



## **Installation and User Guide for Cisco Secure ACS User-Changeable Passwords 4.2**

February 2008

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-14391-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)



## CONTENTS

<b>Preface</b>	<b>v</b>
Audience	v
Conventions	v
Product Documentation	vi
Related Documentation	viii
Open Source License Acknowledgements	viii
OpenSSL/Open SSL Project	viii
License Issues	viii
Obtaining Documentation and Submitting a Service Request	x
<b>Installing and Using Cisco Secure ACS User-Changeable Passwords</b>	<b>1-1</b>
About UCP	1-1
About SSL	1-2
Installing UCP	1-2
Preparing the Web Server	1-2
Preparing ACS for UCP	1-3
Enabling SSL on the Web Server	1-4
Installing UCP Software	1-5
Determining the UCP URL	1-7
Upgrading UCP	1-7
Uninstalling UCP	1-7
Changing Your Password	1-8





## Preface

---

This guide describes the installation, configuration, and use of User-Changeable Passwords (UCP) for Cisco Secure Access Control Server Release 4.2 for Windows, hereafter referred to as ACS.

## Audience

This guide is written for network administrators who install and configure UCP for use with ACS, release 4.2. It also contains information for network users who access the UCP website to change their ACS passwords.

## Conventions

This document uses the following conventions:

Item	Convention
Commands, keywords, special terminology, and options that should be selected during procedures	<b>boldface</b> font
Variables for which you supply values and new or important terminology	<i>italic</i> font
Displayed session and system information, paths, and file names	<code>screen</code> font
Information you enter	<b>boldface</b> <code>screen</code> font
Variables you enter	<i>italic</i> <code>screen</code> font
Menu items and button names	<b>boldface</b> font
Indicates menu items to select, in the order you select them.	<b>Option &gt; Network Preferences</b>



### Tip

Identifies information to help you get the most benefit from your product.



### Note

Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

**Warning**

Identifies information that you must heed to prevent damaging yourself, the state of software, or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.

## Product Documentation

**Note**

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available.

**Table 1**      **Product Documentation**

Document Title	Available Formats
<i>Documentation Guide for Cisco Secure ACS 4.2</i>	<ul style="list-style-type: none"> <li>Printed document with product.</li> <li>PDF on the product CD-ROM.</li> <li>On <a href="http://www.cisco.com">Cisco.com</a>: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/roadmap/DGuide42.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/roadmap/DGuide42.html</a></li> </ul>
<i>User Guide for Cisco Secure Access Control Server 4.2</i>	<ul style="list-style-type: none"> <li>PDF on the ACS Recovery CD-ROM.</li> <li>You can also access the user guide by clicking <b>Online Documentation</b> in the ACS navigation menu. The user guide PDF is available on this page by clicking <b>View PDF</b>.</li> <li>On <a href="http://www.cisco.com">Cisco.com</a>: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/ACS4_2UG.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/ACS4_2UG.html</a></li> </ul>
<i>Configuration Guide for Cisco Secure ACS 4.2</i>	<ul style="list-style-type: none"> <li>PDF on the ACS Recovery CD-ROM.</li> <li>On <a href="http://www.cisco.com">Cisco.com</a>: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs42_config_guide.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs42_config_guide.html</a></li> </ul>

**Table 1**      **Product Documentation (continued)**

Document Title	Available Formats
<i>Installation Guide for Cisco Secure ACS for Windows 4.2</i>	<ul style="list-style-type: none"> <li>• PDF on the ACS Recovery CD-ROM.</li> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/IGwn42.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/IGwn42.html</a></li> </ul>
<i>Installation Guide for Cisco Secure ACS Solution Engine 4.2</i>	<ul style="list-style-type: none"> <li>• PDF on the ACS Recovery CD-ROM.</li> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/solution_engine/SE42.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/solution_engine/SE42.html</a></li> </ul>
<i>Installation and User Guide for Cisco Secure ACS User Changeable Passwords 4.2</i>	<ul style="list-style-type: none"> <li>• PDF on the ACS Recovery CD-ROM.</li> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/user_passwords/ucp42.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/user_passwords/ucp42.html</a></li> </ul>
<i>Installation and Configuration Guide for Cisco Secure ACS Remote Agents 4.2</i>	<ul style="list-style-type: none"> <li>• PDF on the ACS Recovery CD-ROM.</li> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/remote_agent/rmag42.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/remote_agent/rmag42.html</a></li> </ul>
<i>Cisco Secure Access Control Server Troubleshooting Guide</i>	<p>On Cisco.com: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/trouble/guide/ACS_Troubleshooting.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/trouble/guide/ACS_Troubleshooting.html</a></p>
<i>Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine 4.2</i>	<ul style="list-style-type: none"> <li>• Shipped with product.</li> <li>• PDF on the product CD-ROM.</li> <li>• Printed document available by order (part number DOC-7817259).</li> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/regulatory/compliance/RCSI_42.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/regulatory/compliance/RCSI_42.html</a></li> </ul>
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS 4.2</i>	<ul style="list-style-type: none"> <li>• PDF on the ACS Recovery CD-ROM.</li> <li>• On Cisco.com: <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/device/guide/sdt42.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/device/guide/sdt42.html</a></li> </ul>

**Table 1**      **Product Documentation (continued)**

Document Title	Available Formats
<i>Release Notes for Cisco Secure ACS 4.2</i>	On <a href="http://www.cisco.com">Cisco.com</a> : <a href="http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/release/notes/ACS42_RN.html">http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/release/notes/ACS42_RN.html</a>
Online Documentation	In the ACS HTML interface, click Online Documentation.
Online Help	In the ACS HTML interface, online help appears in the right pane when you are configuring a feature.
Short help	Select an option from the ACS web interface; the help appears in the right pane.

## Related Documentation



### Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on [Cisco.com](http://www.cisco.com) for any updates.

To view a set of white papers about Cisco Secure ACS for Windows Server, go to:

[http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/prod\\_white\\_papers\\_list.html](http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/prod_white_papers_list.html)

## Open Source License Acknowledgements

The following acknowledgements pertain to this software license.

### OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

#### OpenSSL License:

© 1998-1999 The OpenSSL Project. All rights reserved.



Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

**Original SSLeay License:**

© 1995-1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). All rights reserved.

This package is an SSL implementation written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



# 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**.

---



## INDEX

---

### A

ACS  
    internal database replication [1-4](#)

---

### C

cautions  
    significance of [1-vi](#)  
CGI files [1-3](#)  
conventions [1-v](#)

---

### D

directories  
    secure [1-3, 1-5](#)  
    securecgi-bin [1-3, 1-6](#)  
documentation  
    conventions [1-v](#)

---

### M

Microsoft IIS  
    versions [1-2](#)  
    virtual directory [1-3](#)

---

### P

password  
    changing [1-8](#)

---

### S

secure sockets layer [1-2](#)  
security [1-2](#)  
SSL  
    enabling [1-4](#)

---

### U

UCP  
    access to web page [1-1](#)  
    installing [1-2](#)  
    software installation [1-5](#)  
    uninstalling [1-7](#)  
    upgrading [1-7](#)  
URL [1-7](#)

---

### V

virtual directories [1-3](#)

---

### W

warnings  
    significance of [1-vi](#)

