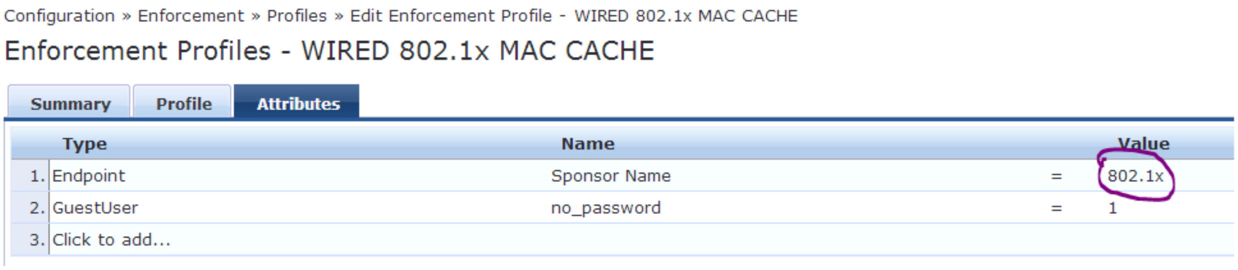
1. Copy “Update Endpoint Known” Enforcement profile
2. Rename, and modify attributes to set Endpoint Sponsor Name = 802.1x (or whatever you want)

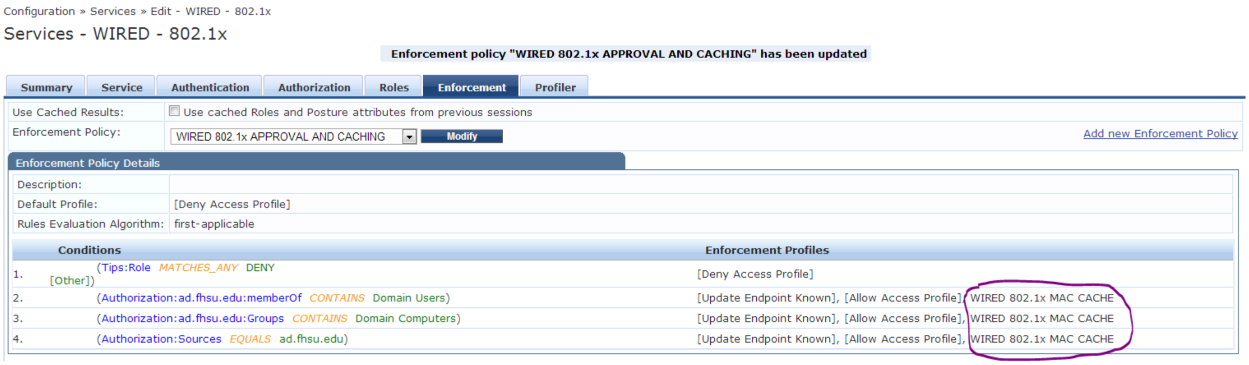


Configuration » Enforcement » Profiles » Edit Enforcement Profile - WIRED 802.1x MAC CACHE

Enforcement Profiles - WIRED 802.1x MAC CACHE

	Type	Name		Value
1.	Endpoint	Sponsor Name	=	802.1x
2.	GuestUser	no_password	=	1
3.	Click to add...			

3. Create generic 802.1x Authentication service to fit your needs
4. In enforcement, add newly created enforcement profile to cache MAC in endpoint db



Configuration » Services » Edit - WIRED - 802.1x

Services - WIRED - 802.1x

Enforcement policy "WIRED 802.1x APPROVAL AND CACHING" has been updated

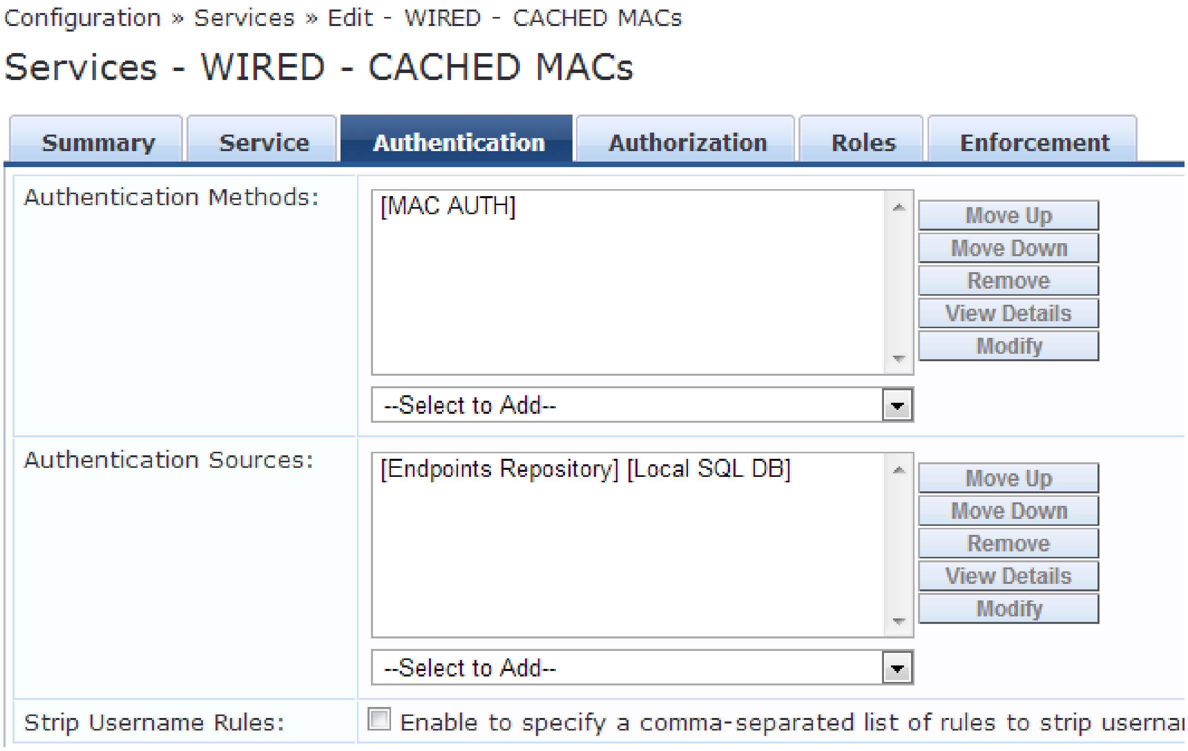
Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	WIRED 802.1x APPROVAL AND CACHING

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role MATCHES_ANY DENY [Other])	[Deny Access Profile]
2.	(Authorization:ad.fhsu.edu:memberOf CONTAINS Domain Users)	[Update Endpoint Known], [Allow Access Profile], WIRED 802.1x MAC CACHE
3.	(Authorization:ad.fhsu.edu:Groups CONTAINS Domain Computers)	[Update Endpoint Known], [Allow Access Profile], WIRED 802.1x MAC CACHE
4.	(Authorization:Sources EQUALS ad.fhsu.edu)	[Update Endpoint Known], [Allow Access Profile], WIRED 802.1x MAC CACHE

5. Create generic MAC AUTH service
6. Configure authentication source to be endpoint database

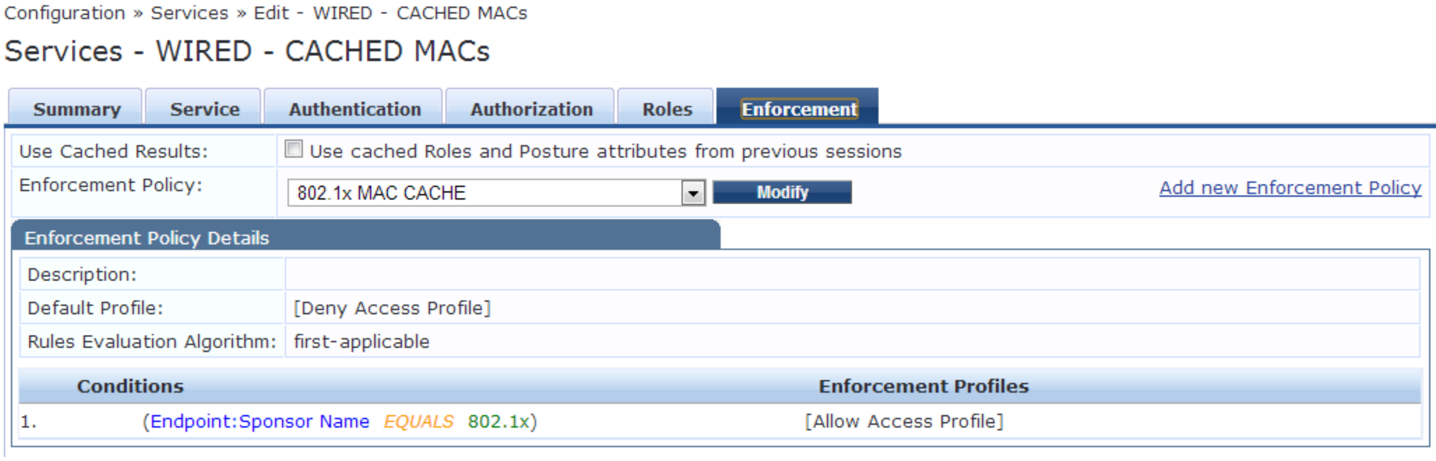


Configuration » Services » Edit - WIRED - CACHED MACs

Services - WIRED - CACHED MACs

Authentication Methods:	[MAC AUTH]
Authentication Sources:	[Endpoints Repository] [Local SQL DB]
Strip Username Rules:	□ Enable to specify a comma-separated list of rules to strip userna

7. Create/use enforcement policy to check for Sponsor Name = 802.1x



Configuration » Services » Edit - WIRED - CACHED MACs

Services - WIRED - CACHED MACs

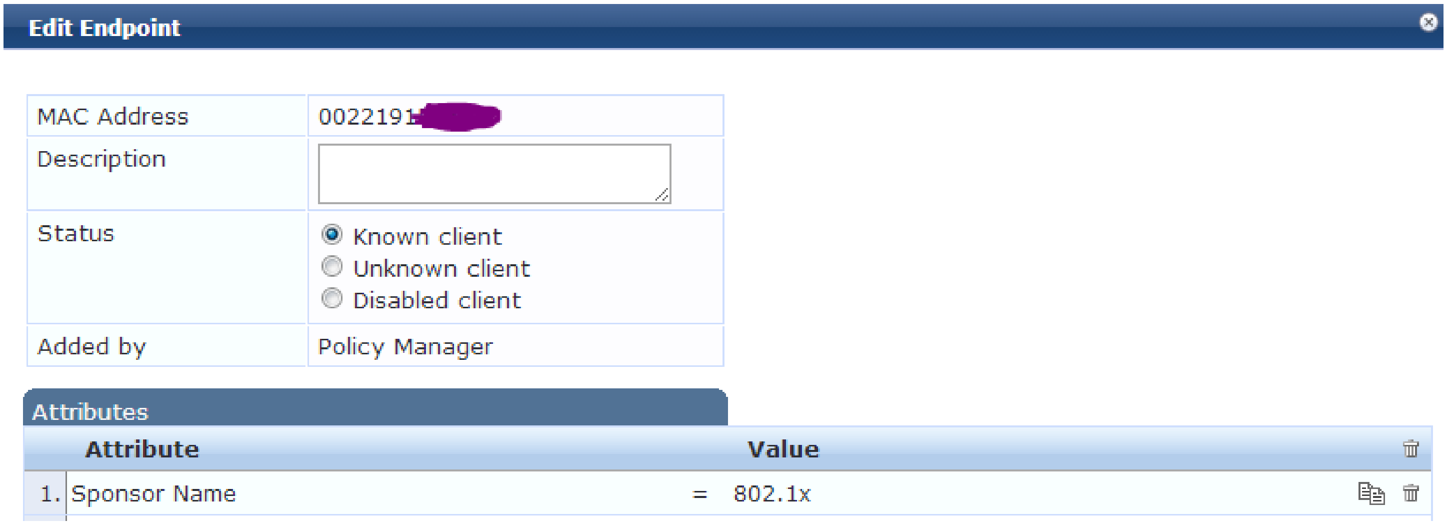
Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	802.1x MAC CACHE

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Endpoint:Sponsor Name *EQUALS* 802.1x)	[Allow Access Profile]

Once a client successfully authenticates using 802.1x, our enforcement profile adds “Sponsor Name = 802.1x” to the endpoint database. This allows us to check for this attribute later on in any other service profile.



Edit Endpoint

MAC Address	0022191[redacted]
Description	
Status	● Known client ○ Unknown client ○ Disabled client
Added by	Policy Manager

Attributes

	Attribute		Value
1.	Sponsor Name	=	802.1x

Why? Broken clients, clients go to sleep, etc. Makes life easier for desktop support when they’re diagnosing authentication problems in the field. No need to worry about port auth, as the device itself should be authorized.