



CHAPTER 1

Installing and Using Cisco Secure ACS User-Changeable Passwords

This guide contains instructions for installing and using UCPs with Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS. You can use UCPs with:

- ACS for Windows, Release 4.2
- Cisco Secure ACS Solution Engine, Release 4.2

This chapter contains:

- [About UCP](#)
 - [About SSL](#)
- [Installing UCP](#)
 - [Preparing the Web Server](#)
 - [Preparing ACS for UCP](#)
 - [Enabling SSL on the Web Server](#)
 - [Installing UCP Software](#)
 - [Determining the UCP URL](#)
- [Upgrading UCP](#)
- [Uninstalling UCP](#)
- [Changing Your Password](#)

About UCP

You use the UCP application to allow users to change their ACS passwords with a web-based utility. When users need to change passwords, they can access the UCP web page by using a supported web browser. For information about web browsers that we tested with ACS, see the release notes for your ACS product.

The UCP web page requires users to log in. The required password is the Password Authentication Protocol (PAP) password for the user account. UCP authenticates the user with ACS and then allows the user to specify a new password. UCP changes the user's PAP and Challenge Handshake Authentication Protocol (CHAP) passwords to the new password.

To install UCP, you must have a web server that runs:

- Microsoft IIS 5.0 (included with Windows 2000)
- Microsoft IIS 6.0 (included with Windows Server 2003)

About SSL

Communication between UCP and ACS is protected with a 128-bit encryption. To further increase security, we recommend implementing the secure sockets layer (SSL) to protect communication between web browsers and UCP. The SSL protocol provides security for remote-access data transfer between the UCP web server and the user's web browser.

Because users change their ACS internal database passwords over a connection between their web browsers and Microsoft IIS, user and password data is vulnerable. The SSL protocol encrypts data transfers, including passwords, between web browsers and Microsoft IIS.

SSL requires Microsoft IIS to present valid certificate credentials. You must obtain a certificate from a Certificate Authority (CA). If you use a public CA, it assigns you keys at a cost, provided you comply with certain requirements. The CA requires you to verify your credentials so that users and relying parties can trust the information in the CAs certificates. These credentials include verification and validation of legal, physical and operational legitimacy of your business.

Installing UCP

This section contains information and procedures for installing UCP.

This section describes:

- [Preparing the Web Server](#)
- [Preparing ACS for UCP](#)
- [Enabling SSL on the Web Server](#)
- [Installing UCP Software](#)
- [Determining the UCP URL](#)

Preparing the Web Server

To prepare the web server, you must create virtual directories. These virtual directories correspond to the file system directories where the UCP setup program places HTML files and Common Gateway Interface (CGI) executable files.

To prepare UCPs:

Step 1 Ensure that the web server uses either:

- Microsoft IIS 5.0 (included with Windows 2000)
- Microsoft IIS 6.0 (included with Windows Server 2003)



Tip To determine the home directory, see the default website properties for Microsoft IIS.

- Step 2** In the web server's home directory, create two directories:
- **secure**—This directory contains the HTML files that UCP uses. You can use a name different from **secure**. You should make note of the directory name for use in other installation steps.
 - **securecgi-bin**—This directory contains the executable CGI files that UCP uses. You can use a name different from **securecgi-bin**. You should keep track of the directory name for use in other installation steps.
- For example, if the home directory of the web server is *C:\inetpub\wwwroot*, you add the directories to *C:\inetpub\wwwroot*.
- Step 3** In Microsoft IIS, add a virtual directory for the HTML files that UCP uses. When you create the virtual directory, use:
- **Virtual Directory Alias**—A name for the virtual directory that corresponds to the **secure** directory, which you created in [Step 2](#). We recommend that you use **secure**. This alias is a component in the URL that you use to access UCP; so, a short but descriptive alias could help users remember the URL.
 - **Web Site Content Directory**—The specified directory must match the **secure** directory, which you created in [Step 2](#). The default directory from [Step 2](#) is *C:\inetpub\wwwroot\secure*.
 - **Access Permissions**—Assign read permission to this virtual directory. No other permissions are necessary.
- For information about creating virtual directories, see the Microsoft documentation for your version of IIS.
- Step 4** Add a virtual directory for the CGI executable files that UCP uses. When you create the virtual directory, use:
- **Virtual Directory Alias**—A name for the virtual directory that corresponds to the **securecgi-bin** directory, which you created in [Step 2](#). We recommend that you use **securecgi-bin**.
 - **Web Site Content Directory**—The specified directory must match the **securecgi-bin** directory created in [Step 2](#). The default directory from [Step 2](#) is *C:\inetpub\wwwroot\securecgi-bin*.
 - **Access Permissions**—Assign read and execute permissions to this virtual directory. No other permissions are necessary.
- For information about creating virtual directories, see the Microsoft documentation for your version of IIS.
- Step 5** If the web server runs IIS 6.0, you must configure IIS to allow unknown CGI extensions. Right click the Web Service Extension node in the IIS Manager window and select the **Allow** option to set the **Allow Unknown CGI Extensions** to **Allowed**.
- Step 6** If you use the IIS Lockdown Tool to help secure your Microsoft IIS 5.0 or IIS 4.0 web server, ensure that the Lockdown Tool allows executable files to run. If the executable files cannot run, UCP fails and users cannot change passwords.
-

Preparing ACS for UCP

To prepare for UCP you must configure ACS to recognize the web server as a type of authentication, authorization, and accounting (AAA) server. Once you perform the steps below [To prepare ACS for UCPs](#), ACS can recognize and respond to user password changes from UCP on the web server. Without this configuration, ACS ignores user password change requests from UCP.

**Note**

If ACS and Microsoft IIS software run on the same computer, you do not need to perform the previous steps. Proceed to [Enabling SSL on the Web Server](#).

To prepare ACS for UCPs:

Step 1 Log in to the web interface of the ACS to which you want UCP to send user password changes.

**Note**

If you are using the ACS Internal Database Replication feature, the ACS to which UCP sends user password changes should be a primary ACS; otherwise, if the user database is replicated, the older information from the primary ACS overwrites user password changes.

Step 2 Choose **Interface Configuration > Advanced Options**.

The Advanced Options page appears.

Step 3 Ensure that you check the **Distributed Systems Settings** check box. Checking this option allows the AAA servers table to appear in the Network Configurations section.

Step 4 Click **Submit**.

Step 5 Click **Network Configuration**.

Step 6 If you enable network device groups (NDGs), click the NDG to which to add the UCP web server.

Step 7 In the AAA Servers table, click **Add Entry**.

Step 8 In the AAA Server Name box, enter the name for the UCP web server. We recommend using the web server hostname; however, you can include additional useful information, such as **UCP**, to readily identify the UCP web server. For example, if the web server hostname is **wwwin**, you could enter **UCP-wwwin** in the AAA Server Name box.

Step 9 In the AAA Server IP Address box, enter the IP address of the UCP web server. Use dotted-decimal format.

**Note**

The other settings on the Add AAA Server page are irrelevant to UCP.

Step 10 Click **Submit + Restart**.

ACS is configured to recognize and respond to password change information from the web server on which you will install UCP.

Enabling SSL on the Web Server

This section explains how to enable SSL to encrypt communication between a user's web browser and the Microsoft IIS that is running UCP.

**Note**

We recommend enabling SSL. If, without exception, every user always accesses UCP from inside a secure perimeter, SSL might not be necessary; otherwise, you should enable SSL so that UCP traffic is encrypted between a user's web browser and the web server that is running UCP.

To enable optional SSL security on the web server:

-
- Step 1** Obtain a certificate from a certificate authority.
- Step 2** After you receive your certificate from the certificate authority, install the certificate on your web server. For information about installing a certificate, see Microsoft documentation for your version of IIS.
- Step 3** Following your Microsoft IIS documentation, activate SSL security on the web server.

When you enable SSL security, remember that:

- You can enable SSL security on the root of your web site or on one or more virtual directories.
 - After SSL is enabled and properly configured, only SSL-enabled clients can communicate with the SSL-enabled WWW directories.
 - URLs that point to documents on an SSL-enabled WWW folder must use *https://* instead of *http://* in the URL. Links that use *http://* in the URL do not work on a secure directory.
-

Installing UCP Software

Before You Begin

The UCP software installation process has the following requirements. Ensure that you have:

- Completed the steps in these sections:
 - [Preparing the Web Server](#)
 - [Preparing ACS for UCP](#)
- Completed the procedure in [Enabling SSL on the Web Server](#), if you intend to implement SSL.
- The ACS installation CD.

To install the User-Changeable Password software:

-
- Step 1** Log in as the local administrator to the web server on which you are installing UCP.
- Step 2** Insert the ACS Installation CD in the drive on the web server.



Tip If `autorun` opens a setup window for ACS, click **Cancel**.

- Step 3** Use Windows Explorer to open the UCP subdirectory on the ACS Installation CD.
- Step 4** Double-click the UCP *setup.exe* file.
The Before You Begin dialog box appears.
- Step 5** Check the check boxes for all items, and then click **Next**.
The Choose Destination Location dialog box displays a default directory for HTML files that UCP uses.
- Step 6** Specify the full path of the secure directory that you created in [Preparing the Web Server](#). If you chose **secure** as the directory name and *C:\inetpub\wwwroot* is the home directory of the web server, you can accept the default location.
- Step 7** Click **Next**.

A second Choose Destination Location dialog box displays a default directory for the CGI executable files that UCP uses.

Step 8 Specify the full path of the **securecgi-bin** directory that you created in [Preparing the Web Server](#). If you chose **securecgi-bin** as the directory name and *C:\inetpub\wwwroot* is the home directory of the web server, you can accept the default location.

Step 9 Click **Next**.

The Enter Information dialog box displays the default URL for the HTML virtual directory by using the web server's IP address.

Step 10 Specify the URL for the HTML virtual directory. If you:

- Are not using SSL and you chose to use **secure** as the virtual directory alias for the UCP HTML directory, you can accept the default value.
- Are using SSL, change the beginning of the URL from *http://* to *https://*. The letter *s* is required after *http*; otherwise, communication between users and UCP will not be SSL-encrypted.
- Chose a name that is different from **secure** as the virtual directory alias for the UCP HTML directory, change **secure** to the name that you chose in [Preparing the Web Server](#).

For example, if you are using SSL and you specified **ucp** as the HTML virtual directory alias, you should change the URL to *https://IPAddress/ucp*, where *IPAddress* is the dotted-decimal IP address of the web server.

Step 11 Click **Next**.

A second Enter Information dialog box displays the default URL for the CGI virtual directory by using the web server's IP address.

Step 12 Specify the URL for the CGI virtual directory, if you:

- Are not using SSL and you chose to use **securecgi-bin** as the virtual directory alias for the UCP CGI directory, you can accept the default value.
- Are using SSL, change the beginning of the URL from *http://* to *https://*. The letter *s* is required after *http*; otherwise, communication between users and UCP will not be SSL-encrypted.
- Choose a name different from **securecgi-bin** as the virtual directory alias for the UCP HTML directory, change **secure** to the name that you chose in [Preparing the Web Server](#).

For example, if you are using SSL and you specified **ucpcgi-bin** as the HTML virtual directory alias, you should change the URL to *https://IPAddress/ucpcgi-bin*, where *IPAddress* is the dotted-decimal IP address of the web server.

Step 13 Click **Next**.

The Connecting to Cisco Secure Server dialog box appears.

Step 14 Enter the IP address of the ACS which, is configured to recognize the UCP client and to receive user password change requests (in [Preparing ACS for UCP](#) sections). Use dotted-decimal format for the IP address.

Step 15 Click **Next**.

Setup tests the connection to the ACS that you specified, and then the Setup Complete dialog box appears.

Step 16 To complete the installation, click **Finish**.

UCP is installed. If the web server is running and accessible, users can change ACS passwords with UCP. For information about accessing UCP, see [Determining the UCP URL](#).

Determining the UCP URL

After you have successfully installed UCP, you can access UCP with a supported web browser. For a list of supported web browsers, see the release notes for the version of ACS that you are accessing. The latest revision to the Release Notes is posted on [Cisco.com](http://www.cisco.com).

The URL for the UCP web page is:

`http://webserver/secure/login.htm`

where *webserver* is the hostname or IP address of the web server that is running UCP and *secure* is the **secure** virtual directory alias that you created in [Preparing the Web Server](#).

**Tip**

For a shorter URL to the UCP page, add *login.htm* to the default documents on the web server. The URL would then be `http://webserver/secure`.

Upgrading UCP

To upgrade the UCP software:

-
- Step 1** Uninstall the old version of UCP by performing the steps in [Uninstalling UCP](#).
 - Step 2** Perform the steps in [Preparing ACS for UCP](#).
 - Step 3** By using the version of UCP to which you want to upgrade, perform the steps in [Installing UCP](#).
-

Uninstalling UCP

To uninstall the UCP software:

-
- Step 1** On the computer that is running UCP, choose **Windows Control Panel > Add or Remove Programs** to uninstall ACS UCP.
 - Step 2** In IIS, remove the virtual directories created for the UCP HTML and CGI files. The default names of these directories are **secure** and **securecgi-bin**; however, you might have customized the directory names when you installed UCP.
 - Step 3** Verify that the directories to which the virtual directories were mapped are deleted. This deletion should occur during [Step 1](#). If the directories are not deleted, delete them now.
 - Step 4** If the web server runs IIS 6.0, consider whether you want IIS to continue to allow unknown CGI extensions. To change this setting, use the Web Service Extension page in the IIS Manager window and modify the status of **Allow Unknown CGI Extensions**.
 - Step 5** In the ACS HTML interface, delete the AAA server configuration that corresponds to the server that ran UCP. For more information about deleting AAA server configurations, see the user guide for your version of ACS.
-

Changing Your Password

**Note**

Check with your system administrator to ensure that you have the appropriate permissions to change your password.

To change your password by using the web server:

Step 1 Open the UCP page in the web browser, using the URL that your administrator provided.

Step 2 Enter your username and password, and then click **Submit**.

The Change Password page opens. The username that you entered on the previous page appears in the Username box.

Step 3 Enter the:

- **Current Password**—Enter your current password.
- **New Password**—Enter the new password.

**Note**

Your password might need to fulfill certain special requirements, such as minimum length. Check with your system administrator for details.

- **Confirm New Password**—Retype the new password.

Step 4 Click **Submit**.

Your password is changed.

Step 5 To exit, click **Logout**.
