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, on page 1
- Security Considerations, on page 2
- Download Migration Tool Files, on page 2
- Initialize the Migration Tool, on page 3

Migration Tool Installation Guidelines

- Ensure that your environment is ready for migration. In addition to a Cisco Secure ACS, Release 4.2 or 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 4.2 or 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 2.7 software on the target machine.
    - If this is a single-appliance migration, you have the Cisco ISE, Release 2.7 software available to re-image the appliance or virtual machine.
    - Have all the appropriate Cisco Secure ACS, Release 4.2 or 5.5 and above and Cisco ISE, Release 2.7 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 2.7 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.

Note It is recommended to provide the hostname of the ACS 4.2 machine in the ACS4 Hostname field.

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-2.7.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.