Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x

October 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25542-01

Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x

CONTENTS

Preface

Revised: October 4, 2013, OL-25542-01

This migration guide covers both Cisco Identity Services Engine Releases 1.1 and 1.1.x. This guide describes the process for migrating data from a Cisco Secure Access Control System (ACS) Release 5.1/5.2 database to a Cisco Identity Services Engine (ISE) Release 1.1 appliance. The migration process uses the Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Migration Tool. This section of the migration guide introduces the purpose, audience, and organization of the guide and covers the following topics:

Purpose of this Guide

This migration guide is part of the Cisco ISE 1.1 documentation set, and it describes how to migrate existing data from a Cisco Secure ACS Release 5.1/5.2 database to a Cisco ISE 1.1 appliance by using the Cisco Secure ACS to Cisco ISE Migration Tool. This migration guide contains the following information:

Note For the remainder of this migration guide, the Cisco Secure ACS to Cisco ISE Migration Tool (and its shorter form, Cisco Secure ACS-Cisco ISE Migration Tool) describe the tool that is used to migrate data from a Cisco Secure ACS 5.1/5.2 database to a Cisco ISE 1.1 appliance.

- Cisco Secure ACS-Cisco ISE Migration Tool installation requirements, prerequisites, and guidelines for migration.
- List of Cisco Secure ACS Release 5.1/5.2 data items that can be migrated and a list of the data items that cannot be migrated.

- Step-by-step procedures for migrating data from a Cisco Secure ACS 5.1/5.2 database to the Cisco ISE 1.1 appliance.
- Reference links to Cisco documentation that defines the upgrade path that is required by earlier releases of Cisco Secure ACS data (Release 3.x and 4.x) before it can be migrated.

Note The Cisco Secure ACS-Cisco ISE Migration Tool only supports migrating Cisco Secure ACS Release 5.1/5.2 data.

To migrate previous releases of Cisco Secure ACS data (for example, 3.x or 4.x) to the Cisco Secure ACS 5.1/5.2 state from which it can be migrated to a Cisco ISE 1.1 appliance, requires a multi-step process:

1. Upgrade the Cisco Secure ACS 3.x or 4.x data to the Cisco Secure ACS Release 5.0 state by using the process described in the Cisco documentation (see Related Documentation in this Preface).
2. Upgrade the Cisco Secure ACS 5.0 data to Cisco Secure ACS Release 5.1/5.2 state by using the process described in the Cisco documentation (see Related Documentation in this Preface).
3. Use the Cisco Secure ACS-Cisco ISE Migration Tool to migrate Cisco Secure ACS 5.1/5.2 data to a Cisco ISE 1.1 appliance using the procedure in this migration guide (see Chapter 4, "Using the Cisco Secure ACS-Cisco ISE Migration Tool").

The focus of this migration guide is on documenting the process for using the Cisco Secure ACS-Cisco ISE Migration Tool to export existing Cisco Secure ACS 5.1/5.2 data and for importing this data into a Cisco ISE 1.1 appliance.

We recommend that you fully understand the related data structure and schema differences between the Cisco Secure ACS 5.1/5.2 and the Cisco ISE 1.1 systems before you attempt to migrate existing Cisco Secure ACS data.

Audience

This migration guide is for network administrators who are responsible for migrating existing Cisco Secure ACS 5.1/5.2 database information to a Cisco ISE 1.1 appliance by using the Cisco Secure ACS-Cisco ISE Migration Tool.

Organization

This migration guide includes the following sections:

Title	Description
Chapter 1, "Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Migration Overview"	Provides an overview of the Cisco Secure ACS-Cisco ISE migration, the software requirements, supported releases, application components, data items that can be migrated, and the software architecture.
Chapter 2, "Understanding the Cisco Secure ACS-Cisco ISE Migration Tool"	Provides a functional description of the Cisco Secure ACS-Cisco ISE Migration Tool, which supports export and import, data persistency, scalability, high availability, and reporting functions.

Title	Description
Chapter 3, "Installing the Cisco Secure ACS-Cisco ISE Migration Tool"	Describes requirements, installation prerequisites and guidelines, and how to install and set up the Cisco Secure ACS-Cisco ISE Migration Tool.
Chapter 4, "Using the Cisco Secure ACS-Cisco ISE Migration Tool"	Describes how to use the Cisco Secure ACS-Cisco ISE Migration Tool to perform operations that export Cisco Secure ACS 5.1/5.2 data from its database and import the migrated data into a Cisco ISE 1.1 appliance.
Chapter 5, "Migrating Data from the Cisco Secure ACS 3.x and 4.x to the ACS 5.1/5.2"	Provides a brief overview and provides documentation links that you need to upgrade earlier releases of Cisco Secure ACS data to the Cisco Secure ACS Release 5.0 state. The only supported migration path for earlier Cisco Secure ACS releases is to upgrade the data to the Cisco Secure ACS Release 5.0 state. Once at the Cisco Secure ACS Release 5.0 state, there is a supported path for upgrading this data to Cisco Secure ACS Release 5.1/5.2.
Appendix A, "Cisco Secure ACS 5.1/5.2 and Cisco ISE 1.1 Data Structure Mapping"	Provides a mapping table that describes how the data objects are mapped between a Cisco Secure ACS Release 5.1/5.2 system and a Cisco ISE 1.1 system.
Appendix B, "Troubleshooting the Cisco Secure ACS-Cisco ISE Migration Tool"	Describes how to troubleshoot any issues that you might encounter when using the Cisco Secure ACS-Cisco ISE Migration Tool.

How to Use this Guide

We recommend that you read and reference the following sections before attempting to migrate Cisco Secure ACS Release 5.1/5.2 data to a Cisco ISE 1.1 appliance:

- See Appendix A, "Cisco Secure ACS 5.1/5.2 and Cisco ISE 1.1 Data Structure Mapping" to ensure that you understand the data object, schema, and attribute differences between Cisco Secure ACS and Cisco ISE prior to migration.
- See Chapter 1, "Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Migration Overview" for an overview of the Cisco Secure ACS 5.1/5.2 database, data objects, architecture, and the process of migrating its data to the Cisco ISE 1.1 appliance.
- See Chapter 2, "Understanding the Cisco Secure ACS-Cisco ISE Migration Tool" to understand the functional and configuration differences and similarities between Cisco Secure ACS 5.1/5.2 and Cisco ISE 1.1, and for specific configuration recommendations.
- See Chapter 3, "Installing the Cisco Secure ACS-Cisco ISE Migration Tool" to understand how to install the Cisco Secure ACS-Cisco ISE Migration Tool.
- See Chapter 4, "Using the Cisco Secure ACS-Cisco ISE Migration Tool" to understand the process that is required for migrating existing Cisco Secure ACS 5.1/5.2 data to Cisco ISE 1.1 using the Cisco Secure ACS-Cisco ISE Migration Tool.

Documentation Conventions

This migration guide uses the following documentation conventions:

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

Caution Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Note Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in this migration guide.

Documentation Updates

Table 1 Updates to Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x

Date	Description
10/31/12	Cisco Identity Services Engine, Release 1.1.2
7/10/12	Cisco Identity Services Engine, Release 1.1.1
3/19/12	Cisco Identity Services Engine, Release 1.1

Related Documentation

Release-Specific Documents

Table 2 lists the product documentation available for the Cisco ISE Release. General product information for Cisco ISE is available at http://www.cisco.com/go/ise. End-user documentation is available on Cisco.com at http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html.

Table 2 Product Documentation for Cisco Identity Services Engine

Document Title	Location
• *Release Notes for the Cisco Identity Services Engine, Release 1.1* • *Release Notes for the Cisco Identity Services Engine, Release 1.1.x*	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
• *Cisco Identity Services Engine Network Component Compatibility, Release 1.1* • *Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x*	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
• *Cisco Identity Services Engine User Guide, Release 1.1* • *Cisco Identity Services Engine User Guide, Release 1.1.x*	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
• *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1* • *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x*	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Upgrade Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine API Reference Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine Troubleshooting Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html

Table 2 Product Documentation for Cisco Identity Services Engine (continued)

Document Title	Location
Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html

Platform-Specific Documents

Links to other platform-specific documentation are available at the following locations:

Cisco ISE
http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html

- Cisco Secure ACS
  http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html
- Cisco NAC Appliance
  http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html
- Cisco NAC Profiler
  http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
- Cisco NAC Guest Server
  http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation and Submitting a Service Request

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

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

Subscribe to the *What's New in Cisco Product Documentation* as a 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.

CHAPTER 1

Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Migration Overview

This chapter provides a brief overview of Cisco Identity Services Engine (ISE) and Cisco Secure Access Control System (ACS). The following topics are discussed in this chapter:

Overview

The Cisco ISE deployment model consists of one primary node with multiple secondary nodes. Each Cisco ISE node in a deployment can take any one or more of the following personas: Administration, Policy Service, and Monitoring.

After you install Cisco ISE, all the nodes will be in the standalone state. You must define one of your Cisco ISE nodes to be the primary (running as an Administration persona). After you have defined the primary node, you can configure other Cisco ISE node personas such as Policy Service and Monitoring for the network. You can then register other secondary nodes with the primary node and define specific roles for each of them.

When you register an Cisco ISE node as a secondary node, Cisco ISE immediately creates a database link from the primary to the secondary node and begins the process of replication. All configuration changes are made on the primary Administration ISE node and are replicated to the secondary nodes. The Monitoring ISE node acts as the log collector.

Cisco Secure Access Control System (ACS) deployment model consists of a single primary and multiple secondary Cisco Secure ACS servers, where configuration changes are made on the primary Cisco Secure ACS server. These configurations are replicated to the secondary Cisco Secure ACS servers.

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

The Cisco Secure ACS and Cisco ISE may exist on different hardware platforms and have different operating system, database, and information model. Therefore, you cannot perform a standard upgrade from the Cisco Secure ACS to Cisco ISE.

Instead, a migration tool and procedure is available that reads the data from the Cisco Secure ACS and creates corresponding data in the Cisco ISE. You can also use this migration procedure in cases where Cisco Secure ACS and Cisco ISE use the same hardware; the CSACS-1121 appliance. The Cisco Secure ACS 5.1/5.2 to the Cisco ISE 1.1 migration process requires minimum user interaction, and the full set of configuration data is migrated from the Cisco Secure ACS to the Cisco ISE.

Supported Migration from the Cisco Secure ACS to the Cisco ISE

The Cisco ISE supports data migration from the Cisco Secure ACS 5.1 and 5.2 by using the Cisco Secure ACS-ISE 1.1 Migration Tool. If you are running Cisco Secure ACS 3.x or Cisco Secure ACS 4.x, you must first upgrade to Cisco Secure ACS 5.0.

After you reach the Cisco Secure ACS 5.0 level, you can then upgrade to Cisco Secure ACS 5.1 or 5.2. At this point, you can then migrate to Cisco ISE 1.1 by using the Cisco Secure ACS-ISE Migration Tool.

Note A direct upgrade is available from the Cisco Secure ACS 5.0 to the Cisco Secure ACS 5.1/5.2. You must first complete upgrading all previous Cisco Secure ACS releases to Cisco Secure ACS 5.1/5.2 before you attempt to migrate any Cisco Secure ACS data to Cisco ISE.

For information on migrating data from the Cisco Secure ACS 3.x or 4.x to the Cisco Secure ACS 5.0, see Chapter 5, “Migrating Data from the Cisco Secure ACS 3.x and 4.x to the ACS 5.1/5.2.”

Software Requirements

Table 1-1 lists the minimum software requirements for migration in the Cisco ISE 1.1.

Table 1-1 Software Requirements for Migration in the Cisco ISE 1.1

Operating System	The Cisco Secure ACS-Cisco ISE Migration Tool runs on Windows and Linux machines. The machine should have JAVA installed on it. For more details, see “System Requirements” section on page 3-2.
Minimum disk space	the minimum disk space required is 1 GB This space is required not only for the installation of the migration tool, but also because the migration tool will store the migrated data and will generate reports and logs.
Minimum RAM	The minimum RAM required is 2 GB. If you have about 300,000 users, 50,000 hosts, 50,000 network devices, then we recommend that you have a minimum of 2 GB of RAM.

Before running the Cisco Secure ACS-Cisco ISE Migration Tool, make sure that you have upgraded to Cisco ISE Release 1.1 and have installed the latest patches for ACS 5.1 and 5.2.

Functional Description

The migration tool is responsible for transferring the Cisco Secure ACS data into Cisco ISE and there are three major steps:

1. Export data from the Cisco Secure ACS.
2. Persist data in the migration tool.
3. Import data into the Cisco ISE 1.1.

The following are the major features of the Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 migration process:

Export

The first stage in the migration process is to export ACS data using the Cisco Secure ACS Programmatic Interface (PI). You have to provide the credentials to connect with the Cisco Secure ACS and request to export the Cisco Secure ACS data into the migration application. During this time the exported data must be validated to verify if it can be imported into a Cisco ISE 1.1 appliance successfully. In cases where the data is invalid, this status is logged in the migration report.

Data Persistency

The Cisco ISE does not support an upgrade from the Cisco Secure ACS to the Cisco ISE 1.1. Therefore, if you want to upgrade your Cisco Secure ACS appliance to the Cisco ISE, you have to uninstall the Cisco Secure ACS and reimage the appliance with the Cisco ISE 1.1 image. The migration tool persists the Cisco Secure ACS data before the reimage takes place and before the next stage (import) begins. The persisted data is in an encrypted format.

Import

At the import stage, the migration tool contains information from the Cisco Secure ACS and is ready to import the data into the Cisco ISE 1.1. If you use the same machine to install Cisco ISE, you have to reimage the Cisco Secure ACS machine with the Cisco ISE 1.1 image and start the import operation. If you want to use a different machine for the Cisco ISE, it should be a clean machine right after installation and without any configuration on it.

You can view the import progress through the Cisco Secure ACS-Cisco ISE Migration Tool user interface. You can see the object types that are being transferred and how many objects are pending for delivery. Any errors during this process are logged in the migration report.

Scalability

The migration application supports object scale as described in Table 1-2.

Table 1-2 Object Scalability for Migration in the Cisco ISE 1.1

Objects	Small Deployment	Medium Deployment	Large Deployment
Users (AD[1]/LDAP[2]/internal) - per deployment	1,000	10,000	25,000
Hosts/endpoints	1,000	10,000	100,000
Network devices	500	1,000	10,000
Identity groups	1	5	20
Authorization profiles	5	10	30
User dictionaries	2	5	20
User attributes	1	5	8
User groups	2	10	100
DACLs[3] (each contain 1,600 entries)	5	20	50

1. AD is an acronym for Microsoft Windows Active Directory (see Active Directory in the Glossary).
2. LDAP is an acronym for Lightweight Directory Access Protocol (see LDAP in the Glossary).
3. DACL is an acronym for downloadable access control list (see DACL in the Glossary).

High Availability

The Cisco Secure ACS-Cisco ISE Migration Tool maintains the state at each stage of the import or export operation. This means that if the process of importing or exporting fails at any point due to import or export failure, you need not start from the beginning, but from the last checkpoint before the failure occurred.

If the migration process fails during the import or export phase, the migration tool terminates the process. If you restart the migration tool after a failure, a dialog box is displayed.

You can either choose to resume the previous import/export or discard the previous process and start a new migration process. If you choose to resume the previous process, the migration process resumes from the last object type. Resuming from a failure also resumes the report to run from the previous process.

Reporting

Three Cisco ISE reports are available while migrating the Cisco Secure ACS 5.1/5.2 data to the Cisco ISE appliance by using the Cisco Secure ACS-Cisco ISE Migration Tool:

- **Export Report**: Indicates specific information or errors that are encountered during the export of data from the Cisco Secure ACS database. See Figure 1-1.

  The export report includes error information for objects that are exported but will not be imported. It contains a data analysis section at the end of the report, which describes the functional gap analysis in the data between the Cisco Secure ACS and the Cisco ISE.

- **Import Report**: Indicates specific information or errors that are encountered during the import of data into the Cisco ISE appliance. See Figure 1-2.

- **Policy Gap Analysis Report**: Indicates specific information that is related to the policy gap between the Cisco Secure ACS and the Cisco ISE. See Figure 1-3.

  The Cisco ISE 1.1 introduces this new report, which is available after the export completes. To view the report, click on the **Policy Gap Analysis Report** button in the user interface.

  If any authentication or authorization policy is not migrated, it is listed in this report. This report lists all the incompatible rules and conditions that are related to policies. It describes data that cannot be migrated and the reason for a manual workaround.

  Some conditions can be migrated by using the Cisco ISE terminology; for example, “Device Type In” is migrated as “Device Type Equals”. In such cases, the condition is automatically migrated. If the condition is supported or can be automatically translated, it does not appear in the report. If one or more condition is found as “Not Supported” or “Partially supported,” the whole policy is not imported, and such conditions appear in the report.

Table 1-3 describes the report type, the message type, and message contents in the import and export reports.

Table 1-3 Cisco Secure ACS 5.1/5.2-Cisco ISE Migration Tool Reports

Report Type	Message Type	Message Description
Export	Informational	Lists the names of the data objects that were exported successfully.
	Warning	Lists an error that is based on an export failure or an export not attempted because the data object is not supported by Cisco ISE 1.1 (for example, if it were a TACACS-based device).

Table 1-3 Cisco Secure ACS 5.1/5.2-Cisco ISE Migration Tool Reports (continued)

Report Type	Message Type	Message Description
Import	Informational	Lists the names of the data objects that were imported successfully.
	Error	Identifies a data object error in which it cannot be imported because it already exists (duplicate).
	Error	Identifies a data object error in which it cannot be imported because the name length exceeds the Cisco ISE character limit.
	Error	Identifies a data object error in which it cannot be imported because the name includes special character that Cisco ISE does not support.
	Error	Identifies a data object error in which it cannot be imported because the object includes data character that is not available or supported in Cisco ISE.

Figure 1-1 Example of Export Report

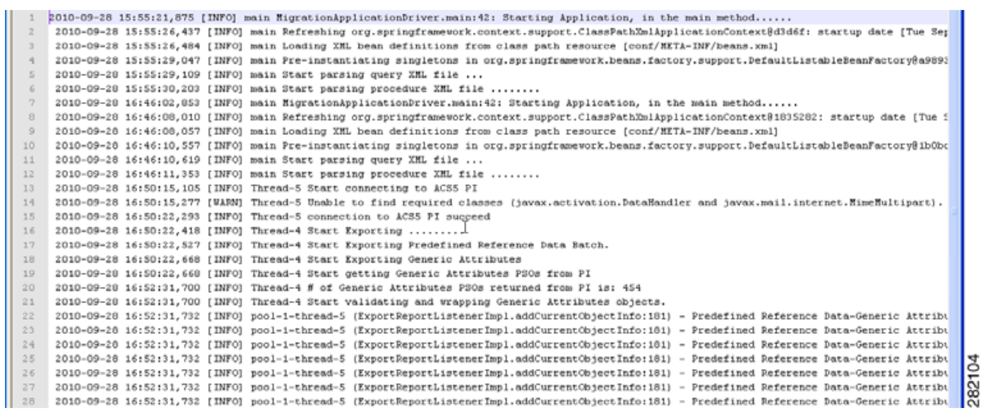
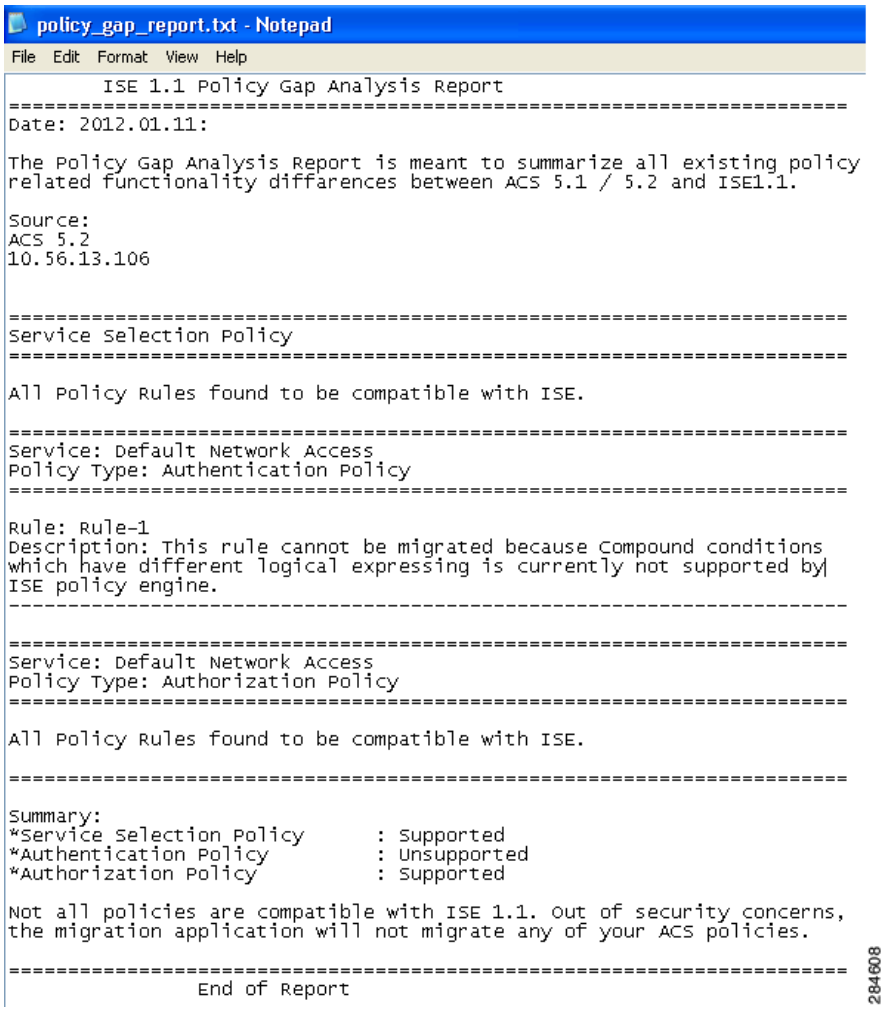


Figure 1-2 Example of Import Report

```
=========================================================
Migration Report
Migration Phase: Import into ISE
Date: Tue Sep 28 17:05:59 IST 2010
Machine: 10.56.13.190
=========================================================


==========================Object Group==============================
Object Group: Predefined Reference Data
==========================Object Group==============================
Object Group: Dictionaries
==========================Object Type===============================
Object Type: VSA Vendors

Info Type: INFO
> 2010.09.28 17:06:07'055 : Added configuration: Cisco VPN 5000
> 2010.09.28 17:06:07'945 : Added configuration: US Robotics
> 2010.09.28 17:06:08'633 : Added configuration: Ascend
> 2010.09.28 17:06:09'367 : Added configuration: Nortel ( Bay )
> 2010.09.28 17:06:10'117 : Added configuration: RedCreek
> 2010.09.28 17:06:10'867 : Added configuration: Juniper
> 2010.09.28 17:06:11'586 : Added configuration: Cisco Aironet
> 2010.09.28 17:06:12'320 : Added configuration: Cisco Airespace

==========================Object Type===============================
Object Type: RADIUS VSAs

Info Type: INFO
> 2010.09.28 17:06:13'523 : Added configuration: Cisco
> 2010.09.28 17:06:14'148 : Added configuration: Cisco
> 2010.09.28 17:06:14'774 : Added configuration: Cisco
> 2010.09.28 17:06:15'477 : Added configuration: Cisco
> 2010.09.28 17:06:16'086 : Added configuration: Cisco
> 2010.09.28 17:06:16'680 : Added configuration: Cisco
> 2010.09.28 17:06:17'430 : Added configuration: Cisco
> 2010.09.28 17:06:18'242 : Added configuration: Cisco
> 2010.09.28 17:06:18'867 : Added configuration: Cisco
> 2010.09.28 17:06:19'477 : Added configuration: Cisco
> 2010.09.28 17:06:20'070 : Added configuration: Cisco
> 2010.09.28 17:06:20'664 : Added configuration: Cisco
> 2010.09.28 17:06:21'305 : Added configuration: Cisco
> 2010.09.28 17:06:21'914 : Added configuration: Cisco
> 2010.09.28 17:06:22'539 : Added configuration: Cisco
> 2010.09.28 17:06:23'180 : Added configuration: Cisco
> 2010.09.28 17:06:23'774 : Added configuration: Cisco
> 2010.09.28 17:06:24'383 : Added configuration: Cisco
```

282105

Figure 1-3 Example of Policy Gap Analysis Report



UTF-8 Support

The Cisco ISE 1.1 supports Universal Character Set Transformation Format 8 bit (UTF-8) for some administration configuration. The following configuration items are exported and imported with UTF-8 encoding:

- **Network Access user configuration**
  - User name
  - Password and re-enter password
  - First name
  - Last name
  - Email
- **RSA:** RSA prompts and messages are shown to the end user by the supplicant.
  - Messages
  - Prompts

- **RADIUS Token**: RADIUS token prompt is presented on the end-user supplicant.
  - Authentication Tab > Prompts
  - Administrator Configuration
  - Administrator username and password
  - Configure administrator by using UTF-8
- **Policies**:
  - Authentication > Value for AV expression
  - Authorization > Other Conditions > Value for AV expression
  - Attribute-value conditions
  - Authentication > Simple Condition/compound Condition > Value for AV expression
  - Authorization > Simple Condition/compound Condition > Value for AV expression

FIPS Support for ISE 802.1X Services

In order to support Federal Information Processing Standard (FIPS), the Cisco Secure ACS-Cisco ISE Migration Tool migrates the default network device keywrap data.

Note The Cisco ISE FIPS mode should not be enabled before the migration process is complete.

FIPS-compliant and supported protocols:

- Process Host Lookup
- Extensible Authentication Protocol-Translation Layer Security (EAP-TLS)
- Protected Extensible Authentication Protocol (PEAP)
- EAP-Flexible Authentication via Secure Tunneling (FAST)

FIPS-noncompliant and unsupported protocols:

- EAP-Message Digest 5 (MD5)
- Password Authentication Protocol and ASCII
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1)
- Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2)
- Lightweight Extensible Authentication Protocol (LEAP)

Cisco Secure ACS/Cisco ISE Version Validation

The Cisco Secure ACS-Cisco ISE Migration tool identifies the Cisco Secure ACS version before the export phase begins. The migration process will not start if the Cisco Secure ACS version is lower than 5.1 or higher than 5.2. In addition, before importing the data to the Cisco ISE, the tool verifies that the Cisco ISE version is 1.1.

CHAPTER 2

Understanding the Cisco Secure ACS-Cisco ISE Migration Tool

This chapter provides information about the Cisco Secure Access Control System (ACS)-Cisco Identity Services Engine (ISE) Migration Tool that is used to migrate data from a Cisco Secure ACS Release 5.1/5.2 database to the Cisco ISE Release 1.1 appliance. The following topics describe what you should know about the Cisco Secure ACS-Cisco ISE Migration Tool before using it to migrate data:

Overview: Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1

The Cisco Secure ACS-Cisco ISE Migration Tool is designed to provide users that have an existing installed Cisco Secure ACS 5.1/5.2 database with a method for transporting that data to a Cisco ISE 1.1 appliance. The design of the tool addresses the inherent migration problems that result from differences in the underlying hardware platforms and systems, databases, and data schemes. There are three steps in the migration process by using the Cisco Secure ACS-Cisco ISE Migration Tool include:

- Exporting the Cisco Secure ACS 5.1/5.2 data from its database
- Persisting this data by using the migration tool
- Importing the persisted data into the Cisco ISE 1.1 appliance

The Cisco Secure ACS-Cisco ISE Migration Tool supports the migration of only Cisco Secure ACS 5.1/5.2 data to a Cisco ISE 1.1 appliance. For example, you can use the Cisco Secure ACS-Cisco ISE Migration Tool to perform the following data migration steps:

1. Export the Cisco Secure ACS 5.1/5.2 data from the Cisco Secure ACS-1121 hardware appliance to a secure external server with a database.
2. Back up the Cisco Secure ACS data.
3. Reimage the Cisco Secure ACS-1121 hardware appliance, which is the same physical hardware as the Cisco ISE 3315 appliance, with the Cisco ISE 1.1 software.
4. Import the converted Cisco Secure ACS Release 5.1/5.2 data from the secure external server into the Cisco ISE 1.1 appliance.

The only supported direct migration process that uses Cisco Secure ACS-Cisco ISE Migration Tool is from a Cisco Secure ACS 5.1/5.2 system to a Cisco ISE 1.1 appliance. However, you upgrade earlier versions of Cisco Secure ACS data to a Cisco Secure ACS 5.1/5.2 state by using the options that are listed in Table 2-1.

The Cisco Secure ACS-Cisco ISE Migration Tool *migrates* data from a Cisco Secure ACS 5.1/5.2 system to a Cisco ISE 1.1 appliance, which is a different process from an *upgrade* that is used for earlier versions of Cisco Secure ACS 3.x to 4.x.

Table 2-1 Cisco Secure ACS Release Data Upgrade Options

ACS Release Version	Upgrade to ACS Release	ACS Data Upgrade References
Cisco Secure ACS Release 3.x	Cisco Secure ACS Release 5.0	• Chapter 5, "Migrating Data from the Cisco Secure ACS 3.x and 4.x to the ACS 5.1/5.2"
Cisco Secure ACS Release 4.x	Cisco Secure ACS Release 5.0	• Chapter 5, "Migrating Data from the Cisco Secure ACS 3.x and 4.x to the ACS 5.1/5.2"
Cisco Secure ACS Release 5.0	Cisco Secure ACS Release 5.1/5.2	• Chapter 5, "Migrating Data from the Cisco Secure ACS 3.x and 4.x to the ACS 5.1/5.2"

Note For information and documentation links about migrating Cisco Secure ACS 3.x and 4.x to 5.0 to Cisco Secure ACS 5.1/5.2, see Chapter 5, "Migrating Data from the Cisco Secure ACS 3.x and 4.x to the ACS 5.1/5.2." Chapter 5 also provides information and documentation links about migrating Cisco Secure ACS 5.0 to Cisco Secure ACS 5.1/5.2.

Cisco Secure ACS-Cisco ISE Migration Tool

This section describes:

The Cisco Secure ACS-Cisco ISE Migration Tool runs on Windows-based systems, and it works by importing the Cisco Secure ACS data files, analyzing the data, and making required data modifications that are necessary for importing the data into a format that is usable by the Cisco ISE 1.1 system.

The Cisco Secure ACS 5.1/5.2 and Cisco ISE 1.1 applications may or may not run on the same type of physical hardware. The Cisco Secure ACS-Cisco ISE Migration Tool uses the Cisco Secure ACS Programmatic Interface (PI) and the Cisco ISE representational state transfer (REST) application programming interfaces (APIs). The Cisco Secure ACS PI and the Cisco ISE REST APIs allow the Cisco Secure ACS and ISE applications to run on any of the supported hardware platforms or VMware servers.

Because the Cisco Secure ACS is considered a closed appliance, running the migration tool directly on the Cisco Secure ACS-1121 appliance is not permitted. Instead, the Cisco Secure ACS PI reads and returns the ACS configuration data in a normalized form. The Cisco ISE REST APIs perform validation and normalize the exported Cisco Secure ACS data to persist it in a form usable by Cisco ISE software.

Note You should run the migration tool only after a fresh Cisco ISE installation or after you have reset the Cisco ISE application configuration and clear the Cisco ISE database using the **application reset-config** command. Therefore, the Cisco ISE FIPS mode should not be enabled before the migration process is complete.

Figure 2-1 explains the deployment scenario when Cisco Secure ACS and Cisco ISE are installed on different appliances (dual-appliance deployment).

Figure 2-1 Cisco Secure ACS and Cisco ISE Installed on Different Appliances

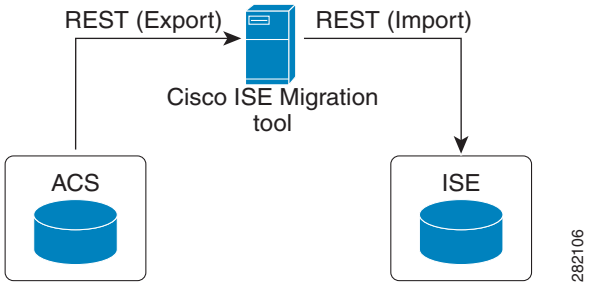


Figure 2-2 shows the deployment scenario when Cisco Secure ACS is installed on the same appliance upon which the Cisco ISE software will be installed (single-appliance deployment). In a single-appliance deployment, complete the following steps:

Step 1 Install the Cisco Secure ACS-Cisco ISE Migration Tool on a standalone Windows machine.

Step 2 Export the Cisco Secure ACS 5.1/5.2 data from the Cisco Secure ACS appliance.

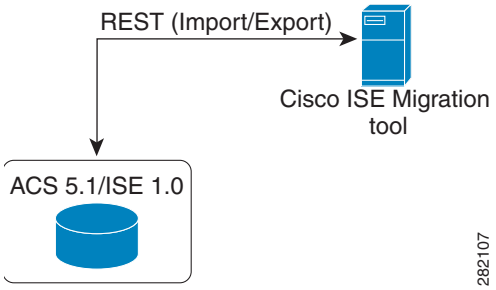
Step 3 Back up the Cisco Secure ACS data.

Step 4 Reimage the appliance with the Cisco ISE 1.1 software.

Step 5 Import the Cisco Secure ACS 5.1/5.2 data into the Cisco ISE 1.1 appliance.

Note When you are ready to start migrating Cisco Secure ACS 5.1/5.2 data to a Cisco ISE appliance, make sure that it is to a standalone Cisco ISE node. Only after migration has been successfully completed should you begin the any deployment configuration (such as setting up Administrator ISE and Policy Service ISE personas). It is a requirement that the migration import phase be performed on a "clean" new installation of the Cisco ISE software on a supported hardware appliance. See the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*, for the list of supported hardware appliance.

Figure 2-2 Cisco Secure ACS and Cisco ISE Installed on a Single Appliance



Migration Tool Components

The migration application consists of the following components:

Data Configuration

A minimal set of configuration data is needed as input at the beginning of the migration process and the application then proceeds to migrate the full set of configuration items. You must enter the IP address (or hostname) of the primary Cisco Secure ACS server and the Cisco ISE server, along with the administrator credentials. After you have been authenticated, the Cisco Secure ACS-Cisco ISE Migration Tool proceeds to migrate the full set of configured data items in a form similar to an upgrade.

Usually no additional operator intervention is required after the migration process starts. However, as the migration progresses, some data may not be mapped automatically between the two applications. The administrator handling the migration is notified of this type of data, which must be resolved before the migration is complete.

Status Reporting

As the migration proceeds, you can monitor the real-time migration status along with the progress of that activity. In case of troubleshooting, detailed logs are available and accessible within the migration tool.

Export and Import

You can perform import and export operations as discrete operations or in sequence. These steps may take a long time, depending upon the amount of data being migrated. So the migration tool periodically displays the checkpoints with the status of the activity being performed. These checkpoints allow you to restart the migration process from the checkpoint in case of any failure.

Export and Data Persistence

The export component is active during the migration phase when Cisco Secure ACS data is exported from the Cisco Secure ACS 5.1/5.2 database using the Cisco Secure ACS PI. You can start the export process after you connect with the Cisco Secure ACS system, request that data be exported, and are authenticated.

A direct upgrade from the Cisco Secure ACS to the Cisco ISE is not supported. The Cisco Secure ACS-Cisco ISE Migration Tool assists you if you want to uninstall the Cisco Secure ACS5.1/5.2 software and reimage the physical hardware with the Cisco ISE 1.1 software. The migration tool persists the Cisco Secure ACS data while the reimage process is completing and before the import stage begins.

Data Analysis and Import

During the export phase, the Cisco Secure ACS-Cisco ISE Migration Tool reads and analyzes the data from the Cisco Secure ACS to confirm that it can be created correspondingly on the Cisco ISE appliance. Since the Cisco Secure ACS and Cisco ISE Policy model are not same, some of the ACS data might not be supported by ISE. The tool reports any issue with the data, which may require administrator intervention at the end of the export phase.

Data Structure Mapping

Data structure mapping from the Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 is the process by which each of the data objects are analyzed and validated during the export phase by the Cisco Secure ACS-Cisco ISE Migration Tool. For a complete list of the data information mapping that takes place during export, see the table in Appendix A, "Cisco Secure ACS 5.1/5.2 and Cisco ISE 1.1 Data Structure Mapping".

CHAPTER 3

Installing the Cisco Secure ACS-Cisco ISE Migration Tool

This chapter provides information about installing the Cisco Secure Access Control System (ACS)-Cisco Identity Services Engine (ISE) Migration Tool, describes important migration tool installation considerations, and describes the migration process in the following topics:

Migration Tool Installation Guidelines

Before you begin the installation, observe the following guidelines:

- Ensure that your environment is ready for migration. In addition to your Cisco Secure ACS 5.1/5.2 Windows or Linux source machine, you must deploy a secure external system with a database for either the single- or dual-appliance migration, and a Cisco ISE 1.1 appliance as your target system.
- Ensure that you have configured the Cisco Secure ACS 5.1/5.2 source machine with a single IP address. The migration tool may fail during migration if each interface has multiple IP address aliases.
- Ensure that you have a backup of ACS data in case the migration from ACS to ISE is performed on the same appliance.
- Ensure that you have completed these tasks:
  - Installed Cisco ISE 1.1 on the target machine (if this is a dual-appliance migration).
  - Have the Cisco ISE 1.1 software available to reimage the CSACS-1121 appliance (if this is single-appliance migration).
  - Have all the proper Cisco Secure ACS 5.1/5.2 and Cisco ISE 1.1 credentials and passwords.
- Be able to establish network connections between the source machine and secure external system with a database.

System Requirements

Your Cisco Secure ACS machines must meet the system requirements described in Table 3-1. All documents are available on Cisco.com.

Table 3-1 System Requirements for Migration Machines

Platform	Requirements
Cisco Secure ACS 5.1/5.2 source machine	Refer to the *Installation Guide for Cisco Secure ACS for Windows 5.1*. Ensure that you have configured the Cisco Secure ACS 5.1 source machine to have a single IP address.
Cisco ISE 1.1 target machine	Refer to the following documents: • *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*. • *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1*. This appliance must have at least 2 GB of RAM.
Linux, Windows XP	Install Java JRE, version 1.6 or higher 32 Bit. The migration tool will not run if you do not install Java JRE on the migration machine.
64 Bit Windows 7	Install Java JRE, version 1.6 or higher 64 Bit. The migration tool will not run if you do not install Java JRE on the migration machine.
32 Bit Windows 7	Install Java JRE, version 1.6 or higher 32 Bit. The migration tool will not run if you do not install Java JRE on the migration machine.

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 to know the Cisco Secure ACS 5.1/5.2 and Cisco ISE 1.1 administrator usernames and passwords to export the Cisco Secure ACS data and import it successfully into the Cisco ISE appliance. You should use a reserved username so that records created by the import utility can be identified in the audit log.

Data Migration and Deployment Scenarios

The Cisco Secure ACS-ISE Migration Tool is designed to migrate Cisco Secure ACS 5.1/5.2 data objects to Cisco ISE 1.1. The process of data migration in a single appliance differs from that of appliances in a distributed environment and the following sections address these topics:

- Guidelines for Data Migration from a Single Cisco Secure ACS Appliance, page 3-3
- Guidelines for Data Migration in a Distributed Environment, page 3-3

Guidelines for Data Migration from a Single Cisco Secure ACS Appliance

If you have a single Cisco Secure ACS appliance in your environment (or several Cisco Secure ACS appliances, but not in a distributed setup), run the Cisco Secure ACS-Cisco ISE Migration Tool against the Cisco Secure ACS appliance as described in Logging In and Using the Migration Tool, page 4-1.

Guidelines for Data Migration in a Distributed Environment

You might run Cisco Secure ACS in a distributed environment. For example, if you have one primary Cisco Secure ACS appliance and one or more secondary Cisco Secure ACS appliances that interoperate with the primary appliance. If you run Cisco Secure ACS in a distributed environment, you must:

Step 1 Back up the primary Cisco Secure ACS appliance and restore it on the migration machine.

Step 2 Run the Cisco Secure ACS-Cisco ISE Migration Tool against the primary Cisco Secure ACS appliance.

Note If you have a large internal database, Cisco recommends that you run the migration from a standalone primary appliance and not to a primary appliance that is connected to several secondary appliances. After the completion of the migration process, you can register all the secondary appliances.

Note The Cisco Secure ACS-Cisco ISE Migration Tool may run for approximately 20 hours to migrate 10,000 devices, 25,000 users, 100,000 hosts, 100 identity groups, 420 downloadable access control lists (DACLs), 320 authorization profiles, 6 devices hierarchies, and 20 network device groups (NDGs).

Note When you are ready to start migrating Cisco Secure ACS 5.1/5.2 data to a Cisco ISE appliance, make sure that it is to a standalone Cisco ISE node. Only after migration has been successfully completed should you begin any deployment configuration (such as setting up Administrator ISE and Policy Service ISE personas). It is a requirement that the migration import phase be performed on a “clean” new installation of the Cisco ISE software on a supported hardware appliance.

Installing and Initializing the Cisco Secure ACS-Cisco ISE Migration Tool

Note You should run the migration tool only after a fresh Cisco ISE installation or after you have reset the Cisco ISE application configuration and clear the Cisco ISE database using the **application reset-config** command. Therefore, the Cisco ISE FIPS mode should not be enabled before the migration process is complete.

You can download the Cisco Secure ACS-Cisco ISE Migration Tool files using the Cisco ISE user interface.

To download and run the Cisco Secure ACS-Cisco ISE Migration Tool software, complete the following steps:

Step 1 If your Cisco Secure ACS and Cisco ISE softwares are installed on different appliances, download the migration tool files by entering the following command on the Cisco ISE user interface address bar:

https://<hostname-or-hostipaddress>/admin/migTool.zip

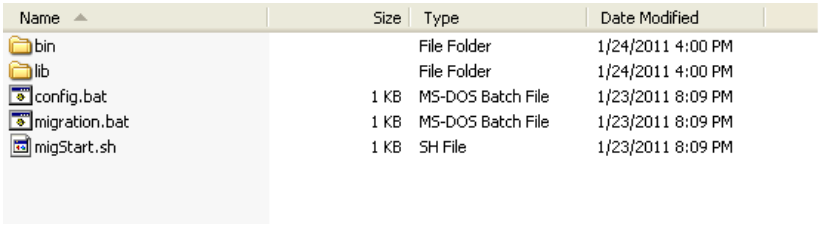
Note The only currently supported browser for downloading the migration tool files is Mozilla Firefox, versions 3.6, 6, 7, 8, 9, and, 10. Microsoft Windows Internet Explorer (IE8 and IE7) browsers are not currently supported in this release.

Step 2 If your Cisco Secure ACS and Cisco ISE softwares are installed on the same appliance, or if you are using a new Cisco ISE hardware appliance, download migTool.zip, the migration tool file from the following location:

http://www.cisco.com/cisco/software/release.html?mdfid=283801620&flowid=26081&softwareid=283802505&release=1.1&relind=AVAILABLE&rellifecycle=&reltype=latest

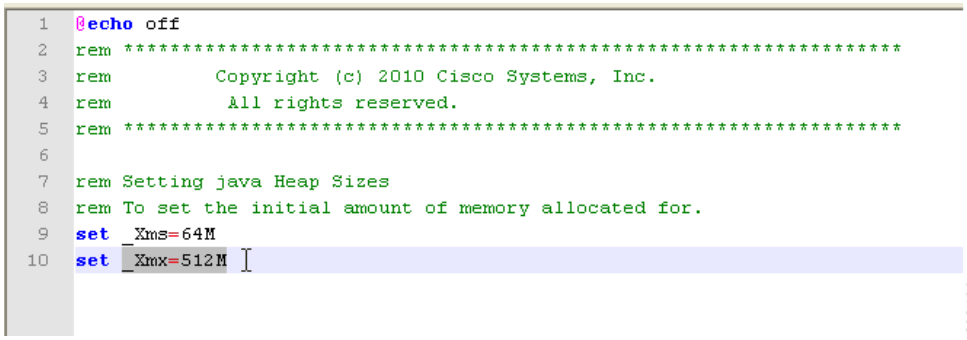
Step 3 Extract the content of the .zip file. Figure 3-1 illustrates the directory structure of the Cisco Secure ACS-Cisco ISE Migration Tool software.

Figure 3-1 Directory Structure of the Cisco ACS 5.1/5.2-Cisco ISE 1.1 Migration Tool



Step 4 Edit the **config.bat** file and allocate the initial amount of memory for the Java heap sizes for the migration process (see Figure 3-2). The memory is 64 and 512 megabytes, respectively.

Figure 3-2 Setting Java Heap Size

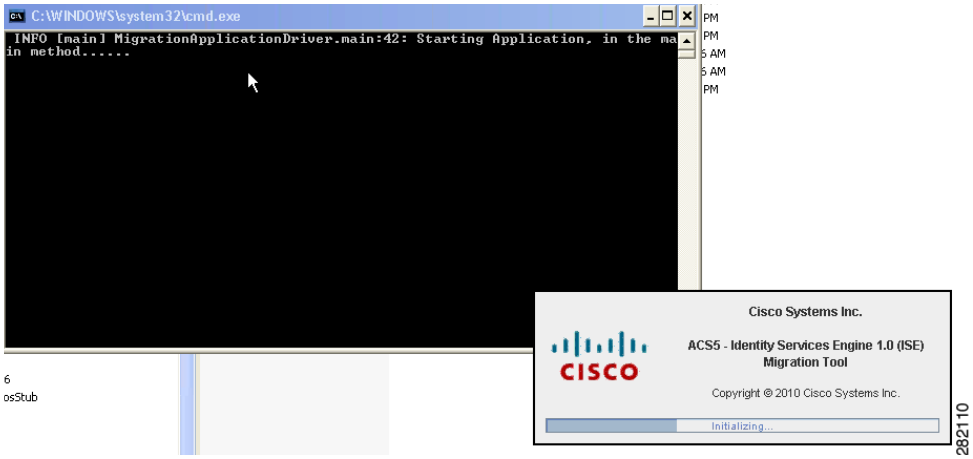


Step 5 Click **Save** to preserve your heap size configuration.

Step 6 Click **migration.bat** to launch the migration process.

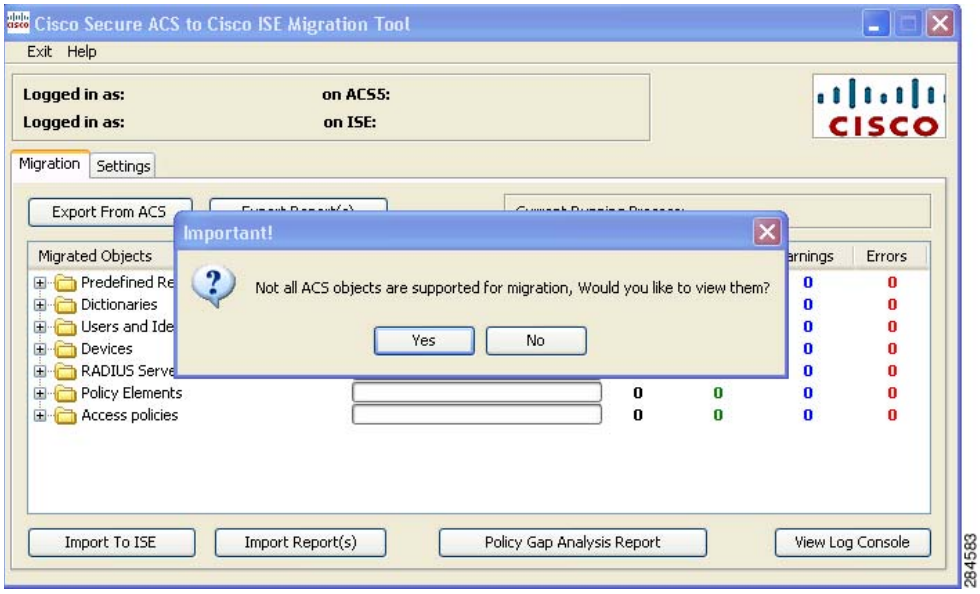
The initializing screen is displayed (see Figure 3-3).

Figure 3-3 Initializing Screen



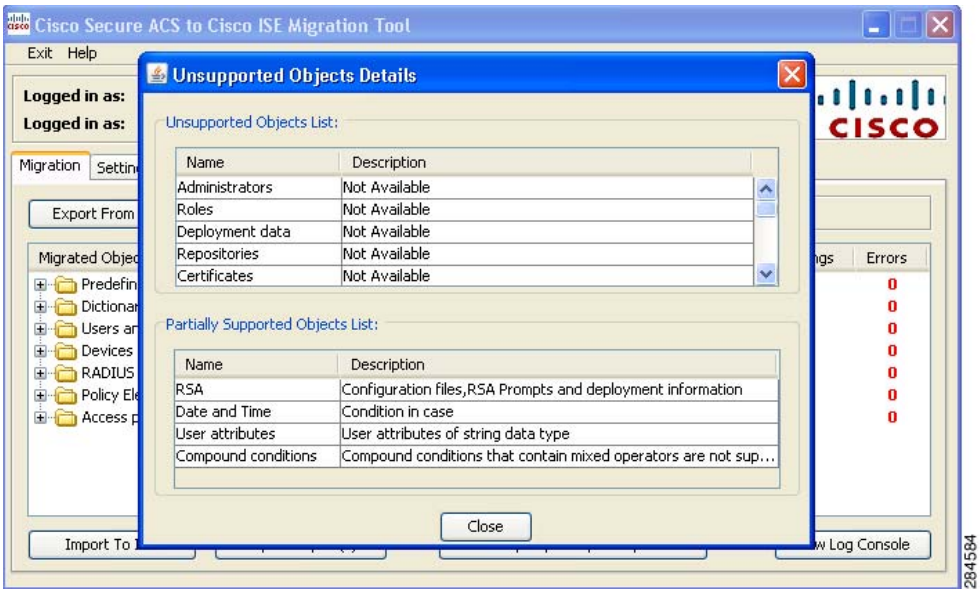
After the migration tool is initialized, unsupported Cisco Secure ACS objects still need to be migrated, and the following message is displayed (see Figure 3-4).

Figure 3-4 Message Displayed for Unsupported Objects



Step 7 Click **Yes** to display a list of unsupported and partially supported objects (see Figure 3-5).

Figure 3-5 List of Unsupported and Partially Supported Objects



Step 8 Click **Close**.

You can also view the list of unsupported objects by selecting **Help > Unsupported Object Details**.

To run the migration tool, see Chapter 4, "Using the Cisco Secure ACS-Cisco ISE Migration Tool".

CHAPTER 4

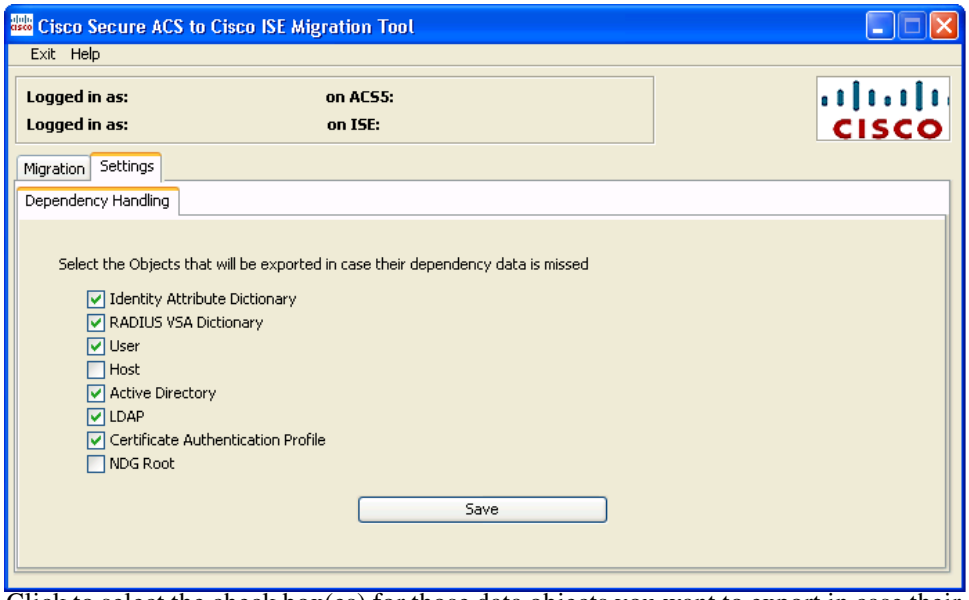
Using the Cisco Secure ACS-Cisco ISE Migration Tool

This chapter describes how to use the Cisco Secure Access Control System (ACS)-Cisco Identity Services Engine (ISE) Migration Tool to migrate data from a Cisco Secure ACS 5.1/5.2 database to a Cisco ISE 1.1 appliance, and includes procedures for running the migration process in the following topics:

Logging In and Using the Migration Tool

After you have started the migration tool, log into the Cisco Secure ACS 5.1/5.2 system from which you will be exporting data. To start using the migration tool, complete the following steps:

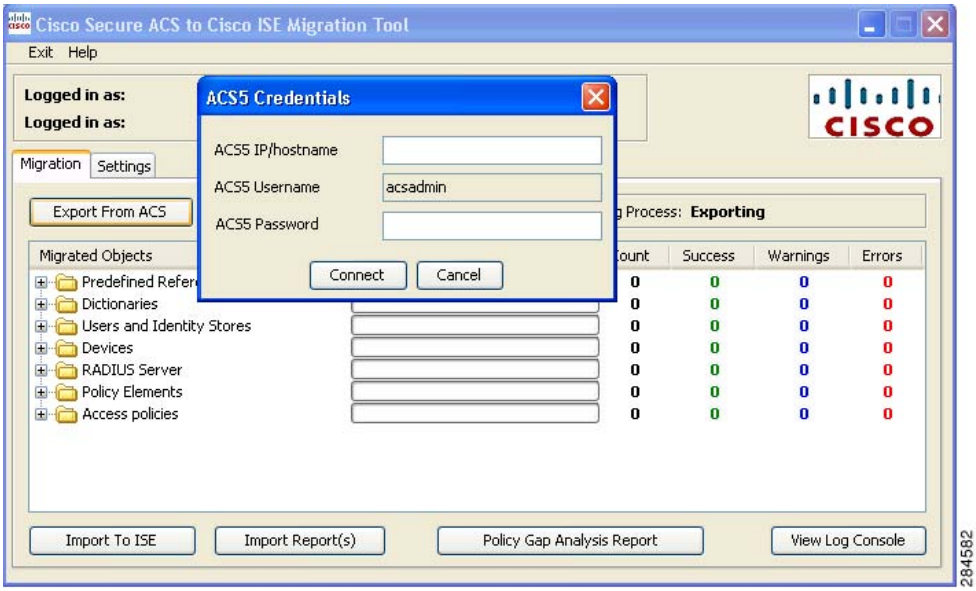
Step 1 In the Cisco Secure ACS-Cisco ISE Migration Tool main window, click **Settings** to display the list of data objects you want to migrate.



Step 2 Click to select the check box(es) for those data objects you want to export in case their dependency data is missed, and click **Save**.

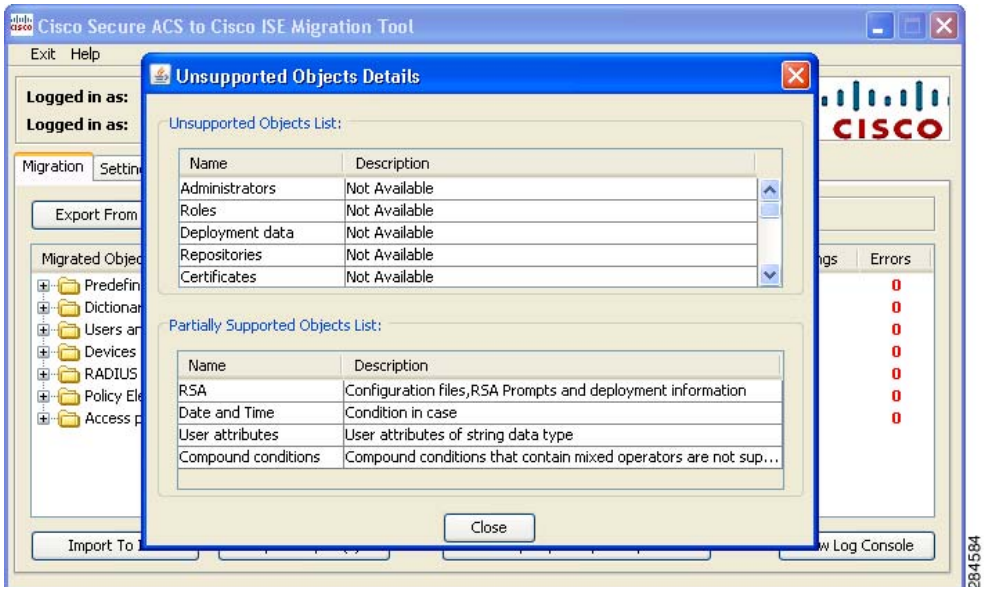
Step 3 In the main window of the Cisco Secure ACS-Cisco ISE Migration Tool, click **Migration** and click **Export from ACS.**

The Login window for the Cisco Secure ACS 5.1/5.2 system is displayed.

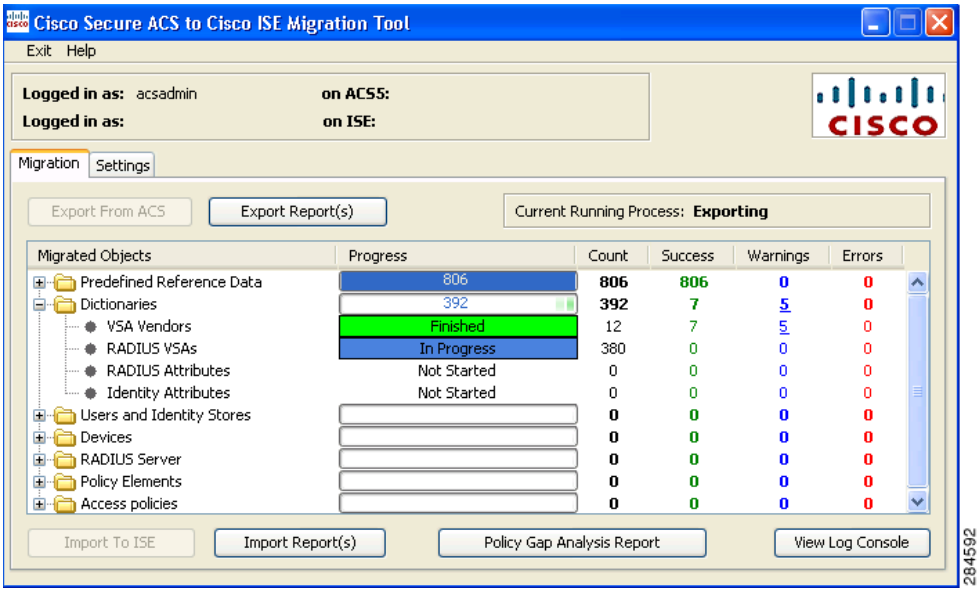


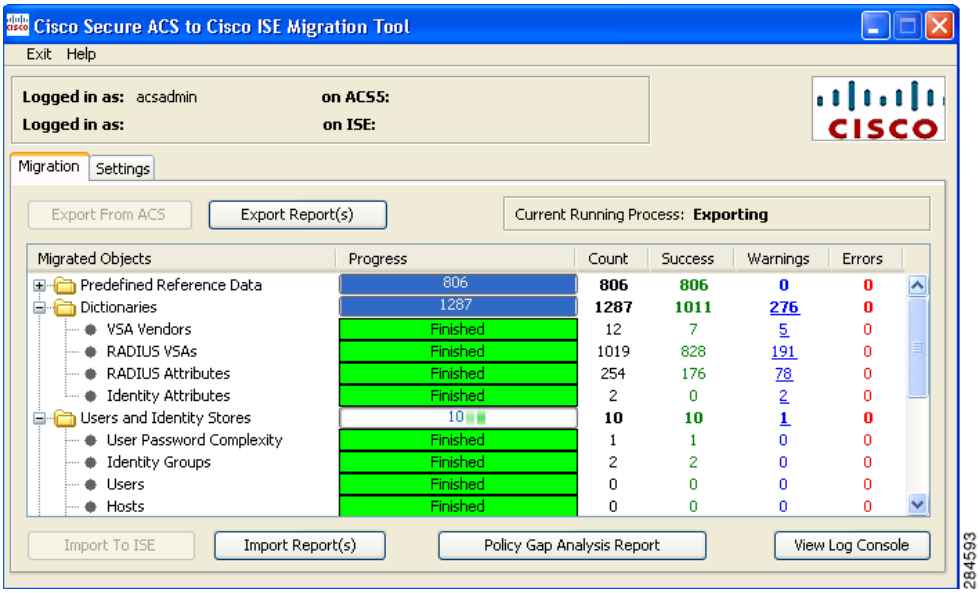
Step 4 Enter the IP address (or hostname) and the password for the Cisco Secure ACS 5.1/5.2 system into the ACS Credentials window, and click **Connect**.

The data migration process begins.


Cisco Secure ACS to Cisco ISE Migration Tool
Exit Help
Logged in as:
Logged in as:
Migration
Export From
Migrated Objec
Predefin
Dictionar
Users ar
Devices
RADIUS
Policy El
Access p
Errors
0
0
0
0
0
0
0
Import To
Log Console
Unsupported Objects Details
Unsupported Objects List:
Name
Description
Administrators
Not Available
Roles
Not Available
Deployment data
Not Available
Repositories
Not Available
Certificates
Not Available
Partially Supported Objects List:
Name
Description
RSA
Configuration files,RSA Prompts and deployment information
Date and Time
Condition in case
User attributes
User attributes of string data type
Compound conditions
Compound conditions that contain mixed operators are not sup...
Close
284584

Step 5 Check the progress of the migration of the Cisco Secure ACS 5.1/5.2 data by viewing the main window of the Cisco Secure ACS-Cisco ISE Migration Tool.

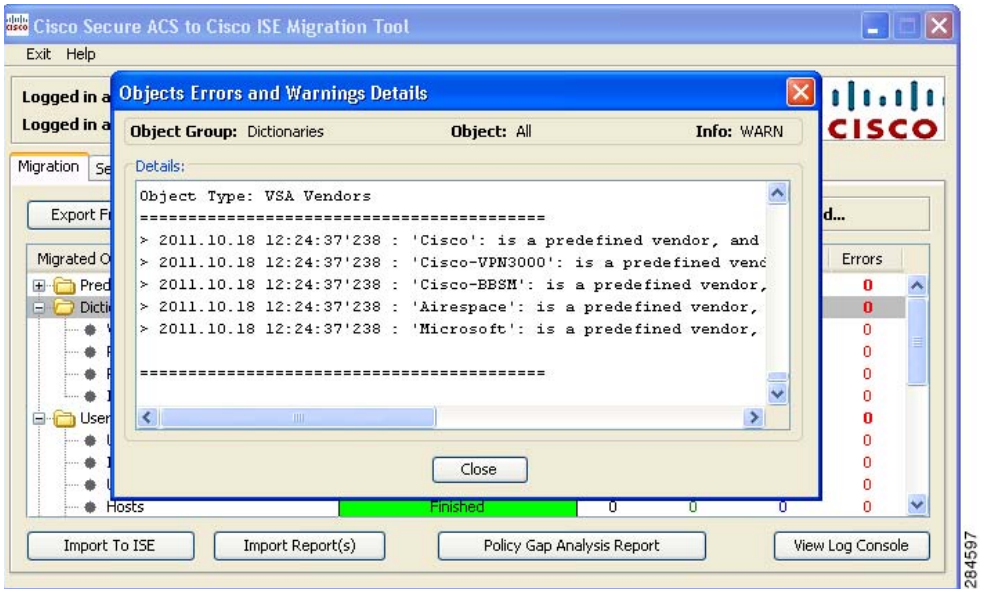




The main window of the Cisco Secure ACS-Cisco ISE Migration Tool displays the current count of successful objects exports, and also lists any objects that triggered warnings or errors.

Step 6 To get more information about a warning or error that occurred during the export process, click any listed **Warnings** or **Errors** in the table. The following example shows the result returned result from choosing an error to display.

The Object Errors and Warnings Details window is displayed, which provides the object group, the type, and a date and time that this error occurred.

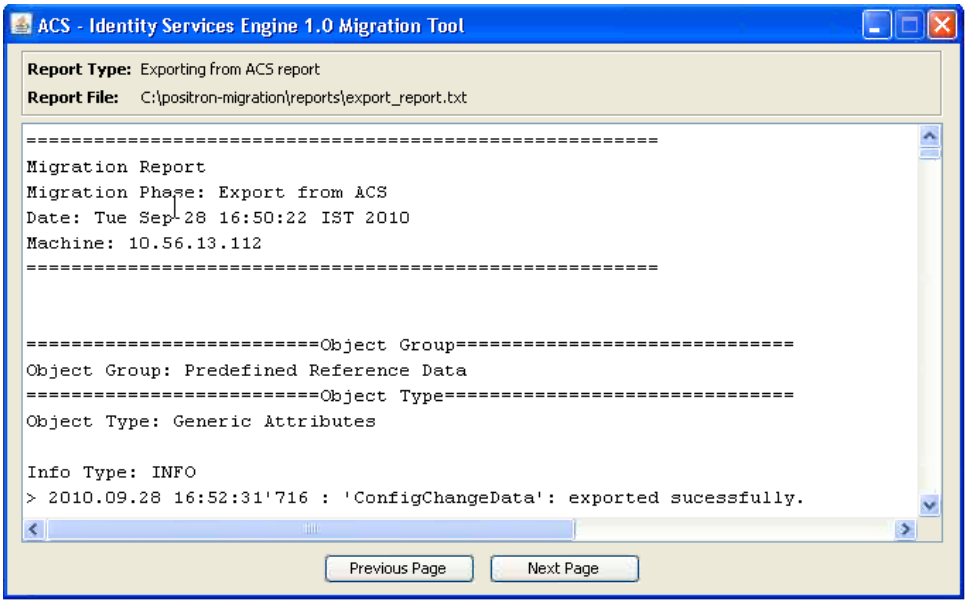


Step 7 Scroll to the right to display the complete set of details, and click **Close** to close this window.

When the data export process from the Cisco Secure ACS 5.1/5.2 system has completed (**Exporting finished...**), the main window of the Cisco Secure ACS-Cisco ISE Migration Tool displays this status.

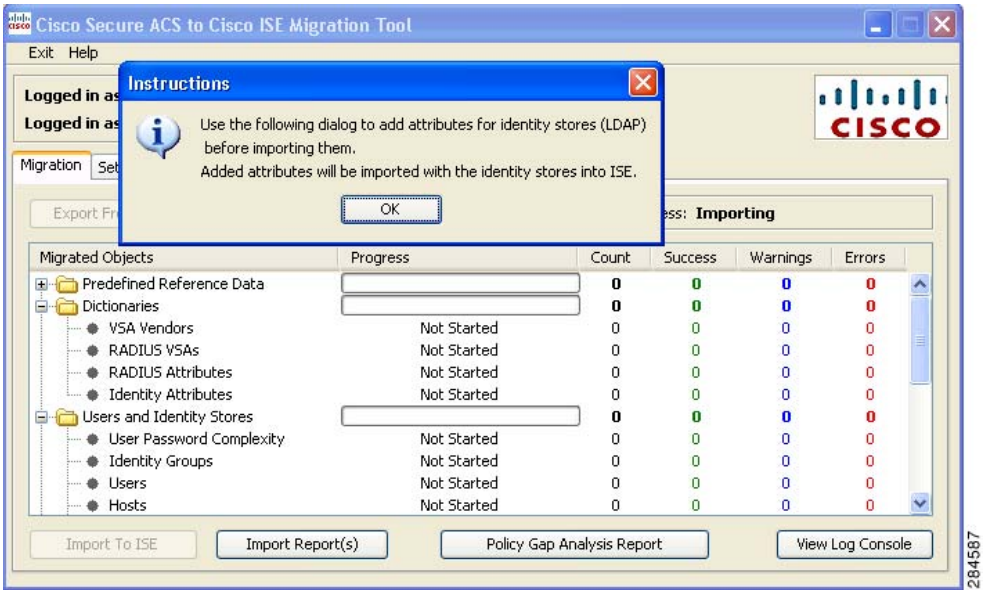
Step 8 Click **Export Report(s)** to view the contents of the report, which summarizes the export operation as shown in the following example.

Each export report contains header information with the operation type, date and time, and system IP address or host name. Each object group details the types and related information for the objects in that group. Each report ends with an report that summarizes the start and end date and time, and the duration of the operation.



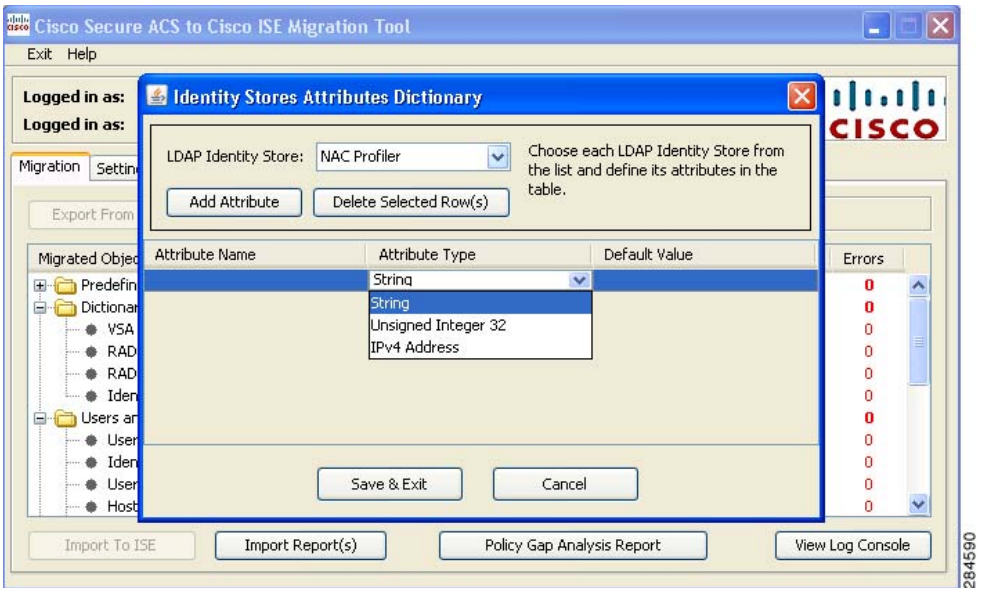
Step 9 To start importing this data into the Cisco ISE appliance, click **Import to ISE** in the main window of the Cisco Secure ACS-Cisco ISE Migration Tool.

You are prompted to add attributes to the LDAP identity stores before they are imported into Cisco ISE.



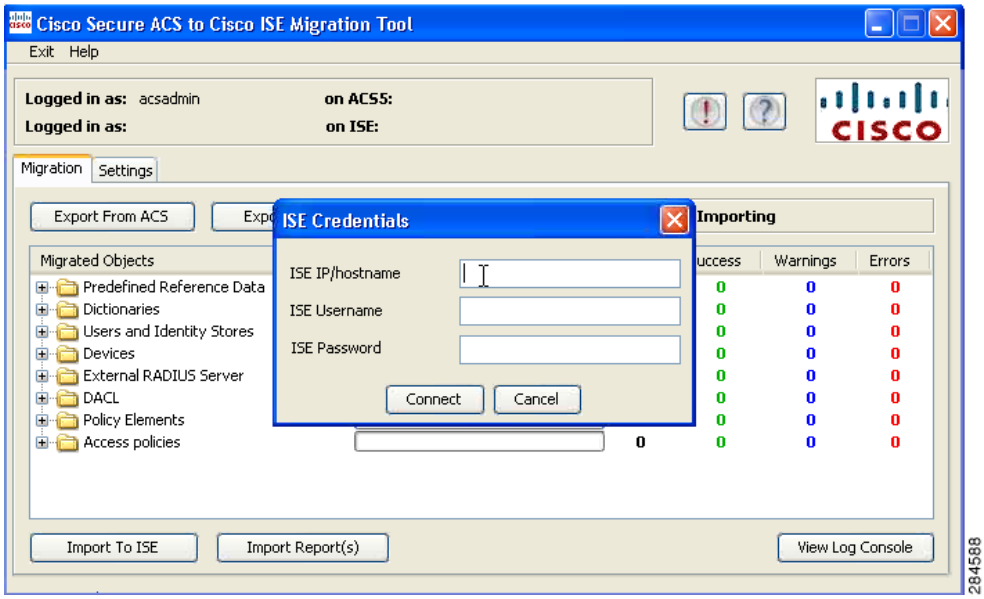
Step 10 Click **OK** to start the attribute add process for your LDAP identity stores.

Step 11 In the LDAP Identity Store drop-down list, select the identity store to which you want to add attributes.

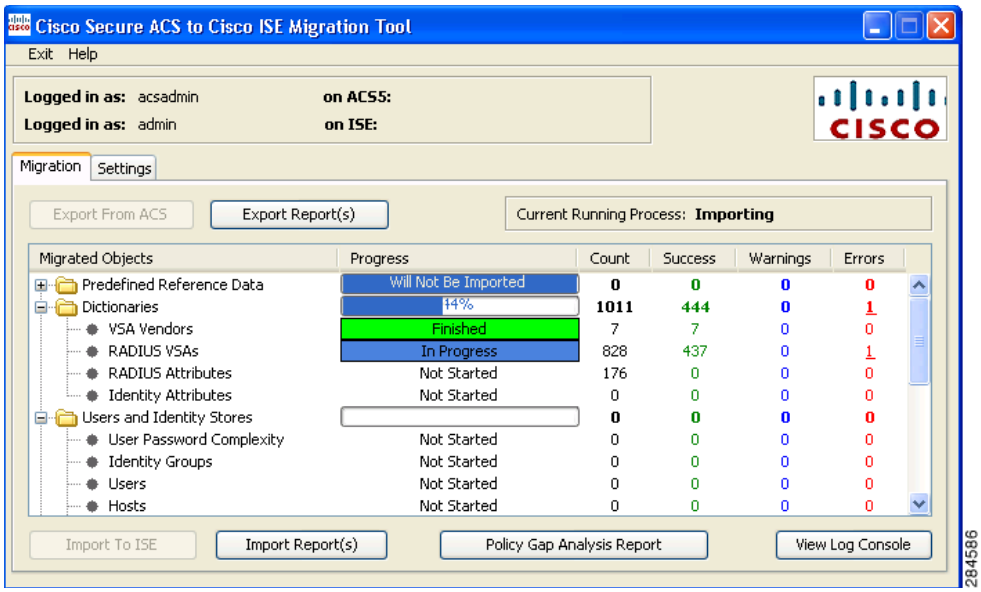


Step 12 Enter a name in the **Attribute Name** field, choose an attribute type from the **Attribute Type** drop-down list, enter a value in the **Default Value** field, and click **Save & Exit**.

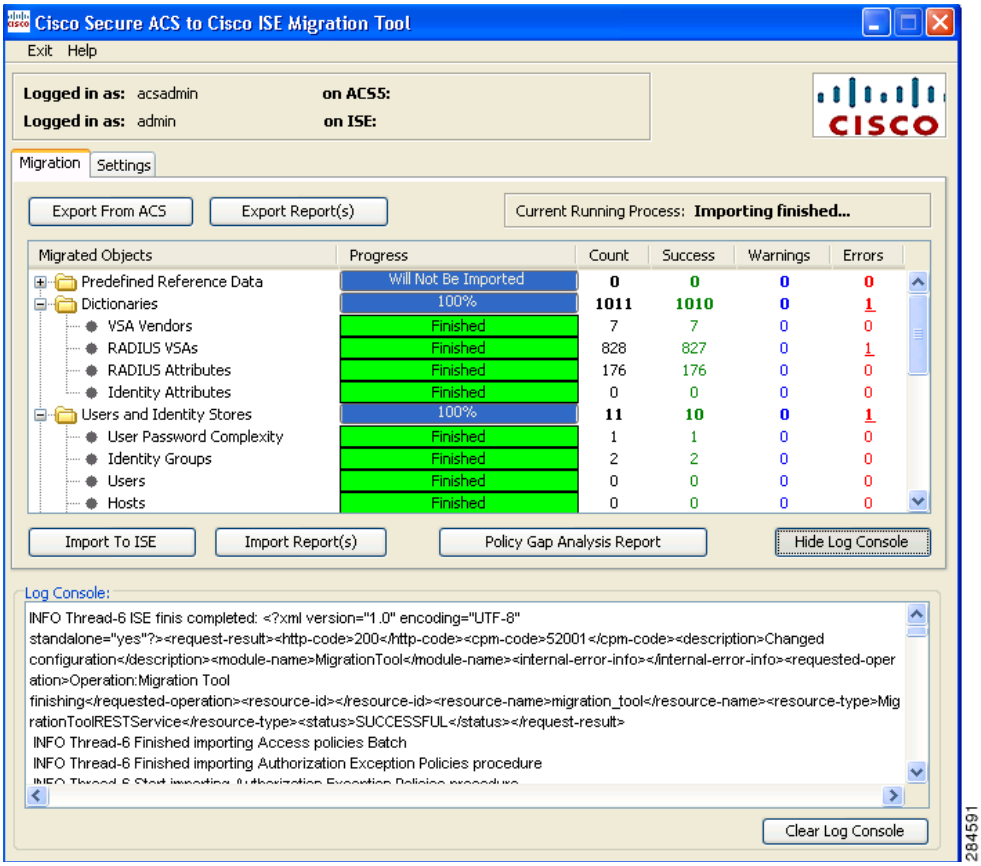
Step 13 After you have completed the attribute addition, click **Import to ISE** to proceed with the importing process, and log into the Cisco ISE system using the ISE Credentials window.



Step 14 Enter the ISE IP address (or hostname), ISE Username, and ISE Password as required, and click **Connect** to start importing data into the Cisco ISE appliance.



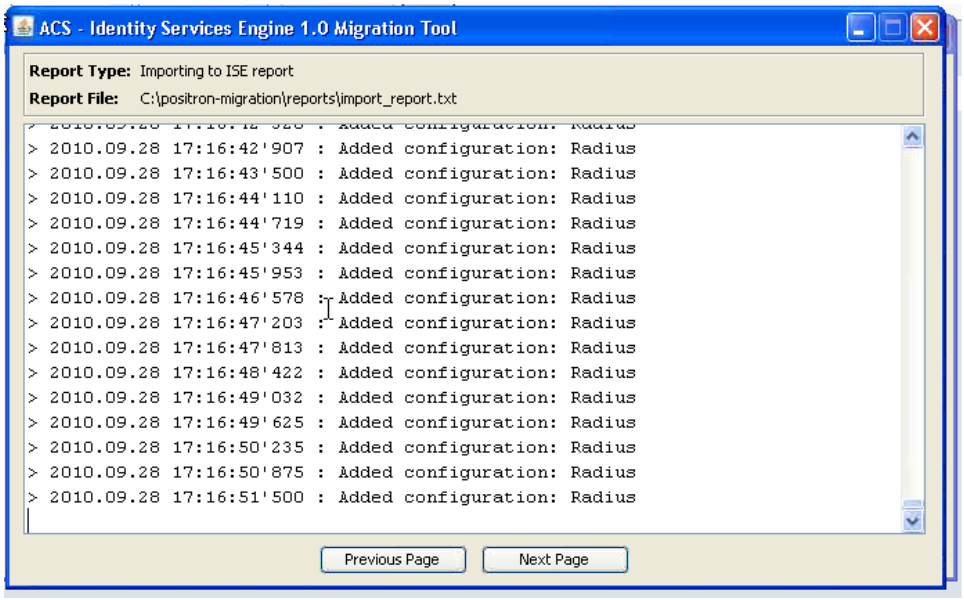
Step 15 At any point in the import or export process, click **View Log Console** to display a real-time look at the current status of the import or export operation.



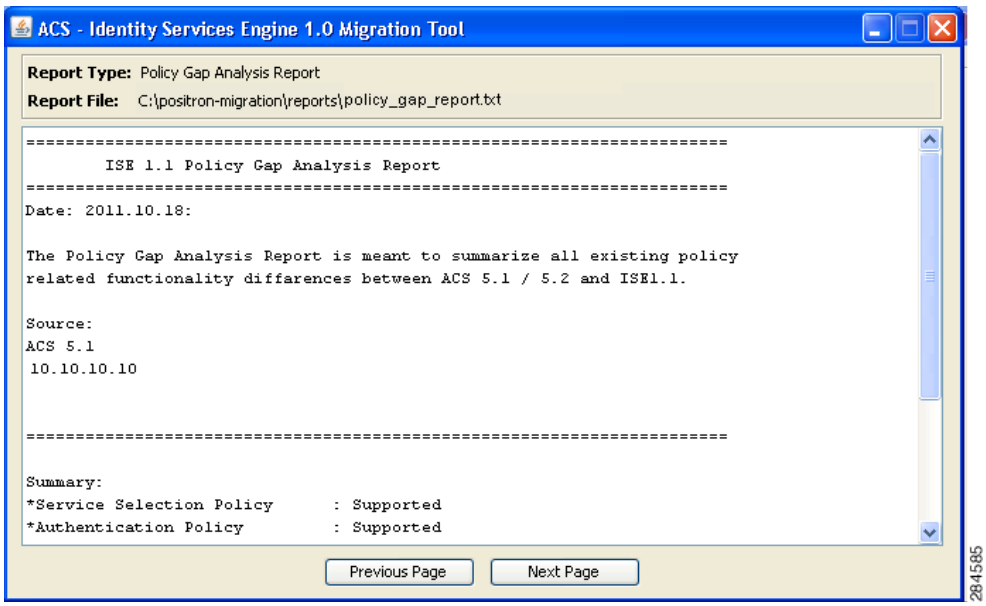
Step 16 To get more information about any warning or error that occurred during the import process, click **Warnings** or **Errors** in the table where it is listed (see Step 6), and view any details.

When the data import operation is complete, this status is displayed in the main window of the Cisco Secure ACS-Cisco ISE Migration Tool.

Step 17 To view the complete report on the data that is imported into the Cisco ISE 1.1 appliance, click **Import Report(s)**. The report is displayed.



Step 18 To analyze the policy gap between the Cisco Secure ACS and the Cisco ISE click **Policy Gap Analysis Report**. The report is displayed.



Verifying the Import Process

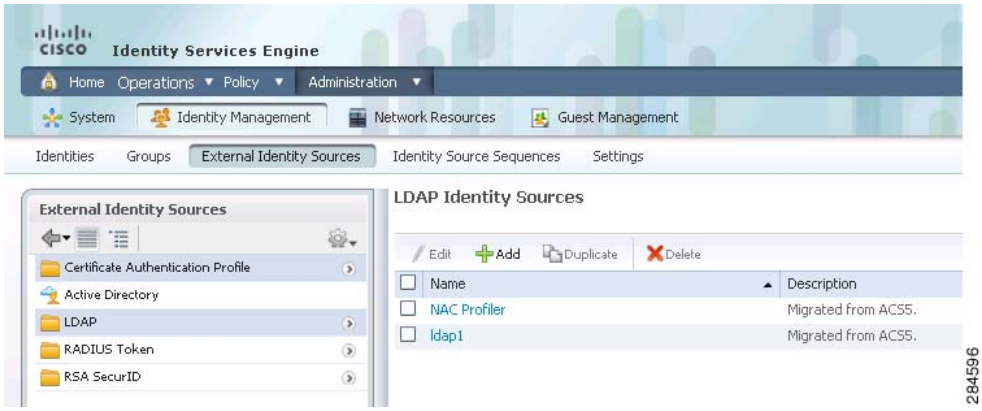
To verify that the import process has completed, complete the following steps:

Step 1 Log into the Cisco ISE 1.1 appliance:

- Enter a valid Username and Password.
- Click **Login**.

Step 2 In the Cisco ISE main window, for example, navigate to **Administration > Identity Management > External Identity Source > LDAP** to display the LDAP Identity source window to verify if any ACS-based LDAP Identity sources were imported.

You can perform the same sort of verification for users or any other attribute to check whether the import was successful.



This concludes the import/export operations by use of the Cisco Secure ACS-Cisco ISE Migration Tool.

Providing Report Files

If you decide to share the report files with anyone, or to save them in another location, you can find the following report files in the Reports folder of the migration tool directory:

- import_report.txt
- export_report.txt
- policy_gap_report.txt

CHAPTER 5

Migrating Data from the Cisco Secure ACS 3.x and 4.x to the ACS 5.1/5.2

This chapter provides links to Cisco documentation that describes how to migrate data from earlier Cisco Secure Access Control System (ACS) 3.x or 4.x releases to a Cisco Secure ACS 5.0 release state. Cisco Secure ACS 5.0 is a key required step for migrating previous releases of Cisco Secure ACS data to Cisco Secure ACS 5.1/5.2.

When you have successfully migrated data from earlier releases to the Cisco Secure ACS 5.1/5.2 stage, you can then migrate your data to a Cisco Identity Services Engine (ISE), Release1.1 appliance. The following topics cover this information:

Introduction

Before you begin any attempt to migrate data to a Cisco ISE 1.1 appliance, make sure that you have read and understand all setup, backup, and installation instructions in Chapter 3, "Installing the Cisco Secure ACS-Cisco ISE Migration Tool"

Depending upon the starting release stage of the Cisco Secure ACS data that you want to migrate to a Cisco ISE 1.1 appliance, there may be several migration stages required before you can use the Cisco Secure ACS-Cisco ISE Migration Tool. For example:

- If you are starting from Cisco Secure ACS 3.x or 4.x, then you first need to migrate your data to the Cisco Secure ACS 5.0.
- If you have migrated your data to or are starting from the Cisco Secure ACS 5.0, then you need to migrate your data to the Cisco Secure ACS Release 5.1/5.2.
- If you have migrated your data to or are starting from Cisco Secure ACS Release 5.1/5.2, then you can use the Cisco Secure ACS-Cisco ISE Migration Tool to migrate your data to a Cisco ISE 1.1 appliance.

Migration From Earlier Cisco Secure ACS Releases

This section contains links to Cisco documentation that can assist in completing the migration of data from earlier releases of Cisco Secure ACS software to a point where you can migrate it to a Cisco ISE 1.1 appliance.

Migrating Cisco Secure ACS Release 3.x or 4.x Data to Cisco Secure ACS 5.0

For information on migrating data from the Cisco Secure ACS Release 3.x or 4.x to Cisco Secure ACS Release 5.0, refer to the following link:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.0/migration/guide/migrationguide.html

Migrating Cisco Secure ACS Release 5.0 Data to Cisco Secure ACS 5.1/5.2

For information on migrating data from the Cisco Secure ACS Release 5.0 to Cisco Secure ACS Release 5.1/5.2, refer to the following link:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/migration/guide/Migration_Book.html

APPENDIX A

Cisco Secure ACS 5.1/5.2 and Cisco ISE 1.1 Data Structure Mapping

This appendix provides information about the following migration-related topics:

Data Objects That Are Migrated

The following data objects are migrated from the Cisco Secure Access Control System (ACS) 5.1/5.2 to the Cisco Identity Services Engine (ISE) 1.1:

- Network device group (NDG) types and hierarchies
- Network devices
- Default network device
- External RADIUS servers
- Identity group
- Internal users
- Internal endpoints (hosts)
- Lightweight Directory Access Protocol (LDAP)
- Microsoft Windows Active Directory (AD)
- RSA (partial support, see Table A-25)
- RADIUS token (see Table A-24)
- Certificate authentication profile
- Date and time condition (partial support, see Migrating Policies)
- RADIUS attribute and vendor-specific attributes (VSA) values (seeTable A-5 and Table A-6)

- RADIUS vendor dictionaries (see Notes for Table A-5 and Table A-6)
- Internal users attributes (see Table A-1 and Table A-2)
- Internal endpoint attributes (see General Migration Rules, page A-3)
- Authorization profile
- Downloadable access control list (DACL)
- Identity (authentication) policy
- Authorization policy (for network access)
- Authorization exception policy (for network access)
- Service selection policy (for network access)
- RADIUS proxy service
- User password complexity
- Identity sequence and RSA prompts
- UTF-8 data (see UTF-8 Support, page 1-8)

Data Objects That Are Not Migrated

The following data objects are not migrated from the Cisco Secure ACS 5.1/5.2 to the Cisco ISE 1.1:

- Monitoring reports
- Scheduled backups
- Repositories
- Administrators, roles, and administrators setting
- Customer/debug log configuration
- Deployment information (secondary nodes)
- Certificates (certificate authorities and local certificates)
- Security Group Access Control Lists (SGACL)
- Security Group (SG)
- AAA servers for supported Security Group Access (SGA) devices
- SG mapping
- Network Device Admission Control (NDAC) policy
- SGA egress matrix (SGA)
- SGA data within network devices
- Security Group Tag (SGT) in SGA authorization policy results
- Network condition (end station filters, device filters, device port filters)
- Device administration authentication and authorization policies

Data Objects That Are Partially Migrated

The following data objects are migrated partially from the Cisco Secure ACS 5.1/5.2 to the Cisco ISE 1.1:

- Identity and host attributes that are of type date are not migrated.
- RSA sdopts.rec file and secondary information are not migrated.
- RADIUS identity server attributes (only the attribute CiscoSecure-Group-Id is migrated).

General Migration Rules

Consider these migration rules while migrating data from the Cisco Secure ACS 5.1/5.2 to the Cisco ISE 1.1:

- Objects with special characters are not migrated.
- Attributes (RADIUS, VSA, identity, and host) of type enum are migrated as integers with allowed values.
- All endpoint attributes (no matter what is the attribute data type) are migrated as String data type.
- You cannot filter RADIUS attributes and VSA values to be added into ISE logs.

Migrating Policies

Authentication and authorization polices are migrated from the Cisco Secure ACS to the Cisco ISE. ACS and ISE have both simple and rule-based authentication paradigms, but ACS and ISE are based on different policy models. As result of the differences between the ACS to ISE policy model, not all ACS policies and rules can be migrated. These are the main reasons:

- Unsupported attributes used by the policy
- Unsupported and/or condition structure (mainly, once complex conditions are configured)
- Unsupported operators (such as “begin with”)

In case a rule cannot be migrated, the policy as a whole is not migrated and the reason and details are listed in the Policy Gap Analysis report. You can view the report and either delete or modify the problematic rules. See “Reporting” section on page 1-5 for more details on the Policy Gap Analysis report.

Note If you do not modify or delete the unsupported rule, no policy is migrated to the Cisco ISE.

This list describes the Cisco Secure ACS 5.1/5.2 to the Cisco ISE 1.1 migration policies guidelines:

- Rules with conditions that include user attributes with a data type other than the “string” data type are not migrated.
- Authentication fails in case the condition refers to host attributes.
- Authorization policies that include a condition that has host (endpoint) attributes are not migrated to Cisco ISE authorization policies.
- Date and time conditions in an authorization policy that has a recurrence weekly setting is not migrated to the Cisco ISE. As a result, the rule is also not migrated.

- Date and time conditions in an authentication policy are not migrated to the Cisco ISE. As a result, the rule is also not migrated.
- The following operands are not supported in conditions:
  - **String**: start with, end with, contains, not contains
  - **Date and time**: not in
  - **Identity group**: not in

  Rules that use these operands in their conditions are also not migrated.
- Authentication policies that include compound conditions that have different logical expressions other than a || b || c || … and/or a && b && c && … such as (a || b) && c are not migrated. Authorization policies that include compound conditions that have different local expressions other than a && b && c && are not migrated as part of the rule condition. As a workaround, you can manually use library compound conditions for some advanced logical expressions.
- Rules that include network conditions only are not migrated. In case the condition includes network conditions and other supported conditions, the network conditions are ignored and are not migrated as part of the rule condition.
- The Cisco ISE does not support TACACS, so any ACS rule that uses a TACACS attribute is not migrated.

Note If during the export phase, the Cisco ACS 5.1/5.2-ISE 1.1 Migration Tool identifies a gap within the authentication and authorization policies (matching any of the migration guidelines that are noted in this section), it is listed in the Policy Gap Analysis report. If this gap identification occurs, it is the responsibility of the administrator who is performing the migration to modify or delete such rules. If such rules are not modified or deleted, no policy is migrated to the Cisco ISE.

Supported Attributes and Data Types

The following tables list the supported attributes that are migrated and their target data type.

Table A-1 User Attributes Migrated from the Cisco Secure ACS 5.1/5.2 to the Cisco ISE 1.1

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.1
String	String
UI32	Not supported
IPv4	Not supported
Boolean	Not supported
Date	Not supported
Enum	Not supported

Table A-2 User Attribute: Association to the User

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.1
String	Supported
UI32	—

Table A-2 User Attribute: Association to the User (continued)

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.1
IPv4	—
Boolean	—
Date	—

Table A-3 Hosts Attributes Migrated from the Cisco Secure ACS 5.1/5.2 to the Cisco ISE 1.1

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.1
String	String
UI32	UI32
IPv4	IPv4
Boolean	Boolean
Date	Not supported
Enum	Integers with allowed values

Table A-4 Host Attribute: Association to the Host

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.1
String	Supported
UI32	Supported (Value is converted to String)
IPv4	Supported (Value is converted to String)
Boolean	Supported (Value is converted to String)
Date	Supported (Value is converted to String)
Enum	Supported (Value is converted to String)

Table A-5 RADIUS Attributes Migrated from the Cisco Secure ACS 5.1/5.2 to the Cisco ISE 1.1

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.1
UI32	UI32
UI64	UI64
IPv4	IPv4
Hex String	Octect String
String	String
Enum	Integers with allowed values

Table A-6 RADIUS Attribute: Association to RADIUS Server

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.1
UI32	Supported
UI64	Supported
IPv4	Supported
Hex String	Supported (Hex strings are converted to octets string)
String	Supported
Enum	Supported (Enums are integers with allowed values)

Data Information Mapping

This section provides series of tables that list the data information that is mapped during export, which includes categories from the Cisco Secure ACS 5.1/5.2 and its equivalent in the Cisco ISE 1.1 for each object. The data mapping tables in this section list the status of what is or is not a valid data object mapped during the data migration during the export stage of the migration process:

- Table A-7 on page A-7 (network device property mapping)
- Table A-8 on page A-7 (Active Directory property mapping)
- Table A-9 on page A-8 (external RADIUS server property mapping)
- Table A-10 on page A-8 (hosts/endpoints property mapping)
- Table A-11 on page A-9 (identity dictionary property mapping)
- Table A-12 on page A-9 (identity group property mapping)
- Table A-13 on page A-9 (LDAP property mapping)
- Table A-14 on page A-11 (NDG types mapping)
- Table A-15 on page A-11 (NDG hierarchy mapping)
- Table A-16 on page A-11 (RADIUS dictionary vendors mapping)
- Table A-17 on page A-12 (RADIUS dictionary attributes mapping)
- Table A-18 on page A-12 (users mapping)
- Table A-19 on page A-12 (certificate authentication profile)
- Table A-20 on page A-13 (authorization profile mapping)
- Table A-21 on page A-13 (DACL mapping)
- Table A-22 on page A-13 (external RADIUS server mapping))
- Table A-23 on page A-14 (identity attributes dictionary mapping)
- Table A-24 on page A-14 (RADIUS token mapping)
- Table A-25 on page A-15 (RSA mapping)

- Table A-26 on page A-15 (RSA Prompts)
- Table A-27 on page A-16 (Identity Store Sequences)
- Table A-28 on page A-16 (Default Network Device)

Note The export and import reports include informational, warning, and error messages that serve as validation of the import and export process.

Table A-7 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Network Device Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Migrate as is
Description	Migrate as is
Network device group	Migrate as is
Single IP address	Migrate as is
Single IP and subnet address	Migrate as is
Collection of IP and subnet addresses	Migrate as is
TACACS information	Not migrated because the TACACS is unsupported in the Cisco ISE 1.1.
RADIUS shared secret	Migrate as is
CTS	Migrate as is
SNMP	SNMP data is available only in Cisco ISE; therefore, there is no SNMP information for migrated devices.
Model name	This is a property available only in Cisco ISE (and its value is the default, “unknown”).
Software version	This is a property available only in Cisco ISE (and its value is the default, “unknown”).

Note Any network devices that are set only as TACACS are not supported for migration and these are listed as non-migrated devices.

Table A-8 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Active Directory Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Domain name	Migrate as is
User name	Migrate as is
Password	Migrate as is
Allow password change	Migrate as is
Allow machine access restrictions	Migrate as is
Aging time	Migrate as is

Table A-8 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Active Directory Mapping (continued)

Cisco Secure ACS Properties	Cisco ISE Properties
User attributes	Migrate as is
Groups	Migrate as is

Note The Cisco Secure ACS-Cisco ISE Migration Tool issues a **join** command after the Active Directory data has been migrated. This "join" operation can fail if the domain name, user name, and password are incorrect. In addition, it is important that the Cisco ISE appliance be properly synchronized with the AD server time, or this can also cause a failure during the "join" operation.

Table A-9 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 External RADIUS Server Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Migrate as is
Description	Migrate as is
Server IP address	Migrate as is
Shared secret	Migrate as is
Authentication port	Migrate as is
Accounting port	Migrate as is
Server timeout	Migrate as is
Connection attempts	Migrate as is

Table A-10 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Hosts (Endpoints) Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
MAC address	Migrate as is
Status	Not migrated
Description	Migrate as is
Identity group	Migrate the association to an endpoint group.
Attribute	Endpoint attribute is migrated.
Authentication state	This is a property available only in Cisco ISE (and its value is a fixed value, "Authenticated").
Class name	This is a property available only in Cisco ISE (and its value is a fixed value, "TBD").
Endpoint policy	This is a property available only in Cisco ISE (and its value is a fixed value, "Unknown").
Matched policy	This is a property available only in Cisco ISE (and its value is a fixed value, "Unknown").
Matched value	This is a property available only in Cisco ISE (and its value is a fixed value, "0").

Table A-10 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Hosts (Endpoints) Mapping (continued)

Cisco Secure ACS Properties	Cisco ISE Properties
NAS IP address	This is a property available only in Cisco ISE (and its value is a fixed value, “0.0.0.0”).
OUI	This is a property available only in Cisco ISE (and its value is a fixed value, “TBD”).
Posture status	This is a property available only in Cisco ISE (and its value is a fixed value, “Unknown”).
Static assignment	This is a property available only in Cisco ISE (and its value is a fixed value, “False”).

Table A-11 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Identity Dictionary Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Attribute	Attribute name
Description	Description
Internal name	Internal name
Attribute type	Data type
Maximum length	Not migrated
Default value	Not migrated
Mandatory fields	Not migrated
User	The dictionary property accepts this value (“user”).

Table A-12 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Identity Group Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
Parent	This property is migrated as part of the hierarchy details.

Note Cisco ISE contains endpoint and identity groups. Identity groups in Cisco Secure ACS 5.1/5.2 are migrated to Cisco ISE as endpoint groups and as identity groups because a user needs to be assigned to an identity group and an endpoint needs to be assigned to an endpoint group.

Table A-13 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 LDAP Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description

Table A-13 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 LDAP Mapping (continued)

Cisco Secure ACS Properties	Cisco ISE Properties
Server connection information	Migrate as is. (Server Connection tab; see Figure A-1 on page A-10.).
Directory organization information	Migrate as is. (Directory Organization tab; see Figure A-2 on page A-10.).
Directory groups	Migrate as is
Directory attributes	Migration is done manually (using the Cisco Secure ACS-Cisco ISE Migration Tool).

Figure A-1 Server Connection Tab

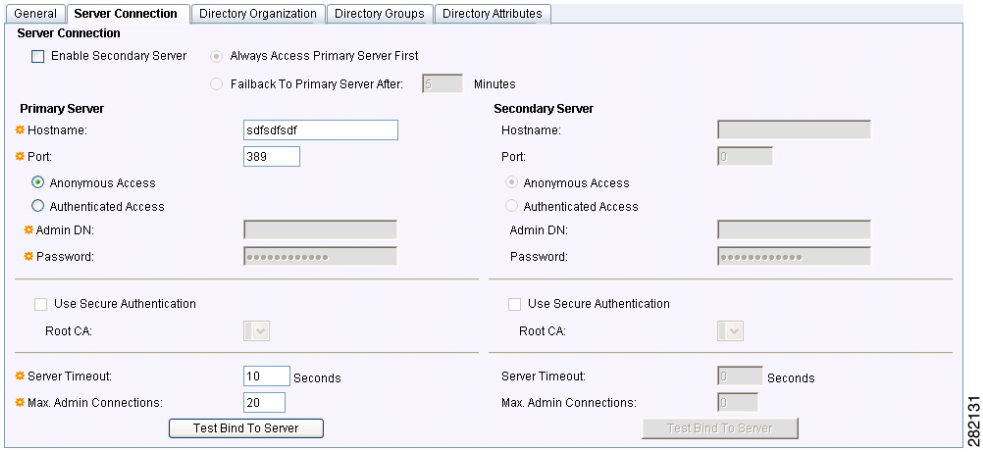


Figure A-2 Directory Organization Tab

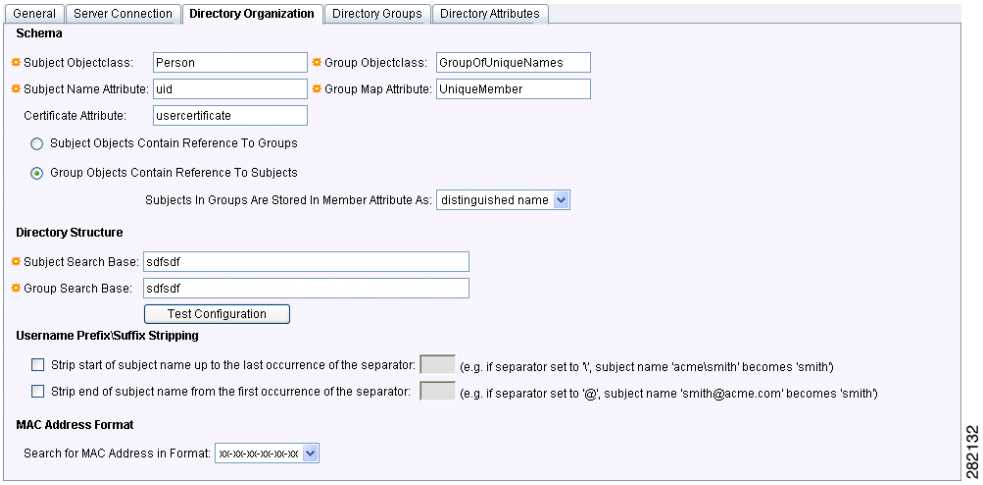


Table A-14 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 NDG Types Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.1 Properties
Name	Name
Description	Description

Note Cisco Secure ACS 5.1/5.2 can support having more than one network device group (NDG) with the same name. Cisco ISE does not support this naming scheme. Therefore, only the first NDG type with any defined name is migrated.

Table A-15 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 NDG Hierarchy Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
Parent	No specific property is associated with this property because this value is entered only as part of the NDG hierarchy name. (In addition, the NDG type is the prefix for this object name).

Note Any NDGs that contain a root name with a colon (:) currently are not migrated because the Cisco ISE 1.1 does not recognized the colon as a valid character.

Table A-16 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 RADIUS Dictionary (Vendors) Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
Vendor ID	Vendor ID
Attribute prefix	No need to migrate this property.
Vendor length field size	Vendor attribute type field length.
Vendor type field size	Vendor attribute size field length.

Note Only those RADIUS vendors that are not part of a Cisco Secure ACS 5.1/5.2 installation are required to be migrated (this affects only the user-defined vendors).

Table A-17 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 RADIUS Dictionary (Attributes) Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
Attribute ID	No specific property associated with this because this value is entered only as part of the NDG hierarchy name. (In addition, the NDG type is the prefix for this object name).
Direction	Not supported in the Cisco ISE
Multiple allowed	Not supported in the Cisco ISE
Attribute type	Migrate as is
Add policy condition	Not supported in the Cisco ISE
Policy condition display name	Not supported in the Cisco ISE

Note Only those RADIUS attributes that are not part of a Cisco Secure ACS 5.1/5.2 installation are required to be migrated (only the user-defined attributes need to be migrated).

Table A-18 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 User Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
Status	No need to migrate this property. (This property does not exist in the Cisco ISE).
Identity group	Migrate to identity groups in the Cisco ISE.
Password	Password.
Enable password	No need to migrate this property. (This property does not exist in the Cisco ISE).
Change password on next login	No need to migrate this property.
User attributes list	User attributes are imported from the Cisco ISE and are associated with the users.

Table A-19 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Certificate Authentication Profile Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
Principle user name (X.509 attribute)	Principle user name (X.509 attribute).

Table A-19 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Certificate Authentication Profile Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Binary certificate comparison with certificate from LDAP or AD	Binary certificate comparison with certificate from LDAP or AD.
AD - LDAP name for certificate fetching	AD - LDAP name for certificate fetching.

Table A-20 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Authorization Profile Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
DACLID (downloadable ACL ID)	Migrate as is
Attribute type (static and dynamic)	• Migrate as is if static attribute. • Migrated as is, if dynamic attribute, except Dynamic VLAN.
Attributes (filtered for static type only)	RADIUS attributes.

Table A-21 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Downloadable ACL Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
DACL content	DACL content

Table A-22 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 External RADIUS Server Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
Server IP address	Hostname
Shared secret	Shared secret
Authentication port	Authentication port
Accounting port	Accounting port
Server timeout	Server timeout
Connection attempts	Connection attempts

Table A-23 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Identity Attributes Dictionary Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Attribute	Attribute name
Description	Internal name
Name	Migrate as is
Attribute type	Data type
No such property	Dictionary (Set with the value “InternalUser” if it is a user identity attribute, or “InternalEndpoint” if it is a host identity attribute.)
Not exported or extracted yet from the Cisco Secure ACS	Allowed value = display name
Not exported or extracted yet from the Cisco Secure ACS	Allowed value = internal name
Not exported or extracted yet from the Cisco Secure ACS	Allowed value is default
Maximum length	None
Default value	None
Mandatory field	None
Add policy condition	None
Policy condition display name	None

Table A-24 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 RADIUS Token Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
Safeword server	Safeword server
Enable secondary appliance	Enable secondary appliance
Always access primary appliance first	Always access primary appliance first
Fallback to primary appliance in minutes	Fallback to primary appliance in minutes
Primary appliance IP address	Primary appliance IP address
Primary shared secret	Primary shared secret
Primary authentication port	Primary authentication port
Primary appliance TO (timeout)	Primary appliance TO
Primary connection attempts	Primary connection attempts
Secondary appliance IP address	Secondary appliance IP address
Secondary shared secret	Secondary shared secret
Secondary authentication port	Secondary authentication port
Secondary appliance TO	Secondary appliance TO

Table A-24 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 RADIUS Token Mapping (continued)

Cisco Secure ACS Properties	Cisco ISE Properties
Secondary connection attempts	Secondary connection attempts
Advanced > treat reject as authentication flag fail	Advanced > treat reject as authentication flag fail.
Advanced > treat rejects as user not found flag	Advanced > treat rejects as user not found flag.
Advanced > enable identity caching and aging value	Advanced > enable identity caching and aging value.
Shell > prompt	Authentication > prompt
Directory attributes	Authorization > attribute name (In cases where the dictionary attribute lists in Cisco Secure ACS includes the attribute “CiscoSecure-Group-Id,” it is migrated to this attribute; otherwise, the default value is “CiscoSecure-Group-Id”.)

Table A-25 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 RSA Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name is always RSA
Description	Not migrated
Realm configuration file	Realm configuration file
Server TO	Server TO
Reauthenticate on change to PIN	Reauthenticate on change to PIN
RSA instance file	Not migrated
Treat rejects as authentication fail	Treat rejects as authentication fail
Treat rejects as user not found	Treat rejects as user not found
Enable identity caching	Enable identity caching
Identity caching aging time	Identity caching aging time

Table A-26 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 RSA Prompts

Cisco Secure ACS Properties	Cisco ISE Properties
Passcode prompt	Passcode prompt
Next Token prompt	Next Token prompt
PIN Type prompt	PIN Type prompt
Accept System PIN prompt	Accept System PIN prompt
Alphanumeric PIN prompt	Alphanumeric PIN prompt
Numeric PIN prompt	Numeric PIN prompt

Table A-27 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Identity Store Sequences

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
Certificate based, certificate authentication profile	Certificate based, certificate authentication profile
Password based	Authentication search list
Advanced options > if access on current IDStore fails than break sequence	Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError."
Advanced options > if access on current IDStore fails then continue to next	Treated as "User Not Found" and proceed to the next store in the sequence.
Attribute retrieval only > exit sequence and treat as "User Not Found"	Not supported (should be ignored)

Table A-28 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.1 Default Network Devices

Cisco Secure ACS Properties	Cisco ISE Properties
Default network device status	Default network device status
Network device group	Not migrated
Authentication Options - Tacacs+	Not migrated
RADIUS - shared secret	Shared Secret
RADIUS - CoA port	Not migrated
RADIUS - Enable keywrap	Enable keywrap
RADIUS - Key encryption key	Key encryption key
RADIUS - Message authenticator code key	Message authenticator code key
RADIUS - Key input format	Key input format

APPENDIX B

Troubleshooting the Cisco Secure ACS-Cisco ISE Migration Tool

This appendix describes some common issues or conditions that you might encounter when using the Cisco Secure Access Control System (ACS)-Cisco Identity Services Engine (ISE) Migration Tool:

Unable to Start the Migration Tool

Condition

Unable to start the migration tool.

Action

Verify that Java JRE, version 1.6 or later is installed on the migration machine and that it is correctly configured in the system path and classpath.

Error Messages Displayed in the Logs

Condition

The following error message is displayed in the logs:

```
"Hosts: Connection to https://hostname-or-ip refused: null"
```

And the object is reported while migrating to Cisco ISE.

Action

- Make sure that the migration application machine is connected to the network and that it is configured correctly.
- Make sure that the Cisco ISE appliance is connected to the network and that it is configured correctly.
- Make sure that the Cisco ISE appliance and the migration machine are able to connect to each other over the network.
- Make sure that the hostname (if any) used in the Cisco ISE primary node is resolvable within the DNS when the migration tool connects to Cisco ISE.
- Make sure that the Cisco ISE appliance is up and running.
- Make sure that the Cisco ISE application server service is up and running.

Condition

The following error message is displayed in the logs:

```
"I/O exception (org.apache.http.NoHttpResponseException) caught when processing
request: The target server failed to respond".
```

Action

- Make sure that the Cisco ISE application server service is up and running.
- Make sure that the Cisco ISE web server thresholds have not been exceeded or that there are no memory exceptions.
- Make sure that the Cisco ISE appliance CPU consumption is not 100 percent and that the CPU is active.

Condition

The following error message displays in the logs:

```
"OutofMemory"
```

Action

Increase the Java heap size to at least 1 GB as described in Installing and Initializing the Cisco Secure ACS-Cisco ISE Migration Tool, page 3-3.

Condition

The following error message is displayed in the logs:

```
Caused by: java.sql.SQLException: [Sybase][ODBC Driver][SQL Anywhere]Temporary
space limit exceeded
```

Action

Install the cumulative patch ACS 5.1.0.44.4 that includes the fix for the temporary database space limit issue.

Default Folders, Files, and Reports are Not Created

Condition

The migration tool fails to create the default folders, log files, reports, and persistence data files.

Action

Make sure the user has file system writing privileges and that there is enough disk space.

Migration Export Phase is Very Slow

Condition

The export phase of the migration process is very slow.

Action

Restart your Cisco Secure ACS appliance before starting the migration process to free up memory space.

Reporting Issues to the Cisco TAC

If you cannot locate the source and potential resolution for a technical issue or problem, you can contact a Cisco customer service representative for information on how to best proceed with resolving your technical issue. For information about the Cisco Technical Assistance Center (TAC), see the *Cisco Information Packet* publication that is shipped with your appliance or visit the following website:

http://www.cisco.com/tac/

Before you contact Cisco TAC, make sure that you have the following information ready:

- The appliance chassis type and serial number.
- The maintenance agreement or warranty information (see the *Cisco Information Packet*).
- The name, type of software, and version or release number (if applicable).
- The date you received the new appliance.
- A brief description of the problem or condition you experienced, the steps you have taken to isolate or re-create the problem, and a description of any steps you took to resolve the problem.
- Backup of the Cisco Secure ACS 4.x database (.dmp file)
- Migration logfile (...migration/bin/migration.log)
- All the reports in the config folder (...migration/config)
- Cisco Secure ACS 5.2 logfiles
- Cisco Secure ACS 5.2 build number
- Cisco Secure ACS 4.x build number

Note Be sure to provide the customer service representative with any upgrade or maintenance information that was performed on the Cisco ISE 3300 Series appliance after your initial installation.

GLOSSARY

A

ACL Access control list. This is a list of access permissions attached to an object that specify which users or processes are granted access to this or other objects, including what operations can be allowed on a given object. Entries in an ACL can specify permission for a user, an operation, a port, or a hostname.

ACS Access Control System. This is a policy-based security server that provides standards-compliant Authentication, Authorization, and Accounting (AAA) services to your network. ACS facilitates the administrative management of Cisco and non-Cisco devices and applications.

Active Directory Microsoft Windows Active Directory. This is a directory service created by Microsoft that stores all information and settings for a deployment in a central database. Active Directory allows administrators to assign policies, and deploy and update software from small network installations with a small number of computers, users, and printers to much larger network environments with multiple domains and different locations.

D

DACL Downloadable access control list. Cisco ISE supports a downloadable list of access permissions attached to an object that specify which users or processes are granted access to this or other objects, including what operations can be allowed on a given object. Entries in an DACL can specify permission for a user, an operation, a port, or a hostname.

H

HTTPS Hypertext Transfer Protocol Secure. This combination of the Hypertext Transfer Protocol (HTTP) with the SSL/TLS protocol provides secure, encrypted communication and secure identification for network and Internet traffic. HTTPS connections are often used for sensitive transactions within corporate, financial, or commercial systems. HTTPS uses a different port that provides an additional layer of encryption and authentication between HTTP and TCP.

L

LDAP Lightweight Directory Access Protocol. It is an application protocol for querying and modifying data in directories using directory services running over TCP/IP. An LDAP directory in this sense is an organized set of records, such as a telephone directory is an alphabetical list of persons and organizations, each with an address and phone number that comprises a “record.” A common method of securing LDAP communication is by using an SSL tunnel.

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

NDG Network device group. In Cisco ISE, a device group is a hierarchical structure that contains network device groups (NDGs) that are a logical grouping of similar devices based on criteria such as location or device type. For example, you can group devices by continent, region, or country location, or you can group devices like firewalls, routers, or switches by types. In Cisco ISE, you can also use NDGs in policy conditions.

P

PI Programmatic Interface. A mechanism for external applications to interact with Cisco Secure 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.

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.

INDEX