

Insominiaを使用したISE 3.3でのJSONまたはXMLおよびAPIコールによる内部ユーザの設定

内容

はじめに

このドキュメントでは、APIコールと組み合わせてJSONまたはXMLデータ形式を活用することにより、Cisco ISEの内部ユーザを設定する方法について説明します。

前提条件

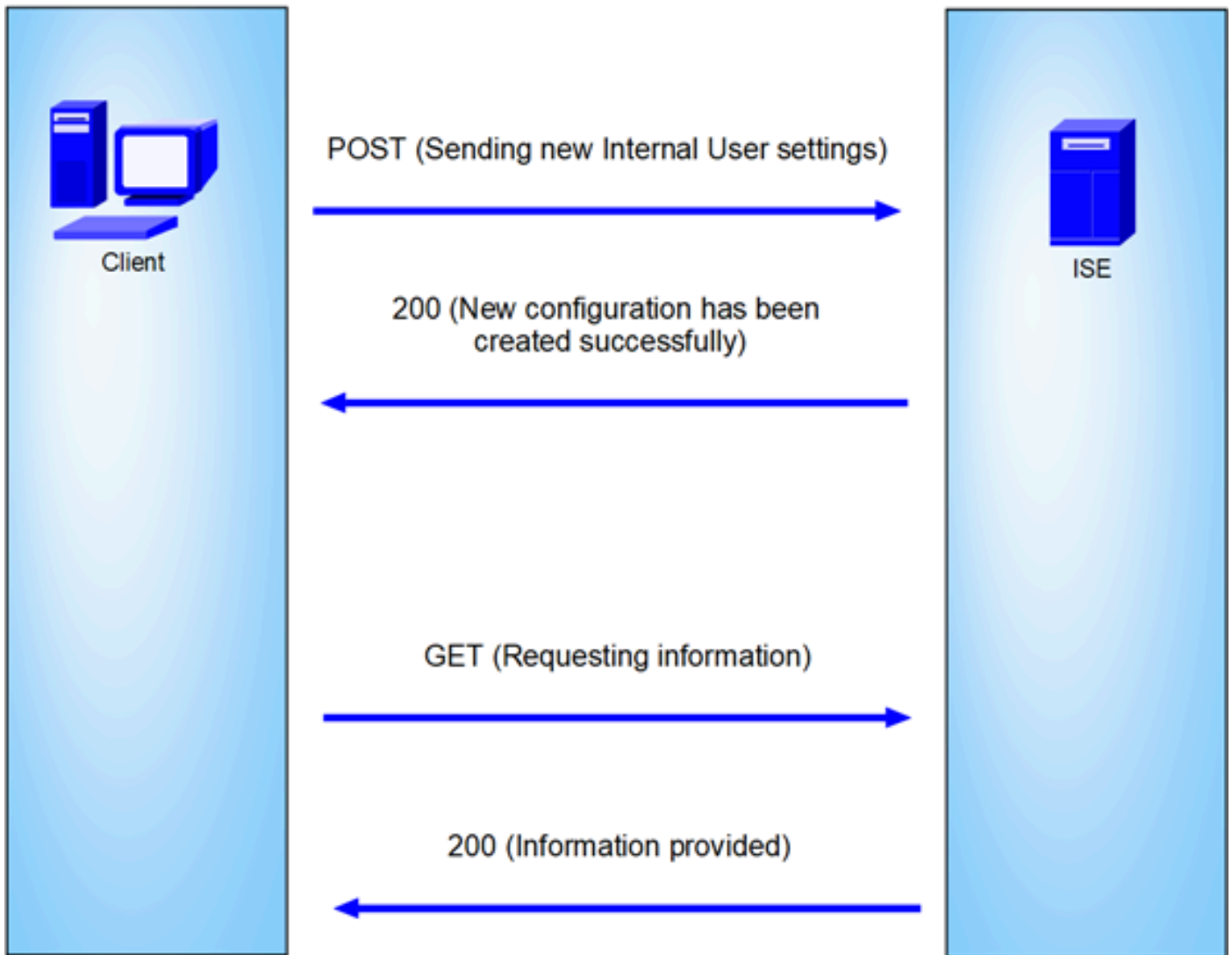
- ISE 3.0以降。
- APIクライアントソフトウェア。

使用するコンポーネント

- ISE 3.3
- Insominia 9.3.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ネットワーク図



一般的なトポロジ

GETとPOSTは、API (アプリケーションプログラミングインターフェイス) 呼び出しで使用される最も一般的なHTTPメソッドの2つです。サーバ上のリソースとの対話に使用され、通常はデータを取得したり、処理のためにデータを送信したりします。

GET APIコール

GETメソッドは、指定されたリソースからデータを要求するために使用します。GET要求は、APIおよびWebサイトで最も一般的で広く使用されているメソッドです。Webページにアクセスすると、ブラウザはWebページをホストしているサーバに対してGET要求を行います。

POST APIコール

POSTメソッドは、リソースを作成または更新するためにサーバにデータを送信するために使用します。POST要求は、フォームデータの送信やファイルのアップロードによく使用されます。

。

コンフィギュレーション

内部ユーザを作成するには、APIクライアントソフトウェアからISEノードに正確な情報を送信する必要があります。

ISEの設定

ERS機能を有効にします。

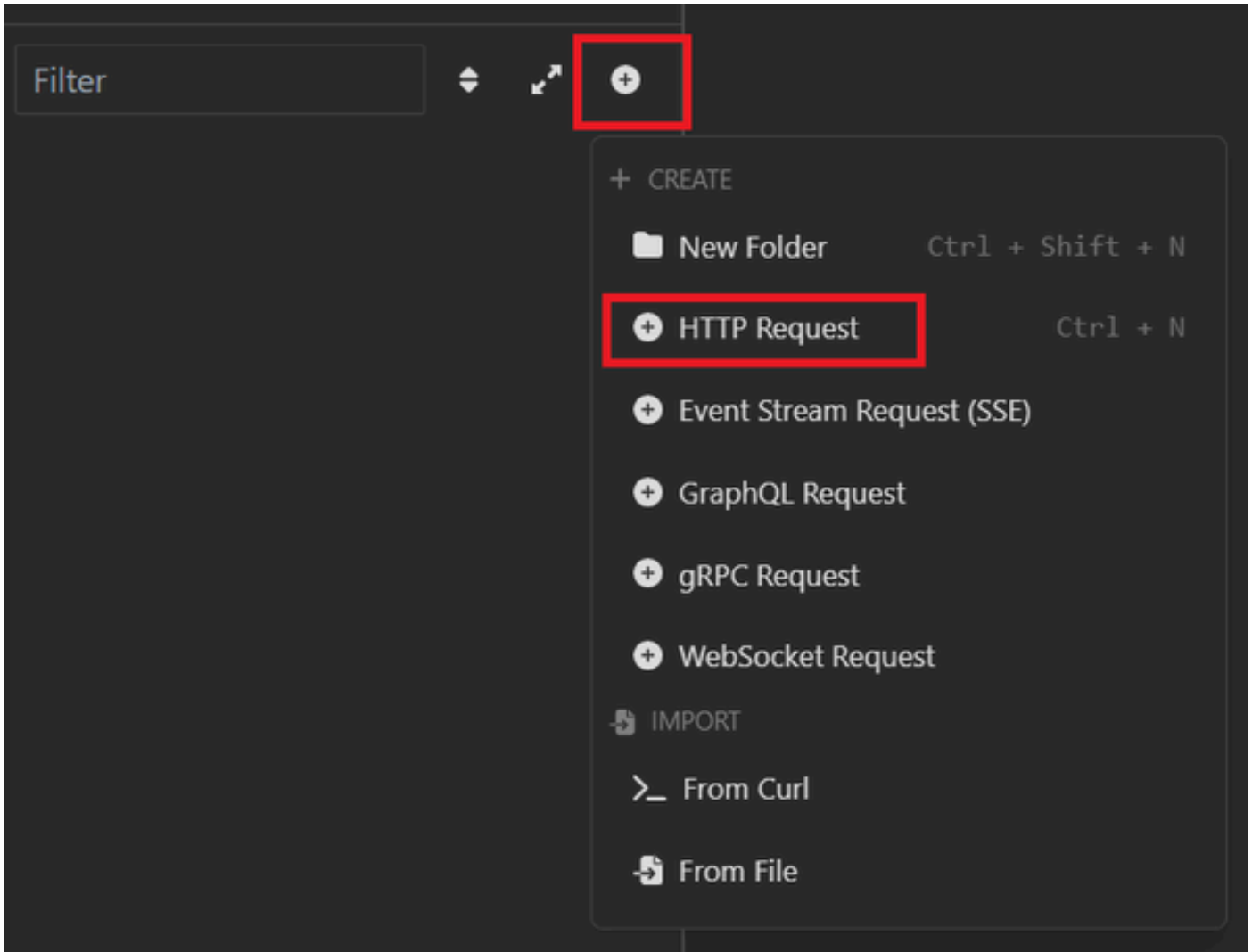
1. [管理] > [システム] > [設定] > [API設定] > [APIサービス設定]に移動します。
2. ERS (読取り/書込み) オプションを使用可能にします。

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System Settings page. The page is titled "API Settings" and has three tabs: "Overview", "API Service Settings", and "API Gateway Settings". The "API Service Settings" tab is active. Under the "API Service Settings for Administration Node" section, the "ERS (Read/Write)" toggle switch is turned on and highlighted with a red box. Below it, the "Open API (Read/Write)" toggle switch is turned off. Under the "CSRF Check (only for ERS Settings)" section, the "Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)" radio button is selected. At the bottom right of the page, there are "Reset" and "Save" buttons, with the "Save" button highlighted with a red box.

API設定

JSON要求。

1. オープン不眠症。
2. 左側に新しいHTTPS要求を追加します。

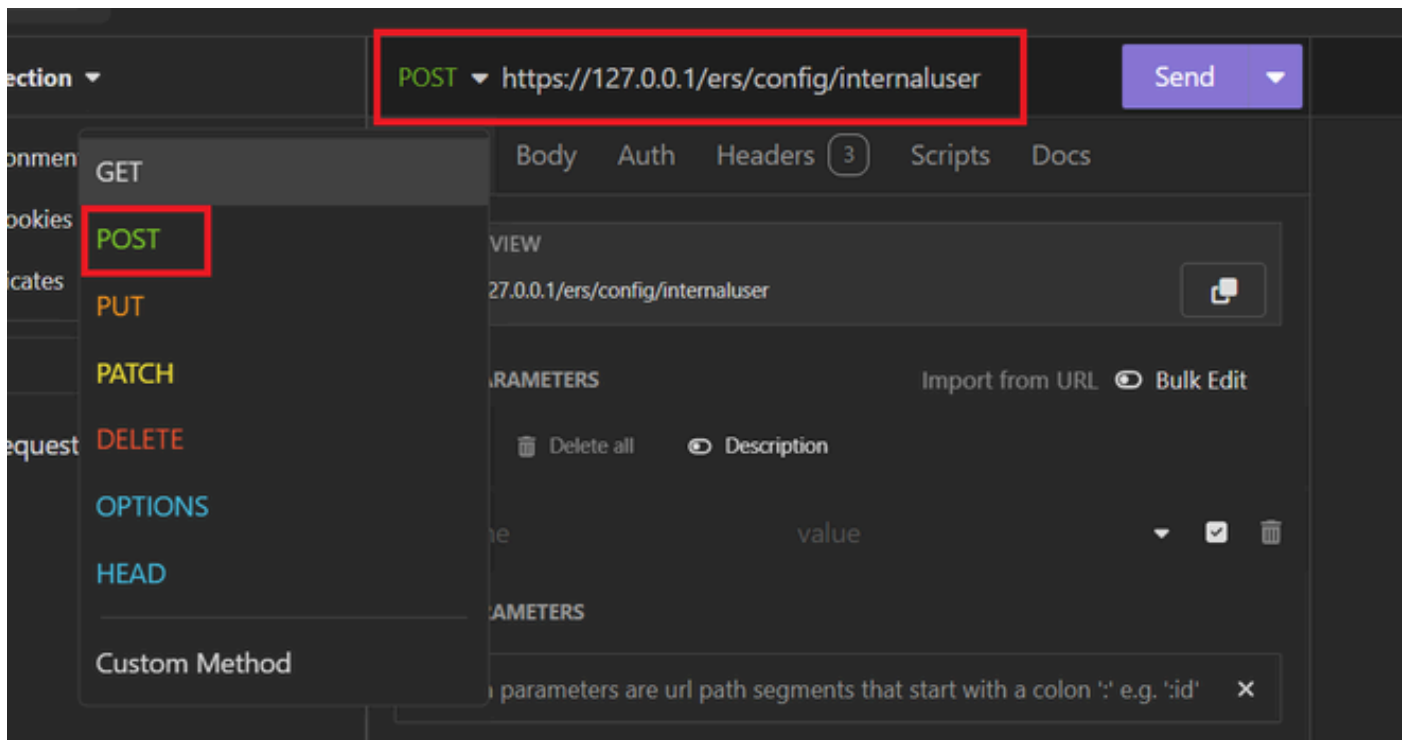


JSON要求

3. ISEノードに情報を送信するには、POSTを選択する必要があります。

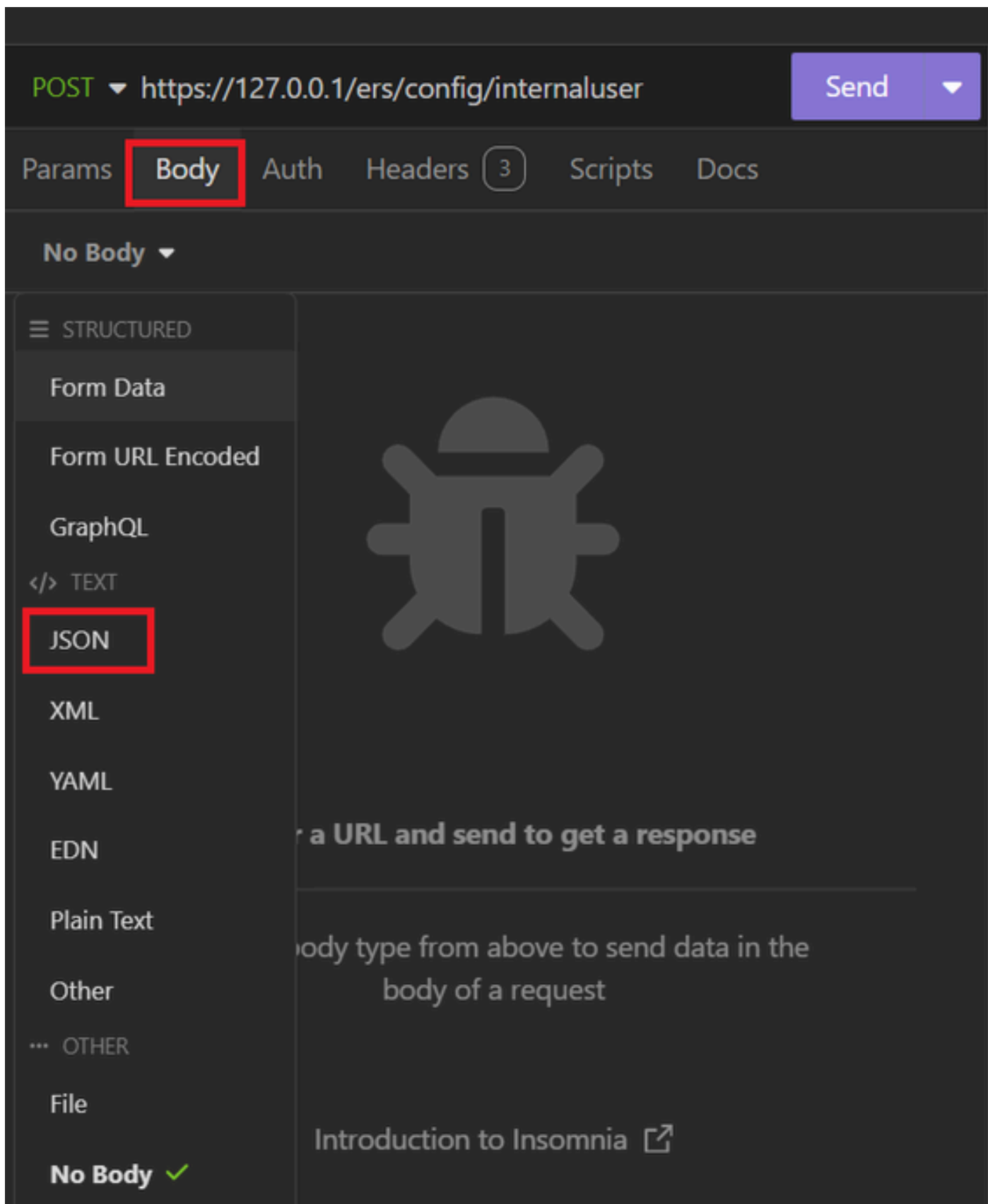
入力する必要があるURLは、ISEノードのIPアドレスによって異なります。

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



JSON投稿

4. Bodyをクリックし、JSONを選択します



JSON本文

5. 構文を貼り付けて、必要に応じてパラメータを変更できます。

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 }
```

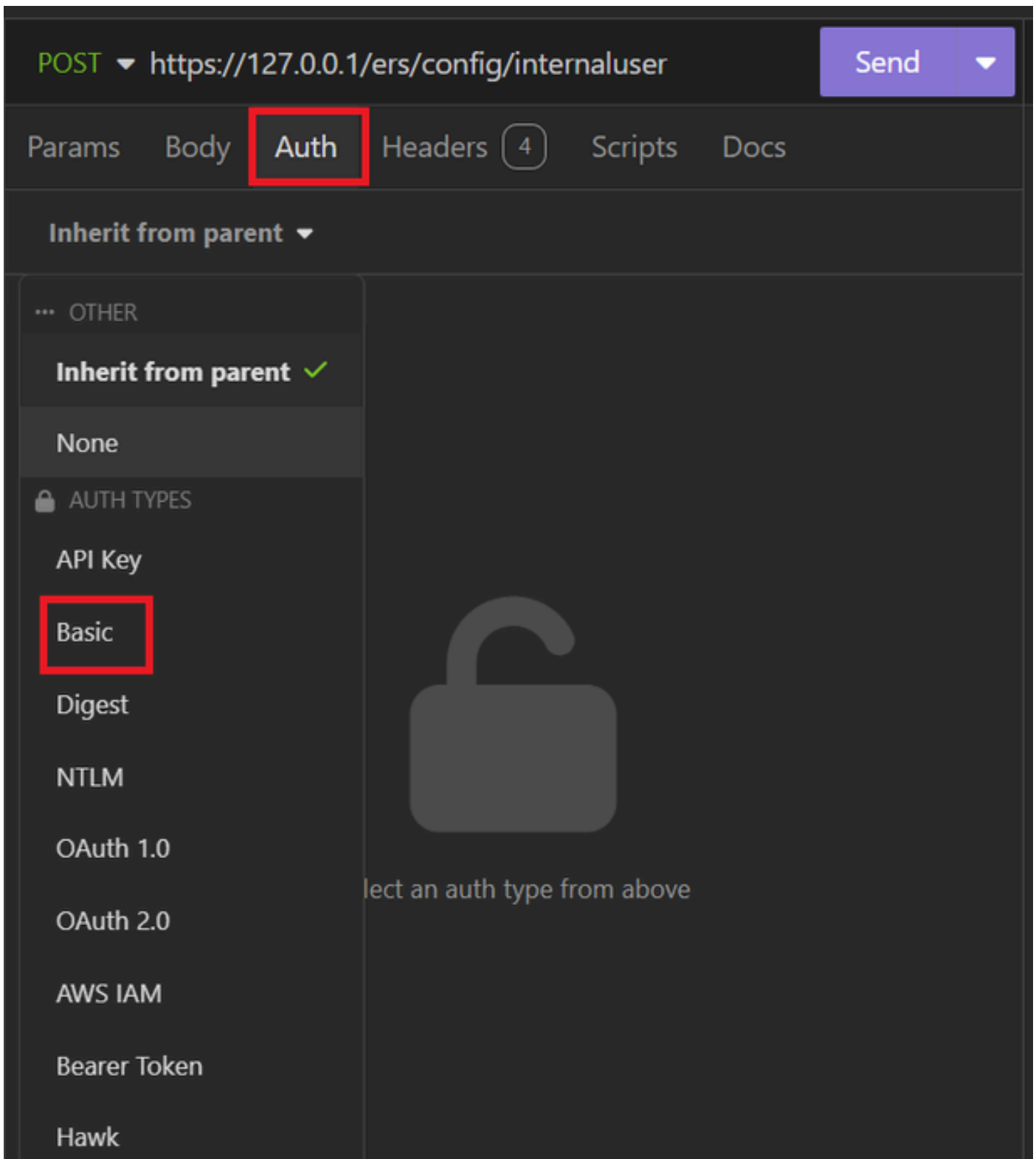
JSON構文

JSON構文

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

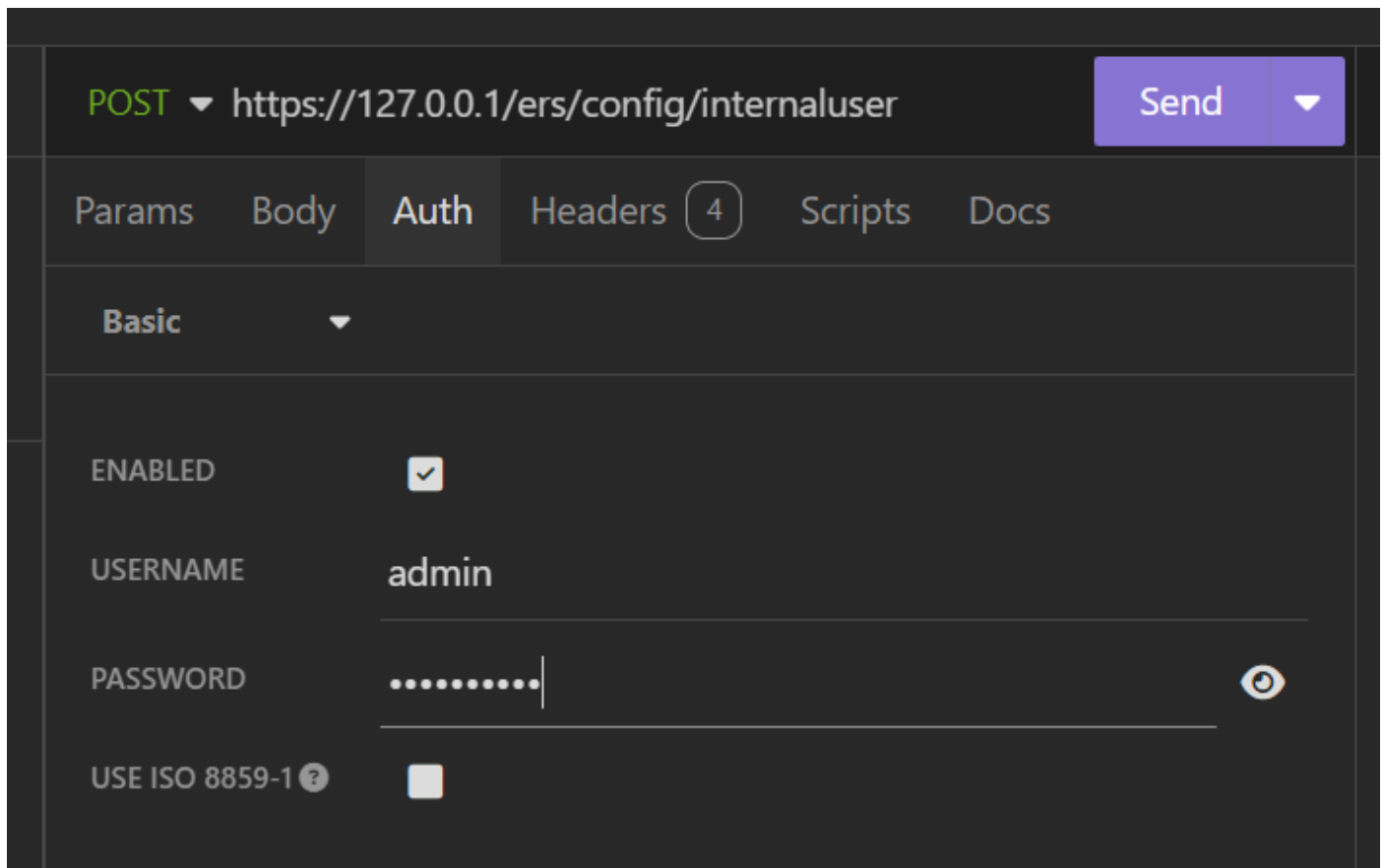
```
"password": "password",
"firstName": "firstName",
"lastName": "lastName",
"changePassword": true,
"identityGroups": "identityGroups",
"passwordNeverExpires": false,
"daysForPasswordExpiration": 60,
"expiryDateEnabled": false,
"expiryDate": "2016-12-11",
"enablePassword": "enablePassword",
"dateModified":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

6. Authをクリックし、Basicを選択します。



JSON認証

7. ISE GUIクレデンシャルを入力します。



管理者JSON資格情報

8. 「ヘッダー」をクリックして、次のメソッドを追加します。
 - Content-Type:application/json
 - 許可 : アプリケーション/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	▼	☑	🗑

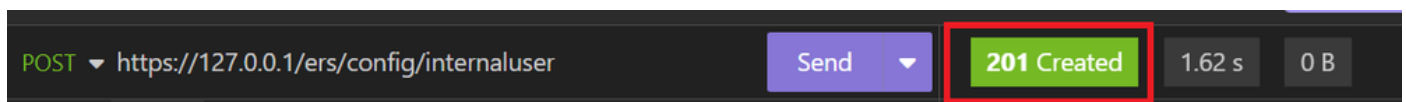
JSONヘッダー

9. 最後に、Sendをクリックします。

注：新しいユーザアカウントにIDグループを割り当てる場合は、そのIDを使用する必要があります。詳細については、「トラブルシューティング」の項を参照してください。

検証

1. POST要求を送信すると、「201 Created」というステータスが表示されます。これは、プロセスが正常に完了したことを意味します。



成功したJSON要求

2. ISE GUIを開き、Administration > Identity Management > Identities > Users > Network Access Usersの順に移動します

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

JSONユーザーアカウント

XML要求

1. オープン不眠症。
2. 左側に新しいHTTPS要求を追加します。

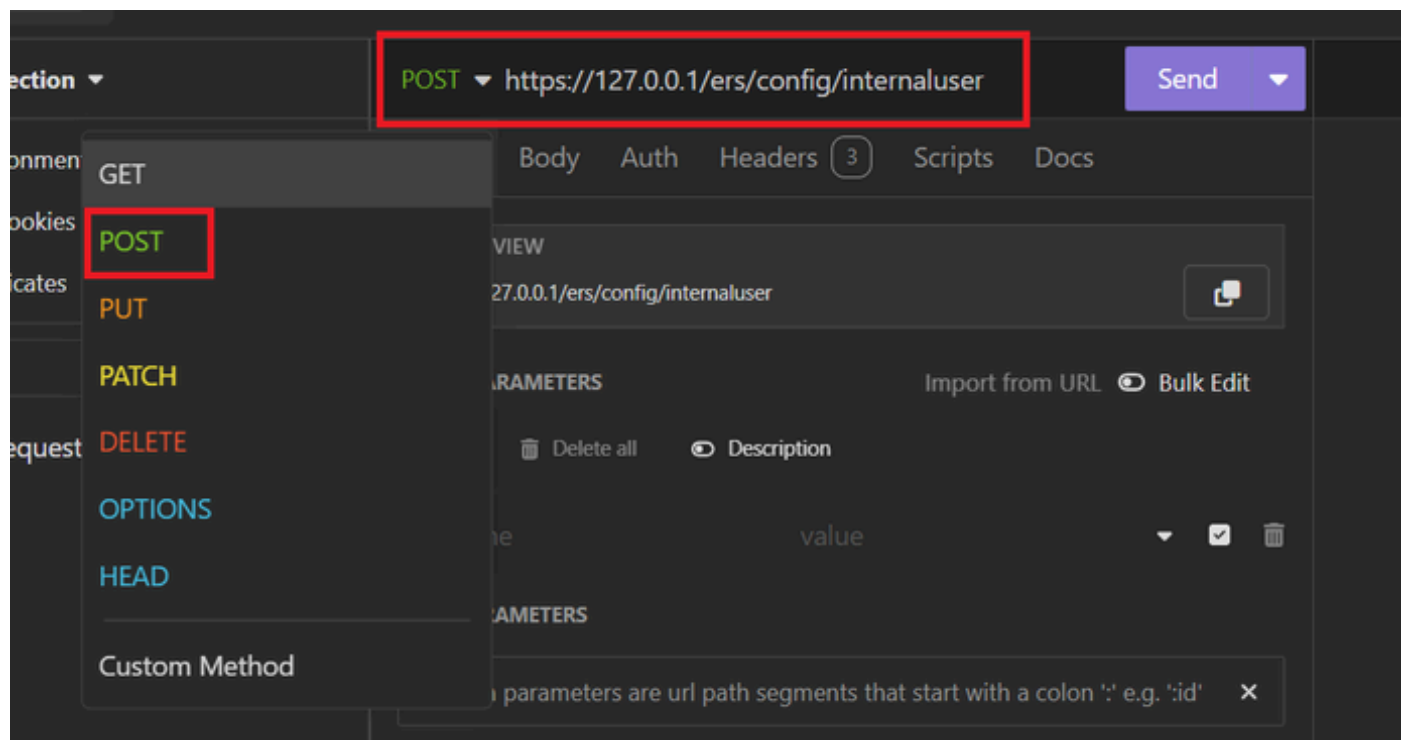
- + CREATE
 - New Folder (Ctrl + Shift + N)
 - HTTP Request (Ctrl + N)**
 - Event Stream Request (SSE)
 - GraphQL Request
 - gRPC Request
 - WebSocket Request
- IMPORT
 - From Curl
 - From File

XML要求

3. ISEノードに情報を送信するには、POSTを選択する必要があります。

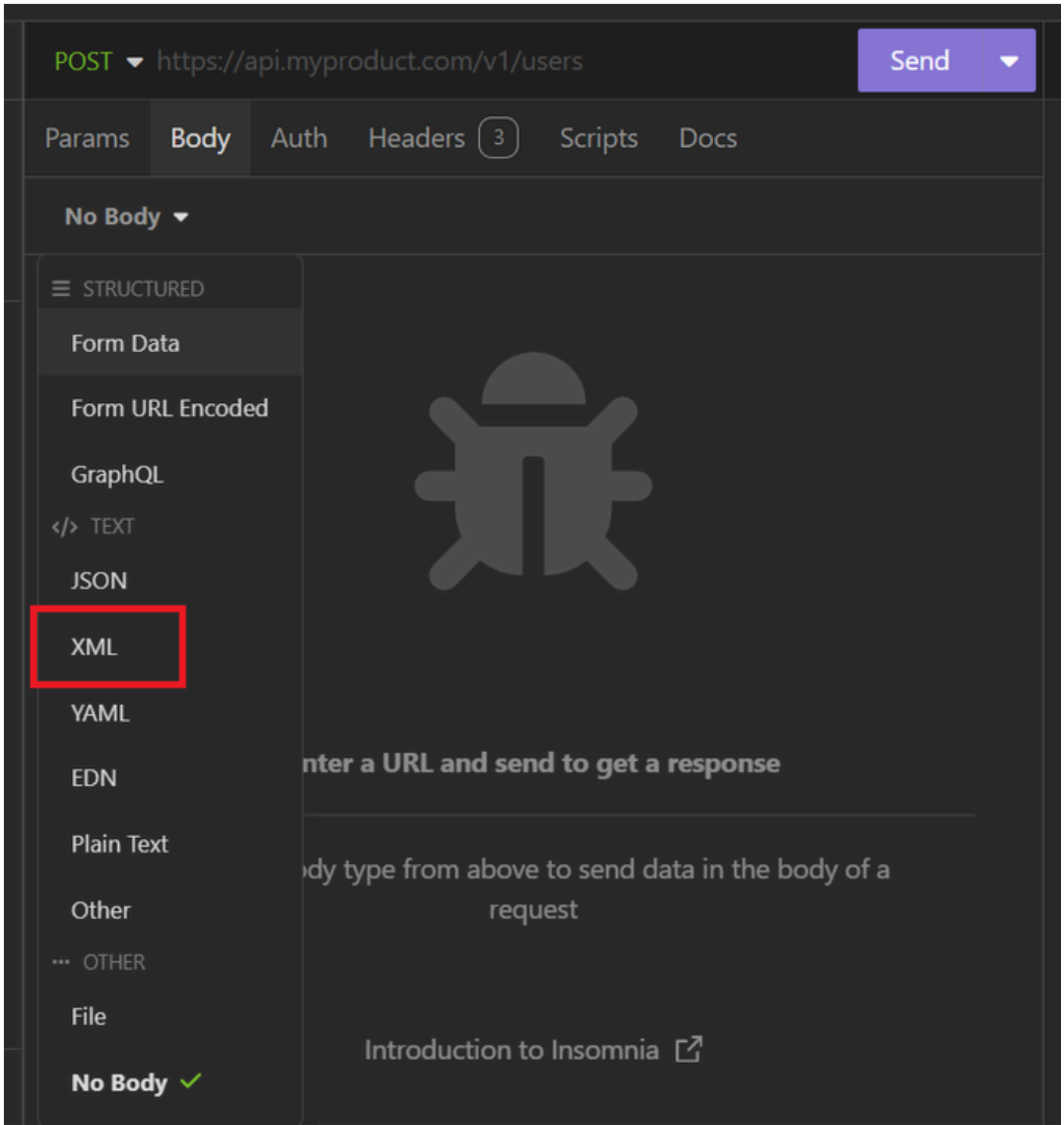
入力する必要があるURLは、ISEノードのIPアドレスによって異なります。

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



XML投稿

4. 次に、BodyをクリックしてXMLを選択します。



XML本文

5. 構文を貼り付けて、必要に応じてパラメータを変更できます。

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>
```

XML 投稿

XML 構文

```
<?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>
```

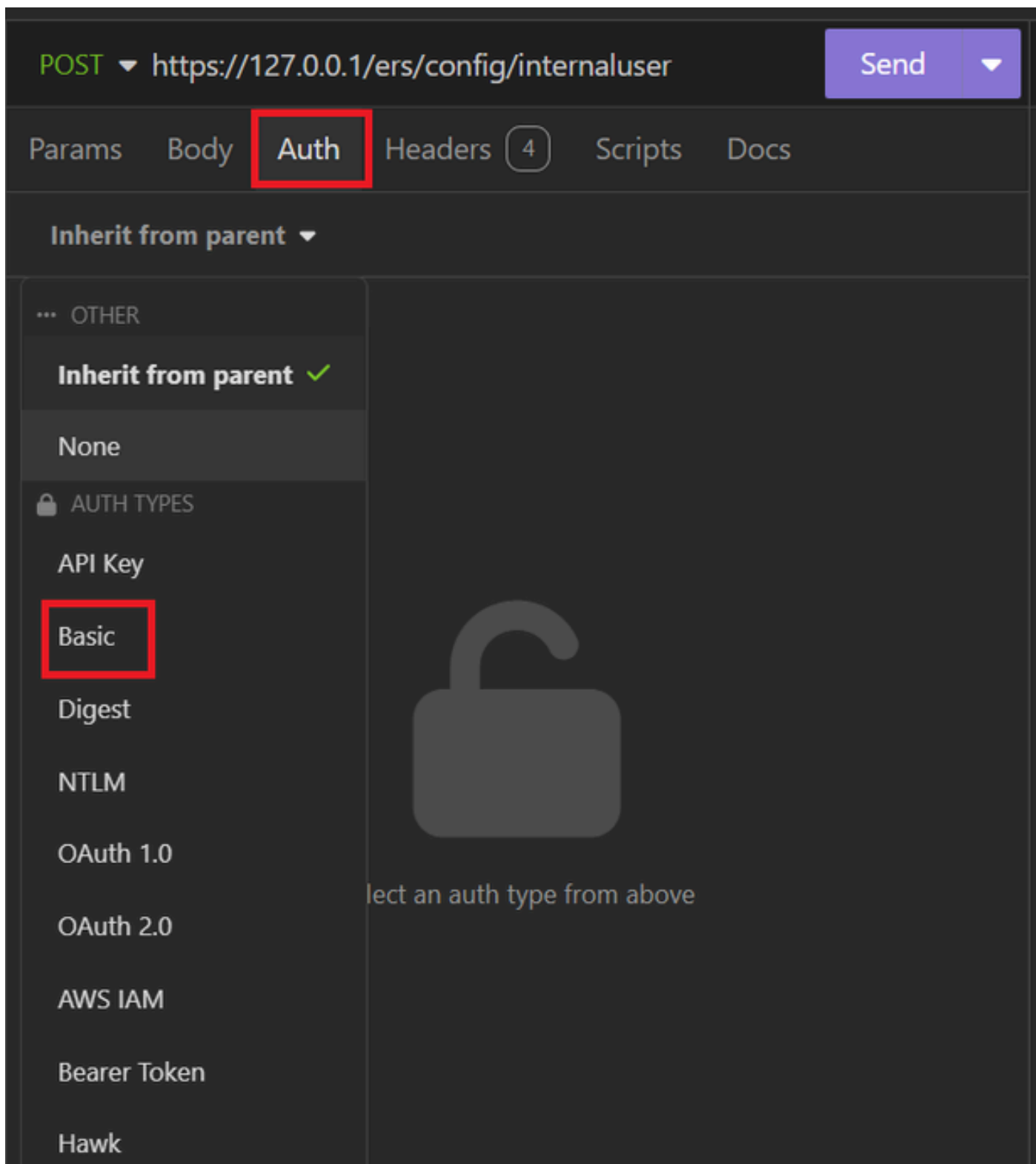
```
  <changePassword>true</changePassword>
```

```
  <customAttributes>
```



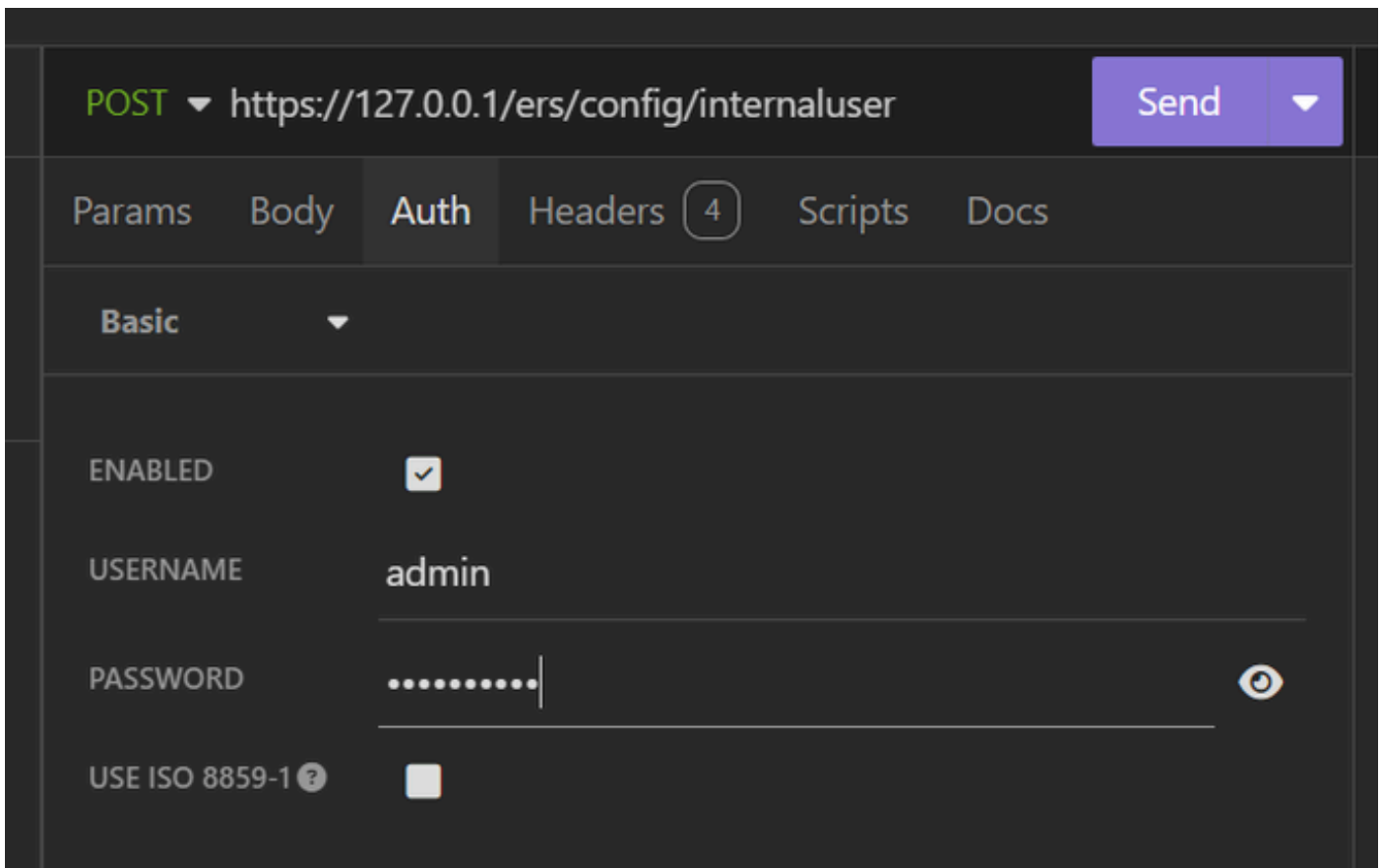
```
<entry>
  <key>key1</key>
  <value>value1</value>
</entry>
<entry>
  <key>key2</key>
  <value>value3</value>
</entry>
</customAttributes>
<dateCreated>2015-12-15</dateCreated>
<dateModified>2015-12-20</dateModified>
<daysForPasswordExpiration>60</daysForPasswordExpiration>
<email>email@domain.com</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. Authをクリックし、Basicを選択します



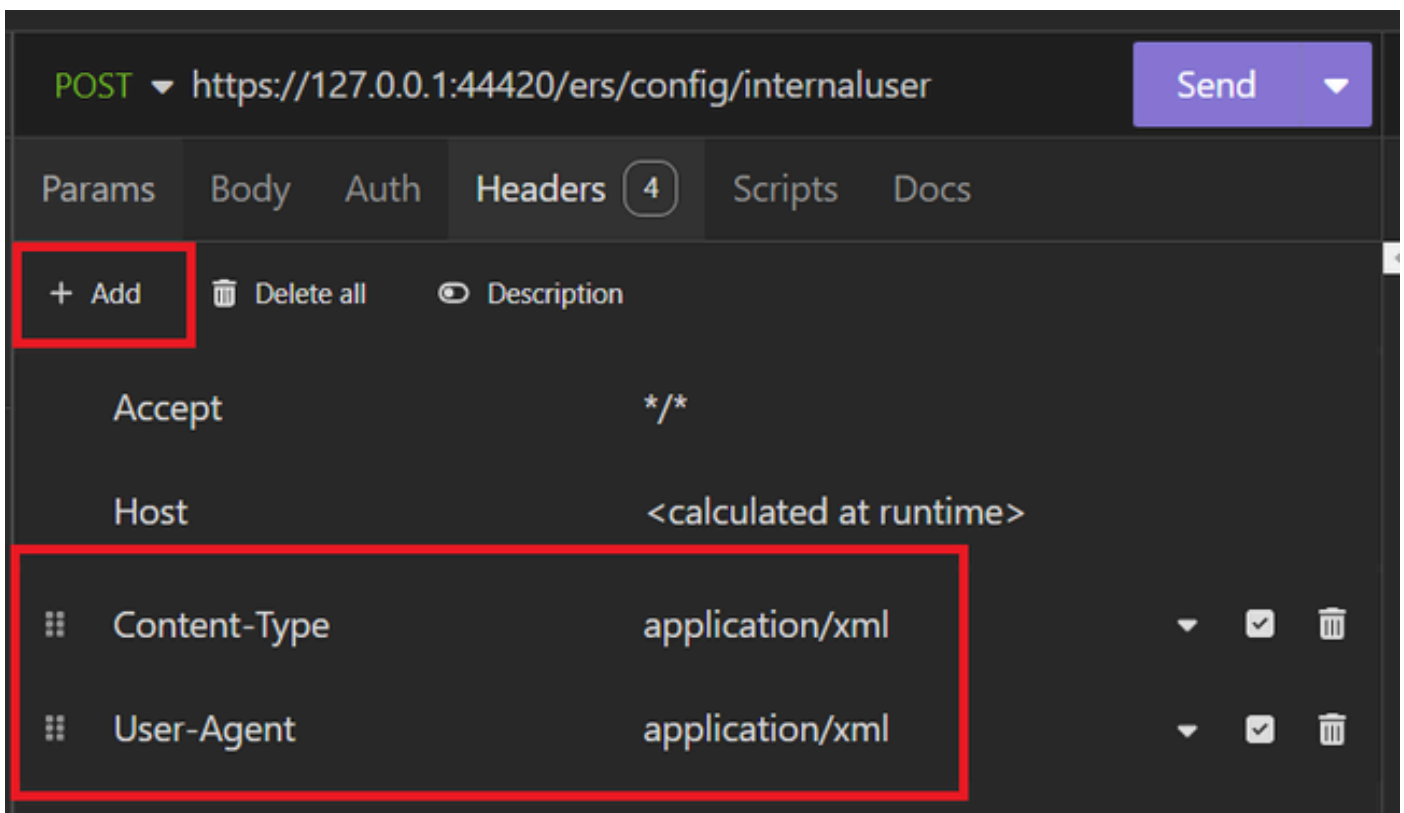
XML認証

7. ISE GUIクレデンシャルを入力します。



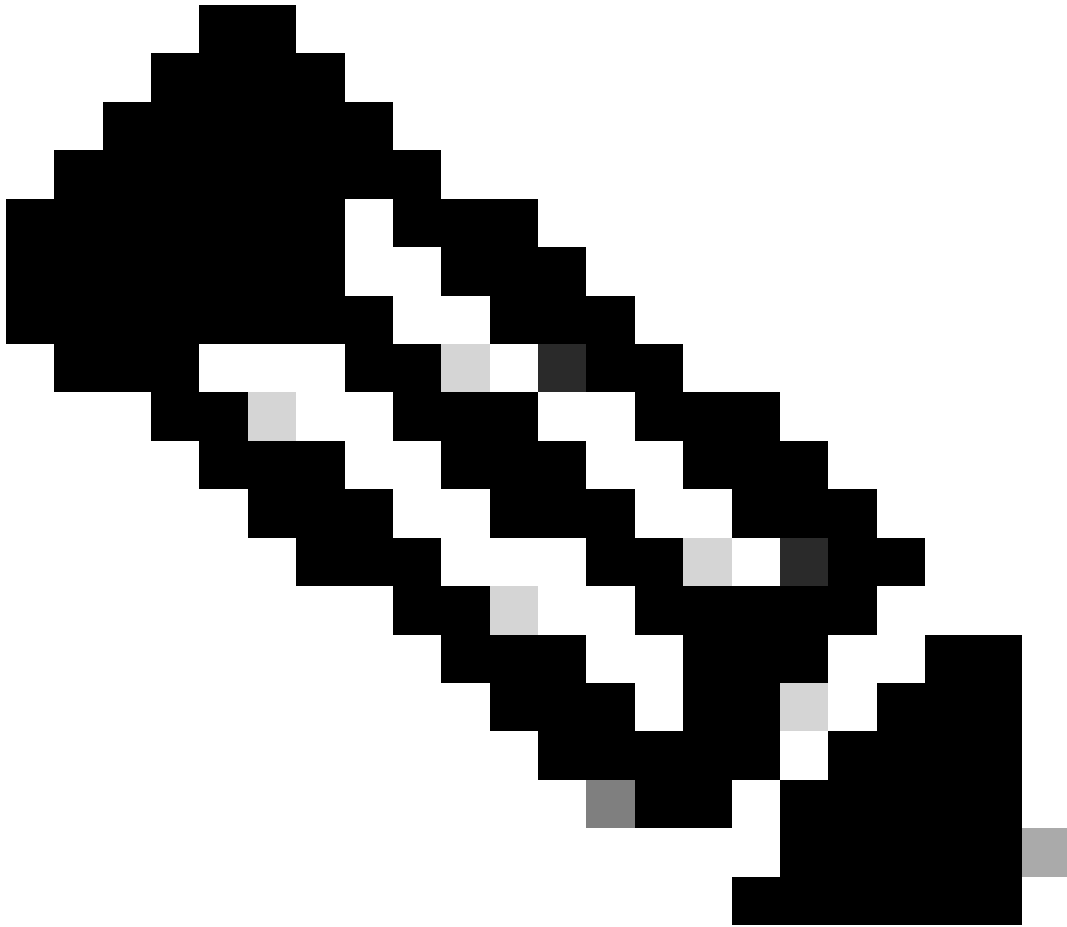
XMLクレデンシャル

- 「ヘッダー」をクリックして、次のメソッドを追加します。
 - コンテンツタイプ : application/xml
 - 許可 : アプリケーション/xml



XMLヘッダー

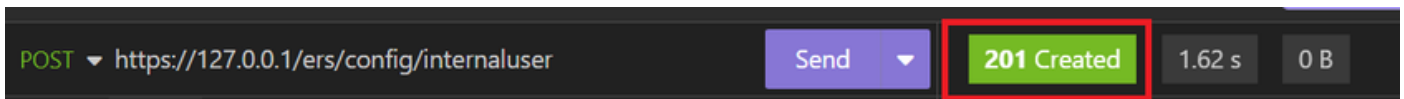
9. 最後に、Sendをクリックします。



注：新しいユーザアカウントにIDグループを割り当てる場合は、そのIDを使用する必要があります。詳細については、「トラブルシューティング」の項を参照してください。

検証



1. POST要求を送信すると、「201 Created」というステータスが表示されます。これは、プロセスが正常に完了したことを意味します。

















正常なXML要求

2. ISE GUIを開き、Administration > Identity Management > Identities > Users > Network Access Usersの順に移動します

Network Access Users

Selected 0 Total 2  

 Edit  + Add  Change Status  Import  Export  Delete  Duplicate All 

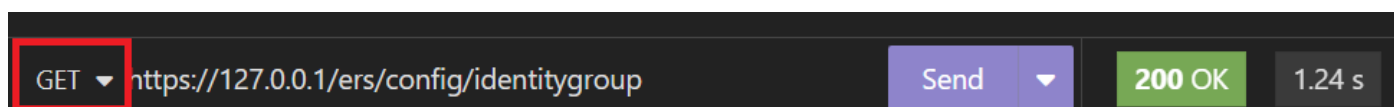
Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	 Enabled  User01	this is the firs...	User	Cisco	user1@local...	Employee	 User Account created by JSON
<input type="checkbox"/>	 Enabled  User02	description	User2	Cisco	user2@local...	Employee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

ユーザアカウントの検証

トラブルシューティング

1. 識別グループのIDを識別します。

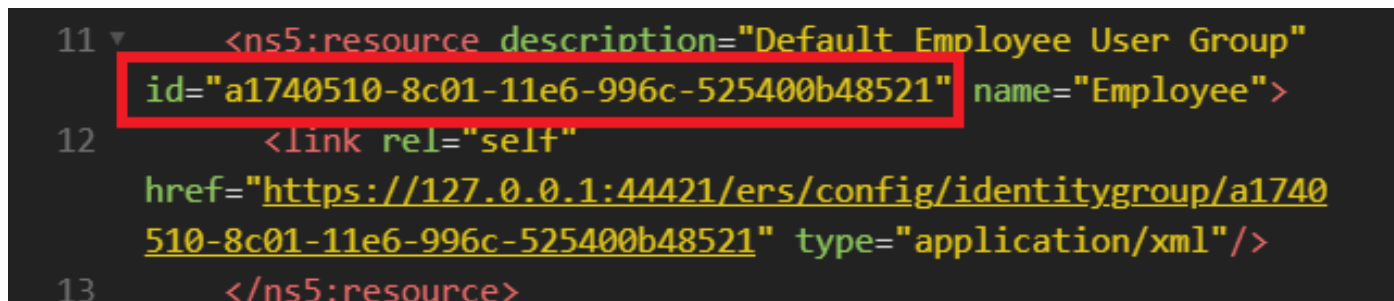
GETおよび<https://X.X.X.X/ers/config/identitygroup>クエリを使用します。



GETオプション

JSON出力。

説明の横にあるIDを指定します。



IDアイデンティティグループ01

XML出力。

説明の横にあるIDを指定します。

```
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アイデンティティグループ02

2. 401 Unauthorized error (不正エラー)。

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

401 エラー

解決方法：[認証]セクションで構成されているアクセスクレデンシャルを確認します

3. エラー：サーバーに接続できませんでした

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

接続エラー

解決策：不眠症で設定されているISEノードのIPアドレスを確認するか、接続を検証します。

4. 400不正な要求。

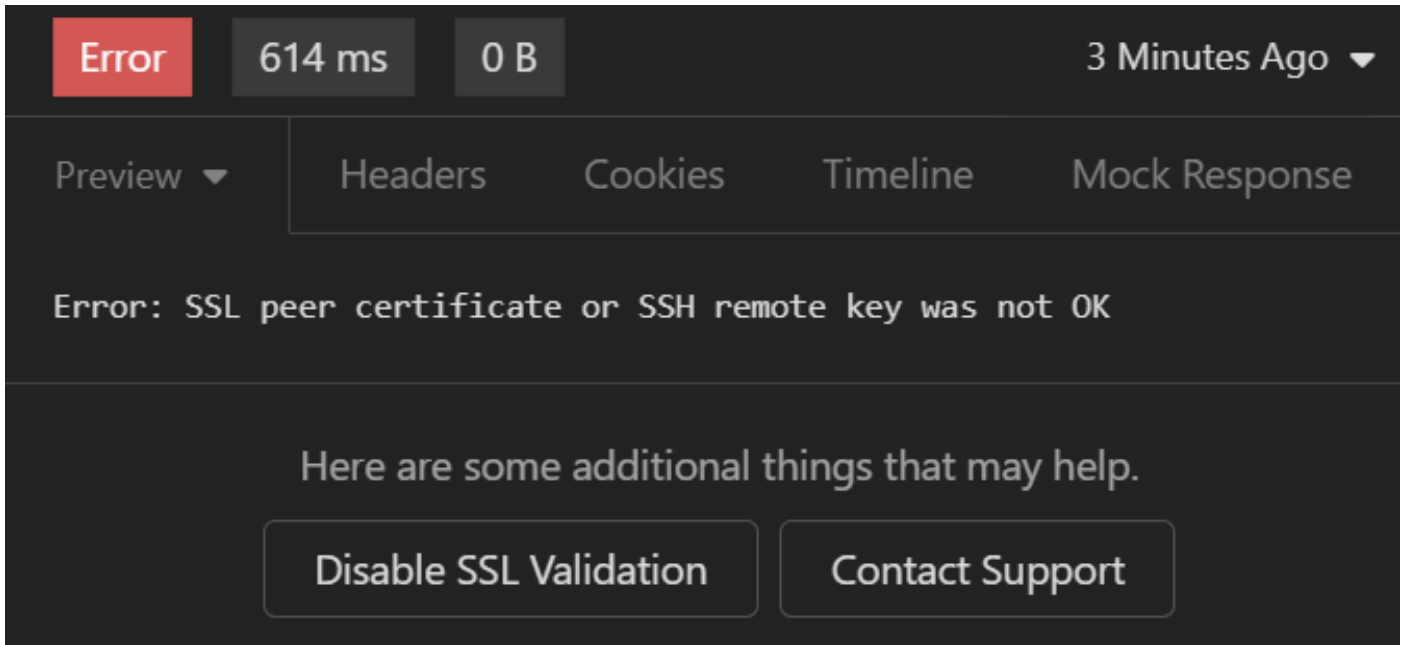
```
POST https://127.0.0.1/ers/config/internaluser Send 400 Bad Request
```

400 エラー

このエラーが発生する原因は複数ありますが、最も一般的な原因は次のとおりです。

- セキュリティパスワードポリシーとの不一致
- 一部のパラメータが正しく設定されていません。
- Sintaxisエラー。
- 情報が重複しています。

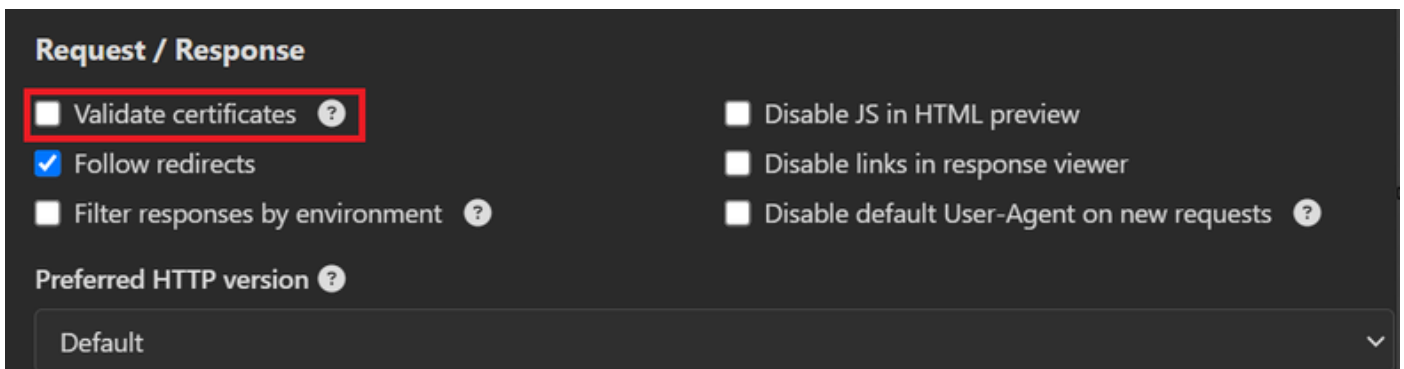
5. エラー：SSLピア証明書またはSSHリモートキーがOKではありませんでした



SSL証明書エラー

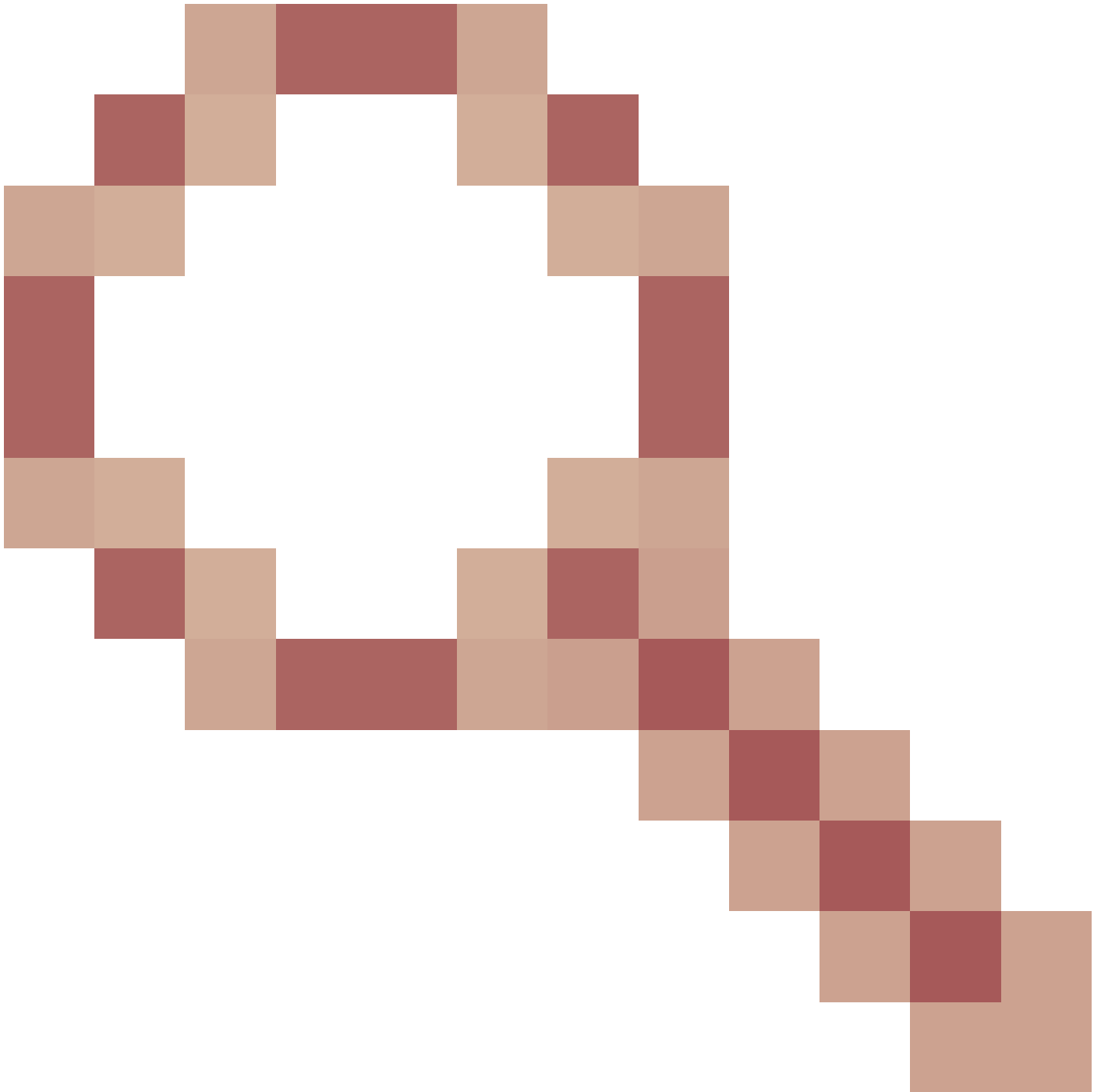
ソリューション：

1. Disable SSL Validationをクリックします。
2. Request / Responseで、Validate Certificatesオプションを無効にします。



Validate certificatesオプション

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



不具合。

イネーブルパスワードは未設定ですが、ランダムに設定されます。この動作は、enable password構文が削除された場合、または値として空のままになっている場合に発生します。詳細については、次のリンクを参照してください。

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

APIコール参照。

ISEがサポートするAPIコールに関するすべての情報を確認できます。

1. 「管理」 > 「システム」 > 「設定」 > 「API設定」 にナビゲートします。

2. ERS API情報リンクをクリックします。

Identity Services Engine Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access **Settings**

Security Settings
Alarm Settings
General MDM / UEM Settings
Posture
Profiling
Protocols
Endpoint Scripts
Proxy
SMTP Server
SMS Gateway
System Time
API Settings
Data Connect
Network Success Diagnostics

API Settings

Overview API Service Settings API Gateway Settings

API Services Overview

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>

API設定

3. 「APIドキュメント」をクリックします。

External RESTful Services (ERS) Online SDK

Quick Reference
API Documentation

- ISE 2.0 Release Notes
- ISE 2.1 Release Notes
- ISE 2.2 Release Notes
- ISE 2.3 Release Notes
- ISE 2.4 Release Notes
- ISE 2.6 Release Notes
- ISE 2.7 Release Notes
- ISE 3.0 Release Notes
- ISE 3.1 Release Notes
- ISE 3.2 Release Notes
- ISE 3.3 Release Notes**
- ANC Endpoint
- ANC Policy
- Aci Bindings
- Aci Settings
- Active Directory

ISE 3.3 Release Notes

• New / Modified Resources

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

APIドキュメント

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。