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

Version 3.3
June 2004

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

Customer Order Number:
Text Part Number: OL-5937-01

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

Preface

This guide describes the installation, configuration, and use of User-Changeable Passwords for Cisco Secure Access Control Server (ACS), version 3.3.

Audience

This guide is written for network administrators who need to install and configure User-Changeable Passwords for use with Cisco Secure ACS, version 3.3. It also contains information for network users who access the User-Changeable Passwords web site to change their Cisco Secure 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	*italic* font
Displayed session and system information, paths and file names	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*italic screen* font

Item	Convention
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
Release Notes for Cisco Secure ACS Solution Engine	• Printed document that was included with the product. • On Cisco.com.
Release Notes for Cisco Secure ACS for Windows Server	• Printed document that was included with the product. • On Cisco.com.
Installation and Setup Guide for Cisco Secure ACS Solution Engine	• PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816532).[1]
Installation Guide for Cisco Secure ACS for Windows Server	• PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816529=)[1]
User Guide for Cisco Secure ACS Solution Engine	• PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816534=).[1]
User Guide for Cisco Secure ACS for Windows Server	• PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-7816592=).[1]
Installation and User Guide for Cisco Secure ACS User-Changeable Passwords	• PDF on the product CD-ROM. • On Cisco.com.
Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine	• Printed document that was included with the product. • PDF on the product CD-ROM. • On Cisco.com.

Table 1 Product Documentation (Continued)

Document Title	Available Formats
Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine	On Cisco.com.
Recommended Resources for the Cisco Secure ACS User	On Cisco.com.
Online Documentation	In the Cisco Secure ACS HTML interface, click Online Documentation.

1. See Obtaining Documentation, page ix.

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.

Table 2 describes a set of white papers about Cisco Secure ACS for Windows Server; however, much of the information contained in these papers is applicable to Cisco Secure ACS Solution Engine. All white papers are available on Cisco.com. To view them, go to the following URL:

http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml

Table 2 Related Documentation

Document Title	Description and Available Formats
Building a Scalable TACACS+ Device Management Framework	This document discusses the key benefits of and how to deploy Cisco Secure ACS Shell Authorization Command sets, which provide the facilities for constructing a scalable network device management system using familiar and efficient TCP/IP protocols and utilities supported by Cisco devices.
Catalyst Switching and ACS Deployment Guide	This document presents planning, design, and implementation practices for deploying Cisco Secure ACS for Windows Server in support of Cisco Catalyst Switch networks. It discusses network topology regarding AAA, user database choices, password protocol choices, access requirements, and capabilities of Cisco Secure ACS.
Deploying Cisco Secure ACS for Windows in a Cisco Aironet Environment	This paper discusses guidelines for wireless network design and deployment with Cisco Secure ACS.
EAP-TLS Deployment Guide for Wireless LAN Networks	This document discusses the Extensible Authentication Protocol Transport Layer Security (EAP-TLS) authentication protocol deployment in wireless networks. It introduces the EAP-TLS architecture and then discusses deployment issues.
Guidelines for Placing ACS in the Network	This document discusses planning, design, and implementation practices for deploying Cisco Secure ACS for Windows Server in an enterprise network. It discusses network topology, user database choices, access requirements, integration of external databases, and capabilities of Cisco Secure ACS.
Initializing MC Authorization on ACS 3.1	This application note explains how to initialize Management Center authorization on Cisco Secure ACS.

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/univercd/home/home.htm

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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

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 automatically provides

recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC 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 TAC 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, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *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

- 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

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

This guide contains instructions for installing and using Cisco Secure Access Control Server (ACS) User-Changeable Passwords (UCP) with either of the two following releases of Cisco Secure ACS:

- Cisco Secure ACS for Windows Server, version 3.3
- Cisco Secure ACS Solution Engine, version 3.3

This chapter contains the following topics:

About UCP

UCP is an application that enables users to change their Cisco Secure ACS passwords with a web-based utility. To install UCP, you must have a web server that runs Microsoft IIS 5.0 or 6.0. IIS 5.0 is included with Windows 2000. IIS 6.0 is included with Windows Server 2003.

When users need to change passwords, they can access the UCP web page using a supported web browser. For information about web browsers tested with Cisco Secure ACS, see the release notes for the Cisco Secure ACS product you are using.

The UCP web page requires users to log in. The password required is the PAP password for the user account. UCP authenticates the user with Cisco Secure ACS and then allows the user to specify a new password. UCP changes both the PAP and CHAP passwords for the user to the password submitted.

Communication between UCP and Cisco Secure ACS is protected with 128-bit encryption. To further increase security, we recommend implementing SSL to protect communication between web browsers and UCP.

About SSL

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 Cisco Secure ACS 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 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

Preparing the web server consists of creating 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, follow these steps:

Step 1 Make sure 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 file system directory that the web server uses as its home directory, create the following two directories:

- **secure**—This directory will contain the HTML files used by UCP. You can use a name different from `secure`. You will use the name you choose later in Step 3 of this procedure and twice more in Installing UCP Software, page 7.
- **securecgi-bin**—This directory will contain the executable CGI files used by UCP. You can use a name different from `securecgi-bin`. You will use the name you choose in Step 4 of this procedure and twice more in Installing UCP Software, page 7.

For example, if the home directory of the web server is `C:\Inetpub\wwwroot`, use My Computer to add the directories to `C:\Inetpub\wwwroot`.

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

Step 3 In Microsoft IIS, add a virtual directory for the HTML files used by UCP. Use the following information when you create the virtual directory:

- **Virtual Directory Alias**—A name for the virtual directory, which 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 directory specified must match the `secure` directory created in Step 2. The default directory from Step 2 is `C:\Inetpub\wwwroot\secure`.
- **Access Permissions**—Give this virtual directory read permissions. No other permissions are necessary.

For information about creating virtual directories, see Microsoft documentation for the version of IIS you are using.

Step 4 Add a virtual directory for the CGI executable files used by UCP. Use the following information when you create the virtual directory:

- **Virtual Directory Alias**—A name for the virtual directory, which corresponds to the `securecgi-bin` directory created in Step 2. We recommend that you use `securecgi-bin`.
- **Web Site Content Directory**—The directory specified must match the `securecgi-bin` directory created in Step 2. The default directory from Step 2 is `C:\Inetpub\wwwroot\securecgi-bin`.
- **Access Permissions**—Give this virtual directory read and execute permissions. No other permissions are necessary.

For information about creating virtual directories, see Microsoft documentation for the version of IIS you are using.

Step 5 If the web server runs IIS 6.0, you must configure IIS to allow unknown CGI extensions. To do so, 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 its executable files cannot run, UCP fails and users cannot change passwords.

Preparing Cisco Secure ACS for UCP

Preparing for Cisco Secure ACS consists of configuring Cisco Secure ACS to recognize the web server as a type of AAA server. This enables Cisco Secure ACS to recognize and respond to user password changes from UCP on the web server. Without this configuration, Cisco Secure ACS ignores user password change requests from UCP.

Note If Cisco Secure 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 6.

To prepare for UCPs, follow these steps:

Step 1 Log in to the HTML interface of the Cisco Secure ACS that you want UCP to send user password changes to.

Note If you are using the CiscoSecure Database Replication feature, the Cisco Secure ACS that UCP sends user password changes to should be a primary Cisco Secure ACS; otherwise, if the user database is replicated, user password changes are overwritten by the older information from the primary Cisco Secure ACS.

Step 2 Click **Interface Configuration**, and then click **Advanced Options**.

The Advanced Options page appears.

Step 3 Make sure the Distributed Systems Settings check box is selected. This enables the AAA Servers table to appear in the Network Configurations section.

Step 4 Click **Submit**.

Step 5 Click **Network Configuration**.

Step 6 If network device groups (NDGs) are enabled, click the NDG that you want to add the UCP web server to.

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

Step 8 In the AAA Server Name box, type the name you want to give to 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 proper functioning of UCP.

Step 10 Click **Submit + Restart**.

Cisco Secure ACS is configured to recognize and respond to password change information from the web server you plan to install UCP on.

Enabling SSL on the Web Server

This procedure contains information about using secure socket layer (SSL) to encrypt communication between a user's web browser and the Microsoft IIS running UCP.

Note We recommend enabling SSL. If, without exception, every user always accesses UCP from within a secure perimeter, SSL may not be necessary; otherwise, it is a worthwhile precaution to enable SSL so that UCP traffic between a user's web browser and the web server running UCP is encrypted.

To enable optional SSL security on the web server, follow these steps:

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 the version of IIS that you are using.

Step 3 Following your Microsoft IIS documentation, activate SSL security on the web server.

Keep in mind the following points when enabling SSL security:

- 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

Be sure you have completed the steps in these sections:

- Preparing the Web Server, page 3
- Preparing Cisco Secure ACS for UCP, page 5

If you intend to implement SSL, be sure you have read Enabling SSL on the Web Server, page 6 and completed the procedure it contains.

You will need the Cisco Secure ACS CD to complete this procedure.

To install the User-Changeable Password software, follow these steps:

Step 1 At the web server that you want to install UCP on, log in as the local administrator.

Step 2 Insert the Cisco Secure ACS CD in a CD-ROM or DVD-ROM drive on the web server.

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

Step 3 Use Windows Explorer to open the UCP subdirectory on the Cisco Secure ACS CD.

Step 4 Double-click the UCP `SETUP.EXE` file.

The Before You Begin dialog box appears.

Step 5 Select 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 3. 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 3. 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, using the web server's IP address.

Step 10 Specify the URL for the HTML virtual directory, following these guidelines:

- 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.
- 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 `secure` as the virtual directory alias for the UCP HTML directory, change "secure" to the name you chose in Preparing the Web Server, page 3.

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 you chose in Preparing the Web Server, page 3.

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 Cisco Secure ACS that you want UCP to send user password changes to. Use dotted decimal format for the IP address.

Step 15 Click **Next**.

Setup tests the connection to the Cisco Secure ACS 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 Cisco Secure ACS passwords with UCP. For information about accessing UCP, see Determining the UCP URL, page 10.

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 Cisco Secure ACS you are accessing. The latest revision to the Release Notes is posted on 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 3.

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

The upgrade process consists of uninstalling the old version of UCP and installing the new version.

To upgrade the User-Changeable Password software, follow these steps:

Step 1 Remove the old version of UCP by performing the steps in Uninstalling UCP, page 11.

Step 2 Perform the steps in Preparing Cisco Secure ACS for UCP, page 5.

Step 3 Using the version of UCP that you want to upgrade to, perform the steps in Installing UCP, page 3.

Uninstalling UCP

To uninstall the User-Changeable Password software, follow these steps:

Step 1 On the computer running UCP, use Control Panel to uninstall Cisco Secure ACS User-Changeable Passwords.

Step 2 In Microsoft 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 may have customized the directory names when you installed UCP.

Step 3 Make sure the directories that the virtual directories were mapped to are deleted. This should have happened as part of Step 1. If the directories were 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 Cisco Secure ACS HTML interface, delete the AAA server configuration that corresponds to the server that ran UCP. For more information about deleting a AAA server configuration, see the user guide for the version of Cisco Secure ACS that you are using.

Changing Your Password

Note Check with your system administrator to be sure you have the appropriate permissions to change your password.

To change your password using the web server, follow these steps:

Step 1 Using a web browser, open the UCP page 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 you entered on the previous page appears in the Username box.

Step 3 Specify the following information:

- **Current Password**—Type your current password.
- **New Password**—Type the new password. Your password might need to fulfill certain special requirements, such as minimum length. Check with your system administrator for details.
- **Confirm New Password**—Re-type the new password.

Step 4 Click **Submit**.

Your password is changed.

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