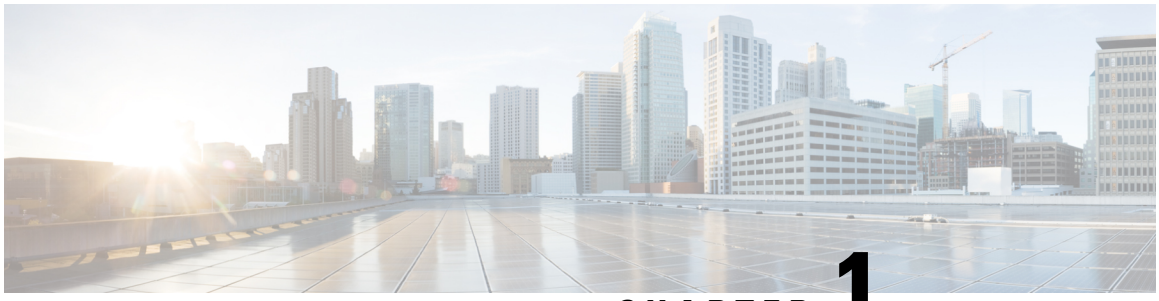
User Guide for Cisco Secure ACS to Cisco ISE Migration Tool, Release 2.2

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

CONTENTS



CHAPTER 1

Getting Started

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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), Release 5.5 or later to Cisco Identity Services Engine (ISE), Release 2.2 .

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

Before you migrate the existing Cisco Secure ACS, Release 5.5 or later data to Cisco ISE, Release 2.2, 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 2.2 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.

Supported Data Migration Paths

Table 1: Cisco Secure ACS Releases to Cisco ISE Release Supported Migration

Cisco ISE	Cisco Secure ACS 3.x, 4.x, and 5.0	Cisco Secure ACS 5.1	Cisco Secure ACS 5.2	Cisco Secure ACS 5.3	Cisco Secure ACS 5.5	Cisco Secure ACS 5.6 or above
1.3	Not Supported	Not Supported	Not Supported	Not Supported	Supported	Supported
1.4	Not Supported	Not Supported	Not Supported	Not Supported	Supported	Supported
2.0	Not Supported	Not Supported	Not Supported	Not Supported	Supported	Supported
2.1	Not Supported	Not Supported	Not Supported	Not Supported	Supported	Supported
2.2	Not Supported	Not Supported	Not Supported	Not Supported	Supported	Supported

Cisco ISE	Cisco Secure ACS 3.x, 4.x, and 5.0	Cisco Secure ACS 5.1	Cisco Secure ACS 5.2	Cisco Secure ACS 5.3	Cisco Secure ACS 5.5	Cisco Secure ACS 5.6 or above
2.3	Supported (Only Cisco Secure ACS 4.2)	Not Supported	Not Supported	Not Supported	Supported	Supported
2.4	Supported (Only Cisco Secure ACS 4.2)	Not Supported	Not Supported	Not Supported	Supported	Supported

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 2.2. 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 2.2.

- 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 2.2 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 2.2, see Migrate from Earlier Releases of Cisco Secure ACS to Cisco ISE, on page 23.

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 2: System Requirements for the Migration Tool

Operating System	The migration tool runs on Windows and Linux machines. The machine should have Java version 1.7 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 3: 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 2.2	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.	
64-Bit Windows and Linux	Install Java JRE, version 1.7 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 1.7 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 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).

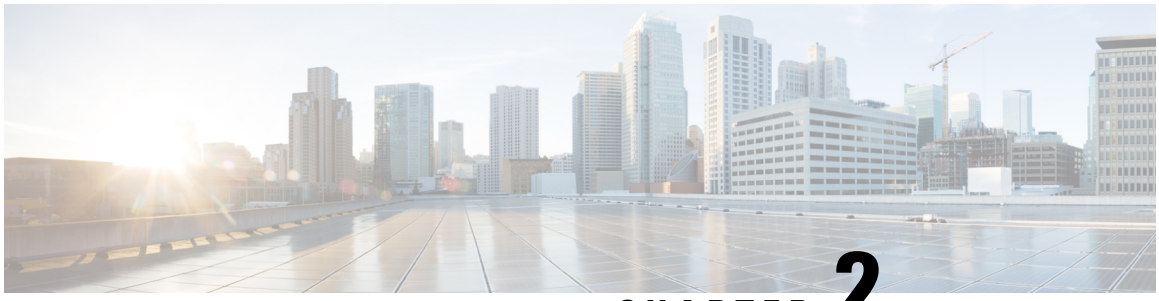
- TACACS Configuration—Migrates all the configurations except RADIUS specific configurations such as authorization profile and access services (network access).

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 . 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.
- 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 the last octet—The migration tools enables migration of network devices configured with IP address ranges in last octet .
- 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.



CHAPTER 2

Install the Migration Tool

This chapter provides guidelines on how to install the Cisco Secure ACS to Cisco ISE Migration Tool.

Migration Tool Installation Guidelines

- Ensure that your environment is ready for migration. In addition to a Cisco Secure ACS, Release 5.5 and above Windows or Linux source machine, you must deploy a secure external system with a database for dual-appliance (migrating data in a distributed deployment) migration.
- Ensure that you have configured the Cisco Secure ACS, Release 5.5 and above 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 configuration data if the migration from Cisco Secure ACS to Cisco ISE is performed on the same appliance.
- Ensure that you have completed these tasks:
  - If this is a dual-appliance migration, you have installed the Cisco ISE, Release 2.2 software on the target machine.
  - If this is a single-appliance migration, you have the Cisco ISE, Release 2.2 software available to re-image the appliance or virtual machine.
  - Have all the appropriate Cisco Secure ACS, Release 5.5 and above and Cisco ISE, Release 2.2 credentials and passwords.
- Ensure that you can establish network connections between the source machine and the secure external system.

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, Release 5.5 and above and Cisco ISE, Release 2.2 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 an audit log.

You must enter the hostname of the primary Cisco Secure ACS server and the Cisco ISE server, along with the administrator credentials. After you have been authenticated, the migration tool proceeds to migrate the full set of configured data items in a form similar to an upgrade. Make sure that you have enabled the PI interface on the ACS server and the ACS migration interface on the ISE server before running the migration tool.

Download Migration Tool Files

Before you begin

- Set the initial amount of memory allocated for the java Heap Sizes for the migration process in the config bat file. The attributes to set the heap size in config.bat are: _Xms = 64 (memory = 64 megabytes) and _Xmx = 1024 (memory = 1024 megabytes).

Step 1 Go to the Download Software web page. You may need to provide login credentials.

You can also view the download link for the migration tool in the **Prepare** section in the Cisco ISE GUI by navigating to the **Work Centers > Device Administration > Overview** page.

Step 2 Choose **Products > Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software.**

Step 3 In the left pane, choose the version.
The Download Software page displays the list of software available for the selected version.

Step 4 Click **Download** corresponding to the migration tool software package to download the ACS-MigrationApplication-2.2.zip file.

Step 5 Extract the contents of the .zip file. The extracted contents of the .zip file creates a directory structure that holds the config.bat and migration.bat files.

Step 6 Edit the **config.bat** file to set the initial amount of memory allocated for the java Heap Sizes.

Step 7 Click **Save**.

Initialize the Migration Tool

Before you begin

When the migration tool is initialized, it pops up a message box providing you the option to migrate configuration of all the supported objects or RADIUS configurations such as authentication profile, access services of type network access and others or TACACS configurations such as command sets, shell profile, access services of type device admin and others. The tool supplies a list of unsupported (or partially supported) objects that it cannot migrate, and the object-level dependencies list. You can also view the list of unsupported objects by selecting **Help > Unsupported Object Details & Object-level dependencies list** from the Cisco Secure ACS to Cisco ISE Migration Tool interface.

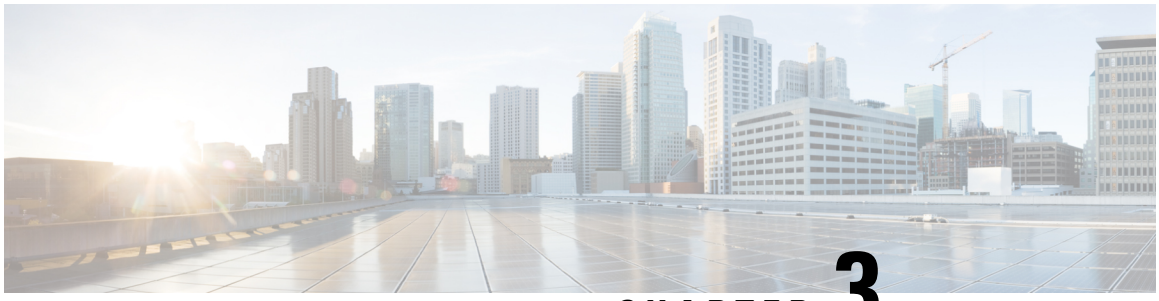
Note Migration can be performed on a fresh Cisco ISE setup or an existing Cisco ISE setup. If the object already exists in Cisco ISE, you will receive a warning message and the objects will be skipped for migration, or else, the object will be created in Cisco ISE.

Step 1 Click **migration.bat** batch file to launch the migration tool.
The Migration selection options window appears.

Step 2 From the list of migration options, click the radio button corresponding to the migration option that you want to choose.

- Configuration of all supported objects—Displays all the supported objects.
- RADIUS configurations such as authentication profile, access services of type network access and others—Displays only the RADIUS related objects and the common objects.
- TACACS configurations such as command sets, shell profile, access services of type device admin and others—Displays only TACACS related objects and the common objects.

Step 3 In the pop-up window, click **Yes** to display the list of unsupported and partially supported objects and object-level migration dependencies.



CHAPTER 3

Plan Your Migration

This chapter provides necessary information to plan your migration. Planning your migration carefully can ensure that your migration proceeds smoothly and it decreases any risk of migration failure.

Prerequisites

This section provides information on the prerequisites to perform the migration process.

Enable the Migration Interfaces

Before you can begin the migration process, you must enable the interfaces used for the data migration on the Cisco Secure ACS and Cisco ISE servers. It is recommended to disable the migration interfaces on both the servers after the migration process is completed.

Step 1 Enable the migration interface on the Cisco Secure ACS machine by entering the following command in the Cisco Secure ACS CLI:

acs config-web-interface migration enable

Step 2 Enable the migration interface on the Cisco ISE server:

a) In the Cisco ISE CLI, enter **application configure ise**.
b) Enter **11** to enable/disable ACS Migration.
c) Enter **Y**.

Note Disable the migration interface on the Cisco Secure ACS machine using the following command: **acs config-web-interface migration disable**, after the migration process is completed.

Note Disable the migration interface on the Cisco ISE server after the migration process is completed.

Enable Trusted Certificates in the Migration Tool

Before you begin

To enable the export of data from the Cisco Secure ACS server to the migration tool , you can either trust the Cisco Secure ACS CA certificate or the Cisco Secure ACS management certificate.

To enable the import of data from the migration tool to the Cisco ISE server, you can either trust the Cisco ISE CA certificate or the Cisco ISE management certificate.

To enable the trusted certificates in the migration tool:

- In Cisco Secure ACS, ensure that the server certificate is in the **System Administration** > **Configuration** > **Local Server Certificates** > **Local Certificates** page. The Common Name (CN attribute in the Subject field) or DNS Name (in the Subject Alternative Name field) in the certificate is used in the ACS5 Credentials dialog box to establish the connection and export data from Cisco Secure ACS.
- In Cisco ISE, ensure that the server certificate is in the **Administration** > **System** > **Certificates** > **Certificate Management** > **System Certificates** page. The Common Name (CN attribute in the Subject field) or DNS Name (in the Subject Alternative Name field) is used in the ISE Credentials dialog box to establish the connection and import data from the migration tool to Cisco ISE.

Step 1 In the Cisco Secure ACS to Cisco ISE Migration Tool window, choose **Settings** > **Trusted Certificates** > **Add** to include the Cisco Secure ACS and Cisco ISE certificates to enable trusted communication.

You can view or delete the certificate in the migration tool.

Step 2 In the **Open** dialog box, choose the folder containing the trusted root certificate and click **Open** to add the selected Cisco ISE certificate to the migration tool.

Step 3 Repeat the previous step to add the Cisco Secure ACS certificate.

Note Ensure that the Cisco Secure ACS and Cisco ISE hostnames are resolvable to IP addresses.

Data Migration Time Estimate

The migration tool may run for approximately 5 hours to migrate the following configurations:

- 10,000 internal users
- 4 identity groups
- 16,000 network devices
- 512 network device groups

- 2 authorization profiles (with or without policy sets)
- 1 command set
- 42 shell profiles
- 9 access services (with 25 authorization rules)

Preparation for Migration from Cisco Secure ACS, Release 5.5 or later

We recommend that you do not change to Simple mode after a successful migration from Cisco Secure ACS. Because, you might lose all the migrated policies in Cisco ISE. You cannot retrieve those migrated polices, but you can switch to Policy Set mode from Simple mode.

You must consider the following before you start migrating Cisco Secure ACS data to Cisco ISE:

- Migrate Cisco Secure ACS, Release 5.5 or above data only in the Policy Set mode in Cisco ISE, Release 2.2.
- Generate one policy set per enabled rule in the Service Selection Policy (SSP) and order them according to the order of the SSP rules.

Note The service that is the result of the SSP default rule becomes the default policy set in Cisco ISE, Release 2.2. For all the policy sets created in the migration process, the first matching policy set is the matching type.

Policy Services Migration Guidelines

Note the following points while migrating the policy services from Cisco Secure ACS to Cisco ISE:

- If the Service Selection Policies (SSP) contain SSP rules that are disabled or monitored in Cisco Secure ACS, Release 5.5 or above, they are not migrated to Cisco ISE.
- When the Service Selection Policy (SSP) contains a SSP rule that is enabled in Cisco Secure ACS, Release 5.5 or above:
  - Requests a service, which contains a Group Mapping policy, it is not migrated to Cisco ISE. Cisco ISE does not support Group Mapping Policy.

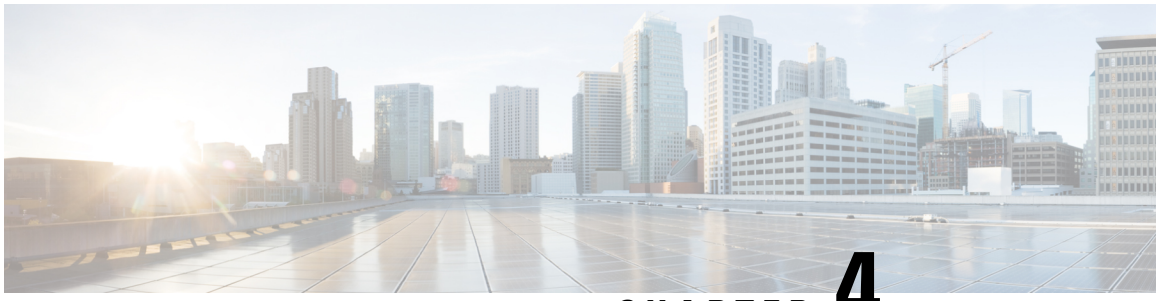
    If a particular access service contains group mapping, the migration tool displays it as a warning in the policy gap analysis report and migrates the authorization rules related to that access service.
  - Requests a service and its identity policy contains rules, which result in RADIUS Identity Server, it is not migrated to Cisco ISE (Cisco ISE differs to use RADIUS Identity Servers for authentication).
  - Requests a service, which has policies that use attributes or policy elements that are not supported by Cisco ISE, it is not migrated to Cisco ISE.

Cisco Secure ACS Policy Rules Migration Guidelines

When rules cannot be migrated, the policy model as a whole cannot be migrated due to security aspects as well as data integrity. You can view details of problematic rules in the Policy Gap Analysis Report. If you do not modify or delete an unsupported rule, the policy is not migrated to Cisco ISE.

In general, you must consider these rules while migrating data from Cisco Secure ACS, Release 5.5 or above to Cisco ISE, Release 2.2:

- Attributes (RADIUS, VSA, identity, and host) of type enum are migrated as integers with allowed values.
- All endpoint attributes (irrespective of the attribute data type) are migrated as String data types.



CHAPTER 4

Migrate Data from Cisco Secure ACS to Cisco ISE

This chapter describes exporting and importing Cisco Secure ACS, Release 5.5 or later data to Cisco ISE, Release 2.2 using the migration tool.

Export Data from Cisco Secure ACS

After starting the migration tool, complete the following steps to export data from Cisco Secure ACS to the migration tool.

Step 1 In the Cisco Secure ACS to Cisco ISE Migration Tool window, click **Settings** to display the list of data objects available for migration.

Step 2 (Optional) You are not required to configure the dependency handling in order to perform migration. Check the check boxes of the data objects you want to export in case their dependency data is missed and click **Save**.

Step 3 In the Cisco Secure ACS to Cisco ISE Migration Tool window, click **Migration** and then click **Export From ACS**.

Step 4 Enter the Cisco Secure ACS host name, user name, and password and click **Connect** in the ACS5 Credentials window.

You can monitor the migration process in the Cisco Secure ACS to Cisco ISE Migration Tool window, which displays the current count of successful object exports and lists any objects that triggered warnings or errors.

To get more information about a warning or an error that occurred during the export process, click any underlined numbers in the Warnings or Errors column in the **Migration** tab. The Object Errors and Warnings Details window displays the result of a warning or an error during export. It provides the object group, the type, and the date and time of a warning or an error.

Step 5 Scroll to display the details of the selected object error, and then click **Close**.

Step 6 When the data export process is completed, the Cisco Secure ACS to Cisco ISE Migration Tool window displays the status of export that Exporting finished.

Step 7 Click **Export Report(s)** to view the contents of the export report.

Step 8 To analyze the policy gap between Cisco Secure ACS and Cisco ISE, click **Policy Gap Analysis Report**.

Note The migration tool maintains a cache for the exported objects and retrieves them for subsequent exports.

Password Compliance during Export

The migration tool adheres to password compliance during the export process.

- **Password Complexity**

  Following is the list of error messages that might occur during the export process if the password of the user does not meet the password complexity requirements:

  user: Failed to Export because its password does not match with the password Complexity

  Password length should be minimum of '5' characters.

  Password should not contain 'cisco' or its characters in reverse.

  Password should not contain 'hello' or its characters in reverse.

  Password should not contain repeated characters four or more times consecutively.

  Password should contain at least one Lower case character.

  Password should contain at least one Upper case character.

  Password should contain at least one Numeric Character.

  Password should contain at least one non alphanumeric characters.

- **Password hash**

  If you enable password hash for internal user in Cisco Secure ACS and try to export the internal user, the migration tool displays the following error message:

  user: Failed to Export because its configured with Password Hash which is not supported by ISE, disable this configuration in ACS and export again.

Import Data in to Cisco ISE

Step 1 In the Cisco Secure ACS to Cisco ISE Migration Tool window, click **Import To ISE**.

Step 2 Click **OK** when you are prompted to add attributes to the LDAP identity stores before they are imported into Cisco ISE.

Step 3 From the **LDAP Identity Store** drop-down list, choose the identity store to which you want to add attributes, and click **Add Attribute**.

Step 4 Enter a name in the **Attribute Name** field, choose an attribute type from the **Attribute Type** drop-down list, enter a value in the **Default Value** field, and click **Save & Exit**.

Step 5 After adding attributes, click **Import To ISE**, enter the Cisco ISE Fully Qualified Domain Name (FQDN), username, and password in the ISE Credentials window and click **Connect**.

Step 6 When the data import process is completed, the Cisco Secure ACS to Cisco ISE Migration Tool window displays the status of import as **Importing finished**.

Step 7 To view a complete report on the imported data, click **Import Report(s)**.

Step 8 To get more information about a warning or an error that occurred during the import process, click any underlined numbers in the Warnings or Errors column in the **Migrations** tab.

Step 9 To analyze the policy gap between Cisco Secure ACS and Cisco ISE, click **Policy Gap Analysis Report**.

Step 10 Click **View Log Console** to display the real-time view of the export or import operations.

Migrated Data Verification in Cisco ISE

To verify that the Cisco Secure ACS 5.5 or above data is migrated into Cisco ISE , log into the Cisco ISE and check that the various Cisco Secure ACS objects can be viewed.

Resume a Failed Data Migration

The migration tool maintains a checkpoint at each stage of the import or export operation. This means that if the process of importing or exporting fails, you do not have to restart the process from the beginning. You can start from the last checkpoint before the failure occurred.

If the migration process fails, the migration tool terminates the process. When you restart the migration tool after a failure, a dialog box is displayed that allows you to 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 checkpoint. Resuming from a failure also resumes the report to run from the previous process.

Migrate Data from a Single Cisco Secure ACS Appliance

Before you begin

When you are ready to start migrating Cisco Secure ACS, Release 5.5 or above data to a Cisco ISE, Release 2.2, ensure that it is to a standalone Cisco ISE node. After the migration is successfully completed, you can begin any deployment configuration (such as setting up Administrator ISE and Policy Service ISE personas).

It is a requirement that the migration import phase be performed on a “clean” new installation of the Cisco ISE software on a supported hardware appliance. For a list of supported hardware appliances, refer to the *Cisco Identity Services Engine Hardware Installation Guide, Release 2.2*.

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 migration tool against the Cisco Secure ACS appliance.

You can use the migration tool and the following migration procedure in cases where Cisco Secure ACS and Cisco ISE use the same hardware; the CSACS-1121 appliance:

Step 1 Install the migration tool on a standalone Windows or Linux machine.

Step 2 Export the Cisco Secure ACS, Release 5.5 or above data from the Cisco Secure ACS-1121 hardware appliance to a secure external server with a database.

Step 3 Back up the Cisco Secure ACS data.

Step 4 Re-image the Cisco Secure ACS-1121 hardware appliance, which has the same physical hardware as any of the supported Cisco ISE appliances, with Cisco ISE, Release 2.2, software.

Step 5 Import the converted Cisco Secure ACS data from the secure external server into Cisco ISE.

Migrate Data from a Distributed Environment

Before you begin

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

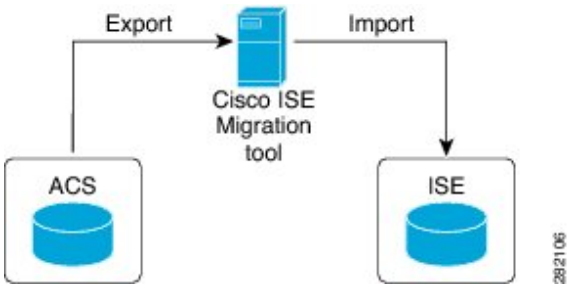
In a distributed environment, there is one primary Cisco Secure ACS appliance and one or more secondary Cisco Secure ACS appliances that interoperate with the primary appliance.

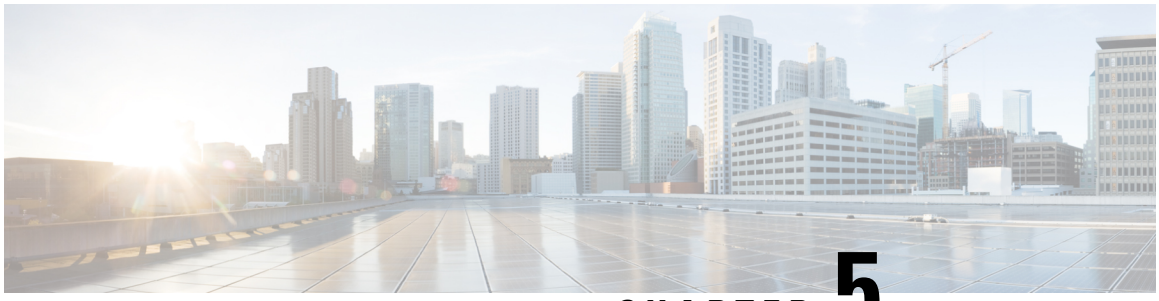
If you are running Cisco Secure ACS in a distributed environment, you must:

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

Step 2 Run the migration tool against the primary Cisco Secure ACS appliance.

Figure 1: Cisco Secure ACS and Cisco ISE Installed on Different Appliances





CHAPTER 5

Reports

The migration tool generates reports for export, import, and policy gap analysis during data migration. You can find the following files in the Reports folder of the migration tool directory:

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

Export Report

This report indicates specific information or errors that are encountered during the export of data from the Cisco Secure ACS database. It contains a data analysis section at the end of the report, which describes the functional gap between Cisco Secure ACS and Cisco ISE. The export report also includes error information for exported objects that will not be imported.

Table 4: Cisco Secure ACS to Cisco ISE Migration Tool Export Report

Report Type	Message Type	Message Description
Export	Success	Lists the names of the data objects that were exported successfully.
	Information	Lists the data objects that are not exported as they are predefined in Cisco ISE.
	Warning	Lists the data objects that were exported but might require some additional configuration in Cisco ISE after migration. Lists the data objects for which the naming conversion is done by the migration tool.
	Error	Lists the data objects that are not exported due to limitation in the configured name or attribute type that is not supported in Cisco ISE. Lists the data objects that are not exported as they are not supported in Cisco ISE.

Policy Gap Analysis Report

This reports lists specific information related to the policy gap between Cisco Secure ACS and Cisco ISE, and is available after completion of the export process by clicking the Policy Gap Analysis Report button in the migration tool user interface.

During the export phase, the migration tool identifies the gaps in the authentication and authorization policies. If any policy is not migrated, it is listed in the Policy Gap Analysis report. The report lists all the incompatible rules and conditions that are related to policies. It describes data that cannot be migrated and the reason with a manual workaround.

Some conditions can be automatically migrated by using the appropriate Cisco ISE terminology, for example, a condition named Device Type In is migrated as Device Type Equals. If a condition is supported or can be automatically translated, it does not appear in the report. If a condition is found as “Not Supported” or “Partially supported,” the policy is not imported and the conditions appear in the report. It is the responsibility of the administrator who is performing the migration to modify or delete such conditions. If they are not modified or deleted, policies are not migrated to Cisco ISE.

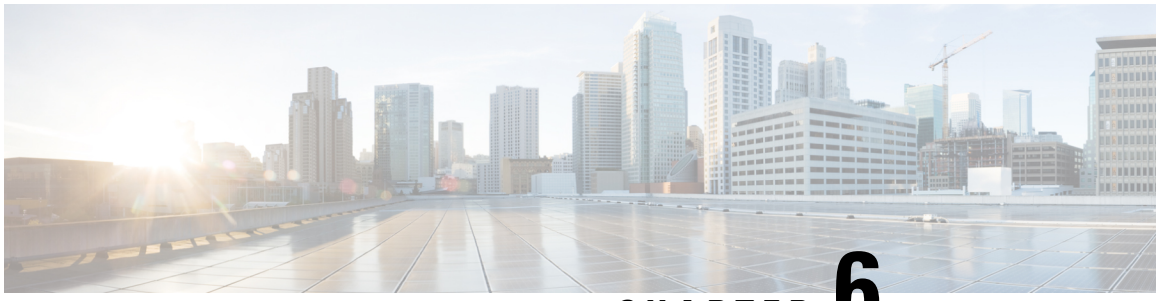
Note After exporting the data, you should analyze the export report and the policy gap report, fix the listed errors in the ACS configuration and address the warnings and other issues. After addressing the errors or warnings, perform the export process again. For information on exporting data from Cisco Secure ACS, see Export Data from Cisco Secure ACS, on page 15.

Import Report

This report indicates specific information or errors that are encountered during the import of data into the Cisco ISE appliance.

Table 5: Cisco Secure ACS to Cisco ISE Migration Tool Import Report

Report Type	Message Type	Message Description
Import	Information	Lists the names of the data objects that were imported successfully.
	Warning	Lists the data objects that were imported but might require some additional configuration in Cisco ISE after migration. Lists the data objects that already exist in Cisco ISE if migration is performed on existing Cisco ISE installation.
	Error	Data objects are not imported due to the following reason: • Some unexpected errors occurred while importing the data objects to Cisco ISE



CHAPTER 6

Migrate from Earlier Releases of Cisco Secure ACS to Cisco ISE

This chapter provides detailed information on migrating data from earlier releases of Cisco Secure ACS to Cisco ISE.

Migrate from Earlier Releases of Cisco Secure ACS to Cisco ISE

You can migrate earlier releases of Cisco Secure ACS data to Cisco Secure ACS, Release 5.5 or above, so that it can be migrated to Cisco ISE, Release 2.2, using the migration tool.

Migrate from Cisco Secure ACS, Release 3.x

If you are running Cisco Secure ACS, Release 3.x in your environment, upgrade to a migration-supported version of Cisco Secure ACS, Release 4.x, and then upgrade to Cisco Secure ACS, Release 5.5 or above .

Step 1 Check the upgrade path for Cisco Secure ACS, Release 3.x, as described in the Installation Guide for Cisco Secure ACS Solution Engine 4.1 or Installation Guide for Cisco Secure ACS Solution Engine 4.2.

Step 2 Upgrade your Cisco Secure ACS, Release 3.x server to a migration-supported version of the Cisco Secure ACS, Release 4.x. For example, upgrade to one of the following Cisco Secure ACS 4.1.1.24 , Cisco Secure ACS 4.1.4, Cisco Secure ACS 4.2.0.124, or Cisco Secure ACS 4.2.1 releases.

Step 3 After the upgrade, follow the steps that describe migrating from Cisco Secure ACS, Release 4.x to Cisco Secure ACS, Release 5.5 or above .

Migrate from Cisco Secure ACS, Release 4.x

If you are not running one of the migration-supported versions of Cisco Secure ACS, Release 4.x in your environment, upgrade to a point where you can migrate from Cisco Secure ACS, Release 4.x to Cisco Secure ACS, Release 5.5 or above.

Step 1 Upgrade Cisco Secure ACS, Release 4.x version to a migration-supported version, if your Cisco Secure ACS, Release 4.x server currently does not run one of the migration-supported versions.

Step 2 Install the same migration-supported version of Cisco Secure ACS on the migration machine, which is a Windows server.

Step 3 Back up the Cisco Secure ACS, Release 4.x data and restore it on the migration machine.

Step 4 Place the Migration utility on the migration machine. You can get the Migration utility from the Installation and Recovery DVD.

Step 5 Run the Analyze and Export phase of the Migration utility on the migration machine.

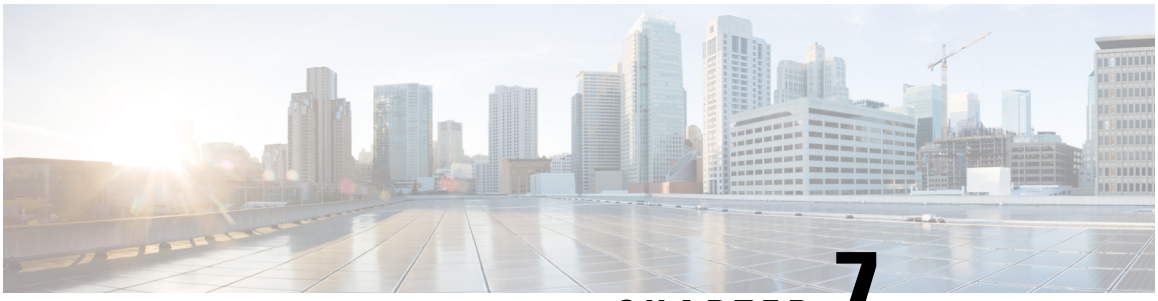
Step 6 Resolve any issues in the Analyze and Export phase.

Step 7 Run the Import phase of the Migration utility on the migration machine, and during this phase, the Migration utility imports data into the Cisco Secure ACS, Release 5.5 or above server.

Migrate from Cisco Secure ACS, Release 5.x

If you are running Cisco Secure ACS, Release 5.x in your environment, you must upgrade to Cisco Secure ACS, Release 5.5 or above.

To migrate internal users from Cisco Secure ACS 5.x to Cisco ISE, you must install Cisco Secure ACS 5.5 Patch 4 or later, ACS 5.6, ACS 5.7 Patch 1 or later, or ACS 5.8, and then start the migration.



CHAPTER 7

Policy Elements

This chapter provides information about the policy elements in Cisco ISE and Cisco Secure ACS.

Cisco ISE and Cisco Secure ACS Parity

Cisco ISE introduces the following features to achieve parity with Cisco Secure ACS.

- Disable user account if the configured date exceeds a specific period for individual users
- Disable user account if the configured date exceeds a specific period for all the users globally
- Disable user accounts after n days of configuration globally
- Disable user accounts after n days of inactivity
- Support for IP address range in the last octet for the network device
- MAR configuration in Active Directory
- Dial-in attribute support
- Enable password change for LDAP
- Configuration of primary and backup LDAP server for each PSN
- Configuration of RADIUS ports
- Authorization profile configured with dynamic attribute
- Two new values for the service-type RADIUS attribute
- Increased internal user support for 300,000 users
- Authenticate internal users against external identity store password
- Dictionary check for passwords of admin user and internal user
- Crytobinding TLV attribute support for allowed protocols

- Use of length included flag while performing EAP-TLS authentication against a Terminal Wireless Local Area Network Unit (TWLU) client
- Common Name and Distinguished Name support for Group Name attribute for LDAP Identity Store

Cisco ISE and Cisco Secure ACS Parity

Cisco ISE introduces the following features to achieve parity with Cisco Secure ACS.

- Disable user account if the configured date exceeds a specific period for individual users
- Disable user account if the configured date exceeds a specific period for all the users globally
- Disable user accounts after n days of configuration globally
- Disable user accounts after n days of inactivity
- Support for IP address range in the last octet for the network device
- MAR configuration in Active Directory
- Dial-in attribute support
- Enable password change for LDAP
- Configuration of primary and backup LDAP server for each PSN
- Configuration of RADIUS ports
- Authorization profile configured with dynamic attribute
- Two new values for the service-type RADIUS attribute
- Increased internal user support for 300,000 users
- Authenticate internal users against external identity store password
- Dictionary check for passwords of admin user and internal user
- Crytobinding TLV attribute support for allowed protocols
- Use of length included flag while performing EAP-TLS authentication against a Terminal Wireless Local Area Network Unit (TWLU) client
- Common Name and Distinguished Name support for Group Name attribute for LDAP Identity Store

Policy Models

Cisco Secure ACS and Cisco ISE have both simple and rule-based authentication paradigms, but Cisco Secure ACS and Cisco ISE are based on different policy models, which makes migrating policies from Cisco Secure ACS 5.5 or above to Cisco ISE a bit complex.

Cisco Secure ACS policy hierarchy starts with the Service selection rule that redirects the authentication requests to the access services. The access services consist of identity and authorization policies that authenticate the user against internal or external identity stores and authorize the users based on the conditions defined.

Authentication and authorization polices are migrated from Cisco Secure ACS, Release 5.5 or above to Cisco ISE, Release 2.2. Cisco ISE supports the Policy Set, which is similar to the Service Selection Policy (SSP) in Cisco Secure ACS.

Cisco Secure ACS Service Selection Policy and Cisco ISE Policy Set

Cisco Secure ACS Service Selection Policy (SSP) distributes requests to the appropriate services based on SSP rules whereas Cisco ISE policy set holds a rule, which contains entry criteria to the policy set. The order of the policy set is in the same order as the entry rules, which is similar to the order of the SSP rules.

Several SSP rules may request the same service or reuse of service in Cisco Secure ACS. However, each policy set carries its own entry condition, therefore, you cannot reuse the policy set in Cisco ISE. If you want to migrate a single service that is requested by several SSP rules, you must create multiple policy sets that are copies of that service, which means that you must create a policy set in Cisco ISE for each SSP rule that requests the same service in Cisco Secure ACS.

You can define SSP rules as disabled or monitored in Cisco Secure ACS, and the equivalent entry rules of a policy set are always enabled in Cisco ISE. If SSP rules are disabled or monitored in Cisco Secure ACS, the policy services that are requested by SSP rules cannot be migrated to Cisco ISE.

Cisco Secure ACS Policy Access Service and Cisco ISE Policy Set

You can define a policy service without requesting that service, which means that you can define a policy service inactive by a rule in the SSP in Cisco Secure ACS. Cisco Secure ACS, Release 5.5 or above has an out-of-the-box DenyAccess service, which has neither policies nor allowed protocols for the default SSP rule in Cisco Secure ACS, which automatically denies all requests. There is no equivalent policy set for Cisco ISE. But, you cannot have a policy set without an entry rule, which refers to the policy set in Cisco ISE.

Allowed protocols are attached to the entire service (not a specific policy) that is not conditioned (except the condition in the SSP that points to the entire service) in Cisco Secure ACS, Release 5.5 or above. Allowed protocols refers only to the authentication policies as a result of a conditioned outer rule in Cisco ISE.

Identity policy is a flat list of rules that results in identity source (identity source and identity store sequence) in Cisco Secure ACS, Release 5.5 or above.

Both Cisco Secure ACS, Release 5.5 or above and Cisco ISE, Release 2.2, include an optional exception policy attached to each authorization policy. Cisco ISE, Release 2.2 provides an optional Global Exception Policy in addition to the exception policy that affects all authorization policies. There is no equivalent policy to that of Global Exception Policy in Cisco Secure ACS, Release 5.5 or above. The local exception policy is processed first followed by the Global Exception Policy and authorization policy for authorization.

FIPS Support for ISE 802.1X Services

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

To support Federal Information Processing Standard (FIPS), the migration tool migrates the default network device keywrap data.

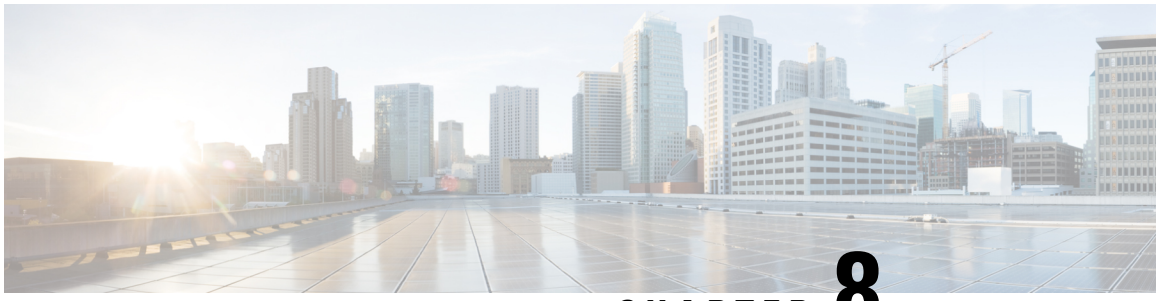
FIPS-compliant and supported protocols:

- Process Host Lookup
- Extensible Authentication Protocol-Translation Layer Security (EAP-TLS)

- Protected Extensible Authentication Protocol (PEAP)
- EAP-Flexible Authentication via Secure Tunneling (FAST)

FIPS-noncompliant and unsupported protocols:

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



CHAPTER 8

Troubleshoot the Migration Tool

Unable to Start the Migration Tool

Condition

Unable to start the migration tool.

Action

Verify that Java JRE, Version 1.7 or later, is installed on the migration machine and that it is correctly configured in the system path and classpath.

Troubleshoot Connection Issues in the Migration Tool

If the migration tool fails to connect to Cisco Secure ACS or ISE, check the migration.log file to identify the problem.

Error Message

The following error message is displayed if the Cisco Secure ACS or ISE host name is not resolvable: "UnknownHostException: hostname"

Action

- Ensure that the Cisco Secure ACS or ISE hostname is resolvable from the client machine where you run the migration tool.
- Check the DNS configuration and connectivity.

Error Message

The following error message is displayed if the Cisco Secure ACS or Cisco ISE hostname entered in the migration tool does not match the name in the certificate: "hostname in certificate didn't match: <hostname> != </hostname_in_certificate>"

Action

Ensure that the certificate's Common Name in the Subject field or DNS name in Subject Alternate Name field in Cisco Secure ACS and Cisco ISE matches the Hostname provided in the migration tool.

Error Message

The following error message is displayed if the Cisco Secure ACS and ISE certificates are not trusted by the migration tool: "SSLHandshakeException: unable to find valid certification path to requested target"

Action

Ensure that Cisco Secure ACS and Cisco ISE certificates are trusted by adding the required certificates in the **Settings** > **Trusted Certificates** page in the **Cisco Secure ACS to Cisco ISE Migration Tool**.

Error Messages Displayed in Logs

Connection Error

Condition

The following error message is displayed in the log: “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 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.

I/O Exception Error

Condition

The following error message is displayed in the log:

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

Action

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

Out of Memory Error

Condition

The following error message is displayed in the log:

"OutofMemory".

Action

Increase the Java heap size to at least 1 GB.

Default Folders, Files, and Reports are Not Created

Condition

The migration tool fails to create 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 the Cisco Secure ACS appliance before starting the migration process to free up memory space.

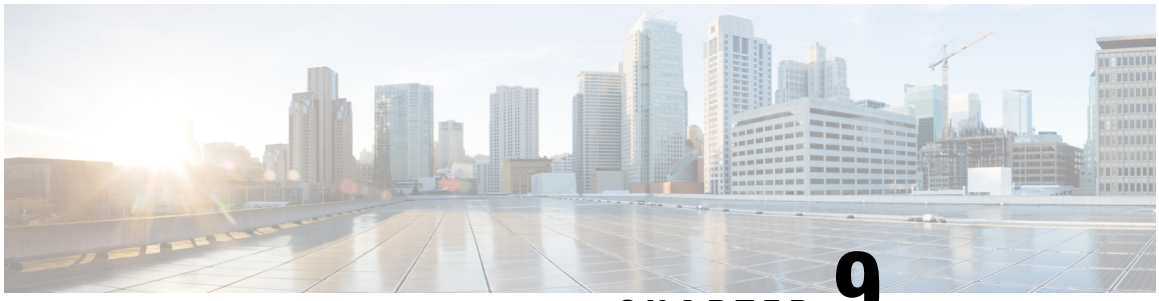
Report Issues to Cisco TAC

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 resolve the 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/cisco/web/support/index.html

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 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.
- Migration logfile (...migration/bin/migration.log).
- All the reports in the config folder (...migration/config).
- Cisco Secure ACS, Release 5.5 or above log files.
- Cisco Secure ACS, Release 5.5 or above build number.



CHAPTER 9

Frequently Asked Questions

Frequently Asked Questions

What happens if I do not migrate?

Cisco Secure ACS has announced EOL up to 5.7 release. Cisco upgrades Cisco ISE to achieve closer parity with Cisco Secure ACS in the future Cisco ISE releases. All the new development efforts are focused towards Cisco ISE. Cisco ISE will be the future platform for both TACACS+ and RADIUS. If you want to use a security product that supports advanced TACACS+ and RADIUS protocols, you must migrate to Cisco ISE.

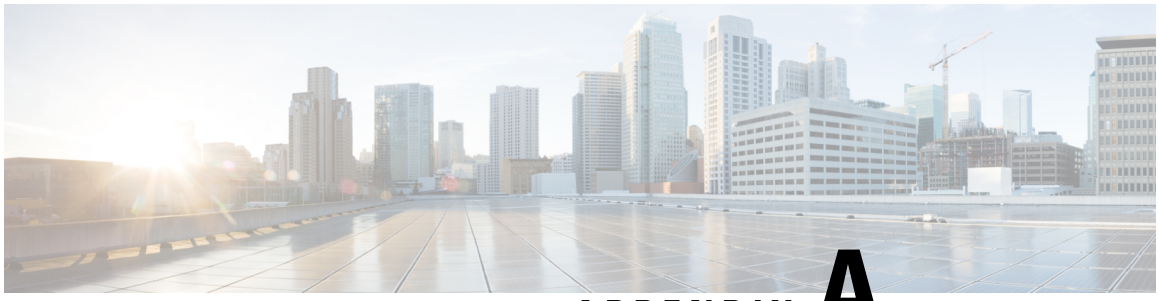
What is the support offered by Cisco during migration?

The migration tool user guide provides information on the migration process. You can also contact Advanced services and partners for performing the migration. If you face any issues during migration, you can reach out to the TAC team.

How does Cisco ISE provide security support during migration?

The Cisco Secure ACS to Cisco ISE migration tool uses a secure connection between Cisco ISE and Cisco Secure ACS and encrypts the data while storing the data after export and before being imported to Cisco ISE.

Frequently Asked Questions



APPENDIX A

Data Structure Mapping

This appendix provides information about the data objects that are migrated, partially migrated, and not migrated from Cisco Secure ACS, Release 5.5 or later to Cisco ISE, Release 2.2.

Data Structure Mapping

Data structure mapping is the process by which data objects are analyzed and validated in the migration tool during the export phase.

Migrated Data Objects

The following data objects are migrated from Cisco Secure ACS to Cisco ISE, :

- Network device group (NDG) types and hierarchies
- Network devices
- Default network device
- Network device ranges (in last octet) (partial support)
- External RADIUS servers
- External TACACS+ servers
- TACACS+ server sequence
- TACACS+ settings
- Stateless session resume capability settings
- Identity groups

- Internal users
- Internal users with enable password change
- Internal users with password type configured as external Identity store
- Disable user account if date exceeds
- Global option for disabling user account after n days of inactivity
- Internal endpoints (hosts)
- Lightweight Directory Access Protocol (LDAP)
- Common Name and Distinguished name for Group Name attribute in LDAP Identity Store
- Microsoft Active Directory (AD)
- RSA
- RADIUS token
- Certificate authentication profiles
- Date and time conditions (Partial support, see Unsupported Rule Elements)
- Network conditions (end station filters, device filters, device port filters)
- Maximum user sessions
- RADIUS attribute and vendor-specific attributes (VSA) values
- RADIUS vendor dictionaries
- Internal users attributes
- Internal endpoint attributes
- TACACS+ Profiles
- Downloadable access control lists (DACLs)
- Identity (authentication) policies
- Authentication, Authorization, and Authorization exception polices for TACACS+ (for policy objects)
- TACACS+ Command Sets
- Authorization exception policies (for network access)
- Service selection policies (for network access)
- RADIUS proxy service
- TACACS+ proxy service
- User password complexity
- Identity sequence and RSA prompts
- UTF-8 data
- EAP authentication protocol—PEAP-TLS

- User check attributes
- Dial-in attributes
- Crypto binding attributes
- Weak ciphers support for allowed protocols
- Identity sequence advanced option
- Additional attributes available in policy conditions—AuthenticationIdentityStore
- Additional string operators—Start with, Ends with, Contains, Not contains
- RADIUS identity server attributes
- Length included flag (L-bit) in EAP-MD5, EAP-TLS, LEAP, PEAP, and EAP-FAST authentication

Partially Migrated Data Objects

The following data objects are partially migrated from Cisco Secure ACS , Release 5.5 or above to Cisco ISE, Release 2.2:

- Host attributes that are of type IP address and Date are not migrated.
- RSA sdopts.rec file and secondary information are not migrated.
- Multi-Active Directory domain (only Active Directory domain joined to the primary) is migrated.
- LDAP configuration defined for primary ACS instance is migrated. Secondary ACS instance specific configurations are not migrated.

Data Objects Not Migrated

The following data objects are not migrated from Cisco Secure ACS to Cisco ISE:

- Monitoring reports
- Scheduled backups
- Repositories
- Administrators, roles, and administrators settings
- Customer/debug log configurations
- Deployment information (secondary nodes)
- Certificates (certificate authorities and local certificates)

  You must manually import your certificates because they are not migrated. For identity stores that use certificates, you must map the imported certificate to the ID store. If you were using identity source sequences, you must create new sequences that duplicate the originals.
- Trustsec related configuration

- Display RSA node missing secret
- Additional attribute available in a policy condition—NumberOfHoursSinceUserCreation
- Wildcards for hosts
- OCSP service
- Syslog messages over SSL/TCP
- Configurable copyright banner
- IP address exclusion

Unsupported Rule Elements

Cisco Secure ACS and Cisco ISE are based on different policy models, and there is a gap between pieces of Cisco Secure ACS data when it is migrated to Cisco ISE. When Cisco Secure ACS and Cisco ISE release versions change, not all Cisco Secure ACS policies and rules can be migrated due to:

- Unsupported attributes used by the policy
- Unsupported AND/OR condition structure (mainly, once complex conditions are configured)
- Unsupported operators

Table 6: Unsupported Rule Elements

Rule Elements	Status of Support	Description
Date and Time	Not Supported	Date and time conditions in an authorization policy that have a weekly recurrence setting, are not migrated to Cisco ISE. As a result, the rules are also not migrated. Date and time conditions in an authentication policy are not migrated to Cisco ISE. As a result, the rules are also not migrated.
Not In	Not Supported	The "Not In" operator is converted to NOT_STARTS_WITH.
Contains Any	Partially Supported	The "Contains Any" operator is converted to a compound condition with EQUALS & OR operators. Example: In ACS, **AD ExternalGrp Contains Any (A, B)** is converted to **(AD ExternalGrp Equals A) OR (AD ExternalGrp Equals B)** in Cisco ISE.

Rule Elements	Status of Support	Description
Contains All	Partially Supported	The "Contains All" operator is converted to a compound condition with EQUALS & AND operators. Example: In ACS **AD:ExternalGrp contains all A;B** is converted to **(AD ExternalGrp Equals A) AND (AD ExternalGrp Equals B)** in Cisco ISE.
Combination of logical expressions	Not Supported	Rules that use these operators in their conditions are not migrated: • Authentication policies that include compound conditions that have different logical expressions other than a || b || c || … and/or a && b && c && … such as (a || b) && c. • Authorization policies that include compound conditions that have different local expressions other than a && b && c && are not migrated as part of the rule condition. As a workaround, you can manually use library compound conditions for some advanced logical expressions.

Data Information Mapping

This section lists the data that is mapped during the export process. The tables include object categories from Cisco Secure ACS, Release 5.5 or above and its equivalent in Cisco ISE, Release 2.2. The data-mapping tables in this section list the status of valid or not valid data objects mapped when migrating data during the export stage of the migration process.

Network Device Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Migrates as is
Description	Migrates as is
Network device group	Migrates as is

Cisco Secure ACS Properties	Cisco ISE Properties
Single IP address	Migrates as is
Single IP and subnet address	Migrates as is
IP ranges	IP ranges in last octet without Exclude IP option, are migrated
Exclude IP address	Not Supported
TACACS information	Migrates as is
RADIUS shared secret	Migrates as is
TACACS+ shared secret	Migrates as is
CTS	Migrates as is
SNMP	SNMP data is available only in Cisco ISE; therefore, there is no SNMP information for migrated devices.
Model name	This property is available only in Cisco ISE (and its value is the default, which is “unknown”).
Software version	This property is available only in Cisco ISE (and its value is the default, which is “unknown”).

NDG Types Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description

Note Cisco Secure ACS, Release 5.5 or above can support more than one network device group (NDG) with the same name. Cisco ISE, Release 2.2 does not support this naming scheme. Therefore, only the first NDG type with any defined name is migrated.

Note If you try to migrate NDGs with more than 101 character limit, the migration tool displays an error message stating the export process failure.

NDG Hierarchy Mapping

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

Default Network Devices Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Default network device status	Default network device status
Network device group	Not migrated
TACACS+ Shared Secret	Shared Secret
TACACS+ Single Connect Device	Enable Single Connect Mode
Legacy TACACS+ Single Connect Support	Legacy Cisco Device
TACACS+ Draft Compliant Single Connect Support	TACACS+ Draft Compliance Single Connect Support
RADIUS - shared secret	Shared Secret
RADIUS - CoA port	Not migrated
RADIUS - Enable keywrap	Enable keywrap
RADIUS - Key encryption key	Key encryption key
RADIUS - Message authenticator code key	Message authenticator code key
RADIUS - Key input format	Key input format

Identity Group Mapping

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

Note Cisco ISE, Release 2.2 contains user and endpoint identity groups. Identity groups in Cisco Secure ACS, Release 5.5 or above are migrated to Cisco ISE, Release 2.2 as user and endpoint identity groups because a user needs to be assigned to a user identity group and an endpoint needs to be assigned to an endpoint identity group.

User Mapping

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

Hosts (Endpoints) Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
MAC address	Migrates as is
Status	Not migrated
Description	Migrates as is
Identity group	Migrates 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”).

Cisco Secure ACS Properties	Cisco ISE Properties
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”).
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”).

LDAP Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
Server connection information	Migrates as is
Directory organization information	Migrates as is
Directory groups	Migrates as is
Directory attributes	Migration is done manually (using the Cisco Secure ACS to Cisco ISE migration tool).

Note Only the LDAP configuration defined for the primary ACS instance is migrated.

Active Directory Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Domain name	Migrates as is
User name	Migrates as is

Cisco Secure ACS Properties	Cisco ISE Properties
Password	Migrates as is
Allow password change	Migrates as is
Allow machine access restrictions	Migrates as is
Aging time	Migrates as is
User attributes	Migrates as is
Groups	Migrates as is
Multiple domain support	Only domains joined to primary ACS instance migrated

Certificate Authentication Profile Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
Principle user name (X.509 attribute)	Principle user name (X.509 attribute).
Binary certificate comparison with certificate from LDAP or AD	Binary certificate comparison with certificate from LDAP or AD.
AD or LDAP name for certificate fetching	AD or LDAP name for certificate fetching.

Identity Store Sequences Mapping

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

Authorization Profile Mapping

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

Shell Profile Attributes Mapping

Cisco Secure ACS	Cisco ISE
Common Task Attributes	
Name	Name
Description	Description
Default Privilege (Static and Dynamic)	Default Privilege (0 to 15)
Maximum Privilege (Static)	Maximum Privilege (0 to 15)
Access Control List (Static and Dynamic)	Access Control List (Static and Dynamic)
Auto Command (Static and Dynamic)	Auto Command (Static and Dynamic)
No Callback Verify (Static and Dynamic)	—
No Escape (Static and Dynamic)	No Escape (True or False)
No Hang up (Static and Dynamic)	—
Timeout (Static and Dynamic)	Timeout (Static and Dynamic)
Idle Time (Static and Dynamic)	Idle Time (Static and Dynamic)
Callback Line (Static and Dynamic)	—
Callback Rotary (Static and Dynamic)	—
Custom Attributes	
Attribute	Name
Requirement (Mandatory and Optional)	Type (Mandatory and Optional)
Value (Static and Dynamic)	Value (Static and Dynamic)

Command Sets Attributes Mapping

Cisco Secure ACS	Cisco ISE
Name	Name
Description	Description
Permit any command that is not in the table below	Permit any command that is not listed below
Grant (Permit, Deny, Deny Always)	Grant (Permit, Deny, Deny Always)
Command	Command
Arguments	Arguments

Downloadable ACL Mapping

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

RADIUS Dictionary (Vendors) Mapping

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

Note The migration tool supports migration of vendor and its attributes based on the ID of the vendor and its attributes.

If the vendor name is user-defined in Cisco Secure ACS and predefined in Cisco ISE and their IDs are different, the export process succeeds but the import process fails. If the vendor name is predefined in Cisco Secure ACS and Cisco ISE and their IDs are same, you will receive a warning message. If the vendor name is user-defined in Cisco Secure ACS and predefined in Cisco ISE and their IDs are same, the export process fails.

RADIUS Dictionary (Attributes) Mapping

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

Note Only the user-defined RADIUS attributes that are not part of Cisco Secure ACS, Release 5.5 or above installation need to be migrated.

Identity Dictionary Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Attribute	Attribute name
Description	Description
Internal name	Internal name
Attribute type	Data type
Maximum length	Not migrated

Cisco Secure ACS Properties	Cisco ISE Properties
Default value	Not migrated
Mandatory fields	Not migrated
User	The dictionary property accepts this value (“user”).

Identity Attributes Dictionary Mapping

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

External RADIUS Server Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
Server IP address	Hostname

Cisco Secure ACS Properties	Cisco ISE Properties
Shared secret	Shared secret
Authentication port	Authentication port
Accounting port	Accounting port
Server timeout	Server timeout
Connection attempts	Connection attempts

External TACACS+ Server Mapping

Cisco Secure ACS Properties	Cisco ISE Properties
Name	Name
Description	Description
IP address	Host IP
Connection Port	Connection Port
Network Timeout	Timeout
Shared secret	Shared secret

RADIUS Token Mapping

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

Cisco Secure ACS Properties	Cisco ISE Properties
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.
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”.)

RSA Mapping

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

RSA Prompts Mapping

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