

Preventing AD account lockout for ClearPass

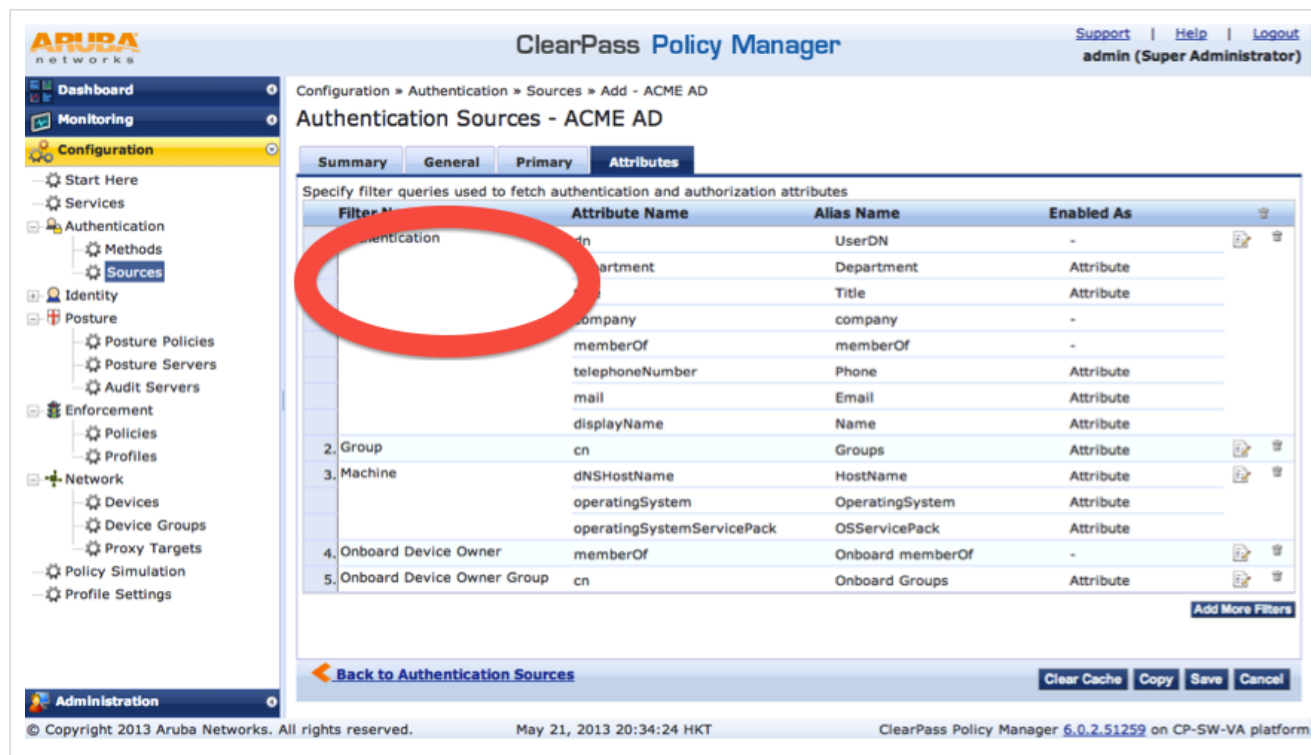
Preventing AD account being locked out by 5 failed auth's via WLAN/Network/Web-Auth

Method: CPPM sends authentication to AD subject to badPwdCount counter in LDAP

Caveat: This won't prevent AD account lock outs by other applications, e.g. Exchange email client

1. Checking on the bad password counter (badPwdCount)

Under Authentication > Sources > [ldap/AD server] > Attributes Click on Filter Name - Authentication



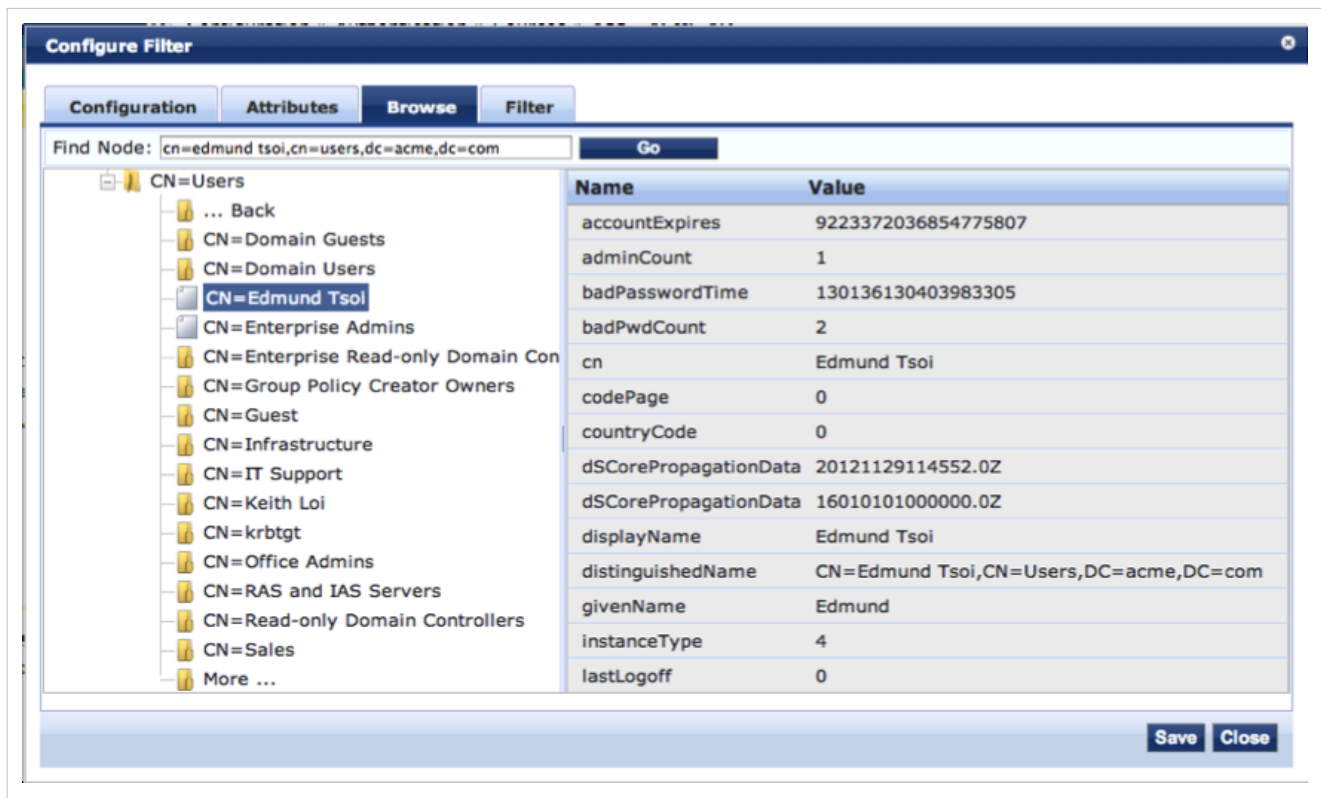
The screenshot shows the ClearPass Policy Manager interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration (selected), Start Here, Services, Authentication (expanded), Identity, Posture, Enforcement, Policies, Profiles, Network, and Administration. The main content area is titled 'Authentication Sources - ACME AD' and has tabs for Summary, General, Primary, and Attributes. The 'Attributes' tab is active, showing a table of LDAP attributes. A red circle highlights the 'Filter Name' column, which contains the value 'Authentication'.

Filter Name	Attribute Name	Alias Name	Enabled As	
Authentication	dn	UserDN	-	
	department	Department	Attribute	
	title	Title	Attribute	
	company	company	-	
	memberOf	memberOf	-	
	telephoneNumber	Phone	Attribute	
	mail	Email	Attribute	
	displayName	Name	Attribute	
	2. Group	cn	Groups	Attribute
	3. Machine	dnsHostName	HostName	Attribute
	operatingSystem	OperatingSystem	Attribute	
	operatingSystemServicePack	OSServicePack	Attribute	
4. Onboard Device Owner	memberOf	Onboard memberOf	-	
5. Onboard Device Owner Group	cn	Onboard Groups	Attribute	

Buttons at the bottom: Back to Authentication Sources, Clear Cache, Copy, Save, Cancel.

Footer: © Copyright 2013 Aruba Networks. All rights reserved. May 21, 2013 20:34:24 HKT ClearPass Policy Manager 6.0.2.51259 on CP-SW-VA platform

Browse the user info > badPwdCount



2. Add the logic into Filter Query

By adding “!(badPwdCount >=4)” into the filter Query, CPPM will not send authentication to AD LDAP if a user has badPwdCount which is not >=4.

The entire filter query is as below: (&(&(sAMAccountName=%{Authentication:Username})(objectClass=user))(!(badPwdCount>=4)))

Configure Filter

Configuration | **Attributes** | **Browse** | **Filter**

Filter Name:

Filter Query:

	Name	Alias Name	Data type	Enabled As	
1.	dn	UserDN	String	-	
2.	department	Department	String	Attribute	
3.	title	Title	String	Attribute	
4.	company	company	String	-	
5.	memberOf	memberOf	String	-	
6.	telephoneNumber	Phone	String	Attribute	
7.	mail	Email	String	Attribute	
8.	displayName	Name	String	Attribute	
9.	Click to add...				

Save **Close**

Article Sources and Contributors

Preventing AD account lockout for ClearPass *Source:* <https://arubapedia.arubanetworks.com/arubapedia/index.php?oldid=94730> *Contributors:* Tarnold, Tbrophy, Trent

Image Sources, Licenses and Contributors

File:CPlockout01.png *Source:* <https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:CPlockout01.png> *License:* unknown *Contributors:* Tbrophy

File:CPlockout02.png *Source:* <https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:CPlockout02.png> *License:* unknown *Contributors:* Tbrophy

File:CPlockout03.png *Source:* <https://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:CPlockout03.png> *License:* unknown *Contributors:* Tbrophy