



CHAPTER 4

Using RDBMS Synchronization to Create dACLs and Specify Network Configuration

This chapter describes how to configure ACS 4.2 to enable new RDBMS Synchronization features introduced with ACS 4.2.

For detailed information on RDBMS Synchronization, see “RDBMS Synchronization” in Chapter 8 of the *User Guide for Cisco Secure ACS, 4.2*, “System Configuration: Advanced.”

For detailed information on the accountActions codes to use with RDBMS Synchronization, see Appendix E of the *User Guide for Cisco Secure ACS, 4.2*, “RDBMS Synchronization Import Definitions.”

This chapter contains:

- [New RDBMS Synchronization Features in ACS Release 4.2, page 4-1](#)
- [Using RDBMS Synchronization to Configure dACLs, page 4-2](#)
- [Reading, Updating, and Deleting dACLs, page 4-12](#)
- [Updating or Deleting dACL Associations with Users or Groups, page 4-14](#)
- [Using RDBMS Synchronization to Specify Network Configuration, page 4-14](#)

New RDBMS Synchronization Features in ACS Release 4.2

ACS 4.2 provides enhanced support for RDBMS Synchronization:

- **Configuration of Downloadable ACLs (dACLs) for Specified Users and Groups**—You can specify dACLs by entering **permit ip** and **deny ip** commands in a comma-separated value (CSV) *accountActions* file. By using new account action codes that you include in the *accountActions* file, you can create a dACL that contains the commands that the text file specifies.

On ACS for Windows, you can perform dACL configuration from the RDBMS Synchronization page in the ACS GUI or by running the **CSDBSync** command.

On the ACS SE, you can perform dACL configuration from the RDBMS Synchronization page in the ACS SE GUI; or, connect to the ACS SE by using an SSH client and then running the **csdbsync -syncnow** command from the SSH shell.

- **Support for Creation, Reading, Updating, and Deleting of Single or Multiple AAA Clients Through RDBMS Synchronization**—With the capability to read AAA client data, you can export the AAA client list for a particular NDG, an AAA client list with a specified IP range, or the list of all AAA clients.

- **Remote Invocation of the CSDBSync Service on the ACS Solution Engine**—With ACS 4.2, you can run the CSDBSync service on a remote ACS SE, over an SSH connection.

Using RDBMS Synchronization to Configure dACLs

With ACS 4.2, you can use RDBMS Synchronization to set up downloadable dACLs and associate dACLs with specified Users or Groups.

To configure dACLs by using RDBMS Synchronization:

-
- Step 1** Enable RDBMS Synchronization and dACLs.
 - Step 2** Create a text file to define the dACLs.
 - Step 3** Code an *accountActions* CSV file to create the dACL, and associate a User or Group with the dACL.
 - Step 4** Configure RDBMS Synchronization to use a local CSV file.
 - Step 5** Perform RDBMS Synchronization in one of two ways:
 - From the ACS GUI.
 - By running the `csdbsync -syncnow` command from the Windows command shell or in an SSH connection with a remote ACS SE.
 - Step 6** View the dACL.
-

Step 1: Enable dACLs

To enable dACLs:

-
- Step 1** In the **Navigation Bar**, click **Interface Configuration**.
 - Step 2** Click **Advanced Options**.
The Advanced Options page opens.
 - Step 3** Check the **User-Level Downloadable ACLs** check box.
 - Step 4** Check the **Group-Level Downloadable ACLs** check box.
This enables assigning a dACL to a Group Name.
 - Step 5** Check the **RDBMS Synchronization** check box.
 - Step 6** Click **Submit**.
-

Step 2: Create a Text File to Define the dACLs

To create a text file to define dACLs:

-
- Step 1** Use a text editor of your choice to create a text file; for example Notepad.

Example 4-1 shows a sample text file.

Example 4-1 Sample Text File for Creating a dACL

```
[DACL#1]
Name = DACL_For_Troy
Description = Test_DACL_For_ACS_42
Content#1= content1
Definition#1#1= permit ip any host 192.168.1.152
Definition#1#2= permit ip any host 192.168.5.152
Definition#1#3= permit ip any host 192.168.29.33
Definition#1#4= permit ip any host 192.168.29.34
Definition#1#5= permit ip any host 192.168.9.50
Definition#1#6= permit ip any host 192.168.9.20
Definition#1#7= permit ip any host 192.168.7.20
Definition#1#8= permit ip any host 192.168.128.1
Definition#1#9= permit ip any 192.168.24.0 0.0.0.255
Definition#1#10= permit ip any 192.168.0 0.0.0.255
Definition#1#11= permit ip any 192.0.0.0 0.255.255.255
Definition#1#12= deny ip any 192.168.0.0 0.3.255.255
Definition#1#13= deny ip any 192.168.0.0 0.1.255.255
Definition#1#14= permit ip any any
```

Step 2 Code the information in the file as described in Table 4-1.

Table 4-1 Keywords for Creating a dACL By Coding a Text File

Keyword	Value
dACL number	The first line of the text file must specify the dACL number, enclosed in square brackets; for example, [DACL#n], where <i>n</i> is the number of the dACL. In Example 4-1, the first line specifies DACL#1, because the file specifies only one dACL.
Name	Specifies the name of the dACL that is created when you run CSDBSync .
Description	Specifies a short description of the dACL.
Content	Specifies the number of a content block that consists of definitions for access privileges associated with the dACL. This keyword has the format <code>Content#n</code> , where <i>n</i> specifies the number of the content block. The file shown in Example 4-1 has only one content block.
Definition keywords	Specify a series of permit IP or deny ip commands that ACS applies to Users or Groups to which you associate the dACL. Each Definition keyword has the format <code>Definition #n#n1</code> , where <i>n</i> is the number of the content block of definition keywords and <i>n1</i> is the number of each definition.

Step 3 Save the file:

- **ACS for Windows**—Save the file to a directory on the Windows machine that is running ACS.
- **ACS SE**—Save the file to a directory on an FTP server used with the ACS SE.

Step 3: Code an *accountActions* File to Create the dACL and Associate a User or Group with the dACL

To create an *AccountActions* CSV file to create a dACL and assign it to a User or Group:

- Step 1** Create a text file by using a text editor of your choice; for example, Notepad.
- Step 2** Code a statement to create a User or Group. For example, to create a User named *Troy*, who belongs to a Group named *Group*, and has an initial password of *ipassword*, code the following statement:

```
1,1,Troy,Group 5,100,ipassword,7/8/2008 15:00,0,,0
```

- Step 3** Code a statement to create a dACL. For example, to create a dACL called *DAcl_for_Troy* that is specified in a text file called *dACL_create.txt*, code the following statement:

```
2,1,,,385,C:\dACL_folder\dACL_create.txt,7/8/2008 15:00,0,,0
```

Action code 385 creates a dACL. The value directly after the action code specifies the directory path and filename of the text file that specifies the dACL. In the sample code shown in [Example 4-1](#) and [Example 4-2](#), this is the *dACL_create.txt* file.

The value after the directory path and filename must specify a timestamp for the file; for example, 7/8/2008 15:00.

- Step 4** Code a statement to associate the dACL with a specified User. For example, to associate the dACL *DAcl_for_Troy* with the User *Troy*, code:

```
3,1,Troy,,380,DAcl_For_Troy,7/8/2008 15:00,0,,0
```

The third value in this statement specifies the User (*Troy*) to associate the dACL with. Action code 380 associates dACL with the User, and the value immediately after the action code specifies the dACL name (*dACL_for_Troy*).

The value after the dACL name must specify a timestamp for the action; for example, 7/8/2008 15:00.

- Step 5** Save the file:
- **ACS for Windows**—Save the file to a directory on the Windows machine that is running ACS.
 - **ACS SE**—Save the file to a directory on an FTP server used with the ACS SE.

Sample *accountActions* CSV File

[Example 4-2](#) shows a sample *accountActions* CSV file.



Note

The default filename for the CSV is *accountactions.csv*. However, you can rename it.

Example 4-2 Sample *accountActions* CSV File

```
SequenceId,Priority,UserName,GroupName,Action,ValueName,DateTime,MessageNo,ComputerNames,AppId,Status
1,1,Troy,Group 5,100,ipassword,7/8/2008 15:00,0,,0
2,1,,,385,C:\dACL_folder\dACL_create.txt,7/8/2008 15:00,0,,0
3,1,Troy,,380,DAcl_For_Troy,7/8/2008 15:00,0,,0
```

Table 4-2 describes the accountActions codes used in Example 4-2 to add a User, create a dACL, and associate the dACL with a specified User or Group.

Table 4-2 Account Action Codes to Create dACLs and Assign Them to Specified Users or Groups

Action Code	Name	Required	Description
100	ADD_USER	UNIGN, V1	Creates a User (32 characters maximum). The variable <i>V1</i> is used as the initial password. Optionally, you can assign the User to a Group.
385	CREATE_DACL	VN	Use this action code to create a dACL. VN = <input_file_name> where <i>input_file_name</i> is a text file that contains definitions for dACLs. On ACS for Windows, this file resides in a directory on the Windows machine that is running ACS. On the ACS SE, this file resides on an FTP server used with the ACS SE. You can specify the absolute file path; for example: <i>C:\DACL\create_DACL_for_User_1.txt</i> for ACS for Windows. The dACL definition is ignored if it is already present, or contains an invalid definition, content name, content definition, or NAF name.
380	CREATE_USER_DACL	UNIGN, VN	This action code associates a specified dACL with a User or Group. The dACL name specified should be valid and present in ACS. The codes are: UN = valid Username GN = Valid Group name (optional) VN = dACL name. (This dACL must be defined in Shared Profile Components).

Step 4: Configure RDBMS Synchronization to Use a Local CSV File

To configure RDBMS Synchronization to use a local CSV file:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.



Note If this feature does not appear, choose **Interface Configuration > Advanced Options**, then check the **RDBMS Synchronization** check box.

The RDBMS Synchronization Setup page appears.

Step 3 If you are using ACS for Windows, complete these steps:

- a. Complete the required fields on the RDBMS Synchronization Setup page (Figure 4-1).

Figure 4-1 RDBMS Synchronization Setup Page (ACS for Windows)

RDBMS Synchronization Setup

Service is Running

RDBMS Synchronization using local CSV ?

Use local CSV file

AccountActions File

Directory

20080605

- b. Check the **Use local CSV file** check box.
- c. In the AccountActions file field, enter the filename of the *accountActions* CSV file that you created in [Step 3: Code an accountActions File to Create the dACL and Associate a User or Group with the dACL, page 4-4](#).
- d. In the Directory field, enter the directory path to the *accountActions* CSV file.

ACS has the information with which to access the accountActions table.

Step 4 If you are using ACS SE:

- a. Complete the required fields on the RDBMS Synchronization Setup page ([Figure 4-2](#)).

Figure 4-2 RDBMS Synchronization Setup Page (ACS SE)

RDBMS Synchronization Setup

Service is Running

FTP Setup For Account Actions Download ?

Actions File

FTP Server

Directory

Login

Password

20080602

- b. Enter the following information:
 - **Actions File**— The name of the *accountActions* file. The default name is *accountactions.csv*. The filename provided must match the name of the *accountActions* file on the FTP server.
 - **FTP Server**—The IP address or hostname of the FTP server from which ACS obtains the *accountActions* file. If you specify a hostname, DNS must be enabled on your network.
 - **Directory**—The relative path from the FTP server root directory to the directory where the *accountActions* file resides. To specify the FTP root directory, enter a single dot (.).
 - **Username**—A valid username to enable ACS to access the FTP server.

- **Password**—The password for the username provided in the Login box.

The ACS SE has the information necessary to get the *accountActions* file from the FTP server.

Step 5 (ACS for Windows and ACS SE) Set the Synchronization Scheduling and Synchronization Partners options as required.

Figure 4-3 shows the Synchronization Scheduling and Synchronization Partners sections of the RDBMS Synchronization Setup page.

Figure 4-3 Synchronization Scheduling and Synchronization Partners Options

The screenshot displays two main sections of the configuration page:

Synchronization Scheduling

- Radio buttons for scheduling options:
 - Manually
 - Every minutes
 - At specific times...
- A grid for specifying times of day (00:00 to 24:00) and days of the week (Mon to Sun).
- Buttons: Set All, Clear All

Synchronization Partners

- Two list boxes: "AAA Servers" (empty) and "Synchronize" (containing "nmdoo-win2k6").
- Navigation buttons: "->" and "<-" between the list boxes.
- Buttons: Back to Help (with a question mark icon), Submit, Synchronize Now, Cancel.

Step 6 Specify the following Synchronization Scheduling information:

- **Manually**—If you want to disable automatic RDBMS Synchronization, check the **Manually** check box.
- **Every X minutes**—ACS performs synchronization on a set frequency. The unit of measurement is minutes, with a default update frequency of 60 minutes.
- **At specific times**—ACS performs synchronization at the time that is specified in the day and hour graph. The minimum interval is one hour, and the synchronization occurs on the hour that you chose.

- Step 7** For each ACS that you want this ACS to update with data from the `accountActions` table, click the ACS in the AAA Servers list, and then click the right arrow button (-->) on the interface.
- The ACS that you chose appears in the Synchronize list.
- Step 8** To remove ACSs from the Synchronize list, click the ACS in the Synchronize list, and then click the left arrow button (<--).
- The ACS that you chose is removed from the Synchronize list.
- Step 9** At the bottom of the browser window, click **Synchronize Now**.
- ACS immediately begins a synchronization event. To check the status of the synchronization, view the RDBMS Synchronization report in Reports and Activity.
-

Step 5: Perform RDBMS Synchronization

You can perform the RDBMS Synchronization and create the dACLs in two ways. By running:

- RDBMS Synchronization from the ACS GUI.
- **CSDBSync** manually to create the dACLs.

Running RDBMS Synchronization from the ACS GUI

When you click **Synchronize Now** on the RDBMS Synchronization page for ACS for Windows or for the ACS SE, ACS begins a synchronization event and creates the dACLs specified in the `accountActions` CSV file.

Running CSDBSync Manually to Create the dACLs

You can run **CSDBSync** manually to create the dACLs.

ACS for Windows

In Windows, use the command line interface to invoke the `csdbsync -run` command.

The **CSDBSync** service reads each statement from the `accountActions` CSV file and updates the ACS internal database as the action codes in the file specify. In a distributed environment, a single ACS, known as the senior synchronization partner, accesses the `accountActions` table and sends synchronization commands to its synchronization partners.

- Step 1** Open a command prompt window.
- Step 2** Enter the following commands:
- To stop the **CSDBSync** service, enter `net stop csdbsync`.
 - Enter `net start csdbsync`.
 - Enter one of the following commands:
 - `csdbsync -run`
 - `csdbsync -syncnow`

ACS fetches the CSV file from the database, reads the action codes in the file, and performs the RDBMS Synchronization operations that the file specifies.

ACS SE

On the ACS SE, you can run the **csdbsync -syncnow** command to invoke RDBMS Synchronization

To run **CSDBSync** manually on the ACS SE:

Step 1 Check connectivity between the ACS SE and the FTP server, and be certain that you have write permissions to the FTP server directory.

Step 2 Start a SSH command shell.

Step 3 Enter the following commands:

- a. To stop the **CSDBSync** service, enter **net stop csdbsync**.
- b. Enter **net start csdbsync**.
- c. Enter one of the following commands:
 - **csdbsync -run**
 - **csdbsync -syncnow**

ACS SE fetches the CSV file from the database, reads the action codes in the file, and performs the RDBMS Synchronization operations that file specifies.

Performing RDBM Synchronization Using a Script

On the ACS SE, you can change ACS configuration from a remote system by using a command-line utility for RDBMS Synchronization that includes SSH support. You can use the mechanism that starts the SSH server to add Administrator privileges and invoke the **csdbsync -syncnow** command. The **csdbsync -syncnow** and **csdbsync -run** commands work the same, without stopping or starting the **CSDBSync** service.

You can include the commands to perform these actions in a script that you run remotely on a specified ACS SE.

Step 6: View the dACLs

After you have run RDBMS Synchronization to create the dACLs, view the dACLs to ensure that they are correct.

To view the dACLs:

Step 1 In the **Navigation Bar**, click **Shared Profile Components**.

Step 2 Click **Downloadable IP ACLs**.

The Downloadable IP ACLs page opens

In the Name column of the Downloadable IP ACLs table, you should see the dACL that was specified in the text file that you coded in [Step 2: Create a Text File to Define the dACLs, page 4-2](#).

Step 3 Click the name of the dACL.

The Downloadable IP ACLs page displays the selected dACL, as shown in [Figure 4-4](#).

Figure 4-4 Entry for the Sample dACL

Downloadable IP ACLs

Name:

Description:

ACL Contents	Network Access Filtering
<input type="radio"/> content1	(All-AAA-Clients)

In the ACL Contents column, you should see the content name specified in the Content#1 block that you coded in the text file in [Step 2: Create a Text File to Define the dACLs, page 4-2](#).

Step 4 Click the content name.

The Downloadable IP ACL Content page appears. The Content Name and ACL Definitions appear on the page, as shown in [Figure 4-5](#).

Figure 4-5 Downloadable IP ACL Content Page

Downloadable IP ACL Content

Name:

ACL Definitions

```

permit ip any host 192.168.1.152
permit ip any host 192.168.5.152
permit ip any host 192.168.29.33
permit ip any host 192.168.29.34
permit ip any host 192.168.9.50
permit ip any host 192.168.9.20
permit ip any host 192.168.7.20
permit ip any host 192.168.128.1
permit ip any 192.168.24.0 0.0.0.255
permit ip any 192.168.0 0.0.0.255
permit ip any 192.0.0.0 0.255.255.255
deny ip any 192.168.0.0 0.3.255.255
deny ip any 192.168.0.0 0.1.255.255
permit ip any any

```

- Step 5** If the dACL was not created correctly, review the steps in [Using RDBMS Synchronization to Configure dACLs, page 4-2](#) and check for errors.
For a list of error messages, see [Error Messages, page 4-11](#).

Error Messages

Table 4-3 lists the error messages associated with dACL creation using CSDBSync.

Table 4-3 dACL Creation Errors

Error Message	Explanation
Failed to process DACL. DACL not defined.	<p>Possible Cause The dACL was not specified correctly in the text file used to define the dACLs.</p> <p>Recommended Action Review the text file that you coded to specify the dACLs and ensure that the syntax is correct.</p>
Failed to process DACL. Could not find NAF.	<p>Possible Cause The text file provided to define the dACL did not correctly define a NAF.</p> <p>Recommended Action Review the text file that you coded to specify the dACLs and ensure that the syntax is correct.</p>
Failed to process DACL. Failed to get UserID.	<p>Possible Cause On the ACS SE, the user ID specified for the FTP server in the RDBMS Synchronization configuration was incorrect.</p> <p>Recommended Action Check to ensure that the specified user ID exists on the FTP server used with the ACS SE.</p>
Failed to process DACL. DACL content not found.	<p>Possible Cause The text file used to specify the dACL did not correctly specify the dACL content.</p> <p>Recommended Action Check the syntax in the text file and ensure that it is correct. Ensure that the ACLs defined in the file are correct.</p>
Failed to upload file into FTP server.	<p>Possible Cause The FTP server was not reachable, or a network error occurred.</p> <p>Recommended Action Ensure that the IP address for the FTP server in the RDBMS configuration is correct and that the network is functioning correctly.</p>

Table 4-3 *dACL Creation Errors (continued)*

Error Message	Explanation
Failed to import DACL file.	<p>Possible Cause The user ID specified in the RDBMS Synchronization configuration does not have write access to the ACS.</p> <p>Recommended Action Ensure that the specified user has write access to the ACS.</p>
Failed to access Host DB.	<p>Possible Cause The CSDBSync service could not access the database on the host ACS.</p> <p>Recommended Action Ensure that the database on the ACS is configured correctly and enabled correctly in the ACS GUI.</p>

Reading, Updating, and Deleting dACLs

Table 4-4 lists the account action codes that you can use to read, update, or delete a dACL.

Table 4-4 Account Action Codes for Creating, Reading, Updating, or Deleting dACLs

Action Code	Name	Required	Description
386	READ_DACL	VN, V1 (optional)	<p>Use this action code to read dACL attributes and save them in a file for later use.</p> <p>VN = contains dACL name or * for all dACLs.</p> <p>V1 = <output_file_name></p> <p>where <i>output_file_name</i> contains the exported dACLs definition.</p> <p>On the ACS SE, <i>output_file_name</i> specifies the file in the FTP server for the ACS SE. If not is specified the default filename <i>DumpDACL.txt</i> is used.</p> <p>On ACS for Windows, you can specify the absolute file path; for example, <i>C:\temp\DACL.txt</i> for ACS for Windows. If you do not specify the file path and filename, ACS writes the data to a file in the <i>ACS\bin</i> directory.</p>
387	UPDATE_DACL	VN, V1(optional)	<p>Use this action code to update dACL attributes.</p> <p>VN = <input_file_name></p> <p>where <i>input_file_name</i> specifies the file that contains the definition for the dACL to be updated.</p> <p>On the ACS SE platform, <i>input_file_name</i> specifies the file name present in the FTP server for ACS SE.</p> <p>You can specify the absolute file path; for example: <i>C:\DACL\dump.txt</i> for ACS for Windows.</p> <p>V1=DACL_REPLACE or DACL_APPEND</p> <p>The default option is:</p> <p>DACL_REPLACE</p> <p>The DACL_REPLACE option replaces the existing dACL with the new one.</p> <p>DACL_APPEND appends the new dACL content and its definition to the existing dACL.</p> <p>If the dACL has not been defined, the new dACL is added to the existing list.</p> <p>The dACL definition is ignored if it contains an invalid definition, content name, content definition or NAF name.</p>
388	DELETE_DACL	VN	<p>Use this action code to delete a dACL.</p> <p>VN = The name of the dACL to delete. To delete all dACLs, code an asterisk (*).</p> <p>By default, all the dACLs are deleted.</p> <p>Users and Groups associated with this dACL will be dereferenced after deleting the dACL.</p>

Updating or Deleting dACL Associations with Users or Groups

Table 4-5 lists the account action codes to update the dACL or remove the association of the dACL and the User or Group.

Table 4-5 Account Action Codes to Create or Remove dACL Associations With Users and User Groups

Action Code	Name	Required	Description
381	UPDATE_USER_DACL	UNIGN, VN	This action code updates the dACL for a specified User or Group. The dACL name specified should be valid and should be present in ACS. UN = Valid Username GN = Valid Group name (optional) VN = dACL name. (This dACL must be defined in Shared Profile Component)
382	DELETE_USER_DACL	UNIGN	This action code disassociates a dACL from a specified User or Group. UN = valid Username GN = Valid Group name (optional)

Using RDBMS Synchronization to Specify Network Configuration

You can use RDBMS Synchronization to perform network configuration tasks, such as:

- Add AAA clients.
- Delete AAA clients.
- Set AAA client configuration details.
- Add AAA servers.
- Delete AAA servers.
- Set AAA server configuration details.
- Add and configure Proxy Distribution Table entries.



Note

For specific information about all actions that RDBMS Synchronization can perform, see Appendix E, “RDBMS Synchronization Import Definition,” in the *User Guide for Cisco Secure ACS, 4.2*.

Creating, Reading, Updating and Deleting AAA clients

The RDBMS Synchronization feature supports creation and deletion of single or multiple AAA clients. In addition, accountActions codes 224 and 225 enable reading and updating AAA client information. This section describes the various RDBMS Synchronization tasks that you can perform on single or multiple AAA clients.

Table 4-6 lists the account action codes that are used to read and update single or multiple AAA clients.

Table 4-6 Account Action Codes for Create, Read, Update, Delete for AAA Clients

Action Code	Name	Required	Description
224	UPDATE_NAS	VN, V1, V2, V3	Use this action code to update AAA clients. VN = AAA Client Name V1 = IP-Address V2 = Shared Secret Key V3 = Vendor
225	READ_NAS	VN, V1 (optional)	Use this action code to export an AAA client list to an output file that can be used to associate the list with members of a particular NDG or with all AAA clients. You can use this output file as input for CSUtil , to import NASs. VN = <output_file_name> where <i>output_file_name</i> specifies the filename for the FTP server used with the ACS SE. If nothing is specified, the default name <i>DumpNAS.txt</i> is used. For the ACS for Windows platform, you can specify the absolute file path; for example: <i>C:\MyNAS\dump.txt</i> . If no value is specified, the AAA client lists is written to the <i>\ACS\bin\DumpNAS.txt</i> file. V1 = NDG name (optional) V1 should contain a valid NDG name.

