Data Migration Principles

This chapter describes data migration from Cisco Secure ACS, Release 5.5 or 5.6 when deployed on a single appliance or in a distributed deployment to Cisco ISE, Release 1.4.

- Data Migration and Deployment Scenarios, page 1
- Preparation for Migration from Cisco Secure ACS, Release 5.5 or 5.6, page 3
- Policy Services Migration Guidelines, page 3
- Per Policy Service Migration Guidelines, page 4
- Unsupported Rule Elements, page 5

Data Migration and Deployment Scenarios

Cisco Secure ACS and Cisco ISE exist on different hardware platforms and have different operating systems, databases, and information models. Therefore, you cannot perform a standard upgrade from Cisco Secure ACS to Cisco ISE. Instead, the migration tool reads data from Cisco Secure ACS and creates corresponding data in Cisco ISE.

Migrating 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 5.6 data to a Cisco ISE, Release 1.4, 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 1.4.

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 5.6 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 1.4, software.
Step 5  Import the converted Cisco Secure ACS, Release 5.5 or 5.6 data from the secure external server into the Cisco ISE, Release 1.4.

Migrating Data from a Distributed Environment

Before You Begin
If you have a large internal database, Cisco recommends 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
Preparation for Migration from Cisco Secure ACS, Release 5.5 or 5.6

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 5.6 data only in the Policy Set mode in Cisco ISE, Release 1.4.

• Migrate on a fresh installation of Cisco ISE, Release 1.4. In Cisco ISE, choose Administration > System > Settings > Policy Sets to enable the policy sets.

• 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 1.4. For all the policy sets created in the migration process, the first matching policy set is the matching type.

Policy Services Migration Guidelines

You must check the following to ensure policy services migration from Cisco Secure ACS to Cisco ISE:

• Service Selection Policies (SSP) contain SSP rules that are disabled or monitored in Cisco Secure ACS, Release 5.5 or 5.6, they are not migrated to Cisco ISE.

• Service Selection Policy (SSP) contains a SSP rule that is enabled in Cisco Secure ACS, Release 5.5 or 5.6
  • that requests a device administration service, it is not migrated to Cisco ISE. (Cisco ISE does not support device administration).
  • that requests a service, which contains a Group Mapping policy, it is not migrated to Cisco ISE. (Cisco ISE does not support Group Mapping Policy).
  • that 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).
  • that 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.
Per Policy Service Migration Guidelines

This section describes the changes for each policy service that you migrate from Cisco Secure ACS, Release 5.5 or 5.6 to Cisco ISE 1.4 because you migrate Cisco Secure ACS data only in the Policy Set mode in Cisco ISE, Release 1.4.

Cisco Secure ACS Service Selection Policy Default Rule Matches Cisco ISE Default Policy Set

You can create a policy set with the name of the service in Cisco ISE. If the policy set matches the service, which is the result of the SSP default rule in Cisco Secure ACS, Release 5.5 or 5.6, then the policy set becomes the default policy set in Cisco ISE, Release 1.4. The condition of the SSP rule in Cisco Secure ACS, Release 5.5 or 5.6 becomes the entry condition of the policy set in Cisco ISE, Release 1.4. In the case of the Cisco ISE, Release 1.4 default policy set, there is no entry condition required.

Migration of Cisco Secure ACS DenyAccess Service to Cisco ISE Authentication and Authorization Policies

When you convert the DenyAccess service in Cisco Secure ACS, Release 5.5 or 5.6 to Cisco ISE, Release 1.4, the authentication and authorization policies change to the following:

- The authentication policy has only the default outer rule with the results set to Default Network Access for the Allowed Protocol and DenyAccess for the identity source.
- The authorization policy has only the default rule set to DenyAccess (standard permission).

Migration of Cisco Secure ACS Service Identity Policy to Cisco ISE Authentication Policy of the Policy Set

When you want to convert the identity policy of the service in Cisco Secure ACS, Release 5.5 or 5.6 to the authentication policy of the policy set in Cisco ISE, Release 1.4, perform the following:

- Create an authentication policy that has a single, enabled, outer rule.
- Specify the condition of the outer rule as Device:Location starts with All Locations (this is always the matched condition).
- Set the results of the default outer rule to Default Network Access for the Allowed Protocol and DenyAccess for the identity source.

The result of the outer rule is the Allowed Protocol of the related service. The inner rules of the authentication policy are the rules of the related identity policy. The order of the inner rules of the authentication policy follows the same order of rules in the related identity policy. The state (enabled, disabled, or monitored) of the inner rules of the authentication policy follows the state of the rules in the related identity policy.

Migration of Cisco Secure ACS Service Authorization Policy to Cisco ISE Authorization Policy of the Policy Set

When you want to convert the authorization policy of the service in Cisco Secure ACS, Release 5.5 or 5.6 to the authorization policy of the policy set in Cisco ISE, Release 1.4:

- The rules of the policy set Local Exception Authorization policy are the rules of the Exception Authorization policy of the related service
- The rules of the policy set Authorization policy are the rules of the Authorization policy of the related service
• The order of the rules of the policy set in Local Exception Authorization policy and Authorization policy follows the order of the rules in Local Exception Authorization policy and Authorization policy of the related service

• The state (enabled, disabled, monitored) of the rules of the policy set Local Exception Authorization policy and Authorization policy follows the state of the rules in Local Exception Authorization policy and Authorization policy in the related service

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 5.6 to Cisco ISE, Release 1.4:

• Objects with special characters are not migrated.
• Attributes (RADIUS, VSA, identity, and host) of type enum are migrated as integers with allowed values.
• All endpoint attributes (no matter the attribute data type) are migrated as String data types.
• RADIUS attributes and VSA values cannot be filtered and added to Cisco ISE logs.

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 1: Unsupported Rule Elements

<table>
<thead>
<tr>
<th>Rule Elements</th>
<th>Status of Support</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and Time</td>
<td>Not Supported</td>
<td>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.</td>
</tr>
<tr>
<td>Date and Time</td>
<td>Not Supported</td>
<td>Date and time conditions in an authentication policy are not migrated to Cisco ISE. As a result, the rules are also not migrated.</td>
</tr>
<tr>
<td>Rule Elements</td>
<td>Status of Support</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>In</td>
<td>Partially Supported</td>
<td>The “In” operator is used for Hierarchies and &quot;Is&quot; for String type only. This can be translated using &quot;Matches&quot;.</td>
</tr>
<tr>
<td>Not In</td>
<td>Partially Supported</td>
<td>The &quot;Not In&quot; operator is used for Hierarchies and &quot;Is&quot; for String type only. This can be translated using &quot;Matches&quot;.</td>
</tr>
<tr>
<td>Contains Any</td>
<td>Not Supported</td>
<td>The “Contains Any” operator is only for external groups such as Active Directory and Lightweight Directory Access Protocol.</td>
</tr>
<tr>
<td>Contains All</td>
<td>Not Supported</td>
<td>The &quot;Contains All” operator is only for external groups such as Active Directory and Lightweight Directory Access Protocol.</td>
</tr>
<tr>
<td>Combination of logical</td>
<td>Not Supported</td>
<td>Rules that use these operators in their conditions are not migrated:</td>
</tr>
<tr>
<td>expressions</td>
<td></td>
<td>- Authentication policies that include compound conditions that have different logical expressions other than a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Authorization policies that include compound conditions that have different local expressions other than a &amp;&amp; b &amp;&amp; c &amp;&amp; are not migrated as part of the rule condition. As a workaround, you can manually use library compound conditions for some advanced logical expressions.</td>
</tr>
<tr>
<td>Network conditions</td>
<td>Not Supported</td>
<td>Rules that include only network conditions are not migrated. In case the condition includes network conditions and other supported conditions, the network conditions are ignored and are not migrated as part of the rule condition.</td>
</tr>
<tr>
<td>User attributes</td>
<td>Partially Supported</td>
<td>Rules with conditions that include user attributes with a data type other than the &quot;String&quot; data type are not migrated.</td>
</tr>
<tr>
<td>Host attributes</td>
<td>Not Supported</td>
<td>Authentication fails in case the condition refers to host attributes. Authorization policies that include a condition that has host (endpoint) attributes are not migrated to Cisco ISE authorization policies.</td>
</tr>
</tbody>
</table>
Cisco ISE does not support Terminal Access Controller Access-Control System (TACACS). Cisco Secure ACS Service Selection Policy rules that use TACACS attributes are not migrated.

<table>
<thead>
<tr>
<th>Rule Elements</th>
<th>Status of Support</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS attributes</td>
<td>Not Supported</td>
<td>Cisco ISE does not support Terminal Access Controller Access-Control System (TACACS). Cisco Secure ACS Service Selection Policy rules that use TACACS attributes are not migrated.</td>
</tr>
</tbody>
</table>