CHAPTER 2

Migrating from ACS 4.x to ACS 5.4

ACS 4.x stores policy and authentication information, such as TACACS+ command sets, in the user and user group records. In ACS 5.4, policy and authentication information are independent shared components that you use as building blocks when you configure policies.

The most efficient way to make optimal use of the new policy model is to rebuild policies by using the building blocks, or policy elements, of the new policy model. This method entails creating appropriate identity groups, network device groups (NDGs), conditions, authorization profiles, and rules.

ACS 5.4 provides a migration utility to transfer data from migration-supported versions of ACS 4.x to an ACS 5.4 machine. The ACS 5.4 migration process requires, in some cases, administrative intervention to manually resolve data before you import it to ACS 5.4.

This process is different from the process of upgrading from versions of ACS 3.x to ACS 4.x, where the ACS 4.x system works the same way as ACS 3.x and no administrative intervention is required.

The migration utility in ACS 5.4 supports multiple-instance migration that migrates all ACS 4.x servers in your deployment to ACS 5.4. For more information on multiple-instance migration, see

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/migration/guide/migration_guide.html.

Upgrade refers to the process of transferring data from ACS 5.3 servers to ACS 5.4. For information on the upgrade process, refer to

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/installation/guide/csacs_upg.html.

This chapter contains the following sections:

Overview of the Migration Process

The Migration utility completes the data migration process in two phases:

- Analysis and Export
- Import

In the Analysis and Export phase, you identify the objects that you want to export into 5.4. The Migration utility analyses the objects, consolidates the data, and exports it.

After the Analysis and Export phase is complete, the Migration utility generates a report that lists any data compatibility errors, which you can manually resolve to successfully import these objects into 5.4.

The Analysis and Export phase is an iterative process that you can rerun many times to ensure that there are no errors in the data to be imported. After you complete the Analysis and Export phase, you can run the import phase to import data into ACS 5.4.

This section contains the following topics:

Migration Requirements

To run the Migration utility, you must deploy the following machines:

- The source ACS 4.x machine—This machine can either be an ACS 4.x solution engine or a ACS for Windows 4.x machine. The source machine must be running a migration-supported version of ACS. See Supported Migration Versions, page 2-2 for more information.
- The migration machine—This machine must be a Windows platform that runs the same version of ACS (including the patch) as the source machine. The migration machine cannot be an ACS production machine or an ACS appliance machine. It has to be a Windows server running ACS for Windows. The migration machine requires 2 GB RAM.
- The target ACS 5.4 machine—Back up your ACS 5.4 configuration data and ensure that the migration interface is enabled on ACS 5.4 before you begin the import process. We recommend that you import data into a fresh ACS 5.4 database. To enable the migration interface, from the ACS CLI, enter:

  ```
  acs config-web-interface migration enable
  ```

Supported Migration Versions

ACS 5.4 supports migration from the following ACS 4.x versions:

- ACS 4.1.1.24
- ACS 4.1.4
- ACS 4.2.0.124
- ACS 4.2.1

Note You must install the latest patch for the supported migration versions listed here. Also, if you have any other version of ACS 4.x installed, you must upgrade to one of the supported versions and install the latest patch for that version before you can migrate to ACS 5.4.

Before You Begin

Before you migrate data from ACS 4.x to ACS 5.4, ensure that you:

- Check for database corruption issues in the ACS 4.x source machine.
- Have the same ACS versions on the source and migration machines (including the patch).
- Have configured a single IP address on the migration machine.
- Take a backup of the source ACS 4.x data.
- Have full network connectivity between the migration machine and the ACS 5.4 server.
- Have enabled the migration interface on the ACS 5.4 server.
- Use only the default superadmin account for ACS 5.4, **acsadmin** while running the Migration utility.

You cannot use the remote desktop to connect to the migration machine to run the Migration Utility. You must run the Migration Utility on the migration machine; or, use VNC to connect to the migration machine.

Note ACS 5.4 migration utility is not supported on Windows 2008 64 bit.

Downloading Migration Files

To download migration application files and the migration guide for ACS 5.4:

Step 1 Select **System Administration > Downloads > Migration Utility**.

The Migration from 4.x page appears.

Step 2 Click **Migration application files**, to download the application file you want to use to run the migration utility.

Step 3 Click **Migration Guide**, to download *Migration Guide for Cisco Secure Access Control System 5.4*.

Migrating from ACS 4.x to ACS 5.4

You can migrate data from any of the migration-supported versions of ACS 4.x to ACS 5.4. The migration utility migrates the following ACS 4.x data entities:

- Network Device Groups (NDGs)
- AAA Clients and Network Devices
- Internal Users

- User-Defined Fields (from the Interface Configuration section)
- User Groups
- Shared Shell Command Authorization Sets
- User TACACS+ Shell Exec Attributes (migrated to user attributes)
- Group TACACS+ Shell Exec Attributes (migrated to shell profiles)
- User TACACS+ Command Authorization Sets
- Group TACACS+ Command Authorization Sets
- Shared, Downloadable ACLs
- EAP-FAST Master Keys
- Shared RADIUS Authorization Components (RACs)
- RADIUS VSAs

Note The Migration utility does not migrate public key infrastructure (PKI) configuration data and does not support certificate migration.

To migrate data from ACS 4.x to ACS 5.4:

Step 1 Upgrade the ACS 4.x version to a migration-supported version if your ACS 4.x server currently does not run one of the migration-supported versions.

For a list of migration-supported ACS versions, see Supported Migration Versions, page 2-2.

Step 2 Install the same migration-supported version of ACS on the migration machine, which is a Windows server.

Step 3 Back up the ACS 4.x data and restore it on the migration machine.

Step 4 Place the Migration utility on the migration machine.

You can get the Migration utility from the Installation and Recovery DVD.

Step 5 Run the Analyze and Export phase of the Migration utility on the migration machine.

Step 6 Resolve any issues in the Analyze and Export phase.

Step 7 Run the Import phase of the Migration utility on the migration machine.

The import phase imports data into the 5.4 server.

Note If you have a large internal database, then we recommend that you import the data into a standalone 5.x primary server and not to a server that is connected to several secondary servers. After data migration is complete, you can register the secondary servers to the standalone 5.x primary server.

For detailed information about using the migration utility, refer to

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/migration/guide/migration_guide.html.

After you migrate the data, you can reconstruct your policies with the migrated objects.

Functionality Mapping from ACS 4.x to ACS 5.4

In ACS 5.4, you define authorizations, shell profiles, attributes, and other policy elements as independent, reusable objects, and not as part of the user or group definition.

Table 2-1 describes where you configure identities, network resources, and policy elements in ACS 5.4. Use this table to view and modify your migrated data identities. See Chapter 3, "ACS 5.x Policy Model" for an overview of the ACS 5.4 policy model.

Table 2-1 Functionality Mapping from ACS 4.x to ACS 5.4

To configure...	In ACS 4.x, choose...	In ACS 5.4, choose...	Additional information for 5.4
Network device groups	Network Configuration page	Network Resources > Network Device Groups See Creating, Duplicating, and Editing Network Device Groups, page 7-2.	You can use NDGs as conditions in policy rules. ACS 5.4 does not support NDG shared password. After migration, member devices contain the NDG shared password information.
Network devices and AAA clients	Network Configuration page	Network Resources > Network Devices and AAA Clients See Network Devices and AAA Clients, page 7-5.	RADIUS KeyWrap keys (KEK and MACK) are migrated from ACS 4.x to ACS 5.4.
User groups	Group Setup page	Users and Identity Stores > Identity Groups See Managing Identity Attributes, page 8-7.	You can use identity groups as conditions in policy rules.
Internal users	User Setup page	Users and Identity Stores > Internal Identity Stores > Users See Managing Internal Identity Stores, page 8-4.	ACS 5.4 authenticates internal users against the internal identity store only. Migrated users that used an external database for authentication have a default authentication password that they must change on first access.
Internal hosts	Network Access Profiles > Authentication	Users and Identity Stores > Internal Identity Stores > Hosts See Creating Hosts in Identity Stores, page 8-16.	You can use the internal hosts in identity policies for Host Lookup.
Identity attributes (user-defined fields)	Interface Configuration > User Data Configuration	System Administration > Configuration > Dictionaries > Identity > Internal Users See Managing Dictionaries, page 18-5.	Defined identity attribute fields appear in the User Properties page. You can use them as conditions in access service policies.

Table 2-1 Functionality Mapping from ACS 4.x to ACS 5.4 (continued)

To configure...	In ACS 4.x, choose...	In ACS 5.4, choose...	Additional information for 5.4
Command sets (command authorization sets)	One of the following: • Shared Profile Components > Command Authorization Set • User Setup page • Group Setup page	Policy Elements > Authorization and Permissions > Device Administration > Command Set See Creating, Duplicating, and Editing Command Sets for Device Administration, page 9-29.	You can add command sets as results in authorization policy rules in a device administration access service.
Shell exec parameters	User Setup page	System Administration > Dictionaries > Identity > Internal Users See Managing Dictionaries, page 18-5.	Defined identity attribute fields appear in the User Properties page. You can use them as conditions in access service policies.
Shell profiles (shell exec parameters or shell command authorization sets)	Group Setup page	Policy Elements > Authorization and Permissions > Device Administration > Shell Profile See Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24.	You can add shell profiles as results in authorization policy rules in a device administration access service.
Date and time condition (Time of Day Access) You cannot migrate the date and time conditions. You have to recreate them in ACS 5.4.	Group Setup page	Policy Elements > Session Conditions > Date and Time See Creating, Duplicating, and Editing a Date and Time Condition, page 9-3.	You can add date and time conditions to a policy rule in the Service Selection policy or in an authorization policy in an access service.
RADIUS Attributes	One of the following: • Shared Profile Components > RADIUS Authorization Component • User Setup page • Group Setup page You cannot migrate the RADIUS attributes from user and group setups. You have to recreate them in ACS 5.4.	Policy Elements > Authorization and Permissions > Network Access > Authorization Profile > Common Tasks tab or Policy Elements > Authorization and Permissions > Network Access > Authorization Profile > RADIUS Attributes tab See Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18.	You configure RADIUS attributes as part of a network access authorization profile. You can add authorization profiles as results in an authorization policy in a network access service.

Table 2-1 Functionality Mapping from ACS 4.x to ACS 5.4 (continued)

To configure...	In ACS 4.x, choose...	In ACS 5.4, choose...	Additional information for 5.4
Downloadable ACLs	Shared Profile Components	Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs See Creating, Duplicating, and Editing Downloadable ACLs, page 9-32.	You can add downloadable ACLs (DACLs) to a network access authorization profile. After you create the authorization profile, you can add it as a result in an authorization policy in a network access service.
RADIUS VSA	Interface Configuration	System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA. See Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes, page 18-6.	You configure RADIUS VSA attributes as part of a network access authorization profile. You can add authorization profiles as results in an authorization policy in a network access service.

Common Scenarios in Migration

The following are some of the common scenarios that you encounter while migrating to ACS 5.4:

- Migrating from ACS 4.2 on CSACS 1120 to ACS 5.4, page 2-7
- Migrating from ACS 3.x to ACS 5.4, page 2-8
- Migrating Data from Other AAA Servers to ACS 5.4, page 2-8

Migrating from ACS 4.2 on CSACS 1120 to ACS 5.4

In your deployment, if you have ACS 4.2 on CSACS 1120 and you would like to migrate to ACS 5.4, you must do the following:

Step 1 Install Cisco Secure Access Control Server 4.2 for Windows on the migration machine.

Step 2 Back up the ACS 4.2 data on CSACS 1120.

Step 3 Restore the data in the migration machine.

Step 4 Run the Analysis and Export phase of the Migration utility on the migration machine.

Step 5 Install ACS 5.4 on CSACS 1120.

Step 6 Import the data from the migration machine to the CSACS 1120 that has ACS 5.4 installed.

See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/migration/guide/migration_guide.html for a detailed description of each of these steps.

Migrating from ACS 3.x to ACS 5.4

If you have ACS 3.x deployed in your environment, you cannot directly migrate to ACS 5.4. You must do the following:

Step 1 Upgrade to a migration-supported version of ACS 4.x. See Supported Migration Versions, page 2-2 for a list of supported migration versions.

Step 2 Check the upgrade paths for ACS 3.x:

- For the ACS Solution Engine, see:

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.1/installation/guide/solution_engine/upgap.html#wp1120037

- For ACS for Windows, see:

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/install.html#wp1102849

Step 3 Upgrade your ACS 3.x server to a migration-supported version of ACS 4.x.

After the upgrade, follow the steps that describe migrating from ACS 4.x to ACS 5.4. Refer to the *Migration Guide for Cisco Secure Access Control System 5.4* for more information.

Migrating Data from Other AAA Servers to ACS 5.4

ACS 5.4 allows you to perform bulk import of various ACS objects through the ACS web interface and the CLI. You can import the following ACS objects:

- Users
- Hosts
- Network Devices
- Identity Groups
- NDGs
- Downloadable ACLs
- Command Sets

ACS allows you to perform bulk import of data with the use of a comma-separated values (.csv) file. You must input data in the .csv file in the format that ACS requires. ACS provides a .csv template for the various objects that you can import to ACS 5.4. You can download this template from the web interface.

To migrate data from other AAA servers to ACS 5.4:

Step 1 Input data into .csv files.

For more information on understanding .csv templates, see

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/cli_imp_exp.html#wp1064565.

Step 2 Set up your ACS 5.4 appliance.

Step 3 Perform bulk import of data into ACS 5.4.

For more information on performing bulk import of ACS objects, see

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/cli_imp_exp.html#wp1056244.

The data from your other AAA servers is now available in ACS 5.4.