

Services

Configuration » Services

Services

Add

Import

Export All

Filter: Name

contains

Go

Clear Filter

Show

10

records

#	Order	Name	Type	Template	Status
1.	1	MKK - Wired TLS	RADIUS	802.1X Wired	
2.	2	MKK - Wired MAC Authentication Service	RADIUS	MAC Authentication	
3.	3	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	
4.	4	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	
5.	5	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	
6.	6	[Guest Operator Logins]	Application	Aruba Application Authentication	
7.	7	[Insight Operator Logins]	Application	Aruba Application Authentication	

Showing 1-7 of 7

Reorder

Copy

Export

Delete

MKK - Wired MAC Authentication Service

Configuration » Services » Edit - MKK - Wired MAC Authentication Service

Services - MKK - Wired MAC Authentication Service

Summary

Service

Authentication

Authorization

Roles

Enforcement

Profiler

Name:

MKK - Wired MAC Authentication Service

Description:

MAC-based Authentication Service

Type:

MAC Authentication

Status:

Enabled

Monitor Mode:

☐ Enable to monitor network access without enforcement

More Options:

☒ Authorization ☐ Audit End-hosts ☒ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

Type	Name	Operator	Value	
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)	
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)	
3. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}	
4. Radius:IETF	NAS-IP-Address	BELONGS_TO_GROUP	Switches	
5. Click to add...				

MKK - Wired MAC Authentication Service

Configuration » Services » Edit - MKK - Wired MAC Authentication Service

Services - MKK - Wired MAC Authentication Service

SummaryServiceAuthenticationAuthorizationRolesEnforcementProfiler

Authentication Methods:

[Allow All MAC AUTH]

Move Up

Move Down

Remove

View Details

Modify

[Add new Authentication Method](#)

Authentication Sources:

[Endpoints Repository] [Local SQL DB]

Move Up

Move Down

Remove

View Details

Modify

[Add new Authentication Source](#)

Strip Username Rules:

☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

MKK - Wired MAC Authentication Service

Configuration » Services » Edit - MKK - Wired MAC Authentication Service

Services - MKK - Wired MAC Authentication Service

SummaryServiceAuthenticationAuthorizationRolesEnforcementProfiler

Authorization Details:

Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

Authentication Source	Attributes Fetched From
1. [Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapping attributes -

[Endpoints Repository] [Local SQL DB]

Remove

View Details

Modify

[Add new Authentication Source](#)

--Select to Add--

2

MKK - Wired MAC Authentication Service

Configuration » Services » Edit - MKK - Wired MAC Authentication Service

Services - MKK - Wired MAC Authentication Service

SummaryServiceAuthenticationAuthorizationRolesEnforcementProfiler

Role Mapping Policy:--Select--ModifyAdd new Role Mapping Policy

Role Mapping Policy Details

Description:-

Default Role:-

Rules Evaluation Algorithm:-

Conditions

Role

MKK - Wired MAC Authentication Service

Services - MKK - Wired MAC Authentication Service

SummaryServiceAuthenticationAuthorizationRolesEnforcementProfiler

Use Cached Results:☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy:MKK - Wired MAC-based Authentication EnforModifyAdd new Enforcement Policy

Enforcement Policy Details

Description:

Default Profile:MKK - VLAN 999 Enforcement Profile

Rules Evaluation Algorithm: first-applicable

Conditions

Enforcement Profiles

1. AND (Authorization:[Endpoints Repository]:Category EQUALS Printer) (Authorization:[Endpoints Repository]:Conflict EQUALS false)

2. (Tips:Role EQUALS [User Authenticated])

MKK - VLAN 10 Enforcement Profile

MKK - VLAN 999 Enforcement Profile

MKK - Wired MAC Authentication Service

Configuration » Services » Edit - MKK - Wired MAC Authentication Service

Services - MKK - Wired MAC Authentication Service

SummaryServiceAuthenticationAuthorizationRolesEnforcementProfiler

Endpoint Classification:Select the classification(s) after which an action must be triggered -

Any Category / OS Family / NameRemove

-- Select --

RADIUS CoA Action:[ArubaOS Switching - Terminate Session]View DetailsModifyAdd new RADIUS CoA Action

Authentication Sources - [Endpoints Repository]

- For testing purpose i disabled the cache timeout temporly

Configuration » Authentication » Sources » Add - [Endpoints Repository]

Authentication Sources - [Endpoints Repository]

Summary	General	Primary	Attributes
Name:	<input type="text" value="[Endpoints Repository]"/>		
Description:	<input type="text" value="Authenticate endpoints against Policy Manager local database"/>		
Type:	Local SQL DB		
Use for Authorization:	<input checked="" type="checkbox"/> Enable to use this Authentication Source to also fetch role mapping attributes		
Authorization Sources:	<div><div></div><div>Remove</div><div>View Details</div></div> <div>-- Select --</div>		
Cache Timeout:	<div><input type="text" value="0"/> seconds</div>		
Backup Servers Priority:	<div><div></div><div>Move Up</div><div>Move Down</div><div>Add Backup</div><div>Remove</div></div>		

Cluster Wide Parameters - Policy result cache timeout

- For testing purpose i disabled the cache timeout temporly

The screenshot displays the 'Server Configuration' window in the ClearPass administration console. A 'Cluster-Wide Parameters' dialog box is open, showing a list of parameters. The 'Policy result cache timeout' parameter is highlighted with a red box, indicating it has been set to 0 minutes, which is less than the default value of 5 minutes.

Parameter Name	Parameter Value	Default Value
Policy result cache timeout	0 minutes	5
Free disk space threshold value	30 %	30
Free memory threshold value	20 %	20
Endpoint Context Servers polling interval	60 minutes	60
Syslog Export Interval	120 seconds	120
Automatically check for available Software Updates	TRUE	TRUE
Automatically download Posture Signature and Windows Hotfixes Updates	FALSE	FALSE
Automatically download Endpoint Profile Fingerprints	FALSE	FALSE
Login Banner Text		
Allow Concurrent Admin Login	TRUE	TRUE
Admin Session Idle Timeout	30 minutes	30
CLI Session Idle Timeout	360 minutes	360
Console Session Idle Timeout	360 minutes	360
Disable TLSv1.0 support	None	None
Disable TLSv1.1 support	None	None
Context Security Policy (CCP)	Disable	Disable

Buttons at the bottom of the dialog: Restore Defaults, Save, Cancel.

Endpoint database

- Before starting the endpoint database is empty. I reset it a hour before the test.

Configuration » Identity » Endpoints

Endpoints

5 endpoints deleted successfully

Filter: MAC Address contains [] Go Clear Filter

Show 10 records

#	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled
1.	000c291dbf5b	clearpass	Server	ClearPass	Unknown	Yes

Showing 1-1 of 1

Authentication Records Bulk Update Bulk Delete Trigger Server Action Update Fingerprint Export Delete

Connect the computer

- When i connect the computer, clearpass receive the DHCP request from the DHCP helper and profiled it correctly.

Configuration » Identity » Endpoints

Endpoints

Filter: MAC Address contains [] Go Clear Filter

Show 10 records

#	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled
1.	000c291dbf5b	clearpass	Server	ClearPass	Unknown	Yes
2.	001e0b059b10	imac2	Computer	Windows	Unknown	Yes

Showing 1-2 of 2

Authentication Records Bulk Update Bulk Delete Trigger Server Action Update Fingerprint Export Delete

Endpoint information

Edit Endpoint

EndpointAttributesFingerprints

MAC Address	001e0b059b10	IP Address	172.16.255.100
Description		Static IP	FALSE
Status	<div><div>Known client</div><div>Unknown client</div><div>Disabled client</div></div>	Hostname	imac2
MAC Vendor	Hewlett Packard	Device Category	Computer
Added by	Policy Manager	Device OS Family	Windows
Online Status	Not Available	Device Name	Windows Vista/7/2008
Connection Type	Wired	Added At	May 13, 2018 20:49:42 CEST
Switch IP	172.16.10.30	Last Profiled At	May 13, 2018 20:49:42 CEST
Switch Port	25		

SaveCancel

Endpoint information

Edit Endpoint

Endpoint

Attributes

Fingerprints

Attribute	Value	
1.	Click to add...	

Endpoint information

- DHCP Fingerprint received

Edit Endpoint

Endpoint

Attributes

Fingerprints

Endpoint Fingerprint Details

DHCP Option60:	MSFT 5.0
DHCP Options:	53,61,50,12,81,60,55
DHCP Option55:	1,15,3,6,44,46,47,31,33,121,249,43

Accesstracker

- After profiling is done correctly the COA Port termination works correctly. Because its a profiled as a computer, its stays in vlan 999. This is out of scope of the test.

Monitoring » Live Monitoring » Access Tracker

Access Tracker May 13, 2018 20:50:29 CEST Auto Refresh

[All Requests] clearpass (172.16.10.3) Last 1 day before Today Edit

Filter: Request ID contains Go Clear Filter Show 100 records

#	Server	Source	Username	Service	Login Status	Request Timestamp	Enforcement Profiles
1.	172.16.10.3	RADIUS	001e0b059b10	MKK - Wired MAC Authentication Service	ACCEPT	2018/05/13 20:49:56	MKK - VLAN 999 Enforcement Profile
2.	172.16.10.3	RADIUS	001e0b059b10	MKK - Wired MAC Authentication Service	ACCEPT	2018/05/13 20:49:39	MKK - VLAN 999 Enforcement Profile

Remove the endpoint

aruba ClearPass Policy Manager Support | Help | Logout
admin (Super Administrator)

Configuration » Identity » Endpoints

Endpoints Add Import Export All

Endpoint deleted successfully

Filter: MAC Address contains Go Clear Filter Show 10 records

#	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled
1.	000c291dbf5b	clearpass	Server	ClearPass	Unknown	Yes

Showing 1-1 of 1 Authentication Records Bulk Update Bulk Delete Trigger Server Action Update Fingerprint Export Delete

Reconnect the computer

- When reconnect within 5 minutes the endpoint isnt doing profiling again.

Configuration » Identity » Endpoints

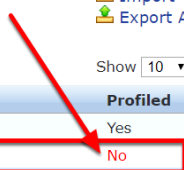
Endpoints

Filter: contains

Show records

#	<input type="checkbox"/>	MAC Address ▲	Hostname	Device Category	Device OS Family	Status	Profiled
1.	<input type="checkbox"/>	000c291dbf5b	clearpass	Server	ClearPass	Unknown	Yes
2.	<input type="checkbox"/>	001e0b059b10				Unknown	No

Showing 1-2 of 2



Endpoint information

- No dhcp fingerprint received
- If i look at the DHCP server, DHCP is updates
- If i look at the coreswitch, display dhcp statistics shows the DHCP request is forwarded to the IP Helper "Clearpass" correctly

Edit Endpoint

Endpoint	Attributes
MAC Address	001e0b059b10
Description	
Status	<input type="checkbox"/> Known client <input checked="" type="radio"/> Unknown client <input type="radio"/> Disabled client
MAC Vendor	Hewlett Packard
Added by	Policy Manager
Online Status	Not Available
Connection Type	Wired
Switch IP	172.16.10.30
Switch Port	25

Save **Cancel**

Accesstracker

- No COA Session termination take place because the is no profiling done.

Monitoring » Live Monitoring » Access Tracker

Access Tracker May 13, 2018 20:51:40 CEST Auto Refresh

[All Requests] clearpass (172.16.10.3) Last 1 day before Today Edit

Filter: Request ID contains Go Clear Filter Show 100 records

#	Server	Source	Username	Service	Login Status	Request Timestamp	Enforcement Profiles
1.	172.16.10.3	RADIUS	001e0b059b10	MKK - Wired MAC Authentication Service	ACCEPT	2018/05/13 20:51:09	MKK - VLAN 999 Enforcement Profile
2.	172.16.10.3	RADIUS	001e0b059b10	MKK - Wired MAC Authentication Service	ACCEPT	2018/05/13 20:49:56	MKK - VLAN 999 Enforcement Profile
3.	172.16.10.3	RADIUS	001e0b059b10	MKK - Wired MAC Authentication Service	ACCEPT	2018/05/13 20:49:39	MKK - VLAN 999 Enforcement Profile