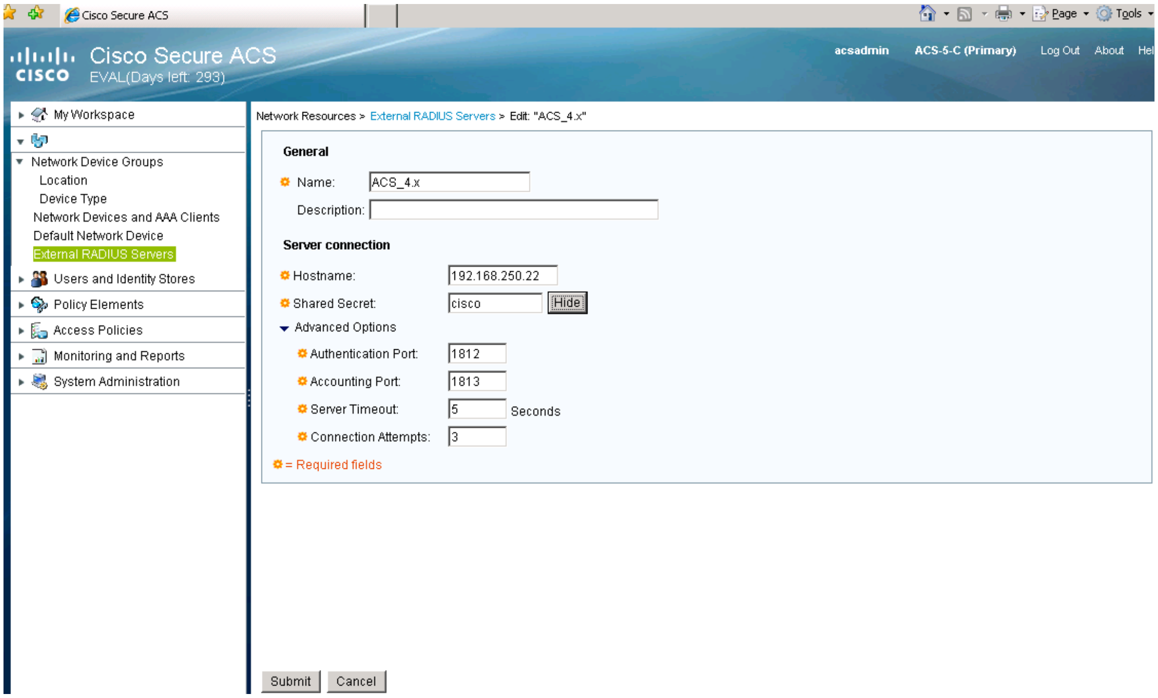
Step 1: Define the Radius server that will be used to forward the authentication requests.
Network Resources / External Radius Server



Network Resources > External RADIUS Servers > Edit: "ACS_4.x"

General

Name: ACS_4.x

Description:

Server connection

Hostname: 192.168.250.22

Shared Secret: cisco

Advanced Options

Authentication Port: 1812

Accounting Port: 1813

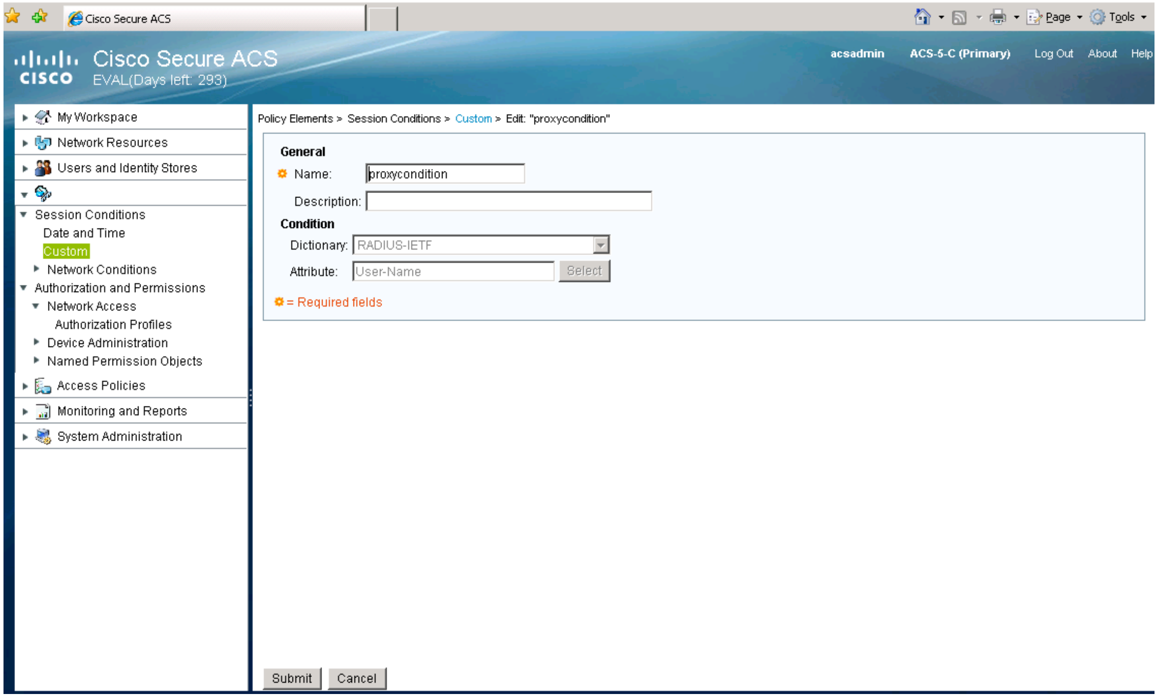
Server Timeout: 5 Seconds

Connection Attempts: 3

= Required fields

Step 2: Create a custom condition that will verify the information contained on the username during the authentication request. You will have to define the dictionary "Radius IETF" with the attribute user-name.

You create the custom condition under "Policy Elements / Session Condition / Custom



Policy Elements > Session Conditions > Custom > Edit: "proxycondition"

General

Name: proxycondition

Description:

Condition

Dictionary: RADIUS-IETF

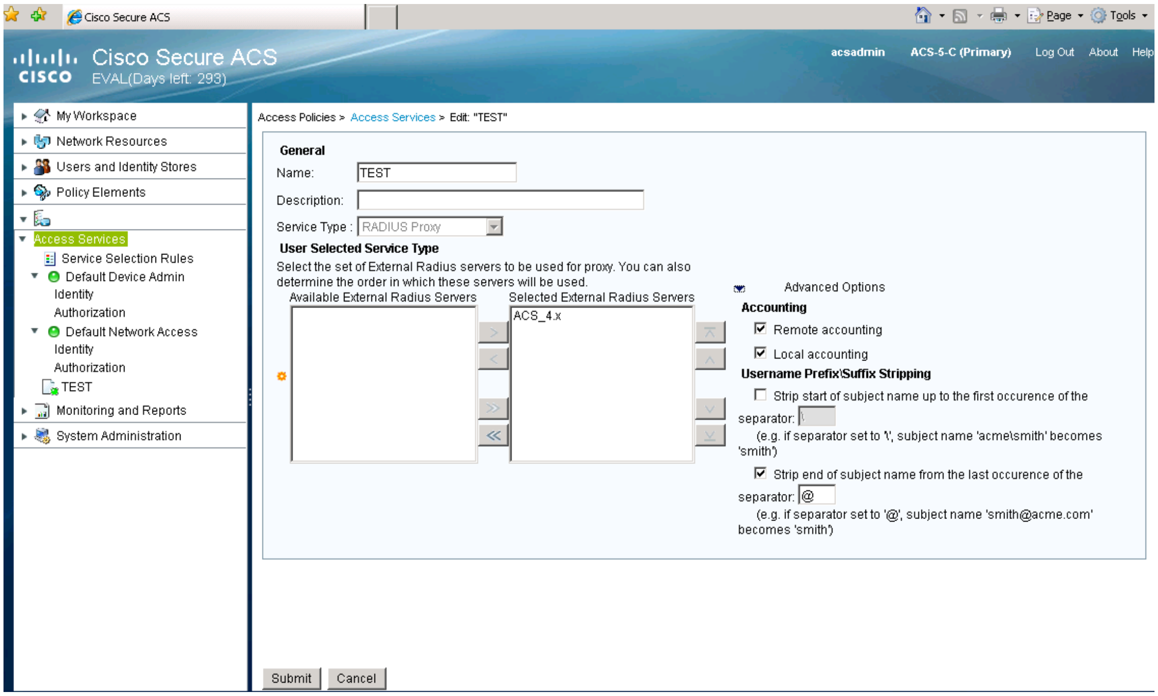
Attribute: User-Name

= Required fields

Step 3: Create an access service that will use the Radius Proxy service that will be used to forward the authentication request to the external server

-Go into Access Policy / Access Service and hit under Create
-Define a name for the rule and move the Radius server that was created under Step 1 to the right box using the right arrow bottom
-Hit under the Advanced option and select strip option that better applies to your setup.

For this example we are using the format "user@cisco.com" so we are selecting the option ***strip end of subject name*** and defined the separator "@"



Access Policies > Access Services > Edit: "TEST"

General

Name: TEST

Description:

Service Type : RADIUS Proxy

User Selected Service Type

Select the set of External Radius servers to be used for proxy. You can also determine the order in which these servers will be used.

Available External Radius Servers	Selected External Radius Servers
	ACS_4.x

Advanced Options

Accounting

☑ Remote accounting

☑ Local accounting

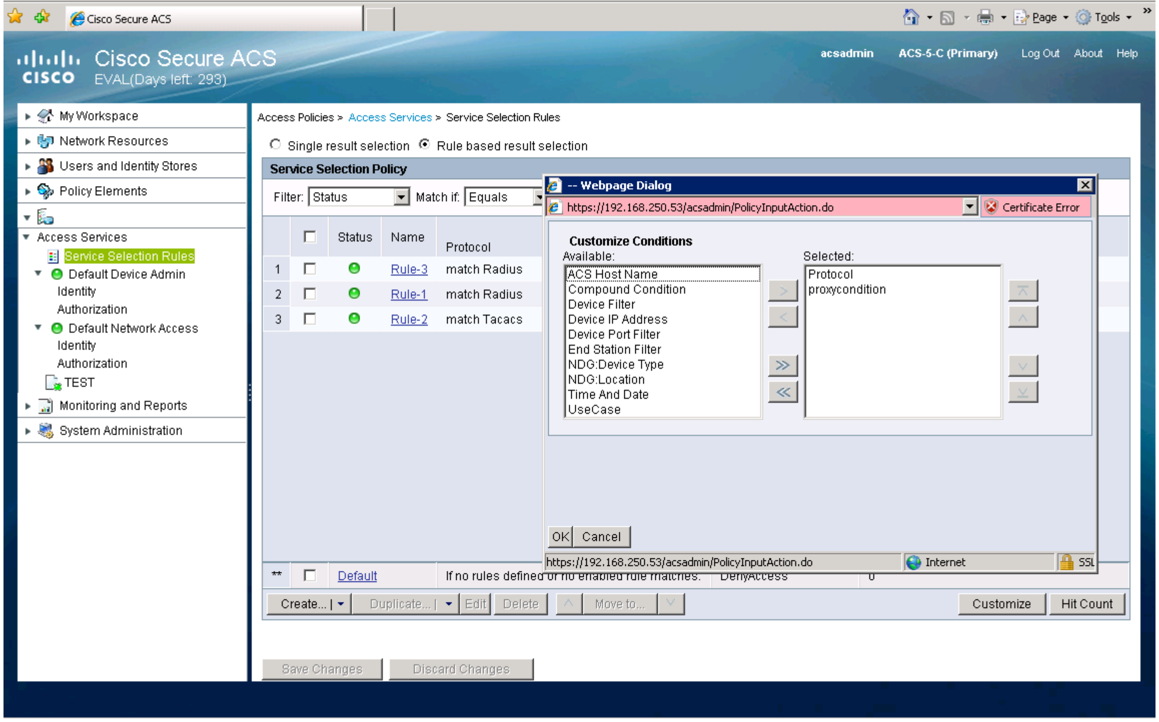
Username Prefix\Suffix Stripping

□ Strip start of subject name up to the first occurence of the separator: \
(e.g. if separator set to '\', subject name 'acme\smith' becomes 'smith')

☑ Strip end of subject name from the last occurence of the separator: @
(e.g. if separator set to '@', subject name 'smith@acme.com' becomes 'smith')

Step 4: The final step is to create a Service Selection Rule that will match with the custom condition we created previously.

Under the main screen hit the option "Customize" and add the custom condition "proxycondition" so it can used when defining the rule.



Access Policies > Access Services > Service Selection Rules

○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status ▾ Match if: Equals ▾

	□	Status	Name	Protocol
1	□	●	Rule-3	match Radius
2	□	●	Rule-1	match Radius
3	□	●	Rule-2	match Tacacs
**	□		Default	If no rules defined or no enabled rule matches. DenyAccess 0

-- Webpage Dialog

https://192.168.250.53/acsadmin/PolicyInputAction.do

Customize Conditions

Available:

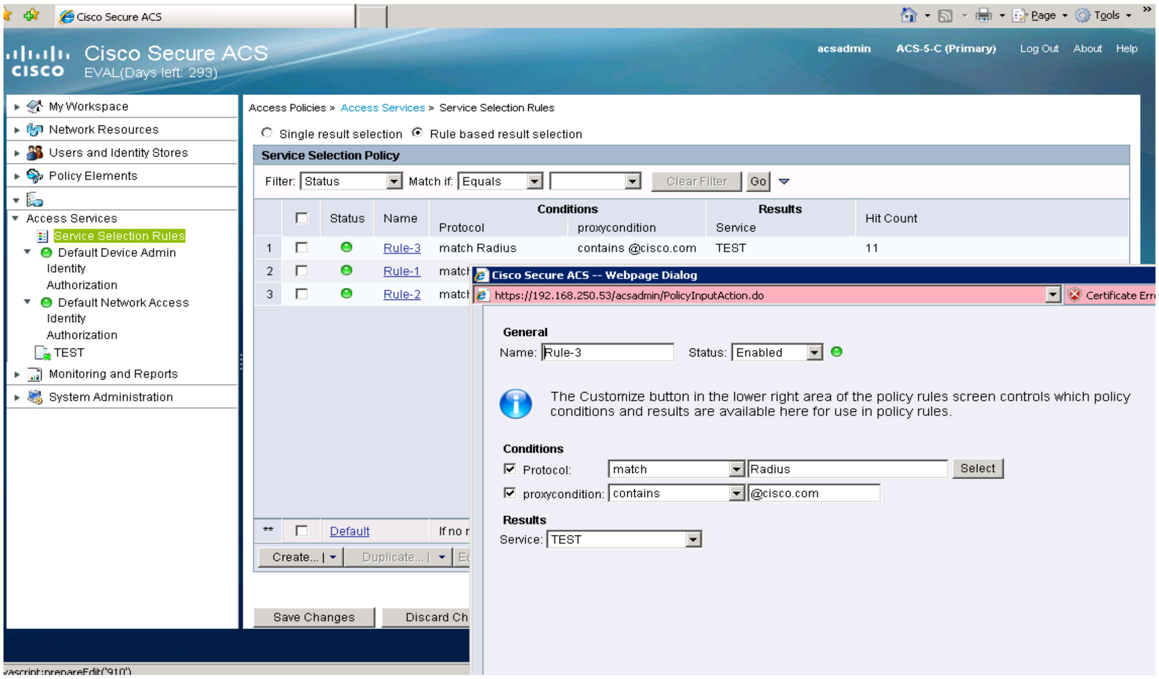
- ACS Host Name
- Compound Condition
- Device Filter
- Device IP Address
- Device Port Filter
- End Station Filter
- NDG:Device Type
- NDG:Location
- Time And Date
- UseCase

Selected:

- Protocol
- proxycondition

https://192.168.250.53/acsadmin/PolicyInputAction.do

Step 5: Create the rule and select the condition protocol for Radius and under the custom condition "proxycondition", use the option "contains" and the domain information that want to strip from the username information.



Access Policies > Access Services > Service Selection Rules

○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status ▾ Match if: Equals ▾

	□	Status	Name	Conditions		Results	Hit Count
				Protocol	proxycondition	Service	
1	□	●	Rule-3	match Radius	contains @cisco.com	TEST	11
2	□	●	Rule-1	matcl			
3	□	●	Rule-2	matcl			
**	□		Default	If no r			

Cisco Secure ACS -- Webpage Dialog

https://192.168.250.53/acsadmin/PolicyInputAction.do

General

Name: Rule-3 Status: Enabled ▾ ●

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

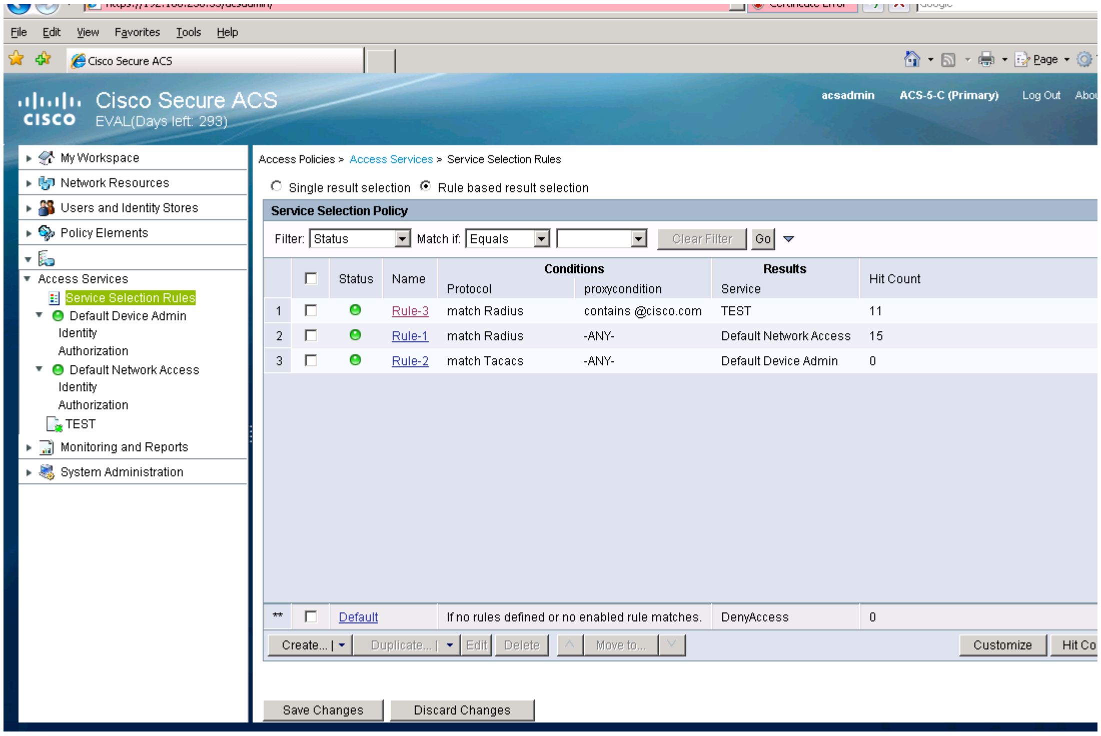
☑ Protocol: match ▾ Radius

☑ proxycondition: contains ▾ @cisco.com

Results

Service: TEST ▾

Step 6: Make sure to move the rule created to the top of the list in order to match the condition in case that you have default rule created just for the Radius protocol for the other devices.



Access Policies > Access Services > Service Selection Rules

○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals

	□	Status	Name	Conditions		Results	Hit Count
				Protocol	proxycondition	Service	
1	□	●	Rule-3	match Radius	contains @cisco.com	TEST	11
2	□	●	Rule-1	match Radius	-ANY-	Default Network Access	15
3	□	●	Rule-2	match Tacacs	-ANY-	Default Device Admin	0
**	□		Default	If no rules defined or no enabled rule matches.		DenyAccess	0