Cisco Secure ACS の User-Changeable Password のインストールと使用

このガイドでは、Cisco Secure Access Control Server Release 4.0（ACS）に User-Changeable Password（UCP）をインストールして使用する方法を説明します。UCP は、次のソフトウェアで使用できます。

- Cisco Secure ACS for Windows, Release 4.0
- Cisco Secure ACS Solution Engine, Release 4.0

この章には、次の項があります。

UCP について

UCP アプリケーションを使用すると、ユーザが Web ベースのユーティリティを使用して自分の ACS パスワードを変更できるようになります。パスワードを変更する必要があるときは、サポート対象の Web ブラウザを使用して UCP Web ページにアクセスできます。ACS で動作確認済みの Web ブラウザについては、ACS 製品のリリース ノートを参照してください。

UCP Web ページでは、ユーザがログインする必要があります。ここで必要なパスワードは、ユーザ アカウントの Password Authentication Protocol（PAP; パスワード認証プロトコル）パスワードです。UCP が ACS のユーザ認証を行うと、ユーザは新しいパスワードを指定できるようになります。UCP はユーザの PAP パスワードと Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）パスワードを新しいパスワードに変更します。

UCP をインストールするには、Microsoft IIS 5.0（Windows 2000 に付属）または 6.0（Windows Server 2003 に付属）を実行する Web サーバが必要です。

SSL について

UCP と ACS 間の通信は、128 ビット暗号化で保護されています。セキュリティを強化するために、Secure Sockets Layer（SSL）を実装して Web ブラウザと UCP の間の通信を保護することをお勧めします。SSL プロトコルを使用すると、UCP Web サーバとユーザの Web ブラウザとの間で行われるリモートアクセスのデータ転送が、セキュリティで保護されます。

ユーザは Web ブラウザと Microsoft IIS 間の接続を通じてユーザの ACS 内部データベース パスワードを変更するため、ユーザとパスワード データは攻撃を受けやすくなります。SSL プロトコルは、Web ブラウザと Microsoft IIS の間で行われるパスワードなどのデータ転送を暗号化します。

SSL は Microsoft IIS に対して、有効な認証証明書の提示を要求します。このためユーザは、認証局から証明書を取得する必要があります。公開認証局を利用する場合は、特定の要件を満たせば、有料でキーが割り当てられます。

UCP のインストール

ここでは、UCP をインストールするための情報や手順について説明します。

この項には、次のトピックがあります。

Web サーバの準備

Web サーバを準備するには、Web サーバ上に仮想ディレクトリを作成する必要があります。この仮想ディレクトリは、UCP セットアップ プログラムが HTML ファイルと CGI 実行ファイルを配置するファイル システム ディレクトリに対応します。

UCP 向けに準備するには、次の手順を実行します。

ステップ 1　Web サーバが Microsoft IIS 5.0 または 6.0 を使用することを確認します。

- IIS 5.0 は Windows 2000 に含まれています。
- IIS 6.0 は Windows Server 2003 に含まれています。

ステップ 2　Web サーバのホーム ディレクトリで、2 つのディレクトリを作成します。

ヒント　ホーム ディレクトリを確認するには、Microsoft IIS の Default Web Site のプロパティを参照してください。

- **secure**：このディレクトリには、UCP によって使用された HTML ファイルが置かれます。**secure** 以外の名前を指定することもできます。ディレクトリ名は、他のインストール手順で使用できるように記録しておく必要があります。
- **securecgi-bin**：このディレクトリには、UCP によって使用された CGI 実行ファイルが置かれます。**securecgi-bin** 以外の名前を指定することもできます。ディレクトリ名は、他のインストール手順で使用できるように記録しておく必要があります。

  たとえば、Web サーバのホーム ディレクトリが *C:\Inetpub\wwwroot* の場合は、これらのディレクトリを *C:\Inetpub\wwwroot* に追加します。

ステップ 3　Microsoft IIS で、UCP で使用される HTML ファイルの仮想ディレクトリを追加します。仮想ディレクトリを作成する場合は、次のように指定します。

- **仮想ディレクトリ エイリアス**：仮想ディレクトリの名前。この仮想ディレクトリは、ステップ 2 で作成した **secure** ディレクトリに対応します。ディレクトリ名を **secure** にすることをお勧めします。このエイリアスは、UCP へのアクセスに使用する URL の一部となるため、簡潔で分かりやすいエイリアスにしておくと、ユーザが URL を覚えやすくなります。
- **Web サイトのコンテンツ ディレクトリ**：指定するディレクトリは、ステップ 2 で作成した **secure** ディレクトリと一致させる必要があります。ステップ 2 のデフォルト ディレクトリは、*C:\Inetpub\wwwroot\secure* です。

- **アクセス権**：この仮想ディレクトリに読み取りアクセス権を付与します。それ以外のアクセス権は不要です。

仮想ディレクトリの作成方法については、使用しているバージョンの IIS に関するマイクロソフトのマニュアルを参照してください。

ステップ 4　UCP で使用される CGI 実行ファイルの仮想ディレクトリを追加します。仮想ディレクトリを作成する場合は、次のように指定します。

- **仮想ディレクトリ エイリアス**：仮想ディレクトリの名前。この仮想ディレクトリは、ステップ 2 で作成した **securecgi-bin** ディレクトリに対応します。ディレクトリ名を **securecgi-bin** にすることをお勧めします。
- **Web サイトのコンテンツ ディレクトリ**：指定するディレクトリは、ステップ 2 で作成した **securecgi-bin** ディレクトリと一致させる必要があります。ステップ 2 のデフォルト ディレクトリは、*C:\Inetpub\wwwroot\securecgi-bin* です。
- **アクセス権**：この仮想ディレクトリに読み取りアクセス権と実行アクセス権を付与します。それ以外のアクセス権は不要です。

仮想ディレクトリの作成方法については、使用しているバージョンの IIS に関するマイクロソフトのマニュアルを参照してください。

ステップ 5　Web サーバが IIS 6.0 を実行している場合、未知の CGI 拡張機能が許可されるように IIS の設定を変更する必要があります。これを行うには、IIS Manager ウィンドウの Web Service Extension ページを使用して、**Allow Unknown CGI Extensions** のステータスを **Allowed** に設定します。

ステップ 6　Microsoft IIS 5.0 Web サーバを保護するために IIS Lockdown Tool を使用している場合は、Lockdown Tool で実行ファイルの起動が許可されていることを確認します。実行ファイルを起動できない場合、UCP が失敗し、ユーザはパスワードを変更できません。

UCP 向けの Cisco Secure ACS の準備

UCP 向けに ACS を準備するには、Web サーバが認証、認可、アカウンティング（AAA）サーバの一種として認識されるように、ACS を設定する必要があります。この設定を実行すると、ACS は、Web サーバ上の UCP によって処理されたユーザ パスワード変更を認識して、応答できるようになります。この設定を行わなかった場合、ACS は、UCP からのユーザ パスワード変更の要求を無視します。

（注）　ACS および Microsoft IIS ソフトウェアを同じコンピュータ上で実行する場合は、この手順を実行する必要はありません。P.1-6 の「Web サーバでの SSL のイネーブル化」に進んでください。

UCP 向けに準備するには、次の手順を実行します。

ステップ 1　UCP からのユーザ パスワード変更の送信先となる、ACS の Web インターフェイスにログインします。

（注）　ACS Internal Database Replication 機能を使用している場合、UCP がユーザ パスワード変更を送信する先の ACS は、プライマリ ACS である必要があります。そうでない場合、ユーザ データベースを複製したときに、プライマリ ACS の古い情報がユーザ パスワードの変更を上書きします。

ステップ 2　**Interface Configuration > Advanced Options** を選択します。

Advanced Options ページが表示されます。

ステップ 3　Distributed Systems Settings チェックボックスがオンになっていることを確認します。オンになっている場合は、Network Configurations セクションに AAA Servers テーブルが表示されます。

ステップ 4　**Submit** をクリックします。

ステップ 5　**Network Configuration** をクリックします。

ステップ 6　Network Device Group（NDG; ネットワーク デバイス グループ）がイネーブルの場合は、UCP Web サーバの追加先となる NDG をクリックします。

ステップ 7　AAA Servers テーブルの **Add Entry** をクリックします。

ステップ 8　AAA Server Name ボックスに、UCP Web サーバの名前を入力します。Web サーバのホスト名を使用することをお勧めします。ただし、UCP Web サーバをより簡単に識別できるように、**UCP** などの追加情報を入れることもできます。たとえば、Web サーバのホスト名が **wwwin** の場合、AAA Server Name ボックスに **UCP-wwwin** と入力できます。

ステップ 9　AAA Server IP Address ボックスに、UCP Web サーバの IP アドレスを入力します。ドット付き 10 進形式を使用します。

（注）　Add AAA Server ページにあるその他の設定は、UCP とは関係ありません。

ステップ 10　**Submit + Restart** をクリックします。

ACS は、UCP のインストール先となる Web サーバからのパスワード変更情報を認識して、応答するよう設定されます。

Web サーバでの SSL のイネーブル化

ここでは、SSL をイネーブルして、ユーザの Web ブラウザと UCP を実行する Microsoft IIS の間の通信を暗号化する方法を説明します。

（注）　SSL はイネーブルにしておくことをお勧めします。すべてのユーザが例外なくセキュア境界の内側から UCP にアクセスする場合は、SSL は不要です。しかしそれ以外の場合は、ユーザの Web ブラウザと UCP を実行する Web サーバとの間の UCP トラフィックを暗号化するように、SSL をイネーブルにする必要があります。

Web サーバでオプションの SSL セキュリティをイネーブルにするには、次の手順を実行します。

ステップ 1　認証局から証明書を取得します。

ステップ 2　認証局から証明書を受け取ったら、証明書を Web サーバにインストールします。証明書のインストール方法については、使用しているバージョンの IIS に関するマイクロソフトのマニュアルを参照してください。

ステップ 3　Microsoft IIS のマニュアルに従って、Web サーバ上で SSL セキュリティを有効にします。

SSL セキュリティを有効にする場合、次の点に留意してください。

- SSL セキュリティは、Web サイトのルートに対して、または 1 つ以上の仮想ディレクトリに対してイネーブルにできます。
- SSL をイネーブルにし、正しく設定すると、SSL 対応のクライアントだけが SSL 対応の WWW ディレクトリと通信できるようになります。
- SSL 対応の WWW フォルダにあるドキュメントを指す URL では、*http://* の代わりに *https://* を使用する必要があります。URL で *http://* を使用するリンクは、セキュア ディレクトリでは動作しません。

UCP ソフトウェアのインストール

始める前に

UCP ソフトウェアのインストール プロセスには、次の要件があります。

- 次の項の手順を完了していることを確認します。
  - Web サーバの準備（P.1-3）
  - UCP 向けの Cisco Secure ACS の準備（P.1-4）
- SSL を実装する場合は、P.1-6 の「Web サーバでの SSL のイネーブル化」の手順を完了していることを確認します。
- ACS の CD が手元にあることを確認します。

User-Changeable Password ソフトウェアをインストールするには、次の手順を実行します。

ステップ 1　UCP をインストールする Web サーバで、ローカル管理者としてログインします。

ステップ 2　Web サーバのドライブに ACS の CD を挿入します。

ヒント　autorun によって ACS のセットアップ ウィンドウが開いた場合は、**Cancel** をクリックします。

ステップ 3　Windows Explorer を使用して、ACS の CD にある UCP サブディレクトリを開きます。

ステップ 4　UCP の SETUP.EXE ファイルをダブルクリックします。

Before You Begin ダイアログボックスが表示されます。

ステップ 5　すべての項目のチェックボックスをオンにして、次に **Next** をクリックします。

Choose Destination Location ダイアログボックスに、UCP で使用される HTML ファイルのデフォルト ディレクトリが表示されます。

ステップ 6　P.1-3 の「Web サーバの準備」で作成した **secure** ディレクトリのフル パスを指定します。ディレクトリ名として **secure** を選択していて、*C:\Inetpub\wwwroot* が Web サーバのホーム ディレクトリであるときは、デフォルトの場所をそのまま使用できます。

ステップ 7　**Next** をクリックします。

2 つ目の Choose Destination Location ダイアログボックスに、UCP で使用される CGI 実行ファイルのデフォルト ディレクトリが表示されます。

ステップ 8　P.1-3 の「Web サーバの準備」で作成した **securecgi-bin** ディレクトリのフル パスを指定します。ディレクトリ名として **securecgi-bin** を選択していて、*C:\Inetpub\wwwroot* が Web サーバのホーム ディレクトリであるときは、デフォルトの場所をそのまま使用できます。

ステップ 9　**Next** をクリックします。

Enter Information ダイアログボックスに、Web サーバの IP アドレスを使用した、HTML 仮想ディレクトリのデフォルト URL が表示されます。

ステップ 10　HTML 仮想ディレクトリの URL を指定します。次の手順に従います。

- SSL を使用*しない*場合で、UCP HTML ディレクトリの仮想ディレクトリ エイリアスとして **secure** を使用するように選択している場合は、デフォルト値をそのまま使用できます。
- SSL を使用する場合は、URL の先頭部分を *http://* から *https://* に変更します。*http* の後ろに *s* が必要です。この文字がないと、ユーザと UCP 間の通信が SSL で暗号化されません。
- UCP HTML ディレクトリの仮想ディレクトリ エイリアスとして **secure** 以外の名前を選択している場合は、**secure** を、P.1-3 の「Web サーバの準備」で選択した名前に変更します。

たとえば、SSL を使用していて、HTML 仮想ディレクトリ エイリアスとして **ucp** を指定しているときは、URL を *https://IPAddress/ucp* に変更する必要があります。*IPAddress* は、Web サーバのドット付き 10 進 IP アドレスです。

ステップ 11　**Next** をクリックします。

2 つ目の Enter Information ダイアログボックスに、Web サーバの IP アドレスを使用した、CGI 仮想ディレクトリのデフォルト URL が表示されます。

ステップ 12 次のガイドラインに従って、CGI 仮想ディレクトリの URL を指定します。

- SSL を使用*しない*場合で、UCP CGI ディレクトリの仮想ディレクトリ エイリアスとして **securecgi-bin** を使用するように選択している場合は、デフォルト値をそのまま使用できます。
- SSL を使用する場合は、URL の先頭部分を *http://* から *https://* に変更します。*http* の後ろに `s` が必要です。この文字がないと、ユーザと UCP 間の通信が SSL で暗号化されません。
- UCP HTML ディレクトリの仮想ディレクトリ エイリアスとして **securecgi-bin** 以外の名前を選択している場合は、**secure** を、P.1-3 の「Web サーバの準備」で選択した名前に変更します。

たとえば、SSL を使用していて、HTML 仮想ディレクトリ エイリアスとして **ucpcgi-bin** を指定しているときは、URL を *https://IPAddress/ucpcgi-bin* に変更する必要があります。IPAddress は、Web サーバのドット付き 10 進 IP アドレスです。

ステップ 13 **Next** をクリックします。

Connecting to Cisco Secure Server ダイアログボックスが表示されます。

ステップ 14 UCP からのユーザ パスワード変更の送信先となる、ACS の IP アドレスを入力します。IP アドレスには、ドット付き 10 進形式を使用します。

ステップ 15 **Next** をクリックします。

指定した ACS への接続がテストされ、Setup Complete ダイアログボックスが表示されます。

ステップ 16 **Finish** をクリックして、インストールを完了します。

UCP がインストールされました。Web サーバが実行中かつアクセス可能な場合、ユーザは UCP を使用して ACS のパスワードを変更できます。UCP へのアクセスについては、P.1-8 の「UCP URL の特定」を参照してください。

UCP URL の特定

UCP のインストールが正常に終了したら、サポート対象の Web ブラウザを使用して UCP にアクセスできます。サポート対象の Web ブラウザのリストについては、アクセスする ACS のバージョンに対応したリリース ノートを参照してください。リリース ノートの最新版は、Cisco.com に掲載されています。

UCP Web ページの URL は次のとおりです。

http://webserver/secure/login.htm

ここで、*webserver* は UCP を実行している Web サーバのホスト名または IP アドレスであり、*secure* は P.1-3 の「Web サーバの準備」で作成した **secure** 仮想ディレクトリ エイリアスです。

ヒント UCP ページへの URL を短くするには、Web サーバ上のデフォルト ドキュメントに `login.htm` を付加します。この場合、URL は *http://webserver/secure* となります。

UCP のアップグレード

UCP ソフトウェアをアップグレードするには、次の手順を実行します。

ステップ 1　P.1-9 の「UCP のアンインストール」の手順を実行して、旧バージョンの UCP をアンインストールします。

ステップ 2　P.1-4 の「UCP 向けの Cisco Secure ACS の準備」の手順を実行します。

ステップ 3　アップグレードする新しいバージョンの UCP を使用して、P.1-3 の「UCP のインストール」の手順を実行します。

UCP のアンインストール

User-Changeable Password ソフトウェアをアンインストールするには、次の手順を実行します。

ステップ 1　UCP を実行しているコンピュータ上で、**Windows Control Panel > Add or Remove Programs** を選択して ACS User-Changeable Password をアンインストールします。

ステップ 2　IIS で、UCP の HTML ファイル用および CGI ファイル用に作成した仮想ディレクトリを削除します。これらのディレクトリのデフォルト名は、**secure** と **securecgi-bin** です。ただし、UCP のインストール時にディレクトリ名をカスタマイズしている可能性もあります。

ステップ 3　仮想ディレクトリがマップされていたディレクトリが削除されたことを確認します。この削除は、ステップ 1 で行われます。ディレクトリが削除されていない場合は、ここで削除します。

ステップ 4　Web サーバが IIS 6.0 を実行している場合は、IIS で未知の CGI 拡張機能を継続して許可するかどうかを検討します。この設定を変更するには、IIS Manager ウィンドウの Web Service Extension ページを使用して、**Allow Unknown CGI Extensions** のステータスを変更します。

ステップ 5　ACS の HTML インターフェイスで、UCP を実行していたサーバに対応する AAA サーバ設定を削除します。AAA サーバ設定の削除方法については、使用しているバージョンの ACS のユーザ ガイドを参照してください。

パスワードの変更

（注）　パスワードを変更するための適切なアクセス権が付与されていることを、システム管理者に確認してください。

Web サーバを使用してパスワードを変更するには、次の手順を実行します。

ステップ 1　Web ブラウザを起動し、管理者から通知された URL を使用して UCP ページを開きます。

ステップ 2　ユーザ名とパスワードを入力し、次に **Submit** をクリックします。

Change Password ページが開きます。前のページで入力したユーザ名が Username ボックスに表示されます。

ステップ 3　次のように入力します。

- **Current Password**：現在のパスワードを入力します。
- **New Password**：新しいパスワードを入力します。

（注）　パスワードは、最小文字数など、特殊な要件を満たさなければならない場合があります。詳細については、システム管理者に問い合せてください。

- **Confirm New Password**：新しいパスワードを再入力します。

ステップ 4　**Submit** をクリックします。

パスワードが変更されます。

ステップ 5　**Logout** をクリックして終了します。