

Authentication

Services - CPPM_OnGuard Aruba 802.1X Wireless

Summary	Service	Authentication	Authorization	Roles	Enforcement
Authentication Methods:					
		[EAP MSCHAPv2] [EAP PEAP]	<div>Move Up</div> <div>Move Down</div> <div>Remove</div> <div>View Details</div> <div>Modify</div>		
		--Select to Add--			
Authentication Sources:					
		HCCI-AD [Active Directory]	<div>Move Up</div> <div>Move Down</div> <div>Remove</div> <div>View Details</div> <div>Modify</div>		
		--Select to Add--			
Strip Username Rules:		<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes			
Service Certificate:		--Select to Add--			

Authorization

Services - CPPM_OnGuard Aruba 802.1X Wireless

Summary	Service	Authentication	Authorization	Roles	Enforcement
Authorization Details:					
Authorization sources from which role mapping attributes are fetched (for each Authentication Source)					
		Authentication Source	Attributes Fetched From		
		1. HCCI-AD [Active Directory]	HCCI-AD [Active Directory]		
Additional authorization sources from which to fetch role-mapping attributes -					
		[Endpoints Repository] [Local SQL DB]	<div>Remove</div> <div>View Details</div> <div>Modify</div>		
		--Select to Add--			

Role Mapping

Services - CPPM_OnGuard Aruba 802.1X Wireless

Summary	Service	Authentication	Authorization	Roles	Enforcement
Role Mapping Policy:		CPPM_OnGuard_Wireless_Role_Mapping		<div>Modify</div>	
Role Mapping Policy Details					
Description:					
Default Role:		[Guest]			
Rules Evaluation Algorithm:		first-applicable			
Conditions		Role			
1. (Endpoint:Ingrnet-Machine-Auth-Device EQUALS true)		Ingrnet-Domain-Device			
2. (Authorization:HCCI-AD:UserDN ENDS_WITH OU=Computers,OU=India,DC=ingrnet,DC=com)		Ingrnet-Machine-Auth			
3. (Authorization:HCCI-AD:Department CONTAINS Information Technology)		HCCI_IT			

Enforcement

Services - CPPM_OnGuard Aruba 802.1X Wireless

Summary

Service

Authentication

Authorization

Roles

Enforcement

Use Cached Results:

☒ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy:

CPPM_OnGuard Aruba 802.1X Wireless Enforcer

Modify

Add new Enfor

Enforcement Policy Details

Description:

Default Profile:

CPPM Quarantine Role

Rules Evaluation Algorithm:

first-applicable

Conditions	Enforcement Profiles
1. <div>(Tips:Role EQUALS HCCI_IT)</div> <div>AND (Tips:Posture EQUALS UNKNOWN (100))</div> <div>AND (Tips:Role EQUALS Ingrnet-Domain-Device)</div> <div>(Tips:Posture EQUALS QUARANTINE (20))</div>	CPPM Unknown Role, Ingrnet - Machine Auth Allowed
2. <div>(Tips:Role EQUALS HCCI_IT)</div> <div>AND (Tips:Role EQUALS Ingrnet-Domain-Device)</div> <div>(Tips:Posture EQUALS HEALTHY (0))</div>	CPPM Employee Role, Ingrnet - Machine Auth Allowed
3. <div>(Tips:Role EQUALS HCCI_IT)</div>	CPPM Employee Role, Ingrnet - Machine Auth Allowed, [Update Endpoint Known]

Endpoint Attribute

Ingrnet-Machine-Auth-Device	Endpoint	Boole
-----------------------------	----------	-------

1-1 of 1

Edit Attribute

Entity

Endpoint

Name

Ingrnet-Machine-Auth-Device

Data Type

Boolean

Is Mandatory

☐ Yes ☒ No

Default Value (optional)

☐ True ☐ False (e.g., true / false)

Save

Cancel

Roles

Configuration » Identity » Roles

Roles

Filter:

Name

contains

ingrnet

Go

Clear Filter

#	<input type="checkbox"/>	Name	Description
1.	<input type="checkbox"/>	Ingrnet-Domain-Device	This role is to validate the Machine Authenticated devices
2.	<input type="checkbox"/>	Ingrnet-Machine-Auth	

Showing 1-2 of 2

Enforcement Profile

Enforcement Profiles - Ingrnet - Machine Auth Allowed

Summary	Profile	Attributes
Profile:		
Name:	Ingrnet - Machine Auth Allowed	
Description:		
Type:	Post_Authentication	
Action:		
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Endpoint	Ingrnet-Machine-Auth-Device	= true

Access Tracker Log

Rebooted the machine and this log is shown while loading the OS.

Request Details			
Summary	Input	Output	Alerts
Login Status:	TIMEOUT		
Session Identifier:	R0002109e-03-5af56d26		
Date and Time:	May 11, 2018 15:45:03 IST		
End-Host Identifier:	FCF8AEE377DB (Computer / Windows / Windows 10)		
Username:	host/IN-NACTEST.ingrnet.com		
Access Device IP/Port:	131.163.152.9:0 (HCCI-WLC / Aruba)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	CPPM_OnGuard Aruba 802.1X Wireless		
Authentication Method:	EAP-PEAP		
Authentication Source:	AD:in-hyd-dc20.ingrnet.com		
Authorization Source:	[Endpoints Repository]		
Roles:	[Guest]		
Enforcement Profiles:	CPPM Quarantine Role		
Service Monitor Mode:	Disabled		
Online Status:	Offline		
◀ Showing 7 of 1-50 records ▶▶			
Show Configuration		Export	Show Logs
Close			