



CiscoSecure ACS 2.3 for UNIX Installation Guide

Product Number DOC-CSASC2.3UX-IG=

Use this guide to install the following CiscoSecure Access Control Server (ACS) products:

- *CiscoSecure ACS 2.3 for UNIX (CSU-2.3)*—Installs a new CiscoSecure ACS 2.3 for UNIX site *without* the optional Distributed Session Manager (DSM) module licensed or enabled.
- *CiscoSecure ACS 2.3 for UNIX Distributed Session Manager (CSU-2.3-DSM)*—Installs a new CiscoSecure ACS 2.3 for UNIX site *with* the DSM module licensed and enabled.
- *CiscoSecure ACS Distributed Session Manager Option (CSU-DSM)*—Adds the licensed and enabled DSM module to an already existing CiscoSecure ACS 2.3 for UNIX site.
- *CiscoSecure ACS for UNIX Upgrade to v2.3 (CSU-2.3-UG)*—Upgrades an existing CiscoSecure ACS 2.x for UNIX site to version 2.3.

This guide contains the following sections:

Section	Description
Considerations Before You Install CiscoSecure, page 2	Start with this section for factors to take into consideration before installing CiscoSecure ACS 2.3 for UNIX software.
Basic Installation Procedures, page 4	Read this section for the basic CiscoSecure ACS installation procedures.
Solaris 2.5.1 Patches, page 12	Read this section if you are installing on top of Solaris 2.5.1. It describes Solaris 2.5.1 patches necessary to run CiscoSecure ACS.
Upgrading from CiscoSecure ACS 2.x to 2.3, page 13	Read this section if you are upgrading from a previous version of CiscoSecure ACS.
Activating the DSM Module on an Existing CiscoSecure ACS 2.3, page 16	Read this section if you are licensing and activating the DSM module on an existing or newly upgraded CiscoSecure ACS 2.3 for UNIX site that is not yet licensed or enabled to support the DSM.
Setting Up an Oracle Database for CiscoSecure, page 17	Read this section if you intend to use an Oracle database engine to support CiscoSecure ACS. It describes the preinstallation Oracle configuration requirements.

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Copyright © 1998
Cisco Systems, Inc.
All rights reserved.

Section	Description
Setting Up a Sybase Enterprise SQL Server for CiscoSecure, page 19	Read this section if you intend to use a Sybase database engine to support CiscoSecure ACS. It describes the preinstallation Sybase configuration requirements.
Accessing CiscoSecure ACS 2.3 for UNIX Documentation, page 21	This section lists the online and printed sources of CiscoSecure documentation.
Installing without a CD-ROM, page 23	Read this section if you intend to install CiscoSecure ACS on a workstation with no CD-ROM.
Manually Enabling Profile Cache Updating, page 24	Read this section if you intend to run third-party programs that directly edit the CiscoSecure profile database.
CiscoSecure System Description, page 25	Read this section for a basic description of how CiscoSecure ACS software works with your other network components to provide authentication, authorization, and accounting services.
Distributed Session Manager Features, page 26	Read this section for a basic description of the Distributed Session Manager (DSM) feature and a summary of DSM installation and post-installation requirements.
Editing Configuration Files to Enable or Disable the DSM Module, page 28	Read this section if you want to enable DSM but do not have access to the CiscoSecure Administrator web pages.
Editing CSU.cfg to Specify a CiscoSecure Software License Key, page 29	Read this section if you want to specify a new or replacement software license key for CiscoSecure ACS but do not have access to the CiscoSecure Administrator web pages.
Cisco Connection Online, page 30	Read this section for guidelines on obtaining assistance and additional information from Cisco Systems.
Documentation CD-ROM, page 31	Read this section for information about Cisco documentation and additional literature.

Considerations Before You Install CiscoSecure

Before you begin, consider the following situations and steps you must take before starting the basic installation procedures in the next section.

Consideration	Requirements
If you are not familiar with how the CiscoSecure ACS software works:	You need to acquaint yourself with the basic CiscoSecure ACS system and how it works with other network components to provide authentication, authorization, and accounting services. First read “CiscoSecure System Description,” page 25.
If you need general information on the optional Distributed Session Manager (DSM) product:	You need to acquaint yourself with the max sessions control features that the optional Distributed Session Manager can provide. First read “Distributed Session Manager Features,” page 26.
If you are installing the product <i>CiscoSecure ACS 2.3 for UNIX</i>, which sets up a new CiscoSecure ACS site <i>without</i> a licensed or activated Distributed Session Manager (DSM) option:	Start with the procedures in “Basic Installation Procedures,” page 4.

Consideration	Requirements
If you are installing the product <i>CiscoSecure ACS for UNIX Upgrade to v2.3</i>, which upgrades a previous version of CiscoSecure ACS to CiscoSecure ACS 2.3:	You need to look up old configuration information to apply to the upgrade. First read “Upgrading from CiscoSecure ACS 2.x to 2.3,” page 13 for additional instructions.
If you are installing the product <i>CiscoSecure ACS 2.3 for UNIX Distributed Session Manager (DSM)</i>, which installs a new CiscoSecure ACS with the optional CiscoSecure Distributed Session Manager (DSM) module licensed and enabled:	- You need to preinstall Oracle Enterprise or Sybase Enterprise software for each of your CiscoSecure ACSes. Read “Setting Up an Oracle Database for CiscoSecure,” page 17 or “Setting Up a Sybase Enterprise SQL Server for CiscoSecure,” page 19. - You need to obtain a special DSM-enabling software license key, run the CiscoSecure installation program, and after installation, start the CiscoSecure Administrator web pages to enable the DSM feature. Read “Basic Installation Procedures,” page 4 for details. - After installation, set up replication among your Oracle or Sybase profile databases. - Enable AAA accounting functions on your client NASes.
If you are using the product, <i>CiscoSecure ACS Distributed Session Manager Option</i>, which enables the optional CiscoSecure Distributed Session Manager (DSM) module on an already existing CiscoSecure ACS 2.3 for UNIX site:	- You need to have installed Oracle Enterprise or Sybase Enterprise software prior to the last installation of your CiscoSecure ACSes. Read “Setting Up an Oracle Database for CiscoSecure,” page 17 or “Setting Up a Sybase Enterprise SQL Server for CiscoSecure,” page 19 - You need to obtain a special DSM-enabling software key and enable it through the CiscoSecure Administrator web pages. Read “Activating the DSM Module on an Existing CiscoSecure ACS 2.3,” page 16 - After enabling the DSM module, set up replication among your Oracle or Sybase profile databases. - Enable AAA accounting in the client NASes.
- If you plan to install more than one CiscoSecure ACS, and have your users authenticated from a common replicated profile database: OR - If you plan to support more than 5,000 users:	You need to purchase and preinstall Oracle Enterprise or Sybase Enterprise software for each of your CiscoSecure ACSes. First read “Setting Up an Oracle Database for CiscoSecure,” page 17 or “Setting Up a Sybase Enterprise SQL Server for CiscoSecure,” page 19.
If you want to download and install CiscoSecure ACS 2.3 for UNIX from the Internet:	You need to follow special procedures for downloading and starting the installation package. First read “Installing without a CD-ROM,” page 23.

Basic Installation Procedures

This section describes the basic procedures for first-time installation of CiscoSecure ACS 2.3 for UNIX at most sites.

Note If you are upgrading from a previous version of CiscoSecure ACS 2.x, see “Upgrading from CiscoSecure ACS 2.x to 2.3,” page 13 for additional instructions.

A. Check Package Contents

The CiscoSecure ACS package includes the following items:

- CD-ROM labeled *CiscoSecure ACS 2.3 for UNIX*
- Release notes (read *before* starting installation)
- *Requires Immediate Attention* form for software key
- *Cisco Information Packet*

B. Check System Requirements

The network components that interact with CiscoSecure ACS 2.3 for UNIX consist of:

- CiscoSecure ACS itself (a primary server installed on an UltraSPARC workstation plus an optional backup server, installed on a second UltraSPARC workstation, that can be activated if the primary unit is disabled)
- One or more client network access servers (NASes)
- Web-based console from which to manage CiscoSecure (this can be a separate workstation or the same UltraSPARC workstation where the CiscoSecure ACS is installed)
- RDBMS database site and server (this can be a separate workstation or the same UltraSPARC workstation where CiscoSecure ACS is installed)
- Optional token servers

Each of these components has certain CiscoSecure configuration requirements.

CiscoSecure ACS Server Requirements

The Cisco Secure ACS (and its optional backup server) requires the following hardware and software:

- UltraSPARC or compatible workstation
 - To support CiscoSecure ACS *without* the licensed Distributed Session Manager option:
 - Ultra 1 with a processor speed of 167 MHz or faster
 - Minimum 200 MHz if the Oracle or Sybase RDBMS is installed on the same system.
 - To support CiscoSecure ACS *with* the licensed Distributed Session Manager option:
 - Ultra 1 or faster
 - Ultra 10 or faster if the Oracle or Sybase RDBMS is installed on the same system

- Minimum 256 MB of swap space
 - Minimum 512 MB of swap space if the Oracle or Sybase RDBMS is installed on the same system
- 128 MB of RAM
 - 256 MB of RAM if the Oracle or Sybase RDBMS is installed on the same system
- Minimum 256 MB of free disk space (if you are using the supplied SQLAnywhere database)
 - Minimum 2 GB disk space if the Oracle or Sybase RDBMS is installed on the same system
- CD-ROM drive

Note If you need to install CiscoSecure on a UltraSPARC workstation with no CD-ROM drive, you can download the CiscoSecure installation package from the Cisco Systems web page. (See “Installing without a CD-ROM,” page 23.)

- Solaris 2.6, or Solaris 2.5.1 with patches (see “Solaris 2.5.1 Patches,” page 12 for special instructions concerning Solaris 2.5.1)

Note To check your version of Solaris, enter the Solaris command **uname -a**. If the system returns 5.5.1, Solaris 2.5.1 is installed. If the system returns 5.6, Solaris 2.6 is installed.

CiscoSecure NAS Requirements

The CiscoSecure ACS works with the following network access servers (NASes):

- Cisco routers (models AS5100 through AS5800 and AS2509 through AS2512) running Cisco IOS software (Release 11.2 or later)
- Selected routers not running Cisco IOS software, running RADIUS protocols conforming to IETF RADIUS, specifically RFCs 2138 and 2139.

CiscoSecure Workstation Console Requirements

The web-browser-based CiscoSecure ACS workstation console requires the following hardware and software:

- Pentium 90 or faster PC, or an UltraSPARC workstation

Note The UltraSPARC workstation can either be a separate workstation or the same UltraSPARC workstation on which CiscoSecure ACS will be installed.

- 32 MB of RAM on a PC
- SVGA display with resolution of 1024 x 768 or higher
- Minimum 1 MB of video RAM (2 MB recommended)
- 17-inch or larger monitor recommended

- One of the following web browsers:
 - Netscape Communicator (version 4.04, 4.05, 4.07 on Windows 95 or NT; version 4.04 on Solaris 2.5.1 or 2.6)
 - Internet Explorer (version 3.x or 4.x on Windows 95 or NT)

Note The browser must be enabled for Java and Java Script.

Database Installation Requirements

To support CiscoSecure database requirements, you have your choice of using the supplied SQLAnywhere database engine, or using supported versions of your own preinstalled Oracle Enterprise or Sybase Enterprise software running on your network.

Supported database engines include:

- The supplied *SQLAnywhere* database—Does not require preinstallation on the network; however please note the limitations of the SQLAnywhere database option. The SQLAnywhere database engine:
 - *Does not* support networks of more than 5,000 users
 - *Does not* support database replication
 - *Does not* support the CiscoSecure Distributed Session Manager (DSM) feature (which requires CiscoSecure database replication setup)

If your network requires these support features, Cisco recommends preinstalling the Oracle Enterprise or Sybase Enterprise database engine.

- *Oracle Enterprise* version 7.3.2, 7.3.3, 7.3.4, or 8.0.x (version 7.33 or higher required for database replication and DSM support.)—Requires preinstallation and configuration. It must be running during the CiscoSecure ACS installation. See “Setting Up an Oracle Database for CiscoSecure,” page 17, for instructions on configuring this software to support CiscoSecure ACS.

Note If you intend to set up CiscoSecure with Oracle database replication, Cisco recommends that you read the PDF document *Using CiscoSecure with Oracle’s Distributed Database Feature* (filename csbsdoc.pdf) before you install the Oracle or CiscoSecure software. This document is located in the /CSCEacs/reloc/FastAdmin/docs directory of the CiscoSecure distribution CD-ROM. It provides an easy-to-understand, start-to-finish, screen-by-screen configuration example of setting up Oracle database replication to work with CiscoSecure.

- *Sybase Enterprise* version 11.0.2 or higher—Requires preinstallation and configuration. It must be running during the CiscoSecure installation. See “Setting Up a Sybase Enterprise SQL Server for CiscoSecure,” page 19 for instructions on configuring this software to support the CiscoSecure ACS.

Token Servers Installed (If You Are Supporting Them)

If you are supporting token servers, they must be installed on the network *before* you install CiscoSecure ACS. Supported token servers include:

- CRYPTOCARD
- Secure Computing
- Security Dynamics, Inc.

C. Obtain a CiscoSecure Software License Key

Note If you are upgrading from a previous version of CiscoSecure 2.x, see “Upgrading from CiscoSecure ACS 2.x to 2.3,” page 13 for instructions on using your old software license key.

If you are installing the CiscoSecure ACS for the first time on this UltraSPARC workstation, do the following:

- Step 1** At the UltraSPARC workstation where you want to install CiscoSecure ACS, enter the **hostid** command to obtain the host ID of the system host. For example:
- ```
/usr/ucb/hostid
55412315
```
- Step 2** Note the host ID for the primary and backup CiscoSecure ACS systems.
- Step 3** Note the token code on the label attached to page 2 of the form titled *Requires Immediate Attention* or *Requires Immediate Attention (Distributed Session Manager)*.
- Step 4** To receive your software license key immediately, access and supply the above information to the CiscoSecure licensing web site at:
- <http://www.cisco.com/public/sw-center/access/ciscosecure/>

---

**Note** Software license keys issued to install CiscoSecure with the Distributed Session Manager (DSM) option will consist of 28 hexadecimal characters. Software license keys issued for CiscoSecure ACS 2.3 for UNIX *without* the DSM option will consist of 20 hexadecimal characters.

---

Alternatively, you can fill out the CiscoSecure Software Key Fax-Back form in one of the following documents and fax it to the number provided:

- *Requires Immediate Attention* —Use to obtain a software license key for the product labeled *CiscoSecure ACS 2.3 for UNIX* to set up new installations of CiscoSecure ACS 2.3 for UNIX *without* the DSM module enabled.
- *Requires Immediate Attention (CiscoSecure Distributed Session Manager)*—Use to obtain a software license key for the product labeled *CiscoSecure ACS 2.3 for UNIX Distributed Session Manager* to set up a new installation of CiscoSecure ACS 2.3 for UNIX with the DSM module enabled

You can also e-mail this information to: [licensing@cisco.com](mailto:licensing@cisco.com).

You'll receive your license key within three business days.

**Step 5** When you get the license key, transcribe it into the blank for **Enter the AAA Server License Key**, in step **D. Prepare Your Answers to the Install Questions**.

---

**Note** The CiscoSecure ACS software is licensed per server. Each CiscoSecure ACS requires its own license. You can also use a backup server license to allow sites to run redundant systems to back up system security and accounting information.

---

## D. Prepare Your Answers to the Install Questions

The questions you will be asked during the CiscoSecure ACS installation are similar to those below.

---

**Note** Save these answers for both *installation* and *post-installation* configuration.

---

- Is this a completely new install (Y/N)? \_\_\_\_\_

The answer is **Yes** unless you have installed a previous version of CiscoSecure ACS (2.x) and want to use the same database information.

- Enter the directory name to install CiscoSecure into.

\_\_\_\_\_

The disk space requirement for this directory is 120 MB.

- IP Address to use for CiscoSecure. \_\_\_\_\_

The default is the primary IP address of the server on which you are installing the CiscoSecure ACS. For single server installation, use the default; otherwise, specify the address of the first ACS.

- **Enter the AAA Server License Key.** \_\_\_\_\_

Specify the software license key code that you received after you accessed the CiscoSecure licensing web site or filled out the "CiscoSecure Software Key Fax Back Form."

- If the hostname of this server is not the same as its fully qualified domain name (FQDN), enter the FQDN. \_\_\_\_\_

Specify the FQDN of the UltraSPARC workstation where you are installing the ACS *only if the FQDN is different* from the host name; otherwise, accept the default (host name) value for this prompt.

- Enter the TACACS+ NAS name you will be using. \_\_\_\_\_

To support TACACS+ enabled NAS(es), either specify the host name of one such NAS, or indicate that any NAS with a specified TACACS+ secret key will be using the CiscoSecure ACS.

When you run the install program, pressing **Enter** for this prompt's default selection, **none**, supports any NAS with a specified TACACS+ secret key.

- Enter the TACACS+ NAS secret key. \_\_\_\_\_

If you intend to support TACACS+ enabled NAS(es), specify a secret TACACS+ key string.

- Select token card(s) or none: (1. CRYPTOCARD, 2. Secure Computing, 3. Security Dynamics, Inc.) \_\_\_\_\_

If you want to support one of the listed Token Cards, specify the card you want to support.

---

**Note** Selecting Security Dynamics, Inc. requires that the SDI client software be properly installed before the ACS is started.

---

- [If Secure Computing] Do you want to use CiscoSecure's SafeWord GUI Software (Y/N)?  
\_\_\_\_\_

This feature requires local root read/write file access to the SafeWord directory.

- [If Secure Computing] Enter the directory path for the SafeWord Software.  
\_\_\_\_\_

Enable SafeWord's IMPORT/EXPORT option in the Secure Computing SafeWord application program.

- [If Secure Computing] Enter the IP Address of the Secure Computing server.  
\_\_\_\_\_

- Choose a Database: (1. SQLAnywhere, 2. Oracle Enterprise, 3. Sybase Enterprise)  
\_\_\_\_\_

Specify the database for the AAA data. SQLAnywhere is the default choice and is supplied with the CiscoSecure ACS. Oracle Enterprise or Sybase Enterprise support require that those products already be installed and accessible on your network during CiscoSecure installation.



**Caution** The SQLAnywhere database engine *does not* support networks of more than 5,000 users, *does not* support database replication, and *does not* support the maximum session limitation feature of the optional CiscoSecure Distributed Session Manager feature. If your network requires these support features, Cisco recommends preinstalling the Oracle Enterprise or Sybase Enterprise database engine.

- If SQLAnywhere, the directory where you want the database files to be created.  
\_\_\_\_\_

This directory requires disk space of 256 MB.

- If Sybase or Oracle, the username and password to the DB account that has been assigned database space for the CiscoSecure ACS data. \_\_\_\_\_

- If Oracle, the path to the \$ORACLE\_HOME directory, where Oracle is installed.  
\_\_\_\_\_

- If Oracle, the TNS Service name of the Oracle server.  
\_\_\_\_\_

- If Sybase [Enterprise], the name of the Sybase SQL server.  
\_\_\_\_\_

- If Sybase [Enterprise], the name of the database to use for CiscoSecure.  
\_\_\_\_\_

- If Sybase [Enterprise], the path to the \$SYBASE directory where Sybase is installed.  
\_\_\_\_\_

- If not a New Install, do you want to drop and re-init existing Database Tables (Y/N)?  
\_\_\_\_\_

If this is not a new installation, specify whether you want to remove the existing tables in the database and create new ones.

---

**Note** Dropping existing tables will delete all existing CiscoSecure ACS data. Existing ACS data will not be carried over to new tables.

---

- Enter an available TCP/IP port to be reserved for the CiscoSecure database server process.  
\_\_\_\_\_

The default port is 9900. Unless you know that port 9900 is used by another process, specify the default.

- Enter a unique name for the CiscoSecure DB server process. \_\_\_\_\_

Specify any unique string. The default value is CSdbServer.

- Enter the directory path to use for the AAA server profile caching.  
\_\_\_\_\_

If no directory is specified, the root directory of the system will be used for profile caching.

## E. Install and Start CiscoSecure ACS

- Step 1** Log in as [Root] at the UltraSPARC workstation where you want to install the CiscoSecure ACS.

---

**Note** Remember, if you are using the Oracle Enterprise or Sybase Enterprise product as your database engine, that database product must be installed, configured, and running *before* you start the install procedures described in this section. If you have not already done so, see “Setting Up an Oracle Database for CiscoSecure,” page 17, or “Setting Up a Sybase Enterprise SQL Server for CiscoSecure,” page 19, for details.

---

- Step 2** Insert the CD-ROM labeled “CiscoSecure ACS 2.3 for UNIX” and enter:

```
pkgadd -d /cdrom/csus_23 CSCEacs
```

The installer displays the first of a series of installation prompts:

```
Is this a completely new install Y/N (Default yes, q to quit)?
```

---

**Note** If you install CiscoSecure using a link defined in the root directory pointing to the actual CiscoSecure base directory, a warning message might appear indicating there is not enough space in root to install CiscoSecure. If you know that there is sufficient space in the linked directory to install CiscoSecure, ignore this message and press **Y** at the prompt to continue the CiscoSecure installation.

---

**Step 3** Complete the installation using the preinstallation information that you recorded in step **D. Prepare Your Answers to the Install Questions**. After installation is complete, the system displays:

Installation of CSCEacs was successful.

**Step 4** Start the CiscoSecure ACS. Enter:

```
/etc/rc2.d/S80CiscoSecure
```

## F. If You Licensed and Installed CiscoSecure with DSM, Enable DSM

If you installed the Distribute Session Manager module using the product labeled *CiscoSecure ACS 2.3 for UNIX Distribute Session Manager*, log in to the CiscoSecure Administrator web site and enable the DSM module as follows:

---

**Note** If you did *not* install CiscoSecure ACS with the Distributed Session Manager option, skip this section. Go to “G. What’s Next,” page 12.

---

After starting the CiscoSecure ACS, access the CiscoSecure Administrator web site to perform some initial configuration:

---

**Note** If you do not have access to the CiscoSecure Administrator web site, you can enable the DSM module by carefully editing the CSU.cfg and CSConfig.ini files. See “Editing Configuration Files to Enable or Disable the DSM Module,” page 28.

---

**Step 1** From a Windows 95 or Windows NT workstation, start your Netscape Navigator or Microsoft Internet Explorer web browser and enter the following URL address:

**http://your\_server/cs**

where *your\_server* is the host name (or the fully qualified domain name, FDQN, if host name and FDQN differ) of the UltraSPARC workstation where you installed the CiscoSecure ACS. You can also substitute the UltraSPARC workstation’s IP address for *your\_server*.

---

**Note** If the security socket layer feature on your browser is enabled, specify “https” rather than “http” as the hypertext transmission protocol. Enter: **https://your\_server/cs**

---

**Step 2** When the CiscoSecure Logon window appears, enter the superuser name and password and click **Submit**. The default superuser name and password in a new CiscoSecure ACS installation are:

username: **superuser**  
password: **changeme**

**Step 3** In the CiscoSecure Administrator web site menu bar, click **AAA** and then click **General**.

**Step 4** In the AAA > General web page locate the Max Sessions Enabled field and select the **Distributed** option. This is the option that enables the full set of Distributed Session Manager features on the CiscoSecure ACS.

- Step 5** To effect this setting, you must stop and restart the CiscoSecure ACS.
- Log in as [Root] to the UltraSPARC workstation where you installed CiscoSecure ACS. To stop CiscoSecure ACS enter:  
  
`# /etc/rc0.d/K80CiscoSecure`
  - To restart CiscoSecure ACS, enter:  
  
`# /etc/rc2.d/S80CiscoSecure`
- Step 6** Confirm that Oracle or Sybase database replication is set up and enabled between your CiscoSecure database sites. For details, see the chapter “Setting Up Database Replication Among CiscoSecure ACSes” in the *CiscoSecure ACS 2.3 for UNIX Reference Guide*.
- Step 7** Confirm that AAA accounting functions are enabled on all client NAs. For details, see the chapter “CiscoSecure ACS Accounting” in the *CiscoSecure ACS 2.3 for UNIX User Guide*.

## G. What's Next

The *CiscoSecure ACS 2.3 for UNIX User Guide* and the *CiscoSecure ACS 2.3 for UNIX Reference Guide* provide information about what to do next.

- If you are using CiscoSecure ACS for the first time, go to the *CiscoSecure ACS 2.3 for UNIX User Guide* chapter “Configuring Initial Test Group and User Profiles” for a tutorial on setting up an initial test user profile.
- If you are familiar with earlier versions of CiscoSecure, go to the *CiscoSecure ACS 2.3 for UNIX User Guide* chapter “Introduction to the CiscoSecure Software” for a listing of new CiscoSecure ACS features.
- If you are upgrading from CiscoSecure Version 1.0x, go to the *CiscoSecure ACS 2.3 for UNIX Reference Guide* chapter “Converting an Existing AA Database to a CiscoSecure ACS 2.3 Database.”
- If you have installed and enabled the CiscoSecure DSM module  
OR
- If you want to set up Oracle or Sybase database replication for any other reason:  
  
Assign a DBA-level Oracle or Sybase administrator to set up replication support for CiscoSecure. Database Replication instructions are included in the *CiscoSecure ACS 2.3 for UNIX Reference Guide* chapter “Setting Up Database Replication Among CiscoSecure ACSes.”

For a list of the documentation available, see “Accessing CiscoSecure ACS 2.3 for UNIX Documentation,” page 21.

## Solaris 2.5.1 Patches

UltraSPARC workstations running Solaris 2.5.1 require the following 4 Solaris patches to support CiscoSecure ACS 2.3:

- 103566-08 (or a later version of this patch)
- 103600-21 (or a later version of this patch)
- 106255-01 (or a later version of this patch)
- 101242-13 (or later version of this patch)

These patches or their latest versions can be downloaded from:

<http://sunsolve.sun.com>

README files for each patch are also available at this site.

---

**Note** You will require a SunSpectrum support contract to obtain some or all of the above mentioned patches.

---

You can use the Solaris **showrev -p** command to determine what Solaris patches are already installed on the system.

## Upgrading from CiscoSecure ACS 2.x to 2.3

The product labeled *CiscoSecure ACS Upgrade to v2.3* upgrades previous versions of CiscoSecure 2.x for UNIX to CiscoSecure ACS 2.3 for UNIX *without* the Distributed Session Manager (DSM) module enabled. If you are upgrading from CiscoSecure ACS 2.0, 2.1, 2.1.2, or 2.2.2, complete the following steps:

---

**Note** If you want CiscoSecure ACS 2.3 for UNIX *with* the DSM module installed, *first* follow this procedure to upgrade to 2.3. *Then* use the *CiscoSecure ACS Distributed Session Manager Option* product to license and enable the DSM module. To support DSM make sure that an Oracle or Sybase RDBMS is installed for CiscoSecure prior to running the CiscoSecure upgrade installation program. For details see “Setting Up an Oracle Database for CiscoSecure,” page 17 or “Setting Up a Sybase Enterprise SQL Server for CiscoSecure,” page 19.

---

**Step 1** Before you start the upgrade installation, read the file `$BASEDIR/config/CSU.cfg` and write down the software key value for use during installation.

`$BASEDIR` is the install directory for CiscoSecure that you specified at the time of installation. For example, if you specified “ciscosecure” as the install location, the file is located at `/ciscosecure/config/CSU.cfg`. Below is an example of the line in the CSU.cfg file that contains the software key value:

```
LIST config_license_key = {"a9505ad08a77f927afa4"};
```

**Step 2** Prepare your CiscoSecure ACS 2.x database for upgrade to ACS 2.3 format:

- Back up your CiscoSecure ACS 2.x database.
- Export all the accounting records to an external file by running the AcctExport utility.

If you are upgrading from CiscoSecure 2.0, 2.1, or 2.1.2, the CiscoSecure ACS installation will implement database schema changes for 2.3 compatibility. These schema changes include recreating a profile data table (`cs_profile`) as well as an accounting data table (`cs_accounting_log`).

**Step 3** (Optional) If you want to preserve your old debug level, local time zone, TACACS+ NAS configurations, and supported authentication methods settings for the ACS, save the current `$BASEDIR/config/CSU.cfg` file to a holding directory.

**Step 4** (Optional) If you want to preserve your old unknown\_user default profile settings, save the current `$BASEDIR/config/DefaultProfile` file to a holding directory.

- Step 5** Remove the current version of the CiscoSecure ACS from the UltraSPARC workstation. Log in as [Root] and enter:

```
pkgrm CSCEacs
```

- Step 6** Install CiscoSecure ACS 2.3 for UNIX following the procedures described in the “Basic Installation Procedures,” page 4.

---

**Note** However, skip the section “C. Obtain a CiscoSecure Software License Key.” You do not need to obtain a new software license key to upgrade from a previous version of CiscoSecure ACS 2.x for UNIX to CiscoSecure ACS 2.3 for UNIX.

---

- Step 7** During installation, enter your old software license key (either primary or backup) when prompted by the installer and complete the installation.

---

**Note** If you did not enter the software key value at the time of installation, you can specify it after installation in the CiscoSecure License Key field in the CiscoSecure ACS AAA General web page.

---

---

**Note** Depending on the number of user profiles existing in the CiscoSecure ACS database, the database upgrade phase of CiscoSecure installation could take some time. Approximately 5 minutes of conversion time is required for every 10,000 user profiles.

---

- Step 8** If the CiscoSecure installation procedure fails during the database upgrade phase due to a fixable condition (such as database resources errors), do the following:

- (a) Fix the condition that caused the failure.

---

**Note** If the failed upgrade was for a Sybase Enterprise database from CiscoSecure ACS 2.0 format to CiscoSecure ACS 2.3 format, you must manually update the database schema. See “If CiscoSecure Installation Does Not Update the Sybase Database,” page 20 for details.

---

- (b) Manually complete the database upgrade procedure by changing to the CiscoSecure \$BASEDIR/utlils/bin directory and running the CSdbTool utility. Enter:

```
./CSdbTool upgrade
```

- (c) Remove the CiscoSecure binary files again. Enter: **pkgrm CSCEacs**

- (d) Restart the CiscoSecure installation. Enter: **pkgadd -d /cdrom/csus\_23 CSCEacs**

Even though the database upgrade is now complete, running the installation procedure again ensures that all other necessary installation tasks will be carried out. Because the CiscoSecure ACS database upgrade is already complete, this portion of the installation will now be skipped.

**Step 9** (Optional) After installation, if you saved your old CSU.cfg file as described in step 3, you can cut and paste your old settings from your old CSU.cfg file to the new CSU.cfg file to restore your original ACS debug level, local time zone, TACACS+ NAS configurations, and supported authentication methods settings. See the section “Server Control File” in the chapter “Tuning CiscoSecure ACS Performance and Configuration” in the *CiscoSecure ACS 2.3 for UNIX Reference Guide* for a listing of CSU.cfg settings.

Alternatively, you can simply reenter these settings through the new CiscoSecure ACS AAA General and AAA NAS web pages.



**Caution** Do not copy the old CSU.cfg file over the new CSU.cfg file. The new CSU.cfg file contains important new settings specific to CiscoSecure ACS 2.3 for UNIX.

**Step 10** (Optional) After installation, if you saved your old DefaultProfile file as described in Step 4, you can use the CiscoSecure ACS 2.3 CSImport utility to import your old unknown\_user default profile settings into your new ACS installation. Enter:

```
$BASEDIR/CSimport -c -p /hold_dir -s DefaultProfile
```

where:

*\$BASEDIR* is the directory where you installed CiscoSecure ACS.

*hold\_dir* is the holding directory where you stored the old DefaultProfile file.

---

**Note** After successfully upgrading to CiscoSecure ACS 2.3 for UNIX, you can activate the optional DSM module. Obtain the *CiscoSecure ACS Distributed Session Manager Option* product to license and enable the DSM module. See “Activating the DSM Module on an Existing CiscoSecure ACS 2.3,” page 16 for details.

---

## Upgrading CiscoSecure at Sites with a Non-Updatable Replicated Database

If you are attempting to upgrade from CiscoSecure 2.2.2 or 2.2.3 to 2.3 in an existing replication environment and your environment includes non-updatable sites, when you upgrade the CiscoSecure software on the non-updatable sites, you will receive an error message at the end of the upgrade process stating that the installation failed. This occurs because the CiscoSecure tables that were set up for replication cannot be written to except by the replication process.

The workaround for this problem is to make sure that you have successfully upgraded CiscoSecure on your Master Definition site. Ignore the error message received on the non-updatable site(s). When you replicate, the tables that were not able to be updated will become updated from the Master site by the replication process.

## Activating the DSM Module on an Existing CiscoSecure ACS 2.3

If you are using the product labeled *CiscoSecure ACS Distributed Session Manager Option* (CSU-DSM) to enable the Distributed Session Manager module on an already existing CiscoSecure ACS 2.3 for UNIX installation, you do not need to run the installation program:

- Step 1** Confirm that a Sybase or Oracle RDBMS site has been set up for your CiscoSecure ACSes prior to the last CiscoSecure ACS installation as described in “Setting Up an Oracle Database for CiscoSecure,” page 17 or in “Setting Up a Sybase Enterprise SQL Server for CiscoSecure,” page 19.
- Step 2** If you have not already done so, follow instructions in the document labeled *Requires Immediate Attention (Distributed Session Manager)* to obtain the special 28-character software license keys required to enable the DSM module.
- Step 3** From any workstation with a web connection to the CiscoSecure ACS, open your web browser and log in to the CiscoSecure Administrator web site as superuser.

---

**Note** If you do not have access to the CiscoSecure Administrator web pages, you can manually edit the CiscoSecure CSU.cfg file to specify the new software license key. See “Editing CSU.cfg to Specify a CiscoSecure Software License Key,” page 29.

---

- Step 4** Locate the CiscoSecure License Key field in the AAA General web page, enter the special 28-character software license key, and click **Re-Initialize**.
- Step 5** Locate the Max Sessions Enabled field in the AAA General web page and select the **Distributed** option to enable the Distributed Session Manager features on this ACS.
- Step 6** Stop and restart the CiscoSecure ACS to effect this setting:
- Log in as [Root] to the UltraSPARC workstation where you installed CiscoSecure ACS. To stop the ACS enter:  

```
/etc/rc0.d/K80CiscoSecure
```
  - To restart the CiscoSecure ACS, enter:  

```
/etc/rc2.d/S80CiscoSecure
```
- Step 7** Confirm that Oracle or Sybase database replication is set up and enabled between your CiscoSecure database sites. For details, see the chapter “Setting up Database Replication Among CiscoSecure ACSes” in the *CiscoSecure ACS 2.3 for UNIX Reference Guide*.
- Step 8** Confirm that AAA accounting functions are enabled on all client NASes. For details, see the *CiscoSecure ACS 2.3 for UNIX User Guide* chapter “CiscoSecure ACS Accounting.”

## Setting Up an Oracle Database for CiscoSecure

---

**Note** If you are installing and supporting the per user, per group, and per VPDN session limitation features of the optional CiscoSecure Distributed Session Manager feature, you must configure your Oracle databases for database replication.

---

Oracle software is not bundled with the CiscoSecure ACS. Therefore the CiscoSecure installation does not install or configure the Oracle product, create an Oracle database, or create a database user.

---

**Note** If you intend to set up CiscoSecure with Oracle database replication, Cisco recommends that you read the PDF document *Using CiscoSecure with Oracle's Distributed Database Feature* (filename csbsd.doc.pdf) before you install the Oracle or CiscoSecure software. This document is located in the /CSCEacs/reloc/FastAdmin/docs directory of the CiscoSecure distribution CD-ROM. It provides an easy-to-understand, start-to-finish, screen-by-screen configuration example of setting up Oracle database replication to work with CiscoSecure.

---

## Oracle Setup Requirements Prior to CiscoSecure Installation

If you intend to use an Oracle database with the CiscoSecure ACS, make sure the Oracle database meets the following requirements before starting the CiscoSecure installation:

- Oracle version should be 7.3.2, 7.3.3, 7.3.4 or 8.0.x.

---

**Note** If you intend to support Oracle database replication, you require Oracle version 7.3.3, 7.3.4, or 8.0x installed. In addition, Oracle 7.3.3 and 7.3.4 require the Symmetric Replication Option and Distributed Database Option packages installed to support database replication. Oracle 8 does not require these packages.

---

- The following Oracle products should be installed with the Oracle server (minimum):
  - Oracle 7 or Oracle 8 server
  - SQL\*Net Version 2 and up
  - Oracle TCP/IP protocol adapter
- The following Oracle products should be installed where the CiscoSecure ACS will be installed (minimum):
  - SQL\*Net Version 2 and up—Module on the CiscoSecure server must be from Oracle 7.3.4 or higher
  - Oracle TCP/IP protocol adapter—Module on the CiscoSecure server must be from Oracle 7.3.4 or higher

---

**Note** To upgrade to the above modules from a lower version, run the Oracle installation program, select the upgrade option, and select to upgrade the client versions of these modules.

---

- Make sure the Oracle server and tnslnr processes are loaded and running before installing the CiscoSecure ACS.

- CiscoSecure ACS requires an Oracle user database account setup prior to the CiscoSecure installation:
  - This user account must have a privilege to create/drop tables. (Connect and Resource privilege).
  - This user account should also have Select privilege on two of Oracle's system views: sys.dba\_free\_space and sys.dba\_users.
  - The Oracle tablespace where the account belongs should have at least 200 MB of data space, 100 MB of rollback tablespace, and 50 MB of temporary tablespace available.

## Oracle Information Required During CiscoSecure Installation

CiscoSecure ACS installation prompts require the following information concerning your Oracle installation:

- TNS name—Name for the Oracle server. It should be defined in Oracle's tnsnames.ora file.
- Oracle user—Database account (not Solaris account) which has Resource privilege.
- Oracle user's password.
- Oracle home—Absolute pathname of the directory where the Oracle product is installed. This should be the same as the ORACLE\_HOME environment variable that is defined when Oracle is installed. Do not confuse this directory with the home directory of the Solaris user account for Oracle, such as /home/oracle.
- Connections—Specifies how many connections CiscoSecure ACS can make to the Oracle server. CiscoSecure ACS will make that number of connections when it starts up.

## Oracle Database Replication Setup Following CiscoSecure Installation

If you want to set up database replication among multiple CiscoSecure ACS sites, assign your Oracle database administrator (DBA) to do so after CiscoSecure installation is complete. See the *CiscoSecure ACS 2.3 for UNIX Reference Guide* chapter "Setting up Database Replication among CiscoSecure ACSes" for details.



**Caution** Database replication setup requires database administrator (DBA) expertise. If you do not possess DBA experience, assign this task to someone who does.

---

**Note** If you are installing and supporting the per user, per group, and per VPDN session limitation features of the optional *CiscoSecure Distributed Session Manager* feature, you must configure your Oracle databases for database replication.

---

---

**Note** If you intend to set up CiscoSecure with Oracle database replication, Cisco recommends that you read the PDF document *Using CiscoSecure with Oracle's Distributed Database Feature* (filename csbsd.doc.pdf) before you install the Oracle or CiscoSecure software. This document is located in the /CSCEacs/reloc/FastAdmin/docs directory of the CiscoSecure distribution CD-ROM. It provides an easy-to-understand, start-to-finish, screen-by-screen configuration example of setting up Oracle database replication to work with CiscoSecure.

---

## Troubleshooting if the CiscoSecure Installation Fails to Access your Oracle Database

Check the following items on the Oracle database:

- SQL\*Net connectivity:
  - Check if SQL\*Net and TCP/IP protocol adapter are installed on the system where the CiscoSecure ACS is being installed.
  - Using Oracle's tools such as SQL\*Plus or tnsping, check if you can connect to the Oracle server using the TNS name, the database username, and the password.

---

**Note** See Oracle's *Network Products Troubleshooting Guide* for help in determining the SQL\*Net configuration problems.

---

- Check if Oracle's shared library exists.

`$ORACLE_HOME/lib/libclntsh.so.1.0`

If the shared library does not exist, then this points to an Oracle installation problem. The library is installed as part of SQL\*Net.

## Setting Up a Sybase Enterprise SQL Server for CiscoSecure

If you intend to use a Sybase Enterprise database with the CiscoSecure ACS, make sure the Sybase Enterprise SQL server meets the following requirements.

### Sybase Setup Requirements Prior to CiscoSecure Installation

Before you install CiscoSecure:

- SQL server should be version 11.0.2 or higher. The SQL server could be on a local or a remote system. At the time of the CiscoSecure ACS installation, the SQL server should be running.
- Sybase Open Client/C of version 11.1 or higher should be installed and configured on the system where the CiscoSecure ACS is installed. This includes proper configuration of the `$SYBASE/interfaces` file.
- Prior to the CiscoSecure installation, set up an SQL server login account that CiscoSecure can use to connect to the SQL server.
- In addition, we recommend that the customer create a separate database for the CiscoSecure ACS and create a database login account as the owner of the database. The size of the database depends on the user/group profiles and accounting data expected.

## Sybase Information Required During CiscoSecure Installation

CiscoSecure installation will prompt for the following information related to Sybase:

- Sybase install directory
- SQL server name—Name of SQL server defined in the `$SYBASE/interfaces` file
- Database user account and password
- Database to use with the CiscoSecure ACS
- Number of database connections that the CiscoSecure ACS can use.

## Sybase Database Replication Setup Following CiscoSecure Installation

If you want to set up database replication among multiple CiscoSecure ACS sites, assign your Sybase database administrator (DBA) to do so after CiscoSecure installation is complete. See the *CiscoSecure ACS 2.3 for UNIX Reference Guide* chapter “Setting up Database Replication among CiscoSecure ACSes.” for details.



**Caution** Database replication setup requires database administrator (DBA) expertise. If you do not possess DBA experience, assign this task to someone who does.

---

**Note** If you are installing and supporting the per user, per group, and per VPDN session limitation features of the *CiscoSecure ACS 2.3 for UNIX with DSM* package, you *must* configure your Sybase databases for database replication.

---

## If CiscoSecure Installation Does Not Update the Sybase Database

The CiscoSecure installation might fail to update the Sybase Enterprise database for early CiscoSecure for UNIX 2.x versions. In such cases, the installation program will stop after the following series of prompts and messages:

```
alter table cs_password add primary key (profile_id, pwd_type)
*** SQLException caught ***
SQLState:
Message: Line 1 Error 1920 Level 16 State 1
 A column in a primary key constraint's
 column list is not constrained to be not null,
 column name: 'profile_id'.
Vendor: 1920
Upgrading schema failed.
```

In such cases, you must use Sybase tools to manually update the Sybase database schema, then rerun the part of the CiscoSecure installation program that updates the CiscoSecure database schema.

- Step 1** Start the Sybase SQL command tool, isql, and enter the following series of commands to update the database schema:

```
create table cs_password_new
(
 profile_id int not null,
 pwd_type varchar(32) not null,
 pwd_value varchar(255) null ,
 pwd_from_date datetime null ,
 pwd_until_date datetime null ,
 pwd_opaque varchar(255) null ,
 pwd_qualifier varchar(10) null ,
)
go

insert into cs_password_new (profile_id, pwd_type, pwd_value,
 pwd_from_date, pwd_until_date, pwd_opaque, pwd_qualifier)
select profile_id, pwd_type, pwd_value, pwd_from_date, pwd_until_date,
 pwd_opaque, pwd_qualifier from cs_password
go

drop table cs_password
go

sp_rename cs_password_new, cs_password
go
```

- Step 2** Run the `$BASEDIR/utls/bin CSdbTool` utility to continue the CiscoSecure database upgrade. Enter:

```
CSdbTool upgrade
```

## Accessing CiscoSecure ACS 2.3 for UNIX Documentation

After you install the CiscoSecure ACS 2.3 for UNIX software, the following documentation is available to you in several formats and several locations:

- Printed documents with the CiscoSecure ACS 2.3 for UNIX product package include:
  - *CiscoSecure ACS 2.3 for UNIX User Guide*
  - *CiscoSecure ACS 2.3 for UNIX Reference Guide*
  - *CiscoSecure ACS 2.3 for UNIX Release Notes*
  - *CiscoSecure ACS 2.3 for UNIX Installation Guide*
- HTML documents at your installed CiscoSecure ACS Administrator web pages include:
  - *CiscoSecure ACS 2.3 for UNIX User Guide*
  - *CiscoSecure ACS 2.3 for UNIX Reference Guide*
  - *Frequently Asked Questions*—A compilation of answers to frequently asked questions about CiscoSecure ACS features
  - *Profile Syntax Guide*—A reference outline of CiscoSecure profile syntax and some common profile examples

**To access**—While running the CiscoSecure Administrator web pages, click **Help**.

If you are *not* running the CiscoSecure ACS Administrator web pages, you can access the *CiscoSecure ACS 2.3 for UNIX User Guide* and *CiscoSecure ACS 2.3 for UNIX Reference Guide* directly at:

**`http://acs_server:9090/docs/csuxug23/index.htm`**

or

**`http://acs_server:9090/docs/csuxrf23/index.htm`**

where *acs\_srvr* is the host name (or the FQDN, if it is different from the host name) of the server where you installed the CiscoSecure ACS. You can also substitute the server's IP address.

- Online help includes descriptions of individual fields in the CiscoSecure ACS Administrator web-based interface.

**To access**—While running the CiscoSecure ACS Administrator web pages, you can access HTML help for an individual field by clicking on that field name.

- HTML documents at the Cisco corporate web site. The documents relevant to CiscoSecure ACS 2.3 for UNIX include:
  - *CiscoSecure ACS 2.3 for UNIX User Guide*
  - *CiscoSecure ACS 2.3 for UNIX Reference Guide*
  - *CiscoSecure ACS 2.3 for UNIX Release Notes*
  - *CiscoSecure ACS 2.3 for UNIX Installation Guide* (this publication)

---

**Note** The documents at this site are likely to be the most recently updated documents available for the CiscoSecure ACS product.

---

**To access**—Use your web browser to view the documents at:

**`http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft`**

- PDF documents at the installed CiscoSecure ACS Administrator web pages include:
  - *CiscoSecure ACS 2.3 for UNIX User Guide*
  - *CiscoSecure ACS 2.3 for UNIX Reference Guide*

These documents are readable with the Adobe Acrobat Reader, with full search capabilities and hypertexted table of contents and index. They are printable with full hard copy formatting and available on your installed CiscoSecure ACS.

**To access**—While running the CiscoSecure ACS Administrator web pages, click **Help**, click **User Guide**, or **Reference Guide** and then click the **PDF** icon on the Contents page of the *CiscoSecure ACS 2.3 for UNIX User Guide* or *CiscoSecure ACS 2.3 for UNIX Reference Guide*. You need Adobe Acrobat Reader installed on your system. Free copies of the Acrobat Reader can be downloaded from the Adobe web site:

**`http://www.adobe.com`**

## Installing without a CD-ROM

If you do *not* have a CD-ROM drive attached to the UltraSPARC workstation where you want to install CiscoSecure ACS, download the installation software from the Cisco web site and run the installation program as follows:

---

**Note** To take the steps described in this section, you must have a valid SmartNet account. If you do not have a SmartNet account, contact your authorized Cisco Systems support representative for instructions.

---

- Step 1** Make sure the UltraSPARC workstation where you want to install the CiscoSecure ACS has at least 150 MB of available disk space to accommodate the CiscoSecure installation download package.
- Step 2** Go to the CiscoSecure Software Planner URL:  
`http://www.in.cisco.com/cmc/cc/cisco/mkt/access/secure/`  
 You are prompted for a username and password in order to access Cisco Connection Online (CCO).
- Step 3** Using your SmartNet account, log in to CCO, specifying your username and password as prompted.
- Step 4** Click **Download CiscoSecure Software**. The CiscoSecure Server Software Images page appears.
- Step 5** Click the button beside the applicable version of CiscoSecure Solaris. If you agree to the terms of the software agreement, click **Execute**. You are prompted to specify the location from which to transfer the software image.
- Step 6** Click the location of the CCO server that is closest to your target CiscoSecure server. You are prompted again for your CCO password.
- Step 7** Enter your CCO password. A file is copied to your home directory.
- Step 8** Uncompress the CiscoSecure ACS software package by entering the following command at the UNIX prompt:  
`uncompress CiscoSecure-2.3.x.x.solaris.PKG.Z`
- Step 9** Translate the package file by entering the following command at the UNIX prompt:  
`pkgtrans CiscoSecure-2.3.x.x.solaris.PKG /tmp`  
 The following output displays:  

```
The following packages are available:
1 CiscoSecure-2.3.x.x CiscoSecure Access Control Software
 (sun4) x.x
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```
- Step 10** Enter **1**.  
 The download operation is now complete.

- Step 11** Obtain your server license key and answer the preinstallation questions according to the instructions in the section “Basic Installation Procedures,” page 4.

---

**Note** Do not enter the “pkgadd -d/cdrom/csus\_23 CSCEacs” string to start the installation program.

---

- Step 12** To start the installation program enter:

```
pkgadd -d /tmp CSCEacs
```

## Manually Enabling Profile Cache Updating

Profile cache updating must be enabled for CiscoSecure ACS servers whose CiscoSecure profile databases are modified directly by Oracle or Sybase database replication implementations or by third-party applications.

In the case of Oracle or Sybase database replication, you enable profile cache updating in the process of implementing the replication.

If you are using third-party applications that directly modify the CiscoSecure ACS profile data, use the following procedure to enable profile cache updating following the normal CiscoSecure installation.

---

**Note** For profile cache updating to work, the database user account used by the third-party application must be *different* from the user account that you specified when you originally installed and configured the Oracle or Sybase engines for CiscoSecure ACS.

---

- Step 1** After completing the CiscoSecure ACS installation on your UNIX host, change to the CiscoSecure \$BASEDIR/utlils/bin directory and run the CSdbTool utility. Enter:

```
./CSdbTool cache_trigger
```

This installs triggers in the CiscoSecure ACS database tables that insert the changes in a special log table, cs\_trans\_log, whenever a third-party program alters any profile data. These changes are periodically incorporated into the profile cache.

- Step 2** In the CSConfig.ini file, make sure the following parameters are set:

```
[ProfileCaching]
EnableProfileCaching = ON
;polling period in minutes for cs_trans_log table
DBPollinterval = number_of_minutes
```

where *number\_of\_minutes* is the time in minutes that the customer wants between profile cache updates. This interval should match the intervals at which database replication or third-party applications directly modify the ACS profile data. For example, if database replication is configured to take place every 15 minutes, then the *number\_of\_minutes* for DBPollinterval should also be set to 15.

The default value is 30 minutes.

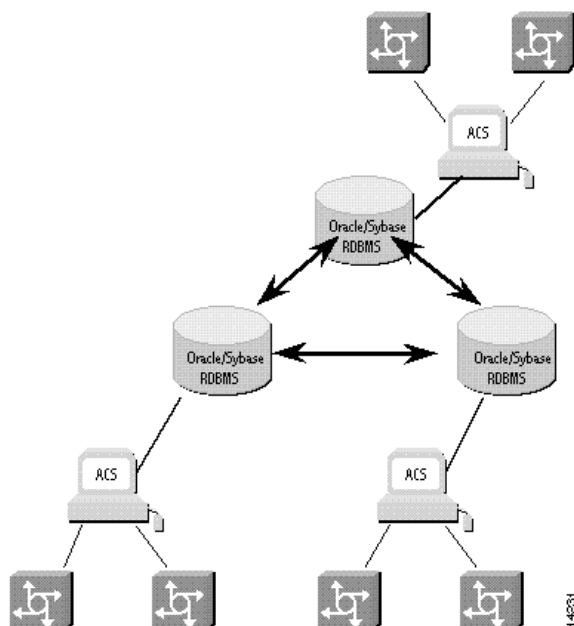


| Node                            | Description                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CiscoSecure workstation console | The CiscoSecure workstation console provides web-based pages through which the CiscoSecure profile database can be administered by the CiscoSecure system administrator or group administrator.                                                   |
| Token server                    | An optional third-party server for executing authentication of token card users entering one-time passwords (OTPs). The CiscoSecure ACS can be configured to forward login requests from token card users for authentication by the token server. |

## Multiple CiscoSecure ACS Installation

Networks that provide access at multiple locations or support large numbers of users (for example, nationwide ISP networks that provide local dial-in login across the nation) are best supported by multiple ACSes with an RDBMS configured to replicate changes to any local CiscoSecure profile database to all other CiscoSecure profile database sites in the network.

**Figure 2 Multiple ACSes and Replicated Profile Databases**



In order to support database replication among your ACSes you need to purchase and preinstall Oracle Enterprise or Sybase Enterprise RDBMS software at each ACS database site where you want replication of the CiscoSecure profile database to be carried out.

The per user, per group, or per VPDN maximum session limit feature of the *CiscoSecure ACS 2.3 for UNIX with DSM* package requires you to configure profile database replication.

## Distributed Session Manager Features

With the CiscoSecure ACS 2.3 for UNIX product, you can purchase a special software license key to enable the Distributed Session Manager (DSM). When installed and enabled, the DSM feature allows access to special DSM-specific web pages that enable the CiscoSecure system administrator

to limit and enforce, on a very fine-grained basis, the number of concurrent sessions allowed per user, per group, or per VPDN either on a network-wide basis, or through a particular “point-of-presence” group of NASes.

---

**Note** If you do *not* purchase the DSM-enabling software license key, you can *still* limit the number of concurrent sessions on a *per user* basis. See the *CiscoSecure ACS 2.3 for UNIX User Guide* chapter “Limiting and Tracking Sessions Per User, Group, or VPDN” for descriptions of maximum session limits supported by the DSM-enabled and the non-DSM-enabled CiscoSecure ACS 2.3 for UNIX packages.

---

## Summary of DSM Installation and Post-Installation Requirements

Before you attempt to configure DSM max sessions control, make sure that you have implemented the following CiscoSecure installation and post-installation requirements:

- You need to have preinstalled Oracle Enterprise version 7.3.3, 7.3.4 or 8.0.x or Sybase Enterprise version 11.0.2 or higher as the RDBMS for the CiscoSecure ACS profiles. For details see “Setting Up an Oracle Database for CiscoSecure,” page 17 or “Setting Up a Sybase Enterprise SQL Server for CiscoSecure,” page 19.
- You need to have enabled the DSM module using the appropriate product:
  - If you were installing CiscoSecure ACS for the first time, you need to have installed the package titled *CiscoSecure ACS 2.3 for UNIX Distributed Session Manager*. See “Basic Installation Procedures,” page 4.
  - If you wanted to upgrade a previous version of CiscoSecure ACS 2.x for UNIX to support the DSM module, you needed to first upgrade to CiscoSecure ACS 2.3 for UNIX. Then you could use the *CiscoSecure ACS Distributed Manager Option* product to activate the DSM module. See “Upgrading from CiscoSecure ACS 2.x to 2.3,” page 13.
  - If you wanted to activate the DSM module at an existing CiscoSecure ACS 2.3 for UNIX site without a licensed DSM module, you needed to use the package titled *CiscoSecure ACS Distributed Session Manager Option*. See “Activating the DSM Module on an Existing CiscoSecure ACS 2.3,” page 16.
- After installation or upgrade, you needed to log in to the CiscoSecure Administrator web site located the Max Sessions Enabled field in the AAA General web page, select **Distributed** to activate the DSM module, and restart the CiscoSecure ACS server.
- You needed to confirm that the AAA accounting functions are enabled on the client NASes. See the *CiscoSecure ACS 2.3 for UNIX User Guide* chapter “CiscoSecure ACS Accounting.”
- If your network is serviced by more than one CiscoSecure ACS installation, database replication must be configured and enabled between the CiscoSecure profile RDBMS sites. See the chapter “Setting up Database Replication among CiscoSecure ACSes” in the *CiscoSecure ACS 2.3 for UNIX Reference Guide*.



**Caution** Database replication setup requires database administrator (DBA) expertise. If you do not possess DBA experience, assign this task to someone who does.

## Editing Configuration Files to Enable or Disable the DSM Module

We strongly recommend using the Max Sessions Enabled field in the CiscoSecure Administrator AAA General web page to enable or disable the Distributed Session Manager or other supported types of max sessions control.

Alternatively, if you do not have access to a web browser, you can enable or disable max sessions control by editing the CSU.cfg and CSConfig.ini configuration files.

**Step 1** In the \$BASEDIR/config directory of your ACS server, edit your CSU.cfg and CSConfig.ini files as specified in the table below to enable the DSM or other supported types of max sessions control.



**Caution** If you edit the CSU.cfg and CSConfig.ini files, make sure that when you *enable* one type of max sessions control that you also *disable* all other types of max sessions control. Enabling the settings for one type of max sessions control in the table below *without* disabling the settings for the other types of max sessions control can cause extremely slow authentication performance and out-of-memory errors.

| Enabling this Type of Max Sessions:                   | Requires These CSU.cfg Settings:                                                                                                                                                                                              | And Requires These CSConfig.ini Settings:                                                                                                                                                                               |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None (all max sessions control disabled)              | <ul style="list-style-type: none"> <li>config_maxsessions_enable= <b>0</b></li> <li>config_distmaxsessions_enable=<b>0</b></li> </ul> <p>These settings disable AAA server and DSM max sessions control.</p>                  | <ul style="list-style-type: none"> <li>ProcessInMemoryMaxSessionInfo = <b>disable</b></li> <li>ArchiveMaxSessionInfoToDB = <b>disable</b></li> </ul> <p>These settings disable DBServer-based max sessions control.</p> |
| Distributed Session <sup>1</sup> Manager (DSM)        | <ul style="list-style-type: none"> <li>config_maxsessions_enable= <b>0</b></li> <li>config_distmaxsessions_enable=<b>1</b></li> </ul> <p>These settings disable AAA server-based max sessions control and enable the DSM.</p> | <ul style="list-style-type: none"> <li>ProcessInMemoryMaxSessionInfo = <b>disable</b></li> <li>ArchiveMaxSessionInfoToDB = <b>disable</b></li> </ul> <p>These settings disable DBServer-based max sessions control</p>  |
| DBServer-based Max Sessions control (default setting) | <ul style="list-style-type: none"> <li>config_maxsessions_enable= <b>0</b></li> <li>config_distmaxsessions_enable=<b>0</b></li> </ul> <p>These settings disable AAA server-based max sessions control and the DSM.</p>        | <ul style="list-style-type: none"> <li>ProcessInMemoryMaxSessionInfo = <b>enable</b></li> <li>ArchiveMaxSessionInfoToDB = <b>enable</b></li> </ul> <p>These settings enable DBServer-based max sessions control</p>     |
| AAA Server-based Max Sessions control                 | <ul style="list-style-type: none"> <li>config_maxsessions_enable= <b>1</b></li> <li>config_distmaxsessions_enable=<b>0</b></li> </ul> <p>These settings enable AAA server-based max sessions control and disable the DSM.</p> | <ul style="list-style-type: none"> <li>ProcessInMemoryMaxSessionInfo = <b>disable</b></li> <li>ArchiveMaxSessionInfoToDB = <b>disable</b></li> </ul> <p>These settings disable DBServer-based max sessions control</p>  |

1.DSM-based session control can only take effect if the optional Distributed Session Manager module has been licensed for this installation of CiscoSecure ACS 2.3 for UNIX.

**Step 2** After making the above settings, stop and restart CiscoSecure ACS to make sure that all the above settings take effect:

- Log in as [Root] to the UltraSPARC workstation where you installed CiscoSecure ACS. To stop CiscoSecure ACS, enter:

```
/etc/rc0.d/K80CiscoSecure
```

- To restart CiscoSecure ACS, enter:

```
/etc/rc2.d/S80CiscoSecure
```

---

**Note** All forms of max sessions control require that the AAA accounting functions be enabled in the client NASes.

---

## Editing CSU.cfg to Specify a CiscoSecure Software License Key

If you want to specify a software license key after installing CiscoSecure ACS, or if you want to modify the software license key for an existing CiscoSecure ACS 2.3 UNIX installation because you have obtained a new key to enable the optional Distributed Session Manager module, you can use the CiscoSecure License Key field in the CiscoSecure Administrator AAA General web page.

Alternatively, you can manually edit the config\_license\_key variable in the CSU.cfg file:

**Step 1** Open the file `$BASEDIR/config/CSU.cfg`.

`$BASEDIR` is the install directory for CiscoSecure that you specified at the time of installation. If you used the default install location, the file is located at `/ciscosecure/config/CSU.cfg`.

**Step 2** Find the config\_license\_key variable and enter or modify the value for software license key number. For example:

```
LIST config_license_key = {"a9505ad08a77f927afa4"};
```

**Step 3** After changing the software license key, stop and restart CiscoSecure ACS for your changes to the CSU.cfg file to take effect.

- Log in as [Root] to the UltraSPARC workstation where you installed CiscoSecure ACS. To stop CiscoSecure ACS, enter:

```
/etc/rc0.d/K80CiscoSecure
```

- To restart CiscoSecure ACS, enter:

```
/etc/rc2.d/S80CiscoSecure
```

## Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: [cco.cisco.com](http://cco.cisco.com)
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact [cco-help@cisco.com](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto:cco-team@cisco.com).

---

**Note** If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or [tac@cisco.com](mailto:tac@cisco.com). To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or [cs-rep@cisco.com](mailto:cs-rep@cisco.com).

---

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar, select **Documentation**, and click **Enter the feedback form**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments

---

This document is to be used in conjunction with the *CiscoSecure ACS 2.3 for UNIX User Guide* publication.

AccessPath, Any to Any, AtmDirector, the CCIE logo, CD-PAC, Centri, the Cisco Capital logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, the Cisco Press logo, the Cisco Technologies logo, ClickStart, ControlStream, DAGAZ, Fast Step, FireRunner, IGX, IOS, JumpStart, Kernel Proxy, LoopRunner, MGX, Natural Network Viewer, NetRanger, NetSonar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RouteStream, Secure Script, SMARTnet, SpeedRunner, Stratm, StreamView, *The Cell*, TrafficDirector, TransPath, VirtualStream, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, Enterprise/Solver, EtherChannel, FastHub, ForeSight, FragmentFree, IP/TV, IPX, LightStream, MICA, Phase/IP, StrataSphere, StrataView Plus, and SwitchProbe are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. (9810R)

Copyright © 1998, Cisco Systems, Inc.  
All rights reserved.

