ACS 5.5 Attribute Support in the Migration Utility

This chapter contains:

Introduction

This chapter describes ACS 4.x to ACS 5.5 attribute migration. To migrate ACS 4.x attributes, they must meet ACS 5.5 criteria. You can migrate some ACS 4.x elements to ACS 5.5, even though some of the attributes for an element might not migrate (or translate) to ACS 5.5.

For example, ACS 5.5 supports the user shell exec privilege level as a numeric value from 1 through 15. If the privilege level for the ACS 4.x User element is not a numeric value from 1 through 15, the User element is migrated, but the user shell exec privilege level attribute is not migrated.

ACS 4.x to 5.5 Migration

The following sections contain element information for:

AAA Client/Network Device

Table A-1 describes the differences between the ACS 4.x network device definitions and the ACS 5.5 network device definitions.

Table A-1 ACS Network Device Definitions

ACS element	ACS 4.x	ACS 5.5 Status
RADIUS and TACACS+	Defines one network device for each protocol. For example, network device1 for RADIUS, network device 2 for TACACS+.	Defines one network device for RADIUS and TACACS+. See Overlapping IP Addresses, page D-3.
IP Address	• Use regular expressions to define the IP address. • You can define more than 40 IP addresses. • Includes wildcards and ranges.	• Define IP addresses as a pair of IP addresses and mask definitions. • Limited to 40 IP addresses. • Definition is in the form of a subnet mask. See Untranslatable IP Addresses, page D-4.

Note ACS 5.5 does not support ACS 4.x authentication by using an attribute for network devices. ACS 5.5 supports only RADIUS and TACACS+. You cannot define a specific vendor.

NDG

ACS 5.5 does not support the ACS 4.x shared key password attribute for NDGs. The Analysis report flags shared key passwords on the NDG level. You can use only shared key passwords on the network device level.

For devices that belong to an NDG where the NDG includes a Key Encryption Key, the NDG's Key Encryption Key will be extracted and included in the network device definition instead of that defined with the network device definition Key Encryption Key.

For devices that belong to an NDG where the NDG includes a Message Authenticator Code Key, the NDG's Message Authenticator Code Key will be extracted and included in the network device definition instead of that defined with the network device definition Message Authenticator Code Key.

Note If a shared key password resides on the NDG level, the shared key password is migrated to all the network devices that belong to this NDG. The network devices' shared key password is migrated only if the NDG shared key password is empty.

Internal User

ACS 5.5 supports the ACS 4.x Password Authentication Type. ACS 5.5 supports authentication on both internal and external databases. You migrate the user object with a default authentication password if the administrator uses Windows or LDAP. You can supply a different password when you run the Migration Utility. See Migration Script User Preferences.

User Policy Components

In ACS 4.x, the policy-related authorization data is embedded within the user definitions. In ACS 5.5, policy-related authorization data is included in shared components that are referenced from within the ACS 5.5 policy tables. Table A-2 shows the attributes for the ACS 4.x user policy components and describes the status in ACS 5.5.

Table A-2 User Policy Component Attributes

ACS 4.x Attribute	ACS 5.5 Status
TACACS+ Shell (exec) Privilege level: The privilege level is a string field without validity checks.	• In ACS 5.5, the default privilege level cannot be larger than the maximum privilege level. • ACS 5.5 supports the privilege level as a numeric value (1-15).
TACACS+ Shell Custom attributes	Phase II does not support custom attributes for privilege levels and shell commands.
TACACS+ Shell Command Authorization Set: You do not have to specify a value for each attribute.	Migration supports only per-user command authorization and does not support the following attributes: • Assign a shell command authorization set for any network device. • Assign a shell command authorization set on a per-network device group basis. You must specify a value for each attribute.

User Group

In ACS 4.x, each user was associated to a single group. The User Group element includes general identity attributes as well as policy component attributes such as shell exec and RADIUS attributes. In ACS 5.5, the equivalent to user group is the identity group. However, each identity group is purely a logical container and does not include policy components.

User Group Policy Components

In ACS 4.x, policy authorization data is embedded within user group definitions. In ACS 5.5, policy authorization data is defined in Session Authorization Profiles. Table A-3 shows the attributes for the policy components of the ACS 4.x user group and describes the status in ACS 5.5.

Table A-3 User Group Policy Component Attributes

ACS 4.x Attribute	ACS 5.5 Status
TACACS+Shell (exec) Privilege level: The privilege level is a string field without validity checks.	• ACS 5.5 supports the privilege level as a numeric value (1-15). • In ACS 5.5, the default privilege level cannot be larger than the maximum privilege level.
TACACS+Shell (exec) Custom attributes	ACS 5.5 does not support shell command custom attributes.
TACACS+Shell Command Authorization Set You do not have to specify a value for each attribute.	ACS 5.5 supports only per-user command authorization and does not support the following attributes: • Assign a shell command authorization set for any network device. • Assign a shell command authorization set on a per-network device group basis. You must specify a value for each attribute.

ACS 4.x is a group based access control system whereas ACS 5.x is a policy based access control system. When you migrate from ACS 4.x to 5.x using the migration utility, the custom attributes are not migrated. As a result, all the authentications and authorizations may fail in ACS 5.x. Therefore, you need to manually configure the custom attributes in Shell Profiles and map it to each user in the Access Policies.

To configure the custom attributes manually, see http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.5/user/guide/pol_elem.html#wp1053110.

To map the custom attributes in the policy conditions, see http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.5/user/guide/access_policies.html.

Shared Shell Command Authorization Sets

No attributes are missing. In ACS 4.x, shell command authorization sets are defined as shared elements included in device administration. The export and import phases migrate these elements to command sets. The ACS 5.5 name and description of each element is the same as in ACS 4.x.

MAB

In ACS 4.x, you can define MAC addresses in the User table as part of the NAP configuration. ACS 5.5 migrates MAC IDs as MacId objects. Each MacId object is added to the MAC Authentication Bypass MAB (Hosts) Identity stores.

DACL

In ACS 4.x, the shared DACL is defined as a shared object to be included in the NAP table, and the user and user group objects. A shared DACL consists of a list of sets of ACL content and Network Access Filter (NAF) ID. You can migrate a single DACL from ACS 4.x to multiple DACLs on ACS 5.5. You can migrate only the ACL content, because ACS 5.5 does not support NAFs.

EAP-FAST Master Keys

The Master Keys definition in ACS 4.x has a schema that is different from that of the ACS 5.5 schema. Therefore, Master Keys are migrated to different ACS 5.5 Information Model Objects (IMOs).

Shared RACs

In ACS 4.x, you can define a shared profile component that contains RADIUS Authorization Components (RACs), and you can define a set of RADIUS attributes and values that are returned in an authorization response. In ACS 5.5, RACs are defined in shared authorization profiles.

Table A-4 shows the attributes for the RACs in ACS 4.x and describes their status in ACS 5.5.

Table A-4 Shared RADIUS Authorization Component Attributes

ACS 4.x Attribute	ACS 5.5 Status
In ACS 4.x, the following attributes can be configured and fixed: • MS-CHAP-MPPE-Keys (12) • MS-MPPE-Send-Key (16) • MS-MPPE-Recv-Key (17)	In ACS 5.5, you cannot configure these attributes. These are added to the profile as required.
In ACS 4.x, Ascend attributes are stored internally with a vendor ID of 0.	In ACS 5.5, you have to assign an Ascend vendor ID of 529.

Customer VSAs

During migration, the dictionary is iterated to identify the missing attributes in ACS 5.5 for each vendor. If the vendor does not exist in the ACS 5.5 dictionary, all the vendor attributes are migrated. If the vendor exists in the ACS 5.5 dictionary, only attributes that are not defined in ACS 5.5 are migrated.

Max User Sessions

In ACS 4.*x*, you can configure the Maximum User Sessions settings at user level, group level, and globally. The maximum user sessions settings are migrated when you migrate from 4.*x* to 5.5.