Understanding ACS 5.8.1 Configuration

ACS 5.8.1 Configuration

This chapter explains the differences in configuration between ACS 3.x and 4.x and ACS 5.8.1 when you convert the existing 3.x and 4.x configurations to 5.8.1.

This chapter contains the following sections:

Table 1 on page 1 describes the main configuration areas in ACS 5.8.1.

Table 1 Main Configuration Areas in ACS 5.8.1

Configuration Area	What Will Be Configured
Network Resources	AAA clients, client grouping, and RADIUS proxy servers
Users and Identity Stores	Internal users, Internal hosts, Active Directory, LDAP directories, one-time password servers, RADIUS identity stores, certificate authority information, and identity store sequences
Policy Elements	Conditions and authorization profiles for network access policy
Access Services	Network access policy to address different access scenarios
Monitoring and Reports	ACS monitoring, reporting and troubleshooting tasks
System Administration	ACS system administration tasks

Network Resources

AAA clients and RADIUS proxy servers are defined and organized under the Network Resources drawer.

The following components are configured under Network Resources:

Network Device Groups

Key changes in ACS 5.8.1:

- A single device can be a member of multiple groups—Network Device Group hierarchies.

- Device group level shared secrets are not available.
- Device group is not a container for AAA server definitions.

Network device groups allow you to group devices based on location, type, and other groupings. This is especially important for applying network access policy based on these groupings. For example, restrict West Coast firewall administrator to have access to only West Coast firewalls.

When you plan to migrate the network device to ACS 5.8.1, we recommend that you plan the device grouping before importing or configuring the devices. This will allow the assignment of groups to devices while they are being created in ACS 5.8.1.

ACS 3.x and 4.x has a flat device grouping model where a single device can belong to only one device group. This model causes a proliferation of groups when you are trying to group devices in multiple ways. Grouping locations hierarchically is very common.

For example, group by continent, region and country. The following example shows groups in ACS 3.x and 4.x:

- Africa-Southern-SouthAfrica
- Africa-Southern-Namibia
- Africa-Southern-Botswana

Devices are often grouped by type. Extending the above example to incorporate type grouping would result in the following groups:

- Africa-Southern-SouthAfrica-Firewalls
- Africa-Southern-SouthAfrica-Switches
- Africa-Southern-SouthAfrica-Routers
- Africa-Southern-Namibia-Firewalls
- Africa-Southern-Namibia-Switches
- Africa-Southern-Namibia-Routers
- Africa-Southern-Botswana-Firewalls
- Africa-Southern-Botswana-Switches
- Africa-Southern-Botswana-Routers

The number of groups increase when other parameters, such as device types, vendors, and so on are added.

ACS 5.8.1 addresses this device group proliferation issue by providing network device group hierarchies. There can be multiple hierarchies representing different groups. A device can belong to one node in each hierarchy. Figure 1 on page 3, Figure 2 on page 3, and Figure 3 on page 3 show three different network device group hierarchies.

Figure 1 Network Device Group Hierarchies

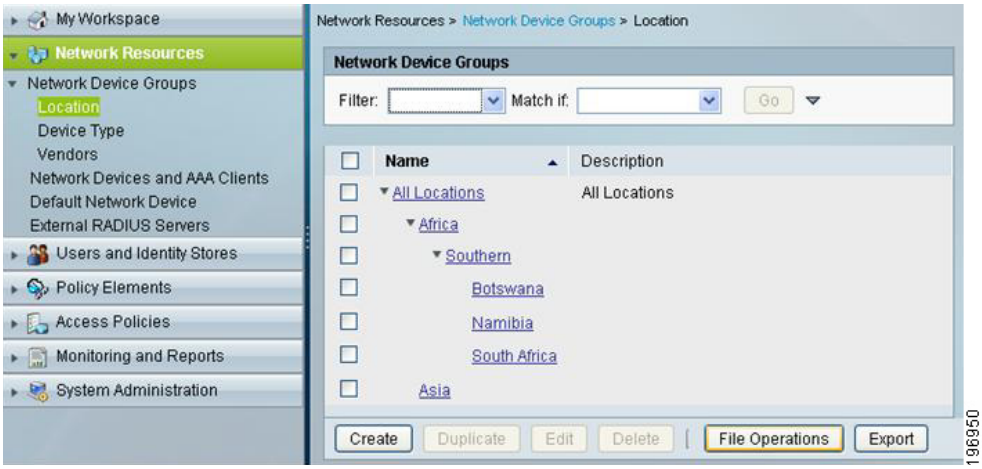


Figure 2 Network Device Group Hierarchies

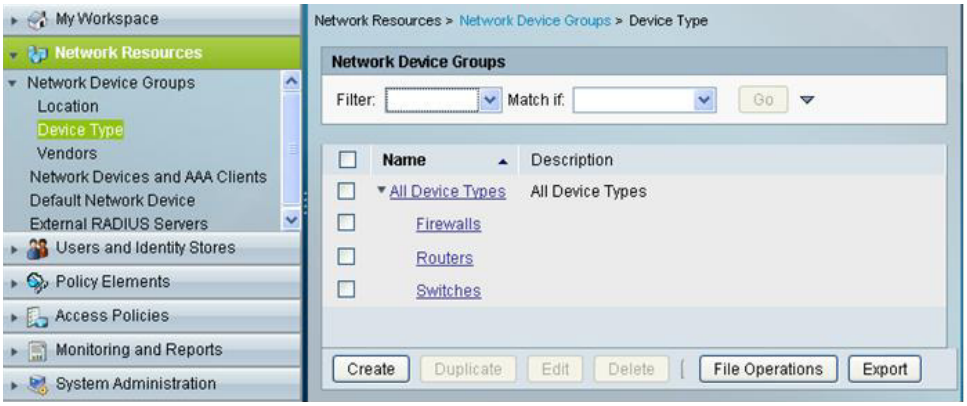
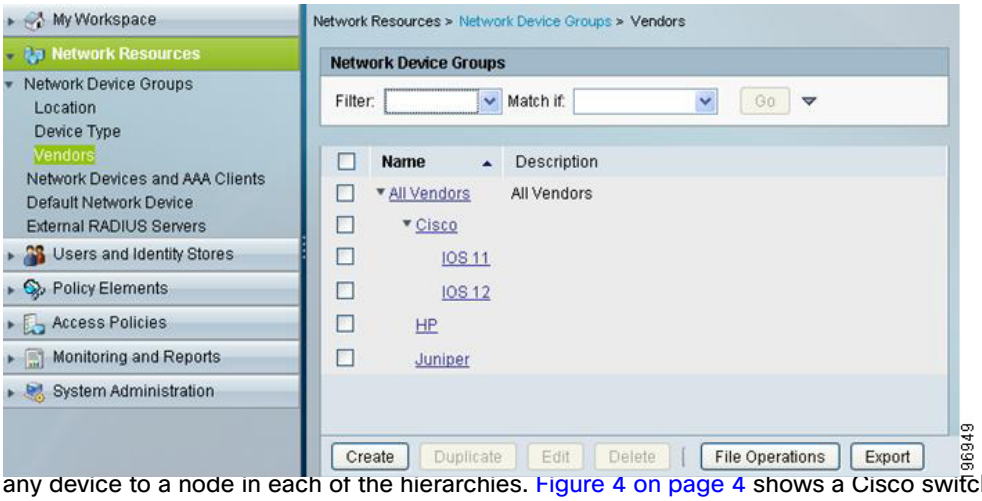
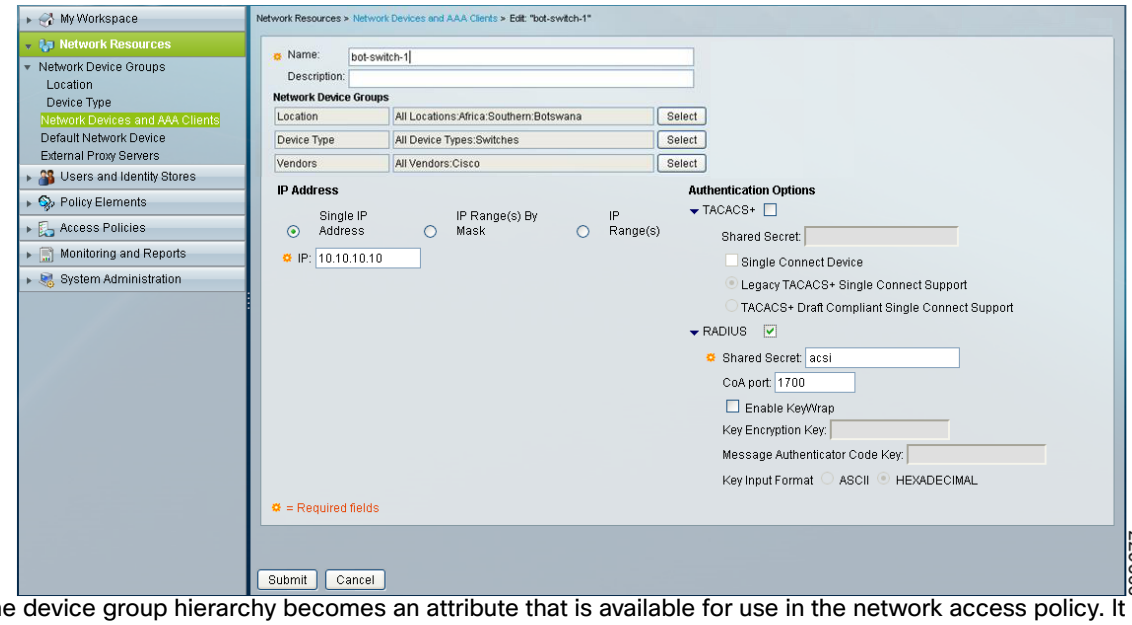


Figure 3 Network Device Group Hierarchies



You can assign any device to a node in each of the hierarchies. Figure 4 on page 4 shows a Cisco switch device that is located in Botswana.

Figure 4 An Example of a Cisco Switch Device Located in Botswana



Each node in the device group hierarchy becomes an attribute that is available for use in the network access policy. It is easy to represent the devices that represent the intersection of multiple hierarchies by referencing nodes in multiple hierarchies.

The following table shows an example of a rule that includes a condition that applies to Cisco firewalls in Namibia:

Conditions			Result
NDG:Location	NDG:Device Type	NDG:Vendors	
Is Namibia	Is Firewall	Is Cisco	...

Migration Notes

- Plan your device grouping approach to make use of the more natural hierarchical grouping in ACS 5.8.1.
- ACS 5.8.1 does not support per device group shared secrets that are available in ACS 3.x and 4.x. ACS 5.8.1 requires a shared secret to be defined for each device definition.

Network Devices

Key changes in ACS 5.8.1:

- Single device definition for a AAA client supporting both TACACS+ and RADIUS—Separate definitions are no longer needed.
- Mask-based IP address.
- A default device definition for both TACACS+ and RADIUS.

Figure 5 on page 5 shows the ACS 5.8.1 network device configuration.

Figure 5 ACS 5.8.1 Network Device Configuration

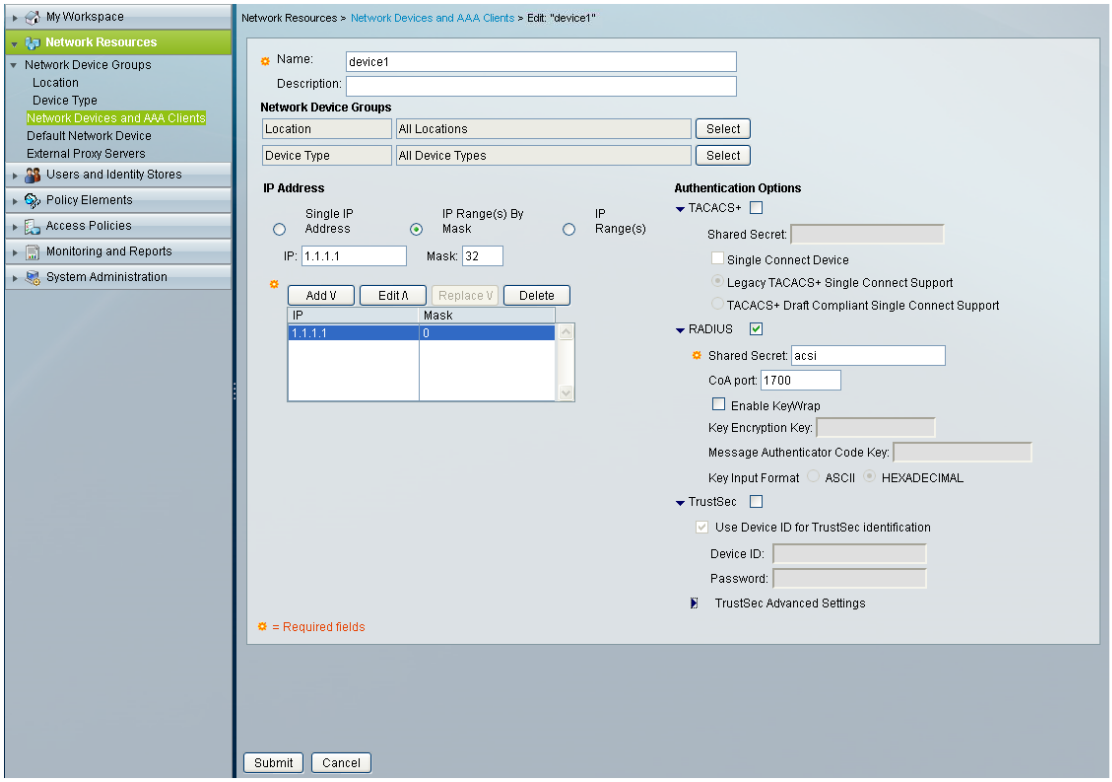
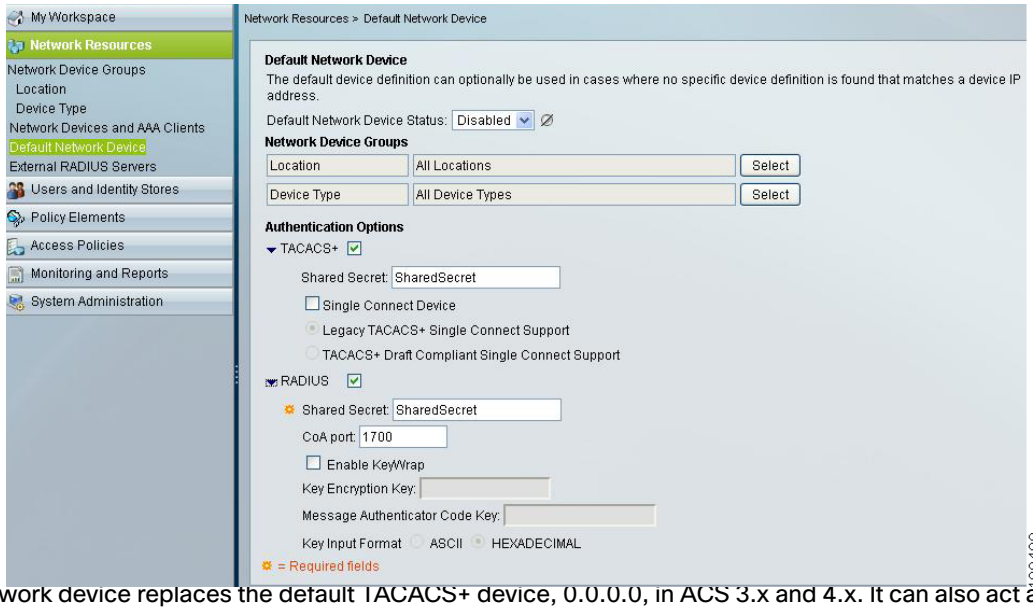


Figure 5 on page 5 shows a device definition representing any client from subnets 10.10.20.0 and 10.10.30.0. These clients can send TACACS+ or RADIUS requests as both are enabled in the device configuration.

Figure 6 on page 5 shows the default network device.

Figure 6 Default Network Device



The default network device replaces the default TACACS+ device, 0.0.0.0, in ACS 3.x and 4.x. It can also act as a default device for RADIUS requests.

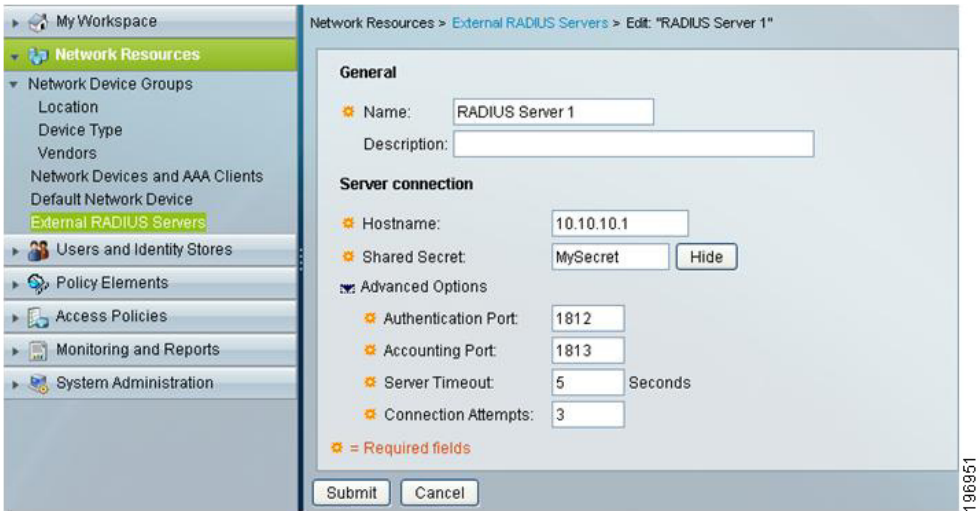
Migration Notes

- Consolidate double device definitions for TACACS+ and RADIUS in ACS 3.x and 4.x to a single device in ACS 5.8.1.
- ACS 5.8.1 uses subnet masks for IP address definitions. Map the ACS 3.x and 4.x configurations using IP ranges and wildcards to subnet mask ranges in ACS 5.8.1.
- The default network device is a useful tool to enable faster migration to ACS 5.8.1. It allows ACS 5.8.1 to start receiving AAA requests while more specific device definitions are being created.

External RADIUS Servers

The last configuration area under the Network Resources drawer is the External RADIUS Servers. This option allows you to define the RADIUS servers to which ACS will proxy. Figure 7 on page 6 shows an External RADIUS server configuration in ACS 5.8.1.

Figure 7 ACS 5.8.1 RADIUS Server Configuration



Migration Notes

- In ACS 5.8.1, there is no proxy distribution table to direct authentication requests to other AAA servers.
- For RADIUS proxy, configure a RADIUS proxy access service.

Users and Identity Stores

The following components are configured under Users and Identity Stores:

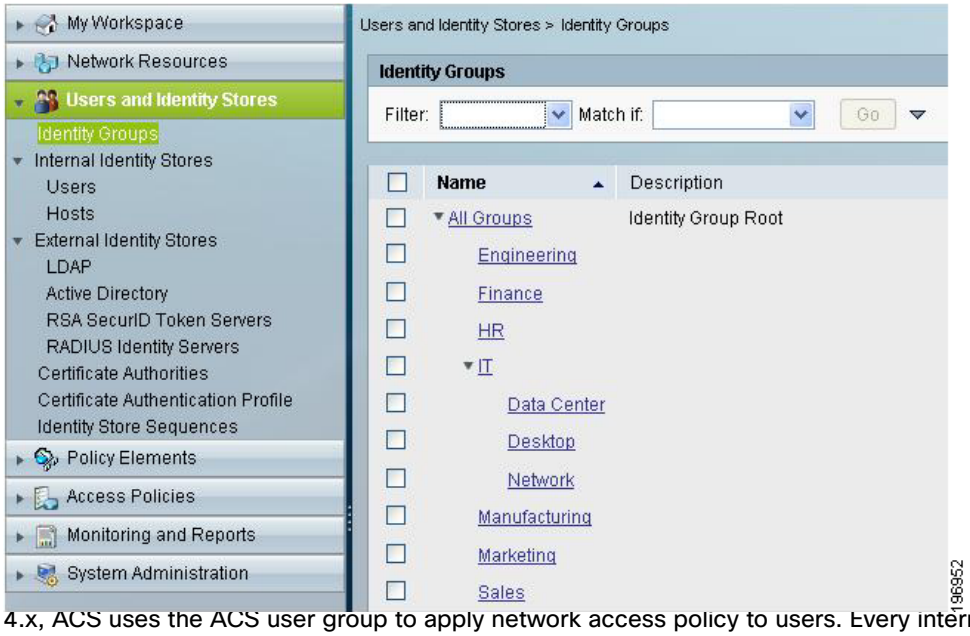
Identity Groups

Key changes in ACS 5.8.1:

- The ACS 5.8.1 identity group does not contain access policy permissions, similar to the ACS 3.x and 4.x user group.

- Users need not be associated to an ACS group.
- External groups need not be mapped to an ACS group.
- The identity group provides hierarchical grouping. Figure 8 on page 7 shows identity group hierarchies in ACS 5.8.1.

Figure 8 Identity Groups in ACS 5.8.1



In ACS 3.x and 4.x, ACS uses the ACS user group to apply network access policy to users. Every internal and external user that is authenticated by ACS is mapped to only one ACS user group. In ACS 5.8.1, network access policy is not applied through a group, but it is applied through access services.

Access services contain rules made up of conditions that govern the policy that will be applied to a user. The user's group membership is one of many attributes that can be used to compose these conditions. As policy is not applied through a group, ACS 5.8.1 does not require the group association.

In ACS 3.x and 4.x, when external identity stores such as Active Directory or LDAP directories are used for user authentication, and when the users' directory group membership is relevant to their network access, a group mapping is required to map users' external group membership to an ACS group. This is to apply the appropriate network access policy.

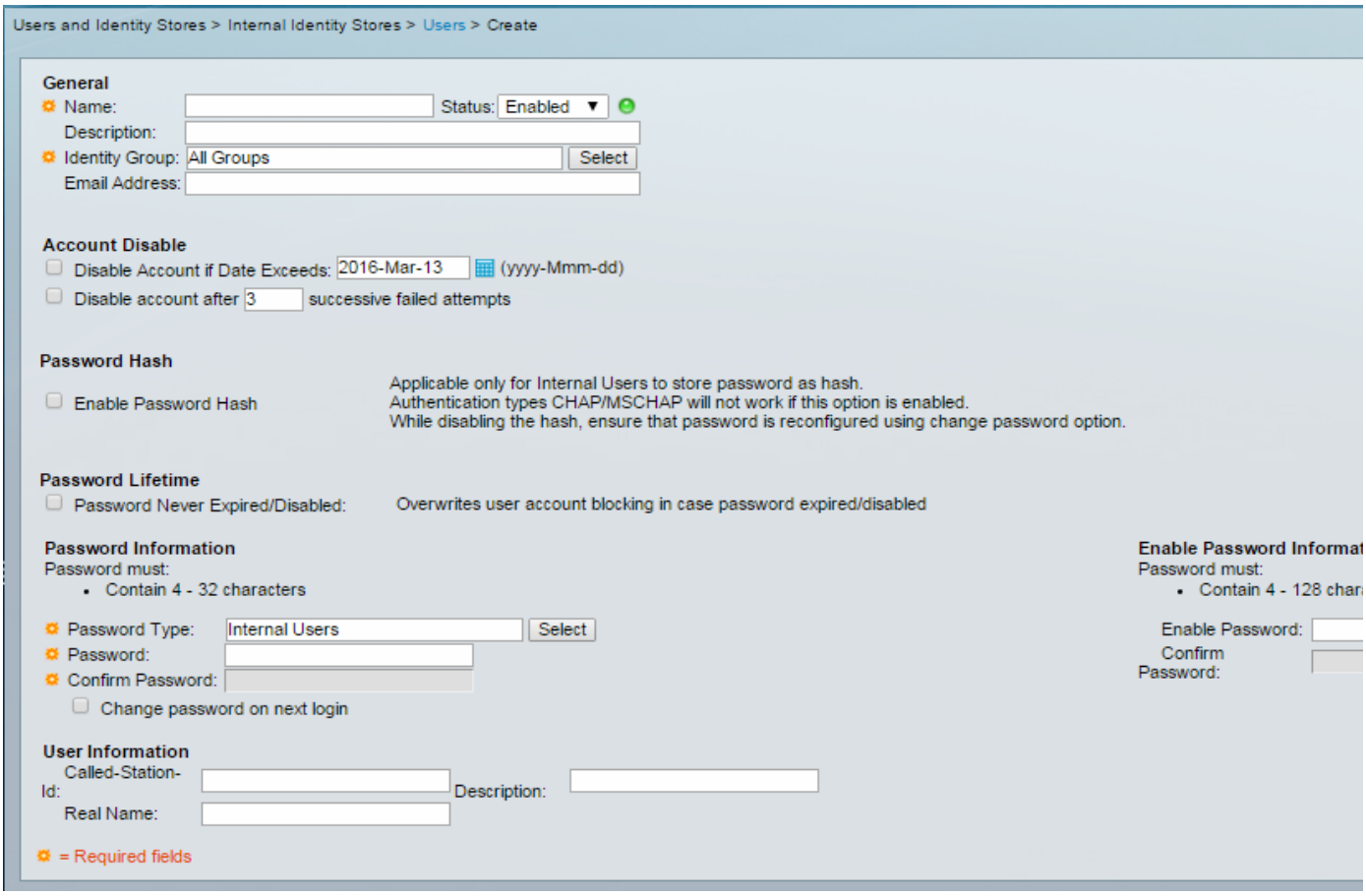
In ACS 5.8.1, external group memberships are attributes that can be used directly when you create the network access policy. Hence, you do not have to use group mapping.

Migration Notes

- Consider if you really need identity groups in ACS 5.8.1—Identity groups are needed only to maintain users within ACS.
- Take advantage of the hierarchical nature of identity groups.
- ACS 3.x and 4.x authorizations that are part of the user group are configured in the Policy Elements and Access Services drawers.
- Instead of creating combination groups that represent users who belong to multiple groups, consider specifying these different groups by extending the internal identity store schema.

  Figure 9 on page 8 shows an example of a user Fred in the IT group, who is also classified by location and whether he can access switches, firewalls, and routers.

Figure 9 Internal Identity Stores in ACS 5.8.1



Internal Identity Stores

Key changes in ACS 5.8.1:

- In addition to a user store, ACS 5.8.1 has a host store for host MAC addresses.
- Access policy permissions do not contain user records.
- Disable user accounts if the configured number of days exceed.
- Disable user accounts if the user is inactive for the specified number of days.
- Enable password hashing for users and administrators.
- User schema can be customized to add extra user fields.
- Custom user fields can store user-specific values that can be leveraged in access policies.

The ACS 5.8.1 user store is simple when compared to ACS 3.x and 4.x, because the policy components have moved to policy elements and access services in ACS 5.8.1. The ACS 5.8.1 user store is similar to an external store, because the schema can be customized to hold user-specific information such as first name, last name, location, and email.

These fields can also become attributes that can be used in access policy. For example, it is possible to use the user's location as a condition, or an IP address value as a RADIUS return value.

ACS 5.8.1 provides a separate hosts store to maintain a MAC address database for agentless host scenarios (MAC authentication bypass). Similar to the user store, custom fields can be added to host records for use in access policy.

Migration Notes

- Use identity store sequences in combination with access service identity policy to implement the ACS 3.x/4x ability to select the password authentication method from the user record.
- User password policy is a set under **System Administration > Users > Authentication Settings**.

External Identity Stores

Key changes in ACS 5.8.1:

- ACS 5.8.1 joins Active Directory (AD) directly and does not rely on a domain-joined Windows Server. ACS Remote Agent is not required.
- ODBC databases are not supported in ACS 5.8.1, but other identity stores are supported, including LDAP directories and one-time password servers.
- ACS 5.8.1 adds RADIUS Identity Store for RADIUS-based one-time passwords servers and for RADIUS proxy where proxy response attributes are required for access policy.
- ACS 5.8.1 adds the ability for AD and LDAP user attributes to be used, in addition to user group membership, in access policy.
- Identity store lists, provided by the unknown user policy in ACS 3.x and 4.x, are configured using identity store sequences in ACS 5.8.1. There is no concept of a dynamic user in ACS 5.8.1.

The External Identity Store configuration is similar to the External User Databases in ACS 3.x and 4.x. In ACS 5.8.1, external identity stores are configured and ACS communicates with them for authentication and authorization.

For Active Directory, ACS 5.8.1 joins an AD domain, rather than leveraging the underlying Windows operating system, similar to ACS 3.x and 4.x. ACS 5.8.1 relies on trust relationships between its domain and other domains to perform cross-domain authentication, as in ACS 3.x and 4.x.

You must enter the username and password credentials in the ACS 5.8.1 configuration for ACS to join and communicate with the AD domain. The credentials must have sufficient permissions to create a computer object. If a user's AD group membership and attribute information are required for access policy, they must first be selected in the AD configuration.

LDAP directory configuration is similar to ACS 3.x and 4.x. Multiple LDAP directories can be defined in ACS 5.8.1, similar to ACS 3.x and 4.x. The LDAP directory configuration allows you to select groups and attributes for use in the access policy.

For one-time password authentication, ACS 5.8.1 supports the RSA SecurID native interface by configuring RSA SecurID Token Servers. For non-RSA one-time password servers, RADIUS interaction can be configured using the RADIUS Identity Server option.

Migration Notes

Go to **System Administration > Configuration > Global System Options > RSA SecurID Prompts** to configure RSA SecurID prompts.

Certificate Authorities and Certificate Authentication Profiles

Key changes in ACS 5.8.1:

- Certificate Authentication Profiles allows you to customize the authentication for different certificate profiles.
- Identity store authorization is optional for certificate-based authentication.
- Root CA certificates must be imported.

Trusted certificate authorities are defined under the certificate configuration options in Users and Identity Stores. Here, the authentication characteristics of different certificate profiles are also specified.

Certificate authentication profiles are referenced in access service identity policy, and they allow you to specify:

- The certificate field that should be used as the principal username.
- Whether a binary comparison of the certificate should be performed.

Migration Notes

- PEM- or DER-formatted X.509 certificates can be imported to create a list of trusted CAs.
- ACS 5.8.1 does not check whether the certificate owner exists in a directory, but you can check the existence of a user attribute in an access service authorization policy.

Identity Store Sequences

Key changes in ACS 5.8.1:

- Provides the ability to specify different identity stores for authentication and authorization
- A list of identity stores can be configured for both authentication and authorization

In most of the deployments, a single identity store is used for user authentication and authorization. There are many deployments where network access relies on more than one identity store.

The identity store sequence in ACS 5.8.1 addresses this requirement and can be referenced instead of an identity store in an access service identity policy. The identity store sequence allows you to specify one list of identity servers for authentication and the other for authorization.

For example, for one-time password users, where a user must be authenticated against a one-time password server, but additional authorization information such as their group memberships, are only available in a directory.

Migration Notes

Use identity store sequences to replace the functionality provided by the unknown user policy in ACS 3.x and 4.x.

Policy Elements

The primary components of access policy are identity and authorization policies. Both these policies are represented in separate rule tables in the ACS 5.8.1 access service. Each rule in a rule table is composed of conditions and results.

In the Policy Elements configuration area, you can create conditions and customize them. Authorization results are created in this area.

The following components are configured under Policy Elements:

- Session Conditions, page 10
- Authorizations and Permissions, page 11
- Access Policies, page 11

Session Conditions

The key changes in ACS 5.8.1 are:

- Network conditions that were formerly known as Network Access Restrictions (NARs) are defined in this configuration area.
- The attributes available to create access service rule conditions include:

  - System dictionary attributes
  - RADIUS and TACACS+ attributes
  - Network Device Groups (NDGs)
  - User attributes and group memberships
  - Certificate attributes
- You can define the following additional conditions under session conditions:
  - Date and Time condition allows you to define date and time ranges.
  - Custom condition allows existing attributes to be renamed to simplify policy representation.
  - Network condition allows you to define ACS 3.x and 4.x equivalent NARs.

Migration Notes

Access policy conditions configured in the ACS 3.x and 4.x user, user group, or shared profile components, should be configured under session conditions.

Authorizations and Permissions

The key changes in ACS 5.8.1 are:

- All access policy authorization must be defined in this configuration area.
- The various types of network authorizations include:
  - Device administration authorization using TACACS+ shell privileges and command sets.
  - Network access authorization using RADIUS attributes.
  - Downloadable ACLs, typically used for remote access authorization.

Migration Notes

Access policy authorizations that were formerly configured in the ACS 3.x and 4.x user, user group, or shared profile components, should be configured under Authorizations and Permissions.

Access Policies

The key changes in ACS 5.8.1 are:

- Access policies are the core of network access policy in ACS 5.8.1.
- All network access policy for RADIUS and TACACS+ authentication and authorization requests is configured here.

All authentication and authorization requests in ACS 5.8.1 must be processed by an access service. An access service defines the authentication and authorization policy. ACS 5.8.1 supports multiple access services for different network access scenarios.

Access services provide a way to logically separate different network access policies. For example, an organization may implement one access service for device administration policy, and another access service for remote VPN access.

Additional access services may also be configured to simplify the policy within any one access service. For example, instead of configuring one access service to address all 802.1X network access, you can use multiple access services to address policy for wired, wireless, machine, and host 802.1X access.

In addition to access services, you must also configure the service selection policy. The service selection policy instructs ACS on how to direct authentication and authorization requests to the appropriate access service.

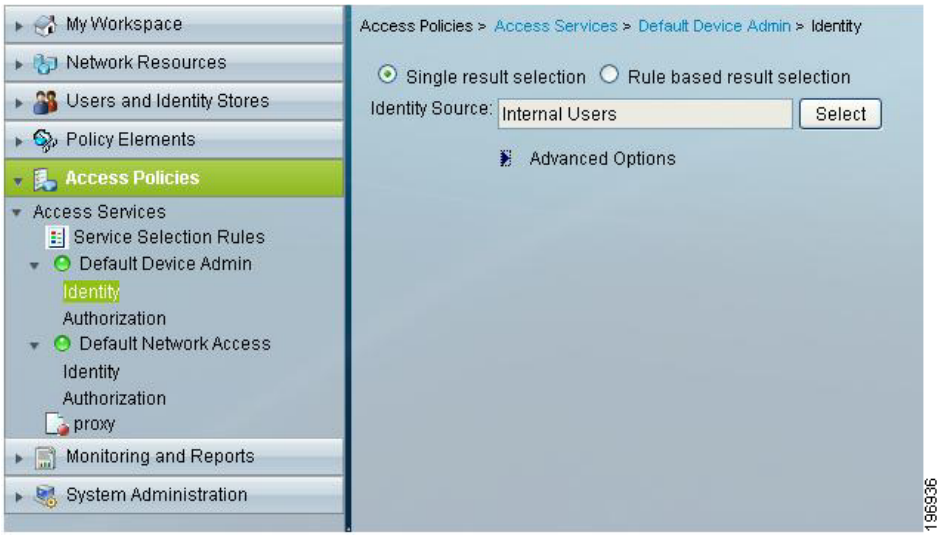
For more information on the Access Policies, see the *User Guide for Cisco Secure Access Control System*.

Migration Notes

- For device administration scenarios using TACACS+, you can update the preconfigured default device admin access service.
  - Modify the identity policy to use another identity store, such as one-time passwords, if the default setting of internal users is not appropriate.
  - Select an identity store sequence, as shown in Figure 10 on page 12, if more than one identity store is required to authenticate and authorize users.

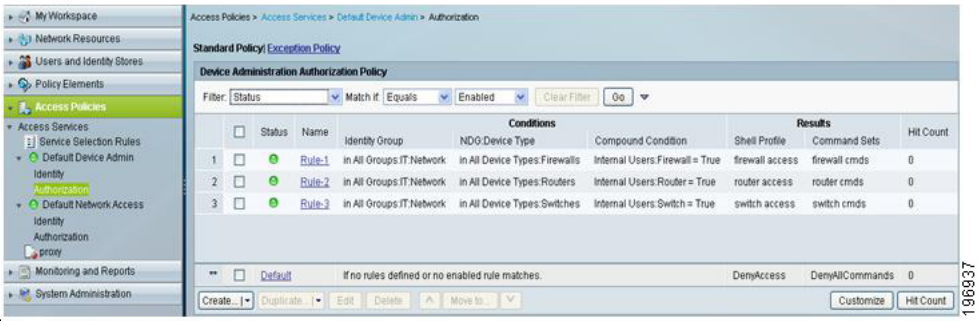
  For example, users may be authenticated to a one-time password server, but the ACS internal user store may be required to retrieve user attributes for authorization. In some cases, ACS may need to check both the ACS internal user store and active directory, to locate a user for authentication.

Figure 10 Identity Store Sequence



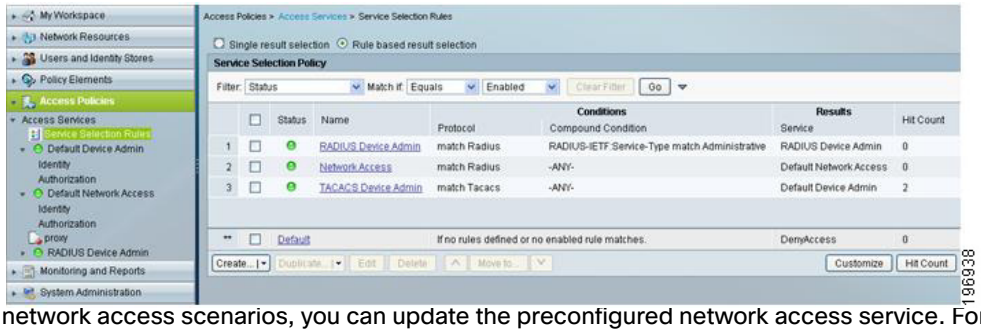
- Utilize the new user and network device groupings to create authorization policy, as shown in Figure 11 on page 12.

Figure 11 Authorization Policy



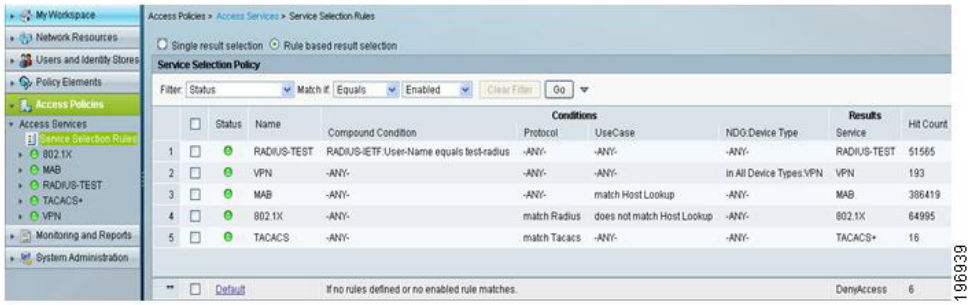
- For RADIUS-based device administration, create a separate access service, and differentiate these authentication and authorization requests from network access services, in the service selection policy. Figure 12 on page 13 shows the service selection policy.

Figure 12 Service Selection Policy



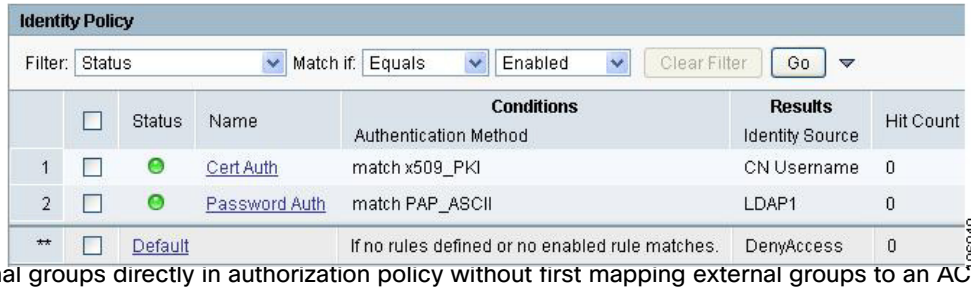
- For simple network access scenarios, you can update the preconfigured network access service. For more complex network access scenarios, introduce additional access services, as shown in Figure 13 on page 13.

Figure 13 Network Access Service Rules



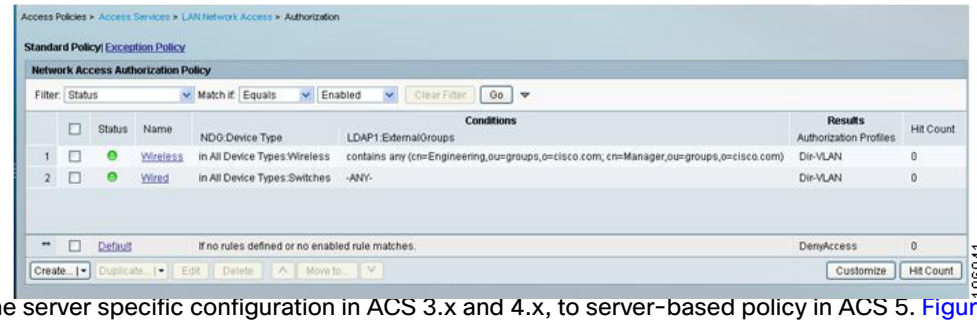
- When creating an access service that addresses both certificate and password-based authentication. For example, certificate-based machine authentication, and password-based user authentication, a rules-based identity policy is required, as in Figure 14 on page 13.

Figure 14 Rules-Based Identity Policy in ACS 5.8.1



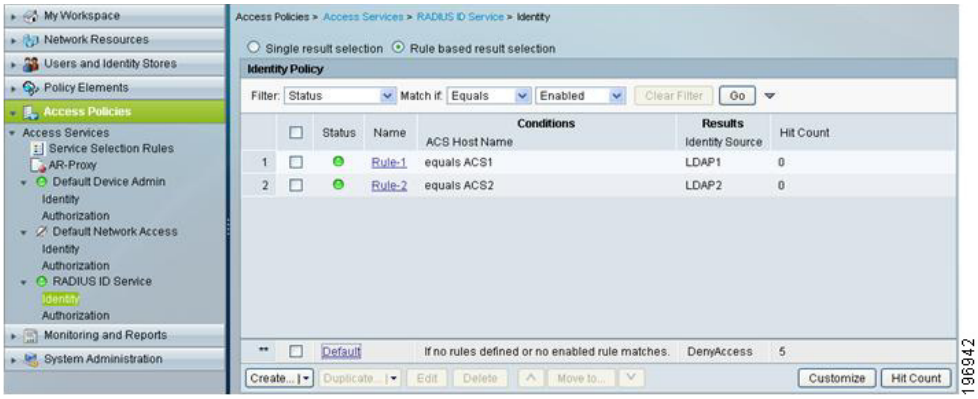
- Use external groups directly in authorization policy without first mapping external groups to an ACS group.

Figure 15 Using External Groups Directly in Authorization Policy



- Convert the server specific configuration in ACS 3.x and 4.x, to server-based policy in ACS 5. Figure 16 on page 14 shows how to use the system condition, and ACS host name to direct requests to different LDAP directories.

Figure 16 System Condition and ACS Host Name



System Administration

The key changes in ACS 5.8.1 are that ACS 5.8.1 provides the following configuration areas for system administration tasks:

- Administrators, page 14
- Users, page 14
- Operations, page 14
- Configuration, page 14
- Downloads, page 15

Administrators

The key changes in ACS 5.8.1 are that ACS administrators can be assigned up to ten predefined roles that govern an administrator's permissions.

Users

The key changes in ACS 5.8.1 are:

- Enhanced password policy can be applied to ACS internal users. This includes:
  - Increased password complexity rules
  - Password history
- Password lifetime policy is based on age only.

Operations

The key changes in ACS 5.8.1 are:

- Ability to assign ACS server roles to the primary or secondary servers.
- Ability to perform local and global software updates.

Configuration

The key changes in ACS 5.8.1 are:

- This configuration area addresses authentication protocol settings, AAA dictionaries, internal user schema changes, ACS certificate management, logging settings, and ACS license management. This includes:
  - Editable AAA protocol dictionaries
  - Editable internal user/host schema
- Ability to assign an ACS server as a log collector for ACS View.

Downloads

The key changes in ACS 5.8.1 are:

- ACS 5.8.1 provides a migration tool to help migrate some parts of ACS 4.2 configuration.
- A web services interface to build a password-change application for ACS internal users.

The configuration area contains links to download the ACS 5.8.1 Migration Utility and web services files to build a change-password application.

ACS 5.8.1 Configuration