



## CHAPTER 2

# UCP Web サービスの使用

この章では、User Change Password (UCP) Web サービスを使用するために設定する必要がある環境と、この Web サービスの使用方法について説明します。

UCP Web サービスを使用すると、内部ユーザの認証と、内部ユーザのパスワードの変更が可能です。この Web サービス インターフェイスを使用して、ACS と社内ポータルを統合し、組織内のユーザが自分のパスワードを変更できるようにします。

UCP Web サービスを使用すると、組織内のユーザは自分のパスワードだけを変更できます。パスワードは、プライマリまたはセカンダリ ACS サーバ上で変更できます。

UCP Web サービスによって、入力した新しいパスワードと ACS でユーザに設定されているパスワードポリシーが比較されます。新しいパスワードが定義されている基準に準拠している場合、新しいパスワードが有効になります。プライマリ ACS サーバでパスワードを変更すると、そのパスワードは ACS によってすべてのセカンダリ ACS サーバに複製されます。

Monitoring and Report Viewer は、ACS Instance カタログの下で使用できる User\_Change\_Password\_Audit レポートを提供します。このレポートを生成すると、内部データベースのユーザパスワードに加えられたすべての変更を、UCP Web サービスを通じて加えられた変更を含めて追跡できます。このレポートを使用して、使用状況および失敗した認証を監視できます。

### ACS CLI での Web インターフェイスのイネーブル化

UCP Web サービスを使用する前に、ACS で Web インターフェイスをイネーブルにする必要があります。ACS で Web インターフェイスをイネーブルにするには、ACS CLI から次のように入力します。

```
acs config-web-interface ucp enable
```

**acs config-web-interface** コマンドの詳細については、次の URL を参照してください。

[http://www.cisco.com/en/US/docs/net\\_mgmt/cisco\\_secure\\_access\\_control\\_system/5.3/command/reference/cli\\_app\\_a.html#wp1887278](http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/command/reference/cli_app_a.html#wp1887278)

### ACS CLI からの Web インターフェイスのステータス表示

Web インターフェイスのステータスを表示するには、ACS CLI から次のように入力します。

```
show acs-config-web-interface
```

**show acs-config-web-interface** コマンドの詳細については、次の URL を参照してください。

[http://www.cisco.com/en/US/docs/net\\_mgmt/cisco\\_secure\\_access\\_control\\_system/5.3/command/reference/cli\\_app\\_a.html#wp1890877](http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/command/reference/cli_app_a.html#wp1890877)

ここでは、UCP Web サービスの使用方法について説明します。

- 「UCP Web サービスのメソッドについて」 (P.2-2)
- 「WSDL ファイルの使用」 (P.2-4)
- 「UCP Web サービスの操作」 (P.2-7)

# UCP Web サービスのメソッドについて

UCP Web サービスは、次のメソッドで構成されています。

- 「[User Authentication](#)」 (P.2-2)
- 「[User Change Password](#)」 (P.2-3)

## User Authentication

User Authentication メソッドは、内部データベースによってユーザの認証を行います。

### 入力パラメータ

- Username
- Password

### 目的

ユーザパスワードの変更を 2 段階の手順で行う必要のあるアプリケーションでは、**authenticateUser** メソッドを使用します。たとえば、プロンプトを表示してユーザにパスワードの変更を要求する ACS ユーザ インターフェイス アプリケーションは、次の 2 つの手順でこの処理を実行しています。

1. ユーザを認証する
2. ユーザパスワードを変更する。

パスワードを変更するには、次の手順に従います。

---

**ステップ 1** UCP Web アプリケーションに接続します。

ログイン ページが表示されます。

**ステップ 2** ユーザ名とパスワードを入力します。

**authenticateUser** Web サービス機能が呼び出されます。クレデンシャルが ACS 内部ストアのデータと一致すると、認証に成功します。

---



(注)

このメソッドは、何も変更せず、タスクの実行も許可しません。このメソッドは、パスワードが正しいかどうかを確認するだけの目的で使用します。ただし、認証が成功した後、[User Change Password](#) メソッドを使用して、パスワード変更ページに移動できます。

---

### 出力パラメータ

User Authentication メソッドからの応答は、次のいずれかです。

- Authentication Succeeded
- Authentication Failed

### 例外

このメソッドは、次の場合にエラー メッセージを表示します。

- ユーザ名またはパスワードが正しくないために認証が失敗した。
- ユーザが無効。

- Web サービス接続エラー（ネットワーク切断、要求タイムアウト エラーなど）が発生した。
- システム障害（データベースがダウンしている、使用できないなど）が発生した。

## User Change Password

User Change Password メソッドは、内部データベースによってユーザの認証を行い、ユーザ パスワードを変更します。

### 入力パラメータ

- Username
- 現在のパスワード
- 新しいパスワード

### 目的

ユーザ パスワードの変更を 1 段階の手順で行う必要のあるアプリケーションでは、**changeUserPassword** メソッドを使用します。通常、ユーザ パスワードの変更は、2 段階の手順で行われます。最初の手順でユーザを認証し、2 番目の手順でユーザ パスワードを変更します。

**changeUserPassword** メソッドを使用すると、2 段階の手順を 1 つに組み合わせることができます。ユーザ パスワードの変更に 1 段階の手順を必要とするアプリケーションの例として、スクリプトまたは単一ページの Web アプリケーションがあります。

パスワードを変更するには、次の手順に従います。

---

**ステップ 1** UCP Web アプリケーションに接続します。

ログイン ページが表示されます。

**ステップ 2** ユーザ名とパスワードを入力します。

**authenticateUser** Web サービス機能が呼び出されます。

認証に成功すると、Web サービスは新しいパスワードと ACS で構成されているパスワード ポリシーを比較します。

新しいパスワードが定義されている基準を満たしている場合、**changeUserPassword** Web サービス機能が呼び出され、パスワードが変更されます。

---

### 出力パラメータ

User Change Password メソッドからの応答は、次のいずれかです。

- Operation Succeeded
- Operation Failed

### 例外

このメソッドは、次の場合にエラーを表示します。

- ユーザ名またはパスワードが正しくないために認証が失敗した。
- ユーザが無効。
- ACS で定義されているパスワードの複雑さに関する規則にパスワードが準拠していないため、パスワード変更操作が失敗した。

- Web サービス接続エラー（ネットワーク切断、要求タイムアウト エラーなど）が発生した。
- システム障害（データベースがダウンしている、使用できないなど）が発生した。

## WSDL ファイルの使用

ここでは、WSDL ファイルについて説明し、User Authentication および User Change Password メソッドの要求および応答スキーマについて説明します。ここでは、次の内容について説明します。

- 「[WSDL ファイルのダウンロード](#)」(P.2-4)
- 「[UCP WSDL ファイル](#)」(P.2-4)
- 「[要求および応答スキーマ](#)」(P.2-7)

## WSDL ファイルのダウンロード

ACS 5.3 Web インターフェイスから WSDL ファイルをダウンロードするには、次の手順に従います。

- 
- ステップ 1** ACS 5.3 Web インターフェイスにログインします。
  - ステップ 2** [System Administration] > [Downloads] > [User Change Password] を選択します。
  - ステップ 3** [UCP WSDL] をクリックして UCP WSDL ファイルを表示します。
  - ステップ 4** WSDL ファイルをローカル ハード ドライブにコピーします。
  - ステップ 5** [UCP web application example] をクリックして、サンプル Web アプリケーションをダウンロードし、ローカル ハード ドライブに保存します。
- 

## UCP WSDL ファイル

WSDL ファイルは、Web サービスと、Web サービスが公開する操作を記述する XML ドキュメントです。UCP WSDL を次に示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!--*****-->
<!-- Copyright (c) 2009 Cisco Systems, Inc.-->
<!-- All rights reserved.-->
<!--*****-->
<definitions name="changePASS"
targetNamespace="http://www.cisco.com/changePASS.service"
xmlns:tns="http://www.cisco.com/changePASS.service"
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:SOAP="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:MIME="http://schemas.xmlsoap.org/wsdl/mime/"
xmlns:DIME="http://schemas.xmlsoap.org/ws/2002/04/dime/wsdl/"
xmlns:WSDL="http://schemas.xmlsoap.org/wsdl/"
xmlns="http://schemas.xmlsoap.org/wsdl/">

<WSDL:documentation>
Copyright (c) 2009 Cisco Systems, Inc.
```

```
ACS5.1 WSDL
Service Interface for change password

This WSDL document defines the publication API calls for
changing user
password.
</WSDL:documentation>

<xsd:types>
<xsd:schema xmlns="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.cisco.com/changepass.service">

  <xsd:simpleType name="UserNameType">
<xsd:restriction base="string">
<xsd:minLength value="1" />
</xsd:restriction>
</xsd:simpleType>

  <xsd:element name="usernameType" type="tns:UserNameType" />

  <xsd:simpleType name="PasswordType">
<xsd:restriction base="string">
<xsd:minLength value="1" />
</xsd:restriction>
</xsd:simpleType>

  <xsd:element name="passwordType" type="tns:PasswordType" />

  <xsd:simpleType name="StatusCodeType">
<xsd:restriction base="string">
<xsd:enumeration value="success" />
<xsd:enumeration value="failure" />
</xsd:restriction>
</xsd:simpleType>

  <xsd:element name="ResponseType">
<xsd:complexType>
<xsd:attribute name="status" type="tns:StatusCodeType" use="required" />
<xsd:sequence>
<xsd:element name="errorMessage" type="xsd:string" minOccurs="0"
  maxOccurs="unbounded" />
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:schema>
</xsd:types>

  <message name="AuthUserRequest">
<part name="user_name" element="tns:usernameType" />
<part name="password" element="tns:passwordType" />
</message>

  <message name="AuthUserResponse">
<part name="authUserResponse" element="tns:ResponseType" />
</message>

  <message name="ChangeUserPassRequest">
<part name="user_name" element="tns:usernameType" />
<part name="old_password" element="tns:passwordType" />
<part name="new_password" element="tns:passwordType" />
</message>
```

```

<message name="ChangeUserPassResponse">
<part name="changeUserPassResponse" element="tns:ResponseType" />
</message>

<WSDL:portType name="ChangePassword">
<operation name="authenticateUser">
<input message="tns:AuthUserRequest" name="authUserRequest" />
<output message="tns:AuthUserResponse" name="authUserResponse" />
</operation>

<operation name="changeUserPass">
<input message="tns:ChangeUserPassRequest" name="changeUserPassRequest" />
<output message="tns:ChangeUserPassResponse" name="changeUserPassResponse" />
</operation>
</WSDL:portType>

<WSDL:binding name="changePassSoapBinding" type="tns:ChangePassword">
<SOAP:binding style="document"
transport="http://schemas.xmlsoap.org/soap/http" />
<!--
This is the SOAP binding for the Change Password publish operations.
-->

<WSDL:operation name="authenticateUser">
<SOAP:operation soapAction="" />
<input>
<SOAP:body use="literal" />
</input>
<output>
<SOAP:body use="literal" />
</output>
</WSDL:operation>

<WSDL:operation name="changeUserPass">
<SOAP:operation soapAction="" />
<input>
<SOAP:body use="literal" />
</input>
<output>
<SOAP:body use="literal" />
</output>
</WSDL:operation>
</WSDL:binding>

<WSDL:service name="changepassword">
<documentation>
ACS5.1 Programmatic Interface Service Definitions
</documentation>
<port name="changepassword" binding="tns:changePassSoapBinding">
<SOAP:address location="https://localhost:8080/PI/services/changepass/" />
</port>
</WSDL:service>

</definitions>

```

## 要求および応答スキーマ

ここでは、User Authentication および User Change Password メソッドの要求および応答スキーマのリストを示します。ここでは、次のスキーマについて説明します。

- 「User Authentication の要求」 (P.2-7)
- 「User Authentication の応答」 (P.2-7)
- 「User Change Password の要求」 (P.2-7)
- 「User Change Password の応答」 (P.2-7)

### User Authentication の要求

```
<message name="AuthUserRequest">
  <part name="user_name" element="changePass:usernameType" />
  <part name="password" element="changePass:passwordType" />
</message>
```

### User Authentication の応答

```
<message name="AuthUserResponse">
  <part name="authUserResponse" element="changePass:ResponseType" />
</message>
```

### User Change Password の要求

```
<message name="ChangeUserPassRequest">
  <part name="user_name" element="changePass:usernameType" />
  <part name="current_password" element="changePass:passwordType" />
  <part name="new_password" element="changePass:passwordType" />
</message>
```

### User Change Password の応答

```
<message name="ChangeUserPassResponse">
  <part name="changeUserPassResponse" element="changePass:ResponseType" />
</message>
```

## UCP Web サービスの操作

ユーザが社内用の自分のパスワードを変更できるようにする、カスタム Web ベース アプリケーションを作成できます。ここでは、Python を使用して開発されたサンプル アプリケーションの実行方法について説明し、クライアント コードの例を示します。

ACS Web インターフェイスが提供するダウンロード可能なパッケージは、次のもので構成されます。

- Linux および Windows 用 Python SOAP ライブラリ
- Python スクリプト
- ReadMe : インストール方法の説明

このパッケージをダウンロードするには、次の手順に従います。

- 
- ステップ 1** ACS 5.3 Web インターフェイスにログインします。
  - ステップ 2** [System Administration] > [Downloads] > [Scripts] を選択します。  
[Sample Python Scripts] ページが表示されます。
  - ステップ 3** [Python Script for Using the User Change Password Web Service] をクリックします。
  - ステップ 4** ローカル ハード ドライブに .zip ファイルを保存します。
- 

クライアント コードの例に .zip ファイルの例を示します。このファイルには .war ファイルが含まれています。この .war ファイルを Web サーバ (Tomcat など) に展開する必要があります。この例を使用すると、アプリケーションが UCP Web サービスを通じて ACS と通信できます。

**(注)**

シスコのテクニカル サポートでは、デフォルトの Python スクリプトだけがサポートされています。変更されたスクリプトはサポートされていません。

---

## クライアント コードの例

```
from SOAPpy import SOAPProxy

# Get the ACS host / IP
host = raw_input('Please enter ACS host name or IP address:\n')
targetUrl = 'https://' + host + '/PI/services/UCP/'

server = SOAPProxy(targetUrl, 'UCP')

# Get the username
username = raw_input('Please enter user name:\n')

# Get the old password
oldPassword = raw_input('Please enter old password:\n')

# Get the new password
newPassword = raw_input('Please enter new password:\n')

# Call the changeUserPassword with the given input
ans = server.changeUserPass(username, oldPassword, newPassword)

# Password changing failed
if ans.status == 'failure':
    print '\nFailure:'

# Print all failure reasons
for err in ans.errors:
    print err
else:
    # Password was changed successfully
    print 'Success'
```

**(注)**

このスクリプトを実行するには、Python ソフトウェアが必要です。

---