APPENDIX A

# Cisco Secure ACS 5.1/5.2 and Cisco ISE 1.0 Data Structure Mapping

This appendix provides information about the following migration-related topics:



## Data Objects That Are Migrated

The following data objects are migrated from Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0:

- Network device group (NDG) types and hierarchies
- Network devices
- Default network device
- External Remote Authentication Dial-In Service (RADIUS) servers
- Identity group
- Internal users
- Internal endpoints (hosts)
- Lightweight Directory Access Protocol (LDAP)
- AD
- RSA (partial support, see Table A-25)
- RADIUS token (see Table A-24)
- Certificate authentication profile

- Date and time condition (partial support, see Migration Policies, page A-3)
- RADIUS attribute and vendor-specific attributes (VSA) values (seeTable A-5 and Table A-6)
- RADIUS vendor dictionaries (see Notes for Table A-5 and Table A-6)
- Internal users attributes (see Table A-1 and Table A-2)
- Internal endpoint attributes (see General Migration Rules, page A-3)
- Authorization profile
- DACL
- Service selection policy (for network access)
- Identity (authentication) policy
- Authorization policy (for network access)
- Authorization exception policy (for network access)
- RADIUS proxy service
- User password complexity

# Data Objects That Are Not Migrated

The following data objects are not migrated from Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0:

- Monitoring reports
- Scheduled backups
- Repositories
- Administrators, roles, and administrators setting
- Customer/debug log configuration
- Deployment information (secondary nodes)
- Certificates (certificate authorities and local certificates)
- Security Group Access Control Lists (SGACL)
- Security Group (SG)
- AAA servers for supported Security Group Access (SGA) devices
- SG mapping
- Network Device Admission Control (NDAC) policy
- SGA egress matrix (SGA)
- SGA data within network devices
- Security Group Tag (SGT) in SGA authorization policy results
- Network condition (end station filters, device filters, device port filters)
- Authentication and authorization services which are unused in Cisco Secure ACS (disabled or SSP rule is not using them)
- Device administration authentication and authorization policies

# Data Objects That Are Partially Migrated

The following data objects are migrated partially from Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0:

- Identity and host attributes that are of type date are not migrated.
- RSA sdopts.rec file and secondary information are not migrated.
- RADIUS identity server attributes (only the attribute CiscoSecure-Group-Id is migrated).

# General Migration Rules

Consider these migration rules while migrating data from Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0:

- UTF8 data is not supported.
- 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 what is the attribute data type) are migrated as String data type.
- You cannot filter RADIUS attributes and VSA values to be added into ISE logs.

# Migration Policies

The following list describes Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 migration policies guidelines:

- Rules with conditions that include user attributes with a data type other than the “string” data type are not migrated.
- Authentication fails in case condition refers to host attributes.
- Authorization policies that include a condition that has host (endpoint) attributes are not migrated to Cisco ISE authorization policies.
- Date and time conditions in an authorization policy that has a recurrence weekly setting is not migrated to Cisco ISE. As a result, the rule is also not migrated.
- Date and time conditions in an authentication policy are not migrated to Cisco ISE. As a result, the rule is also not migrated.
- The following operands are not supported in conditions:
  - String: start with, end with, contains, not contains
  - Date and time: not in
  - Identity group: not in

  Rules that use these operands in their conditions are also 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 are not migrated. 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.

- Rules that include network conditions only 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.

**Note** If during the export phase, the Cisco ACS 5.1/5.2-ISE 1.0 Migration Tool identifies a gap within the authentication/authorization policies (matching any of the migration guidelines noted in this section), then all authentication and authorization policies will not be migrated. If this occurs, it is the responsibility of the administrator performing the migration to define the policies manually.

# Supported Attributes and Data Types

The following tables list the supported attributes that are migrated and their target data type.

*Table A-1 User Attributes Migrated from Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0*

| Cisco Secure ACS 5.1/5.2 | Cisco ISE 1.0 |
|---|---|
| String | String |
| UI32 | Not supported |
| IPv4 | Not supported |
| Boolean | Not supported |
| Date | Not supported |
| Enum | Not supported |

*Table A-2 User Attribute: Association to the User*

| Cisco Secure ACS 5.1/5.2 | Cisco ISE 1.0 |
|---|---|
| String | Supported |
| UI32 | — |
| IPv4 | — |
| Boolean | — |
| Date | — |

*Table A-3 Hosts Attributes Migrated from Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0*

| Cisco Secure ACS 5.1/5.2 | Cisco ISE 1.0 |
|---|---|
| String | String |
| UI32 | UI32 |
| IPv4 | IPv4 |
| Boolean | Boolean |
| Date | Not supported |
| Enum | Integers with allowed values |

*Table A-4 Host Attribute: Association to the Host*

| Cisco Secure ACS 5.1/5.2 | Cisco ISE 1.0 |
|---|---|
| String | Supported |
| UI32 | Supported (Value is converted to String) |
| IPv4 | Supported (Value is converted to String) |
| Boolean | Supported (Value is converted to String) |
| Date | Supported (Value is converted to String) |
| Enum | Supported (Value is converted to String) |

*Table A-5 RADIUS Attributes Migrated from Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0*

| Cisco Secure ACS 5.1/5.2 | Cisco ISE 1.0 |
|---|---|
| UI32 | UI32 |
| UI64 | UI64 |
| IPv4 | IPv4 |
| Hex String | Octect String |
| String | String |
| Enum | Integers with allowed values |

*Table A-6 RADIUS Attribute: Association to RADIUS Server*

| Cisco Secure ACS 5.1/5.2 | Cisco ISE 1.0 |
|---|---|
| UI32 | Supported |
| UI64 | Supported |
| IPv4 | Supported |
| Hex String | Supported (Hex strings are converted to octets string) |
| String | Supported |
| Enum | Supported (Enums are integers with allowed values) |

# Data Information Mapping

This section provides series of tables that list the data information that is mapped during export, which includes categories from Cisco Secure ACS 5.1/5.2 and its equivalent in Cisco ISE 1.0 for each object. The data mapping tables in this section list the status of what is or is not a valid data object mapped during the data migration during the export stage of the migration process:

- Table A-7 on page A-6 (network device property mapping)
- Table A-8 on page A-7 (Active Directory property mapping)

- Table A-9 on page A-7 (external RADIUS server property mapping)
- Table A-10 on page A-8 (hosts/endpoints property mapping)
- Table A-11 on page A-8 (identity dictionary property mapping)
- Table A-12 on page A-9 (identity group property mapping)
- Table A-13 on page A-9 (LDAP property mapping)
- Table A-14 on page A-10 (NDG types mapping)
- Table A-15 on page A-10 (NDG hierarchy mapping)
- Table A-16 on page A-11 (RADIUS dictionary vendors mapping)
- Table A-17 on page A-11 (RADIUS dictionary attributes mapping)
- Table A-18 on page A-11 (users mapping)
- Table A-19 on page A-12 (certificate authentication profile)
- Table A-20 on page A-12 (authorization profile mapping)
- Table A-21 on page A-12 (DACL mapping)
- Table A-22 on page A-13 (external RADIUS server mapping))
- Table A-23 on page A-13 (identity attributes dictionary mapping)
- Table A-24 on page A-13 (RADIUS token mapping)
- Table A-25 on page A-14 (RSA mapping)

**Note** The export and import reports include informational, warning, and error messages that serve as validation of the import and export process.

*Table A-7 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 Network Device Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Name | Migrate as is. |
| Description | Migrate as is. |
| Network device group | Migrate as is. |
| Single IP address | Migrate as is. |
| Single IP and subnet address | Migrate as is. |
| Collection of IP and subnet addresses | Migrate as is. |
| TACACS information | Not migrated because the Terminal Access Controller Access-Control System (TACACS) is unsupported in Cisco ISE 1.0. |
| RADIUS shared secret | Migrate as is. |
| CTS | Migrate as is. |
| SNMP | SNMP data is available only in Cisco ISE; therefore, there is no SNMP information for migrated devices. |

*Table A-7 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 Network Device Mapping (continued)*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Model name | This is a property available only in Cisco ISE (and its value is the default, "unknown"). |
| Software version | This is a property available only in Cisco ISE (and its value is the default, "unknown"). |

**Note** Any network devices that are set only as TACACS are not supported for migration and these are listed as non-migrated devices.

*Table A-8 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 Active Directory Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Domain name | Migrate as is. |
| User name | Migrate as is. |
| Password | Migrate as is. |
| Allow password change | Migrate as is. |
| Allow machine access restrictions | Migrate as is. |
| Aging time | Migrate as is. |
| User attributes | Migrate as is. |
| Groups | Migrate as is. |

**Note** The Cisco Secure ACS 5.1/5.2-ISE 1.0 Migration Tool issues a "join" command after the Active Directory data has been migrated. This "join" operation can fail if the domain name, user name, and password are incorrect. In addition, it is important that the Cisco ISE appliance be properly synchronized with the AD server time, or this can also cause a failure during the "join" operation.

*Table A-9 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 External RADIUS Server Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Name | Migrate as is. |
| Description | Migrate as is. |
| Server IP address | Migrate as is. |
| Shared secret | Migrate as is. |
| Authentication port | Migrate as is. |
| Accounting port | Migrate as is. |
| Server timeout | Migrate as is. |
| Connection attempts | Migrate as is. |

*Table A-10 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 Hosts (Endpoints) Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| MAC address | Migrate as is. |
| Status | Not migrated. |
| Description | Migrate as is. |
| Identity group | Migrate 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”). |
| 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”). |

*Table A-11 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 Identity Dictionary Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Attribute | Attribute name |
| Description | Description |
| Internal name | Internal name |
| Attribute type | Data type |
| Maximum length | Not migrated |
| Default value | Not migrated |
| Mandatory fields | Not migrated |
| User | The dictionary property accepts this value (“user”). |

*Table A-12 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 Identity Group Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Name | Name |
| Description | Description |
| Parent | This property is migrated as part of the hierarchy details. |

**Note** Cisco ISE contains endpoint and identity groups. Identity groups in Cisco Secure ACS 5.1/5.2 are migrated to Cisco ISE as endpoint groups and as identity groups because a user needs to be assigned to an identity group and an endpoint needs to be assigned to an endpoint group.

*Table A-13 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 LDAP Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Name | Name |
| Description | Description |
| Server connection information | Migrate as is. (Server Connection tab; see Figure A-1 on page A-9.) |
| Directory organization information | Migrate as is. (Directory Organization tab; see Figure A-2 on page A-10.) |
| Directory groups | Migrate as is. |
| Directory attributes | Migration is done manually (using the Cisco ACS 5.1/5.2-ISE 1.0 Migration Tool). |

*Figure A-1 Server Connection Tab*

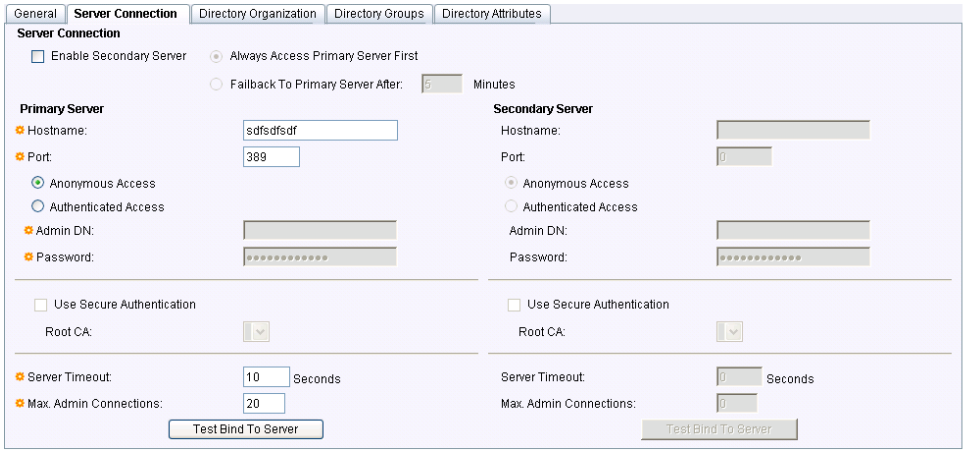

*Figure A-2 Directory Organization Tab*

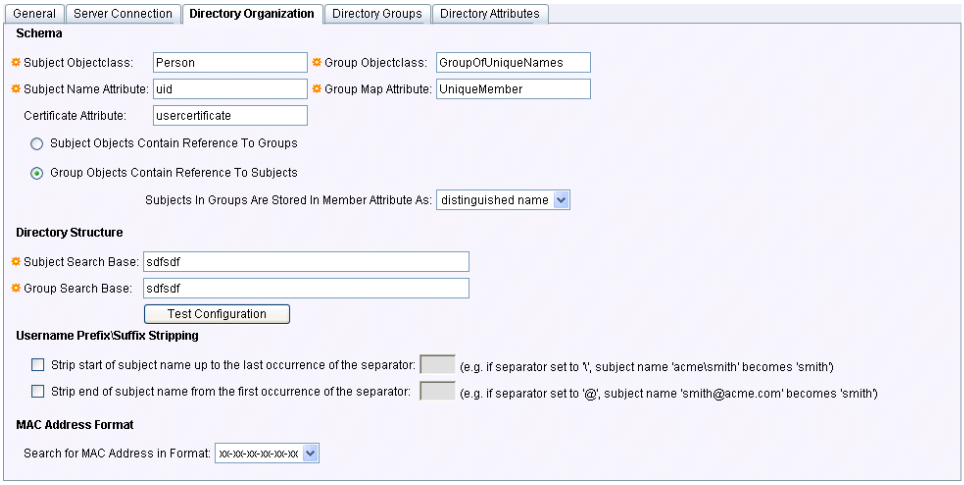


*Table A-14 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 NDG Types Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Name | Name |
| Description | Description |

**Note** Cisco Secure ACS 5.1/5.2 can support having more than one network device group (NDG) with the same name. Cisco ISE does not support this naming scheme. Therefore, only the first NDG type with any defined name is migrated.

*Table A-15 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 NDG Hierarchy Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 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.) |

**Note** Any NDGs that contain a root name with a colon (:) currently are not migrated because Cisco ISE 1.0 does not recognized the colon as a valid character.

*Table A-16 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 RADIUS Dictionary (Vendors) Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 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** Only those RADIUS vendors that are not part of a Cisco Secure ACS 5.1/5.2 installation are required to be migrated (this affects only the user-defined vendors).

*Table A-17 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 RADIUS Dictionary (Attributes) Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 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 nam.e (In addition, the NDG type is the prefix for this object name.) |
| Direction | Not supported in Cisco ISE. |
| Multiple allowed | Not supported in Cisco ISE. |
| Attribute type | Migrate as is. |
| Add policy condition | Not supported in Cisco ISE. |
| Policy condition display name | Not supported in Cisco ISE. |

**Note** Only those RADIUS attributes that are not part of a Cisco Secure ACS 5.1/5.2 installation are required to be migrated (only the user-defined attributes need to be migrated).

*Table A-18 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 User Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Name | Name |
| Description | Description |
| Status | No need to migrate this property. (This property does not exist in Cisco ISE.) |
| Identity group | Migrate to identity groups in Cisco ISE. |
| Password | Password |

*Table A-18 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 User Mapping (continued)*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Enable password | No need to migrate this property. (This property does not exist in Cisco ISE.) |
| Change password on next login | No need to migrate this property. |
| User attributes list | User attributes are imported from Cisco ISE and associated with the users. |

*Table A-19 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 Certificate Authentication Profile Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 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 - LDAP name for certificate fetching | AD - LDAP name for certificate fetching |

*Table A-20 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 Authorization Profile Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Name | Name |
| Description | Description |
| DACLid (downloadable ACL ID) | Migrate as is. |
| Attribute type (static and dynamic) | • Migrate as is if static attribute.<br>• Migrated as is, if dynamic attribute, except Dynamic VLAN. |
| Attributes (filtered for static type only) | RADIUS attributes |

*Table A-21 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 Downloadable ACL Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Name | Name |
| Description | Description |
| DACL content | DACL content |

*Table A-22 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 External RADIUS Server Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Name | Name |
| Description | Description |
| Server IP address | Hostname |
| Shared secret | Shared secret |
| Authentication port | Authentication port |
| Accounting port | Accounting port |
| Server timeout | Server timeout |
| Connection attempts | Connection attempts |

*Table A-23 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 Identity Attributes Dictionary Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Attribute | Attribute name |
| Description | Internal name |
| Name | Migrate 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/extracted yet from Cisco Secure ACS | Allowed value = display name |
| Not exported/extracted yet from Cisco Secure ACS | Allowed value = internal name |
| Not exported/extracted yet from 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 |

*Table A-24 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 RADIUS Token Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| Name | Name |
| Description | Description |
| Safeword server | Safeword server |
| Enable secondary appliance | Enable secondary appliance |

*Table A-24 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 RADIUS Token Mapping (continued)*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 Properties |
|---|---|
| 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 |
| 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”) |

*Table A-25 Cisco Secure ACS 5.1/5.2 to Cisco ISE 1.0 RSA Mapping*

| Cisco Secure ACS 5.1/5.2 Properties | Cisco ISE 1.0 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 |