Cisco Secure Access Control Server Version 2.6 External ODBC Authentication

Abstract

This paper presents concepts and configuration issues in deploying Cisco Secure Access Control Server (ACS) for Windows 2000 and NT servers to authenticate users against an external open database connectivity (ODBC) database. This paper also describes configuring a relational database management system (RDBMS) with ODBC and the Cisco Secure Access Control Server, testing and troubleshooting the configuration, and sample Structured Query Language (SQL) procedures.

Introduction

Cisco Secure ACS for Windows 2000 and NT servers enable users to authenticate against external databases in preference to their internal databases. This allows a Cisco Secure ACS installation to "back end" onto a variety of authentication sources, including Windows NT/2000, Novell Directory Services (NDS), Lightweight Directory Access Protocol (LDAP), various token-card servers, and ODBC databases.

This feature is commonly referred to as "unknown user authentication" because when the external database is configured, you do not need to manually enter a user record into the database of the Cisco Secure ACS. When it receives a request to authenticate a user who is not in the internal database, the Cisco Secure ACS attempts to authenticate the user against each configured external database until either a matching user ID is found in a database or all databases have been tried. If a result is positive, the Cisco Secure ACS creates a "cached" record internally so that next time it can authenticate directly to the appropriate external database[1].

The ODBC external authenticator allows ACS to integrate with your RDBMS user database by defining the interface to a stored SQL procedure. This procedure, implemented by you, returns basic authentication pass/fail data back to the Cisco Secure ACS. Cisco Systems provides the template or "stub" procedure, but only you can complete it because the procedure must interact with one system or more within your organization.

In addition to authenticating the user, the SQL procedure might return the number of the Cisco Secure ACS group to which the user is assigned. The Cisco Secure ACS then applies the authorization and profile data of this group to the user before the requested service is granted.

The Cisco Secure ACS uses a System Data Source Name (System DSN) configured locally in the ODBC32 Control Panel applet to access the stored SQL procedure.

1. The user's credentials are not stored internally.

General Security Issue

While there are various schemes of password encryption/obfuscation used among a network client, network access server (NAS), and access control server (ACS), between ACS and the RDBMS backend there are only mechanisms provided by the ODBC driver. If the RDBMS resides on a separate computer, unencrypted SQL traffic may be traveling over the network. The user should check the security of network ODBC connections with the ODBC driver vendor and take appropriate steps to secure the network segment over which the traffic will flow.

Authentication Protocols Supported

The Cisco Secure ACS supports the following authentication protocols via ODBC external authentication:

- PAP
- CHAP
- MSCHAP/MPPE
- ARAP

There are configuration implications between the PAP and CHAP/ARAP protocols. These are discussed in later sections.

Cisco Secure ACS Group Mapping

ODBC authentication has basic support for assignment of a Cisco Secure ACS group. The SQL procedure may optionally return a group number that corresponds to a group within the Cisco Secure ACS configuration. By default Cisco Secure ACS groups are named Default Group, Group 1, Group 2, and so on, where the Default Group is numeric group 0.

Cisco Secure ACS Software Versions

Cisco Secure ACS version 2.3(1) was the first version to support ODBC authentication. This feature did not significantly change in Cisco Secure ACS 2.4(1), except for the addition of Oracle support. In Cisco Secure ACS 2.5(1) and later, the MSCHAP authentication protocol supports MPPE.

Supported Database Vendors

Although several standards govern the use of SQL, the following two different methods return data from a stored SQL procedure:

- Recordset, as used by Microsoft SQL Server and Access
- Output Parameters, as used by Oracle

The Cisco Secure ACS configuration (detailed in later sections) must be set appropriately for the RDBMS being used. For RDBMSs other than Microsoft SQL Server, Microsoft Access, or Oracle, refer to the RDBMS documentation to find out which method is used.

RDBMS/ODBC Configuration

The first step in configuration is to create the stored procedure within the RDBMS.

Depending on the authentication protocols required, one or two procedures may be required. For basic PAP authentication, the Cisco Secure ACS uses the PAP SQL procedure where the username and password are passed to the procedure for authentication. The default name for the PAP SQL procedure is *CSNTAuthUserPAP*. For CHAP, MSCHAP and ARAP, the ACS has to receive from the procedure a copy of the user's clear text password to perform authentication. The default name for the CHAP/MSCHAP/ARAP SQL procedure is *CSNTExtractClearTextPw*.

The two procedures are defined in the following sections.

Variable/Field Types

Variable types mentioned below in the discussion of the SQL procedures may have one or more matching SQL types; hence, assume the following:

- *Integer*—SQL_INTEGER
- *String*—SQL_CHAR and/or SQL_VARCHAR

SQL Procedure Definitions

CSNTAuthUserPAP

Procedure Inputs

The procedure *CSNTAuthUserPAP* will take the following named input parameters[2, 3]:

- CSNTusername—String, 0...64 characters
- CSNTpassword—String, 0...255 characters

Procedure Results

Depending on the procedure type (recordset or parameter based), the SQL procedure returns the following named values as either a single row or a set of named output parameters:

CSNTresult	Integer, see section "Procedure Result Codes."
CSNTgroup	Integer, ACS group number for Authorization. 0xFFFFFFFF (-1) used to assign default. Values outside the 0...499 range are converted to the default.
CSNTacctInfo	String, 0...15 characters, 3rd party defined string added to subsequent accounting log file entries.
CSNTerrorString	String, 0...255 characters, 3rd party defined string written to the ACS service log file on error.

The fields *CSNTgroup* and *CSNTacctInfo* are processed on a successful authentication only. Similarly, CSNTerrorString is logged only after a failure, where result >= 4 (see "Procedure Result Codes").

CSNTExtractClearTextPw

Procedure Inputs

The procedure *CSNTExtractClearTextPw* takes the following named parameter:

- CSNTusername—String, 0...64 characters

Procedure Results

Depending on the procedure type (recordset or parameter based), the SQL procedure returns the following named values as either a single row or a set of named output parameters:

2. The parameter names are for guidance only and may be changed; however, the order may not—the username must precede the password parameter.
3. Passwords supplied via the RADIUS protocol are 0...128 characters

CSNTresult	Integer, see section "Procedure Result Codes".
CSNTgroup	Integer, ACS group number for Authorization. 0xFFFFFFFF (-1) used to assign default. Values outside the 0...499 range will be converted to the default.
CSNTacctInfo	String, 0...15 characters, 3rd party defined string added to subsequent accounting log file entries.
CSNTerrorString	String, 0...255 characters, 3rd party defined string written to the ACS service log file on error.
CSNTpassword	String, 0...255 characters, password for use by ACS for (MS)CHAP/ARAP authentication

The fields *CSNTgroup* and *CSNTacctInfo* are processed on a successful authentication only. Similarly, *CSNTerrorString* is logged only after a failure, where result >= 4 (see section "Procedure Result Codes").

Procedure Result Codes

One of the following result codes should be returned in the *CSNTresult* field.

- 0 (zero)—Authentication successful
- 1—Username unknown
- 2—Supplied password invalid
- 3—Unknown username or password invalid
- 4+—Internal procedure error - authentication not processed

Write your SQL procedures so that they decide among error code 1, 2, or 3 to indicate a failure depending on how much information is to be included in the failed authentication log files.

A return code of 4 (or higher) results in an authentication error event. Result codes in this range can be returned to indicate that it was not possible to process the authentication because of some fault condition. Such errors do not increment per-user failed attempt counters. Also, error codes are returned to the NAS so that it can distinguish between errors and failures and (if configured) fail over to a backup Cisco Secure ACS or alternate AAA server.

RDBMS Login For ACS

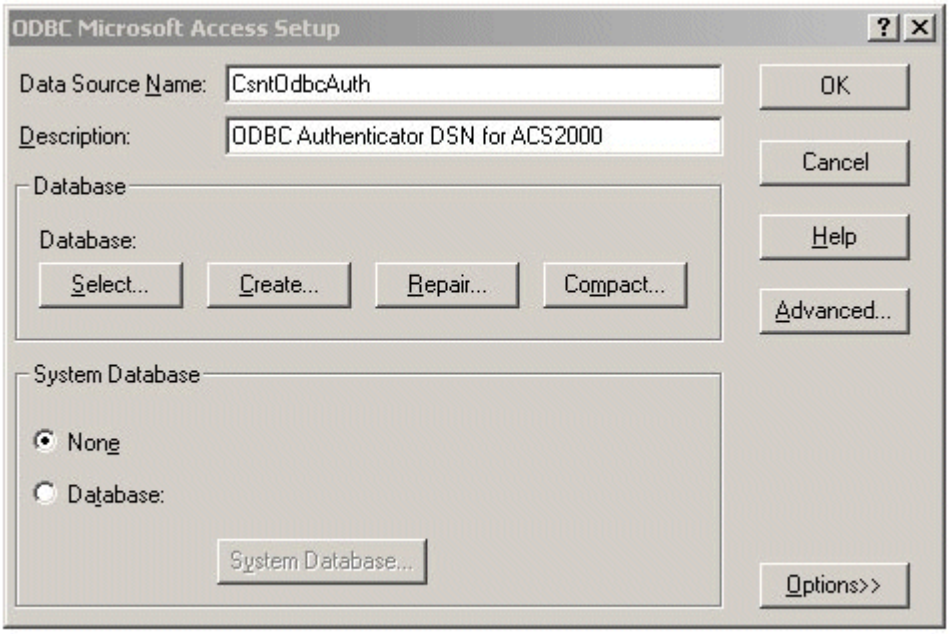
After you have implemented the SQL procedures in the RDBMS, access should be granted to the procedures that is sufficient to allow the Cisco Secure ACS to run them via the System DSN created in the following section. This is typically done by creating a login account for use by the Cisco Secure ACS. The account will require execution rights on these procedures and may need other rights/permissions depending on what actions the procedures perform. The account name and password are entered in the Cisco Secure ACS during its configuration process.

ODBC DSN

The Cisco Secure ACS communicates with the RDBMS using an ODBC driver running on the same server as the Cisco Secure ACS. With Windows 2000, this method is an integral part of the operating system; however, with Windows NT 4.0, it is not. The Cisco Secure ACS installer program automatically detects whether the ODBC driver is present. If the driver is not present, the installer displays an error message and you must exit the installation, install the ODBC driver, and restart the Cisco Secure ACS installation.

In Windows NT 4.0, the ODBC32 Data Source Administrator can be found in Control Panel. In Windows 2000, the ODBC32 Data Source Administrator is found on the Administrative Tools menu.

Figure 1 Microsoft Access ODBC Configuration Dialog Box



The ODBC DSN Administrator window has several tabs, including User DSN and System DSN. Because the Cisco Secure ACS runs as an NT service, it is important to create the DSN under the System DSN tab. The DSN specifies the RDBMS vendor (and hence which ODBC driver) and how to reach the database. For Microsoft Access, this is the location of the .mdb database file. For Microsoft SQL Server or Oracle, it may include the name/IP address of the computer on which the database resides. Detailed discussion about the configuration options is beyond the scope of this paper. For more information, please refer to your RDBMS documentation.

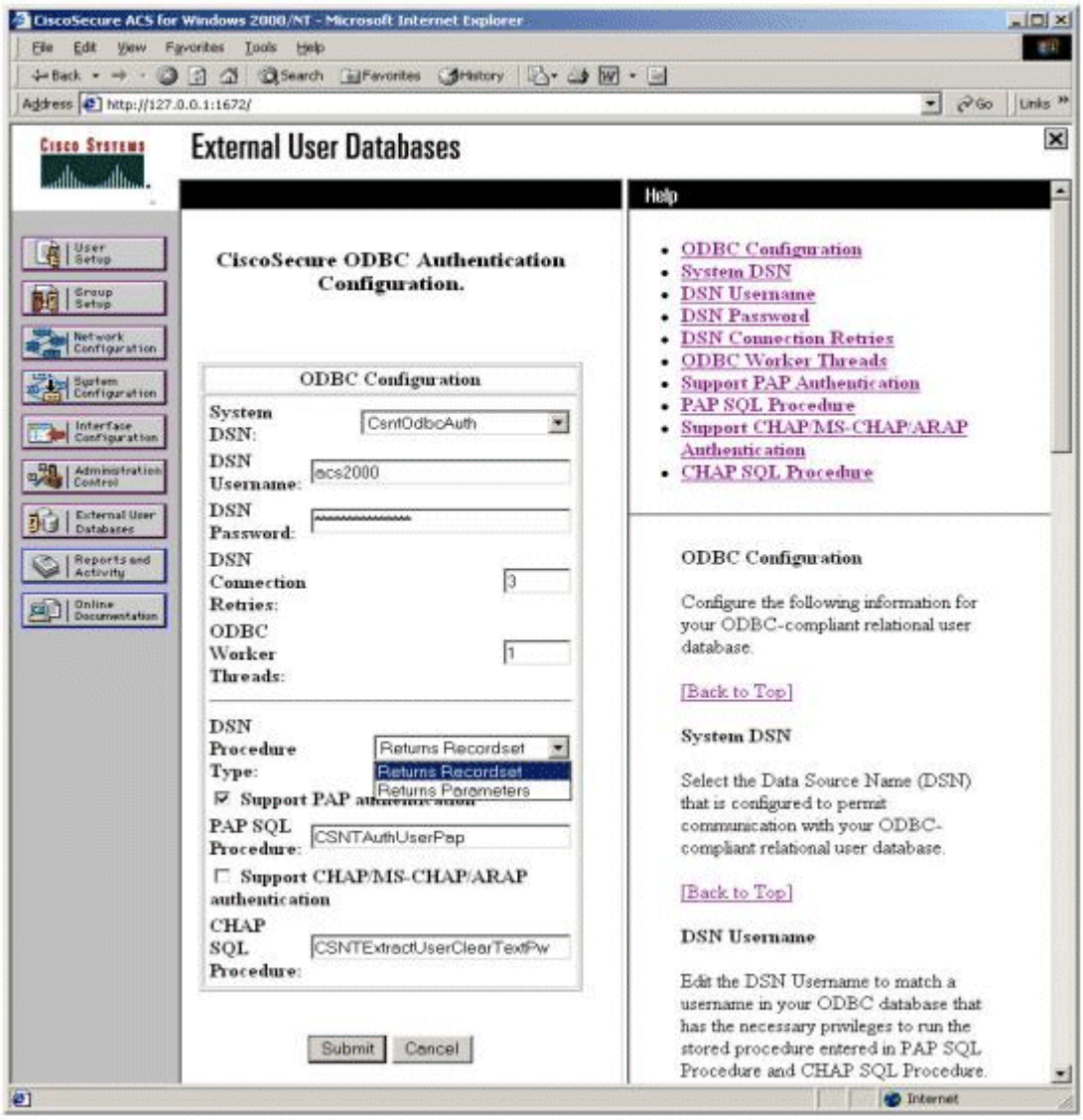
When configuring the Cisco Secure ACS, select the DSN name that is chosen during creation of the System DSN.

ACS Configuration

Create External DB Config

The first step in configuring the Cisco Secure ACS is to create an instance of the ODBC external authenticator. This is done by following the links through *External User Databases*, *Database Configuration*, and *External ODBC Database*. If no configuration exists, select *Create New Configuration*, type a configuration name in the text box, and click *Submit*. After you've created the configuration, or if a configuration already exists, click *Configure*.

Figure 2 ODBC External Database Configuration Page



On the ODBC External Database Configuration page, select the System DSN from the list. This should be the same System DSN configured previously in the ODBC32 Control Panel applet. If the correct DSN does not appear on the list, it was most likely created incorrectly as a User DSN instead of System DSN.

Next, enter the RDBMS account name and password into the DSN Username and DSN Password fields, respectively. These are the credentials created for the Cisco Secure ACS within the RDBMS that allow the Cisco Secure ACS to run the stored procedures via the System DSN.

The Connection Retries and ODBC Worker Threads boxes should be left at their default values unless there are connectivity or performance issues. The Connection Retries value specifies how many times the Cisco Secure ACS tries to connect to an ODBC data source upon failure. The ODBC Worker Threads value can be increased to create a set of pooled connections to

the RDBMS; however, this can only be increased from the default if the ODBC driver in use is "thread safe." For example, the Microsoft Access ODBC is not thread safe, and the Cisco Secure ACS may become unstable if more than a single thread is used. Microsoft SQL Server and Oracle ODBC drivers are thread safe. For other ODBC drivers, refer to documentation supplied with the driver.

The DSN Procedure Type defines whether the RDBMS returns recordset or parameter data from SQL procedures. If your database is Microsoft SQL Server or Access select *Returns Recordset*. If your database is an Oracle database, select *Returns Parameters*.

Lastly, use the check boxes to specify the authentication protocols to support, and then enter the SQL procedure name for each. The default procedure names appear in the procedure name text boxes; however, you can use any procedure name that matches the name of the procedure implemented in the RDBMS. At least one procedure must be implemented: PAP or CHAP/MS-CHAP/ARAP. If, for example, the PAP procedure is not implemented, the Support PAP authentications box should remain unchecked. Any PAP authentications will automatically fail with the message "Auth type not supported by External DB" logged in the Failed Attempts report.

When the ODBC External Database Configuration page is submitted, the Cisco Secure ACS attempts to connect to the DSN to check connectivity, but it does not check to ensure that the procedures specified in the procedure name text boxes exist in the RDBMS.

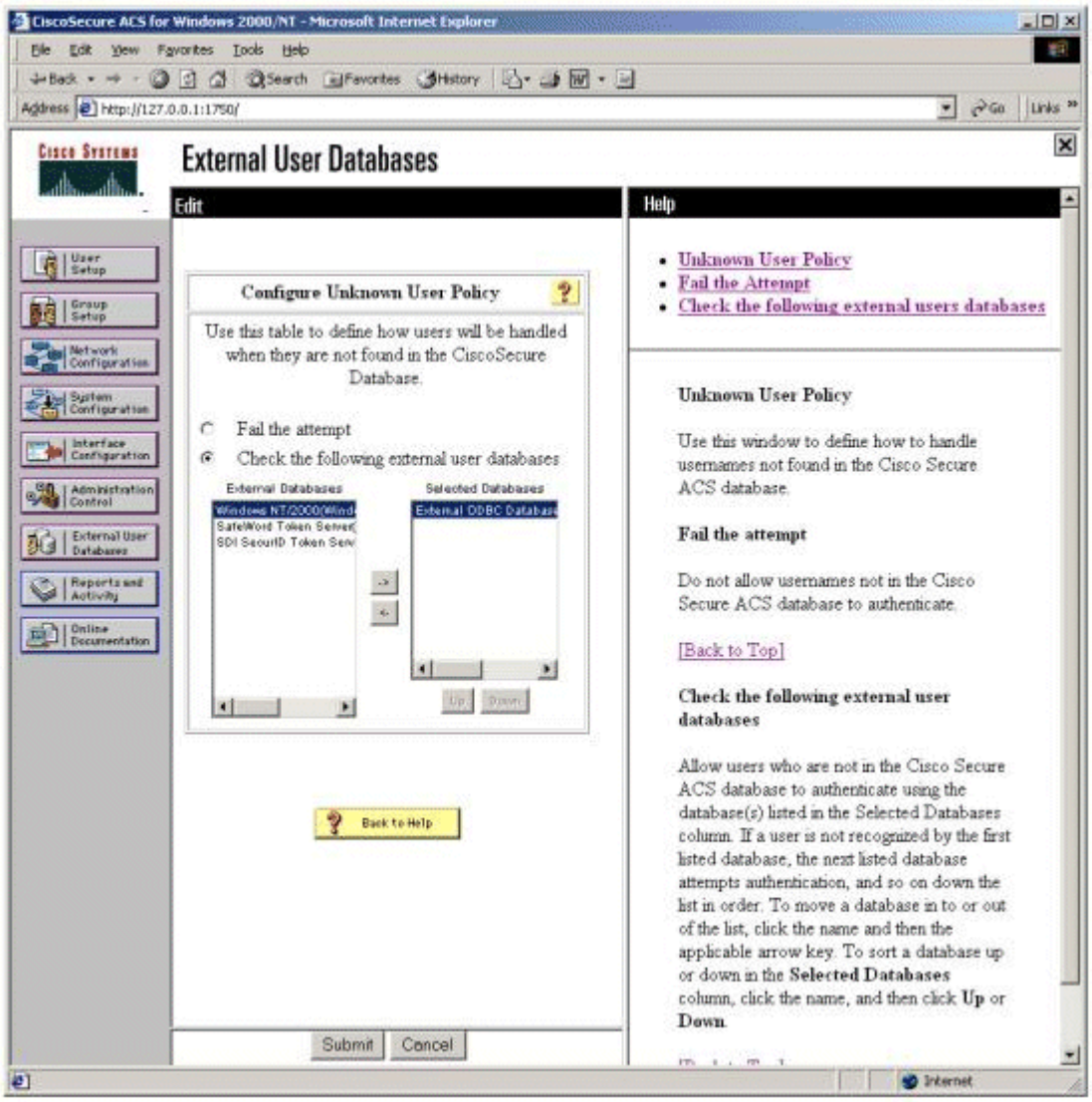
Default Group Mapping

If the SQL procedures are not coded to return a group assignment (or if they return an illegal value), the user is assigned to the default group for the ODBC External Database. Follow the links *External User Databases, Database Group Mappings*, and *External ODBC Database*, and then set the group to which the user is mapped. This value defaults to Default Group—that is, numeric group 0.

Set Unknown User Policy

After you configure the ODBC External Database, enable the Unknown User Policy in the same way as for any other external user databases. By default, the Cisco Secure ACS rejects any user that is not defined locally to its internal database. After Unknown User Policy is enabled, it defines which external databases are contacted and in which order. In the example below, only ODBC authentication has been selected from the list of available databases. Databases are not listed on this page until a configuration has been created.

Figure 3 Unknown User Policy Configuration Page



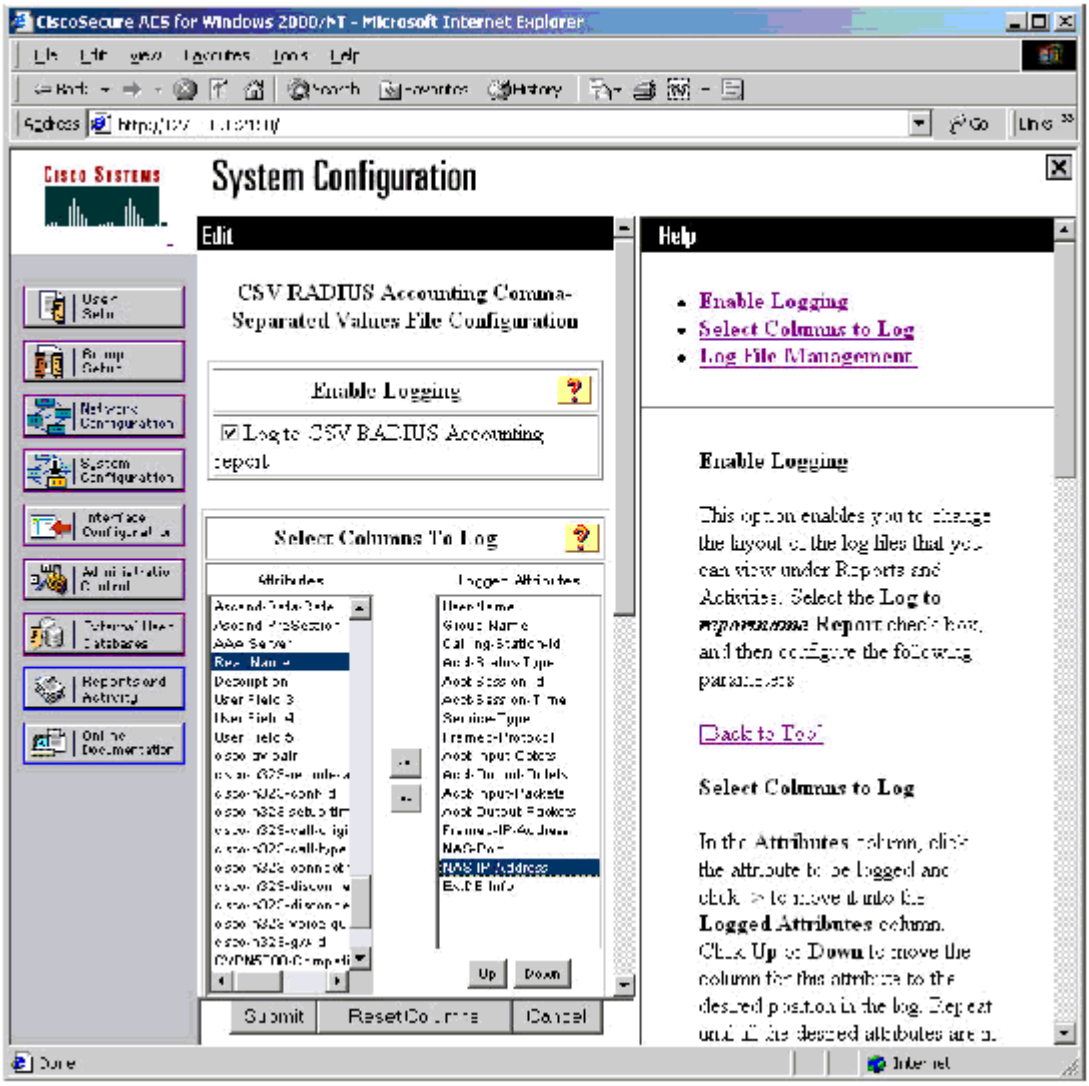
Add CSNTaccInfo to Reporting Logs

The procedure result field/parameter *CSNTacctInfo* can be used to include a string in some of the various reports generated by the Cisco Secure ACS, such as RADIUS and TACACS+ accounting CSV reports. The field can contain up to 15 characters and is intended to enable the RDBMS to include a short client-defined sequence of characters into reports such as a billing code or a user's department.

If the SQL procedures return a value that is to be included in a Cisco Secure ACS report, the report configuration must be changed from the default to include this field. To add the *CSNTacctInfo* to RADIUS accounting, from the main Cisco Secure ACS admin page, select *System Configuration* followed by *Logging.* Next, select either *CSV RADIUS Accounting* or

ODBC RADIUS Accounting, depending on which is desired. Under *Select Columns To Log*, scroll through the left window until the attribute *ExtDB Info* is visible. This is the attribute to which *CSNTacctInfo* is mapped. Select the attribute, and then click the right arrow to add this attribute to the report. Then, submit the page to save the new configuration.

Figure 4 CSV Radius Accounting Configuration



Testing and Troubleshooting the Configuration

There are three main aspects to achieving a working system:

1. Cisco Secure ACS/ODBC configuration
2. RDBMS SQL procedure interface
3. Customer-specific authentication SQL code

By using the stub procedures given in "Example SQL Procedures," the testing aspects 1 and 2 are simplified because the stub procedures allow these to be tested in isolation of aspect 3. These basic "just say yes" procedures enable testing of the Cisco Secure ACS configuration, the ODBC DSN, and the SQL procedure within the RDBMS without requiring that the procedures have been finished. You must write the final version of the procedures such that the appropriate databases, tables, columns, and rows are accessed to return the required data to the Cisco Secure ACS.

After successful authentications have been achieved using a basic procedure, the stub can be replaced by the real authentication SQL code and aspect 3 can be tested.

Failed Attempts Report

Most authentication failures result from the user incorrectly entering the credentials when connecting to the NAS. Such failed attempts are logged to the Cisco Secure ACS *Failed Attempts* report. Entries in this report have a *Message-Type* of *Authen Failed* and a failure code set to one of the values below.

Auth type not supported by External DB	Example: PAP request made when only CHAP has been configured
External DB user unknown	SQL proc returned user unknown
External DB user invalid or bad password	SQL proc returned user unknown or bad password
External DB CHAP password invalid	CHAP authentication failed
External DB MSCHAP password invalid	MSCHAP authentication failed
External DB ARAP password invalid	ARAP authentication failed
External DB not operational	ODBC connection is down. Refer to the CSAuth service log file for more detail
External DB reports error condition	An unknown error has occurred. Refer to the CSAuth service log file for more detail

Debugging the Cisco Secure ACS Service Log Files

During the initial testing period it is useful to enable maximal logging within the Cisco Secure ACS. To do so, select *System Configuration* and then *Service Control*. Under *Services Log File Configuration*, set the *Level of Detail* to *Full*, and then select *Restart*. This results in each Cisco Secure ACS service writing full diagnostic traces to its respective log file.

The service log file of most interest when you are debugging ODBC authentication is the CSAuth log. This is the central authentication service within the Cisco Secure ACS and is responsible for interaction with the external ODBC database also. If the Cisco Secure ACS was installed to its default location, the CSAuth logs are located in following:

\Program Files\CiscoSecure ACS v2.x\CSAuth\Logs

The active file is named `auth.log` while previous logs are named according to their creation dates, for example, `auth 2000-12-12.log`. Entries in the log are time stamped and relate to several Cisco Secure ACS features. To locate entries that are relevant to ODBC authentication, open the file with a text editor such as Notepad and search for instances of the string "External DB [ODBCAuthDll.dll]".

Successful PAP authentication Example

Attempting authentication for Unknown User 'testuser'

External DB [ODBCAuthDll.dll]: Authen PAP start for user [testuser]

External DB [ODBCAuthDll.dll]: Authentication OK for user [testuser]

If the group assignment field is out of range, the user will still authenticate; however, the default group will be used for authorization—which may lead to unexpected results. In which case the log would show the following:

External DB [ODBCAuthDll.dll]: Invalid group [654] for user [testuser], assigning default

Failed PAP Authentication Example

Attempting authentication for Unknown User 'testuser'

External DB [ODBCAuthDll.dll]: Authen PAP start for user [testuser]

External DB [ODBCAuthDll.dll]: Authen failed for user [testuser] (-1065)

UnConfigured Protocol Authentication Attempt

If a particular protocol has not been configured (for example, PAP), any attempt to authenticate will result in the following failure:

Attempting authentication for Unknown User 'testuser'

External DB [ODBCAuthDll.dll]: Authen PAP start for user [testuser]

External DB [ODBCAuthDll.dll]: PAP authentication not configured

ODBC/DSN Problem

If there are problems with either the DSN or the ODBC connection, look for messages such as the following:

External DB [ODBCAuthDll.dll]: CAuthenDb::Open—Data source name not found and no default driver specified

External DB [ODBCAuthDll.dll]: Failed to open DSN 'CiscoSecure ODBCAuth'

External DB [ODBCAuthDll.dll]: Error during authentication, closing DSN connection

RDBMS Reported Error

If an SQL procedures indicates an RDBMS/internal procedure error (with a return code of 4+ and an error string) the following would be logged:

Attempting authentication for Unknown User 'testuser'

External DB [ODBCAuthDll.dll]: Authen PAP start for user [testuser]

External DB [ODBCAuthDll.dll]: Authen error for user [testuser] <returned string>

Example SQL Procedures

CSNTAuthUserPAP

The examples given in this section are stubs that return a hard-coded data set for a successful authentication.

SQL Server

```
CREATE PROCEDURE CSNTAuthUser
  @username varchar(64), @password varchar(255)
AS
SELECT 0,1,"account info","No Error"
GO
```

Oracle

```
create or replace procedure CSNTAuthUserPap
 usernameIN  varchar2,
 passwordIN  varchar2,
 CSNTresultOUT int,
 CSNTgroupOUT varchar2,
 CSNTaccInfoOUT varchar2,
 CSNTErrorStringOUT varchar2
)
as
begin
  CSNTresult  := 0;
  CSNTgroup := 1;
  CSNTaccInfo :='account info';
  CSNTErrorString :='No Error';
end;
```

MS-Access

```
create a procedure CSNTAuthUserPap
SELECT tabUsers.CSNTresult, tabUsers.CSNTgroup, tabUsers.CSNTacctInfo, tabUsers.CSNTerrorString
FROM tabUser
WHERE (((tabUsers.CSNTusername)=[@CSNTusername]) AND ((tabUsers.CSNTpassword)=[@CSNTpassword]))
```

CSNTExtractClearTextPw

The examples given in this section are stubs that return a hard-coded data set for a successful authentication.

SQL Server

```
CREATE PROCEDURE CSNTExtractUserClearTextPw
@username varchar(64)
AS
SELECT 0,1,"account info","No Error","MyChapPassword"
GO
```

Oracle

```
create or replace procedure CSNTExtractUserClearTextPw
(
 usernameIN  varchar2,
 CSNTresultOUT int,
 CSNTgroupOUT varchar2,
 CSNTaccInfoOUT varchar2,
 CSNTErrorStringOUT varchar2,
 CSNTPasswordOUT varchar2
)
as
begin
  CSNTresult  := 0;
  CSNTgroup := 1;
  CSNTaccInfo :='account info';
  CSNTErrorString :='No Error';
  CSNTPassword    :='MyChapPassword';
end;
```


Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia
Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

SPS / 05/2001