

Preventing AD account being knockout by 5 failed auth

Objective:

Preventing AD account being knockout by 5 failed auth via WLAN/Network/Web-Auth

Method:

CPPM sends authentication to AD subject to badPwdCount counter in LDAP

Caveat:

This won't prevent AD account knockout by other application, 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

ClearPass Policy Manager

Configuration » Authentication » Sources » Add - ACME AD

Authentication Sources - ACME AD

Filter Name	Attribute Name	Alias Name	Enabled As
1. 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

Back to Authentication Sources

Clear Cache Copy Save Cancel

© 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

Configure Filter

Configuration Attributes Browse Filter

Find Node: cn=edmund tsoi,cn=users,dc=acme,dc=com Go

Name	Value
accountExpires	9223372036854775807
adminCount	1
badPasswordTime	130136130403983305
badPwdCount	2
cn	Edmund Tsoi
codePage	0
countryCode	0
dSCorePropagationData	20121129114552.0Z
dSCorePropagationData	16010101000000.0Z
displayName	Edmund Tsoi
distinguishedName	CN=Edmund Tsoi,CN=Users,DC=acme,DC=com
givenName	Edmund
instanceType	4
lastLogoff	0

Save Close

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**