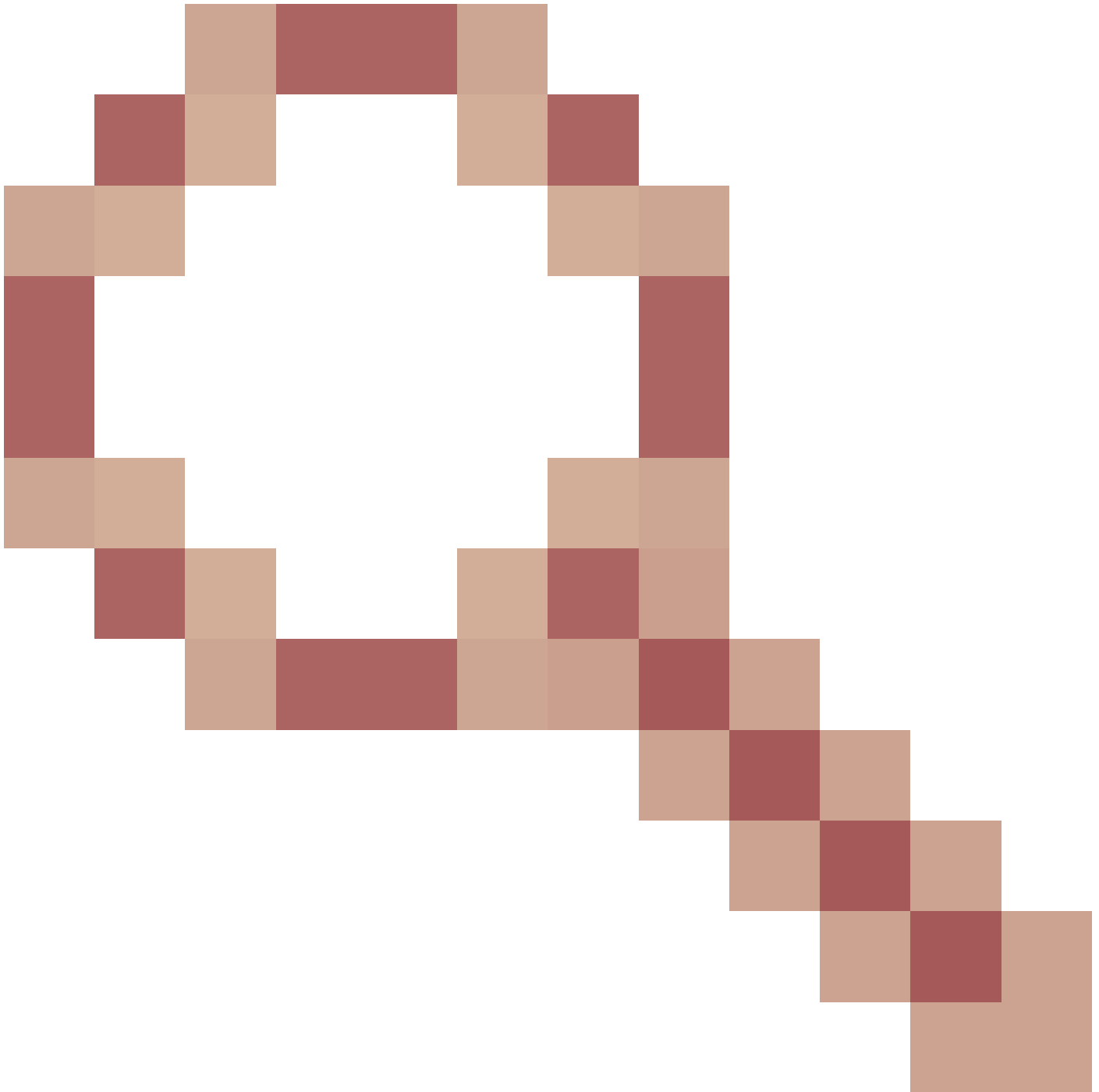
Solution :

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.

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 tabs for Overview, API Service Settings, and API Gateway Settings. The Overview tab is active, showing an 'API Services Overview' section. The text explains that Cisco ISE nodes can be managed through External Restful Services (ERS) and OpenAPI. It notes that starting with ISE Release 3.1, new APIs are available in the OpenAPI format. ERS and OpenAPI services are HTTPS-only REST APIs that operate over port 443. Currently, ERS APIs also operate over port 9060, but port 9060 might not be supported for ERS APIs in later releases. Both API services are disabled by default. A red box highlights a link for more information on ISE ERS API: <https://127.0.0.1:44421/ers/sdk>. Below this, there is a link for OpenAPI documentation: <https://127.0.0.1:44421/api/swagger-ui/index.html>.

Paramètres API

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

The screenshot shows the 'External RESTful Services (ERS) Online SDK' documentation page. The left sidebar has a 'Quick Reference' section with a red box around 'API Documentation'. Below it is a list of release notes for ISE versions 2.0 through 3.3, with 'ISE 3.3 Release Notes' highlighted. The main content area is titled 'ISE 3.3 Release Notes' and has a section for 'New / Modified Resources'. Below this is a table with the following data:

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

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.