Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0.4

September 2011

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-25622-01

Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0.4

CONTENTS

Preface

Revised: September 30, 2011, OL-25622-01

This migration 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 1.0.4 appliance. The migration process uses the Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 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 Identity Services Engine Release 1.0.4 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 1.0.4 appliance using the Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 Migration Tool. This migration guide contains the following information:

Note For the remainder of this migration guide, the Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 Migration Tool (and its shorter form, Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool) describe the tool used to migrate data from a Cisco Secure ACS 5.1/5.2 database to a Cisco ISE 1.0.4 appliance.

- Cisco ACS 5.1/5.2-ISE 1.0.4 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 Release 5.1/5.2 database to the Cisco ISE 1.0.4 appliance.
- Reference links to Cisco documentation that defines the upgrade path required by earlier releases of Cisco Secure ACS data (Release 3.x and 4.x) before it can be migrated.

Note The Cisco ACS 5.1/5.2-ISE 1.0.4 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, Release 3.x or 4.x) to the Cisco Secure ACS Release 5.1/5.2 state where it can be migrated to a Cisco ISE 1.0.4 appliance, requires a multi-step process:

1. Upgrade the Cisco Secure ACS Release 3.x or 4.x data to the Cisco Secure ACS Release 5.0 state using the process described in the Cisco documentation (see Related Documentation in this Preface).
2. Upgrade the Cisco Secure ACS Release 5.0 data to Cisco Secure ACS Release 5.1/5.2 state using the process described in the Cisco documentation (see Related Documentation in this Preface).
3. Use the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool to migrate Cisco Secure ACS Release 5.1/5.2 data to a Cisco ISE 1.0.4 appliance using the procedure in this migration guide (see Chapter 4, "Using the Cisco Secure ACS 5.1/5.2-Cisco ISE 1.0.4 Migration Tool").

The focus of this migration guide is on documenting the process for using the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool to export existing Cisco Secure ACS Release 5.1/5.2 data, and import this data into a Cisco ISE 1.0.4 appliance.

We recommend that you fully understand the related data structure and schema differences between the Cisco Secure ACS Release 5.1/5.2 and Cisco ISE 1.0.4 systems before any attempt is made to migrate existing Cisco Secure ACS data.

Audience

This migration guide is for network administrators who are responsible for migrating existing Cisco Secure ACS Release 5.1/5.2 database information to a Cisco ISE 1.0.4 appliance using the Cisco Secure ACS 5.1/5.2-ISE 1.0.4 Migration Tool.

Organization

This migration guide includes the following sections:

Title	Description
Chapter 1, "Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 Migration Overview"	Provides an overview of the Cisco Secure ACS 5.1/5.2-ISE 1.0.4 migration, the software requirements, supported releases, application components, data items that can be migrated, and the software architecture.
Chapter 2, "Understanding the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool"	Provides a functional description of the Cisco Secure ACS 5.1/5.2-ISE 1.0.4 Migration Tool, which supports export and import, data persistency, scalability, high availability, and reporting functions.

Title	Description
Chapter 3, "Installing the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool"	Describes requirements, installation prerequisites and guidelines, and how to install and set up the Cisco Secure ACS 5.1/5.2-ISE 1.0.4 Migration Tool.
Chapter 4, "Using the Cisco Secure ACS 5.1/5.2-Cisco ISE 1.0.4 Migration Tool"	Describes how to use the Cisco Secure ACS 5.1/5.2-ISE 1.0.4 Migration Tool to perform operations that export Cisco Secure ACS Release 5.1/5.2 data from its database and import the migrated data into a Cisco ISE 1.0.4 appliance.
Chapter 5, "Migrating Data from Cisco Secure ACS 3.x and 4.x to 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 1.0.4 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 1.0.4 system.
Appendix B, "Troubleshooting the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool"	Describes how to troubleshoot an issues you might encounter with using the Cisco Secure ACS 5.1/5.2-ISE 1.0.4 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 1.0.4 appliance:

- See Appendix A, "Cisco Secure ACS 5.1/5.2 and Cisco ISE 1.0.4 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 1.0.4 Migration Overview" for an overview of the Cisco Secure ACS 5.1/5.2 database, data objects, and architecture and the process of migrating its data to the Cisco ISE 1.0.4 appliance.
- See Chapter 2, "Understanding the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool" to understand the functional and configuration differences and similarities between Cisco Secure ACS Release 5.1/5.2 and Cisco ISE 1.0.4, and for specific configuration recommendations.
- See Chapter 3, "Installing the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool" to understand how to install the Cisco Secure ACS 5.1/5.2-ISE 1.0.4 Migration Tool.
- See Chapter 4, "Using the Cisco Secure ACS 5.1/5.2-Cisco ISE 1.0.4 Migration Tool" to understand the process required for migrating existing Cisco Secure ACS Release 5.1/5.2 data to Cisco ISE 1.0.4 using the Cisco Secure ACS 5.1/5.2-ISE 1.0.4 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.

Related Documentation

Release-Specific Documents

Table 1 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 1 Product Documentation for Cisco Identity Services Engine

Document Title	Location
Release Notes for the Cisco Identity Services Engine, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
Cisco Identity Services Engine Network Component Compatibility, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
Cisco Identity Services Engine User Guide, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4	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 1.0.4	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine API Reference Guide, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine Troubleshooting Guide, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html
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 Policy Management Business Unit documentation are available on www.cisco.com 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

Documentation Updates

Table 2 Updates to Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0.4

Date	Description
9/30/2011	Cisco Identity Services Engine Maintenance Release 1.0.4.573
8/26/2011	Content updates for Cisco Identity Services Engine Maintenance Release 1.0.4.558: • Fixed CSCtr69676

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 1.0.4 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.

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 Cisco Secure ACS to Cisco ISE.

Instead, a migration tool and procedure is available that reads the data from Cisco Secure ACS and creates corresponding data in 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 Cisco ISE 1.0.4 migration process requires minimum user interaction and the full set of configuration data is migrated from Cisco Secure ACS to Cisco ISE.

Supported Migration from Cisco Secure ACS to Cisco ISE

Cisco ISE supports data migration from Cisco Secure ACS 5.1 and 5.2 using the Cisco Secure ACS-ISE 1.0.4 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 1.0.4 using the Cisco Secure ACS-ISE 1.0.4 Migration Tool.

Note A direct upgrade is available from Cisco Secure ACS 5.0 to 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 Cisco Secure ACS 3.x or 4.x to Cisco Secure ACS 5.0, see Migrating Data from Cisco Secure ACS 3.x and 4.x to ACS 5.1/5.2.

Software Requirements

The Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool runs on a Windows machine. The machine should have JAVA installed on it.

The minimum disk space required is 512 megabytes (MB). 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.

The minimum RAM required is 1 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 RAM.

Before running the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool, make sure that you have upgraded to the latest Cisco ISE Maintenance Release 1.0.4 and have installed the latest patches for ACS 5.1 and 5.2.

Functional Description

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

1. Export data from Cisco Secure ACS.
2. Persist data in the migration tool.
3. Import data into Cisco ISE 1.0.4.

The following are the major features of the Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 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 Cisco Secure ACS and request to export 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 1.0.4 appliance successfully. In cases where the data is invalid, this status is logged in the migration report.

Data Persistency

Cisco ISE does not support an upgrade from Cisco Secure ACS to Cisco ISE 1.0.4. Therefore, if you want to upgrade your Cisco Secure ACS appliance to Cisco ISE, you have to uninstall Cisco Secure ACS and reimage the appliance with the Cisco ISE 1.0.4 image. The migration tool persists 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 Cisco Secure ACS and is ready to import the data into Cisco ISE 1.0.4. At this point, you have to reimage the Cisco Secure ACS machine with the Cisco ISE 1.0.4 image and start the import operation. You can view the import progress through the Cisco ACS 5.1/5.2-ISE 1.0.4 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 1-1.

Table 1-1 Object Scalability for Migration in Cisco ISE 1.0.4

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

Table 1-1 Object Scalability for Migration in Cisco ISE 1.0.4 (continued)

Objects	Small Deployment	Medium Deployment	Large Deployment
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
Certificates	2	5	10

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

High Availability

The Cisco ACS 5.1/5.2-ISE 1.0.4 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, 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

Two Cisco ISE reports are available while migrating Cisco Secure ACS 5.1/5.2 data to the Cisco ISE appliance using the Cisco Secure ACS 5.1/5.2-ISE 1.0.4 Migration Tool. The two types of reports (export and import) indicate specific information or errors that are encountered during the export of data from the Cisco Secure ACS database or during the import of data into the Cisco ISE appliance.

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 Cisco Secure ACS and Cisco ISE.

Table 1-2 describes the report type, the message type, and message contents in these import or export reports.

Table 1-2 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 based on an export failure or an export not attempt because the data object is not supported by Cisco ISE 1.0.4 (for example, if it were a TACACS-based device).
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 and Figure 1-2 are examples of the export and import reports, respectively.

Figure 1-1 Example of Export Report

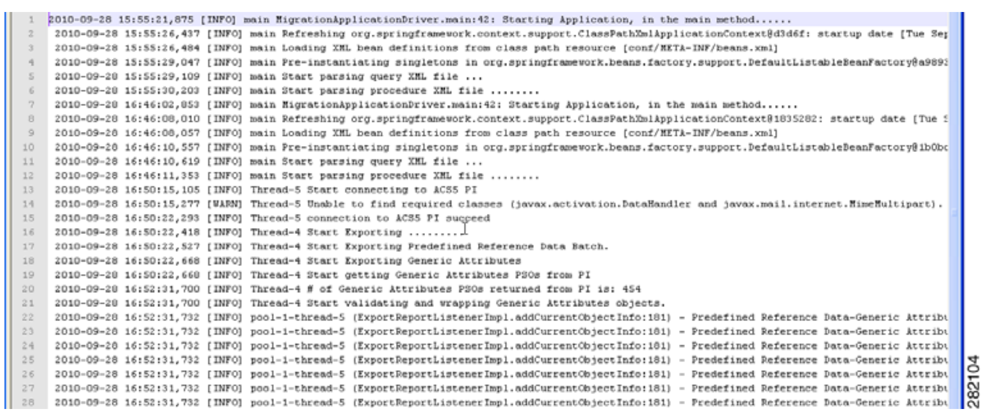


Figure 1-2 Example of Import Report

```
==========================================================
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

CHAPTER 2

Understanding the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool

This chapter provides information about the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool that is used to migrate data from a Cisco Secure ACS 5.1/5.2 database to Cisco ISE Release 1.0.4 appliance. The following topics describe what you should know about the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool before using it to migrate data:

Overview: Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4

The Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool is designed to provide users that have existing installed Cisco Secure ACS 5.1/5.2 database with a method for transporting that data to a Cisco ISE 1.0.4 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. The three steps in the migration process using the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool include:

- Exporting the Cisco Secure ACS 5.1/5.2 data from its database
- Persisting this data using the migration tool
- Importing the persisted data into the Cisco ISE 1.0.4 appliance

The Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool supports the migration of only Cisco Secure ACS Release 5.1/5.2 data to a Cisco ISE 1.0.4 appliance, which requires a three-step process. For example, you can use the Cisco ACS 5.1/5.2-ISE 1.0.4 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. Reimage the Cisco Secure ACS-1121 hardware appliance, which is the same physical hardware as the Cisco ISE 3315 appliance, with the Cisco ISE 1.0.4 software.
3. Import the converted Cisco Secure ACS Release 5.1/5.2 data from the secure external server into the Cisco ISE 1.0.4 appliance.

The only supported direct migration process using the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool is from a Cisco Secure ACS Release 5.1/5.2 system to a Cisco ISE 1.0.4 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 listed in Table 2-1.

The Cisco Secure ACS 5.1/5.2-ISE 1.0.4 Migration Tool *migrates* data from a Cisco Secure ACS 5.1/5.2 system to a Cisco ISE 1.0.4 appliance, which is a different process from an *upgrade* used for earlier versions of Cisco Secure ACS Release 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 Cisco Secure ACS 3.x and 4.x to ACS 5.1/5.2"
Cisco Secure ACS Release 4.x	Cisco Secure ACS Release 5.0	• Chapter 5, "Migrating Data from Cisco Secure ACS 3.x and 4.x to ACS 5.1/5.2"
Cisco Secure ACS Release 5.0	Cisco Secure ACS Release 5.1/5.2	• Chapter 5, "Migrating Data from Cisco Secure ACS 3.x and 4.x to ACS 5.1/5.2"

Note For information and documentation links about migrating Cisco Secure ACS Release 3.x and 4.x to 5.0 to Cisco Secure ACS 5.1/5.2, see Chapter 5, "Migrating Data from Cisco Secure ACS 3.x and 4.x to 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 5.1/5.2-ISE 1.0.4 Migration Tool

This section describes:

- Migration Tool Components, page 2-3
- Data Items Migrated, page 2-4
- Data Structure Mapping, page 2-5

The Cisco Secure ACS 5.1/5.2-ISE 1.0.4 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 necessary for importing the data into a format usable by the Cisco ISE 1.0.4 system.

The Cisco Secure ACS 5.1/5.2 and Cisco ISE 1.0.4 applications may or may not run on the same type physical hardware. So the Cisco Secure ACS 5.1/5.2-ISE 1.0.4 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.

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

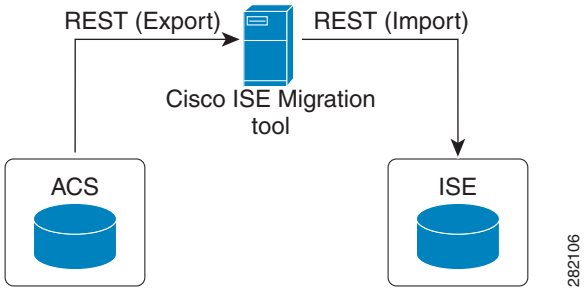


Figure 2-2 shows the deployment scenario when Cisco Secure ACS is installed on the same appliance upon which the Cisco ISE software will be installed (single-appliance deployment). In a single-appliance deployment, complete the following steps:

Step 1 Install the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool on a standalone Windows machine.

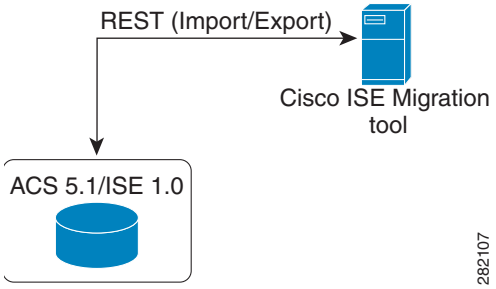
Step 2 Export the Cisco Secure ACS 5.1/5.2 data from the Cisco Secure ACS appliance.

Step 3 Reimage the appliance with the Cisco ISE 1.0.4 software.

Step 4 Import the Cisco Secure ACS 5.1/5.2 data into the Cisco ISE 1.0.4 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.

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, page 2-4
- Status Reporting, page 2-4
- Export and Import, page 2-4

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 5.1/5.2-ISE 1.0.4 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 Cisco Secure ACS to Cisco ISE is not supported. The Cisco Secure ACS 5.1/5.2-ISE 1.0.4 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 1.0.4 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, Cisco Secure ACS 5.1/5.2-ISE 1.0.4 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. The tool reports any issue with the data, which may require administrator intervention at the end of the export phase.

Data Items Migrated

The following factors are considered when the priority is assessed. A weight of 1-3 is assigned, except for the Required for Policy factor, which has a dominant weight of up to 5.

- Required for Policy—The prime objective of the migration tool is to migrate effortlessly the Cisco Secure ACS 5.1/5.2 operational policies to Cisco ISE 1.0.4. The policy may involve many types of configuration items. For example, identity stores contain attributes that may be used in policy, and likewise, network devices related to Network Device Groups may also be used similarly. The policy

affects and defines the order of object migration. The items on which policy is dependent are migrated but not the policy itself. Ths Cisco ISE administrator has to manually define the policies after migration.

- Data Set Size— The number of each type of data item is also considered. There may be thousands of users or devices which you cannot recreate manually. Alternatively, there are some objects of which there is only a single instance, such as global protocol settings or the default device.
- Manual Migration Complexity— This factor indicates how difficult it is to migrate the data manually. Configuration data with a small number of parameters would be easy to recreate manually, but complex data sets or data difficult to configure will be much harder to recreate.

Some items related to the Security Group Access are also migrated. This solution has a very limited deployment, so priority for migration of these items is reduced by giving a low weightage for Data Set Size.

For a complete list of data objects that are migrated and data information mapping that takes place during export, see Appendix A, “Cisco Secure ACS 5.1/5.2 and Cisco ISE 1.0.4 Data Structure Mapping”.

Data Structure Mapping

Data structure mapping from Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 is the process by which each of the data objects are analyzed and validated during the export phase by the Cisco Secure ACS 5.1/5.2-ISE 1.0.4 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 1.0.4 Data Structure Mapping”.

CHAPTER 3

Installing the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool

This chapter provides information about installing the Cisco ACS 5.1/5.2-ISE 1.0.4 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 1.0.4 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:
  - Installed Cisco ISE 1.0.4 on the target machine (if this is a dual-appliance migration).
  - Have the Cisco ISE 1.0.4 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 1.0.4 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 1.0.4 target machine	Refer to the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4*. This appliance must have at least 2 GB of RAM.
Java JRE 1.6	Install Java JRE, version 1.6 or higher. 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 1.0.4 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 ACS 5.1/5.2-ISE 1.0.4 Migration Tool is designed to migrate Cisco Secure ACS 5.1/5.2 data objects to Cisco ISE 1.0.4. 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 3-2
- 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 ACS 5.1/5.2-ISE 1.0.4 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 ACS 5.1/5.2-ISE 1.0.4 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 ACS 5.1/5.2-ISE 1.0.4 Migration Tool may run for approximately 20 hours to migrate 10,000 devices, 25,000 users, 100,000 hosts, 100 identity group, 420 DACL, 320 authorization profile, 6 devices hierarchies, and 20 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 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.

Installing and Initializing the ACS 5.1/5.2-ISE 1.0.4 Migration Tool

You can download the Cisco Secure ACS 5.1/5.2-ISE 1.0.4 Migration Tool files using the Cisco ISE user interface.

To download and run the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool software, complete the following steps:

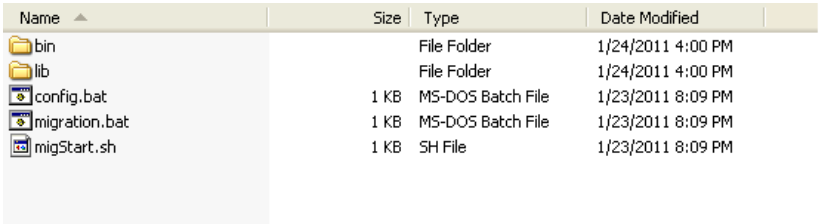
Step 1 Download the migration tool files by entering the following command on the Cisco ISE user interface address bar:

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

Note The only currently supported browser for downloading the migration tool files is Firefox version 3.6.x. Microsoft Windows Internet Explorer (IE8 and IE7) browsers are not currently supported in this release.

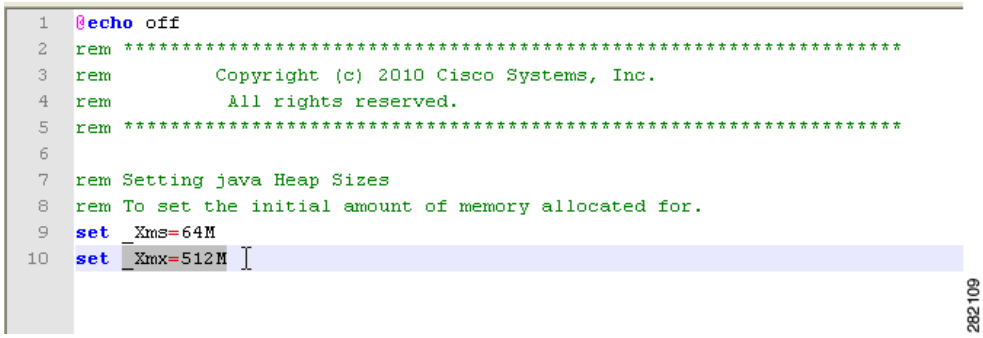
Step 2 Extract the content of the .zip file. Figure 3-1 illustrates the directory structure of the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool software.

Figure 3-1 Directory Structure of the Cisco ACS 5.1/5.2-Cisco ISE 1.0.4 Migration Tool



Step 3 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

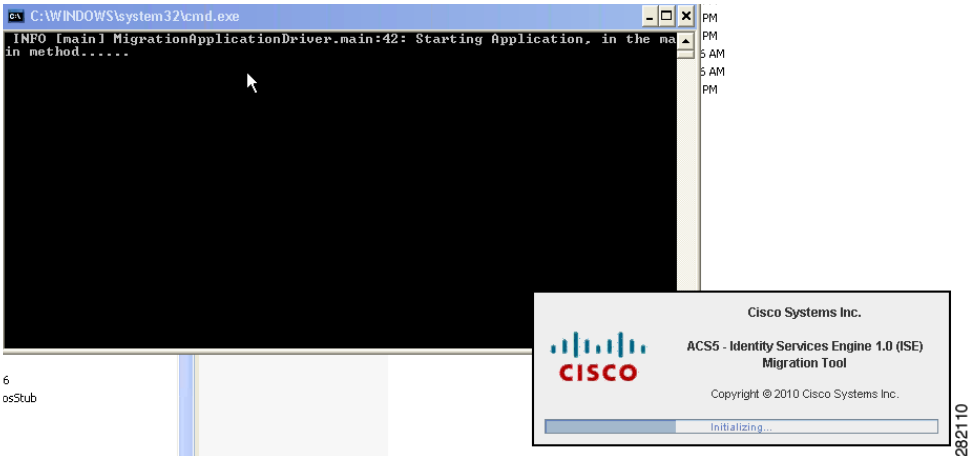


Step 4 Click **Save** to preserve your heap size configuration.

Step 5 Click **migration.bat** to launch the migration process.

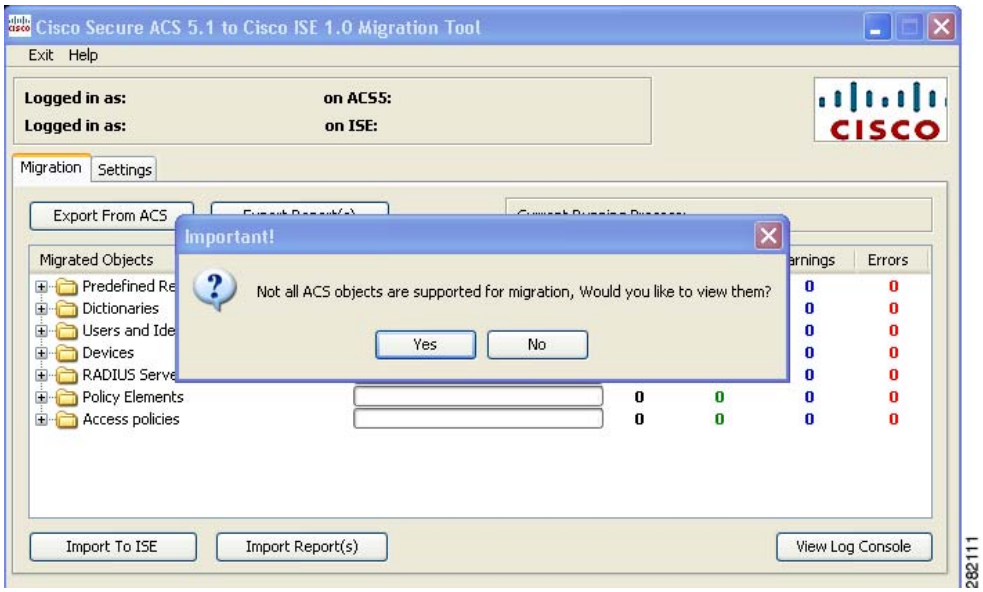
The initializing screen is displayed (see Figure 3-3).

Figure 3-3 Initializing Screen



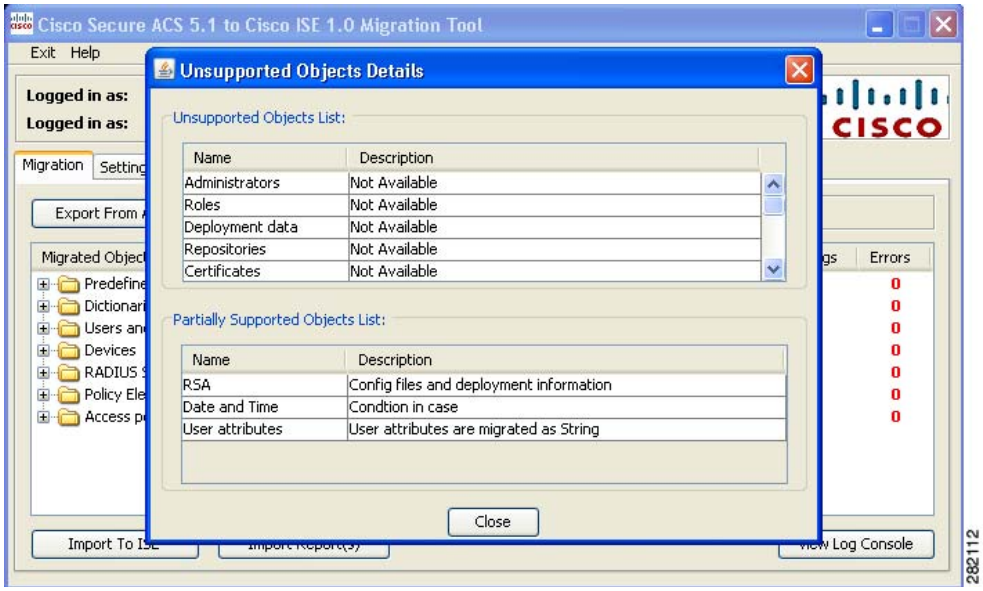
After the migration tool is initialized, unsupported Cisco Secure ACS objects still need to be migrated, and the following message is displayed (see Figure 3-4).

Figure 3-4 Message Displayed for Unsupported Objects



Step 6 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 7 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 5.1/5.2-Cisco ISE 1.0.4 Migration Tool".

CHAPTER 4

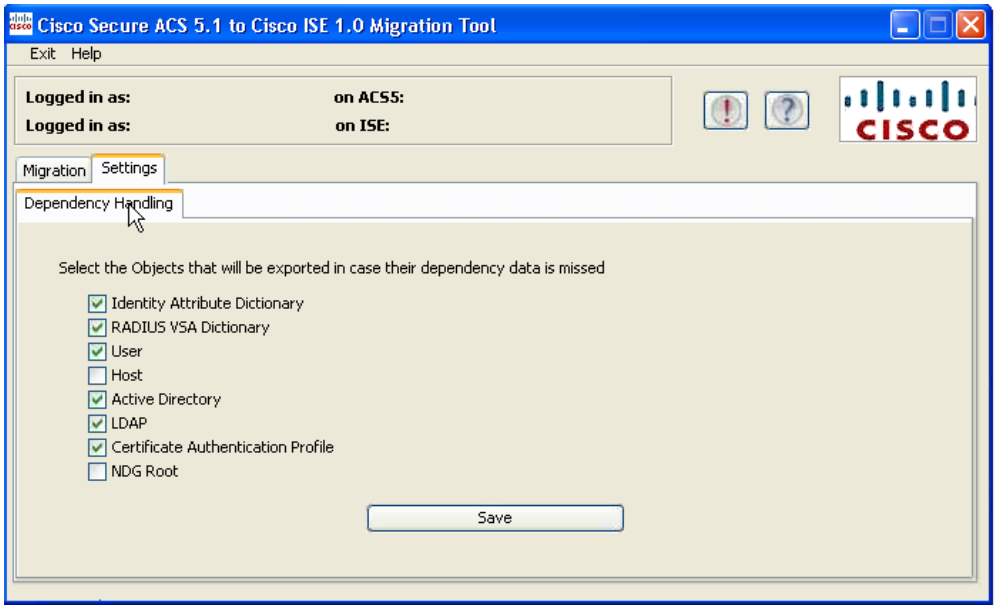
Using the Cisco Secure ACS 5.1/5.2-Cisco ISE 1.0.4 Migration Tool

This chapter describes how to use the Cisco Secure ACS 5.1/5.2-Cisco ISE 1.0.4 migration tool to migrate data from a Cisco Secure ACS 5.1/5.2 database to a Cisco ISE 1.0.4 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:

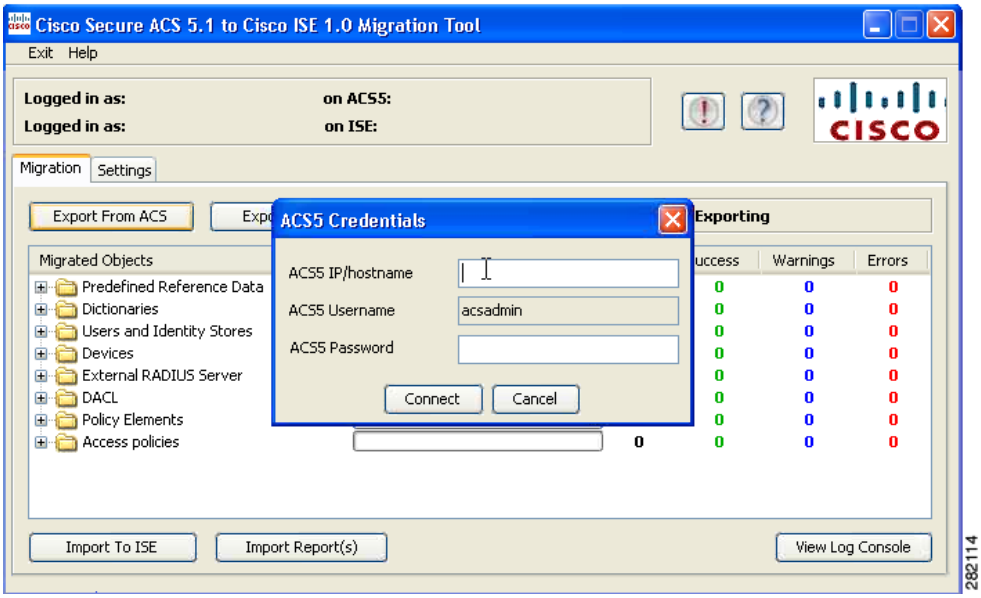
Step 1 In the Cisco Secure ACS 5.1/5.2-Cisco ISE 1.0.4 migration tool main window, click **Settings** to display the list of data objects you want to migrate.



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**.

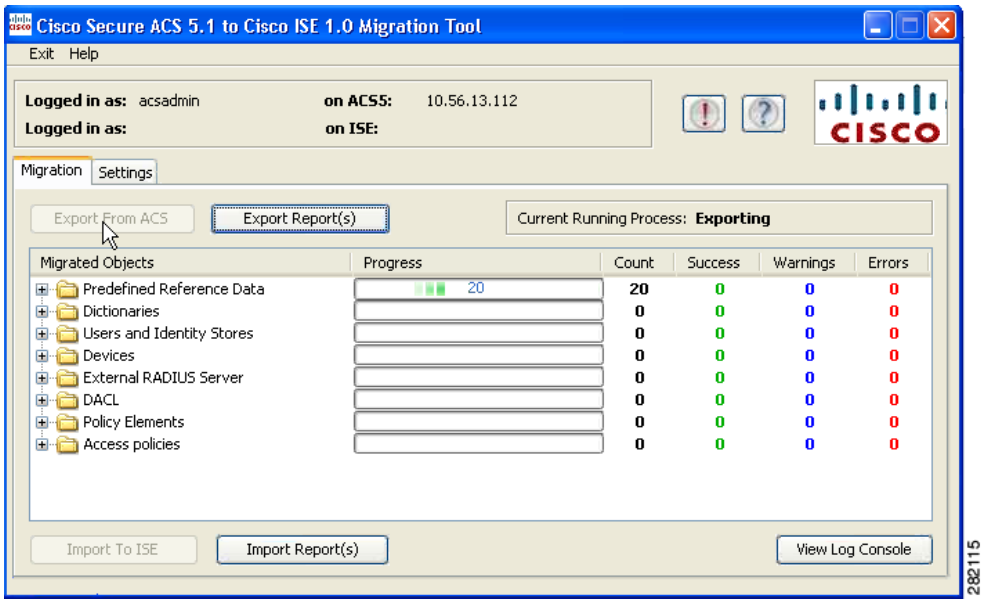
Step 3 In the main window of the Cisco Secure ACS 5.1/5.2-Cisco ISE 1.0.4 migration tool, click **Migration** and click **Export from ACS.**

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

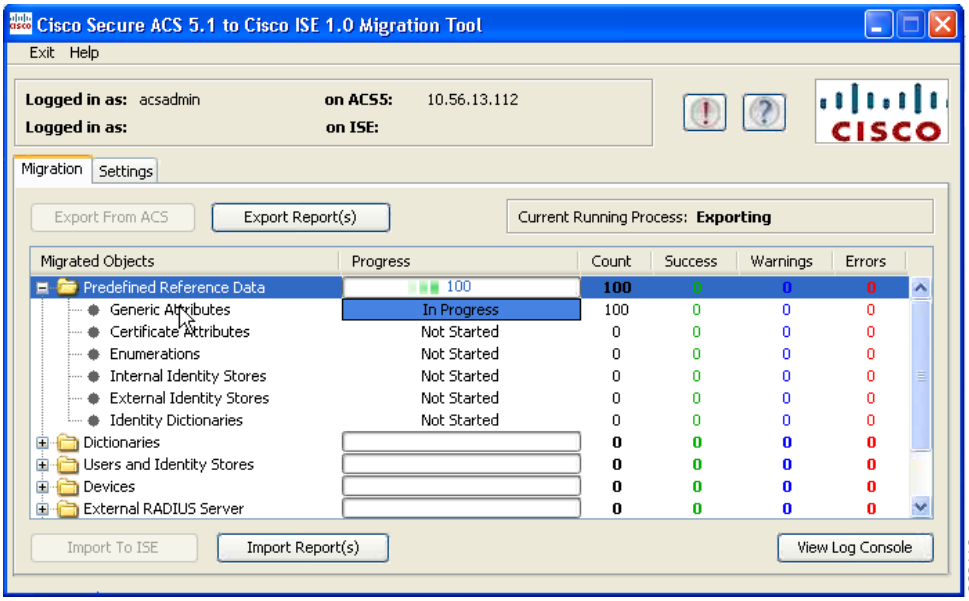


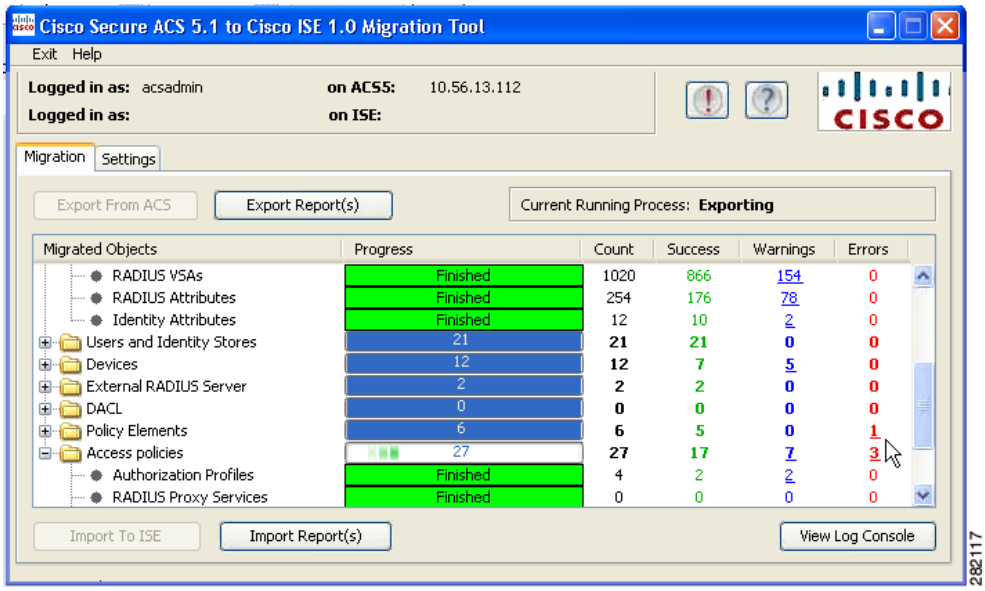
Step 4 Enter the IP address (or host name) and the password for the Cisco Secure ACS 5.1/5.2 system into the ACS Credentials window, and click **Connect**.

The data migration process begins.



Step 5 Check the progress of the migration of Cisco Secure ACS 5.1/5.2 data by viewing the main window of the Cisco Secure ACS 5.1/5.2-Cisco ISE 1.0.4 migration tool.

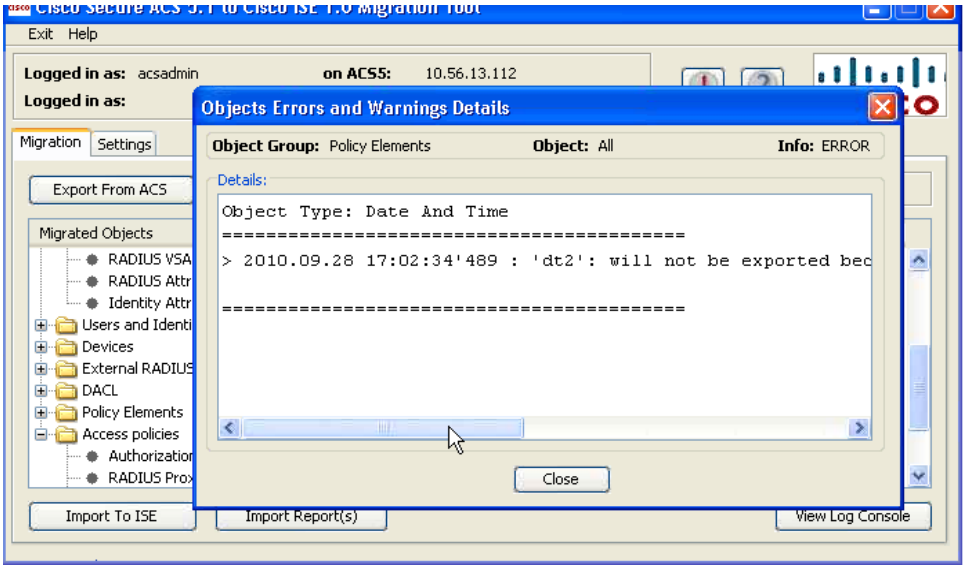




The main window of the Cisco Secure ACS 5.1/5.2-Cisco ISE 1.0.4 migration tool displays the current count of successful objects exports, and also lists any objects that triggered warnings or errors.

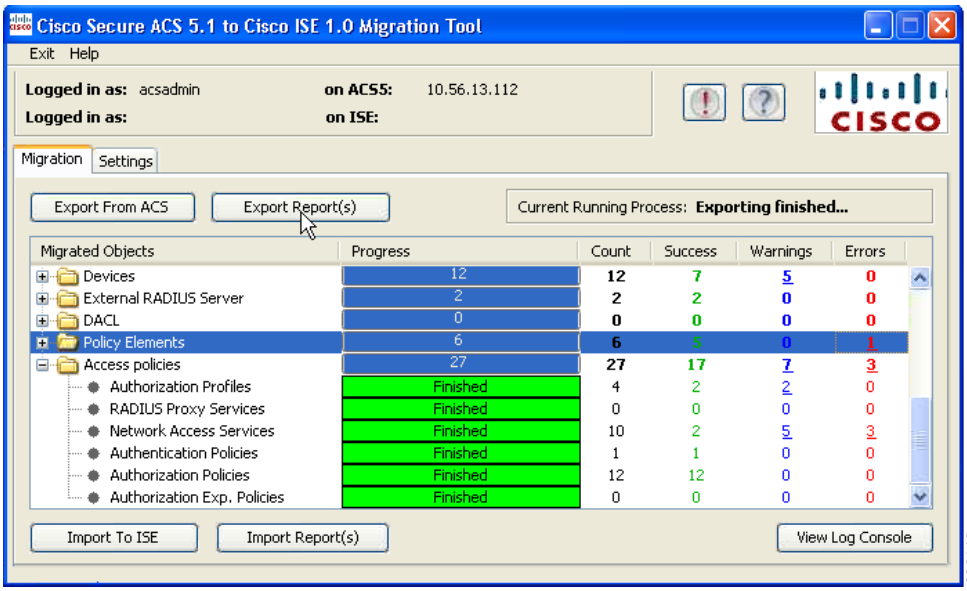
Step 6 To get more information about a warning or error that occurred during the export process, click any listed **Warnings** or **Errors** in the table. The following example shows the result returned result from choosing an error to display.

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.



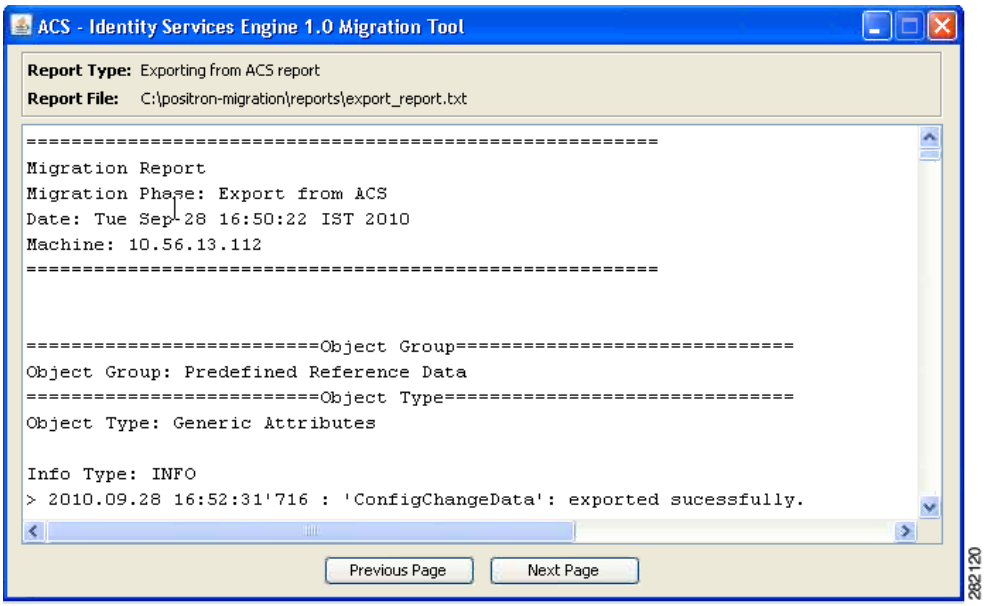
Step 7 Scroll to the right to display the complete set of details, and click **Close** to close this window.

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 5.1/5.2-Cisco ISE 1.0.4 migration tool displays this status.



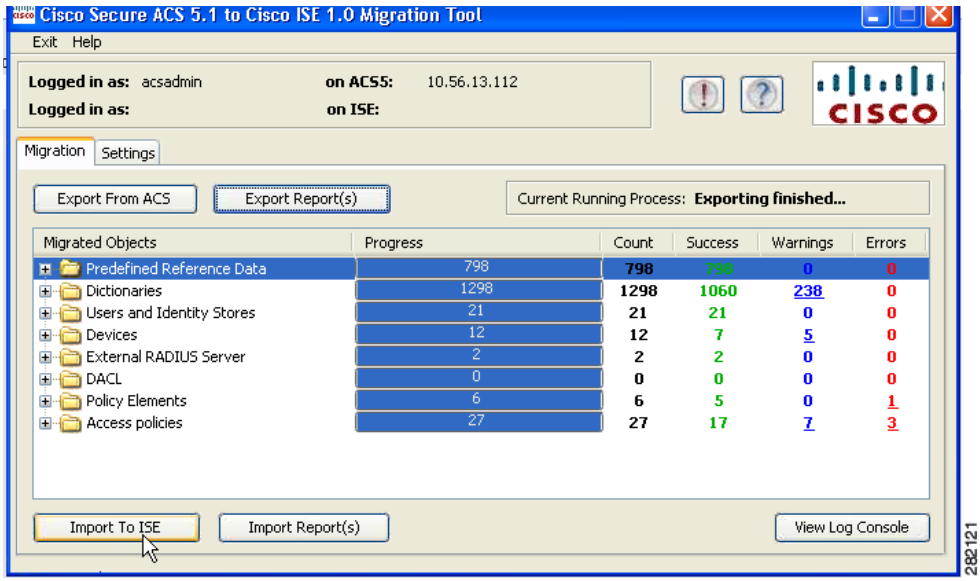
Step 8 Click **Export Report(s)** to view the contents of the report, which summarizes the export operation as shown in the following example.

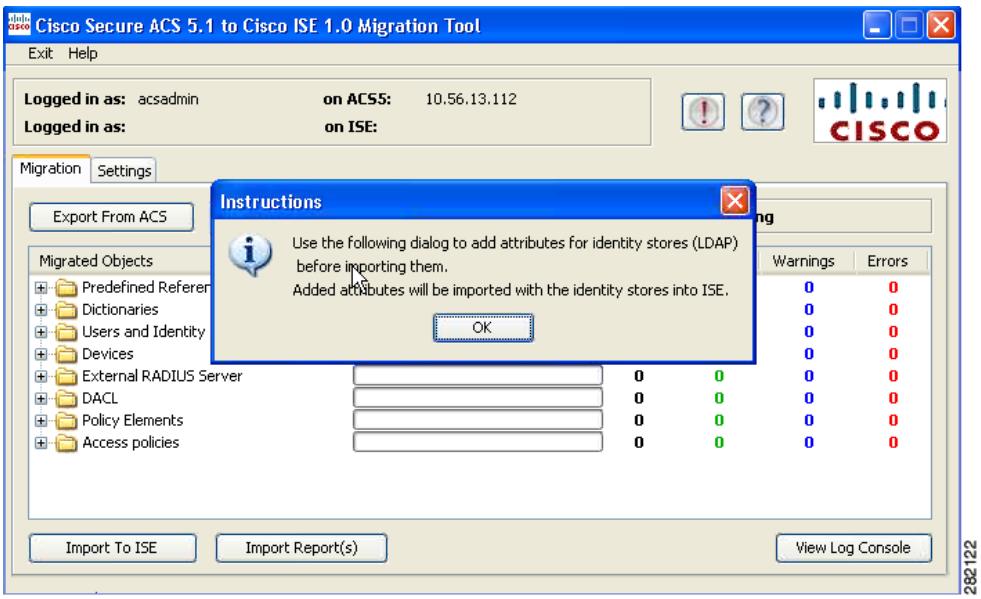
Each export report contains header information with the operation type, date and time, and system IP address or host name. Each object group details the types and related information for the objects in that group. Each report ends with an report that summarizes the start and end date and time, and the 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 5.1/5.2-Cisco ISE 1.0.4 migration tool.

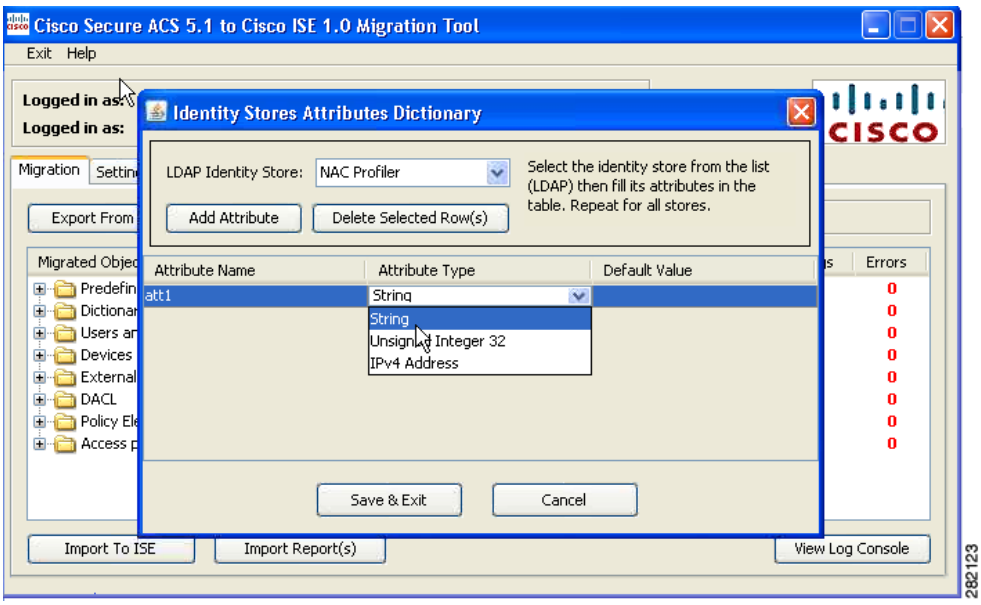
You are prompted to add attributes to the LDAP identity stores before they are imported into Cisco ISE 1.0.4.





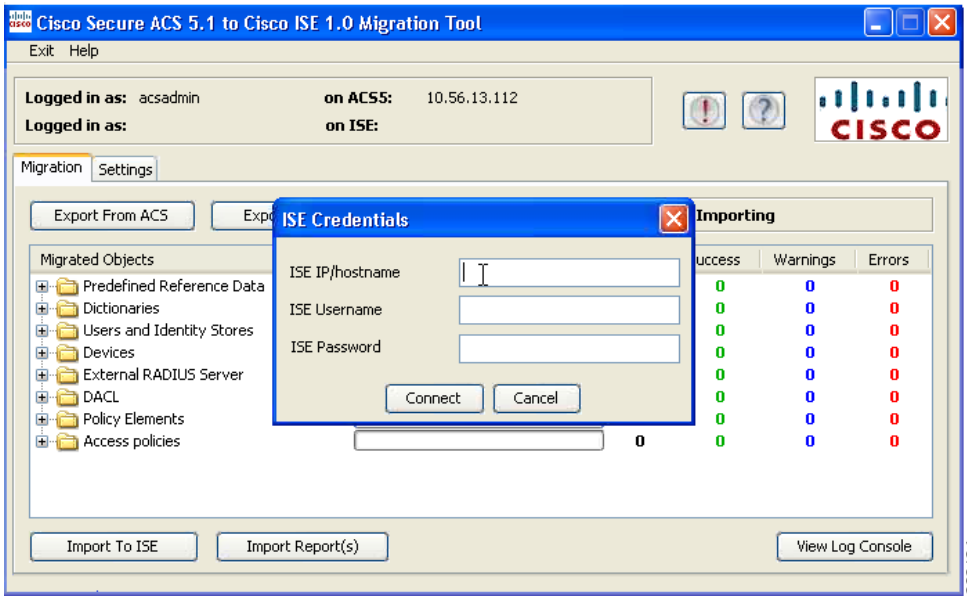
Step 10 Click **OK** to start the attribute add process for your LDAP identity stores.

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

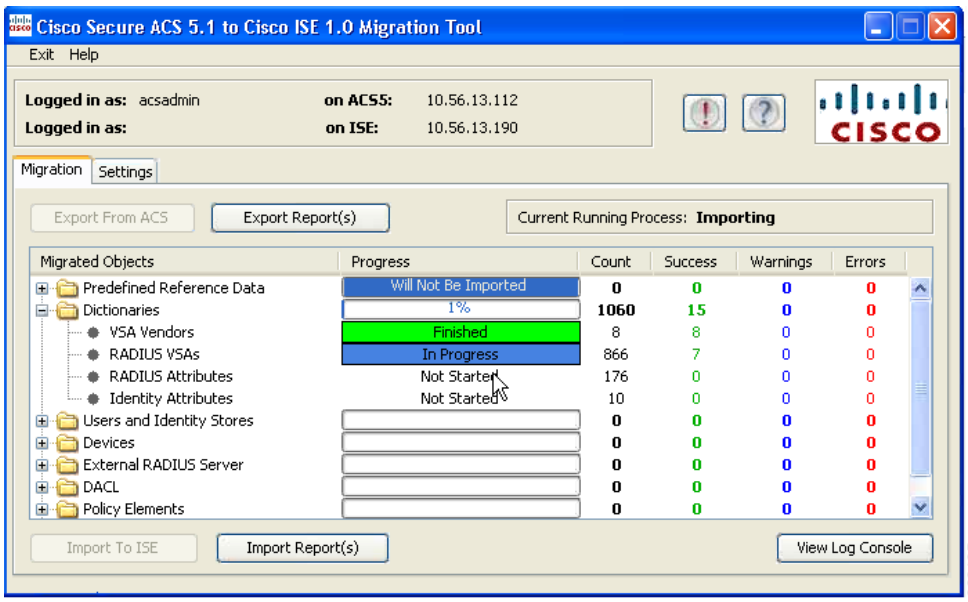


Step 12 Enter a name in the **Attribute Name** field, select an attribute type from the **Attribute Type** pull-down list, enter a value in the **Default Value** field, and click **Save & Exit**.

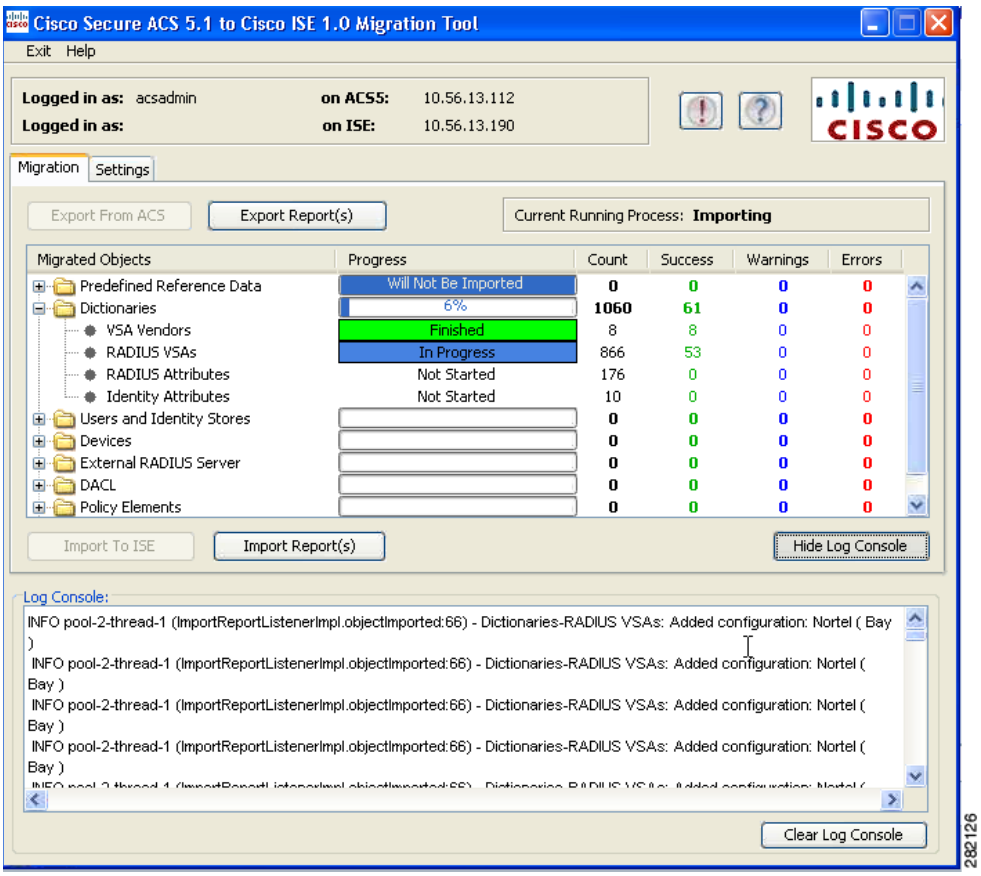
Step 13 After you have completed the attribute addition, click **Import to ISE** to proceed with the importing process, and log into the Cisco ISE system using the ISE Credentials window.



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.

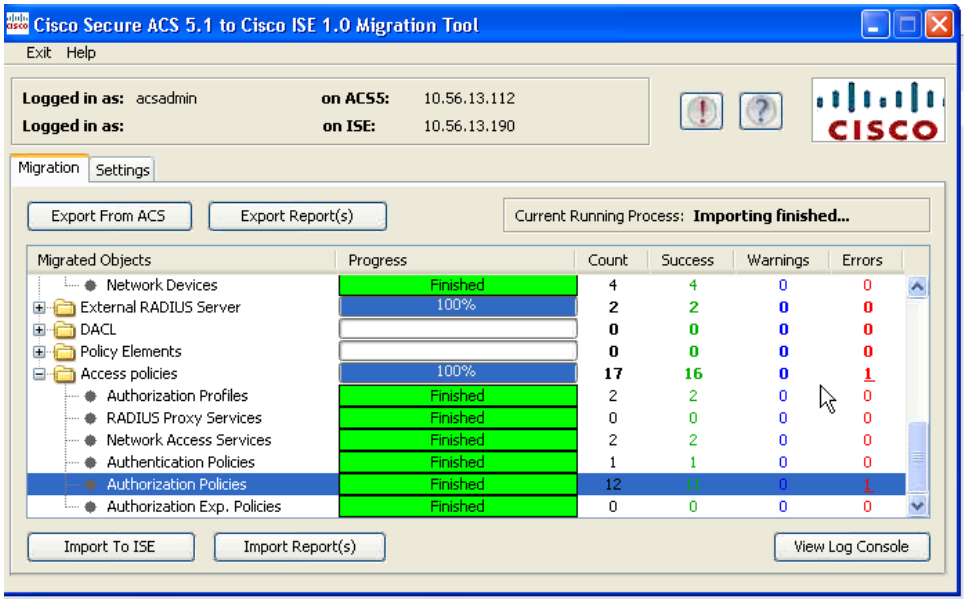


Step 15 At any point in the import or export process, click **View Log Console** to display a real-time look at the current status of the import or export operation.

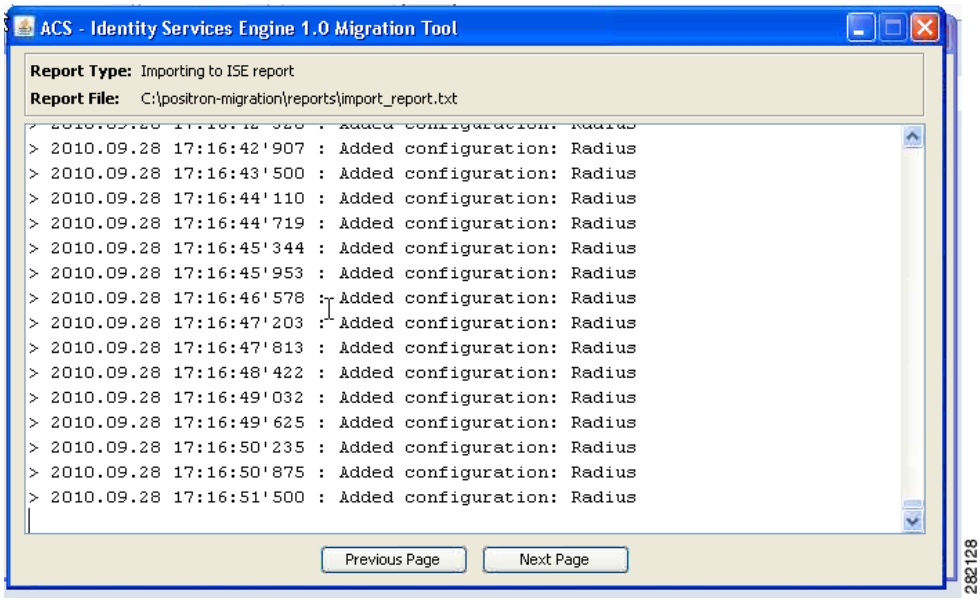


Step 16 To get more information about any warning or error that occurred during the import process, click **Warnings** or **Errors** in the table where it is listed (see step 6), and view any details.

When the data import operation is complete, this status is displayed in the main window of the Cisco Secure ACS 5.1/5.2-Cisco ISE 1.0.4 migration tool.



Step 17 To view the complete report on the data imported into the Cisco ISE 1.0.4 appliance, click **Import Report(s)**. The report is displayed.

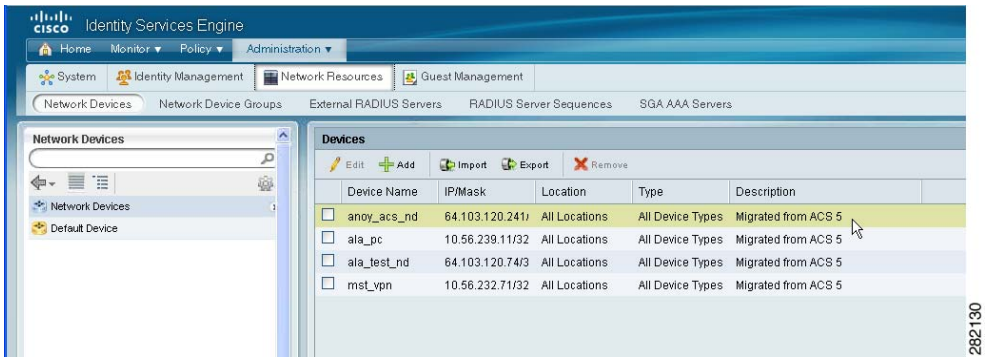


Step 18 To verify that the import process has completed, log into the Cisco ISE 1.0.4 appliance:

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

Step 19 In the Cisco ISE main window for example, navigate to **Administration > Network Resources > Network Devices** to display the Network Devices window to verify if any ACS-based devices were imported.

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



This concludes the import/export operations using the Cisco Secure ACS 5.1/5.2-Cisco ISE 1.0.4 migration tool.

Providing Import and Export Report Files

If you decide to share the import report or export report files with anyone, or to save them in another location, you can find them in the Reports folder in the migration tool directory (import_report.txt and export_report.txt).

CHAPTER 5

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

This chapter provides links to Cisco documentation that describes how to migrate data from earlier Cisco Secure 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.

Once 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, Release1.0.4 appliance. The following topics cover this information:

Introduction

Before you begin any attempt to migrate data to a Cisco ISE 1.0.4 appliance, make sure you have read and understand all setup, backup, and installation instructions in Chapter 3, "Installing the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool."

Depending upon the starting release stage of the Cisco Secure ACS data that you want to migrate to a Cisco ISE 1.0.4 appliance, there may be several migration stages required before you can use the Cisco Secure ACS 5.1/5.2-Cisco ISE 1.0.4 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 Cisco Secure ACS 5.0.
- If you have migrated your data to or are starting from Cisco Secure ACS 5.0, then you need to migrate your data to 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 5.1/5.2-Cisco ISE 1.0.4 migration tool to migrate your data to a Cisco ISE 1.0.4 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 1.0.4 appliance.

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

For information on migrating data from 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 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 1.0.4 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 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4:

- Network device group (NDG) types and hierarchies
- Network devices
- Default network device
- External Remote Authentication Dial-In Service (RADIUS) servers
- Identity group
- Internal users
- Internal endpoints (hosts)
- Lightweight Directory Access Protocol (LDAP)
- AD
- RSA (partial support, see Table A-25)
- RADIUS token (see Table A-24)
- Certificate authentication profile

- Date and time condition (partial support, see Migration Policies, page A-3)
- 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
- DACL
- RADIUS proxy service
- User password complexity
- Identity sequence and RSA prompts

Data Objects That Are Not Migrated

The following data objects are not migrated from Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4:

- Identity (authentication) policy
- Authorization policy (for network access)
- Authorization exception policy (for network access)
- Service selection policy (for network access)
- 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 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4:

- 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 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4:

- UTF8 data is not supported.
- 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.

Migration Policies

Authentication and Authorization policies are not migrated and it is the responsibility of the administrator performing migration to define the policies manually.

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 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.0.4
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 1.0.4
String	Supported
UI32	—
IPv4	—
Boolean	—
Date	—

Table A-3 Hosts Attributes Migrated from Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.0.4
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 1.0.4
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 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.0.4
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 1.0.4
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 Cisco Secure ACS 5.1/5.2 and its equivalent in Cisco ISE 1.0.4 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-6 (network device property mapping)
- Table A-8 on page A-6 (Active Directory property mapping)
- Table A-9 on page A-7 (external RADIUS server property mapping)
- Table A-10 on page A-7 (hosts/endpoints property mapping)
- Table A-11 on page A-8 (identity dictionary property mapping)
- Table A-12 on page A-8 (identity group property mapping)
- Table A-13 on page A-8 (LDAP property mapping)
- Table A-14 on page A-9 (NDG types mapping)
- Table A-15 on page A-10 (NDG hierarchy mapping)
- Table A-16 on page A-10 (RADIUS dictionary vendors mapping)
- Table A-17 on page A-10 (RADIUS dictionary attributes mapping)
- Table A-18 on page A-11 (users mapping)
- Table A-19 on page A-11 (certificate authentication profile)
- Table A-20 on page A-12 (authorization profile mapping)
- Table A-21 on page A-12 (DACL mapping)
- Table A-22 on page A-12 (external RADIUS server mapping))
- Table A-23 on page A-12 (identity attributes dictionary mapping)
- Table A-24 on page A-13 (RADIUS token mapping)
- Table A-25 on page A-14 (RSA mapping)

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 1.0.4 Network Device Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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 Terminal Access Controller Access-Control System (TACACS) is unsupported in Cisco ISE 1.0.4.
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 1.0.4 Active Directory Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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.
User attributes	Migrate as is.
Groups	Migrate as is.

Note The Cisco Secure ACS 5.1/5.2-ISE 1.0.4 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 1.0.4 External RADIUS Server Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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 1.0.4 Hosts (Endpoints) Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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").
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").

Table A-10 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 Hosts (Endpoints) Mapping (continued)

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 Properties
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 1.0.4 Identity Dictionary Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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 1.0.4 Identity Group Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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 1.0.4 LDAP Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 Properties
Name	Name
Description	Description
Server connection information	Migrate as is. (Server Connection tab; see Figure A-1 on page A-9.)
Directory organization information	Migrate as is. (Directory Organization tab; see Figure A-2 on page A-9.)

Table A-13 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 LDAP Mapping (continued)

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 Properties
Directory groups	Migrate as is.
Directory attributes	Migration is done manually (using the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool).

Figure A-1 Server Connection Tab

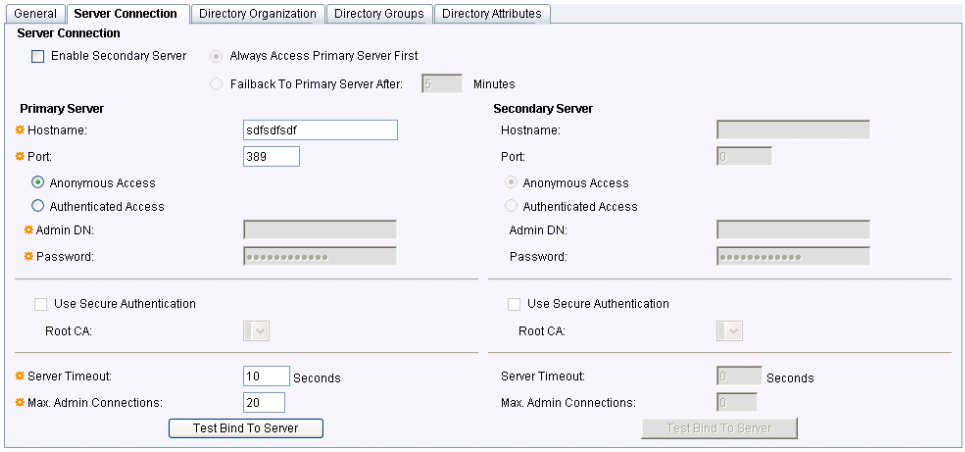


Figure A-2 Directory Organization Tab

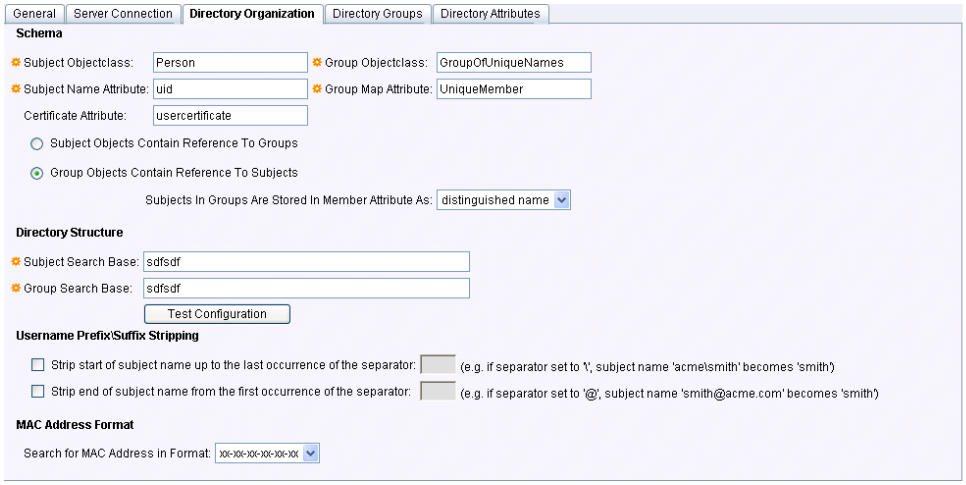


Table A-14 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 NDG Types Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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 1.0.4 NDG Hierarchy Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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 Cisco ISE 1.0.4 does not recognized the colon as a valid character.

Table A-16 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 RADIUS Dictionary (Vendors) Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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 1.0.4 RADIUS Dictionary (Attributes) Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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 nam.e (In addition, the NDG type is the prefix for this object name.)
Direction	Not supported in Cisco ISE.

Table A-17 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 RADIUS Dictionary (Attributes) Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 Properties
Multiple allowed	Not supported in Cisco ISE.
Attribute type	Migrate as is.
Add policy condition	Not supported in Cisco ISE.
Policy condition display name	Not supported in 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 1.0.4 User Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 Properties
Name	Name
Description	Description
Status	No need to migrate this property. (This property does not exist in Cisco ISE.)
Identity group	Migrate to identity groups in Cisco ISE.
Password	Password
Enable password	No need to migrate this property. (This property does not exist in Cisco ISE.)
Change password on next login	No need to migrate this property.
User attributes list	User attributes are imported from Cisco ISE and associated with the users.

Table A-19 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 Certificate Authentication Profile Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 Properties
Name	Name
Description	Description
Principle user name (X.509 attribute)	Principle user name (X.509 attribute)
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 1.0.4 Authorization Profile Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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 1.0.4 Downloadable ACL Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 Properties
Name	Name
Description	Description
DACL content	DACL content

Table A-22 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 External RADIUS Server Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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 1.0.4 Identity Attributes Dictionary Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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.)

Table A-23 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 Identity Attributes Dictionary Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 Properties
Not exported/extracted yet from Cisco Secure ACS	Allowed value = display name
Not exported/extracted yet from Cisco Secure ACS	Allowed value = internal name
Not exported/extracted yet from 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 1.0.4 RADIUS Token Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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
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

Table A-24 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0.4 RADIUS Token Mapping (continued)

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 Properties
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 1.0.4 RSA Mapping

Cisco Secure ACS 5.1/5.2 Properties	Cisco ISE 1.0.4 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

APPENDIX B

Troubleshooting the Cisco ACS 5.1/5.2-ISE 1.0.4 Migration Tool

This appendix describes some common issues or conditions that you might encounter when using the Cisco ACS 5.1/5.2-ISE 1.0.4 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% and the CPU is active.

Condition

The following error message is displayed in the logs:

```
"OutofMemory"
```

Action

Increase the Java heap size to at least 1 GB as described in "Installing and Initializing the ACS 5.1/5.2-ISE 1.0.4 Migration Tool" section on 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.

AD Active Directory. This is a directory service created by Microsoft that stores all information and settings for a deployment in a central database. AD 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 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