# Data Structure Mapping

This appendix provides information about the data objects that are migrated, partially migrated, and not migrated from Cisco Secure ACS, Release 5.5 or later to Cisco ISE, Release 2.2.



## Data Structure Mapping

Data structure mapping is the process by which data objects are analyzed and validated in the migration tool during the export phase.

## Migrated Data Objects

The following data objects are migrated from Cisco Secure ACS to Cisco ISE, :

- Network device group (NDG) types and hierarchies
- Network devices
- Default network device
- Network device ranges (in last octet) (partial support)
- External RADIUS servers
- External TACACS+ servers
- TACACS+ server sequence
- TACACS+ settings
- Stateless session resume capability settings
- Identity groups

- Internal users
- Internal users with enable password change
- Internal users with password type configured as external Identity store
- Disable user account if date exceeds
- Global option for disabling user account after n days of inactivity
- Internal endpoints (hosts)
- Lightweight Directory Access Protocol (LDAP)
- Common Name and Distinguished name for Group Name attribute in LDAP Identity Store
- Microsoft Active Directory (AD)
- RSA
- RADIUS token
- Certificate authentication profiles
- Date and time conditions (Partial support, see Unsupported Rule Elements)
- Network conditions (end station filters, device filters, device port filters)
- Maximum user sessions
- RADIUS attribute and vendor-specific attributes (VSA) values
- RADIUS vendor dictionaries
- Internal users attributes
- Internal endpoint attributes
- TACACS+ Profiles
- Downloadable access control lists (DACLs)
- Identity (authentication) policies
- Authentication, Authorization, and Authorization exception polices for TACACS+ (for policy objects)
- TACACS+ Command Sets
- Authorization exception policies (for network access)
- Service selection policies (for network access)
- RADIUS proxy service
- TACACS+ proxy service
- User password complexity
- Identity sequence and RSA prompts
- UTF-8 data
- EAP authentication protocol—PEAP-TLS

- User check attributes
- Dial-in attributes
- Crypto binding attributes
- Weak ciphers support for allowed protocols
- Identity sequence advanced option
- Additional attributes available in policy conditions—AuthenticationIdentityStore
- Additional string operators—Start with, Ends with, Contains, Not contains
- RADIUS identity server attributes
- Length included flag (L-bit) in EAP-MD5, EAP-TLS, LEAP, PEAP, and EAP-FAST authentication

# Partially Migrated Data Objects

The following data objects are partially migrated from Cisco Secure ACS , Release 5.5 or above to Cisco ISE, Release 2.2:

- Host attributes that are of type IP address and Date are not migrated.
- RSA sdopts.rec file and secondary information are not migrated.
- Multi-Active Directory domain (only Active Directory domain joined to the primary) is migrated.
- LDAP configuration defined for primary ACS instance is migrated. Secondary ACS instance specific configurations are not migrated.

# Data Objects Not Migrated

The following data objects are not migrated from Cisco Secure ACS to Cisco ISE:

- Monitoring reports
- Scheduled backups
- Repositories
- Administrators, roles, and administrators settings
- Customer/debug log configurations
- Deployment information (secondary nodes)
- Certificates (certificate authorities and local certificates)

  You must manually import your certificates because they are not migrated. For identity stores that use certificates, you must map the imported certificate to the ID store. If you were using identity source sequences, you must create new sequences that duplicate the originals.
- Trustsec related configuration

- Display RSA node missing secret
- Additional attribute available in a policy condition—NumberOfHoursSinceUserCreation
- Wildcards for hosts
- OCSP service
- Syslog messages over SSL/TCP
- Configurable copyright banner
- IP address exclusion

# 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***

| Rule Elements | Status of Support | Description |
|---|---|---|
| Date and Time | Not Supported | 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.<br>Date and time conditions in an authentication policy are not migrated to Cisco ISE. As a result, the rules are also not migrated. |
| Not In | Not Supported | The "Not In" operator is converted to NOT_STARTS_WITH. |
| Contains Any | Partially Supported | The "Contains Any" operator is converted to a compound condition with EQUALS & OR operators.<br>Example: In ACS, **AD ExternalGrp Contains Any (A, B)** is converted to **(AD ExternalGrp Equals A) OR (AD ExternalGrp Equals B)** in Cisco ISE. |

| Rule Elements | Status of Support | Description |
|---|---|---|
| Contains All | Partially Supported | The "Contains All" operator is converted to a compound condition with EQUALS & AND operators.<br>Example: In ACS **AD:ExternalGrp contains all A;B** is converted to **(AD ExternalGrp Equals A) AND (AD ExternalGrp Equals B)** in Cisco ISE. |
| Combination of logical expressions | Not Supported | Rules that use these operators in their conditions are not migrated:<br>• 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.<br>• 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. As a workaround, you can manually use library compound conditions for some advanced logical expressions. |

# Data Information Mapping

This section lists the data that is mapped during the export process. The tables include object categories from Cisco Secure ACS, Release 5.5 or above and its equivalent in Cisco ISE, Release 2.2. The data-mapping tables in this section list the status of valid or not valid data objects mapped when migrating data during the export stage of the migration process.

## Network Device Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Name | Migrates as is |
| Description | Migrates as is |
| Network device group | Migrates as is |

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Single IP address | Migrates as is |
| Single IP and subnet address | Migrates as is |
| IP ranges | IP ranges in last octet without Exclude IP option, are migrated |
| Exclude IP address | Not Supported |
| TACACS information | Migrates as is |
| RADIUS shared secret | Migrates as is |
| TACACS+ shared secret | Migrates as is |
| CTS | Migrates as is |
| SNMP | SNMP data is available only in Cisco ISE; therefore, there is no SNMP information for migrated devices. |
| Model name | This property is available only in Cisco ISE (and its value is the default, which is “unknown”). |
| Software version | This property is available only in Cisco ISE (and its value is the default, which is “unknown”). |

# NDG Types Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Name | Name |
| Description | Description |

**Note** Cisco Secure ACS, Release 5.5 or above can support more than one network device group (NDG) with the same name. Cisco ISE, Release 2.2 does not support this naming scheme. Therefore, only the first NDG type with any defined name is migrated.

**Note** If you try to migrate NDGs with more than 101 character limit, the migration tool displays an error message stating the export process failure.

# NDG Hierarchy Mapping

| Cisco Secure ACS Properties | Cisco ISE 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. |

# Default Network Devices Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Default network device status | Default network device status |
| Network device group | Not migrated |
| TACACS+ Shared Secret | Shared Secret |
| TACACS+ Single Connect Device | Enable Single Connect Mode |
| Legacy TACACS+ Single Connect Support | Legacy Cisco Device |
| TACACS+ Draft Compliant Single Connect Support | TACACS+ Draft Compliance Single Connect Support |
| RADIUS - shared secret | Shared Secret |
| RADIUS - CoA port | Not migrated |
| RADIUS - Enable keywrap | Enable keywrap |
| RADIUS - Key encryption key | Key encryption key |
| RADIUS - Message authenticator code key | Message authenticator code key |
| RADIUS - Key input format | Key input format |

# Identity Group Mapping

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

**Note** Cisco ISE, Release 2.2 contains user and endpoint identity groups. Identity groups in Cisco Secure ACS, Release 5.5 or above are migrated to Cisco ISE, Release 2.2 as user and endpoint identity groups because a user needs to be assigned to a user identity group and an endpoint needs to be assigned to an endpoint identity group.

# User Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Name | Name |
| Description | Description |
| Status | No need to migrate this property. This property does not exist in Cisco ISE. |
| Identity group | Migrates to identity groups in Cisco ISE |
| Password | Password |
| Enable password | Password |
| Change password on next login | Not migrated |
| User attributes list | User attributes are imported from the Cisco ISE and are associated with users |
| Expiry days | Supported |

# Hosts (Endpoints) Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| MAC address | Migrates as is |
| Status | Not migrated |
| Description | Migrates as is |
| Identity group | Migrates 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”). |

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| 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”). |

# LDAP Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Name | Name |
| Description | Description |
| Server connection information | Migrates as is |
| Directory organization information | Migrates as is |
| Directory groups | Migrates as is |
| Directory attributes | Migration is done manually (using the Cisco Secure ACS to Cisco ISE migration tool). |

**Note** Only the LDAP configuration defined for the primary ACS instance is migrated.

# Active Directory Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Domain name | Migrates as is |
| User name | Migrates as is |

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Password | Migrates as is |
| Allow password change | Migrates as is |
| Allow machine access restrictions | Migrates as is |
| Aging time | Migrates as is |
| User attributes | Migrates as is |
| Groups | Migrates as is |
| Multiple domain support | Only domains joined to primary ACS instance migrated |

# Certificate Authentication Profile Mapping

| Cisco Secure ACS Properties | Cisco ISE 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 or LDAP name for certificate fetching | AD or LDAP name for certificate fetching. |

# Identity Store Sequences Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Name | Name |
| Description | Description |
| Certificate based, certificate authentication profile | Certificate based, certificate authentication profile |
| Password based | Authentication search list |
| Advanced options > if access on current IDStore fails than break sequence | Do not access other stores in the sequence and set the “AuthenticationStatus” attribute to “ProcessError.” |
| Advanced options > if access on current IDStore fails then continue to next | Treated as “User Not Found” and proceed to the next store in the sequence. |
| Attribute retrieval only > exit sequence and treat as “User Not Found” | Not supported (should be ignored) |

# Authorization Profile Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Name | Name |
| Description | Description |
| DACLID (downloadable ACL ID) | Migrates as is |
| Attribute type (static and dynamic) | • Migrates as is if static attribute.<br>• Migrated as is if dynamic attribute. |
| Attributes (filtered for static type only) | RADIUS attributes |

# Shell Profile Attributes Mapping

| Cisco Secure ACS | Cisco ISE |
|---|---|
| **Common Task Attributes** | |
| Name | Name |
| Description | Description |
| Default Privilege (Static and Dynamic) | Default Privilege (0 to 15) |
| Maximum Privilege (Static) | Maximum Privilege (0 to 15) |
| Access Control List (Static and Dynamic) | Access Control List (Static and Dynamic) |
| Auto Command (Static and Dynamic) | Auto Command (Static and Dynamic) |
| No Callback Verify (Static and Dynamic) | — |
| No Escape (Static and Dynamic) | No Escape (True or False) |
| No Hang up (Static and Dynamic) | — |
| Timeout (Static and Dynamic) | Timeout (Static and Dynamic) |
| Idle Time (Static and Dynamic) | Idle Time (Static and Dynamic) |
| Callback Line (Static and Dynamic) | — |
| Callback Rotary (Static and Dynamic) | — |
| **Custom Attributes** | |
| Attribute | Name |
| Requirement (Mandatory and Optional) | Type (Mandatory and Optional) |
| Value (Static and Dynamic) | Value (Static and Dynamic) |

# Command Sets Attributes Mapping

| Cisco Secure ACS | Cisco ISE |
|---|---|
| Name | Name |
| Description | Description |
| Permit any command that is not in the table below | Permit any command that is not listed below |
| Grant (Permit, Deny, Deny Always) | Grant (Permit, Deny, Deny Always) |
| Command | Command |
| Arguments | Arguments |

# Downloadable ACL Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Name | Name |
| Description | Description |
| DACL content | DACL content |

# RADIUS Dictionary (Vendors) Mapping

| Cisco Secure ACS Properties | Cisco ISE 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** The migration tool supports migration of vendor and its attributes based on the ID of the vendor and its attributes.

If the vendor name is user-defined in Cisco Secure ACS and predefined in Cisco ISE and their IDs are different, the export process succeeds but the import process fails. If the vendor name is predefined in Cisco Secure ACS and Cisco ISE and their IDs are same, you will receive a warning message. If the vendor name is user-defined in Cisco Secure ACS and predefined in Cisco ISE and their IDs are same, the export process fails.

# RADIUS Dictionary (Attributes) Mapping

| Cisco Secure ACS Properties | Cisco ISE 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 name (NDG type is the prefix for this object name). |
| Direction | Not supported in Cisco ISE |
| Multiple allowed | Not supported in Cisco ISE |
| Attribute type | Migrates as is |
| Add policy condition | Not supported in Cisco ISE |
| Policy condition display name | Not supported in Cisco ISE |

**Note** Only the user-defined RADIUS attributes that are not part of Cisco Secure ACS, Release 5.5 or above installation need to be migrated.

# Identity Dictionary Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Attribute | Attribute name |
| Description | Description |
| Internal name | Internal name |
| Attribute type | Data type |
| Maximum length | Not migrated |

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Default value | Not migrated |
| Mandatory fields | Not migrated |
| User | The dictionary property accepts this value (“user”). |

# Identity Attributes Dictionary Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Attribute | Attribute name |
| Description | Internal name |
| Name | Migrates 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 or extracted yet from the Cisco Secure ACS | Allowed value = display name |
| Not exported or extracted yet from the Cisco Secure ACS | Allowed value = internal name |
| Not exported or extracted yet from the 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 |

# External RADIUS Server Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Name | Name |
| Description | Description |
| Server IP address | Hostname |

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Shared secret | Shared secret |
| Authentication port | Authentication port |
| Accounting port | Accounting port |
| Server timeout | Server timeout |
| Connection attempts | Connection attempts |

# External TACACS+ Server Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Name | Name |
| Description | Description |
| IP address | Host IP |
| Connection Port | Connection Port |
| Network Timeout | Timeout |
| Shared secret | Shared secret |

# RADIUS Token Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Name | Name |
| Description | Description |
| Safeword server | Safeword server |
| Enable secondary appliance | Enable secondary appliance |
| 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 |

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| 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”.) |

# RSA Mapping

| Cisco Secure ACS Properties | Cisco ISE 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 |

# RSA Prompts Mapping

| Cisco Secure ACS Properties | Cisco ISE Properties |
|---|---|
| Passcode prompt | Passcode prompt |
| Next Token prompt | Next Token prompt |
| PIN Type prompt | PIN Type prompt |
| Accept System PIN prompt | Accept System PIN prompt |
| Alphanumeric PIN prompt | Alphanumeric PIN prompt |
| Numeric PIN prompt | Numeric PIN prompt |