Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.8

This chapter describes how to migrate data from ACS 4.x to ACS 5.8 and contains:

Introduction

This chapter contains information to migrate data from ACS 4.x to ACS 5.8. Before you begin, you must follow the setup, backup, and installation instructions in Migration Utility Setup and Installation, page 1

Before you begin migration, ensure that you have enabled the migration interface on the ACS 5.8 server.

From the command line interface, enter:

acs config-web-interface migration enable

To verify that the migration interface is enabled on the ACS 5.8 server, from the command line interface, enter:

show acs-config-web-interface

See the *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.8* for more information.

Running the Migration Utility

To run the Migration Utility:

1. Open a command prompt and change directory to `C:\Migration Utility\migration\bin.`

You can specify any directory in which to install the Migration Utility. This example uses the Migration Utility as the root directory.

2. At the command prompt, type **`migration.bat`**.

Example 1: Migration Script (User Input), page 2 shows the prompts that appear when you run the Migration Utility.

```
Example 1: Migration Script (User Input)
Copyright (c) 2008-2009 Cisco Systems, Inc.
All rights reserved.
-------------------------------------------------------------------------------------
This utility migrates data from ACS 4.x to ACS 5. You can migrate directly from the following ACS
versions:

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

Data migration involves the following:
a. The migration utility analyzes the ACS 4.x data, exports any data from ACS 4.x that can be migrated
automatically, and imports the data into ACS 5.
b. Before the import stage, you can manually consolidate and resolve data according to the analysis
report, to maximize the amount of data that the utility can migrate.
c. After migration, use the imported data to recreate your policies in ACS 5.
-------------------------------------------------------------------------------------

Make sure that the database is running.
Enter ACS 5 IP address or hostname:[nn.nn.nnn.nnn]
Enter ACS 5 administrator username:[test]
Enter ACS 5 password:
Change user preferences?[no]
yes

User Groups
--------------------------------------------------------------------------------
Existing user groups will be migrated to the Identity Group.
Enter new Root name:[Migrated Group]

Network Device Groups
--------------------------------------------------------------------------------

Existing network device groups will be migrated to the Network Device Group.
Enter new Root name:[Migrated NDGs]

Consolidation Prefix
--------------------------------------------------------------------------------
Identical objects found will be consolidated into one object.
Enter a prefix to add to the consolidated object:[cons]

Users
--------------------------------------------------------------------------------
ACS 5 supports authentication for internal users against the internal database only.
ACS 4.x users who were configured to use an external database for authentication will be migrated with
a default authentication password.
Specify a default password.

Disabled Group Users
--------------------------------------------------------------------------------
ACS 4.x users and hosts that are associated with disabled groups will be migrated as disabled:[yes]
```

```
Configure these users as disabled in ACS 5, or ask for a change of password on a user's first attempt
to access ACS 5.
Select the option:
1 - DisableExternalUser
2 - SetPasswordChange
Selected option:[2]
2

Network Devices
--------------------------------------------------------------------------------
TACACS+ and RADIUS network devices with same IP address will be unified.
Select a name to be used for unified devices.
1 - RADIUSName
2 - TACACSName
3 - CombinedName
Selected option:[3]

DACL name construction
--------------------------------------------------------------------------------
Existing downloadable ACL will be migrated.
Select a name to be used for the migrated DACL
1 - DaclName_AclName
2 - AclName
Selected option:[1]

Save user defaults? [yes]
yes

Enter ACS 4.x Server ID:
acs1

Add server-specific migration prefixes?[no]
yes

You can add a global prefix to all migrated objects from this server.
Enter a global prefix:[]
s1

Use special prefixes for specific object types?[no]
yes

** To input an empty prefix, enter the keyword EMPTY.

User Attributes Prefix: You can add an additional prefix to the user attributes.
Enter a prefix to add to these objects:[s1]

Network Device Prefix: You can add an additional prefix to the network devices names.
Enter a prefix to add to these objects:[s1]

Users Command Set Prefix: Extracted command sets are migrated to a shared named object with an optional
prefix.
Enter a prefix to add to these objects:[s1]

Groups Command Set Prefix: Extracted command sets will be given the group name with an optional prefix.
Enter a prefix to add to these objects:[s1]

Groups Shell Exec Prefix: Extracted shell profile will be given the group name with an optional prefix.
Enter a prefix to add to these objects:[s1]

Shared Command Sets Prefix: Extracted command sets are migrated to a shared named object with an
optional prefix.
Enter a prefix to add to these objects:[s1]
```

```
Shared Downloadable ACL Prefix: Extracted Downloadable ACL will be given a name with an optional
prefix.
Enter the prefix to add to such objects:[s1]

RAC Prefix: Existing RAC will be migrated with an optional prefix.
Enter the prefix to add to such objects:[s1]

User Groups Root Prefix: You can add a prefix to the user groups root.
Enter a prefix to add to the user groups root:[s1

Network Device Groups Root Prefix: You can add a prefix to the network device groups root.
Enter a prefix to add to the network device groups root:[s1]

Save server migration prefixes?[yes]
yes

Show full report on screen?[yes]
yes

--------------------------------------------------------------------------------

Select the ACS 4.x Configuration groups to be migrated:[1]
1 - ALLObjects
2 - AllUsersObjects
3 - AllDevicesObjects
4 - SharedCommandSet
5 - SharedDACLObject
6 - MasterKeys
7 - SharedRACObjectWithVSA
--------------------------------------------------------------------------------

6
--------------------------------------------------------------------------------

The following object types will be extracted:
--------------------------------------------------------------------------------

EAP FAST - Master Keys
--------------------------------------------------------------------------------

Choose one of the following:
1 - AnalyzeAndExport
2 - Import
3 - CreateReportFiles
4 - Exit
--------------------------------------------------------------------------------

4
--------------------------------------------------------------------------------
Would you like to migrate another ACS4.x server? [no]
yes

--------------------------------------------------------------------------------
Enter ACS 4.x Sever ID:
```

Migration Script Sections

- Migration environment information. See Table 1Migration Script Environment Information, page 5.
- Migration user preferences. See Table 2Migration Script User Preferences, page 6.
- Migration groups. See Table 3Migration Script Object Groups, page 8.

- Migration phases. See Table 4Migration Script Phases, page 9.

Table 1 Migration Script Environment Information

Script Element	Description
`Use saved user defaults?[yes]`	This prompt is displayed when you rerun the Migration Utility to migrate multiple instances. The default is yes. Enter **no** if you want to enter a different IP address and credentials for the ACS 5.8 target machine.
`Make sure that the database is running.`	Informational message. Ensure that: ■ ACS 4.x services are active. ■ You back up the database on the ACS 4.x source machine. ■ You have IP address connectivity. ■ You can access the ACS 5.8 target machine from the ACS 4.x migration machine. Access the web interface to verify that the ACS 5.8 machine is available. The migration interface is enabled after you run the **`acs config-web-interface migration enable`** command.
`Enter ACS 5 IP address or hostname:[`*`nn.nn.nnn.nnn`*`]`	Enter the IP address or the hostname for the ACS 5.8 target machine. You migrate the ACS 4.x data to the ACS 5.8 target machine.
`Enter ACS 5 administrator username:[`*`test`*`]`	Enter the username for the ACS 5.8 target machine. ACS 5.8 supports only admin users. ACS 5.8 supports migration operation with any ACS administrator with a recovery superadmin role.
`Enter ACS 5 password:`	Enter the password for the ACS 5.8 target machine.
`Change user preferences?[no]`	The default value is **no**. ■ Enter **no** to retain the defined values. These become the UseDefaults values when you rerun the Migration Utility. ■ Enter **yes** to change the user preferences.

Table 2 Migration Script User Preferences

Script Element	Description
User Groups Existing user groups will be migrated to the Identity Group Enter new Root name:[Migrated Group]	The default name for the Identity Group is *Migrated Group*. For example, user *acs_3* is in the following Identity Group: *All Groups:Migrated Group:ACS_Migrate 2*. Type a new name and press **Enter** to change the default name.
Network Device Groups Existing network device groups will be migrated to the Network Device Group. Enter new Root name:[Migrated NDGs]	The default name for a Network Device Group (NDG) is *Migrated NDGs*. Type a new name and press **Enter** to change the default name.
Consolidation Prefix Identical objects found will be consolidated into one object. Enter a prefix to add to the consolidated object:[cons]	Enter a prefix that you want to add to the consolidated objects.
Users ACS 5 supports authentication for internal users against the internal database only. ACS 4.x users who were configured to use an external database for authentication will be migrated with a default authentication password. Specify a default password.	The default password for external users for the User object. Type a new password and press **Enter** to change the default password. ACS 5.8 supports authentication for internal users against the internal database only. ACS 4.x users who were configured to use an external database for authentication are migrated with a default authentication password. You can configure the default password in ACS 5.8.
Disabled Group Users ACS 4.x users and hosts that are associated with disabled group will be migrated as disabled:[yes]	Users and hosts who are associated with disabled user groups are migrated under one group as disabled.
Configure these users as disabled in ACS 5, or ask for a change of password on a user's first attempt to access ACS 5. Select the option: 1 - DisableExternalUser 2 - SetPasswordChange Selected option:[2]	ACS 4.x users authenticated on an external database are migrated as internal users with a static password. ■ Select option 1 to disable the external user. ■ Select option 2 to change the password for the migrated external user.
Network Devices TACACS+ and RADIUS network devices with same IP address will be unified. Select the name to be used for unified devices. 1 - RADIUSName 2 - TACACSName 3 - CombinedName Selected option:[3]	Combines the TACACS+ and RADIUS network devices with the same IP address into one name. For example, if the TACACS+ network device name is *MyTacacsDev* and the RADIUS network device is *MyRadiusDev*, choose option 3 to create the combined name *MyTacacsDev_MyRadiusDev*.
DACL name construction Existing downloadable ACL will be migrated. Select the name to be used for the migrated DACL 1 - DaclName_AclName 2 - AclName Selected option:[1]	Select a naming convention to be used for the migrated ACS 4.x DACL: 1 - DACL_ACL Name 2 - ACL Name
Save user deafults?[yes]	The default value is **yes**. Enter **no** if you do not want to preserve the setting that you used in this session.
Enter ACS 4.x Server ID:	Enter the ACS 4.x server ID from which the data is to be migrated.
Add server specific migration prefixes?[no]	The default is **no**. Enter **yes** to add prefix to each 4.x server name.

Table 2 Migration Script User Preferences (continued)

Script Element	Description

`You can add a global prefix to all migrated`
`objects from this server.`
`Enter a global prefix:[]`
`s1`
	Enter a prefix you want to add to all the objects migrated from one particular server.

`Use special prefixes for specific object`
`types?[no]`
`yes`
`** To input an empty prefix, enter the keyword`
`EMPTY.`
	The default is **no**. This adds the global prefix to all the object types migrated. Enter **yes** if you want to add special prefixes for specific object types to be migrated.

`User Attributes Prefix: You can add an additional`
`prefix to the user attributes.`
`Enter a prefix to add to these objects:[s1]`
	The default is the value entered for global prefix. Enter a prefix if you want to add a special prefix for all migrated user attributes.

`Network Device Prefix: You can add an additional`
`prefix to the network devices names.`
`Enter a prefix to add to these objects:[s1]`
	The default is the value entered for global prefix. Enter a prefix if you want to add special prefix for all migrated network devices.

`Users Command Set Prefix: Extracted command sets`
`are migrated to a shared named object with an`
`optional prefix.`
`Enter a prefix to add to these objects:[s1]`
	The default is the value entered for global prefix. Enter a prefix if you want to add special prefix for all migrated users command sets.

`Groups Command Set Prefix: Extracted command sets`
`will be given the group name with an optional`
`prefix.`
`Enter a prefix to add to these objects:[s1]`
	The default is the value entered for global prefix. Enter a prefix if you want to add special prefix for all migrated groups command sets.

`Groups Shell Exec Prefix: Extracted shell profile`
`will be given the group name with an optional`
`prefix.`
`Enter a prefix to add to these objects:[s1]`
	The default is the value entered for global prefix. Enter a prefix if you want to add special prefix for all migrated groups shell execs.

`Shared Command Sets Prefix: Extracted command sets`
`are migrated to a shared named object with an`
`optional prefix.`
`Enter a prefix to add to these objects:[s1]`
	The default is the value entered for global prefix. Enter a prefix if you want to add special prefix for all migrated shared command sets.

`Shared Downloadable ACL Prefix: Extracted`
`Downloadable ACL will be given a name with an`
`optional prefix.`
`Enter the prefix to add to such objects:[s1]`
	The default is the value entered for global prefix. Enter a prefix if you want to add special prefix for all migrated shared downloadable ACLs.

`RAC Prefix: Existing RAC will be migrated with an`
`optional prefix.`
`Enter the prefix to add to such objects:[s1]`
	The default is the value entered for global prefix. Enter a prefix if you want to add special prefix for all migrated RACs.

`User Groups Root Prefix: You can add a prefix to`
`the user groups root.`
`Enter a prefix to add to the user groups root:[s1]`
	The default is the value entered for global prefix. Enter a prefix if you want to add special prefix for all migrated user groups root.

`Network Device Groups Root Prefix: You can add a`
`prefix to the network device groups root.`
`Enter a prefix to add to the network device groups`
`root:[s1]`
	The default is the value entered for global prefix. Enter a prefix if you want to add special prefix for all migrated network device groups root.

Table 2 Migration Script User Preferences (continued)

Script Element	Description
`Save server migration prefixes?[yes]`	The default is **yes**. Enter **no if you do not want** to save the server migration prefixes.
`Show full report on screen?[yes]`	The default value is **yes**. Enter **no** if you do not want to view the log information on screen.
`Update RADIUS dictionary cache?[no]`	Used to cache the current ACS 5.8 RADIUS dictionary. If you migrate a vendor that was already migrated and deleted in ACS 5.8, you should update the RADIUS dictionary cache. Otherwise, that vendor will not be migrated and will be rejected, and you will receive a message stating that it already exists.

Table 3 Migration Script Object Groups

Script Element	Description

`Select the ACS 4.x Configuration groups to be migrated:`
`1 - ALLObjects`
`2 - AllUsersObjects`
`3 - AllDevicesObjects`
`4 - SharedCommandSet`
`5 - SharedDACLObject`
`6 - MasterKeys`
`7 - SharedRACObjectsWithVSA`
 	
`The following object types will be extracted:`
 	
`User Attributes`
`User Attribute Values`
`Network Device Groups`
`User Groups`
`Groups Shell Exec`
`Groups Command Set`
`Users Shell Exec`
`Users Command Set`
`Shared Command Sets`
`Network Devices`
`Users`
`Shared Downloadable ACL`
`EAP FAST - Master Keys`
`MAB`
`RAC`
`VSA Vendors`
`VSA`
	The ACS elements to be migrated. Choose one of the following options to run each phase against the ACS 4.x elements to be migrated:
	1. ALLObjects. You can run each migration phase against the supported ACS objects.
	2. AllUsersObjects. You can run each migration phase against the User object.
	3. AllDevicesObjects. You can run each migration phase against the Device object.
	4. SharedCommandSet. You can run each migration phase against the Shared Command Set object.
	5. SharedDACLObject. You can run each migration phase against the Shared DACL object.
	6. MasterKeys. You can run each migration phase against the master key object.
	7. SharedRACObjectsWithVSA. You can run each migration phase against the Shared RAC object and VSA.

Table 4 Migration Script Phases

Script Element	Description

`Choose one of the following:`
`1 - AnalyzeAndExport`
`2 - Import`
`3 - CreateReportFiles`
`4 - Exit`
	Migration Utility options:
	■ AnalyzeAndExport—Choose option 1 to analyze and export the ACS 4.x data. This is an iterative process. You can analyze the data, make corrections, and rerun the Analysis phase to see the results.
	If data passes the Analysis phase, it can be exported and imported to ACS 5.8. See Migration of ACS 4.x Objects, page 9.
	Ensure that you back up your ACS 5.8 database.
	■ Import—Choose option 2 to import the ACS 4.x data from the external data file. After the migration process creates the data export file, the data is imported into ACS 5.8. See Importing the ACS 4.x Data to ACS 5.8, page 36.
	■ CreateReportFiles—Choose option 3 to create a comma-separated value (CSV) file containing a full and summary report for each phase. You can upload the CSV file to an Excel spreadsheet or any other editor that supports CSV files.
	The *config* folder in the migration directory contains the full and summary reports. See Printing Reports and Report Types, page 39.
	■ Exit—Choose option 4 to exit the Migration Utility or if you want to migrate another ACS 4.x instance.

`Would you like to migrate another ACS 4.x server? [no]`	The default value is **no**. Enter **yes to migrate another ACS 4.x instance.**

Migration of ACS 4.x Objects

The following sections describe in detail the various phases in the migration procedure and the impact and considerations for each object type.

- AAA Client/Network Device, page 10
- NDG, page 14
- Internal User, page 16
- User Group, page 23
- User Group Policy Components, page 24
- Shared DACL Objects, page 28
- Shared RACs, page 30
- RADIUS VSAs, page 31
- EAP-Fast Master Keys and the Authority ID, page 33

AAA Client/Network Device

In ACS 4.x, the Network Configuration option contains NDGs, which in turn can contain AAA servers or AAA clients. The AAA client definitions are migrated and stored within the Network Devices and AAA Clients option in ACS 5.8.

This section contains:

- Data Mapping, page 10
- Analysis and Export, page 11
- Import, page 13
- Multiple-Instance Support, page 13

Data Mapping

Table 5 on page 10 shows the data mapping between ACS 4.x and ACS 5.8, for the AAA client or Network Devices.

Table 5 Data Mapping for AAA Client or Network Devices

4.x Attribute Name	5.8 Attribute Name	Comment
AAA Client Hostname	Name	–
–	Description	There is no description to be retrieved from ACS 4.x. A predefined description of *Migrated* is used for all the migrated devices.
Shared Secret	Shared Secret	ACS 5.8 records contains separate fields for RADIUS and TACACS+ shared secrets. The specific field set in an ACS 5.8 record depends on the setting for the Authentication using field.
Network Device Group	Network device group under All migrated NDGs	–
Authentication using	Selection of either RADIUS or TACACS+ options	ACS 4.x has a list of all the supported RADIUS vendors. This information is not retained in ACS 5.8. If a RADIUS vendor is selected, it is marked as Authenticating using RADIUS.
AAA Client IP Address	IP	Representations are different.
Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	Single Connect Device	–
Legacy TACACS+ Single Connect support for this AAA client	Legacy TACACS+ Single Connect Support	Available only in 4.2 cumulative patch 1 and 4.1.4.13 patch 10 and higher.
TACACS+ Draft compliant Single Connect support for this AAA client	TACACS+ Draft Compliant Single Connect Support	Available only in ACS 4.2 cumulative patch 1 and ACS 4.1.4.13 patch 10 and higher.

Table 5 Data Mapping for AAA Client or Network Devices (continued)

4.x Attribute Name	5.8 Attribute Name	Comment
■ Log Update/Watchdog Packets from this AAA Client (the only option for servers) ■ Log RADIUS Tunneling Packets from this AAA Client ■ Replace RADIUS Port info with Username from this AAA Client ■ Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	—	Not supported in ACS 5.8.
Key Encryption Key	keyEncryptionKey	The key length depends on the following display type: ■ HEX—The key length is 32 characters ■ ASCII—The key length is 16 characters
Message Authenticator Code Key	messageAuthenticatorCodeKey	The key length depends on the following display type: ■ HEX—The key length is 40 characters ■ ASCII—The key length is 20 characters
Key Input Format	Key Input Format	Boolean

Note: The group’s Single Connect flag overwrites the device’s Single Connect flag.

Analysis and Export

There are three major differences between the AAA Client (ACS 4.x) and Network Device (ACS 5.8) definitions:

- In ACS 5.8, it is possible to define one network device that handles both RADIUS and TACACS+, while in ACS 4.x, two different AAA clients are required.
- In ACS 5.8, IP address is defined as a pair consisting of an IP address and a mask, while in ACS 4.1, IP address is defined using regular expressions.
- In ACS 5.8, each network device definition is limited to storing 40 IP addresses. In ACS 4.x, it is possible to define more than 40 IP addresses.

This section contains:

Unsupported Characters in a Device Name

Some special characters are not allowed in the device name during export. You will get an error message during the analysis and the export will not proceed if the following characters are used in the device name:

{} " '

Overlapping IP Addresses

In ACS 4.x, you can create definitions with overlapping IP addresses as part of a network device, where the first IP address utilizes TACACS+ and the second IP address utilizes RADIUS.

In ACS 5.8, TACACS+ and RADIUS are unified within a single network device definition. However, the unification is not possible if TACACS+ and RADIUS are part of different NDGs in ACS 4.x.

In the migration analysis phase, the network group and overlapping IP addresses are identified and reported to the administrator so that these definitions can be modified to conform to the ACS 5.8 requirements.

For example:

`Network device` *`AA`*`: IP address` = *23.8.23.*, 45.87.*.8*, `protocol` = *RADIUS*, `group` = *HR*

`Network device` *`BB`*`: IP address` = *45.*.6.8, 1.2.3.4*, `protocol` = *TACACS*, `group` = *Admin*

In this example, the second IP address in the *AA* network device list overlaps the first IP address in the *BB* network device list, and each of the network devices is part of a different NDG.

Consolidation between separate entries for RADIUS and TACACS+ network devices is possible only if the IP addresses are identical and both of the network devices are part of the same NDG. All consolidation is reported in the Analysis report.

IP Address Translation

ACS 5.8 supports wildcards and ranges. If you specify the IP address as in ACS 4.x, all existing IP addresses in ACS 4.x are migrated to ACS 5.8.

For example, the following IP address patterns can be translated:

- 1.*.*.10-15
- 1.2.3.13-17

IP Subnets Limit

The migration analysis process identifies the network devices with more than 40 IP subnets and reports that these devices cannot be migrated. To allow migration, you can change them to subnet masks or split them into multiple network device definitions to conform to the ACS 5.8 format. *Table 6 on page 13 describes the ACS 4.x attributes that can be modified to conform to ACS 5.8 limitations.*

Key Wrap Attributes

The keys that contain the following characters are identified during the analysis phase:

- 27 HEX
- 22 HEX

An error message appears during the analysis phase and the export will not proceed, if any of the following characters are found in the network device's Key Encryption Key or in the Message Authenticator Code Key:

' "

Table 6 on page 13 describes the ACS 4.x attributes that can be modified to conform to ACS 5.8 limitations.

Table 6 Attribute Modification

Attribute Name in 4.x	Comment
Authentication using	Any selection for a specific RADIUS vendor is translated to *Authenticate Using RADIUS*. For example, RADIUS (Cisco Aironet) is translated to RADIUS.
AAA Client IP Address	ACS 5.8 supports wildcards and ranges. If you specify the IP address as in ACS 4.x, all existing IP addresses in ACS 4.x are migrated to ACS 5.8.
Shared Secret	For devices that belong to an NDG where the NDG includes a shared secret. The NDG's shared secret is extracted and included in the network device definition, instead of in the network device definition shared secret.
Key Encryption Key	For devices that belong to an NDG where the NDG includes a Key Encryption Key. The NDG's Key Encryption Key is extracted and included in the network device definition, instead of being defined with the network device definition Key Encryption Key.
Message Authenticator Code Key	For devices that belong to an NDG where the NDG includes a Message Authenticator Code Key. The NDG's Message Authenticator Code Key is extracted and included in the network device definition instead of being defined with the network device definition Message Authenticator Code Key.

Import

The Unified Device Name setting is used during import of network devices. In ACS 5.8, configuration options are available to determine the name of the new device in ACS 5.8, if there are separate RADIUS and TACACS+ devices in ACS 4.x that can be unified into a single network device definition. The following options are available in ACS 5.8:

- Name of RADIUS Device
- Name of TACACS+ Device

ACS 4.x contains a single-level hierarchy between a network device and an NDG. Each defined network device (AAA client) must be included in one of the NDGs. To keep this association between the network device and the NDG, ACS 5.8 first exports and imports the NDGs, and then the network devices with an association to the NDGs. NDGs and network devices are processed as a single object group.

When a new record is imported into ACS 5.8, a default description field called Migrated is created.

Multiple-Instance Support

In ACS 5.8, you cannot define different network devices with an overlapping IP address. You may define a specific (or global) prefix for the network device name to avoid duplicates. However, devices that have overlapping IP addresses are reported as duplicates and are not migrated, even though their names are unique. Also, merge between two such instances is not supported.

For example:

`Instance` = *X,* `network device` = *AA,* `IP address` = *23.8.23.12,* `protocol` = *RADIUS,* `group` = *HR*

`Instance` = *Y,* `network device` = *BB,* `IP address` = *23.8.23.12,* `protocol` = *TACACS+,* `group` = *HR*

In this example, you cannot create a unified device, since the network device *AA* is from instance X and the network device *BB* is from instance Y. If the TACACS+ and RADIUS devices are from the same instance, unified device creation is supported.

Devices that are associated to an NDG that was imported in a previous migration instance are associated to the NDG that already exists in ACS 5.8.

NDG

To facilitate migration of the ACS 4.x NDG definitions, an additional NDG hierarchy has been created in ACS 5.8.

During the migration process, you are prompted to enter the name of the hierarchy root that stores the ACS 4.x NDG definitions. The prompt offers a default name of the migrated NDG; you can modify this name as desired.

ACS 4.x contains an unsaved group known as Not Assigned NDG for all the devices that do not belong to any group. The Not Assigned NDG group is created after export to ACS 5.8.

In ACS 4.x, the NDGs contain attributes such as shared secret and Legacy TACACS+ Single Connect support for the AAA client. However, in ACS 5.8, the NDGs are labels that can be attached to the network device definitions and do not contain data. If a value is set for the shared secret in an ACS 4.x NDG, this value is extracted to set the value for each network device that is associated with the group.

This section contains:

- Data Mapping, page 14
- Analysis and Export, page 15
- Import, page 16
- Multiple-Instance Support, page 16

Data Mapping

Table 7 on page 14 shows the data mapping between ACS 4.x and ACS 5.8 for the NDGs.

Table 7 Data Mapping for NDGs

4.x Attribute Name	5.8 Attribute Name	Comment
Network Device Group Name	Name	–
–	Description	There is no description to be retrieved from ACS 4.x. A predefined description of *Migrated* is used for all the migrated devices.
Shared Secret	–	Value defined in the group is extracted and defined for each network device associated with the group.

Table 7 Data Mapping for NDGs (continued)

4.x Attribute Name	5.8 Attribute Name	Comment
Key Encryption Key	keyEncryptionKey	The key length depends on the following display type: ■ HEX—The key length is 32 characters ■ ASCII—The key length is 16 characters Value defined in the group is extracted and defined for each network device associated with the group.
Message Authenticator Code Key	messageAuthenticatorCodeKey	The key length depends on the following display type: ■ HEX—The key length is 40 characters ■ ASCII—The key length is 20 characters Value defined in the group is extracted and defined for each network device associated with the group.
Key Input Format	Key Input Format	Boolean Value defined in the group is extracted and defined for each network device associated with the group.

Analysis and Export

The following items are reported during the analysis phase:

- Special characters in the NDG name—Some special characters are not allowed in the NDG name during export. An error message appears during the analysis and the export will not proceed if the following characters are used in the NDG name:

  {} | " = ' :

- NDGs that contains a shared secret definition—A message indicates that the shared secret definition will override the values defined at the device level.
- NDGs that contain either Key Encryption Key or Message Authenticator Code Key definition—A message indicates that Key Encryption Key or Message Authenticator Code Key definition will override the values defined at the device level.
- Special characters in the network device's Key Encryption Key or in the Message Authenticator Code Key—An error message appears during the analysis phase and the export will not proceed, if any of the following characters are found in the network device's Key Encryption Key or in the Message Authenticator Code Key:

  ' "

No similar information is displayed during the export phase.

Import

During the import phase, a new NDG hierarchy is created, with the name as defined in the User Preferences. A root node with name as per the User Preferences, prefixed by *All,* is also created. All the migrated NDGs are created under this root node.

Multiple-Instance Support

In ACS 5.8, you cannot define two NDGs (hierarchy node) with the same name on one hierarchy root; however, it is possible to define them on different hierarchies. For example, you can define two groups named *Engineers*, one on the root *SJ* and the other on the root *NY*. Multiple-instance support allows you to do one of the following to migrate the NDGs:

- Define a different root for each instance and import all the NDGs of the instance under the instance root.
- Define one root for all the migrated NDGs; the Migration Utility adds only the unique NDGs to the root. NDGs that already exist are reported as duplicates and are not imported. However, in this case the ID of the already existing NDG is retrieved for association purposes.

To choose either of these options, go to **Preferences > User Interface**. For each selection, the association between the NDG and the network devices is maintained according to the logic of that selection.

For example, Device *ABC* (with a unique name and IP address) associated to an NDG *SJ* is migrated from the first ACS 4.x instance. When you select any of the above two options, *ABC* is associated to NDG *SJ*, but *SJ* can be defined either in the root *All* or in the specific root *Engineers*.

Internal User

In ACS 5.8, policy components are reusable objects that can be selected as policy results.

Migration activities that are related to internal users consist of the following aspects:

- Basic User Definition, page 16
- Multiple-Instance Support, page 18
- User Data Configuration and User Mapping, page 18
- User Shell Command Authorization, page 20
- Shell Exec Parameters, page 22

ACS 4.x can contain dynamic users. External databases, such as LDAP, can manage dynamic users, their identities, and other related properties.

Dynamic users are created in the ACS internal database after they are successfully authenticated against external sources. Dynamic users are created for optimization, and removing them does not affect ACS functionality. Dynamic users are ignored by the Migration Utility and are not processed.

Basic User Definition

For each user, the basic definition includes username, password, disable or enable status, and identity group.

This section contains:

- Data Mapping, page 17
- Analysis and Export, page 17
- Import, page 18

Data Mapping

Table 8 on page 17 shows the user interface data mapping of ACS 4.x with ACS 5.8 for internal users.

Table 8 Data Mapping for Internal Users

4.x Attribute Name	5.8 Attribute Name	Comment
User Name	Name	–
Account Disable	■ Status: – Enabled – Disabled ■ Disable Account if Date Exceeds	–
–	Description	There is no description to be retrieved from ACS 4.x. The description used in ACS 5.8 varies depending on the type of user that is defined, as follows: ■ Migrated Internal User ■ Migrated User with External Authentication
Password	Password	–
Group to which the user is assigned	Identity Group	User groups must be migrated first; association to the migrated identity group is retained.
Separate TACACS+ Enable Password	Enable Password	–

Analysis and Export

Some special characters and <space> are not allowed in the username during export. It is reported in the Analysis report if the following characters are used in the username:

<> " * ? { }

By default, internal users who are authenticated to use an external password type are migrated as internal users with an internal password type. with external password type are migrated with the password type, as internal users. Users with an internal password type are reported in the Analysis report.

Users with a password of fewer than four characters are not exported. The option “Disable Account if Date Exceeds” is also migrated in ACS 5.8.

Note: User Command Sets are not migrated for users whose username contains an apostrophe (’).

The following options are available in the password definitions for internal users:

- Internal—Password is stored internally in ACS.
- External Database—Password is stored in an external database, and authentication is performed against this database.
- Empty Password—VoIP users can be defined by associating them with a group that has the following settings selected “*T***his is a Voice-over-IP (VoIP) group** and **all users of this group are VoIP users”**. In this case, no password is defined for the user.

Import

Externally authenticated users are not supported in ACS 5.8. The following configuration options are available to define the import of such users:

- Default authentication password—All externally authenticated users are assigned with this password.
- Disabled or Change password—You can select whether such users are defined in ACS 5.8 as disabled or are required to change their password on the next login.

No analysis warnings are displayed for such users, because there could be a large number of users.

Note: VoIP is not supported in ACS 5.8. Users that are associated with a VoIP-enabled user group are reported as part of the analysis and are not exported.

Multiple-Instance Support

Duplicate identification of users from different ACS 4.x instances is based on the username and is reported in the Import report. Only unique users are migrated. There is no support for a name prefix or merge between users' data from multiple ACS 4.x instances.

For example, it is not possible to add an enable password to the user *Jeff,* if *Jeff* exists in multiple ACS 4.x instances and the enable password exists only on the instance that was not migrated first.

Users who have a unique username and are associated to a user group are migrated and the association preserved, even if the user group itself was migrated in the same instance as the user or in a previous instance.

Note: If the user does not pass migration, user attribute values and policy components such as TACACS+ and Shell attribute values and the Command Set that originated from the user, are also not migrated, even if they are valid.

User Data Configuration and User Mapping

ACS 4.x contains up to five user-defined fields that can be selected for inclusion in the user record. For each such field, a corresponding field name can be defined. In ACS 5.8, these fields are migrated so that equivalent user attributes can be created and then populated for each user.

To configure these fields, select **Interface Configuration > User Data Configuration**. You must repeat the configuration for each of the five fields.

This section contains:

- Data Mapping, page 18
- Analysis and Export, page 19
- Import, page 19
- Multiple-Instance Support, page 19

Data Mapping

Table 9 on page 19 shows the user interface data mapping between ACS 4.x and ACS 5.8 for User Data Configuration and User Mapping.

Table 9 Data Mapping for User Data Configuration and User Mapping

4.x Attribute Name	5.8 Attribute Name	Comment
Display	–	If enabled, the corresponding field name is extracted; otherwise it is ignored.
Field Name	Attribute	–
–	Description	There is no description to be retrieved from ACS 4.x. A predefined description of *Attribute added as part of the migration process* is used for all attributes.

Analysis and Export

Analysis is performed on the field name to check:

- The field length does not exceed 32 characters.
- The field does not contain the following special characters

  { } ' "

Import

In ACS 4.x, you can define multiple field names with the same name. However, in ACS 5.8, user-defined attributes must have unique names. If multiple attributes have the same name, the original name is retained only for the first attribute found. For subsequent attribute, the suffix _1 is added.

For example, if three attributes in ACS 4.x have the name *ACS*, after import to ACS 5.8, the attribute names are as follows:

- First attribute–ACS
- Second attribute–ACS_1
- Third attribute–ACS_2

Multiple-Instance Support

In ACS 5.8, you cannot define two user attributes with the same name on the identity dictionary. However, you can create a name prefix for each ACS 4.x instance and add the attribute for each instance.

You can select one of the following options to migrate the user attributes:

- Define a different name prefix for each instance and import all the user attributes with different names.
- Do not define a prefix. This results in unique attributes migration only. Attributes that already exist are reported as duplicates. In this case, the ID of the existing user attribute is preserved for association purposes.

User data for any user is taken only from a single ACS 4.x instance. If the same user exists in another ACS 4.x instance, the user is not imported but the user attributes are migrated with null values. There is a single set of internal user attributes that applies to all users.

For example, you migrate the user, *user1* with user attribute *A* with value *x* and user attribute *B* with value *y,* from first ACS 4.x instance. Then, you migrate the same user, *user1* with user attributes *C* with value *z* and user attribute *D* with value w, from the second ACS 4.x instance.

Here, the user *user1* from the second instance is not migrated, but the user attributes *C* and *D* are migrated with null values. The user *user1* in ACS 5.8 contains the following attributes:

- *A* with value *x*
- *B* with value *y*
- *C* with null value from the second instance.
- *D* with null value from the second instance.

The same user can contain attributes from second instance but not the attribute values. You cannot merge user attributes from multiple ACS 4.x instances.

For example, it is not possible to add only the attribute *Real Name: Jeffrey* to user *jeff,* if the user already exists in ACS 5.8 (migrated from another ACS 4.x instance) and the attribute *Real Name: Jeffrey* exists only on the current ACS 4.x instance.

The association between the user and the user attribute is preserved regardless of the migration run (current or previous migration) when the user attribute definition is migrated. A user with a unique username (that can be added in the current run) that is associated with a user attribute that already exists in ACS 5.8 (and was migrated in a previous run of the migration) is associated to the existing user attribute.

In ACS 5.8, every identity attribute that gets added to the dictionary also gets added to all the users, even if the value is blank.

For example, you create user, *User1* in ACS 4.x first instance and start the Migration Utility. Enter the first instance server ID and add server specific migration prefix *global1*. Migrate the user, *User1* with user attributes city, real name and description.

Create user, *User2* in ACS 4.x second instance and start the Migration Utility. Enter the second instance server ID and add server specific migration prefix *global2*. Migrate the user, *User2* with user attributes city, country and state.

After migration to ACS 5.8, *user1* will contain the attributes, *global1_city, global1_Description, global1_Real Name, global2_city, global2_country and global2_state*.

User2 will contain the attributes, *global1_city, global1_Description, global1_Real Name, global2_city, global2_country and global2_state*.

Here, attributes with prefix *global1* should be used for *User1* and attributes with prefix *global2* should be used for *User2.*

User Shell Command Authorization

In ACS 4.x, a shell command set can be embedded in the user record. As part of the migration functionality, this command set is extracted and defined as a shared object. A user attribute contains the name of a command associated with a user that was retrieved from the user record.

User command sets are migrated to shared command sets only if the user is migrated. The name is generated from the username.

Shared command sets are extracted only if the corresponding user was migrated.

This section contains:

- Data Mapping, page 20
- Analysis and Export, page 21
- Import, page 21
- Multiple-Instance Support, page 21

Data Mapping

Table 10 on page 21 shows the user interface data mapping between ACS 4.x and ACS 5.8 for the user shell command authorization.

Table 10 Data Mapping for User Shell Command Authorization

4.x Attribute Name	5.8 Attribute Name	Comment
Unmatched Cisco IOS Commands (Permit / Deny)	Permit any command that is not in the list of commands.	–
Command, followed by list of arguments each of format: `permit / deny < arguments >`	List of commands in the format: permit / deny <command> <arguments>	–
–	Description	There is no description to be retrieved from ACS 4.x. A predefined description of *Attribute added as part of migration process* is used for all the attributes.
Unlisted arguments (Permit / Deny)	Additional entry after each list of arguments for specific command, in the format: permit / deny <command>	–

Analysis and Export

In ACS 4.x, you can assign a shell command authorization set on a per-NDG basis, where the user record contains pairs of device group names and command set names. This equivalent functionality is not supported in ACS 5.8, and a message is displayed during analysis.

Import

The following user settings are used during import of each user command set:

- Command set name format options–Add Prefix | User Name only.
- Text for prefix.
- Prefix to be added for consolidated objects in addition to the previous prefix–Default is an empty string

The user attribute *cmd-set* is used to store the name of the ACS 5.8 command set that is migrated from a user definition.

To import a user command set:

1. Create the *cmd-set* user attribute.
2. For users who have a per-user definition of a command set:

a. If the command set has been consolidated into another record, then proceed to process the next user.

   a. Determine the name of the command set as a combination of the username and any defined prefixes.

   b. Create the migrated command set.

3. Set the name of the migrated command set in the *cmd-set* user attribute for the user.

Multiple-Instance Support

In ACS 5.8, you cannot define two command sets with the same name. However, you can create a command set with a name prefix per ACS 4.x instance and migrate the command sets for each ACS 4.x instance.

Thus, you can choose one of the following options to migrate command sets:

- Define a different name prefix for each instance and import all the command sets with different names.
- Do not define a prefix. Only unique command sets are migrated. The command sets that already exist (migrated in the previous instance), are reported as duplicates.

Shell Exec Parameters

In ACS 4.x, the user record contains shell (exec) TACACS+ settings. These settings are migrated to ACS 5.8 as attributes of the user record. If one of these attributes is in use for any of the migrated user records, it is created as a user attribute. The value is set in the corresponding attribute in the migrated user definition.

The user shell attribute values are migrated only if the user is migrated.

This section contains:

- Data Mapping, page 22
- Analysis and Export, page 22
- Import, page 23
- Multiple-Instance Support, page 23

Data Mapping

Table 11 on page 22 shows the data mapping between ACS 4.x and ACS 5.8 for the user shell attribute. All attributes, except the Max Privilege attribute, are taken from the TACACS+ shell (exec) settings.

Table 11 Data Mapping for User Shell Attribute

4.x Attribute Name	5.8 Attribute Name	Comment
TACACS+ Enable Control: Max Privilege for any AAA Client	Max_priv_lvl (unsigned integer 32)	–
Access control list	ACL (string)	–
Auto command	Autocmd (string)	–
Callback line	Callback-line (string)	–
Callback rotary	Callback-rotary (string)	–
Idle time	Idle time (unsigned integer 32)	–
No callback verify	No callback-verify (Boolean)	–
No escape	No escape (Boolean)	–
No hangup	No hangup (Boolean)	–
Privilege level	Priv_lvl (unsigned integer 32)	–
Timeout	Conn-timeout (unsigned integer 32)	–

Analysis and Export

ACS 5.8 supports the privilege level as a numeric value (0-9999). In ACS 4.x, privilege level is a string field with no validity checks. If the privilege level is not within the valid range, it is reported to the administrator.

This check is not applicable to the enable password, where the privilege level is selected from a valid list. However, an additional analysis verifies that the privilege level in the shell exec settings does not exceed the maximum enable privilege. Custom parameters defined in the shell exec are not supported in ACS 5.8. Invalid idle time and timeout values are reported in the Analysis report.

Import

The shell exec parameters for all the users are collected. If a parameter exists for at least one of the users being migrated, it is migrated as a user attribute. In ACS 4.x, if the shell exec value is defined for each user being migrated, in ACS 5.8, this value is set in a user attribute associated with the user in ACS 5.8. If the attribute is not defined in ACS 4.x, it is left blank in ACS 5.8.

Multiple-Instance Support

The Shell attribute has a fixed name. You cannot create Shell attributes with a name prefix per ACS 4.x instance. Also, you cannot merge the Shell attributes data (values) from multiple ACS 4.x instances.

For example, you cannot add only the attribute *Timeout:123* to user *jeff*, if the user already exists in ACS 5.8 and that shell attribute is not defined on the user.

The association between a user and the shell attribute is preserved regardless of the run (current or previous migration) when the shell attribute definition is migrated.

A user with a unique username (that is added in the current run) is associated with a shell attribute that already exists in the ACS 5.8 identity dictionary (that was migrated in the previous run of the migration).

If the same user exists in another ACS 4.x instance, the user is not imported, but the user shell attributes are migrated with null values. There is a single set of internal user shell attributes that applies to all users. In ACS 5.8, every user shell attribute that gets added to the dictionary also gets added to all the users.

User Group

In ACS 5.8, the identity group is equivalent to the user groups. However, each identity group is purely a logical container to group sets of users for the purposes of policy processing and selection in rules conditions.

The user group names are migrated and merged into the identity group hierarchy. A new node is created beneath the root node of the identity hierarchy and under this node, all the migrated user groups are placed in a flat structure. You are prompted to define the name of this node. A default name is also presented.

In ACS 4.x, 500 user groups are created by default, and these groups can be edited by the administrator. In ACS 5.8, only the user groups that are being utilized and referenced from user or MAC definitions are migrated.

To keep the association between the users and user groups (the identity groups), you must first export (and import) the user groups, followed by the internal users with associations to those user groups.

This section contains:

Analysis and Export

A user group that does not contain any internal users or MAC definitions is not exported. It is reported to the administrator that such user groups have not been migrated. In addition, some special characters are not allowed in the group name during export. This will be reported in the Analysis report and the export will not proceed if the following characters are used in the group name:

{ } | ' " = :

Import

During import, a new identity group node, with a name defined in the User Preferences, is created under the root node of the identity group hierarchy. The default name is *Migrated Group*. All migrated user groups are created in a flat hierarchy under this newly created node.

In ACS 4.x, each user was associated to a single group. To keep the association between the users and user groups (the identity group) the user groups are imported first, followed by the internal users with associations to the user group.

Multiple-Instance Support

In ACS 5.8, you cannot define two identity groups with the same name on one hierarchy root. However, you can define them on different hierarchies.

For example, you can define two groups named *Engineers,* one on the root *NY* and the other on the root *SJ*. The multiple-instance support allows you to select one of the following options to migrate the groups:

- Define a different root for each instance and import all the user groups of the instance under the instance root.
- Define one root for all the migrated groups. The Migration Utility adds only unique groups to the root. Groups that already exist are reported as duplicates and are not imported. However, the ID of the already exiting user group is retrieved for association purposes.

To select either of the options, go to **User Preferences**. The association between user group and users is maintained according to the logic of that selection.

For example, the user *john* (unique username) is associated to the group *Management,* which was migrated from a previous run of an ACS 4.x instance. On any option selected, *john* is associated to the group *Management*, but *Management* is defined in the root *All* or in the specific root *Engineers*.

User Group Policy Components

In ACS 4.x, most of the policy-related authorization data is embedded within the user group definitions, whereas in ACS 5.8, this data is defined as shared objects.

Data is migrated only from the groups that are in use. The following data is extracted from the group data:

- TACACS+ shell command authorization set is migrated to a command set.
- TACACS+ shell exec (+max privilege level) is migrated to a shell profile.

This section contains:

Group Command Set

The names of the command sets extracted from the users are stored in a user attribute. No similar action is performed when the data is extracted from the user groups. The multiple-instance support for the groups’ command sets is similar to the users’ command sets.

Note: Group command sets are migrated only when the groups are migrated.

Group Shell Exec

This section contains:

- Data Mapping, page 25
- Analysis and Export, page 25
- Import, page 25
- Multiple-Instance Support, page 26

Data Mapping

Table 12 on page 25 shows the mapping of attributes from the group data to attributes in the shell profile. Each field in a shell profile has a flag to indicate whether the field is present in the profile. If a field is not enabled in the group record, it is marked as not present in the shell profile.

Table 12 Data Mapping for Group Shell Exec

4.x Attribute Name	5.8 Attribute Name	Comment
Enable Options: Max Privilege for any AAA client	Maximum Privilege Level	–
Access control list	Access Control List	–
Auto command	Auto Command	–
Callback line	Callback Line	–
Callback rotary	Callback Rotary	–
Idle time	Idle time	–
No callback verify	No Callback Verify	–
No escape	No Escape	–
No hangup	No Hang Up	–
Privilege level	Default Privilege Level	–
Timeout	Timeout	–

Analysis and Export

Analysis is performed on all groups that are determined to be in use and that are associated either with users or MAC addresses. The analysis verifies that the following values entered in ACS 4.x are in a valid range for the corresponding ACS 5.8 object:

- Timeout: 0-9999
- Idle Time: 0-9999
- Privilege Level: 0-15

In ACS 5.8, you can include wildcards in the MAC address, but wildcards can be used only with a specific ObjectID for example, "00-00-00-*. The following wildcard format is not supported: 11-11-11-11-11-*

The analysis also verifies that the new default privilege level value is not higher than the maximum value. If a group to be migrated has custom attributes defined, it is not migrated to ACS 5.8, and a warning is displayed.

Import

The following user settings are used during import of the group shell exec:

- Shell profile name format. Options available are:
  - Add prefix
  - Group name only
- Text for prefix.
- Prefix to be added for consolidated objects in addition to the prefix above. The default is an empty string.

The import process is performed for each shell exec that is not consolidated into another object. The name of the ACS 5.8 object is determined based on the user settings and the created shell profile.

Note: Group shell attributes are migrated only when the group is migrated.

Multiple-Instance Support

Group Shell attributes are migrated to shared shell profiles and the name is generated from the group name.

In ACS 5.8, you cannot define two shell profiles with the same name. However, you can create shell profiles with a name prefix per ACS 4.x instance, and thus you can add a shell profile for each instance. With multiple-instance support, you can select one of the following options to migrate the shell profiles:

- Define a different name prefix for each instance and import all the shell profiles with different names.
- Do not define a prefix. This results in a uniquely named shell profile migration. Shell profiles that already exist are reported as duplicates.

MAC Addresses and Internal Hosts

In ACS 4.x, support for authentication based on MAC address is as follows:

- Define the MAC address as an internal username with a Password Authentication Protocol (PAP) password that is identical to the username. The user is migrated into the internal user database and there is no need for additional support for MAC addresses.
- Define the MAC address in the NAP table as part of the authentication policy. Within the authentication policy, you can configure to authenticate the MAC address with the ACS internal database. You can then provide a list of MAC addresses and a corresponding identity. The MAC addresses are migrated to the corresponding records in the internal host's database.

In ACS 5.8, you can define additional attributes to be associated with the hosts, as is done for the users. However, in ACS 4.x, there is no additional data associated with the MAC definitions, and hence no additional attributes are required for migration. However, the association with the identity group is retained.

This section contains:

Data Mapping

Table 13 on page 27 shows the data mapping between ACS 4.x and ACS 5.8 for MAC addresses and internal hosts.

Table 13 Data Mapping for MAC Addresses and Internal Hosts

4.x Attribute Name	5.8 Attribute Name	Comment
MAC Addresses stored in authentication section of a NAP	MAC Address	Can contain a list of addresses. An internal host definition is created for each address that is defined.
–	Status	All migrated entries are set as enabled.
–	Description	There is no description to be retrieved from ACS 4.x. A predefined description of *Migrated From ACS 4.x* is used for all the definitions.
User Group	Identity Group	Set to reference the same identity group, located in the ACS 5.8 identity group hierarchy.

Analysis and Export

You can enter MAC addresses in multiple formats, but they are always stored in *12-34-56-78-90-AB* format. However, in ACS 4.x it is possible to include a wildcard in the address; for example, *12-34-56-78**.

In ACS 5.8, you can include a wildcard in the MAC address. You can migrate hosts with wildcards that are specified only after the first three octets of the MAC address, along with its associated user group. Hosts without wildcards can also be migrated.

For example:

NAP A has the following MAC addresses: 1-2-3-4-5-6 Group 10.

NAP B has the following MAC address: 1-2-4-* Group 24.

Here, the NAP A MAC address 1-2-3-4-5-6 is migrated along with its associated to group 10. Also, NAP B MAC address 1-2-4-* is migrated along with its associated group 24.

Multiple-Instance Support

In ACS 4.x, duplicate MACs are identified based on the MAC address and are reported in the Import report. Only unique MAC addresses are migrated. There is no support for the name prefix. Unique MAC addresses that are associated to a user group are migrated.

The association is preserved, regardless of whether or not the user group itself was migrated in the same instance as the MAC address or in a previous instance.

Shared Shell Command Authorization Sets

In ACS 4.x, the shell command authorization set can be defined as shared objects, as part of the device administration. Such objects are migrated to the command sets. The name and the description of each object is the same as in ACS 4.x.

This section contains:

Data Mapping

Table 14 on page 28 shows the data mapping between ACS 4.x and ACS 5.8 for shared shell command authorization sets.

Table 14 Data Mapping for Shared Shell Command Authorization sets

4.x Attribute Name	5.8 Attribute Name	Comment
Name	Name	–
Description	Description	–
Unmatched Commands ■ Permit ■ Deny	Check box labeled *Permit any command that is not in the table*	–
Command, followed by the list of arguments each of format: `permit / deny <arguments>`	Entries in command table: ■ Grant: Permit / Deny ■ Command ■ Arguments	–
Unlisted arguments ■ Permit ■ Deny	Additional entry after each list of arguments for a specific command in the format: permit / deny <command>	–

Analysis and Export

Some special characters are not allowed in the shell command authorization set during export. It will be reported in the Analysis report if the following characters are used in the device name:

{ } ' "

Multiple-Instance Support

In ACS 5.8, you cannot define two command sets with the same name. However, you can create them with a name prefix per ACS 4.x instance, and thus you can add a command set for each instance. Thus, with the multiple-instance support, you can select one of the following options to migrate the shared command sets:

- Define a different name prefix for each ACS 4.x instance and import all the command sets with different names.
- Do not define a prefix, resulting in a uniquely named command set migration. Command sets that already exist are reported as duplicates.

Shared DACL Objects

In ACS 4.x, a shared downloadable access control list (DACL) can be defined as a shared object to be referenced from the application. A shared DACL consists of a set of ACL contents, where each ACL is associated with a specific Network Access Filtering (NAF) selection. When the object is referenced, the actual ACL that is utilized depends on the NAF condition that matches first.

ACS 5.8 contains the authorization policy that results in the selection of a DACL from an authorization profile. Therefore, each ACL that is contained within an ACS 4.x shared DACL is mapped to a separate DACL in ACS 5.8.

This section contains:

- Data Mapping, page 29
- Analysis and Export, page 29
- Import, page 29

- Multiple-Instance Support, page 29

Data Mapping

Table 15 on page 29 shows the data mapping between ACS 4.x and ACS 5.8 for shared DACL objects.

Table 15 Data Mapping for Shared DACL Objects

4.x Attribute Name	5.8 Attribute Name	Comment
Name	Name	Configuration options determine the value used for Name.
Description	Description	–
ACL Definitions	Downloadable ACL Content	–
	GenID	This attribute is not visible in the GUI, but it is updated on each update to the ACL definition. It is set to the time of the object creation. It is used by the devices to detect changes in the ACL.

Analysis and Export

The following configuration options are available and affect the analysis and the import behavior:

- The name of the object created for each ACL can be either a combination of the DACL name and the ACL name or just the ACL name.
- In addition to the previously mentioned name, you can also add a prefix.

The created object name is analyzed and the following analysis issues, if present, are reported:

- If the object name exceeds 32 characters, the report shows that the final object name is truncated to 32 characters.
- All the object names that contain the following invalid characters:

  { }' "

  The invalid characters may come from the shared DACL part or the ACL part of the name. If the DACL name contains invalid characters, the report shows all the combinations of the ACL.

Note: If the ACL name is used, multiple ACL records could be created on ACS 5.8 with the same name. You should utilize this option only if you are sure that the ACL name is unique, or there are duplicate ACLs and you want to import only one.

No analysis is required for the ACL definition.

Import

You cannot create multiple DACLs with the same name. If you do so, it is reported in the Import report. This occurs when you use the ACL option for the DACL name to migrate multiple shared ACLs that contain the same ACL.

Multiple-Instance Support

In ACS 5.8, you cannot define two DACLs with the same name. However, you can create DACLs with a name prefix per ACS 4.x instance and thus add DACLs for each instance. With the multiple-instance support, you can select one of the following options to migrate the DACLs:

- Define a different name prefix for each instance and import all the DACLs with different names.

- Do not define a prefix. Only uniquely named DACLs are migrated. DACLs that already exist are reported as duplicates.

Shared RACs

In ACS 4.x, you can define a shared profile component that contains RADIUS Authorization Components (RACs) and defines a set of RADIUS attributes and values that are to be returned in an authorization response. These shared objects map the direction to the authorization profiles that are defined in ACS 5.8.

In ACS 4.x, an attribute is identified in the GUI as a combination of the vendor name and the attribute name. In ACS 5.8, it is defined as a combination of the dictionary and attribute name. Internally, the vendor or dictionary and attribute are identified by IDs that are, in turn, the values that are used while forming the RADIUS response.

This section contains:

- Data Mapping, page 30
- Analysis and Export, page 30
- Import, page 31
- Multiple-Instance Support, page 31

Data Mapping

Table 16 on page 30 shows the data mapping between ACS 4.x and ACS 5.8 for the shared RACs.

Table 16 Data Mapping for Shared RADIUS Authorization Components

4.x Attribute Name	5.8 Attribute Name	Comment
Name	Name	Configuration options determine the value used for Name.
Description	Description	–
List of vendor / attribute / value triplets	List of dictionary / attribute / value	The list of attributes appears in the manually entered section of the RADIUS Attributes tab of the Authorization Profile.

Analysis and Export

Some special characters are not allowed in the shared RAC during export. It will be reported in the Analysis report if the following characters are used in the shared RAC:

{ } ' "

In ACS 4.x, the Microsoft vendor attributes can be included in a RAC, but values cannot be set, and a fixed string of *<Value set by ACS>* is displayed. The following Microsoft vendor attributes can be selected:

- MS-CHAP-MPPE-Keys (12)
- MS-MPPE-Send-Key (16)
- MS-MPPE-Recv-Key (17)

In ACS 5.8, you cannot configure these attributes, but they are added to the profile as required, depending on the type of authentication being performed and the corresponding required response. If these attributes are defined in ACS 4.x, the Analysis report states that they have not been migrated, although the RAC that contains them was migrated.

Import

You can optionally configure a prefix to be added to the name of all the migrated RACs. In ACS 5.8, attributes are included in an authorization profile if they meet the following conditions for the relevant properties:

- Direction: OUT or BOTH
- Available: TRUE

The import process verifies that these conditions are met for all the attributes to be included in a profile, and any discrepancy is reported in the Import report.

Multiple-Instance Support

In ACS 5.8, you cannot define two RACs with the same name. However, you can create RACs with a name prefix per ACS 4.x instance and add RACs for each instance. With multiple-instance support, you can select one of the following options to migrate the RACs:

- Define a different name prefix for each instance, and import all the RACs with different names.
- Do not define a prefix. Only uniquely named RACs are migrated. RACs that already exist are reported as duplicates.

RADIUS VSAs

The dictionary and its content (the attribute definitions) are an important and core part of ACS 4.x. The dictionary defines the attributes specified by the IETF for the RADIUS protocol, and it is augmented by the vendor-specific attributes (VSAs) defined by different device vendors. VSAs are allocated a structured name space within the value of one of the IETF attributes (Attribute 26).

The majority of the used attributes are predefined in the dictionaries shipped with ACS. However, as vendors expand the capabilities of their devices, new VSAs are added.

If you do not wish to wait for the next release of ACS to get the updated dictionaries, you can use the Command Line Utility to define new dictionary slots for the new vendors, to augment the attributes of an already existing vendor in the dictionary, or to update already defined VSAs (for example, with additional enumeration values).

During migration, the dictionary is iterated to identify the missing attributes in ACS 5.8 for each vendor. There are two possible cases during this identification process:

- If the vendor does not exist in the ACS 5.8 dictionary, all the vendor attributes are migrated.
- If the vendor exists in the ACS 5.8 dictionary, only attributes that are not defined in ACS 5.8 are migrated.

For the Cisco Airespace attribute Aire-QoS-Level(2), the description of the enumerated values is different between ACS 4.1.x and ACS 5. Since the numeric value gets migrated, there is no difference in the response sent when using RACs that include this attribute and the same numeric value will be sent in the response. However, the string presented in the ACS GUI for this value is different.

For example, in ACS 4.1.x the value of 1 is displayed as *Silver,* whereas in ACS 5.8 this is displayed as *Gold*.

Table 17 on page 32 shows the mapping of Aire-QoS-Level (2) values between ACS 4.1.x and ACS 5.8.

Table 17 Aire-QoS-Level (2) values in ACS 4.1.x and ACS 5.8

Values in ACS 4.1.x	Values in ACS 5.8
Bronze (0)	Silver (0)
Silver (1)	Gold (1)
Gold (2)	Platinum (2)
Platinum (3)	Bronze (3)
Uranium (4)	Uranium (4)

Description of the enumerated values of Cisco Airespace attribute Aire-QoS-Level(2), between ACS 4.2 and ACS 5.8 is the same.

This section contains:

- Data Mapping, page 32
- Analysis and Export, page 33
- Import, page 33

Data Mapping

Table 18 on page 32 shows the data field mapping between ACS 4.x and ACS 5.8 for RADIUS vendors.

Table 18 Data Mapping for RADIUS Vendors

4.x Attribute Name	5.8 Attribute Name	Comment
Vendor Name	Name	–
–	Description	Generated during migration.
Vendor ID	Vendor ID	The vendor ID in ACS 4.x is extracted by examining the least significant unit in the path of the key, while enumerating the subkeys under the following key: CiscoACS\Dictionaries\002\026

Table 19 on page 32 shows the data field mapping between ACS 4.x and ACS 5.8 for RADIUS VSAs.

Table 19 Data Mapping for RADIUS VSAs

4.x Attribute Name	5.8 Attribute Name	Comment
Name	Name	ACS 5.8 has a very short maximum name length.
–	Description	Generated during migration.
Attribute Number	Attribute Number	The attribute number in ACS 4.x is extracted by examining the least significant unit in the path of the key, while enumerating the subkeys under the vendor key.
Profile	Direction	IN – 1 (Inbound) OUT – 2 (Outbound) IN OUT – 3 (Both)
Type	ValueType	Syntax ID is mapped.

Analysis and Export

The analysis phase for the RADIUS VSAs focuses on merging the dictionary content of ACS 4.x with the dictionary content of ACS 5.8. There are two cases for analysis:

- Generally, for ACS 4.x supported vendors, the dictionary in ACS 5.8 is more up-to-date. However, you may have modified some ACS 4.x vendor dictionaries to include new VSAs, or to modify the existing VSAs (for example, new enumeration values). The migration behavior is as follows:
  - An attribute defined in ACS 5.8 is not altered during migration. A warning is displayed for such attributes.
  - An attribute not defined in ACS 5.8, but present in ACS 4.x, is migrated.
- The vendors that are imported by you into ACS 4.x, and are not present in ACS 5.8, are migrated without any analysis warning.

Note: Difference between ACS 4.x and ACS 5.8 VSA attributes (profile, name, type) are reported in the Analysis report.

Import

All the exported VSAs are imported to ACS 5.8.

EAP-Fast Master Keys and the Authority ID

In ACS 5.8, you can preserve support for all objects (users or devices) that authenticated on ACS 4.x. Therefore, all the master keys and the authority ID from ACS 4.x are migrated.

The master keys in ACS 4.x have a schema that is different from that of ACS 5.8, and they are migrated to different IM objects. ACS 4.x stores the authority ID per node, whereas ACS 5.8 stores the authority ID only in the primary database and then applies it to the entire deployment.

This section contains:

- Data Mapping, page 33
- Analysis and Export, page 34
- Import, page 34
- Multiple-Instance Support, page 34

Data Mapping

Table 20 on page 33 shows the data mapping between ACS 4.x and ACS 5.8 for EAP-FAST master keys and the authority ID.

Table 20 Data Mapping for EAP-FAST Master Keys and the Authority ID

4.x Attribute Name	5.8 Attribute Name	Comment
Master Key ID	Identifier	ACS 4.x internal ID
Encryption key	EncriptionKey	Byte 32
Authentication key	AuthenticationKey	Byte 32

Table 20 Data Mapping for EAP-FAST Master Keys and the Authority ID (continued)

4.x Attribute Name	5.8 Attribute Name	Comment
Cipher suite	Cipher	–
Creation Time	–	–
Expiration Time (TTL)	Expiration Time	The Expiration time is calculated by adding the Current time and the Retired master key TTL.

The expiration time is calculated as follows:

1. From the list of keys in the database, the tail key is checked to determine whether or not it has expired.
2. Key creation time is saved as KeyCtime for the current key.
3. Current time is calculated by Calling Time(NULL).
4. TTL is taken for the key stored in **AuthenConfig > EAP-FAST.**
5. The Expiration time is calculated by adding the Current time and the Retired master key TTL.

The master key TTL unit is represented as follows:

Minutes: 1, Hours: 2, Days: 3, Weeks: 4, Months: 5, Years: 6

For example, if the active master key TTL is selected as 1 month, it equates to 1 * 30 * 24 * 3600.

Analysis and Export

No analysis is done. Expired keys are not migrated.

Import

In ACS 5.8, the objects are added to the Master Key table and are not available through the GUI. The authority ID is migrated to the EAP-FAST global settings.

Multiple-Instance Support

In ACS 5.8, you cannot define two master keys with the same ID; therefore, only unique master keys are migrated from multiple instances of ACS 4.x.

In ACS 5.8, the authority ID is stored as a global EAP setting and not stored per node or instance. Hence, it can be migrated only from one instance.

Analysis and Export of ACS 4.x Data

Choose option 1 in the Migration Utility to run AnalyzeAndExport. See This utility migrates data from ACS 4.x to ACS 5. You can migrate directly from the following ACS versions:, page 2. The Analyze and Export phase runs on the ACS 4.x migration machine by using data restored from the backup of the ACS 4.x source machine. The AnalyzeAndExport Summary Report lists the total:

- Detected objects.
- Issues reported for each object.
- Objects that can be migrated.
- Information on issues for each object.

- Data to be consolidated. See Consolidating Data, page 35.

The Analyze and Export phase can be run multiple times to make configuration changes between analysis cycles. For example, you might have overlapping IP addresses for network devices. You can use the ACS 4.x application to correct this problem. After you correct the problem, you can rerun the Analyze and Export phase and proceed to the Import phase. See Overlapping IP Addresses, page 3.

This section contains:

- Consolidating Data, page 35
- Issues Resulting from the Analysis and Export Phase, page 36

ExampleAnalyzeAndExport Summary Report, page 35 shows a sample summary report for the Analyze and Export phase. This example shows the report generated if you select *option 3- AllDevicesObjects*, in the Migration Utility.

```
ExampleAnalyzeAndExport Summary Report
--------------------------------------------------------------------------------
        Summary Report for phase AnalyzeAndExport
--------------------------------------------------------------------------------
Network Device Groups
--------------------------------------------------------------------------------
Total:3        Successful:3       Reported issues:0
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Network Device
--------------------------------------------------------------------------------
Total:5        Successful:5       Reported Issues:0
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
         Analysis and Export Report
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
        Network Device Group
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
INFO: The following objects are password_included
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
1. Name: NDG01 Comment: NDG has shared key password
2. Name: NDG02 Comment: NDG has shared key password
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
       Network Device
-------------------------------------------------------------------------------
```

See ACS 5.8 Attribute Support in the Migration Utility for a list of the attributes that are migrated.

Consolidating Data

The consolidation process occurs in the Analysis and Export phase and:

- Analyzes the created shared objects.
- Identifies the objects that are identical.
- Ensures that duplicate ACS 4.x objects are collapsed to a single object, which is migrated to ACS 5.8. This object can then be referenced by ACS 5.8 policies.

For example, the Analysis report might show multiple command sets that appear to be different, but are actually the same command set. This might be because of the command set shortcuts, such as *show* or *sho*. In ACS 5.8, you can define polices such that they incorporate the migrated command set information. See the *User Guide for Cisco Secure Access Control System 5.8* for more details on ACS 5.8 policies.

- Consolidates the following:
  - User and user group command set into a command set profile.
  - Group shell exec into a shell profile.

Issues Resulting from the Analysis and Export Phase

Not all data entities can migrate from ACS 4.x to ACS 5.8. The Analysis and Export phase might reveal issues such as overlapping IP addresses for the network devices.

Another issue is that the ACS 4.x IP address network device definitions could include wildcards and ranges. ACS 5.8 uses a standard subnet mask representation. Therefore, the network device definitions might not be compatible.

The Analysis and Export reports detail these issues. You can address these issues in the ACS 4.x application and subsequently rerun AnalyzeAndExport. You can rerun this process as many times as required. After you fix the issues, you can import the exported data to the ACS 5.8 machine.

Importing the ACS 4.x Data to ACS 5.8

Choose option 2 in the Migration Utility to run Import. See This utility migrates data from ACS 4.x to ACS 5. You can migrate directly from the following ACS versions:, page 2. This phase imports the ACS 4.x data export file created in the Export phase.

The import process can take a long time if you migrate data from a large database.

Note: If the ACS 5.8 import fails, restore your ACS 5.8 database.

ExampleSample Progress Report for the Import Phase, page 36 shows a sample progress report from the Import phase. This phase generates two reports:

- ExampleImport Summary Report, page 37 shows the Import Summary Report.
- ExampleImport Report, page 37 shows the Import Report.

```
ExampleSample Progress Report for the Import Phase
3
Tue Jul 20 14:57:00 EST 2007 Network Device Group 1 / 3 (33%) complete.
Tue Jul 20 14:57:00 EST 2007 Network Device Group 2 / 3 (66%) complete.
Tue Jul 20 14:57:00 EST 2007 Network Device Group 3 / 3 (100%) complete.
Imported 3 items of type: Network Device Group
Imported 2 items of type: User Group
Tue Jul 20 14:57:02 EST 2007 Group Shell Exec 1 / 1 (100%) complete.
Imported 1 items of type: Group Shell Exec
Tue Jul 20 14:57:03 EST 2007 Group Command Set 1 / 1 (100%) complete.
Imported 1 items of type: Group Command Set
Imported 0 items of type: User Shell Exec
Imported 0 items of type: User Command Set
Tue Jul 20 14:57:06 EST 2007 Shared Command Set 1 / 2 (50%) complete.
Tue Jul 20 14:57:24 EST 2007 Shared Command Set 2 / 2 (100%) complete.
Imported 2 items of type: Shared Command Set
Tue Jul 20 14:57:25 EST 2007 User 1 / 5 (20%) complete.
Tue Jul 20 14:57:25 EST 2007 User 2 / 5 (40%) complete.
Tue Jul 20 14:57:25 EST 2007 User 3 / 5 (60%) complete.
Tue Jul 20 14:57:25 EST 2007 User 4 / 5 (80%) complete.
Tue Jul 20 14:57:26 EST 2007 User 5 / 5 (100%) complete.
```

```
Imported 5 items of type: User
Tue Jul 20 14:57:26 EST 2007 Network Device 1 / 6 (16%) complete.
Tue Jul 20 14:57:27 EST 2007 Network Device 2 / 6 (33%) complete.
Tue Jul 20 14:57:28 EST 2007 Network Device 3 / 6 (50%) complete.
Tue Jul 20 14:57:28 EST 2007 Network Device 4 / 6 (66%) complete.
Tue Jul 20 14:57:29 EST 2007 Network Device 5 / 6 (83%) complete.
Tue Jul 20 14:57:29 EST 2007 Network Device 6 / 6 (100%) complete.
ExampleImport Summary Report
--------------------------------------------------------------------------------
        Summary Report for phase imported
--------------------------------------------------------------------------------
User Attributes
--------------------------------------------------------------------------------
Total:2         Successful:0    Reported issues:2
--------------------------------------------------------------------------------
Network Device Groups
--------------------------------------------------------------------------------
Total:3         Successful:2    Reported issues:1
--------------------------------------------------------------------------------
Groups Shell Exec
--------------------------------------------------------------------------------
Total:1         Successful:0    Reported issues:1
--------------------------------------------------------------------------------
Groups Command Set
--------------------------------------------------------------------------------
Total:1         Successful:1    Reported issues:0
--------------------------------------------------------------------------------
Users Shell Exec
--------------------------------------------------------------------------------
Total:0         Successful:0    Reported issues:0
--------------------------------------------------------------------------------
Users Command Set
--------------------------------------------------------------------------------
Total:0         Successful:0    Reported issues:0
--------------------------------------------------------------------------------
Shared Command Sets
--------------------------------------------------------------------------------
Total:2         Successful:2    Reported issues:0
--------------------------------------------------------------------------------
Network Devices
--------------------------------------------------------------------------------
Total:5         Successful:5    Reported issues:0
--------------------------------------------------------------------------------
Users
--------------------------------------------------------------------------------
Total:6         Successful:6    Reported issues:0
--------------------------------------------------------------------------------
Shared Downloadable ACL
--------------------------------------------------------------------------------
Total:6         Successful:6    Reported issues:0
--------------------------------------------------------------------------------
EAP FAST - Master Keys
--------------------------------------------------------------------------------
Total:6         Successful:6    Reported issues:0
--------------------------------------------------------------------------------
Mab
--------------------------------------------------------------------------------
Total:6         Successful:6    Reported issues:0
--------------------------------------------------------------------------------

ExampleImport Report
---------------------------------------------------------------------------------------
        Import Report
```

```
--------------------------------------------------------------------------------------
The following User Attributes were not imported:
--------------------------------------------------------------------------------------
1. Name: Real Name      Comment: Attribute cannot be added.
2. Name: Description    Comment: Attribute cannot be added.
The following Network Device Groups were not imported:
--------------------------------------------------------------------------------------
1. Name: Not Assigned   Comment: Error 1: Failure to add object: Migrated NDGs:All Migrated NDGs:Not
Assigned in function: createGroup

The following User Groups were not imported:
--------------------------------------------------------------------------------------
1. Name: IdentityGroup:All Groups:Migrated Group       Comment: Failure to add object:
IdentityGroup:All Groups:Migrated Group in function: createGroup

The following Group Shell Exec were not imported:
--------------------------------------------------------------------------------------
1. Name: ACS_Migrate_Priv Comment: customError CRUDex002 Object already exist exception
The following Group Command Set failed on import:
--------------------------------------------------------------------------------------
The following User Shell Exec were not imported:
--------------------------------------------------------------------------------------
The following User Command Set were not imported:
--------------------------------------------------------------------------------------
The following Shared Command Set were not imported:
--------------------------------------------------------------------------------------
The following Network Devices were not imported:
--------------------------------------------------------------------------------------
The following Users were not imported:
--------------------------------------------------------------------------------------
The following Shared Downloadable ACL were not imported:
-----------------------------------------------------------------------------------------
The following EAP FAST - Master Keys were not imported:
-----------------------------------------------------------------------------------------
The following Mab were not imported:
-----------------------------------------------------------------------------------------
```

Migrating Multiple Instances

Choose option 4 in the Migration Utility to import another ACS 4.x instance. See This utility migrates data from ACS 4.x to ACS 5. You can migrate directly from the following ACS versions:, page 2. You can import multiple ACS 4.x instances to ACS 5.8. ExampleImporting Multiple Instances, page 38 shows the prompts that appear if you decide to migrate multiple instances.

```
ExampleImporting Multiple Instances
Choose one of the following:
1 - AnalyzeAndExport
2 - Import
3 - CreateReportFiles
4 - Exit
--------------------------------------------------------
4

Would you like to migrate another ACS4.x server? [no]
yes
Enter ACS 4.x Sever ID:
--------------------------------------------------------
```

After you enter the server ID or hostname of another ACS 4.x instance, the whole migration process starts again. In this way, you can migrate several ACS 4.x instances to ACS 5.8.

Migration Impact on Memory and Performance

Data export is performed from the ACS 4.x migration server and not directly from the ACS 4.x production server or source server. Therefore, the migration has no impact on the performance of the ACS 4.x production server. The Migration Utility can be run on a standard PC environment.

During the import of the migrated data, the ACS 5.8 server should be idle and should not be processing any AAA requests.

Printing Reports and Report Types

Choose option 3 in the Migration Utility to print full reports and summary reports to a CSV file. See This utility migrates data from ACS 4.x to ACS 5. You can migrate directly from the following ACS versions:, page 2. The *config* folder in the migration directory contains the Migration Utility reports. In the *config* folder, a new folder with the same name as the server ID is created for each
ACS 4.x server that you migrate.

For example, if the server ID is *test1*, a folder *test1* is created under the *config* folder and it contains the Migration Utility reports. The report name has the server ID attached. This section contains:

- Analyze and Export Summary Report, page 40
- Analyze and Export Full Report, page 41
- Import Summary Report, page 42
- Import Full Report, page 43
- Validating Import, page 44
- Summary Report, page 45
- Full Report, page 45

Table 21 on page 39 lists the migration phases and the reports that are generated in each phase.

Table 21 Reports Generated During Migration

Migration Phase	Reports Generated
AnalyzeandExport	■ AnalyzeAndExport_*server ID*_Summary_report.csv ■ AnalyzeAndExport_*server ID*_full_report.csv
Import	■ ImportSummary_*server ID*_report.csv ■ Importfull_*server ID*_report.csv

Table 22 on page 40 describes the Migration Utility reports.

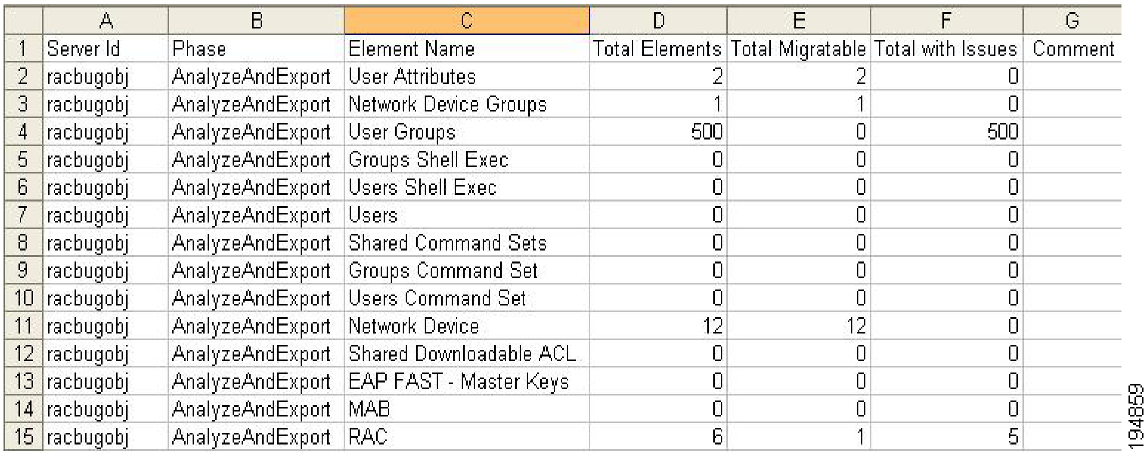
Table 22 Migration Utility Reports

Migration Report	Description
AnalyzeAndExport_Summary_report.csv	Summary report for the Analyze and Export phase. Shows the total number of objects you can migrate and any related problems.
AnalyzeAndExport_full_report.csv	Full report for the Analyze and Export phase. Shows the total number of objects you can migrate and includes descriptive comments for each object.
ImportSummary_report.csv	Summary report for the Import phase. Shows the total number of imported objects and any related problems.
Importfull_report.csv	Full report for the Import phase. Shows the total number of imported objects and includes descriptive comments for each object.
Full_report.csv	Combines all the Migration Utility reports into one file.
Summary_report.csv	Shows summary information for all the migration phases.

Analyze and Export Summary Report

Figure 1Analyze and Export Summary Report, page 41 shows the Analyze and Export Summary Report. Table 23 on page 41 contains the Analyze and Export Summary Report column definitions.

Figure 1 Analyze and Export Summary Report



	A	B	C	D	E	F	G
1	Server Id	Phase	Element Name	Total Elements	Total Migratable	Total with Issues	Comment
2	racbugobj	AnalyzeAndExport	User Attributes	2	2	0	
3	racbugobj	AnalyzeAndExport	Network Device Groups	1	1	0	
4	racbugobj	AnalyzeAndExport	User Groups	500	0	500	
5	racbugobj	AnalyzeAndExport	Groups Shell Exec	0	0	0	
6	racbugobj	AnalyzeAndExport	Users Shell Exec	0	0	0	
7	racbugobj	AnalyzeAndExport	Users	0	0	0	
8	racbugobj	AnalyzeAndExport	Shared Command Sets	0	0	0	
9	racbugobj	AnalyzeAndExport	Groups Command Set	0	0	0	
10	racbugobj	AnalyzeAndExport	Users Command Set	0	0	0	
11	racbugobj	AnalyzeAndExport	Network Device	12	12	0	
12	racbugobj	AnalyzeAndExport	Shared Downloadable ACL	0	0	0	
13	racbugobj	AnalyzeAndExport	EAP FAST - Master Keys	0	0	0	
14	racbugobj	AnalyzeAndExport	MAB	0	0	0	
15	racbugobj	AnalyzeAndExport	RAC	6	1	5	

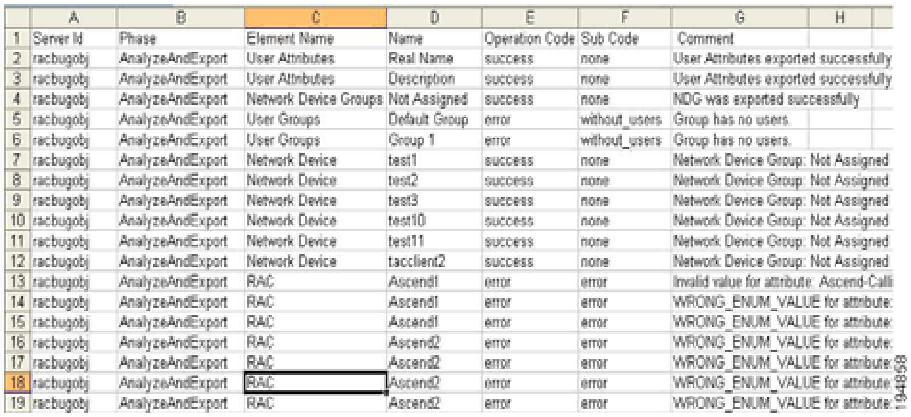
Table 23 Analyze and Export Summary Report Column Definitions

Column	Description
Server ID	Name of the server.
Phase	Name of the migration phase.
Element Name	Name of the ACS object type to be migrated.
Total Elements	Total number of elements.
Total Migratable	Total number of elements that can be migrated.
Total with Issues	Total number of elements that have issues.
Comment	Message indicating the status of the ACS object.

Analyze and Export Full Report

Figure 2Analyze and Export Full Report, page 42 shows the Analyze and Export Full Report. Table 24 on page 42 contains the Analyze and Export Full Report column definitions.

Figure 2 Analyze and Export Full Report



	A	B	C	D	E	F	G	H
1	Server Id	Phase	Element Name	Name	Operation Code	Sub Code	Comment	
2	racbugobj	AnalyzeAndExport	User Attributes	Real Name	success	none	User Attributes exported successfully	
3	racbugobj	AnalyzeAndExport	User Attributes	Description	success	none	User Attributes exported successfully	
4	racbugobj	AnalyzeAndExport	Network Device Groups	Not Assigned	success	none	NDG was exported successfully	
5	racbugobj	AnalyzeAndExport	User Groups	Default Group	error	without_users	Group has no users.	
6	racbugobj	AnalyzeAndExport	User Groups	Group 1	error	without_users	Group has no users.	
7	racbugobj	AnalyzeAndExport	Network Device	test1	success	none	Network Device Group: Not Assigned	
8	racbugobj	AnalyzeAndExport	Network Device	test2	success	none	Network Device Group: Not Assigned	
9	racbugobj	AnalyzeAndExport	Network Device	test3	success	none	Network Device Group: Not Assigned	
10	racbugobj	AnalyzeAndExport	Network Device	test10	success	none	Network Device Group: Not Assigned	
11	racbugobj	AnalyzeAndExport	Network Device	test11	success	none	Network Device Group: Not Assigned	
12	racbugobj	AnalyzeAndExport	Network Device	tacclient2	success	none	Network Device Group: Not Assigned	
13	racbugobj	AnalyzeAndExport	RAC	Ascend1	error	error	Invalid value for attribute: Ascend-Calli	
14	racbugobj	AnalyzeAndExport	RAC	Ascend1	error	error	WRONG_ENUM_VALUE for attribute:	
15	racbugobj	AnalyzeAndExport	RAC	Ascend1	error	error	WRONG_ENUM_VALUE for attribute:	
16	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute:	
17	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute:	
18	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute:	
19	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute:	

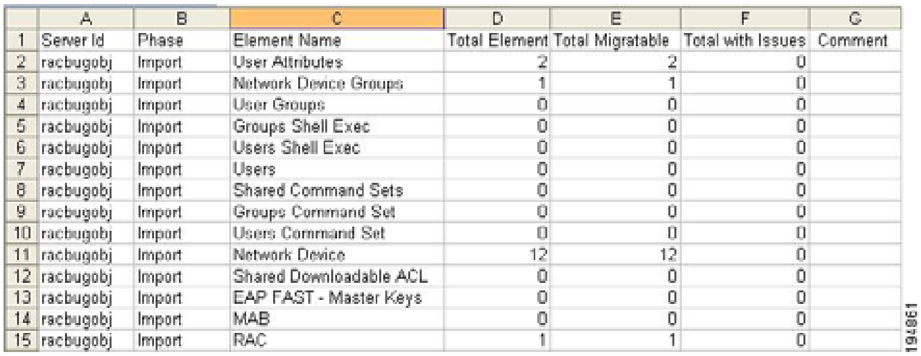
Table 24 Analyze and Export Full Report Column Definitions

Column	Description
Server ID	Name of the server.
Phase	Name of the migration phase.
Element Name	Name of the extracted ACS object type.
Name	Name of the ACS object type to be migrated.
Operation Code	Status of the Analyze and Export phase. Valid values are success, error, and info (informational message).
Sub Code	Code associated with the status of the operation.
Comment	Message indicating the status of the ACS object.

Import Summary Report

Figure 3Import Summary Report, page 43 shows the Import Summary Report. Table 25 on page 43 contains the Import Summary Report column definitions.

Figure 3 Import Summary Report



	A	B	C	D	E	F	G
1	Server Id	Phase	Element Name	Total Element	Total Migratable	Total with Issues	Comment
2	racbugobj	Import	User Attributes	2	2	0	
3	racbugobj	Import	Network Device Groups	1	1	0	
4	racbugobj	Import	User Groups	0	0	0	
5	racbugobj	Import	Groups Shell Exec	0	0	0	
6	racbugobj	Import	Users Shell Exec	0	0	0	
7	racbugobj	Import	Users	0	0	0	
8	racbugobj	Import	Shared Command Sets	0	0	0	
9	racbugobj	Import	Groups Command Set	0	0	0	
10	racbugobj	Import	Users Command Set	0	0	0	
11	racbugobj	Import	Network Device	12	12	0	
12	racbugobj	Import	Shared Downloadable ACL	0	0	0	
13	racbugobj	Import	EAP FAST - Master Keys	0	0	0	
14	racbugobj	Import	MAB	0	0	0	
15	racbugobj	Import	RAC	1	1	0	

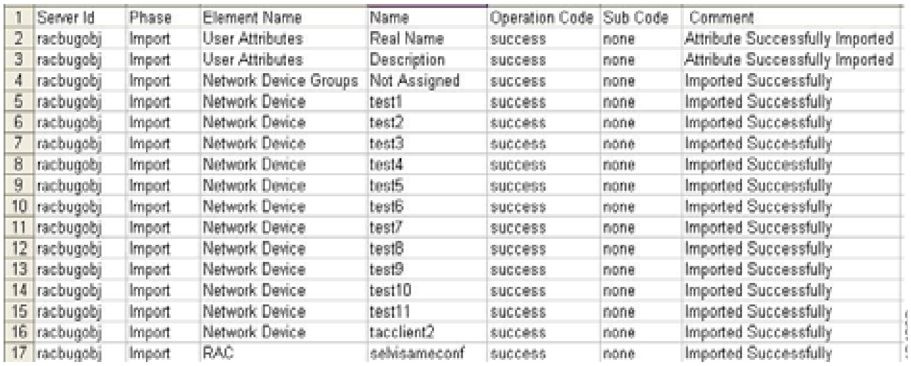
Table 25 Import Summary Report Column Definitions

Column	Description
Server ID	Name of the server.
Phase	Name of the migration phase.
Element Name	Name of the ACS object type to be migrated.
Total Elements	Total number of elements.
Total Migratable	Total number of elements that are migrated.
Total with Issues	Total number of elements that have issues.
Comment	Message indicating the status of the ACS object.

Import Full Report

Figure 4Import Full Report, page 44 shows the Import Full Report. Table 26 on page 44 contains the Import Full Report column definitions.

Figure 4 Import Full Report



1	Server Id	Phase	Element Name	Name	Operation Code	Sub Code	Comment
2	racbugobj	Import	User Attributes	Real Name	success	none	Attribute Successfully Imported
3	racbugobj	Import	User Attributes	Description	success	none	Attribute Successfully Imported
4	racbugobj	Import	Network Device Groups	Not Assigned	success	none	Imported Successfully
5	racbugobj	Import	Network Device	test1	success	none	Imported Successfully
6	racbugobj	Import	Network Device	test2	success	none	Imported Successfully
7	racbugobj	Import	Network Device	test3	success	none	Imported Successfully
8	racbugobj	Import	Network Device	test4	success	none	Imported Successfully
9	racbugobj	Import	Network Device	test5	success	none	Imported Successfully
10	racbugobj	Import	Network Device	test6	success	none	Imported Successfully
11	racbugobj	Import	Network Device	test7	success	none	Imported Successfully
12	racbugobj	Import	Network Device	test8	success	none	Imported Successfully
13	racbugobj	Import	Network Device	test9	success	none	Imported Successfully
14	racbugobj	Import	Network Device	test10	success	none	Imported Successfully
15	racbugobj	Import	Network Device	test11	success	none	Imported Successfully
16	racbugobj	Import	Network Device	tacclient2	success	none	Imported Successfully
17	racbugobj	Import	RAC	selvisameconf	success	none	Imported Successfully

Table 26 Import Full Report Column Definitions

Column	Description
Server ID	Name of the server.
Phase	Name of the migration phase.
Element Name	Name of the ACS object type to be migrated.
Name	User-supplied name.
Operation Code	Indicates if the operation was a success or if an error occurred.
Sub Code	Code associated with the status of the operation.
Comment	Message indicating the status of the ACS object.

Validating Import

After the import phase is complete, you must manually analyze the Import Summary Report. This lists:

- The total number of objects to be migrated.
- The number of objects that successfully migrated.
- The number of objects that failed to migrate.

You can check the Import Full Report for information on the objects that did not migrate. This lists:

- The name of the objects.
- The status of the objects.
- The reason for the errors.

If any of the ACS 4.x objects are not migrated, you must:

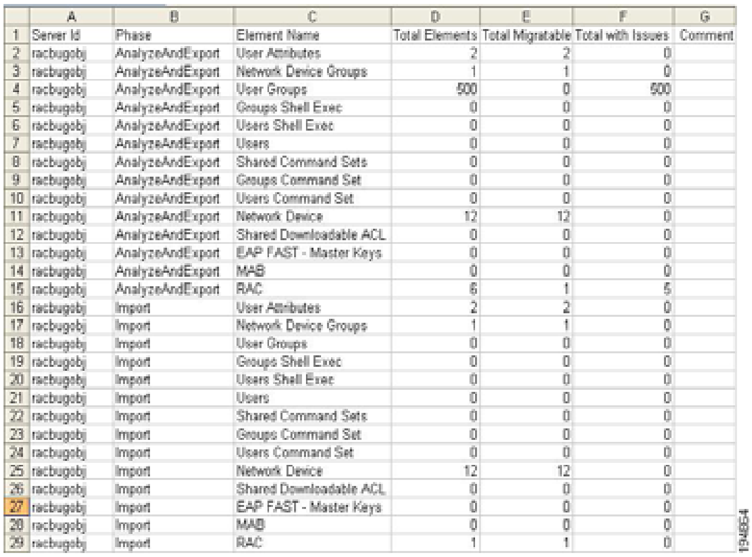
1. Manually add the objects that are not migrated, or address these issues in the ACS 4.x application.
2. Rerun the Analyze and Export phase.
3. Restore the ACS 5.8 database to its previous state (before import).
4. Rerun the Import phase.

Note: To verify that migration is complete, analyze the Import Summary Report. If the report indicates that all objects have migrated successfully, migration is complete.

Summary Report

Figure 5Summary Report, page 45 shows the Summary Report statistics for all migration phases. Table 27 on page 45 contains the Summary Report column definitions.

Figure 5 Summary Report



	A	B	C	D	E	F	G
1	Server Id	Phase	Element Name	Total Elements	Total Migratable	Total with Issues	Comment
2	racbugobj	AnalyzeAndExport	User Attributes	2	2	0	
3	racbugobj	AnalyzeAndExport	Network Device Groups	1	1	0	
4	racbugobj	AnalyzeAndExport	User Groups	500	0	500	
5	racbugobj	AnalyzeAndExport	Groups Shell Exec	0	0	0	
6	racbugobj	AnalyzeAndExport	Users Shell Exec	0	0	0	
7	racbugobj	AnalyzeAndExport	Users	0	0	0	
8	racbugobj	AnalyzeAndExport	Shared Command Sets	0	0	0	
9	racbugobj	AnalyzeAndExport	Groups Command Set	0	0	0	
10	racbugobj	AnalyzeAndExport	Users Command Set	0	0	0	
11	racbugobj	AnalyzeAndExport	Network Device	12	12	0	
12	racbugobj	AnalyzeAndExport	Shared Downloadable ACL	0	0	0	
13	racbugobj	AnalyzeAndExport	EAP FAST - Master Keys	0	0	0	
14	racbugobj	AnalyzeAndExport	MAB	0	0	0	
15	racbugobj	AnalyzeAndExport	RAC	6	1	5	
16	racbugobj	Import	User Attributes	2	2	0	
17	racbugobj	Import	Network Device Groups	1	1	0	
18	racbugobj	Import	User Groups	0	0	0	
19	racbugobj	Import	Groups Shell Exec	0	0	0	
20	racbugobj	Import	Users Shell Exec	0	0	0	
21	racbugobj	Import	Users	0	0	0	
22	racbugobj	Import	Shared Command Sets	0	0	0	
23	racbugobj	Import	Groups Command Set	0	0	0	
24	racbugobj	Import	Users Command Set	0	0	0	
25	racbugobj	Import	Network Device	12	12	0	
26	racbugobj	Import	Shared Downloadable ACL	0	0	0	
27	racbugobj	Import	EAP FAST - Master Keys	0	0	0	
28	racbugobj	Import	MAB	0	0	0	
29	racbugobj	Import	RAC	1	1	0	

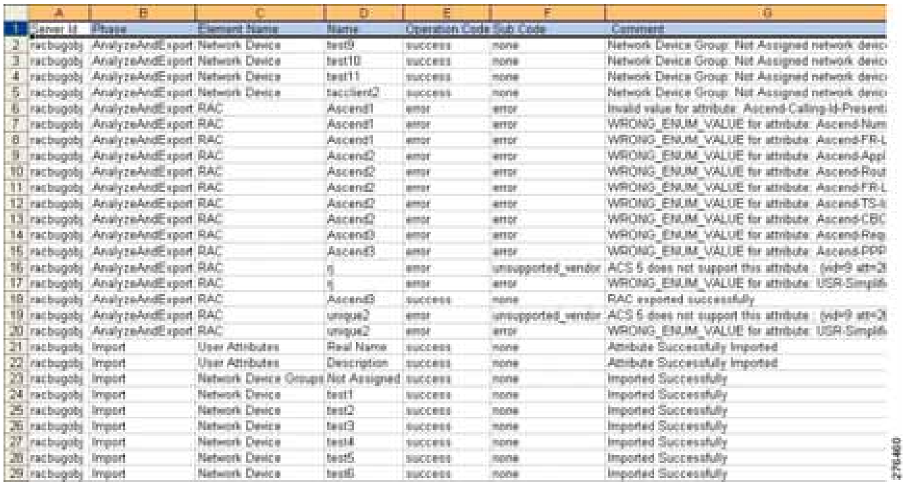
Table 27 Summary Report Column Definitions

Column	Description
Server ID	Name of the server.
Phase	Name of the migration phase.
Element Name	Name of the migrated ACS object.
Total Elements	Total number of ACS objects processed.
Total Migratable	Total number of ACS objects migrated.
Total with Issues	Total number of issues for each ACS object.
Comment	Message indicating the status of the ACS object.

Full Report

Figure 6Full Report, page 46 shows the Full Report statistics for all migration phases. Table 28 on page 46 contains the Full Report column definitions.

Figure 6 Full Report



	A	B	C	D	E	F	G
1	Server Id	Phase	Element Name	Name	Operation Code	Sub Code	Comment
2	racbugobj	AnalyzeAndExport	Network Device	test9	success	none	Network Device Group: Not Assigned network devic
3	racbugobj	AnalyzeAndExport	Network Device	test10	success	none	Network Device Group: Not Assigned network devic
4	racbugobj	AnalyzeAndExport	Network Device	test11	success	none	Network Device Group: Not Assigned network devic
5	racbugobj	AnalyzeAndExport	Network Device	tacclient2	success	none	Network Device Group: Not Assigned network devic
6	racbugobj	AnalyzeAndExport	RAC	Ascend1	error	error	Invalid value for attribute: Ascend-Calling-Id-Presenta
7	racbugobj	AnalyzeAndExport	RAC	Ascend1	error	error	WRONG_ENUM_VALUE for attribute: Ascend-Num
8	racbugobj	AnalyzeAndExport	RAC	Ascend1	error	error	WRONG_ENUM_VALUE for attribute: Ascend-FR-L
9	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute: Ascend-Appl
10	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute: Ascend-Rout
11	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute: Ascend-FR-L
12	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute: Ascend-TS-I
13	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute: Ascend-CBC
14	racbugobj	AnalyzeAndExport	RAC	Ascend3	error	error	WRONG_ENUM_VALUE for attribute: Ascend-Req
15	racbugobj	AnalyzeAndExport	RAC	Ascend3	error	error	WRONG_ENUM_VALUE for attribute: Ascend-PPP
16	racbugobj	AnalyzeAndExport	RAC	rj	error	unsupported_vendor	ACS 5 does not support this attribute : (vid=9 att=2
17	racbugobj	AnalyzeAndExport	RAC	rj	error	error	WRONG_ENUM_VALUE for attribute: USR-Simplifi
18	racbugobj	AnalyzeAndExport	RAC	Ascend3	success	none	RAC exported successfully
19	racbugobj	AnalyzeAndExport	RAC	unique2	error	unsupported_vendor	ACS 5 does not support this attribute : (vid=9 att=2
20	racbugobj	AnalyzeAndExport	RAC	unique2	error	error	WRONG_ENUM_VALUE for attribute: USR-Simplifi
21	racbugobj	Import	User Attributes	Real Name	success	none	Attribute Successfully Imported
22	racbugobj	Import	User Attributes	Description	success	none	Attribute Successfully Imported
23	racbugobj	Import	Network Device Groups	Not Assigned	success	none	Imported Successfully
24	racbugobj	Import	Network Device	test1	success	none	Imported Successfully
25	racbugobj	Import	Network Device	test2	success	none	Imported Successfully
26	racbugobj	Import	Network Device	test3	success	none	Imported Successfully
27	racbugobj	Import	Network Device	test4	success	none	Imported Successfully
28	racbugobj	Import	Network Device	test5	success	none	Imported Successfully
29	racbugobj	Import	Network Device	test6	success	none	Imported Successfully

Table 28 Full Report Column Definitions

Column	Description
Server ID	Name of the server.
Phase	Name of the migration phase.
Element Name	Name of the migrated ACS object.
Name	User-supplied name.
Operation Code	Indicates if the operation was a success or if an error occurred.
Sub Code	Code associated with the status of the operation.
Comment	Message indicating the status of the ACS object.

Errors and Exception Handling

Any errors during the Analysis and Export or Import phases are reported in the respective reports. For more information on the migration errors and the steps to resolve them, seeResolving Migration Issues, page 2.

For the error and informational messages that may appear during the migration of various ACS objects, seeMigration Utility Messages, page 5.

Confirming the Migration

Log into your ACS 5.8 target machine to confirm that you successfully migrated the ACS 4.x elements. In the migration process, the following ACS elements that were defined in ACS 4.x are migrated to
ACS 5.8:

- User Attributes
- User Attribute Values
- NDGs
- User Groups
- Groups Shell Exec

- Groups Command Set
- Users Shell Exec
- Users Command Set
- Shared Command Sets
- Network Devices
- Users
- Shared DACL
- EAP-FAST Master Keys
- MAB
- Shared RACs
- Customers VSAs

To access the ACS 4.x objects, follow the instructions in the *User Guide for Cisco Secure Access Control Server 4.2*. To access the ACS 5.8 objects, follow the instructions in the *User Guide for Cisco Secure Access Control System 5.8.*

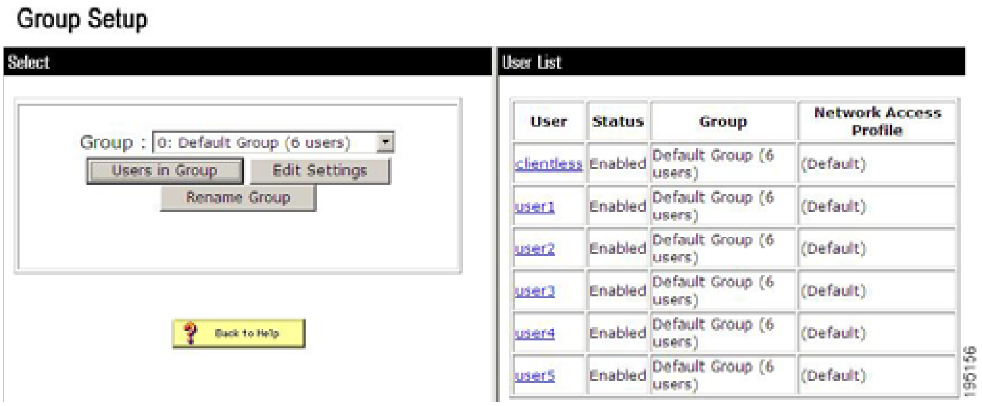
The following sections provide information on confirming the migration of:

- Users and User Groups, page 47
- Command Shell Migration, page 48
- Command Set Migration, page 50
- NDG Migration, page 51
- Network Device Migration, page 52
- DACL Migration, page 53
- MAB Migration, page 54
- Shared RACs, page 55
- RADIUS VSA, page 56
- KEK and MACK Keys, page 58

Users and User Groups

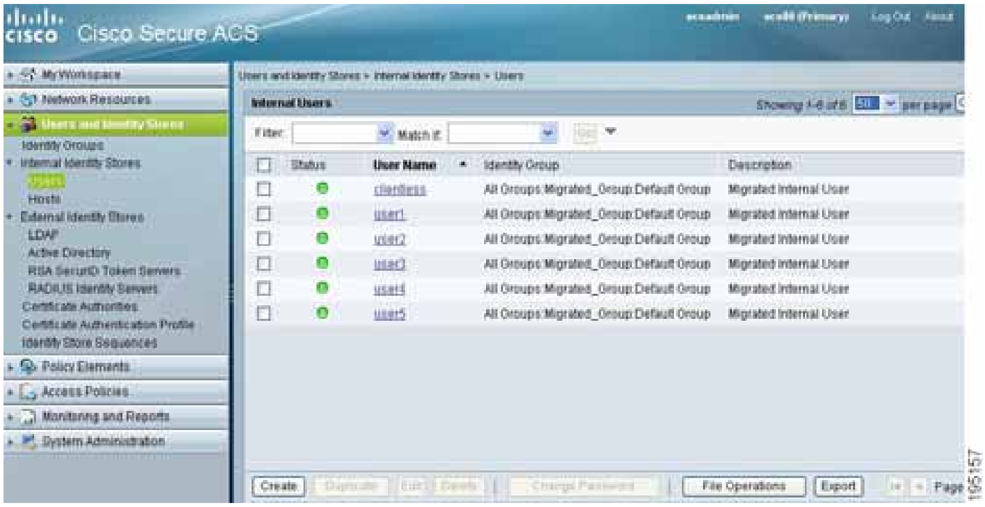
Figure 7 on page 48 shows the users and user groups in ACS 4.x, and Figure 8 on page 48 shows the users and user groups migrated to ACS 5.8. Choose **Users and Identity Stores > Internal Identity Stores > Users** to access the migrated users and user groups.

Figure 7 Users and User Groups Defined in ACS 4.x



User	Status	Group	Network Access Profile
clientless	Enabled	Default Group (6 users)	(Default)
user1	Enabled	Default Group (6 users)	(Default)
user2	Enabled	Default Group (6 users)	(Default)
user3	Enabled	Default Group (6 users)	(Default)
user4	Enabled	Default Group (6 users)	(Default)
user5	Enabled	Default Group (6 users)	(Default)

Figure 8 Users and User Groups Migrated to ACS 5.8



☐	Status	User Name	Identity Group	Description
☐	●	clientless	All Groups:Migrated_Group:Default Group	Migrated Internal User
☐	●	user1	All Groups:Migrated_Group:Default Group	Migrated Internal User
☐	●	user2	All Groups:Migrated_Group:Default Group	Migrated Internal User
☐	●	user3	All Groups:Migrated_Group:Default Group	Migrated Internal User
☐	●	user4	All Groups:Migrated_Group:Default Group	Migrated Internal User
☐	●	user5	All Groups:Migrated_Group:Default Group	Migrated Internal User

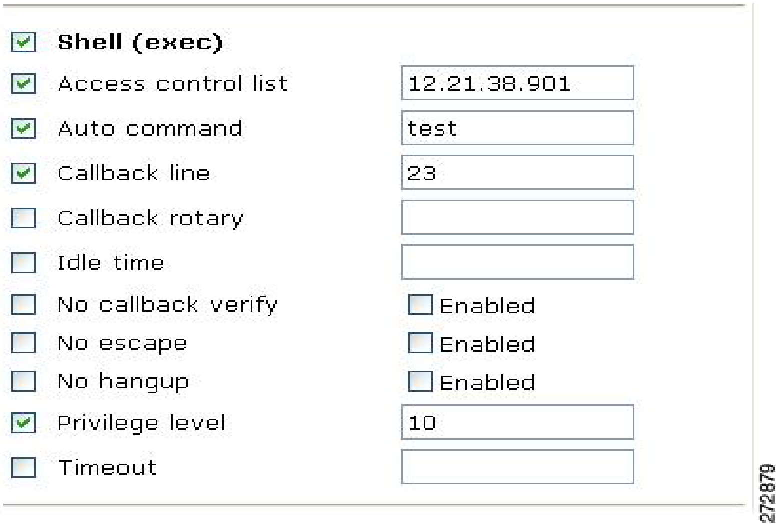
Command Shell Migration

Figure 9 on page 49 shows the command shell attributes in ACS 4.x, and Figure 10 on page 49 shows the group shell attributes migrated to ACS 5.8 as shell profiles.

Choose **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles** and click **Edit** to access the migrated group shell attributes.

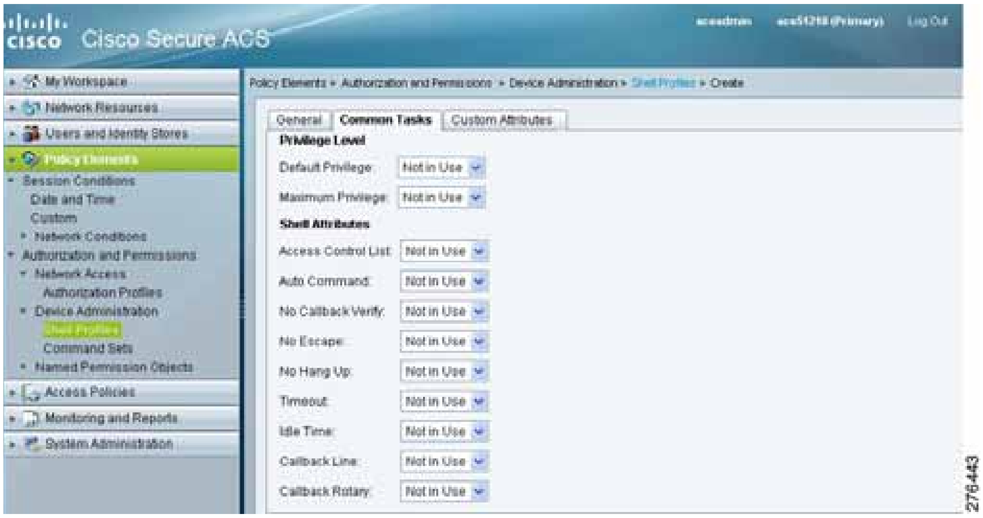
Choose **User and Identity Stores > Internal Identity Stores > Users** and click on any user to access the migrated user shell attributes. Figure 11 on page 50 shows the user shell attributes migrated to ACS 5.8.

Figure 9 Command Shell Attributes Defined in ACS 4.x



☑ **Shell (exec)**
☑ Access control list 12.21.38.901
☑ Auto command test
☑ Callback line 23
□ Callback rotary
□ Idle time
□ No callback verify □ Enabled
□ No escape □ Enabled
□ No hangup □ Enabled
☑ Privilege level 10
□ Timeout

Figure 10 Group Shell Attributes Migrated to ACS 5.8



Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create

General | Common Tasks | Custom Attributes

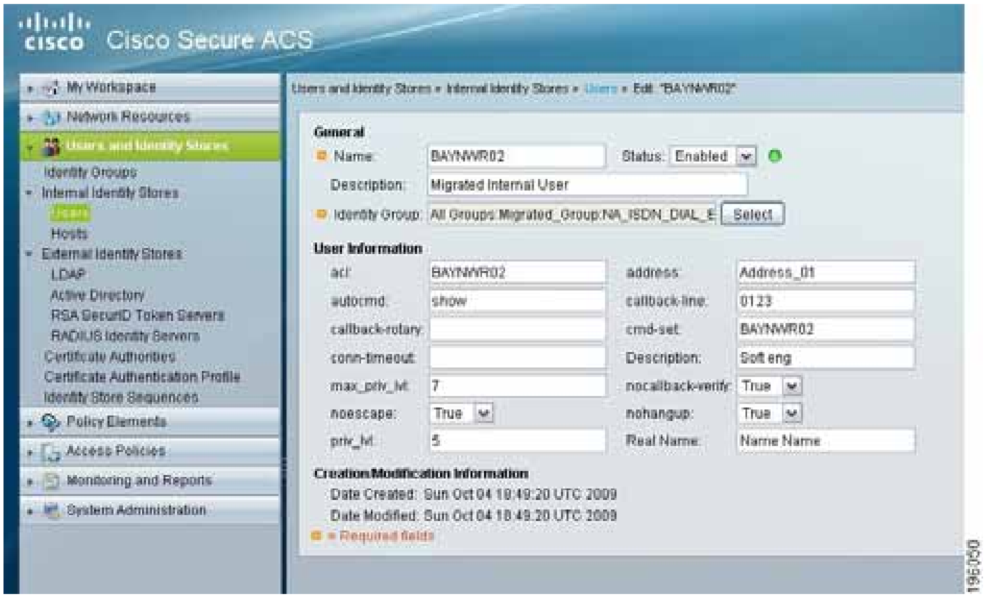
Privilege Level

Default Privilege: Not in Use
Maximum Privilege: Not in Use

Shell Attributes

Access Control List: Not in Use
Auto Command: Not in Use
No Callback Verify: Not in Use
No Escape: Not in Use
No Hang Up: Not in Use
Timeout: Not in Use
Idle Time: Not in Use
Callback Line: Not in Use
Callback Rotary: Not in Use

Figure 11 User Shell Attribute Migrated to ACS 5.8



General

Name:	BAYNWR02	Status:	Enabled
Description:	Migrated Internal User		
Identity Group:	All Groups:Migrated_Group:NA_ISDN_DIAL_E		

User Information

acl:	BAYNWR02	address:	Address_01
autocmd:	show	callback-line:	0123
callback-rotary:		cmd-set:	BAYNWR02
conn-timeout:		Description:	Soft eng
max_priv_lvl:	7	nocallback-verify:	True
noescape:	True	nohangup:	True
priv_lvl:	5	Real Name:	Name Name

Creation/Modification Information

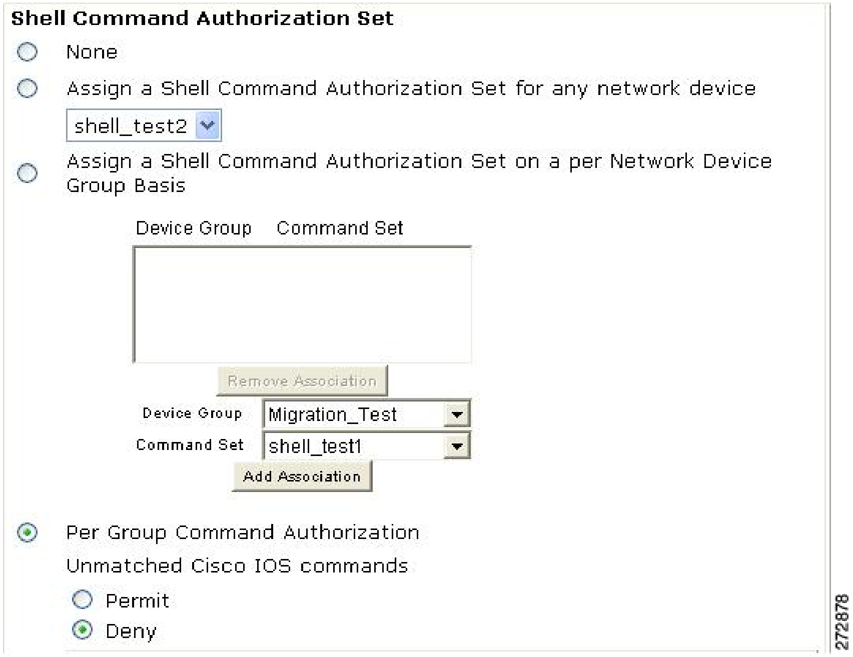
Date Created: Sun Oct 04 18:49:20 UTC 2009

Date Modified: Sun Oct 04 18:49:20 UTC 2009

Command Set Migration

Figure 12 on page 51 shows the command set in ACS 4.x, and Figure 13 on page 51 shows the command set migrated to ACS 5.8. Choose **Policy Elements > Device Administration > Command Sets** to access the migrated command set attributes.

Figure 12 Command Set Defined in ACS 4.x



Shell Command Authorization Set

○ None

○ Assign a Shell Command Authorization Set for any network device

shell_test2

○ Assign a Shell Command Authorization Set on a per Network Device Group Basis

Device Group Command Set

Remove Association

Device Group: Migration_Test

Command Set: shell_test1

Add Association

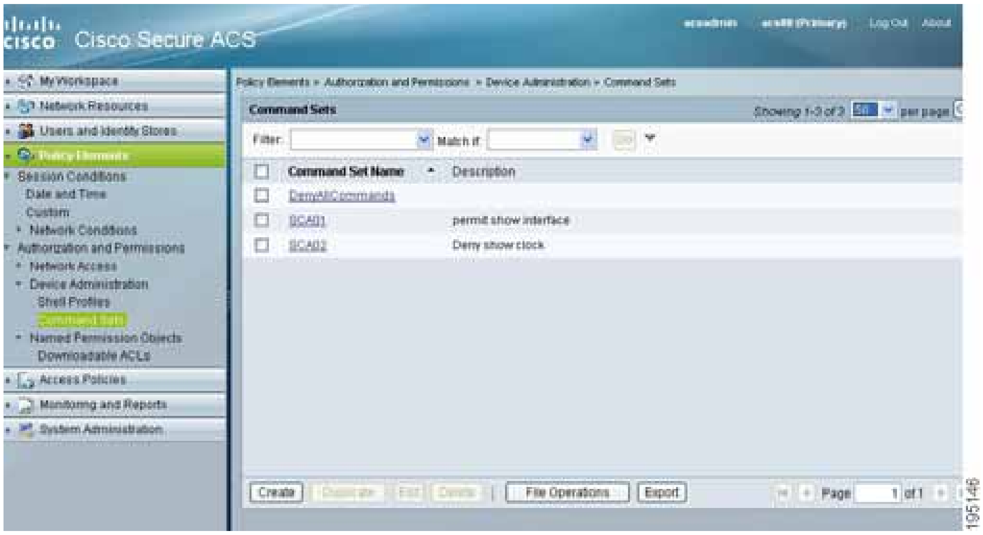
● Per Group Command Authorization

Unmatched Cisco IOS commands

○ Permit

● Deny

Figure 13 Command Set Migrated to ACS 5.8



Policy Elements > Authorization and Permissions > Device Administration > Command Sets

Command Sets

Showing 1-3 of 3 50 per page

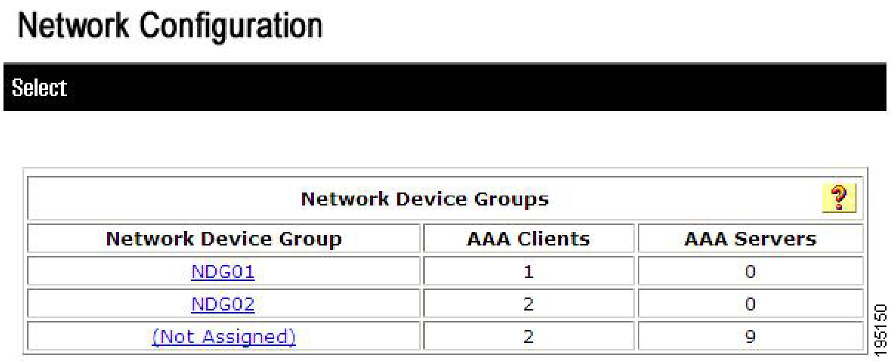
Filter: Match if:

☐	Command Set Name	Description
☐	DenyAllCommands	
☐	SCA01	permit show interface
☐	SCA02	Deny show clock

NDG Migration

Figure 14 on page 52 shows the NDGs in ACS 4.x, and Figure 15 on page 52 shows the NDGs migrated to ACS 5.8. Choose **Network Resources > Network Device Groups** to access the migrated NDGs.

Figure 14 NDGs Defined in ACS 4.x

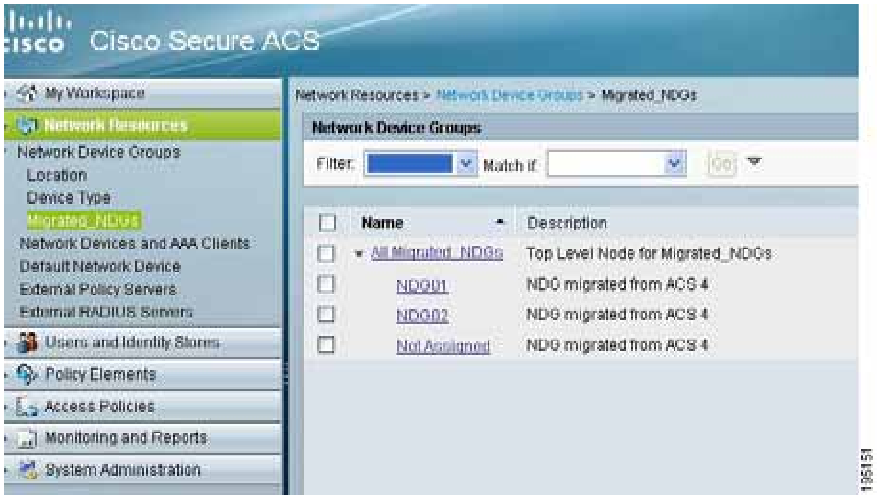


Network Configuration

Select

Network Device Groups		
Network Device Group	**AAA Clients**	**AAA Servers**
NDG01	1	0
NDG02	2	0
(Not Assigned)	2	9

Figure 15 NDGs Migrated to ACS 5.8

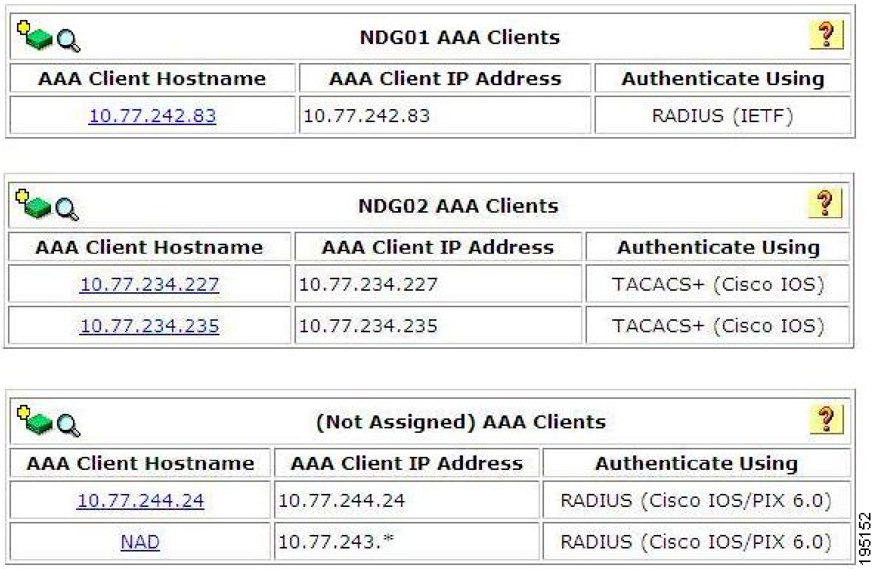


Name	Description
All Migrated_NDGs	Top Level Node for Migrated_NDGs
NDG01	NDG migrated from ACS 4
NDG02	NDG migrated from ACS 4
Not Assigned	NDG migrated from ACS 4

Network Device Migration

Figure 16 on page 53 shows the network devices in ACS 4.x, and Figure 17 on page 53 shows the network devices migrated to ACS 5.8. Choose **Network Resources > Network Devices and AAA Clients** to access the migrated network devices.

Figure 16 Network Devices Defined in ACS 4.x



NDG01 AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
10.77.242.83	10.77.242.83	RADIUS (IETF)

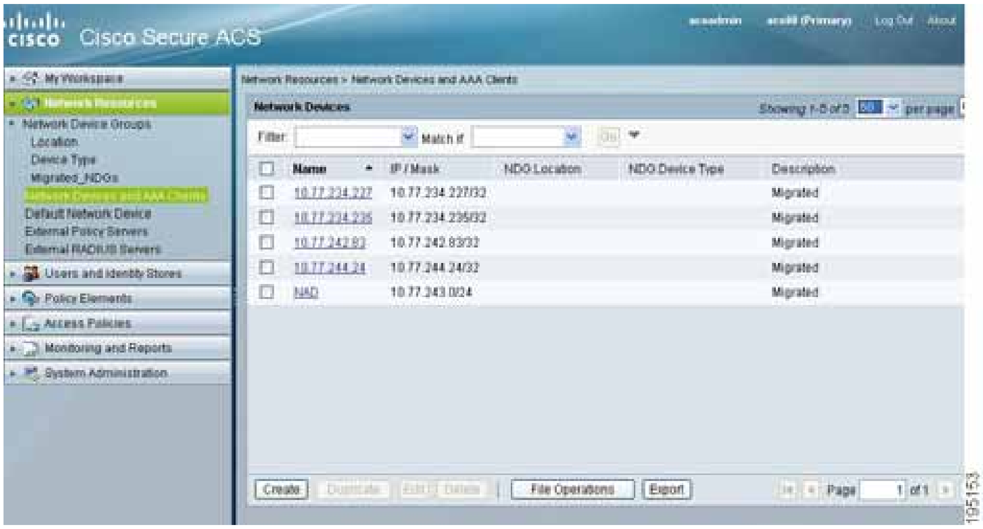
NDG02 AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
10.77.234.227	10.77.234.227	TACACS+ (Cisco IOS)
10.77.234.235	10.77.234.235	TACACS+ (Cisco IOS)

(Not Assigned) AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
10.77.244.24	10.77.244.24	RADIUS (Cisco IOS/PIX 6.0)
NAD	10.77.243.*	RADIUS (Cisco IOS/PIX 6.0)

Figure 17 Network Devices Migrated to ACS 5.8



Network Resources > Network Devices and AAA Clients

Network Devices

Showing 1-5 of 5 50 per page

Filter: Match if: Go

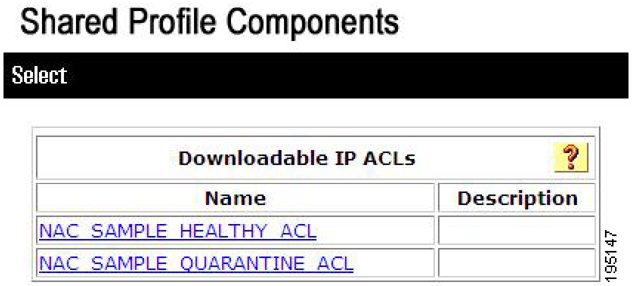
□	Name	IP / Mask	NDG Location	NDG Device Type	Description
□	10.77.234.227	10.77.234.227/32			Migrated
□	10.77.234.235	10.77.234.235/32			Migrated
□	10.77.242.83	10.77.242.83/32			Migrated
□	10.77.244.24	10.77.244.24/32			Migrated
□	NAD	10.77.243.0/24			Migrated

DACL Migration

Figure 18 on page 54 shows the downloadable access control lists (DACLs) in ACS 4.x, and Figure 19 on page 54 shows the DACLs migrated to ACS 5.8.

Choose **Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs** to access the migrated DACLs.

Figure 18 DACLs Defined in ACS 4.x

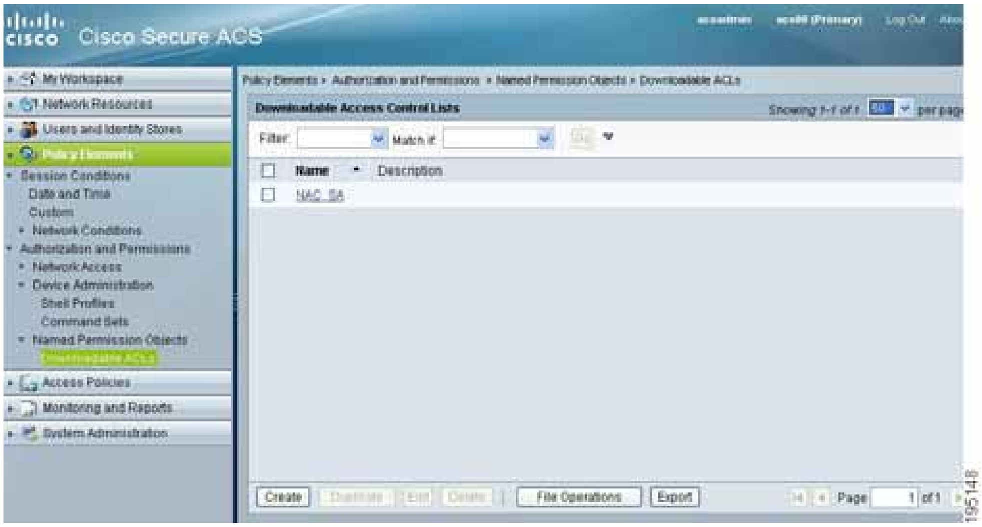


Shared Profile Components

Select

Downloadable IP ACLs	
Name	Description
NAC_SAMPLE_HEALTHY_ACL	
NAC_SAMPLE_QUARANTINE_ACL	

Figure 19 DACLs Migrated to ACS 5.8



Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs

Downloadable Access Control Lists — Showing 1-1 of 1, 50 per page

Filter: Match if:

	Name	Description
□	NAC_SA	

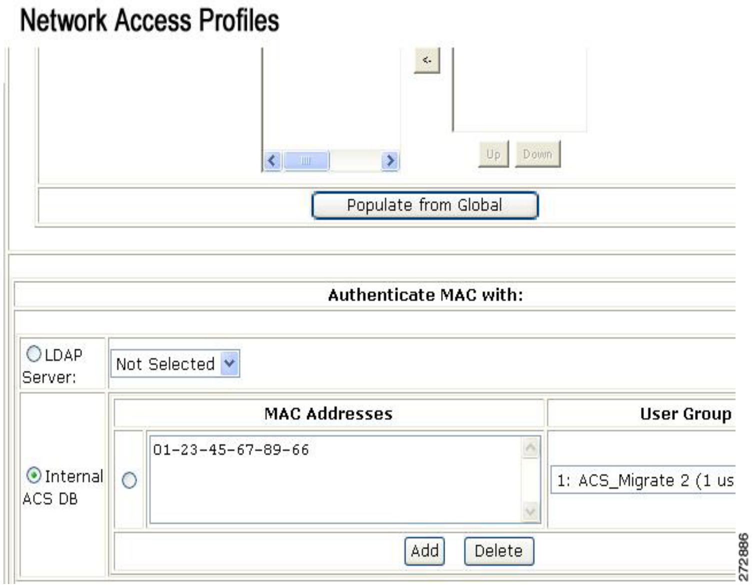
Page 1 of 1

MAB Migration

Figure 20 on page 55 shows MAC Authentication Bypass (MAB) defined in ACS 4.x, and Figure 21 on page 55 shows MAB migrated to ACS 5.8.

Choose **Users and Identity Stores > Internal Identity Stores > Hosts** and click **Create** to access the migrated MABs.

Figure 20 MAB Defined in ACS 4.x



Network Access Profiles

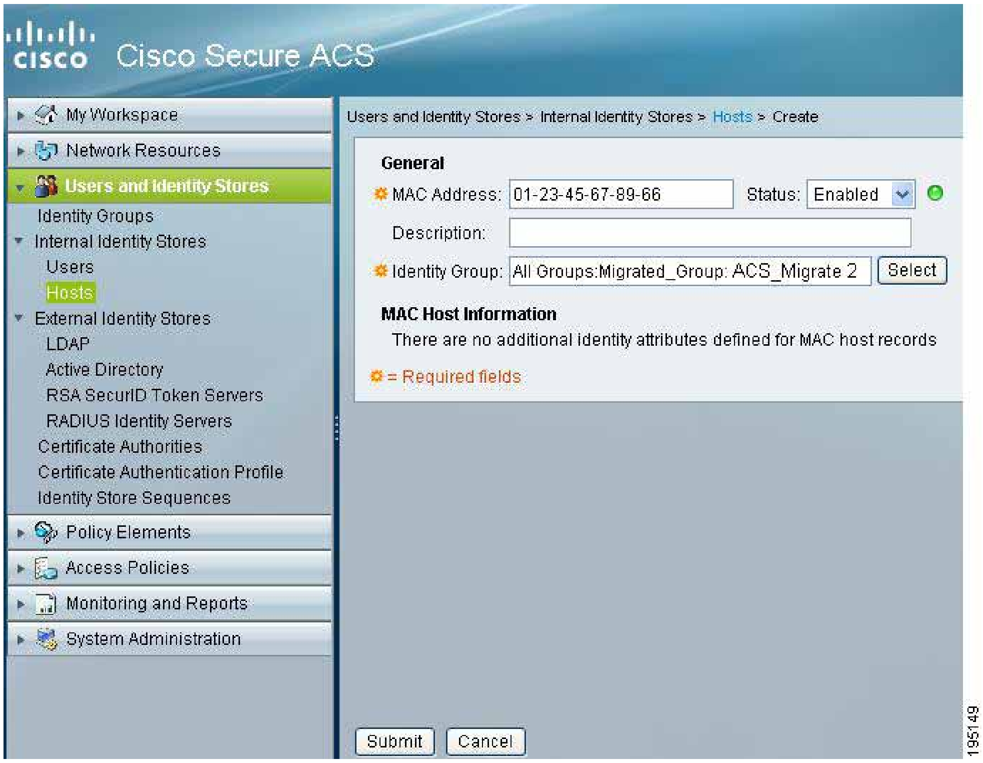
Authenticate MAC with:

○ LDAP Server: Not Selected

● Internal ACS DB

MAC Addresses	User Group
01-23-45-67-89-66	1: ACS_Migrate 2 (1 us

Figure 21 MAB Migrated to ACS 5.8



Users and Identity Stores > Internal Identity Stores > Hosts > Create

General

MAC Address: 01-23-45-67-89-66 Status: Enabled

Description:

Identity Group: All Groups:Migrated_Group: ACS_Migrate 2

MAC Host Information

There are no additional identity attributes defined for MAC host records

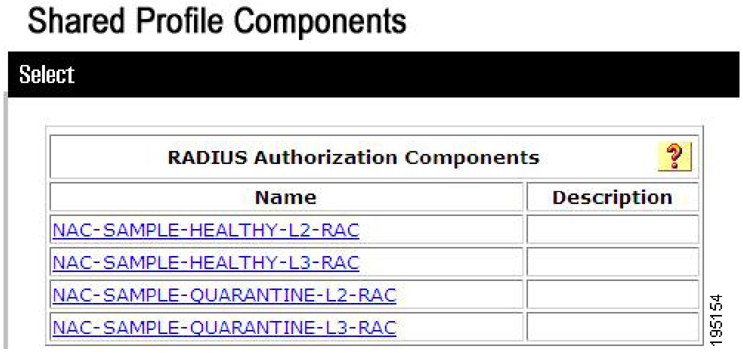
= Required fields

Shared RACs

Figure 22 on page 56 shows shared RADIUS Authorization Components (RACs) defined in ACS 4.x, and Figure 23 on page 56 shows shared RACs migrated to ACS 5.8.

Choose **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles** to access the migrated RACs.

Figure 22 Shared RACs Defined in ACS 4.x

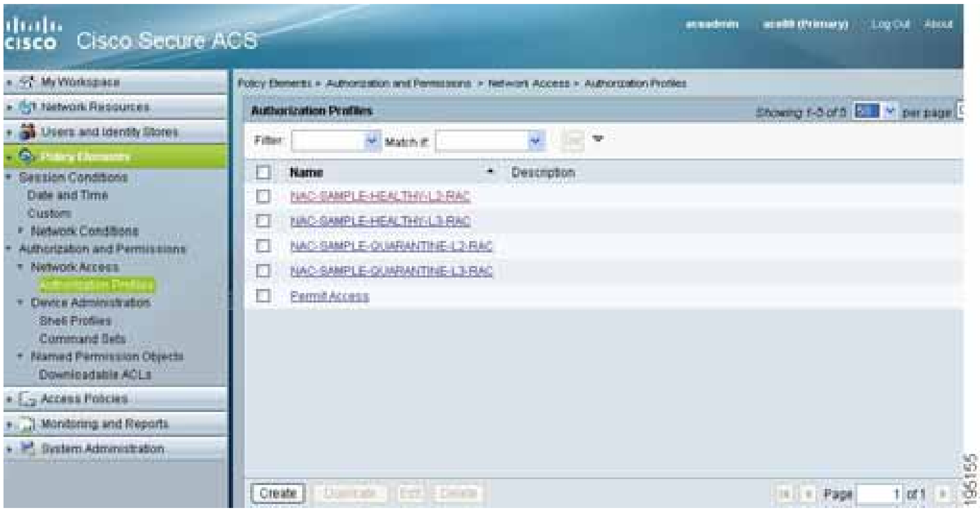


Shared Profile Components

Select

RADIUS Authorization Components	
Name	Description
NAC-SAMPLE-HEALTHY-L2-RAC	
NAC-SAMPLE-HEALTHY-L3-RAC	
NAC-SAMPLE-QUARANTINE-L2-RAC	
NAC-SAMPLE-QUARANTINE-L3-RAC	

Figure 23 Shared RACs Migrated to ACS 5.8



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles

Authorization Profiles — Showing 1-5 of 5 per page

Filter: Match if:

□	Name	Description
□	NAC-SAMPLE-HEALTHY-L2-RAC	
□	NAC-SAMPLE-HEALTHY-L3-RAC	
□	NAC-SAMPLE-QUARANTINE-L2-RAC	
□	NAC-SAMPLE-QUARANTINE-L3-RAC	
□	Permit Access	

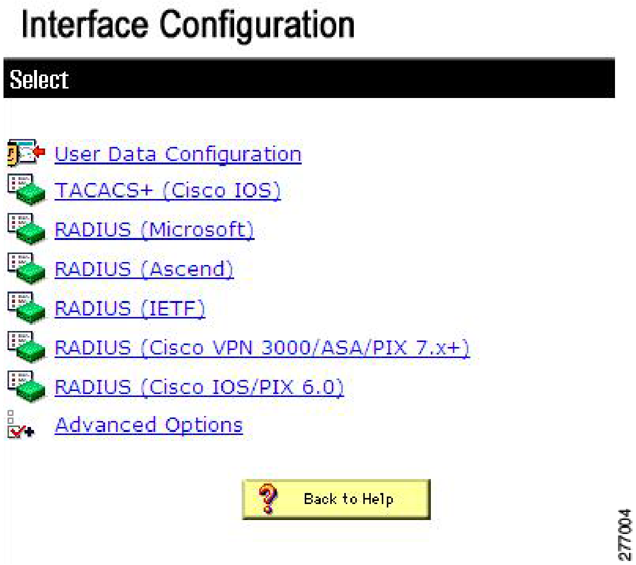
Page 1 of 1

RADIUS VSA

Figure 24 on page 57 shows RADIUS VSAs defined in ACS 4.x, and Figure 25 on page 57 shows RADIUS VSAs migrated to ACS 5.8.

Choose **System Administration > Configuration > Dictionaries > RADIUS > RADIUS VSA** to access the migrated RADIUS VSAs.

Figure 24 RADIUS VSAs in ACS 4.x

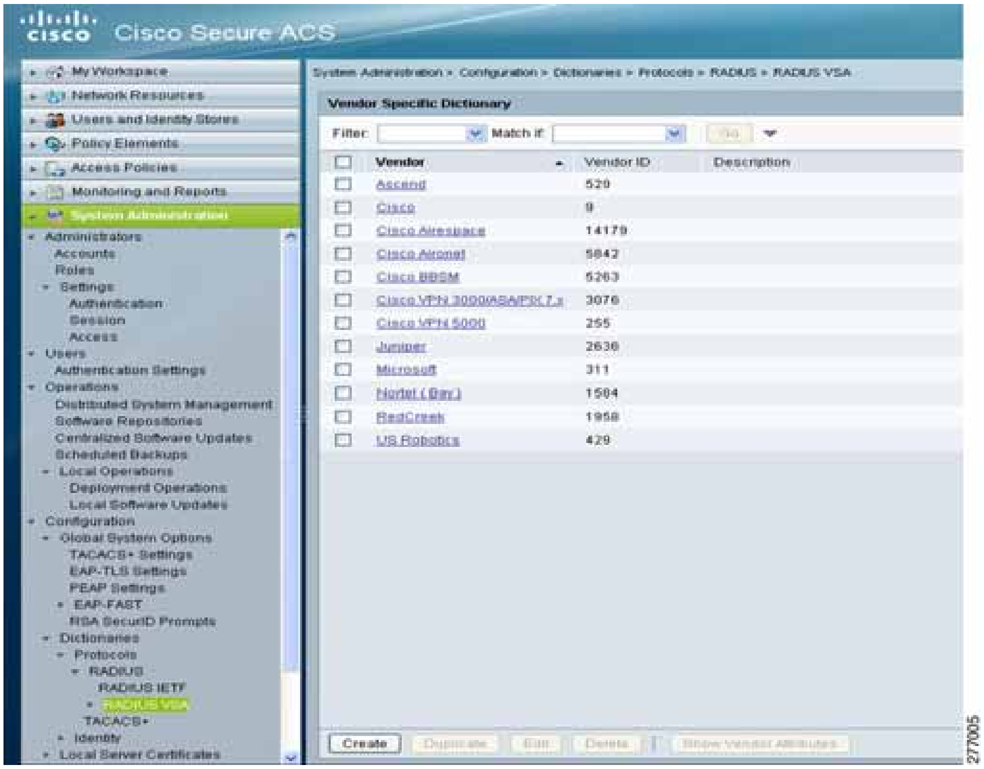


Interface Configuration

Select

- User Data Configuration
- TACACS+ (Cisco IOS)
- RADIUS (Microsoft)
- RADIUS (Ascend)
- RADIUS (IETF)
- RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)
- RADIUS (Cisco IOS/PIX 6.0)
- Advanced Options

Figure 25 RADIUS VSAs Migrated to ACS 5.8



System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA

Vendor Specific Dictionary

Filter: [ ] Match if: [ ] Go

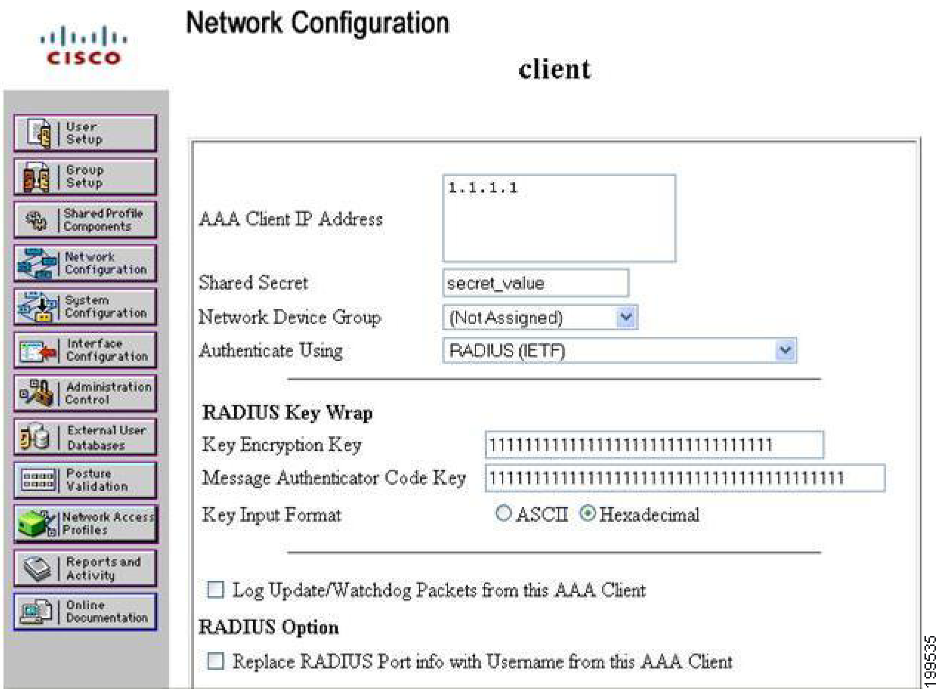
□	Vendor	Vendor ID	Description
□	Ascend	529	
□	Cisco	9	
□	Cisco Airespace	14179	
□	Cisco Aironet	5842	
□	Cisco BBSM	5263	
□	Cisco VPN 3000/ASA/PIX 7.x	3076	
□	Cisco VPN 5000	255	
□	Juniper	2636	
□	Microsoft	311	
□	Nortel (Bay)	1584	
□	RedCreek	1958	
□	US Robotics	429	

KEK and MACK Keys

Figure 26 on page 58 shows Key Encryption Key (KEK) and Message Authentication Code Key (MACK) keys defined in ACS 4.x, and Figure 27 on page 59 shows the KEK and MACK keys migrated to ACS 5.8.

Choose **Network Devices > Network Devices and AAA Clients**, select a device and click **Edit** to access the migrated KEK and MACK keys.

Figure 26 KEK and MACK Keys Defined in ACS 4.x



Network Configuration

client

AAA Client IP Address: 1.1.1.1

Shared Secret: secret_value

Network Device Group: (Not Assigned)

Authenticate Using: RADIUS (IETF)

RADIUS Key Wrap

Key Encryption Key: 11111111111111111111111111111111

Message Authenticator Code Key: 1111111111111111111111111111111111111111

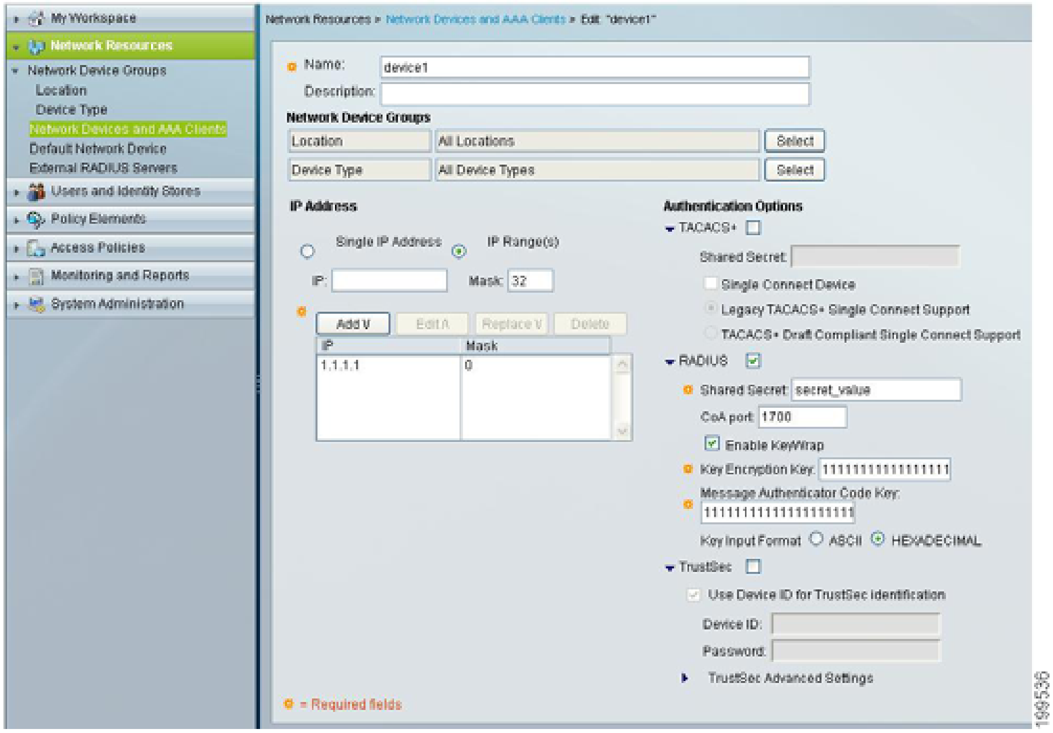
Key Input Format: ○ ASCII ● Hexadecimal

☐ Log Update/Watchdog Packets from this AAA Client

RADIUS Option

☐ Replace RADIUS Port info with Username from this AAA Client

Figure 27 KEK and MACK Keys Migrated to ACS 5.8



Network Resources > Network Devices and AAA Clients > Edit: "device1"

Name: device1

Description:

Network Device Groups

Location	All Locations	Select
Device Type	All Device Types	Select

IP Address

○ Single IP Address ● IP Range(s)

IP: Mask: 32

IP	Mask
1.1.1.1	0

Authentication Options

TACACS+ □

Shared Secret:

□ Single Connect Device

● Legacy TACACS+ Single Connect Support

○ TACACS+ Draft Compliant Single Connect Support

RADIUS ☑

Shared Secret: secret_value

CoA port: 1700

☑ Enable KeyWrap

Key Encryption Key: 1111111111111111

Message Authenticator Code Key: 11111111111111111111

Key Input Format ○ ASCII ● HEXADECIMAL

TrustSec □

☑ Use Device ID for TrustSec identification

Device ID:

Password:

TrustSec Advanced Settings

= Required fields