ōrdr

Ordr and HPE Aruba ClearPass Policy Manager Integration Guide

Organizations in healthcare, manufacturing, retail, transportation, and logistics are embracing digital transformation, powered by connected devices including Internet of Things (IoT) and Operational Technology (OT). The enterprise IT network is now the melting pot for a highly eclectic, hyperconnected mix of devices that businesses must manage and protect or face immediate security risk.

Ordr allows organizations to rapidly inventory every **thing** in their network, classify it based on type and business function, and assess it for risk. Ordr learns behaviors and creates device flow genomes, so security teams can baseline what each device or group of devices should be talking to. When combined with HPE Aruba ClearPass Policy Manager (CPPM), organizations can quickly gain complete visibility into every connected device and deploy segmentation to proactively protect and reactively respond and mitigate threats. This includes Zero Trust policy enforcement and microsegmentation to isolate groups or individual devices from non-essential access while protecting them from attack and compromise on existing networking and security infrastructure.

This guide describes in detail how to configure Ordr SCE with HPE Aruba CPPM to provide advanced connected device discovery (including IoT/OT), classification, and the simplification of secure network access control and segmentation policy to all networked users and devices.

Table of Contents

Ordr SCE and HPE Aruba CPPM Integration	3
Ordr SCE and HPE Aruba CPPM Integration Use Cases	5
Configuration	7
Prerequisites	7
Supported Software Versions	7
Communication Ports	7
RADIUS Change of Authorization	7
Overview	8
Part 1: Basic ClearPass Setup	8
Step 1 Create an Ordr API admin user	9
Step 2 Configure a new ClearPass operator profile	
Step 3 Configure an API client with new operator role	
Step 4 Configure ClearPass service to enable OAuth2 API User Access	
Step 5 Optional: Enable ClearPass for Insight Integration	
Step 6 Configure Ordr SCE Service Integration for ClearPass	
Part 2: Rich Device Context Sharing	20
Step 1 Verify creation of new custom dictionary attributes in ClearPass	
Step 2 Verify automated endpoint creation and context sharing from Ordr SCE to ClearPass	
Step 3 Verify enhanced visibility in ClearPass Policy Manager (Optional)	25
Part 3: Blocklisting and Dynamic Quarantine of Threats	26
Step 1 Create a ClearPass role for Quarantine/Blocklist devices	
Step 2 Bind an Enforcement Profile to Ordr blocklisted devices	
Step 3 Trigger device blocklisting in Ordr SCE	
Step 4 Verify endpoint quarantine in ClearPass Policy Manager	
Step 5 Verify new policy assignment for the blocklisted endpoint(s)	
Summary	36

Ordr SCE and HPE Aruba CPPM Integration

HPE Aruba ClearPass Policy Manager (to be referenced simply as CPPM or ClearPass from this point on) provides endpoint visibility and identity-based access control for the Enterprise. To make these technologies effective for IoT requires additional intelligence and automation. This is where Ordr Systems Control Engine (SCE) adds significant value. Ordr SCE helps you to maximize your HPE Aruba CPPM investment to deliver effective IoT and digital OT security to devices previously hard to secure. Its device classification, network awareness, security intelligence, and ability to suggest enforcement rules simplifies the process of creating, provisioning, and managing your IoT segmentation policy.

Ordr SCE complements HPE Aruba CPPM to simplify the tasks that often overwhelm and stall IoT security initiatives by:

- Automating IoT inventory discovery, classification, and categorization, and sharing detailed device context with ClearPass
- Providing rich analytics about the behavior of all devices that guides segmentation design, streamlines the segmentation implementation, and audits the result to assure accuracy and effectiveness
- Quickly contain threats and protect at-risk devices
- Accelerating ClearPass deployments with powerful yet easy-to-use tools that provide accurate device information and automate steps that are traditionally error-prone and labor intensive



The integrated Ordr SCE and HPE Aruba CPPM solution makes it easy to get rich visibility for IoT and unmanaged devices and to simplify segmentation projects. The solution provides detailed classification and context for every connected device, automatically groups devices into CPPM policy groups for role-based access and facilitates software-defined segmentation to provide more precise controls for every IoT device in the network. By providing continuous, multi-level security monitoring of all device communications, Ordr SCE detects anomalous behavior and shares this information with ClearPass to implement network access control based on vulnerability, threat, and risk ratings. Ordr SCE also integrates with HPE Aruba CPPM to streamline the process of containing threats based on the organization's access policy such as blocking unauthorized devices, quarantining them, or limiting their network access.

Ordr SCE and HPE Aruba CPPM Integration Use Cases

This document focuses on how to integrate Ordr SCE with HPE Aruba CPPM for the following use cases:

- Seamless sharing of Ordr SCE device classification, grouping, and highdefinition details
- Continuous update of device compliance, threats, vulnerabilities and risk scores—all without the use of agents
- Dynamic containment of threats based on anomalous behavior or other indicators of compromise
- Automatic learning of device behavior and detection of abnormal traffic to augment ClearPass anomaly tracking

The diagram below illustrates the integration of Ordr SCE with HPE Aruba CPPM. Ordr SCE Sensors provide agentless, passive data collection which feeds the Ordr SCE Analytics Server. Sensors may be centralized or distributed based on collection requirements. The Analytics Server analyzes the data to automatically discover and classify all IoT and non-IoT devices. It then feeds the rich contextual data to ClearPass.



Providing advanced IoT device information to ClearPass is only one piece of the puzzle. To move to segmentation and the enforcement of policies, NAC administrators must understand which traffic to allow and deny. Ordr SCE provides this insight by tracking all device communications to assist administrators in the creation of segmentation and enforcement policies in HPE Aruba CPPM.

Once granted network access by ClearPass, Ordr SCE continuously tracks all devices for known threats and vulnerabilities and monitors communication flows for anomalous traffic and threat activity. Ordr SCE can notify HPE Aruba CPPM of at-risk, vulnerable, and compromised devices to trigger the necessary quarantine and remediation response.

Configuration

Prerequisites

Supported Software Versions

- Ordr SCE version 7.2.R6 and above
- ClearPass Policy Manager version 6.8.7 and above

Communication Ports

• API from the Ordr service integration node to CPPM server: TCP/443

Note: All communications between Ordr SCE and Aruba CPPM occur through the Ordr service integration node. While the Ordr integration node can be deployed on a dedicated hardware or virtual appliance, it is commonly enabled on one of the existing Ordr Sensors with Service Node set to 'Yes'. This ensures a secure communication channel between an on-premises node and the ClearPass servers.

Be sure to have at least one Network Device Group configured in CPPM to facilitate the provisioning of quarantine and segmentation policies from Ordr SCE. Network Device Groups are referenced in CPPM Enforcement Profiles.

It is also recommended to perform a backup of the ClearPass Policy Manager configuration database and export all endpoint data as well as enforcement policies and profiles prior to starting the integration.

RADIUS Change of Authorization

Dynamic containment of threats is based on the Ordr SCE blocklisting feature. Realtime enforcement of blocklisted/quarantined devices relies on RADIUS Change of Authorization (CoA) support. RADIUS CoA allows network sessions to be reauthorized

on demand and not wait for the client to manually reconnect or the network device to reauthentication based on a fixed interval. To support on-demand reauthorization, Aruba CPPM must be configured for RADIUS Change of Authorization (CoA). Additionally, the wired switches and wireless controllers to which target devices are connected must also be configured for RADIUS CoA. The RADIUS CoA standard is defined by RFC 3576 so some network device configurations may refer to this specification. For example, Aruba wireless controllers should define Aruba CPPM as an RFC 3576 (CoA) server. If RADIUS CoA is not configured, or improperly configured, then the Ordr blocklisting feature can still function, but the quarantine enforcement policy will not take effect until the client manually disconnects/reconnects to the network, or the network device performs a periodic reauthentication on the session.

Overview

- Part 1: Basic setup
 - Configure ClearPass API access for Ordr SCE
 - Configure Ordr SCE Service Integration with ClearPass
- Part 2: Rich device context sharing to ClearPass
 - Verify creation of new custom dictionary attributes in ClearPass
 - Verify automated device update and context sharing from Ordr SCE to ClearPass
 - Verify enhanced visibility in ClearPass Policy Manager and Insight
- Part 3: Blocklisting and dynamic quarantine of threats
 - o Bind quarantine Enforcement Profile to Ordr blocklisted devices
 - Trigger device blocklisting in Ordr SCE
 - Verify endpoint quarantine in ClearPass

Part 1: Basic ClearPass Setup

Ordr SCE integration with HPE Aruba CPPM uses the ClearPass REST APIs secured through an OAuth2 framework. CPPM supports the use of different grant types for OAuth. SCE uses the *password* grant-type.

Ordr SCE can also leverage the legacy "tips" XML API. For the legacy XML API, basic HTTP authentication is used. The XML API is an optional API that can be enabled/disabled to directly update CPPM's derived endpoint fingerprint/classification for a profiled endpoint.

These steps enable Ordr SCE to update ClearPass endpoints with rich device context and facilitate threat containment.

Step 1 Create an Ordr API admin user

For Ordr SCE to share rich device context with ClearPass Policy Manager and ClearPass Insight, as well as automate policy enforcement and segmentation, an admin account is required that provides the minimal but necessary access using ClearPass APIs.

- 1) Login to ClearPass Policy Manager and define a new admin user for Ordr SCE integration under **Administration > Users and Privileges > Admin Users**.
- 2) Click **Add** in the upper right corner and complete the form as shown in the example:
 - a. Assign a User ID such as **ordradmin**. Store the User ID and Password values in a secure location. These credentials will be required to complete the integration from Ordr SCE.
 - b. Verify the user account is enabled.
 - c. Set Privilege Level to **API Administrator.** Specific API access privileges will be configured for the API client in the following steps.

Edit Admin User	8
User ID:	ordradmin
Name:	Ordr API Admin
Password:	
Verify Password:	
Enable User:	✓ (Check to enable user)
Privilege Level	API Administrator
	Save Cancel

3) Click Add when finished.

Step 2 Configure a new ClearPass operator profile

Operator Profiles are used extensively within ClearPass to secure access to any CPPM function. Operator Proles were originally created to administer and control ClearPass Guest access but have since been extended to control access to Policy Manager functions as well. The profiles also provide granular control over API access using configurable permissions over policy functions that include no-access, read, read/write, and read/write/delete.

- Login to ClearPass Guest and configure a new Operator Role under Administration > Operator Logins > Profiles.
- 2) Click Create a new operator profile in the upper right corner.
- 3) Assign a name to the new role such as Ordr API Administrator
- 4) The Access section is used to configure access permissions. By default, the new Operator Profile should have "No Access" assigned to all functions.
 - a. Change the Operator Privileges for API Services from "No Access" to "Custom..." and then set the individual privileges as shown in the example:

Ordr and HPE ARUBA CPPM Integration Guide

A	P ele	PI Services Cust lect operator permissions for API access and management.	tom	▼
4	2	Allow API Access O N Operators with this privilege are permitted to make API calls. Additio	No Access 🔘 mal privileges ar	Allow Access e also required, depending on the API.
æ	2	API Documentation Operators with this privilege can browse and interact with the API Ex	No Access O	Allow Access
đ	2	Configure SOAP Web Services (Legacy)	No Access O eb services.	Read Only O Full
6	2	List SOAP Web Services (Legacy) Operators with this privilege can browse the available SOAP web serv	No Access O	Read Only O Full the service definitions (WSDL).
æ	2	Manage API Clients O M Operators with this privilege may view and manage API clients (OAut	No Access O	Read Only 🖲 Full on).
đ	2	SOAP API (Legacy) Operators with this privilege can use SOAP web services to perform s	No Access O system functions	Read Only O Full . Additional privileges are also required, depending on the API
æ	3	NMLRPC API (Legacy)	No Access 🔘 e XMLRPC API. A	Allow Access Additional privileges are also required, depending on the API.

b. Change the Operator Privileges for Policy Manager from "No Access" to "Custom..." and then set the individual privileges as shown in the table:

Policy Manager Permissions	No Access	Read	Read,	Read, Write,
			Write	Delete
Agentless OnGuard - Settings	•			
Agentless OnGuard - Subnet Mappings	•			
Application Licenses	•			
Authentication - Methods	•			
Certificate - Revocation List	•			
Certificate - Trust List	•			
Certificates	•			
Clearpass Portal	•			
Configuration - Network Scan	•			
Configuration - Services	•			
Device Profiler - Device Fingerprint	•			
Dictionaries - Attributes				•
Dictionaries - Context Server Actions				•
Dictionaries - Fingerprints				•
Dynamic Authorization - Session Action				•
Events - Login Audit	•			
Events - System Events	•			
External Accounts	•			
External Accounts - Profiler Subnet Mappings	•			
External Servers - Endpoint Context Servers	•			
External Servers - File Backup Server	•			
External Servers - SNMP trap receivers	•			
External Servers - Syslog Export Filters				•

Ordr and HPE ARUBA CPPM Integration Guide

External Servers - Syslog Targets			•
Identity - Endpoints			•
Identity - Local Users	•		
Identity - LocalUser Password Policy	•		
Identity - Role Mapping			•
Identity - Roles			•
Identity - Static Host Lists			•
Insight - Endpoints			•
Messaging Services - Messaging Setup	•		
Network - Device Groups			•
Network - Devices			•
Network - Event Sources			•
Network - Proxy Targets	•		
OnGuard - Policy Manager Zones	•		
OnGuard - Settings	•		
Platform - Access Control			•
Platform - Cluster Wide Parameters	•		
Platform - Device Insight	•		
Platform - Policy Manager Zones	•		
Platform - Server SNMP	•		
Platform - Servers		•	
Platform - Service Parameters	•		
Platform - Services	•		
Users and Privileges - Admin Privileges	•		
Users and Privileges - Admin User Password Policy	•		
Users and Privileges - Admin Users			•

- 5) Click **Save Changes** to commit the changes.
- 6) From the list of Operator Profiles, select the newly created profile for Ordr SCE API access, and then click **Show Details**. The profile information including permission settings should appear like the following example:

இ Ordr API Ad	ministrator Ordr API user to attributes and e	update ClearPass Policy Manager endpoint nable automated policy enforcement					
1 Hide Details	📴 Edit 😵 Delete 📄 Duplicate 🔩 Sho	w Usage					
Operator Profile							
Name:	Ordr API Administrator						
Description:	Ordr API user to update ClearPass Policy Mana policy enforcement	ager endpoint attributes and enable automated					
Operator logins:	Enabled						
	API Services	Custom					
	💩 Allow API Access	🖌 Allow Access					
	🚵 Manage API Clients	🖌 Full Access					
	🚵 XMLRPC API (Legacy)	🖌 Allow Access					
	Policy Manager	Custom					
	💩 Dictionaries - Attributes	🖌 Full Access					
	💩 Dictionaries - Context Server Actions	🖌 Full Access					
	💩 Dictionaries - Fingerprints	🖌 Full Access					
	💩 Dynamic Authorization - Session Action	n 🧹 Full Access					
	💩 External Servers - Syslog Export Filter:	s 🧹 Full Access					
Privileges:	🚵 External Servers - Syslog Targets	✓ Full Access					
	🚵 Identity - Endpoints	Full Access					
	🚵 Identity - Role Mapping	Full Access					
	Identity - Koles	Full Access					
	Insight - Endpoints						
	A Network - Device Groups	Full Access					
	🚵 Network - Devices	✓ Full Access					
	📥 Network - Event Sources	🖌 Full Access					
	💩 Platform - Access Control	🖌 Full Access					
	💩 Platform - Servers	🛶 Read Only					
	🚵 Users and Privileges - Admin Users	🖌 Full Access					
Skin:							
Start Page:	(Default)						
Language:	(Default)						
Time Zone:	(GMT-05:00) America/New York; Eastern (mo	st areas)					

If changes are required, simply click **Edit** under the profile name and make changes as needed. Be sure to click **Save Changes** when finished.

Step 3 Configure an API client with new operator role

- In the ClearPass Guest interface, navigate to Administration > API Services > API Clients.
- 2) Click Create API Client in upper right corner.
- 3) Complete the form as shown in the example:
 - a. For Client ID, assign the same name used to create the Ordr API Admin in Step 1 (**ordradmin** in our example).
 - b. Under Operating Mode, select ClearPass REST API Client will be used for API calls to ClearPass
 - c. Under Operator Profile, select the profile created in the previous steps (**Ordr API Administrator** in our example).
 - d. Set Grant Type to Username and password credentials (grant_type=password).
 - e. Enable the checkbox This client is a public (trusted) client.

	Edit API Client
* Client ID:	ordradmin The unique string identifying this API client. Use this value in the OAuth2 "client_id" parameter.
Description:	Ordr API user to update ClearPass Policy Manager endpoint attributes and enable automated policy enforcement Use this field to store comments or notes about this API client.
Enabled:	Enable API client
* Operating Mode:	ClearPass REST API - Client will be used for API calls to ClearPass Select the purpose of this API Client.
* Operator Profile:	Ordr API Administrator V The operator profile applies role-based access control to authorized OAuth2 clients. This determines what API objects and methods are available for use.
* Grant Type:	Username and password credentials (grant_type=password) Only the selected authentication method will be permitted for use with this client ID.
Refresh Token:	Allow the use of refresh tokens for this client An OAuth2 refresh token may be used to obtain an updated access token. Use grant_type=refresh_token for this.
Public Client:	This client is a public (trusted) client Public clients have no client secret.
Access Token Lifetime:	8 hours Specify the lifetime of an OAuth2 access token.
Refresh Token Lifetime:	14 days ▼ Specify the lifetime of an OAuth2 refresh token.
	Save Changes 🚫 Cancel

4) Click Create API Client to commit the changes.

Step 4 Configure ClearPass service to enable OAuth2 API User Access

To permit the Ordr API client to authenticate to ClearPass using grant_type=password, it is necessary to add an OAuth2 application service to ClearPass Policy Manager that uses the Admin User Repository for checking credentials. A Service Template will be used to simplify the process.

- Return to the ClearPass Policy Manager interface and navigate to Configuration > Service Templates & Wizards.
- 2) Select OAuth2 API User Access from the list:



3) Enter Ordr under Name Prefix and click Add Service:

Service Templates	s - OAuth2 API User Access			
Name Prefix.**:	Ordr			
	Dese	ription		
Service template for API clients authenticating with username and password (OAuth2 grant type "password").				
Back to Service Templa	ates & Wizards	Delete Next →	Add Service Cano	

- 4) A new Service should appear under Configuration > Services named Ordr OAuth2 API User Access. Verify that the OAuth2 service is listed with status enabled ♥.
- 5) Open the OAuth2 service and under the Summary tab, verify the Admin User Repository is listed as an Authentication Source. This is the repository where the Ordr API Admin User was created in Step 1.

Configuration » Services » Edit - OrdrAPIClientAuthService						
Services - OrdrAPIClientAuthService						
Summary	Service	Authentication	Roles	Enforcement		
Service:						
Name: OrdrAPIClientAuthService						
Description:		Authentication	Service fo	r Applications		
Type:		Aruba Applicati	on Auther	itication		
Status:		Enabled				
Monitor Mode	:	Disabled				
More Options	:	-				
Service Rule						
Match ANY of the following conditions:						
Match ANY of	the followin	g conditions:				
Match ANY of Type	the followin	g conditions: Name	Oper	ator	Value	
Match ANY of Type 1. Applica	the followin ation	g conditions: Name Name	Oper EQUA	ator LS	Value OAuth2	
Match ANY of Type 1. Applica Authenticati	the followin ation on:	g conditions: Name Name	Oper EQUA	ator LS	Value OAuth2	
Match ANY of Type 1. Applica Authentication Authentication	the followin ation on: n Sources:	g conditions: Name Name 1. [Admin User 2. [Local User I	Oper EQUA Repositor	ator LS 'Y] [Local SQL D '] [Local SQL DB	Value OAuth2 B]	
Match ANY of Type 1. Applica Authenticati Authentication Strip Usernan	the followin ation on: n Sources: ne Rules:	g conditions: Name Name 1. [Admin User 2. [Local User I -	Oper EQUA Repository	ator LS 'Y] [Local SQL D '] [Local SQL DB	Value OAuth2 B]	
Match ANY of Type 1. Applica Authenticati Authentication Strip Usernan Roles:	the followin ation on: n Sources: ne Rules:	g conditions: Name Name 1. [Admin User 2. [Local User I -	Oper EQUA Repository	ator LS 'Y] [Local SQL D '] [Local SQL DB	Value OAuth2 B]	
Match ANY of Type 1. Applica Authentication Strip Usernan Roles: Role Mapping	the following ation on: n Sources: ne Rules: Policy:	g conditions: Name Name 1. [Admin User 2. [Local User I - [Guest Roles]	Oper EQUA Repositor	ator LS 'Y] [Local SQL D '] [Local SQL DB	Value OAuth2 B]	
Match ANY of Type 1. Applica Authentication Strip Usernan Roles: Role Mapping Enforcement	the following ation on: n Sources: ne Rules: Policy: t:	g conditions: Name Name 1. [Admin User 2. [Local User I - [Guest Roles]	Oper EQUA Repository	ator LS 'Y] [Local SQL D '] [Local SQL DB	Value OAuth2	
Match ANY of Type 1. Applica Authentication Strip Usernan Roles: Role Mapping Enforcement Use Cached R	the following ation on: n Sources: ne Rules: Policy: t: Results:	g conditions: Name Name 1. [Admin User 2. [Local User I - [Guest Roles] Disabled	Oper EQUA Repositor	ator LS 'Y] [Local SQL D '] [Local SQL DB	Value OAuth2	

6) From the Authentication tab, select Admin User Repository in the list and Move Up above Local User Repository. This will ensure the Admin User Repository is checked first for the new API user account.

Note: The Local User Repository is not required for Ordr API access.

Step 5 Optional: Enable ClearPass for Insight Integration

- From the ClearPass Policy Manager interface, navigate to Administration > Server Manager > Server Configuration.
- 2) Select the ClearPass Policy Manager node for Insight integration.
- 3) Under the **System** menu tab, verify **Enable Insight** is checked under the Insight Setting field.

System Services Control	Service	Parameters	System Monitoring	Network	FIPS	
Hostname:		cppm69				
FQDN:		cppm69.ordr-de	emo.net			
Policy Manager Zone:		default	~			
Enable Performance Monitorin	g Display:	Enable this	server for performance	e monitoring	display	
Insight Setting:		🗹 Enable Insi	ght 🗹 Ena	ble as Insigh	nt Master	Current Master:cppm68(10.1.100.120)
Enable Ingress Events Process	sing:	🗆 Enable Ing	ress Events processing	on this serve	er	
Master Server in Zone:		Primary maste	er 🗸			
			IPv4			IPv6
	IP Addres	s	10.1.100.	120		
Management Port	Subnet M	lask	255.255.2	55.0		
	Default G	ateway	10.1.100.	1		

4) If changes made, click **Save** when finished.

Step 6 Configure Ordr SCE Service Integration for ClearPass

- From the Ordr SCE management interface, navigate to Network > Network
 Services > Policy and select ClearPass from the list of Policy Servers.
- 2) Test the connection to the ClearPass Policy Manager server:
 - a. From the **Test Connectivity** tab, complete the form:
 - i. Enter the **ClearPass Server URL** based on FQDN or IP address of the ClearPass Policy Manager
 - ii. Enter the **ClearPass Admin Username** and **Password** using the credentials of the Ordr API Admin User defined in Step 1.
 - b. Click the **Test** button. All test results should be successful as shown in the example:

ClearPass (Service D)etail)			
🅸 Configuration 🔧 Tes	t Connectivity			×
ClearPass Server URL ClearPass Admin Username ClearPass Admin Password	https://clearpass.ordr-demo.net ordradmin 	Q	Tact	Cancel
Connection status: Con DNS status: DNS resolv PING status: PING test TCP status: TCP connection Test is Complete of	 nnection test successful! wed to IP: 10.1.100.121 t successful, configured URL is reachable ction established on port 80 			

If any failures, check the following:

- i. Ensure the credentials are correct and re-save values in Ordr SCE.
- Ensure TCP/443 (or designated API port) is permitted between the Ordr integration/services node and ClearPass Policy Manager. This node is typically an existing Ordr sensor with the specific designation of Services Node. All communications between Ordr SCE and Aruba CPPM occur through an integration/services node. Therefore, verify connectivity between this nodes management IP address and CPPM.
- iii. Verify DNS is properly configured on the Ordr appliances and CPPM and that the ClearPass FQDN is configured in DNS if using its name rather than IP address in the connection URL.
- iv. Verify the ClearPass Server URL is using secure HTTP, or https. There will be an error if you enter http://.
- 3) Once Test Connectivity is successful, go to the Configuration tab and re-enter the Server URL and Ordr API admin credentials. Leave the Polling Interval at its default setting unless instructed otherwise. This sets the interval used to poll for any new client authentications not received via Context Server notifications.

4) Click Save when finished.

ClearPass (Service D	etail)			
🅸 Configuration 🌂 Test	t Connectivity			×
ClearPass Server URL	https://clearpass.ordr-d	emo.net	Last Successful Act	tivity @ 12/2/2021 6:55:09 PM
ClearPass Admin Username ClearPass Admin Password	ordradmin 		ø	
Polling Interval Successfully saved changes. Service Status: Successful		Minutes (30-360)	Save	Delete

5) Once successfully integrated, the status bar in the Service Integration icon for ClearPass should turn green as shown:



If the status bar turns red, repeat the Test Connectivity step and review the troubleshooting hints provided.

Part 2: Rich Device Context Sharing

Ordr Systems Control Engine automatically classifies all devices on the network inclusive of medical and industrial IoT, building automation, media, phones, printers,

servers, and user workstations and mobile devices. Beyond dynamic classification and grouping by Device Type, Device Category, and Device Profile, Ordr SCE collects detailed asset and device attributes such as manufacturer, model/serial number, hardware/software versions, vulnerability/threat risk ratings, and other rich data.

🛈 Details 🏾 🏔 Se	curity Incidents 🛛 🕱 Flo	w Genome 🛄 Netv	work Stats		© C ≡ ×
DEVICE INFORMATION Mac Address : Device Description : Manufacturer : Model Name/No. : Serial No. : OS Type : OS Version : SW Version :	A0:48:1C:A9:C5:BA MRI Philips Medical Systems Panorama HFO 19226 Windows XP 64bit 5.2 3.2.3\3.2.3.4	CLASSIFICATION Classification State : Classification Source : Device Type : Group : Profile : End Point Type : Criticality : Alarm Count :	Classified PROFILE_LIB MRI Medical Devices Philips-MRI IoT Endpoint LEVEL_3 193	CONNECTIVITY SCE Sensor : IP Address : Subnet : VLAN : Access Type : Network Device : Access Interface : First Seen :	abc-cpnanalytics-engine Offline (last IP = 10.21.136.19) 10.21.136.0/22 Vlan(1910) WIRED <u>10.172.3.1 (accsw-f01-2)</u> GigabitEthernet1/0/7 4/11/2018 12:11:43 PM
FQDN : DHCP Hostname : Has PHI : DICOM AE Title :	mri_1.mcd.pri N/A Yes CHR_MR1	Risk Score : Vuln :	80 normal	Last Seen : Location :	6/18/2018 2:05:03 PM Redwood City
		Device Name: CHR_MR1 Tags: New Tag Description: Descriptio	n for this device		SAVE CHANGES
		Profile Name Philips-M	RI		

This information is shared with ClearPass to provide exceptional visibility and context needed to make enforcement and segmentation policy decisions for IoT and other non-authenticating devices.

Step 1 Verify creation of new custom dictionary attributes in ClearPass

- From ClearPass Policy Manager, navigate to Administration > Dictionaries > Dictionary Attributes.
- Apply a filter to display only attributes where Name contains "Ordr" and click Go.
- 3) The list displays attributes populated by the Ordr SCE API as shown in the example.

Admini	stratio	n » Dictionaries » Dictionary A	ttributes			- Add			
Dicti	Dictionary Attributes								
The At	tribute	s dictionary page allows you to	o specify unique sets of crit	eria for local users, guest users, e	endpoints, and device	es.			
Filter: Name Show 50 V									
#		Name A	Entity	Data Type	Is Mandatory	Allow Multiple			
1.		OrdrBehaviorState	Endpoint	String	No	No			
2.		OrdrBlacklist	Endpoint	Boolean	No	No			
з.		OrdrCategory	Endpoint	String	No	No			
4.		OrdrCurrIpAddress	Endpoint	IPv4Address	No	No			
5.		OrdrDeviceType	Endpoint	String	No	No			
6.		OrdrDhcpHostname	Endpoint	String	No	No			
7.		OrdrEndPointType	Endpoint	String	No	No			
8.		OrdrEnforcementProfile	Endpoint	String	No	No			
9.		OrdrFirstSeen	Endpoint	Date-Time	No	No			
10.		OrdrHasAlarms	Endpoint	Boolean	No	No			
11.		OrdrLastSeen	Endpoint	Date	No	No			
12.		OrdrLongMfgName	Endpoint	String	No	No			
13.		OrdrModelNameNo	Endpoint	String	No	No			
14.		OrdrOsType	Endpoint	String	No	No			
15.		OrdrPolicyStatus	Endpoint	String	No	No			
16.		OrdrProfile	Endpoint	String	No	No			
17.		OrdrRiskScore	Endpoint	Integer32	No	No			
18.		OrdrVlanId	Endpoint	Integer32	No	No			
19.		OrdrVuln	Endpoint	String	No	No			

Step 2 Verify automated endpoint creation and context sharing from Ordr SCE to ClearPass

- Within ClearPass Policy Manager, navigate to Configuration > Identity > Endpoints
 - a. Filter the list to display all endpoints where **Description contain "Ordr"** as shown in the example. All endpoints discovered by Ordr SCE and populated automatically into the ClearPass Policy Manager endpoint repository are displayed.

Endpoints

This pa tablets,	ge auto etc.).	matically lists all a	authenticated	d endpoints. An en	ndpoint	: device is an Inter	rnet-capable	e hardware device on a TC	P/IP network (e.	g. laptops, sm	art phones,
Filter:	Descripti	on	contains	ᅌ Ordr		+ Go	Clear Filter			Show 50	ᅌ records
#		MAC Address		Hostname		Device Categor	у 🔺	Device OS Family	Status	Profiled	
1.		600308c7eb39		GreatRoAppleTV2	2	Media Devices		Television	Known	Yes	
2.		0009ef00a0a1				Media Devices		Badge	Known	Yes	
3.		005056d797db		MR2		Medical Devices		MRI	Known	Yes	
4.		0050565457f0		CT5		Medical Devices		CT Scanner	Known	Yes	
5.		00505640f6e4				Medical Devices		MRI	Known	Yes	
6.		0050568239c9		CR1		Medical Devices		CR Reader	Known	Yes	
7.		0009fb479c49				Medical Devices		Patient Monitoring	Known	Yes	
8.		02accd000001				Medical Devices		Hemodialysis Machine	Known	Yes	
9.		0050567a21ae		CT4		Medical Devices		CT Scanner	Known	Yes	
10.		00163e6d3602				Medical Devices		Infusion Pump	Known	Yes	
11.		00505664e393		CT7		Medical Devices		CT Scanner	Known	Yes	
12.		005056ac9c8c		US5		Medical Devices		Ultrasound	Known	Yes	
13.		00409d594bbc				Medical Devices		Spectrum Infusion Pump	Known	Yes	
14.		00163e1c989a				Medical Devices		Infusion Pump	Known	Yes	
15.		005056ec6a69				Medical Devices		CR Reader	Known	Yes	
16.		005056e4028f		MR3		Medical Devices		MRI	Known	Yes	
17.		0009fbf669f7				Medical Devices		Patient Monitoring	Known	Yes	
18.		005056fc78ba		MR5		Medical Devices		MRI	Known	Yes	
19.		0050564a0843		CT2		Medical Devices		CT Scanner	Known	Yes	
20.		005056e1f33a		US4		Medical Devices		Ultrasound	Known	Yes	
21.		0050566460cb		CR2		Medical Devices		CR Reader	Known	Yes	
22.		005056355212		US2		Medical Devices		Ultrasound	Known	Yes	
23.		005056bf880e		CT3		Medical Devices		CT Scanner	Known	Yes	

Note: By default, Ordr does not populate the Device Category, Device OS and Device Name fields to avoid potential conflict with existing ClearPass policies that may reference these fields. Please contact Ordr if prefer to have these fields updated by SCE based on the values for Ordr device classification Group, Manufacturer, and Classification Profile, respectively.

b. Click on the MAC Address for one of the endpoints and view the Endpoint details:

Endpoint Att	ributes Device Fingerprints		
MAC Address	005056e4028f	IP Address	10.200.204.12
Description	Ordr discovered: MRI	Static IP	FALSE
		Hostname	MR3
Ctatura		Device Category	Medical Devices
Status	• Known client	Device OS Family	MRI
	 Disabled client 	Device Name	MR3
MAC Vendor	VMware, Inc.	Added At	Apr 13, 2019 15:02:04 UTC
Added by	OrdrApiClient	Last Profiled At	Apr 13, 2019 15:02:04 UTC
Online Status	Not Available		
Connection Type	Unknown		

Note the Description field has been auto-populated as "Ordr discovered: MRI". Ordr will not update this field for devices already discovered by CPPM, but the custom dictionary attributes for all devices known to Ordr will be populated to the ClearPass endpoint repository.

c. Click the **Attributes** tab to view the rich device context automatically populated to the selected endpoint by Ordr SCE.

Edit	Endpoint					8
E	ndpoint Attributes	Device Fingerprints				
	Attribute			Value		
1.	OrdrBehaviorState		=	NORMAL	Ť	L
2.	OrdrCategory		=	Medical Devices	Ť	
3.	OrdrCurrIpAddress		=	10.200.204.12	Ť	L
4.	OrdrDeviceType		=	MRI	Ť	L
5.	OrdrDhcpHostname		=	MR3	Ť	
6.	OrdrEndPointType		=	IOT_ENDPOINT	Ť	L
7.	OrdrFirstSeen		=	2019-04-13 09:31:02	Ť	
8.	OrdrHasAlarms		=	false	Ť	
9.	OrdrLongMfgName		=	Philips	Ť	
10.	OrdrOsType		=	Linux	Ť	L
11.	OrdrProfile		=	Philips-MRI	Ť	L
12.	OrdrRiskScore		=	0	Ť	L
13.	OrdrVlanId		=	204	ŵ	L
14.	OrdrVuln		=	NORMAL	Ť	
15	Click to add			Save	ancel	

d. Click **Cancel** when finished.

Step 3 Verify enhanced visibility in ClearPass Policy Manager (Optional)

If elected to have Ordr SCE populate the Device Category, Device OS and Device Name, the results can be viewed under CPPM Endpoint Profiler.

 Navigate to Monitoring > Profiler and Network Scan > Endpoint Profiler. If enabled by Ordr support, SCE will automatically update ClearPass Device Category, Device Family, and Device Name attributes based on its highfidelity classification and data collection engine. Select various values to show the impact of Ordr SCE device context updates and the resulting list of matching endpoints.

			ClearPass	Policy Manager		Menu =
Monitori	ng » Profi	ler and Network Scan »	Endpoint Profiler			
Endpo	oint Pr	ofiler				
If the Pr	ofiler lice	nse is enabled, a list of t	he profiled endpoints is v	isible on this page.		
					Toggle Das	hboard View
366	Total Devi	ces 0(0%) Smartdev	rices 0(0%) Compute	rs 366(100%) Other Devices	Filter: A	Il Endpoints ᅌ
		Device Category	,	Device Family	Device Name	
	Generic Media D Medical Mobile F	(6) evices (2) Devices (25) Phones and Tablets (3)	0	CR Reader (5) CT Scanner (6) Hemodialysis Machine (1) Infusion Pump (2)	(1) CR1 (1) CR2 (1) CR3 (1)	
			*		*	
		Server Switch Gener Network Devices Media Medical Devices Workst Servers Mobile Phones a Other Physical Security I	ric Devices ations und Tablets Devices	Hemodialysis Machine Spectrum Infusion Pump Infusion Pump Ratient Montoring Ultrasound CR Reader		13
				↓ Change Filter S	Selection 📀 Mark Known 😑 Mark Unknown 🔘 M	lark Disabled
#		MAC Address 🔺	Hostname	Device Category	Device OS Family Status	
1.		0050561f7d7e	CR4	Medical Devices	CR Reader Known	
2.		0050566460cb	CR2	Medical Devices	CR Reader Known	
3.		00505670952c	CR3	Medical Devices	CR Reader Known	
4.		0050568239c9	CR1	Medical Devices	CR Reader Known	
5.		005056ec6a69		Medical Devices	CR Reader Known	

2) The same data can be viewed in the ClearPass Insight database. If Insight is enabled, Open the Insight interface and navigate to **Inventory**. Again, the results are enhanced by additional context and update of the Device Category, OS Family, and Device Name attributes by Ordr SCE.

aruba a	learPass Insi	ight	АТОТ	L AUTH 17 FAILED AUTH	0 UNIQUE ENDPOINT	S 2 UNIQUE USERS 2		Menu
Dashboard	In	ıve	ntory					
Inventory	-							
	ľ	Inver	itory					9 a 7 x
		#	MAC ADDRESS 🗵	IP ADDRESS 🗵	HOSTNAME -	CATEGORY	FAMILY -	DEVICE NAME
		1	0009ef00a0a1	192.168.104.117		Media Devices	Badge	
		2	600308c7eb39	192.168.101.133	GreatRoAppleTV2	Media Devices	Television	GreatRoAppleTV2
		3	005056fc78ba	10.200.204.14	MR5	Medical Devices	MRI	MR5
		4	0050566460cb	10.200.204.20	CR2	Medical Devices	CR Reader	CR2
		5	005056e1f33a	10.200.204.17	US4	Medical Devices	Ultrasound	US4
		6	005056ec6a69	10.200.204.23		Medical Devices	CR Reader	
		7	00505664e393	10.200.204.25	СТ7	Medical Devices	CT Scanner	СТ7
		8	00163e6d3602	192.168.104.171		Medical Devices	Infusion Pump	
		9	00409d594bbc	192.168.104.100		Medical Devices	Spectrum Infusion Pump	
		10	0050565457f0	10.200.204.8	CT5	Medical Devices	CT Scanner	CT5

Part 3: Blocklisting and Dynamic Quarantine of Threats

Blocklisting enables network and security operators to quickly quarantine endpoints deemed high-risk or a security threat and their access needs immediate containment. This feature enables operators to deny or restrict network access to these endpoints through ClearPass by automatically triggering a policy which blocks their access. The specific policy for blocklisted endpoints is entirely configurable within ClearPass Policy Manager, based on the enforcement policy.

Note: Realtime blocklisting/quarantine requires RADIUS CoA (RFC3576) to be enabled and properly configured on Aruba CPPM and the network devices where endpoints connect to the network. Without CoA support, policy changes will not take effect until the device reconnects or reauthenticates to the network. RADIUS CoA configuration for different network device vendors, models, and versions is beyond the scope of this guide. Please refer to your network

device and Aruba CPPM documentation for details on specific configuration steps to support RADIUS CoA.

When a device is blocklisted from Ordr SCE its endpoint attributes in ClearPass are dynamically updated to mark the endpoint for active quarantine. Additionally, during the initial integration with Ordr SCE, sample enforcement profiles are created in ClearPass to facilitate the quarantine of blocklisted devices connected to HPE-Aruba wireless controllers and Cisco wired switches.

Edit	Endpoint				
E	ndpoint Attributes Device Fingerprints				
	Attributo		Value		
1	OrdrBobaviorState	_	NORMAL	B.	÷.
1.	OrdrBlocklist	_	true		
2.	OrdrEsteropy	_	Mabile Dhanas and Tablata		
3.	OrdrCategory	=			
4.		=	10.1.44.101		
5.	OrdrDeviceType	=	iPhone		T
6.	OrdrDhcpHostname	=	Apple-1pad	6	
7.	OrdrEndPointType	=	NONIOT_ENDPOINT	ĒÐ	Ť
8.	OrdrEnforcementProfile	=	[Enf-Prof-Radius-Ordr-Cisco-Device- Blocklist, Enf-Prof-Radius-Ordr-HPE-Device- Blocklist]	Ē	Ť
9.	OrdrFirstSeen	=	2022-01-07 22:18:48	Ē	Ť
10.	OrdrHasAlarms	=	false	Ē	Ť
11.	OrdrLastSeen	=	2021-12-29	Ê	ŵ
12.	OrdrLongMfgName	=	Apple	Ē	Ť
13.	OrdrModelNameNo	=		Ē	ŵ
14.	OrdrOsType	=	ios	Ē	ŵ
15.	OrdrPolicyStatus	=	Enforced	Ē	ŵ
16.	OrdrProfile	=	Apple-iPhone	Ē	Ť
17.	OrdrRiskScore	=	0	Ē	ŵ
18.	OrdrVlanId	=	44	Ē	ŵ
19.	OrdrVuln	=	NORMAL		ŵ
20.	Click to add				
			Save	C	ancel

The example above highlights the custom Ordr attributes updated for a blocklisted endpoint. These include:

- OrdrBlocklist: Value set to "true" if device is blocklisted from Ordr SCE
- OrdrEnforcementProfile = Value set to the name or names of applicable ClearPass Enforcement Profiles to quarantine the blocklisted endpoint
- OrdrPolicyStatus: Value set to "Enforced" when policy is enforced from Ordr SCE

Using these attributes, an administrator can easily apply an enforcement policy and profile in ClearPass to limit or block network access to an Ordr-blocklisted device. While there are many ways these attributes can be leveraged for dynamic threat containment, one of the simplest options would be to match endpoints with the OrdrBlocklist attribute is set to "true" and apply the desired quarantine policy in Aruba CPPM.

The following steps illustrate one example of how to apply a restricted access policy to a blocklisted endpoint.

Step 1 Create a ClearPass role for Quarantine/Blocklist devices

- 1) From ClearPass Policy Manager, navigate to **Configuration > Identity > Roles**.
- 2) Click **Add** from the upper right window and enter the Name of the new role such as "Ordr_Blocklist" and include an optional Description.

Configuration » Identity » Roles	
Roles	🚽 Add
	Import
Roles exist independently of an individual service and can be accessed globally through the role-mapping policy of any	service.
Filter: Name Contains Block Go Clear Filter	Show 20 🗸 records
# 📕 Name 🗚 Description	
1. Ordr_Blocklist Ordr Quarantine Role	
Showing 1-1 of 1	Export Delete

3) Under Configuration > Identity > Role Mappings, create a new role mapping (or update an existing role mapping) that includes a rule to match endpoints with OrdrBlocklist attribute equal to "true" and maps them to the blocklist role created above (for example, Ordr_Blocklist).

Configuration » Identity » Role Mappings » Edit - Ordr_MAC Auth Roles							
Role Mappings - Ordr_MAC Auth Roles							
Summary Policy Mapping Rules							
Policy:							
Policy Name:	Policy Name: Ordr_MAC Auth Roles						
Description:							
Default Role:	[Device Registrat	tion]					
Mapping Rules:							
Rules Evaluation Algorithm	First applicable						
Conditions Role Name							
1. (Endpoint:OrdrBlocklist	EQUALS true)	Ordr_Blocklist					

The Role Mapping policy used should be the one defined in your organization's ClearPass Services to enforce authentication and authorization for devices to be quarantined as defined under **Configuration > Services**.

Configuration » Services » Edit - Ordr_Aruba Wireless MAC Authentication Service								
Services - Ordr_Aruba Wireless MAC Authentication Service								
Summary	Service	Authentication	Roles	Enforcement	Profiler			
Role Mapping	Role Mapping Policy: Ordr_MAC Auth Roles Modify							
				Role M	lapping Pol	icy Details		
Description:								
Default Role:		[Device Regist	ration]					
Rules Evaluat	ion Algorithm	n: first-applicable	9					
Conditions Role								
1. (Endpo	. (Endpoint:OrdrBlacklist EQUALS true) Ordr_Blocklist							

4) Under the Enforcement tab of the selected Services policy, make note of the associated Enforcement Policy.

Configuration » Services » Edit - Ordr_Aruba Wireless MAC Authentication Service									
Services - Ordr_Aruba Wireless MAC Authentication Service									
Summary	Service	Authentication	Roles	Enforcement	Profiler				
Use Cached R	lesults:	Use cached F	oles and	Posture attribute	s from prev	vious sessions			
Enforcement	Policy:	Ordr Aruba Wire	less Enford	cement Policy 🗸	Modify				
				Enforce	ement Polic	y Details			
Description:									
Default Profile	e:	[Allow Access	Profile]						
Rules Evaluat	Rules Evaluation Algorithm: evaluate-all								
Condit	ions			Enforce	ement Pro	files			

5) Under the Profiler tab, verify the RADIUS CoA Action setting is correct for triggering reauthorization of endpoints using this Services policy.

Configuration	» Services	» Edit - Ordr_Arub	a Wireles	s MAC Authentic	ation Servic	e				
Services - Ordr_Aruba Wireless MAC Authentication Service										
Summary Service Authentication Roles Enforcement Profiler										
Endpoint Clas	sification:	Select the class Any Category / C	sification(DS Family /	s) after which an Name	Remove	st be triggered -				
RADIUS CoA	Action:	[ArubaOS Wirel	ess - Termi	nate Session] 🗸	View Deta	nils Modify				

Step 2 Bind an Enforcement Profile to Ordr blocklisted devices

- Go to Configuration > Enforcement > Policies and select the enforcement policy identified in Step 1.
- 2) Go to the Rules tab and map the Tips:Role=Ordr_Blocklist (or name assigned to Ordr Quarantine Role) to the desired Enforcement Profile.
 - a. For endpoints connected to Aruba wireless controllers, you can leverage the Enforcement Profile preconfigured by Ordr SCE to deny all IP network access to blocklisted devices.

Configuration » Enforcement » Policies » Edit - Ordr Aruba Wireless Enforcement Policy								
Enforcement Policies - Ordr Aruba Wireless Enforcement Policy								
Summary Enforcement	Summary Enforcement Rules							
Enforcement:								
Name:	Ordr Aruba Wireless Enforcement Policy							
Description:								
Enforcement Type:	RADIUS							
Default Profile:	[Allow Access Profile]							
Rules:								
Rules Evaluation Algorithm: Evaluate all								
Conditions Actions								
1. (Tips:Role EQUALS Ordr_Blocklist) Enf-Prof-Radius-Ordr-HPE-Device-Blocklist								

Note: Be sure to move the Quarantine rule to the top of the list.

This specific profile uses an Aruba Downloadable User Roles (DUR) for centralized policy and access control.

Enforcement Pro	rof-Radius-Ordr-HPE-Device-Blocklist					
Summary Profile	Role Configuration	on				
Profile:						
Name:	Enf-Prof-Radiu	s-Ordr-HPE-Device-Blocklist				
Description:						
Туре:	Aruba_DUR					
Action:	Accept					
Device Group List:	 Cisco Wired Aruba Wired Aruba Wirel 	d ess				
Product:	Mobility Contro	oller				
Role Configuration:						
Captive Portal Profile:		-				
Policer Profile:		-				
QoS Profile:		-				
VoIP Profile:		-				
Re-authentication Interva	al Time (0-4096):	- minutes				
VLAN:						
VLAN ID <1-4094>:		-				
VLAN Name:		-				
ACL:		Ordr-HPE-Device-Blocklist [Session]				
User Role Configuration:		ip access-list session Ordr-HPE-Device-Blocklist any any any deny ! user-role cppmrole access-list session Ordr-HPE-Device-Blocklist !				

b. For endpoints connected to Cisco wired switches, you can leverage the Enforcement Profile preconfigured by Ordr SCE to deny all IP network access to blocklisted devices.

Configuration » Enforcement » Policies » Edit - Ordr Cisco Wired Enforcement Policy								
Enforcement Policies - Ordr Cisco Wired Enforcement Policy								
Summary Enforcement	Summary Enforcement Rules							
Enforcement:								
Name:	Ordr Cisco Wired Enforcement Policy							
Description:								
Enforcement Type:	RADIUS							
Default Profile:	[Allow Access Profile]							
Rules:								
Rules Evaluation Algorithm: Evaluate all								
Conditions	Conditions Actions							
1. (Tips:Role EQUALS C	Ordr_Blocklist) Enf-Prof-Radius-Ordr-Cisco-Device-Blocklist							

Note: Be sure to move the Quarantine rule to the top of the list.

This specific profile uses a Cisco Downloadable ACL (dACL) for centralized policy and access control.

Configuration » Enforcement » Profiles » Edit Enforcement Profile - Enf-Prof-Radius-Ordr-Cisco-Device-Blocklist									
Enforcement Profiles - Enf-Prof-Radius-Ordr-Cisco-Device-Blocklist									
Summ	Summary Profile Attributes								
Profile:									
Name:		Enf-Prof-R	adius-Ordr-Cisco-Device-Blocklist						
Descript	Description:								
Type:		RADIUS	RADIUS						
Action:		Accept	Accept						
Device (Group List:	1. Cisco W 2. Aruba V 3. Aruba V	/ired Nired Nireless						
Attributes:									
Т	Type Name Value								
1. R	Radius:Cisco Cisco-IP-Downloadable-ACL = deny ip any any								

3) Click **Save** to add the rule and click **Save** again to save the updated policy.

Step 3 Trigger device blocklisting in Ordr SCE

- 1) From the Ordr SCE management interface, go to **Device > Device List**.
- 2) Click the Bulk Action icon. This displays a list of actions that may be taken across one or multiple devices at one time.
- 3) Select the device or devices to be quarantined and click the **Add to Blocklist** box.

List	of De	vices										
Total 7 Devices match 1 filter 🗞 🙀 Any Visible Field									Apply Action to Multiple Devices	e substring to ma	tch Manage 🕰	
🔀 Clear all criteria 🛛 [Group] is "Facility Devices" 🗙												
🗢 🗄 🗠 Kassification View										tion View 🗸 🗸		
	Adu Bloc (1F	d to klist kow)	⊗ Blocklist & Port Sh (1 Row	t Remove Blocklist) (0 Rows)	Remove Blocklist & Enable Ports (O Rows)	Cenerate Blocklist CLI	Fetch Installed Software Info (1 Row)	♦ Change VLAN (enforce) (1 Row)	(1 Row)	Delete Devices (1 Row)	i Change Attributes (1 Row)	Analyze App Usage (1 Row)
=,∕	No.	Mac Ad	ldress 🗘	IP Address	🗘 Device Name 🗘	Group	Profile	🗘 Risk 🔇	Vuln 🗘 I	Info		
		00:C0:B7	7:65:1F:BC	172.16.1.13	00:C0:B7:65:1F:BC	Facility Devices	APC-UPS	normal	critical	止 ≢		
		00:C0:B7	7:7C:05:F9	172.16.1.14	00:C0:B7:7C:05:F9	Facility Devices	APC-AP9619-Ne	twork 🔵 normal	critical	⊠ ш. 🖗 ≇		
		00:C0:B7	7:2E:7B:22	172.16.1.16	00:C0:B7:2E:7B:22	Facility Devices	APC-AP9619-Ne	twork 🔵 normal	critical	Z III 🖗 🕸		

4) Confirm the **Blocklist** operation.



Note: To remove a device from quarantine, select the device in Ordr SCE and click the **Remove Blocklist** box and confirm the operation.

Step 4 Verify endpoint quarantine in ClearPass Policy Manager

- From ClearPass Policy Manager, navigate to Configuration > Identity > Endpoints.
- 2) Filter the list of endpoints by "Attributes equals OrdrBlocklist equals true".

Filter:	Attribute		ᅌ equals	OrdrBlacklist	equals	ᅌ true 💌	+	Go Clear Filter		Show 50 ᅌ records
#		MAC Address		Hostname 🔺		Device Category		Device OS Family	Status	Profiled
1.		600308c7eb39		GreatRoAppleTV2		Media Devices		Television	Known	Yes
2.	0	0009ef00a0a1				Media Devices		Badge	Known	Yes

The list displays all endpoints where Ordr SCE has updated the quarantine flag (OrdrBlocklist set to "true") for the device and have been assigned a quarantine role. This role is assigned a Blocklist Enforcement Profile. The default Blocklist profiles can be modified to ensure the desired policy is applied to endpoints blocklisted through Ordr SCE.

Step 5 Verify new policy assignment for the blocklisted endpoint(s)

- From ClearPass Policy Manager, navigate to Monitoring > Live Monitoring > Access Tracker.
- 2) Find the entry in the table for endpoint(s) blocklisted from Ordr.
- Verify the correct Service, Role, Enforcement Policy, Enforcement Profile applied.

Summary

Without Ordr SCE, customers can struggle for months or years to achieve a comprehensive inventory and device visibility. Often the topic of real NAC enforcement and microsegmentation is just a distant vision as the classification of endpoints with confidence becomes the all-consuming task. With Ordr SCE integration, the ability to accurately identify endpoints—IoT and non-IoT—is drastically accelerated allowing customers to seamlessly apply policy enforcement and microsegmentation using HPE Aruba CPPM.

info@ordr.net

www.ordr.net

2445 Augustine Drive Suite 601

Santa Clara, CA 95054