



# 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、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。

これで、ACS 5.7 から UCP.war ファイルをダウンロードし、jdk6 とともに JBoss 5.1.0.GA アプリケーションで使用できます。

## 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、『[CLI Reference Guide for Cisco Secure Access Control System 5.7](#)』を参照してください。

## 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
```

`acs config-web-interface` コマンドの詳細については、『[CLI Reference Guide for Cisco Secure Access Control System 5.7](#)』を参照してください。

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 \(1 ページ\)](#)
- [WSDL ファイルの使用 \(4 ページ\)](#)
- [UCP Web サービスの操作 \(7 ページ\)](#)

## 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 \(2 ページ\)](#)
- [User Change Password \(3 ページ\)](#)

## 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。

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。
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 \(3 ページ\)](#) 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
- Current password
- New password

### 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が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 段階の手順で実行されます。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。

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。

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。この項の構成は、次のとおりです。

- [WSDL ファイルのダウンロード \(4 ページ\)](#)
- [UCP WSDL ファイル \(4 ページ\)](#)
- [要求および応答スキーマ \(6 ページ\)](#)

## WSDL ファイルのダウンロード

ACS 5.7 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。

1. ACS 5.7 Web インターフェイスにログインします。
2. [System Administration] > [Downloads] > [User Change Password] を選択します。
3. [UCP WSDL] をクリックして UCP WSDL ファイルを表示します。
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。
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.

ACS5.7 WSDL
Service Interface for change password

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

## WSDL ファイルの使用

```
<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" />
```

## WSDL ファイルの使用

```
</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>
ACS5.7 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 \(7 ページ\)](#)
- [User Authentication の応答 \(7 ページ\)](#)
- [User Change Password の要求 \(7 ページ\)](#)
- [User Change Password の応答 \(7 ページ\)](#)

## 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。

1. ACS 5.7 Web インターフェイスにログインします。
2. [System Administration] > [Downloads] > [Sample Python Scripts] を選択します。  
[Sample Python Scripts] ページが表示されます。
3. [Python Script for Using the User Change Password Web Service] をクリックします。
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 (8 ページ)** 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。

## JBoss サーバでの UCP.war のインストール

JBoss サーバで UCP.war を展開するには、次の手順を実行します。

1. `JAVA_HOME` が正しく設定されていることを確認します。`JAVA_HOME` は、JDK がインストールされている場所です。
2. リンク <http://www.jboss.org/jbossas/downloads/> から 5.1.0.GA JBoss をダウンロードし、展開します。
3. JBoss サーバを起動します。<JBASS\_HOME>\bin\に移動し、この場所から **run.bat** (Windows の場合) または **run.sh** (Linux の場合) コマンドを実行して JBoss サーバを起動する必要があります。JBoss サーバが正常に起動したことをコマンドプロンプトでチェックします。JBoss サーバが正常に起動しない場合は、JBoss サポート チームに問い合わせてください。
4. ブラウザで `http://<JBASS_Installed_Server_IP/HOSTNAME>:<PORT_CONFIGURED>` と入力して JBoss サーバを起動します。JBoss サーバが正常に起動しない場合は、JBoss サポート チームに問い合わせる必要があります。
5. <JBASS\_HOME>\bin\shutdown.bat または **shutdown.sh** コマンドを使用して JBoss サーバを停止します。
6. Cisco Secure ACS にログインし、[System Administration] > [Downloads] > [User Change Password] を選択して UCP.war をダウンロードします。
7. JBoss サーバの場所 <JBASS\_HOME>\server\default\deploy に UCP.war ファイルを配置します。
8. JBoss サーバを起動します。<JBASS\_HOME>\bin\に移動し、この場所から **run.bat** (Windows の場合) または **run.sh** (Linux の場合) コマンドを実行して JBoss サーバを起動する必要があります。JBoss サーバが正常に起動したことを確認する必要があります。



9. 場所 <JBoss\_HOME>\server\default\work\jboss.web\localhost\ に UCP ディレクトリが存在することを確認します。UCP ディレクトリが見つからない場合は、UCP.war を再度ダウンロードし、ステップ 7~10 を繰り返す必要があります。
10. UCP.war を再度展開した後も、エラーまたは例外が見つかった場合は、場所 <JBoss\_HOME>\server\default\log\ にあるログを収集して、更に分析する必要があります。

