Migration Guide for Cisco Secure Access Control System 5.5

November 2013

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
CONTENTS

Preface ix
   Audience ix
   Organization ix
   How to Use This Document x
   Conventions x
   Documentation Updates xi
   Product Documentation xi
   Related Documentation xii
   Obtaining Documentation and Submitting a Service Request xii

CHAPTER 1
ACS 5.5 Deployment Overview 1-1
   Windows Versus Linux-Based Applications 1-2
   Replication 1-2
   Identity Stores 1-3
   Logging 1-3
   Configuration 1-4
   Licensing 1-4
   Server Deployment Recommendations 1-5
   Performance 1-6

CHAPTER 2
Understanding ACS 5.5 Configuration 2-1
   ACS 5.5 Configuration 2-1
   Network Resources 2-2
      Network Device Groups 2-2
      Network Devices 2-5
      External RADIUS Servers 2-6
   Users and Identity Stores 2-7
      Identity Groups 2-7
      Internal Identity Stores 2-9
      External Identity Stores 2-10
      Certificate Authorities and Certificate Authentication Profiles 2-10
      Identity Store Sequences 2-11
   Policy Elements 2-11
   Session Conditions 2-12
Contents

Migration Guide for Cisco Secure Access Control System 5.5
OL-28604-01

Chapter 3
Configuration Migration Methods in ACS 5.5

Migration Methods 3-1
- Migration Utility 3-1
- CSV Import Tool 3-2

About the Migration Utility 3-3

Migrating from ACS 4.x to 5.5 3-3
- Multiple-Instance Migration 3-3

Migration Phases for ACS 5.5 3-4
- Analysis Phase 3-4
- Migration Phase 3-4

Data Model Organization 3-4

Multiple-Instance Migration Support 3-5

Migrating Data 3-7
- Object Group Selection 3-8
- Analysis and Export 3-9
- Import 3-9
- Multiple-Instance Support 3-9

Chapter 4
ACS 5.5 Migration Utility Support

ACS 4.x to 5.5 Migration Version Support 4-1
ACS 4.0 Migration Support 4-1
ACS 4.x Appliance Support 4-2
CSACS-1120 Series Appliance Support 4-2
Remote Desktop Support 4-2
Multiple-Instance Support 4-2
ACS 4.x Elements Supported in the Migration Process 4-3
ACS 4.x Elements Not Supported in the Migration Process 4-4

User Interface 4-5
- CLI-Based Migration Utility 4-5
Phases of the CLI-Based Migration Utility 4-5

CHAPTER 5

Migration Utility Setup and Installation 5-1
Migration Preinstallation Considerations 5-1
System Requirements 5-2
ACS Software Accessory Kit DVDs 5-3
Security Considerations 5-4
Accessing the Migration Utility 5-4
Migration Utility Packaging 5-4
Data Migration and Deployment Scenarios 5-5
Guidelines for Data Migration in a Single ACS Server 5-5
Guidelines for Data Migration in a Distributed Environment 5-5
Data Migration Between Platforms 5-6

CHAPTER 6

Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5 6-1
Introduction 6-1
Running the Migration Utility 6-2
Migration Script Sections 6-5
Migration of ACS 4.x Objects 6-9
AAA Client/Network Device 6-10
Data Mapping 6-10
Analysis and Export 6-11
Import 6-13
Multiple-Instance Support 6-14
NDG 6-14
Data Mapping 6-14
Analysis and Export 6-15
Import 6-15
Multiple-Instance Support 6-16
Internal User 6-16
Basic User Definition 6-16
Multiple-Instance Support 6-18
User Data Configuration and User Mapping 6-18
User Shell Command Authorization 6-20
Shell Exec Parameters 6-22
User Group 6-23
Analysis and Export 6-24
Import 6-24
Multiple-Instance Support 6-24
User Group Policy Components 6-24
   Group Command Set 6-25
   Group Shell Exec 6-25
   MAC Addresses and Internal Hosts 6-27
   Shared Shell Command Authorization Sets 6-28
Shared DACL Objects 6-29
   Data Mapping 6-29
   Analysis and Export 6-30
   Import 6-30
   Multiple-Instance Support 6-30
Shared RACs 6-30
   Data Mapping 6-31
   Analysis and Export 6-31
   Import 6-31
   Multiple-Instance Support 6-32
RADIUS VSAs 6-32
   Data Mapping 6-33
   Analysis and Export 6-34
   Import 6-34
EAP-Fast Master Keys and the Authority ID 6-34
   Data Mapping 6-34
   Analysis and Export 6-35
   Import 6-35
   Multiple-Instance Support 6-35
Analysis and Export of ACS 4.x Data 6-36
   Consolidating Data 6-37
   Issues Resulting from the Analysis and Export Phase 6-37
Importing the ACS 4.x Data to ACS 5.5 6-37
Migrating Multiple Instances 6-40
Migration Impact on Memory and Performance 6-40
Printing Reports and Report Types 6-40
   Analyze and Export Summary Report 6-42
   Analyze and Export Full Report 6-42
   Import Summary Report 6-43
   Import Full Report 6-44
   Validating Import 6-45
   Summary Report 6-45
   Full Report 6-46
Errors and Exception Handling | 6-47
Confirming the Migration | 6-47
  Users and User Groups | 6-48
Command Shell Migration | 6-49
Command Set Migration | 6-50
NDG Migration | 6-51
Network Device Migration | 6-52
DACL Migration | 6-53
MAB Migration | 6-54
Shared RACs | 6-55
RADIUS VSA | 6-56
KEK and MACK Keys | 6-57

APPENDIX A
ACS 5.5 Attribute Support in the Migration Utility | A-1
  Introduction | A-1
  ACS 4.x to 5.5 Migration | A-1
    AAA Client/Network Device | A-2
    NDG | A-2
    Internal User | A-2
    User Policy Components | A-3
    User Group | A-3
    User Group Policy Components | A-4
    Shared Shell Command Authorization Sets | A-4
    MAB | A-5
    DACL | A-5
    EAP-FAST Master Keys | A-5
    Shared RACs | A-5
    Customer VSAs | A-5
    Max User Sessions | A-6

APPENDIX B
Configuration Mapping from ACS 3.x and 4.x to ACS 5.5 | B-1

APPENDIX C
Feature Comparison of ACS 3.x and 4.x with ACS 5.5 | C-1

APPENDIX D
Troubleshooting the Migration Utility | D-1
  Unable to Restore the ACS 4.x Database on the Migration Machine | D-1
  Remote Desktop Connection Not Supported for the Migration Utility | D-2
  Migrating Objects from Large-Scale Databases | D-2
Import Phase Only Adds Partial Data  D-2
ACS 5.5 Machine Does Not Respond After Import  D-3
Resolving Migration Issues  D-3
  Overlapping IP Addresses  D-3
  Untranslatable IP Addresses  D-4
  Network Devices with More Than 40 IP Addresses  D-4
  Invalid TACACS+ Shell Privilege Level  D-5
  TACACS+ Custom Attributes Are Not Migrated  D-5
  Shell Command Authorization Set Not Associated with User or Group  D-6
Migration Failed with Manually Created Super Admin  D-6
Migration Utility Messages  D-6
  Downloadable ACLs  D-7
  MABs  D-7
  NDGs  D-8
  Master Keys  D-8
  Network Devices  D-9
  RACs  D-10
  Command Set  D-11
  Shell Exec  D-12
  Users  D-13
  User Attributes  D-14
  User Attribute Values  D-14
  User Groups  D-15
  VSA Vendors  D-15
  VSAs  D-15
Reporting Issues to Cisco TAC  D-16
Preface

Published: November 27, 2013

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 5.5. ACS 5.5 provides many new features and functionality.

There are several differences between ACS 3.x and 4.x and ACS 5.5 platforms. You should clearly understand these differences before attempting to migrate to ACS 5.5. This document highlights these differences and provides guidance on how to migrate your ACS 3.x and 4.x configuration to ACS 5.5.

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 5.5 platform.

Organization

This guide includes the following sections:

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “ACS 5.5 Deployment Overview”</td>
<td>Provides an overview of the ACS 5.5 deployment model in comparison with ACS 3.x and 4.x.</td>
</tr>
<tr>
<td>Chapter 2, “Understanding ACS 5.5 Configuration”</td>
<td>Explains the configuration areas in ACS 5.5 in comparison with ACS 3.x and 4.x, to help understand how older configurations can be converted to ACS 5.5.</td>
</tr>
<tr>
<td>Chapter 3, “Configuration Migration Methods in ACS 5.5”</td>
<td>Describes different methods to migrate the configuration from existing systems to ACS 5.5.</td>
</tr>
<tr>
<td>Chapter 4, “ACS 5.5 Migration Utility Support”</td>
<td>Describes the scope of migration using the Migration Utility.</td>
</tr>
<tr>
<td>Chapter 5, “Migration Utility Setup and Installation”</td>
<td>Describes system requirements, preinstallation considerations, and how to access the Migration Utility.</td>
</tr>
<tr>
<td>Chapter 6, “Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5”</td>
<td>Describes the data migration process in various phases using the Migration Utility.</td>
</tr>
</tbody>
</table>
How to Use This Document

The following chapters and appendices contain instructions to migrate to ACS 5.5 from earlier releases:

- See Appendix C, “Feature Comparison of ACS 3.x and 4.x with ACS 5.5” to ensure that all the key features for your deployment are met in ACS 5.5.
- See Chapter 1, “ACS 5.5 Deployment Overview” to understand the ACS 5.5 system level details such as platform support, the distributed deployment model, and system interfaces.
- See Chapter 2, “Understanding ACS 5.5 Configuration” to understand the key functional and configuration differences in ACS 5.5, and for specific configuration recommendations and examples.
- See Chapter 3, “Configuration Migration Methods in ACS 5.5” to understand the approaches for migrating an existing configuration.

Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands, keywords, and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
</tbody>
</table>
| [ ] | 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. |
Documentation Updates

Table 1 lists the updates to the Migration Guide for Cisco Secure Access Control System 5.5.

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>

Product Documentation

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 lists the product documentation that is available for ACS 5.5. To find end-user documentation for all the products on Cisco.com, go to: http://www.cisco.com/go/techdocs


<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
</table>

Note: Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.
Table 2  Product Documentation (continued)

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
</table>

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 lists the related documentation that is available for ACS 4.x.

Table 3  Related Documentation

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Available Formats</th>
</tr>
</thead>
</table>

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:


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 5.5 Deployment Overview

The ACS 5.5 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 5.5 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 5.5.

Table 1-1 describes the various ACS server roles.

<table>
<thead>
<tr>
<th>ACS Server Roles</th>
<th>Role Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>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.</td>
</tr>
<tr>
<td>Secondary</td>
<td>All ACS servers that receive configuration changes from the ACS primary server, are secondary servers.</td>
</tr>
<tr>
<td>Log Collector</td>
<td>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.</td>
</tr>
</tbody>
</table>
The following sections describe the deployment differences between ACS 4.x and ACS 5.5, as well as some considerations when deploying ACS 5.5:

- Windows Versus Linux-Based Applications, page 1-2
- Replication, page 1-2
- Identity Stores, page 1-3
- Logging, page 1-3
- Configuration, page 1-4
- Licensing, page 1-4
- Server Deployment Recommendations, page 1-5
- Performance, page 1-6

**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 5.5 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 ESX 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 5.5 hardware appliance and the ACS 5.5 installed on a virtual machine. Deployments that consist of ACS 5.5 hardware appliances and ACS 5.5 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.
Chapter 1      ACS 5.5 Deployment Overview

The ACS 5.5 replication model is simple, efficient, and robust. The characteristics of the ACS 5.5 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 5.5 network access policy configuration. This is because ACS 5.5 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 5.5 is that ACS 5.5 does not support Open DataBase Connectivity (ODBC) for authentication to databases and proxy forwarding of TACACS+ requests. ACS 5.5 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 5.5, the Monitoring and Report Viewer functionality is part of ACS. In an ACS 5.5 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 5.5 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 5.5, the primary mode for configuration is a web-based user interface. ACS 5.5 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 1-2 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>
<thead>
<tr>
<th>ACS Object</th>
<th>Configuration Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Users</td>
<td>300,000</td>
</tr>
<tr>
<td>Network Devices</td>
<td>100,000</td>
</tr>
</tbody>
</table>

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 5.5 licenses are available at:

http://cisco.com/go/license

Table 1-3 lists the available ACS 5.5 licenses.

<table>
<thead>
<tr>
<th>License</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Server</td>
<td>One for each ACS instance.</td>
</tr>
<tr>
<td>Large Deployment</td>
<td>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.</td>
</tr>
</tbody>
</table>
Server Deployment Recommendations

Table 1-4 describes the component mapping from ACS 3.x and 4.x to ACS 5.5.

Table 1-4   Component Mapping

<table>
<thead>
<tr>
<th>ACS 3.x and 4.x Component</th>
<th>ACS 5.5 Component</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACS for Windows VM in VMware ESX, 1120, 1121, 3415, or 3495 appliance</td>
<td>VM in VMware ESX, 1120, 1121, 3415, or 3495 appliance</td>
<td>There is no ACS 5.5 Windows option. ACS 5.5 is an application that can run on a VMware or supported appliance.</td>
</tr>
<tr>
<td>ACS Solution Engine (1111, 1112, 1113) VM in VMware ESX, 1120, 1121, 3415, or 3495 appliance</td>
<td>VM in VMware ESX, 1120, 1121, 3415, or 3495 appliance</td>
<td>ACS 1111, 1112 and 1113 platforms do not support ACS 5.5. ACS 4.2 can run on the 1120.</td>
</tr>
<tr>
<td>ACS Remote Agent N/A</td>
<td></td>
<td>Remote Agent is not required in ACS 5.5.</td>
</tr>
<tr>
<td>ACS View 4.0 VM in VMware ESX, 1120, 1121, 3415, or 3495 appliance</td>
<td></td>
<td>ACS 5.5 has built-in ACS View functionality.</td>
</tr>
</tbody>
</table>

Deployment guidelines for ACS 5.5:

- In most cases, a one-to-one ACS server replacement is appropriate.
  - The authentication performance of ACS 5.5 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-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 1-1.
Performance

A single ACS 5.5 server that does not act as the log collector can process more than 100 authentications per second. You should make sure that a single ACS server processing AAA requests is able to manage the load during peak hours. Peak hours typically occur when users arrive to work, or when network equipment reboots. This creates a large amount of authentication requests.

For example, 50,000 employees of a company log on to a network evenly, over a fifteen minute period. This translates to approximately 56 authentications per second as the peak authentication rate. In this case, a single ACS server that does not act as the log collector, can support this peak authentication rate.

Table 1-5 shows the number of authentications a single ACS server can support for different time periods, assuming a minimal rate of 100 authentications per second.

<table>
<thead>
<tr>
<th>Time Period</th>
<th>Authentications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 second</td>
<td>100 authentications</td>
</tr>
<tr>
<td>60 seconds</td>
<td>6000 authentications</td>
</tr>
<tr>
<td>5 minutes</td>
<td>30000 authentications</td>
</tr>
<tr>
<td>15 minutes</td>
<td>90000 authentications</td>
</tr>
<tr>
<td>1 hour</td>
<td>360000 authentications</td>
</tr>
</tbody>
</table>

There are many factors that affect ACS authentication performance, such as configuration size, policy complexity, communication with external servers and authentication protocol complexity.

Table 1-6 lists the ACS performance for different authentication environments. This performance data represents the lower range of authentication rates observed while testing ACS with complex configurations. The performance is higher for simpler configurations.

<table>
<thead>
<tr>
<th>Authentication Types</th>
<th>Identity Stores</th>
<th>Internal</th>
<th>AD</th>
<th>LDAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAP</td>
<td></td>
<td>500</td>
<td>100</td>
<td>800</td>
</tr>
<tr>
<td>CHAP</td>
<td></td>
<td>500</td>
<td>500</td>
<td>N/A</td>
</tr>
</tbody>
</table>
There is an approximate 50% drop in authentication performance if the ACS server is also being used as the log collector for the Monitoring and Report Viewer.

There is an approximate 10% to 15% increase in performance, on the CSACS-1121, Cisco SNS-3415, or Cisco SNS-3495 appliance than the numbers shown in Table 1-6.

Performance on a virtual machine is slower than on an actual 1120 appliance because of the virtual machine overhead. Performance of a virtual machine increases when you increase the CPU resources.

For virtual machine environments, the minimum requirements are similar to the CSACS-1121, Cisco SNS-3415, or Cisco SNS-3495 appliance. For more information on virtual machine environments, see the Installation and Upgrade Guide for Cisco Secure Access Control System 5.5.
Understanding ACS 5.5 Configuration

ACS 5.5 Configuration

This chapter explains the differences in configuration between ACS 3.x and 4.x and ACS 5.5 when you convert the existing 3.x and 4.x configurations to 5.5.

This chapter contains the following sections:

- **Network Resources**, page 2-2
- **Users and Identity Stores**, page 2-7
- **Policy Elements**, page 2-11
- **System Administration**, page 2-15

Table 2-1 describes the main configuration areas in ACS 5.5.

<table>
<thead>
<tr>
<th>Configuration Area</th>
<th>What Will Be Configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Resources</td>
<td>AAA clients, client grouping, and RADIUS proxy servers</td>
</tr>
<tr>
<td>Users and Identity Stores</td>
<td>Internal users, Internal hosts, Active Directory, LDAP directories, one-time password servers, RADIUS identity stores, certificate authority information, and identity store sequences</td>
</tr>
<tr>
<td>Policy Elements</td>
<td>Conditions and authorization profiles for network access policy</td>
</tr>
<tr>
<td>Access Services</td>
<td>Network access policy to address different access scenarios</td>
</tr>
<tr>
<td>Monitoring and Reports</td>
<td>ACS monitoring, reporting and troubleshooting tasks</td>
</tr>
<tr>
<td>System Administration</td>
<td>ACS system administration tasks</td>
</tr>
</tbody>
</table>
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, page 2-2
- Network Devices, page 2-5
- External RADIUS Servers, page 2-6

Network Device Groups

Key changes in ACS 5.5:

- 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 5.5, 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 5.5.

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 5.5 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 2-1, Figure 2-2, and Figure 2-3 show three different network device group hierarchies.
You can assign any device to a node in each of the hierarchies. Figure 2-4 shows a Cisco switch device that is 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:

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDG:Location</td>
<td></td>
</tr>
<tr>
<td>Is Namibia</td>
<td></td>
</tr>
<tr>
<td>NDG:Device Type</td>
<td></td>
</tr>
<tr>
<td>Is Firewall</td>
<td></td>
</tr>
<tr>
<td>NDG:Vendors</td>
<td></td>
</tr>
<tr>
<td>Is Cisco</td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>
Migration Notes

- Plan your device grouping approach to make use of the more natural hierarchical grouping in ACS 5.5.
- ACS 5.5 does not support per device group shared secrets that are available in ACS 3.x and 4.x. ACS 5.5 requires a shared secret to be defined for each device definition.

Network Devices

Key changes in ACS 5.5:

- 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 2-5 shows the ACS 5.5 network device configuration.

Figure 2-5 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 2-6 shows the 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 5.5.
- ACS 5.5 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 5.5.
- The default network device is a useful tool to enable faster migration to ACS 5.5. It allows ACS 5.5 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 2-7 shows an External RADIUS server configuration in ACS 5.5.
Migration Notes

- In ACS 5.5, 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, page 2-7
- Internal Identity Stores, page 2-9
- External Identity Stores, page 2-10
- Identity Store Sequences, page 2-11

Identity Groups

Key changes in ACS 5.5:

- The ACS 5.5 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 2-8 shows identity group hierarchies in ACS 5.5.
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 5.5, 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 5.5 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 5.5, 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 5.5—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 2-9** 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.
Internal Identity Stores

Key changes in ACS 5.5:

- In addition to a user store, ACS 5.5 has a host store for host MAC addresses.
- Access policy permissions do not contain user records.
- 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 5.5 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 5.5. The ACS 5.5 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 5.5 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 5.5:

- ACS 5.5 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 5.5, but other identity stores are supported, including LDAP directories and one-time password servers.
- ACS 5.5 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 5.5 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 5.5. There is no concept of a dynamic user in ACS 5.5.

The External Identity Store configuration is similar to the External User Databases in ACS 3.x and 4.x. In ACS 5.5, external identity stores are configured and ACS communicates with them for authentication and authorization.

For Active Directory, ACS 5.5 joins an AD domain, rather than leveraging the underlying Windows operating system, similar to ACS 3.x and 4.x. ACS 5.5 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 5.5 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 5.5, 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 5.5 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 5.5:

- 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 5.5 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 5.5:

- 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 5.5 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 5.5 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 2-12
- Authorizations and Permissions, page 2-12
- Access Policies, page 2-12
Session Conditions

The key changes in ACS 5.5 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 5.5 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 5.5 are:

- Access policies are the core of network access policy in ACS 5.5.
- All network access policy for RADIUS and TACACS+ authentication and authorization requests is configured here.

All authentication and authorization requests in ACS 5.5 must be processed by an access service. An access service defines the authentication and authorization policy. ACS 5.5 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 2-10, 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.

- Utilize the new user and network device groupings to create authorization policy, as shown in Figure 2-11.
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 2-12 shows the 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 2-13.

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 2-14.
Use external groups directly in authorization policy without first mapping external groups to an ACS group.

Convert the server specific configuration in ACS 3.x and 4.x, to server-based policy in ACS 5. Figure 2-16 shows how to use the system condition, and ACS host name to direct requests to different LDAP directories.

System Administration

The key changes in ACS 5.5 are that ACS 5.5 provides the following configuration areas for system administration tasks:

- Administrators, page 2-16
- Users, page 2-16
- Operations, page 2-16
Administrators

The key changes in ACS 5.5 are that ACS administrators can be assigned up to ten predefined roles that govern an administrator's permissions.

Users

The key changes in ACS 5.5 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 5.5 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 5.5 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 5.5 are:
- ACS 5.5 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 5.5 Migration Utility and web services files to build a change-password application.
This chapter describes ACS 4.x to 5.5 migration and contains:

- Migration Methods, page 3-1
- About the Migration Utility, page 3-3
- Migrating from ACS 4.x to 5.5, page 3-3
- Multiple-Instance Migration Support, page 3-5
- Migrating Data, page 3-7

**Migration Methods**

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

- Migration Utility, page 3-1
- CSV Import Tool, page 3-2

**Migration Utility**

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

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

The Migration Utility migrates data from an ACS 4.x Windows machine to an ACS 5.5 machine. This process is different from the upgrade process for versions of ACS from 3.x to 4.x or for any 4.x upgrades. In the upgrade process, the ACS 4.x system works in the same way, without the need for administrative support. The migration process entails, in some cases, administrative support to consolidate and manually resolve data before you import the data to ACS 5.5.

The Migration Utility in ACS 5.5 supports multiple-instance migration that migrates all ACS 4.x servers in your deployment to ACS 5.5. To differentiate between several ACS 4.x instances, you can add a prefix. The prefix is used to retain server-specific identification of data elements and prevent duplication of object names for different servers.
Migrating an ACS 4.x deployment is a complex process and needs to be planned carefully. You need to consider the ACS 4.x replication hierarchy before you perform the migration.

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

**CSV Import Tool**

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

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

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

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

**Migration Recommendations**

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

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

The two phases of the migration process are:

- Analysis and Export
- Import

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

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

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

Note

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

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

Migrating from ACS 4.x to 5.5

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

- Multiple-Instance Migration, page 3-3
- Migration Phases for ACS 5.5, page 3-4
- Data Model Organization, page 3-4

Multiple-Instance Migration

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

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

ACS 5.5 follows a two-phase migration approach:

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

Analysis Phase

In this phase, an analysis of the existing ACS 4.x configuration is performed. It reports the possible migration issues and recommends resolutions, if any. Before running the Migration Utility, you must install ACS 4.x on the migration machine and restore the data. You can run the analysis tool on the data restored from the backup of an ACS 4.x server. You can run the analysis tool multiple times to make changes in the ACS 4.x configuration in the migration machine, if necessary.

Note

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

Migration Phase

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

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

Data Model Organization

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

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

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

- Model Organization, page 3-5
- Model Storage, page 3-5
- Replication Model, page 3-5
Model Organization
ACS 5.5 extends the Network Access Profile (NAP)-related functionality to a full policy-based authentication, authorization, and accounting (AAA) solution for both RADIUS and TACACS+.
Specific policy and authentication information, such as sets of RADIUS attributes, are not maintained within the user or group records, as in ACS 4.x. Instead, the entire set of 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 5.5 model.
• It consists of data that is not generated during run-time operation; for example, dynamic-user.

Replication Model
In ACS 5.5, multiple database instances of ACS 4.x are combined and migrated into a single database. In ACS 4.x, selective data replication can be defined such that different ACS instances maintain distinct subsets of the overall system configuration.
ACS 5.5 contains a consolidated database that is replicated to all the ACS instances. This consolidated database contains all the local configuration definitions from each of the ACS 4.x instances.
The ACS 5.5 data model is much more uniform than the ACS 4.x data model. The ACS 5.5 data model contains a single master instance, where all configuration changes are made. All subtending secondary instances maintain a full copy of the configuration and receive updates for all configuration changes.

Multiple-Instance Migration Support

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

Step 1
Choose an ACS 4.x instance to be migrated.
The primary ACS 4.x instance (if exists in the deployment) should be migrated first. Back up the chosen ACS 4.x instance.

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

Step 3
Run the migration process.

Step 4
After you complete the migration process for one ACS 4.x instance, continue with another instance or terminate the process.
If you restore any instance of ACS 4.x, it deletes the previous ACS 4.x instance data.
In the analysis and export phase, no changes are made with regard to multiple instance.
For example, the Migration Utility does not detect duplicate objects between different ACS 4.x instances. Duplicate and discrepant data objects that exist on multiple ACS 4.x instances are detected and reported in the migration import phase.
Figure 3-1 illustrates the multiple-instance migration process.

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

- Start
- Choose ACS 4.x instance to be migrated to ACS 5.x
- Backup ACS 4.x and restore on migration machine
- Run migration Process
- Have more services to migrate?
  - Yes
  - No -> End
Migrating Data

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

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

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

To migrate data:

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

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

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

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

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

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

See **Importing the ACS 4.x Data to ACS 5.5**, page 6-37.
Figure 3-2 illustrates the migration process.

**Object Group Selection**

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

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

- All Objects—All ACS objects that are supported in the migration process.
- All User Objects—Identity groups and all objects extracted from users
- All Device Objects—Network devices and NDGs
- Shared command sets
- Shared downloadable access control lists (DACLs)
• Master Keys—Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) master keys
• Shared RADIUS Authorization Components (RACs) and vendor-specific attributes (VSAs)

## Analysis and Export

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

In this phase, you identify:

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

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

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

The export process reports the following issues:

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

## Import

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

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

## Multiple-Instance Support

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

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

• Duplicate Object Reporting, page 3-10
• Object Name Prefix Per Instance, page 3-10
• Shared Object Handling, page 3-10
**Duplicate Object Reporting**
Duplicate data objects on multiple ACS 4.x instances are detected in the import phase. For most of the objects types, you can identify duplicates by name. Additionally, in the import report, information about duplicate objects is mentioned, see “Migration of ACS 4.x Objects” section on page 6-9.

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

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

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

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

This chapter describes:

- ACS 4.x to 5.5 Migration Version Support, page 4-1
- ACS 4.0 Migration Support, page 4-1
- ACS 4.x Appliance Support, page 4-2
- CSACS-1120 Series Appliance Support, page 4-2
- Remote Desktop Support, page 4-2
- Multiple-Instance Support, page 4-2
- ACS 4.x Elements Supported in the Migration Process, page 4-3
- ACS 4.x Elements Not Supported in the Migration Process, page 4-4
- User Interface, page 4-5

ACS 4.x to 5.5 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 5.5. See the 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. See the 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 can also run ACS 5.5 on this appliance. If you currently have ACS 4.2 installed on a CSACS-1120 appliance, and you want to install ACS 5.5 on the same appliance, you must first back up the ACS 4.2 data before proceeding to the ACS 5.5 installation.

To migrate data from ACS 4.2 to ACS 5.5 on a CSACS-1120 series appliance:

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Back up ACS 4.2 data on the appliance.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Restore the ACS 4.2 data on an intermediate migration machine.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Install ACS 5.5 on the appliance.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Migrate ACS 4.2 objects from the intermediate migration machine to ACS 5.5 that is installed on the appliance.</td>
</tr>
</tbody>
</table>

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 5.5, 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 5.5, 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 4-1 shows the ACS 4.x elements that the Migration Utility supports and the corresponding ACS 5.5 element.

<table>
<thead>
<tr>
<th>ACS 4.x Element</th>
<th>ACS 5.5 Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Client/Network Device</td>
<td>Network Device. See AAA Client/Network Device, page 6-10 for more information.</td>
</tr>
<tr>
<td>Internal User</td>
<td>Internal User. See Internal User, page 6-16 for more information.</td>
</tr>
<tr>
<td>User Defined Fields (within Interface Configuration section)</td>
<td>Identity Attributes/Internal User. See User Group, page 6-23 for more information.</td>
</tr>
<tr>
<td>User T+ Shell Exec Attributes</td>
<td>Identity Attributes/Internal User. See User Group, page 6-23 for more information.</td>
</tr>
<tr>
<td>Group T+ Shell Exec Attributes</td>
<td>Shell Profile. See User Group Policy Components, page 6-24 for more information.</td>
</tr>
<tr>
<td>User T+ Command Authorization Sets</td>
<td>Command Set. See User Group, page 6-23 for more information.</td>
</tr>
<tr>
<td>MAC Authentication Bypass (MAB) Addressed</td>
<td>Internal Host Database. See MAC Addresses and Internal Hosts, page 6-27 for more information.</td>
</tr>
<tr>
<td>Shared Downloadable Access Control List (DACL)</td>
<td>Downloadable ACL. See Shared DACL Objects, page 6-29 for more information.</td>
</tr>
<tr>
<td>EAP-FAST Master keys</td>
<td>EAP-FAST Master keys. See EAP-Fast Master Keys and the Authority ID, page 6-34 for more information.</td>
</tr>
<tr>
<td>Customer Vendor-Specific Attributes</td>
<td>Customer VSAs. See Customer VSAs, page A-5 for more information.</td>
</tr>
</tbody>
</table>

**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
User Interface

This section describes the end user interface for the ACS 5.5 Migration Utility.

CLI-Based Migration Utility

ACS 5.5 supports a CLI-based Migration Utility. For more information on the migration settings, see Running the Migration Utility, page 6-2.

Phases of the CLI-Based Migration Utility

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

- Settings, page 4-5
- Object Group Selection, page 4-5
- Operation Selection, page 4-6

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” section on page 6-2.

The settings are of two types:

- ACS 5.5 Identification and Credentials—IP address or hostname of the ACS 5.5 server to which the data is being migrated. The administrator username and password that are used to import data in the ACS 5.5 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 5.5, 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” section on page 6-9.

For a detailed procedure on selecting the available options, see “Running the Migration Utility” section on page 6-2.
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” section on page 6-40.
Migration Utility Setup and Installation

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

- Migration Preinstallation Considerations, page 5-1
- System Requirements, page 5-2
- ACS Software Accessory Kit DVDs, page 5-3
- Security Considerations, page 5-4
- Accessing the Migration Utility, page 5-4
- Data Migration and Deployment Scenarios, page 5-5
- Data Migration Between Platforms, page 5-6

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 5.5 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 5.5 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.
  
- 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.
Use the migration machine when you make any changes to the ACS 4.x data.

- Perform a full database backup on the ACS 5.5 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 5.5.
- Ensure that you:
  - Install ACS 5.5 on the target machine.
  - Use a compatible ACS 5.5 license.
  - Establish network connection between the migration machine and ACS 5.5 server.
- Back up your ACS 5.5 database before you run the Import phase.
- Enable the migration interface on the ACS 5.5 server. For more information on how to enable the migration interface and run the Migration Utility, see Chapter 6, “Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5”.

System Requirements

Your ACS machines must meet the system requirements described in Table 5-1. All documents are available on Cisco.com.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The machine must have 2 GB of RAM.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>ACS 5.5 target machine</td>
<td>See the following:</td>
</tr>
<tr>
<td></td>
<td>- Installation and Setup Guide for ACS 5.5</td>
</tr>
<tr>
<td></td>
<td>- Cisco Application Deployment Engine (ADE) 1010 and 2120 Series Appliance Hardware Installation Guide.</td>
</tr>
<tr>
<td></td>
<td>- Cisco Application Deployment Engine (ADE) 2130 and 2140 Series Appliance Hardware Installation Guide.</td>
</tr>
</tbody>
</table>
# ACS Software Accessory Kit DVDs

Table 5-2 describes the ACS software accessory kit DVDs.

<table>
<thead>
<tr>
<th>DVDs</th>
<th>Description</th>
<th>Part Number</th>
</tr>
</thead>
</table>
| Cisco Secure Access Control System-Installation and Recovery DVD, Version 5.5 | Use this DVD to:  
  - Install the ACS 5.5_ISO image.  
  - Install the Application Upgrade Bundle.  
  - Install VMware.  
  - Recover the ACS 5.5 appliance.  
  - Reset the password. | 80-10897-01  |
| Cisco Secure Access Control System-Upgrade and Migration_Documentation DVD, Version 5.5 | Use this DVD to:  
  - ACS 5.1 Upgrade Package (upgrade from 5.0 to 5.1).  
  - ACS 5.2 Upgrade Package (upgrade from 5.1 to 5.2)  
  - ACS 5.5 Upgrade Package (upgrade from 5.3/5.4 to 5.5)  
  - 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 4.1.1 before migration.  
  - Documentation:  
    - ACS_5.5_CLI_Reference_Guide.pdf  
    - ACS_5.5_Installation_and_Upgrade_Guide.pdf  
    - ACS_5.5_5x5_Pointer_Card_ChinaRoHS.pdf  
    - ACS_5.5_Migration_Guide.pdf  
    - ACS_5.5_Regulatory_Compliance_and_Safety_Information.pdf  
    - ACS_5.5_SDT_Guide.pdf  
    - ACS_5.5_Software_Developer’s_Guide.pdf  
    - ACS_5.5_User_Guide.pdf | 80-10898-01  |
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:

- **Step 1** Make a backup from any supported version of the ACS 4.x appliance.
- **Step 2** Restore the appliance backup on the same supported version of the ACS 4.x software.
- **Step 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 5.5. 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 5.5 web interface.

To download migration application files:

- **Step 1** Choose **System Administration > Downloads > Migration Utility**. The Migration from 4.x page appears.
- **Step 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 5.5, available in the migration software accessory kit, to download the *migration.zip* file.

**Related Topics**

- ACS Software Accessory Kit DVDs, page 5-3
- Chapter 6, “Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5”

### 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 5-1.
Data Migration and Deployment Scenarios

The Migration Utility migrates ACS 4.x objects to ACS 5.5. 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 5-5
- Guidelines for Data Migration in a Distributed Environment, page 5-5

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 6-45.

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:

Step 1  Back up the primary ACS appliance and restore it on the migration machine.
Step 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 5.5 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 5.5, the startup process takes about 15 minutes before ACS 5.5 is available for use. The behavior of ACS 5.5 for data migration beyond 400,000 users and 200,000 devices is unknown.

**Data Migration Between Platforms**

Figure 5-2 shows the data migration flow between platforms. See Chapter 6, “Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5.”
Introduction

This chapter contains information to migrate data from ACS 4.x to ACS 5.5. Before you begin, you must follow the setup, backup, and installation instructions in Chapter 5, “Migration Utility Setup and Installation.”

Before you begin migration, ensure that you have enabled the migration interface on the ACS 5.5 server.

From the command line interface, enter:

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

To verify that the migration interface is enabled on the ACS 5.5 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 5.5 for more information.
Running the Migration Utility

To run the Migration Utility:

**Step 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.

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

Example 6-1 shows the prompts that appear when you run the Migration Utility.

---

Example 6-1  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]

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]
Running the Migration Utility

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

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 6-1 on page 6-5.
- Migration user preferences. See Table 6-2 on page 6-6.
- Migration groups. See Table 6-3 on page 6-8.
- Migration phases. See Table 6-4 on page 6-9.

Table 6-1 Migration Script Environment Information

<table>
<thead>
<tr>
<th>Script Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use saved user defaults? [yes]</td>
<td>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 5.5 target machine.</td>
</tr>
<tr>
<td>Make sure that the database is running.</td>
<td>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 5.5 target machine from the ACS 4.x migration machine. Access the web interface to verify that the ACS 5.5 machine is available.  The migration interface is enabled after you run the \acs config-web-interface migration enable \command.</td>
</tr>
<tr>
<td>Enter ACS 5 IP address or hostname: [nn.nn.nnn.nnn]</td>
<td>Enter the IP address or the hostname for the ACS 5.5 target machine. You migrate the ACS 4.x data to the ACS 5.5 target machine.</td>
</tr>
<tr>
<td>Enter ACS 5 administrator username: [test]</td>
<td>Enter the username for the ACS 5.5 target machine. ACS 5.5 supports only admin users.  ACS 5.5 supports migration operation with any ACS administrator with a recovery superadmin role.</td>
</tr>
<tr>
<td>Enter ACS 5 password:</td>
<td>Enter the password for the ACS 5.5 target machine.</td>
</tr>
<tr>
<td>Change user preferences? [no]</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 6-2 Migration Script User Preferences

<table>
<thead>
<tr>
<th>Script Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Groups</td>
<td>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.</td>
</tr>
<tr>
<td>Network Device Groups</td>
<td>The default name for a Network Device Group (NDG) is Migrated NDGs. Type a new name and press Enter to change the default name.</td>
</tr>
<tr>
<td>Consolidation Prefix</td>
<td>Enter a prefix that you want to add to the consolidated objects.</td>
</tr>
<tr>
<td>Users</td>
<td>The default password for external users for the User object. Type a new password and press Enter to change the default password. ACS 5.5 supports authentication for internal users against the internal database only. ACS 4.x users who were configured to use an external database for authentication are migrated with a default authentication password. You can configure the default password in ACS 5.5.</td>
</tr>
<tr>
<td>Disabled Group Users</td>
<td>Users and hosts who are associated with disabled user groups are migrated under one group as disabled.</td>
</tr>
<tr>
<td>Network Devices</td>
<td>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.</td>
</tr>
<tr>
<td>DACL name construction</td>
<td>Select a naming convention to be used for the migrated ACS 4.x DACL: 1 - DACL_ACL Name 2 - ACL Name</td>
</tr>
<tr>
<td>Save user deafults?</td>
<td>The default value is yes. Enter no if you do not want to preserve the setting that you used in this session.</td>
</tr>
<tr>
<td>Enter ACS 4.x Server ID:</td>
<td>Enter the ACS 4.x server ID from which the data is to be migrated.</td>
</tr>
<tr>
<td>Add server specific migration prefixes?</td>
<td>The default is no. Enter yes to add prefix to each 4.x server name.</td>
</tr>
</tbody>
</table>
## Migration Script Sections

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]

### Table 6-2 Migration Script User Preferences (continued)

<table>
<thead>
<tr>
<th>Script Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can add a global prefix to all migrated objects from this server. Enter a global prefix: [s1]</td>
<td>Enter a prefix you want to add to all the objects migrated from one particular server.</td>
</tr>
<tr>
<td>Use special prefixes for specific object types? [no] yes ** To input an empty prefix, enter the keyword EMPTY.</td>
<td>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.</td>
</tr>
<tr>
<td>User Attributes Prefix: You can add an additional prefix to the user attributes. Enter a prefix to add to these objects: [s1]</td>
<td>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.</td>
</tr>
<tr>
<td>Network Device Prefix: You can add an additional prefix to the network devices names. Enter a prefix to add to these objects: [s1]</td>
<td>The default is the value entered for global prefix. Enter a prefix if you want to add special prefix for all migrated network devices.</td>
</tr>
<tr>
<td>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]</td>
<td>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.</td>
</tr>
<tr>
<td>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]</td>
<td>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.</td>
</tr>
<tr>
<td>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]</td>
<td>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.</td>
</tr>
<tr>
<td>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]</td>
<td>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.</td>
</tr>
<tr>
<td>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]</td>
<td>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.</td>
</tr>
<tr>
<td>RAC Prefix: Existing RAC will be migrated with an optional prefix. Enter the prefix to add to such objects: [s1]</td>
<td>The default is the value entered for global prefix. Enter a prefix if you want to add special prefix for all migrated RACs.</td>
</tr>
<tr>
<td>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]</td>
<td>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.</td>
</tr>
<tr>
<td>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]</td>
<td>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.</td>
</tr>
<tr>
<td>Save server migration prefixes? [yes]</td>
<td>The default is yes. Enter no if you do not want to save the server migration prefixes.</td>
</tr>
</tbody>
</table>
### Table 6-2 Migration Script User Preferences (continued)

<table>
<thead>
<tr>
<th>Script Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show full report on screen?[yes]</td>
<td>The default value is yes. Enter no if you do not want to view the log information on screen.</td>
</tr>
<tr>
<td>Update RADIUS dictionary cache?[no]</td>
<td>Used to cache the current ACS 5.5 RADIUS dictionary. If you migrate a vendor that was already migrated and deleted in ACS 5.5, 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.</td>
</tr>
</tbody>
</table>

### Table 6-3 Migration Script Object Groups

<table>
<thead>
<tr>
<th>Script Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the ACS 4.x Configuration groups to be migrated: 1 - ALLObjects 2 - AllUsersObjects 3 - AllDevicesObjects 4 - SharedCommandSet 5 - SharedDACLObject 6 - MasterKeys 7 - SharedRACObjectsWithVSA</td>
<td>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:</td>
</tr>
<tr>
<td>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</td>
<td>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.</td>
</tr>
</tbody>
</table>
Migration of ACS 4.x Objects

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

- AAA Client/Network Device, page 6-10
- NDG, page 6-14
- Internal User, page 6-16
- User Group, page 6-23
- User Group Policy Components, page 6-24
- Shared DACL Objects, page 6-29
- Shared RACs, page 6-30
- RADIUS VSAs, page 6-32
- EAP-Fast Master Keys and the Authority ID, page 6-34

Migration Script Phases

<table>
<thead>
<tr>
<th>Script Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose one of the following:</td>
<td>Migration Utility options:</td>
</tr>
<tr>
<td>1 - AnalyzeAndExport</td>
<td>• 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.</td>
</tr>
<tr>
<td>2 - Import</td>
<td>If data passes the Analysis phase, it can be exported and imported to ACS 5.5. See Migration of ACS 4.x Objects, page 6-9.</td>
</tr>
<tr>
<td>3 - CreateReportFiles</td>
<td>Ensure that you back up your ACS 5.5 database.</td>
</tr>
<tr>
<td>4 - Exit</td>
<td>• 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 5.5. See Importing the ACS 4.x Data to ACS 5.5, page 6-37.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>The config folder in the migration directory contains the full and summary reports. See Printing Reports and Report Types, page 6-40.</td>
</tr>
<tr>
<td></td>
<td>• Exit—Choose option 4 to exit the Migration Utility or if you want to migrate another ACS 4.x instance.</td>
</tr>
</tbody>
</table>

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.
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 5.5.

This section contains:
- Data Mapping, page 6-10
- Analysis and Export, page 6-11
- Import, page 6-13
- Multiple-Instance Support, page 6-14

Data Mapping

Table 6-5 shows the data mapping between ACS 4.x and ACS 5.5, for the AAA client or Network Devices.

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Client Hostname</td>
<td>Name</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>There is no description to be retrieved from ACS 4.x. A predefined description of Migrated is used for all the migrated devices.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Shared Secret</td>
<td>ACS 5.5 records contains separate fields for RADIUS and TACACS+ shared secrets. The specific field set in an ACS 5.5 record depends on the setting for the Authentication using field.</td>
</tr>
<tr>
<td>Network Device Group</td>
<td>Network device group under All migrated NDGs</td>
<td>—</td>
</tr>
<tr>
<td>Authentication using</td>
<td>Selection of either RADIUS or TACACS+ options</td>
<td>ACS 4.x has a list of all the supported RADIUS vendors. This information is not retained in ACS 5.5. If a RADIUS vendor is selected, it is marked as Authenticating using RADIUS.</td>
</tr>
<tr>
<td>AAA Client IP Address</td>
<td>IP</td>
<td>Representations are different.</td>
</tr>
<tr>
<td>Single Connect TACACS+ AAA Client (Record stop in accounting on failure)</td>
<td>Single Connect Device</td>
<td>—</td>
</tr>
<tr>
<td>Legacy TACACS+ Single Connect support for this AAA client</td>
<td>Legacy TACACS+ Single Connect Support</td>
<td>Available only in 4.2 cumulative patch 1 and 4.1.4.13 patch 10 and higher.</td>
</tr>
<tr>
<td>TACACS+ Draft compliant Single Connect support for this AAA client</td>
<td>TACACS+ Draft Compliant Single Connect Support</td>
<td>Available only in ACS 4.2 cumulative patch 1 and ACS 4.1.4.13 patch 10 and higher.</td>
</tr>
</tbody>
</table>
Table 6-5      Data Mapping for AAA Client or Network Devices (continued)

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Log Update/Watchdog Packets from this AAA Client (the only option for servers)</td>
<td>—</td>
<td>Not supported in ACS 5.5.</td>
</tr>
<tr>
<td>• Log RADIUS Tunneling Packets from this AAA Client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Replace RADIUS Port info with Username from this AAA Client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Match Framed-IP-Address with user IP address for accounting packets from this AAA Client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Encryption Key</td>
<td>keyEncryptionKey</td>
<td>The key length depends on the following display type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HEX—The key length is 32 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASCII—The key length is 16 characters</td>
</tr>
<tr>
<td>Message Authenticator Code Key</td>
<td>messageAuthenticatorCodeKey</td>
<td>The key length depends on the following display type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HEX—The key length is 40 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASCII—The key length is 20 characters</td>
</tr>
<tr>
<td>Key Input Format</td>
<td>Key Input Format</td>
<td>Boolean</td>
</tr>
</tbody>
</table>

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 5.5) definitions:

• In ACS 5.5, 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 5.5, 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 5.5, 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, page 6-12
• Overlapping IP Addresses, page 6-12
• IP Address Translation, page 6-12
• IP Subnets Limit, page 6-12
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 5.5, 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 5.5 requirements.

For example:

Network device AA: IP address = 23.8.23.*, 45.67.*, 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 5.5 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 5.5.

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 5.5 format. Table 6-6 describes the ACS 4.x attributes that can be modified to conform to ACS 5.5 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 6-6 describes the ACS 4.x attributes that can be modified to conform to ACS 5.5 limitations.
Chapter 6 Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5

Migration of ACS 4.x Objects

Import

The Unified Device Name setting is used during import of network devices. In ACS 5.5, configuration options are available to determine the name of the new device in ACS 5.5, 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 5.5:

- 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 5.5 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 5.5, a default description field called Migrated is created.

<table>
<thead>
<tr>
<th>Attribute Name in 4.x</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication using</td>
<td>Any selection for a specific RADIUS vendor is translated to Authenticate Using RADIUS. For example, RADIUS (Cisco Aironet) is translated to RADIUS.</td>
</tr>
<tr>
<td>AAA Client IP Address</td>
<td>ACS 5.5 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 5.5.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>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.</td>
</tr>
<tr>
<td>Key Encryption Key</td>
<td>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.</td>
</tr>
<tr>
<td>Message Authenticator Code Key</td>
<td>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.</td>
</tr>
</tbody>
</table>
Multiple-Instance Support

In ACS 5.5, 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 5.5.

NDG

To facilitate migration of the ACS 4.x NDG definitions, an additional NDG hierarchy has been created in ACS 5.5.

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 5.5.

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 5.5, the NDGs are labels that can be attached to the network device definitions and do not contain data. If a value is set for the shared secret in an ACS 4.x NDG, this value is extracted to set the value for each network device that is associated with the group.

This section contains:

- Data Mapping, page 6-14
- Analysis and Export, page 6-15
- Import, page 6-15
- Multiple-Instance Support, page 6-16

Data Mapping

Table 6-7 shows the data mapping between ACS 4.x and ACS 5.5 for the NDGs.

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Device Group Name</td>
<td>Name</td>
<td>—</td>
</tr>
<tr>
<td>—</td>
<td>Description</td>
<td>There is no description to be retrieved from ACS 4.x. A predefined description of Migrated is used for all the migrated devices.</td>
</tr>
</tbody>
</table>
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 5.5, 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 5.5, 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 6-16
- **Multiple-Instance Support**, page 6-18
- **User Data Configuration and User Mapping**, page 6-18
- **User Shell Command Authorization**, page 6-20
- **Shell Exec Parameters**, page 6-22

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 6-16
- **Analysis and Export**, page 6-17
- **Import**, page 6-18

**Data Mapping**

Table 6-8 shows the user interface data mapping of ACS 4.x with ACS 5.5 for internal users.
Chapter 6  Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5

Migration of ACS 4.x Objects

Table 6-8  Data Mapping for Internal Users

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Account Disable</td>
<td>• Status:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disable Account if Date Exceeds</td>
<td></td>
</tr>
</tbody>
</table>
| Description                 |                             | There is no description to be retrieved from ACS 4.x. The description used in ACS 5.5 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. Users 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 5.5.

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 “This 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 5.5. 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 5.5 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 5.5. 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 5.5, these fields are migrated so that equivalent user attributes can be created and then populated for each user.

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

This section contains:

- Data Mapping, page 6-18
- Analysis and Export, page 6-19
- Import, page 6-19
- Multiple-Instance Support, page 6-19

Data Mapping

Table 6-9 shows the user interface data mapping between ACS 4.x and ACS 5.5 for User Data Configuration and User Mapping.
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 5.5, 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 5.5, the attribute names are as follows:

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

Multiple-Instance Support
In ACS 5.5, 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 5.5 contains the following attributes:

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>—</td>
<td>If enabled, the corresponding field name is extracted; otherwise it is ignored.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Attribute</td>
<td>—</td>
</tr>
<tr>
<td>—</td>
<td>Description</td>
<td>There is no description to be retrieved from ACS 4.x. A predefined description of \textit{Attribute added as part of the migration process} is used for all attributes.</td>
</tr>
</tbody>
</table>
Migration of ACS 4.x Objects

- 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 5.5 (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 5.5 (and was migrated in a previous run of the migration) is associated to the existing user attribute.

In ACS 5.5, 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 5.5, user1 will contain the attributes, global1_city, global1_Description, global1_Real Name, global2_city, global2_country and global2_state.

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

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

User Shell Command Authorization

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

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

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

This section contains:
- Data Mapping, page 6-21
- Analysis and Export, page 6-21
- Import, page 6-21
- Multiple-Instance Support, page 6-22
Data Mapping

Table 6-10 shows the user interface data mapping between ACS 4.x and ACS 5.5 for the user shell command authorization.

Table 6-10  Data Mapping for User Shell Command Authorization

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unmatched Cisco IOS Commands (Permit / Deny)</td>
<td>Permit any command that is not in the list of commands.</td>
<td>—</td>
</tr>
<tr>
<td>Command, followed by list of arguments each of format: permit / deny &lt; arguments &gt;</td>
<td>List of commands in the format: permit / deny &lt;command&gt; &lt;arguments&gt;</td>
<td>—</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
<td>—</td>
</tr>
<tr>
<td>Unlisted arguments (Permit / Deny)</td>
<td>Additional entry after each list of arguments for specific command, in the format: permit / deny &lt;command&gt;</td>
<td>—</td>
</tr>
</tbody>
</table>

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 5.5, 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 5.5 command set that is migrated from a user definition.

To import a user command set:

**Step 1** Create the cmd-set user attribute.

**Step 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.

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

c. Create the migrated command set.

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

In ACS 5.5, 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 5.5 as attributes of the user record. If one of these attributes is in use for any of the migrated user records, it is created as a user attribute. The value is set in the corresponding attribute in the migrated user definition.

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

This section contains:

- Data Mapping, page 6-22
- Analysis and Export, page 6-23
- Import, page 6-23
- Multiple-Instance Support, page 6-23

Data Mapping

Table 6-11 shows the data mapping between ACS 4.x and ACS 5.5 for the user shell attribute. All attributes, except the Max Privilege attribute, are taken from the TACACS+ shell (exec) settings.

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS+ Enable Control: Max Privilege for any AAA Client</td>
<td>Max_priv_lvl (unsigned integer 32)</td>
<td>—</td>
</tr>
<tr>
<td>Access control list</td>
<td>ACL (string)</td>
<td>—</td>
</tr>
<tr>
<td>Auto command</td>
<td>Autocmd (string)</td>
<td>—</td>
</tr>
<tr>
<td>Callback line</td>
<td>Callback-line (string)</td>
<td>—</td>
</tr>
<tr>
<td>Callback rotary</td>
<td>Callback-rotary (string)</td>
<td>—</td>
</tr>
<tr>
<td>Idle time</td>
<td>Idle time (unsigned integer 32)</td>
<td>—</td>
</tr>
<tr>
<td>No callback verify</td>
<td>No callback-verify (Boolean)</td>
<td>—</td>
</tr>
<tr>
<td>No escape</td>
<td>No escape (Boolean)</td>
<td>—</td>
</tr>
<tr>
<td>No hangup</td>
<td>No hangup (Boolean)</td>
<td>—</td>
</tr>
<tr>
<td>Privilege level</td>
<td>Priv_lvl (unsigned integer 32)</td>
<td>—</td>
</tr>
<tr>
<td>Timeout</td>
<td>Conn-timeout (unsigned integer 32)</td>
<td>—</td>
</tr>
</tbody>
</table>
Analysis and Export

ACS 5.5 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 5.5. 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 5.5, this value is set in a user attribute associated with the user in ACS 5.5. If the attribute is not defined in ACS 4.x, it is left blank in ACS 5.5.

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 5.5 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 5.5 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 5.5, every user shell attribute that gets added to the dictionary also gets added to all the users.

User Group

In ACS 5.5, 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 5.5, 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, page 6-24
- Import, page 6-24
- Multiple-Instance Support, page 6-24
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 5.5, 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 5.5, 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, page 6-25
• Group Shell Exec, page 6-25
• MAC Addresses and Internal Hosts, page 6-27
• Shared Shell Command Authorization Sets, page 6-28

Group Command Set

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

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

Group Shell Exec

This section contains:
• Data Mapping, page 6-25
• Analysis and Export, page 6-26
• Import, page 6-26
• Multiple-Instance Support, page 6-26

Data Mapping

Table 6-12 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>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Options: Max Privilege for any AAA client</td>
<td>Maximum Privilege Level</td>
<td>—</td>
</tr>
<tr>
<td>Access control list</td>
<td>Access Control List</td>
<td>—</td>
</tr>
<tr>
<td>Auto command</td>
<td>Auto Command</td>
<td>—</td>
</tr>
<tr>
<td>Callback line</td>
<td>Callback Line</td>
<td>—</td>
</tr>
<tr>
<td>Callback rotary</td>
<td>Callback Rotary</td>
<td>—</td>
</tr>
<tr>
<td>Idle time</td>
<td>Idle time</td>
<td>—</td>
</tr>
<tr>
<td>No callback verify</td>
<td>No Callback Verify</td>
<td>—</td>
</tr>
<tr>
<td>No escape</td>
<td>No Escape</td>
<td>—</td>
</tr>
<tr>
<td>No hangup</td>
<td>No Hang Up</td>
<td>—</td>
</tr>
<tr>
<td>Privilege level</td>
<td>Default Privilege Level</td>
<td>—</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout</td>
<td>—</td>
</tr>
</tbody>
</table>
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 5.5 object:

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

In ACS 5.5, 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-*"

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 5.5, 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 5.5 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 5.5, 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 5.5, 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, page 6-27
- Analysis and Export, page 6-27
- Multiple-Instance Support, page 6-28

Data Mapping

Table 6-13 shows the data mapping between ACS 4.x and ACS 5.5 for MAC addresses and internal hosts.

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Addresses stored in authentication section of a NAP</td>
<td>MAC Address</td>
<td>Can contain a list of addresses. An internal host definition is created for each address that is defined.</td>
</tr>
<tr>
<td>—</td>
<td>Status</td>
<td>All migrated entries are set as enabled.</td>
</tr>
<tr>
<td>—</td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td>User Group</td>
<td>Identity Group</td>
<td>Set to reference the same identity group, located in the ACS 5.5 identity group hierarchy.</td>
</tr>
</tbody>
</table>

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 5.5, 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, page 6-28
- Analysis and Export, page 6-29
- Multiple-Instance Support, page 6-29

**Data Mapping**
Table 6-14 shows the data mapping between ACS 4.x and ACS 5.5 for shared shell command authorization sets.

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name</td>
<td>—</td>
</tr>
<tr>
<td>Description</td>
<td>Description</td>
<td>—</td>
</tr>
<tr>
<td>Unmatched Commands</td>
<td>Check box labeled Permit any command that is not in the table</td>
<td>—</td>
</tr>
<tr>
<td>• Permit</td>
<td>Entries in command table:</td>
<td></td>
</tr>
<tr>
<td>• Deny</td>
<td>• Grant: Permit / Deny</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Command</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Arguments</td>
<td></td>
</tr>
<tr>
<td>Command, followed by the list of arguments each of format: permit / deny &lt;arguments&gt;</td>
<td>Unlisted arguments Additional entry after each list of arguments for a specific command in the format: permit / deny &lt;command&gt;</td>
<td>—</td>
</tr>
<tr>
<td>• Permit</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>• Deny</td>
<td>—</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 6  Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5

Migration of ACS 4.x Objects

### 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 5.5, 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 5.5 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 5.5.

This section contains:

- Data Mapping, page 6-29
- Analysis and Export, page 6-30
- Import, page 6-30
- Multiple-Instance Support, page 6-30

### Data Mapping

Table 6-15  shows the data mapping between ACS 4.x and ACS 5.5 for shared DACL objects.

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name</td>
<td>Configuration options determine the value used for Name.</td>
</tr>
<tr>
<td>Description</td>
<td>Description</td>
<td>—</td>
</tr>
<tr>
<td>ACL Definitions</td>
<td>Downloadable ACL Content</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>GenID</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

Tip

If the ACL name is used, multiple ACL records could be created on ACS 5.5 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 5.5, 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 5.5.

In ACS 4.x, an attribute is identified in the GUI as a combination of the vendor name and the attribute name. In ACS 5.5, it is defined as a combination of the dictionary and attribute name. Internally, the vendor or dictionary and attribute are identified by IDs that are, in turn, the values that are used while forming the RADIUS response.
This section contains:

- **Data Mapping, page 6-31**
- **Analysis and Export, page 6-31**
- **Import, page 6-31**
- **Multiple-Instance Support, page 6-32**

### Data Mapping

Table 6-16 shows the data mapping between ACS 4.x and ACS 5.5 for the shared RACs.

**Table 6-16 Data Mapping for Shared RADIUS Authorization Components**

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name</td>
<td>Configuration options determine the value used for Name.</td>
</tr>
<tr>
<td>Description</td>
<td>Description</td>
<td>—</td>
</tr>
<tr>
<td>List of vendor / attribute / value triplets</td>
<td>List of dictionary / attribute / value</td>
<td>The list of attributes appears in the manually entered section of the RADIUS Attributes tab of the Authorization Profile.</td>
</tr>
</tbody>
</table>

### 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 5.5, 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 5.5, 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 5.5, 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 5.5 for each vendor. There are two possible cases during this identification process:

- If the vendor does not exist in the ACS 5.5 dictionary, all the vendor attributes are migrated.
- If the vendor exists in the ACS 5.5 dictionary, only attributes that are not defined in ACS 5.5 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 5.5 this is displayed as Gold.

Table 6-17 shows the mapping of Aire-QoS-Level (2) values between ACS 4.1.x and ACS 5.5.

<table>
<thead>
<tr>
<th>Values in ACS 4.1.x</th>
<th>Values in ACS 5.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bronze (0)</td>
<td>Silver (0)</td>
</tr>
<tr>
<td>Silver (1)</td>
<td>Gold (1)</td>
</tr>
<tr>
<td>Gold (2)</td>
<td>Platinum (2)</td>
</tr>
<tr>
<td>Platinum (3)</td>
<td>Bronze (3)</td>
</tr>
<tr>
<td>Uranium (4)</td>
<td>Uranium (4)</td>
</tr>
</tbody>
</table>

Description of the enumerated values of Cisco Airespace attribute Aire-QoS-Level(2), between ACS 4.2 and ACS 5.5 is the same.
This section contains:

- Data Mapping, page 6-33
- Analysis and Export, page 6-34
- Import, page 6-34

### Data Mapping

Table 6-18 shows the data field mapping between ACS 4.x and ACS 5.5 for RADIUS vendors.

#### Table 6-18  Data Mapping for RADIUS Vendors

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Name</td>
<td>Name</td>
<td>—</td>
</tr>
<tr>
<td>—</td>
<td>Description</td>
<td>Generated during migration.</td>
</tr>
<tr>
<td>Vendor ID</td>
<td>Vendor ID</td>
<td>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</td>
</tr>
</tbody>
</table>

Table 6-19 shows the data field mapping between ACS 4.x and ACS 5.5 for RADIUS VSAs.

#### Table 6-19  Data Mapping for RADIUS VSAs

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name</td>
<td>ACS 5.5 has a very short maximum name length.</td>
</tr>
<tr>
<td>—</td>
<td>Description</td>
<td>Generated during migration.</td>
</tr>
<tr>
<td>Attribute Number</td>
<td>Attribute Number</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Profile            | Direction          | IN — 1 (Inbound)  
|                    |                    | OUT — 2 (Outbound)  
|                    |                    | IN OUT — 3 (Both)  |
| Type               | ValueType          | Syntax ID is mapped. |
Chapter 6    Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5

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 5.5. There are two cases for analysis:

- Generally, for ACS 4.x supported vendors, the dictionary in ACS 5.5 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 5.5 is not altered during migration. A warning is displayed for such attributes.
  - An attribute not defined in ACS 5.5, 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 5.5, are migrated without any analysis warning.

Note

Difference between ACS 4.x and ACS 5.5 VSA attributes (profile, name, type) are reported in the Analysis report.

Import

All the exported VSAs are imported to ACS 5.5.

EAP-Fast Master Keys and the Authority ID

In ACS 5.5, 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 5.5, and they are migrated to different IM objects. ACS 4.x stores the authority ID per node, whereas ACS 5.5 stores the authority ID only in the primary database and then applies it to the entire deployment.

This section contains:
- Data Mapping, page 6-34
- Analysis and Export, page 6-35
- Import, page 6-35
- Multiple-Instance Support, page 6-35

Data Mapping

Table 6-20 shows the data mapping between ACS 4.x and ACS 5.5 for EAP-FAST master keys and the authority ID.

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Key ID</td>
<td>Identifier</td>
<td>ACS 4.x internal ID</td>
</tr>
<tr>
<td>Encryption key</td>
<td>EncryptionKey</td>
<td>Byte 32</td>
</tr>
<tr>
<td>Authentication key</td>
<td>AuthenticationKey</td>
<td>Byte 32</td>
</tr>
</tbody>
</table>
Migration of ACS 4.x Objects

Chapter 6      Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5

Migration of ACS 4.x Objects

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 5.5, 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 5.5, 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 5.5, 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.

Table 6-20 Data Mapping for EAP-FAST Master Keys and the Authority ID (continued)

<table>
<thead>
<tr>
<th>4.x Attribute Name</th>
<th>5.5 Attribute Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cipher suite</td>
<td>Cipher</td>
<td>—</td>
</tr>
<tr>
<td>Creation Time</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Expiration Time (TTL)</td>
<td>Expiration Time</td>
<td>The Expiration time is calculated by adding the Current time and the Retired master key TTL.</td>
</tr>
</tbody>
</table>

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 of ACS 4.x Data

Choose option 1 in the Migration Utility to run AnalyzeAndExport. See Example 6-1 on page 6-2. 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 6-37.

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 D-3.

This section contains:

- Consolidating Data, page 6-37
- Issues Resulting from the Analysis and Export Phase, page 6-37

Example 6-2 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.

Example 6-2 AnalyzeAndExport 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 Appendix A, “ACS 5.5 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 5.5. This object can then be referenced by ACS 5.5 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 5.5, you can define policies such that they incorporate the migrated command set information. See the User Guide for Cisco Secure Access Control System 5.5 for more details on ACS 5.5 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 5.5. 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 5.5 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 5.5 machine.

Importing the ACS 4.x Data to ACS 5.5

Choose option 2 in the Migration Utility to run Import. See Example 6-1 on page 6-2. 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 5.5 import fails, restore your ACS 5.5 database.

Example 6-3 shows a sample progress report from the Import phase. This phase generates two reports:

- Example 6-4 shows the Import Summary Report.
- Example 6-5 shows the Import Report.
Example 6-3  Sample 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.

Example 6-4  Import 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

Example 6-5  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 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 Example 6-1 on page 6-2. You can import multiple ACS 4.x instances to ACS 5.5. Example 6-6 shows the prompts that appear if you decide to migrate multiple instances.

**Example 6-6  Importing Multiple Instances**

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

Would you like to migrate another ACS4.x server? [no]
yes
Enter ACS 4.x Server 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 5.5.

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 5.5 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 Example 6-1 on page 6-2. The config folder in the migration directory contains the Migration Utility reports. In the config folder, a new folder with the same name as the server ID is created for each ACS 4.x server that you migrate.

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

- Analyze and Export Summary Report, page 6-42
- Analyze and Export Full Report, page 6-42
- Import Summary Report, page 6-43
- Import Full Report, page 6-44
- Validating Import, page 6-45
- Summary Report, page 6-45
- Full Report, page 6-46
Table 6-21 lists the migration phases and the reports that are generated in each phase.

<table>
<thead>
<tr>
<th>Migration Phase</th>
<th>Reports Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnalyzeandExport</td>
<td>• AnalyzeAndExport_server ID_Summary_report.csv</td>
</tr>
<tr>
<td></td>
<td>• AnalyzeAndExport_server ID_full_report.csv</td>
</tr>
<tr>
<td>Import</td>
<td>• ImportSummary_server ID_report.csv</td>
</tr>
<tr>
<td></td>
<td>• Importfull_server ID_report.csv</td>
</tr>
</tbody>
</table>

Table 6-22 describes the Migration Utility reports.

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

Figure 6-1 shows the Analyze and Export Summary Report. Table 6-23 contains the Analyze and Export Summary Report column definitions.

Table 6-23 Analyze and Export Summary Report Column Definitions

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server ID</td>
<td>Name of the server.</td>
</tr>
<tr>
<td>Phase</td>
<td>Name of the migration phase.</td>
</tr>
<tr>
<td>Element Name</td>
<td>Name of the ACS object type to be migrated.</td>
</tr>
<tr>
<td>Total Elements</td>
<td>Total number of elements.</td>
</tr>
<tr>
<td>Total Migratable</td>
<td>Total number of elements that can be migrated.</td>
</tr>
<tr>
<td>Total with Issues</td>
<td>Total number of elements that have issues.</td>
</tr>
<tr>
<td>Comment</td>
<td>Message indicating the status of the ACS object.</td>
</tr>
</tbody>
</table>

Analyzing and Exporting Full Report

Figure 6-2 shows the Analyze and Export Full Report. Table 6-24 contains the Analyze and Export Full Report column definitions.
Chapter 6  Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5

Printing Reports and Report Types

Figure 6-2  Analyze and Export Full Report

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Server ID</td>
<td>Phase</td>
<td>Element Name</td>
<td>Name</td>
<td>Operation Code</td>
<td>Sub Code</td>
<td>Comment</td>
</tr>
<tr>
<td>2</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>User Attributes</td>
<td>Default Group</td>
<td>success</td>
<td>none</td>
<td>User Attributes exported successfully</td>
</tr>
<tr>
<td>3</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>User Attributes</td>
<td>Description</td>
<td>success</td>
<td>none</td>
<td>User Attributes exported successfully</td>
</tr>
<tr>
<td>4</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>Network Device Groups</td>
<td>Not Assigned</td>
<td>success</td>
<td>none</td>
<td>Network Device Group was not assigned</td>
</tr>
<tr>
<td>5</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>User Groups</td>
<td>Default Group</td>
<td>error</td>
<td>without_users</td>
<td>Group has no users</td>
</tr>
<tr>
<td>6</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>User Groups</td>
<td>Group 1</td>
<td>error</td>
<td>without_users</td>
<td>Group has no users</td>
</tr>
<tr>
<td>7</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>Network Device</td>
<td>test1</td>
<td>success</td>
<td>none</td>
<td>Network Device Group was not assigned</td>
</tr>
<tr>
<td>8</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>Network Device</td>
<td>test2</td>
<td>success</td>
<td>none</td>
<td>Network Device Group was not assigned</td>
</tr>
<tr>
<td>9</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>Network Device</td>
<td>test3</td>
<td>success</td>
<td>none</td>
<td>Network Device Group was not assigned</td>
</tr>
<tr>
<td>10</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>Network Device</td>
<td>test0</td>
<td>success</td>
<td>none</td>
<td>Network Device Group was not assigned</td>
</tr>
<tr>
<td>11</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>Network Device</td>
<td>test11</td>
<td>success</td>
<td>none</td>
<td>Network Device Group was not assigned</td>
</tr>
<tr>
<td>12</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>Network Device</td>
<td>test30</td>
<td>success</td>
<td>none</td>
<td>Network Device Group was not assigned</td>
</tr>
<tr>
<td>13</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>RAC</td>
<td>Ascend1</td>
<td>error</td>
<td>error</td>
<td>Invalid value for attribute Ascend-Cali</td>
</tr>
<tr>
<td>14</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>RAC</td>
<td>Ascend1</td>
<td>error</td>
<td>error</td>
<td>WRONG_EIUM_VALUE or attribute</td>
</tr>
<tr>
<td>15</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>RAC</td>
<td>Ascend2</td>
<td>error</td>
<td>error</td>
<td>WRONG_EIUM_VALUE or attribute</td>
</tr>
<tr>
<td>16</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>RAC</td>
<td>Ascend2</td>
<td>error</td>
<td>error</td>
<td>WRONG_EIUM_VALUE or attribute</td>
</tr>
<tr>
<td>17</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>RAC</td>
<td>Ascend2</td>
<td>error</td>
<td>error</td>
<td>WRONG_EIUM_VALUE or attribute</td>
</tr>
<tr>
<td>18</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>RAC</td>
<td>Ascend2</td>
<td>error</td>
<td>error</td>
<td>WRONG_EIUM_VALUE or attribute</td>
</tr>
<tr>
<td>19</td>
<td>racbugs0</td>
<td>AnalyzeAndExport</td>
<td>RAC</td>
<td>Ascend2</td>
<td>error</td>
<td>error</td>
<td>WRONG_EIUM_VALUE or attribute</td>
</tr>
</tbody>
</table>

Table 6-24  Analyze and Export Full Report Column Definitions

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

Import Summary Report

Figure 6-3 shows the Import Summary Report. Table 6-25 contains the Import Summary Report column definitions.

Figure 6-3  Import Summary Report

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Server ID</td>
<td>Phase</td>
<td>Element Name</td>
<td>Total Element</td>
<td>Total Migratable</td>
<td>Total with Issues</td>
<td>Comment</td>
</tr>
<tr>
<td>2</td>
<td>racbugs0</td>
<td>Import</td>
<td>User Attributes</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>racbugs0</td>
<td>Import</td>
<td>Network Device Groups</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>racbugs0</td>
<td>Import</td>
<td>User Groups</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>racbugs0</td>
<td>Import</td>
<td>Groups Shell Exec</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>racbugs0</td>
<td>Import</td>
<td>Users Shell Exec</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>racbugs0</td>
<td>Import</td>
<td>Users</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>racbugs0</td>
<td>Import</td>
<td>Shared Command Sets</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>racbugs0</td>
<td>Import</td>
<td>Groups Command Set</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>racbugs0</td>
<td>Import</td>
<td>Users Command Set</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>racbugs0</td>
<td>Import</td>
<td>Network Device</td>
<td>12</td>
<td>12</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>racbugs0</td>
<td>Import</td>
<td>Shared Downloadable ACL</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>racbugs0</td>
<td>Import</td>
<td>EAP FAST - Master keys</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>racbugs0</td>
<td>Import</td>
<td>MAB</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>racbugs0</td>
<td>Import</td>
<td>RAC</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Table 6-25  Import Summary Report Column Definitions

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server ID</td>
<td>Name of the server.</td>
</tr>
<tr>
<td>Phase</td>
<td>Name of the migration phase.</td>
</tr>
<tr>
<td>Element Name</td>
<td>Name of the ACS object type to be migrated.</td>
</tr>
<tr>
<td>Total Elements</td>
<td>Total number of elements.</td>
</tr>
<tr>
<td>Total Migratable</td>
<td>Total number of elements that are migrated.</td>
</tr>
<tr>
<td>Total with Issues</td>
<td>Total number of elements that have issues.</td>
</tr>
<tr>
<td>Comment</td>
<td>Message indicating the status of the ACS object.</td>
</tr>
</tbody>
</table>

Figure 6-4 Import Full Report

Table 6-26  Import Full Report Column Definitions

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

Figure 6-4 shows the Import Full Report. Table 6-26 contains the Import Full Report column definitions.
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 5.5 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 6-5 shows the Summary Report statistics for all migration phases. Table 6-27 contains the Summary Report column definitions.
Full Report

Figure 6-6 shows the Full Report statistics for all migration phases. Table 6-28 contains the Full Report column definitions.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server ID</td>
<td>Name of the server.</td>
</tr>
<tr>
<td>Phase</td>
<td>Name of the migration phase.</td>
</tr>
<tr>
<td>Element Name</td>
<td>Name of the migrated ACS object.</td>
</tr>
<tr>
<td>Total Elements</td>
<td>Total number of ACS objects processed.</td>
</tr>
<tr>
<td>Total Migratable</td>
<td>Total number of ACS objects migrated.</td>
</tr>
<tr>
<td>Total with Issues</td>
<td>Total number of issues for each ACS object.</td>
</tr>
<tr>
<td>Comment</td>
<td>Message indicating the status of the ACS object.</td>
</tr>
</tbody>
</table>

Table 6-28 Full Report Column Definitions

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server ID</td>
<td>Name of the server.</td>
</tr>
<tr>
<td>Phase</td>
<td>Name of the migration phase.</td>
</tr>
<tr>
<td>Element Name</td>
<td>Name of the migrated ACS object.</td>
</tr>
<tr>
<td>Name</td>
<td>User-supplied name.</td>
</tr>
<tr>
<td>Operation Code</td>
<td>Indicates if the operation was a success or if an error occurred.</td>
</tr>
<tr>
<td>Sub Code</td>
<td>Code associated with the status of the operation.</td>
</tr>
<tr>
<td>Comment</td>
<td>Message indicating the status of the ACS object.</td>
</tr>
</tbody>
</table>
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, see Resolving Migration Issues, page D-3.

For the error and informational messages that may appear during the migration of various ACS objects, see Migration Utility Messages, page D-6.

Confirming the Migration

Log into your ACS 5.5 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 5.5:

- 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 5.5 objects, follow the instructions in the User Guide for Cisco Secure Access Control System 5.5.

The following sections provide information on confirming the migration of:

- Users and User Groups, page 6-48
- Command Shell Migration, page 6-49
- Command Set Migration, page 6-50
- NDG Migration, page 6-51
- Network Device Migration, page 6-52
- DACL Migration, page 6-53
- MAB Migration, page 6-54
Chapter 6  Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5

Confirming the Migration

- Shared RACs, page 6-55
- RADIUS VSA, page 6-56
- KEK and MACK Keys, page 6-57

Users and User Groups

Figure 6-7 shows the users and user groups in ACS 4.x, and Figure 6-8 shows the users and user groups migrated to ACS 5.5. Choose Users and Identity Stores > Internal Identity Stores > Users to access the migrated users and user groups.

Figure 6-7  Users and User Groups Defined in ACS 4.x

Figure 6-8  Users and User Groups Migrated to ACS 5.5
Command Shell Migration

Figure 6-9 shows the command shell attributes in ACS 4.x, and Figure 6-10 shows the group shell attributes migrated to ACS 5.5 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 6-11 shows the user shell attributes migrated to ACS 5.5.

### Figure 6-9  Command Shell Attributes Defined in ACS 4.x

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shell (exec)</td>
<td></td>
</tr>
<tr>
<td>Access control list</td>
<td>12.21.38.901</td>
</tr>
<tr>
<td>Auto command</td>
<td>test</td>
</tr>
<tr>
<td>Callback line</td>
<td>23</td>
</tr>
<tr>
<td>Callback rotary</td>
<td></td>
</tr>
<tr>
<td>Idle time</td>
<td></td>
</tr>
<tr>
<td>No callback verify</td>
<td>Enabled</td>
</tr>
<tr>
<td>No escape</td>
<td>Enabled</td>
</tr>
<tr>
<td>No hangup</td>
<td>Enabled</td>
</tr>
<tr>
<td>Privilege level</td>
<td>10</td>
</tr>
<tr>
<td>Timeout</td>
<td></td>
</tr>
</tbody>
</table>

### Figure 6-10  Group Shell Attributes Migrated to ACS 5.5
Confirming the Migration

**Figure 6-11** User Shell Attribute Migrated to ACS 5.5

![User Shell Attribute Migrated to ACS 5.5](image)

**Command Set Migration**

Figure 6-12 shows the command set in ACS 4.x, and Figure 6-13 shows the command set migrated to ACS 5.5. Choose Policy Elements > Device Administration > Command Sets to access the migrated command set attributes.

**Figure 6-12** Command Set Defined in ACS 4.x

Shell Command Authorization Set
- None
- Assign a Shell Command Authorization Set for any network device
  - shell_test2
- Assign a Shell Command Authorization Set on a per Network Device Group Basis

<table>
<thead>
<tr>
<th>Device Group</th>
<th>Command Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration_T1</td>
<td>shell_test1</td>
</tr>
</tbody>
</table>

  Remove Association

<table>
<thead>
<tr>
<th>Device Group</th>
<th>Command Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration_T2</td>
<td>shell_test2</td>
</tr>
</tbody>
</table>

- Per Group Command Authorization
  - Unmatched Cisco IOS commands
    - Permit
    - Deny
Figure 6-13  Command Set Migrated to ACS 5.5

NDG Migration

Figure 6-14 shows the NDGs in ACS 4.x, and Figure 6-15 shows the NDGs migrated to ACS 5.5. Choose Network Resources > Network Device Groups to access the migrated NDGs.

Figure 6-14  NDGs Defined in ACS 4.x

Network Configuration
Network Device Migration

Figure 6-16 shows the network devices in ACS 4.x, and Figure 6-17 shows the network devices migrated to ACS 5.5. Choose Network Resources > Network Devices and AAA Clients to access the migrated network devices.

Figure 6-16     Network Devices Defined in ACS 4.x

<table>
<thead>
<tr>
<th>AAA Client Hostname</th>
<th>AAA Client IP Address</th>
<th>Authenticate Using</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.77.242.83</td>
<td>10.77.242.83</td>
<td>RADIUS (IETF)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AAA Client Hostname</th>
<th>AAA Client IP Address</th>
<th>Authenticate Using</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.77.234.227</td>
<td>10.77.234.227</td>
<td>TACACS+ (Cisco IOS)</td>
</tr>
<tr>
<td>10.77.234.235</td>
<td>10.77.234.235</td>
<td>TACACS+ (Cisco IOS)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AAA Client Hostname</th>
<th>AAA Client IP Address</th>
<th>Authenticate Using</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.77.244.24</td>
<td>10.77.244.24</td>
<td>RADIUS (Cisco IOS/PIX 6.0)</td>
</tr>
<tr>
<td>NAD</td>
<td>10.77.243.*</td>
<td>RADIUS (Cisco IOS/PIX 6.0)</td>
</tr>
</tbody>
</table>
Figure 6-17  Network Devices Migrated to ACS 5.5

DACL Migration

Figure 6-18 shows the downloadable access control lists (DACLs) in ACS 4.x, and Figure 6-19 shows the DACLs migrated to ACS 5.5.

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

Figure 6-18  DACLs Defined in ACS 4.x

Shared Profile Components
Figure 6-19  DACLs Migrated to ACS 5.5

MAB Migration

Figure 6-20 shows MAC Authentication Bypass (MAB) defined in ACS 4.x, and Figure 6-21 shows MAB migrated to ACS 5.5.

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

Figure 6-20  MAB Defined in ACS 4.x
Shared RACs

Figure 6-22 shows shared RADIUS Authorization Components (RACs) defined in ACS 4.x, and Figure 6-23 shows shared RACs migrated to ACS 5.5.

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

Shared Profile Components
RADIUS VSA

Figure 6-24 shows RADIUS VSAs defined in ACS 4.x, and Figure 6-25 shows RADIUS VSAs migrated to ACS 5.5.

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

Interface Configuration
Figure 6-25  RADIUS VSAs Migrated to ACS 5.5

KEK and MACK Keys

Figure 6-26 shows Key Encryption Key (KEK) and Message Authentication Code Key (MACK) keys defined in ACS 4.x, and Figure 6-27 shows the KEK and MACK keys migrated to ACS 5.5.

Choose Network Devices > Network Devices and AAA Clients, select a device and click Edit to access the migrated KEK and MACK keys.
Chapter 6  
Using the Migration Utility to Migrate Data from ACS 4.x to ACS 5.5

Confirming the Migration

Figure 6-26  KEK and MACK Keys Defined in ACS 4.x

Network Configuration

client

AAA Client IP Address

Shared Secret

Network Device Group

Authenticate Using

RADIUS Key Wrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format

Log Update/Watchdog Packets from the AAA Client

RADIUS Option

Replace RADIUS Port info with Username from this AAA Client

Figure 6-27  KEK and MACK Keys Migrated to ACS 5.5
ACS 5.5 Attribute Support in the Migration Utility

This chapter contains:
- Introduction, page A-1
- ACS 4.x to 5.5 Migration, page A-1

Introduction

This chapter describes ACS 4.x to ACS 5.5 attribute migration. To migrate ACS 4.x attributes, they must meet ACS 5.5 criteria. You can migrate some ACS 4.x elements to ACS 5.5, even though some of the attributes for an element might not migrate (or translate) to ACS 5.5.

For example, ACS 5.5 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 5.5 Migration

The following sections contain element information for:
- AAA Client/Network Device, page A-2
- NDG, page A-2
- Internal User, page A-2
- User Policy Components, page A-3
- User Group, page A-3
- User Group Policy Components, page A-4
- Shared Shell Command Authorization Sets, page A-4
- MAB, page A-5
- DACL, page A-5
- EAP-FAST Master Keys, page A-5
- Shared RACs, page A-5
- Customer VSAs, page A-5
AAA Client/Network Device

Table A-1 describes the differences between the ACS 4.x network device definitions and the ACS 5.5 network device definitions.

Table A-1  ACS Network Device Definitions

<table>
<thead>
<tr>
<th>ACS element</th>
<th>ACS 4.x</th>
<th>ACS 5.5 Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS and TACACS+</td>
<td>Defines one network device for each protocol. For example, network device1 for RADIUS, network device 2 for TACACS+.</td>
<td>Defines one network device for RADIUS and TACACS+. See Overlapping IP Addresses, page D-3.</td>
</tr>
<tr>
<td>IP Address</td>
<td>• Use regular expressions to define the IP address.</td>
<td>• Define IP addresses as a pair of IP addresses and mask definitions.</td>
</tr>
<tr>
<td></td>
<td>• You can define more than 40 IP addresses.</td>
<td>• Limited to 40 IP addresses.</td>
</tr>
<tr>
<td></td>
<td>• Includes wildcards and ranges.</td>
<td>• Definition is in the form of a subnet mask. See Untranslatable IP Addresses, page D-4.</td>
</tr>
</tbody>
</table>

Note  ACS 5.5 does not support ACS 4.x authentication by using an attribute for network devices. ACS 5.5 supports only RADIUS and TACACS+. You cannot define a specific vendor.

NDG

ACS 5.5 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 5.5 supports the ACS 4.x Password Authentication Type. ACS 5.5 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 Migration Script User Preferences.
User Policy Components

In ACS 4.x, the policy-related authorization data is embedded within the user definitions. In ACS 5.5, policy-related authorization data is included in shared components that are referenced from within the ACS 5.5 policy tables. Table A-2 shows the attributes for the ACS 4.x user policy components and describes the status in ACS 5.5.

<table>
<thead>
<tr>
<th>ACS 4.x Attribute</th>
<th>ACS 5.5 Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS+ Shell (exec) Privilege level:</td>
<td>• In ACS 5.5, the default privilege level cannot be larger than the maximum privilege level.</td>
</tr>
<tr>
<td>The privilege level is a string field without validity checks.</td>
<td>• ACS 5.5 supports the privilege level as a numeric value (1-15).</td>
</tr>
<tr>
<td>TACACS+ Shell Custom attributes</td>
<td>Phase II does not support custom attributes for privilege levels and shell commands.</td>
</tr>
<tr>
<td>TACACS+ Shell Command Authorization Set:</td>
<td>Migration supports only per-user command authorization and does not support the following attributes:</td>
</tr>
<tr>
<td>You do not have to specify a value for each attribute.</td>
<td>• Assign a shell command authorization set for any network device.</td>
</tr>
<tr>
<td></td>
<td>• Assign a shell command authorization set on a per-network device group basis.</td>
</tr>
<tr>
<td></td>
<td>You must specify a value for each attribute.</td>
</tr>
</tbody>
</table>

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 5.5, 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 5.5, policy authorization data is defined in Session Authorization Profiles. Table A-3 shows the attributes for the policy components of the ACS 4.x user group and describes the status in ACS 5.5.

### Table A-3 User Group Policy Component Attributes

<table>
<thead>
<tr>
<th>ACS 4.x Attribute</th>
<th>ACS 5.5 Status</th>
</tr>
</thead>
</table>
| TACACS+Shell (exec) Privilege level: The privilege level is a string field without validity checks. | • ACS 5.5 supports the privilege level as a numeric value (1-15).  
• In ACS 5.5, the default privilege level cannot be larger than the maximum privilege level. |
| TACACS+Shell (exec) Custom attributes | ACS 5.5 does not support shell command custom attributes. |
| TACACS+Shell Command Authorization Set You do not have to specify a value for each attribute. | ACS 5.5 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 [http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.5/user/guide/pol_elem.html#wp1053110](http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.5/user/guide/pol_elem.html#wp1053110).

To map the custom attributes in the policy conditions, see [http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.5/user/guide/access_policies.html](http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.5/user/guide/access_policies.html).

**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 5.5 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 5.5 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 5.5. You can migrate only the ACL content, because ACS 5.5 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 5.5 schema. Therefore, Master Keys are migrated to different ACS 5.5 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 5.5, RACs are defined in shared authorization profiles.

Table A-4 shows the attributes for the RACs in ACS 4.x and describes their status in ACS 5.5.

<table>
<thead>
<tr>
<th>ACS 4.x Attribute</th>
<th>ACS 5.5 Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>In ACS 4.x, the following attributes can be configured and fixed:</td>
<td>In ACS 5.5, you cannot configure these attributes. These are added to the profile as required.</td>
</tr>
<tr>
<td>• MS-CHAP-MPPE-Keys (12)</td>
<td></td>
</tr>
<tr>
<td>• MS-MPPE-Send-Key (16)</td>
<td></td>
</tr>
<tr>
<td>• MS-MPPE-Recv-Key (17)</td>
<td></td>
</tr>
<tr>
<td>In ACS 4.x, Ascend attributes are stored internally with a vendor ID of 0.</td>
<td>In ACS 5.5, you have to assign an Ascend vendor ID of 529.</td>
</tr>
</tbody>
</table>

Customer VSAs

During migration, the dictionary is iterated to identify the missing attributes in ACS 5.5 for each vendor. If the vendor does not exist in the ACS 5.5 dictionary, all the vendor attributes are migrated. If the vendor exists in the ACS 5.5 dictionary, only attributes that are not defined in ACS 5.5 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 5.5.
# Configuration Mapping from ACS 3.x and 4.x to ACS 5.5

Table B-1 lists the configuration areas in ACS 3.x and 4.x and their equivalents in ACS 5.5.

<table>
<thead>
<tr>
<th>ACS 3.x and 4.x Configuration Areas</th>
<th>ACS 5.5 Configuration Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Setup</td>
<td>Users and Identity Stores, Policy Elements, Access Policies, System Administration</td>
</tr>
<tr>
<td>Group Setup</td>
<td>Users and Identity Stores, Policy Elements, Access Policies</td>
</tr>
<tr>
<td>Shared Profile Components</td>
<td>Policy Elements</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>Network Resources</td>
</tr>
<tr>
<td>System Configuration</td>
<td>System Administration</td>
</tr>
<tr>
<td>Interface Configuration</td>
<td>NA</td>
</tr>
<tr>
<td>Administration Control</td>
<td>System Administration</td>
</tr>
<tr>
<td>External User Databases</td>
<td>Users and Identity Stores</td>
</tr>
<tr>
<td>Posture Validation</td>
<td>NA</td>
</tr>
<tr>
<td>Network Access Profiles</td>
<td>Access Policies</td>
</tr>
<tr>
<td>Reports and Activity</td>
<td>Monitoring and Reports</td>
</tr>
</tbody>
</table>
# Feature Comparison of ACS 3.x and 4.x with ACS 5.5

## Table C-1 Feature Comparison List—ACS 3.x/4.x and ACS 5.5

<table>
<thead>
<tr>
<th>Feature</th>
<th>ACS 3.x and 4.x</th>
<th>ACS 5.5</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Support</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1111</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>1112</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>1113</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>1120</td>
<td>Yes (4.2)</td>
<td>Yes</td>
<td>ACS 5.0 shipping appliance</td>
</tr>
<tr>
<td>1121</td>
<td>No</td>
<td>Yes</td>
<td>ACS 5.2, 5.3, 5.4, and 5.5 shipping appliance</td>
</tr>
<tr>
<td>3415</td>
<td>No</td>
<td>Yes</td>
<td>ACS 5.4 and 5.5 shipping appliance</td>
</tr>
<tr>
<td>3495</td>
<td>No</td>
<td>Yes</td>
<td>ACS 5.5 shipping appliance</td>
</tr>
<tr>
<td>Windows Server</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Virtual machine</td>
<td>ESX 3.x</td>
<td>ESX i5.0, i5.0 update 2, and i5.1</td>
<td></td>
</tr>
<tr>
<td>Components</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACS for Windows</td>
<td>Yes</td>
<td>No</td>
<td>No Windows Server support in ACS 5.5</td>
</tr>
<tr>
<td>ACS Solution Engine</td>
<td>Yes</td>
<td>No</td>
<td>ACS 5.5 provides its own appliance option</td>
</tr>
<tr>
<td>ACS View 4.0</td>
<td>Yes</td>
<td>No</td>
<td>ACS 5.5 has integrated View functionality</td>
</tr>
<tr>
<td>ACS Remote Agent</td>
<td>Yes</td>
<td>No</td>
<td>Remote Agent not required in 5.5</td>
</tr>
<tr>
<td>ACS Express 5.0</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Application Integration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CiscoWorks Common Services</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>(for CSM/LMS)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Table C-1  Feature Comparison List—ACS 3.x/4.x and ACS 5.5 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>ACS 3.x and 4.x</th>
<th>ACS 5.5</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Wireless Control System (WCS)</strong></td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Distributed Model</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Single primary/multiple secondary</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Cascading replication</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Replication trigger</td>
<td>Manual or per schedule</td>
<td>On configuration change</td>
<td></td>
</tr>
<tr>
<td>Replication unit</td>
<td>Whole replication component</td>
<td>Configuration delta only</td>
<td></td>
</tr>
<tr>
<td>Synchronization</td>
<td>Loose</td>
<td>Tight</td>
<td></td>
</tr>
<tr>
<td>Automatic outage resynchronization</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Internal user password updates</td>
<td>On primary only</td>
<td>On primary only</td>
<td></td>
</tr>
<tr>
<td>Role-based secondary to primary promotion</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Identity Store Support</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Active Directory</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>RDBMS</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>RSA SecurID</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Other One-time Password Servers</td>
<td>Yes</td>
<td>Yes</td>
<td>Uses RADIUS interface to OTP server</td>
</tr>
<tr>
<td><strong>AAA Proxy Support</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RADIUS proxy</td>
<td>Yes</td>
<td>Yes</td>
<td>Includes EAP Proxy</td>
</tr>
<tr>
<td>TACACS+ proxy</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Logging Destinations</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACS View</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Syslog</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ODBC</td>
<td>Yes</td>
<td>No</td>
<td>ACS 5.5 provides View log data synchronization with an external database for archival purposes</td>
</tr>
<tr>
<td><strong>Configuration Query/Provisioning</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-based GUI</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CSV-based updates</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### Table C-1 Feature Comparison List—ACS 3.x/4.x and ACS 5.5 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>ACS 3.x and 4.x</th>
<th>ACS 5.5</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSUtil</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>RDBMS Synchronization</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP query</td>
<td>Yes (appliance only)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>SNMP traps</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>View alarms</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>GUI</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Cisco standard look and feel GUI</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CLI</td>
<td>Yes (limited, appliance only)</td>
<td>Yes (similar to IOS)</td>
<td></td>
</tr>
<tr>
<td>System restart after some configuration changes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>KVM console access</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Choice of file transfer storage repositories</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>In-place, cross-version upgrade procedure</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Remote upgrades/patching</td>
<td>Partial</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Supported Protocols</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAP</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CHAP</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>MS-CHAPv1</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>MS-CHAPv2</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>MAB</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>EAP-MD5</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>PEAP-MSCHAPv2</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>PEAP-GTC</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>PEAP-TLS</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>FAST-MSCHAPv2</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>FAST-GTC</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>FAST-TLS</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>LEAP</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>TACACS+</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command authorization</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Accounting</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### Table C-1  Feature Comparison List—ACS 3.x/4.x and ACS 5.5 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>ACS 3.x and 4.x</th>
<th>ACS 5.5</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single connect</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Change password</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Enable handling</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Custom services</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Optional attributes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CHAP/MSCHAP authentication</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Attribute substitution</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>ACS Password Policy</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complexity</td>
<td>Yes</td>
<td>Yes</td>
<td>(stronger)</td>
</tr>
<tr>
<td>History</td>
<td>Yes (last only)</td>
<td>Yes</td>
<td>(multiple)</td>
</tr>
<tr>
<td>Expiry</td>
<td>Yes (age by days, logins, first login)</td>
<td>Yes (age by days)</td>
<td></td>
</tr>
<tr>
<td>Expiry warning</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Grace period</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td><strong>Account Disablement</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>By date</td>
<td>Yes</td>
<td>Yes</td>
<td>Can be implemented using authorization policy</td>
</tr>
<tr>
<td>By failed attempts</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>By inactivity</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Network Devices</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Separate TACACS+/RADIUS entries</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Hierarchical, scalable device grouping</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Default network device</td>
<td>TACACS+ only</td>
<td>RADIUS and TACACS+</td>
<td></td>
</tr>
<tr>
<td>Group-level shared secrets</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Wildcard for IP address</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Access Policy</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flexible, rules-based policy model</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Mandatory ACS group assignment</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Multiple group membership</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Static IP address assignment</td>
<td>Yes</td>
<td>Yes</td>
<td>Extend schema, policy</td>
</tr>
<tr>
<td>Maximum sessions</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Group disablement</td>
<td>Yes</td>
<td>Yes</td>
<td>Implement in ACS 5.5 policy</td>
</tr>
</tbody>
</table>
### Table C-1  Feature Comparison List—ACS 3.x/4.x and ACS 5.5 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>ACS 3.x and 4.x</th>
<th>ACS 5.5</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VOIP support</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>ToD settings</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Callback</td>
<td>Yes</td>
<td>Yes</td>
<td>Use of Windows Callback setting is not available in ACS 5.5</td>
</tr>
<tr>
<td>Network Access Restrictions</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Usage quotas</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Enable options</td>
<td>Yes</td>
<td>Yes</td>
<td>Implement in ACS 5 policy</td>
</tr>
<tr>
<td>Token caching</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>IP address assignment</td>
<td>Yes</td>
<td>Yes (static and AAA client pool only)</td>
<td>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 &quot;ip-pool-definition&quot; on ACS. The pool itself will be defined on the switch or router itself.</td>
</tr>
<tr>
<td>Downloadable ACLs</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Supplementary user information</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Extendable ACS user schema for use in policy conditions and for authorization values</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>User attributes (internal, AD, LDAP), that can be leveraged in policy conditions and as authorization values</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>External password authentication for ACS internal users</td>
<td>Yes</td>
<td>Yes</td>
<td>In ACS 5, the password store must be specified through Access Service Identity Policy, and cannot be specified in the user's record.</td>
</tr>
<tr>
<td>Time bound alternate group</td>
<td>Yes</td>
<td>Yes</td>
<td>In ACS 5, time-based conditions are used to specify different permissions based on time of the day.</td>
</tr>
<tr>
<td>Windows dial-in support</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**ACS Administrators**

<table>
<thead>
<tr>
<th>Feature</th>
<th>ACS 3.x and 4.x</th>
<th>ACS 5.5</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network restrictions</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Entitlement reports</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Password complexity</td>
<td>Yes</td>
<td>Yes (stronger)</td>
<td>In ACS 5, time-based conditions are used to specify different permissions based on time of the day.</td>
</tr>
<tr>
<td>Feature</td>
<td>ACS 3.x and 4.x</td>
<td>ACS 5.5</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------</td>
<td>---------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Password aging</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Password history</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>password inactivity</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Account disablement because of failed attempts</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Account disablement because of account inactivity</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Permission control</td>
<td>Yes</td>
<td></td>
<td>Yes (role-based)</td>
</tr>
</tbody>
</table>

**Certificate-based Authentication/Authorization**

<table>
<thead>
<tr>
<th>Feature</th>
<th>ACS 3.x and 4.x</th>
<th>ACS 5.5</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory AD authorization</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>SAN/CN Comparison</td>
<td>Yes</td>
<td>No</td>
<td>Can be implemented indirectly in ACS 5.5 by checking for user attribute existence</td>
</tr>
<tr>
<td>Certificate binary comparison</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
App-1

APPENDIX D

Troubleshooting the Migration Utility

This chapter describes common problems associated with the ACS 5.5 Migration Utility:

- Unable to Restore the ACS 4.x Database on the Migration Machine, page D-1
- Remote Desktop Connection Not Supported for the Migration Utility, page D-2
- Migrating Objects from Large-Scale Databases, page D-2
- Import Phase Only Adds Partial Data, page D-2
- ACS 5.5 Machine Does Not Respond After Import, page D-3
- Resolving Migration Issues, page D-3
- Migration Failed with Manually Created Super Admin, page D-6
- Migration Utility Messages, page D-6
- Reporting Issues to Cisco TAC, page D-16

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 5.5 server.
   • Network connections are enabled.
   • ACS 5.5 services are up and running.
   • You use a compatible ACS 5.5 license.
2. Restore the ACS 5.5 database to its previous version of the database.
3. Restart the Migration Utility.
4. Rerun the Import phase.
ACS 5.5 Machine Does Not Respond After Import

Condition
The ACS 5.5 machine does not respond after import.

Action
Restart ACS 5.5.

Resolving Migration Issues

These sections discuss manual methods for resolving migration issues. The following migration issues are discussed:
- Overlapping IP Addresses, page D-3
- Untranslatable IP Addresses, page D-4
- Network Devices with More Than 40 IP Addresses, page D-4
- Invalid TACACS+ Shell Privilege Level, page D-5
- TACACS+ Custom Attributes Are Not Migrated, page D-5
- Shell Command Authorization Set Not Associated with User or Group, page D-6

Overlapping IP Addresses

The Analysis phase might report overlapping IP addresses for network devices in ACS 4.x. Example D-1 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.

Example D-1  Overlapping 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 5.5 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. Example D-2 illustrates the resolution.

Example D-2  Resolved 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 5.5, 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 5.5 subnet mask definition. However, not all combinations of IP addresses can be translated into an ACS 5.5 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 5.5 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:

Step 1 Choose Network Configuration.
Step 2 Choose the NDG to which the network device belongs.
Step 3 Choose the network device.
Step 4 Edit the AAA Client IP Address field. Ensure that the AAA client has 40 or fewer IP addresses.
Step 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:

Step 1 Choose User Setup.
Step 2 Choose the user.
The Edit screen appears.
Step 3 Check the Privilege level check box of the TACACS+ Settings table and enter a value between 0 and 15.
Step 4 Click Submit.

To edit the T+ settings at the group level:

Step 1 Choose Group Setup.
Step 2 Choose the group and click Edit Settings.
Step 3 Check the Privilege level check box of the TACACS+ Settings table and enter a value between 0 and 15.
Step 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 5.5 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 5.5 application to:
1. Access the migrated command sets. See “Command Set Migration” section on page 6-50, for more information.
2. Create a policy for the users and identity groups.
See the *User Guide for Cisco Secure Access Control System 5.5* 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 5.5. Migration fails when *Admin1* is used as the administrator username.

**Action**
Check if the migration steps are correct. ACS 5.5 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, page D-7
- MABs, page D-7
- NDGs, page D-8
- Master Keys, page D-8
- Network Devices, page D-9
- RACs, page D-10
- Command Set, page D-11
- Shell Exec, page D-12
- Users, page D-13
Migration Guide for Cisco Secure Access Control System 5.5

Appendix D  Troubleshooting the Migration Utility

- User Attributes, page D-14
- User Attribute Values, page D-14
- User Groups, page D-15
- VSA Vendors, page D-15
- VSAs, page D-15

Downloadable ACLs

Table D-1 gives the detail of the errors and informational messages that may appear during the migration of the Downloadable ACLs.

Table D-1  Error and Informational Messages for Downloadable ACLs

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Information</td>
<td>Shared DACL name after migration has been changed to: name after truncation.</td>
<td>Truncation</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Cannot migrate a shared DACL with a name that contains any of the following characters: illegal characters for the object.</td>
<td>Name error</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Error from PI. For example, object already exists in the ACS 5.5 database.</td>
<td>None</td>
</tr>
</tbody>
</table>

MABs

Table D-2 gives the detail of the errors and informational messages that may appear during the migration of the MABs.

Table D-2  Error and Informational Messages for MABs

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Information</td>
<td>MAB name after migration has been changed to: name after truncation.</td>
<td>Truncation</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Cannot migrate a MAB with a name that contains any of the following characters: illegal characters for the object.</td>
<td>Name error</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Invalid MAC ID.</td>
<td>Untranslatable</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Error from PI. For example, Object already exists in the ACS 5.5 database.</td>
<td>None</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Group ID: group ID referenced object was not imported.</td>
<td>No reference import</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Group could not be found for: MAB name Group ID: group ID.</td>
<td>Log error</td>
</tr>
</tbody>
</table>
NDGs

Table D-3 gives the detail of the errors and informational messages that may appear during the migration of the NDGs.

Table D-3  Error and Informational Messages for NDGs

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Information</td>
<td>Network device name after migration has been changed to: name after truncation.</td>
<td>Truncation</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Cannot migrate an NDG with a name that contains any of the following characters: illegal characters for the object.</td>
<td>Name error</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>NDG has a shared key password.</td>
<td>Password included</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Error from PI. For example, failed to add object: NDG root name in function: method name.</td>
<td>None</td>
</tr>
<tr>
<td>Import</td>
<td>Information</td>
<td>Object already exists in the ACS 5.5 database.</td>
<td>Duplicate</td>
</tr>
</tbody>
</table>

Master Keys

Table D-4 gives the detail of the errors and informational messages that may appear during the migration of the Master Keys.

Table D-4  Error and Informational Messages for Master Keys

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Information</td>
<td>Fatal Error: Authority ID is null - Import Failed.</td>
<td>None</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Error from PI. For example, object already exists in the ACS 5.5 database.</td>
<td>None</td>
</tr>
</tbody>
</table>
# Network Devices

*Table D-5* gives the detail of the errors and informational messages that may appear during the migration of the Network Devices.

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

Table D-6 gives the detail of the errors and informational messages that may appear during the migration of the RACs.

### Table D-6: Error and Informational Messages for RACs

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Information</td>
<td>RAC name after migration has been changed to: <code>name after truncation</code>.</td>
<td>Truncation</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>ACS 5.5 does not support this attribute: <code>vid= vendor ID, att= attribute value</code>. No other attributes in RAC will be migrated.</td>
<td>Unsupported vendor</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>RAC does not contain any supported attributes.</td>
<td>No value</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Cannot migrate an RAC with a name that contains any of the following characters: <em>Illegal characters for the object.</em></td>
<td>Name error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Wrong enum value for attribute: <code>attribute name</code>. No other attributes in RAC will be migrated.</td>
<td>Error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Invalid value for attribute: VSA <code>attribute name</code>. No other attributes in RAC will be migrated.</td>
<td>Error</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>The following attribute was not migrated: <code>attribute name</code>.</td>
<td>Unsupported vendor</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>ACS 5.5 does not support this attribute: <code>vid= vendor ID, att= attribute value, name= attribute name</code>. No other attributes in RAC will be migrated.</td>
<td>Unsupported vendor</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>RAC exception, for example, Invalid attribute number.</td>
<td>None</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Error from PI. For example, Object already exists in the ACS 5.5 database.</td>
<td>None</td>
</tr>
<tr>
<td>Import</td>
<td>Fatal</td>
<td>An error occurred in createCapabilitiesAll(): <em>Exception details.</em></td>
<td>Log error</td>
</tr>
</tbody>
</table>
# Command Set

Table D-7 gives the detail of the errors and informational messages that may appear during the migration of the Command Sets.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Information</td>
<td>Command set name after migration has been changed to: <em>name after truncation</em>.</td>
<td>Truncation</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Identical objects cannot be migrated: <em>identical object name</em>.</td>
<td>Consolidated</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Command set value: <em>Invalid Command Set value</em>.</td>
<td>Untranslatable</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Cannot migrate a command set with a name that contains any of the following characters: <em>Illegal characters for the object</em>.</td>
<td>Name error</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td><em>Command set name</em> was not imported and shell exec and command set for this user/group were not imported.</td>
<td>Name error</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Shared command sets name cannot contain apostrophes or curly braces.</td>
<td>Name error</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Command Set name contains a duplicate argument.</td>
<td>With duplicate argument</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>The selected network device NDG is not supported.</td>
<td>Unsupported option</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Translation failed. The argument does not start with Unmatched.</td>
<td>Log error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Translation failed. An equals sign (=) is missing after Unmatched.</td>
<td>Log error</td>
</tr>
<tr>
<td>Export</td>
<td>Fatal</td>
<td>Translation failed since Unmatched is not set to permit or deny: <em>unmatched value</em>.</td>
<td>Log error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Group T+ shell command translation failed: <em>exception details</em>.</td>
<td>Log error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Group T+ shell command translation failed. The argument is not a prefix with permit/deny: <em>argument action value</em>.</td>
<td>Log error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Command name Group T+ command set translation failed: <em>exception details</em>.</td>
<td>Log error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Command description, Exception details.</td>
<td>Log error</td>
</tr>
</tbody>
</table>
### Table D-7 Error and Informational Messages for Command Sets (continued)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Error</td>
<td>Referenced object was not imported.</td>
<td>No reference import</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Error from PL. For example, object already exists in the ACS 5.5 database.</td>
<td>Error</td>
</tr>
</tbody>
</table>

### Shell Exec

Table D-8 gives the detail of the errors and informational messages that may appear during the migration of the shell exec.

### Table D-8 Error and Informational Messages for Shell Exec

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Information</td>
<td>Command set name after migration has been changed to: name after truncation.</td>
<td>Truncation</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Identical objects cannot be migrated: identical object name.</td>
<td>Consolidated</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Shell Exec value Invalid shell exec value. No other T+ shell exec attributes will be migrated.</td>
<td>Untranslatable</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Parsing error. No other T+ shell exec attributes will be migrated.</td>
<td>Untranslatable</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>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.</td>
<td>Name error</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>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.</td>
<td>Name error</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>ACS 5.5 does not support custom attributes present in T+ shell exec. No other T+ shell exec attributes will be migrated.</td>
<td>Inset</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>T+ shell exec not defined for user or user group. No other T+ shell exec attributes will be migrated.</td>
<td>Inset</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Idle time for shell exec should be in the range of 0-9999. No other T+ shell exec attributes will be migrated.</td>
<td>Invalid idle time</td>
</tr>
</tbody>
</table>
### Appendix D  Troubleshooting the Migration Utility

#### Migration Utility Messages

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

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Information</td>
<td>Time out for shell exec should be in the range of 0-9999. No other T+ shell exec attributes will be migrated.</td>
<td>Invalid timeout</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>T+ shell priv-lvl is invalid value. No other T+ shell exec attributes will be migrated.</td>
<td>Invalid privilege level</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>T+ shell priv-lvl value is higher than max-priv-lvl max value. No other T+ shell exec attributes will be migrated.</td>
<td>Invalid privilege level</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>ACS 5.5 does not support custom attributes present in T+ shell exec.</td>
<td>Unsupported option</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Group T+ shell exec translation failed: exception details.</td>
<td>Log error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>An error occurred while retrieving the max privilege: exception details.</td>
<td>Log error</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Referenced object was not imported.</td>
<td>No reference import</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Error from Pl. For example, object already exists in the ACS 5.5 database.</td>
<td>Error</td>
</tr>
</tbody>
</table>

### Users

Table D-9 gives the detail of the errors and informational messages that may appear during the migration of the Users.

**Table D-9**  Error and Informational Messages for Users

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Information</td>
<td>User name after migration has been changed to: name after truncation.</td>
<td>Truncation</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Cannot migrate users with names that contain any of the following characters: Illegal characters for the object.</td>
<td>Name error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Cannot migrate users whose password does not conform to the ACS 5 password policy. Passwords should be between 4 and 32 characters in length.</td>
<td>Password error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Cannot migrate users with empty password to ACS 5.5.</td>
<td>No password</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Cannot migrate VoIP users to ACS 5.5.</td>
<td>VoIP group</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>A problem occurred while reading the expiry data for the user.</td>
<td>Log error</td>
</tr>
</tbody>
</table>
Table D-9  Error and Informational Messages for Users

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Error</td>
<td>Referenced object was not imported.</td>
<td>No reference import</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Group could not be found for: MAB name Group ID: group ID.</td>
<td>Log error</td>
</tr>
</tbody>
</table>

User Attributes

Table D-10 gives the detail of the errors and informational messages that may appear during the migration of the User attributes.

Table D-10  Error and Informational Messages for User Attributes

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Information</td>
<td>User attribute after migration has been changed to: name after truncation.</td>
<td>Truncation</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Cannot migrate a user attribute with a name that contains any of the following characters: Illegal characters for the object.</td>
<td>Name error</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>User attribute name User-defined name is not unique. It will be disambiguated for import by appending a suffix.</td>
<td>Repeated</td>
</tr>
<tr>
<td>Import</td>
<td>Information</td>
<td>Attribute added with warning: Object already exists in the ACS 5.5 database.</td>
<td>Duplicate</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Error from PI.</td>
<td>Error</td>
</tr>
</tbody>
</table>

User Attribute Values

Table D-11 gives the detail of the errors and informational messages that may appear during the migration of the User attribute values.

Table D-11  Error and Informational Messages for User Attribute Values

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Error</td>
<td>User attribute value was not imported and user attribute values for this user were not imported.</td>
<td>Log error</td>
</tr>
</tbody>
</table>
User Groups

Table D-12 gives the detail of the errors and informational messages that may appear during the migration of the User Groups.

Table D-12  Error and Informational Messages for User Groups

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Error</td>
<td>Group has no users.</td>
<td>Without users</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Cannot migrate a user group with a name that contains any of the following characters: Illegal characters for the object.</td>
<td>Name error</td>
</tr>
<tr>
<td>Import</td>
<td>Information</td>
<td>Error from PI.</td>
<td>Duplicate</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>Error from PI.</td>
<td>Error</td>
</tr>
</tbody>
</table>

VSA Vendors

Table D-13 gives the detail of the errors and informational messages that may appear during the migration of the VSA vendors IDs.

Table D-13  Error and Informational Messages for VSA Vendors

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Error</td>
<td>Object already exists in the ACS 5.5 database.</td>
<td>Duplicate</td>
</tr>
<tr>
<td>Export</td>
<td>Information</td>
<td>Vendor name conflict. ACS 5.5 vendor name: vendor name.</td>
<td>Name error</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>VSA vendor ID vendor id import failed. Error from PI:</td>
<td>Enum error</td>
</tr>
</tbody>
</table>

VSAs

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

Table D-14  Error and Informational Messages for VSAs

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Error</td>
<td>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.</td>
<td>Profile error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>VSA ID (attribute id) has attribute name conflicts: In ACS 4.x, it is attribute name, but in ACS 5.5, it is attribute name.</td>
<td>Name error</td>
</tr>
</tbody>
</table>
### Table D-14  Error and Informational Messages for VSAs

<table>
<thead>
<tr>
<th>Phase</th>
<th>Type</th>
<th>Error</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Error</td>
<td>VSA ID attribute id has attribute type conflicts: In ACS 4.x, it is attribute type, but in ACS 5.5 attribute type value.</td>
<td>Type error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>There is a problem with the VSA ID attribute id enum values (see log for details)</td>
<td>Enum error</td>
</tr>
<tr>
<td>Export</td>
<td>Error</td>
<td>Object already exists in the ACS 5.5 database.</td>
<td>None</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>VSA attribute id enum import failed. Error from PI;</td>
<td>Enum error</td>
</tr>
<tr>
<td>Import</td>
<td>Information</td>
<td>VSA attribute ID enabling log failed.</td>
<td>None</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>VSA attribute ID attribute import failed. Error from PI.</td>
<td>Unsupported attribute</td>
</tr>
<tr>
<td>Import</td>
<td>Error</td>
<td>VSA attribute ID vendor ID vendor ID import failed. Error from PI.</td>
<td>No reference import</td>
</tr>
</tbody>
</table>

### 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 5.5 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 5.5 logfiles
- ACS 5.5 build number
- ACS 4.x build number
**A**

- **ACL**: Access control list. A list of permissions attached to an object.
- **ACS**: Access control system.
- **AD**: Active Directory.

**C**

- **CN**: Common Name.

**E**

- **EAP**: Extensible Authentication Protocol. It is an authentication framework frequently used in wireless networks and Point-to-Point connections.
- **EAP-FAST**: Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling. EAP-FAST is compliant with IEEE 802.1X and IEEE 802.11i. Like all EAP types, EAP-FAST can be used with WPA and WPA2 networks.

**H**

- **HTTPS**: Hypertext Transfer Protocol Secure. A URL scheme which is syntactically identical to the HTTP scheme normally used for accessing resources using HTTP. Using an HTTPS: URL indicates that HTTP is to be used, but with a different default port (443) and an additional encryption/authentication layer between HTTP and TCP.

**J**

- **JDBC**: JAVA Database Connectivity. An API for the JAVA programming language that defines how a client may access a database. It provides methods for querying and updating data in a database.
**L**

**LDAP**
Lightweight Directory Access Protocol. It is an application protocol for querying and modifying data using directory services running over TCP/IP.

**M**

**MAC address**
Media Access Control address. A quasi-unique identifier assigned by the manufacturer to most network adapters or network interface cards for identification.

**N**

**NAP**
Network Access Profile.

**NDG**
Network Device Group.

**P**

**PI**
Programmatic Interface. A mechanism for external applications to interact with ACS.

**R**

**RADIUS**
Remote Authentication Dial In User Service. This is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.

**S**

**SOAP**
Simple Object Access Protocol. A protocol for exchanging XML-based messages over a computer network, normally using HTTP. SOAP forms the foundation layer of the Web services stack.

**SAN**
Subject Alternative Name.

**T**

**TACACS**
Terminal Access Controller Access-Control System. It is a remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network.
### V

**VSA**
Vendor specific attribute. A proprietary property or characteristic not provided by the standard RADIUS attribute set. VSAs are defined by vendors of remote access servers to customize RADIUS for their servers.

### X

**XML**
Extensible Markup Language.
INDEX

A

ACS 4.x Appliance Support 4-2
ACS 4.x elements
  supported in the migration process 4-3
  unsupported in the migration process 4-4
ACS 4.x machine
  migration 3-3, 5-1
  source 3-3, 5-1
ACS 4.x to 5.5 migration 3-1
ACS 5.5 target machine 3-3, 5-1
Analysis and Export of 4.x data 6-36
Analysis and Export of ACS 4.x Data
  Consolidating Data 6-37
Analyze the ACS 4.x data 3-7
Analyzing the ACS 4.x data 6-36
Appliance Support
  ACS 4.x Appliance 4-2
  CSACS-1121 Appliance 4-2

B

back up the ACS 4.x Windows source machine 5-1
back up the ACS 5.5 target machine 5-2

C

Command Set Migration 6-50
Command Shell Migration 6-49
Configuration differences between ACS 4.x and 5.5
  Network Resources
    external RADIUS servers 2-6
    network device groups 2-2
  Policy Elements
    session conditions 2-12
System Administration
  administrators 2-16
  configuration 2-16
  downloads 2-16
  operations 2-16
  users 2-16
Users and Identity Stores
  certificate authorities and certificate authentication profiles 2-10
  external identity stores 2-10
  identity groups 2-7
  identity store sequences 2-11
  internal identity stores 2-9
  configuration mapping 8-1
  configure your environment for migration 5-1
  confirm 6-47
  consolidating data 6-37

D

Data Migration and Deployment Scenarios 5-5
  in a distributed environment 5-5
  in a single ACS appliance 5-5
Deployment differences between ACS 4.x and 5.5
  Configuration 1-4
  Identity Stores 1-3
  Licensing 1-4
  Logging 1-3
  Performance 1-6
  Replication 1-2
Index

Server Deployment Recommendations 1-5
Windows Versus Linux Based Application 1-2
Downloadable ACL in ACS 4.x 6-53

F

feature comparison C-1
AAA proxy support C-2
access policy C-4
account disablement C-4
ACS administrators C-5
ACS password policy C-4
application integration C-1
components C-1
configuration query/provisioning C-2
distributed models C-2
identity store support C-2
logging destinations C-2
management C-3
network devices C-4
platform support C-1
supported protocols C-3
TACACS+ C-3

Migration issues
resolving D-3
Migration log file D-16
Migration Methods 3-1
about the Migration Utility 3-3
CSV import tool 3-2
Migration Utility 3-1
Migration phases 3-4
analysis phase 3-4
migration phase 3-4
migration process 3-7, 3-8
Migration Script 6-5
migration software accessory kit DVD and CDs 5-3, 5-4
migration support 4-1
Migration Utility
Errors D-6
Migration Utility Files
accessing 5-4
extracting 5-4
Migration Utility options 6-9
Migration Utility reports 6-40
Multi Instance Migration 3-5

N

Network Device Group Migration 6-51

R

Report Types
Analyze and Export Full Report 6-42
Analyze and Export Summary Report 6-42
Import Full Report 6-44
Import Summary Report 6-43
requirements, server 5-2
restore your ACS 5.5 database if import fails 6-37
Running the Migration Utility 6-2
Index

S

server requirements  5-2
Shared key password  A-2
Support
  4.x Appliance  4-2
  4.x Elements  4-3
  ACS 4.x Objects  6-9
    AAA Client/Network Device  6-10
    EAP-Fast Master Keys and Authority ID  6-34
    Internal User  6-16
    NDG  6-14
    RADIUS VSAs  6-32
    Shared DACL Objects  6-29
    Shared RACs  6-30
    User Group  6-23
      User Group Policy Components  6-24
  CSACS-1120  4-2
  Migration Support  4-1
  Multiple Instance  4-2
  Remote Desktop  4-2
system requirements  5-2
  server  5-2

T

Troubleshooting  D-1

U

User Group  A-3
  policy components  A-4
User policy components  A-3