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.