ACS 4.x to 5.x Migration

Aruna Yerragudi, Technical Marketing

Migration Overview

- What is migration?
  - Process of moving data from previous ACS versions
  - Migration Utility provides tools to import key data elements
  - Not a seamless process and need to manually setup policies
- Why is this a migration and not an upgrade?
  - ACS 5.x introduces a new rule-based, attribute-driven policy model
  - In 4.x, policy and authentication information are stored in user and user group records

The New Rules-based Policy Model

ACS 4.x: Group-Based Policy Model

Group-based policy

User is authenticated & associated to a group

- Authorization based on static permissions and restrictions for the user's group

User subjected to SAME restrictions and gets SAME permissions ALWAYS

User Groups

NetAdmin Group

Permissions – Full Access
Restrictions – None

Employee Group

Permissions – Employee_VLAN
Restrictions – None

Guest Group

Permissions – Guest_VLAN
Restrictions – Time_of_Day

- Works well if Identity is the dominant or only condition
- Does not work well for complex authorization policies based on dynamic conditions
  - Employee gets full access when on-site & restricted access when coming in remotely

Group-based Model Forces Group Proliferation

- Example: 7 groups required for a 3 condition scenario:

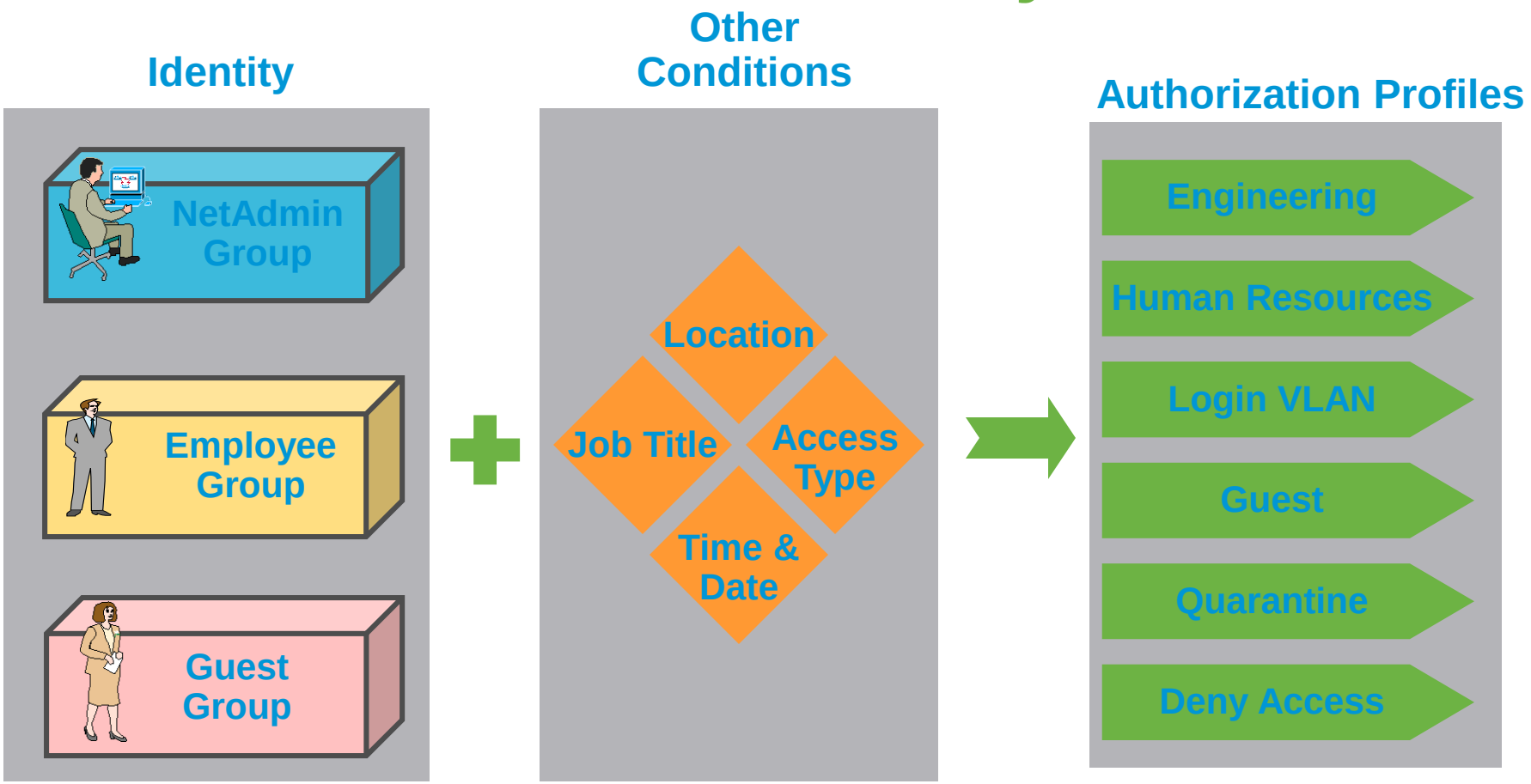
Wired users	**Wired+Wireless**	**Wired+Wireless+ VPN**
Wireless users	**Wireless+VPN**	
VPN users	**Wired+VPN**	

- 2^n - 1 groups required (n is the number of policy conditions)

n	2	3	4	5	6
2^n - 1	3	7	15	31	63

- Potentially update 2^{n-1} groups for a single condition authorization change. (4 groups edits in the above example)

ACS 5 : Rules-Based Policy Model



Policy Rules

Policy Elements

CONDITIONS		RESULT
ID GROUP	LOCATION	AZN PROFILE
ENG	SJ_CAMPUS	SJ_ENG
ENG	RTP_CAMPUS	RTP_ENG
ENG	EXTERNAL	EXT
IF NO MATCH		DENY ACCESS

Identity is decoupled from permissions
Authorization based on identity and conditions specified as policy rules

- IF <condition(s)> THEN <permission>

Policy Simplification

- 7 groups in the group-based model:

Wired users	**Wired+Wireless**	**Wired+Wireless+ VPN**
Wireless users	**Wireless+VPN**	
VPN users	**Wired+VPN**	

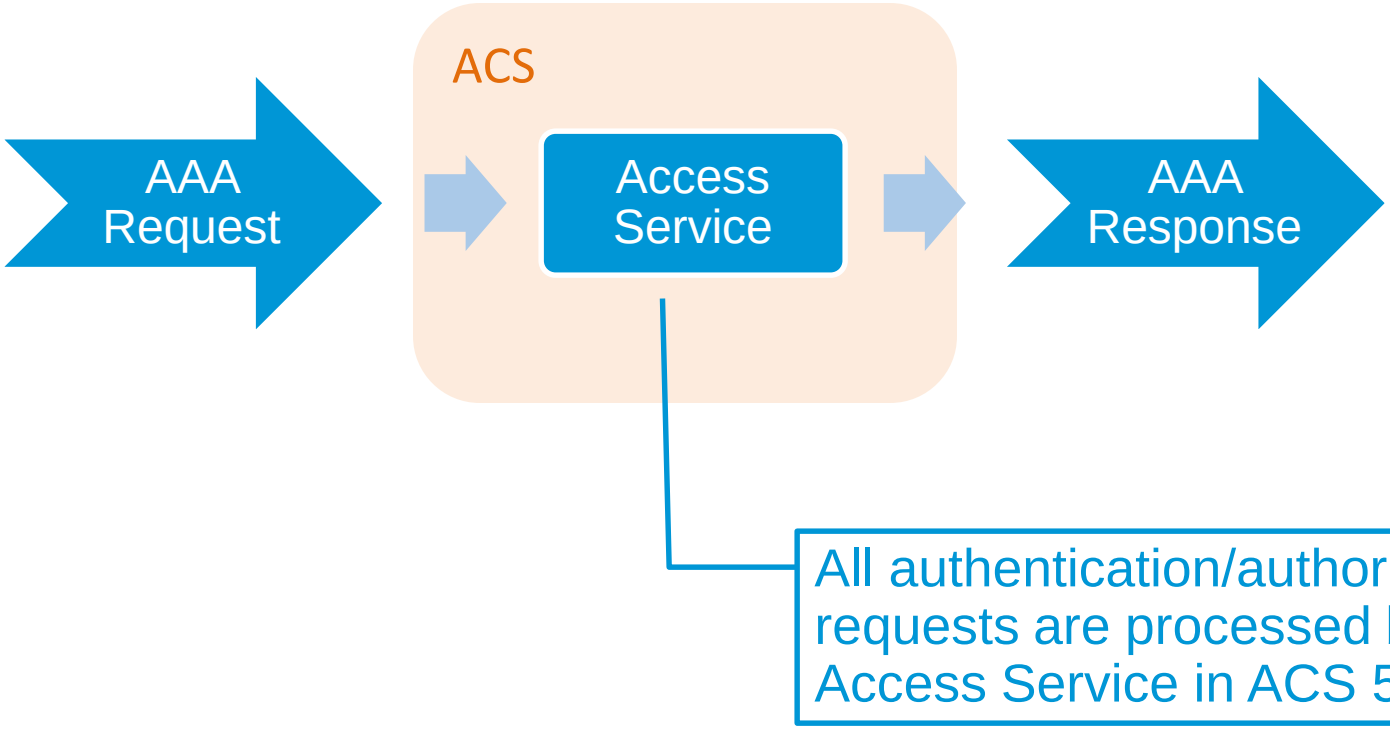
- Become 3 rules in the rules-based model:

ID Group	Access Type	Authorization
Wired users	Wired	Wired access
Wireless users	Wireless	Wireless access
VPN users	VPN	VPN access

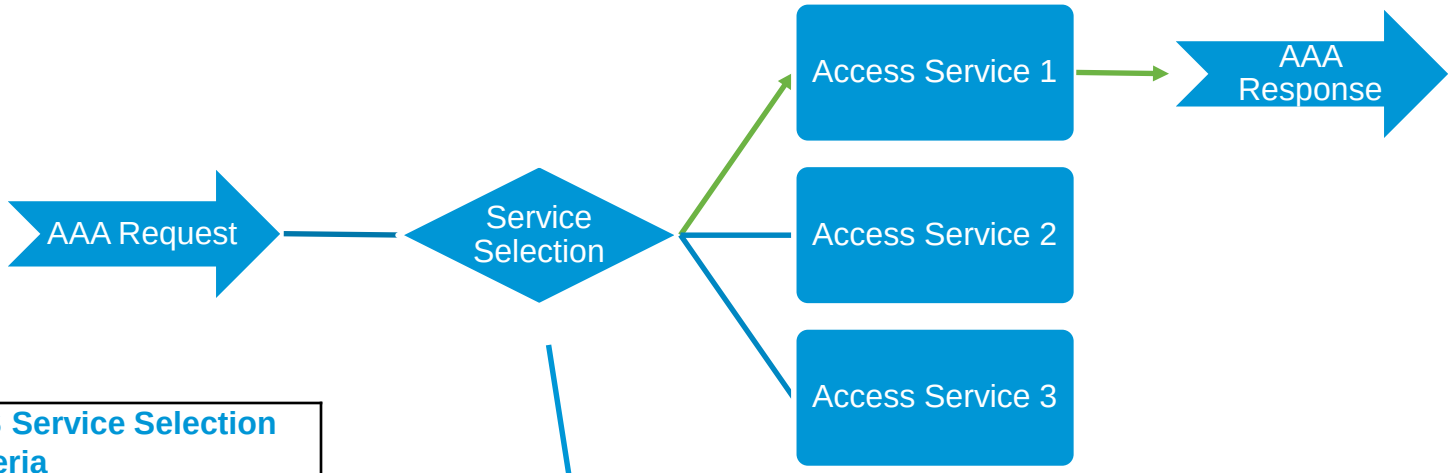
Flexible Policy Conditions

- Network information – AAA protocol, AAA client, network device group
- AAA information – EAP type, MAC address, other AAA attributes
- Certificate attributes
- Identity store user attributes and group memberships
  - ACS internal store, Active Directory, LDAP directories

Access Services Implement ACS Policy



ACS Service Selection Policy



ACS Service Selection Criteria
AAA protocol
Network device group
ACS server
Request attributes
Date and time
AAA client

Service Selection policy defines to which Access Service ACS should direct authentication requests

Access Service Components

- Identity Policy

  Selects the Identity Store (or stores) to be used for authentication and retrieval of identity attributes

- Authorization Policy

  This is the heart of ACS, where all collected attributes are evaluated to arrive at an authorization policy decision

Identity Policy

- Policy to select identity stores that are used to authenticate and retrieve attributes/group info
- Flexibility in selection of identity store
  - Static
    - “Always use LDAP”
  - Conditional -
    - “Use CORP_AD if MSCHAPv2 is used”

Authentication Method	
X509 Certificate	Certificate Profile
MSCHAPv2	CORP_AD
If no match	Deny Access

Authorization Policy

- First match (permissions cannot be merged)
- Discrete columns per condition element
- Authorization profiles may be combined in Rule results
  - Conflict resolution via precedence order
  - Allows “hierarchy” of authorization profiles, reduces proliferation of individual profiles
- Default rule (If no match found)

ID Group	Location	Access Type	Time & Date	Compliance	Azn Profile
ENGR	-	-	-	Compliant	ENG
ENGR	-	-	-	Not Compliant	PUB, ENG
CONT	CAMPUS	WIRED	DAY	Compliant	CONT
CONT	CAMPUS	WIRELESS	DAY	Compliant	CONT_WLAN
PRINTERS	CAMPUS	WIRED	-	-	PTR
DEFAULT (If no match found)					QUAR

Configuration Migration Techniques

Configuration Migration Approach

- Understand the new ACS 5 configuration and policy model
- Design the ACS 5.x Deployment
  - What are the requirements?
  - Is there a consolidation of multiple infrastructures?
  - How will changes be maintained?
  - How will these influence how NDGs, Identity Stores, and Policies created in ACS 5.x?
- To create ACS 5 primary server configuration, use a combination of:
  - Manual configuration
  - Import tool
  - Migration tool

Configuration Migration Methods
Manual Configuration

- Required for all migrations
  - ACS 5 has a new configuration model that doesn't translate directly from previous versions.
  - Migration and import tools will help to transfer some configuration areas, but other areas will require manual re-configuration
- Good option for:
  - Small configurations
  - Configurations that don't use internal users
  - Every migration

Configuration Migration Methods
Import Tools

- ACS 5.x provides csv file-based configuration update for some configuration areas
- Supported config areas

  Users, hosts, network devices, identity groups, NDGs, downloadable ACLs, command sets
- Good option for:

  Config areas that can be created in text files

  Pre-4.x configs that can't be upgraded easily

Configuration Migration Methods
Migration Tool

- A utility that analyzes a 4.x configuration, provides an analysis report, and can convert and push configuration to an ACS 5 server
- Supported config areas

  Users/user groups, devices/device groups, command sets, T+ shell exec attrs, RACs, FAST master key & auth ID
- Prerequisites

  Source configuration on ACS 4.x

  ACS 4.x (Windows) lab machine (to run tool)
- Good option:

  For 4.x migrations with large internal user or device configs

Server Migration Strategy

- Establish a primary ACS 5 configuration for testing and then phased production roll out
- Maintain existing ACS deployment as a fall-back contingency
- In most cases, a one-for-one server replacement is appropriate
- Understand the peak authentications rates
- Use ACS View System Health alarms to monitor server utilization

Configuration Migration Methods Summary

Approach	Notes
Manual configuration	Necessary for areas such as initial setup tasks and config areas that don't translate easily from 3.x/4.x. A useful approach for learning ACS 5 and for migrating smaller configurations.
Import tools	Good option for migrating large configuration areas that are available in a CSV file. Easy to manipulate data
Migration tool	Can analyze 4.1.4/4.2 configs, analyze, report on, and migrate many configuration areas. Provides config analysis and transfers config directly to ACS 5. Requires ACS 4.x Windows lab machine to run the tool.

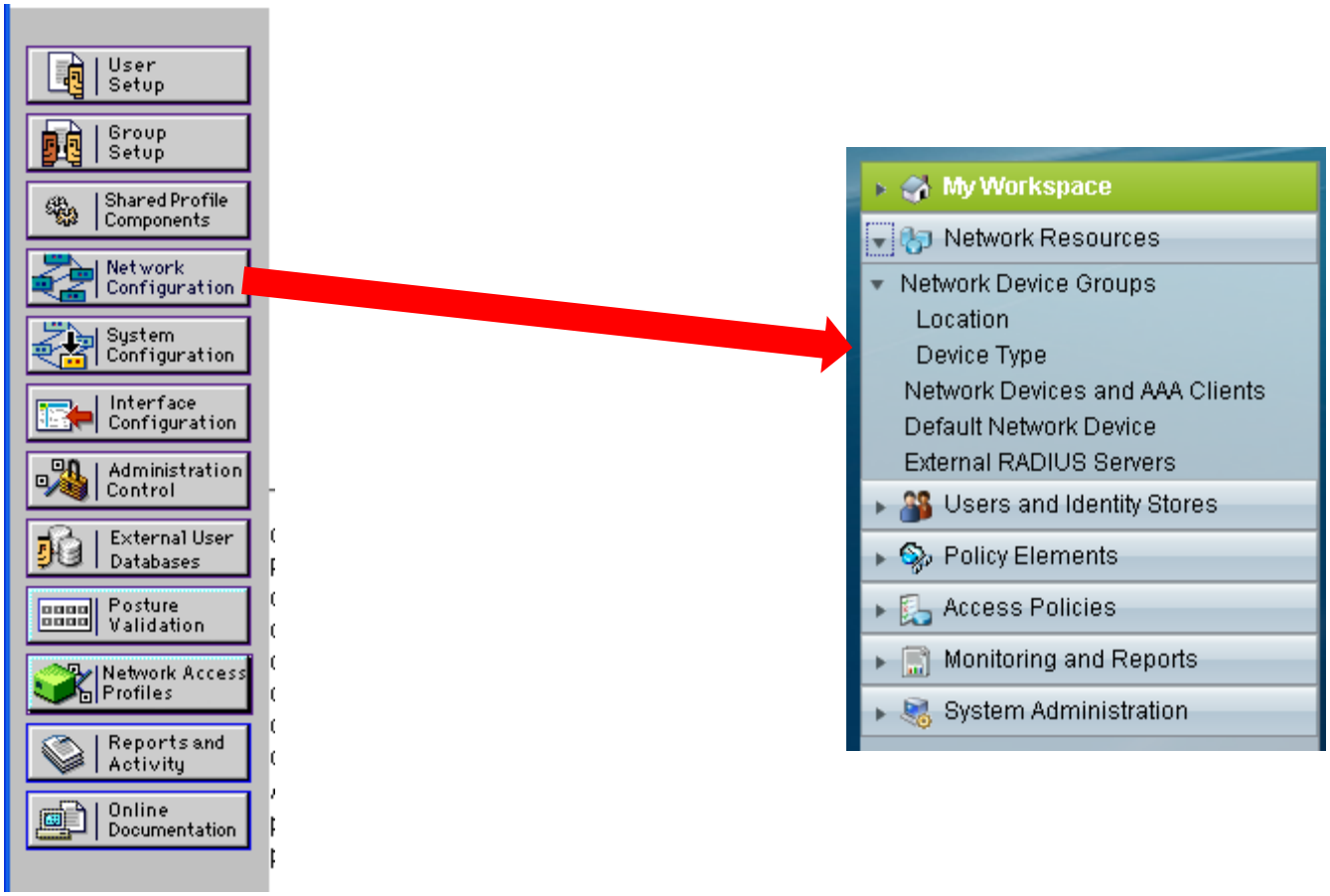
ACS 5 Policy Configuration Overview

Access Service building blocks

Service Selection policy and Access Service definition

Network Resource Configuration

Network Resources



ACS 4

ACS 5

Network Resources

Key Changes

- ACS 5 supports a single device definition for the same RADIUS and TACACS+ client
- Change from flat, exclusive, device grouping, to overlapping, multiple, hierarchical grouping
- ACS 5.x supports a Default Network Device

Powerful ACS 5 Device Grouping

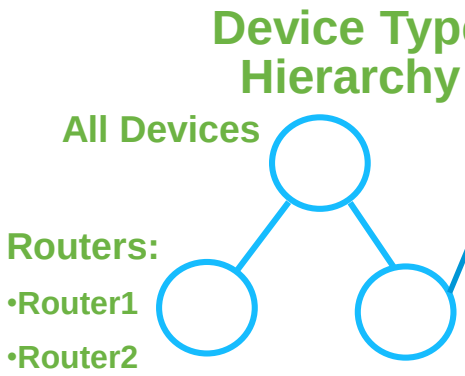
Africa-Southern-SouthAfrica-Firewalls
Africa-Southern-SouthAfrica-Switches
Africa-Southern-SouthAfrica-Routers
Africa-Southern-Namibia-Firewalls
Africa-Southern-Namibia-Switches
Africa-Southern-Namibia-Routers
Africa-Southern-Botswana-Firewalls
Africa-Southern-Botswana-Switches
Africa-Southern-Botswana-Routers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

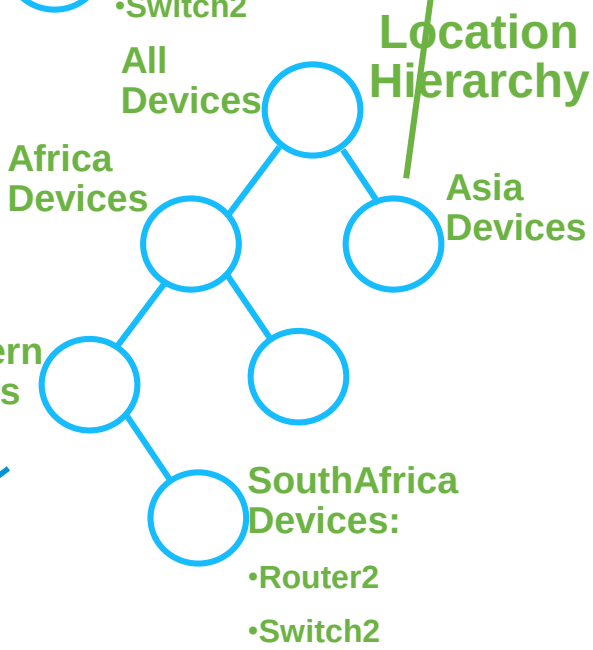
Flat ACS 4 device grouping

Single attribute to reference all Southern African devices

ACS 5 multiple device hierarchies

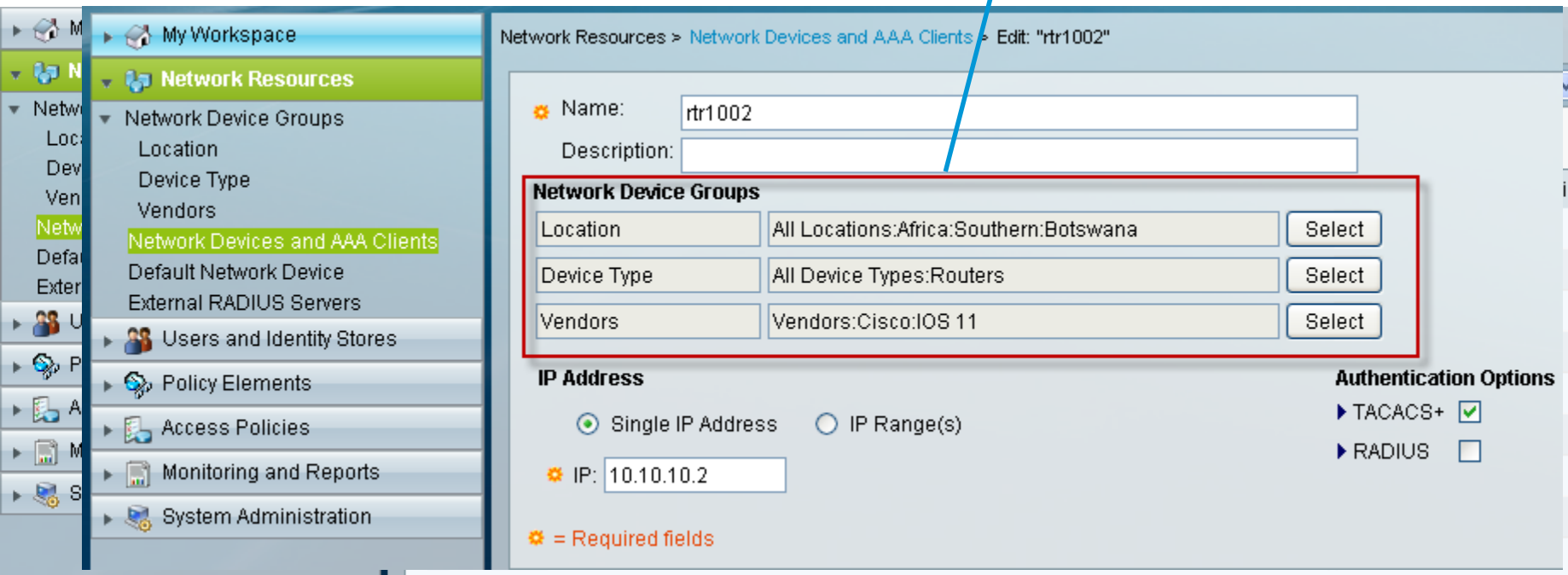
Combine nodes in policy to reference device intersection

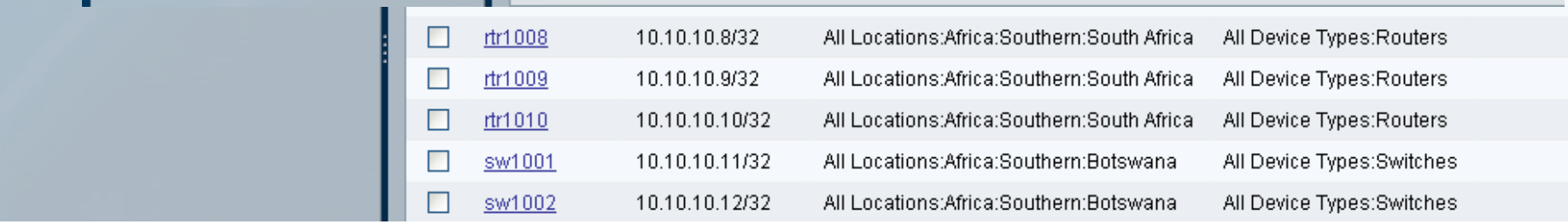




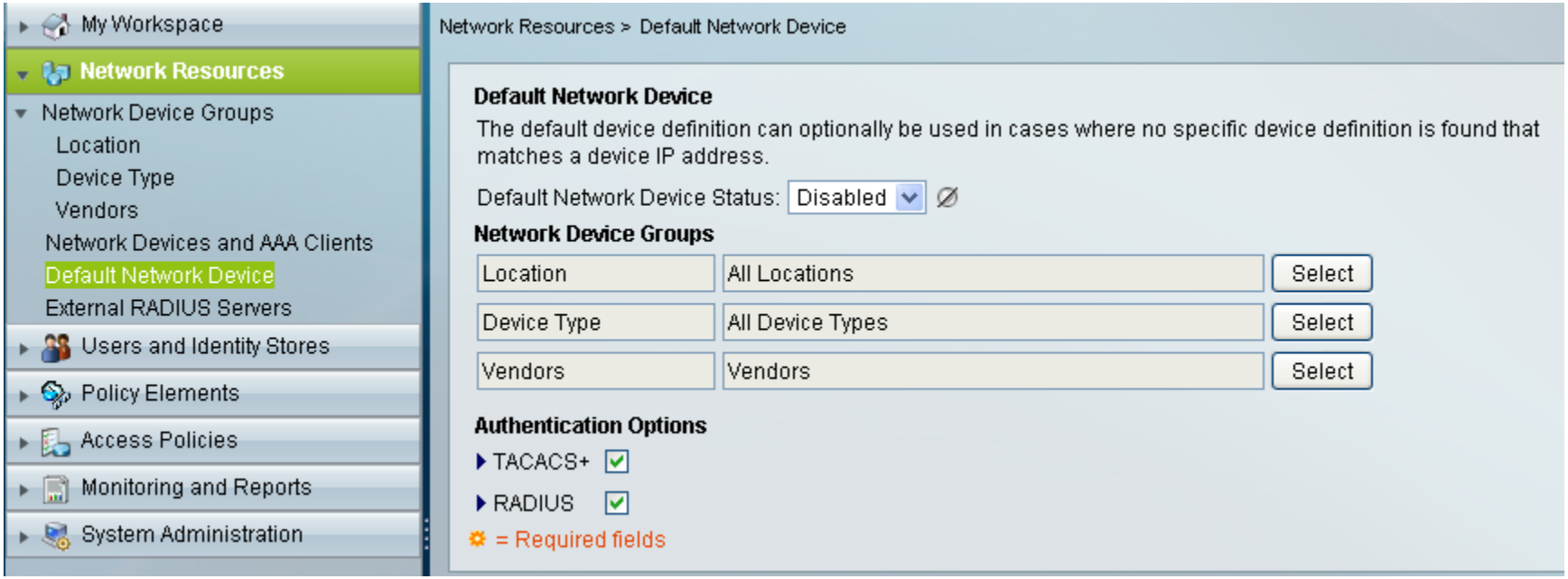
Network Devices With Multiple Group Assignment

Adding devices to device groups





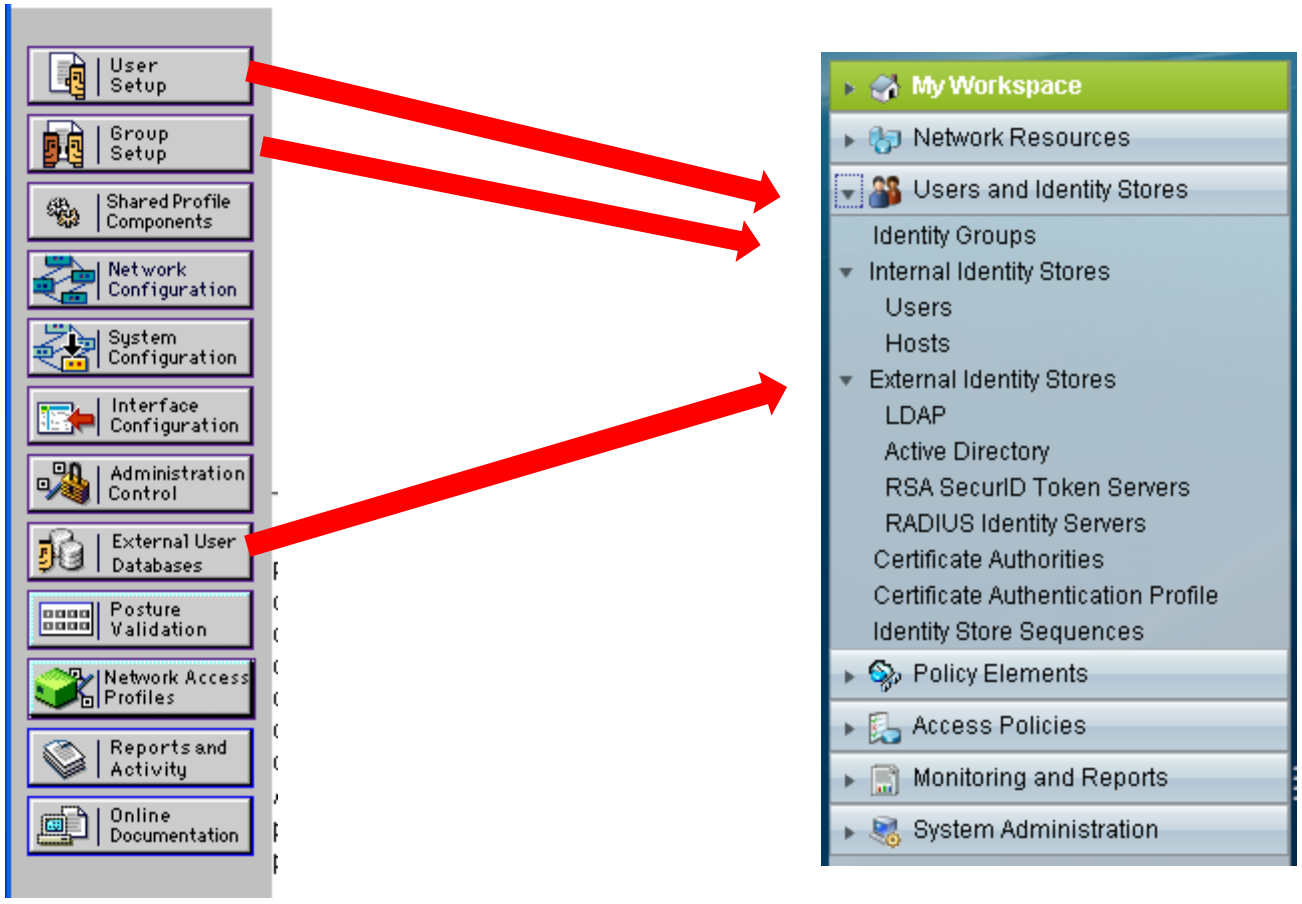
Default Network Device



ACS will use the Default Network Device for AAA clients that haven't been defined in ACS

User and Identity Store Configuration

Users and Identity Stores



ACS 4

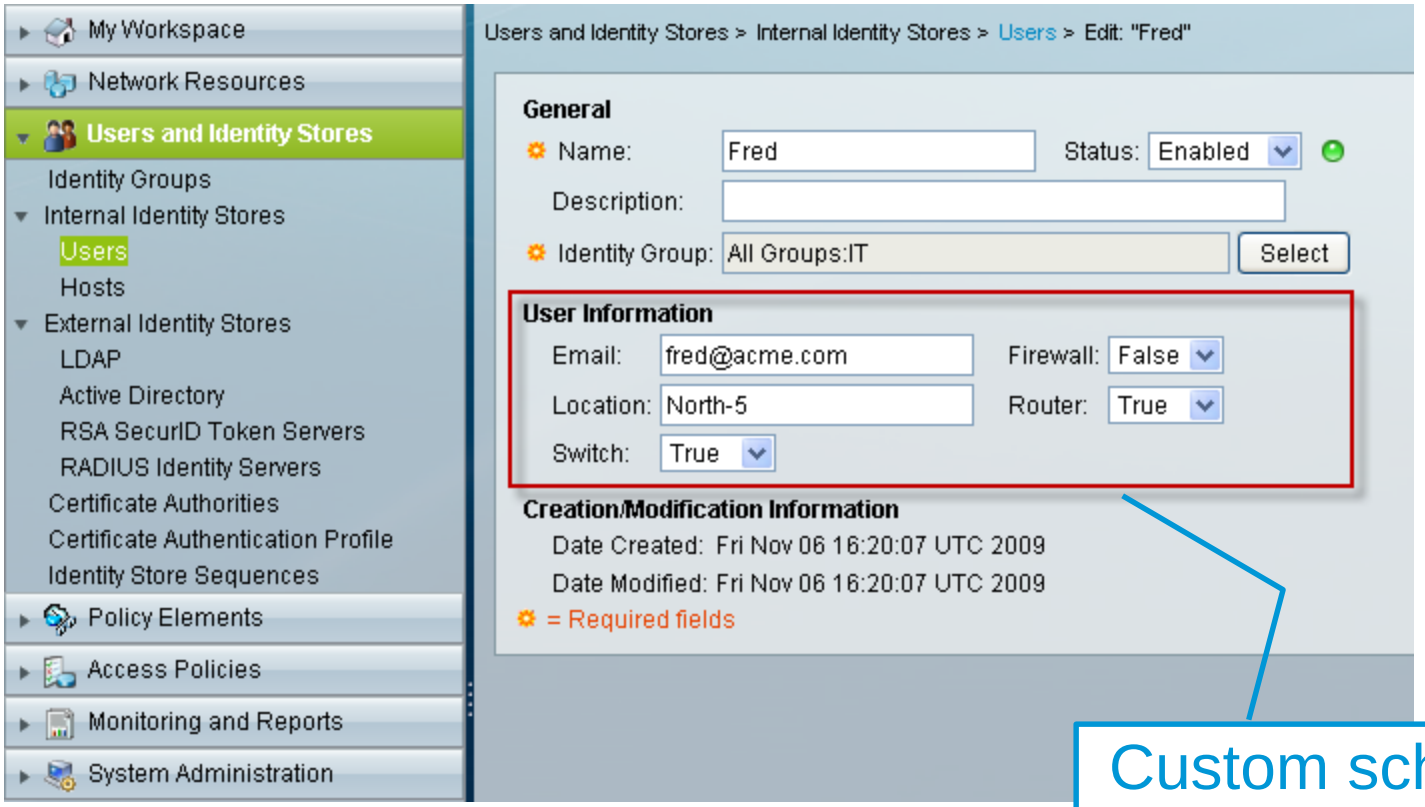
ACS 5

Users and Identity Stores

Key Changes

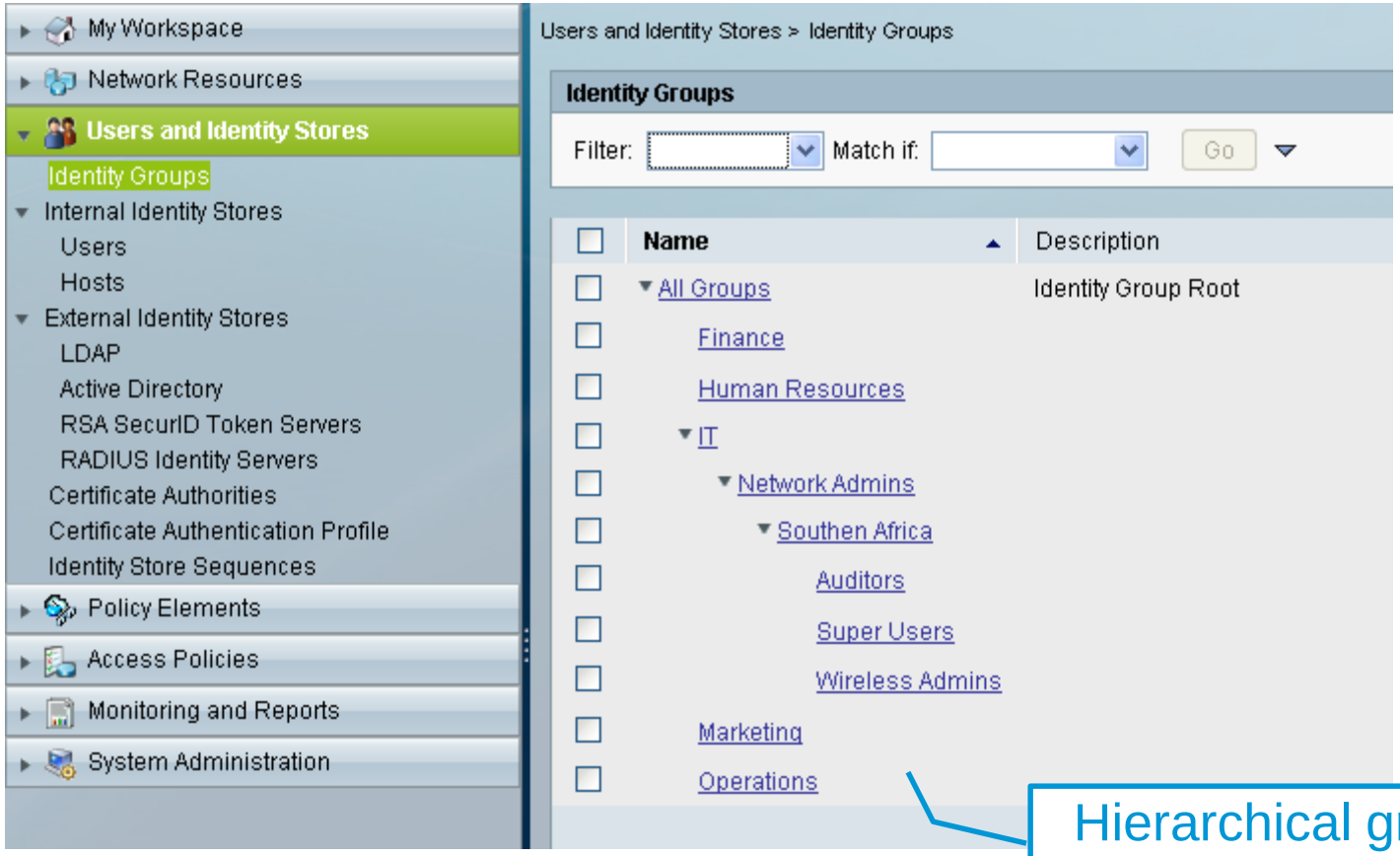
- ACS internal users and user-groups are no longer containers of permissions and no longer define access policy
  - All access policy is rules-based and attribute-driven
- ACS no longer requires a user to be assigned to a user-group
- External user-groups are attributes that can be used directly in access policy – group mapping is no longer required
- ACS 5.x internal users provide extensible schema to define user-level attributes that can be used in access policy rules
- ACS 5 internal ‘groups’ are described in a hierarchical tree where each node is a group attribute that can be assigned to an internal user, and therefore be referenced in access policy
- Identity Store Sequences are used to combine different identity stores for use in a single authentication/authorization request

Extensible ACS User Schema



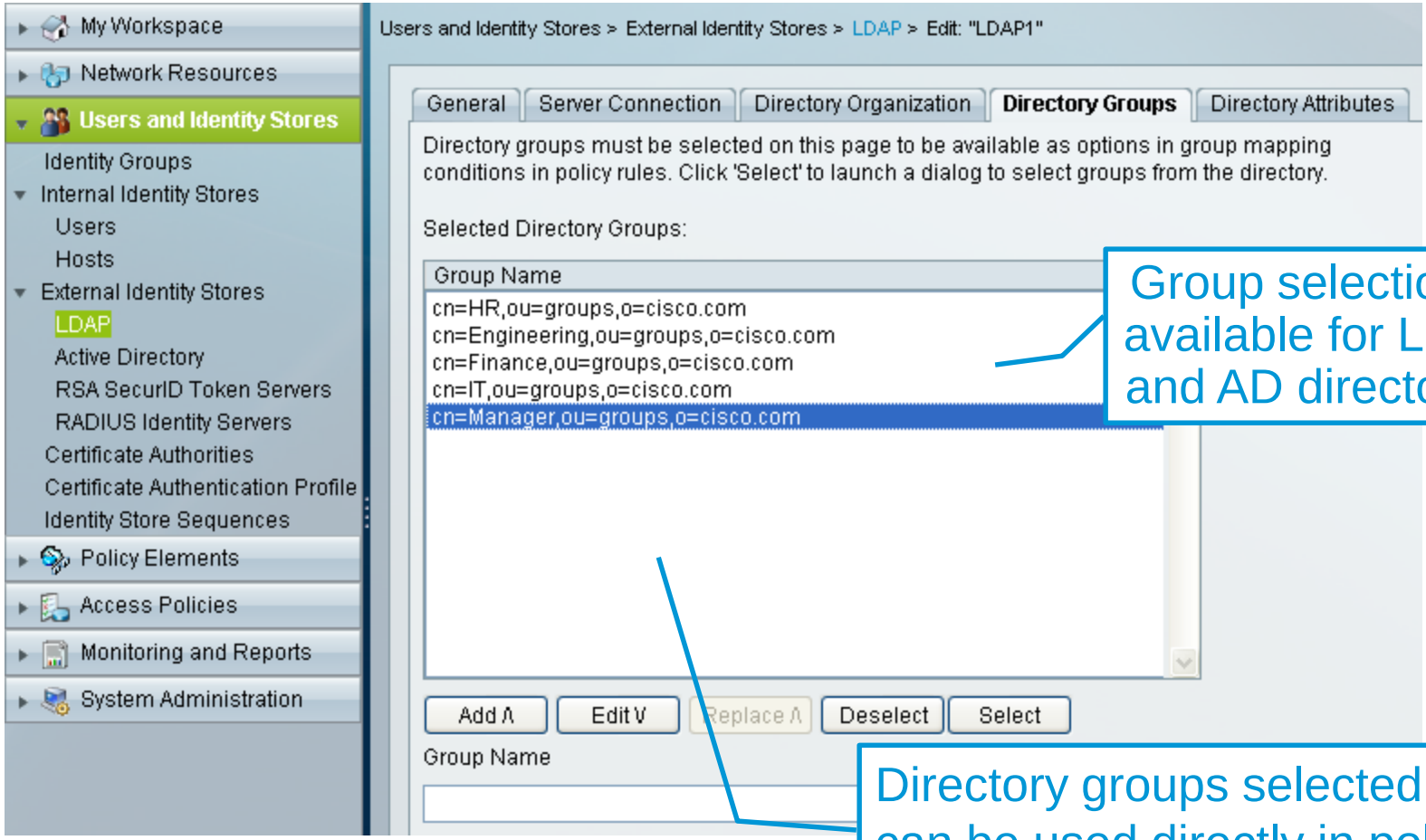
Custom schema attributes are available as policy attributes

Hierarchical User Grouping

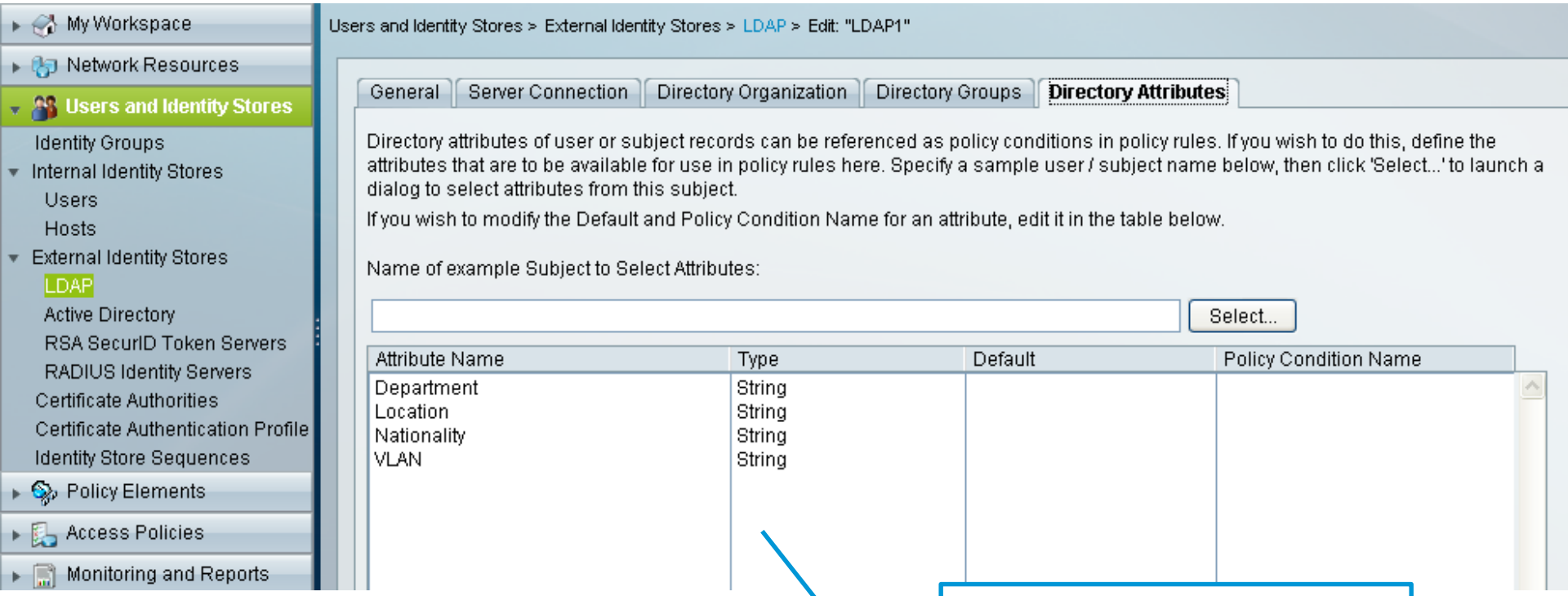


Hierarchical grouping for ACS internal users - also available in policy

External Groups - Mapping Not Required

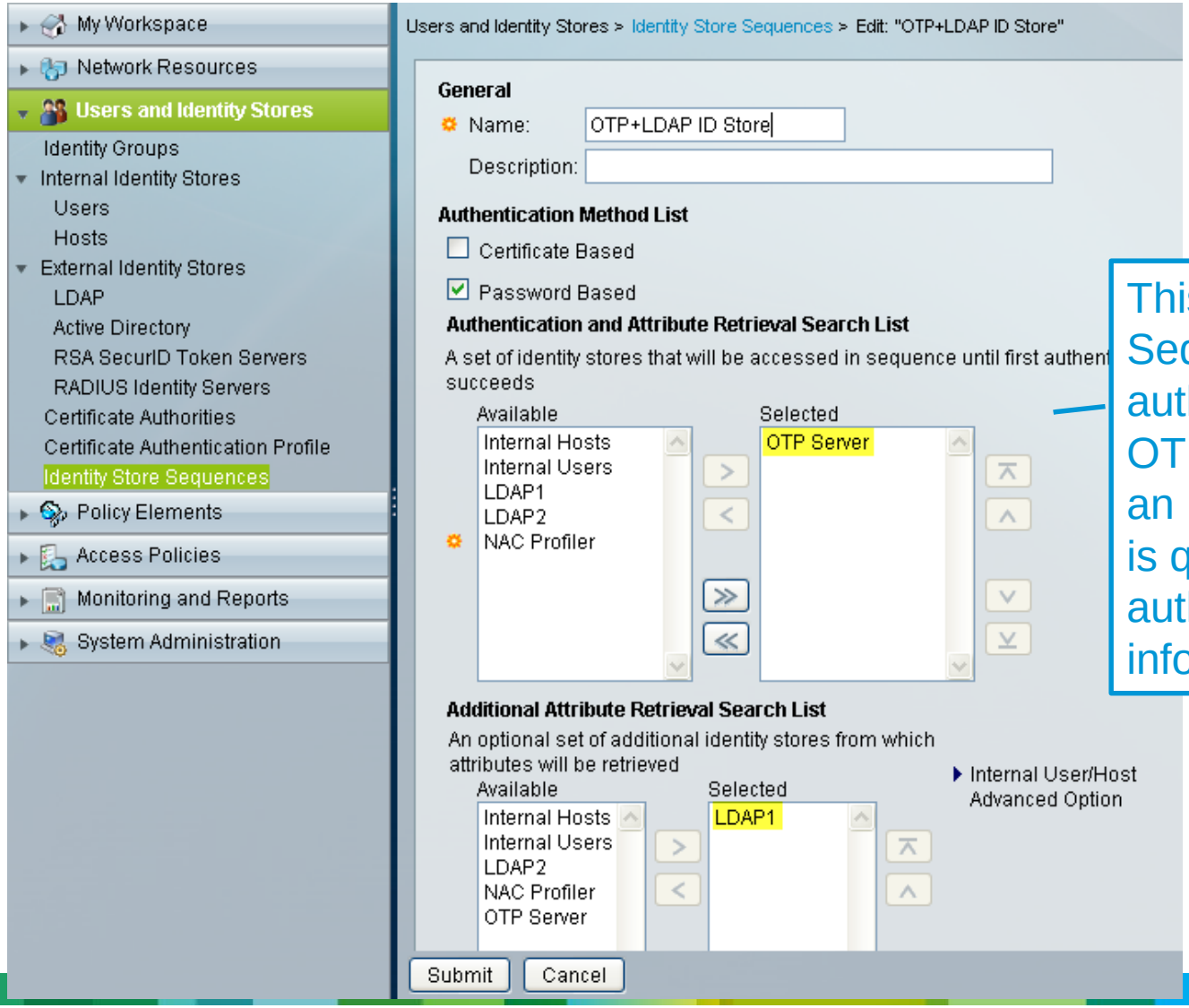


Directory Attributes



Directory attributes specified here become available as conditions and result values in access policy

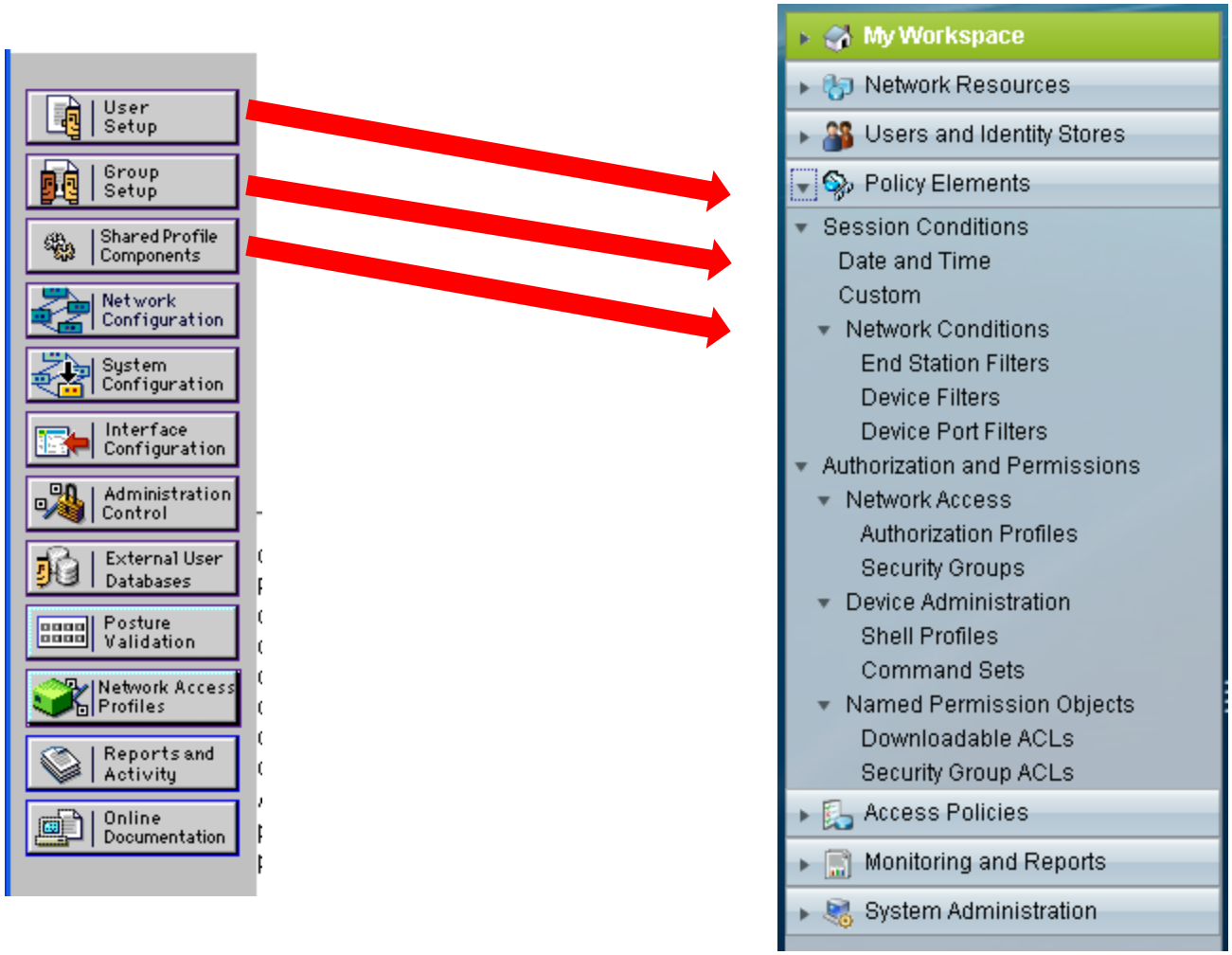
Different Identity Stores For Authentication And Authorization



This Identity Store Sequence allows authentication to an OTP server, while an LDAP directory is queried for authorization information

Policy Element Configuration

Policy Elements



ACS 4

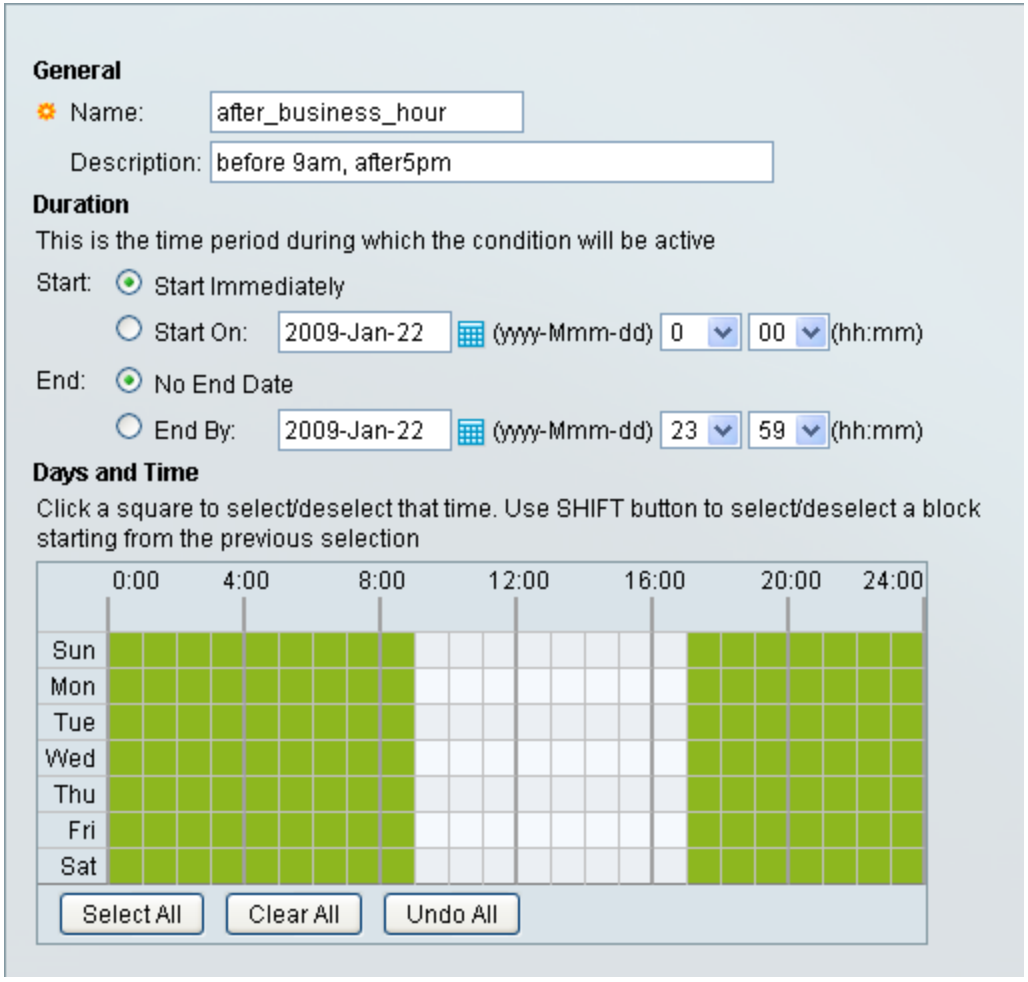
ACS 5

Policy Elements - Conditions and Authorization Profiles

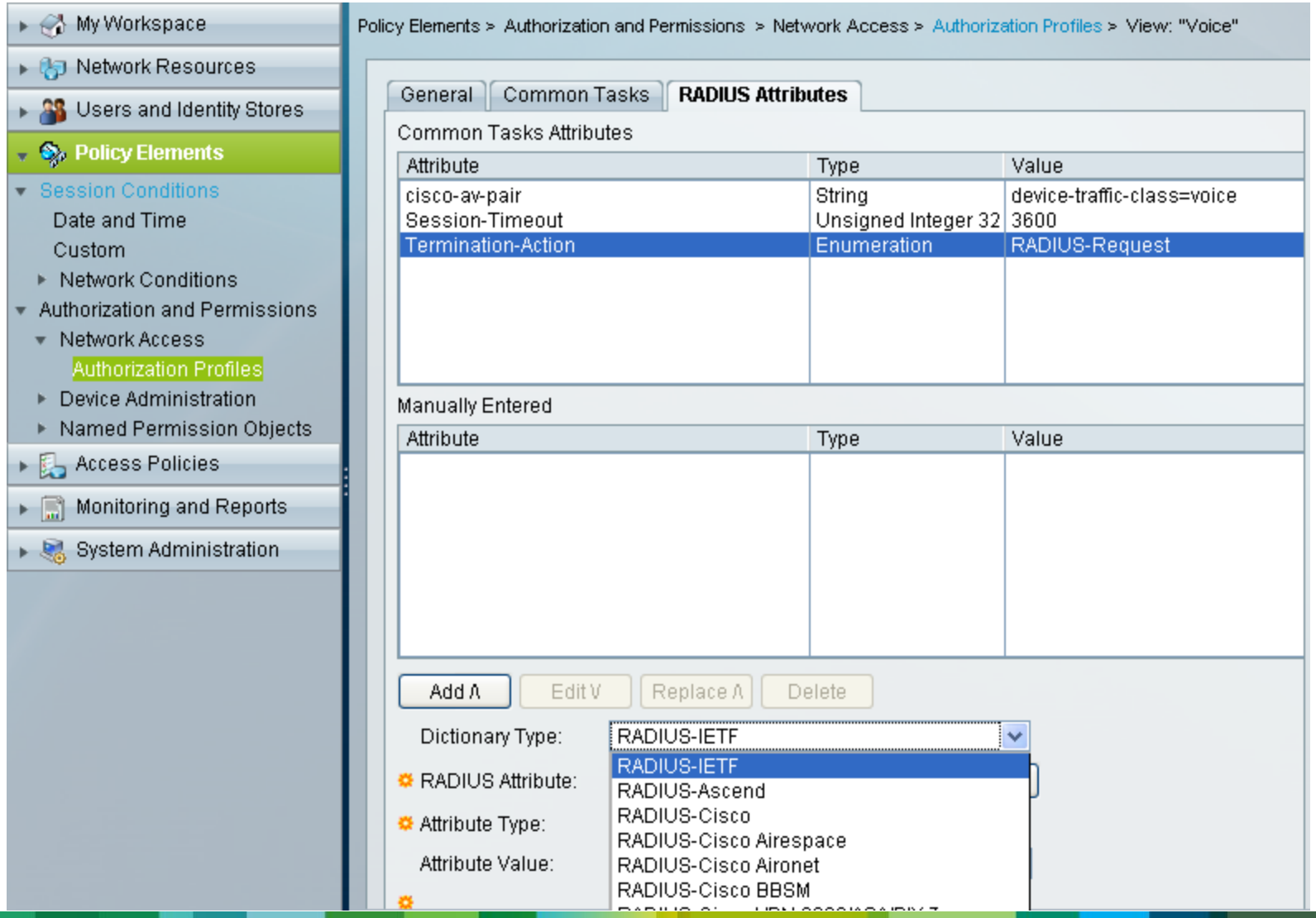
Key Changes

- Policy conditions and authorization permissions no longer part of users and user-groups
  - The ACS 5 model extends the ACS 4 Shared Profile Components concept
  - All conditions and permissions are defined as reusable components
  - These reusable components are referenced in the rules-based policy

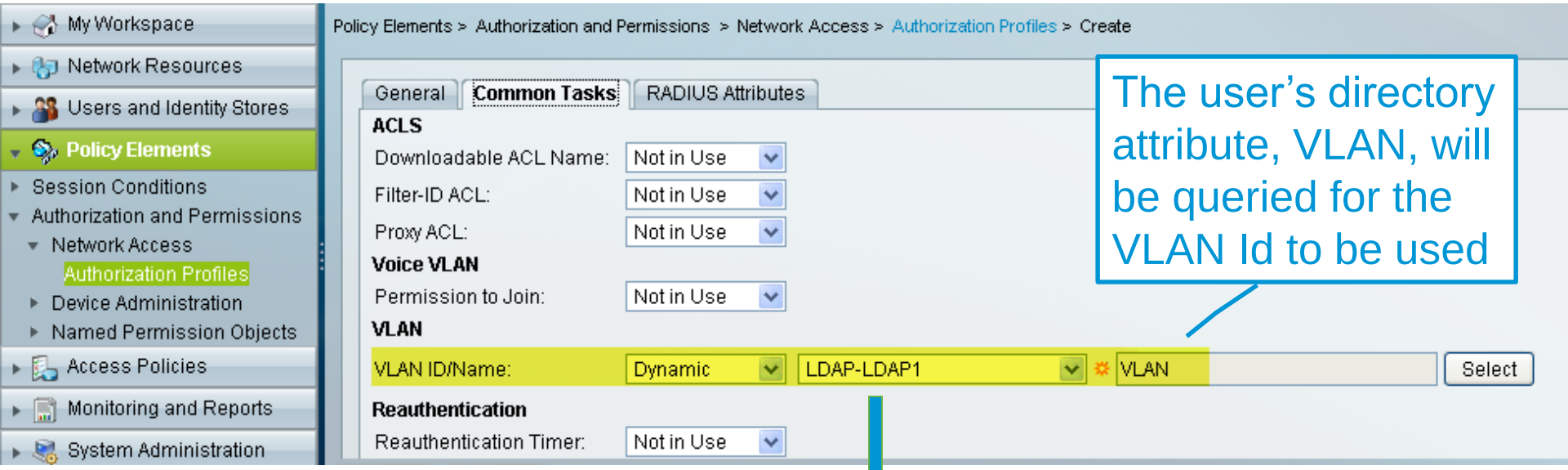
Date & Time Condition Elements



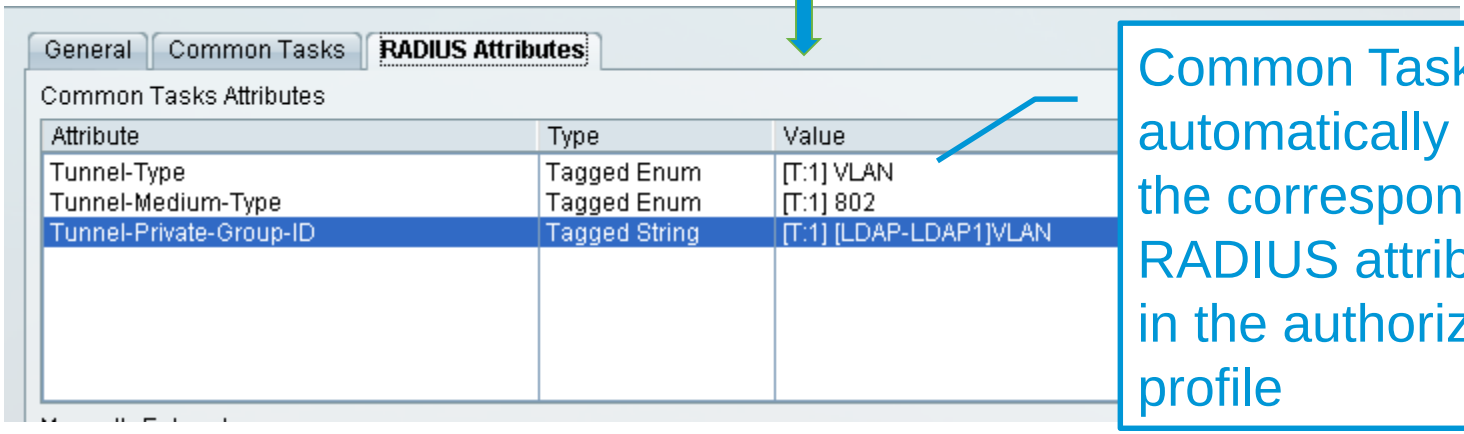
RADIUS Attributes In Authorization Profiles



Dynamic Authorization Values
Using Directory Attributes in Authorization Profiles

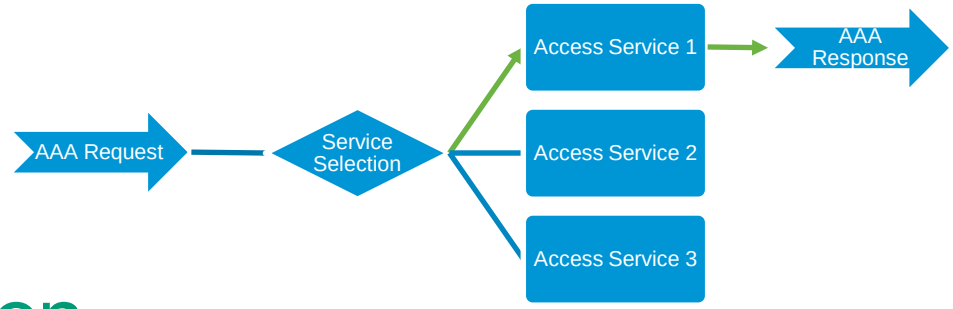


The user's directory attribute, VLAN, will be queried for the VLAN Id to be used

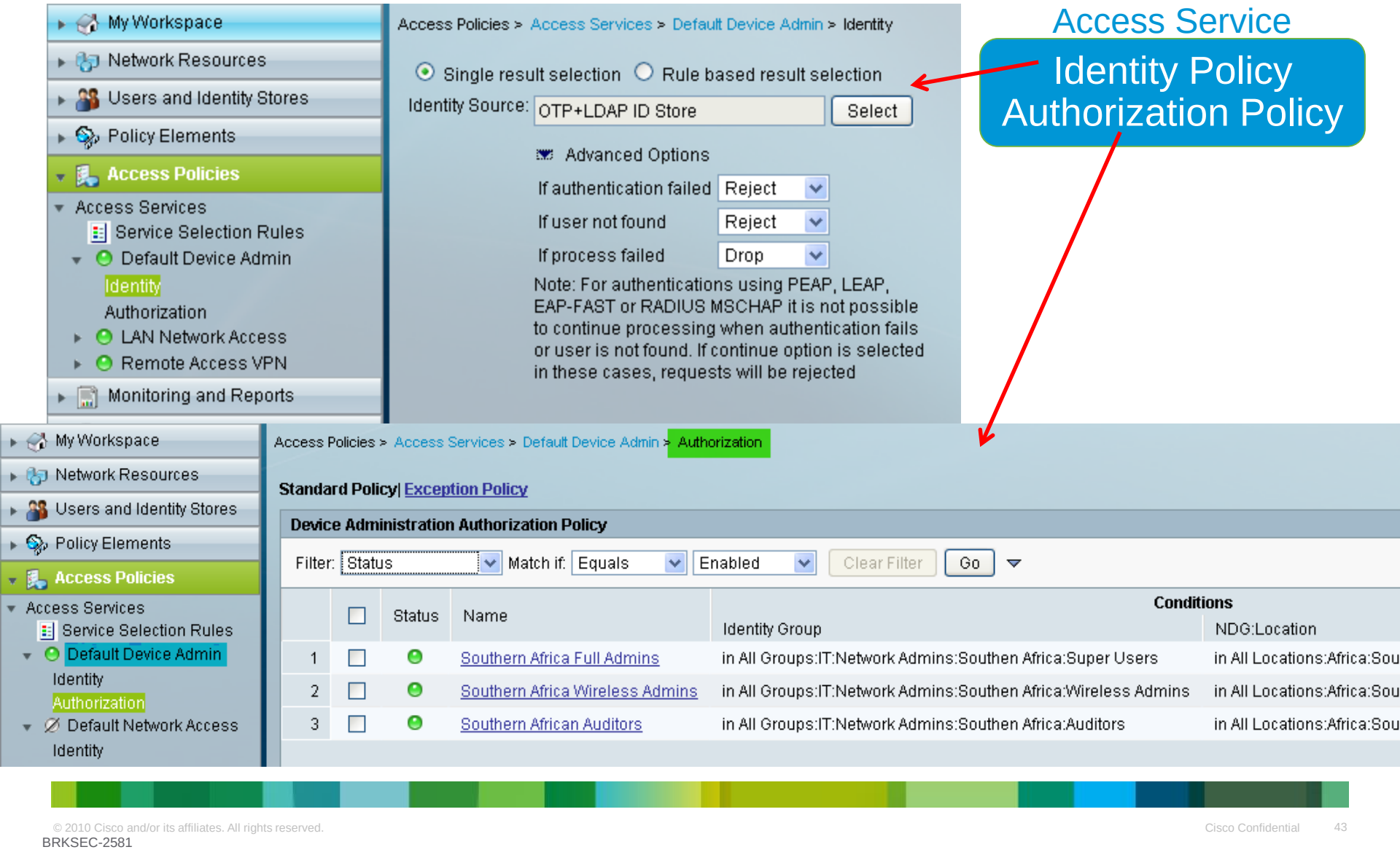


Common Tasks automatically create the corresponding RADIUS attributes in the authorization profile

Access Policy Configuration



A Device Admin Access Service



Developing Device Administration Authorization Policy

Identity Policy Authorization Policy

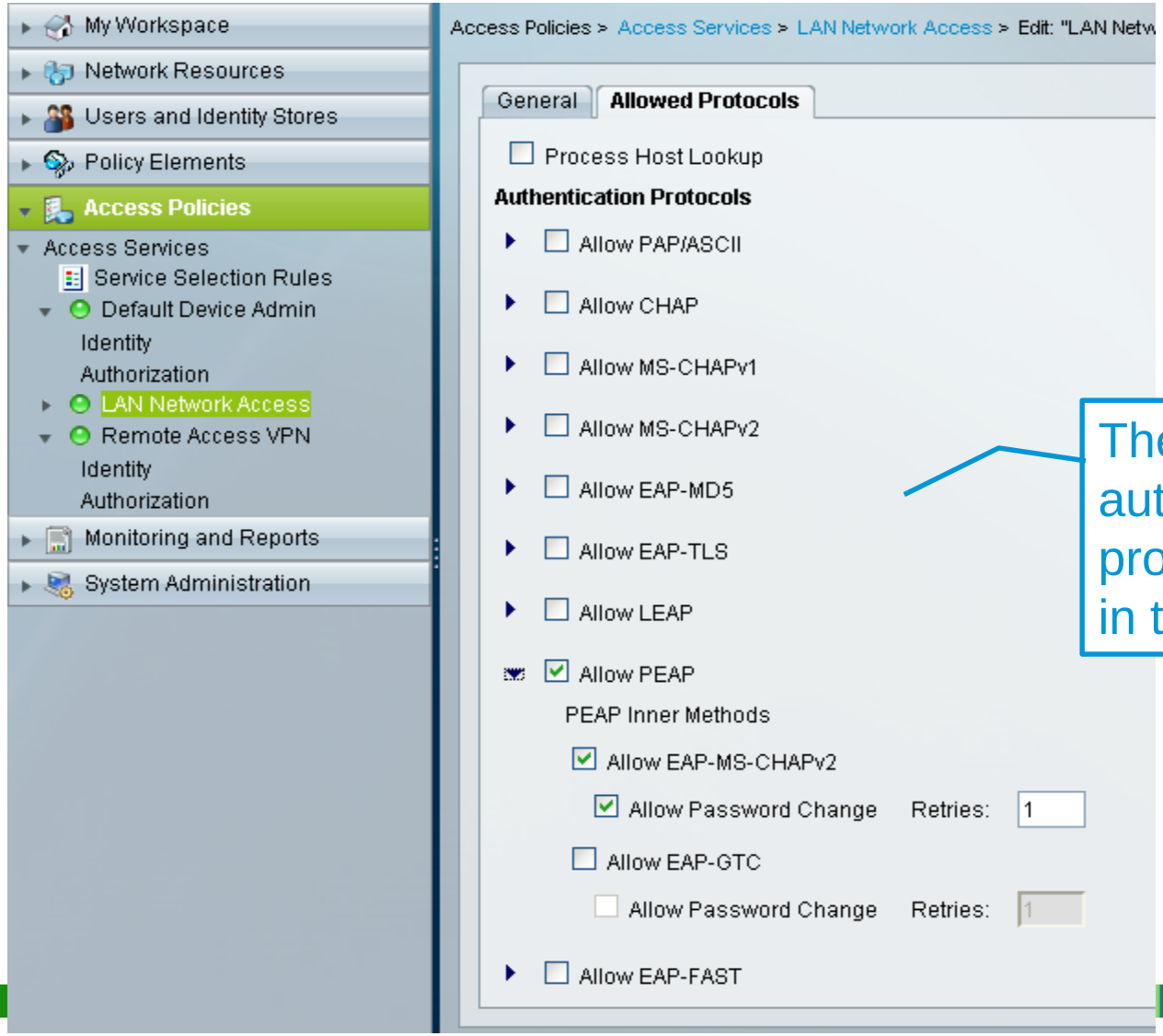
Name	Conditions			Results	
	Identity Group	NDG:Location	NDG:Device Type	Shell Profile	Command Sets
Southern Africa Full Admins	in All Groups:IT:Network Admins:Southen Africa:Super Users	in All Locations:Africa:Southern	in All Device Types	Priv Level 15	Full Command Access
Southern Africa Wireless Admins	in All Groups:IT:Network Admins:Southen Africa:Wireless Admins	in All Locations:Africa:Southern	in All Device Types:Wireless	Priv Level 15	Full Command Access
Southern African Auditors	in All Groups:IT:Network Admins:Southen Africa:Auditors	in All Locations:Africa:Southern	in All Device Types	Priv Level 15	Read-Only

User Group Conditions

Multiple Device Group Conditions

Shell and Cmd Set Authorization Results

Creating An Access Service – Allowed Protocols



The supported authentication protocols are defined in the access service

Creating An Access Service - Identity Policy

Identity Policy
Authorization Policy

Identity Policy

Filter: Status | Match if: Equals | Enabled | Clear Filter | Go

		Status	Name	Conditions: Authentication Method	Results: Identity Source	Hit Count
1	☐	●	Cert Auth	match x509_PKI	CN Username	0
2	☐	●	Password Auth	match PAP_ASCII	LDAP1	0
**	☐	Default		If no rules defined or no enabled rule matches.	DenyAccess	0

Identity policy to authenticate both cert and password-based auths

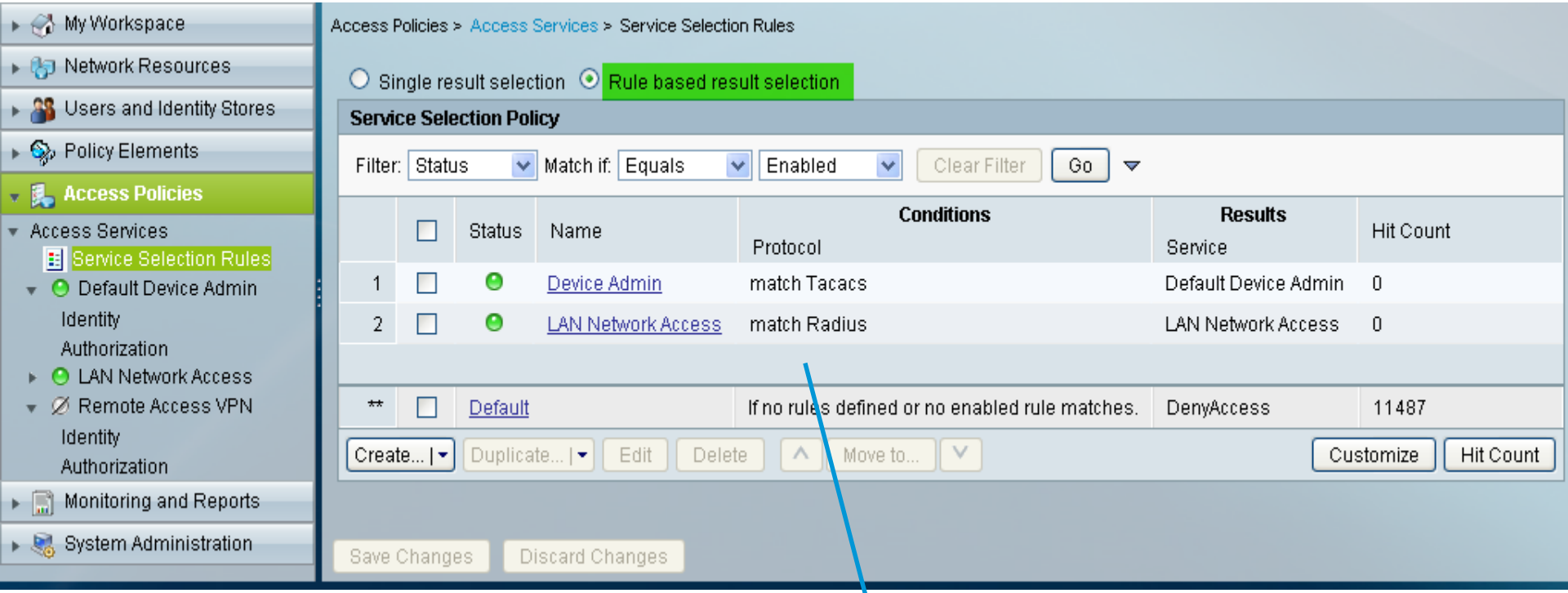
		Status	Name	Conditions: NDG:Device Type	Conditions: LDAP1:ExternalGroups	Results: Authorization Profiles
1	☐	●	Wireless	in All Device Types:Wireless	contains any (cn=Engineering,ou=groups,o=cisco.com; cn=Manager,ou=groups,o=cisco.com)	Dir-VLAN
2	☐	●	Wired	in All Device Types:Switches	-ANY-	Dir-VLAN
**	☐	Default		If no rules defined or no enabled rule matches.		DenyAccess

This authorization policy limits wireless access to engineering and manager groups.
Users' directory VLAN attribute is used to assign the VLAN

Implementing Rules-based Service Selection

A Simple, Protocol-based Service Selection Policy Example

Service Selection



Service selection based on AAA protocol

Service Selection Policy

Example Service Selection For Three Access Services

Access Policies > Access Services > Service Selection Rules

Single result selection Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

		Status	Name	Conditions		Results
				Protocol	NDG:Device Type	Service
1			Device Admin	match Tacacs	-ANY-	Default Device Admin
2			Remote Access	match Radius	in All Device Types:VPN Concentrators	Remote Access VPN
3			LAN Network Access	match Radius	-ANY-	LAN Network Access

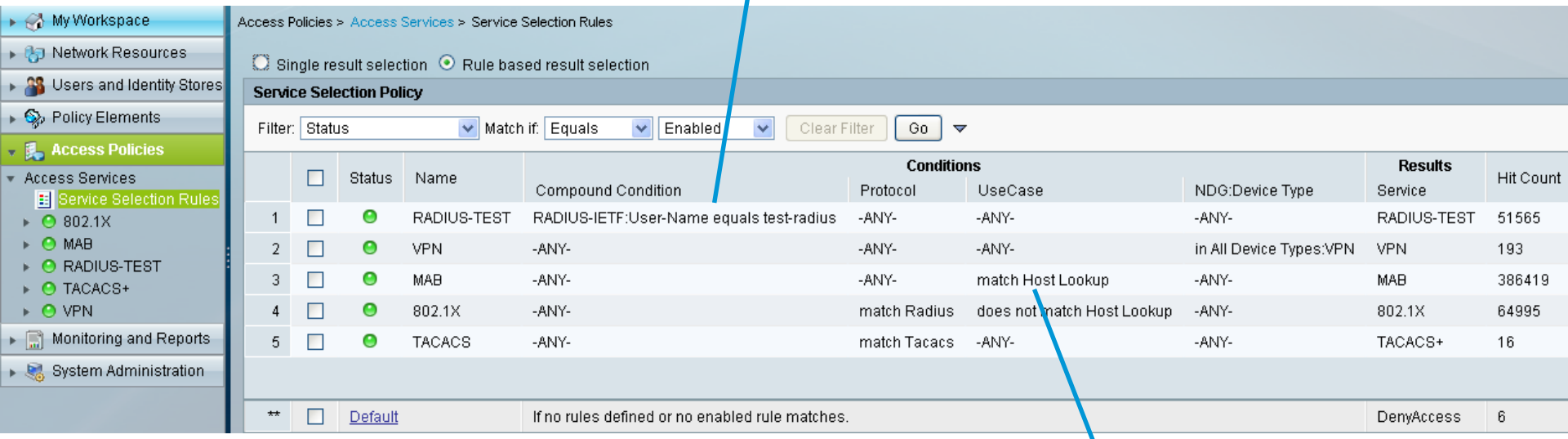
Available Policy Conditions

Service Selection	Identity	Authorization
ACS Host Name	[Previous column]	[Both previous columns]
Device Filter	Authentication Method	Authentication Status
Device IP Address	[Certificate attributes]	Identity Group
Device Port Filter	EAP Authentication Method	[Internal user attributes]
End Station Filter	EAP Tunnel Building Method	[Directory groups]
NDGs		[Directory attributes]
Protocol		System:UserName
Time And Date		Was Machine Authenticated
Use Case		
[RADIUS and TACACS+ attributes]		

Cisco Alpha Network Service Selection Policy

RADIUS attribute condition

Service Selection



Condition using the system 'UseCase' condition for MAB requests

Permission Based On EAP Type

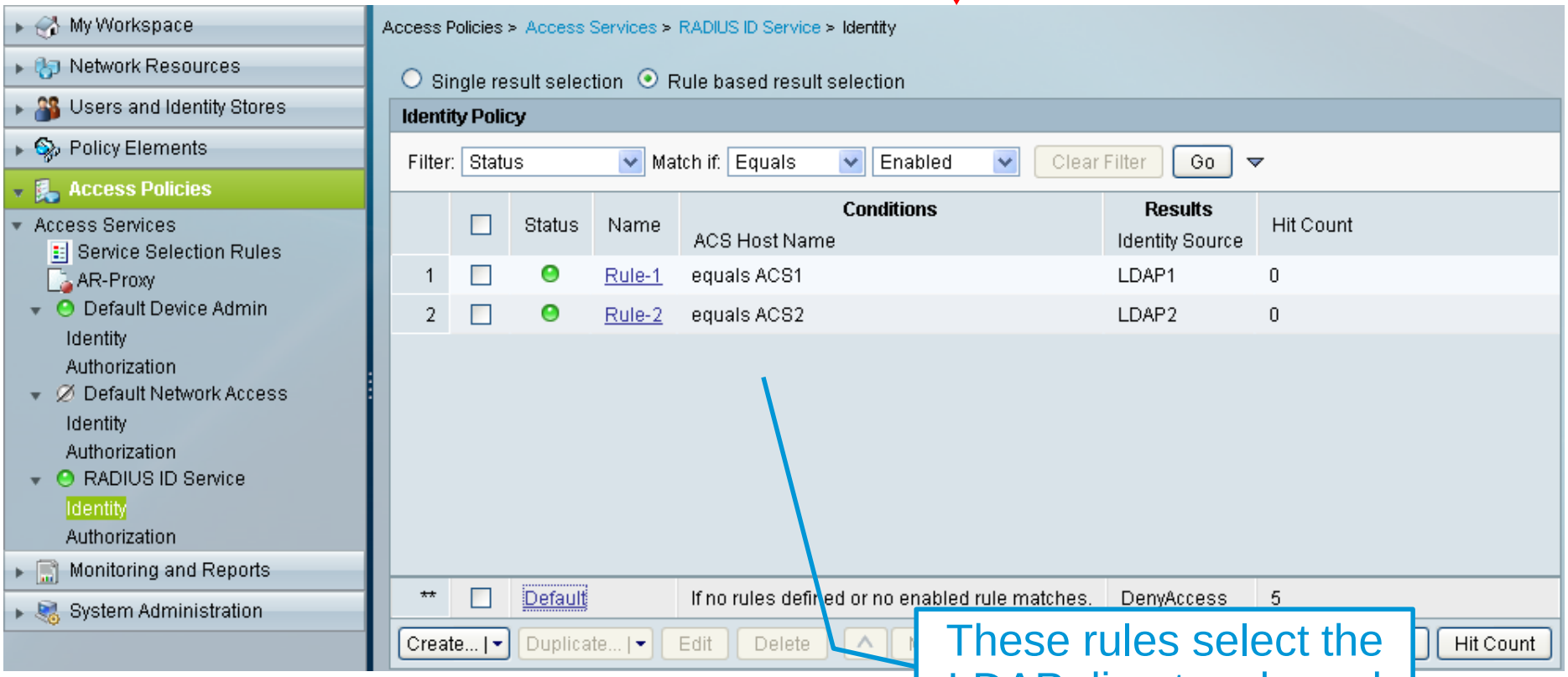
Identity Policy
Authorization Policy

		Status	Name	Conditions		Results
				LDAP1-Dept	Eap Authentication Method	Authorization Profiles
1			Rule-1	equals Sales	-ANY-	Medium
2			Rule-2	equals Marketing	match EAP-MSCHAPv2	Medium
3			Rule-3	equals Marketing	match EAP-TLS	High

Marketing users get different permissions based on whether they are using certificates or passwords for authentication

Identity Store Selection Based On ACS Server

Identity Policy
Authorization Policy



These rules select the LDAP directory based on the ACS server receiving the request

Deployment Overview

ACS 5.x Platform Options

1121 Hardware Appliance

One rack-unit (1RU) Linux-based appliance

3415 Hardware Appliance

One rack-unit (1RU) Linux-based appliance

VMware Appliance

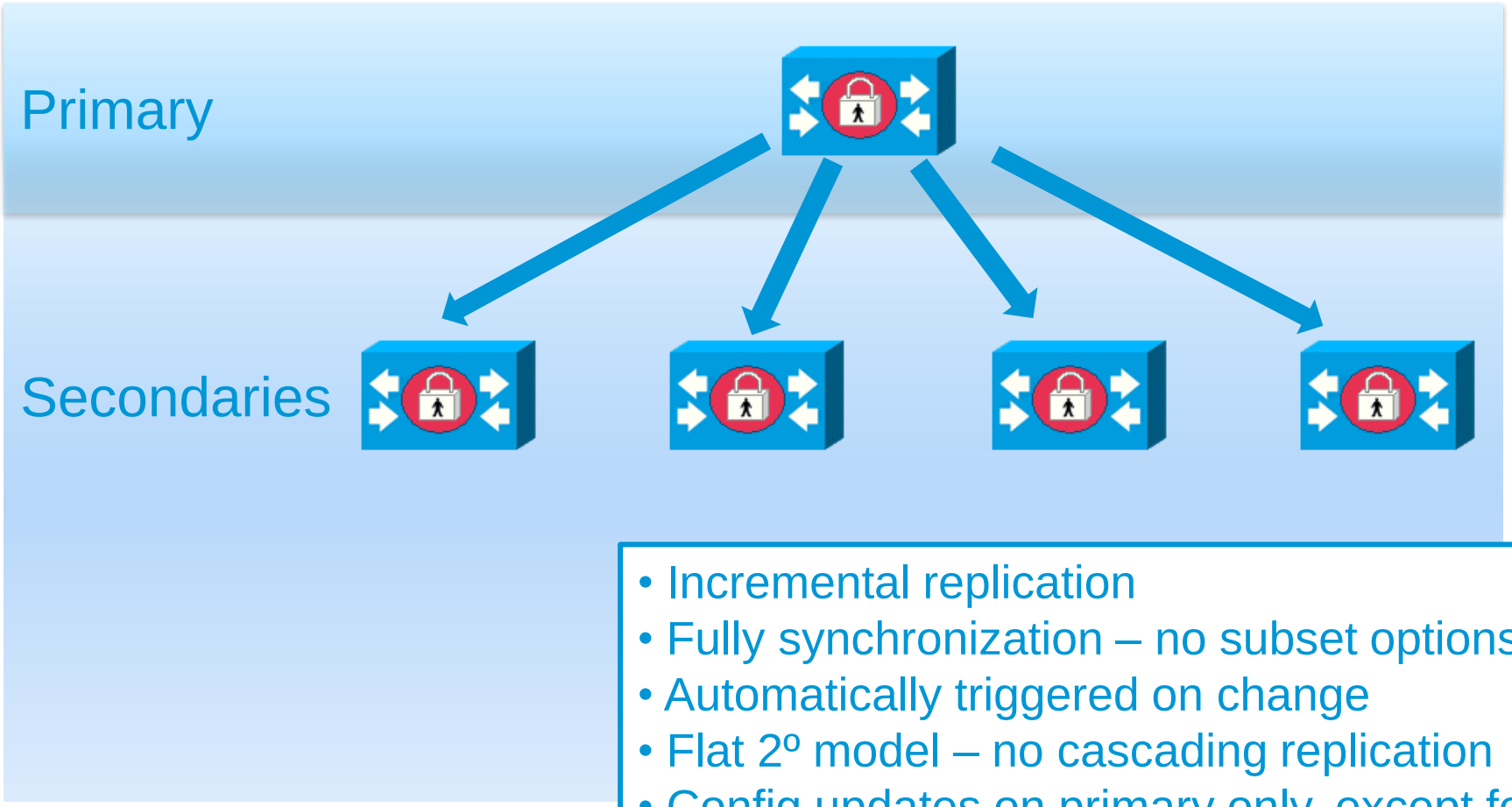
Complete appliance image for installation on VMware ESXi 5.0

vmware

ACS 3/4 to 5 Component Mapping

3.x/4.x Component	5.4 Option	Notes
ACS for Windows	VM in VMware ESX or 1121/3415 appliance	There is no ACS 5 Windows option. ACS 5 is an application/OS bundle that can run in a VM or supported appliance.
ACS Solution Engine (1111, 1112, 1113)	VM in VMware ESX or 1121/3415 appliance	1111/2/3 platforms do not support ACS 5.x. 4.2 can run on the 1120.
ACS Remote Agent	N/A	The Remote Agent is no longer required in ACS 5.

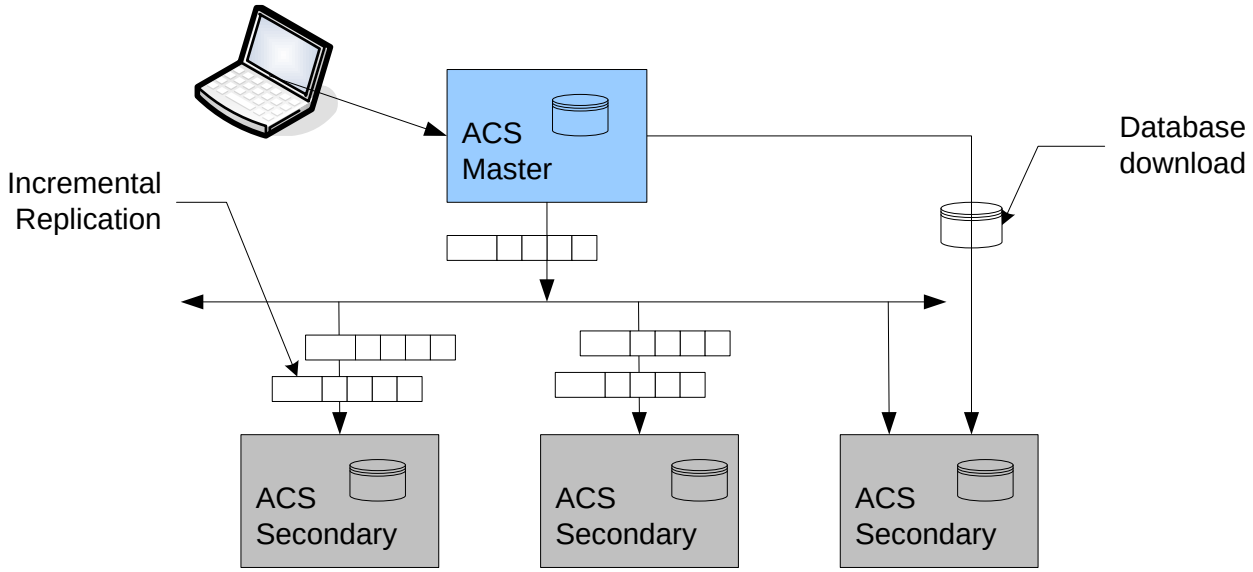
ACS 5.x Configuration Replication Model



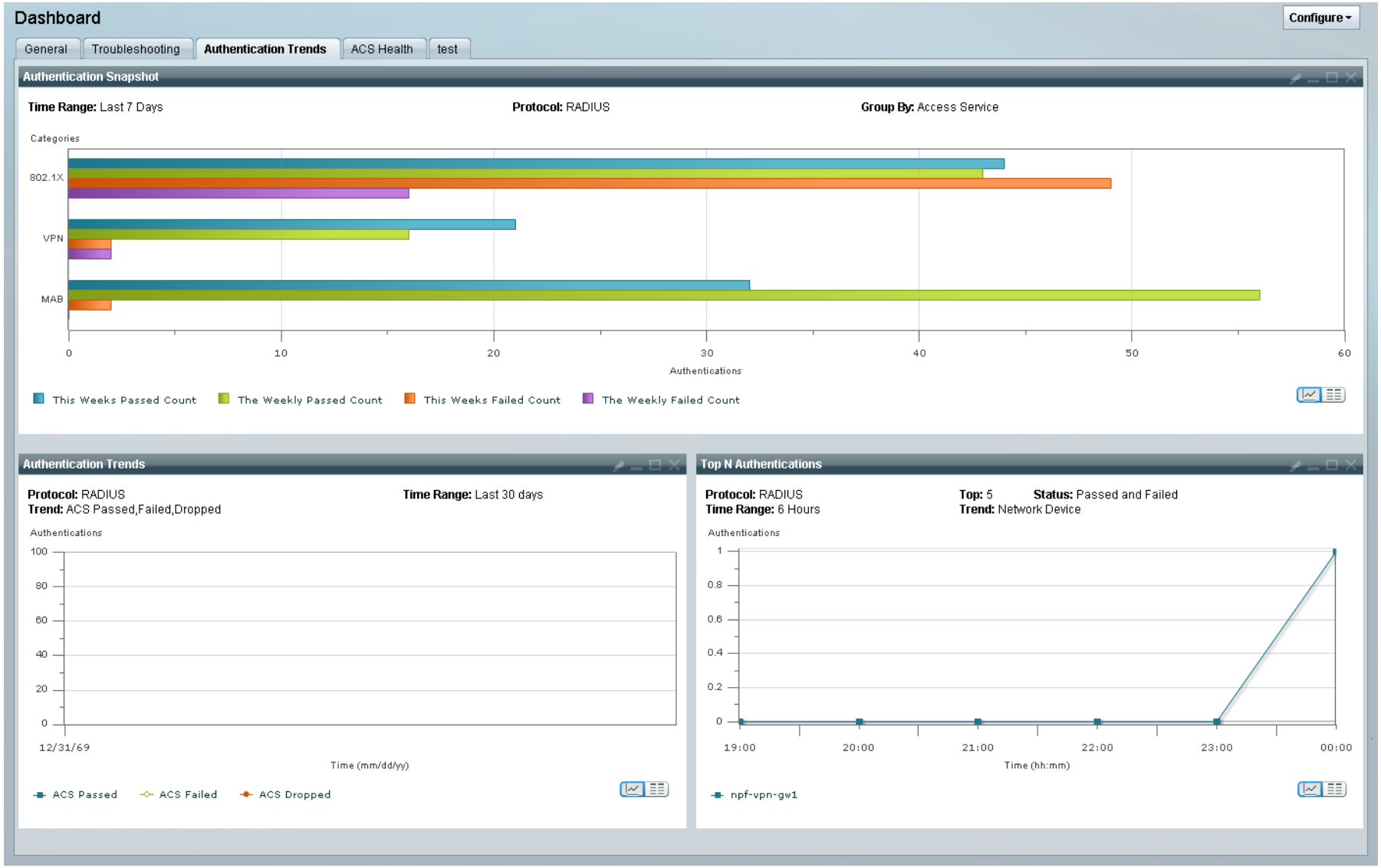
- Incremental replication
- Fully synchronization – no subset options
- Automatically triggered on change
- Flat 2º model – no cascading replication
- Config updates on primary only, except for AAA password updates

ACS Distributed Deployment

- Consists of multiple ACS's that are managed together
  - One Primary and multiple Secondary servers
  - All ACS instances are identical (run full ACS software version)
  - Each ACS can play a specific role in the deployment
- Incremental replication model
  - Primary ACS is single point of configuration & to monitor secondary servers
  - Automatic incremental replication to Secondary servers



ACS 5.x View Dashboard



ACS View Detailed Authentication Information

AAA Protocol > RADIUS Authentication

Authentication Status : Pass or Fail
Date : January 19, 2010 (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on January 20, 2010 12:50:01 AM PST

✔=Pass ✖=Fail 🔍=Click for details =Mouse over item for additional information

Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Instance
Jan 19,10 8:57:21.440 PM	✔		🔍	terwong	99.187.226.91	VPN	PAP_ASCII	npf-vpn-gw1	10.35.17.92			sjc23-npf-acs1
Jan 19,10 4:35:07.006 PM	✔		🔍	#ACSACL#IP-Quarantine-4b0354b3				sjcm-21a-npf-sw1.cisco.com	10.34.74.4			sjc23-npf-acs1
Jan 19,10 4:35:07.006 PM	✔		🔍	00-1C-23-00-3A-78	00-1C-23-00-3A-78	MAB	Lookup	sjcm-21a-npf-sw1.cisco.com	10.34.74.4	GigabitEthernet2/30		sjc23-npf-acs1
Jan 19,10 4:05:32.330 PM	✔		🔍	#ACSACL#IP-Quarantine-4b0354b3				sjcm-21a-npf-sw1.cisco.com	10.34.74.4			sjc23-npf-acs1
Jan 19,10 4:05:32.330 PM	✔		🔍	00-1C-23-00-3A-78	00-1C-23-00-3A-78	MAB	Lookup	sjcm-21a-npf-sw1.cisco.com	10.34.74.4	GigabitEthernet1/47		sjc23-npf-acs1
Jan 19,10 3:43:33.370 PM	✖		🔍		00-0B-CD-94-47-19			sjcm-21a-npf-sw1.cisco.com	10.34.74.4	GigabitEthernet2/8		sjc23-npf-acs1
Jan 19,10 3:43:28.070 PM	✖		🔍		00-0B-CD-94-47-19			sjcm-21a-npf-sw1.cisco.com	10.34.74.4	GigabitEthernet2/8		sjc23-npf-acs1
Jan 19,10 3:43:22.930 PM	✖		🔍									pf-acs1
Jan 19,10 3:43:17.310 PM	✖		🔍									pf-acs1
Jan 19,10 3:43:04.770 PM	✖		🔍									pf-acs1
Jan 19,10 3:42:59.233 PM	✖		🔍									pf-acs1
Jan 19,10 3:42:53.850 PM	✖		🔍									pf-acs1
Jan 19,10 3:42:49.910 PM	✔		🔍	#ACSACL#IP-Quarantine-4b03								pf-acs1
Jan 19,10 3:42:49.910 PM	✔		🔍	00-1F-E2-16-20-A9								pf-acs1
Jan 19,10 3:42:48.190 PM	✖		🔍									pf-acs1
Jan 19,10 3:42:47.690 PM	✖		🔍	anonymous								pf-acs1
Jan 19,10 3:42:33.930 PM	✖		🔍									pf-acs1
Jan 19,10 3:42:28.360 PM	✖		🔍									pf-acs1
Jan 19,10 3:42:22.680 PM	✖		🔍									pf-acs1
Jan 19,10 3:42:17.340 PM	✖		🔍									pf-acs1

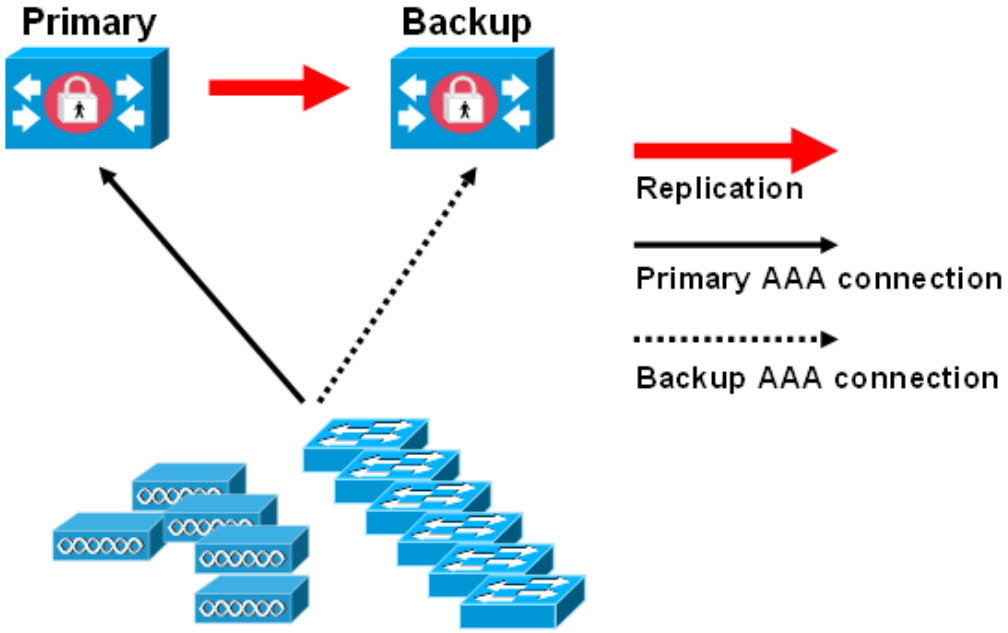
12104 Extracted EAP-Response containing EAP-FAST challenge-response
12105 Prepared EAP-Request with another EAP-FAST challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12104 Extracted EAP-Response containing EAP-FAST challenge-response
12105 Prepared EAP-Request with another EAP-FAST challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12104 Extracted EAP-Response containing EAP-FAST challenge-response
12815 Extracted TLS Alert message.
12153 EAP-FAST failed SSL/TLS handshake because the client rejected the ACS local-certificate
11504 Prepared EAP-Failure
11003 Returned RADIUS Access-Reject

Licensing

License	Description
Base Server	One per ACS instance.
Large Deployment	One per ACS deployment when the network device count (based on IP address) in ACS exceeds 500. (Configuring the Default Network Device does contribute to the device count).

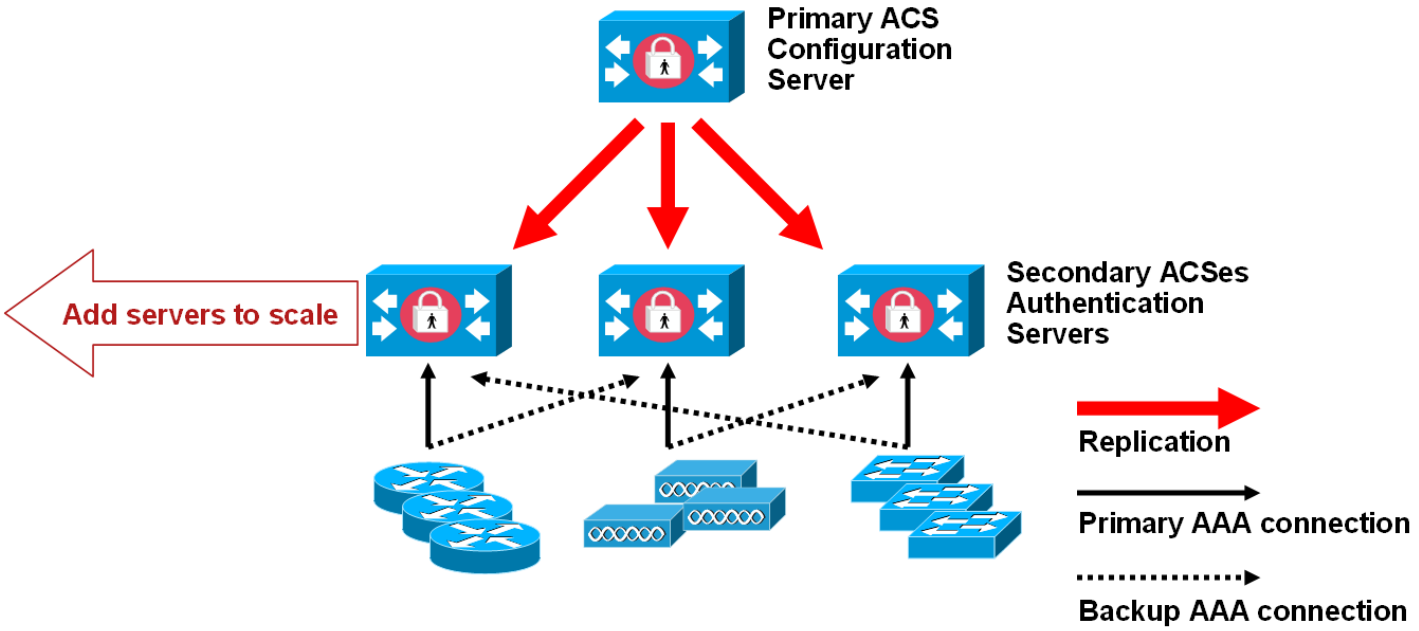
Minimum ACS Deployment

- Consists of 2 servers
- Primary server provides all the configuration, authentication and policy requirements for the network.
- Second server used as a backup server.
- Replication from primary ACS to secondary ACS to keep the secondary server in synchronization.



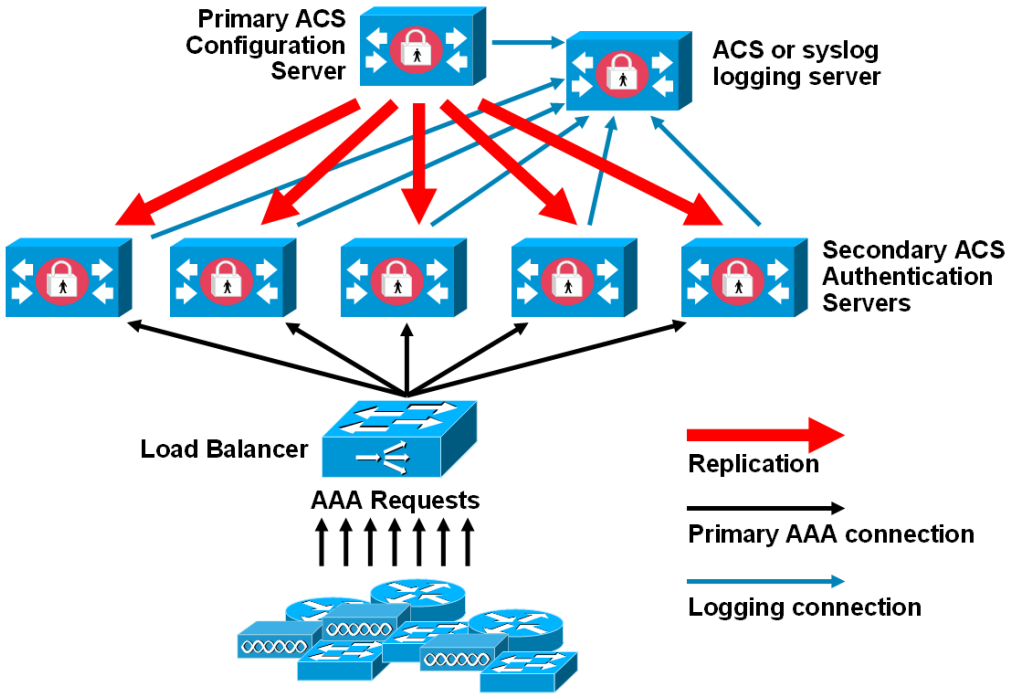
Medium Growing ACS Deployment

- As the AAA traffic grows, add additional Cisco Secure ACS servers
- Consider splitting server functions - the primary server for configuration and log collection only, using the secondary servers for AAA functions.



Larger ACS Deployment

- In a large, centralized network consider the use of a load balancer
- Dedicated primary and log collector ACS servers



References and Resources

- User guide migration chapter

  http://cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/user/guide/migrate.html

- Migration tool document

  http://cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/migration/guide/Migration_Book.html

- CSV file import tool chapter

  http://cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/cli_imp_exp.html

- Partner forum

  https://www.myciscocommunity.com/community/partner/security?view=overview

Thank you.

Migration Tool

Migration Scenarios

- The migration utility supports the following versions:
  - 4.1.1.24
  - 4.1.4
  - 4.2.0.124
  - 4.2.1
- Customers that use any lower version need to perform an upgrade to either of the supported version. Recommendation is to go to 4.1.1.24 or 4.2.0.124

Migration Tool – Element Support

- Migration utility migrates the following ACS 4.x data entities:
  - AAA Clients and Network Devices
  - Internal Users
  - User-Defined Fields (from the Interface Configuration section)
  - User Groups
  - Shared Shell Command Authorization Sets
  - User TACACS+ Shell Exec Attributes (migrated to user attributes)
  - Group TACACS+ Shell Exec Attributes (migrated to shell profiles)
  - User TACACS+ Command Authorization Sets
  - Group TACACS+ Command Authorization Sets
  - MAB Addresses
  - Shared, Downloadable ACLs
  - EAP-FAST Master Keys
  - Custom Vendor Specific Attributes

ACS 5.4 Migration - Unsupported Objects

- The ACS migration utility will NOT migrate the following data from an ACS 4.x system to ACS 5.4:
  - AD/LDAP/RSA configuration
  - All Certificates
  - User & Group RADIUS attributes
  - Admin Accounts
  - Date & time
  - Shared, User, and Group NARs
  - MAR
  - Many more….. Check Migration Guide:

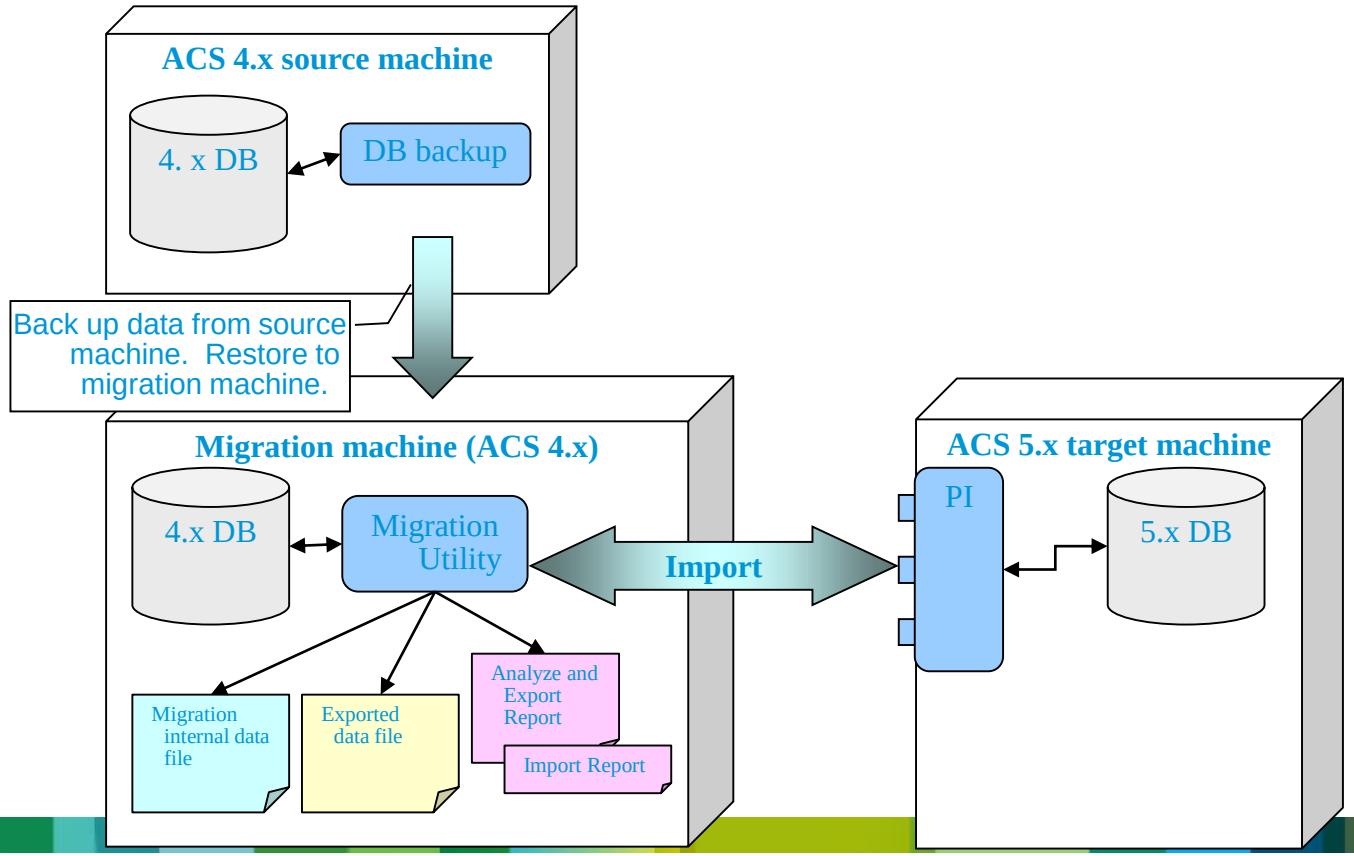
  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/migration/guide/Migration_support.html#wp1019460

Migration Tool

- ACS 5.4 Migration Utility is a windows standalone application whose purpose is to migrate data from ACS 4.x DB to ACS 5.x deployment.
- The customer must backup the ACS 4.x DB on the source machine and restore it on the migration machine.
- The customer must enable the migration interface on 5.x (CLI: acs config-web-interface migration enable) before running the migration.

Migration Tool

- The set up include 3 machines: source (ACS4.x), migration (ACS 4.x) and target (ACS5.x)



Migration Machine Requirements

- Windows platform running ACS 4.x with the exact version of the course machine, NOT an appliance machine
- Do NOT use a machine that is in production
- Use at least 2GB of RAM

Migration Pre-Installation Checks

- Ensure that there is no database corruption on the ACS 4.x migration system
- The ACS 4.x migration system should have only 1 IP address (Single NIC)
- Network Connectivity between the migration machine and the ACS 5.x server
- The Migration Interface is enabled on the ACS 5.x server

  Display status: `show acs-migration-interface`

  Enable interface: `acs migration-interface enable`

Migration Utility Access

- Available via the ACS 5.x web interface under

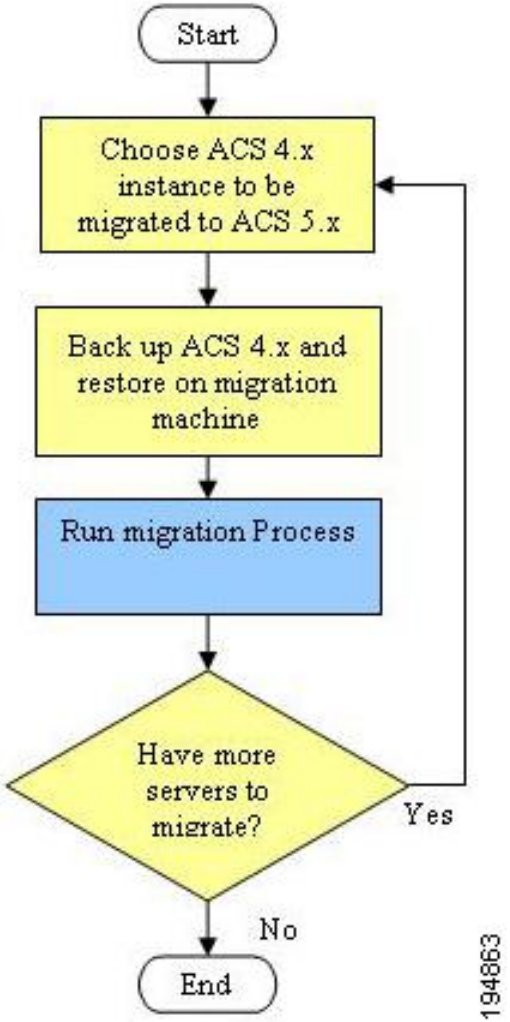
  System Administration > Downloads > Migration Utility

- Download the *migration.zip* file from the Migration application files
- Extract the contents of the zip file on to the 4.x migration machine

ACS 4.x Multi-instances Support

- Consolidation of multiple distinct database instances (4.x) into a single consolidated database.
- In ACS 4.x selective data replication could be defined such that different ACS instances would maintain distinct subsets of the overall system configuration.
- In ACS 5.x there is a single consolidated database that is replicated to all ACS instances in the deployment and so the Primary database would need to contain all the local configuration definitions from each of the ACS 4.x instances.

Multiple-Instance Migration Process



Multi instance Migration process

The multi-instance migration process in ACS 5.x will be as follows for each 4.x instance:

1. The user will select a 4.x instance to be migrated, the primary 4.x ACS instance (if exists in the deployment) should be migrated first.
2. The instance will be backed-up and restored on the Migration machine. After the restore operation completes, the migration process can be executed.
3. Upon completing of the migration process (per instance) that user will be prompted to continue with another instance, or terminate the migration process.
4. The impact on the Migration process itself would be that the instance name would be added to the migration process and to all the migration reports. Duplicate and discrepancy data objects that existed on multiple ACS 4.x instances will be detected and reported on the migration import phase.

Multi-instance - Duplicate object reporting

Duplicate Object Reporting

- Duplicate data objects on multiple ACS 4.x instances are detected in the import phase. For most of the objects types, we identify duplicates by name (network device by IP address).
- The import report, include information about duplicate objects.

Object Name Prefix Per Instance

- You can define a different name prefix to each ACS 4.x instance. The prefix is used to retain server-specific identification of data elements and prevent duplication of names of objects for different servers.
- You can change the name prefix at the beginning of each run of the Migration Utility (per ACS 4.x instance).
- You can configure a global name prefix for all prefixes in the instance or per-object-type name prefix (for object types that supports name prefix). This enables you to preserve associations between shared objects.

Multi-instance – Restrictions

- Merge or override data between 4.x instances is not supported.
- Every object will be migrated (added to ACS 5.x) only once and it will not be updated (override) with any other value or the additional value will not be added.

Multi-instance – Restrictions (*Example*)

- For example, 2 instances to migrate X and Y:

  Server X: User: **John** with attribute: Age: 32

  Server X: User: **Smith** with attribute: Age: 25

  Server Y: User: **John** with attributes: Age: 37, Eyes: Blue

  Server Y: User: **Smith** with attributes: Age: 25, Eyes: Brown

  Server Y: User: **Fox** with attributes: Age: 55, Eyes: Green

  At the end of the migration from **server X**, ACS 5.x data will include 2 users: John and Smith each with 1 Identity Attribute: Age.

  On the process of the migration from **server Y**, the migration utility will identify that the users: **John** and **Smith** already exists on ACS 5.x, and therefore all the data (attributes) that belongs to the users will be skipped as well, even if the data on **server Y** is different from **server X**, it will not be updated or added, and the values attribute: Eyes will not be added nor the value of the attribute: age will be updated to 37.

  User **Fox** will be migrated with the 2 attributes because its does not exists in **server X**.

Multi-instance – Restrictions (*Example*)

- Merged ACS 5.x Result:

  User: **John** with attribute: Age: 32

  User: **Smith** with attribute: Age: 25

  User: **Fox** with attributes: Age: 55, Eyes: Green

Shared Object Handling

- Shared objects between the ACS 4.x instances: NDGs, user attribute definitions, and user groups are migrated only once.
- The object associations are created according to the up to date status of ACS 5.x data.
- For example:

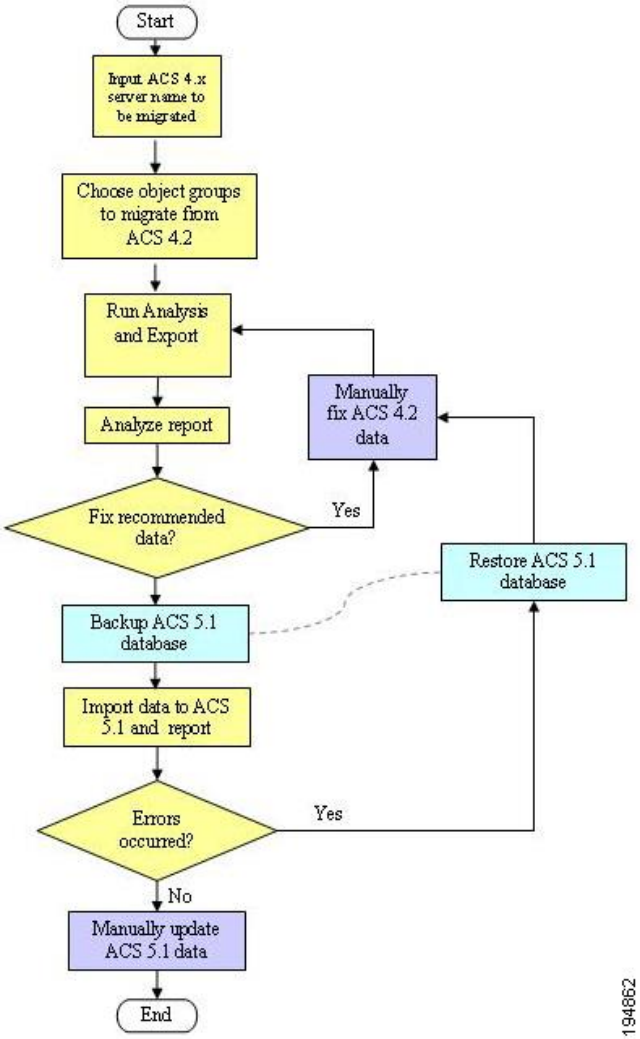
  If user A is associated to group BB and neither the user nor the group were migrated, both objects are created and then associated in ACS 5.x.

  If user D is associated to group CC and the user was not migrated in previous instance but the group CC was migrated, only the user D is created and then associated in ACS 5.x to CC.

Unify the Analysis and Export Phases

- The export and analysis phases will be implemented as a single phase in the migration process.
- The impact will be both in the User Experience of the migration where a single phase ("Analysis & Export") will be visible to the user, and also in the Migration reports.
- The Analysis & Export report will include analysis and export information.

Migration process



Migration Phases

The Migration Utility includes 2 main Phases:

- **Analysis & Export** –

  Analyzes the ACS 4.x configuration to identify possible migration issues which could affect the ability to perform a successful data migration.

  Exports the selected set of objects from the ACS 4.x data to an external data file that can be processed by the import process.

- **Import –** the data will then be imported into ACS 5.0 using the PI client application

RAC-Shared Radius Attributes

- In ACS 4.x, you can define a shared profile component that contains RADIUS Authorization Components (RACs) and defines a set of RADIUS attributes and values that are to be returned in an authorization response.
- These shared objects map the direction to the authorization profiles that are defined in ACS 5.x..

Important Notes

- For large DBs (more than 100K users), it is recommended to import the objects by group types (all users, all devices etc.) and not to import “AllObjects”.
- The migration utility ***cannot be run over MS Remote Desktop***

  Run the migration utility via VNC to the migration machine instead
- NAT is not supported

  You cannot use NAT between the migration machine and the ACS 5.x server.

Troubleshooting

- The import phase can be stopped for several reasons:
  - A network connection problem
  - ACS 5.x the migration is not enabled

```
acs config-web-interface migration enable
```

  - ACS 5.x services are down:

```
show application status acs
```

- If the ACS machine is not responding after import then try to restart the ACS 5.x

```
acs stop
acs start
```

Migration Performance

- Performances for large scale DB:

  Import of 100K Users ~ 3.5 H

  Import of 300K Users ~ 11 H

  Import of 45K Devices ~ 5 H

- Note: The performance of the user import is mainly a factor of the amount of user's attributes (supplementary fields and T+ Shell Exec attributes).
- It is recommended to run the migration against standalone (primary) ACS 5.x and connect all the secondaries after the migration is completed.