Konfiguration interner Benutzer über JSON oder XML und API-Aufrufe in ISE 3.3 mit Insominia

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration interner Benutzer in der Cisco ISE durch die Nutzung von JSON- oder XML-Datenformaten in Verbindung mit API-Aufrufen beschrieben.

Voraussetzungen

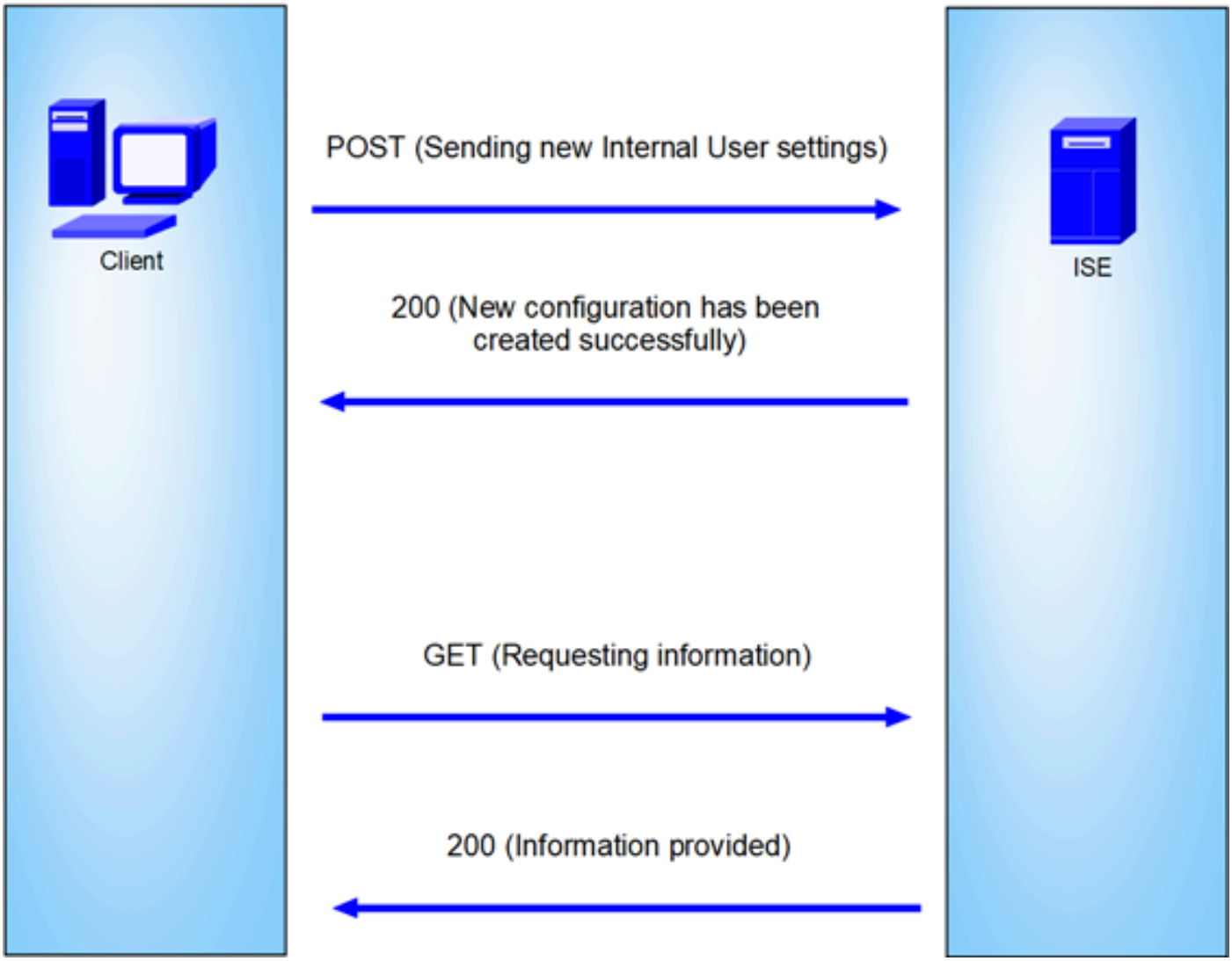
- ISE 3.0 oder höher
- API-Client-Software.

Verwendete Komponenten

- ISE 3.3
- Insominia 9.3.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerkdiagramm



Allgemeine Topologie

GET und POST sind zwei der gebräuchlichsten HTTP-Methoden für API-Aufrufe (Application Programming Interface). Sie werden verwendet, um mit Ressourcen auf einem Server zu interagieren, in der Regel um Daten abzurufen oder zur Verarbeitung zu übermitteln.

GET-API-Aufruf

Die GET-Methode wird verwendet, um Daten von einer angegebenen Ressource anzufordern. GET-Anfragen sind die gebräuchlichsten und am häufigsten verwendeten Methoden in APIs und Websites. Wenn Sie eine Webseite besuchen, sendet Ihr Browser eine GET-Anforderung an den Server, der die Webseite hostet.

POST-API-Aufruf

Die POST-Methode wird verwendet, um Daten an den Server zu senden, um eine Ressource zu erstellen oder zu aktualisieren. POST-Anfragen werden häufig verwendet, wenn Formulardaten gesendet oder eine Datei hochgeladen wird.

Konfigurationen

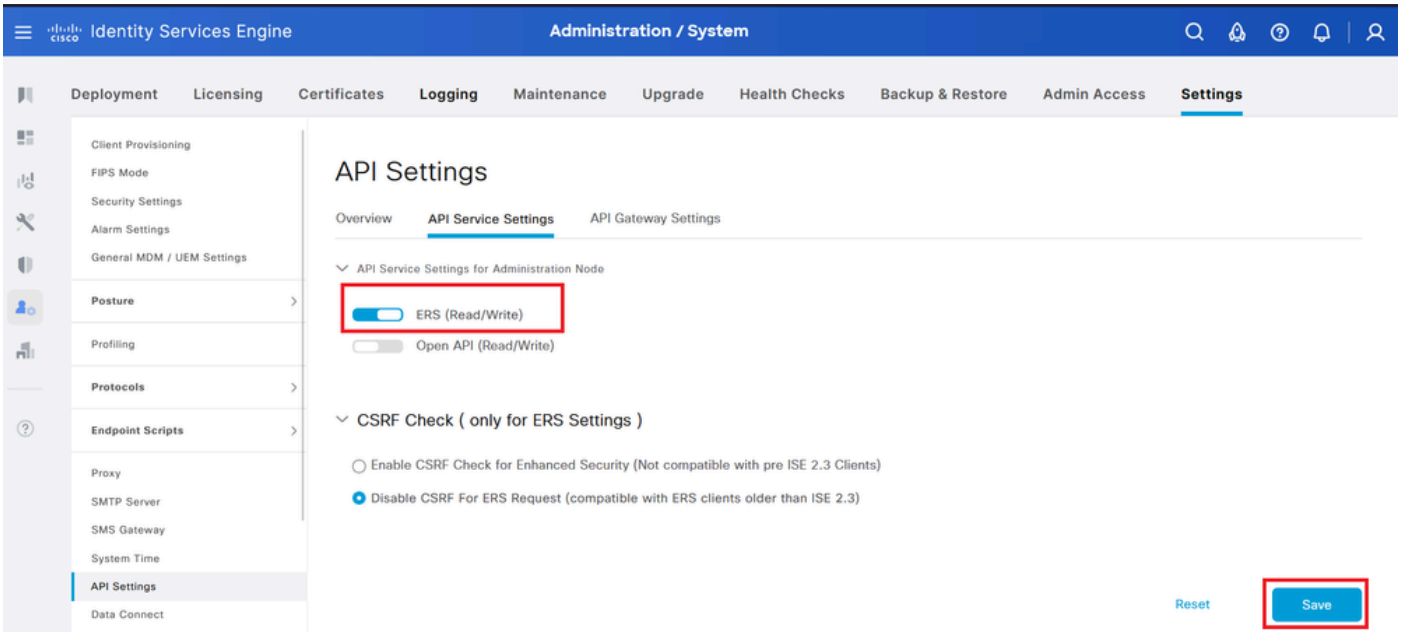
Wir müssen die genauen Informationen von der API-Client-Software an den ISE-Knoten senden, um einen internen Benutzer zu erstellen.

ISE-Konfigurationen

Aktivieren der ERS-Funktion

1. Navigieren Sie zu Administration > System > Settings > API Settings > API Service Settings.

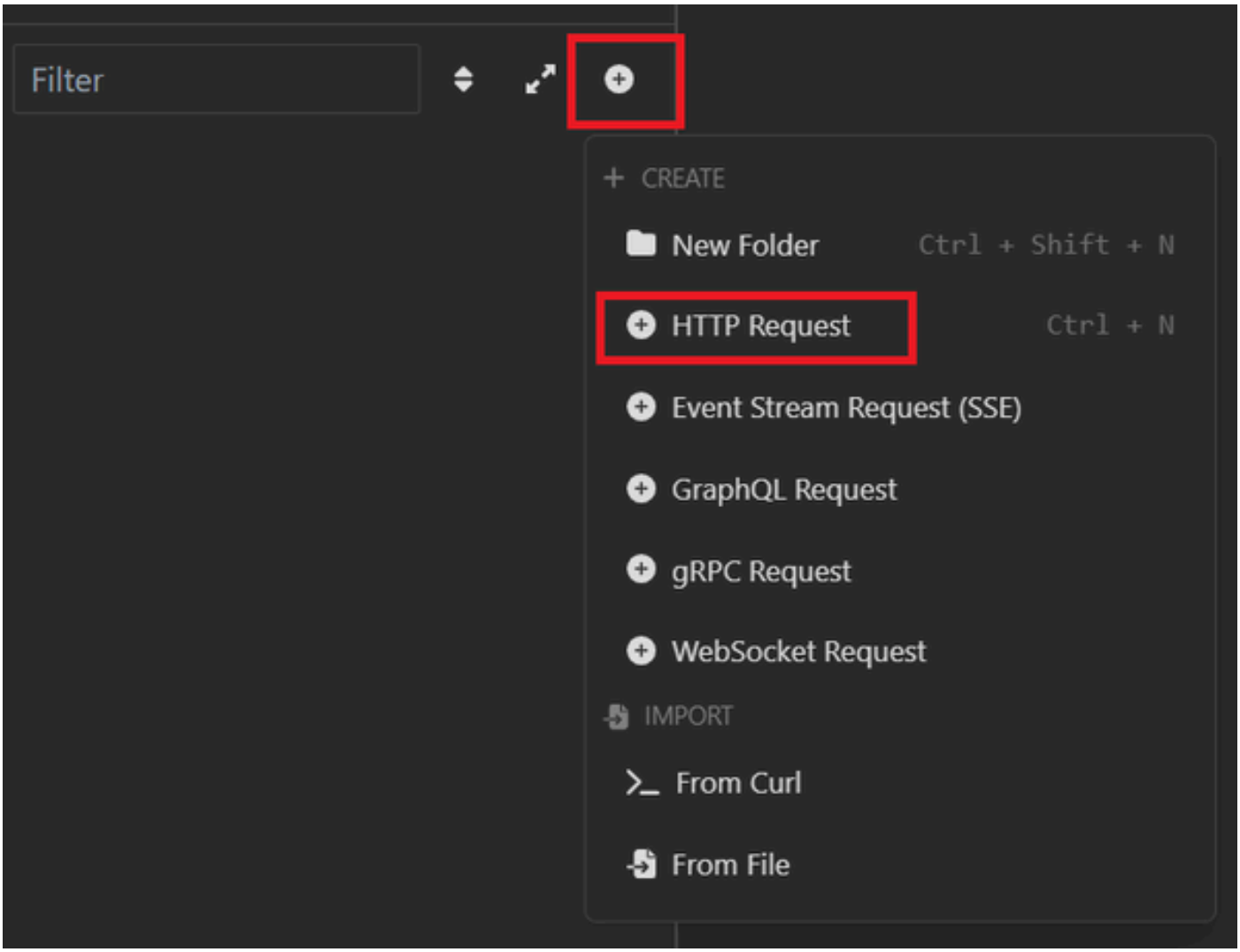
2. Aktivieren Sie die ERS-Option (Lesen/Schreiben).



API-Einstellungen

JSON-Anfrage.

1. Offene Schlaflosigkeit.
2. Fügen Sie auf der linken Seite eine neue HTTPS-Anforderung hinzu.

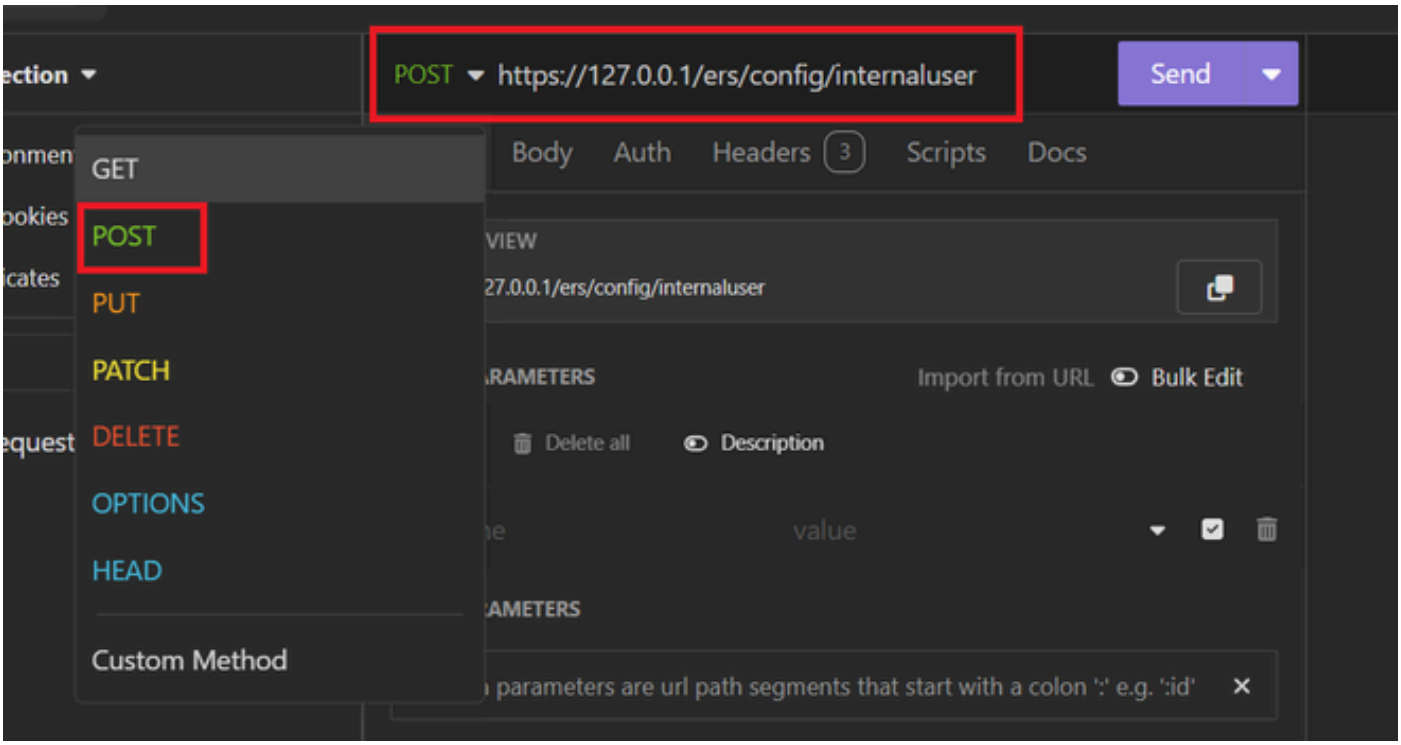


JSON-Anforderung

3. Sie müssen POST auswählen, um die Informationen an den ISE-Knoten zu senden.

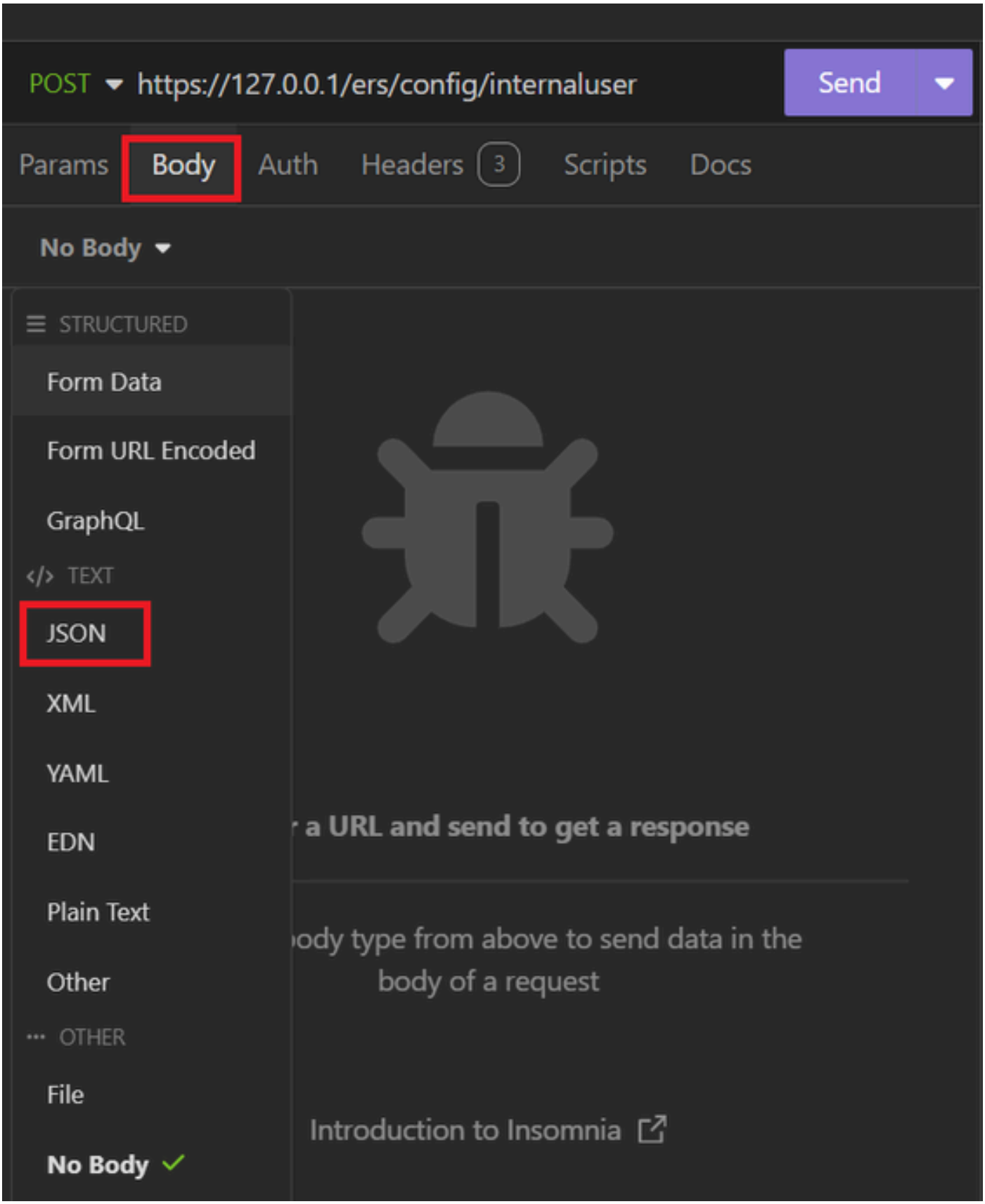
Die einzugebende URL hängt von der IP-Adresse des ISE-Knotens ab.

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



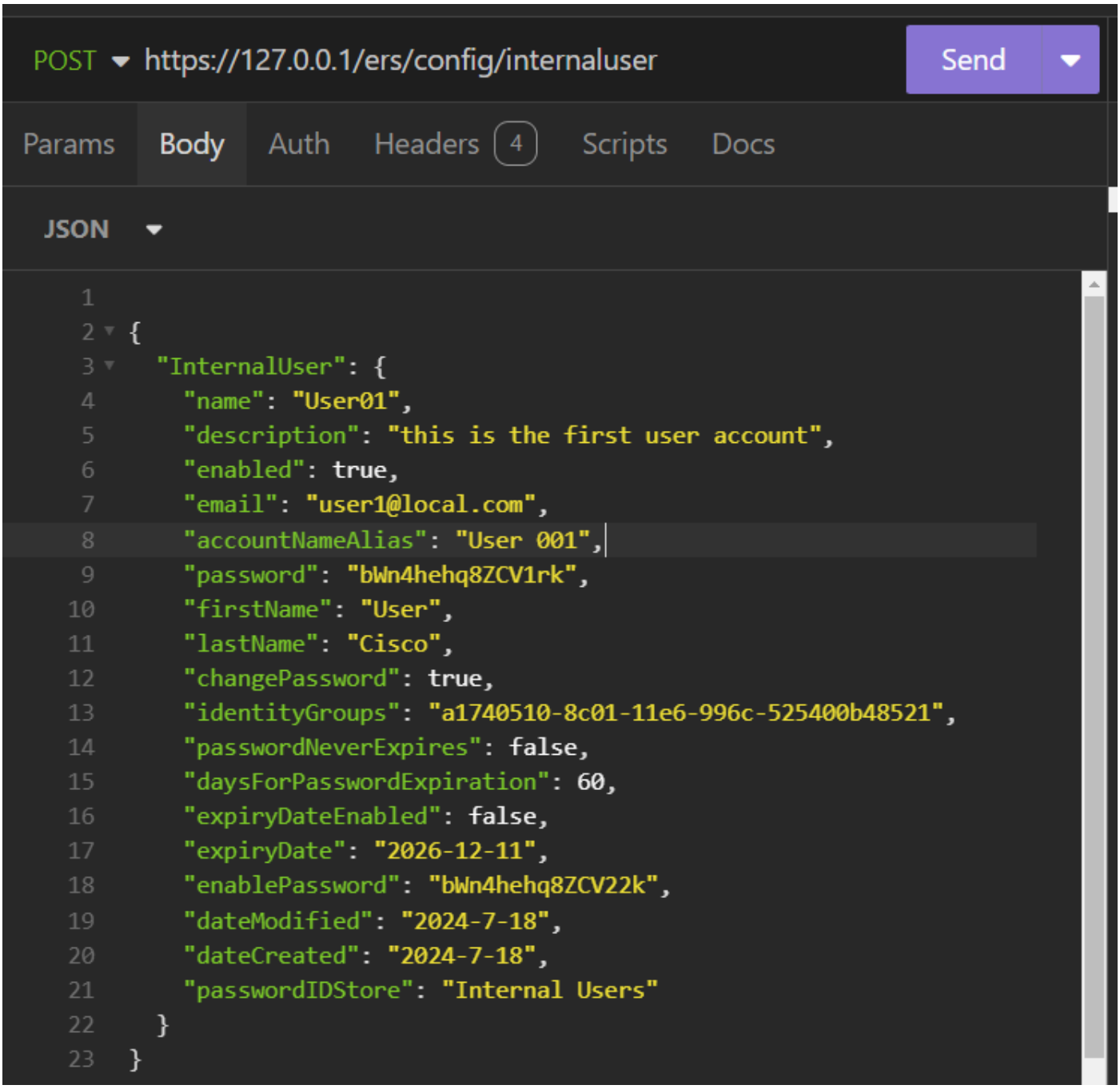
JSON POST

4. Klicken Sie anschließend auf Body und wählen Sie JSON aus.



JSON-Body

5. Sie können die Syntax einfügen und die Parameter ändern, je nachdem, was Sie möchten.



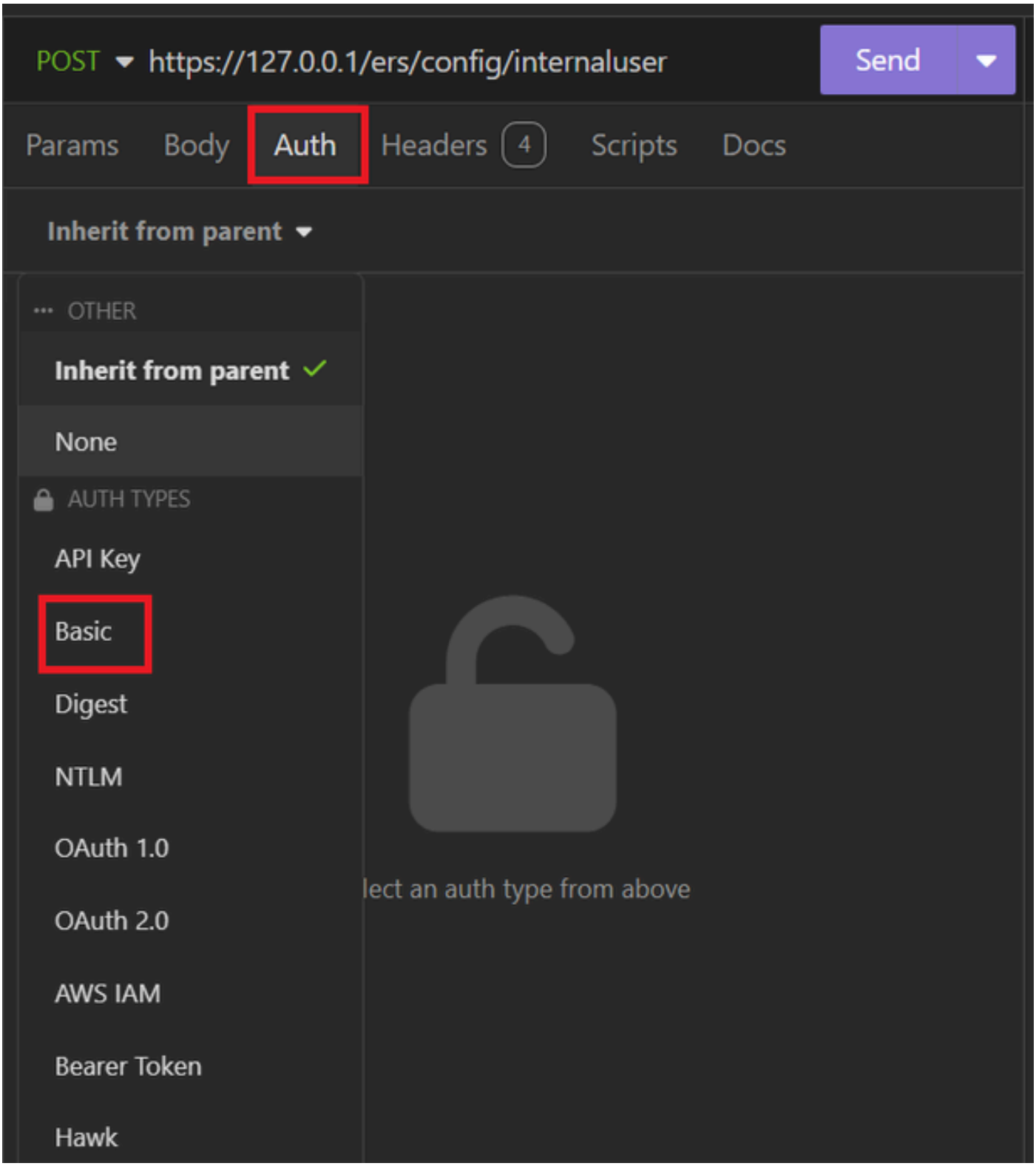
JSON-Syntax

JSON-Syntax

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

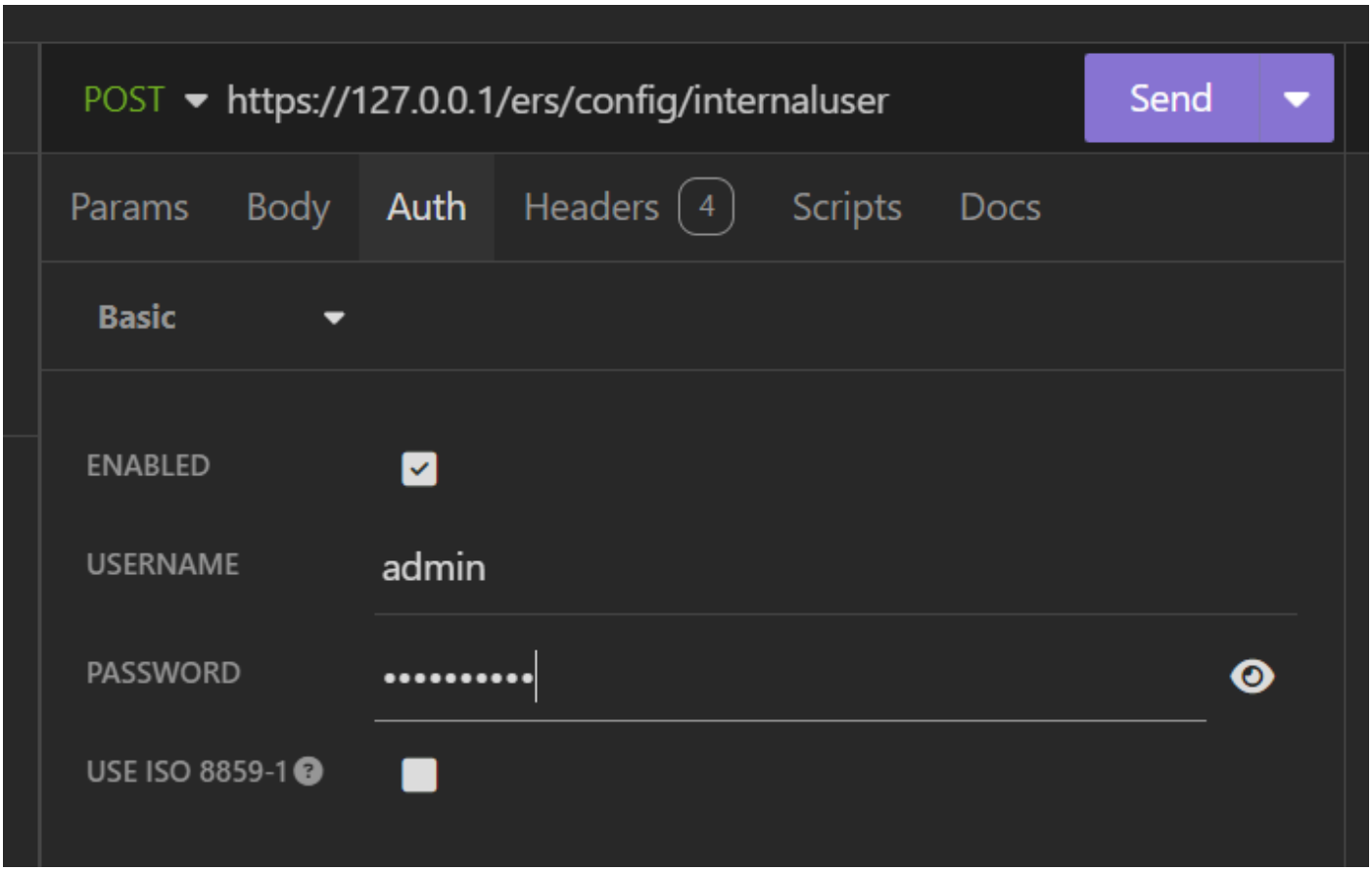
```
    "password": "password",
    "firstName": "firstName",
    "lastName": "lastName",
    "changePassword": true,
    "identityGroups": "identityGroups",
    "passwordNeverExpires": false,
    "daysForPasswordExpiration": 60,
    "expiryDateEnabled": false,
    "expiryDate": "2016-12-11",
    "enablePassword":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


6. Klicken Sie auf Auth, und wählen Sie Basics (Grundlegend) aus.



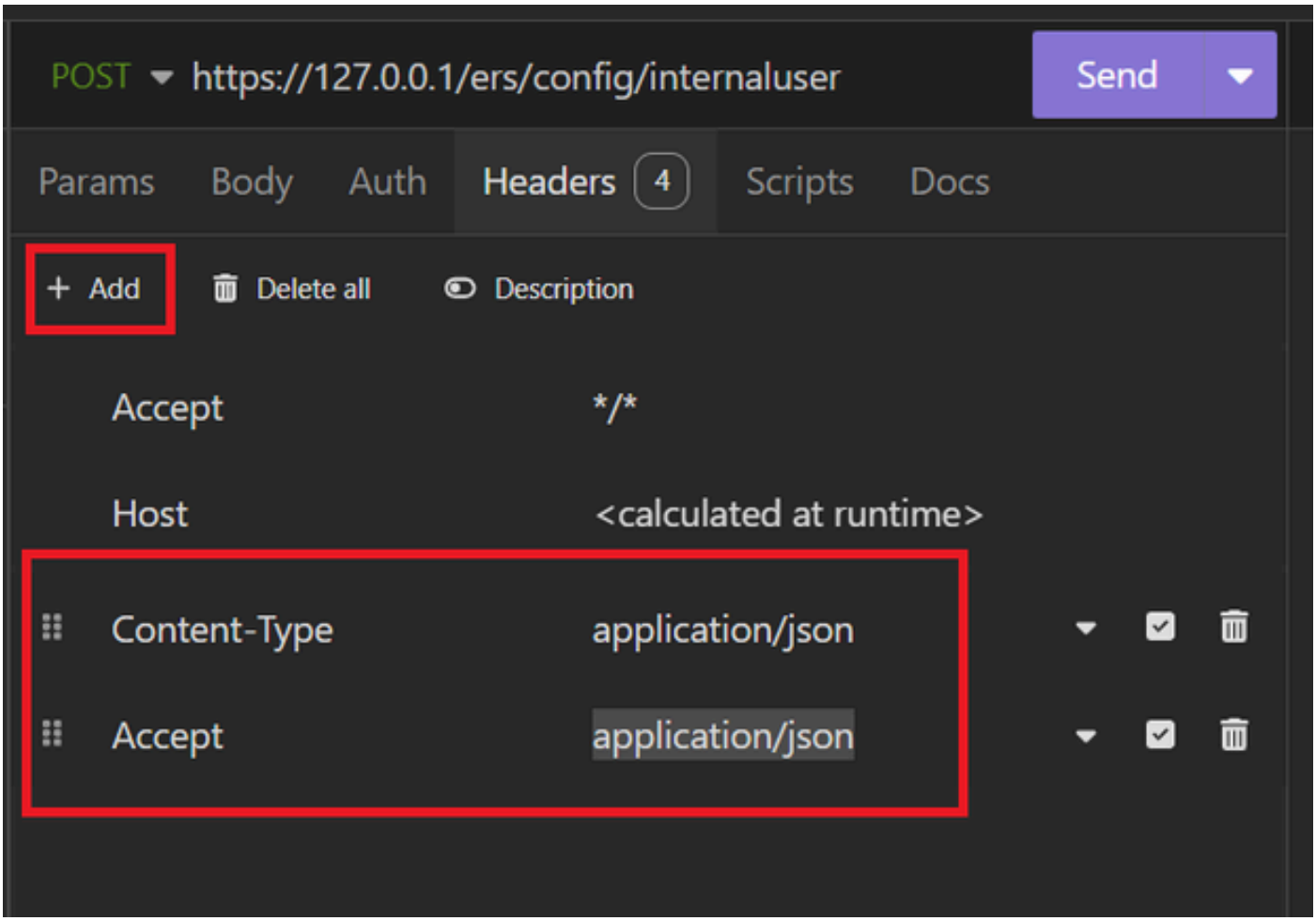
JSON-Authentifizierung

7. Geben Sie die Anmeldeinformationen für die ISE-GUI ein.



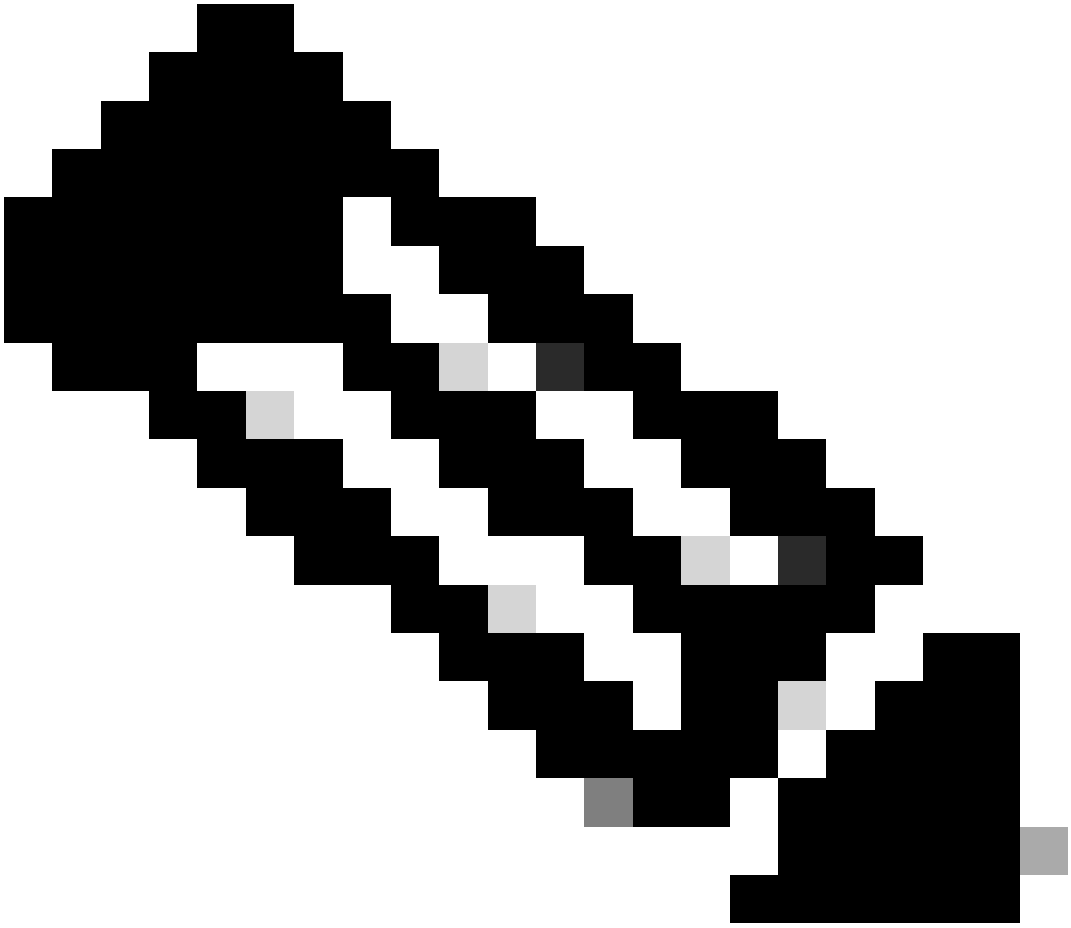
Admin-JSON-Anmeldedaten

8. Klicken Sie auf Headers, um die folgenden Methoden hinzuzufügen:
    - Inhaltstyp: Anwendung/json
    - Akzeptieren: Anwendung/json



JSON-Header

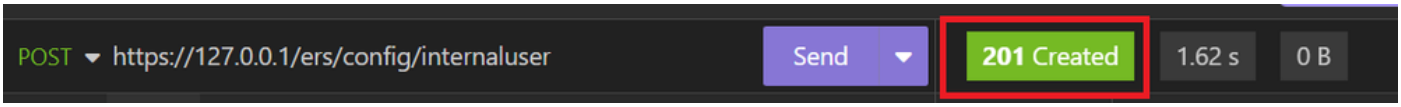
9. Klicken Sie abschließend auf Senden.



Hinweis: Wenn Sie dem neuen Benutzerkonto eine Identitätsgruppe zuweisen möchten, müssen Sie die ID der Identitätsgruppe verwenden. Weitere Informationen finden Sie **im Abschnitt** zur **Fehlerbehebung**.

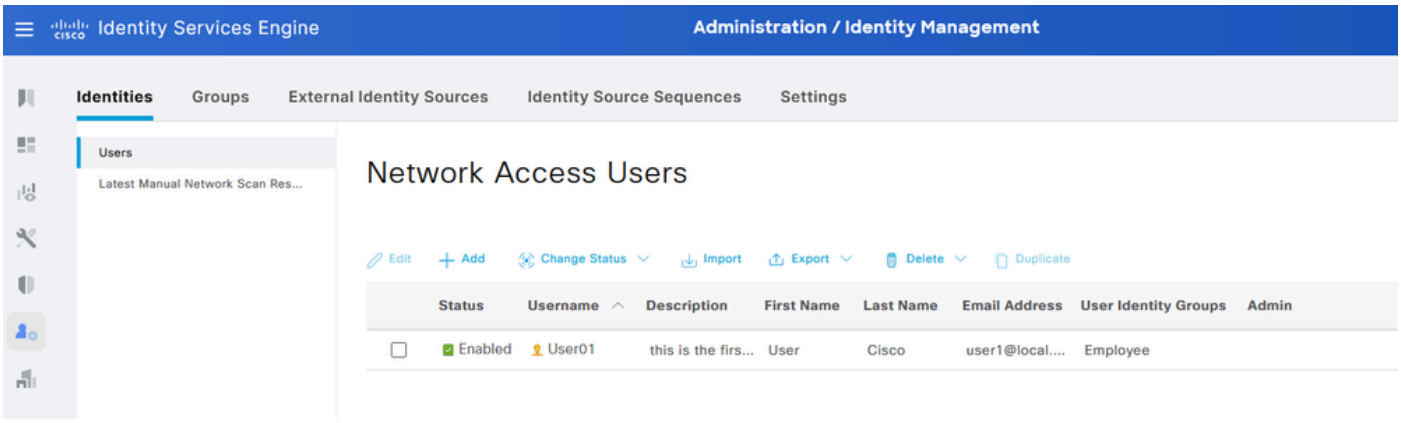
Validierung

1. Nachdem Sie die POST-Anfrage gesendet haben, wird der Status "201 Created" angezeigt. Das bedeutet, dass der Prozess erfolgreich abgeschlossen wurde.



JSON-Anforderung erfolgreich

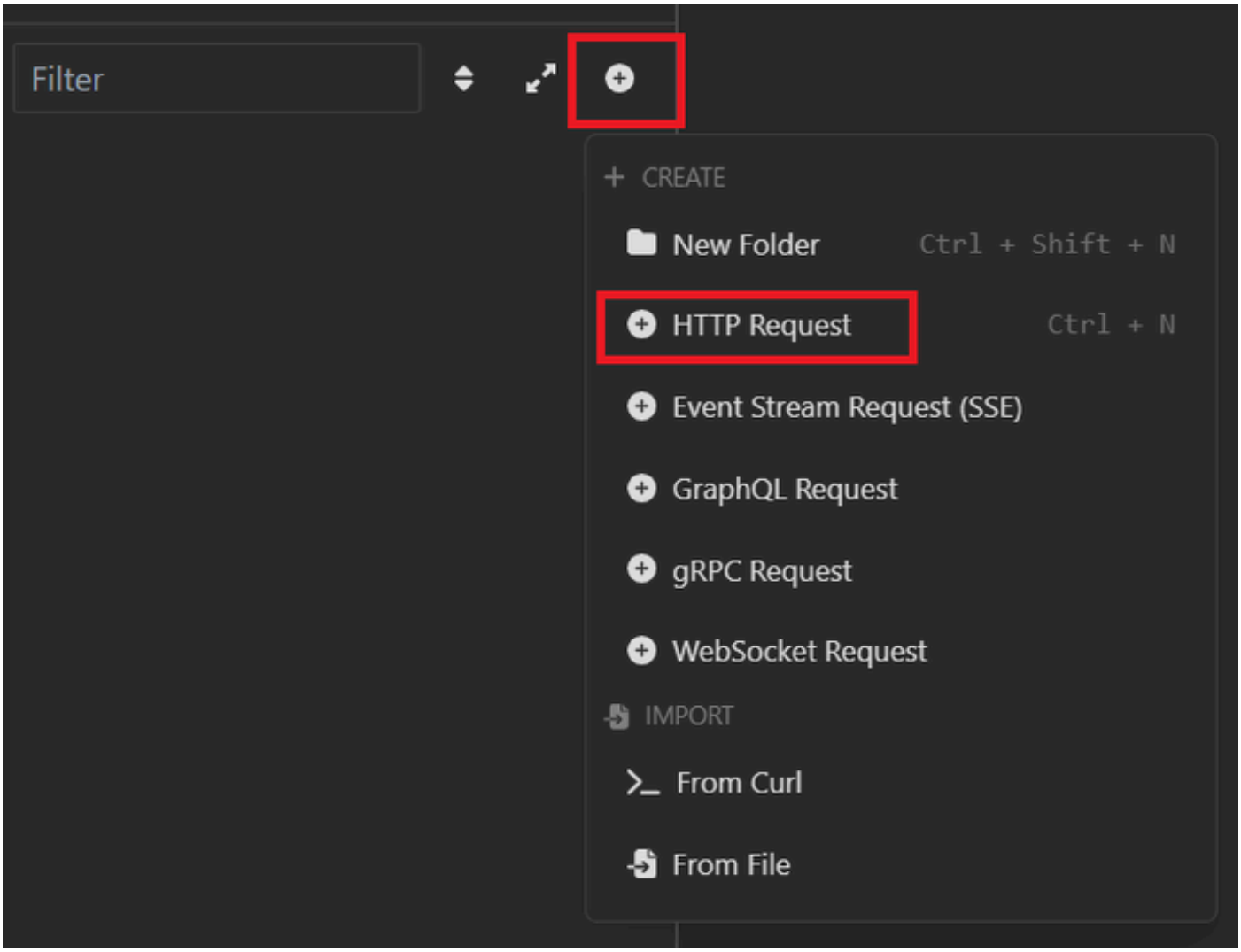
2. Öffnen Sie die ISE-GUI, und navigieren Sie zu Administration > Identity Management > Identities > Users > Network Access Users



JSON-Benutzerkonto

XML-Anforderung

1. Offene Schlaflosigkeit.
2. Fügen Sie auf der linken Seite eine neue HTTPS-Anforderung hinzu.

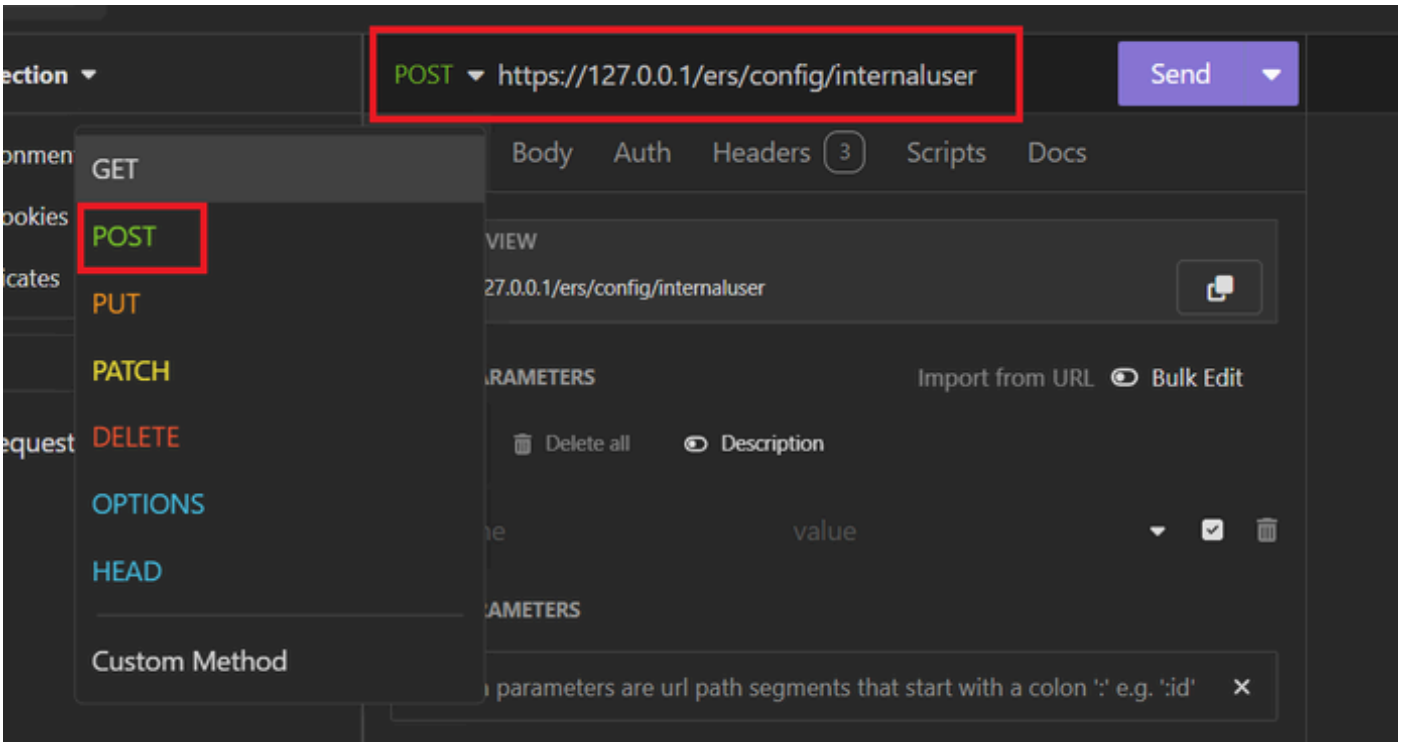


XML-Anforderung

3. Sie müssen POST auswählen, um die Informationen an den ISE-Knoten zu senden.

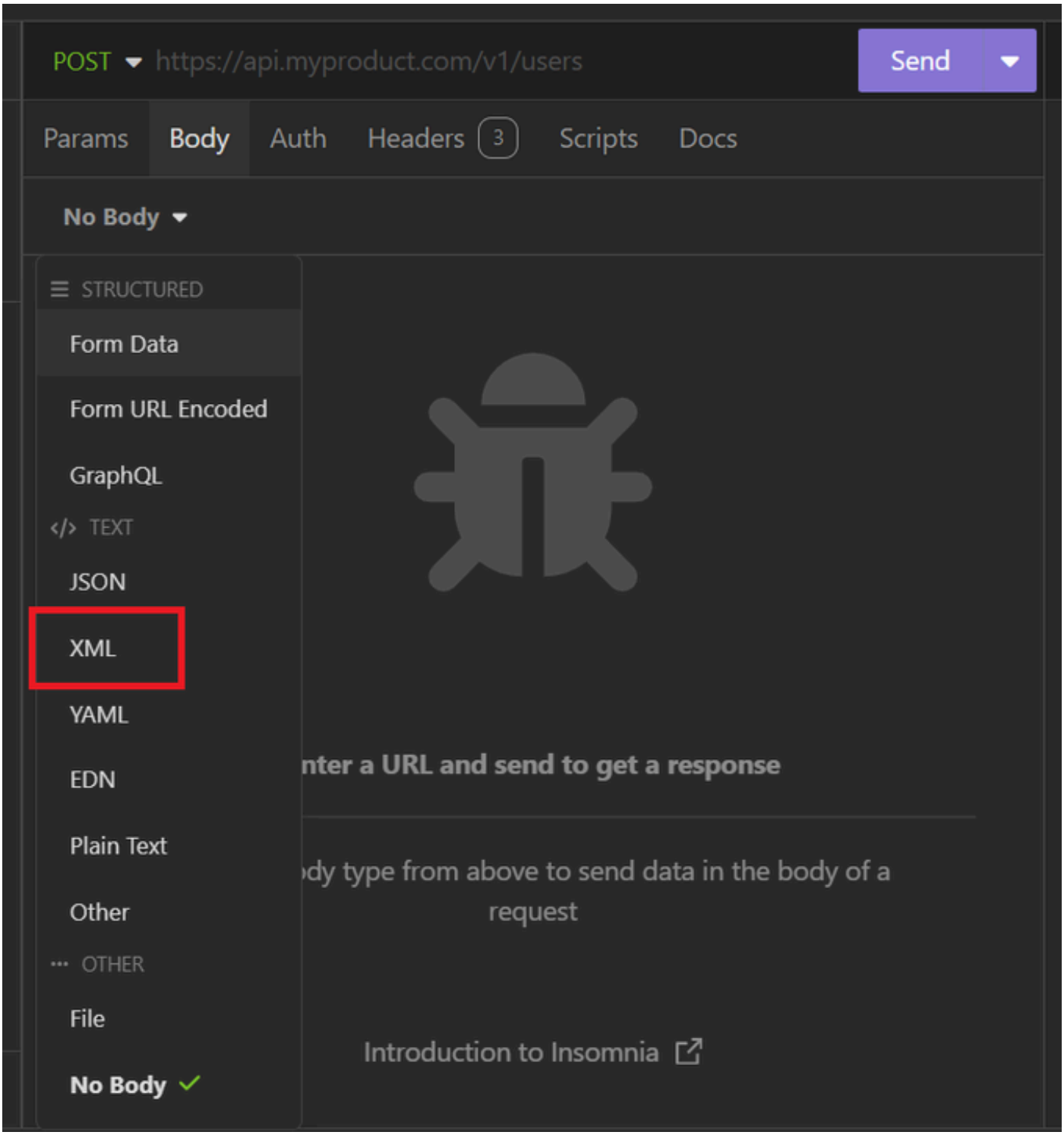
Die einzugebende URL hängt von der IP-Adresse des ISE-Knotens ab.

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



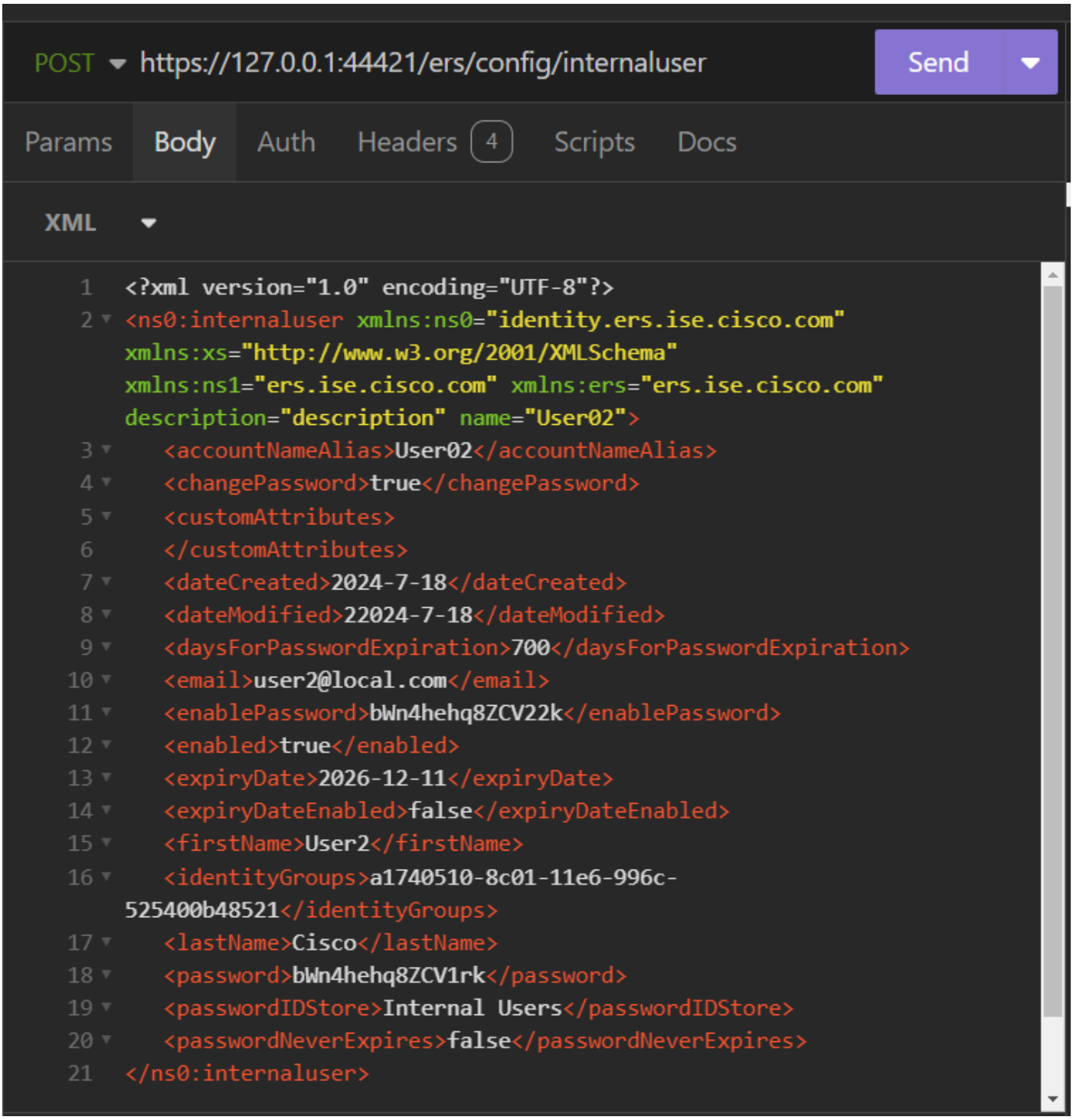
XML-POST

4. Klicken Sie dann auf Text, und wählen Sie XML aus.



XML-Text

5. Sie können die Syntax einfügen und die Parameter ändern, je nachdem, was Sie möchten.



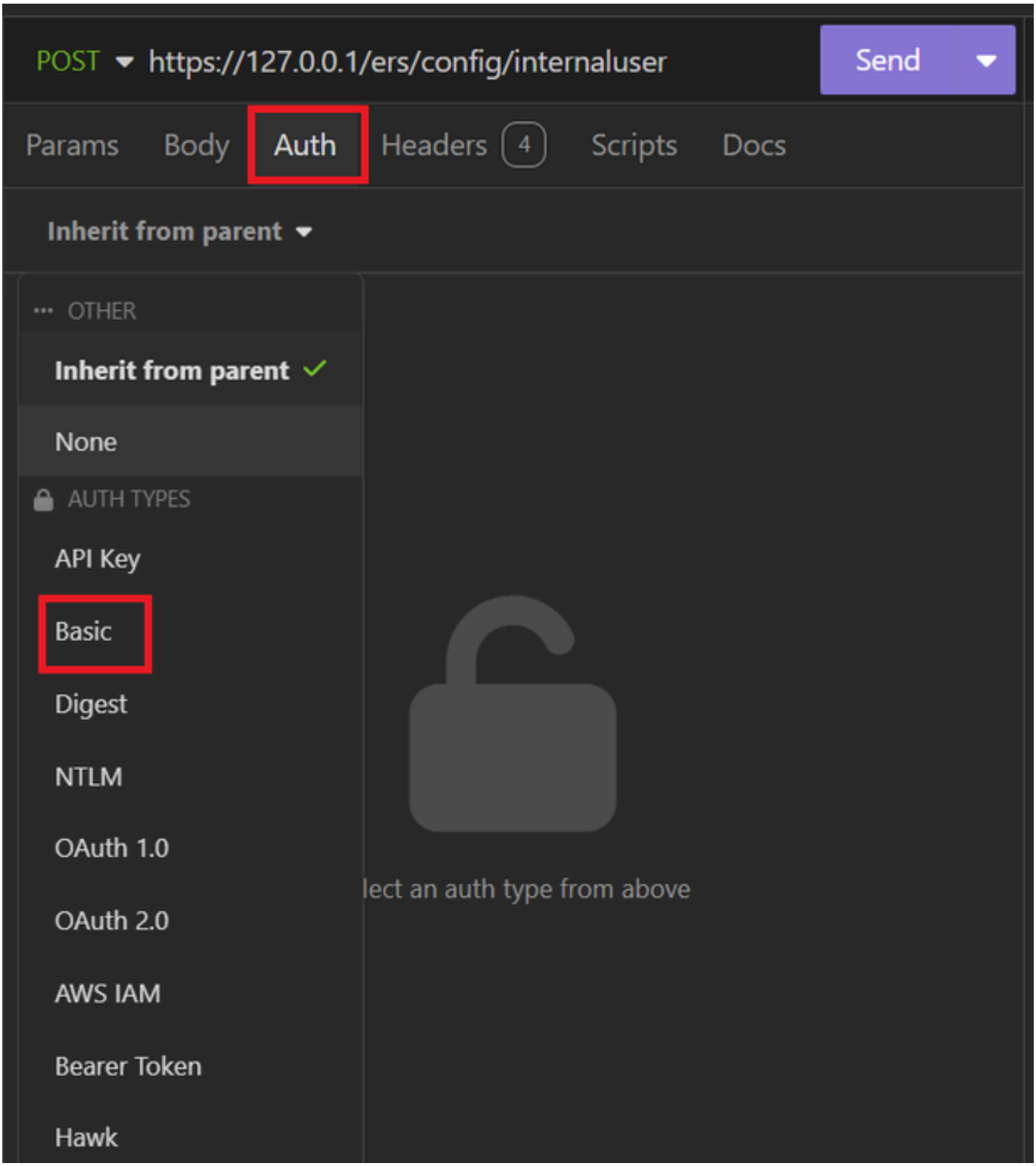
XML-Beitrag

XML-Syntax

```
<?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>
```

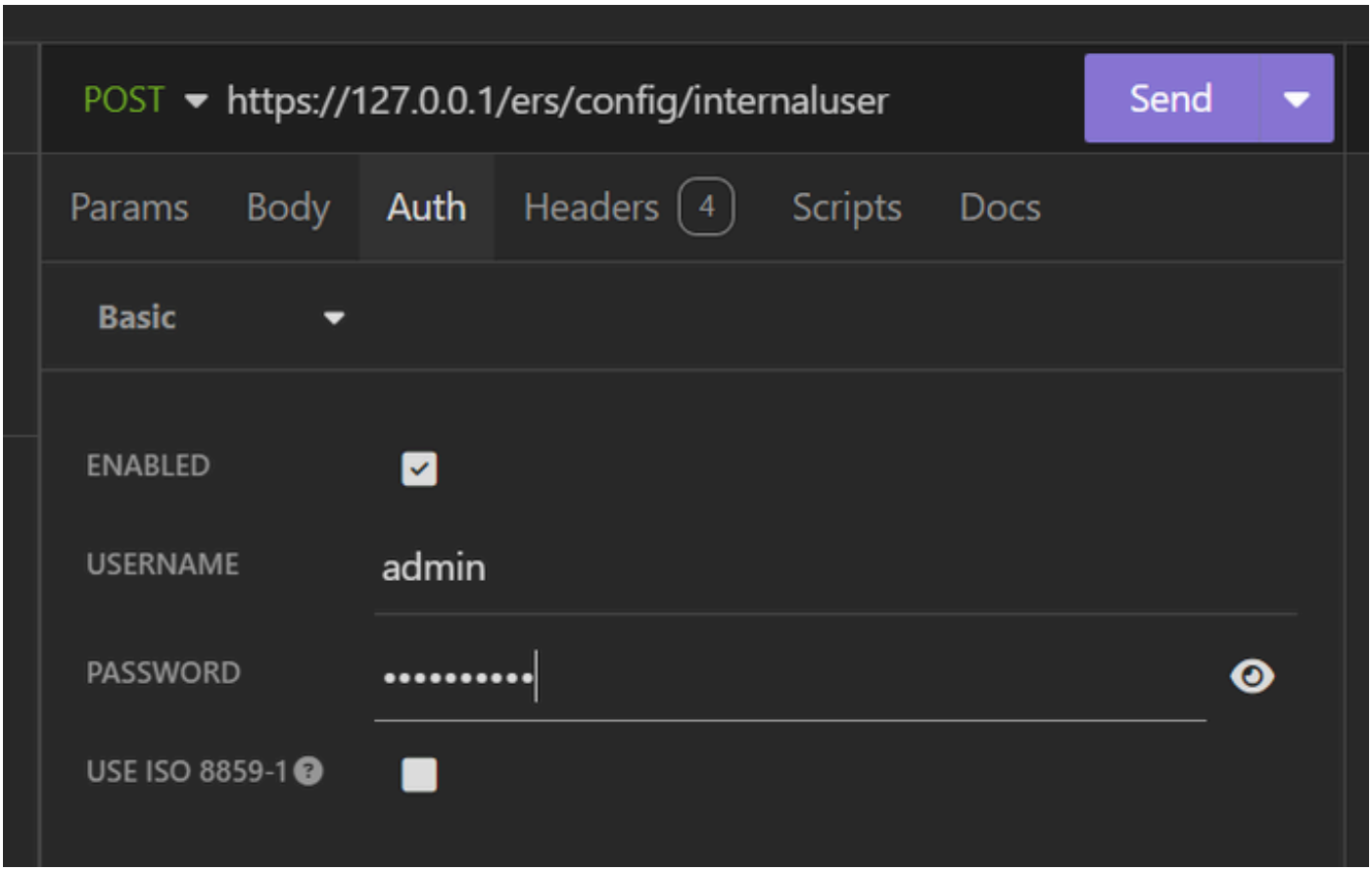
```
        <entry>
            <key>key1</key>
            <value>value1</value>
        </entry>
        <entry>
            <key>key2</key>
            <value>value3</value>
        </entry>
    </customAttributes>
    <dateCreated>2015-12-15</dateCreated>
    <dateModified>2015-12-20</dateModified>
    <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. Klicken Sie auf Auth. und wählen Sie Basic.



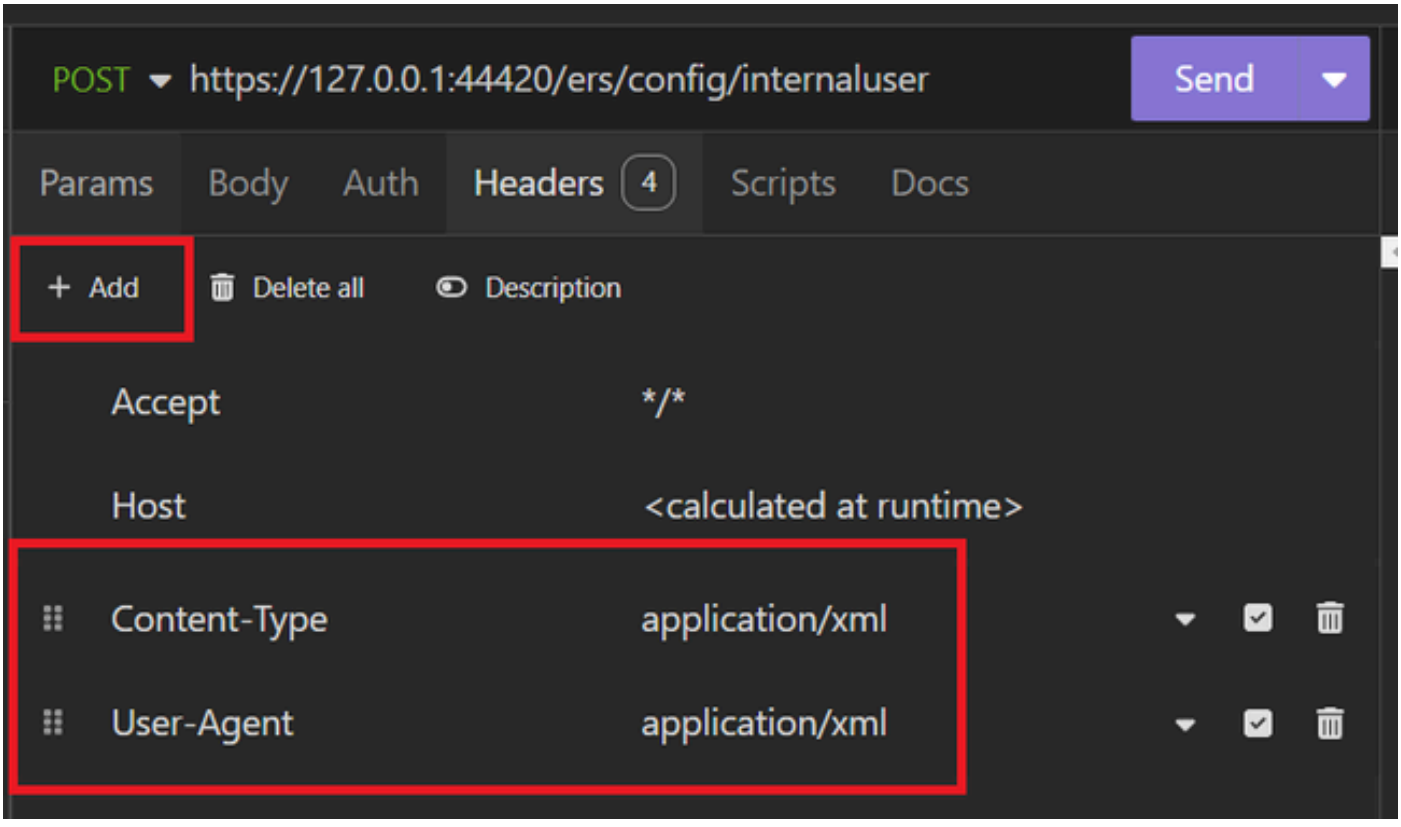
XML-Authentifizierung

7. Geben Sie die Anmeldeinformationen für die ISE-GUI ein.



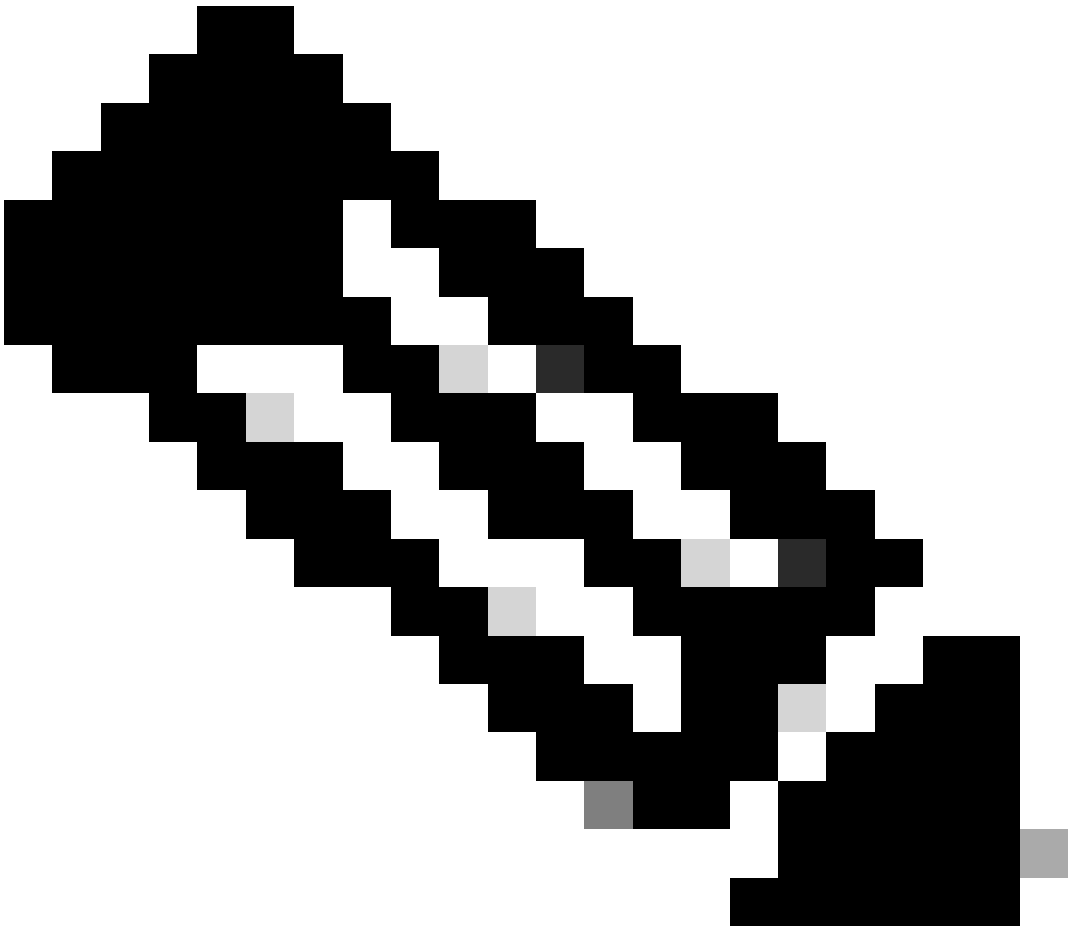
XML-Anmeldeinformationen

8. Klicken Sie auf Headers, um die folgenden Methoden hinzuzufügen:
    - Inhaltstyp: Anwendung/XML
    - Akzeptieren: Anwendung/XML



XML-Header

9. Klicken Sie abschließend auf Senden.



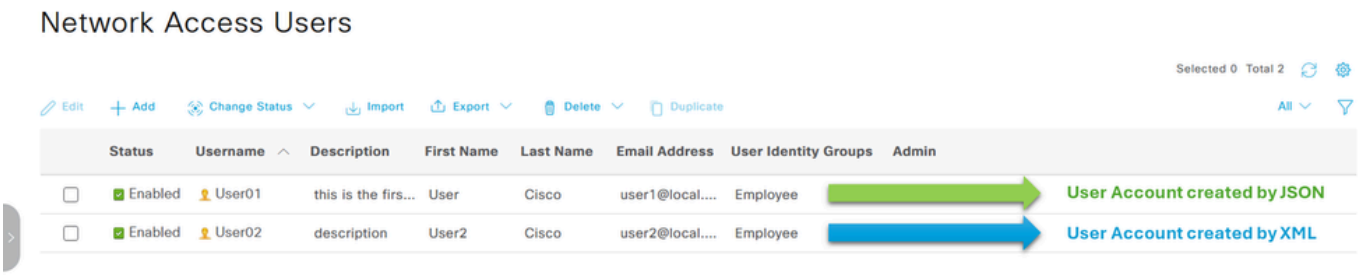
Hinweis: Wenn Sie dem neuen Benutzerkonto eine Identitätsgruppe zuweisen möchten, müssen Sie die ID der Identitätsgruppe verwenden. Weitere Informationen finden Sie **im Abschnitt** zur **Fehlerbehebung**.

Validierung

1. Nachdem Sie die POST-Anfrage gesendet haben, wird der Status "201 Created" angezeigt. Das bedeutet, dass der Prozess erfolgreich abgeschlossen wurde.

XML-Anforderung erfolgreich

2. Öffnen Sie die ISE-GUI, und navigieren Sie zu Administration > Identity Management > Identities > Users > Network Access Users

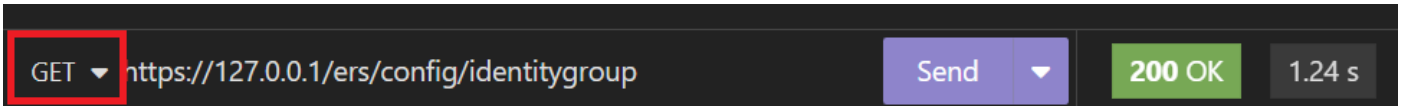


Validierung von Benutzerkonten

Fehlerbehebung

1. Geben Sie die ID der Identitätsgruppe an.

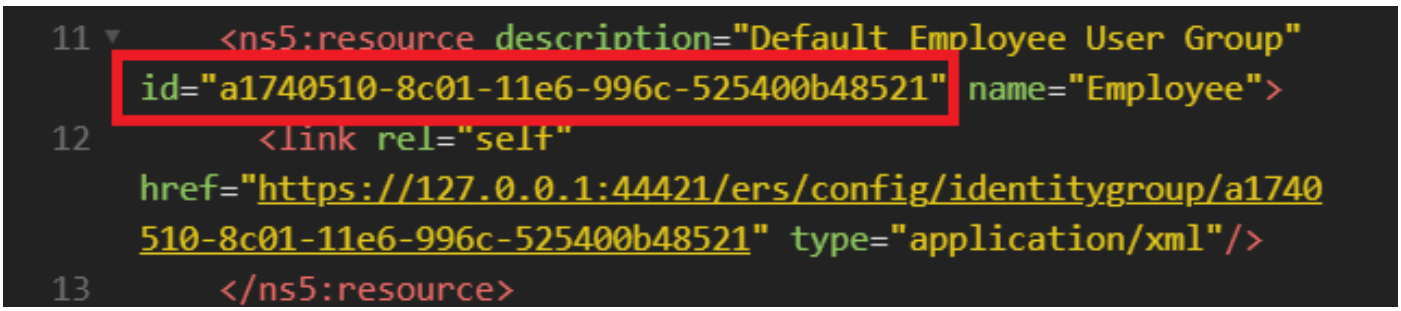
Verwenden Sie GET und die Abfrage https://X.X.X.X/ers/config/identitygroup.



GET-Option

JSON-Ausgabe

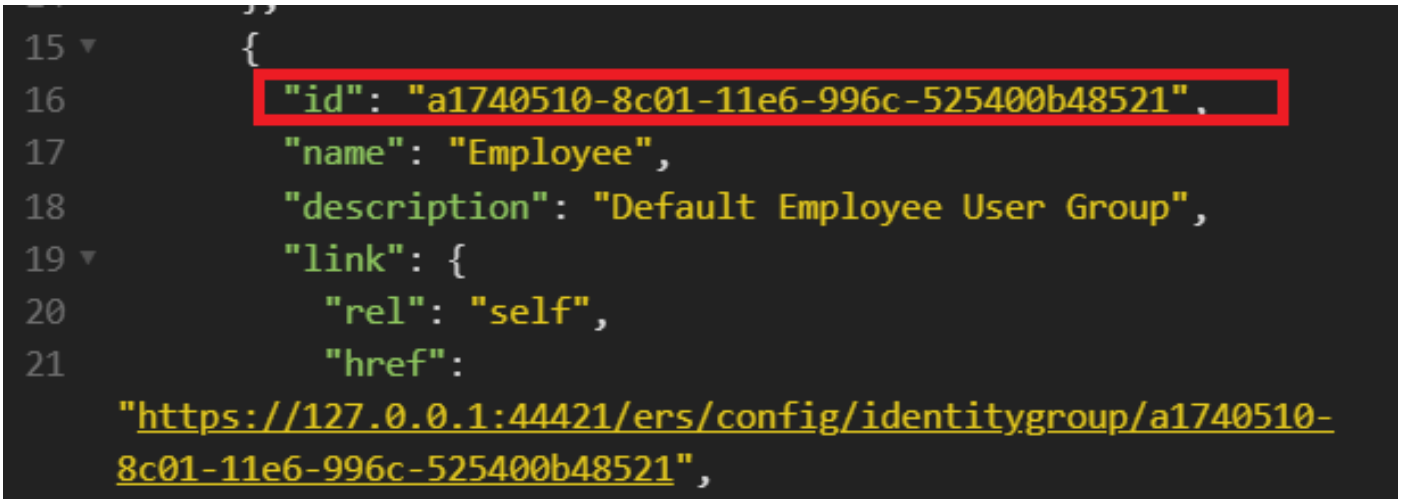
Geben Sie die ID neben der Beschreibung an.



ID-Identitätsgruppe 01

XML-Ausgabe.

Geben Sie die ID neben der Beschreibung an.



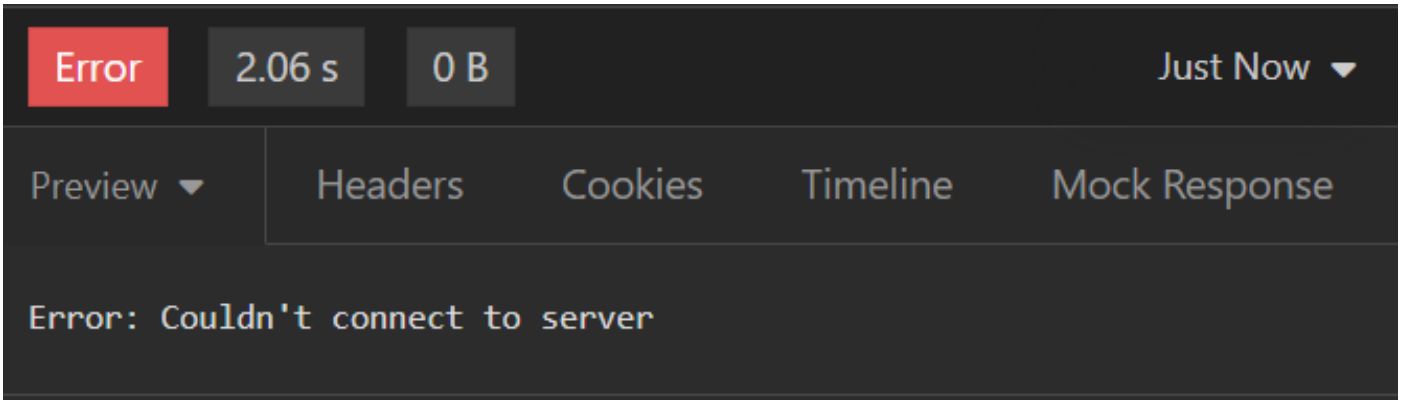
ID-Identitätsgruppe 02

2. 401 Unberechtigter Fehler.

401 Fehler

Lösung: Überprüfen Sie die im Abschnitt "Authentifizierung" konfigurierten Zugriffsberechtigungen.

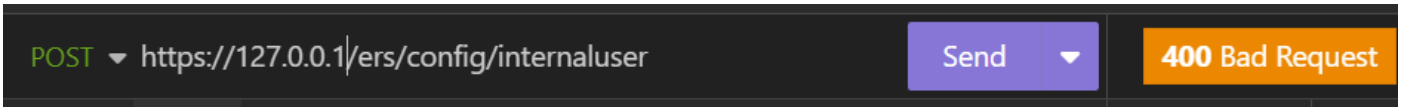
3. Fehler: Verbindung zum Server konnte nicht hergestellt werden



Verbindungsfehler

Lösung: Überprüfen Sie die IP-Adresse des in Schlaflosigkeit konfigurierten ISE-Knotens, oder validieren Sie die Verbindung.

4. 400 Unzulässige Anfrage.

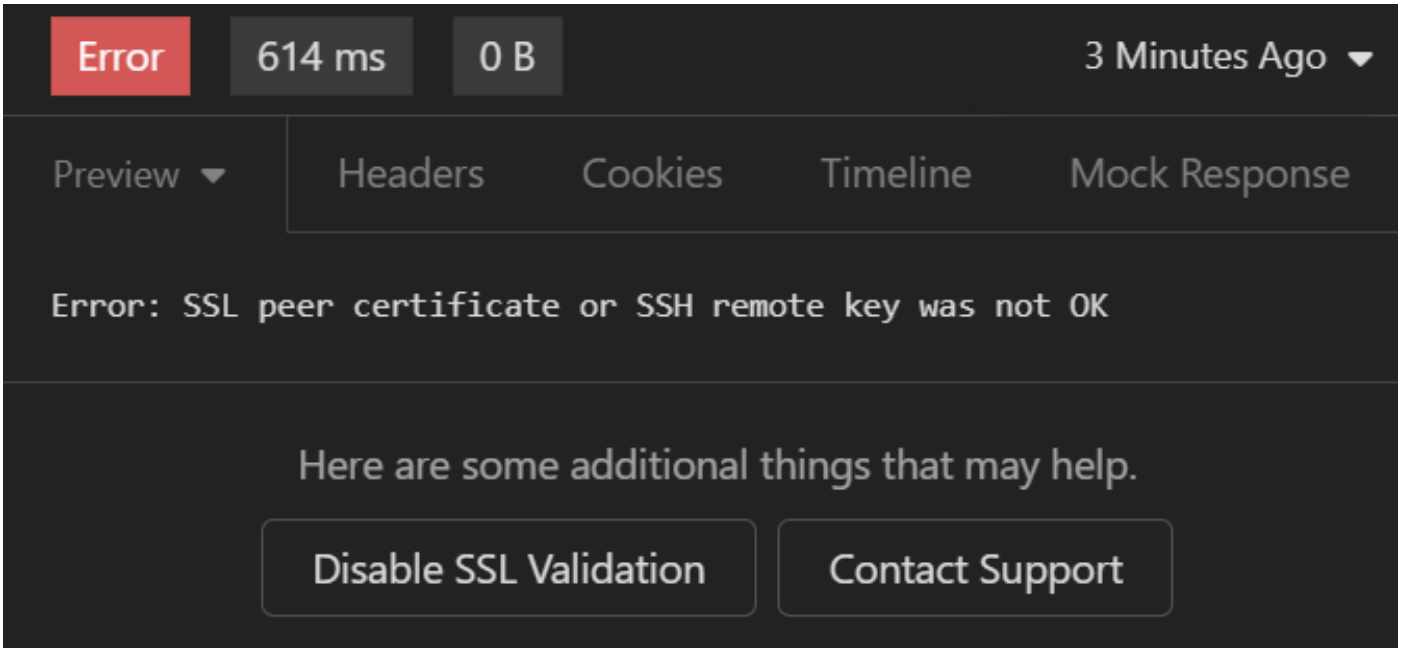


400 Fehler

Es gibt mehrere Gründe für diesen Fehler, die häufigsten sind:

- stimmt nicht mit der Richtlinie für Sicherheitskennwörter überein
- Einige Parameter wurden falsch konfiguriert.
- Sintaxis-Fehler.
- Informationen dupliziert.

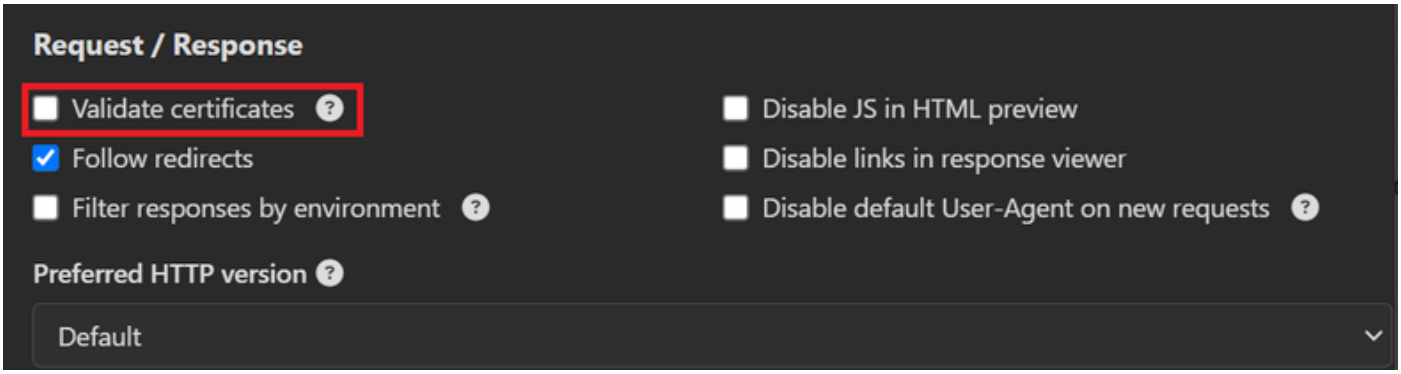
5. Fehler: SSL-Peer-Zertifikat oder SSH-Remote-Schlüssel war nicht OK



SSL-Zertifikatfehler

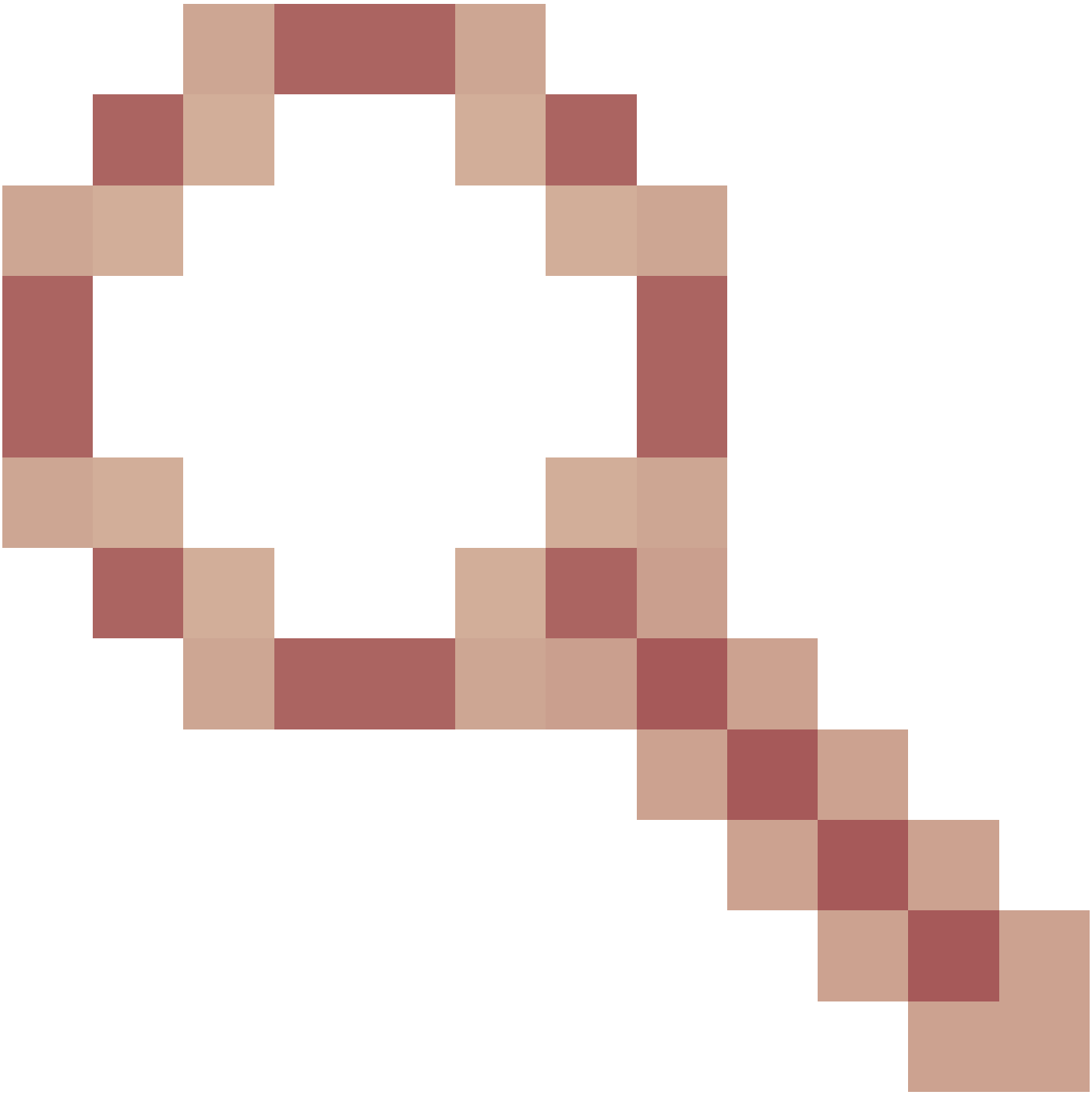
Lösung:

1. Klicken Sie auf SSL-Validierung deaktivieren.
2. Deaktivieren Sie unter Anforderung/Antwort die Option Zertifikate validieren.



Option Zertifikate überprüfen

6. CSCwh71435



defekt.

Das enable-Kennwort wird nach dem Zufallsprinzip konfiguriert, obwohl Sie es nicht konfiguriert haben. Dieses Verhalten tritt auf, wenn die enable password-Syntax entfernt oder als Wert leer gelassen wird. Unter dem nächsten Link finden Sie weitere Informationen:

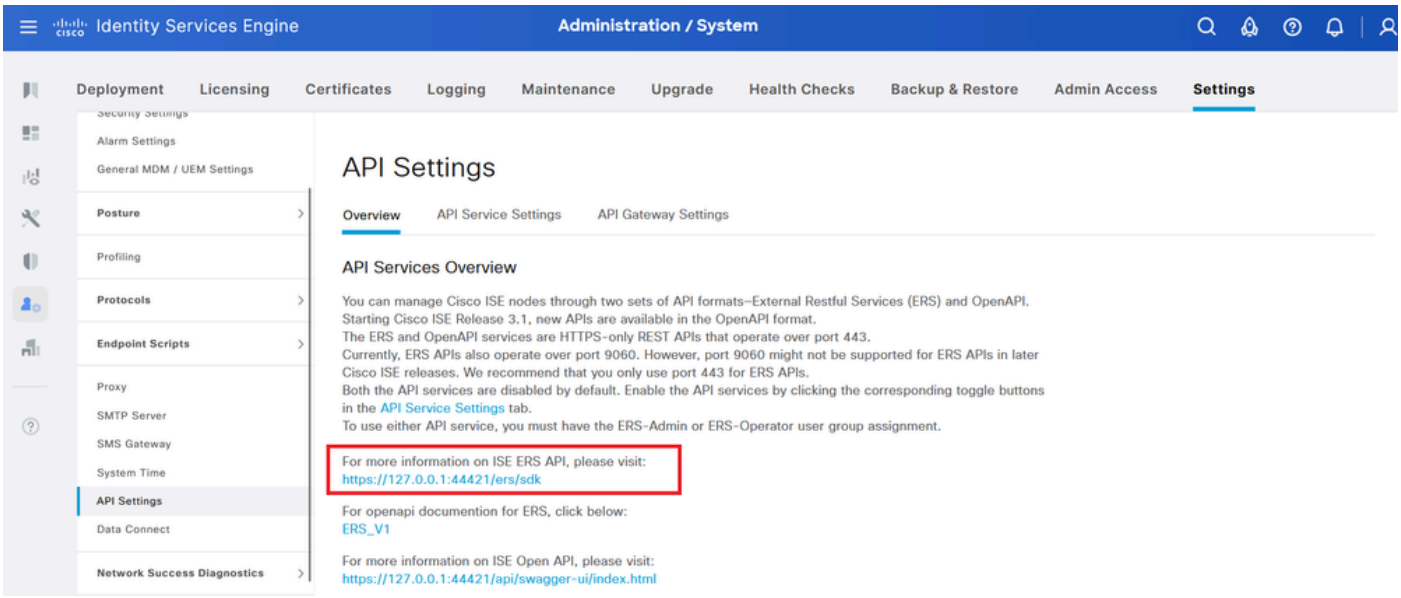
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh71435

API-Aufrufreferenzen.

Sie können alle Informationen zu den API-Aufrufen sehen, die von der ISE unterstützt werden.

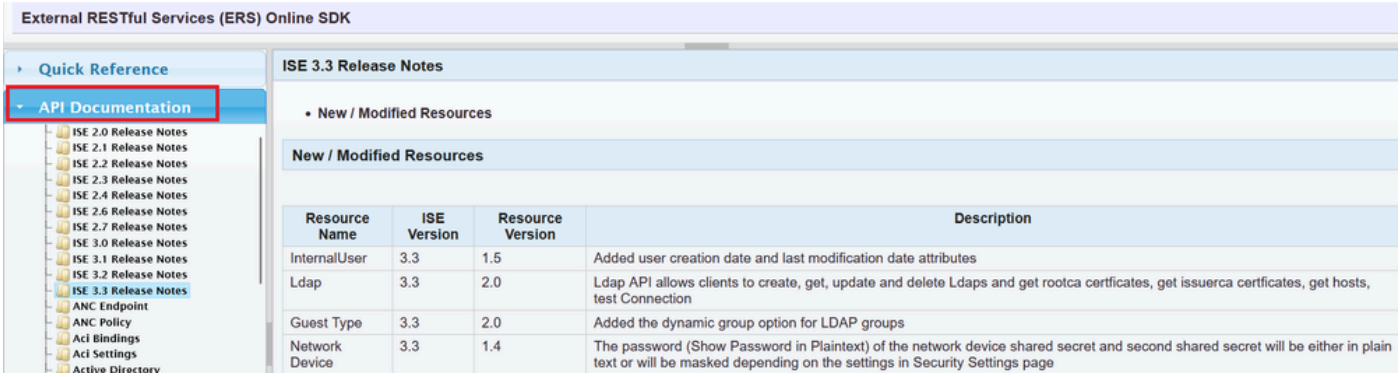
1. Navigieren Sie zu Administration > System > Settings > API Setting.

2. Klicken Sie auf den Informationslink zur ERS API.



API-Einstellungen

3. Und klicken Sie auf API-Dokumentation.



API-Dokumentation

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.