
# Configuration Migration Methods in ACS 5.5

This chapter describes ACS 4.x to 5.5 migration and contains:



## Migration Methods

The ACS 5.5 configuration model differs from ACS 3.x and 4.x. You cannot directly migrate data and configurations from ACS 3.x and 4.x to ACS 5.5. ACS 5.5 migration requires some manual reconfiguration. ACS 5.5 provides the following tools for the migration process:



### Migration Utility

The Migration Utility is a tool that runs on an ACS 4.x Windows machine. This tool helps you to import the ACS 4.x backup files, analyze the data, and make the required modifications before importing the data to ACS 5.5.

The Migration Utility supports the migration of the configurations that are shown in Table 3-1. You can download the Migration Utility from the ACS 5.5 web interface under **System Configuration > Downloads**.

The Migration Utility *migrates* data from an ACS 4.x Windows machine to an ACS 5.5 machine. This process is different from the *upgrade* process for versions of ACS from 3.x to 4.x or for any 4.x upgrades.

In the upgrade process, the ACS 4.x system works in the same way, without the need for administrative support. The migration process entails, in some cases, administrative support to consolidate and manually resolve data before you import the data to ACS 5.5.

The Migration Utility in ACS 5.5 supports multiple-instance migration that migrates all ACS 4.x servers in your deployment to ACS 5.5. To differentiate between several ACS 4.x instances, you can add a prefix. The prefix is used to retain server-specific identification of data elements and prevent duplication of object names for different servers.

Migrating an ACS 4.x deployment is a complex process and needs to be planned carefully. You need to consider the ACS 4.x replication hierarchy before you perform the migration.

For example, if one ACS 4.x server has data replicated from another ACS 4.x server, there is no need to migrate the same data set from both these ACS servers, since the data will be identical. Therefore, you must carefully consider the order of migration of the ACS instances in the deployment.

# CSV Import Tool

ACS 5.5 allows you to import some of the data objects from comma-separated value (CSV) text files, as listed in Table 3-1. If you do not want to manually configure all the data objects in ACS 5.5 through the web interface, you can create the configuration in CSV text files and import the configuration.

In many instances, ACS configuration data, such as device and user information is maintained externally to ACS. You can export this data in a text format for importing into ACS 5.5.

For more information on the CSV Import Tools, see the Using the Scripting Interface chapter of the *Software Developer's Guide for Cisco Secure Access Control System 5.5*.

***Table 3-1 ACS 5.5 Migration Utility And Import Tool Options***

| ACS 5.5 Configuration Areas | ACS 5.5 Migration Utility Support | ACS 5.5 Import Tools |
|---|---|---|
| NDGs | Yes | Yes |
| Network Devices | Yes | Yes |
| RADIUS Proxy Servers | No | No |
| Internal Users/Hosts | Yes | Yes |
| Identity Groups | Yes | Yes |
| External Identity Stores | No | No |
| Policy Elements | Shared command sets, RACs, shared DACLs | Shared command sets, shared DACLs |
| Access Policies | No | No |
| Monitoring and Reports | No | No |
| System Administration | FAST master keys, VSAs | No |

### Migration Recommendations

- For small ACS configurations, use a combination of manual configuration and CSV import. This is in cases such as:
  - Where users are not maintained in ACS
  - Where network device wildcard is used
  - Where user and network device information is available in CSV text format
- For other configurations, use the ACS 5.5 Migration Utility in addition to manual configuration and CSV import.

# About the Migration Utility

Use the Migration Utility to migrate the different types of data from ACS 4.x to ACS 5.5. In addition to your ACS 4.x Windows source machine, you must deploy an ACS 4.x migration machine and an ACS 5.5 target machine.

The two phases of the migration process are:

- Analysis and Export
- Import

You run the Migration Utility on the ACS 4.x migration machine. The migration machine is a Windows platform running ACS 4.x. You can run the analysis and export phases independently, several times, to ensure that the data is appropriate for the import phase.

Data that passes the analysis phases can be exported and then imported to ACS 5.5. See the *User Guide for Cisco Secure Access Control System 5.5* for details on ACS 5.5 policies.

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. You must run the Migration Utility on a 32-bit version of Windows.

**Note** ACS 5.5 Migration Utility is not supported on a 64-bit version of Windows.

The Migration Utility supports a subset of the ACS 4.x data elements. For a complete list, see ACS Elements that Migration Process Supports in Table 4-1 on page 4-3.

# Migrating from ACS 4.x to 5.5

This section describes the approach that is used in migrating from ACS 4.x to ACS 5.5. This section includes:



## Multiple-Instance Migration

ACS 5.5 has one primary database that holds the data for all the ACS 4.x instances. Data from each ACS 4.x instance is migrated to this primary database. In ACS 4.x, selective data replication can be defined such that different ACS instances maintain distinct subsets of the overall system configuration.

ACS 5.5 contains a consolidated database, which is replicated to all the ACS instances. The consolidated database contains all the local configuration definitions from each of the ACS 4.x instances.

# Migration Phases for ACS 5.5

ACS 5.5 follows a two-phase migration approach:


- Analysis Phase, page 3-4
- Migration Phase, page 3-4


## Analysis Phase

In this phase, an analysis of the existing ACS 4.x configuration is performed. It reports the possible migration issues and recommends resolutions, if any. Before running the Migration Utility, you must install ACS 4.x on the migration machine and restore the data.

You can run the analysis tool on the data restored from the backup of an ACS 4.x server. You can run the analysis tool multiple times to make changes in the ACS 4.x configuration in the migration machine, if necessary.

**Note** The analysis and export phases are implemented as a single phase in the migration process. The Analysis reports include both the analysis and the export information.

## Migration Phase

In this phase, the Migration Utility extracts the configuration data from an ACS 4.x server and prepares the data to be migrated in a format that can be imported into an ACS 5.5 server. The migration tool provides options to migrate data in one or more categories, such as:

- Inventory data migration (Users, Network Devices, MAC)
- Policy data migration (Network Device Groups, Identity Groups, Command Sets, RADIUS Authorization Components (RACs), vendor-specific attributes (VSAs), and downloadable access control lists (dACLs))

# Data Model Organization

ACS 5.5 is a policy-based access control system. The term *policy model* in ACS 5.5 refers to the presentation of policy elements, objects, and rules to the policy administrator. ACS 5.5 uses a rule-based policy model instead of the group-based model that was used in previous versions.

The rule-based policy model provides more powerful and flexible access control than is possible with the older group-based approach. For more information on the policy model, see the *User Guide for Cisco Secure Access Control System 5.5*.

The following are the three major data model-related points in ACS 5.5:


- Model Organization, page 3-5
- Model Storage, page 3-5
- Replication Model, page 3-5

### Model Organization

ACS 5.5 extends the Network Access Profile (NAP)-related functionality to a full policy-based authentication, authorization, and accounting (AAA) solution for both RADIUS and TACACS+.

Specific policy and authentication information, such as sets of RADIUS attributes, are not maintained within the user or group records, as in ACS 4.x. Instead, the entire set of retuned authentication data is selected.

### Model Storage

The migration process covers the ACS 4.x data that fulfills the following criteria:

- It can be translated to the ACS 5.5 model.
- It consists of data that is not generated during run-time operation; for example, dynamic-user.

### Replication Model

In ACS 5.5, multiple database instances of ACS 4.x are combined and migrated into a single database. In ACS 4.x, selective data replication can be defined such that different ACS instances maintain distinct subsets of the overall system configuration.

ACS 5.5 contains a consolidated database that is replicated to all the ACS instances. This consolidated database contains all the local configuration definitions from each of the ACS 4.x instances.

The ACS 5.5 data model is much more uniform than the ACS 4.x data model. The ACS 5.5 data model contains a single master instance, where all configuration changes are made. All subtending secondary instances maintain a full copy of the configuration and receive updates for all configuration changes.

# Multiple-Instance Migration Support

To migrate multiple instances of ACS 4.x to ACS 5.5:

**Step 1** Choose an ACS 4.x instance to be migrated.

The primary ACS 4.x instance (if exists in the deployment) should be migrated first. Back up the chosen ACS 4.x instance.

**Step 2** Restore the backed up ACS 4.x instance on the migration machine.

**Step 3** Run the migration process.

**Step 4** After you complete the migration process for one ACS 4.x instance, continue with another instance or terminate the process.

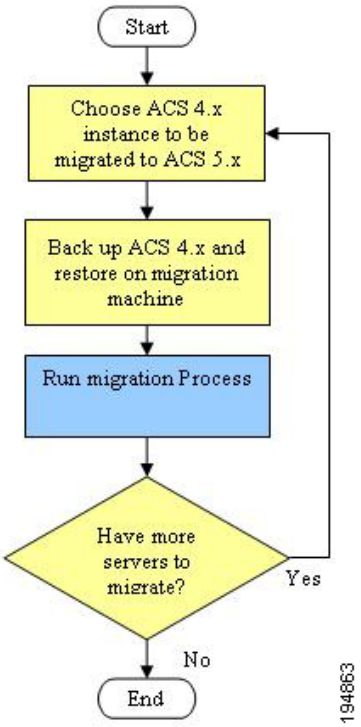
If you restore any instance of ACS 4.x, it deletes the previous ACS 4.x instance data.

In the analysis and export phase, no changes are made with regard to multiple instance.

For example, the Migration Utility does not detect duplicate objects between different ACS 4.x instances. Duplicate and discrepant data objects that exist on multiple ACS 4.x instances are detected and reported in the migration import phase.

Figure 3-1 illustrates the multiple-instance migration process.

***Figure 3-1 Multiple-Instance Migration Process***



# Migrating Data

The migration process exports data from a source ACS 4.x server and imports the corresponding data entities to a target ACS 5.5 server. The export process does not run on the operational 4.x server. Instead, you must back up the database from the ACS 4.x source server and restore the data to an additional ACS 4.x migration machine, where you run the Migration Utility.

**Note** You must perform a full database backup on the ACS 4.x source machine before you start the migration process. Restore the backed-up data to an additional ACS 4.x migration machine and fix issues before you import the data to the ACS 5.5 machine.

The ACS 4.x database password should be less than 37 characters.

To migrate data:

**Step 1** Run Analyze and Export on the ACS 4.x data and review the AnalyzeAndExport Summary report and the Analyze and Export full report.

See Analysis and Export of ACS 4.x Data, page 6-36. In this phase, you:

- Identify issues for data that cannot be migrated and review manual migration considerations. See Resolving Migration Issues, page D-3.
- Identify issues to fix prior to migration.
- Identify the data to consolidate. See "Consolidating Data" section on page 6-37 for more information.

Only data that passes the Analyze and Export phase can be exported and later imported to ACS 5.5.

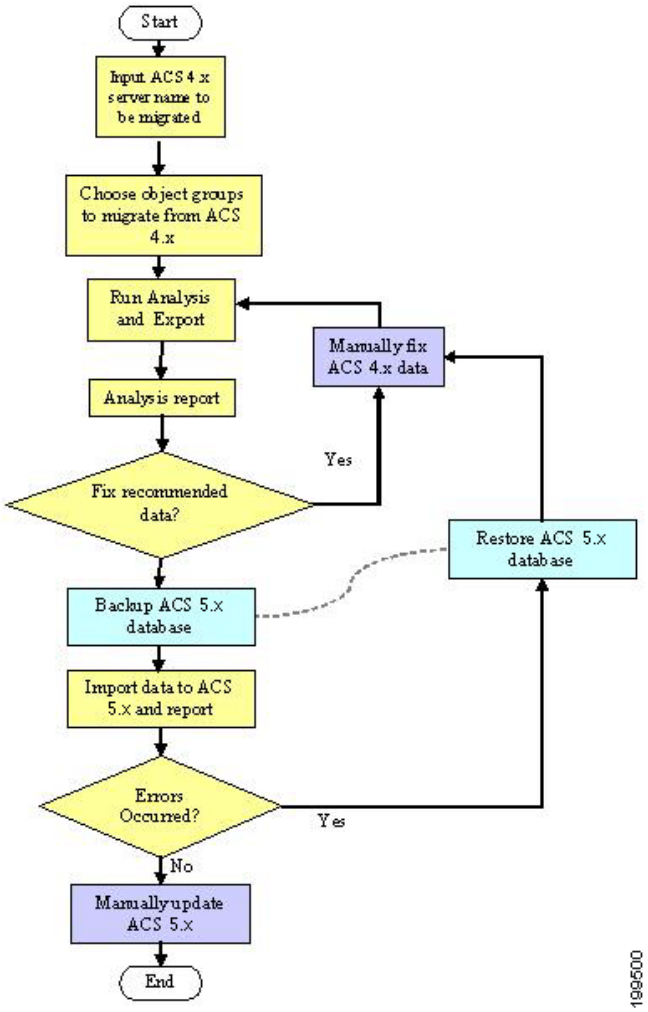
**Step 2** Back up the ACS 5.5 target machine database.

**Step 3** Import the ACS 4.x data to ACS 5.5 and review the Import Summary Report.

See Importing the ACS 4.x Data to ACS 5.5, page 6-37.

Figure 3-2 illustrates the migration process.

***Figure 3-2 Migration Process***




# Object Group Selection

You can choose to perform a full or partial migration. For partial migration, you have to choose the object groups to be migrated.

The object groups are defined according to dependencies between the objects. You can migrate either a group of the object types supported by the application or all supported object types. You can select from the following groups of objects:

- All Objects—All ACS objects that are supported in the migration process.
- All User Objects—Identity groups and all objects extracted from users
- All Device Objects—Network devices and NDGs
- Shared command sets
- Shared downloadable access control lists (DACLs)

- Master Keys—Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) master keys
- Shared RADIUS Authorization Components (RACs) and vendor-specific attributes (VSAs)

# Analysis and Export

You must analyze the existing configuration of ACS 4.x and identify the possible migration issues or problems that could affect your ability to perform a successful data migration.

In this phase, you identify:

- Issues for data that cannot be migrated. You are also provided opportunities to rectify this data prior to the migration.
- Issues to fix before migration.
- The data to consolidate. See "Consolidating Data" section on page 6-37 for more information.

**Note** Only data that passes the analysis phase can be exported and later imported to ACS 5.5.

The export process exports the selected set of objects from the ACS 4.x data to an external data file that is processed during the import process.

The export process reports the following issues:

- Data that was not exported, and the reason.
- Data that was exported, and the statistics.

# Import

The data export file from ACS 4.x is imported into ACS 5.5.

You can run the Import on a full database. We recommend that you manually back up the ACS 5.5 database. The backup version of the database can be used to restore the system, if any unexpected errors occur during the data import process.

# Multiple-Instance Support

For multiple-instance migration, every instance is restored on the same migration machine, and the results from all the instances are maintained. For more information on the specific changes for each data type, related to multiple-instance support, see Migration of ACS 4.x Objects, page 6-9.

The multiple-instance support in ACS 5.5 has the following key features:

- Duplicate Object Reporting, page 3-10
- Object Name Prefix Per Instance, page 3-10
- Shared Object Handling, page 3-10

### Duplicate Object Reporting

Duplicate data objects on multiple ACS 4.x instances are detected in the import phase. For most of the objects types, you can identify duplicates by name. Additionally, in the import report, information about duplicate objects is mentioned, see "Migration of ACS 4.x Objects" section on page 6-9

### Object Name Prefix Per Instance

You can define a different name prefix to each ACS 4.x instance. The prefix is used to retain server-specific identification of data elements and prevent duplication of names of objects for different servers. You can change the name prefix at the beginning of each run of the Migration Utility (per ACS 4.x instance).

You can have an instance-specific prefix and thus import all the data regardless of duplication between ACS 4.x instances. You can configure a global name prefix or per-object-type name prefix. This enables you to preserve associations between shared objects. For more information, see "Migration of ACS 4.x Objects" section on page 6-9.

### Shared Object Handling

Shared objects between the ACS 4.x instances—such as NDGs, user attribute definitions, and user groups—are migrated only once. However, because of the association support for multiple instances, object associations are created according to the status of ACS 5.5 data. For more information, see "Migration of ACS 4.x Objects" section on page 6-9.

For example, if user *A* is associated to group *BB* and neither the user nor the group were migrated, both objects are created and then associated in ACS 5.5.