CHAPTER 13

Troubleshooting Cisco Secure ACS on Windows

Cisco Secure Access Control Server, which is known as CS ACS, fills the server-side requirement of the Authentication, Authorization, and Accounting (AAA) client server equation. For many security administrators, the robust and powerful AAA engine, along with CS ACS's ability to flexibly integrate with a number of external user databases, makes the CS ACS software the first and sometimes only choice for an AAA server-side solution. This chapter explores CS ACS in detail and walks you through troubleshooting steps. The chapter focuses on the approach required to troubleshoot any issue efficiently, either with the CS ACS software itself or with the whole AAA process.

Overview of CS ACS

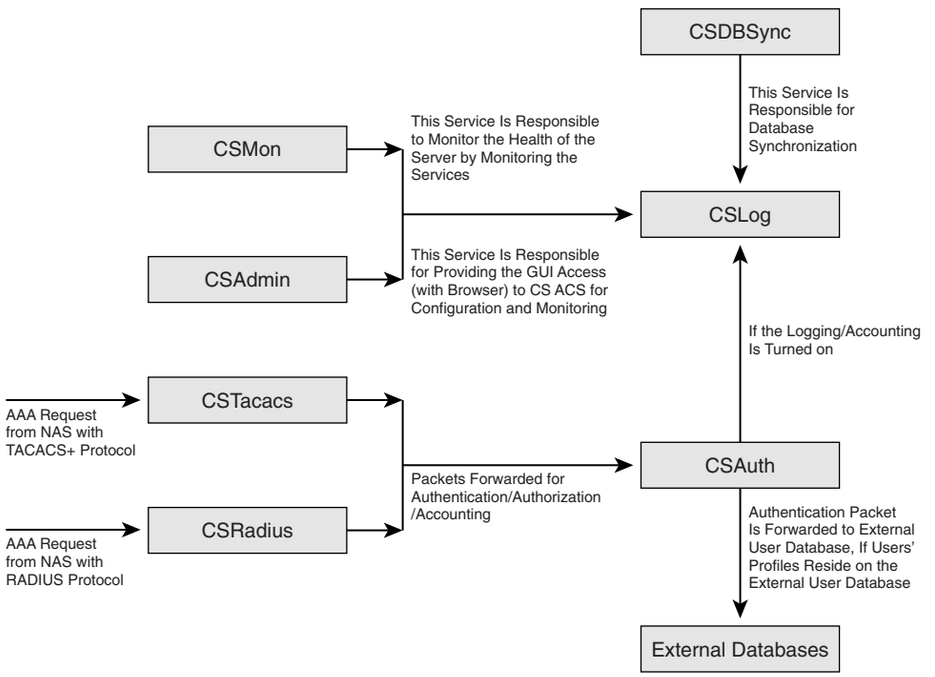
Before delving into the details of how an AAA request from a network access server (NAS) is processed by CS ACS, you need a good understanding of all the components that bring the Cisco Secure ACS into existence.

CS ACS Architecture

As shown in Figure 13-1, Cisco Secure ACS comprises a number of services.

- **CSAdmin**—This service provides the Web interface for administration of Cisco Secure ACS. Although it is possible, and sometimes desirable, to use the Command Line Interface (CLI) for CS ACS configuration, the Graphical User Interface (GUI) is a must because certain attributes may not be configured via CLI. In addition, with the GUI, the administrator has little or no chance to insert bad data, which could lead to database corruption, because the GUI has a sanity check mechanism for user data insertion. The web server used by CS ACS is Cisco proprietary and uses TCP/2002 rather than the standard port 80. Therefore, another web server may be running on the CS ACS server, but this is not recommended because of the security risk and other possible interference.

Figure 13-1 *Diagram of the Relationship Among Cisco Secure ACS Services*



Because CSAdmin service is coded as multi-threaded, it is possible to open multiple sessions from different locations to the CS ACS Server for configuration purposes, but CS ACS does not allow making the same profile or attribute changes by multiple administrators at the same time. For instance, group 200 may not be modified by two administrators at the same time. You need to create an admin account to allow remote access to CS ACS from another machine; you do not need the admin account, however, if you access it from the CS ACS server itself. To bring up the CS ACS GUI from a host other than CS ACS, point to the following location:

```
http://<ip_address_of_CS ACS_server>:2002
```

All the services except CSAdmin can be stopped and restarted from the GUI (**System > Service Control>Stop/Restart**). CSAdmin can be controlled via a Windows Services applet, which can be opened by browsing to **Start > Programs > Administrative Tools > Services applet**.

- **CSAuth**—CSAuth is the heart of CS ACS server, which processes the authentication and authorization requests from the NAS. It also manages the Cisco Secure CS ACS database.
- **CSDBSync**—CSDBSync is the database synchronization service, which allows the CS ACS database to be in sync with third-party relational database management system (RDBMS) systems. This feature is very useful when an organization has multiple data feed locations.

- **CSLog**—This is a logging service for audit-trailing, accounting of authentication, and authorization packets. CSLog collects data from the CSTacacs or CSRadius packet and CSAuth, and then scrubs the data so that data can be stored into comma-separated value (CSV) files or forwarded to an Open DataBase Connectivity (ODBC)-compliant database.
- **CSMon**—CSMon service is responsible for the monitoring, recording, and notification of Cisco Secure CS ACS performance, and includes automatic response to some scenarios. For instance, if either Terminal Access Controller Access Control System (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) service dies, CS ACS by default restarts all the services, unless otherwise configured. Monitoring includes monitoring the overall status of Cisco Secure ACS and the system on which it is running. CSMon actively monitors three basic sets of system parameters:
  - **Generic host system state**—monitors disk space, processor utilization, and memory utilization.
  - **Application-specific performance**—periodically performs a test login each minute using a special built-in test account by default.
  - **System resource consumption by Cisco Secure ACS**—CSMon periodically monitors and records the usage by Cisco Secure ACS of a small set of key system resources. Handles counts, memory utilization, processor utilization, thread used, and failed log-on attempts, and compares these to predetermined thresholds for indications of atypical behavior.

  CSMon works with CSAuth to keep track of user accounts that are disabled for exceeding their failed attempts count maximum. If configured, CSMon provides immediate warning of brute force attacks by alerting the administrator that a large number of accounts have been disabled.

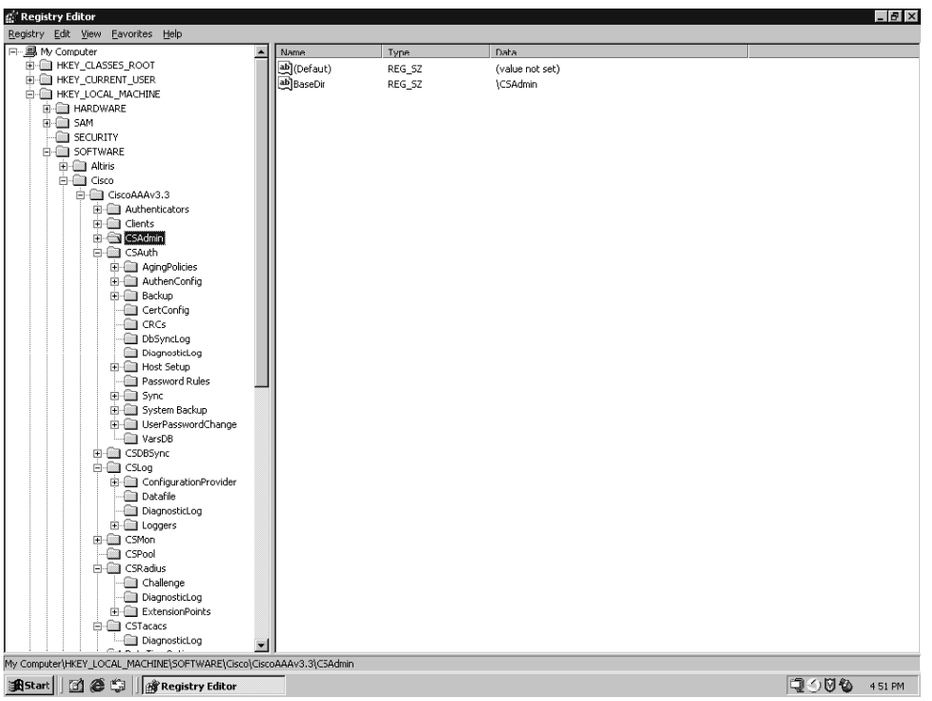
  By default CSMon records exception events in logs both in the CSV file and Windows Event Log that you can use to diagnose problems. Optionally you can configure event notification via e-mail so that notification for exception events and outcomes includes the current state of Cisco Secure ACS at the time of the message transmission. The default notification method is simple mail-transfer protocol (SMTP) e-mail, but you can create scripts to enable other methods. However, if the event is a failure, CSMon takes the actions that are hard-coded when the triggering event is detected. Running the CSSupport utility, which captures most of the parameters dealing with the state of the system at the time of the event, is one such example. If the event is a warning event, it is logged, the administrator is notified if it is configured, and no further action is taken. After a sequence of re-tries, CSMon also attempts to fix the cause of the failure and individual service restarts. It is possible to integrate custom-defined action with CSMon service, so that a user-defined action can be taken based on specific events.

- **CSTacacs**—The CSTacacs service is the communication bridge between the NAS and the CSAuth service. This service listens on TCP/49 for any connection from NAS. For security reasons, the NAS identity (IP) must be defined as an AAA client with a shared secret key, so that CS ACS accepts only a valid NAS.
- **CSRadius**—CSRadius service serves the same purpose as CSTacacs service, except that it serves the RADIUS protocol. CSRadius service listens on UDP/1645 and UDP/1812 for authentication and authorization packets. For accounting, it listens on both UDP/1646 and UDP/1813 so that NAS can communicate on either port. However, it is recommended to use UDP/1812 and 1813 because UDP/1645 and 1646 are standard ports for other applications.

The Cisco Secure ACS information is located in the following Windows Registry key as shown in Figure 13-2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\CISCO
```

Figure 13-2 *Cisco Secure ACS Registries Location*



You can get to the screen shown in Figure 13-2 by browsing **Start>Run>Type** and entering "regedit" in the text box. Do not make any changes to Windows Registry settings related to CS ACS unless advised by a Cisco representative, as you may inadvertently corrupt your application. This chapter explains where the Registry entry should be added or modified.

The Life of an AAA Packet in CS ACS

This section builds on the knowledge that you have gained from the preceding section, to examine the life of an AAA packet within CS ACS when it hits the CS ACS server. When the packet reaches the CS ACS, the following events occur:

1. NAS interacts with CS ACS Server using CSTacacs or CSRadius Services. So, CSTacacs or CSRadius service receives the packet from the NAS.
2. Then NAS checking is performed with the IP address and shared secret and if successful, then CSTacacs or CSRadius performs the Network Access Restrictions (NAR) checking. If CSTacacs or CSRadius decides that it is a valid packet and passes the NAR test, the packet goes to the CSAuth Service.
3. The CSAuth checks the Proxy Distribution table and finds out if there is any matching string for the username in the Character String Column of the Proxy Distribution Table. If there is a match, and AAA proxy information is defined, then the authentication request is forwarded to the appropriate AAA server, and CS ACS at this stage acts as a middle man for AAA services. However, if there is no matching string found, ACS Local database performs the AAA services as described in the next step.
4. The CSAuth service looks up the user's information in its own internal database and if the user exists, it either allows or denies access based on password and other parameters. This status information, and any authorization parameters, are sent to the CSTacacs or CSRadius service, which then forwards the status information to the NAS.
5. If the user does not exist in the CS ACS local database, CS ACS marks that user as unknown and checks for an unknown user policy. If the unknown user policy is to fail the user, CS ACS fails the user. Otherwise, if external database is configured, CS ACS forwards that information to the configured external user database. Cisco Secure CS ACS tries each external user database until the user succeeds or fails.
6. If the authentication is successful, the user information goes into the cache of CS ACS, which has a pointer for using the external user database. This user is known as a dynamic user.
7. The next time the dynamic user tries to authenticate, Cisco Secure ACS authenticates the user against the database that was successful the first time. These cached user entries are used to speed up the authentication process. Dynamic users are treated in the same way as known users.
8. If the unknown user fails authentication with all configured external databases, the user is not added to the Cisco Secure user database and the authentication fails.
9. When a user is authenticated, Cisco Secure ACS obtains a set of authorizations from the user profile and the group to which the user is assigned. This information is stored with the username in the Cisco Secure user database. Some of the authorizations included are the services to which the user is entitled, such as IP over Point-to-Point Protocol (PPP), IP pools from which to draw an IP address, access lists, and password-aging information.

10 The authorizations, with the approval of authentication, are then passed to the CSTacacs or CSRadius modules to be forwarded to the requesting device.

11 If configured on the NAS, accounting starts right after the successful user authentication. Accounting can be configured for authorization as well. A **START** record from NAS is sent which follows the same paths as authentication requests on CS ACS with the addition of **CSLog** service involvement. For instance, if the radius protocol is used, packets go through **CSRadius** service first, then **CSAuth**. **CSAuth** then forwards the packet to the **CSLog** service. **CSLog** service decides if the accounting requests should be forwarded to another AAA server based on the Proxy Distribution Table, or should be processed locally. Additionally, if ODBC logging is configured for accounting, the packet is forwarded to the ODBC database. The same path is followed for the **STOP** record from the NAS, which completes the accounting record for a specific session.

CS ACS can integrate with a number of external user databases. Table 13-1 shows the components that are needed to integrate with those external user databases.

Table 13-1 *Components Needed to Integrate with External Databases*

External Database	What CS ACS Uses to Communicate to the External Database
NT/2K & Generic LDAP	CS ACS and OS contain all the files needed. No extra files required.
Novell Netware Directory Service (NDS)	NDS client.
ODBC	Windows ODBC and third party ODBC driver.
Token Server	Client software provided by vendor.
Radius Token Server	Use RADIUS interface.

CS ACS can be integrated with many external user databases; however, not every database supports every authentication protocol. Table 13-2 shows the protocols supported for specific databases.

Table 13-2 *Protocols Supported on Various Databases*

	ASCII	PAP	CHAP	ARAP	MS CHAP v.1	MS CHAP v.2	LEAP	EAP-MD5	EAP-TLS
CS ACS Local Database	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	Yes	No	No	Yes	Yes	Yes	No	No
Windows AD	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes
Novell NDS	Yes	Yes	No	No	No	No	No	No	No
LDAP	Yes	Yes	No	No	No	No	No	No	Yes

Table 13-2 *Protocols Supported on Various Databases (Continued)*

	ASCII	PAP	CHAP	ARAP	MS CHAP v.1	MS CHAP v.2	LEAP	EAP-MD5	EAP-TLS
ODBC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
LEAP Proxy RADIUS	No	No	No	No	Yes	No	Yes	No	No
Active Card	Yes	Yes	No	No	No	No	No	No	No
Crypto Card	Yes	Yes	No	No	No	No	No	No	No
RADIUS Token Server	Yes	Yes	No	No	No	No	No	No	No
VASCO	Yes	Yes	No	No	No	No	No	No	No
Axent	Yes	Yes	No	No	No	No	No	No	No
RSA	Yes	Yes	No	No	No	No	No	No	No
SafeWord	Yes	Yes	No	No	No	No	No	No	No

Diagnostic Commands and Tools

Cisco Secure ACS has extensive logging capability that allows an administrator to troubleshoot any issue pertaining to CS ACS Server itself (for example, replication) or an AAA requests problem (for example, an authentication problem) from NAS. This section explores these tools and how to use them efficiently.

Reports and Activity (Real-time Troubleshooting)

The **Failed Attempts** log under the **Reports and Activity** from the GUI is the quickest and best way to find out the reasons for authentication failure. **Failed Attempts** logs are turned on by default. However, if you want to add additional fields to the Default, you may by browsing to **System Configuration > Logging > CSV Failed Attempts**. In the **CSV Failed Attempts File Configuration** page, move desired attributes from **Attributes** to **Logged Attributes**. Then click on **Submit**. These additional attributes are shown under **Reports and Activity**. Occasionally, you might need to look at the **Passed Authentications** to troubleshoot authorization or NAS Access Restriction (NAR) issues. By default, the **Passed Authentication** log is not turned on. To turn it on, go to **System Configuration > Logging > CSV Passed Authentications,** and check **Log to CSV Passed Authentications report** under **Enable Logging**. There are other logs available for different services. For instance, for replication issues, there is a corresponding CSV file called **Database Replication** under **Reports and Activity**.

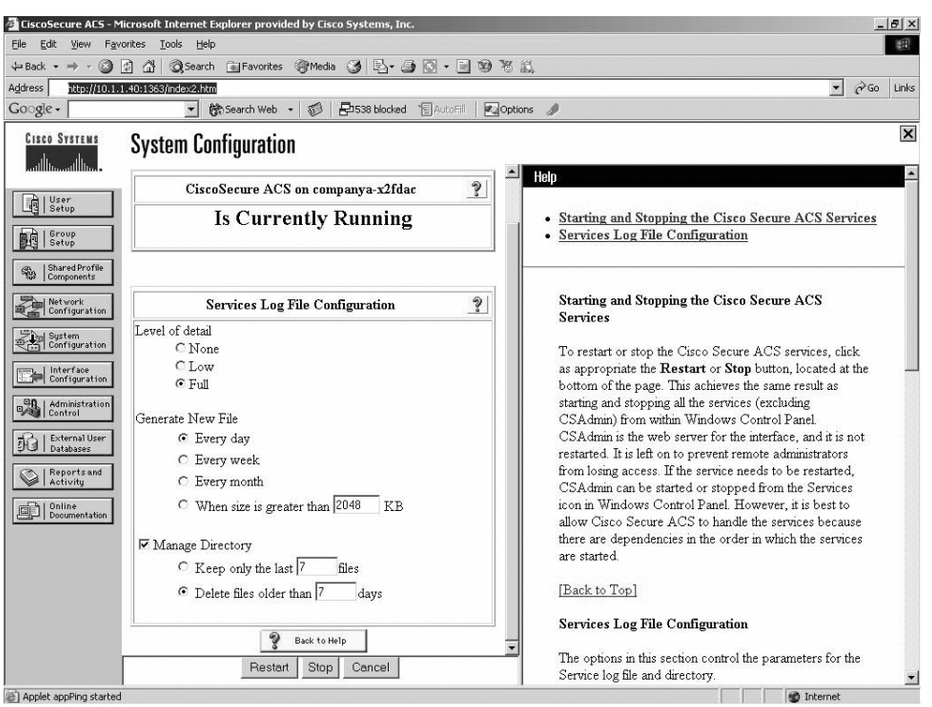
Radtest and Tactest

These tools are available to simulate AAA requests from the CS ACS server itself, which eliminates any possibilities of NAS configuration issues. This is especially important for troubleshooting the authentication issues with external user database authentication, for example, Microsoft Active Directory (AD) or Secure ID server. These tools are installed as part of CS ACS installation and located at **C:\Program Files\CiscoSecure ACS v3.3\Utils>**. More details on how to run these tools can be found at the following location: http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_tech_note09186a00800afec1.shtml#auth_of

Package.cab File

Package.cab is the result of execution of the CSSupport utility, which includes all the log files for every service that we have discussed in the section entitled "CS ACS Architecture." Before running the CSSupport utility as shown in the paragraphs that follow, to capture the debug level logging, be sure to collect the "FULL" logging (on CS ACS, **System Configuration > Service Control > Level of detail > Choose FULL > Restart**). This is shown in Figure 13-3. Also be sure to check Manage Directory and set the appropriate option.

Figure 13-3 *Turning on Full Logging on CS ACS*

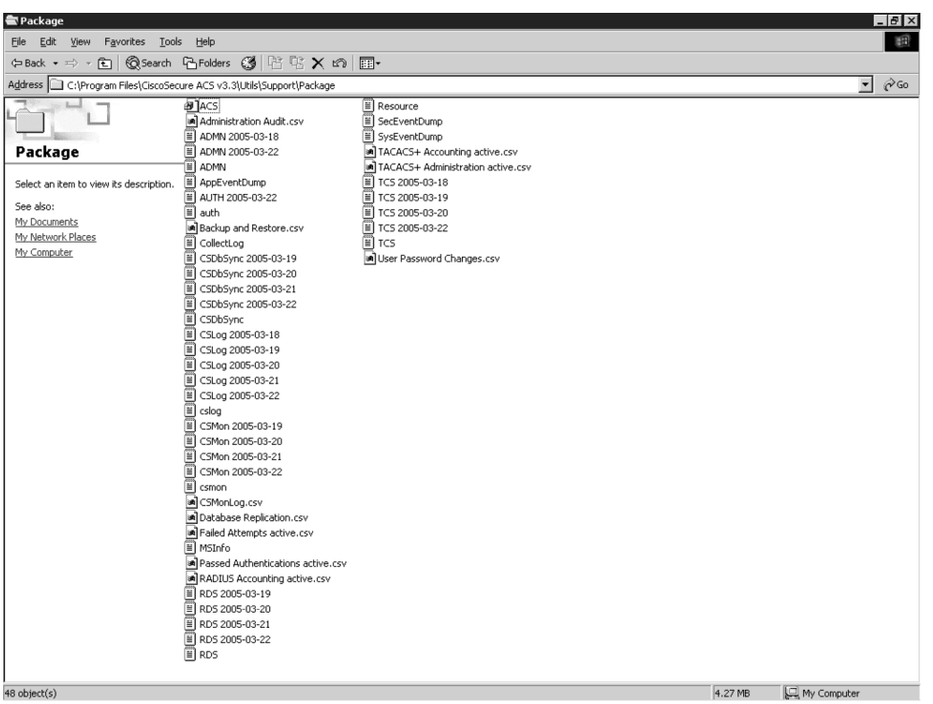


Once you set up the logging level to "FULL", run a few tests that are sure to fail and then run cssupport.exe as shown below:

```
C:\Program Files\CiscoSecure ACS v3.3\utils\CSSupport.exe
```

The Package.cab file contains a good deal of meaningful information, but the amount of information may be overwhelming. So, being able to read the file efficiently is a key to success in isolating issues from the Package.cab file logs. Before getting into any more detail, you need to understand what goes into the makings of the package.cab file. Figure 13-4 shows the unzipped version of package.cab with a listing of files (icons are arranged by type).

Figure 13-4 *Listing of Files in package.cab*



The following are short descriptions of the files of package.cab:

- **CSV Files**—CSV files contain the information about Audit log, Accounting, and Failed and Passed Authentication. Most of the files contain statistics, but to troubleshoot issues, Failed and Passed Authentication files are often used in conjunction with the log files that are discussed in the paragraphs that follow. The CSV files are created every day. Each file name without the date is the Active file. So, Failed Attempts active.csv is the active file, which stores the Failed Attempts information from the NAS.

- **Log Files**—Every service discussed in the "CS ACS Architecture" section of this chapter has a corresponding log file. These files contain extensive logs about each and every service. For instance, auth.log contains all the current log information of CSAuth service. Just like CSV files, log files are created every day and the active log file is the one without the date in its name.
- **User Database Files**—Three files go into making the CS ACS database. These files are **user.dat**, **user.idx**, and **varsdb.mdb**. You should *not* manipulate these files. Unless otherwise requested by Cisco, capturing these files is not necessary when running the CSSupport.exe utility.
- **Registry File**—ACS.reg contains the Registry information of the CS ACS Server. Substantial CS ACS configuration (for example, NAS) goes into the Windows Registry. So, reading this file may be required for some troubleshooting. Do not import this file into another server; instead, open it with a text editor of your choice.
- **Other Files**—Another useful file is MSInfo.txt, which contains the server and the OS information. The resource.txt file contains the resource information on the server, and SecEventDump.txt, AppEventDump.txt, and SysEventDump.txt contain an additional event dump on the server that may be used occasionally to troubleshoot any issues with the server itself.

As mentioned before, reading these files efficiently to isolate the problem is a key to success in troubleshooting CS ACS. To illustrate how to analyze the files, examine an example. The example assumes that a regular login authentication by the CS ACS Server is failing. The NAS debug does not give any conclusive output that indicates the reason for the failure.

To analyze this, first look at the Failed Attempts active.csv file to see why the user is failing. Quite often the information obtained from this file gives you the reason, so that no further analysis is needed; however, that's not always the case. For this example, assume that you have no conclusive reason for failure from the CSV file. However, you do have the username. The next step is to analyze the auth.log, because that contains more detailed information.

So, you search the username in the auth.log file. In this case, unfortunately, you receive no results from the search based on that username. So there must be a problem. It could be that CSTacacs service cannot process and forward the authentication request to the CSAuth service. Because you see the authentication failure in the Failed Attempts log, the authentication request must be reaching the CS ACS, and the first service that receives that packet is the CSTacacs, as the communication protocol configured between NAS and CS ACS is TACACS+. So, you need to analyze the TCS.log file, which contains all the activities that CSTacacs performs. As expected, you see the user request coming from the NAS. However, the user request is not being forwarded to the CSAuth service. After a little investigation, we find that NAR is configured for this user and, hence, packets are being dropped by the CSTacacs service; therefore, they are not being forwarded to the CSAuth service. Hence, you do not see the user in the auth.log. For every AAA request failure, you must look at the Failed Attempt first, and then search for the username in the auth.log. If an additional detail is needed, you need to analyze either the TCS.log or the RDS.log. Note

that both CSTacacs and CSRadius form the communication bridge between the NAS and CS ACS, and CSAuth is the communication bridge between the CSTacacs/CSRadius and any external user databases such as Active Directory, NDS, and so on.

Categorization of Problem Areas

The problem areas of CS ACS can be categorized as follows:

- Installation and upgrade issues
- CS ACS with Active Directory integration
- CS ACS with Novell NDS integration
- CS ACS with ACE Server (Secure ID [SDI]) integration
- Replication issues
- Network access restrictions (NAR) issues
- Downloadable ACL issues

Installation and Upgrade Issues

If you follow the procedure properly, installation or upgrade is a fairly easy process for both CS ACS on Windows and CS ACS Appliance. This section examines the installation and upgrade procedure, important issues to be aware of, things that may go wrong, and how to resolve the problems.

CS ACS on Windows Platform

Depending on the version of CS ACS that needs to be installed, check the following documentation to make sure all the minimum requirements for the Operating System version, Service Packs (SPs), and so on, are met. Otherwise, abnormal failure might occur that might not be diagnosed or supported by Cisco TAC unless the documented minimum requirement is fulfilled.

http://www.cisco.com/warp/public/480/csnt.html

Installation steps are intuitive, and therefore they are not covered here.

Upgrading from an older to a new version is a little more complex than installing a new version. However, if you work through the following steps carefully, you can minimize the chance of upgrade failure substantially:

Step 1 Review the prerequisites for installation of the version that you are trying to upgrade. If you must perform an incremental upgrade, for instance, from CS ACS 2.3 on NT platform to CS ACS 3.3 on Win 2K platform, define the strategy.

Step 2 Back up the database using C:\Program Files\CiscoSecure ACS v3.3\Utils>**CSUtil -b** (full backup including NAS information) and C:\Program Files\CiscoSecure ACS v3.3\Utils>**CSUtil -d** (partial backup, only users/groups information) options, and save the files offline in a different location.

Step 3 Run the **setup.exe** file of the new version.

Step 4 If the standard upgrade procedure in Step 3 fails, run the uninstall shield or uninstaller from the control panel, and choose the option during uninstall to keep the old database. Then install the new version. These procedures should find the information saved by the uninstall procedure and import it.

Step 5 If Step 4 fails, chances are very high that your Registry has been corrupted. If so, uninstall the CS ACS completely, and run the **clean.exe** files, which come in the CS ACS CD. These files will clean up the Registry. Then proceed with the installation. In the newer version (for instance, CS ACS 3.3), the Clean utility comes as **setup.exe** within the **Clean** directory, which is in the **ACS Utilities\Support** directory of the installation CD.

Step 6 If all the services started on the newer version, import the **dump.txt** that you have created in Step 2 with the **csutil -d** option, which contains only the user and group information. You still need to define the NASs. If there is a small number of NASs, this may work.

Step 7 If you have a large number of NASs, build another server with a version that runs the old version of code and import the database that is created in Step 2 with the **csutil -b** option, which includes the whole database that has the NAS information in it. Then follow Steps 2–6.

You should be aware of the following important facts if you are trying to upgrade one of the older CS ACS versions or from the trial version:

- The minimum CS ACS version requirement to run on the Windows platform is CS ACS 2.5.
- If you are upgrading CS ACS from 2.3 on a Windows NT platform to CS ACS 3.3 on the Windows 2000 platform, be sure to upgrade to CS ACS 2.6 on the NT platform first, and be sure the database upgraded and data migrated properly. As CS ACS 2.6 can run on Windows 2000, upgrade the OS of your CS ACS server to Windows 2000 after ensuring that the service packs and other prerequisites are fulfilled, and, finally, upgrade to the target version of CS ACS, which is CS ACS 3.3.
- If you are running a trial version, to migrate that version to production, just upgrade or install the production CS ACS version on top of the trial version. For example, you can install the CS ACS 3.1 production version over the CS ACS 2.6 trial version, or install the CS ACS 3.3 production version over the CS ACS 3.3 trial version.

CS ACS installation or upgrade may fail for the following reasons:

- Running an unsupported version of OS, service pack (SP), or browser.
- CS ACS services are crashing.

  If you are running a supported browser and service pack but CS ACS is still crashing, upgrade to the latest build of the CS ACS release that you are running. There may be a bug that has been fixed in the latest build of that release. If you are running the latest release, provide Cisco TAC with the package.cab file or, at least, run **drwtsn32** in a DOS prompt, with the following box checked: Dump Symbol Table.

CS ACS with Active Directory Integration

To integrate with the Active Directory, Cisco Secure ACS can be installed in one of the following modes:

- **Standalone Server**—If CS ACS is installed on a standalone server, CS ACS can authenticate Windows users only against the local SAM database.
- **Domain Controller**—If CS ACS is installed on a Primary Domain Controller (PDC) or Backup Domain Controller (BDC), it will be able to authenticate Windows users who are defined in any trusted domain.
- **Member Server**—CS ACS on a member server will also authenticate users defined in any trusted domains. However, lack of permissions could cause issues with domain lists, authentication, and Remote Access Service (RAS) flag fetching.

Cisco Secure ACS services run under the local system account on the server. The local system account has almost the same privileges as the administrator.

When a new external WindowsNT/2000 database is defined on CS ACS, CS ACS fetches the list of domains trusted by the domain of the computer where the server is installed. CS ACS fetches the list of trusted domains only to populate it to Java control. The user can add domains manually as well. CS ACS uses the list of enumerated domains to determine the order in which they will be checked when an external authentication is presented.

When a new mapping between Windows NT/2000 user groups and Cisco Secure ACS user group is defined, CS ACS obtains and displays the list of the user groups defined in the selected Windows domain.

When a windows user is being authenticated, CS ACS uses Microsoft's Network Logon on behalf of the user to verify the user's credentials. This is a noninteractive login, as opposed to a desktop login.

CS ACS fetches the following information about that user:

- List of user groups to which the user belongs.
- Callback flag.

Values are set on the MS user definition page, which includes Admin set phone #, and user set (send by the client during authentication).

- Dialin permission (RAS flag).
- Password status.
- Microsoft Point-to-Point Encryption (MPPE) keys (there are two, a 56-bit and 128-bit key).

Until CS ACS version 3.0, there were no "hooks" into the Security Accounts Manager (SAM) database to change the password through CS ACS. CS ACS 3.0 uses an API to change MS-CHAP passwords, but the MS-CHAPv2 protocol must be supported end-to-end.

Table 13-3 shows the trust relationship for CS ACS with the domain controller when the CS ACS is on the member server of Domain A.

Table 13-3 *Trust Relationship of CS ACS and Windows Domain Controller When CS ACS Is on a Member Server of Domain A*

Task	Trust Direction	Description
Fetch list of domains trusted by Domain A.	A trusts other domains.	The list includes domains trusted by A.
Fetch list of user groups from a trusted Domain B.	B trusts A.	CS ACS reads information (accesses resources) on Domain B.
Authenticate a user with account on Domain B.	A trusts B.	CS ACS performs the network logon with user name. The user with an account on Domain B is going to access a computer in Domain A.
Fetch information (callback, and so on) on user with account on Domain B.	B trusts A.	CS ACS reads information (accesses resources) on Domain B.
Change password of a user with account on Domain B (CS ACS v3.0).	B trusts A.	CS ACS changes information (Access ressources) on Domain B.

Configuration Steps

The following steps are required to integrate CS ACS with the domain controller:

On the domain controller serving the CS ACS server follow these steps:

Step 1 Create a user.

Step 2 Make the user hard to hack by giving it a very long, complicated password.

Step 3 Make the user a member of the Domain Administrator group.

Step 4 Make the user a member of the Administrators group.

On the Windows 2000 server running CS ACS, follow these steps:

Step 1 Add a new user to the proper local group. Go to **Start > Settings > Control Panel > Administrative Tools > Computer Management**. Open **Local Users and Groups** and then **Groups**. Double-click the **Administrators** group. Click **Add**. Choose the domain from the **Look in** box. Double-click the user created earlier to add it. Click **OK**.

Step 2 Give the new user special rights on CS ACS server. Go to **Start > Settings > Control Panel > Administrative Tools > Local Security Policy > Local Policies**. Open **User Rights Assignment**. Double-click on **Act as part of the operating system**. Click **Add**. Choose the domain from the **Look in** box. Double-click the user created earlier to add it. Click **OK**. Double-click **Log on as a service**. Click **Add**. Choose the domain from the **Look in** box. Double-click the user created earlier to add it. Click **OK**.

Step 3 Set the CS ACS services to run as the created user. Open **Start > Settings > Control Panel > Administrative Tools > Services**. Double-click the **CSADMIN** entry. Click the **Log On** tab. Click **This Account** and then the **Browse** button. Choose the domain, and double-click the user created earlier. Click **OK**. Repeat for the remainder of the CS services.

Step 4 Wait for Windows to apply the security policy changes, or reboot the server. If you rebooted the server, skip the rest of these instructions. Otherwise, stop and then start the **CSADMIN** service. Open the CS ACS GUI. Click on **System Config**. Click on **Service Control**. Click **Restart**.

NOTE If the Domain Security Policy is set to override settings for "Act as part of the operating system" and "Log on as a service" rights, the user rights changes listed in the previous steps also need to be made there.

Troubleshooting Steps

This section discusses some of the common issues that you may run into when integrating with Active Directory.

Windows Group to CS ACS Group Mapping Problems

During Configuring of Group mapping, the user sees a pop-up window. If you are having problems with Group mapping, you may see the following message:

```
Failed to enumerate Windows groups. If you are using AD consult the installation
guide for information
```

Possible causes of the problems are as follows:

- **CS ACS services do not have privileges to execute the NetGroupEnum function**—Refer to Configuration steps discussed for "CS ACS with Active Directory Integration" in the preceding section to correct the permission issue.
- **NetBIOS over Transmission Control Protocol (TCP) is not enabled**—NetBIOS over TCP must be enabled; otherwise, group mapping will fail.
- **Domain Name System (DNS) is not working correctly**—You may try to reregister DNS with commands: "ipconfig/flushdns" then "ipconfig/registerdns" at the DOS prompt.
- **Remote Procedure Call (RPC) is not working correctly (for example, after applying the blaster patch)**—In that case, consult with Microsoft.
- **Domain Controller (DCs) are not time-synchronized**—Run the command net time /Domain: <DomainName> to synchronize time.
- **Different service packs**—If you run different SPs on different DCs, you may run into this problem. Apply the same patch to fix the problem.
- **NetLogon Services are not running**—NetLogon Services must up and running on all DCs.
- **Check that no firewall (FW) packet filters are installed**—If there is a packet-filtering firewall installed, be sure to select **Yes** on DNS properties to "allow dynamic updates".

CS ACS Maps User to Wrong Group of CS ACS (Default Group)

After successful user authentication based on the group mapping configuration, the user is mapped to a specific CS ACS group. The following list summarizes some of the reasons why the user may be mapped to the wrong CS ACS group:

- **Misconfiguration of group mapping**—If the user belongs to both group X and group Y, CS ACS assigns the user according to the order in which the user was configured.
- **Service accounts under which CS ACS services are running do not have permission to validate groups for another user**—Log in as user, under the CS ACS services that are running. Check if you have access to get the groups of another user.

CS ACS with Novell NDS Integration

This section works through the configuration steps that lead in turn to sections that cover troubleshooting steps.

Configuration Steps

Use the following steps to configure an NDS database with CS ACS on Windows.

Step 1 Consult with your Novell NetWare administrator to get administrator context information for CS ACS and the names of the Tree, Container, and Context details.

Step 2 On CS ACS, click on **External User Databases > Database Configuration > Novell NDS > Configure**.

Step 3 In the **Novell NDS** configuration window, enter a name for the configuration. This is for information purposes only.

Step 4 Enter the **Tree name**.

Step 5 Enter the full **Context List**, with items separated by dots(.). You can enter more than one context list. If you do, separate the lists with a comma and space. For example, if your Organization is Corporation, your Organization Name is Chicago, and you want to enter two Context names, Marketing and Engineering, you would enter**: Engineering.Chicago. Corporation**, **Marketing.Chicago.Corporation**. You do not need to add users in the Context List.

Step 6 Click **Submit**. Changes take effect immediately; you do not need to restart the Cisco Secure ACS.

Caution If you click **Delete**, your NDS database is deleted.

Step 7 Then perform the Group Mappings (between the Novell NDS Database Groups and CS ACS Groups) by browsing to **External User Databases > Database Group Mappings > Novell NDS.**

Step 8 Finally, configure the unknown user policy by selecting **Check the following external user databases** and moving the **Novell NDS** database from the **External Databases** to the **Selected Databases** text box on the **External User Databases > Unknown User Policy** page.

Troubleshooting Steps

You can isolate any problem that you may have with the troubleshooting steps in the sections that follow.

Novell Client Is Not Installed

You must install the Novell client on the CS ACS server, so that CS ACS can talk to the Novell NDS database. If you do not have the Novell client installed on the CS ACS, and you try to configure Novell NDS database settings from the **External User Database > Database Configuration > Novel NDS**, you will receive an error message similar to the following:

```
An error has occurred while processing the External Database Configuration Page
because of an internal error..
```

Revise the Configuration on CS ACS

Most of the time, the Novell NDS authentication failure is caused by misconfiguration. Therefore, check to see if the tree name, context, and container name are all specified correctly. Start with one container in which users are present; later more containers can be added if needed.

Check Admin Username

Check the admin username to be sure it is correct, and that you have defined a fully qualified path. For example, instead of admin, define admin.cisco, as the latter is a fully qualified name.

Example 13-1 shows the incorrect provision of admin credentials.

Example 13-1 *Incorrect Admin Credentials*

```
AUTH 03/22/2005 10:40:21 I 0360 0676 External DB [NDSAuth.dll]: Tree 224462640 could
not log in with admin credentials supplied
```

Perform Group Mapping

Performing Group Mapping is an excellent test to ensure the admin context can connect and pull the group information from the Novell NDS database. Therefore, if you are unable to map groups, the admin user does not have permission to list the groups. Under that circumstance, check that the admin can list users in the other domain. One way to verify that is as follows: on the CS ACS Server, using Nwadmin, examine the groups from the other domain. If you cannot do so, consult with the Novell administrator.

Authentication Failure with a Bad Password

Before looking at authentication that has failed either due to the wrong username or a bad password, it's extremely important to understand and be familiar with the sequence of events that occur within CS ACS with Novell NDS authentication. Therefore, closely observe the successful user authentication log shown in Example 13-2.

Example 13-2 *Successful User Authentication Against NDS Database*

```
AUTH 03/22/2005 12:20:56 I 5081 1764 Start RQ1026, client 2 (127.0.0.1)
! As the user doesn't exist on the local database, CS ACS is tagging this as unknown user
AUTH 03/22/2005 12:20:56 I 4683 1764 Attempting authentication for Unknown User
'cisco'
! The following two lines indicate that Novell NDS is configured to this user
! authentication. This is being done by selecting Novell NDS database for Unknown User
! Policy
AUTH 03/22/2005 12:20:56 I 1280 1764 ReadSupplierRegistry: Novell NDS loaded
```

Example 13-2 *Successful User Authentication Against NDS Database (Continued)*

```
AUTH 03/22/2005 12:20:56 I 0863 1764 pvAuthenticateUser: authenticate 'cisco'
against Novell NDS
! Following lines indicate that CS ACS is trying to lock a thread for this user
! Authentication.
AUTH 03/22/2005 12:20:56 I 0360 1764 External DB [NDSAuth.dll]: User cisco waiting
for lock
AUTH 03/22/2005 12:20:56 I 0360 1764 External DB [NDSAuth.dll]: User cisco waiting
in lock
! A new thread is getting initialized here for the user authentication under ndstest
tree
AUTH 03/22/2005 12:20:56 I 0360 1764 External DB [NDSAuth.dll]: Initializing thread
0 for tree ndstest
AUTH 03/22/2005 12:20:56 I 0360 0472 External DB [NDSAuth.dll]: Starting Thread 0
! The following two lines indicate that the user authentication is under works
AUTH 03/22/2005 12:20:56 I 0360 0472 External DB [NDSAuth.dll]: Thread 0 for tree
ndstest Waiting for work
AUTH 03/22/2005 12:20:56 I 0360 0472 External DB [NDSAuth.dll]: Thread 0 for tree
ndstest Got work
! This is where the user is authenticated.
AUTH 03/22/2005 12:20:56 I 0360 0472 External DB [NDSAuth.dll]: Authenticated
cisco.OU=SJ.TESTING.LAB, Response 0
AUTH 03/22/2005 12:20:56 I 0360 1764 External DB [NDSAuth.dll]: Back from Wait for
user cisco with code 0
AUTH 03/22/2005 12:20:56 I 0360 1764 External DB [NDSAuth.dll]: Response 0 from
successful Tree ndstest
AUTH 03/22/2005 12:20:56 I 0360 0472 External DB [NDSAuth.dll]: Response 0 from Tree
ndstest
AUTH 03/22/2005 12:20:56 I 0360 0472 External DB [NDSAuth.dll]: Thread 0 for tree
ndstest Waiting for work
! Following three lines indicates that the group mappings between Novell NDS and CS ACS
! are successful. Third line in particular indicates that user is mapped to CS ACS Group
! number 150.
AUTH 03/22/2005 12:20:56 I 0360 1764 External DB [NDSAuth.dll]: Added
'sj_acs.SJ.testing.LAB' to Group List for user: cisco.OU=SJ.TESTING.LAB
AUTH 03/22/2005 12:20:56 I 0360 1764 External DB [NDSAuth.dll]: There were 1 Groups
for this user: cisco.OU=SJ.TESTING.LAB
AUTH 03/22/2005 12:20:56 I 0360 1764 External DB [NDSAuth.dll]: User cisco
authenticated into group 150
AUTH 03/22/2005 12:20:56 I 0360 1764 External DB [NDSAuth.dll]: User cisco out from lock
AUTH 03/22/2005 12:20:56 I 3421 1764 User cisco password type changed
AUTH 03/22/2005 12:20:56 I 1586 1764 User cisco feature flags changed
AUTH 03/22/2005 12:20:56 I 1586 1764 User cisco feature flags changed
AUTH 03/22/2005 12:20:56 I 5081 1764 Done RQ1026, client 2, status 0
```

As mentioned before, it is extremely important to understand the sequence of events that occur with a successful user authentication as shown in Example 13-2, before you can analyze and find the cause of failure for a bad user password. With the knowledge gained from Example 13-2, examine example 13-3, which shows failed authentication due to a bad password.

Example 13-3 *Shows a Failed Authentication Attempt Due to Bad Password to NDS Database*

```
AUTH 08/13/2003 14:11:47 I 0276 2212 External DB [NDSAuth.dll]: User cisco waiting
for lock
AUTH 08/13/2003 14:11:47 I 0276 2212 External DB [NDSAuth.dll]: User cisco waiting
in lock
AUTH 08/13/2003 14:11:47 I 0276 2212 External DB [NDSAuth.dll]: Initializing thread
0 for tree ndstest
AUTH 08/13/2003 14:11:47 I 0276 1968 External DB [NDSAuth.dll]: Thread 0 for tree
ndstest Got work
AUTH 08/13/2003 14:11:50 I 0276 1968 External DB [NDSAuth.dll]: Response 1 from Tree
ndstest
AUTH 08/13/2003 14:11:50 I 0276 1968 External DB [NDSAuth.dll]: Thread 0 for tree
ndstest Waiting for work
! In the following line, code 102 indicates that authentication fails due to bad
username
! or wrong password.
AUTH 08/13/2003 14:11:53 I 0276 2212 External DB [NDSAuth.dll]: Back from Wait for
user cisco with code 102
! Then eventually it times out trying.
AUTH 08/13/2003 14:11:53 I 0276 2212 External DB [NDSAuth.dll]: Timeout trying User
cisco
AUTH 08/13/2003 14:11:53 I 0276 2212 External DB [NDSAuth.dll]: User cisco out from
lock
```

Authentication Failure When the User Does Not Exist

If the user does not exist on the Novell NDS database or the user enters the wrong username, the authentication will fail, giving the same error code as a bad password (error code 102). Example 13-4 shows the output when the user does not exist on the database.

Example 13-4 *Failed Authentication Due to Unknown User*

```
AUTH 08/13/2003 14:13:24 I 0276 2212 External DB [NDSAuth.dll]: User cisco123
waiting for lock
AUTH 08/13/2003 14:13:24 I 0276 2212 External DB [NDSAuth.dll]: User cisco123
waiting in lock
AUTH 08/13/2003 14:13:24 I 0276 2212 External DB [NDSAuth.dll]: Initializing thread
0 for tree ndstest
AUTH 08/13/2003 14:13:24 I 0276 1968 External DB [NDSAuth.dll]: Thread 0 for tree
ndstest Got work
AUTH 08/13/2003 14:13:24 I 0276 1968 External DB [NDSAuth.dll]: Response 1 from Tree
ndstest
AUTH 08/13/2003 14:13:24 I 0276 1968 External DB [NDSAuth.dll]: Thread 0 for tree
ndstest Waiting for work
AUTH 08/13/2003 14:13:26 I 5094 2220     Worker 3 processing message 275.
AUTH 08/13/2003 14:13:26 I 5081 2220 Start RQ1012, client 27 (127.0.0.1)
AUTH 08/13/2003 14:13:26 I 5081 2220 Done RQ1012, client 27, status 0
AUTH 08/13/2003 14:13:26 I 5094 2220     Worker 3 processing message 276.
AUTH 08/13/2003 14:13:26 I 5081 2220 Start RQ1031, client 27 (127.0.0.1)
AUTH 08/13/2003 14:13:26 I 5081 2220 Done RQ1031, client 27, status 0
! In the following line, the code 102 is an indication that user authentication failed
! either due to bad username or wrong password.
AUTH 08/13/2003 14:13:30 I 0276 2212 External DB [NDSAuth.dll]: Back from Wait for
user cisco123 with code 102
```

Example 13-4 *Failed Authentication Due to Unknown User (Continued)*

```
! Eventually will timeout
AUTH 08/13/2003 14:13:30 I 0276 2212 External DB [NDSAuth.dll]: Timeout trying User
cisco123
AUTH 08/13/2003 14:13:30 I 0276 2212 External DB [NDSAuth.dll]: User cisco123 out
from lock
AUTH 08/13/2003 14:13:30 I 0276 2212 External DB [NTAuthenDLL.dll]: Starting
authentication for user [cisco123]
! Following lines indicate that NT/2K domain is also configured next in order, so
! attempting authentication to NT/2K domain as well and eventually fails.
AUTH 08/13/2003 14:13:30 I 0276 2212 External DB [NTAuthenDLL.dll]: Attempting NT/
2000 authentication
AUTH 08/13/2003 14:13:30 E 0276 2212 External DB [NTAuthenDLL.dll]: NT/2000
authentication FAILED (error 1326L)
AUTH 08/13/2003 14:13:30 I 1547 2212 Unknown User 'cisco123' was not authenticated
```

Wrong Group Mapping

After successful user authentication, the user is mapped to a specific CS ACS group. Two things determine which CS ACS group the user is mapped to: the Novell NDS group or groups the user belongs to, and the CS ACS group mapping configuration under the External Database Configuration page. If there are problems with proper group assignment by CS ACS after successful Novell NDS user authentication, analyze the **auth.log** file to find out which NDS database groups a specific user belongs to, and if the same group or groups are mapped to the desired CS ACS group. Examine the following example. Assume that the user belongs to all the following groups and maps to the CS ACS Group 10:

- superuser.xyz
- http_only.xyz
- http_ftp.xyz
- http_netmeeting.xyz

Analyze the log as shown in Example 13-5.

Example 13-5 *Sample Output: User Saad Belongs to Multiple Groups That Do Not Match with the Group Mapped to CS ACS*

```
AUTH 10/13/2004 10:20:49 I 0259 1340 External DB [NDSAuth.dll]: Initializing
thread 0 for tree XYZ
AUTH 10/13/2004 10:20:49 I 0259 0676 External DB [NDSAuth.dll]: Thread 0 for
tree XYZ Got work
AUTH 10/13/2004 10:20:52 A 0259 0676 External DB [NDSAuth.dll]: Login
Attempt: Context 'MKT.DH.XYZ' User 'saad.MKT.DH.XYZ'
Password 'saad' result 0
AUTH 10/13/2004 10:20:52 I 0259 0676 External DB [NDSAuth.dll]:
Authenticated saad.MKT.DH.XYZ, Response 0
AUTH 10/13/2004 10:20:52 I 0259 1340 External DB [NDSAuth.dll]: Back from
Wait for user saad with code 0
AUTH 10/13/2004 10:20:52 I 0259 1340 External DB [NDSAuth.dll]: Response 0
from successful Tree XYZ
```

continues

Example 13-5 *Sample Output: User Saad Belongs to Multiple Groups That Do Not Match with the Group Mapped to CS ACS (Continued)*

```
AUTH 10/13/2004 10:20:52 I 0259 0676 External DB [NDSAuth.dll]: Response 0
from Tree XYZ
AUTH 10/13/2004 10:20:52 I 0259 0676 External DB [NDSAuth.dll]: Thread 0 for
tree XYZ Waiting for work
AUTH 10/13/2004 10:20:52 I 0259 1340 External DB [NDSAuth.dll]: Added
'Everyone.MKT.DH.XYZ' to Group List for user:
saad.MKT.DH.XYZ
AUTH 10/13/2004 10:20:52 I 0259 1340 External DB [NDSAuth.dll]: Added
'http netmeeting.XYZ' to Group List for user:
saad.MKT.DH.XYZ
AUTH 10/13/2004 10:20:52 I 0259 1340 External DB [NDSAuth.dll]: There were 2
Groups for this user: saad.MKT.DH.XYZ
AUTH 10/13/2004 10:20:52 I 0259 1340 External DB [NDSAuth.dll]: User saad
authenticated into group 0
```

So, from Example 13-5, you see that user saad belongs to NDS groups "Everyone.MKT.DH.XYZ" and "http_netmeeting.XYZ". Thus, the user does *not* meet the requirements to be mapped to group 10 on CS ACS, as both of the groups are not mapped on the CS ACS to group 10. As any unmatched group defaults to the CS ACS Default Group, saad is mapped to Group 0. So, the user must belong to *all* the NDS groups in the mapping, to be mapped into the configured CS ACS group, not just one.

On CS ACS to map this user into group 10, you need a map, which has one of the following combinations of NDS groups:

- Everyone.MKT.DH.XYZ
- http_netmeeting.XYZ
- Everyone.MKT.DH.XYZ' and 'AAA_http netmeeting.XYZ'

It does not matter if a user also belongs in other NDS groups, in addition to those listed in the mapping, but the user must belong in all the NDS groups listed in a mapping to be mapped to a proper CS ACS group.

CS ACS with ACE Server (Secure ID [SDI]) Integration

Cisco Secure ACS can integrate with a few token servers, but this chapter discusses only the ACE server. The ACE server is also known as the SDI server, so both names will be used interchangeably throughout this chapter. Because the implementation of other token servers is very similar to the implementation of the ACE server, the discussion of ACS integration with ACE is applicable for the other token servers as well. The SDI server can be installed on the same machine on which Cisco Secure ACS is running, or on a separate machine. ACE client software is required on the system running Cisco Secure ACS software.

Installation and Configuration Steps

Use the following steps to install and configure CS ACS with SDI Software

Step 1 Install the ACE server as per ACE direction.

Step 2 Bring the ACE server into host configuration mode (run sdadmin).

Step 3 Be sure you have configured the hostname/ip-address of Cisco Secure ACS system as a client in the ACE server setup. This can be verified under **Client > Edit Client** from ACE Server Host configuration window. For CS ACS Windows client, encryption should be Data Encryption Standard (DES), because the client is Windows, and you have to choose **Net OS Client**. When you click the **User Activations** tab, you must see the **SDI user** under **Directly Activated Lists**.

Step 4 Be sure the user is activated on the client—the client is the system on which Cisco Secure ACS is installed. This can be verified under **Users > Edit Users > Client Activations**. In this window you will see a list of available clients. Choose the right one and move them under **Clients Directly Activated On**.

Step 5 Be sure the CS ACS client and the SDI server can perform forward and reverse lookups of each other (that is, ping by name or IP).

Step 6 Copy the SDI server's **sdconf.rec** to the CS ACS client; this can reside anywhere on the CS ACS client.

Step 7 The installation of the ACE client on Windows may differ slightly by version. Run **agent.exe** to initiate the installation process of the ACE client. During installation, when asked to install **Network Access Protection Software**, answer **No**, and leave the **root certificate** box blank. Then go to **Next**. When prompted, specify the path to the **sdconf.rec** file, including the file name.

Step 8 After the client installation and reboot, go to Windows **Control Panel > SDI Agent > Test Authentication with Ace Server > Ace/Server Test Directly** and enter the **username**, **code**, and **card** configured on the Ace server to perform an authentication test and check the communication between the SDI client and the server. If this test does not work, it means the SDI client is not communicating with the SDI server. It also means the CS ACS Windows will not be able to communicate with the SDI Server. This is because CS ACS uses an SDI client interface to communicate with the SDI server.

Step 9 Then install **CS ACS** on Windows as usual.

Step 10 From **Navigation**, go to **External User Databases > Database Configurations > Configure**. ACS should be able to find the SDI Dynamic Linked Library (DLL).

Step 11 Go back to **External User Databases.** Click on **Unknown User Policy** and check the **second radio button.** Then move the SDI database from External Databases to Selected databases.

Step 12 Go back to **External User Databases** and click on **Database Group Mapping > SDI Database > Cisco Secure ACS group** to pick the group that will be mapped to SDI group.

Step 13 Go to Group setup and edit the settings for the group that was mapped to SDI. In this case, it is **Default Group**. Add appropriate attributes for TACACS+ & RADIUS depending on what kind of service the user will use (either Shell or PPP).

Troubleshooting Steps

Use the following step-by-step procedures to troubleshoot the SDI issues with CS ACS:

Step 1 First, authenticate the user with the ACE test agent.

Step 2 If this works, confirm that the card is synchronized with the database. Be sure to use DES encryption on the SDI server when the card is initialized. Choosing SDI will not work.

Step 3 If this does not work, resynchronize from the Token menu in host configuration mode. Click on **Token > Edit Token**, and then choose the token that you want to resynchronize. You will have a menu to resynchronize.

Step 4 Next, bring up the activity monitor (**Report > Log Monitor > Activity Monitor**) on the ACE server while attempting Telnet authentication to a device.

Step 5 Then check to see if there are any errors on the activity monitor on the ACE server.

Step 6 If the ACE server works, but there is a problem with the dial users, check the settings on the network access servers (NASs) to be sure that Password Authentication Protocol (PAP) is configured. Then try connecting as a non-SDI user.

Step 7 If that works, connecting as an SDI user should work. Put the username in the username tab and the passcode in the password tab on Dial-up Networking.

Step 8 If the client from where you are dialing is configured to bring up the post terminal screen after dialing, then be sure the following AAA statement is on the NAS:

```
aaa authentication ppp default if-needed    tacacs+/Radius
```

The key is to use **>if-needed>**. This means that if the user is already authenticated by the following AAA statement:

```
aaa authentication login default tacacs+/radius
```

then you do not have to authenticate the user again when doing PPP. This also applies when using the normal PAP password.

Here are some common problems that you might face with SDI and CS ACS integration:

- **The ACE log displays the message "Passcode accepted", but the user still fails**—Check the CS ACS Failed Attempts log to determine the cause of the problem. The failure could be due to authorization issues.
- **The ACE log displays the message "Access Denied, passcode incorrect"**—This is an ACE problem with the passcode. During this time, the CS ACS Failed Attempts log shows either the message **External DB auth failed** or **External DB user invalid** or **bad password**.
- **The ACE log displays the message "User not in database"**—Check the ACE database. During this time, the CS ACS Failed Attempts log shows either the message **External DB auth failed** or **External DB user invalid or bad password**.
- **The ACE log displays the message "User not on agent host"**—This is an ACE configuration problem. To solve this problem, configure the user on the agent host.
- **The CS ACS log displays the message "External database not operational"**—If the ACE log does not show any attempts, confirm the operation with the ACE client test authentication and check to be sure that the ACE/server authentication engine is running.
- **The CS ACS log displays the message "CS user unknown" or "Cached token rejected/expired" with nothing in the ACE log**—If the network device is sending a Challenge Handshake Authentication Protocol (CHAP) request and the CS ACS does not have an enumerated ACE user with a separate CHAP password, CS ACS does not send the user to ACE because token-only authentication requires PAP.

Replication Issues

Replication allows the CS ACS Server to maintain distributed databases. This helps the NAS to improve fault tolerance (by providing a backup server) or to improve performance (by sharing throughput across several servers). Replication can be configured as a straightforward master-to-slave relationship, or as a pipeline, or even as a tree in which each slave automatically replicates to its children upon receipt of replicated data from its parent.

Configuration

Replication is configured by the GUI. The GUI is used on both the master and slave to configure both ends of the replication.

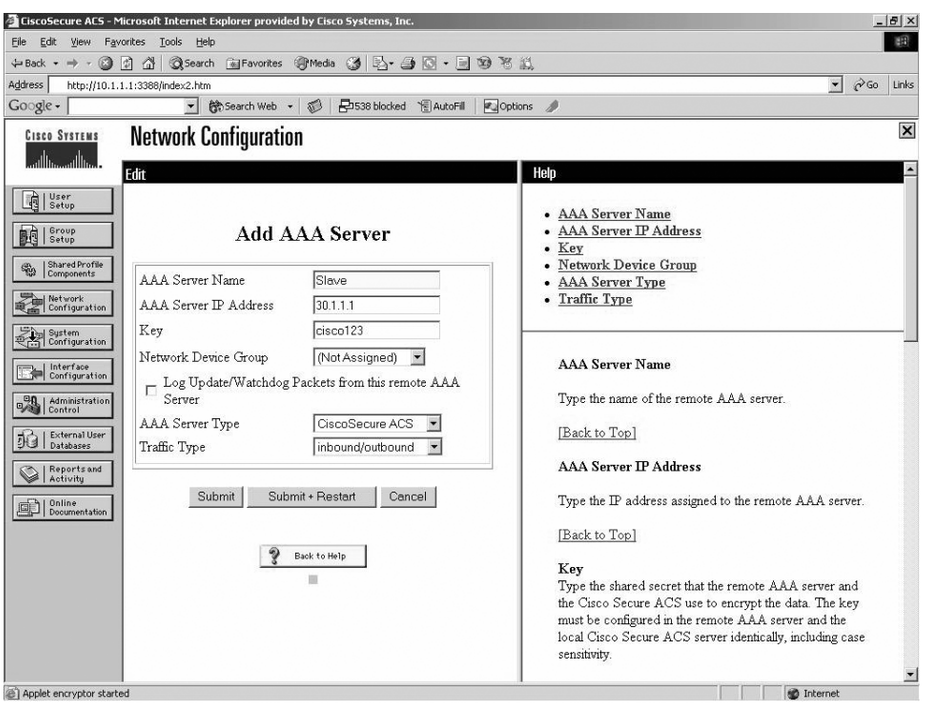
The following are the steps required for replication on the master (IP Address 10.1.1.1) and the slave (IP address 30.1.1.1). Use the following steps to configure the master CS ACS:

Step 1 Log in to the primary CS ACS server GUI.

Step 2 Turn on **Distributed System Settings** and enable **Cisco Secure Database Replication** options—found under **Interface Configuration->Advanced Options**.

Step 3 In the **Network Configuration** section, add each secondary server to the AAA Servers table as shown in Figure 13-5. The Traffic Type should be left defaulting to *inbound/outbound* unless there is a good reason to do otherwise.

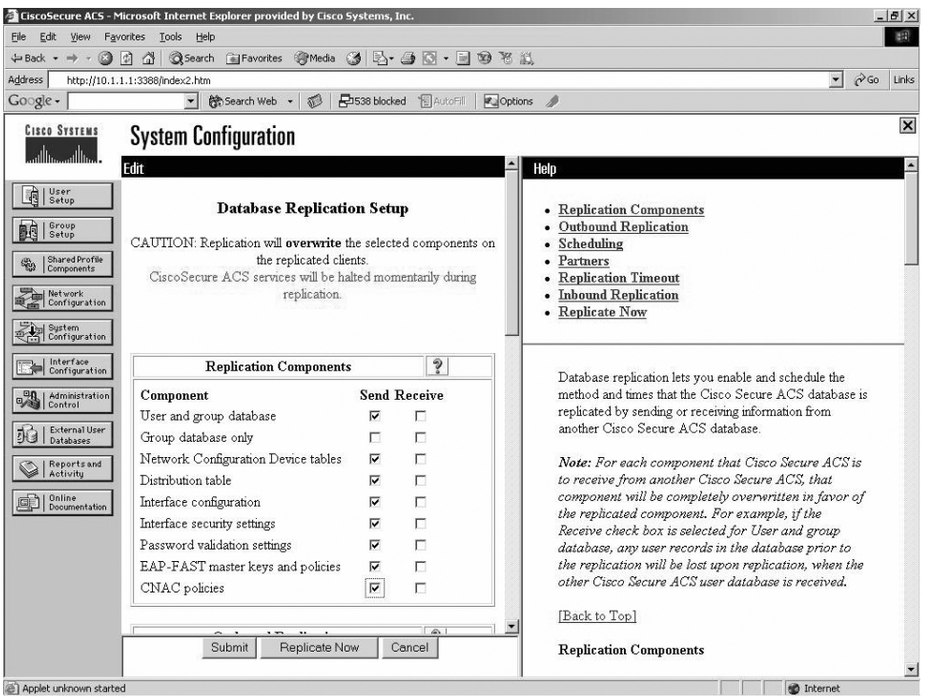
Figure 13-5 *Slave CS ACS Server Entry Configuration on the Primary CS ACS Server*



Step 4 In the navigation bar, click **System Configuration.** Then click **Cisco Secure Database Replication**, which brings up the **Database Replication Setup** page.

Step 5 Select the **Send** check box for each database component to send to the secondary server as shown in Figure 13-6.

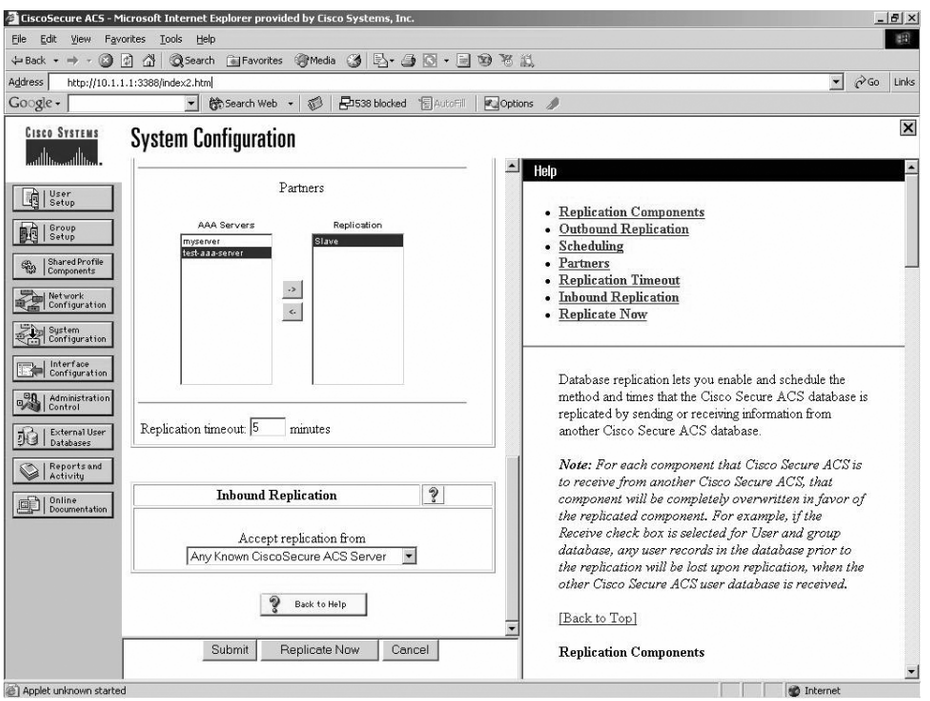
Figure 13-6 *Replication Component Configuration on the Master CS ACS*



Step 6 Select a scheduling option from one of the four options: **Manually**, **Automatically Triggered Cascade, Every X Minutes,** or **At Specific times**. To set up Auto Replication, you *must not* select **manually,** and the **Scheduling Option** must be set up on Master, not on the slave.

Step 7 Under the **Replication Partners**, add the **secondary CS ACS server** to the Replication Partner column as shown in Figure 13-7.

Figure 13-7 *Replication Partner Configuration on Master*



Step 8 Click **Submit.** Note that **Accept Replication from** does not have any meaning on the master.

Use the following steps to configure steps required the slave CS ACS server:

Step 1 Follow the preceding Steps 1-4, which were outlined for the master server.

Step 2 Click the **Receive** check box for each database component to be received from a primary server as shown in Figure 13-8.

Step 3 Leave the Scheduling Option set to **Manually**.

Step 4 Do not add the primary server to the **Replication Partner** column, under the Replication Partners; the replication partner column should be blank as shown in Figure 13-9.

Figure 13-8 *Replication Components Configuration on the Slave*

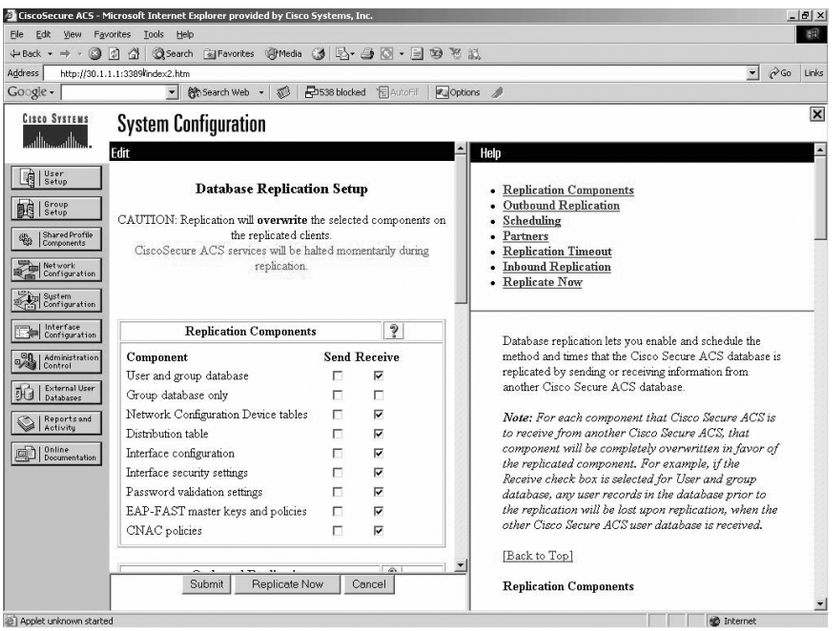
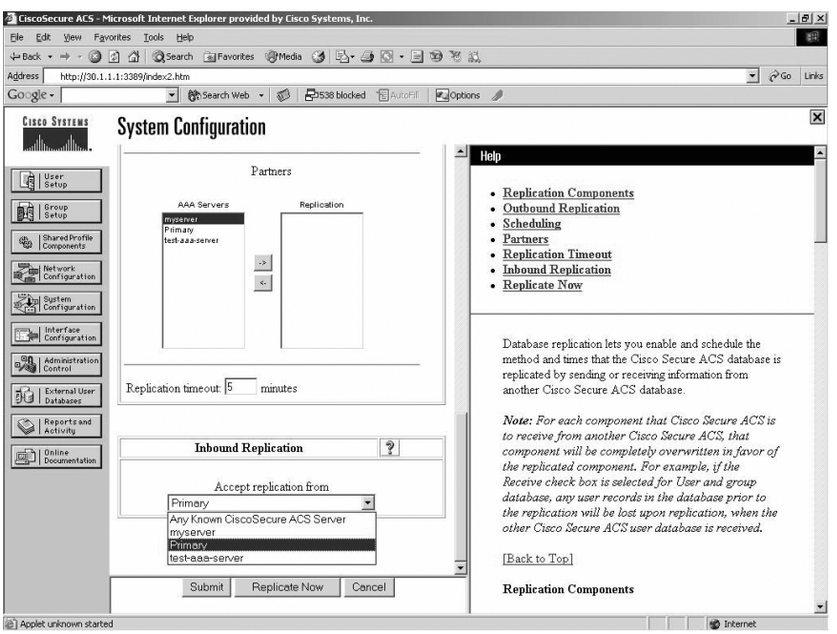


Figure 13-9 *Replication Partners Configuration on the Slave*



Step 5 From the **Accept Replication From** drop-down list, select **Master Server**. If you have more than one Master server, select **Any Known Cisco Secure ACS for Windows 2000/NT Server**.

Step 6 Click **Submit**.

Troubleshooting Steps

Before getting into the details of some of the common problems that you might face with replication, it is useful to examine the internal workings of replication.

On the master, a dedicated thread within the CSAuth service continually monitors the time and controls the outbound replication when due. The following actions are performed:

1. Lockout and wait for any open transactions to complete (authentication's and admin's updates).
2. Dump the required **registry keys** and copy/compress required files to a temporary location.
3. Release lockouts, allowing normal service to resume.

For each child replication partner, CSAuth then performs the following tasks:

1. Connects to remote CSAuth server.
2. Exchanges version and component specifications.
3. Copies permitted files onto remote AAA server.
4. Initiates replication take-up on the remote AAA server. This request also specifies where the files are located on the remote AAA server.

On the slave, the CSAuth service performs the following task:

1. Opens a connection as per any client request.
2. Responds to the master's request for version and replication information checks by verifying that the two servers are running the same software version. The master will have sent a list of components it is allowed to send. The slave then removes any components it is not allowed to receive. The resultant list is returned to the master.
3. Performs remote file copy operations as the master transmits the replication set.

When the slave receives the replication take-up command from the master, it performs the following:

1. Lockout and wait for any open transactions to complete (authentications and administrator updates).
2. Load the required Registry keys. Uncompress and save required files from the temporary location.

3 Release lockouts, allowing normal service to resume.

4 Restart any services as configured in the Registry (default CSRadius and CSTacacs).

5 Kick the replication thread so that if so configured, "cascade" replication occurs.

To view the actions performed by the CSAuth service for replication as described in the previous steps, analyze the **auth.log** file. The replication CSV file gives a summary version of the status of replication. Therefore, to troubleshoot the replication issues, first look at the CSV file, which is under **Reports & Activity,** or in the logs directory of the CS ACS installation. If the problem cannot be resolved with the CSV file, you can analyze the **auth.log** (…\csauth\logs\auth.log), which shows details of failure (be sure to turn logging to FULL).

To see only the replication log on auth.log file, search for string "**dbreplicate(out)**" on the master and "**dbreplicate(in)**" on the slave server. Example 13-6 shows the output of auth.log file on the Master Server.

Example 13-6 *Replication Only Log on the Master Server*

```
DBReplicate(OUT) attempting to exchange sync info with host acs1
DBReplicate(OUT) attempting to tx files to host acs1
DBReplicate(OUT) - one or more files could not be sent to acs1
DBReplicate(OUT) to host acs1 was denied
Etc.
```

The following are some of the issues that you might encounter, and their resolutions.

- **Compatible version numbers**—Both ends of a replication *must* be running the same version. However, they may be running different builds of the same version, that is, 2.3(1.24) and 2.3(1.29). This has caused a few problems in clients replicating from 2.3 betas to 2.3 FCS systems due a change in Registry encryption. This might be rectified in the future but is worth bearing in mind.
- **Master being rejected by the slave**—The slave AAA server may reject connection attempts from the master due to the master PC having several network adapter cards. This is because the slave can see the IP address of the wrong card, that is, it does not see the one configured in its network configuration. Either the second card can be removed, or another dummy AAA server (with the second IP address) can be added.
- **Secret value/shared key problems**—Both AAA servers must share the same secret key.
- **Proxy entries on slave overwritten**—If you use replication to update several distributed masters, each with its own proxy distribution table, you might see that the slave will keep on losing its proxy table. This is a misconfiguration, and can be resolved by unchecking the component **Distribution Table** on the tx/rx list.

- **Replication timeout**—After issuing the replication take-up request, the master waits up to 5 minutes before assuming that the slave died and reporting it as such. Should the slave be configured so that it uses RDBMS synchronization, it is possible that a large number of transactions could block the slave from accepting the replication before the master gives up. Try to avoid this type of setting.
- **Master CS ACS entry is missing on the slave server**—In the auth.log file of the secondary server, you may see the following message:

```
Worker 2 message from unknown host x.x.x.x - closing conn 41
```

  So, on the slave, configure the master CS ACS entry.

- **CS ACS's own server entry is missing from the server list**—When CS ACS is installed, its own entry is created as an AAA server. If you remove that, you may run into problems with the CS ACS replication, and the auth.log could display the following message:

```
"ERROR  Inbound database replication aborted - check IP address for this AAA
Server"
```

  This appears when the AAA server's list does not contain the CS ACS machine itself. You need to investigate further the Registry of both master and slave. After checking the Registry of both master and slave, you might find that the slave machine on the AAA Servers list has only the master configured and does not have its own definition. On the slave CS ACS, only MASTER (Master CS ACS) is configured as an AAA server (type=1) as shown in Example 13-7.

Example 13-7 *Registry on the Slave Server*

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv3.1\Hosts\MASTER]
"key"=hex:36,2e,70,77,e6,24,01,37,73,59,da,d9,b3,61,1d,d9,de,47,79,e2,28,b4,cd,\
  27,42,11,7d,a4,c9,6e,bd,85
"vendor"=dword:ffffffff
"protocol"=dword:00000063
"type"=dword:00000001
"direction"=dword:00000003
"acct Packet Filter"=dword:00000005
"network device group"=dword:00000006
"ip"=hex(7):31,00,37,00,32,00,2e,00,32,00,35,00,2e,00,35,00,37,00,2e,00,39,00,\
  31,00,00,00,00,00
"lastModified"=hex:50,7c,26,f8,fb,0d,c3,01
```

On the master server, there are two AAA servers configured : MASTER(the Master itself) and SLAVE(the Slave CS ACS) as shown in Example 13-8.

Example 13-8 *Registries of the CS ACS Servers*

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv3.1\Hosts\CPFACS01]
"key"=hex:eb,e5,07,d8,98,ad,fe,5b,f2,88,81,e8,83,1f,e0,00,36,d6,57,03,f7,fd,dc,\
  5b,61,89,6a,a6,a8,78,b9,5b
"vendor"=dword:ffffffff
```

Example 13-8 *Registries of the CS ACS Servers (Continued)*

```
"protocol"=dword:00000063
"type"=dword:00000001
"direction"=dword:00000003
"acct Packet Filter"=dword:00000005
"network device group"=dword:00000000
"ip"=hex(7):31,00,37,00,32,00,2e,00,32,00,35,00,2e,00,35,00,37,00,2e,00,39,00,\
  31,00,00,00,00,00
"lastModified"=hex:80,06,62,dd,e5,07,c3,01

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv3.1\Hosts\HQACS02]
"key"=hex:58,a5,28,70,6e,50,f6,80,64,7c,fe,1f,70,c1,b1,bb,8d,d7,0f,1f,7a,11,ac,\
  64,86,b3,4a,c9,a5,37,db,a4
"vendor"=dword:ffffffff
"protocol"=dword:00000063
"type"=dword:00000001
"direction"=dword:00000003
"acct Packet Filter"=dword:00000005
"network device group"=dword:00000006
"ip"=hex(7):31,00,37,00,32,00,2e,00,32,00,35,00,2e,00,35,00,37,00,2e,00,39,00,\
  32,00,00,00,00,00
"lastModified"=hex:c0,be,de,ab,fb,0d,c3,01
```

Add a profile of the slave CS ACS to the slave CS ACS AAA Server's list to fix the problem.

- **Bi-directional replication between two CS ACS Servers**—Bi-directional replication is not supported. If you configure the bi-directional replication, you will see messages like the one in Example 13-9 in the auth.log file and the replication will fail. So avoid configuring bidirectional replication.

Example 13-9 *Auth.log Output for Bidirectional Replication*

```
03/22/2005      21:26:19        ERROR   Inbound database replication from ACS
'dumb' denied
03/22/2005      21:36:36        INFO    Outbound replication cycle starting...
03/22/2005      21:36:42        ERROR   ACS 'dumb' has denied replication request
```

- **NAT or Firewall device between the replication partners**—If there is a Network Address Translation (NAT) or firewall device between the replication partners, you may see the following message on the auth.log

  ```
  denied - shared secret mismatch
  ```

  From CS ACS version 3.1 and above, the IP address is embedded in the data and used as part of the server verification process. Hence, if the NAT device changes the source IP of the server, replication no longer works. To get around the problem, you may want to configure the firewall or NAT device so that it keeps the same source IP address. In addition to taking care of the NAT issue, be sure to allow TCP/2000 for the communication to take place.

- **Replication is not working for some components**—A master CS ACS has a **dirty** flag for each replication component. If no data changes on the master between replication cycles, nothing is replicated. To see which components are being replicated, be sure that **user.dat, user.idx,** and **varsdb.mdb** are being transmitted. The users are listed in **user.dat**. The advanced settings for users and groups are in **varsdb.mdb**.
- **Slave server does not have enough space**—If you have a **10-MB** database that needs to be replicated to a slave CS ACS, there must be enough space to hold the compressed file set, you need space in temp during de-compress, and you need space for uncompressed files. For a **10-MB** database, **50-MB** should be comfortable.

Network Access Restrictions (NARs) Issues

Network Access Restrictions (NARs) allow you to define additional authorization conditions that must be met before a user can gain access to the network. Even though it is an authorization condition, NAR is indeed an authentication process.

Cisco Secure ACS supports two basic types of network access restrictions:

- IP-based restrictions in which the originating request relates to an existing IP address
- Non-IP-based filters for all other cases in which the automatic number identification (ANI) may be used

A non-IP-based NAR is a list of permitted or denied "calling"/"point of access" locations that you can employ in restricting an AAA client when you do not have an IP-based connection established. The non-IP-based NAR generally uses the calling line ID (CLI) number and the Dialed Number Identification Service (DNIS) number.

Configuration Steps

To illustrate the functionality of NAR, consider the following example. Table 13-4 shows how users belonging to a default group can connect via Router1. Users in Group1 can connect only via AP11 and Group2 users get access via Router2 and AP11.

Table 13-4 *Configuration Metric*

Group	User	Router1	Router2	AP11
Default	Laci	Pass	Fail	Fail
Group1	Magi	Fail	Fail	Pass
Group2	Torri	Fail	Pass	Pass

This can be accomplished in several ways: using per "User defined Network Access Restriction" and using "Shared Profile Component for NAR", whereas all NAR is applied on Group-Settings.

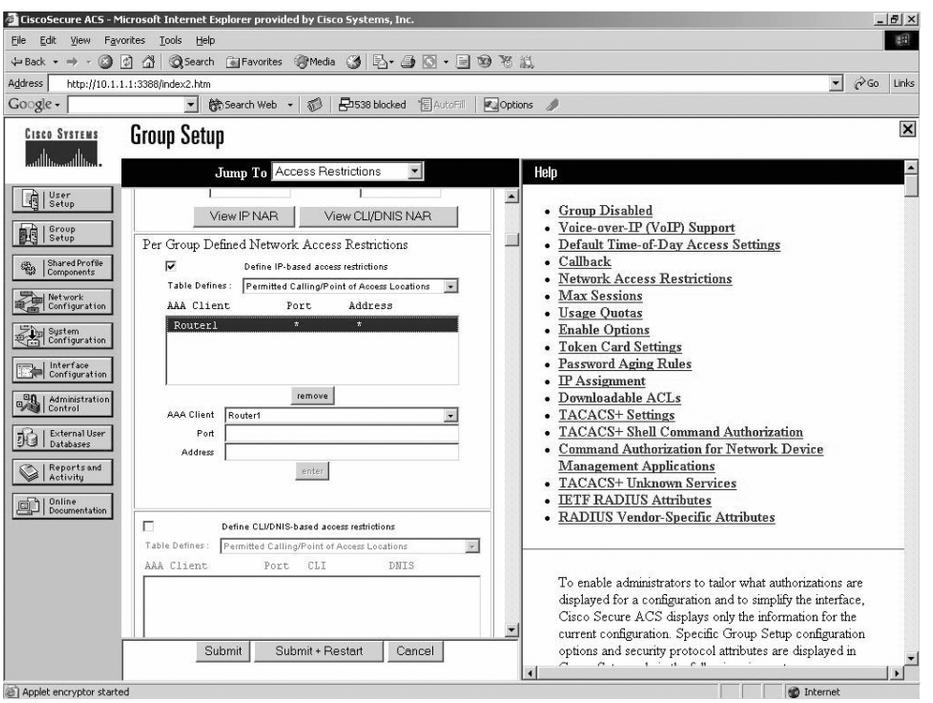
The following are the configuration steps for NAR:

Step 1 Define Router1, Router2, and AP11 as AAA client under AAA client, if not defined already.

Step 2 Define users listed in Table 13-4 and map them to corresponding groups.

Step 3 Go to each group's settings and under **Access Restrictions**, define the parameters as shown in Figure 13-10 for all three devices such as Default Group, which allows only Router1.

Figure 13-10 *NAR Configuration for Group*



Step 4 If Shared Profile components is the component that is used instead, then from Navigation, click on **Shared Profile Component**, and define three NARs: NAR-AP, NAR-router1, and NAR-router2 in a manner similar to that shown in Figure 13-11 for Router1. The name of the NAR is NAR-router1.

Step 5 Now apply the NAR defined in Step 4 on all three groups under network access restrictions in a manner similar to that shown in Figure 13-12, which is configured for Default Group.

Figure 13-11 *Shared Profile Component for NAR*

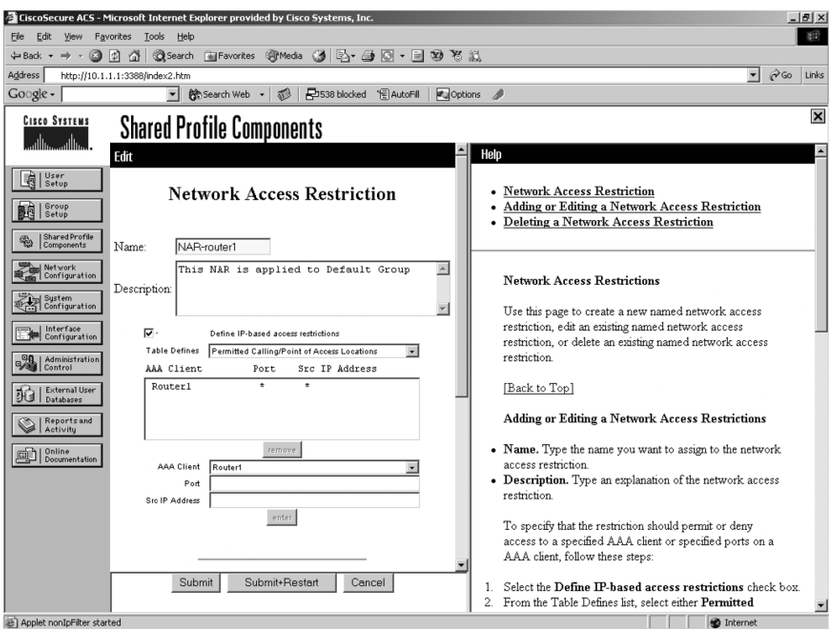
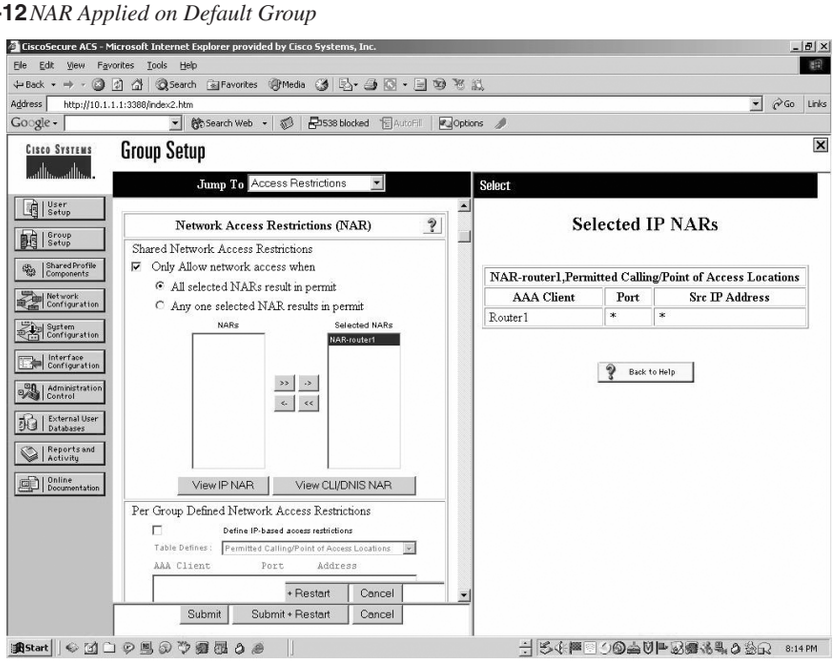


Figure 13-12 *NAR Applied on Default Group*



NOTE This setup can also be extended to use Network Device Groups (NDG). Configuration steps are exactly the same, but instead of selecting NAS, select NDG.

Troubleshooting Steps

The best way to troubleshoot the NAR issues is to use Failed Attempts or Passed Authentications reports to understand why access was or was not granted to a certain user. Usually, the caller ID, network access server (NAS) port, and NAS IP address fields are available and can be used to debug the session. When the reason for acceptance or denial is unclear, you can add the Filter Information field to these reports (both to Failed Attempts and Passed Authentications). This field will provide additional data. However, remember that you must use the Shared Profile Component (SPC) NARs configuration to get this additional information. With traditional NARs, it is hard to find the cause of acceptance or denial, as the first message (No Filter Activated) always appears regardless of the results. For additional details, look at the **RDS.log** or **TCS.log** and see how the packet is coming to the CS ACS Server from NAS and if it is getting forwarded to the **CSAuth** service, which shows the information on **auth.log**.

Example 13-10 shows the auth.log file for successful authentication.

Example 13-10 *Snippet of auth.log File Shows NAR Passing*

```
03/22/2005,18:41:21,Authen OK,laci,Default Group,10.0.0.2,66,10.0.0.171,,,,,,All
Access Filters Passed.,,router1,,,No,laci,cisco,,,
03/22/2005,18:42:08,Authen OK,torri,Group 2,10.0.0.2,66,10.0.0.172,,,,,,Access
Filter NAR-router2 from Group 2 permitted on Filter Line: 'router2 (Port=*) (IP=*)'.
This is sufficient to satisfy an 'Any Selected' SPC NAR
config.,,router2,,,No,torri,cisco,,,
03/22/2005,18:42:59,Authen OK,magi,Group 1,0040.9638.8e9a,99,10.0.0.1,,,,,,All
Access Filters Passed.,,ap11,,,No,magi,cisco,,,
03/22/2005,18:43:10,Authen OK,torri,Group 2,0040.9638.8e9a,99,10.0.0.1,,,,,,Access
Filter NAR-AP from Group 2 permitted on Filter Line: 'ap11 (Port=*) (CLI=*)
(DNIS=*)'. This is sufficient to satisfy an 'Any Selected' SPC NAR
config.,,ap11,,,No,torri,cisco,,,
```

Example 13-11 shows the auth.log file for unsuccessful authentication.

Example 13-11 *Snippet of auth.log File Shows NAR Failing*

```
03/22/2005,18:41:39,Authen failed,magi,Group 1,10.0.0.2,User Access
Filtered,,,66,10.0.0.171,Access Filter NAR-AP from Group 1 denied on Filter Line:
'* (Port=*) (IP=*)'. This is sufficient to reject an 'All Selected' SPC NAR
config.,,,,,,,,router1,,,,No,magi,cisco,,,
03/22/2005,18:41:44,Authen failed,torri,Group 2,10.0.0.2,User Access
Filtered,,,66,10.0.0.171,No Access Filters
Passed.,,,,,,,,router1,,,,No,torri,cisco,,,
03/22/2005,18:41:57,Authen failed,laci,Default Group,10.0.0.2,User Access
Filtered,,,66,10.0.0.172,Access Filter NAR-router1 from Default Group Did not permit
any criteria. This is sufficient to reject an 'All Selected' SPC NAR
config.,,,,,,,,router2,,,,No,laci,cisco,,,
```

continues

Example 13-11 *Snippet of auth.log File Shows NAR Failing (Continued)*

```
03/22/2005,18:42:03,Authen failed,magi,Group 1,10.0.0.2,User Access
Filtered,,,66,10.0.0.172,Access Filter NAR-AP from Group 1 denied on Filter Line:
'* (Port=*) (IP=*)'. This is sufficient to reject an 'All Selected' SPC NAR
config.,,,,,,,,router2,,,,No,magi,cisco,,,
03/22/2005,18:42:45,Authen failed,laci,Default Group,0040.9638.8e9a,User Access
Filtered,,,97,10.0.0.1,Access Filter NAR-router1 from Default Group denied on Filter
Line: '* (Port=*) (CLI=*) (DNIS=*)'. This is sufficient to reject an 'All Selected'
SPC NAR config.,,,,,,,,ap11,,,,No,laci,cisco,,,
```

The following link contains some interesting and useful discussion about NAR and how to troubleshoot it efficiently:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_white_paper09186a00801a8fd0.shtml

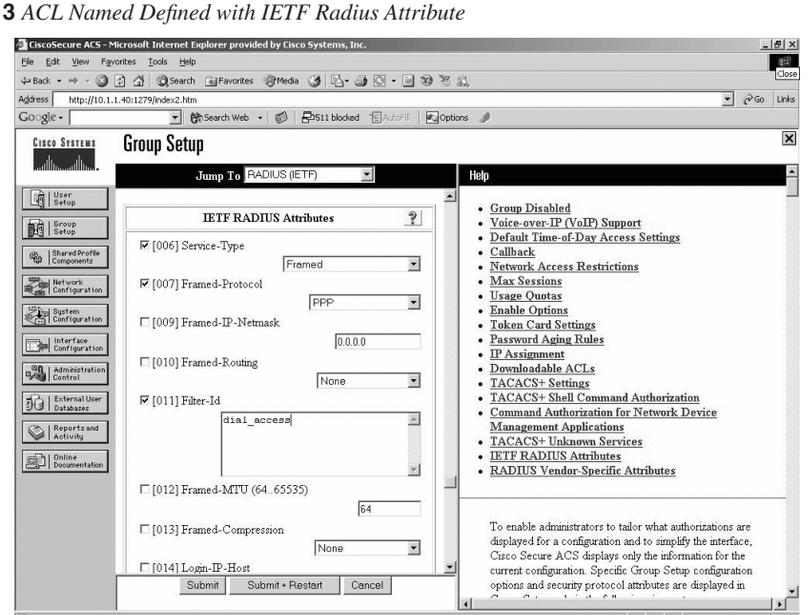
Downloadable ACL Issues

You can download ACL from the CS ACS Server to NAS to control which resources the user can access after getting access to the network. There are three ways to configure this, as described in the sections that follow.

Downloading ACL per User Basis Using Filter-id

With this option, you need to define the ACL in the NAS, and on the CS ACS server, and you need to define the name of the ACL using the Internet Engineering Task Force (IETF) RADIUS attribute 11 as shown in Figure 13-13.

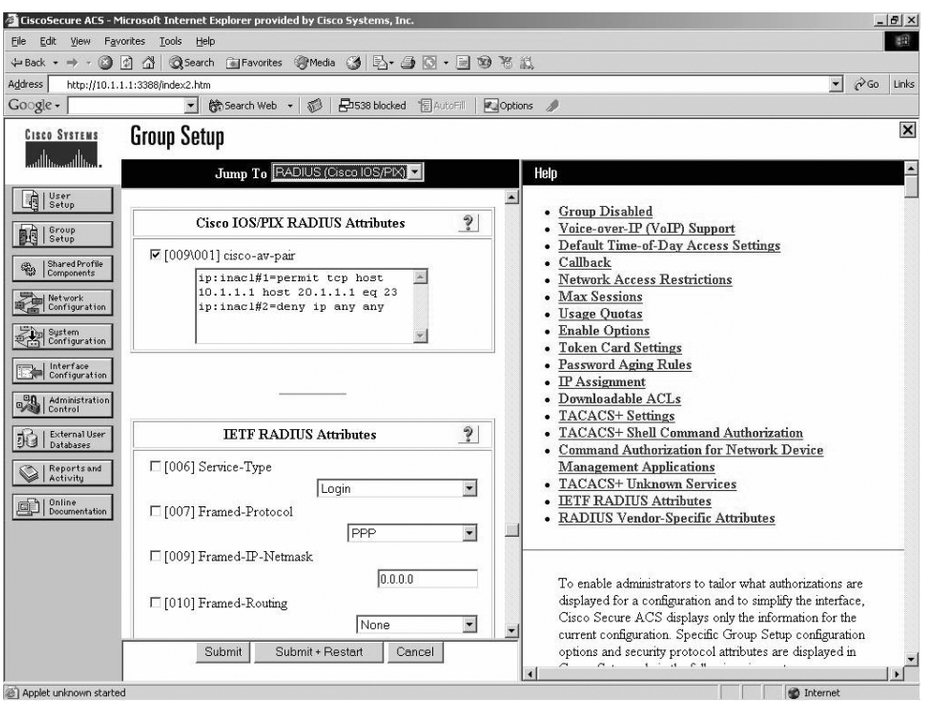
Figure 13-13 *ACL Named Defined with IETF Radius Attribute*



Using Cisco AV-Pair

On the NAS, you must have authorization turned on; otherwise, the AV pair will not be applied on the NAS. On CS ACS, you need to configure this under Group Profile. Click on **Group Setup > Select a Group** from drop-down, and then click on **Edit Settings**. In the Group Setup page, select **Cisco IOS/PIX RADIUS** from the **Jump To** drop-down. Then check "[009\001] cisco-av-pair" box, and define your ACL in the rectangle text box underneath as shown in Figure 13-14.

Figure 13-14 *ACL Defined Using Cisco AV Pair*



NOTE The variable x (ip:inacl#<x> . . .) must be defined with different numbers (for example 1, 2, 3 and so on) if multiple ACL entries are defined in the ACL. This ensures the order of the ACE in the ACL when downloaded to the NAS. If the same number is used for variable x for multiple ACL entries, then it may work, but the order of ACL entries will not be maintained, which may cause unexpected problems.

Using Shared Profile Components

If you are running CS ACS 3.0 and 3.1, under the Shared Profile component, the only option available to download ACL is for the PIX Firewall, which is called "Downloadable PIX

ACL." From CS ACS version 3.2 and above, "Downloadable IP ACL" is available under "Shared Profile Components", which is supported by PIX firewall, VPN Concentrator 4.0 code and above, and IOS version 12.3T and above.

The following sequence of events occurs if ACLs via Shared Profile Components are used:

1. The first stage is to download the name and version of the ACL where the device validates it against the local ACL cache.
2. In the second stage, the device (if needed) requests the ACL content, where CS ACS uses **inacl** for downloading the ACL.

The following step-by-step example shows the user fred when the Shared Profile component ACL is configured.

Step 1 Access a request from PIX (initial user authentication).

```
User-Name[1] = "fred"
User-Password[2] = <whatever>
...
<Other attributes>
...
```

Step 2 Access an acceptance from CS ACS (authentication response and ACL set assignment).

```
AV-Pair[26/9/1] ="ACS:CiscoSecure-Defined-ACL=#ACSACL#-myAcl-
1e45bc4890fa12b2
...
<Other attributes>
...
```

Step 3 Access a request from PIX (initiation of ACL download).

```
User-Name = "#ACSACL#-myAcl-1e45bc4890fa12b2"
...
<Other attributes>
...
```

Step 4 Access a challenge from CS ACS (first ACL fragment returned—more to follow).

```
State[24] = "TBD"
AV-Pair[26/9/1] = "ip:inacl#1 = permit tcp any anyestablished"
AV-Pair[26/9/1] = "ip:inacl#2 = permit ip any any"
...
<ACLs 3..59>
...
AV-Pair[26/9/1] = "ip:inacl#60 = deny icmp 2.2.2.0 0.0.0.255
9.9.9.00.0.0.255"
```

Troubleshooting Steps

Most of the time, downloadable ACL issues arise from mis-configuration either on the NAS or on the CS ACS server. So, first you must always perform a sanity check on the

configuration, if there is any issue with downloadable ACL. Analyze **auth.log** and **RDS.log** files to find out what information CS ACS is sending to the NAS as reply attributes for authorization. Then look at the debug information on the NAS to see if the NAS understands the ACL that CS ACS is sending. Keep the following points in mind when you configure downloadable ACL:

1. Perform a sanity check on the configuration both on the NAS and CS ACS server.
2. Be sure to have the authorization turned on for the NAS; otherwise, even though CS ACS sends the ACL name or the ACL itself, NAS will not install it. In the authorization debug, you will see that ACL is downloading from CS ACS, but when you execute **show access-list** command, you will not see the ACL being installed.
3. If using filter ID to download only the ACL name to NAS, be sure that ACL is defined locally on the NAS first. Then be sure that the name of the ACL matches on both CS ACS and the NAS. Note that name is case sensitive.
4. When an AV pair is used to download ACL, be sure to define the ACL entries with different numbers to maintain the order of ACL entries.

Case Studies

This case study examines the csutil.exe, a very useful utility that comes with the CS ACS software. Csutil.exe is in the following location:

<ACS_install_directory>\utils\

For example, C:\Program Files\CiscoSecure ACS v3.2\utils\

The command syntax is as follows:

```
CSUtil.exe [-q] [-c] [-d] [-g] [-i filename] [[-p] -l filename] [-e - number] [-b
filename] [-r filename] [-f] [-n] [-u] [-y] [-listUDV] [-addUDV slotfilename] [-
delUDV slot]
```

To run this utility, some options require you to stop the services. To do this, use the **net stop** command. Example 13-12 shows the **CSAuth** service stopped with the **net stop** command.

Example 13-12 *Stopping the CSAuth Service*

```
C:\> net stop CSAuth
The CSAuth service is stopping.
The CSAuth service was stopped successfully.

C:\>
```

Csutil.exe has many options/arguments for different purposes. Table 13-5 summarizes the options.

Table 13-5 *Options Available for the csutil.exe Utility*

Arguments	Descriptions
-b	Back up system to a named file
-d	Export internal data to named file
-g	Export group information
-I	Import user or NAS information
-l	Load internal data from a named file
-n	Create/initialize the ACS database
-q	Run csutil.exe in quiet mode
-r	Restore system from a named file
-u	Export user information

Back Up and Restore the CS ACS Database

Database backup and restore can be accomplished from the GUI and by browsing to the System Configuration option. However, due to csadmin failure, GUI access may be unavailable. Besides, if performing backup/restore requires an external script, using csutil.exe is very handy. When performing the backup function, services will automatically be stopped, which means no user authentication occurs during the backup. You are prompted for confirmation. You may use the quiet mode to bypass this confirmation. The backup will contain the following information:

- User and group information
- System configuration

If a component of the backup is empty, a Backup Failed notice will be displayed for that component only. To uninstall or upgrade, copy the backup file to a safe location; otherwise it will be removed. The command syntax for database backup is as follows:

```
C:\Program Files\CiscoSecure ACS v3.2\csutil -b filename
```

Example 13-13 shows the sample output of a database backup.

Example 13-13 *Sample Run of Database Backup*

```
C:\Program Files\CiscoSecure ACS v3.3\Utils>csutil -b backup.dat
CSUtil v3.3(2.2), Copyright 1997-2004, Cisco Systems Inc
All running services will be stopped and re-started automatically.
Are you sure you want to proceed? (Y or N)(Y)
Done
C:\Program Files\CiscoSecure ACS v3.3\Utils>
```

If you restore the CS ACS database, services will automatically be stopped. You can restore user and group information or system configuration or both. Note that you can restore

data only to the same version of CS ACS as the backup file, which means that this is not a system upgrade path. The following is the syntax used for database restore:

```
C:\> csutil -r [users|config | all] filename
```

Example 13-14 shows an example of database restore.

Example 13-14 *Sample Run of Database Restore*

```
C:\Program Files\CiscoSecure ACS v3.3\Utils>csutil -r all backup.dat
CSUtil v3.3(2.2), Copyright 1997-2004, Cisco Systems Inc
Reloading a system backup will overwrite ALL current configuration information
All Running services will be stopped and re-started automatically.
Are you sure you want to proceed? (Y or N)(Y)
CSBackupRestore(IN) file C:\Program Files\CiscoSecure ACS v3.3\Utils\System Back
up\CRL Reg.RDF not received, skipping..
Done
C:\Program Files\CiscoSecure ACS v3.3\Utils>
```

Creating a Dump Text File

A dump text file contains only the user and group information. This is useful for troubleshooting user profile issues. Cisco support may be able to load a dump file from your dump file to view user configuration to troubleshoot any possible configuration issue. Before creating a dump file, you need to manually stop the CSAuth service with the following command:

```
C:\> net stop CSAuth
```

Note that no user authentication takes place while the service is stopped. You must start the service manually with **net start CSAuth** once you are finished creating the dump. Command syntax to create dump file is as follows:

```
csutil -d filename
```

Example 13-15 shows a sample run of the creation of a dump file.

Example 13-15 *A Sample Run of Dump Text File Creation*

```
C:\Program Files\CiscoSecure ACS v3.3\Utils>net stop CSAuth
The CSAuth service is stopping.
The CSAuth service was stopped successfully.


C:\Program Files\CiscoSecure ACS v3.3\Utils>csutil -d dump.txt
CSUtil v3.3(2.2), Copyright 1997-2004, Cisco Systems Inc
Done

C:\Program Files\CiscoSecure ACS v3.3\Utils>
```

To load the dump file into CS ACS, first stop the **CSAuth** service, which means that user authentication will be stopped during that time. Loading a dump file will replace existing data. You can use the **-p** option to reset password aging counters. The syntax to use for loading the dump file is as follows:

```
csutil -p -l filename
```

Example 13-16 shows a sample run of a creation of a dump.txt file.

Example 13-16 *Sample Run of Dump.txt File Creation*

```
C:\Program Files\CiscoSecure ACS v3.3\Utils>net stop CSAuth
The CSAuth service is stopping.
The CSAuth service was stopped successfully.


C:\Program Files\CiscoSecure ACS v3.3\Utils>csutil -p -l dump.txt
CSUtil v3.3(2.2), Copyright 1997-2004, Cisco Systems Inc
Loading a database dump file will overwrite the existing database.
Are you sure you want to proceed? (Y or N)Y

Initializing database...
Loading database from file...
Password aging counters will be reset
Done

C:\Program Files\CiscoSecure ACS v3.3\Utils>
```

User/NAS Import Options

This feature allows changes either online or offline, and allows updating of the CS ACS database with a colon-delimited file. The following are the actions available for user and NAS:

- Users: add, change, and delete
- NAS: add and delete

You must restart **CSRadius** and **CSTacacs** for changes to take effect.

The following are some of the important points about importing:

- The first line must contain ONLINE or OFFLINE.

  This determines if the CSAuth service needs to be stopped during this process.

- CSUtils cannot distinguish between multiple instances of an external database.

  CSUtil will use the first instance of an external database.

Import User Information

You can add users to the existing database with the entry shown in Example 13-17. This entry adds the user Joe to group 2 in the CS ACS database. It also points authentication for this user to the internal CS ACS database with a password of **my1Password**.

Example 13-17 *Adding a User to CS ACS*

```
ADD:Joe:PROFILE:2:CSDB:my1Password
```

To change the CS ACS profile for Joe, use the command shown in Example 13-18. This entry updates Joe to group 3 and points the password to the NT domain database.

Example 13-18 *Updating a User to CS ACS*

```
UPDATE:Joe:PROFILE:3:EXT_NT
```

The DELETE entry can be used to delete users as shown in Example 13-19.

Example 13-19 *Deleting a User from CS ACS*

```
DELETE:Joe
```

Import NAS Information

Use the entry shown in Example 13-20 to add an NAS to the CS ACS database. This entry adds the router named router1, using the shared secret of my1NAS. This NAS will use RADIUS.

Example 13-20 *Adding NAS*

```
ADD_NAS:router1:IP:10.10.10.10:KEY:my1NAS:VENDER:"RADIUS (Cisco IOS/PIX)"
```

If you need to delete a specific NAS, use the command shown in Example 13-21, which deletes NAS router1.

Example 13-21 *How to Delete a Specific NAS*

```
DEL_NAS:router1
```

You can also choose to run all the previously shown procedures using a single text file. Example 13-22 shows a sample text file that contains multiple actions for different users.

Example 13-22 *import.txt File Whose Content Can Be Imported Once*

```
OFFLINE
ADD:user01:CSDB:userpassword:PROFILE:1
ADD:user02:EXT_NT:PROFILE:2
ADD:chapuser:CSDB:hello:CHAP:chappw:PROFILE:3
ADD:mary:EXT_NT:CHAP:achappassword
ADD:joe:EXT_SDI
ADD:user4:CSDB:user4password
ADD:user5:CSDB_UNIX:unixpassword
UPDATE:user9:PROFILE:10
DELETE:user10
ADD_NAS:router1:IP:10.10.10.10:KEY:my1NAS:VENDOR:"TACACS+ (Cisco
IOS)":NDG:"California"
DEL_NAS:router2
```

Compact User Database

When you delete a user from the CS ACS database, the record is marked as deleted. You might need to compact the database to actually remove the "deleted records". Compacting the database addresses this issue. When you compact a database, it first dumps the data, then creates a new database, and finally imports all the data that was dumped earlier. The following is the syntax for compacting a database:

```
csutil.exe  -q -d -n -l
```

Example 13-23 shows the sample of database compact run.

Example 13-23 *Sample Database Compact Command*

```
C:\Program Files\CiscoSecure ACS v3.3\Utils>net stop CSAuth
The CSAuth service is stopping.
The CSAuth service was stopped successfully.


C:\Program Files\CiscoSecure ACS v3.3\Utils>csutil -q -d -n -l
CSUtil v3.3(2.2), Copyright 1997-2004, Cisco Systems Inc
Done

Initializing database....
Done

Initializing database...
Loading database from dump.txt...
Done

C:\Program Files\CiscoSecure ACS v3.3\Utils>
```

Export User and Group Information

Export User and Group Information may be useful for troubleshooting the configuration issue by Cisco support. You will need to stop CSAuth before exporting this information.

To export user information to users.txt, enter the following command:

```
csutil.exe -u
```

To export group information to groups.txt, enter the following command:

```
csutil.exe -g
```

Other features of CSUtil.exe include the following:

- Export Registry information to setup.txt.
- Decode CS ACS internal error codes.
- Recalculate Cyclic Redundancy Check (CRC) values for manually copied files.
- Import user-defined RADIUS vendors and VSA sets.

Common Problems and Resolutions

This section examines some of the commonly encountered problems that were not discussed earlier.

1. I am getting "Crypto Error" while trying to install/upgrade CS ACS. How do I fix this?

   Answer: Use an administrator account when performing the installation.

   Rename the **pdh.dll** file in the system32 directory.

   The problem lies in MS CryptoAPI settings. If you remove or customize Internet Explorer or install any security patches, the IE updates and security updates often distribute modified CryptoAPI files. Installing these can sometimes break existing CryptoAPI clients. You might also receive this error message if the CS ACS services are being run as another user (or were installed as another user) or if the file permissions to the CryptoAPI data do not permit access. If nothing has changed on IE, follow these steps:

   1. Uninstall CS ACS.
   2. Search the Documents and Settings folder for any files with **CiscoSecure ACS** in the file name; they will be in a user's **Application Data\Microsoft\Crypto\RSA folder**.
   3. If found, delete the CS ACS file.
   4. Search the Registry for a key named **CiscoSecure ACS v2.0 Container**.
   5. If found, delete the key. This removes any existing CiscoSecure CryptoAPI references. Now try to reinstall.

   Uninstalling CS ACS manually:

   1. Under **HKEY_LOCAL_MACHINE\SOFTWARE\CISCO**, delete the **Cisco\CiscoAAAvX** Registry tree.
   2. From the same location, delete the directory.
   3. Then go to Services applet and make sure none of the seven services for CS ACS are listed there.
   4. If the services are installed and show up in the service list, there are entries in the Registry for them. Search the Registry for **Cisco** and selectively delete the keys and values.

2. What can I do when my Registry of CS ACS is corrupted?

   Answer: It is a good idea to back up the Registry of Windows when it is clean, before even installing the CS ACS software, so that it can be imported back if the Registry is corrupted and the CS ACS needs to be reinstalled.

   Execute the **clean.exe** utility on the CS ACS CD.

3 What can I do when I get the following error when upgrading from an older to a newer version?

"The old installation folder appears to be locked by another application:
c:\Program Files\CiscoSecureACSv3.X
Please close any applications that are using any files or directories in this folder and re-run setup."

Answer: Get a **dump.txt**, uninstall, reinstall, and reconfigure NAS only if you have a small number of NASs. If you have a large number of NASs, this may not work.

Reboot the server to ensure that it is not locked up by other applications.

Are there any shared directories on the CS ACS machine?

If you are installing remotely via either VNC or "Terminal Services" or "Remote Desktop", try installing locally.

If you *must* install remotely, try installing by using **Control Panel > Add/Remove Programs** (then browse to setup.exe). This helps occasionally when using a terminal service connection.

If the problem still persists, download the **Filemon** utility from the following location and run it while the installation is getting the error.

http://www.sysinternals.com/ntw2k/source/filemon.shtml

Filemon captures all file activity and shows the error code, so you can see which particular file is causing trouble with the install shield. You may also find out which process is locking the file by using the **Handle** tool that can be downloaded from the following location.

http://www.sysinternals.com/ntw2k/freeware/handle.shtml

Killing the process and deleting the file may resolve the issue.

You may want to turn on the **Manage Log Directory** option under **System Config > Service Control** and **System Config > Logging > <all CSV logs>**. During an upgrade under some circumstances, this may fix the message stating that the folder is locked.

4 I am trying to upgrade a CS ACS that is installed under D: drive, but am having problems with space issues under C:. Why?

Answer: When performing a clean install, the Installation Wizard gives you the option of choosing the location in which you want to install the CS ACS software. However, this option is not available for upgrades. For example, when you try to upgrade by running the new version of CS ACS setup.exe, the Installation Wizard

drops the new version on the C: drive. So, whenever the installation process finds a previous configuration and prompts the user to keep the existing database and configuration, you do not have the option of selecting an installation location. Whenever the installation process is clean and the user is not prompted to keep the existing database and configuration, you will have the option of selecting a different installation location. This might create a problem if the C: drive is low in space. To get around the problem, the only option available is to create more disk space on the C: drive.

5 What's the minimum CS ACS version requirement for MS-CHAP v2 support?

Answer: The minimum requirement is version CS ACS 3.0.

6 Is it possible to force the user to provide login credentials when trying to launch the CS ACS Windows Admin GUI from the CS ACS Server itself locally?

Answer: Yes, it is possible. If you have **allowAutoLocalLogin** set to 1 in the Registry, you do not need to provide login credentials. So to force the user to provide login credentials if accessing CS ACS locally, change value for **allowAutoLocalLogin** to 0. To find out this key, you can search using this keyword.

7 If I lose the admin password to get into the GUI, how can I recover it?

Answer: By default, the CS ACS does not require you to provide login credentials if you are accessing it locally from the CS ACS server itself. However, if you force local login by un-checking the **Allow automatic local login** check box under **Administration Control > Session Policy** (this essentially sets the **allowAutoLocalLogin** in the Registry to 0 as discussed in question 6), and you lose the admin password, the best solution is to set the **allowAutoLocalLogin** to **1**. Then you can log in to the CS ACS locally from the server and add or modify administrators. The Registry location for the **allowAutoLocalLogin** is as follows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv3.3\CSAdmin\Security
```

8 Under the **Security** key, you can modify **allowAutoLocalLogin** by right-clicking and choosing **modify**. How can I set up a default NAS so that I do not have to create multiple AAA clients on CS ACS for every NAS that uses the same shared secret key?

Answer: You can add a default NAS in the NAS configuration area by leaving the host name and IP address blank. Put in only the key. Click **Submit**, and you will see NAS **others** and ***.*.*.***. Note that this works only for TACACS+, not RADIUS.

9 Which registries pertain to the CS ACS Server?

Answer: HKEY_local_machine\software\cisco\CiscoAAAv3.x and HKEY_local_machine\software\cisco\CiscoSecureACSv3.x

10 I want to use TACACS+ for router management and one RADIUS for dial on the same CS ACS Server. Is it possible? How?

Answer: Yes, it is possible. Just configure the NAS method lists for login authentication with TACACS+ and PPP authentication with RADIUS. On CS ACS, just define two AAA clients with the same IP, different names and different protocols (TACACS+ and RADIUS).

11 How do I capture debugs for Cisco to use to troubleshoot my issue?

Answer: On CS ACS GUI, select **System configuration > Service control** and **set logging to FULL**. Then in the section underneath, select **Manage Logs** so that they do not grow out of control. Then wait until AAA fails again and the logs on the server are collected by running **cssupport.exe** from the command-line. This is found in the utils directory in the Cisco Secure ACS directory.

12 How do I find the exact release of Cisco Secure ACS?

Answer: There are two ways of checking:

First, when you bring up the browser, look for the following at the bottom of the page:

```
CiscoSecure ACS
!The following line indicates the release
Release 3.3(2) Build 2
Copyright ©2004 Cisco Systems, Inc.
```

The second way is to bring up a DOS prompt on the CiscoSecure ACS machine and run the following:

```
C:\Program Files\CiscoSecure ACS v3.3\Utils>CSUtil.exe
CSUtil v3.3(2.2), Copyright 1997-2004, Cisco Systems Inc

Usage: [-q] [-b <backup filename> ] [-c] [-d] [-e <number>] [-g] [-i <file>]
     [[-p] -l <file>] [-n] [-r <all¦users¦config> <backup file> ] [-s] [-u] [-y]
! Rest of the output it removed as irrelevant for this question.
C:\Program Files\CiscoSecure ACS v3.3\Utils>
```

The second option is better.

13 Can ACE server (SDI) and Cisco Secure ACS be installed on the same system?

Answer: Yes there is no problem with running both Cisco Secure ACS and the ACE server (SDI) on the same machine.

14 Do I need to have the SDI client installed?

Answer: When using the SDI database as an external database, it is necessary to install SDI ACE client on the same machine on which Cisco Secure ACS is running. Also note that it is a good practice to install SDI before installing Cisco Secure ACS.

15 Can we send accounting information to another system and also have a copy on the local system?

Answer: Yes this is possible and it is configured under **System configuration: Logging.**

16 Can CS ACS act as a proxy server to other servers?

Answer: Yes, CS ACS can receive authentication requests from the network access servers (NASs) and forward them to other servers. You need to define the other servers by going to the **Network Configuration > AAA Servers** section on the source. The source server is defined as a TACACS+ or RADIUS NAS on the target. Once those are defined, configure the Distributed System Settings in the source Network Configuration to define the proxy parameters.

17 What kind of web server and database does CS ACS use? Who provides patches for those two components?

Answer: CS ACS has its own proprietary database, which spreads over to multiple files. The CS ACS web server is also Cisco proprietary. If any vulnerability is found, Cisco provides the patches because, unlike other software, those components are Cisco proprietary.

18 How do I back up CS ACS?

Answer: You can back up CS ACS through the GUI using the System Configuration tab, or you can use the command-line interface (CLI). If you use the GUI, there is a backup of the users, groups, and Registry settings. If you use the CLI, to back up users and group information, use **$BASE\utils\csutil –d**. To back up users, groups and Registry settings, use **$BASE\utils\csutil -b**.

19 Can I use the backup utility on one CS ACS and then restore the information on another server?

Answer: No, the backup utility is intended to save the user, group, and Registry information from one CS ACS box and restore it to the same CS ACS box running the same version of software. If there is a need to clone a CS ACS box, replication is available instead.

If you need to copy only users and groups from one server to another, use the **csutil -d** command. The resulting dump text (.txt) file is then copied to the target box, and you can use the **csutil -n -l** command to initialize the database and import the users and groups.

20 Is domain stripping supported with CS ACS?

Answer: Yes, CS ACS does support domain stripping. This is useful when there is a combination of Virtual Private Dialup Network (VPDN) and non-VPDN users.

Domain stripping is also useful when the external NT database is used for authentication. The first time the users log in, the username is populated automatically in CS ACS. Since a user may come in as "DOMAIN_X\user" or as "user," names may appear in the CS ACS as "DOMAIN_X\user" or as "user," resulting in both entries in the database. The duplicate entries can be avoided by using domain stripping, wherein the prefix domain with the delimiter "\" can be erased to have a consistent database. You can set this up by going to **Network Configuration > Proxy Distribution Table**.

21 After successful installation of CS ACS, services are running. However, when I try to bring up the GUI, I get this error: "Invalid administration control." What should I do?

Answer: If you have proxy server configured on the browser, you will see this message. To work around the problem, disable the proxy server completely.

22 What is the limit of NASs that can be supported by CiscoSecure ACS for Windows?

Answer: There is no limit. The number simply depends on the number that the Windows Registry can hold, as the NAS information goes to Windows Registry. It is estimated that the Windows Registry can hold thousands of NASs. Note that, unlike users or groups information, NAS information does not go the CS ACS database.

23 Where does the CS ACS copy the configuration of the old CS ACS and how can that be useful if the upgrade fails?

Answer: When upgrade is performed from one version to another. The previous CS ACS version configuration is copied to the following hidden folder:

```
%systemroot%\Program Files\CiscoSecure ACS Configuration
```

If you run into a problem with an upgrade, the system can be purged of all information, such as the Registry, folders and so on. If you leave the saved configuration folder, the next installation will find this information and will try to import the configuration from the old settings. This may come to your rescue when an upgrade fails due to file permission problems and so on. So, you must not remove this folder.

24 How can I disable the users' option to change the password by using Telnet to access the router?

Answer: You can change the password after using Telnet to access the router and click **Enter** without entering any password. This behavior can be prevented with the following setting on CS ACS.

Step 1 Back up the local Registry.

Step 2 Go to Registry key

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv<your_version>\CSTacacs.
```

Step 3 Add a Registry value by highlighting **CSTacacs**, right-clicking and selecting **NEW-DWORD**.

Step 4 When the new key appears on the right-hand side of the window, type **disablechangepassword** into the new key window.

Step 5 The default value for the new key is 0, which allows users to change the password. Right-click on the new key, select **Modify**, and then change the key value to **1** to disable the ability to change the password.

Step 6 After adding this new key, restart the **CSTacacs** and **CSAuth services**.

25 When was PPTP (Point-to-Point Tunneling Protocol) with MPPE (Microsoft Point to Point Encryption) keying support introduced to Cisco Secure ACS for Windows?

Answer: This was introduced on CS ACS version 2.6.

26 How can I import a large number of NASs?

Answer: The procedure to bulk import NASs is similar to the import of users. The following flat-file is an example:

```
ONLINE
ADD_NAS:sam_i_am:IP:10.31.1.51:KEY:cisco:VENDOR:CISCO_T+
ADD_NAS:son_of_sam:IP:10.31.1.52:KEY:cisco:VENDOR:CISCO_R
```

The NASs may also be imported into a particular Network Device Group. The following flat-file is an example:

```
ADD_NAS:koala:IP:10.31.1.53:KEY:cisco:VENDOR:CISCO_R:NDG:my_ndg
```

27 What databases are supported for the synchronization?

Answer: CSV files and any ODBC-compliant database such as Oracle and MS SQL are supported.

28 With Cisco Secure you can force users to change their passwords after a given time period. Can you do this when you are using the Windows NT database for authentication?

Answer: This feature is available in all versions when you are using the Cisco Secure database for authentication. From version 3.0, support of Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) Version 2 and MS-CHAP Password Aging is available. This works with the Microsoft Dial-Up Networking client, the Cisco VPN Client (versions 3.0 and later), and any desktop client that supports MS-CHAP. This feature prompts you to change your password after a login attempt when the password has expired. The MS-CHAP-based password-aging feature supports users who authenticate with a Windows user database and is offered in addition to password aging supported by the Cisco Secure ACS user database. This feature has been added in CS ACS 3.0, but it also requires device/client support. Cisco Systems is gradually adding such device/client support to various hardware.

29 How can users change their own passwords?

Answer: Users can be notified of expiring Cisco Secure ACS database passwords on dial connections if the Cisco Secure Authentication Agent is on the PC. You can also use User Changeable Password (UCP) software, which runs with Microsoft IIS, once the users are in the network. When the users are on the network, they can point their browsers to the system where User Control Point (UCP) is installed and change their passwords.

30 My CS ACS "Logged in Users" report works with some devices, but not with others. What is the problem?

Answer: For the "Logged in Users" report to work (and this also applies to most other features involving sessions), packets should include at least the following fields:

- Authentication Request packet

  nas-ip-address
  nas-port

- Accounting Start packet

  nas-ip-address
  nas-port
  session-id
  framed-ip-address

- Accounting Stop packet

  nas-ip-address
  nas-port
  session-id
  framed-ip-address

Attributes (such as nas-port and nas-ip-address) that appear in multiple packets should contain the same value in all packets.

If a connection is so brief that there is little time between the start and stop packets (for example, HTTP through the PIX), then the report entitled "Logged-in Users" will not work either.

CS ACS versions 3.0 and later allow the device to send either nas-port or nas-port-id.

31 How are user passwords stored in CS ACS?

Answer: Passwords are encrypted using the Crypto API Microsoft Base Cryptographic Provider v1.0. This offers either 56-bit or 128-bit encryption, depending on how the server is set up. The default cipher will be RC4.

32 Can I change the default port for RADIUS and TACACS+ protocols on CS ACS?

Answer: Yes, you can, but it is strongly discouraged. RADIUS Protocol listens on UDP/1645 and UDP/1812 for Authentication & Authorization and UDP/1646 and UDP/1813 for accounting. The location for ports for RADIUS is as follows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv3.3\CSRadius
"AuthenticationPort"=dword:1812
"AccountingPort"=dword:1813
This can also be changed in the newer version:
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv3.3\CSRadius
AccountingPort = 1646
AccountingPortNew = 1813
AuthenticationPort = 1645
AuthenticationPortNew = 1812
```

You can change any of the values previously listed. TACACS+ protocol on CS ACS listens by default on TCP/49. You can change the TACACS+ port by editing attribute values of the proper key in the Windows Registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv3.3\CSTacacs
"Port"=dword:59
```

As mentioned before, it is strongly discouraged to change these default ports to something else.

33 I am unable to delete the users and some users seem to belong to multiple groups. How may I get around the problem?

Answer: Open up DOS prompt of CS ACS Server and type **$BASE\utils\csutil -q -d -n -l dump.txt**. Here "$BASE" is the directory where the software was installed. Issuing this command causes the database to be unloaded and reloaded to clear up the counters. Before performing this task, we strongly recommend that you back up the CS ACS database.

34 I cannot start services for RADIUS after re-installing the software a few times. The event error says that service was terminated with "service specific error 11".

Answer: Here are some possible reasons for encountering the problem:

- The most common problems occur when you run Windows with an unsupported service pack or there is software contention with another application. Check installation guide and the release notes for the supported OS and service pack.
- To check for port conflicts, go to the command line of the server and type **netstat -an | findstr 1645** and **netstat -an | findstr 1646** to see if any other

service is using these User Data Protocol (UDP) ports. If another service is using these ports, you will see something similar to the following:

```
UDP 0.0.0.0:1645 *:*
UDP 0.0.0.0:1646 *:*
```

- Microsoft Server services may not have been started. To check this, go to **Control Panel > Services** and ensure that the Server service options for **Started** and **Automatic** are selected.

35 When accessing CS ACS GUI through a firewall, the address for the server in the URL field changes from a global IP address to a local address. Why does this happen?

Answer: The global IP address does not change when you change to subsequent pages after the initial login from version CS ACS 3.0.

36 Can a user be in more than one group at a time?

Answer: No, a user cannot be in more than one group at a time.

37 Are the dynamically mapped users stored in cache replicated?

Answer: Yes. Dynamically mapped users are stored in cache in the same way as internal users. Those dynamic users simply never refer to the password fields and the group can be dynamic (mapped by the external authenticator). CS ACS replicates the group/user database with both internal and external users at the same time. You cannot do one type without the other, as replication simply performs remote file copies from master to slave.

Best Practices

The following are best practices for the CS ACS Server:

- Before CS ACS installation, back up the Windows Registries, so that if a new installation of CS ACS or upgrade is needed, and if the Registries are corrupted, you can restore the Registries without re-imaging the operating system.
- Before performing any upgrade, always back up the database either via Web or using CLI (csutil). Also perform regular scheduled backups depending on how often you make changes.
- Unless it is absolutely necessary, do not install any web server, FTP server, and so on, which may introduce vulnerabilities to the server. Follow the Windows Operating System (Windows OS) Security Guidelines to harden the Windows OS before installing CS ACS.
- To attain maximum availability, configure replication and schedule replication at least once in a day (the scheduling depends on how many changes are made to the server).

- Protect the CS ACS Server from malicious viruses or worms by using Enterprise Anti-Virus Software and host-based IDSs (CSA Agent for example) and Personal Firewall.
- If you have a small LAN environment, then put the CS ACS on your internal LAN and protect it from outside access by using a firewall and the NAS. For high availability, configure database replication to a secondary CS ACS as a backup. However, if you have a large enterprise network, which is geographically dispersed, where access servers may be located in different parts of a city, in different cities, or on different continents, a central ACS may work if network latency is not an issue. But connection reliability over long distances may cause problems. In this case, local ACS installations may be preferable to a central server. If you want to maintain the same database for all the CS ACS servers, database replication or synchronization from a central server may be necessary. Using external user databases such as Microsoft Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) for authentication may complicate this even more. Additional security measures may be required to protect the network and user information being forwarded across the WAN. In this case, the addition of an encrypted connection between regions would be required.
- When replication is performed, the services are stopped on the server. Therefore, the server does not perform authentication. To eliminate this downtime, it is always a good idea to configure on the authentication device for failover. To clarify this, assume that you have one CS ACS in the U.S. replicating to a second CS ACS in Canada. Configuring the authenticating devices to try the U.S. and then Canada may not be the best plan. You might consider installing a second local server (in the U.S.) and replicating from the U.S. master to the U.S. slave. The U.S. slave could then replicate to the Canada slave.