

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

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

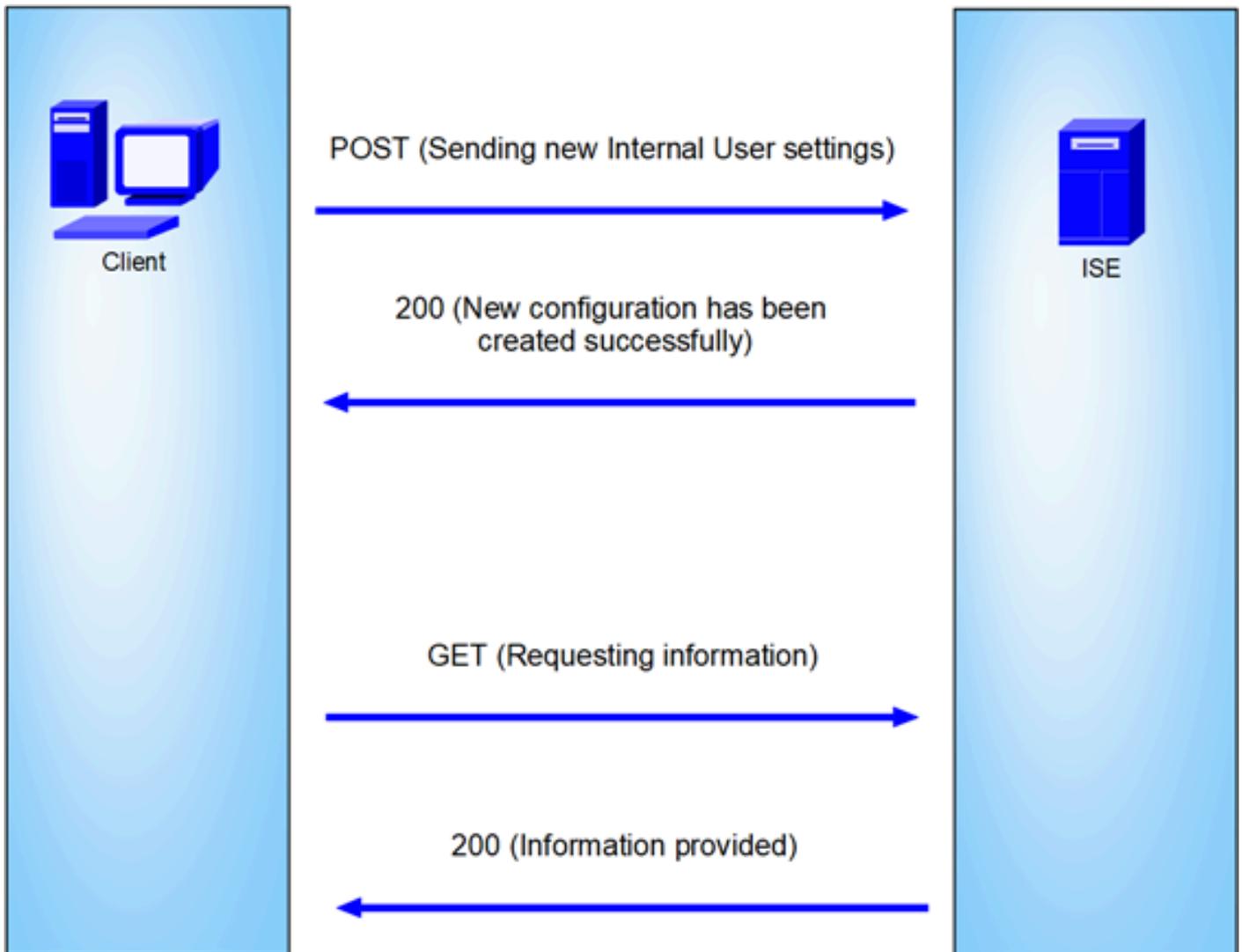
- ISE 3.0 oder höher
- API-Client-Software.

Verwendete Komponenten

- ISE 3.3
- Insomnia 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

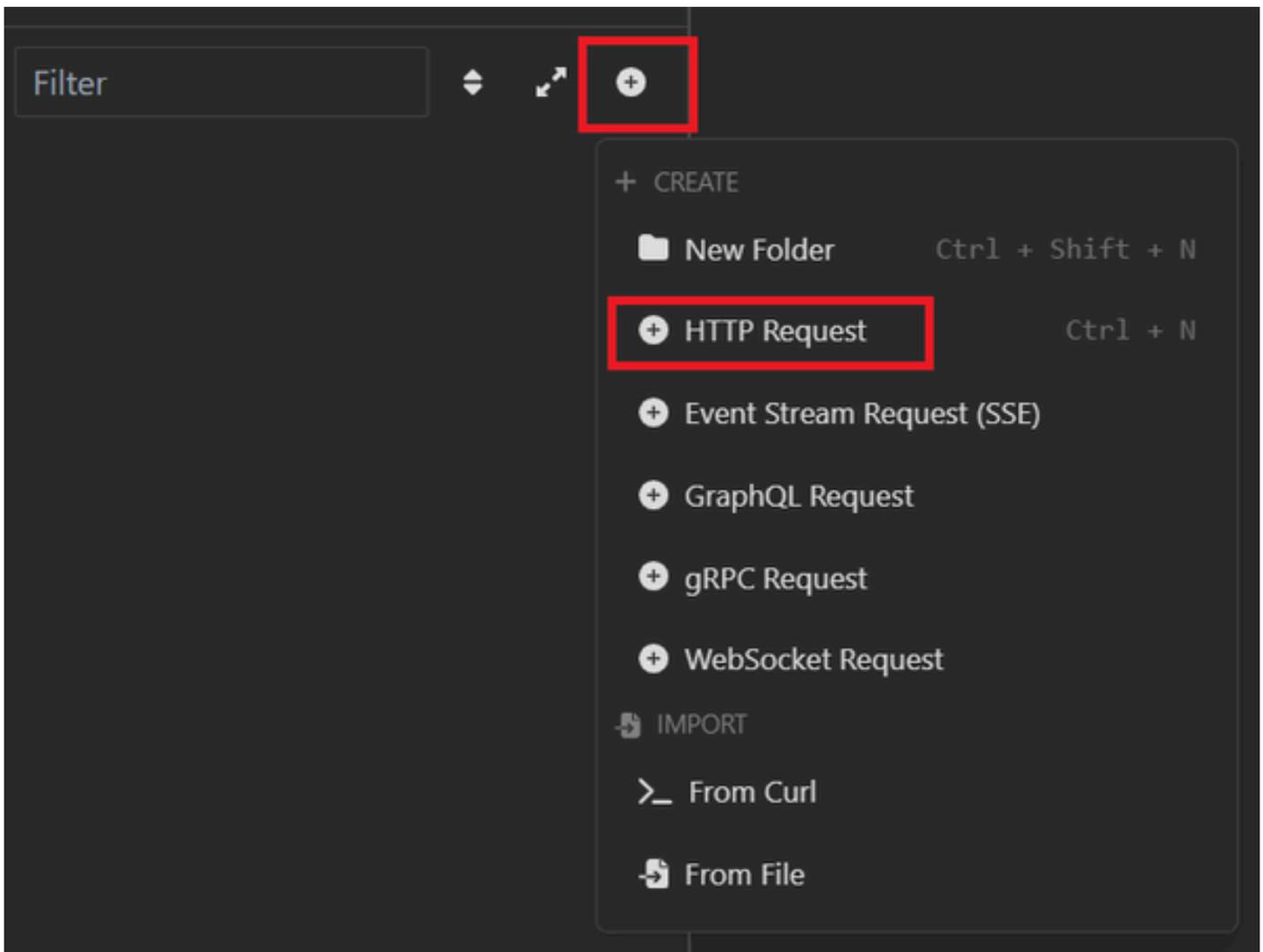
1. Navigieren Sie zu Administration > System > Settings > API Settings > API Service Settings.
2. Aktivieren Sie die ERS-Option (Lesen/Schreiben).

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' 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, 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.

API-Einstellungen

JSON-Anfrage.

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

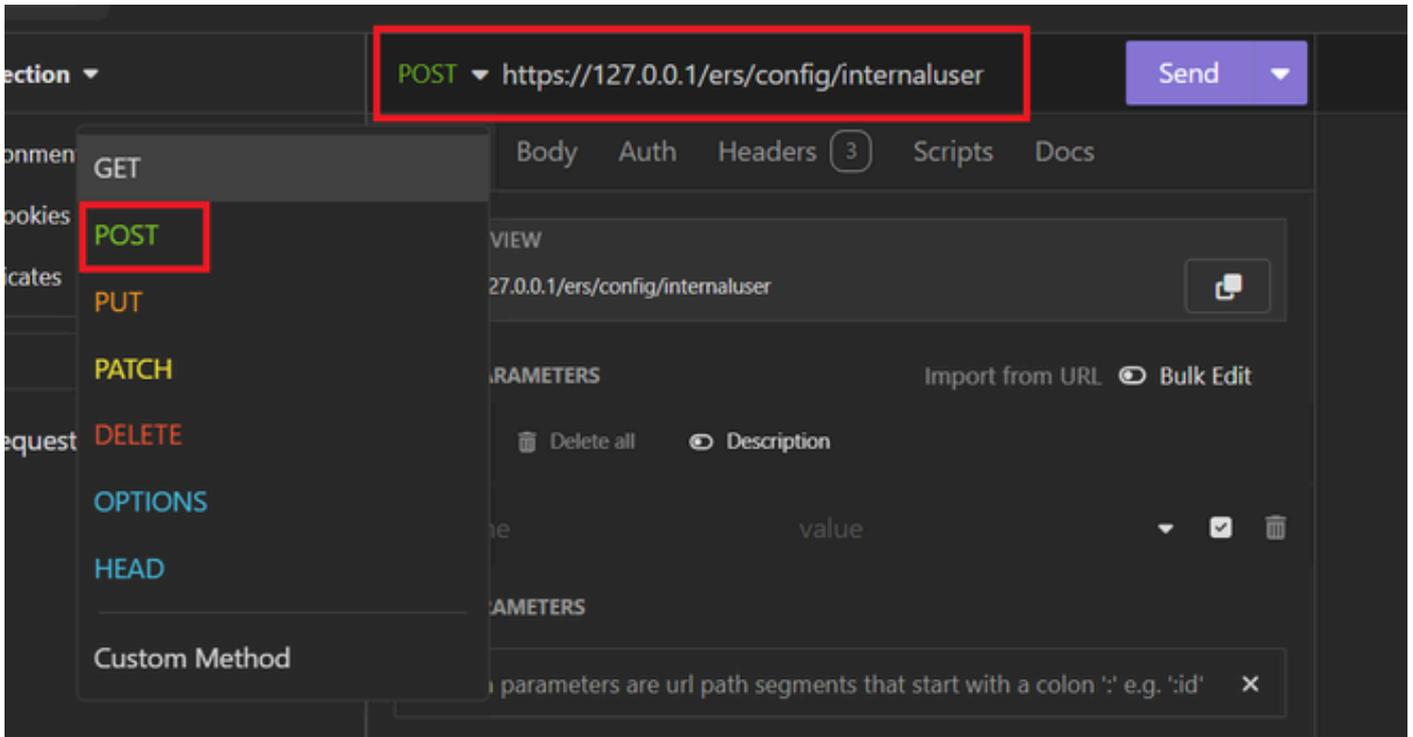


JSON-Anforderung

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

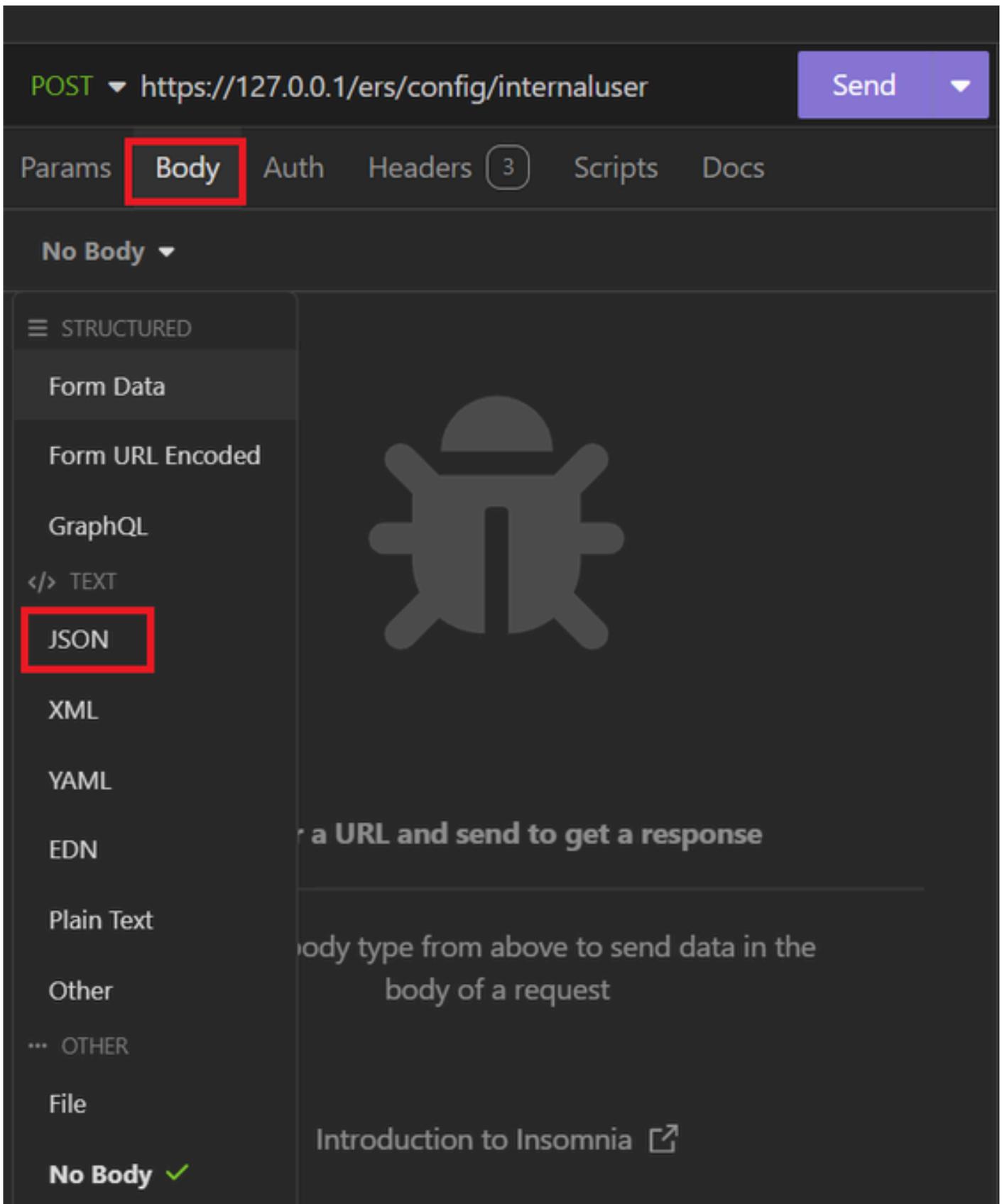
Die einzugebende URL hängt von der IP-Adresse des ISE-Knotens ab.

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.

```
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 }
```

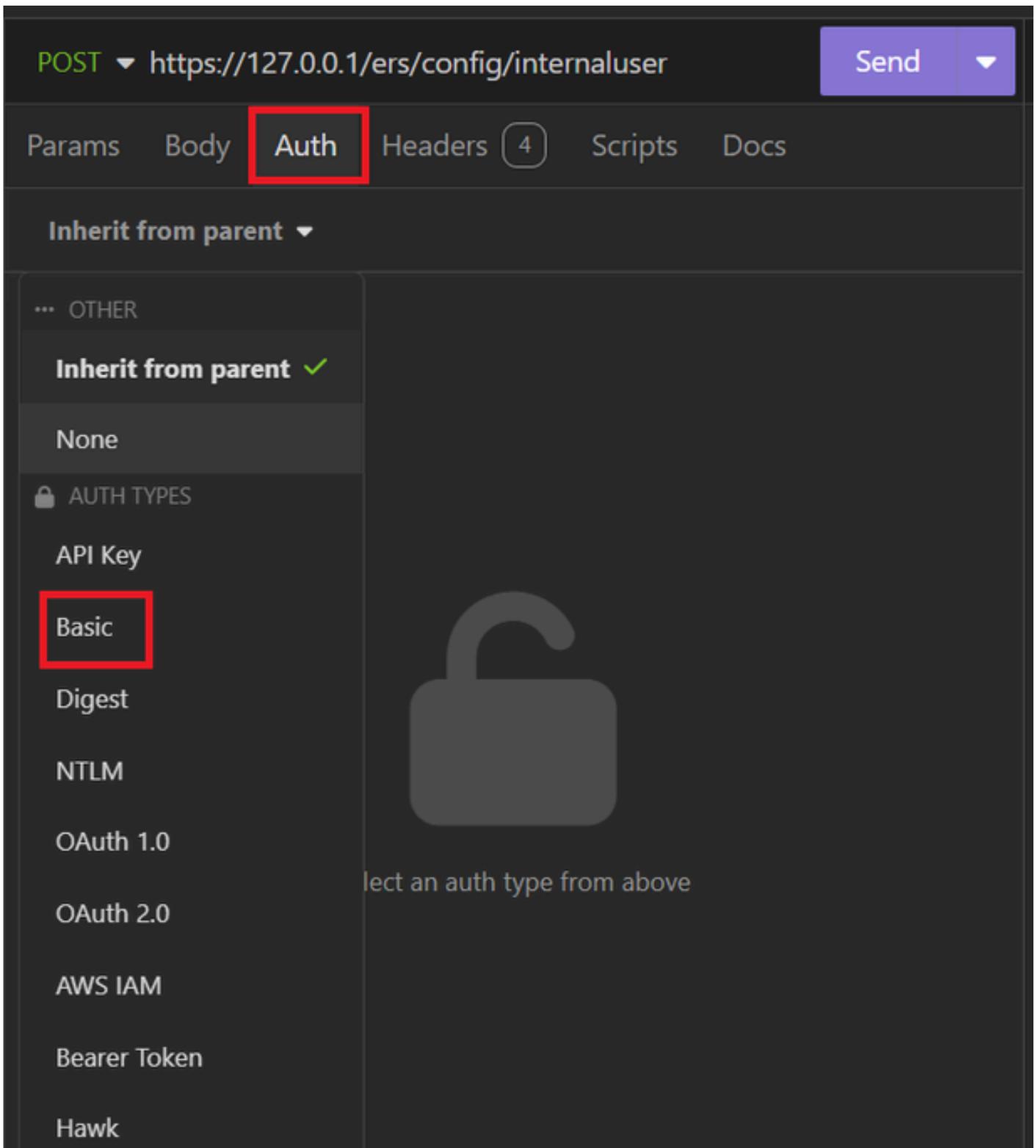
JSON-Syntax

JSON-Syntax

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

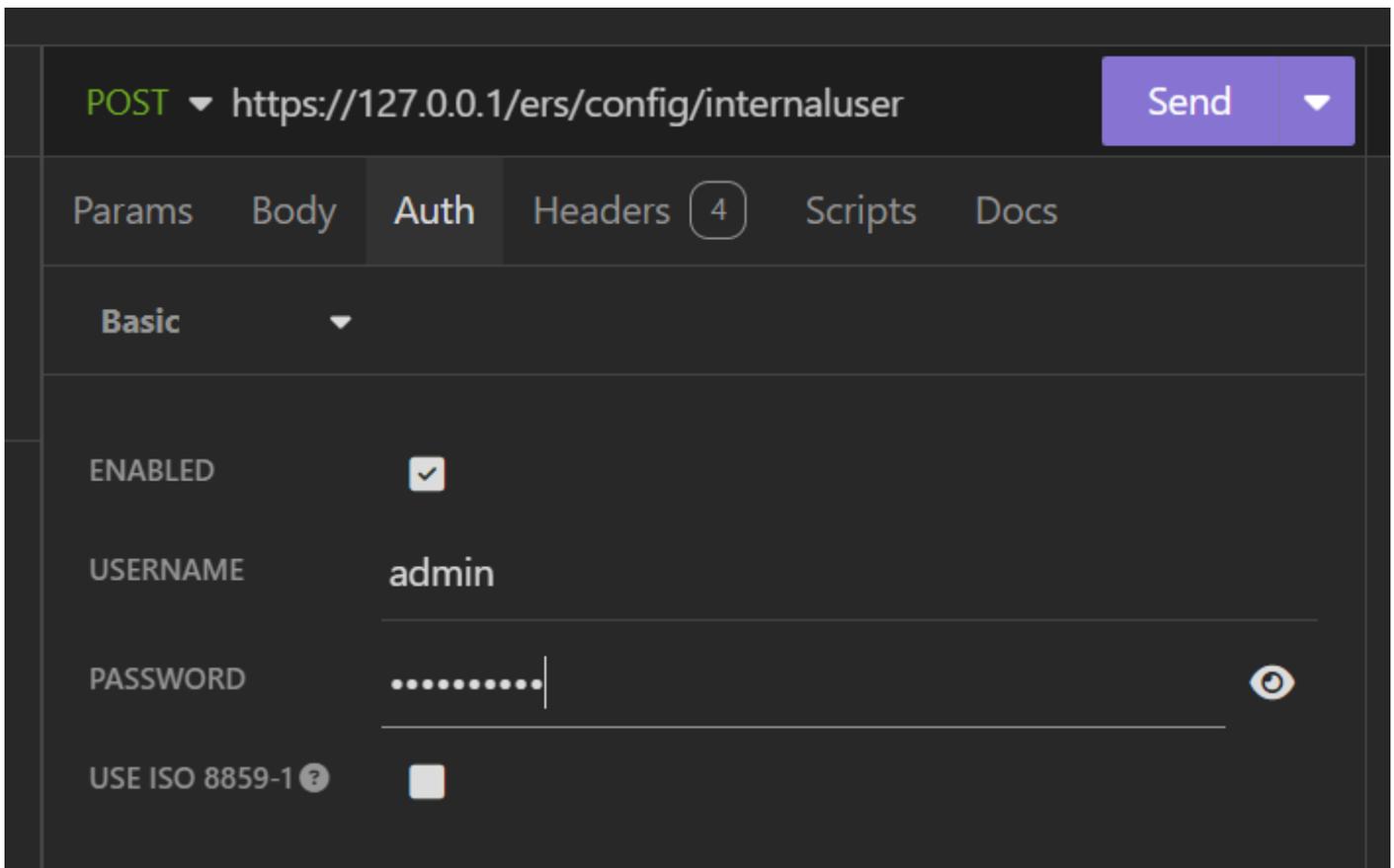
```
"password": "password",
"firstName": "firstName",
"lastName": "lastName",
"changePassword": true,
"identityGroups": "identityGroups",
"passwordNeverExpires": false,
"daysForPasswordExpiration": 60,
"expiryDateEnabled": false,
"expiryDate": "2016-12-11",
"enablePassword": "enablePassword",
"dateModified": "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

POST ▼ https://127.0.0.1/ers/config/internaluser Send ▼

Params Body Auth **Headers** 4 Scripts Docs

+ Add 🗑 Delete all 👁 Description

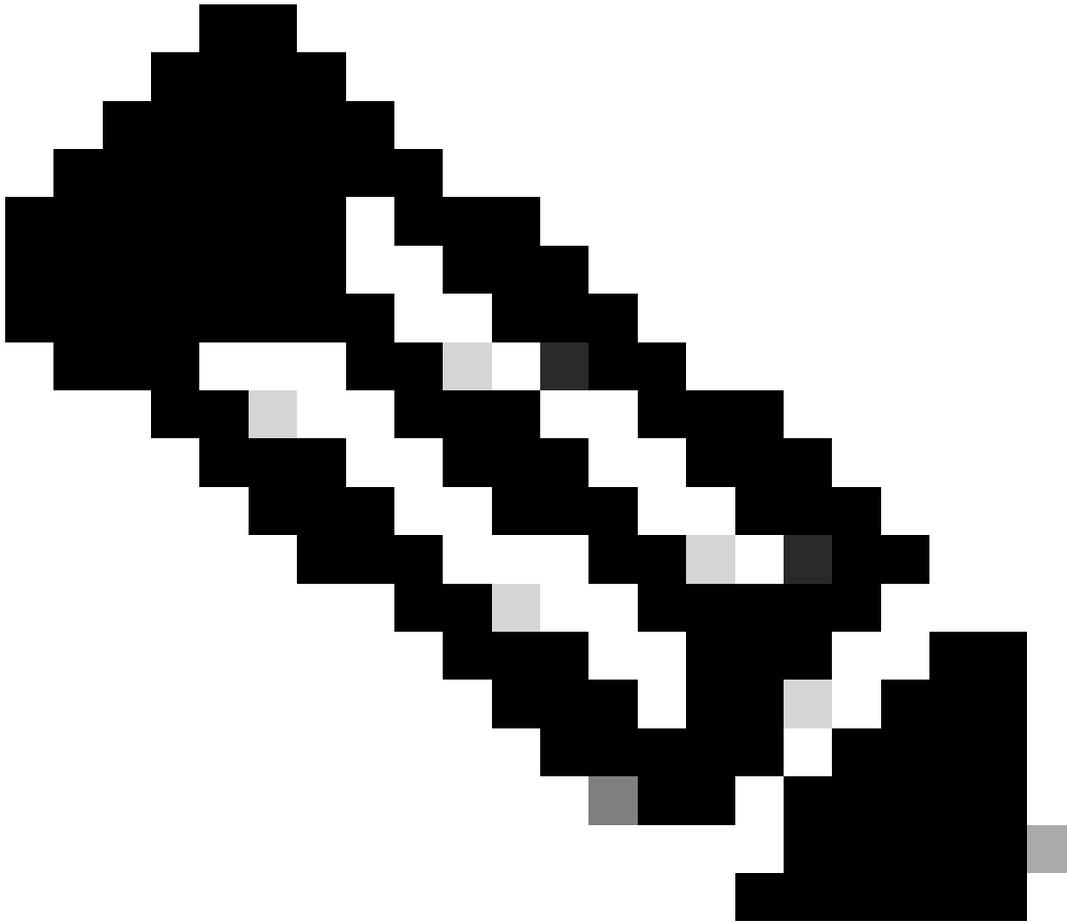
Accept */*

Host <calculated at runtime>

☰	Content-Type	application/json	▼	☑	🗑
☰	Accept	application/json	▼	☑	🗑

JSON-Header

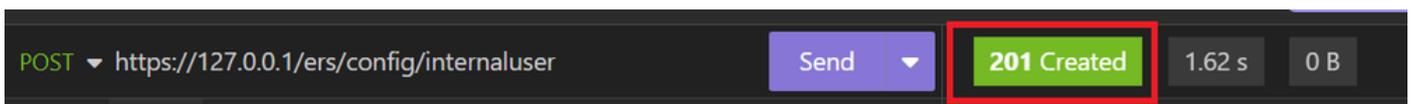
9. Klicken Sie abschließend auf Senden.



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**.

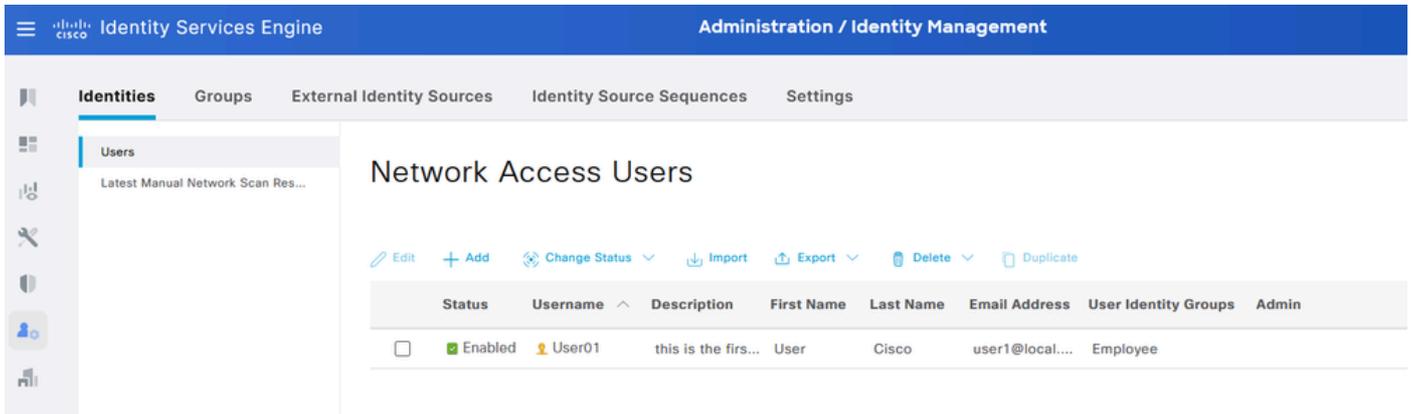
Validierung

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

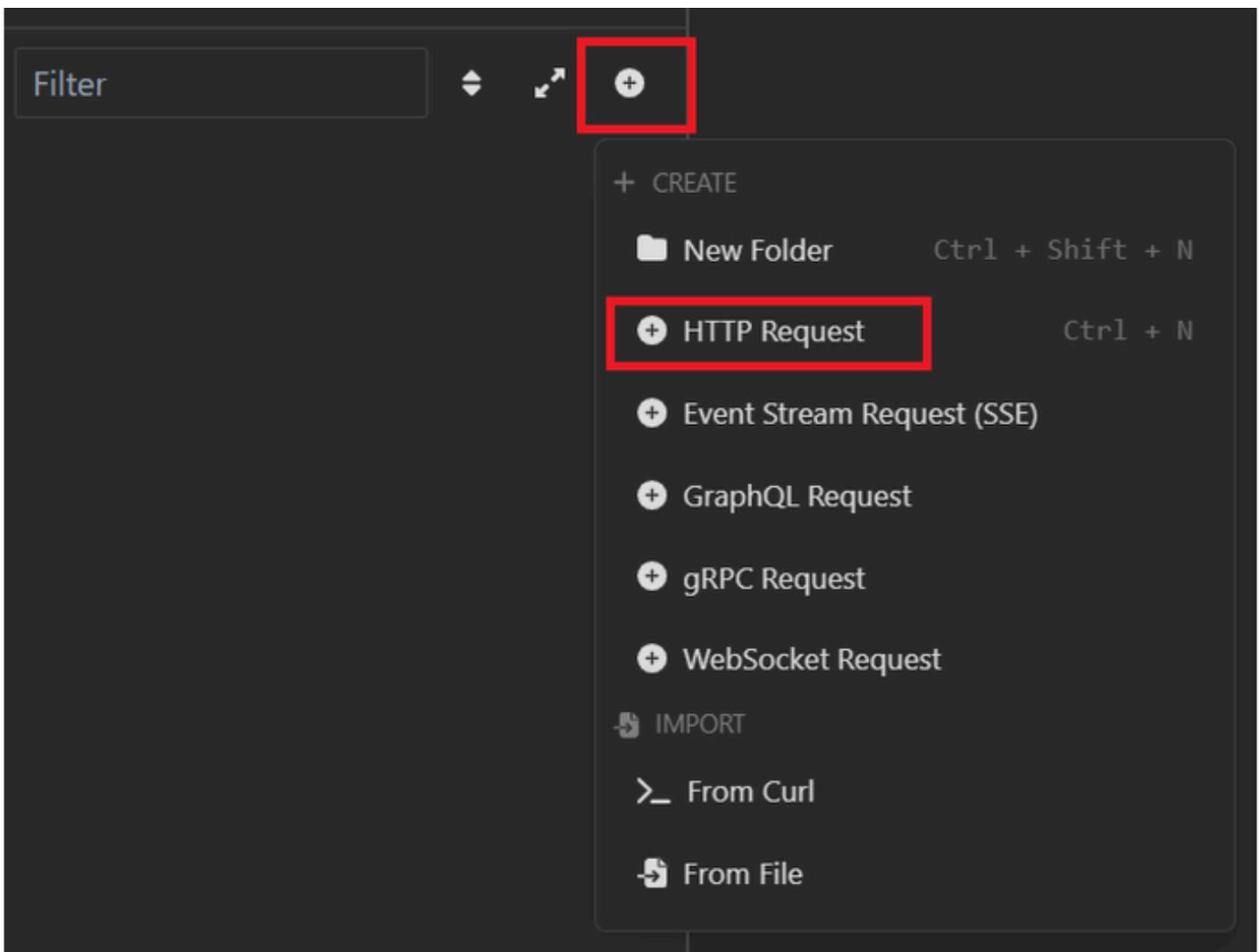
2. Öffnen Sie die ISE-GUI, und navigieren Sie zu Administration > Identity Management > Identities > Users > Network Access Users



JSON-Benutzerkonto

XML-Anforderung

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

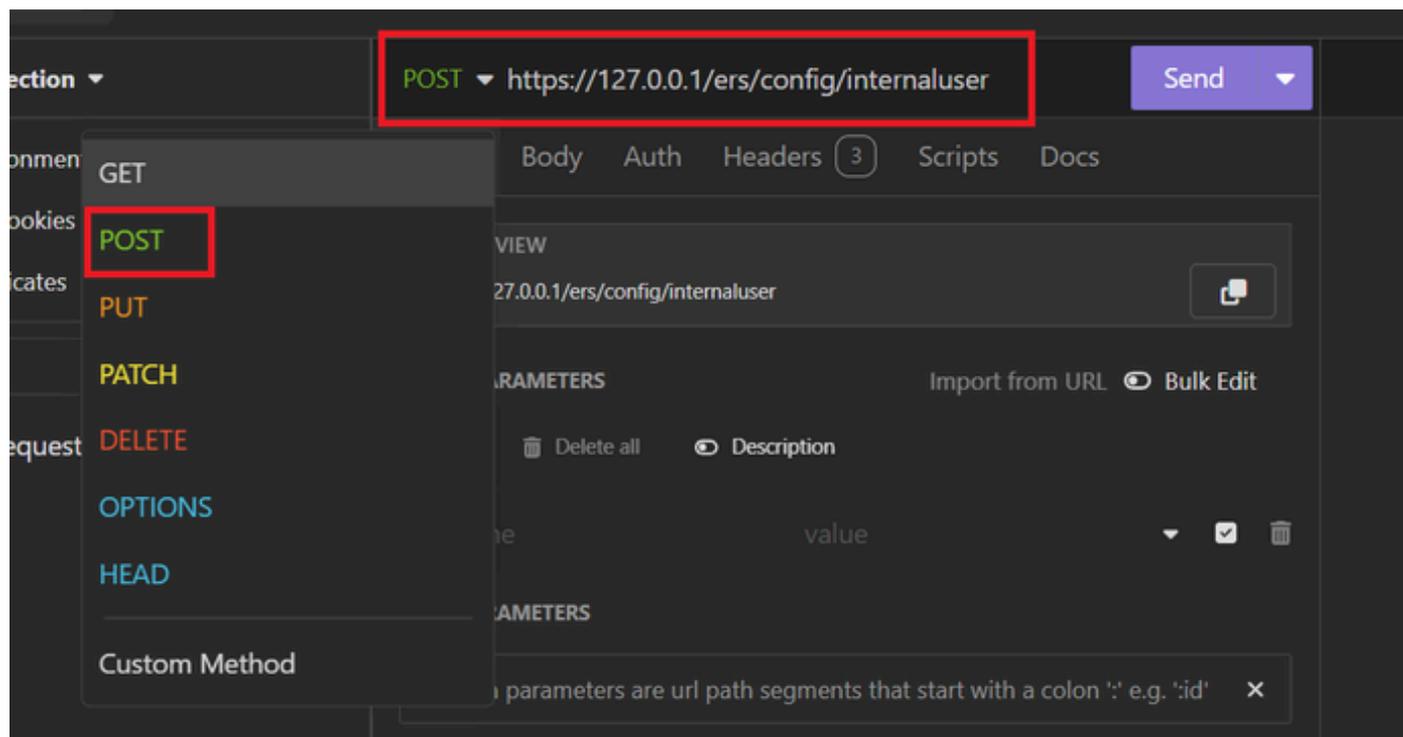


XML-Anforderung

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

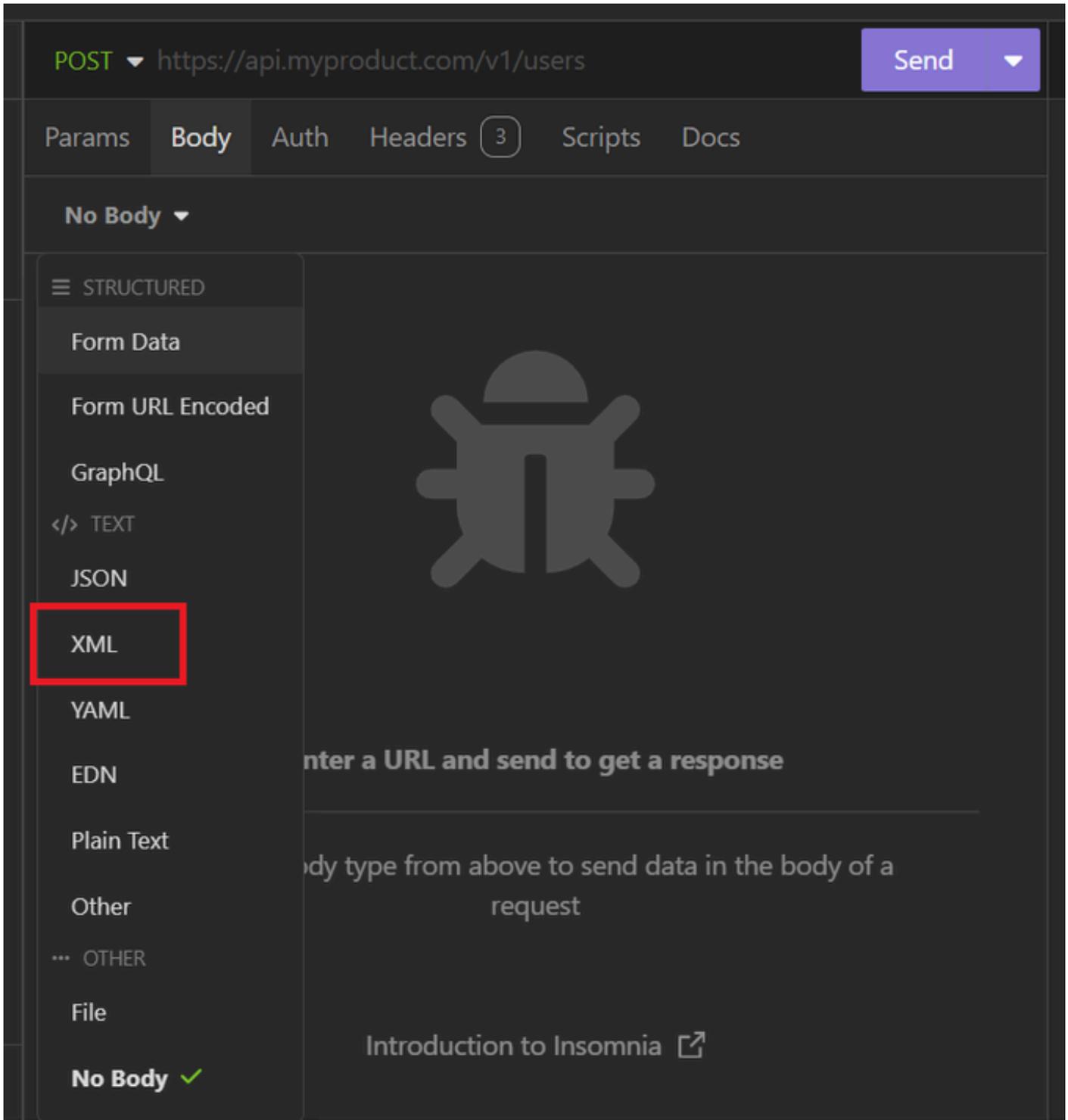
Die einzugebende URL hängt von der IP-Adresse des ISE-Knotens ab.

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.

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-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
```

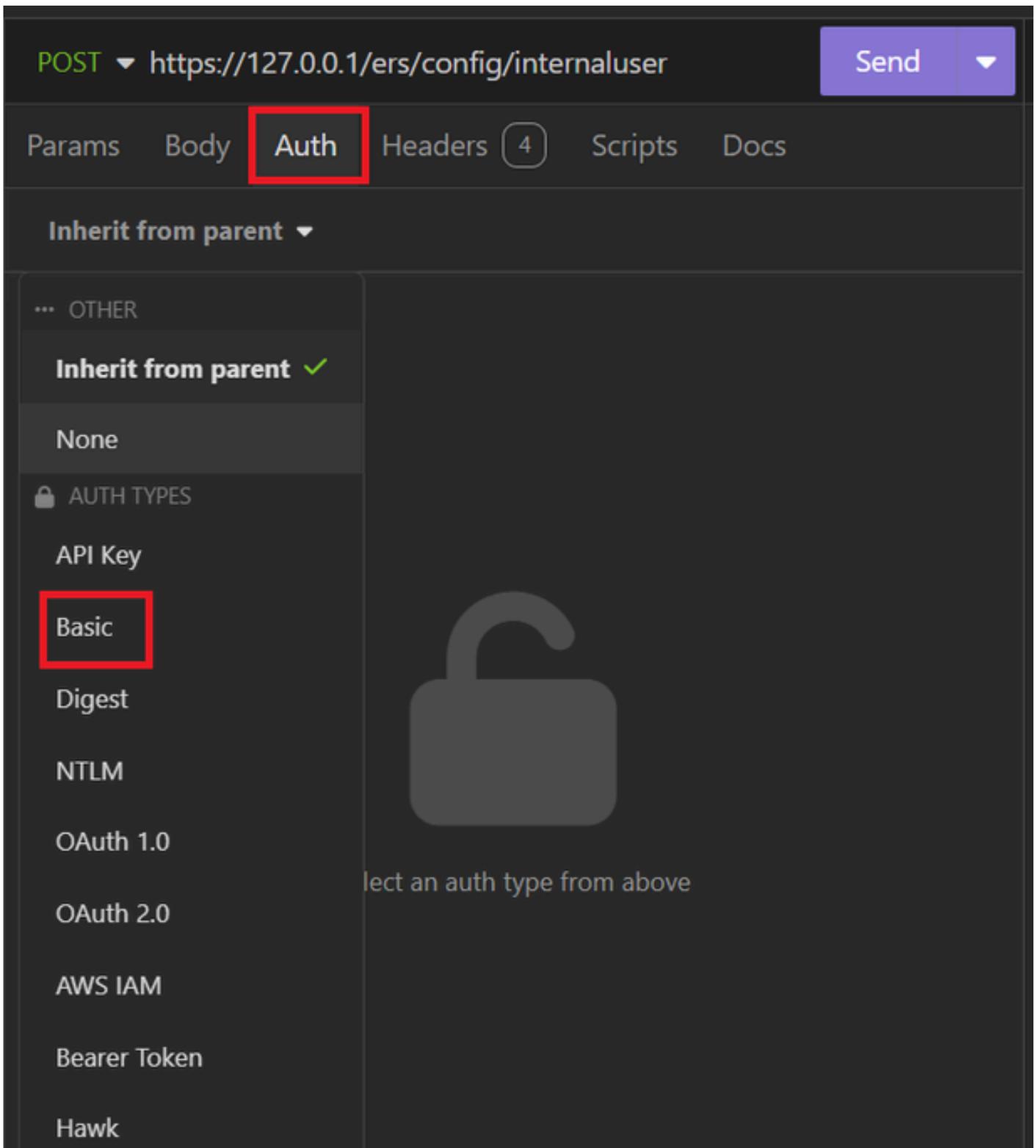
```
  <accountNameAlias>accountNameAlias</accountNameAlias>
```

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

```
  <customAttributes>
```

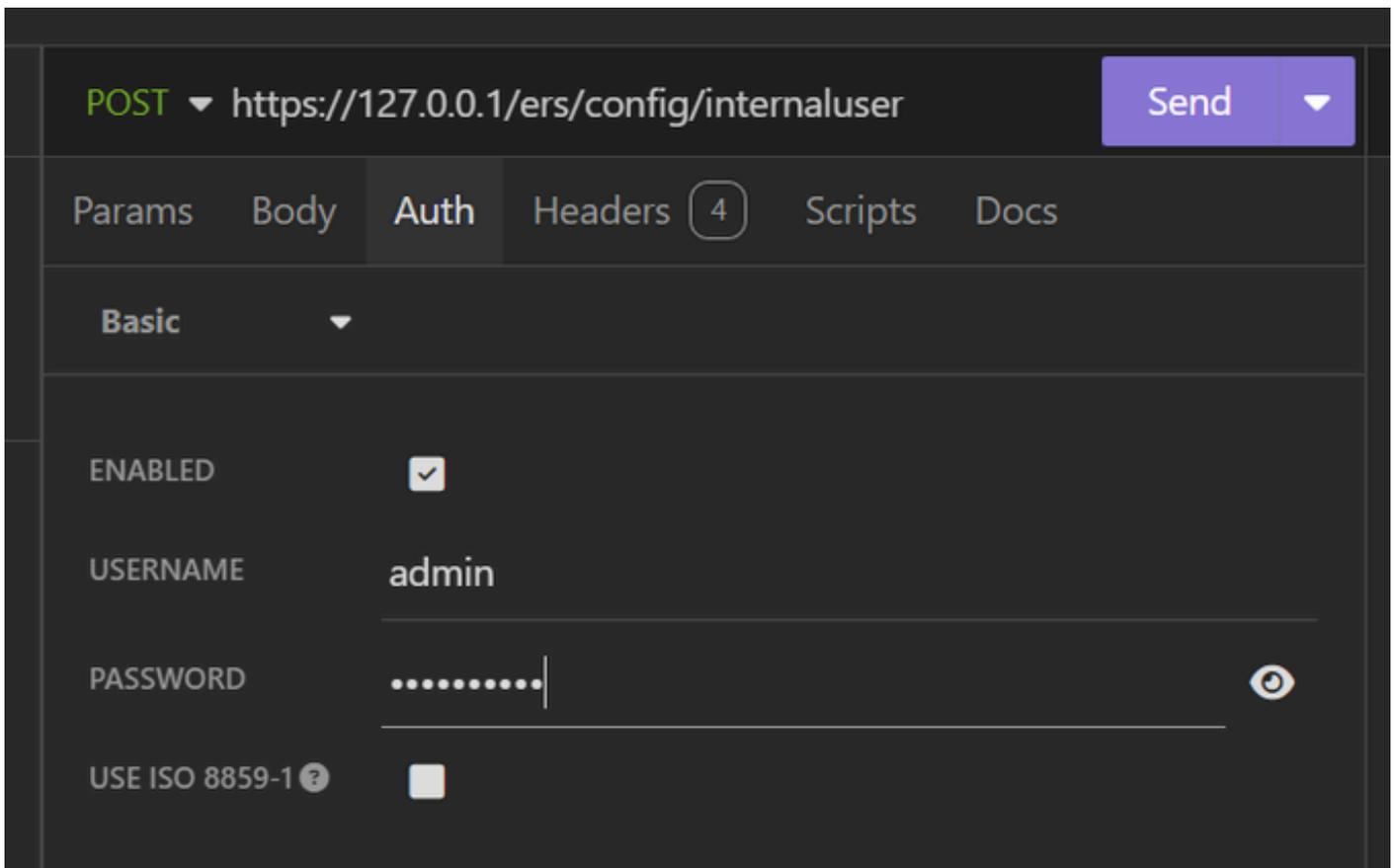
```
<entry>
  <key>key1</key>
  <value>value1</value>
</entry>
<entry>
  <key>key2</key>
  <value>value3</value>
</entry>
</customAttributes>
<dateCreated>2015-12-15</dateCreated>
<dateModified>2015-12-20</dateModified>
<daysForPasswordExpiration>60</daysForPasswordExpiration>
<email>email@domain.com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



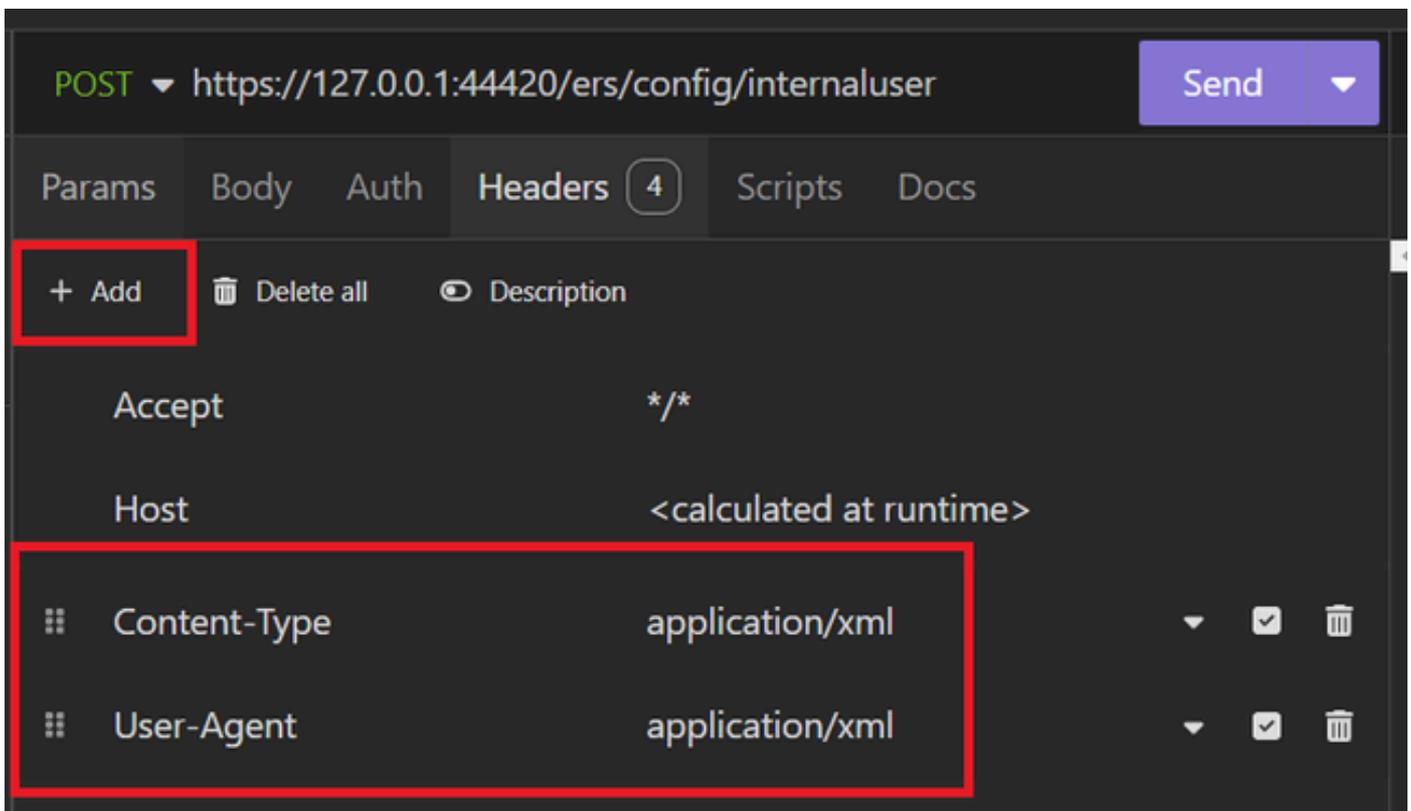
XML-Authentifizierung

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



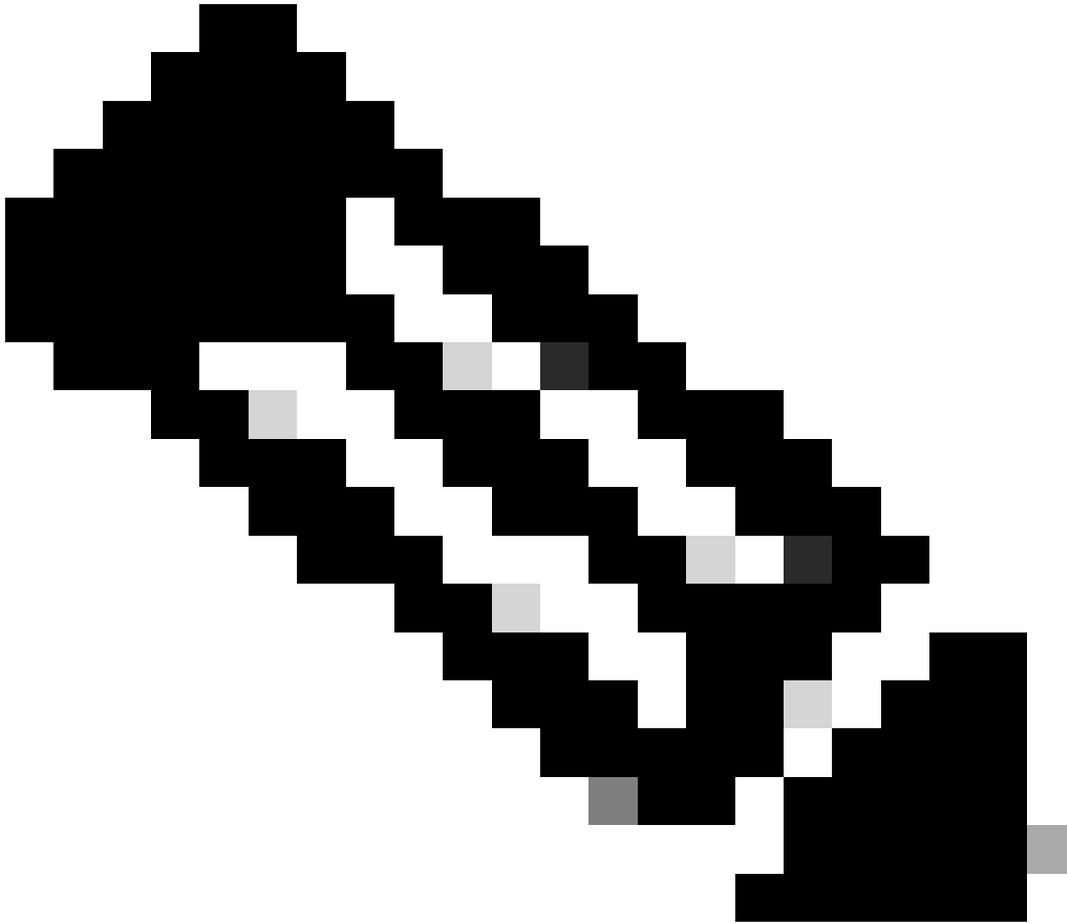
XML-Anmeldeinformationen

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



XML-Header

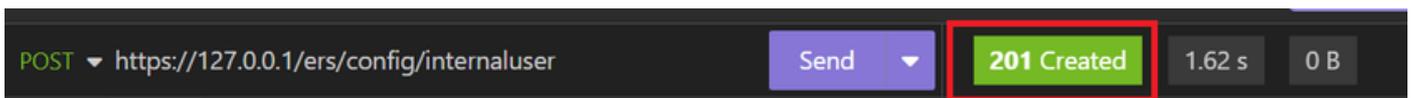
9. Klicken Sie abschließend auf Senden.



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

Network Access Users

Selected 0 Total 2  

 Edit  + Add  Change Status  Import  Export  Delete  Duplicate  All 

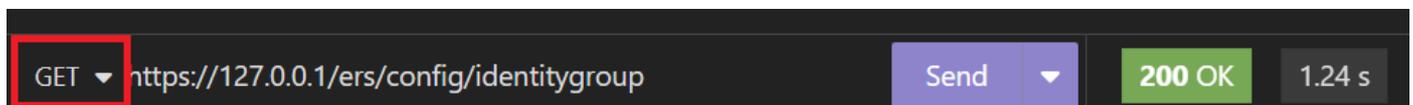
Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	 Enabled  User01	this is the firs...	User	Cisco	user1@local...	Employee	 User Account created by JSON
<input type="checkbox"/>	 Enabled  User02	description	User2	Cisco	user2@local...	Employee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

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.

```
11 <ns5:resource description="Default Employee User Group"
    id="a1740510-8c01-11e6-996c-525400b48521" name="Employee">
12   <link rel="self"
    href="https://127.0.0.1:44421/ers/config/identitygroup/a1740
    510-8c01-11e6-996c-525400b48521" type="application/xml"/>
13 </ns5:resource>
```

ID-Identitätsgruppe 01

XML-Ausgabe.

Geben Sie die ID neben der Beschreibung an.

```
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-Identitätsgruppe 02

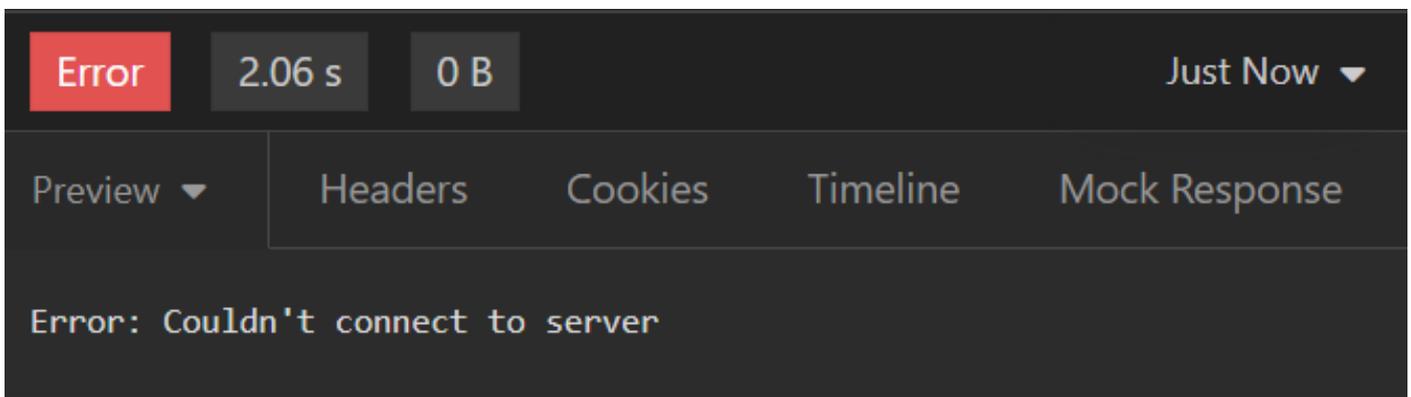
2. 401 Unberechtigter Fehler.



401 Fehler

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

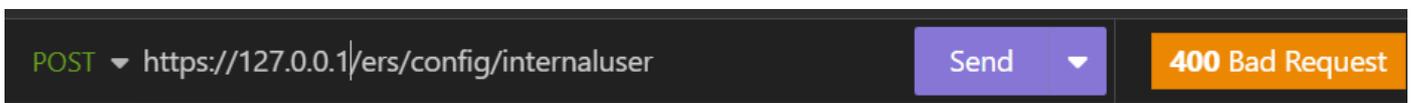
3. Fehler: Verbindung zum Server konnte nicht hergestellt werden



Verbindungsfehler

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

4. 400 Unzulässige Anfrage.

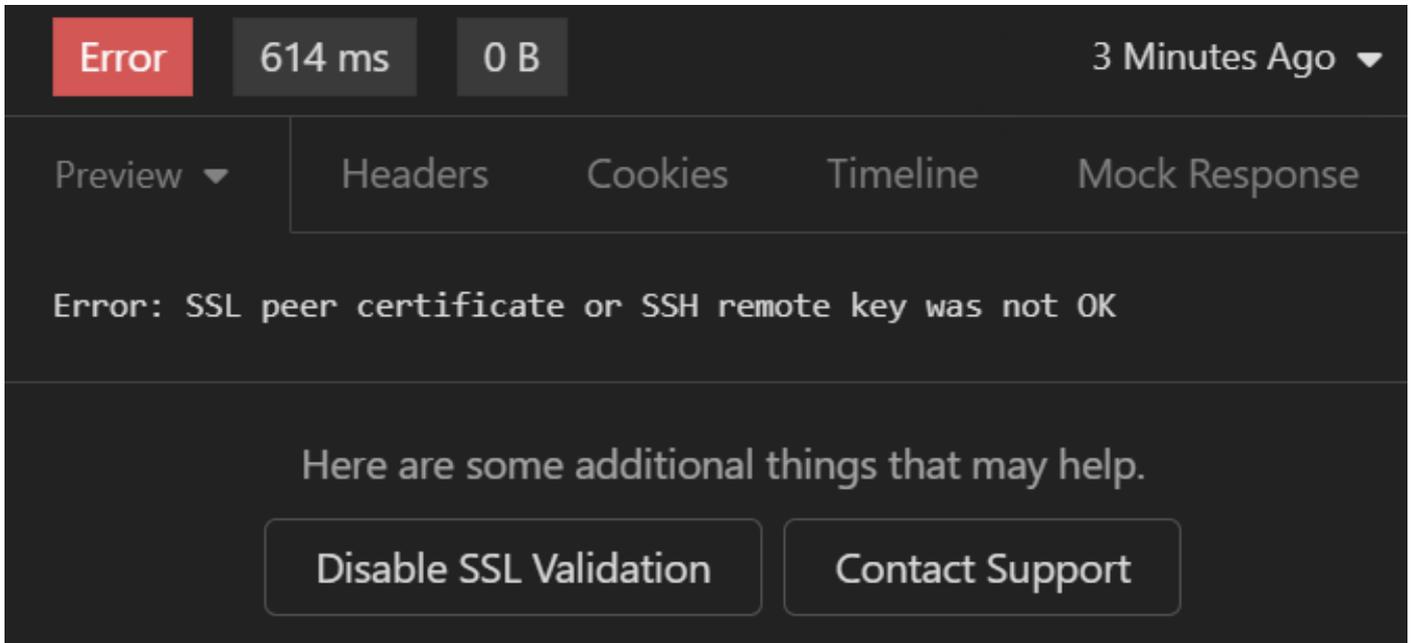


400 Fehler

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.

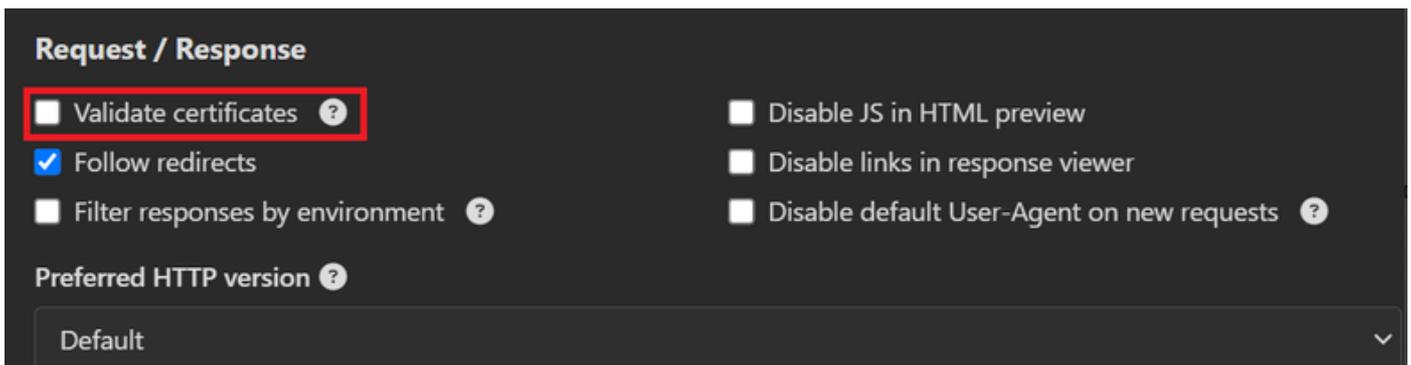
5. Fehler: SSL-Peer-Zertifikat oder SSH-Remote-Schlüssel war nicht OK



SSL-Zertifikatfehler

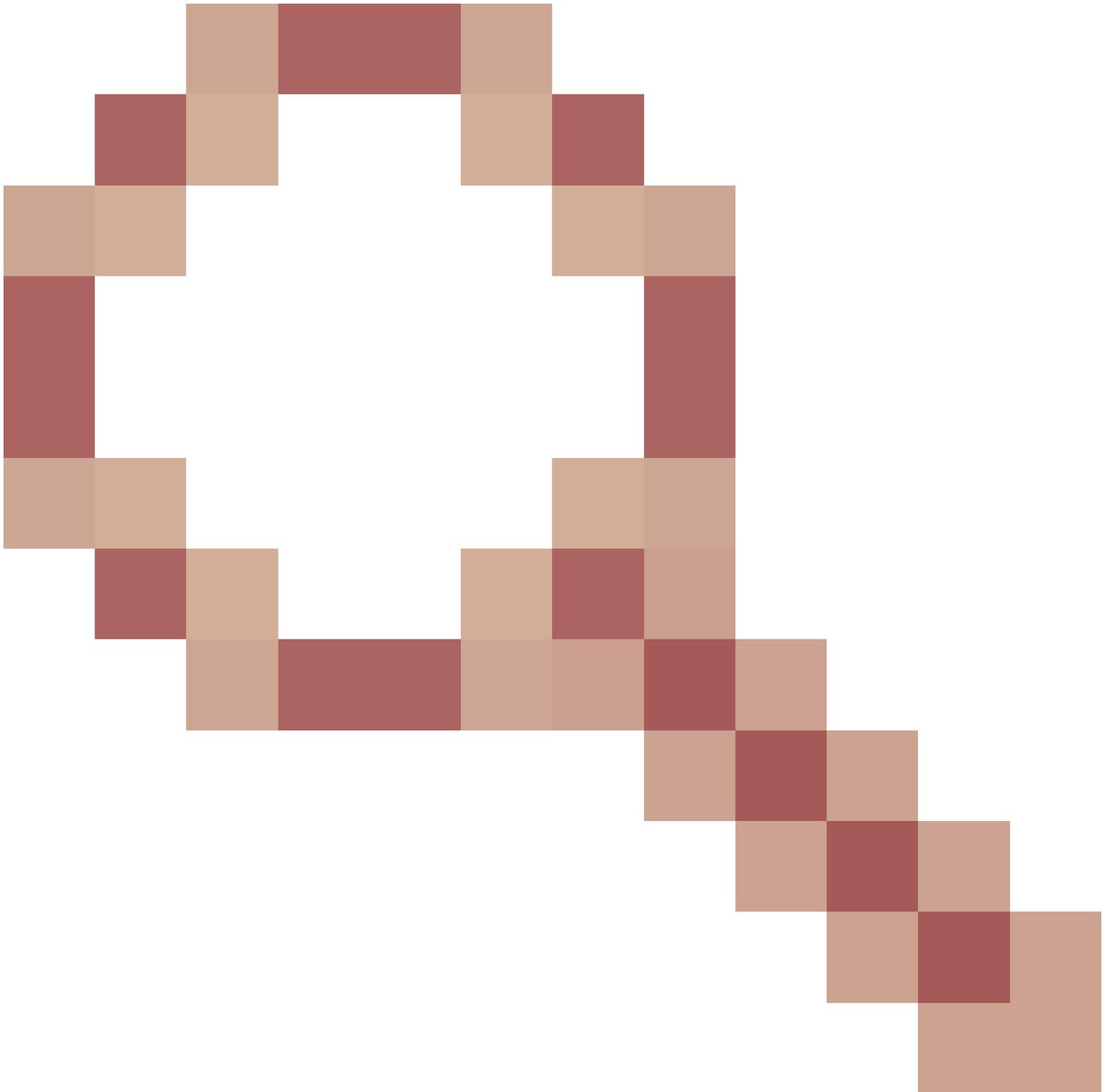
Lösung:

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.

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. This section 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 operating on port 443. ERS APIs also operate on port 9060, but this port may not be supported in later releases. 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>.

API-Einstellungen

3. Und klicken Sie auf API-Dokumentation.

The screenshot shows the 'External RESTful Services (ERS) Online SDK' page. The left sidebar has a 'Quick Reference' section with a sub-section 'API Documentation' highlighted by a red box. Below this, a list of release notes is shown, with 'ISE 3.3 Release Notes' selected. The main content area is titled 'ISE 3.3 Release Notes' and contains 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

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.