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

🍃 🍄 🏾 🌈 Cisco Secure ACS			🚹 🔹 🗟 👻 🖶 🔹 📴 Page 🔹 🎯 T <u>o</u> ol	ls +
Cisco Secure A EVAL(Days left: 293)		acsadmin	ACS-5-C (Primary) Log Out About	Hel
🕨 🛠 My Workspace	Network Resources > External RADIUS Servers > Edit: "ACS_4.x"			
 Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers Susers and Identity Stores Policy Elements Access Policies Access Policies Monitoring and Reports System Administration 	General Image: ACS_4.x Description: Server connection Hostname: 192.168.250.22 Shared Secret: cisco Advanced Options Advanced Options Advanced Options Advanced Options Advanced Port: 1812 Accounting Port: 1813 Server Timeout: 5 Seconds Connection Attempts: 3]		
	Submit Cancel			

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

😭 🏟 🛛 🌈 Cisco Secure ACS			🐴 • 🗟 • 🖶 •	🔂 Page 👻 🎯 Tools 🔹
Cisco Secure A(CISCO EVAL(Days left: 293)		acsadmin	ACS-5-C (Primary)	Log Out About Help
CISCO EVAL(Days left: 293)	Policy Elements > Session Conditions > Custom > Edit: "proxycondition" General Name: proxycondition Description: Condition Dictionary: RADIUS-IETF Attribute: User-Name Belect = Required fields			
System Administration	Submit Cancel			

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 "<u>user@cisco.com</u>" so we are selecting the option *strip end of subject name* and defined the separator "@"

🔆 🏘 🏀 Cisco Secure ACS		🛐 🔹 🔝 👻 🖶 Page 🔹 🎯 Tools 🔹
Cisco Secure A	cs	acsadmin ACS-3-C (Primary) Log Out About Help
My Workspace My Workspace My Workspace More Second Seco	Access Policies > Access Services > Edit "TEST" General Name: TEST Description: Service Type: Service Type: RaDius Proxy User Selected Service Type Selected Service Type: Available External Radius Servers Selected External Radius Servers Available External Radius Servers Selected External Radius Servers ACS=4.x Selected Servers Output Servers Selected External Radius Servers Selected Servers Output Servers Selected External Radius Servers Selected Servers Servers Selected External Radius Servers Selected External Radius Servers Selected Servers Servers Selected External Radius Servers Selected External Radius Servers Selected Servers Servers Selected Servers Selected External Radius Servers Selected Servers Selected Servers Sel	★ Advanced Options ★ Ccounting ✓ 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 't, subject name 'acmetsmith' 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')
	ounini	

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.

🚖 🏘 🏾 🏀 Cisco Secure ACS					🟠 🔹 🖾 👻 🖶 🔹 🔂 Page 🔹 🍈 Tools 🔹					
Cisco Secure A				acsadmin	ACS-5-C (Primary) Log Out About Help					
🕨 🖑 My Workspace	Access Policies > A	ccess Services	> Service Selection F	lles						
▶ 🦃 Network Resources	O Single result	C Single result selection C Rule based result selection								
With the series and Identity Stores	-	Service Selection Policy								
Policy Elements	Filter: Status	-	ch if: Equals	💋 Webpage Dialog	×					
• 🐻	Filter. Jotatus	- Mar	ciril: Equals	https://192.168.250.53/acsadmin/PolicyInputAction.do	🗾 🐼 Certificate Error					
Access Services Service Selection Rules	- 🗖 Stat	tus Name	Protocol	Customize Conditions Available: Selected:						
 Default Device Admin 	1 🗆 🤤	Rule-3	match Radius	ACS Host Name Protocol						
Identity	2 🗖 🤮	Rule-1	match Radius	Compound Condition proxycondition	$\overline{\mathbf{x}}$					
Authorization	3 🗖 🤮	Rule-2	match Tacacs	Device IP Address Device Port Filter						
Identity Authorization TEST Monitoring and Reports System Administration	-			End Station Filter NDG Device Type NDG Castion Time And Date UseCase						
				OK Cancel						
	** E Def		16	https://192.168.250.53/acsadmin/PolicyInputAction.do	SSL					
	** <u>Def</u> Create •	Duplicate	Edit Delete	Or no enabled role matches. DenyAccess O	Customize Hit Count					
	Save Change:	s Disc	ard Changes							

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.

👌 🏟 🛛 🏉 Cisco Secure ACS		🏠 🔹 🔜 👻 🖶 🔹 Page 🔹 🎯 Tojols 🔹 🎽
Cisco Secure A Cisco EVAL(Days left: 293)	CS	acsadmin ACS-S-C (Primary) Log Out About Help
🕨 🚭 My Workspace	Access Policies > Access Services > Service Selection Rules	
Image:	○ Single result selection	
Users and Identity Stores	Service Selection Policy	
Policy Elements	Filter: Status 💌 Match if: Equals 💌 💽 Clear Filter Go	▼
Access Services		esults Hit Count
Service Selection Rules Service Selection Rules	1 🗖 😑 <u>Rule-3</u> match Radius contains @cisco.com TEST	11
Identity	2 🗖 🕒 Rule-1 match 🖉 Cisco Secure ACS Webpage Dialog	
Authorization	3 🔲 🤒 Rule-2 match 🧃 https://192.168.250.53/acsadmin/PolicyInputAction.do	🗾 😵 Certificate Err
Identity Authorization TEST Monitoring and Reports System Administration	Conditions and results are available	right area of the policy rules screen controls which policy e here for use in policy rules.

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.

Isolation in the second sec	um q							abogic
Eile Edit View Favorites Tools Help								
😭 🏟 🏾 🏉 Cisco Secure ACS								🟠 • 🖾 • 🖶 • 🛃 Page • 🍥
Cisco Secure AC	cs						acsadr	nin ACS-5-C (Primary) Log Out Abo
🕨 😪 My Workspace	Acces	s Policie	s > Acces	s Services	> Service Selection	n Rules		
🕨 🦃 Network Resources	0	Sinale	result sele	ection	Rule based resu	It selection		
🕨 🎳 Users and Identity Stores		-	election P					
🕨 🦃 Policy Elements	Filt	ter: St	atus	- Mat	ch if: Equals	Clear F	ilter Go 🔻	
▼ 5₀				mar	on in Feddalo			
 Access Services 			Status	Name	Protocol	Conditions proxycondition	Results Service	Hit Count
 Service Selection Rules Default Device Admin 	1		•	Rule-3	match Radius	contains @cisco.com	TEST	11
Identity	2		0	Rule-1	match Radius	-ANY-	Default Network Access	15
Authorization	3		•	Rule-2	match Tacacs	-ANY-	Default Device Admin	0
 Default Network Access Identity 	-							
Authorization								
🕞 TEST								
Monitoring and Reports								
🕨 🍓 System Administration								
	**		Default		lf no rules defir	ied or no enabled rule matches.	DenyAccess	0
	С	reate	. • Dt	uplicate	Edit Dele	te 🔺 Move to 🗸		Customize Hit Co
	S	ave Ch	ianges	Disc	ard Changes			