Getting Started

This chapter provides detailed information about the Cisco Secure ACS to Cisco ISE Migration Tool that is used for data migration from Cisco Secure Access Control Server (ACS) to Cisco Identity Services Engine (ISE).

The migration tool migrates the configuration data from the following Cisco Secure ACS versions to Cisco ISE 3.0:

- Cisco Secure ACS 5.5 or later—Select the **ACS 5.x Supported Objects** option in the migration tool to migrate all data objects.

  The migration tool migrates the data objects to Cisco ISE initially followed by the corresponding policy configuration when you migrate the data objects from Cisco Secure ACS 5.5 or later.

Migration Overview

The differences in Cisco Secure ACS 5.x and Cisco ISE platforms, operating systems, databases, and information models, mandate a migration application that reads data from Cisco Secure ACS and creates the corresponding data in Cisco ISE. The migration application is a utility that Cisco provides to extract the configuration from Cisco Secure ACS and import it to Cisco ISE. The migration administrator can view the current progress as well as the detailed logs related to the ACS configuration during the entire migration process for troubleshooting purposes. Error messages are displayed for objects, attributes, and policies that are not migrated. After migration, we **strongly** recommend you to verify the accuracy of the migrated configurations. Please ensure that you understand the semantics and structure of the policy sets in Cisco ISE and verify them against the access policies in Cisco Secure ACS.

Note It is possible to leverage the migration application to extract data from Cisco Secure ACS even before installing Cisco ISE. In this manner, the migration application can be leveraged to determine the readiness for migration from Cisco Secure ACS to Cisco ISE.

ISE Community Resource

How To Migrate from ACS 5.x to ISE 2.x

ACS vs ISE Comparison

ACS to ISE Migration

Note The examples and screenshots provided in the ISE Community resources might be from earlier releases of Cisco ISE. Check the GUI for newer or additional features and updates.

Data Migration from Cisco Secure ACS to Cisco ISE

You must first upgrade from Cisco secure ACS, Releases 5.5, 5.6, 5.7 or 5.8 Patch 3 to Cisco secure ACS, Release 5.8 Patch 4 in order to migrate data to Cisco ISE Release 3.0. For more information on Cisco secure ACS, Release 5.8 Patch 4 and TLS 1.2 compatibility, see TLS 1.2 Settings in the *Cisco secure ACS, Release 5.8 Release Notes*.

Before you migrate the existing Cisco Secure ACS, Release 5.5 or later data to Cisco ISE, Release 3.0, VM or appliance, ensure that you have read and understood all setup, backup, and installation instructions.

We recommend that you fully understand the related data structure and schema differences between Cisco Secure ACS, Release 5.5 or later and Cisco ISE, Release 3.0 before you attempt to migrate existing Cisco Secure ACS, Release 5.5 or later data.

Note Due to the differences in the Cisco ISE and Cisco Secure ACS data related to the naming convention, policy hierarchy, pre-defined objects, and so on, the migration tool may not support all objects. However, it displays warnings and errors for objects that are not migrated to facilitate corrective measures.

Overview of Cisco Secure ACS to Cisco ISE Migration Tool

The migration tool helps you to migrate the data from Cisco Secure ACS, Release 5.5 or later to Cisco ISE, Release 3.0. 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 migration tool runs on Linux-based and Windows-based systems. The migration tool works by exporting the Cisco Secure ACS data files, analyzing the data, and making the required data modifications that are necessary for importing the data into a format that is usable by the Cisco ISE, Release 3.0.

- The migration tool requires minimum user interaction, and full set of configuration data.
- The migration tool provides you a complete list of unsupported objects.

The Cisco Secure ACS, Release 5.5 or later and Cisco ISE, Release 3.0 applications may or may not run on the same type of physical hardware. The 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 Cisco ISE applications to run on supported hardware platforms or VMware servers. You cannot directly run the migration tool on a Cisco Secure ACS appliance. The Cisco Secure ACS PI reads and returns the 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 For information about the migration process from earlier releases of Cisco secure ACS to Cisco ISE 3.0, see Migrate from Earlier Releases of Cisco Secure ACS to Cisco ISE.

You must first upgrade from Cisco secure ACS, Releases 5.5, 5.6, 5.7 or 5.8 Patch 3 to Cisco secure ACS, Release 5.8 Patch 4 in order to migrate data to Cisco ISE Release 3.0. For more information on Cisco secure ACS, Release 5.8 Patch 4 and TLS 1.2 compatibility, see TLS 1.2 Settings in the *Cisco secure ACS, Release 5.8 Release Notes*.

Note SID values of AD groups is not migrated from Cisco Secure ACS, Release 5.x to Cisco ISE Release, 2.0 or later as a part of Migration Tool process. Only External Group Names will be migrated. Once Migration process is done, we need to Join AD in Cisco ISE and update Group SID by clicking **Update SID values** button available in AD Groups tab. Authorization Rule won't match If Policy conditions created AD external Groups until the AD group SID is updated manually

System Requirements

Table 1: System Requirements for the Migration Tool

Operating System	The migration tool runs on Windows and Linux machines. The machine should have Java version 1.8 or later, installed on it.
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 for storing the migrated data and generating 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.

Table 2: System Requirements for Source and Target Migration Machines

Platform	Requirements
Cisco Secure ACS, Release 5.5 or later	Ensure that you have configured the Cisco Secure ACS source machine to have a single IP address.
Cisco ISE, Release 3.0	Ensure that the Cisco ISE target machine has at least 2 GB of RAM.
Migration machine—Ensure that the migration machine has a minimum of 2 GB of RAM.	

Platform	Requirements
64-Bit Windows and Linux	Install Java JRE, version 1.8 or higher 64 Bit. The migration tool will not run if you do not install Java JRE on the migration machines.
32-Bit Windows and Linux	Install Java JRE, version 1.8 or higher 32 Bit. The migration tool will not run if you do not install Java JRE on the migration machines.

Migration Tool Enhancements

The migration tool provides options to migrate ACS 5.x supported objects. The migration tool lists the data objects based on the selected version.

The migration tool supports:

- Migration of RADIUS or TACACS based configurations—The migration tool allows you to choose the migration of objects specific to either RADIUS or TACACS. You can choose these options if your Cisco Secure ACS deployment includes only TACACS or RADIUS configurations.
  - RADIUS Configuration—Migrates all the configurations except TACACS specific configuration such as shell profile, command sets, and access services (Device admin).
  - TACACS Configuration—Migrates all the configurations except RADIUS specific configurations such as authorization profile and access services (network access).

Note Regardless of the selected TACACS or RADIUS migration option, the migration tool migrates some TACACS and RADIUS objects to Cisco ISE.

When migration is performed in the existing Cisco ISE installation or from different deployment of Cisco Secure ACS to the same Cisco ISE server,

- The object is created if the object with same name does not exist in Cisco ISE.
- The migration tool displays a warning message "object already exists/resource already exists" with the details of the object name if the data object with same name exists in Cisco ISE.
- Protocol settings are updated if the network device with the same name exists in Cisco ISE in case of TACACS or RADIUS based migration.

- Selective object migration—The migration tool allows you to select the high-level configuration components such as predefined reference data, global operations, dictionaries, external servers, users and identity stores, devices, policy elements, and access policies, to be migrated from Cisco Secure ACS, Release 5.5 or later to Cisco ISE 3.0. It is recommended to refer the object level dependency list before performing selective object migration. Based on your requirement, you can migrate all the supported configuration components or select some of the high-level configuration components from the list of configuration components. This selective object migration can be performed based on the export and policy gap analysis reports.

Note You must select all the objects from the migrated objects list for the migration of access policies to be successful.

- Special characters in object names—If the name of the data objects in Cisco Secure ACS contains any special characters, which are not supported by Cisco ISE, the migration tool converts the unsupported special characters to underscore (_) and migrates the data objects to Cisco ISE. The auto-converted data objects are displayed as warnings in the export report. However, if LDAP and AD attributes, RSA, RSA realm prompts, internal user, and all predefined reference data contain Cisco ISE unsupported special characters, the export process fails.
- Migration of network devices with IP address ranges in all the octets—The migration tools enables migration of network devices configured with IP address ranges in all the octets. The migration reports the overlapping of IP address ranges in all the octets.
- Migration of policy rules with compound condition—The migration tool allows migration of authentication and authorization (standard and exception) rules with compound conditions having AND and OR operators.
- Migration of date and time conditions—The migration tool performs the migration of date and time conditions by dividing the data object into multiple data objects, if the days and time grid in ACS is configured with different days and timings.
- Enhanced help—In the migration tool UI, you can navigate to **Help > Migration Tool Usage** to view the details of the options available in the migration tool.