Migration Guide for Cisco Secure Access Control System 5.8.1

March 2016

- Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.
-

Preface

Published: March 21, 2016

This document describes the data migration process from Cisco Secure Access Control System (ACS) Releases 3.x and 4.x to Cisco Secure ACS Release 5.8.1. ACS 5.8.1 provides many new features and functionality.

There are several differences between ACS 3.x and 4.x and ACS 5.8.1 platforms. You should clearly understand these differences before attempting to migrate to ACS 5.8.1. This document highlights these differences and provides guidance on how to migrate your ACS 3.x and 4.x configuration to ACS 5.8.1.

In addition to understanding the information in this document, Cisco recommends that you perform a thorough evaluation of the ACS 5.x platform.

Audience

This guide is for administrators who want to migrate to the ACS 5.8.1 platform.

Organization

This guide includes the following sections:

Title	Description
ACS 5.8.1 Deployment Overview, page 1	Provides an overview of the ACS 5.8.1 deployment model in comparison with ACS 3.x and 4.x.
Understanding ACS 5.8.1 Configuration, page 1	Explains the configuration areas in ACS 5.8.1 in comparison with ACS 3.x and 4.x, to help understand how older configurations can be converted to ACS 5.8.1.
Configuration Migration Methods in ACS 5.8.1, page 1	Describes different methods to migrate the configuration from existing systems to ACS 5.8.1.
ACS 5.8.1 Migration Utility Support, page 1	Describes the scope of migration using the Migration Utility.
Migration Utility Setup and Installation, page 1	Describes system requirements, preinstallation considerations, and how to access the Migration Utility.
Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.8.1, page 1	Describes the data migration process in various phases using the Migration Utility.
ACS 5.8.1 Attribute Support in the Migration Utility	Describes attribute migration from ACS 4.x to ACS 5.8.1.
Configuration Mapping from ACS 3.x and 4.x to ACS 5.8.1	Provides configuration mapping from ACS 3.x and 4.x to ACS 5.8.1
Feature Comparison of ACS 3.x and 4.x with ACS 5.8.1	Provides detailed feature comparison of ACS 3.x and 4.x to ACS 5.8.1
Troubleshooting the Migration Utility	Describes how to troubleshoot the Migration Utility.

How to Use This Document

The following chapters and appendices contain instructions to migrate to ACS 5.8.1 from earlier releases:

- See Feature Comparison of ACS 3.x and 4.x with ACS 5.8.1 to ensure that all the key features for your deployment are met in ACS 5.8.1.
- See ACS 5.8.1 Deployment Overview, page 1 to understand the ACS 5.8.1 system level details such as platform support, the distributed deployment model, and system interfaces.
- See Understanding ACS 5.8.1 Configuration, page 1 to understand the key functional and configuration differences in ACS 5.8.1, and for specific configuration recommendations and examples.
- See Configuration Migration Methods in ACS 5.8.1, page 1 to understand the approaches for migrating an existing configuration.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands, keywords, and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Square brackets can indicate one of the following: ■ An optional element. ■ Default responses to system prompts.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Documentation Updates

Table 1 on page 3 lists the updates to the *Migration Guide for Cisco Secure Access Control System 5.8.1*.

Table 1 Updates to the Migration Guide for Cisco Secure Access Control System 5.8.1

Date	Description
03/21/2016	Cisco Secure Access Control System, Release 5.8.1.

Product Documentation

Note: It is possible for the printed and electronic documentation to be updated after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 2 on page 3 lists the product documentation that is available for ACS 5.8.1. To find end-user documentation for all the products on Cisco.com, go to: http://www.cisco.com/go/techdocs

Choose **Products > Security > Access Control and Policy > Policy and Access Management > Cisco Secure Access Control System**.

Table 2 Product Documentation

Document Title	Available Formats
Cisco Secure Access Control System In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-documentation-roadmaps-list.html
User Guide for Cisco Secure Access Control System 5.8.1	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html
CLI Reference Guide for Cisco Secure Access Control System 5.8.1	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-command-reference-list.html
Supported and Interoperable Devices and Software for Cisco Secure Access Control System 5.8.1	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-device-support-tables-list.html
Installation and Upgrade Guide for Cisco Secure Access Control System 5.8.1	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-installation-guides-list.html
Release Notes for Cisco Secure Access Control System 5.8.1	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-release-notes-list.html
Regulatory Compliance and Safety Information for Cisco Secure Access Control System	http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-6/regulatory/compliance/csacsrcsi.html

Related Documentation

Note: It is possible for the printed and electronic documentation to be updated after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 3 on page 4 lists the related documentation that is available for ACS 4.x.

Table 3 Related Documentation

Document Title	Available Formats
Installation Guide for Cisco Secure ACS for Windows 4.0	http://www.cisco.com/c/en/us/support/security/secure-access-control-server-windows/products-installation-guides-list.html
User Guide for Cisco Secure Access Control Server for Windows 4.0	http://www.cisco.com/c/en/us/support/security/secure-access-control-server-windows/products-user-guide-list.html
Installation Guide for Cisco Secure ACS for Windows 4.x	http://www.cisco.com/c/en/us/support/security/secure-access-control-server-windows/products-installation-guides-list.html
User Guide for Cisco Secure Access Control Server for Windows 4.1	http://www.cisco.com/c/en/us/support/security/secure-access-control-server-windows/products-user-guide-list.html
Installation Guide for Cisco Secure ACS for Windows 4.2	http://www.cisco.com/c/en/us/support/security/secure-access-control-server-windows/products-installation-guides-list.html
User Guide for Cisco Secure Access Control Server for Windows 4.2	http://www.cisco.com/c/en/us/support/security/secure-access-control-server-windows/products-user-guide-list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

ACS 5.8.1 Deployment Overview

The ACS 5.8.1 deployment model, which is similar to ACS 4.x, consists of a single primary and multiple secondary ACS servers, where configuration changes are made on the primary ACS server. These configurations are replicated to the secondary ACS servers.

All primary and secondary ACS servers can process AAA requests. The primary ACS server is also the default log collector for the Monitoring and Report Viewer, although you can configure any ACS server to be the log collector.

Although you can manage with a single ACS server, we recommend that you have two or more ACS servers, to provide AAA request processing redundancy. ACS 5.8.1 provides syslog support for external logging, and interfaces for automated and batch configuration provisioning.

An ACS deployment can scale for increased AAA request processing capacity by adding secondary servers. In large deployments, the secondary servers can be dedicated for specific functions. For example, you can use the primary ACS server only for configuration changes and not for processing AAA requests. You can designate a secondary ACS server only as the log collector.

In large environments, you can use load balancers to distribute AAA requests among the ACS servers in the deployment, simplify AAA client management, and provide high availability.

ACS servers are typically placed in the data centers or close to user clusters, for example, at regional sites.

For additional deployment information, see Understanding the ACS Server Deployment in the *Installation and Upgrade Guide for Cisco Secure Access Control System 5.8.1*.

Table 1 on page 1 describes the various ACS server roles.

Table 1 ACS Server Roles

ACS Server Roles	Role Descriptions
Primary	Configuration changes performed on the primary ACS server are replicated to all the secondary ACS servers in the deployment. At a time, you can have only one ACS server as the primary server.
Secondary	All ACS servers that receive configuration changes from the ACS primary server, are secondary servers.
Log Collector	ACS primary or secondary server that is also the log collector for the Monitoring and Report Viewer. There can only be one log collector in a deployment. Other ACS deployments (servers not synchronized with this deployment) cannot send ACS logs to this server.

The following sections describe the deployment differences between ACS 4.x and ACS 5.8.1, as well as some considerations when deploying ACS 5.8.1:

Windows Versus Linux-Based Applications

ACS 3.x and 4.x releases are available as Windows-based applications that can be installed on a Windows server platform. These applications are also available on an appliance called the ACS Solution Engine. This appliance is a hardware platform that is preloaded with ACS and Windows operating systems.

ACS 5.8.1 is a Linux-flavour application and is packaged with a Linux operating system. The application and the operating system package are shipped on an appliance, and they can also be installed in a virtual machine on a VMware ESXi Server.

There are functional and deployment differences between ACS for Windows and the ACS Solution Engine, but there is no functional difference between the ACS 5.8.1 hardware appliance and the ACS 5.8.1 installed on a virtual machine. Deployments that consist of ACS 5.8.1 hardware appliances and ACS 5.8.1 virtual machines are also supported.

Replication

ACS 3.x and 4.x provide a loose replication model. The characteristics of the ACS 3.x and 4.x replication model are:

- The configuration blocks represent logical areas of ACS configuration. For example, users and usergroups, usergroups only, network devices, distribution table, interface configuration, interface security settings, password validation settings, EAP-FAST settings, network access profiles, and logging configuration.
- The option to replicate one or more of the configuration blocks from the primary to secondary server.
- The whole block is replicated, regardless of the size of the configuration change.
- Cascading replication, which is the ability for a secondary ACS server to push a replication update to another ACS server.
- Replication can be initiated manually or according to a schedule.
- TACACS+ password updates are received on the primary server only.

In this loose replication model, the replicated blocks are synchronized between the primary and secondary servers, but other parts of the configuration can be different and tailored for the local environment.

The ACS 5.8.1 replication model is simple, efficient, and robust. The characteristics of the ACS 5.8.1 replication model are:

- Full synchronization between the primary and secondary servers.
- Transparent and immediate replication.
- Only configuration changes are replicated.
- Configuration changes can be made only on the primary server.
- No cascading replication.
- Automatic recovery for missed updates.
- Ability to promote a secondary server to primary server.

- TACACS+ password updates can be received on any ACS instance.

A region-specific access policy must be implemented in the ACS 5.8.1 network access policy configuration. This is because ACS 5.8.1 configuration is fully synchronized between the primary and secondary servers, and configuration changes cannot be made directly to the secondary servers.

Identity Stores

The main difference related to identity store support between ACS 3.x and 4.x and 5.8.1 is that ACS 5.8.1 does not support Open Database Connectivity (ODBC) for authentication to databases and proxy forwarding of TACACS+ requests. ACS 5.8.1 supports the following identity stores for authentication:

- ACS internal store
- Active Directory
- Lightweight Directory Access Protocol (LDAP) directories
- One-time password servers, using the
  - RSA SecurID interface
  - RADIUS interface
- Proxy forwarding to other stores through RADIUS (RADIUS proxy)

Logging

In ACS 5.8.1, the Monitoring and Report Viewer functionality is part of ACS. In an ACS 5.8.1 deployment, an ACS server is designated as the log collector for the reporting and monitoring functionality. All of the other ACS servers send log messages to the designated log collector.

ACS supports syslog for logging to external servers.

ACS 5.8.1 provides a web service interface for the Cisco Wireless Control System (WCS) to obtain user authentication information from the Monitoring and Report Viewer.

Configuration

In ACS 5.8.1, the primary mode for configuration is a web-based user interface. ACS 5.8.1 also has a command-line interface (CLI) through which system tasks and file-based configuration updates can be made.

You can access the CLI from the console port, keyboard, video, mouse (KVM), and SSH. A web-service interface is provided to develop password change applications for internal ACS users.

Table 2 on page 4 provides the number of internal users and network devices supported by ACS. Users and network devices are the commonly used and largely populated ACS objects.

Table 2 Internal Users and Device Configuration Capacity

ACS Object	Configuration Capacity
Internal Users	300,000
Internal Hosts	150,000
Network Devices	100,000

Licensing

The 3.x and 4.x releases of ACS did not require application of the key or license files. However, you need to apply a license file for the 5.x releases. The ACS 5.8.1 licenses are available at: http://cisco.com/go/license

Table 3 on page 4 lists the available ACS 5.8.1 licenses.

Table 3 Available ACS 5.8.1 Licenses

License	Description
Base Server	One for each ACS instance.
Large Deployment	One for each ACS deployment when the network device count (based on IP address) in ACS exceeds 500. Configuring the Default Network Device contributes to the device count.

Server Deployment Recommendations

Table 4 on page 4 describes the component mapping from ACS 3.x and 4.x to ACS 5.8.1.

Table 4 Component Mapping

ACS 3.x and 4.x Component	ACS 5.8.1 Component	Notes
ACS for Windows	VM in VMware ESXi, 1121, 3415, 3495, 3515, or 3595 appliance	There is no ACS 5.8.1 Windows option. ACS 5.8.1 is an application that can run on a VMware or supported appliance.
ACS Solution Engine (1111, 1112, 1113)	VM in VMware ESXi, 1121, 3415, 3495, 3515, or 3595 appliance	ACS 1111, 1112 and 1113 platforms do not support ACS 5.8.1. ACS 4.2 can run on the 1120.
ACS Remote Agent	N/A	Remote Agent is not required in ACS 5.8.1.
ACS View 4.0	VM in VMware ESXi, 1121, 3415, 3495, 3515, or 3595 appliance	ACS 5.8.1 has built-in ACS View functionality.

Deployment guidelines for ACS 5.8.1:

- In most cases, a one-to-one ACS server replacement is appropriate.

  The authentication performance of ACS 5.8.1 is same as the previous versions.

- Deploy at least two ACS instances to provide redundancy.

- Add more ACS servers to scale the authentication performance.

  Ensure that a single ACS server can handle peak authentication rates of its AAA clients and any AAA clients that rely on it as a backup AAA server.

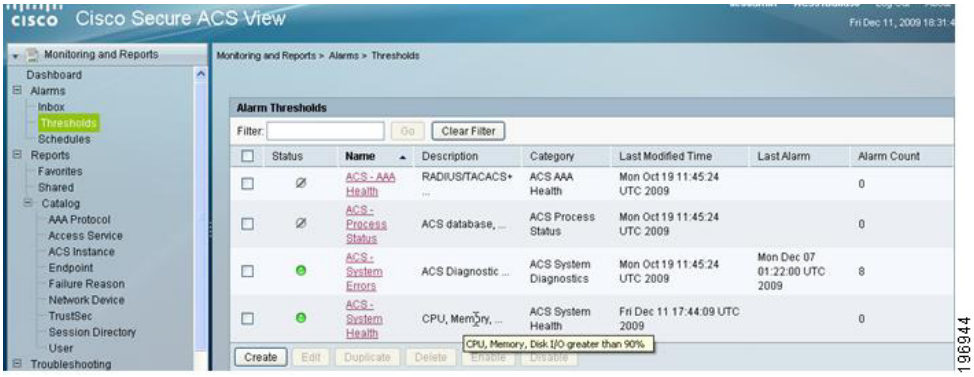
- You can use secondary ACS servers to process AAA requests only to scale a deployment environment. Use the primary for configuration updates and log collection only.

  Use the most powerful hardware for the log collector. For example, the Cisco SNS-3515, Cisco SNS-3595, Cisco SNS-3415 or Cisco SNS-3495 appliances over the 1121 appliance.

- Use load balancers to receive AAA requests, simplify AAA client management, improve resiliency, and better utilize ACS authentication capacity.

- Monitor the ongoing resource utilization. You can do this by enabling the ACS system health alarm threshold in the Monitoring and Report Viewer, as shown in Figure 1 on page 5.

Figure 1 Alarm Threshold in ACS 5.8.1



Understanding ACS 5.8.1 Configuration

ACS 5.8.1 Configuration

This chapter explains the differences in configuration between ACS 3.x and 4.x and ACS 5.8.1 when you convert the existing 3.x and 4.x configurations to 5.8.1.

This chapter contains the following sections:

Table 1 on page 1 describes the main configuration areas in ACS 5.8.1.

Table 1 Main Configuration Areas in ACS 5.8.1

Configuration Area	What Will Be Configured
Network Resources	AAA clients, client grouping, and RADIUS proxy servers
Users and Identity Stores	Internal users, Internal hosts, Active Directory, LDAP directories, one-time password servers, RADIUS identity stores, certificate authority information, and identity store sequences
Policy Elements	Conditions and authorization profiles for network access policy
Access Services	Network access policy to address different access scenarios
Monitoring and Reports	ACS monitoring, reporting and troubleshooting tasks
System Administration	ACS system administration tasks

Network Resources

AAA clients and RADIUS proxy servers are defined and organized under the Network Resources drawer.

The following components are configured under Network Resources:

Network Device Groups

Key changes in ACS 5.8.1:

- A single device can be a member of multiple groups—Network Device Group hierarchies.

- Device group level shared secrets are not available.
- Device group is not a container for AAA server definitions.

Network device groups allow you to group devices based on location, type, and other groupings. This is especially important for applying network access policy based on these groupings. For example, restrict West Coast firewall administrator to have access to only West Coast firewalls.

When you plan to migrate the network device to ACS 5.8.1, we recommend that you plan the device grouping before importing or configuring the devices. This will allow the assignment of groups to devices while they are being created in ACS 5.8.1.

ACS 3.x and 4.x has a flat device grouping model where a single device can belong to only one device group. This model causes a proliferation of groups when you are trying to group devices in multiple ways. Grouping locations hierarchically is very common.

For example, group by continent, region and country. The following example shows groups in ACS 3.x and 4.x:

- Africa-Southern-SouthAfrica
- Africa-Southern-Namibia
- Africa-Southern-Botswana

Devices are often grouped by type. Extending the above example to incorporate type grouping would result in the following groups:

- Africa-Southern-SouthAfrica-Firewalls
- Africa-Southern-SouthAfrica-Switches
- Africa-Southern-SouthAfrica-Routers
- Africa-Southern-Namibia-Firewalls
- Africa-Southern-Namibia-Switches
- Africa-Southern-Namibia-Routers
- Africa-Southern-Botswana-Firewalls
- Africa-Southern-Botswana-Switches
- Africa-Southern-Botswana-Routers

The number of groups increase when other parameters, such as device types, vendors, and so on are added.

ACS 5.8.1 addresses this device group proliferation issue by providing network device group hierarchies. There can be multiple hierarchies representing different groups. A device can belong to one node in each hierarchy. Figure 1 on page 3, Figure 2 on page 3, and Figure 3 on page 3 show three different network device group hierarchies.

Figure 1 Network Device Group Hierarchies

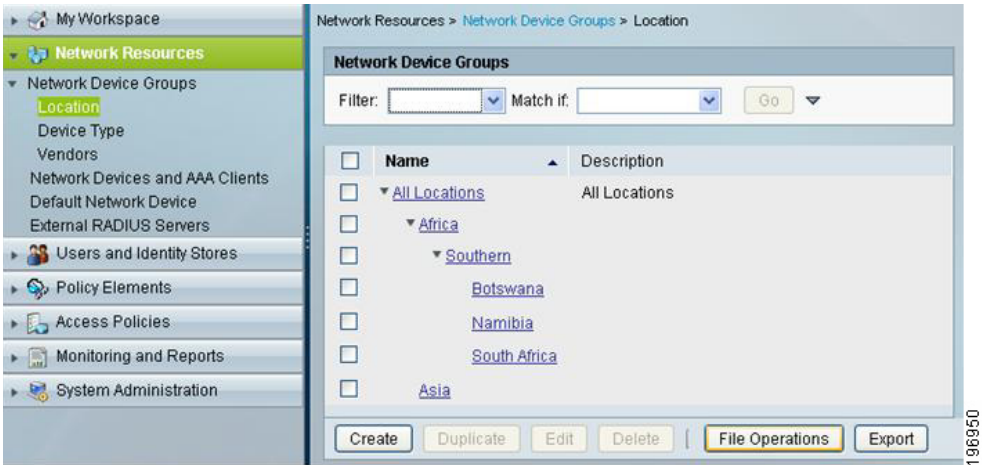


Figure 2 Network Device Group Hierarchies

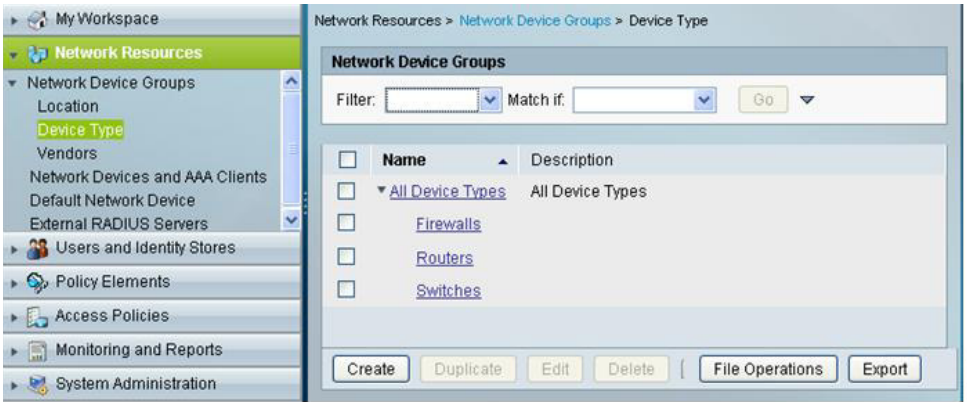
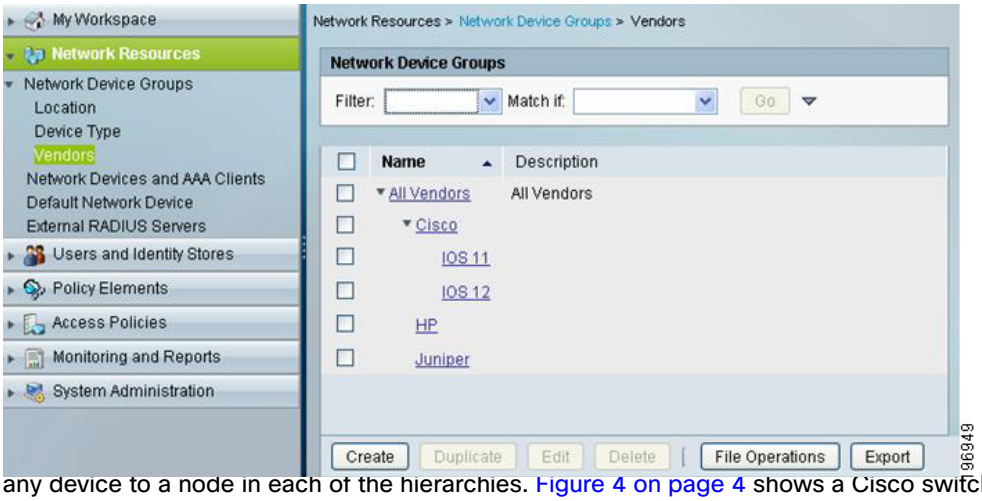
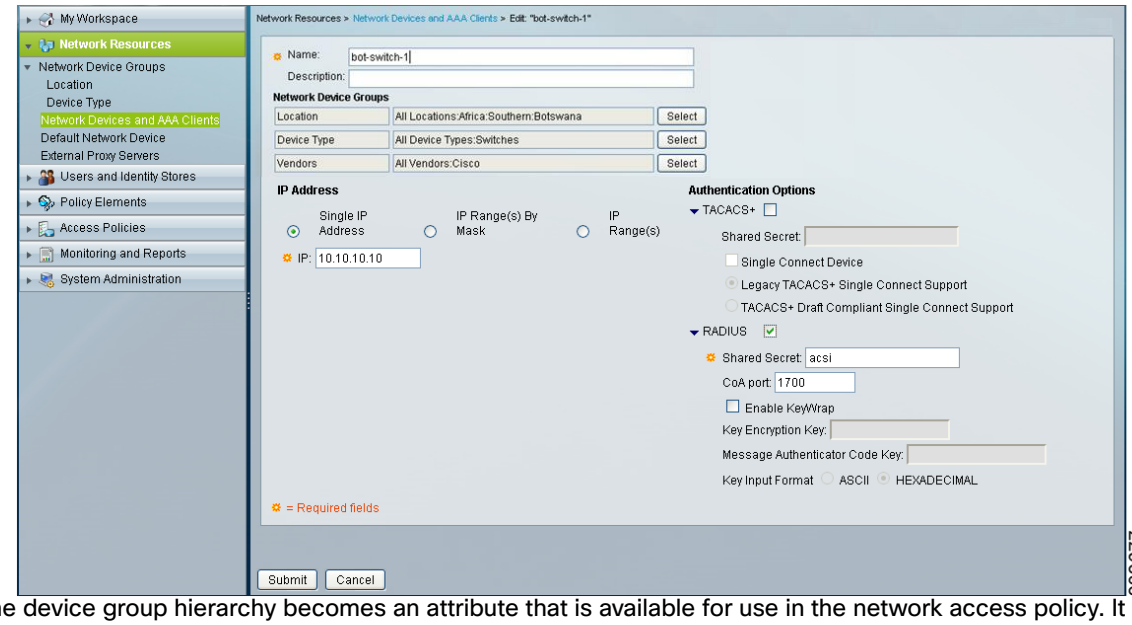


Figure 3 Network Device Group Hierarchies



You can assign any device to a node in each of the hierarchies. Figure 4 on page 4 shows a Cisco switch device that is located in Botswana.

Figure 4 An Example of a Cisco Switch Device Located in Botswana



Each node in the device group hierarchy becomes an attribute that is available for use in the network access policy. It is easy to represent the devices that represent the intersection of multiple hierarchies by referencing nodes in multiple hierarchies.

The following table shows an example of a rule that includes a condition that applies to Cisco firewalls in Namibia:

Conditions			Result
NDG:Location	NDG:Device Type	NDG:Vendors	
Is Namibia	Is Firewall	Is Cisco	...

Migration Notes

- Plan your device grouping approach to make use of the more natural hierarchical grouping in ACS 5.8.1.
- ACS 5.8.1 does not support per device group shared secrets that are available in ACS 3.x and 4.x. ACS 5.8.1 requires a shared secret to be defined for each device definition.

Network Devices

Key changes in ACS 5.8.1:

- Single device definition for a AAA client supporting both TACACS+ and RADIUS—Separate definitions are no longer needed.
- Mask-based IP address.
- A default device definition for both TACACS+ and RADIUS.

Figure 5 on page 5 shows the ACS 5.8.1 network device configuration.

Figure 5 ACS 5.8.1 Network Device Configuration

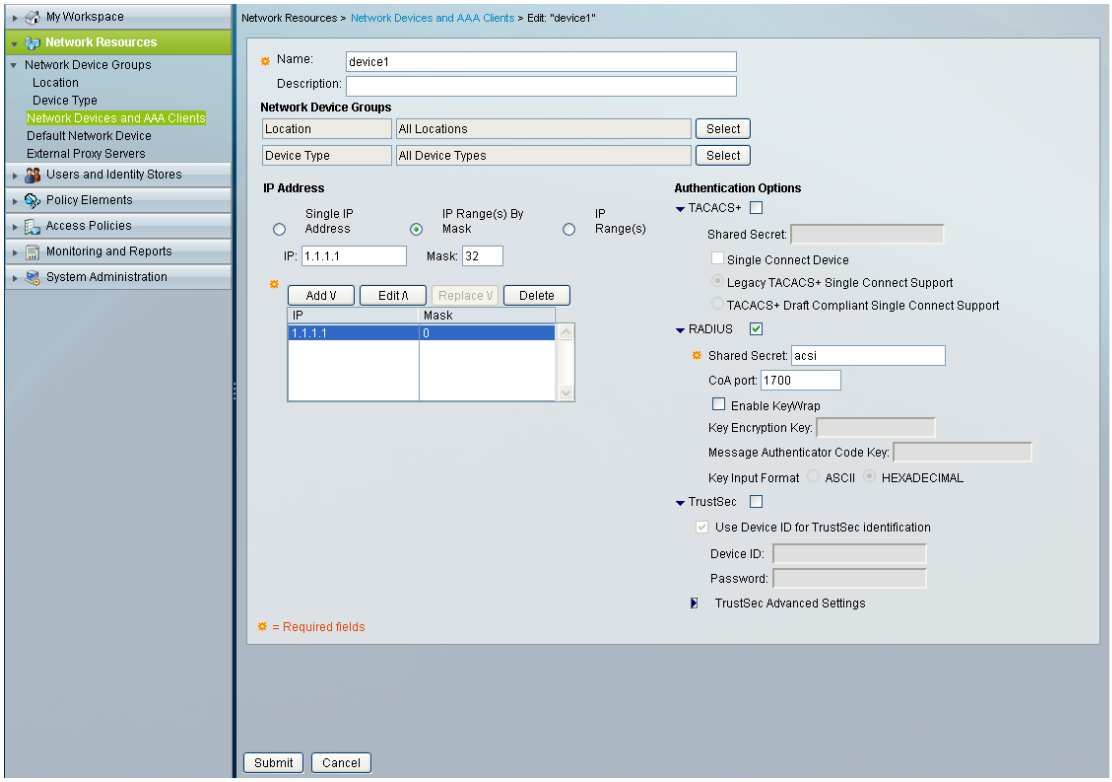
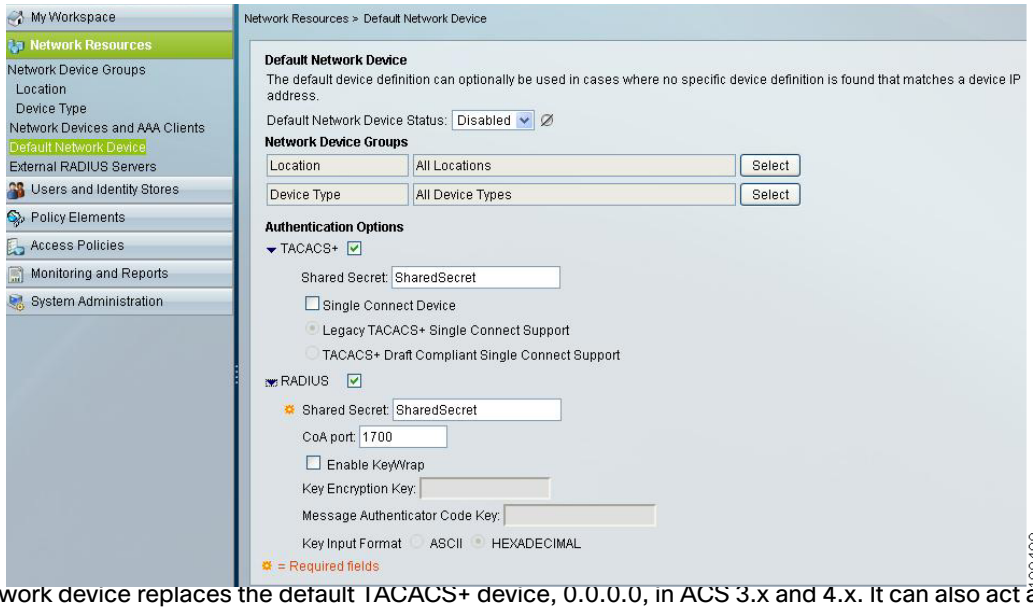


Figure 5 on page 5 shows a device definition representing any client from subnets 10.10.20.0 and 10.10.30.0. These clients can send TACACS+ or RADIUS requests as both are enabled in the device configuration.

Figure 6 on page 5 shows the default network device.

Figure 6 Default Network Device



The default network device replaces the default TACACS+ device, 0.0.0.0, in ACS 3.x and 4.x. It can also act as a default device for RADIUS requests.

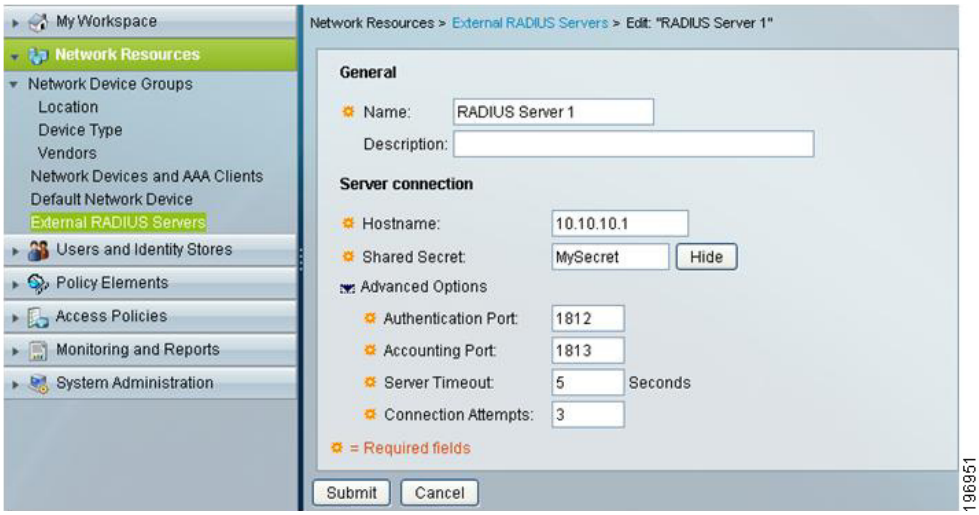
Migration Notes

- Consolidate double device definitions for TACACS+ and RADIUS in ACS 3.x and 4.x to a single device in ACS 5.8.1.
- ACS 5.8.1 uses subnet masks for IP address definitions. Map the ACS 3.x and 4.x configurations using IP ranges and wildcards to subnet mask ranges in ACS 5.8.1.
- The default network device is a useful tool to enable faster migration to ACS 5.8.1. It allows ACS 5.8.1 to start receiving AAA requests while more specific device definitions are being created.

External RADIUS Servers

The last configuration area under the Network Resources drawer is the External RADIUS Servers. This option allows you to define the RADIUS servers to which ACS will proxy. Figure 7 on page 6 shows an External RADIUS server configuration in ACS 5.8.1.

Figure 7 ACS 5.8.1 RADIUS Server Configuration



Migration Notes

- In ACS 5.8.1, there is no proxy distribution table to direct authentication requests to other AAA servers.
- For RADIUS proxy, configure a RADIUS proxy access service.

Users and Identity Stores

The following components are configured under Users and Identity Stores:

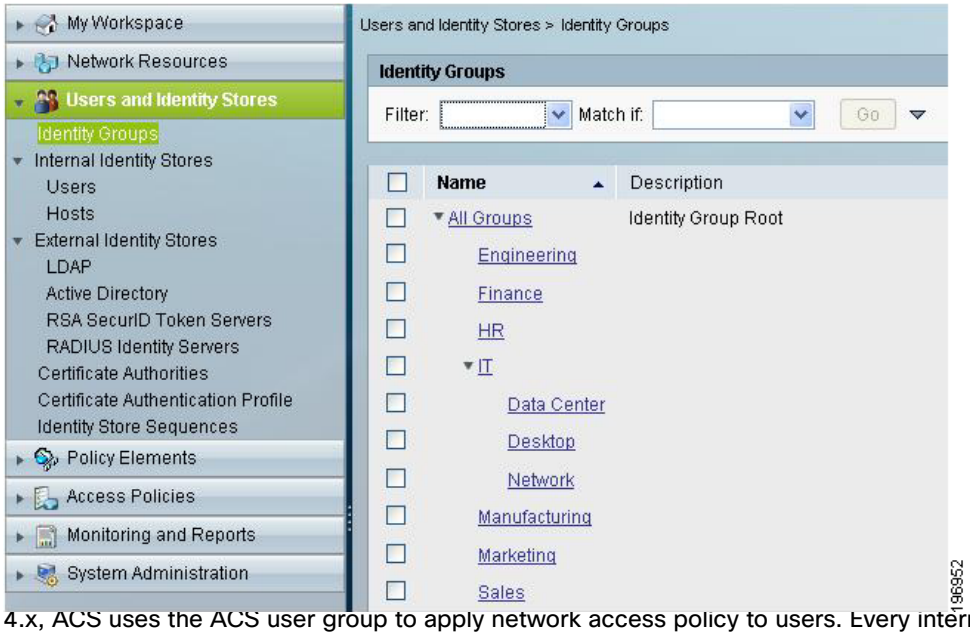
Identity Groups

Key changes in ACS 5.8.1:

- The ACS 5.8.1 identity group does not contain access policy permissions, similar to the ACS 3.x and 4.x user group.

- Users need not be associated to an ACS group.
- External groups need not be mapped to an ACS group.
- The identity group provides hierarchical grouping. Figure 8 on page 7 shows identity group hierarchies in ACS 5.8.1.

Figure 8 Identity Groups in ACS 5.8.1



In ACS 3.x and 4.x, ACS uses the ACS user group to apply network access policy to users. Every internal and external user that is authenticated by ACS is mapped to only one ACS user group. In ACS 5.8.1, network access policy is not applied through a group, but it is applied through access services.

Access services contain rules made up of conditions that govern the policy that will be applied to a user. The user's group membership is one of many attributes that can be used to compose these conditions. As policy is not applied through a group, ACS 5.8.1 does not require the group association.

In ACS 3.x and 4.x, when external identity stores such as Active Directory or LDAP directories are used for user authentication, and when the users' directory group membership is relevant to their network access, a group mapping is required to map users' external group membership to an ACS group. This is to apply the appropriate network access policy.

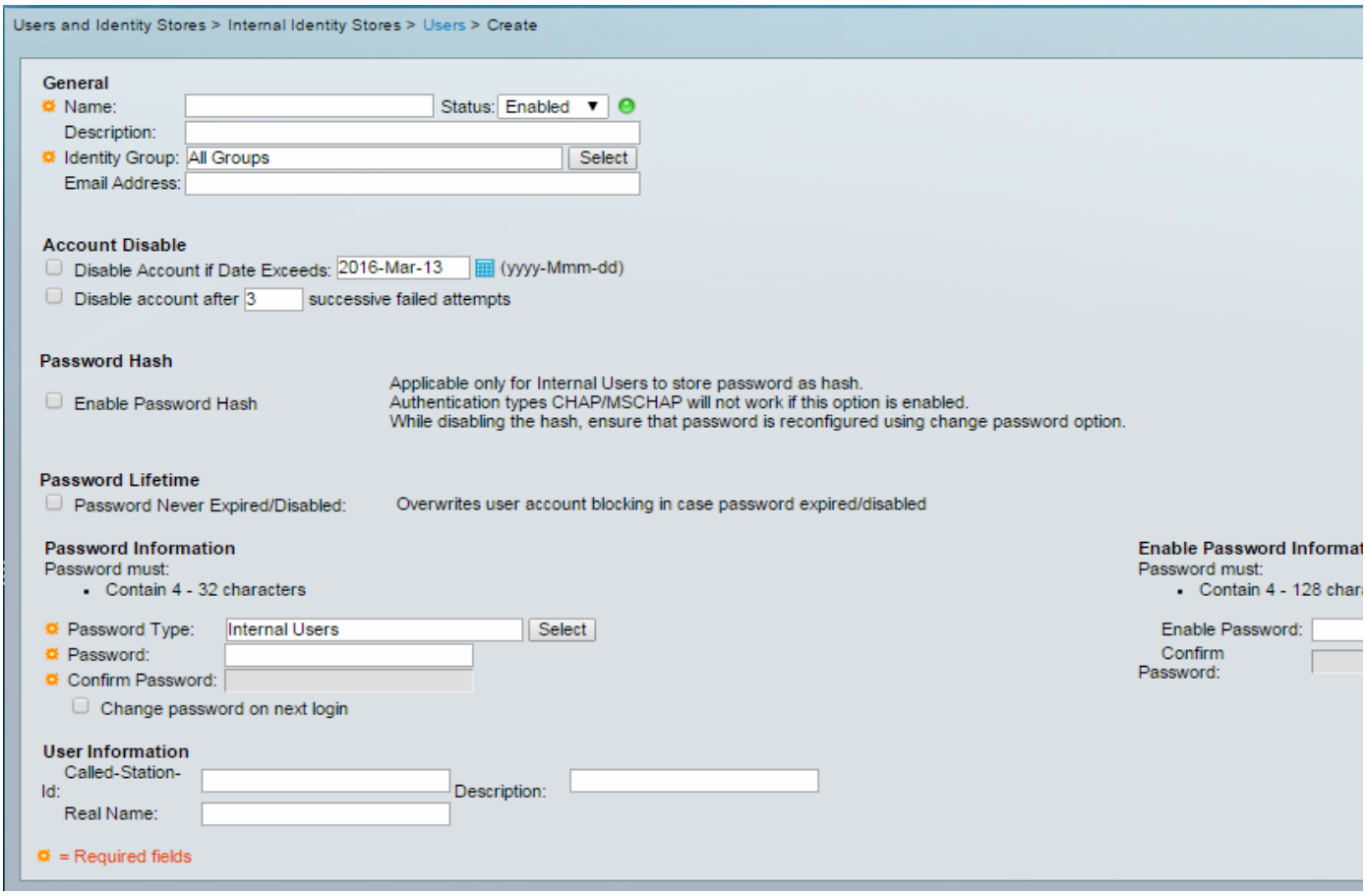
In ACS 5.8.1, external group memberships are attributes that can be used directly when you create the network access policy. Hence, you do not have to use group mapping.

Migration Notes

- Consider if you really need identity groups in ACS 5.8.1—Identity groups are needed only to maintain users within ACS.
- Take advantage of the hierarchical nature of identity groups.
- ACS 3.x and 4.x authorizations that are part of the user group are configured in the Policy Elements and Access Services drawers.
- Instead of creating combination groups that represent users who belong to multiple groups, consider specifying these different groups by extending the internal identity store schema.

  Figure 9 on page 8 shows an example of a user Fred in the IT group, who is also classified by location and whether he can access switches, firewalls, and routers.

Figure 9 Internal Identity Stores in ACS 5.8.1



Internal Identity Stores

Key changes in ACS 5.8.1:

- In addition to a user store, ACS 5.8.1 has a host store for host MAC addresses.
- Access policy permissions do not contain user records.
- Disable user accounts if the configured number of days exceed.
- Disable user accounts if the user is inactive for the specified number of days.
- Enable password hashing for users and administrators.
- User schema can be customized to add extra user fields.
- Custom user fields can store user-specific values that can be leveraged in access policies.

The ACS 5.8.1 user store is simple when compared to ACS 3.x and 4.x, because the policy components have moved to policy elements and access services in ACS 5.8.1. The ACS 5.8.1 user store is similar to an external store, because the schema can be customized to hold user-specific information such as first name, last name, location, and email.

These fields can also become attributes that can be used in access policy. For example, it is possible to use the user's location as a condition, or an IP address value as a RADIUS return value.

ACS 5.8.1 provides a separate hosts store to maintain a MAC address database for agentless host scenarios (MAC authentication bypass). Similar to the user store, custom fields can be added to host records for use in access policy.

Migration Notes

- Use identity store sequences in combination with access service identity policy to implement the ACS 3.x/4x ability to select the password authentication method from the user record.
- User password policy is a set under **System Administration > Users > Authentication Settings**.

External Identity Stores

Key changes in ACS 5.8.1:

- ACS 5.8.1 joins Active Directory (AD) directly and does not rely on a domain-joined Windows Server. ACS Remote Agent is not required.
- ODBC databases are not supported in ACS 5.8.1, but other identity stores are supported, including LDAP directories and one-time password servers.
- ACS 5.8.1 adds RADIUS Identity Store for RADIUS-based one-time passwords servers and for RADIUS proxy where proxy response attributes are required for access policy.
- ACS 5.8.1 adds the ability for AD and LDAP user attributes to be used, in addition to user group membership, in access policy.
- Identity store lists, provided by the unknown user policy in ACS 3.x and 4.x, are configured using identity store sequences in ACS 5.8.1. There is no concept of a dynamic user in ACS 5.8.1.

The External Identity Store configuration is similar to the External User Databases in ACS 3.x and 4.x. In ACS 5.8.1, external identity stores are configured and ACS communicates with them for authentication and authorization.

For Active Directory, ACS 5.8.1 joins an AD domain, rather than leveraging the underlying Windows operating system, similar to ACS 3.x and 4.x. ACS 5.8.1 relies on trust relationships between its domain and other domains to perform cross-domain authentication, as in ACS 3.x and 4.x.

You must enter the username and password credentials in the ACS 5.8.1 configuration for ACS to join and communicate with the AD domain. The credentials must have sufficient permissions to create a computer object. If a user's AD group membership and attribute information are required for access policy, they must first be selected in the AD configuration.

LDAP directory configuration is similar to ACS 3.x and 4.x. Multiple LDAP directories can be defined in ACS 5.8.1, similar to ACS 3.x and 4.x. The LDAP directory configuration allows you to select groups and attributes for use in the access policy.

For one-time password authentication, ACS 5.8.1 supports the RSA SecurID native interface by configuring RSA SecurID Token Servers. For non-RSA one-time password servers, RADIUS interaction can be configured using the RADIUS Identity Server option.

Migration Notes

Go to **System Administration > Configuration > Global System Options > RSA SecurID Prompts** to configure RSA SecurID prompts.

Certificate Authorities and Certificate Authentication Profiles

Key changes in ACS 5.8.1:

- Certificate Authentication Profiles allows you to customize the authentication for different certificate profiles.
- Identity store authorization is optional for certificate-based authentication.
- Root CA certificates must be imported.

Trusted certificate authorities are defined under the certificate configuration options in Users and Identity Stores. Here, the authentication characteristics of different certificate profiles are also specified.

Certificate authentication profiles are referenced in access service identity policy, and they allow you to specify:

- The certificate field that should be used as the principal username.
- Whether a binary comparison of the certificate should be performed.

Migration Notes

- PEM- or DER-formatted X.509 certificates can be imported to create a list of trusted CAs.
- ACS 5.8.1 does not check whether the certificate owner exists in a directory, but you can check the existence of a user attribute in an access service authorization policy.

Identity Store Sequences

Key changes in ACS 5.8.1:

- Provides the ability to specify different identity stores for authentication and authorization
- A list of identity stores can be configured for both authentication and authorization

In most of the deployments, a single identity store is used for user authentication and authorization. There are many deployments where network access relies on more than one identity store.

The identity store sequence in ACS 5.8.1 addresses this requirement and can be referenced instead of an identity store in an access service identity policy. The identity store sequence allows you to specify one list of identity servers for authentication and the other for authorization.

For example, for one-time password users, where a user must be authenticated against a one-time password server, but additional authorization information such as their group memberships, are only available in a directory.

Migration Notes

Use identity store sequences to replace the functionality provided by the unknown user policy in ACS 3.x and 4.x.

Policy Elements

The primary components of access policy are identity and authorization policies. Both these policies are represented in separate rule tables in the ACS 5.8.1 access service. Each rule in a rule table is composed of conditions and results.

In the Policy Elements configuration area, you can create conditions and customize them. Authorization results are created in this area.

The following components are configured under Policy Elements:

- Session Conditions, page 10
- Authorizations and Permissions, page 11
- Access Policies, page 11

Session Conditions

The key changes in ACS 5.8.1 are:

- Network conditions that were formerly known as Network Access Restrictions (NARs) are defined in this configuration area.
- The attributes available to create access service rule conditions include:

  - System dictionary attributes
  - RADIUS and TACACS+ attributes
  - Network Device Groups (NDGs)
  - User attributes and group memberships
  - Certificate attributes
- You can define the following additional conditions under session conditions:
  - Date and Time condition allows you to define date and time ranges.
  - Custom condition allows existing attributes to be renamed to simplify policy representation.
  - Network condition allows you to define ACS 3.x and 4.x equivalent NARs.

Migration Notes

Access policy conditions configured in the ACS 3.x and 4.x user, user group, or shared profile components, should be configured under session conditions.

Authorizations and Permissions

The key changes in ACS 5.8.1 are:

- All access policy authorization must be defined in this configuration area.
- The various types of network authorizations include:
  - Device administration authorization using TACACS+ shell privileges and command sets.
  - Network access authorization using RADIUS attributes.
  - Downloadable ACLs, typically used for remote access authorization.

Migration Notes

Access policy authorizations that were formerly configured in the ACS 3.x and 4.x user, user group, or shared profile components, should be configured under Authorizations and Permissions.

Access Policies

The key changes in ACS 5.8.1 are:

- Access policies are the core of network access policy in ACS 5.8.1.
- All network access policy for RADIUS and TACACS+ authentication and authorization requests is configured here.

All authentication and authorization requests in ACS 5.8.1 must be processed by an access service. An access service defines the authentication and authorization policy. ACS 5.8.1 supports multiple access services for different network access scenarios.

Access services provide a way to logically separate different network access policies. For example, an organization may implement one access service for device administration policy, and another access service for remote VPN access.

Additional access services may also be configured to simplify the policy within any one access service. For example, instead of configuring one access service to address all 802.1X network access, you can use multiple access services to address policy for wired, wireless, machine, and host 802.1X access.

In addition to access services, you must also configure the service selection policy. The service selection policy instructs ACS on how to direct authentication and authorization requests to the appropriate access service.

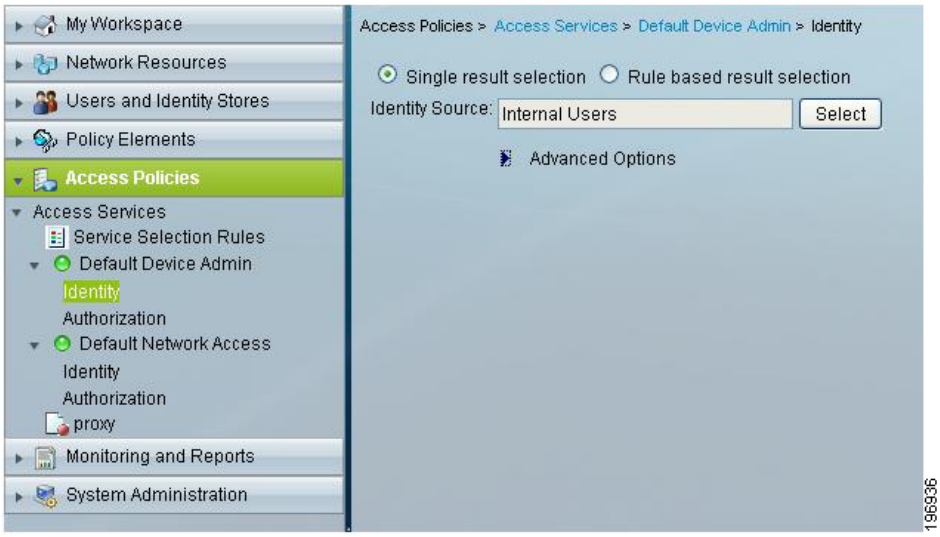
For more information on the Access Policies, see the *User Guide for Cisco Secure Access Control System*.

Migration Notes

- For device administration scenarios using TACACS+, you can update the preconfigured default device admin access service.
  - Modify the identity policy to use another identity store, such as one-time passwords, if the default setting of internal users is not appropriate.
  - Select an identity store sequence, as shown in Figure 10 on page 12, if more than one identity store is required to authenticate and authorize users.

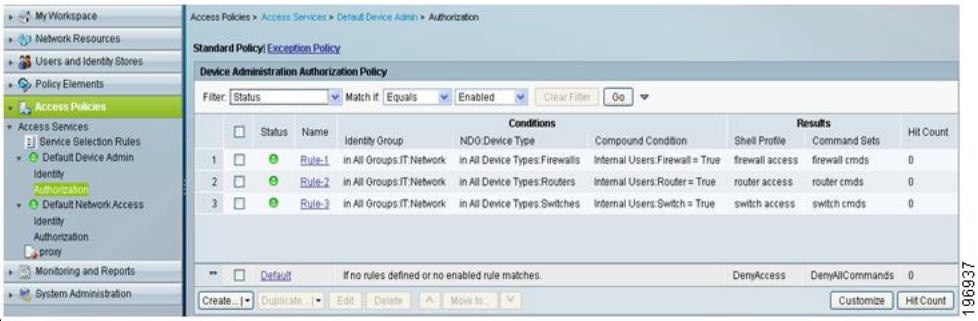
  For example, users may be authenticated to a one-time password server, but the ACS internal user store may be required to retrieve user attributes for authorization. In some cases, ACS may need to check both the ACS internal user store and active directory, to locate a user for authentication.

Figure 10 Identity Store Sequence



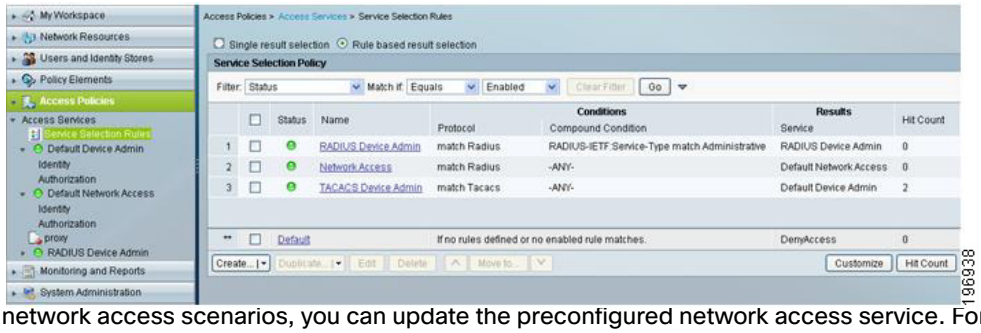
- Utilize the new user and network device groupings to create authorization policy, as shown in Figure 11 on page 12.

Figure 11 Authorization Policy



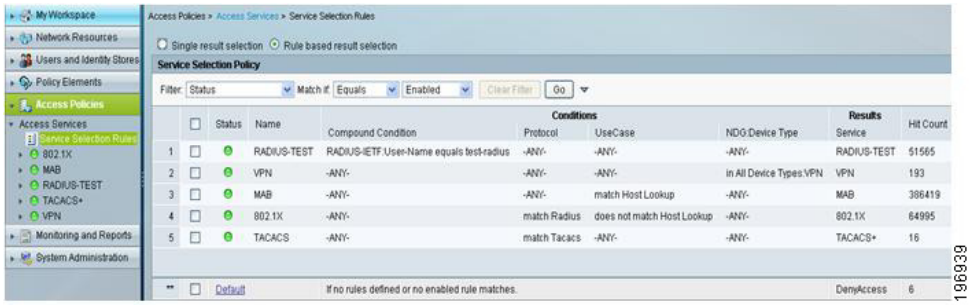
- For RADIUS-based device administration, create a separate access service, and differentiate these authentication and authorization requests from network access services, in the service selection policy. Figure 12 on page 13 shows the service selection policy.

Figure 12 Service Selection Policy



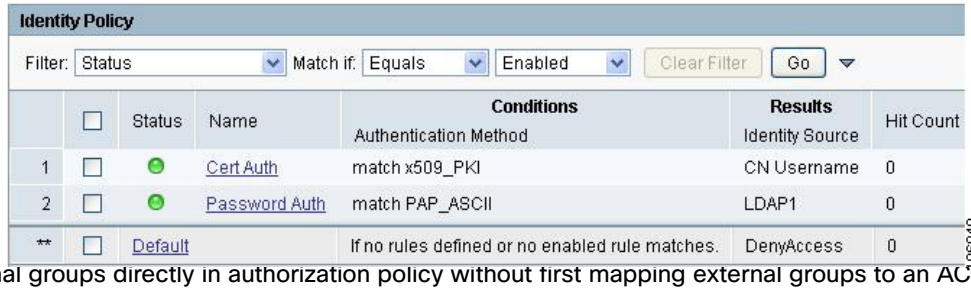
- For simple network access scenarios, you can update the preconfigured network access service. For more complex network access scenarios, introduce additional access services, as shown in Figure 13 on page 13.

Figure 13 Network Access Service Rules



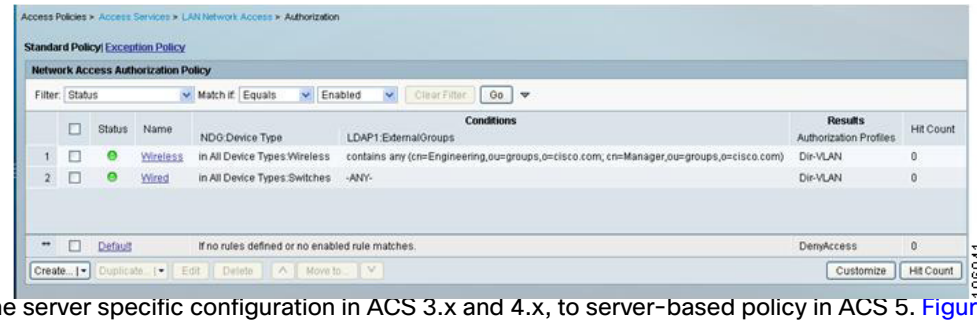
- When creating an access service that addresses both certificate and password-based authentication. For example, certificate-based machine authentication, and password-based user authentication, a rules-based identity policy is required, as in Figure 14 on page 13.

Figure 14 Rules-Based Identity Policy in ACS 5.8.1



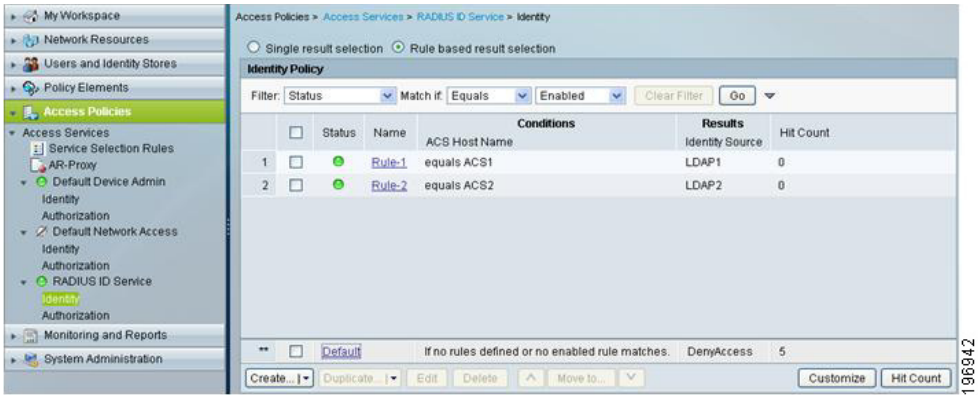
- Use external groups directly in authorization policy without first mapping external groups to an ACS group.

Figure 15 Using External Groups Directly in Authorization Policy



- Convert the server specific configuration in ACS 3.x and 4.x, to server-based policy in ACS 5. Figure 16 on page 14 shows how to use the system condition, and ACS host name to direct requests to different LDAP directories.

Figure 16 System Condition and ACS Host Name



System Administration

The key changes in ACS 5.8.1 are that ACS 5.8.1 provides the following configuration areas for system administration tasks:

- Administrators, page 14
- Users, page 14
- Operations, page 14
- Configuration, page 14
- Downloads, page 15

Administrators

The key changes in ACS 5.8.1 are that ACS administrators can be assigned up to ten predefined roles that govern an administrator's permissions.

Users

The key changes in ACS 5.8.1 are:

- Enhanced password policy can be applied to ACS internal users. This includes:
  - Increased password complexity rules
  - Password history
- Password lifetime policy is based on age only.

Operations

The key changes in ACS 5.8.1 are:

- Ability to assign ACS server roles to the primary or secondary servers.
- Ability to perform local and global software updates.

Configuration

The key changes in ACS 5.8.1 are:

- This configuration area addresses authentication protocol settings, AAA dictionaries, internal user schema changes, ACS certificate management, logging settings, and ACS license management. This includes:
  - Editable AAA protocol dictionaries
  - Editable internal user/host schema
- Ability to assign an ACS server as a log collector for ACS View.

Downloads

The key changes in ACS 5.8.1 are:

- ACS 5.8.1 provides a migration tool to help migrate some parts of ACS 4.2 configuration.
- A web services interface to build a password-change application for ACS internal users.

The configuration area contains links to download the ACS 5.8.1 Migration Utility and web services files to build a change-password application.

ACS 5.8.1 Configuration

Configuration Migration Methods in ACS 5.8.1

This chapter describes ACS 4.x to 5.8.1 migration and contains:

Migration Methods

The ACS 5.8.1 configuration model differs from ACS 3.x and 4.x. You cannot directly migrate data and configurations from ACS 3.x and 4.x to ACS 5.8.1. ACS 5.8.1 migration requires some manual reconfiguration. ACS 5.8.1 provides the following tools for the migration process:

Migration Utility

The Migration Utility is a tool that runs on an ACS 4.x Windows machine. This tool helps you to import the ACS 4.x backup files, analyze the data, and make the required modifications before importing the data to ACS 5.8.1.

The Migration Utility supports the migration of the configurations that are shown in Table 1 on page 2. You can download the Migration Utility from the ACS 5.8.1 web interface under **System Configuration > Downloads**.

The Migration Utility *migrates* data from an ACS 4.x Windows machine to an ACS 5.8.1 machine. This process is different from the *upgrade* process for versions of ACS from 3.x to 4.x or for any 4.x upgrades.

In the upgrade process, the ACS 4.x system works in the same way, without the need for administrative support. The migration process entails, in some cases, administrative support to consolidate and manually resolve data before you import the data to ACS 5.8.1.

The Migration Utility in ACS 5.8.1 supports multiple-instance migration that migrates all ACS 4.x servers in your deployment to ACS 5.8.1. To differentiate between several ACS 4.x instances, you can add a prefix. The prefix is used to retain server-specific identification of data elements and prevent duplication of object names for different servers.

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

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

CSV Import Tool

ACS 5.8.1 allows you to import some of the data objects from comma-separated value (CSV) text files, as listed in Table 1 on page 2. If you do not want to manually configure all the data objects in ACS 5.8.1 through the web interface, you can create the configuration in CSV text files and import the configuration.

In many instances, ACS configuration data, such as device and user information is maintained externally to ACS. You can export this data in a text format for importing into ACS 5.8.1.

For more information on the CSV Import Tools, see the Using the Scripting Interface chapter of the *Software Developer's Guide for Cisco Secure Access Control System 5.8.1*.

Table 1 ACS 5.8.1 Migration Utility And Import Tool Options

ACS 5.8.1 Configuration Areas	ACS 5.8.1 Migration Utility Support	ACS 5.8.1 Import Tools
NDGs	Yes	Yes
Network Devices	Yes	Yes
RADIUS Proxy Servers	No	No
Internal Users/Hosts	Yes	Yes
Identity Groups	Yes	Yes
External Identity Stores	No	No
Policy Elements	Shared command sets, RACs, shared DACLs	Shared command sets, shared DACLs
Access Policies	No	No
Monitoring and Reports	No	No
System Administration	FAST master keys, VSAs	No

Migration Recommendations

- For small ACS configurations, use a combination of manual configuration and CSV import. This is in cases such as:
  - Where users are not maintained in ACS
  - Where network device wildcard is used
  - Where user and network device information is available in CSV text format
- For other configurations, use the ACS 5.8.1 Migration Utility in addition to manual configuration and CSV import.

About the Migration Utility

Use the Migration Utility to migrate the different types of data from ACS 4.x to ACS 5.8.1. In addition to your ACS 4.x Windows source machine, you must deploy an ACS 4.x migration machine and an ACS 5.8.1 target machine.

The two phases of the migration process are:

- Analysis and Export
- Import

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

Data that passes the analysis phases can be exported and then imported to ACS 5.8.1. See the *User Guide for Cisco Secure Access Control System 5.8.1* for details on ACS 5.8.1 policies.

You cannot use the remote desktop to connect to the migration machine to run the Migration Utility. You must run the Migration Utility on the migration machine or, use VNC to connect to the migration machine. You must run the Migration Utility on a 32-bit version of Windows.

Note: ACS 5.8.1 Migration Utility is not supported on a 64-bit version of Windows.

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

Migrating from ACS 4.x to 5.8.1

This section describes the approach that is used in migrating from ACS 4.x to ACS 5.8.1. This section includes:

Multiple-Instance Migration

ACS 5.8.1 has one primary database that holds the data for all the ACS 4.x instances. Data from each ACS 4.x instance is migrated to this primary database. In ACS 4.x, selective data replication can be defined such that different ACS instances maintain distinct subsets of the overall system configuration.

ACS 5.8.1 contains a consolidated database, which is replicated to all the ACS instances. The consolidated database contains all the local configuration definitions from each of the ACS 4.x instances.

Migration Phases for ACS 5.8.1

ACS 5.8.1 follows a two-phase migration approach:

Analysis Phase

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

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

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

Migration Phase

In this phase, the Migration Utility extracts the configuration data from an ACS 4.x server and prepares the data to be migrated in a format that can be imported into an ACS 5.8.1 server. The migration tool provides options to migrate data in one or more categories, such as:

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

Data Model Organization

ACS 5.8.1 is a policy-based access control system. The term *policy model* in ACS 5.8.1 refers to the presentation of policy elements, objects, and rules to the policy administrator. ACS 5.8.1 uses a rule-based policy model instead of the group-based model that was used in previous versions.

The rule-based policy model provides more powerful and flexible access control than is possible with the older group-based approach. For more information on the policy model, see the *User Guide for Cisco Secure Access Control System 5.8.1*.

The following are the three major data model-related points in ACS 5.8.1:

- Model Organization, page 4
- Model Storage, page 4
- Replication Model, page 4

Model Organization

ACS 5.8.1 extends the Network Access Profile (NAP)-related functionality to a full policy-based authentication, authorization, and accounting (AAA) solution for both RADIUS and TACACS+.

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

Model Storage

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

- It can be translated to the ACS 5.8.1 model.
- It consists of data that is not generated during run-time operation; for example, dynamic-user.

Replication Model

In ACS 5.8.1, multiple database instances of ACS 4.x are combined and migrated into a single database. In ACS 4.x, selective data replication can be defined such that different ACS instances maintain distinct subsets of the overall system configuration.

ACS 5.8.1 contains a consolidated database that is replicated to all the ACS instances. This consolidated database contains all the local configuration definitions from each of the ACS 4.x instances.

The ACS 5.8.1 data model is much more uniform than the ACS 4.x data model. The ACS 5.8.1 data model contains a single master instance, where all configuration changes are made. All subtending secondary instances maintain a full copy of the configuration and receive updates for all configuration changes.

Multiple-Instance Migration Support

To migrate multiple instances of ACS 4.x to ACS 5.8.1:

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

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

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

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

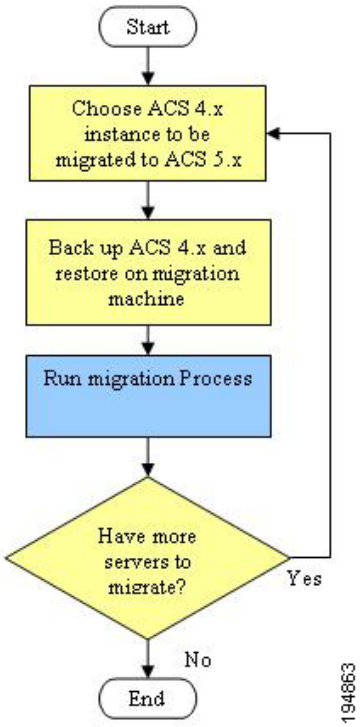
   If you restore any instance of ACS 4.x, it deletes the previous ACS 4.x instance data.

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

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

Figure 1 on page 5 illustrates the multiple-instance migration process.

Figure 1 Multiple-Instance Migration Process



Migrating Data

The migration process exports data from a source ACS 4.x server and imports the corresponding data entities to a target ACS 5.8.1 server. The export process does not run on the operational 4.x server. Instead, you must back up the database from the ACS 4.x source server and restore the data to an additional ACS 4.x migration machine, where you run the Migration Utility.

Note: You must perform a full database backup on the ACS 4.x source machine before you start the migration process. Restore the backed-up data to an additional ACS 4.x migration machine and fix issues before you import the data to the ACS 5.8.1 machine.

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

To migrate data:

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

   See Analysis and Export of ACS 4.x Data, page 34. In this phase, you:

- Identify issues for data that cannot be migrated and review manual migration considerations. See Resolving Migration Issues, page 2.
- Identify issues to fix prior to migration.
- Identify the data to consolidate. See Consolidating Data, page 35 for more information.

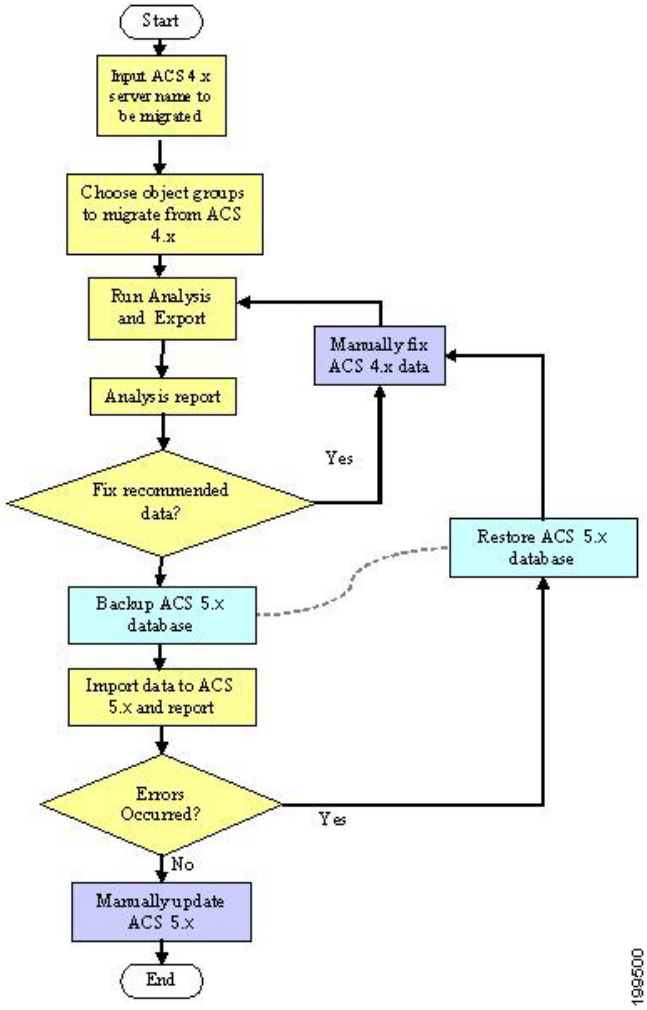
  Only data that passes the Analyze and Export phase can be exported and later imported to ACS 5.8.1.

2. Back up the ACS 5.8.1 target machine database.
3. Import the ACS 4.x data to ACS 5.8.1 and review the Import Summary Report.

   See Importing the ACS 4.x Data to ACS 5.8.1, page 36.

Figure 2 on page 7 illustrates the migration process.

Figure 2 Migration Process



Object Group Selection

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

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

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

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

Analysis and Export

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

In this phase, you identify:

- Issues for data that cannot be migrated. You are also provided opportunities to rectify this data prior to the migration.
- Issues to fix before migration.
- The data to consolidate. See Consolidating Data, page 35 for more information.

  Note: Only data that passes the analysis phase can be exported and later imported to ACS 5.8.1.

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

The export process reports the following issues:

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

Import

The data export file from ACS 4.x is imported into ACS 5.8.1.

You can run the Import on a full database. We recommend that you manually back up the ACS 5.8.1 database. The backup version of the database can be used to restore the system, if any unexpected errors occur during the data import process.

Multiple-Instance Support

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

The multiple-instance support in ACS 5.8.1 has the following key features:

- Duplicate Object Reporting, page 8
- Object Name Prefix Per Instance, page 9
- Shared Object Handling, page 9

Duplicate Object Reporting

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

Object Name Prefix Per Instance

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

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

Shared Object Handling

Shared objects between the ACS 4.x instances—such as NDGs, user attribute definitions, and user groups—are migrated only once. However, because of the association support for multiple instances, object associations are created according to the status of ACS 5.8.1 data. For more information, see Migration of ACS 4.x Objects, page 9.

For example, if user *A* is associated to group *BB* and neither the user nor the group were migrated, both objects are created and then associated in ACS 5.8.1.

ACS 5.8.1 Migration Utility Support

This chapter describes:

ACS 4.x to 5.8.1 Migration Version Support

You can migrate the following ACS 4.x versions:

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

ACS 4.0 Migration Support

You must upgrade from ACS for Windows Server 4.0 to ACS for Windows Server 4.1.1.24 to migrate your data to ACS 5.8.1. seethe *Installation Guide for Cisco Secure ACS for Windows 4.1* for more information.

ACS 4.x Appliance Support

You can migrate data from ACS 4.x only on Windows software. If you have an ACS 4.x appliance, you must back up the ACS 4.x configuration and restore and upgrade it to ACS for Windows Server 4.1.1.24.

- If the appliance version is ACS 4.1.1.24, you must install the corresponding ACS 4.x version on the Windows server and then restore the data from the appliance.

- If you are using ACS version 4.1.1.24 or above, you do not have to upgrade. seethe *Installation Guide for Cisco Secure ACS for Windows 4.1* for more information.

CSACS-1120 Series Appliance Support

The CSACS-1120 appliance can be used to install either ACS 4.2 or ACS 5.0. You cannot run ACS 5.8.1 on CSACS-1120. If you currently have ACS 4.2 installed on a CSACS-1120 appliance, and you want to migrate to ACS 5.8.1, you must first back up the ACS 4.2 data before proceeding to the ACS 5.8.1 installation.

To migrate data from ACS 4.2 on CSACS-1120 to ACS 5.8.1 on a 3400 or 3500 series appliance:

1. Back up ACS 4.2 data from CSACS-1120 appliance.
2. Restore the ACS 4.2 data on an intermediate migration machine.
3. Install ACS 5.8.1 on a 3400 or 3500 series appliance.
4. Migrate ACS 4.2 objects from the intermediate migration machine to ACS 5.8.1 that is installed on the 3400 or 3500 series appliance.

Upgrading ACS 5.8 or a lower version on CSACS 1120 or 3400 series appliance to ACS 5.8.1 on 3500 series appliance

To upgrade data from ACS 5.8 or a lower version on CSACS 1120 or 3400 series appliance to ACS 5.8.1 on 3500 series appliance:

1. Back up ACS 5.8 or a lower version data from CSACS-1120 or a 3400 series appliance.
2. Install ACS 5.8.1 on the 3500 series appliance.
3. Restore the backup taken from ACS 5.8 or a lower version on CSACS 1120 or 3400 series appliance in ACS 5.8.1 on a 3500 series appliance.

Remote Desktop Support

The Migration Utility does not support Remote Desktop Connection. You must run the Migration Utility on the migration machine or use VNC to connect to the migration machine.

Multiple-Instance Support

In ACS 5.8.1, multiple distinct database instances (4.x) are combined into a single consolidated database. In ACS 4.x, selective data replication can be defined so that different ACS instances maintain distinct subsets of the overall system configuration, while in ACS 5.8.1, a single consolidated database is replicated to all ACS instances in the deployment.

As a result, the primary database contains all the local configuration definitions from each of the ACS 4.x instances.

ACS 4.x Elements Supported in the Migration Process

Table 1 on page 3 shows the ACS 4.x elements that the Migration Utility supports and the corresponding ACS 5.8.1 element.

Table 1 ACS Elements that Migration Process Supports

ACS 4.x Element	ACS 5.8.1 Element
AAA Client/Network Device	Network Device. See AAA Client/Network Device, page 10 for more information.
Internal User	Internal User. See Internal User, page 16 for more information.
User Defined Fields (within Interface Configuration section)	Identity Attributes/Internal User. See User Group, page 23 for more information.
User Group	Identity Group. See User Group, page 23 for more information.
Shared Shell Command Authorization Sets	Command Set. See Shared Shell Command Authorization Sets, page 27 for more information.
User T+ Shell Exec Attributes	Identity Attributes/Internal User. See User Group, page 23 for more information.
Group T+ Shell Exec Attributes	Shell Profile. See User Group Policy Components, page 24 for more information.
User T+ Command Authorization Sets	Command Set. See User Group, page 23 for more information.
MAC Authentication Bypass (MAB) Addressed	Internal Host Database. See MAC Addresses and Internal Hosts, page 26 for more information.
Shared Downloadable Access Control List (DACL)	Downloadable ACL. See Shared DACL Objects, page 28 for more information.
EAP-FAST Master keys	EAP-FAST Master keys. See EAP-Fast Master Keys and the Authority ID, page 33 for more information.
Shared RADIUS Authorization Components	Authorization Profiles. See Shared RACs, page 5 for more information.
Customer Vendor-Specific Attributes	Customer VSAs. See Customer VSAs, page 5 for more information.
Max User Sessions	Maximum User Sessions. See Max User Sessions, page 5 for more information.

Note: You migrate command sets from shared objects or from within the user or group definitions. Shell profiles are created from the shell exec parameters within group definitions. However, shell exec parameters stored in user records are migrated as identity attributes associated with the individual user.

ACS 4.x Elements Not Supported in the Migration Process

The Migration Utility does not support:

- Group DACLs
- Group RADIUS Attributes
- Active Directory (AD) Configuration
- AD Group Mapping
- Admin Accounts
- Admin Users
- Authority Certificates
- Certificate Trust List (CTL)

- Certificate Revocation List (CRL)
- Date and Time
- External Database Configuration
- Generic Lightweight Directory Access Protocol (LDAP) Configuration
- Group Shell Custom Attributes
- Group Private Internet Exchange, Adaptive Security Appliance (ASA), and Shell Command Authorization Sets
- Group Network Access Restrictions (NARs)
- Internal ID Password Enforcement—Sarbanes-Oxley (SOX)
- LDAP Group Mapping
- Logging Configuration
- Machine Access Restrictions (MARs)
- Network Access Profiles (NAPs)
- Protocol Settings (system and global authentication)
- Proxy RADIUS and T+ (migrates only external access control server credentials)
- TACACS+ Dictionary
- RADIUS One-Time Password (OTP)
- RSA OTP
- Shared NARs
- Server Certificate
- Shared Network Access Filtering (NAF)
- Shared PIX and ASA Command Authorization Sets
- Time-of-Day Access Settings
- User PIX/ASA Shell Command Authorization
- User DACLs
- User NARs
- User RADIUS Attributes
- IP Pools
- Dial-In Support

See the *User Guide for Cisco Secure Access Control Server 4.2* for descriptions of the attributes that do not migrate.

User Interface

This section describes the end user interface for the ACS 5.8.1 Migration Utility.

CLI-Based Migration Utility

ACS 5.8.1 supports a CLI-based Migration Utility. For more information on the migration settings, see Running the Migration Utility, page 1.

Phases of the CLI-Based Migration Utility

The CLI-based Migration Utility consists of the following parts:

- Settings, page 5
- Object Group Selection, page 5
- Operation Selection, page 6

Settings

The Migration Utility uses operator-configured settings that can be saved persistently. Every invocation of the Migration Utility prompts you to use the previously defined values or select new ones. For more information on the migration settings, see Running the Migration Utility, page 1.

The settings are of two types:

- ACS 5.8.1 Identification and Credentials—IP address or hostname of the ACS 5.8.1 server to which the data is being migrated. The administrator username and password that are used to import data in the ACS 5.8.1 server are also specified.

  We recommend that you define a unique administrator for the migration operations to make it easy to identify them while browsing the configuration records. While running the Migration Utility, only the default superadmin account *acsadmin* or the recovery superadmin should be used for ACS 5.8.1, while running the Migration Utility.

- Configuration Options—Associated with the migration of certain object types. After you configure the settings, you are prompted to acknowledge whether to save them as the defaults for use during subsequent invocations of the utility.

Object Group Selection

You can migrate either a group of the object types that are supported by the Migration Utility or all supported object types. For more information on the details of the various phases in the migration procedure and the impact and considerations for each object type, see Migration of ACS 4.x Objects, page 9.

For a detailed procedure on selecting the available options, seeRunning the Migration Utility, page 1.

The following groups of objects are available for selection:

- All Objects—All ACS objects
- All User Objects—Identity groups and all objects that are extracted from users
- All Device Objects—Network devices and NDGs
- Shared command sets
- Shared DACLs
- Master Keys—EAP-FAST master keys
- Shared RACs and VSAs

Operation Selection

After you select a set of object types, you must select the migration phase to be performed. The following options are available:

- Analyze and Export
- Import

After you select an option, the corresponding process runs, and the relevant reports are displayed on the screen. For each operation, two type of reports are displayed:

- Summary
- Detailed

For more information on the reports that are generated during different phases of the migration, see Printing Reports and Report Types, page 39.

Migration Utility Setup and Installation

This chapter describes migration considerations for each machine in the migration process and contains:

Migration Preinstallation Considerations

Before you begin, ensure that you configure your environment for migration. In addition to your ACS 4.x Windows source machine, you must deploy an ACS 4.x migration machine and an ACS 5.8.1 target machine. Keep in mind the following considerations:

- Ensure that the ACS 4.x database does not have any database corruption issues.
- Ensure that you configure the ACS 4.x migration machine for a single IP address. Migration fails on a migration machine with multiple IP address aliases per interface.
- Perform a full database backup on the ACS 4.x Windows source machine. Use this machine to maintain your ACS 4.x data. Restore the backed-up data to an additional ACS 4.x migration machine, and fix issues before importing the data to the ACS 5.8.1 machine.

  For database backup instructions, see the *Installation Guide for Cisco Secure ACS for Windows 4.1*.
- The migration machine should have the same 4.x version as the source machine. You should back up the ACS 4.x version you wish to migrate on the 4.x Windows source machine and restore the same 4.x version on the migration machine. The restore fails if the migration machine does not have the same 4.x version as the source machine.

  See the *Installation Guide for Cisco Secure ACS for Windows 4.1*.
- Restore data from the ACS 4.x Windows source machine to the migration machine. The migration machine is a Windows platform running ACS 4.x. Use this machine solely for the purpose of migration. The migration machine cannot be an appliance machine.

Note: Use the migration machine when you make any changes to the ACS 4.x data.

- Perform a full database backup on the ACS 5.8.1 target machine. Use this machine to process the imported data. For database backup instructions, see the *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.8.1*.
- Ensure that you:

  - Install ACS 5.8.1 on the target machine.
  - Use a compatible ACS 5.8.1 license.
  - Establish network connection between the migration machine and ACS 5.8.1 server.

- Back up your ACS 5.8.1 database before you run the Import phase.
- Enable the migration interface on the ACS 5.8.1 server. For more information on how to enable the migration interface and run the Migration Utility, see Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.8.1, page 1.

System Requirements

Your ACS machines must meet the system requirements described in Table 1 on page 2. All documents are available on Cisco.com.

Table 1 System Requirements for Migration Machines

Platform	Requirements
ACS 4.x source machine	See the *Installation Guide for Cisco Secure ACS for Windows 4.1*.
ACS 4.x migration machine	See the *Installation Guide for Cisco Secure ACS for Windows 4.1*. The machine must have 2 GB of RAM. Ensure that you configure the ACS 4.x migration machine for a single IP address. Migration fails on a migration machine with multiple IP address aliases per interface.
ACS 5.8.1 target machine	See the following: ■ *Installation and Setup Guide for ACS 5.8.1* ■ *Cisco Application Deployment Engine (ADE) 1010 and 2120 Series Appliance Hardware Installation Guide.* ■ *Cisco Application Deployment Engine (ADE) 2130 and 2140 Series Appliance Hardware Installation Guide.*

ACS Software Accessory Kit DVDs

Table 2 on page 3 describes the ACS software accessory kit DVDs.

Table 2 ACS Software Accessory Kit DVD

DVDs	Description
Cisco Secure Access Control System-Installation and Recovery DVD, Version 5.8.1	Use this DVD to: ■ Install the ACS 5.8.1_ISO image. ■ Install the Application Upgrade Bundle. ■ Install VMware. ■ Recover the ACS 5.8.1 appliance. ■ Reset the password.
Cisco Secure Access Control System-Upgrade and Migration_Documentation DVD, Version 5.8.1	Use this DVD to: ■ ACS 5.5 Upgrade Package (upgrade from 5.3 or 5.4 to 5.5). ■ ACS 5.6 Upgrade Package (upgrade from 5.4 or 5.5 to 5.6) ■ ACS 5.7 Upgrade Package (upgrade from 5.5 or 5.6 to 5.7) ■ ACS 5.8 Upgrade Package (upgrade from 5.5, 5.6 or 5.7 to 5.8) ■ ACS 5.8.1 Upgrade Package (upgrade from 5.5, 5.6, 5.7, or 5.8 to 5.8.1) ■ Install the Migration Utility, if you are running one of the following ACS versions: – 4.1.1.24 – 4.1.4.13 – 4.2.0.124 ■ Upgrade the server to ACS 4.2.0.124 before migration. ■ Documentation: – ACS_5.8.1_5x5_Pointer_Card_ChinaRoHS.pdf – ACS_5.8.1_CLI_Reference_Guide.pdf – ACS_5.8.1_Installation_and_Upgrade_Guide.pdf – ACS_5.8.1_Migration_Guide.pdf – ACS_5.8.1_Regulatory_Compliance_and_Safety_Information.pdf – ACS_5.8.1_Release_Notes.pdf – ACS_5.8.1_SDT_Guide.pdf – ACS_5.8.1_Software_Developer's_Guide.pdf – ACS_5.8.1_User_Guide.pdf

Migration from ACS 4.x to ACS 5.x is supported only from the software version of ACS 4.x.

To migrate from the ACS 4.x appliance version, complete the following steps:

1. Make a backup from any supported version of the ACS 4.x appliance.
2. Restore the appliance backup on the same supported version of the ACS 4.x software.
3. Now run the Migration Utility.

Security Considerations

The export phase of the migration process creates a data file that is used as the input for the import process. The content of the data file is encrypted and cannot be read directly.

You need an ACS administrator username and password to import data into ACS 5.8.1. You should use a reserved username, so that records created by the import utility can be identified in the audit log.

Accessing the Migration Utility

To access the Migration Utility, download it from the ACS 5.8.1 web interface.

To download migration application files:

1. Choose **System Administration > Downloads > Migration Utility**.

   The Migration from 4.x page appears.

2. Click **Migration application files** to download *migration.zip*, which contains the application files you use to run the Migration Utility.

You may also use the Cisco Secure Access Control System–Installation and Recovery DVD, Version 5.8.1, available in the migration software accessory kit, to download the *migration.zip* file.

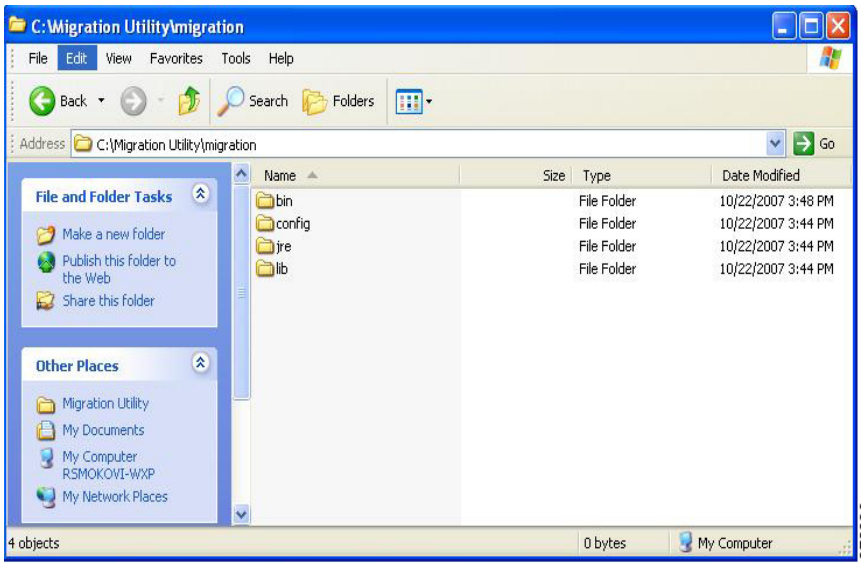
Related Topics

- ACS Software Accessory Kit DVDs, page 3
- Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.8.1, page 1

Migration Utility Packaging

The zip file *migration.zip* contains the Migration Utility files. Extract this file to a migration directory. This document uses the migration directory structure shown in Figure 1 on page 5.

Figure 1 Migration Utility Directory Structure



Related Topics

- ACS Software Accessory Kit DVDs, page 3
- Accessing the Migration Utility, page 4
- Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.8.1, page 1

Data Migration and Deployment Scenarios

The Migration Utility migrates ACS 4.x objects to ACS 5.8.1. The process of data migration in a single ACS appliance differs from that of ACS appliances in a distributed environment. This section contains:

- Guidelines for Data Migration in a Single ACS Server, page 5
- Guidelines for Data Migration in a Distributed Environment, page 5

Guidelines for Data Migration in a Single ACS Server

If you have a single ACS appliance in your environment (or several ACS appliances, but not in a distributed setup), run the Migration Utility against the ACS appliance as described in this guide.

For instructions to verify that migration is complete, see Validating Import, page 44.

Guidelines for Data Migration in a Distributed Environment

If you run ACS in a distributed environment (for example, if you have one primary ACS appliance and one or more secondary ACS appliances that interoperate with the primary ACS), you must:

1. Back up the primary ACS appliance and restore it on the migration machine.
2. Run the Migration Utility against the primary ACS appliance.

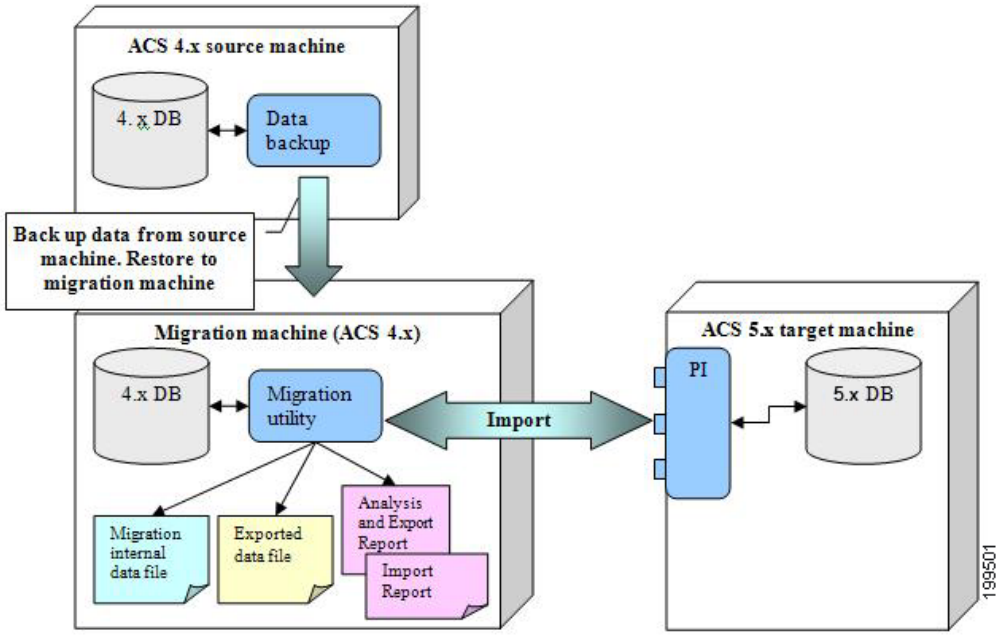
If you have large internal database, we recommend that you run the migration from an ACS 4.x to an ACS 5.8.1 standalone primary server, and not to a primary server that is connected to several secondary appliances. After the completion of the migration process, you can register all the secondaries.

The Migration Utility runs for approximately 15 hours to migrate 300,000 users, 50,000 devices, and 50,000 MAB. When you restart ACS 5.8.1, the startup process takes about 15 minutes before ACS 5.8.1 is available for use. The behavior of ACS 5.8.1 for data migration beyond 400,000 users and 200,000 devices is unknown.

Data Migration Between Platforms

Figure 2 on page 6 shows the data migration flow between platforms. See Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.8.1, page 1

Figure 2 Migration Flow Between Platforms



Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.8.1

This chapter describes how to migrate data from ACS 4.x to ACS 5.8.1 and contains:

Introduction

This chapter contains information to migrate data from ACS 4.x to ACS 5.8.1. 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 5.8.1 server.

From the command line interface, enter:

acs config-web-interface migration enable

To verify that the migration interface is enabled on the ACS 5.8.1 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 5.8.1* 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 5.8.1 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 5.8.1 target machine from the ACS 4.x migration machine. Access the web interface to verify that the ACS 5.8.1 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 5.8.1 target machine. You migrate the ACS 4.x data to the ACS 5.8.1 target machine.
`Enter ACS 5 administrator username:[`*`test`*`]`	Enter the username for the ACS 5.8.1 target machine. ACS 5.8.1 supports only admin users. ACS 5.8.1 supports migration operation with any ACS administrator with a recovery superadmin role.
`Enter ACS 5 password:`	Enter the password for the ACS 5.8.1 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 5.8.1 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 5.8.1.

`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 5.8.1 RADIUS dictionary. If you migrate a vendor that was already migrated and deleted in ACS 5.8.1, 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 5.8.1. See Migration of ACS 4.x Objects, page 9.
	Ensure that you back up your ACS 5.8.1 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 5.8.1. See Importing the ACS 4.x Data to ACS 5.8.1, 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

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 5.8.1.

This section contains:

Data Mapping

Table 5 on page 10 shows the data mapping between ACS 4.x and ACS 5.8.1, for the AAA client or Network Devices.

Table 5 Data Mapping for AAA Client or Network Devices

4.x Attribute Name	5.8.1 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 5.8.1 records contains separate fields for RADIUS and TACACS+ shared secrets. The specific field set in an ACS 5.8.1 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 5.8.1. 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	5.8.1 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 5.8.1.
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 5.8.1) definitions:

- In ACS 5.8.1, 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 5.8.1, 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 5.8.1, 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 5.8.1, 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 5.8.1 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 5.8.1 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 5.8.1.

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 5.8.1 format. *Table 6 on page 13 describes the ACS 4.x attributes that can be modified to conform to ACS 5.8.1 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 5.8.1 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 5.8.1 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 5.8.1.
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 5.8.1, configuration options are available to determine the name of the new device in ACS 5.8.1, 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 5.8.1:

- 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 5.8.1 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 5.8.1, a default description field called Migrated is created.

Multiple-Instance Support

In ACS 5.8.1, 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 5.8.1.

NDG

To facilitate migration of the ACS 4.x NDG definitions, an additional NDG hierarchy has been created in ACS 5.8.1.

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 5.8.1.

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 5.8.1, 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

Table 7 on page 14 shows the data mapping between ACS 4.x and ACS 5.8.1 for the NDGs.

Table 7 Data Mapping for NDGs

4.x Attribute Name	5.8.1 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	5.8.1 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 5.8.1, 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 5.8.1, 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 5.8.1 for internal users.

Table 8 Data Mapping for Internal Users

4.x Attribute Name	5.8.1 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 5.8.1 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 5.8.1.

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 5.8.1. 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 5.8.1 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 5.8.1. 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 5.8.1, 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

Table 9 on page 19 shows the user interface data mapping between ACS 4.x and ACS 5.8.1 for User Data Configuration and User Mapping.

Table 9 Data Mapping for User Data Configuration and User Mapping

4.x Attribute Name	5.8.1 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 5.8.1, 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 5.8.1, the attribute names are as follows:

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

Multiple-Instance Support

In ACS 5.8.1, 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 5.8.1 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 5.8.1 (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 5.8.1 (and was migrated in a previous run of the migration) is associated to the existing user attribute.

In ACS 5.8.1, 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 5.8.1, *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

Table 10 on page 21 shows the user interface data mapping between ACS 4.x and ACS 5.8.1 for the user shell command authorization.

Table 10 Data Mapping for User Shell Command Authorization

4.x Attribute Name	5.8.1 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 5.8.1, 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 5.8.1 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 5.8.1, 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 5.8.1 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

Table 11 on page 22 shows the data mapping between ACS 4.x and ACS 5.8.1 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	5.8.1 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 5.8.1 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 5.8.1. 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 5.8.1, this value is set in a user attribute associated with the user in ACS 5.8.1. If the attribute is not defined in ACS 4.x, it is left blank in ACS 5.8.1.

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 5.8.1 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 5.8.1 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 5.8.1, every user shell attribute that gets added to the dictionary also gets added to all the users.

User Group

In ACS 5.8.1, 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 5.8.1, 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 5.8.1, 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 5.8.1, 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

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	5.8.1 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 5.8.1 object:

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

In ACS 5.8.1, 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 5.8.1, 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 5.8.1 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 5.8.1, 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 5.8.1, 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 5.8.1 for MAC addresses and internal hosts.

Table 13 Data Mapping for MAC Addresses and Internal Hosts

4.x Attribute Name	5.8.1 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 5.8.1 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 5.8.1, 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 5.8.1 for shared shell command authorization sets.

Table 14 Data Mapping for Shared Shell Command Authorization sets

4.x Attribute Name	5.8.1 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 5.8.1, 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 5.8.1 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 5.8.1.

This section contains:

Data Mapping

Table 15 on page 29 shows the data mapping between ACS 4.x and ACS 5.8.1 for shared DACL objects.

Table 15 Data Mapping for Shared DACL Objects

4.x Attribute Name	5.8.1 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 5.8.1 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 5.8.1, 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 5.8.1.

In ACS 4.x, an attribute is identified in the GUI as a combination of the vendor name and the attribute name. In ACS 5.8.1, 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

Table 16 on page 30 shows the data mapping between ACS 4.x and ACS 5.8.1 for the shared RACs.

Table 16 Data Mapping for Shared RADIUS Authorization Components

4.x Attribute Name	5.8.1 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 5.8.1, 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 5.8.1, 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 5.8.1, 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 5.8.1 for each vendor. There are two possible cases during this identification process:

- If the vendor does not exist in the ACS 5.8.1 dictionary, all the vendor attributes are migrated.
- If the vendor exists in the ACS 5.8.1 dictionary, only attributes that are not defined in ACS 5.8.1 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 5.8.1 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 5.8.1.

Table 17 Aire-QoS-Level (2) values in ACS 4.1.x and ACS 5.8.1

Values in ACS 4.1.x	Values in ACS 5.8.1
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 5.8.1 is the same.

This section contains:

Data Mapping

Table 18 on page 32 shows the data field mapping between ACS 4.x and ACS 5.8.1 for RADIUS vendors.

Table 18 Data Mapping for RADIUS Vendors

4.x Attribute Name	5.8.1 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 5.8.1 for RADIUS VSAs.

Table 19 Data Mapping for RADIUS VSAs

4.x Attribute Name	5.8.1 Attribute Name	Comment
Name	Name	ACS 5.8.1 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 5.8.1. There are two cases for analysis:

- Generally, for ACS 4.x supported vendors, the dictionary in ACS 5.8.1 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 5.8.1 is not altered during migration. A warning is displayed for such attributes.
  - An attribute not defined in ACS 5.8.1, 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 5.8.1, are migrated without any analysis warning.

Note: Difference between ACS 4.x and ACS 5.8.1 VSA attributes (profile, name, type) are reported in the Analysis report.

Import

All the exported VSAs are imported to ACS 5.8.1.

EAP-Fast Master Keys and the Authority ID

In ACS 5.8.1, 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 5.8.1, and they are migrated to different IM objects. ACS 4.x stores the authority ID per node, whereas ACS 5.8.1 stores the authority ID only in the primary database and then applies it to the entire deployment.

This section contains:

Data Mapping

Table 20 on page 33 shows the data mapping between ACS 4.x and ACS 5.8.1 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	5.8.1 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	5.8.1 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 5.8.1, 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 5.8.1, 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 5.8.1, 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:

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 5.8.1 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 5.8.1. This object can then be referenced by ACS 5.8.1 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 5.8.1, you can define polices such that they incorporate the migrated command set information. See the *User Guide for Cisco Secure Access Control System 5.8.1* for more details on ACS 5.8.1 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 5.8.1. 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 5.8.1 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 5.8.1 machine.

Importing the ACS 4.x Data to ACS 5.8.1

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 5.8.1 import fails, restore your ACS 5.8.1 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 5.8.1. 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 5.8.1.

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 5.8.1 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:

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	

194859

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:	

194858

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	

194861

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

	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 5.8.1 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	

194864

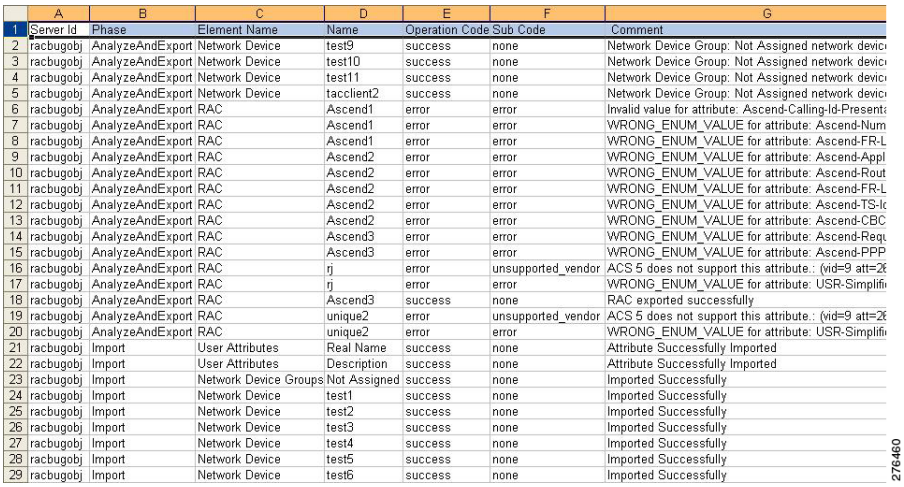
Table 27 Summary Report Column Definitions

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-Present
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-Id
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-Requ
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

276460

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 5.8.1 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 5.8.1:

- 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 5.8.1 objects, follow the instructions in the *User Guide for Cisco Secure Access Control System 5.8.1.*

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 5.8.1. 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

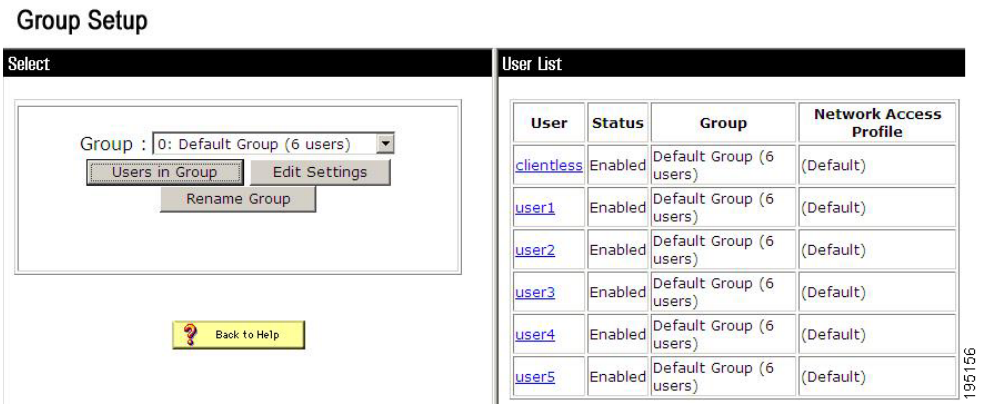
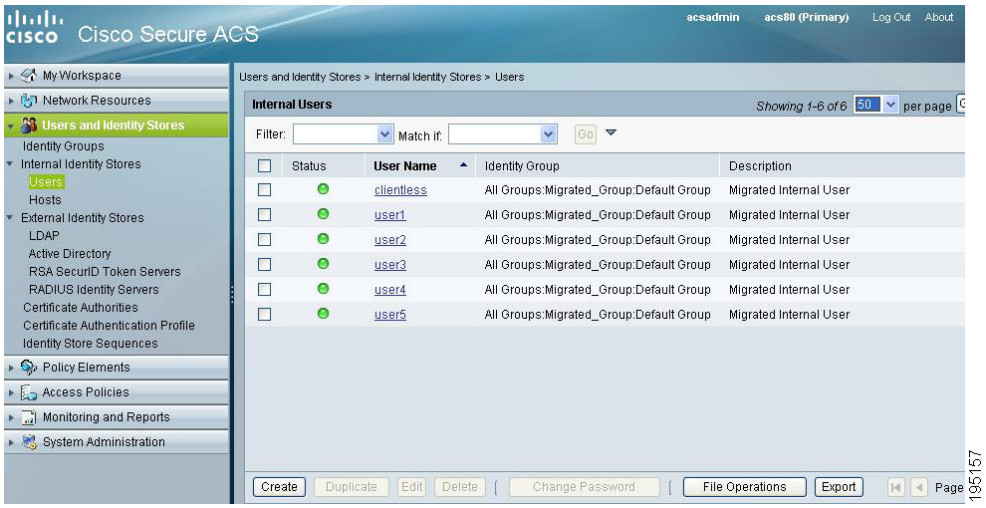


Figure 8 Users and User Groups Migrated to ACS 5.8.1



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 5.8.1 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 5.8.1.

Figure 9 Command Shell Attributes Defined in ACS 4.x

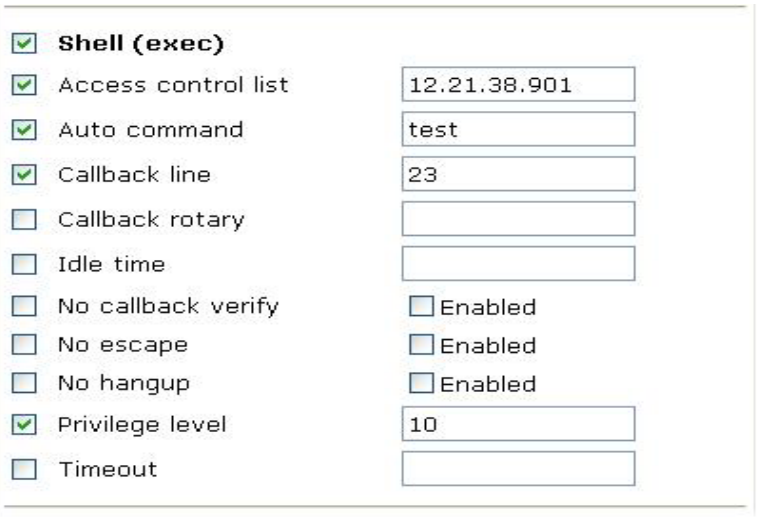


Figure 10 Group Shell Attributes Migrated to ACS 5.8.1

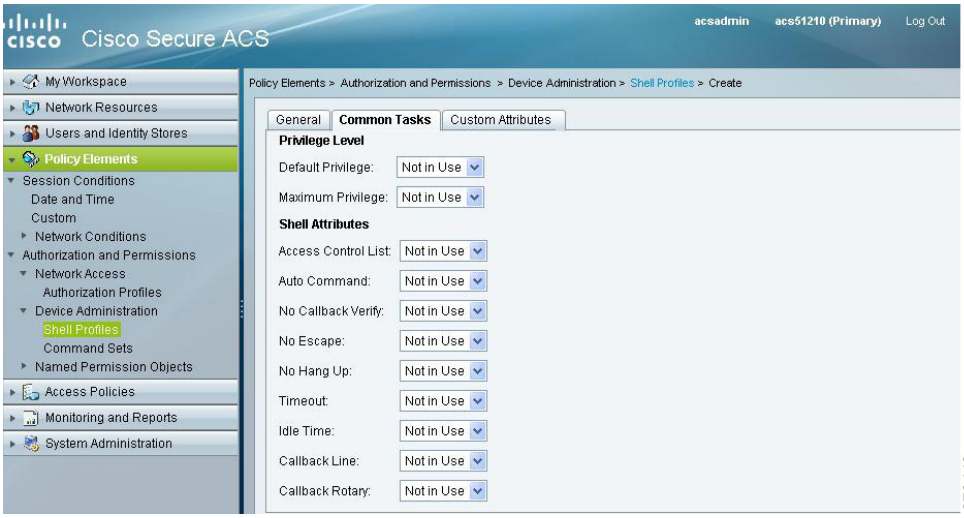
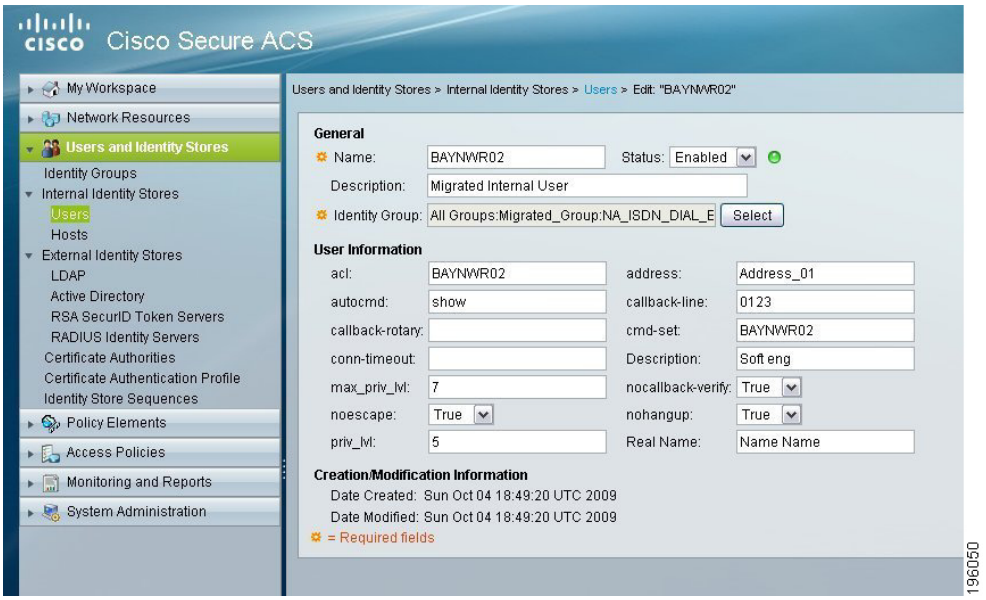


Figure 11 User Shell Attribute Migrated to ACS 5.8.1



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 5.8.1. Choose **Policy Elements > Device Administration > Command Sets** to access the migrated command set attributes.

Figure 12 Command Set Defined in ACS 4.x

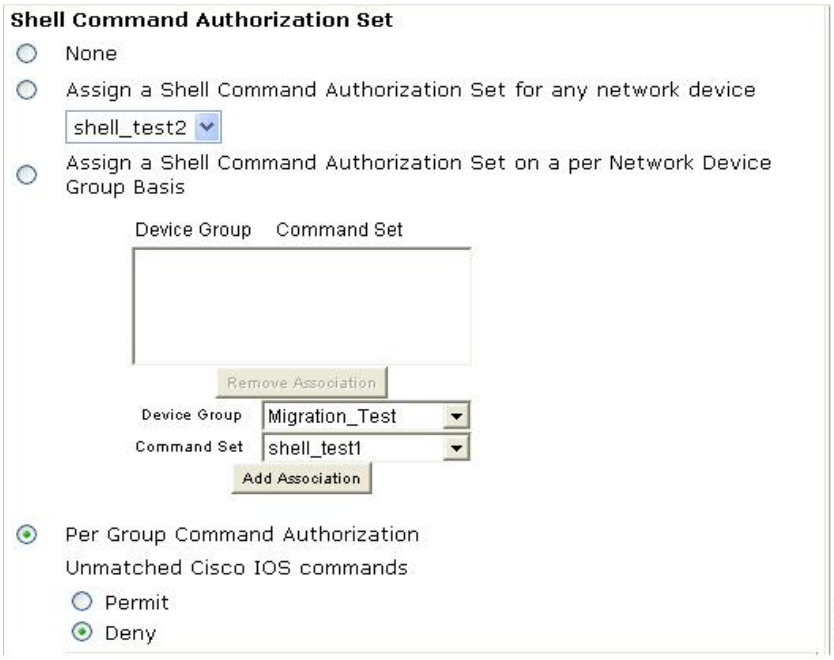
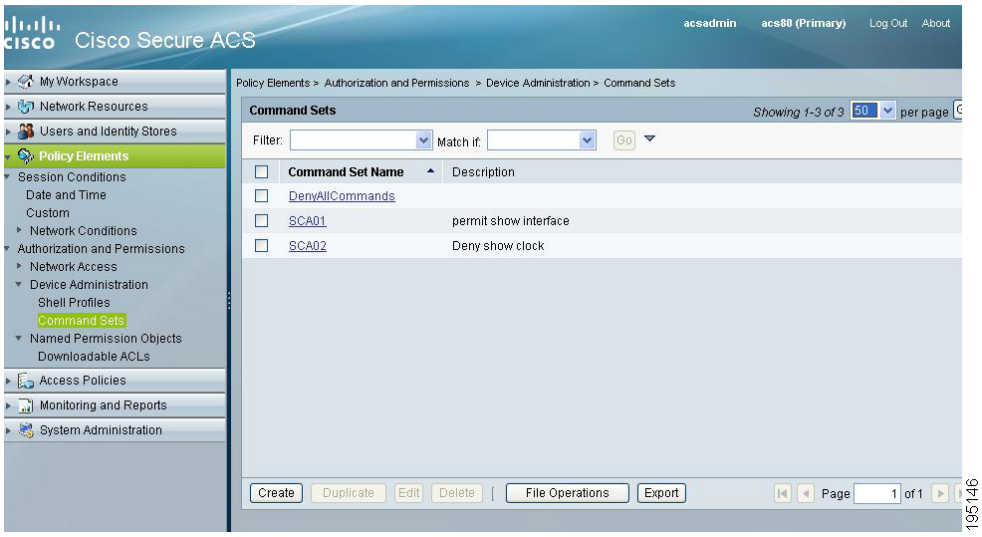


Figure 13 Command Set Migrated to ACS 5.8.1



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 5.8.1. Choose **Network Resources > Network Device Groups** to access the migrated NDGs.

Figure 14 NDGs Defined in ACS 4.x

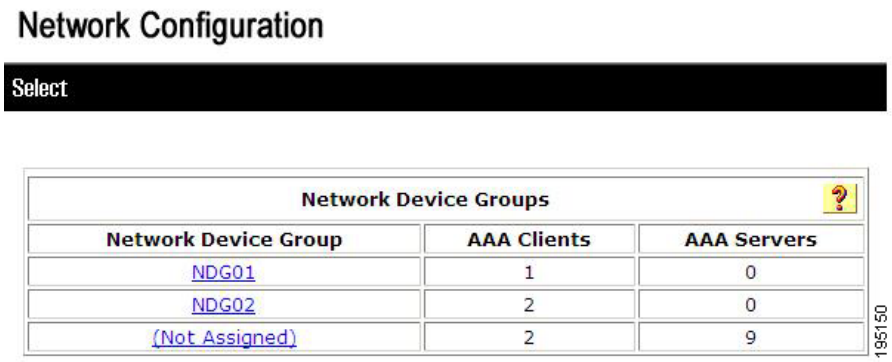
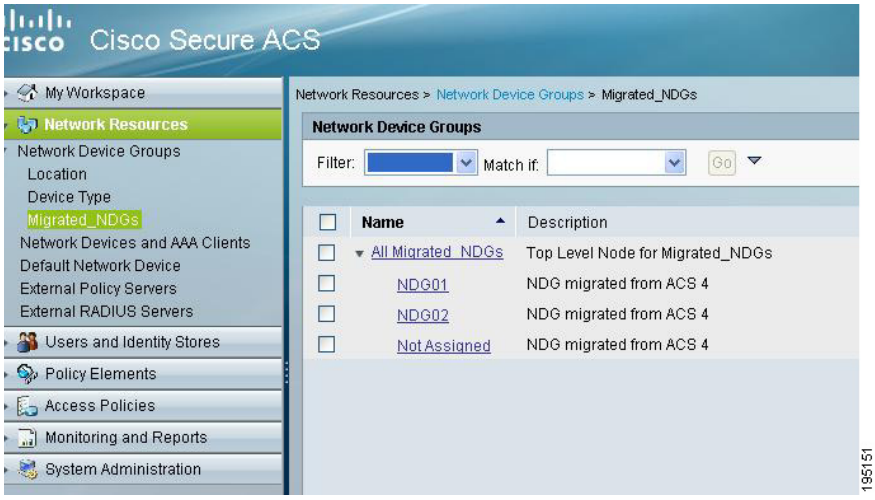


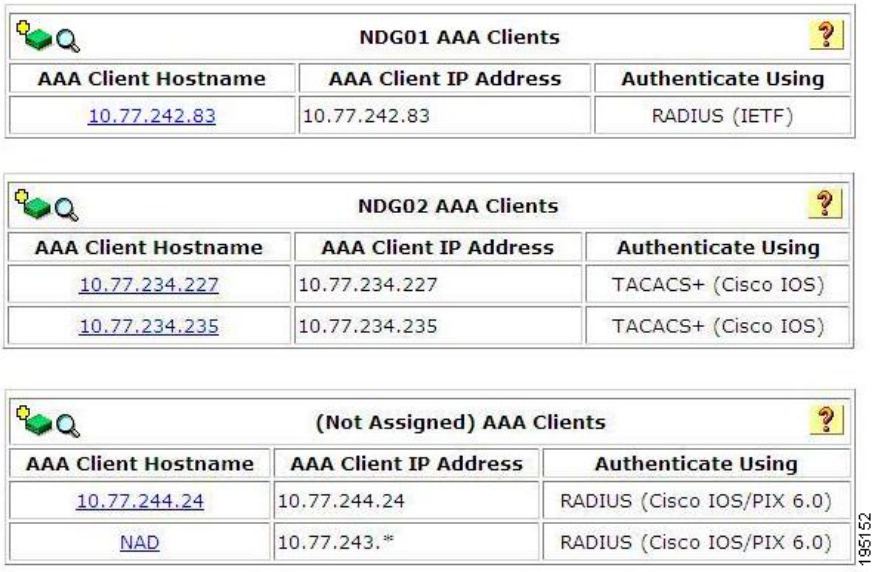
Figure 15 NDGs Migrated to ACS 5.8.1



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 5.8.1. 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

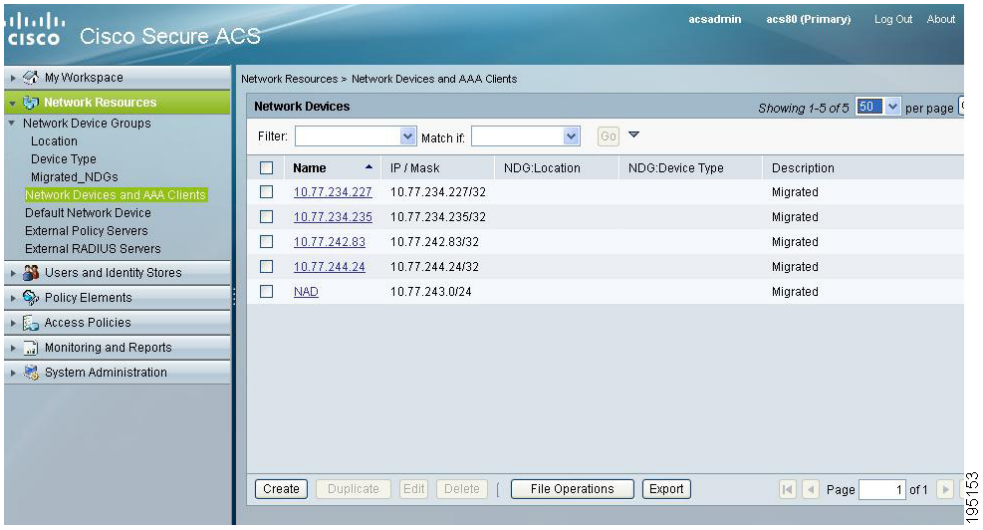
AAA Client Hostname	AAA Client IP Address	Authenticate Using
10.77.234.227	10.77.234.227	TACACS+ (Cisco IOS)
10.77.234.235	10.77.234.235	TACACS+ (Cisco IOS)

(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)

195152

Figure 17 Network Devices Migrated to ACS 5.8.1



195153

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 5.8.1.

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

Figure 18 DACLs Defined in ACS 4.x

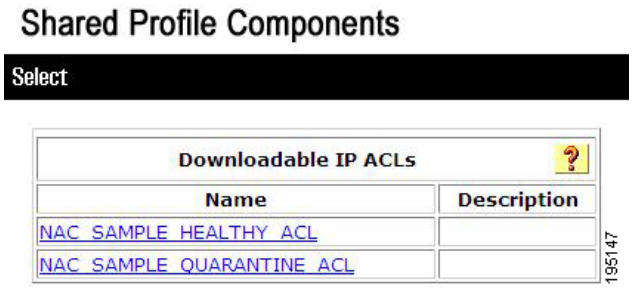
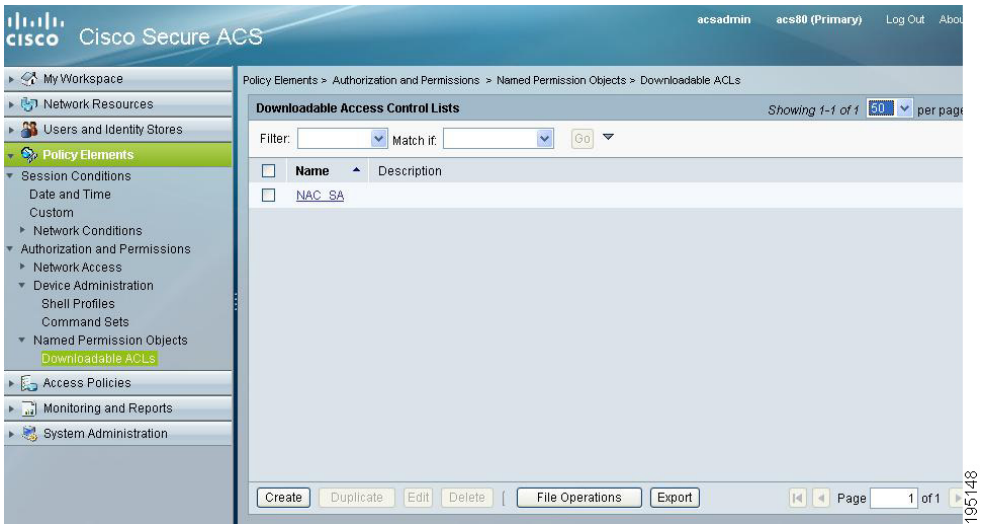


Figure 19 DACLs Migrated to ACS 5.8.1



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 5.8.1.

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

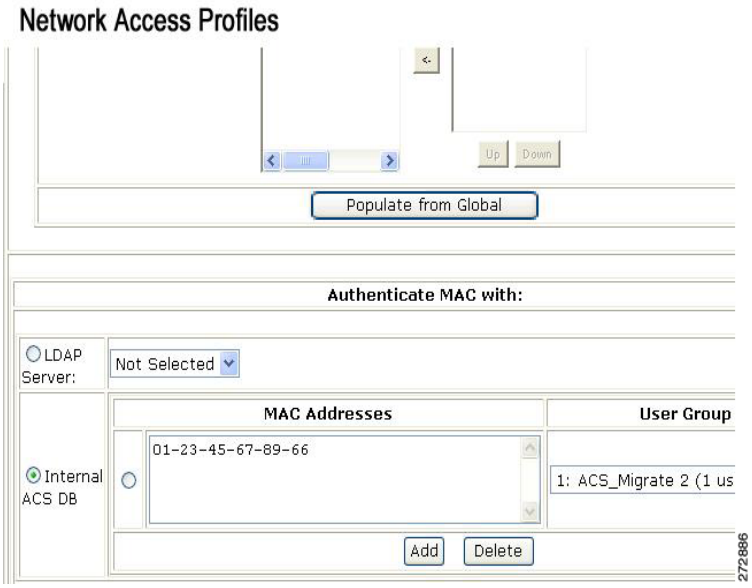
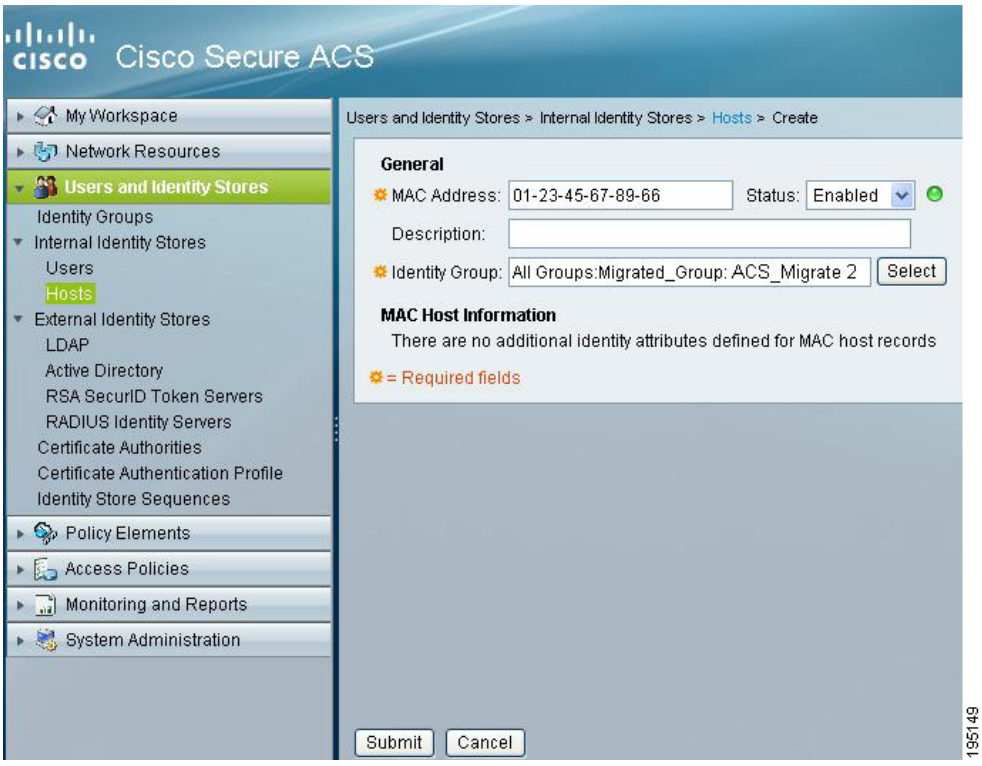


Figure 21 MAB Migrated to ACS 5.8.1



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 5.8.1.

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

Figure 22 Shared RACs Defined in ACS 4.x

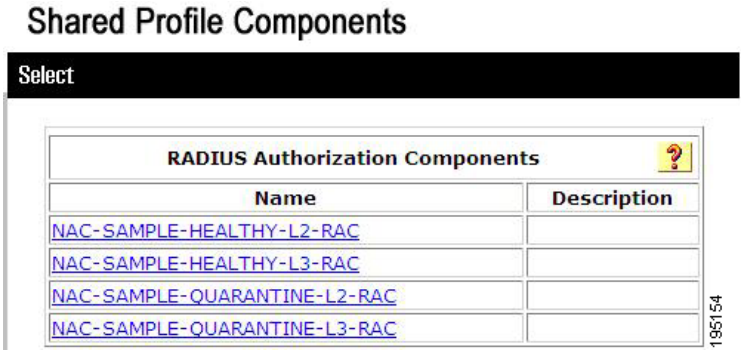
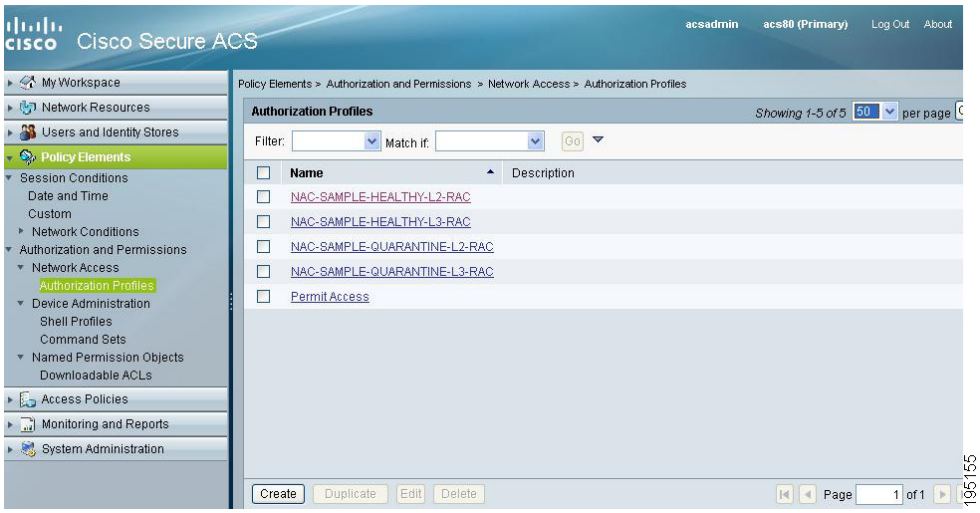


Figure 23 Shared RACs Migrated to ACS 5.8.1



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 5.8.1.

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

Figure 24 RADIUS VSAs in ACS 4.x

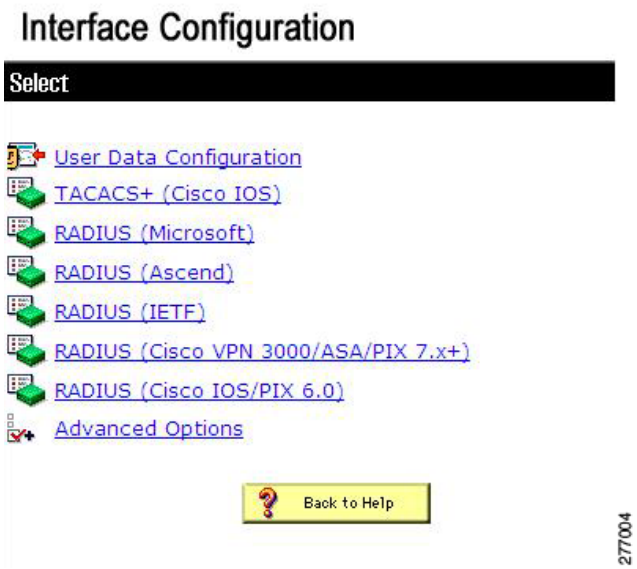
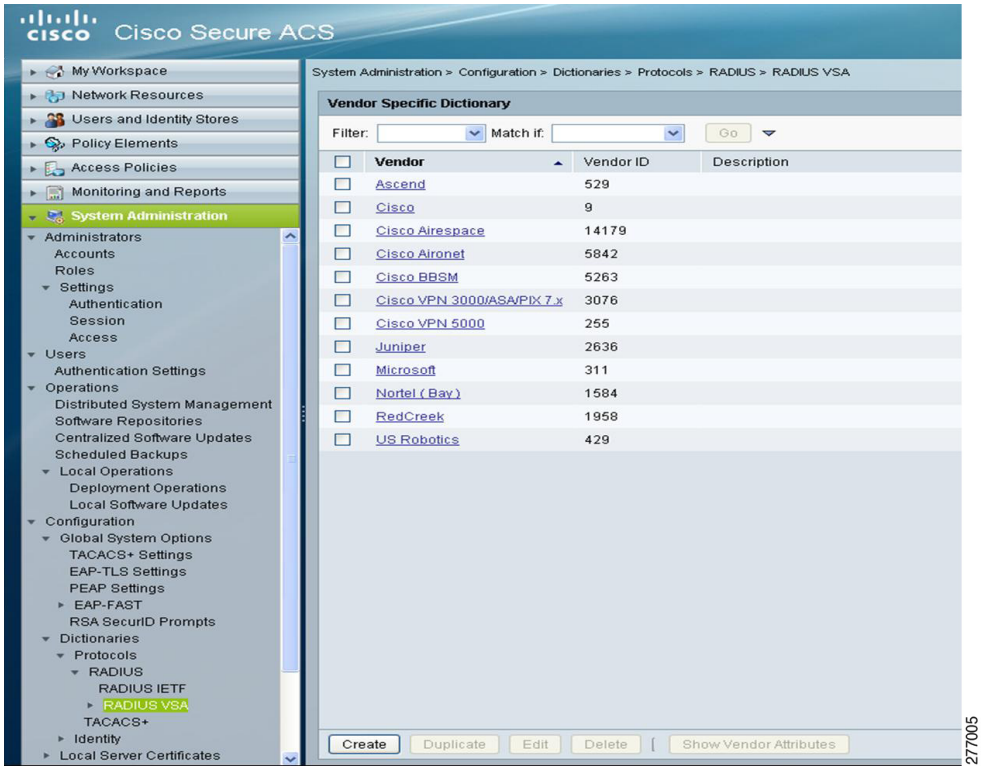


Figure 25 RADIUS VSAs Migrated to ACS 5.8.1



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 5.8.1.

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

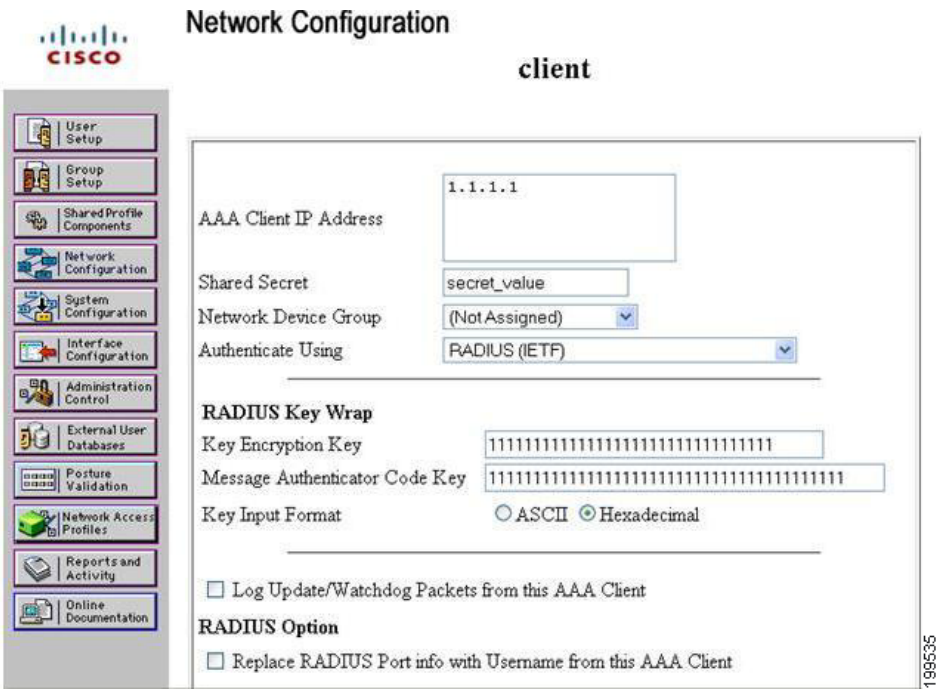
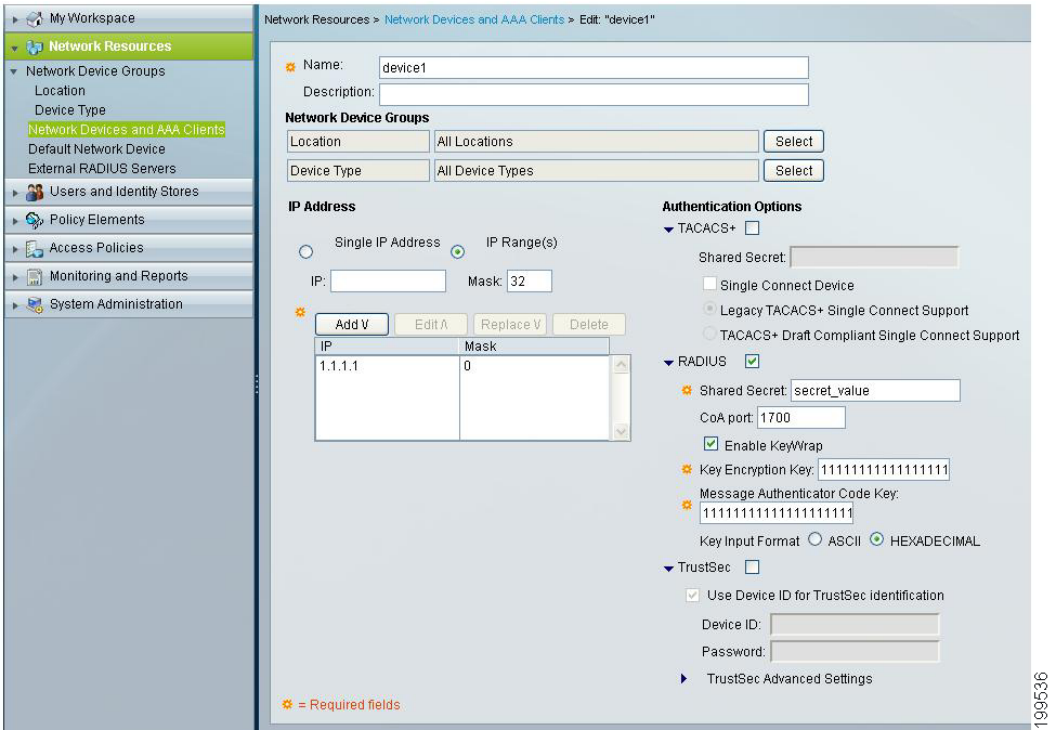


Figure 27 KEK and MACK Keys Migrated to ACS 5.8.1



ACS 5.8.1 Attribute Support in the Migration Utility

This chapter contains:

Introduction

This chapter describes ACS 4.x to ACS 5.8.1 attribute migration. To migrate ACS 4.x attributes, they must meet ACS 5.8.1 criteria. You can migrate some ACS 4.x elements to ACS 5.8.1, even though some of the attributes for an element might not migrate (or translate) to ACS 5.8.1.

For example, ACS 5.8.1 supports the user shell exec privilege level as a numeric value from 1 through 15. If the privilege level for the ACS 4.x User element is not a numeric value from 1 through 15, the User element is migrated, but the user shell exec privilege level attribute is not migrated.

ACS 4.x to 5.8.1 Migration

The following sections contain element information for:

AAA Client/Network Device

Table 1 on page 2 describes the differences between the ACS 4.x network device definitions and the ACS 5.8.1 network device definitions.

Table 1 ACS Network Device Definitions

ACS element	ACS 4.x	ACS 5.8.1 Status
RADIUS and TACACS+	Defines one network device for each protocol. For example, network device1 for RADIUS, network device 2 for TACACS+.	Defines one network device for RADIUS and TACACS+. See Overlapping IP Addresses, page 3.
IP Address	■ Use regular expressions to define the IP address. ■ You can define more than 40 IP addresses. ■ Includes wildcards and ranges.	■ Define IP addresses as a pair of IP addresses and mask definitions. ■ Limited to 40 IP addresses. ■ Definition is in the form of a subnet mask. See Untranslatable IP Addresses, page 3.

Note: ACS 5.8.1 does not support ACS 4.x authentication by using an attribute for network devices. ACS 5.8.1 supports only RADIUS and TACACS+. You cannot define a specific vendor.

NDG

ACS 5.8.1 does not support the ACS 4.x shared key password attribute for NDGs. The Analysis report flags shared key passwords on the NDG level. You can use only shared key passwords on the network device level.

For devices that belong to an NDG where the NDG includes a Key Encryption Key, the NDG's Key Encryption Key will be extracted and included in the network device definition instead of that defined with the network device definition Key Encryption Key.

For devices that belong to an NDG where the NDG includes a Message Authenticator Code Key, the NDG's Message Authenticator Code Key will be extracted and included in the network device definition instead of that defined with the network device definition Message Authenticator Code Key.

Note: If a shared key password resides on the NDG level, the shared key password is migrated to all the network devices that belong to this NDG. The network devices' shared key password is migrated only if the NDG shared key password is empty.

Internal User

ACS 5.8.1 supports the ACS 4.x Password Authentication Type. ACS 5.8.1 supports authentication on both internal and external databases. You migrate the user object with a default authentication password if the administrator uses Windows or LDAP. You can supply a different password when you run the Migration Utility. See Table 2Migration Script User Preferences, page 6.

User Policy Components

In ACS 4.x, the policy-related authorization data is embedded within the user definitions. In ACS 5.8.1, policy-related authorization data is included in shared components that are referenced from within the ACS 5.8.1 policy tables. Table 2 on page 3 shows the attributes for the ACS 4.x user policy components and describes the status in ACS 5.8.1.

Table 2 User Policy Component Attributes

ACS 4.x Attribute	ACS 5.8.1 Status
TACACS+ Shell (exec) Privilege level: The privilege level is a string field without validity checks.	■ In ACS 5.8.1, the default privilege level cannot be larger than the maximum privilege level. ■ ACS 5.8.1 supports the privilege level as a numeric value (1-15).
TACACS+ Shell Custom attributes	Phase II does not support custom attributes for privilege levels and shell commands.
TACACS+ Shell Command Authorization Set: You do not have to specify a value for each attribute.	Migration supports only per-user command authorization and does not support the following attributes: ■ Assign a shell command authorization set for any network device. ■ Assign a shell command authorization set on a per-network device group basis. You must specify a value for each attribute.

User Group

In ACS 4.x, each user was associated to a single group. The User Group element includes general identity attributes as well as policy component attributes such as shell exec and RADIUS attributes. In ACS 5.8.1, the equivalent to user group is the identity group. However, each identity group is purely a logical container and does not include policy components.

User Group Policy Components

In ACS 4.x, policy authorization data is embedded within user group definitions. In ACS 5.8.1, policy authorization data is defined in Session Authorization Profiles. Table 3 on page 4 shows the attributes for the policy components of the ACS 4.x user group and describes the status in ACS 5.8.1.

Table 3 User Group Policy Component Attributes

ACS 4.x Attribute	ACS 5.8.1 Status
TACACS+ Shell (exec) Privilege level: The privilege level is a string field without validity checks.	■ ACS 5.8.1 supports the privilege level as a numeric value (1-15). ■ In ACS 5.8.1, the default privilege level cannot be larger than the maximum privilege level.
TACACS+ Shell (exec) Custom attributes	ACS 5.8.1 does not support shell command custom attributes.
TACACS+ Shell Command Authorization Set You do not have to specify a value for each attribute.	ACS 5.8.1 supports only per-user command authorization and does not support the following attributes: ■ Assign a shell command authorization set for any network device. ■ Assign a shell command authorization set on a per-network device group basis. You must specify a value for each attribute.

ACS 4.x is a group based access control system whereas ACS 5.x is a policy based access control system. When you migrate from ACS 4.x to 5.x using the migration utility, the custom attributes are not migrated. As a result, all the authentications and authorizations may fail in ACS 5.x. Therefore, you need to manually configure the custom attributes in Shell Profiles and map it to each user in the Access Policies.

To configure the custom attributes manually, see *User Guide for Cisco Secure Access Control System 5.8.1*.

To map the custom attributes in the policy conditions, see *User Guide for Cisco Secure Access Control System 5.8.1*.

Shared Shell Command Authorization Sets

No attributes are missing. In ACS 4.x, shell command authorization sets are defined as shared elements included in device administration. The export and import phases migrate these elements to command sets. The ACS 5.8.1 name and description of each element is the same as in ACS 4.x.

MAB

In ACS 4.x, you can define MAC addresses in the User table as part of the NAP configuration. ACS 5.8.1 migrates MAC IDs as MacId objects. Each MacId object is added to the MAC Authentication Bypass MAB (Hosts) Identity stores.

DACL

In ACS 4.x, the shared DACL is defined as a shared object to be included in the NAP table, and the user and user group objects. A shared DACL consists of a list of sets of ACL content and Network Access Filter (NAF) ID. You can migrate a single DACL from ACS 4.x to multiple DACLs on ACS 5.8.1. You can migrate only the ACL content, because ACS 5.8.1 does not support NAFs.

EAP-FAST Master Keys

The Master Keys definition in ACS 4.x has a schema that is different from that of the ACS 5.8.1 schema. Therefore, Master Keys are migrated to different ACS 5.8.1 Information Model Objects (IMOs).

Shared RACs

In ACS 4.x, you can define a shared profile component that contains RADIUS Authorization Components (RACs), and you can define a set of RADIUS attributes and values that are returned in an authorization response. In ACS 5.8.1, RACs are defined in shared authorization profiles.

Table 4 on page 5 shows the attributes for the RACs in ACS 4.x and describes their status in ACS 5.8.1.

Table 4 Shared RADIUS Authorization Component Attributes

ACS 4.x Attribute	ACS 5.8.1 Status
In ACS 4.x, the following attributes can be configured and fixed: ■ MS-CHAP-MPPE-Keys (12) ■ MS-MPPE-Send-Key (16) ■ MS-MPPE-Recv-Key (17)	In ACS 5.8.1, you cannot configure these attributes. These are added to the profile as required.
In ACS 4.x, Ascend attributes are stored internally with a vendor ID of 0.	In ACS 5.8.1, you have to assign an Ascend vendor ID of 529.

Customer VSAs

During migration, the dictionary is iterated to identify the missing attributes in ACS 5.8.1 for each vendor. If the vendor does not exist in the ACS 5.8.1 dictionary, all the vendor attributes are migrated. If the vendor exists in the ACS 5.8.1 dictionary, only attributes that are not defined in ACS 5.8.1 are migrated.

Max User Sessions

In ACS 4.*x*, you can configure the Maximum User Sessions settings at user level, group level, and globally. The maximum user sessions settings are migrated when you migrate from 4.*x* to 5.8.1.

Configuration Mapping from ACS 3.x and 4.x to ACS 5.8.1

Table 1 on page 1 lists the configuration areas in ACS 3.x and 4.x and their equivalents in ACS 5.8.1.

Table 1 Configuration Mapping from ACS 3.x and 4.x to ACS 5.8.1

ACS 3.x and 4.x Configuration Areas	ACS 5.8.1 Configuration Areas
User Setup	Users and Identity Stores, Policy Elements, Access Policies, System Administration
Group Setup	Users and Identity Stores, Policy Elements, Access Policies
Shared Profile Components	Policy Elements
Network Configuration	Network Resources
System Configuration	System Administration
Interface Configuration	NA
Administration Control	System Administration
External User Databases	Users and Identity Stores
Posture Validation	NA
Network Access Profiles	Access Policies
Reports and Activity	Monitoring and Reports

Feature Comparison of ACS 3.x and 4.x with ACS 5.8.1

Table 1 Feature Comparison List–ACS 3.x/4.x and ACS 5.8.1

Feature	ACS 3.x and 4.x	ACS 5.8.1	Notes
Platform Support			
1111	Yes	No	
1112	Yes	No	
1113	Yes	No	
1120	Yes (4.2)	Yes	ACS 5.0 shipping appliance
1121	No	Yes	ACS 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, and 5.8 shipping appliance
3415	No	Yes	ACS 5.4, 5.5, 5.6, 5.7, and 5.8 shipping appliance
3495	No	Yes	ACS 5.5, 5.6, 5.7, and 5.8 shipping appliance
3515	No	Yes	ACS 5.8.1 shipping appliance
3595	No	Yes	ACS 5.8.1 shipping appliance
Windows Server	Yes	No	
Virtual machine	ESX 3.x	ESX i5.0, i5.0 update 2, i5.1, i5.5, i5.5 update 1, and i5.5 update 2	
Components			
ACS for Windows	Yes	No	No Windows Server support in ACS 5.8.1
ACS Solution Engine	Yes	No	ACS 5.8.1 provides its own appliance option
ACS View 4.0	Yes	No	ACS 5.8.1 has integrated View functionality
ACS Remote Agent	Yes	No	Remote Agent not required in 5.8.1
ACS Express 5.0	No	No	
Application Integration			
CiscoWorks Common Services (for CSM/LMS)	Yes	No	
Cisco Wireless Control System (WCS)	Yes	Yes	
Distributed Model			

Table 1 Feature Comparison List—ACS 3.x/4.x and ACS 5.8.1 (continued)

Feature	ACS 3.x and 4.x	ACS 5.8.1	Notes
Single primary/multiple secondary	Yes	Yes	
Cascading replication	Yes	No	
Replication trigger	Manual or per schedule	On configuration change	
Replication unit	Whole replication component	Configuration delta only	
Synchronization	Loose	Tight	
Automatic outage resynchronization	No	Yes	
Internal user password updates	On primary only	On primary only	
Role-based secondary to primary promotion	No	Yes	
Identity Store Support			
Internal	Yes	Yes	
Active Directory	Yes	Yes	
LDAP	Yes	Yes	
RDBMS	Yes	No	
RSA SecurID	Yes	Yes	
Other One-time Password Servers	Yes	Yes	Uses RADIUS interface to OTP server
AAA Proxy Support			
RADIUS proxy	Yes	Yes	Includes EAP Proxy
TACACS+ proxy	Yes	Yes	
Logging Destinations			
ACS View	Yes	Yes	
Syslog	Yes	Yes	
ODBC	Yes	No	ACS 5.8.1 provides View log data synchronization with an external database for archival purposes
Configuration Query/Provisioning			
Web-based GUI	Yes	Yes	
CSV-based updates	Yes	Yes	
CSUtil	Yes	No	
RDBMS Synchronization	Yes	No	
Management			
SNMP query	Yes (appliance only)	Yes	
SNMP traps	No	Yes	
View alarms	Yes	Yes	
GUI	Yes	Yes	
Cisco standard look and feel GUI	No	Yes	

Table 1 Feature Comparison List–ACS 3.x/4.x and ACS 5.8.1 (continued)

Feature	ACS 3.x and 4.x	ACS 5.8.1	Notes
CLI	Yes (limited, appliance only)	Yes (similar to IOS)	
System restart after some configuration changes	Yes	No	
KVM console access	No	Yes	
Choice of file transfer storage repositories	No	Yes	
In-place, cross-version upgrade procedure	No	Yes	
Remote upgrades/patching	Partial	Yes	
Supported Protocols			
PAP	Yes	Yes	
CHAP	Yes	Yes	
MS-CHAPv1	Yes	Yes	
MS-CHAPv2	Yes	Yes	
MAB	Yes	Yes	
EAP-MD5	Yes	Yes	
EAP-TLS	Yes	Yes	
PEAP-MSCHAPv2	Yes	Yes	
PEAP-GTC	Yes	Yes	
PEAP-TLS	Yes	Yes	
FAST-MSCHAPv2	Yes	Yes	
FAST-GTC	Yes	Yes	
FAST-TLS	Yes	No	
LEAP	Yes	Yes	
TACACS+			
Command authorization	Yes	Yes	
Accounting	Yes	Yes	
Single connect	Yes	Yes	
Change password	Yes	Yes	
Enable handling	Yes	Yes	
Custom services	Yes	Yes	
Optional attributes	Yes	Yes	
CHAP/MSCHAP authentication	Yes	Yes	
Attribute substitution	Yes	Yes	
ACS Password Policy			
Complexity	Yes	Yes (stronger)	
History	Yes (last only)	Yes (multiple)	

Table 1 Feature Comparison List—ACS 3.x/4.x and ACS 5.8.1 (continued)

Feature	ACS 3.x and 4.x	ACS 5.8.1	Notes
Expiry	Yes (age by days, logins, first login)	Yes (age by days)	
Expiry warning	Yes	Yes	
Grace period	Yes	No	
Account Disablement			
By date	Yes	Yes	Can be implemented using authorization policy
By failed attempts	Yes	Yes	
By inactivity	No	Yes	
Network Devices			
Separate TACACS+/RADIUS entries	Yes	Yes	
Hierarchical, scalable device grouping	No	Yes	
Default network device	TACACS+ only	RADIUS and TACACS+	
Group-level shared secrets	Yes	No	
Wildcard for IP address	Yes	Yes	
Access Policy			
Flexible, rules-based policy model	No	Yes	
Mandatory ACS group assignment	Yes	No	
Multiple group membership	No	Yes	
Static IP address assignment	Yes	Yes	Extend schema, policy
Maximum sessions	Yes	Yes	
Group disablement	Yes	Yes	Implement in ACS 5.8.1 policy
VOIP support	Yes	No	
ToD settings	Yes	Yes	
Callback	Yes	Yes	Use of Windows Callback setting is not available in ACS 5.8.1
Network Access Restrictions	Yes	Yes	
Usage quotas	Yes	No	
Enable options	Yes	Yes	Implement in ACS 5 policy
Token caching	Yes	No	
IP address assignment	Yes	Yes (static and AAA client pool only)	For assigning static IP address, implement in authorization policy by adding IP address field to user schema. AAA client pool refers to the ability to set the VSA attribute "ip-pool-definition" on ACS. The pool itself will be defined on the switch or router itself.
Downloadable ACLs	Yes	Yes	

Table 1 Feature Comparison List–ACS 3.x/4.x and ACS 5.8.1 (continued)

Feature	ACS 3.x and 4.x	ACS 5.8.1	Notes
Supplementary user information	Yes	Yes	
Extendable ACS user schema for use in policy conditions and for authorization values	No	Yes	
User attributes (internal, AD, LDAP), that can be leveraged in policy conditions and as authorization values	No	Yes	
External password authentication for ACS internal users	Yes	Yes	In ACS 5, the password store must be specified through Access Service Identity Policy, and cannot be specified in the user's record.
Time bound alternate group	Yes	Yes	In ACS 5, time-based conditions are used to specify different permissions based on time of the day.
Windows dial-in support	Yes	No	
ACS Administrators			
Network restrictions	Yes	Yes	
Entitlement reports	Yes	Yes	
Password complexity	Yes	Yes (stronger)	
Password aging	Yes	Yes	
Password history	Yes	Yes	
password inactivity	Yes	Yes	
Account disablement because of failed attempts	Yes	Yes	
Account disablement because of account inactivity	Yes	Yes	
Permission control	Yes	Yes (role-based)	
Certificate-based Authentication/Authorization			
Mandatory AD authorization	Yes	No	
SAN/CN Comparison	Yes	No	Can be implemented indirectly in ACS 5.8.1 by checking for user attribute existence
Certificate binary comparison	Yes	Yes	

Troubleshooting the Migration Utility

This chapter describes common problems associated with the ACS 5.8.1 Migration Utility:

Unable to Restore the ACS 4.x Database on the Migration Machine

Condition

Unable to restore the ACS 4.x database on the migration machine.

Action

Verify and ensure that the ACS 4.x production machine (for which a backup was created) and the ACS 4.x migration machine (on which backup was restored) have identical versions of the system software. The problem might be caused by a missing patch level.

Remote Desktop Connection Not Supported for the Migration Utility

Condition

You cannot use Remote Desktop Connection (RDC) to run the Migration Utility.

Action

Use Virtual Network Computing (VNC) to run the Migration Utility on the migration machine.

Migrating Objects from Large-Scale Databases

You might encounter several issues when you attempt to migrate objects from a large database.

Condition

Performance problems can occur when you attempt to migrate a large number of objects from an ACS 4.x database.

Action

We recommend that you run the Migration Utility for *each* object group. For example, from the Migration Utility, enter **2** to choose option 2, AllUsersObjects. In this example, you would only run the Migration Utility against the Users object.

Import Phase Only Adds Partial Data

Condition

Import only adds partial data.

Action

1. Ensure that:

- Migration interface is enabled on the ACS 5.8.1 server.
- Network connections are enabled.
- ACS 5.8.1 services are up and running.
- You use a compatible ACS 5.8.1 license.

2. Restore the ACS 5.8.1 database to its previous version of the database.
3. Restart the Migration Utility.
4. Rerun the Import phase.

ACS 5.8.1 Machine Does Not Respond After Import

Condition

The ACS 5.8.1 machine does not respond after import.

Action

Restart ACS 5.8.1.

Resolving Migration Issues

These sections discuss manual methods for resolving migration issues. The following migration issues are discussed:

Overlapping IP Addresses

The Analysis phase might report overlapping IP addresses for network devices in ACS 4.x. ExampleOverlapping IP Addresses, page 3 shows that the IP address in the AA network device overlaps with the IP address in the BB network device, and each network device belongs to a different NDG. From the ACS 4.x perspective, these are two separate objects.

```
ExampleOverlapping IP Addresses
The following Network Devices are overlapped:
Network device: AA, IP Address = 23.8.23.*, 45.67.*.8, protocol =RADIUS, Group= HR
Network device: BB, IP Address = 45.*.6.8, 1.2.3.4, protocol =TACACS, Group = Admin
```

However, ACS 5.8.1 defines TACACS+ and RADIUS as one object.

The solution is to use the ACS 4.x application to redefine the network devices to have identical IP addresses and ensure that they belong to the same NDG. ExampleResolved IP Addresses, page 3 illustrates the resolution.

```
ExampleResolved IP Addresses
Network device: CC, IP Address = 1.2.3.*, protocol =RADIUS, Group= HR
Network device: DD, IP Address = 1.2.3.*, protocol =TACACS, Group = HR
```

In this example, you consolidate the RADIUS and TACACS+ network devices; the IP addresses are identical and both network devices are part of the same NDG. You can export CC and DD as one object named CC+DD.

Untranslatable IP Addresses

The IP address definition in ACS 4.x can include wildcards and ranges. In ACS 5.8.1, the IP address definition is in the form of a subnet mask. The analysis phase identifies network groups with untranslatable IP addresses.

You can use the ACS 4.x application to modify the IP address ranges to an ACS 5.8.1 subnet mask definition. However, not all combinations of IP addresses can be translated into an ACS 5.8.1 subnet mask definition. For example:

```
Network device: AA, IP Address =23.8.23.12-221 protocol =RADIUS, Group= HR
```

In this example, the IP address contains a range, **12-221**, and cannot be translated into a subnet mask definition.

You cannot migrate IP addresses that contain wildcards (*) or ranges (x-y) in the middle of the address. You cannot migrate the following pattern of IP addresses:

- 1.*.2.*,
- *.*.*.1,
- *.*.*.*

The following patterns of IP addresses can be translated:

- 1.*.*.*
- 1.2.*.*
- 1.2.3.*
- 1.2.3.13-17

Note: Migration supports IP ranges from 0 to 255.

Network Devices with More Than 40 IP Addresses

Condition

Network devices in ACS 4.x have more than 40 IP addresses. ACS 5.8.1 does not migrate network devices that have more than 40 IP addresses.

Action

Use the ACS 4.x application on the migration machine and edit the network device settings. To do this:

1. Choose **Network Configuration**.
2. Choose the NDG to which the network device belongs.
3. Choose the network device.
4. Edit the **AAA Client IP Address** field. Ensure that the AAA client has 40 or fewer IP addresses.
5. Click **Submit + Apply**.

Rerun the Migration Utility (Analyze and Export phase and Import phase).

Invalid TACACS+ Shell Privilege Level

Condition

TACACS+ (T+) shell privilege level not in the range 0 to 15.

Action

Use the ACS 4.x application on the migration machine and edit T+ settings. Ensure that the T+ privilege level is in the range 0 to 15.

To edit the T+ settings at the user level:

1. Choose **User Setup**.
2. Choose the user.

   The Edit screen appears.
3. Check the **Privilege level** check box of the TACACS+ Settings table and enter a value between 0 and 15.
4. Click **Submit**.

To edit the T+ settings at the group level:

1. Choose **Group Setup**.
2. Choose the group and click **Edit Settings**.
3. Check the **Privilege level** check box of the TACACS+ Settings table and enter a value between 0 and 15.
4. Click **Submit + Restart**.

Rerun the Migration Utility (Analyze and Export phase and Import phase).

TACACS+ Custom Attributes Are Not Migrated

Condition

T+ custom attributes are defined for users and groups in ACS 4.x. ACS 5.8.1 does not support TACACS+ custom attributes.

Action

No action is required. All the other T+ shell exec attributes that are defined for users and groups are not migrated. T+ custom attributes are dropped.

Shell Command Authorization Set Not Associated with User or Group

Condition

Shell command authorization sets are assigned to users and user groups in ACS 4.x. After migration, the association between the shell command authorization set and the User or Group is lost.

Action

Use the ACS 5.8.1 application to:

1. Access the migrated command sets. See Command Set Migration, page 50, for more information.
2. Create a policy for the users and identity groups.

See the *User Guide for Cisco Secure Access Control System 5.8.1* for more information on creating policies.

Migration Failed with Manually Created Super Admin

Condition

User *Admin1* is created under **System Administration > Administrators > Accounts, with the** role as a super admin in ACS 5.8.1. Migration fails when *Admin1* is used as the administrator username.

Action

Check if the migration steps are correct. ACS 5.8.1 now supports migration with any ACS administrator account assigned with recovery superadmin role.

Migration Utility Messages

The following tables describe the error and informational messages that may appear during the migration of various ACS objects.

Downloadable ACLs

Table 1 on page 6 gives the detail of the errors and informational messages that may appear during the migration of the Downloadable ACLs.

Table 1 Error and Informational Messages for Downloadable ACLs

Phase	Type	Error	Diagnosis
Export	Information	Shared DACL name after migration has been changed to: *name after truncation.*	Truncation
Export	Error	*Cannot migrate a shared DACL with a name that contains any of the following characters: illegal characters for the object*.	Name error
Import	Error	*Error from PI*. For example, object already exists in the ACS 5.8.1 database.	None

MABs

Table 2 on page 6 gives the detail of the errors and informational messages that may appear during the migration of the MABs.

Table 2 Error and Informational Messages for MABs

Phase	Type	Error	Diagnosis
Export	Information	MAB name after migration has been changed to: *name after truncation*.	Truncation
Export	Information	Cannot migrate a MAB with a name that contains any of the following characters: *illegal characters for the object*.	Name error
Export	Information	Invalid MAC ID.	Untranslatable

Table 2 Error and Informational Messages for MABs

Phase	Type	Error	Diagnosis
Import	Error	*Error from PI.* For example, Object already exists in the ACS 5.8.1 database.	None
Import	Error	Group ID: *group ID* referenced object was not imported.	No reference import
Import	Error	Group could not be found for: *MAB name* Group ID: *group ID*.	Log error

NDGs

Table 3 on page 7 gives the detail of the errors and informational messages that may appear during the migration of the NDGs.

Table 3 Error and Informational Messages for NDGs

Phase	Type	Error	Diagnosis
Export	Information	Network device name after migration has been changed to: *name after truncation.*	Truncation
Export	Information	Cannot migrate an NDG with a name that contains any of the following characters: *illegal characters for the object.*	Name error
Export	Information	NDG has a shared key password.	Password included
Import	Error	*Error from PI.* For example, failed to add object: *NDG root name* in function: *method name.*	None
Import	Information	Object already exists in the ACS 5.8.1 database.	Duplicate

Master Keys

Table 4 on page 7 gives the detail of the errors and informational messages that may appear during the migration of the Master Keys.

Table 4 Error and Informational Messages for Master Keys

Phase	Type	Error	Diagnosis
Export	Information	Fatal Error: Authority ID is null – Import Failed.	None
Import	Error	*Error from PI.* For example, object already exists in the ACS 5.8.1 database.	None

Network Devices

Table 5 on page 8 gives the detail of the errors and informational messages that may appear during the migration of the Network Devices.

Table 5 Error and Informational Messages for Network Devices

Phase	Type	Error	Diagnosis
Export	Information	*Network device name after migration has been changed to: name after truncation.*	Truncation.
Export	Information	Network Device has shared key password.	Password included.
Export	Information	NDG *referenced NDG* unified with *Name of the Network device overlapped with* from NDG *NDG name.*	Unified NDG: *Referenced NDG.*
Export	Error	Cannot migrate an NDG with a name that contains any of the following characters: *Illegal characters for the object.*	Name error.
Export	Error	NDG referenced object was not exported.	No reference object exported.
Export	Error	NDG: *referenced NDG* there are *number of subnets* subnets in the following IP address *IP address.*	Over subnet limit.
Export	Error	Unable to translate network device IP address.	Untranslatable NDG: *Referenced NDG.*
Export	Error	NDG *referenced NDG*: Network device IP address overlaps the same device.	Overlapping NDG: *Referenced NDG.*
Export	Error	Network device has been discarded as it is unified with: *unified NDG*.	Unified partner NDG: *Referenced NDG.*
Export	Error	Network device IP is overlapping with other device.	Overlapping NDG: *Referenced NDG.*
Export	Error	Overlaps with: *Network device name* from NDG: *NDG name*.	Overlapping NDG: *Referenced NDG* IP address: *IP address.*
Import	Error	NDG referenced object was not imported.	No reference import.
Import	Error	*Error from PI.* For example, Object already exists in the ACS 5.x database.	None.

RACs

Table 6 on page 9 gives the detail of the errors and informational messages that may appear during the migration of the RACs.

Table 6 Error and Informational Messages for RACs

Phase	Type	Error	Diagnosis
Export	Information	RAC name after migration has been changed to: *name after truncation.*	Truncation
Export	Error	ACS 5.8.1 does not support this attribute: vid= *vendor ID*, att= *attribute value*. No other attributes in RAC will be migrated.	Unsupported vendor
Export	Error	RAC does not contain any supported attributes.	No value
Export	Error	Cannot migrate an RAC with a name that contains any of the following characters: *Illegal characters for the object.*	Name error
Export	Error	Wrong enum value for attribute: *attribute name.* No other attributes in RAC will be migrated.	Error
Export	Error	Invalid value for attribute: *VSA attribute name.* No other attributes in RAC will be migrated.	Error
Export	Information	The following attribute was not migrated: *attribute name.*	Unsupported vendor
Export	Error	ACS 5.8.1 does not support this attribute: vid= *vendor ID*, att= *attribute value*, name= *attribute name.* No other attributes in RAC will be migrated.	Unsupported vendor
Import	Error	RAC exception, for example, Invalid attribute number.	None
Import	Error	*Error from PI.* For example, Object already exists in the ACS 5.8.1 database.	None
Import	Fatal	An error occurred in createCapabilitiesAll(): *Exception details.*	Log error

Command Set

Table 7 on page 10 gives the detail of the errors and informational messages that may appear during the migration of the Command Sets.

Table 7 Error and Informational Messages for Command Sets

Phase	Type	Error	Diagnosis
Export	Information	Command set name after migration has been changed to: *name after truncation.*	Truncation
Export	Information	Identical objects cannot be migrated: *identical object name.*	Consolidated
Export	Information	*Command set value:* Invalid Command Set value.	Untranslatable
Export	Information	Cannot migrate a command set with a name that contains any of the following characters: *Illegal characters for the object.*	Name error
Export	Information	*Command set name* was not imported and shell exec and command set for this user/group were not imported.	Name error
Export	Information	Shared command sets name cannot contain apostrophes or curly braces.	Name error
Export	Information	*Command Set name* contains a duplicate argument.	With duplicate argument
Export	Information	The selected network device NDG is not supported.	Unsupported option
Export	Error	Translation failed. The argument does not start with Unmatched.	Log error
Export	Error	Translation failed. An equals sign (=) is missing after Unmatched	Log error
Export	Fatal	Translation failed since Unmatched is not set to permit or deny: *unmatched value.*	Log error
Export	Error	Group T+ shell command translation failed: *exception details*.	Log error
Export	Error	Group T+ shell command translation failed. The argument is not a prefix with permit/deny: *argument action value*.	Log error
Export	Error	*Command name* Group T+ command set translation failed: *exception details*.	Log error
Export	Error	*Command description, Exception details*.	Log error
Import	Error	Referenced object was not imported.	No reference import
Import	Error	*Error from PI.* For example, object already exists in the ACS 5.8.1 database.	Error

Shell Exec

Table 8 on page 11 gives the detail of the errors and informational messages that may appear during the migration of the shell exec.

Table 8 Error and Informational Messages for Shell Exec

Phase	Type	Error	Diagnosis
Export	Information	Command set name after migration has been changed to: *name after truncation.*	Truncation
Export	Information	Identical objects cannot be migrated: *identical object name.*	Consolidated
Export	Information	*Shell Exec value* Invalid shell exec value. No other T+ shell exec attributes will be migrated.	Untranslatable
Export	Information	Parsing error. No other T+ shell exec attributes will be migrated.	Untranslatable
Export	Information	Cannot migrate a command set with a name that contains any of the following characters: *Illegal characters for the object*. No other T+ shell exec attributes will be migrated.	Name error
Export	Information	*Shell Exec name* was not imported and shell exec and command set for this user/group were not imported. No other T+ shell exec attributes will be migrated.	Name error
Export	Information	ACS 5.8.1 does not support custom attributes present in T+ shell exec. No other T+ shell exec attributes will be migrated.	Inset
Export	Information	T+ shell exec not defined for user or user group. No other T+ shell exec attributes will be migrated.	Inset
Export	Information	Idle time for shell exec should be in the range of 0-9999. No other T+ shell exec attributes will be migrated.	Invalid idle time
Export	Information	Time out for shell exec should be in the range of 0-9999. No other T+ shell exec attributes will be migrated.	Invalid timeout
Export	Information	T+ shell priv-lvl is invalid *value.* No other T+ shell exec attributes will be migrated.	Invalid privilege level
Export	Information	T+ shell priv-lvl *value* is higher than max-priv-lvl *max value*. No other T+ shell exec attributes will be migrated.	Invalid privilege level
Export	Information	ACS 5.8.1 does not support custom attributes present in T+ shell exec.	Unsupported option
Export	Error	Group T+ shell exec translation failed: *exception details*.	Log error

Table 8 Error and Informational Messages for Shell Exec (continued)

Phase	Type	Error	Diagnosis
Export	Error	An error occurred while retrieving the max privilege: *exception details*.	Log error
Import	Error	Referenced object was not imported.	No reference import
Import	Error	*Error from PI*. For example, object already exists in the ACS 5.8.1 database.	Error

Users

Table 9 on page 12 gives the detail of the errors and informational messages that may appear during the migration of the Users.

Table 9 Error and Informational Messages for Users

Phase	Type	Error	Diagnosis
Export	Information	User name after migration has been changed to: *name after truncation.*	Truncation
Export	Error	Cannot migrate users with names that contain any of the following characters: *Illegal characters for the object.*	Name error
Export	Error	Cannot migrate users whose password does not conform to the ACS 5 password policy. Passwords should be between 4 and 32 characters in length.	Password error
Export	Error	Cannot migrate users with empty password to ACS 5.8.1.	No password
Export	Error	Cannot migrate VoIP users to ACS 5.8.1.	VoIP group
Export	Error	A problem occurred while reading the expiry data for the user.	Log error
Import	Error	Referenced object was not imported.	No reference import
Import	Error	Group could not be found for: *MAB name* Group ID: *group ID.*	Log error

User Attributes

Table 10 on page 13 gives the detail of the errors and informational messages that may appear during the migration of the User attributes.

Table 10 Error and Informational Messages for User Attributes

Phase	Type	Error	Diagnosis
Export	Information	User attribute after migration has been changed to: *name after truncation*.	Truncation
Export	Information	Cannot migrate a user attribute with a name that contains any of the following characters: *Illegal characters for the object.*	Name error
Export	Information	*User attribute name* User-defined name is not unique. It will be disambiguated for import by appending a suffix.	Repeated
Import	Information	Attribute added with warning: Object already exists in the ACS 5.8.1 database.	Duplicate
Import	Error	*Error from PI.*	Error

User Attribute Values

Table 11 on page 13 gives the detail of the errors and informational messages that may appear during the migration of the User attribute values.

Table 11 Error and Informational Messages for User Attribute Values

Phase	Type	Error	Diagnosis
Export	Error	*User attribute value* was not imported and user attribute values for this user were not imported.	Log error

User Groups

Table 12 on page 13 gives the detail of the errors and informational messages that may appear during the migration of the User Groups.

Table 12 Error and Informational Messages for User Groups

Phase	Type	Error	Diagnosis
Export	Error	Group has no users.	Without users
Export	Error	Cannot migrate a user group with a name that contains any of the following characters: *Illegal characters for the object.*	Name error
Import	Information	*Error from PI.*	Duplicate
Import	Error	*Error from PI.*	Error

VSA Vendors

Table 13 on page 14 gives the detail of the errors and informational messages that may appear during the migration of the VSA vendors IDs.

Table 13 Error and Informational Messages for VSA Vendors

Phase	Type	Error	Diagnosis
Export	Error	Object already exists in the ACS 5.8.1 database.	Duplicate
Export	Information	Vendor name conflict. ACS 5.8.1 vendor name: *vendor name.*	Name error
Import	Error	VSA vendor ID *vendor id* import failed. *Error from PI*:	Enum error

VSAs

Table 14 on page 14 gives the detail of the errors and informational messages that may appear during the migration of VSAs.

Table 14 Error and Informational Messages for VSAs

Phase	Type	Error	Diagnosis
Export	Error	VSA ID *attribute id value* has attribute profile conflicts: In ACS 4.x, it is *name for the profile*, but in ACS 5.0, it is *direction value*.	Profile error
Export	Error	VSA ID (attribute id) has attribute name conflicts: In ACS 4.x, it is *attribute name*, but in ACS 5.8.1, it is *attribute name*.	Name error
Import	Error	VSA ID *attribute id* has attribute type conflicts: In ACS 4.x, it is *attribute type*, but in ACS 5.0, it is *ACS 5.8.1 attribute type value.*	Type error
Export	Error	There is a problem with the VSA ID *attribute id* enum values (see log for details)	Enum error
Export	Error	Object already exists in the ACS 5.8.1 database.	None
Import	Error	VSA *attribute id* enum import failed. *Error from PI:*	Enum error
Import	Information	VSA *attribute ID* enabling log failed.	None
Import	Error	VSA *attribute ID* attribute import failed. *Error from PI.*	Unsupported attribute
Import	Error	VSA *attribute ID* vendor ID *vendor ID* import failed. *Error from PI*.	No reference import

Reporting Issues to Cisco TAC

Note: Technical Support for ACS is limited to standard Cisco product installation, configuration, and operational troubleshooting. Questions and support issues related to ACS 4.x to 5.8.1 migration are not covered by Cisco Technical Support.

Note: The Cisco Technical Assistance Center (TAC) does not offer any support for migrating from Cisco Secure ACS for Windows or Solutions Engine to ACS 5.x. Contact your account team for assistance.

Include information about the following when you report a case to Cisco TAC:

- Backup of the ACS 4.x database (.dmp file)
- Migration logfile (...migration/bin/migration.log)
- All the reports in the config folder (...migration/config)
- ACS 5.8.1 logfiles
- ACS 5.8.1 build number
- ACS 4.x build number