



Integration
Between
Identity Services Engine (ISE) 2.x
And
HPE-ArubaOS 16.02 Switches

Version: 1.0

Date: January 1, 2017



Shlomo

Table of Contents

1	Introduction	3
2	Overview.....	4
2.1	HPE-ArubaOS-device configuration:.....	4
2.1.1	ISE PSN Server configuration	4
2.1.2	AAA configuration	4
2.1.3	Captive-portal configuration.....	4
2.1.4	CoA configuration	4
3	Identity Services Engine Configuration	5
3.1	Step by step ISE Configuration with 3d party device	5
3.2	Import HPE-ArubaOS NAD Profile in ISE	5
3.3	Adding 3rd Party Device in ISE (AAA client)	7
3.4	Creating authorization Profiles for each flows	8
3.4.1	Creating Guest flow (CWA) authorization profile	8
3.4.2	Create BYOD flow (NSP) authorization profile.....	9
3.4.3	Create Posture flow (CPP) authorization profile.....	10
3.4.4	Create FullAccess authorization profile post Guest/BYOD/Posture	11
3.5	Identity Services Engine Authorization policy Configuration	12
3.5.1	Create authorization rule for each flows	12
3.6	Identity Services Engine Client Provisioning Policy Configuration	13
4	Troubleshooting	14
4.1	Switch side:.....	14
4.2	ISE SIDE	15
5	Device Configuration:	15

1 Introduction

The Cisco Identity Services Engine (ISE) is a next-generation identity and access control policy platform that enables enterprises to facilitate new business services, enhance infrastructure security, enforce compliance, and streamline service operations. Its unique architecture allows enterprises to gather real-time contextual information from networks, users, and devices to make proactive governance decisions by enforcing policy across the network infrastructure – wired, wireless, and remote.

3rd Party Device (NAD) Support - customers can now deploy ISE services such as Profiling, Posture, Guest and BYOD (on top of the already-working 802.1x) with Network Access Devices (NADs) manufactured by non-Cisco third party vendors. This includes support for standard CoA and URL Redirection with capabilities to pass the client's MAC address within the redirection.

2 Overview

HPE has released new software for Procurve platform, now it is HPE-ArubaOS (current release is 16.02) and they are supporting now dynamic URL-Redirection from AAA server. The doc covers how this new feature works with ISE.

2.1 HPE-ArubaOS-device configuration:

2.1.1 ISE PSN Server configuration

```
Radius-server host <ise_psn> (e.g.10.10.13.245)  
Radius-server key "acsi"
```

2.1.2 AAA configuration

```
aaa accounting update periodic 1  
aaa accounting network start-stop radius  
aaa authentication port-access eap-radius  
aaa port-access authenticator 1-2  
aaa port-access authenticator 2 quiet-period 30  
aaa port-access authenticator 2 logoff-period 862400  
aaa port-access authenticator 2 client-limit 3  
aaa port-access authenticator active  
aaa port-access mac-based 2 addr-limit 32
```

2.1.3 Captive-portal configuration

```
aaa authentication captive-portal enable
```

2.1.4 CoA configuration

```
Radius-server host 10.10.13.245 dyn-authorization  
Radius-server host 10.10.13.245 time-window 0
```

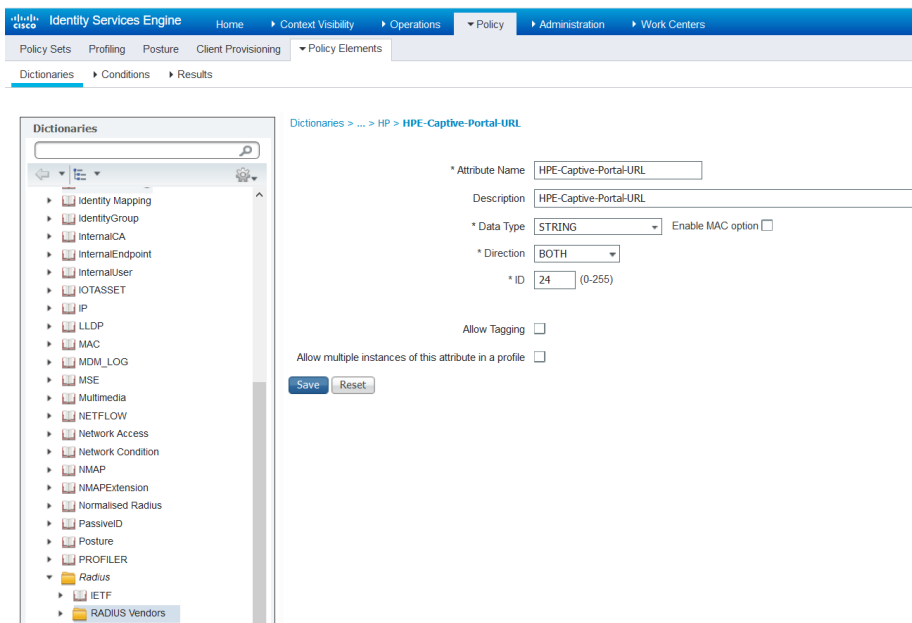
3 Identity Services Engine Configuration

3.1 Step by step ISE Configuration with 3d party device

3.2 Adding new HP attribute into HP dictionaries in ISE

Step 1 Go **Policy > Policy Elements > Dictionaries > System > Radius > RADIUS Vendors > HP.**

Step 2 Add **“HPE-Captive-Portal-URL” with ID 24**



3.3 Import HPE-ArubaOS NAD Profile in ISE

Download HPE-ArubaOS NAD profile from [communities web site](#) and import into ISE using import option under **Administration > Network Resources > Network Device Profiles**

Step 1 Choose **Administration > Network Resources > Network Device Profiles.**

Step 2 Click on **Import** option

Step 3 Click on **Browse ...**

Step 4 Click on **Import.**

Identity Services Engine Administration > Network Device Profiles

Network Device Profiles

Edit
 Add
 Duplicate
 Import
 Cisco Communities Import
 Export Selected
 Delete Selected

Name	Description	Vendor
<input type="checkbox"/> AlcatelWired	Profile for Alcatel switches	Alcatel
<input type="checkbox"/> ArubaWireless	Profile for Aruba wireless network access devices	Aruba
<input type="checkbox"/> BrocadeWired	Profile for Brocade switches	Brocade
<input type="checkbox"/> Cisco	Generic profile for Cisco network access devices	Cisco
<input type="checkbox"/> HPE-ArubaOSWired	HPE-ArubaOSWired	HP
<input type="checkbox"/> HPWired	Profile for HP switches	HP
<input type="checkbox"/> HPWired_SNMP_CoA	Profile for HP switches with no RADIUS CoA	HP
<input type="checkbox"/> HPWireless	Profile for HP wireless	HP
<input type="checkbox"/> MotorolaWireless	Profile for Motorola wireless	Motorola
<input type="checkbox"/> RuckusWireless	Profile for Ruckus wireless	Ruckus

Browse... HPE-ArubaOSWired.xml

Import Cancel

Here is how it looks the URL-redirection option:

Identity Services Engine Administration > Network Device Profiles

Permissions

Change of Authorization (CoA)

Redirect

Type:

=

Dynamic URL Parameter

Session ID
 Client MAC Address
 None

Redirect URL Parameter Names

Client IP Address:
 Client MAC Address:
 Originating URL:
 Session ID:
 SSID:

3.4 Adding 3rd Party Device in ISE (AAA client)

- Step 1** Choose **Administration > Network Resources > Network Devices**.
- Step 2** Click **Add**.
- Step 3** Enter valid name (e.g. 'HPE-ArubaOS-Switch')
- Step 4** Enter valid IP Address
- Step 5** Select under Device Profile '**HPE-ArubaOSWired**' (default NAD profile is **Cisco**)
- Step 6** Enter Shared Secret Under **RADIUS Authentication Settings**
- Step 7** Click **Submit** to save your changes to the Cisco ISE system database.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Network Devices. The page title is "Network Devices List > HP-2920".

Network Devices

- * Name: HP-2920
- Description: [Empty]
- * IP Address: 10.10.48.249 / 32
- * Device Profile: HPE-ArubaOSWired
- Model Name: [Empty]
- Software Version: [Empty]

* Network Device Group

- Device Type: All Device Types (Set To Default)
- Location: All Locations (Set To Default)

RADIUS Authentication Settings

Enable Authentication Settings

- Protocol: **RADIUS**
- * Shared Secret: [Masked] (Show)
- Enable KeyWrap: (i)
- * Key Encryption Key: [Empty] (Show)

3.5 Creating authorization Profiles for each flows

3.5.1 Creating Guest flow (CWA) authorization profile

- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.
- Step 2** Click **Add**.
- Step 3** Enter valid name (e.g. 'HPE-CWA-Profile')
- Step 4** Select '**ACCESS_ACCEPT**' in Access Type option
- Step 5** Select under Network Device Profile '**HPE-ArubaOSWired**'
- Step 6** Add VLAN-ID under Common tasks in VLAN option
- Step 7** Enable '**Web Redirection (CWA, MDM, NSP, CPP)**' option and select '**Centralized Web Auth**' and portal '**Self-Registered Guest Portal (default)**'
- Step 8** Click **Submit** to save your changes to the Cisco ISE system database to create an authorization profile.

The screenshot displays the Cisco ISE configuration interface for an Authorization Profile. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Elements > Results > Authorization Profiles > HPE-CWA-Profile. The main configuration area includes:

- Authorization Profile:**
 - Name: HPE-CWA-Profile
 - Description: (empty)
 - Access Type: ACCESS_ACCEPT
 - Network Device Profile: HPE-ArubaOSWired
- Common Tasks:**
 - Centralized Web Auth: Value Self-Registered Guest Portal (c)
 - Display Certificates Renewal Message:
- Advanced Attributes Settings:**
 - HP:HP-Nas-Filter-Rule: deny in tcp from any to any 80,4
 - HP:HP-Nas-Filter-Rule: permit in udp from any to any 53
 - HP:HP-Nas-Filter-Rule: permit in tcp from any to any 84*
- Attributes Details:**
 - Access Type = ACCESS_ACCEPT
 - Tunnel-Private-Group-ID = 1:114
 - Tunnel-Type = 1:13
 - Tunnel-Medium-Type = 1:6
 - HPE-Captive-Portal-URL = https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a692c530-2230-11e6-99ab-005056bf55e0&daysToExpiry=value&action=cwa
 - HP-Nas-Filter-Rule = deny in tcp from any to any 80,443 cpy
 - HP-Nas-Filter-Rule = permit in udp from any to any 53,67-68,389
 - HP-Nas-Filter-Rule = permit in tcp from any to any 8443-8909

Buttons for Save and Reset are located at the bottom left of the configuration area.

3.5.2 Create BYOD flow (NSP) authorization profile

-
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.
 - Step 2** Click **Add**.
 - Step 3** Enter valid name (e.g. 'HPE-BYOD-Profile')
 - Step 4** Select '**ACCESS_ACCEPT**' in Access Type option
 - Step 5** Select under Network Device Profile '**HPE-ArubaOSWired**'
 - Step 6** Add VLAN-ID under Common tasks in VLAN option
 - Step 7** Enable '**Web Redirection (CWA, MDM, NSP, CPP)**' option and select '**Native Supplicant Provisioning**' and portal '**BYOD Portal (default)**'
 - Step 8** Click **Submit** to save your changes to the Cisco ISE system database to create an authorization profile.
-

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for an Authorization Profile. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Sets > Profiling > Posture > Client Provisioning > Policy Elements > Results. The main content area is titled 'Authorization Profiles > HPE_BYOD_Profile' and 'Authorization Profile'. The configuration includes:

- Name:** HPE_BYOD_Profile
- Description:** (empty field)
- Access Type:** ACCESS_ACCEPT
- Network Device Profile:** HPE-ArubaOSWired
- Common Tasks:**
 - Web Redirection (CWA, MDM, NSP, CPP) (i)
 - Native Supplicant Provisioning (Native Supplicant Provisioning) Value: BYOD Portal (default)
 - Static IP/net name/EoDM
- Advanced Attributes Settings:**
 - HP:HP-Nas-Filter-Rule = deny in tcp from any to any 80,4
 - HP:HP-Nas-Filter-Rule = permit in udp from any to any 53
 - HP:HP-Nas-Filter-Rule = permit in tcp from any to any 84+
- Attributes Details:**

```

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:114
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
HPE-Captive-Portal-URL = https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a6d1f110-2230-11e6-99ab-005056bf55e0&action=ns
HP-Nas-Filter-Rule = deny in tcp from any to any 80,443 cpy
HP-Nas-Filter-Rule = permit in udp from any to any 53,67-68,389
HP-Nas-Filter-Rule = permit in tcp from any to any 8443-8909

```

Buttons for 'Save' and 'Reset' are located at the bottom of the configuration area.

3.5.3 Create Posture flow (CPP) authorization profile

- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.
- Step 2** Click **Add**.
- Step 3** Enter valid name (e.g. 'HPE-Posture-Profile')
- Step 4** Select '**ACCESS_ACCEPT**' in Access Type option
- Step 5** Select under Network Device Profile '**HPE-ArubaOSWired**'
- Step 6** Add VLAN-ID under Common tasks in VLAN option
- Step 7** Enable '**Web Redirection (CWA, MDM, NSP, CPP)**' option and select '**Client Provisioning (Posture)**' and portal '**Client Provisioning Portal (default)**'
- Step 8** Click **Submit** to save your changes to the Cisco ISE system database to create an authorization profile.

The screenshot shows the Cisco ISE configuration interface for an Authorization Profile. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Elements > Results > Authorization Profiles > HPE_Posture_Profile.

Authorization Profile Configuration:

- Name:** HPE_Posture_Profile
- Description:** (Empty text box)
- Access Type:** ACCESS_ACCEPT
- Network Device Profile:** HPE-ArubaOSWired

Common Tasks:

- Web Redirection (CWA, MDM, NSP, CPP)
 - Client Provisioning (Posture)
 - Value: Client Provisioning Portal (def)
- Display Certificates Renewal Message

Advanced Attributes Settings:

HP:HP-Nas-Filter-Rule	=	deny in tcp from any to any 80 c
HP:HP-Nas-Filter-Rule	=	deny in tcp from any to any 443
HP:HP-Nas-Filter-Rule	=	permit in udp from any to any 1-4
HP:HP-Nas-Filter-Rule	=	permit in tcp from any to any 8443-8909

Attributes Details:

```

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:114
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
HP-Captive-Portal-URL = https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a6bb0db0-2230-11e6-99ab-005056bf55e0&action=cpp
HP-Nas-Filter-Rule = deny in tcp from any to any 80 cpy
HP-Nas-Filter-Rule = deny in tcp from any to any 443 cpy
HP-Nas-Filter-Rule = permit in udp from any to any 1-65535
HP-Nas-Filter-Rule = permit in tcp from any to any 8443-8909
  
```

3.5.4 Create FullAccess authorization profile post Guest/BYOD/Posture

-
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.
 - Step 2** Click **Add**.
 - Step 3** Enter valid name (e.g. **'HPE-Corporate-VLAN114'**)
 - Step 4** Select **'ACCESS_ACCEPT'** in Access Type option
 - Step 5** Select under Network Device Profile **'HPE-ArubaOSWired'**
 - Step 6** Add VLAN-ID under Common tasks in VLAN option
 - Step 7** Click **Submit** to save your changes to the Cisco ISE system database to create an authorization profile.
-

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for an Authorization Profile. The breadcrumb navigation shows 'Authorization Profiles > HPE-Corporate-VLAN114'. The main configuration area includes:

- Authorization Profile:**
 - * Name: HPE-Corporate-VLAN114
 - Description: (empty text box)
 - * Access Type: ACCESS_ACCEPT
 - Network Device Profile: HPE-ArubaOSWired
- Common Tasks:**
 - ACL
 - VLAN: Tag ID 1, ID/Name 114
- Advanced Attributes Settings:**
 - Select an item = (empty text box)
- Attributes Details:**
 - Access Type = ACCESS_ACCEPT
 - Tunnel-Private-Group-ID = 1:114
 - Tunnel-Type = 1:13
 - Tunnel-Medium-Type = 1:6

Buttons for 'Save' and 'Reset' are located at the bottom of the configuration area.

3.6 Identity Services Engine Authorization policy Configuration

3.6.1 Create authorization rule for each flows

- Step 1** Choose **Policy > Policy Sets**.
- Step 2** Click the down arrow on the far-right and select either **Insert New Rule Above** or **Insert New Rule Below**.
- Step 3** Enter the rule name and select identity group, condition, attribute and permission for the authorization policy.
 Not all attributes you select will include the “Equals,” “Not Equals,” “Matches,” “Starts with,” or “Not Starts with” operator options.
 The “Matches” operator supports and uses regular expressions (REGEX) not wildcards.
- Step 4** Click **Done**.

Step 5 Click **Save** to save your changes to the Cisco ISE system database and create this new authorization policy.

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description	Conditions
<input checked="" type="checkbox"/>	HPE Network	HPE devices in Network:2920, 3800	DEVICE:Network Device Profile EQUALS HPE-ArubaOSWired

Authentication Policy

Status	Name	Conditions	Permissions
<input checked="" type="checkbox"/>	MAB	If Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/>	Default	use Internal Endpoints	and
<input checked="" type="checkbox"/>	Dot1X	If Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/>	Default	use All_User_ID_Stores	and
<input checked="" type="checkbox"/>	Default Rule (if no match)	Allow Protocols : Default Network Access	and use : All_User_ID_Stores

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
<input checked="" type="checkbox"/>	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then HPE-Corporate-VLAN114
<input checked="" type="checkbox"/>	Employee_EAP-TLS	if (Wired_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_in_SAN)	then HPE-Corporate-VLAN114
<input checked="" type="checkbox"/>	Employee_Posture_unknown	if (Wired_802.1X AND EAP-MSCHAPv2 AND Session:PostureStatus NOT_EQUALS Compliant)	then HPE-Posture-Profile
<input checked="" type="checkbox"/>	Employee_Onboarding	if (Wired_802.1X AND EAP-MSCHAPv2)	then HPE_BYOD_Profile
<input checked="" type="checkbox"/>	Guest_Access	if (Guest_Flow AND Wired_MAB)	then HPE-Corporate-VLAN114

3.7 Identity Services Engine Client Provisioning Policy Configuration

Note: make sure you have download AnyConnect against into ISE and configured correctly.

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
<input checked="" type="checkbox"/> Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
<input checked="" type="checkbox"/> Windows	If Any	and Windows All	and Condition(s)	then AnyConnectDesktopWindows4.4.243 And WinSPWizard 2.1.0.51 And Wired
<input checked="" type="checkbox"/> MAC OS	If Any	and Mac OSX	and Condition(s)	then MacOsXSPWizard 2.1.0.40 And Cisco-ISE-NSP
<input checked="" type="checkbox"/> Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

4 Troubleshooting

4.1 Switch side:

3rd-hp-2920# show port-access clients detailed

Port Access Client Status Detail

Client Base Details:

Port : 2 Authentication Type: 802.1x
Client Status : authenticated Session Time : 2 seconds
Client name : NA\DT01 Session Timeout : 0 seconds
MAC Address : 74da38-4a082d
IP : n/a

Access Policy Details :

COS Map : Not Defined In Limit Kbps : Not Set
Untagged VLAN : 114 Out Limit Kbps : Not Set
Tagged VLANs : No Tagged VLANs
Port Mode : 100FDx

RADIUS ACL List:

deny in tcp from any to any 80,443 cpy
permit in udp from any to any 53,67-68,389
permit in tcp from any to any 8443-8909

Captive Portal Details :

URL :

https://ise-3rd-vm-

2.cisco.com:8443/portal/gateway?sessionId=0a3837f53515e59bYck7HRNNVPxfc4JcSoElnoINZHhHLN
MrsZ4&portal=a6d1f110-2230-11e6-99a...

3rd-hp-2920#

4.2 ISE SIDE

Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Posture Status	Authorization P...	Authorizati...	Network Device	Device Port
Jan 26, 2017 04:52:34.340 PM			NA\DT01	74.DA.38.4A.08.2D	Windows10-Work...	Compliant	HPE Network >> ...	HPE-Corpor...		
Jan 26, 2017 04:51:33.025 PM			NA\DT01	74.DA.38.4A.08.2D	Windows10-Work...	Compliant	HPE Network >> ...	HPE-Corpor...	HP-2920	2
Jan 26, 2017 04:51:16.655 PM				74.DA.38.4A.08.2D		Compliant			HP-2920	
Jan 26, 2017 04:50:09.232 PM			NA\DT01	74.DA.38.4A.08.2D	Windows10-Work...	Pending	HPE Network >> ...	HPE-Postur...	HP-2920	2

5 Device Configuration:

Insecure Connection

https://ise-3rd-vm-2.cisco.com:8443/portal/gateway?sessionId=0a3837f5xGC

Your connection is not secure

The owner of this website has not secured this connection. Learn more


Remember this choice

Cisco AnyConnect Secure Mobility Client

VPN:
Ready to connect.

10.0.10.2

System Scan:
Compliant.
Network access allowed.

 Cisco AnyConnect
Network access allowed.
Cisco AnyConnect Secure Mobility Client

Ask me anything

3:49 PM
1/26/2017