

REST APIを使用したISEゲストアカウントの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ISEでのERSの有効化](#)

[ERSの管理者およびスポンサーアカウントの設定](#)

[ゲストアカウントの作成](#)

[ゲストデータの読み取り、更新、削除](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Representational State Transfer (REST) API機能を使用して、Identity Services Engine (ISE) でゲスト関連のタスクを実行する方法について説明します。Cisco Guest APIは、RESTベースの一連の操作で、シスコのゲストユーザを管理するためのセキュアなHTTPSおよび認証されたアクセスを提供します。APIを使用すると、ゲストユーザを作成、読み取り、更新、削除、および検索できます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ISE
- 外部RESTfulサービス
- 不眠症、休眠状態などのRESTクライアント

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE、リリース 2.6
- Insomnia REST client v7.1.1

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、初期（デフォルト）設定の状態から起動しています。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。

注：この手順は、他のISEバージョンと同じか、同じです。特に明記されていない限り、すべての2.x ISEソフトウェアリリースで次の手順を使用できます。

背景説明

APIを使用するには、外部RESTfulサービス(ERS)を有効にし、スポンサー認証をISEで設定する必要があります。ERSは基本認証をサポートし、ポート9060で実行されます。認証クレデンシャルは暗号化され、要求ヘッダーの一部です。ERSでは、操作を実行するためにISE管理者がユーザに特別な権限を割り当てる必要があります。

このドキュメントでは、次の設定手順について説明します。

1. ISEでのERSの有効化
2. ERSの管理者およびスポンサーアカウントの設定
3. ゲストアカウントの作成
4. ゲストデータの読み取り、更新、削除

設定

ISEでのERSの有効化

ISEでREST API機能を使用するには、ERSを有効にする必要があります。

図に示すように、[Administration] > [System] > [Settings] > [ERS settings] > [Enable ERS for read/write]に移動します。

ERS Settings

▼ General

External RESTful Services (ERS) is a REST API based on HTTPS over port 9060.
The ERS service is disabled by default.
An ISE Administrator with the "ERS-Admin" or "ERS-Operator" group assignment is required to use the API.
For more information, please visit the ERS SDK page at:
[https://\[redacted\]:9060/ers/sdk](https://[redacted]:9060/ers/sdk)

▼ ERS Setting for Administration Node

- Enable ERS for Read/Write
 Disable ERS

▼ CSRF Check

- USE CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)
 Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)

ERSに関連するすべての情報は、ISEのHTTPSポート9060でソフトウェア開発キット(SDK)として利用できます。これは、ERSを有効にし、「ERS-Admin」または「ERS-Operator」の権限を持つ管理者アカウントでログインした後にアクセスできます。

ERSの管理者およびスポンサーアカウントの設定

ERSを使用するには、ISEにERS-AdminまたはERS-operatorの権限が割り当てられた管理者アカウントが必要です。管理者アカウントを作成し、それぞれのグループに追加する必要があります。また、ERSアクセスはスーパー管理者アカウントにも使用できます。

ゲスト機能にAPIを使用するには、ポータルID、ゲストIDグループなどのポータルのrawデータがERS管理者に必要です。ただし、ゲストデータの読み取り/作成/更新または削除を行うには、ERSアクセスが有効になっているスポンサーアカウントが必要です。

- このドキュメントでは、スポンサーとして内部ISEユーザアカウントを使用します。
- 図に示すように、[Administration] > [Identity Management] > [Identities]に移動し、ネットワークアクセスユーザを追加します。

Network Access Users List > New Network Access User

▼ Network Access User

* Name

Status Enabled

Email

▼ Passwords

Password Type:

Password Re-Enter Password

* Login Password

Enable Password

▼ User Information

First Name

Last Name

▼ Account Options

Description

Change password on next login

▼ Account Disable Policy

Disable account if date exceed

▼ User Groups

Submit Cancel

User Groups

- ALL_ACCOUNTS (default)
- Employee
- GROUP_ACCOUNTS (default)
- GuestType_Contractor (default)
- GuestType_Daily (default)
- GuestType_SocialLogin (default)
- GuestType_Weekly (default)
- OWN_ACCOUNTS (default)

- このユーザアカウントは、スポンサーグループのいずれかに追加する必要があります。
- この例のアカウントは、デフォルトのスポンサーグループALL_ACCOUNTSにマップされます。
- このスポンサーグループに対してERSアクセスを許可するには、[Work Centers] > [Guest Access] > [Portal & Components] > [Sponsor Groups]に移動し、割り当てられたスポンサーグループを開きます。
- 次のオプションを有効にします。図に示すように、プログラマティックインターフェイス（ゲストREST API）を使用してCisco ISEゲストアカウントにアクセスします。

Sponsor Can

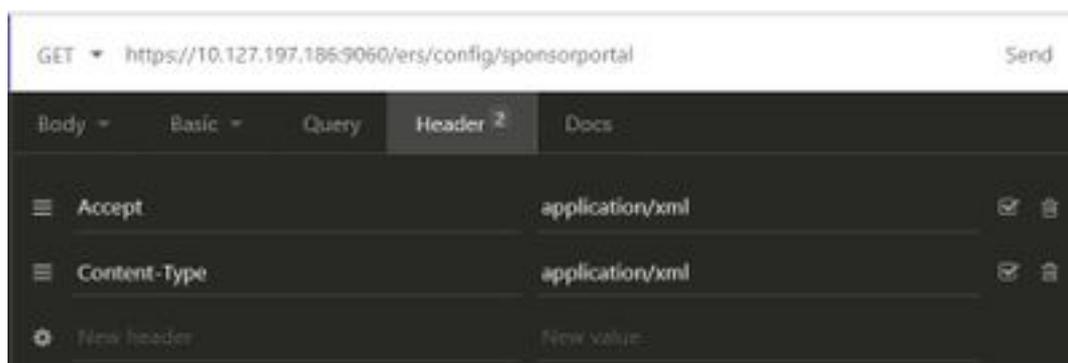
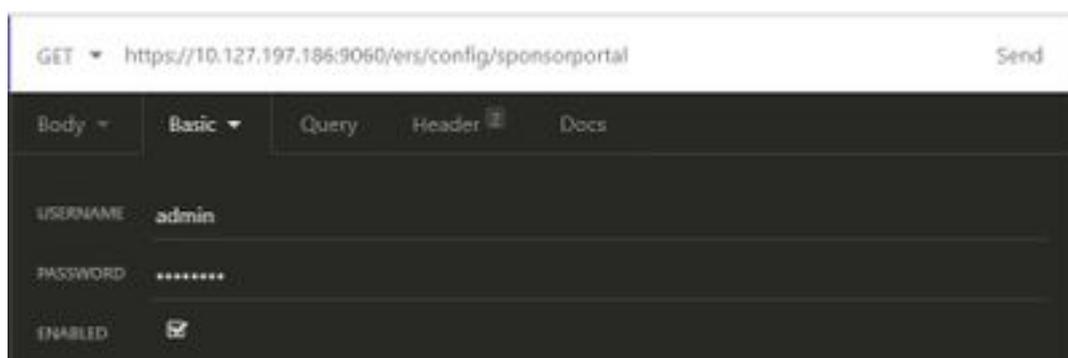
- Update guests' contact information (email, Phone Number)
- View/print guests' passwords
- Send SMS notifications with guests' credentials
- Reset guests' account passwords
- Extend guest accounts
- Delete guests' accounts
- Suspend guests' accounts
 - Require sponsor to provide a reason
- Reinstate suspended guests' accounts
- Approve and view requests from self-registering guests
 - Any pending accounts
 - Only pending accounts assigned to this sponsor ⓘ
- Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)

ゲストアカウントの作成

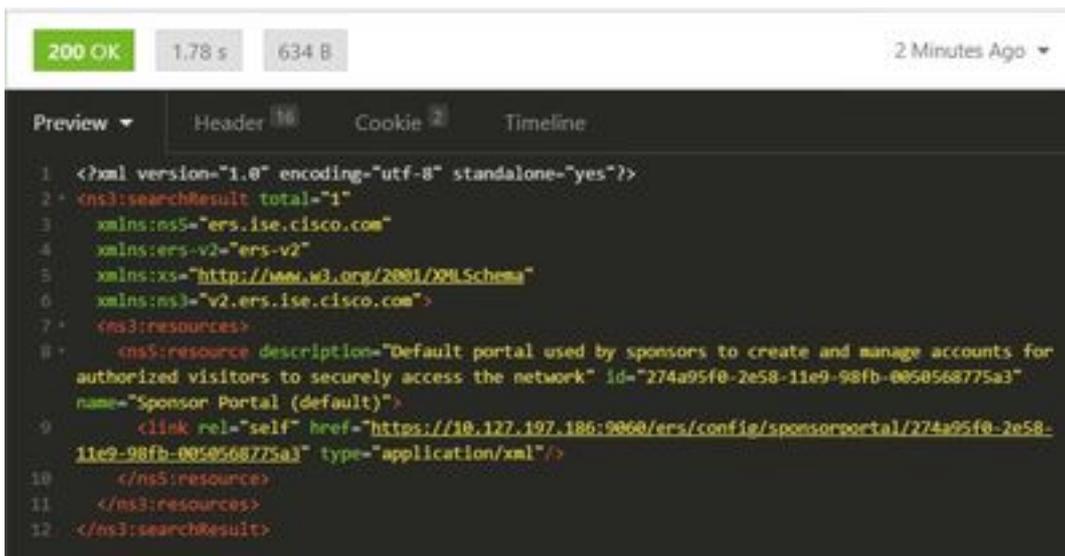
APIを介してゲストアカウントを作成するには、スポンサーとして、またスポンサーが認識するポータルを介してISEにAPIコールを発信する必要があります。

ステップ1: ISEで事前設定されているすべてのスポンサーポータルのポータルIDを取得するには、次の情報を含む任意のRESTクライアントを使用します。

メソッド	GET
URL	https://<ISE-IP>:9060/ers/config/sponsorportal
Credentials	ERS管理者クレデンシャルを使用する
ヘッダー	Content-type:application/xml Accept:application/xml



予想される出力 :



```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<ns3:searchResult total="1"
xmlns:ns5="ers.ise.cisco.com"
xmlns:ers-v2="ers-v2"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ns3="v2.ers.ise.cisco.com">
<ns3:resources>
<ns5:resource description="Default portal used by sponsors to create and manage accounts for
authorized visitors to securely access the network"
id="274a95f0-2e58-11e9-98fb-0050568775a3" name="Sponsor Portal (default)">
<link rel="self" href="https://10.127.197.186:9060/ers/config/sponsorportal/274a95f0-2e58-11e9-
98fb-0050568775a3" type="application/xml"/>
</ns5:resource>
</ns3:resources>
</ns3:searchResult>
```

関心の値は、ゲストユーザの作成に使用するスポンサーポータルIDです。この例では、IDは「274a95f0-2e58-11e9-98fb-0050568775a3」です。

ステップ2: このAPIコールを使用して、ゲストアカウントを作成します。ここでportalIDの値は、ステップ1から取得した値です。

メソッド	POST
URL	https://<ISE-IP>:9060/ers/config/guestuser/
Credentials	スポンサーアカウントの資格情報を使用する
ヘッダー	Content-type:application/vnd.com.cisco.ise.identity.guestuser.2.0+xml Accept:application/vnd.com.cisco.ise.identity.guestuser.2.0+xml
本文	<?xml version="1.0" encoding="UTF-8"?> <ns2:guestuser xmlns:ns2="identity.ers.ise.cisco.com"> <customFields> </customFields> <guestAccessInfo> <fromDate>04/25/2020 18:55</fromDate> <location>デリー</location>

```
<toDate>04/28/2020 19:55</toDate>
<validDays>3</validDays>
</guestAccessInfo>
<guestInfo>
<company>シスコ</company>
<emailAddress>abcd@cisco.com</emailAddress>
<firstName>John</firstName>
<lastName>Doe</lastName>
<notificationLanguage>英語
</notificationLanguage>
<password>9618</password>
<phoneNumber>9999998877</phoneNumber>
<smsServiceProvider>グローバルのデフォルト
</smsServiceProvider>
<userName>johndoe</userName>
</guestInfo>
<guestType>請負業者 ( デフォルト )
</guestType>
<personBeingVisited>abcd3@cisco.com</personBeingVisited>
<portalId>274a95f0-2e58-11e9-98fb-0050568775a3</portalId>
<reasonForVisit>会計からのボブの訪問
</reasonForVisit>
</ns2:guestuser>
```

注：ここに示す本文コンテンツは、テンプレートとして使用できます (SDKでも利用可能)。 fromDate、 toDateが validDaysに対応していることを確認します。 ロケーション、 ゲストタイプ、 およびその他の値は、使用するISEを参照して有効である必要があります。 有効な場合は、コールが成功します。

注：このコールを発信するときに使用するクレデンシャルは、スポンサーグループにマッピングされた有効なスポンサーアカウントである必要があります。ここでERSの管理者クレデンシャルは機能しません。詳細については、このガイドの前のセクションを参照してください。

POST <https://10.127.197.186:9060/ers/config/guestuser/> Send

XML ▾ Basic ▾ Query Header ² Docs

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ns1:guestuser xmlns:ns1="identity.ers.ise.cisco.com">
3 <customFields>
4 </customFields>
5 <guestAccessInfo>
6 <fromDate>04/25/2020 18:55</fromDate>
7 <location>Delhi</location>
8 <toDate>04/28/2020 19:55</toDate>
9 <validDays>3</validDays>
10 </guestAccessInfo>
11 <guestInfo>
12 <company>Cisco</company>
13 <emailAddress>abc@cisico.com</emailAddress>
14 <firstName>John</firstName>
15 <lastName>Doe</lastName>
16 <notificationLanguage>English</notificationLanguage>
17 <password>9618</password>
18 <phoneNumber>9999990877</phoneNumber>
19 <serviceProvider>Global Default</serviceProvider>
20 <username>johndoe</username>
21 </guestInfo>
22 <guestType>Contractor (default)</guestType>
23 <personBeingVisited>abc3@cisico.com</personBeingVisited>
24 <portalId>274a95f8-2e58-11e9-98fb-0050568775a3</portalId>
25 <reasonForVisit>Netflix and chill</reasonForVisit>
26 </ns1:guestuser>
27

```

POST <https://10.127.197.186:9060/ers/config/guestuser/> Send

XML ▾ Basic ▾ Query Header ² Docs

USERNAME

PASSWORD

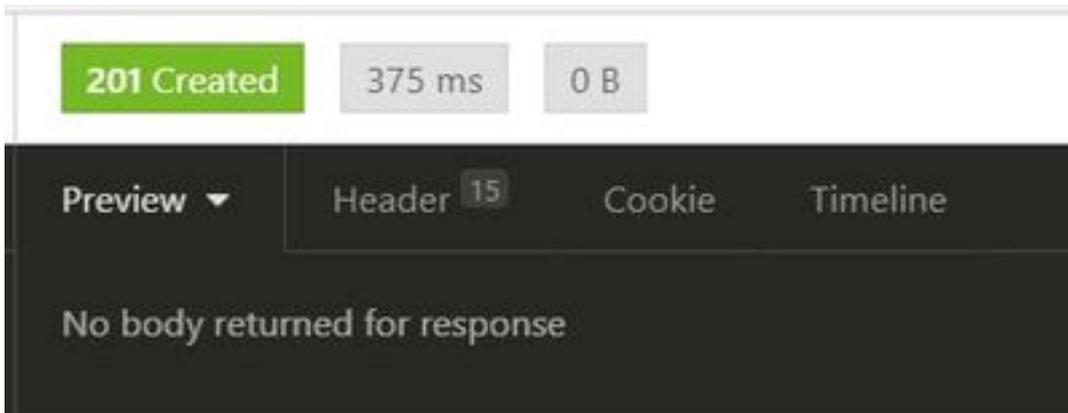
ENABLED

POST <https://10.127.197.186:9060/ers/config/guestuser/> Send

XML ▾ Basic ▾ Query Header ² Docs

Content-Type	application/vnd.com.cisco.ise.identity.guestuser	<input type="checkbox"/>	<input type="checkbox"/>
Accept	application/vnd.com.cisco.ise.identity.guestuser	<input type="checkbox"/>	<input type="checkbox"/>
New header	<input type="text" value="New value"/>		

予想される出力 :



[ISE GUI] > [Master GuestReport]に移動して、アカウントが作成されたかどうかを確認します。



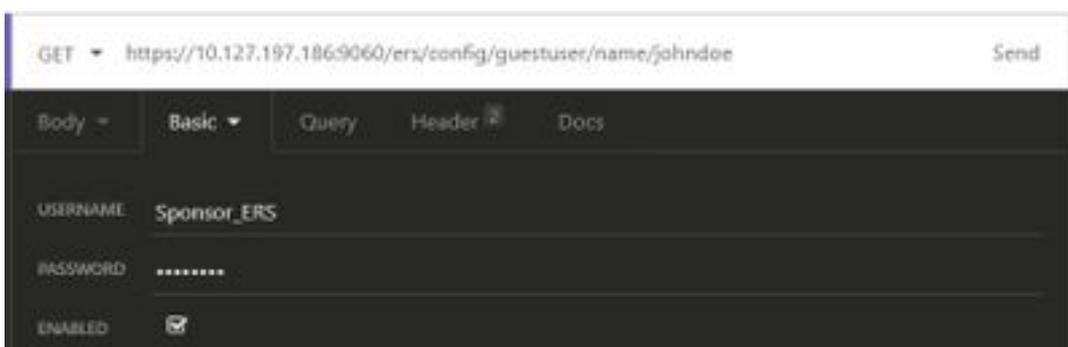
注：スポンサーポータルから、ゲストアカウントごとにカスタマイズされたユーザ名とパスワードの組み合わせを指定するオプションはありません。このAPIメソッドは、その要件を満たすために使用できます。

ゲストデータの読み取り、更新、削除

ゲストデータにさまざまなアクションを実行するためのAPIコールの例を次に示します。利用可能なすべてのオプションとその形式は、SDKで利用できます。

- ゲストユーザアカウントの詳細を名前で取得します。

メソッド GET
URL https://<ISE-IP>:9060/ers/config/guestuser/name/{name}
Credentials スポンサーアカウントの資格情報を使用する
ヘッダー Content-type:application/xml
 Accept:application/xml



予想される出力：

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<ns4:guestuser id="3b967932-86f8-11ea-aafe-72889dc971d1" name=" johndoe"
xmlns:ers="ers.ise.cisco.com"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ns4="identity.ers.ise.cisco.com">
<link rel="self" href="https://10.127.197.186:9060/ers/config/guestuser/name/johndoe"
type="application/xml"/>
<customFields/>
<guestAccessInfo>
<fromDate>04/25/2020 18:55</fromDate>
<location>Delhi</location>
<toDate>04/28/2020 19:55</toDate>
<validDays>3</validDays>
</guestAccessInfo>
<guestInfo>
<company>Cisco</company>
<creationTime>04/25/2020 18:55</creationTime>
<emailAddress>abcd@cisco.com</emailAddress>
<enabled>>false</enabled>
<firstName>John</firstName>
<lastName>Doe</lastName>
<notificationLanguage>English</notificationLanguage>
<password>9618</password>
<phoneNumber>9999998877</phoneNumber>
<smsServiceProvider>Global Default</smsServiceProvider>
<userName>johndoe</userName>
</guestInfo>
<guestType>Contractor (default)</guestType>
<personBeingVisited>abcd3@cisco.com</personBeingVisited>
<reasonForVisit>Visiting Bob from Accounting</reasonForVisit>
<sponsorUserId>1f7627f0-86f8-11ea-aafe-72889dc971d1</sponsorUserId>
<sponsorUserName>Sponsor_ERS</sponsorUserName>
<status>AWAITING_INITIAL_LOGIN</status>
</ns4:guestuser>
```

200 OK

422 ms

1244 B

3 Minutes Ago

```

Preview ▾ Header Cookie Timeline
1 <?xml version="1.0" encoding="utf-8" standalone="yes"?>
2 <ns4:guestuser id="3b967932-86f8-11ea-aafe-72889dc971d1" name="johndoe"
3   xmlns:ers="ers.ise.cisco.com"
4   xmlns:xs="http://www.w3.org/2001/XMLSchema"
5   xmlns:ns4="identity.ers.ise.cisco.com">
6 <link rel="self" href="https://19.127.197.186:9060/ers/config/guestuser/name/johndoe"
7 type="application/xml"/>
8 <customFields/>
9 <guestAccessInfo>
10 <fromDate>04/25/2020 18:55</fromDate>
11 <location>Dolh1</location>
12 <toDate>04/28/2020 19:55</toDate>
13 <validDays>3</validDays>
14 </guestAccessInfo>
15 <guestInfo>
16 <company>Cisco</company>
17 <creationTime>04/25/2020 18:55</creationTime>
18 <emailAddress>abcd@cisco.com</emailAddress>
19 <enabled>false</enabled>
20 <firstName>John</firstName>
21 <lastName>Doe</lastName>
22 <notificationLanguage>English</notificationLanguage>
23 <password>9618</password>
24 <phoneNumber>9999998877</phoneNumber>
25 <serviceProvider>Global Default</serviceProvider>
26 <username>johndoe</username>
27 </guestInfo>
28 <guestType>Contractor (default)</guestType>
29 <personBeingVisited>abcd@cisco.com</personBeingVisited>
30 <reasonForVisit>Netflix and chill</reasonForVisit>
31 <sponsorUserId>1f7627f8-86f8-11ea-aafe-72889dc971d1</sponsorUserId>
32 <sponsorUsername>Sponsor_ERS</sponsorUsername>
33 <status>AWAITING_INITIAL_LOGIN</status>
34 </ns4:guestuser>

```

- ゲストユーザパスワードをリセットします。

これは、最初にゲストIDをコールから取得し、このAPIで使用する必要があります。この例では、guestuser IDは「3b967932-86f8-11ea-aafe-72889dc971d1」です。

メソッド	PUT
URL	https://<ISE-IP>:9060/ers/config/guestuser/resetpassword/{id}
Credentials	スポンサーアカウントの資格情報を使用する
ヘッダー	Content-type:application/xml Accept:application/xml

この方法では、新しいパスワードを指定できません。ISEは、新しい自動生成パスワードを使用して出力を返します。

予想される出力：

200 OK

```

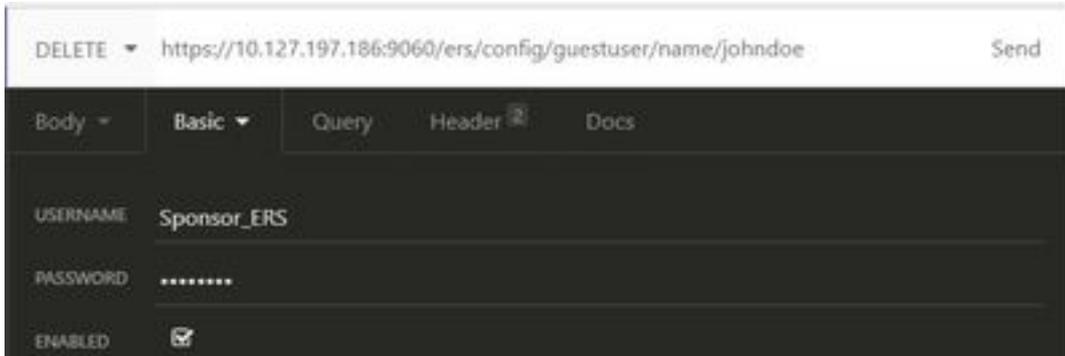
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<ns3:operationResult
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ns3="ers.ise.cisco.com">
<attributesList>
<attribute name="password" value="2557"/>
</attributesList>

```

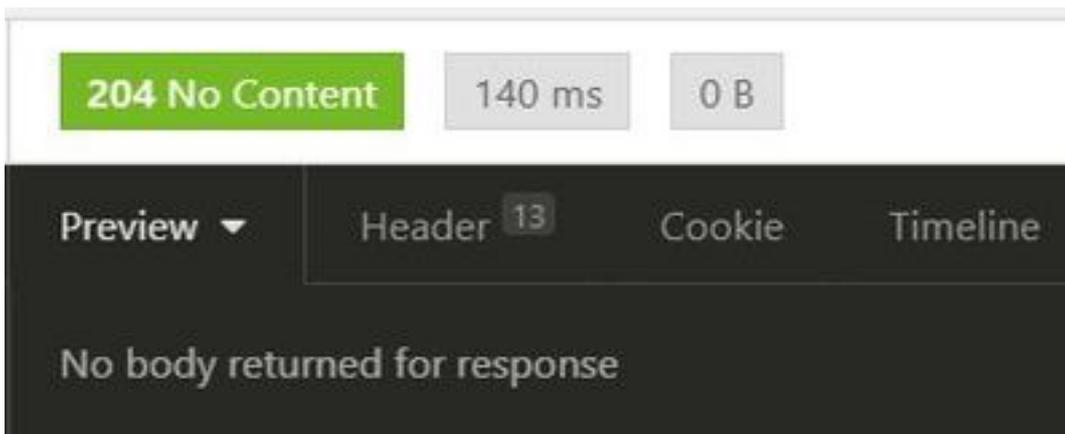
</ns3:operationResult>

- ・ ゲストアカウントを名前で削除します。

メソッド 削除
URL https://<ISE-
 IP>:9060/ers/config/guestuser/name/{name}
Credentials スポンサーアカウントの資格情報を使用する
ヘッダー Content-type:application/xml
 Accept:application/xml



予想される出力 :



確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

一般的なエラーとその考えられる原因 :

- ・ ゲストアカウントの作成が次のエラーで失敗します。

401 Unauthorized

```
<message type="ERROR" code="CRUD operation exception">  
<title>Sponsor does not have permission to access REST Apis</title>
```

</message>

修正：これは、ゲストアカウントの作成に使用されるスポンサーアカウントが、ERSアクセスが有効になっていないスポンサーグループにマッピングされることを意味します。これに対応するスポンサーグループを編集し、プログラマティックインターフェイス (ゲストREST API) を使用してAccess Cisco ISEゲストアカウントを有効にします。

400 Bad Request

```
<message type="ERROR" code="CRUD operation exception">
  <title>Creating GuestUser failed due to
com.cisco.cpm.guestaccess.validation.GuestAccessValidationException: Portal not found for portal
session elfc15a7-a170-4d6a-b02c-0ab7b0bc54ff</title>
```

修正：コールで入力されたポータルIDがISEに存在しないか、正しくありません。スポンサーポータルの「Get」コールから、ポータルの正しいポータルIDを取得します。

• API応答コードとその考えられる意味：

200 (OK):REST APIが目的のアクションを正常に実行したことを示します。

201 (作成日時) :コレクション内でリソースが作成されたことを示します。

204 (コンテンツなし) :これは通常、PUT、POST、またはDELETE要求への応答として送信されます。

400 (Bad Request):不正な要求構文、無効なパラメータなどの問題に対する一般的なエラーコード。メッセージの詳細を読んで、原因を理解してください。

401 (無許可) :これは、アクションが誤ったクレデンシャルで実行されたか、クレデンシャルがないか、アカウントがこのアクションの実行を許可されていないことを示します。

500 (内部サーバエラー) :サーバ側の問題を示します。ISEのログが原因の理解に役立つ場合があります。

ISEでのREST APIの使用方法の詳細については、「ゲストREST API」を[参照してください](#)。