

Installation and User Guide for Cisco Secure ACS User-Changeable Passwords

Release 4.0
November 2005

Corporate 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: 408 526-4100

Text Part Number: OL-7465-01



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.

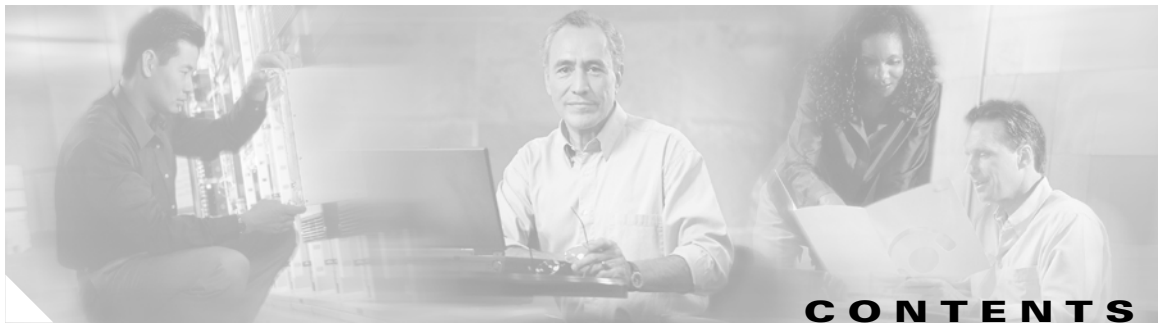
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0502R)

Installation and User Guide for Cisco Secure ACS User-Changeable Passwords
Copyright © 2003–2005, Cisco Systems, Inc. All rights reserved.



Preface	v	
Audience	v	
Conventions	v	
Product Documentation	vi	
Related Documentation	vii	
Obtaining Documentation	vii	
Cisco.com	vii	
Product Documentation DVD	viii	
Ordering Documentation	viii	
Documentation Feedback	viii	
Cisco Product Security Overview	viii	
Reporting Security Problems in Cisco Products	ix	
Obtaining Technical Assistance	ix	
Cisco Technical Support & Documentation Website	x	
Submitting a Service Request	x	
Definitions of Service Request Severity	x	
Obtaining Additional Publications and Information	xi	
CHAPTER 1	Installing and Using Cisco Secure ACS User-Changeable Passwords	1-1
About UCP	1-1	
About SSL	1-2	
Installing UCP	1-2	
Preparing the Web Server	1-2	
Preparing Cisco Secure 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 for Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

Audience

This guide is written for network administrators who install and configure User-Changeable Passwords for use with ACS, release 4.0. It also contains information for network users who access the User-Changeable Passwords 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	boldface font
Variables for which you supply values and new or important terminology	<i>italic font</i>
Displayed session and system information, paths and file names	<code>screen font</code>
Information you enter	boldface screen font
Variables you enter	<i>italic screen font</i>
Menu items and button names	boldface font
Indicates menu items to select, in the order you select them.	Option > Network Preferences



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>Release Notes for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com.
<i>Release Notes for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com.
<i>Installation and Setup Guide for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com. Printed document available by order (part number DOC-7816532).¹
<i>Installation Guide for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com. Printed document available by order (part number DOC-7816529=).¹
<i>User Guide for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com. Printed document available by order (part number DOC-7816534=).¹
<i>User Guide for Cisco Secure ACS for Windows Server</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com. Printed document available by order (part number DOC-7816592=).¹

Table 1 **Product Documentation (Continued)**

Document Title	Available Formats
<i>Installation and User Guide for Cisco Secure ACS User-Changeable Passwords</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com.
<i>Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine</i>	<ul style="list-style-type: none"> • Printed document that was included with the product. • PDF on the product CD-ROM. • On Cisco.com.
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine</i>	On Cisco.com .
<i>Recommended Resources for the Cisco Secure ACS User</i>	On Cisco.com .
Online Documentation	In the Cisco Secure ACS HTML interface, click Online Documentation.

1. See [Obtaining Documentation](#), page vii.

Related 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.

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

Obtaining Documentation

Cisco documentation and additional literature are available on [Cisco.com](#). Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



Installing and Using Cisco Secure ACS User-Changeable Passwords

This guide contains instructions for installing and using User-Changeable Passwords (UCP) with Cisco Secure Access Control Server Release 4.0, hereafter referred to as ACS. You can use UCP with:

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

This chapter contains the following topics:

- [About UCP, page 1-1](#)
 - [About SSL, page 1-2](#)
- [Installing UCP, page 1-2](#)
 - [Preparing the Web Server, page 1-2](#)
 - [Preparing Cisco Secure ACS for UCP, page 1-3](#)
 - [Enabling SSL on the Web Server, page 1-4](#)
 - [Installing UCP Software, page 1-5](#)
 - [Determining the UCP URL, page 1-7](#)
- [Upgrading UCP, page 1-7](#)
- [Uninstalling UCP, page 1-7](#)
- [Changing Your Password, page 1-8](#)

About UCP

You use the UCP application to enable 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) or 6.0 (included with Windows Server 2003).

About SSL

Communication between UCP and ACS is protected with 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. If you use a public certificate authority, the certificate authority assigns your keys for a fee, provided that you comply with certain requirements.

Installing UCP

This section contains information and procedures for installing UCP.

This section contains the following topics:

- [Preparing the Web Server, page 1-2](#)
- [Preparing Cisco Secure ACS for UCP, page 1-3](#)
- [Enabling SSL on the Web Server, page 1-4](#)
- [Installing UCP Software, page 1-5](#)
- [Determining the UCP URL, page 1-7](#)

Preparing the Web Server

To prepare the web server, you must create virtual directories on the web server. These virtual directories correspond to the file system directories where the UCP setup program will place HTML files and CGI executable files.

To prepare for UCPs:

Step 1 Ensure that the web server uses Microsoft IIS 5.0 or 6.0:

- IIS 5.0 is included with Windows 2000.
- IIS 6.0 is included with Windows Server 2003.

Step 2 In the web server's home directory, create two directories:



Tip To determine the home directory, see the Default Web Site properties for Microsoft IIS.

- **secure**—This directory will contain the HTML files used by UCP. You can use a name different from **secure**. You should keep track of the directory name for use in other installation steps.
- **securecgi-bin**—This directory will contain the executable CGI files used by UCP. 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 used by UCP. When you create the virtual directory, use:
- **Virtual Directory Alias**—A name for the virtual directory that corresponds to the **secure** directory created in [Step 2](#). We recommend that you use **secure**. This alias will be a component in the URL used 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 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 used by UCP. When you create the virtual directory, use:
- **Virtual Directory Alias**—A name for the virtual directory that corresponds to the **securecgi-bin** directory 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. Use the Web Service Extension page in the IIS Manager window and set the status of **Allow Unknown CGI Extensions** to **Allowed**.
- Step 6** If you use the IIS Lockdown Tool to help secure your Microsoft IIS 5.0 web server, be sure that the Lockdown Tool allows executable files to run. If the executable files cannot run, UCP fails and users cannot change passwords.

Preparing Cisco Secure ACS for UCP

To prepare ACS for UCP, you must configure ACS to recognize the web server as a type of authentication, authorization, and accounting (AAA) server. Once you perform this step, 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 these steps. Proceed to [Enabling SSL on the Web Server, page 1-4](#).

To prepare 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 the Distributed Systems Settings check box is checked. This option enables the AAA Servers table to appear in the Network Configurations section.

Step 4 Click **Submit**.

Step 5 Click **Network Configuration**.

Step 6 If you have enabled 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, type 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 type **UCP-wwwin** in the AAA Server Name box.

Step 9 In the AAA Server IP Address box, type 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 within 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 have received 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, page 1-2](#)
 - [Preparing Cisco Secure ACS for UCP, page 1-3](#)
- Ensure that you have completed the procedure in [Enabling SSL on the Web Server, page 1-4](#), if you intend to implement SSL.
- Ensure that you have the ACS CD.

To install the User-Changeable Password software:

-
- Step 1** At the web server on which to install UCP, log in as the local administrator.
- Step 2** Insert the ACS 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 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 used by UCP.
- Step 6** Specify the full path of the **secure** directory that you created in [Preparing the Web Server, page 1-2](#). 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 used by UCP.

Step 8 Specify the full path of the **securecgi-bin** directory that you created in [Preparing the Web Server, page 1-2](#). If you chose **securecgi-bin** as the directory name and *C:\netpub\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 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, page 1-2](#).

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, using the web server's IP address.

Step 12 Specify the URL for the CGI virtual directory, following these guidelines:

- 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.
- If you 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.
- If you chose 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, page 1-2](#).

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 Type the IP address of the ACS to which you want UCP to send user password changes. Use dotted decimal format for the IP address.

Step 15 Click **Next**.

Setup tests the connection to 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, page 1-7](#).

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 running UCP and *secure* is the **secure** virtual directory alias created in [Preparing the Web Server, page 1-2](#).



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, page 1-7](#).
 - Step 2** Perform the steps in [Preparing Cisco Secure ACS for UCP, page 1-3](#).
 - Step 3** Using the version of UCP to which you want to upgrade, perform the steps in [Installing UCP, page 1-2](#).
-

Uninstalling UCP

To uninstall the User-Changeable Password software:

-
- Step 1** On the computer running UCP, choose **Windows Control Panel > Add or Remove Programs** to uninstall ACS User-Changeable Passwords.
 - 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 Using a web browser, open the UCP page by using the URL that your administrator provided.

Step 2 Type 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**—Type your current password.
- **New Password**—Type 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**.
