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 2.7 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.

If you choose the migration of ACS 4.x supported objects, you must enter the hostname of the ACS 4.x machine in the ACS4 Hostname field and click **Connect** in the ACS4 Host Information 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 2.7, 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 2.7, 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 2.7*.

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 2.7, 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