Tech Zone > Tech Zone Knowledge Base > Security Knowledge Base > AAA and Identity Management Knowledge Base > ISE

Integration Between ISE2.1 and Ruckus 1200 Wireless -BYOD/Posture flows using Auth VLAN

(124 Views)

by smashash on 06-19-2016 03:45 AM

Activity: Configuration, Deploy, Integration
Product (Cisco): ISE

Table of Contents

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.

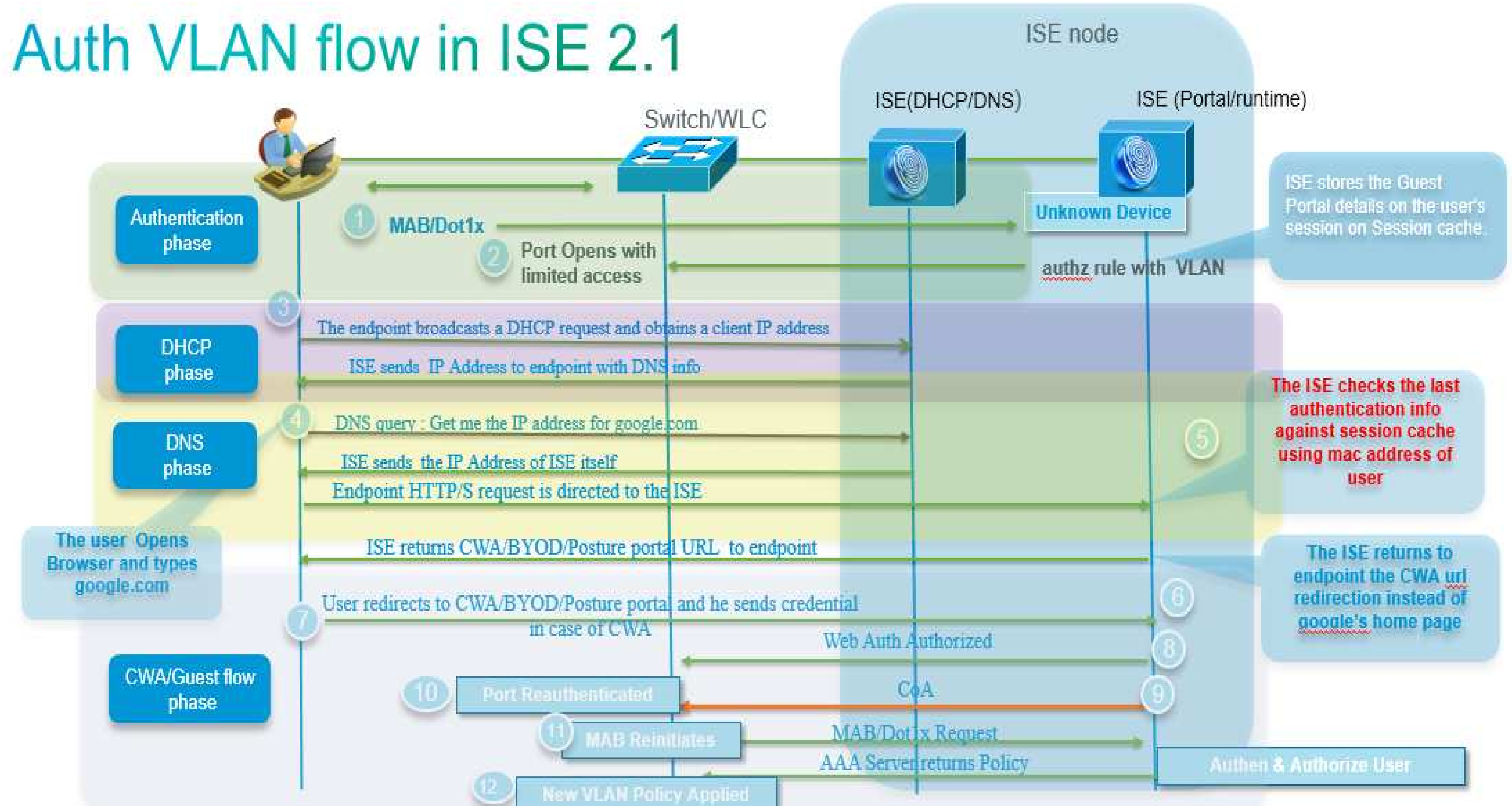
In ISE 2.1 we have added new functionalities:

- **Auth VLAN flow** – for third party device which doesn’t support URL Redirection.
- **SNMP CoA** – for third party device which doesn’t support RADIUS CoA

What is Auth VLAN and how it works:

Auth VLAN is new way to do URL-Redirection for devices which not support dynamic or static URL-redirection.e.g. Ruckus WLC or Juniper EX switches.To support that we added in ISE 2.1 new DHCP/DNS functionally.

The endpoint client sends DHCP request and ISE provides ip address with ip of DNS server (which is ISE itself).



Auth VLAN flow in ISE 2.1

ISE node

Switch/WLC

ISE(DHCP/DNS)

ISE (Portal/runtime)

Unknown Device

ISE stores the Guest Portal details on the user's session on Session cache

Authentication phase

1 MAB/Dot1x

2 Port Opens with limited access

authz rule with VLAN

DHCP phase

3 The endpoint broadcasts a DHCP request and obtains a client IP address

ISE sends IP Address to endpoint with DNS info

DNS phase

4 DNS query : Get me the IP address for google.com

ISE sends the IP Address of ISE itself

Endpoint HTTP/S request is directed to the ISE

5 The ISE checks the last authentication info against session cache using mac address of user

The user Opens Browser and types google.com

ISE returns CWA/BYOD/Posture portal URL to endpoint

6 The ISE returns to endpoint the CWA url redirection instead of google's home page

7 User redirects to CWA/BYOD/Posture portal and he sends credential in case of CWA

8 Web Auth Authorized

CWA/Guest flow phase

9 CoA

10 Port Reauthenticated

11 MAB Reinitiates

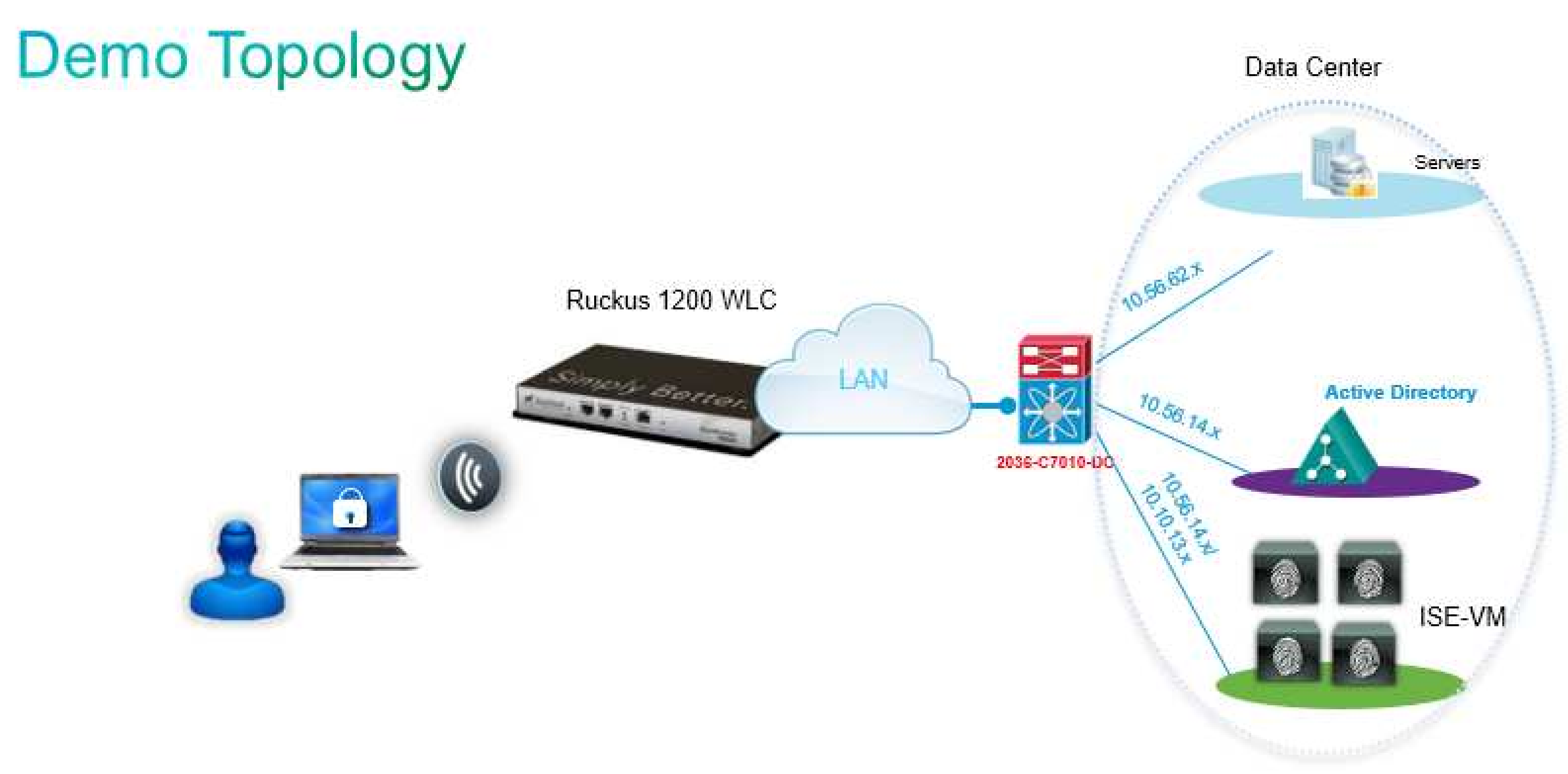
MAB/Dot1x Request

AAA Server returns Policy

Authen & Authorize User

12 New VLAN Policy Applied

2 Pre-requirements to deployment the new features for ISE 2.1



Demo Topology

2.1 Configuring the 3rd party (Optional- if it already configured):

2.1.1 Defining trunk VLAN between 3rd party device to uplink Aggregation/ Distribution switches

2.1.2 Defining DHCP Snooping/IP helper-address (to get IP address from DHCP server/ISE)

2.1.3 Defining VLANs (Management and Access as required)

2.1.4 Validating the L3 connectivity cross to Data Center

2.1.5 Defining RADIUS configurations (Dot1X, MAB)

2.1.6 Getting much information about Dynamic VLAN assignments format, ACL (Access control list) format, URL-Redirection that the device is using.

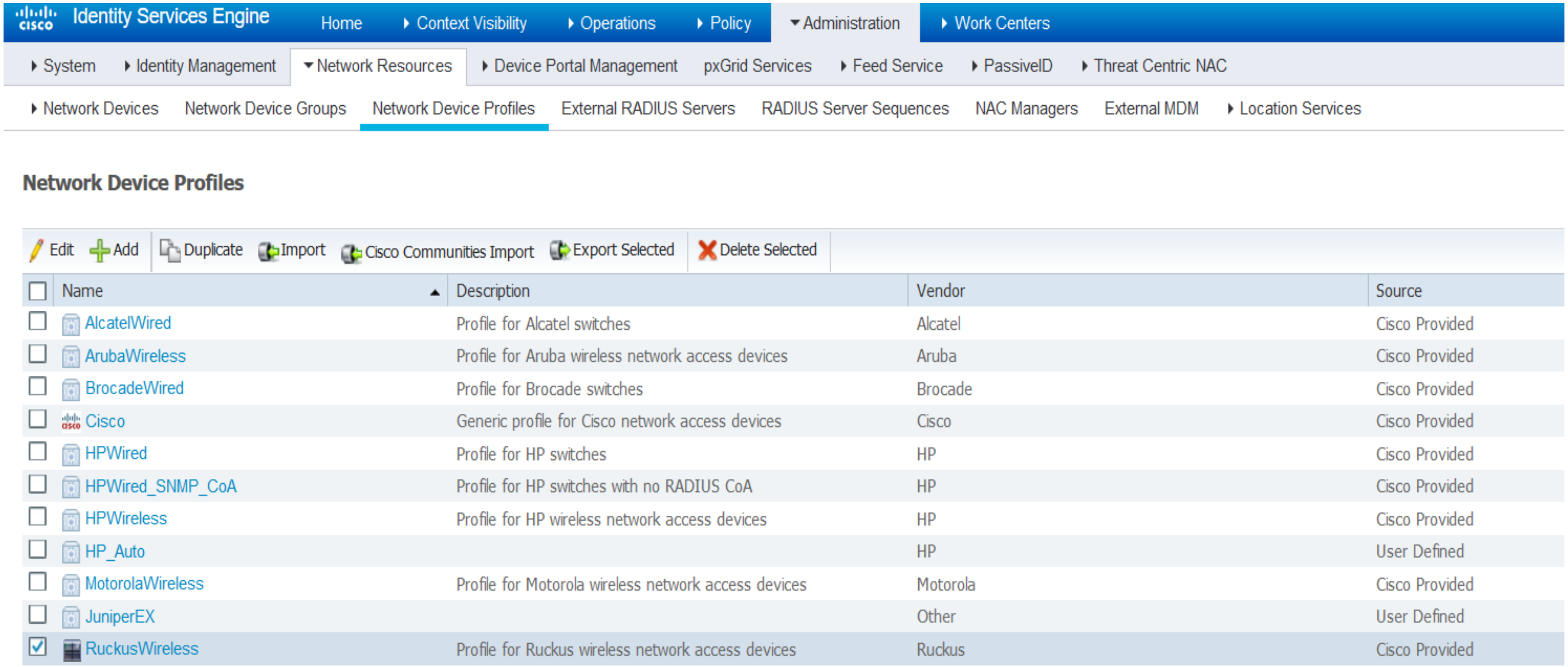
2.1.7 Change of authorization (CoA) format (Radius or SNMP) of that device is using

3 Identity Services Engine 2.1 Configuration

3.1 Creating (Modifying) Ruckus NAD Profile in ISE (optional)

ISE has built-in Ruckus NAD profile for wired scenario. Customer may create the new NAD profile by duplicating the exist profile.

Step 1	Choose **Administration** > **Network Resources** > **Network Device Profiles.**
Step 2	Click **Add** or **Duplicate**(after selecting exist NAD profile).
Step 3	Modify the section requires
Step 4	Click **Save.**

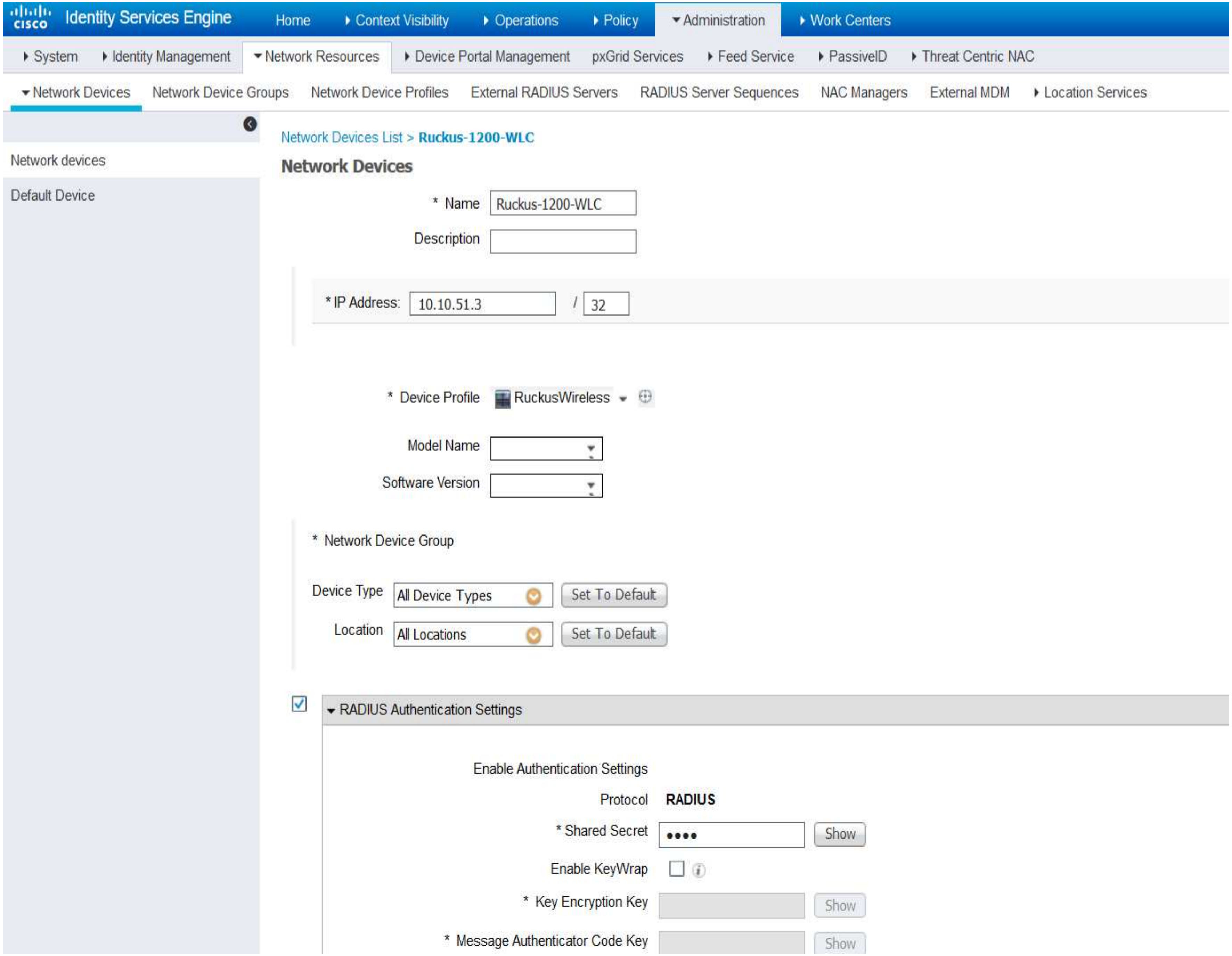


Network Device Profiles

	Name	Description	Vendor	Source
□	AlcatelWired	Profile for Alcatel switches	Alcatel	Cisco Provided
□	ArubaWireless	Profile for Aruba wireless network access devices	Aruba	Cisco Provided
□	BrocadeWired	Profile for Brocade switches	Brocade	Cisco Provided
□	Cisco	Generic profile for Cisco network access devices	Cisco	Cisco Provided
□	HPWired	Profile for HP switches	HP	Cisco Provided
□	HPWired_SNMP_CoA	Profile for HP switches with no RADIUS CoA	HP	Cisco Provided
□	HPWireless	Profile for HP wireless network access devices	HP	Cisco Provided
□	HP_Auto		HP	User Defined
□	MotorolaWireless	Profile for Motorola wireless network access devices	Motorola	Cisco Provided
□	JuniperEX		Other	User Defined
☑	RuckusWireless	Profile for Ruckus wireless network access devices	Ruckus	Cisco Provided

3.2 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. '**Ruckus-1200-WLC**')
Step 4	Enter valid IP Address
Step 5	Select under Device Profile **'RuckusWireless'** (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.



Network Devices List > **Ruckus-1200-WLC**

Network Devices

* Name: Ruckus-1200-WLC

Description:

* IP Address: 10.10.51.3 / 32

* Device Profile: RuckusWireless

Model Name:

Software Version:

* Network Device Group

Device Type: All Device Types

Location: All Locations

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: ••••

Enable KeyWrap: □

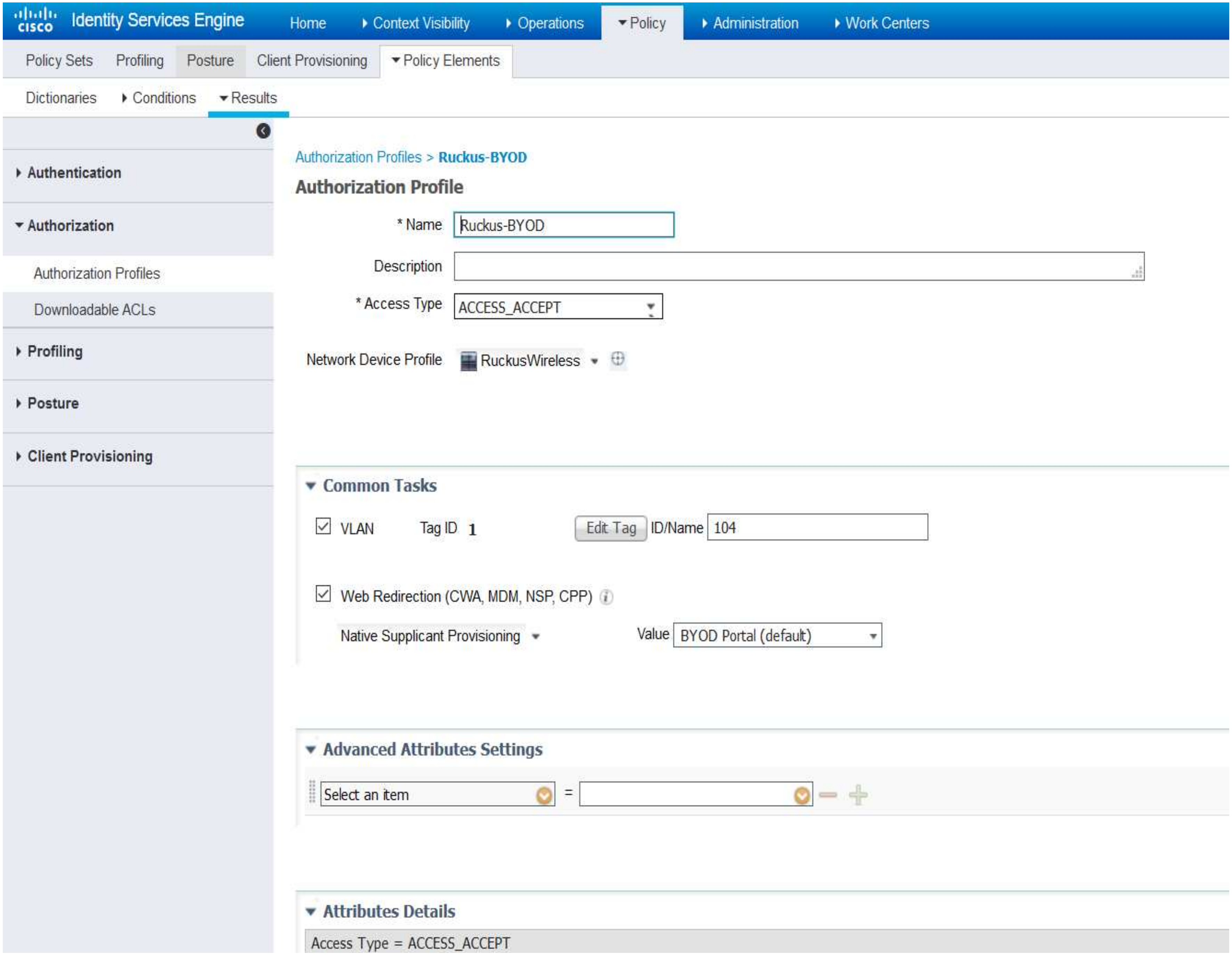
* Key Encryption Key:

* Message Authenticator Code Key:

3.3 Creating authorization Profiles for each flows

3.3.1 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. '**Ruckus**-BYOD')
Step 4	Select **'ACCESS_ACCEPT'** in Access Type option
Step 5	Select under Network Device Profile **'RuckusWireless'**
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.



Authorization Profiles > Ruckus-BYOD

Authorization Profile

* Name: Ruckus-BYOD

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: RuckusWireless

Common Tasks

☑ VLAN Tag ID 1 Edit Tag ID/Name 104

☑ Web Redirection (CWA, MDM, NSP, CPP)

Native Supplicant Provisioning Value BYOD Portal (default)

Advanced Attributes Settings

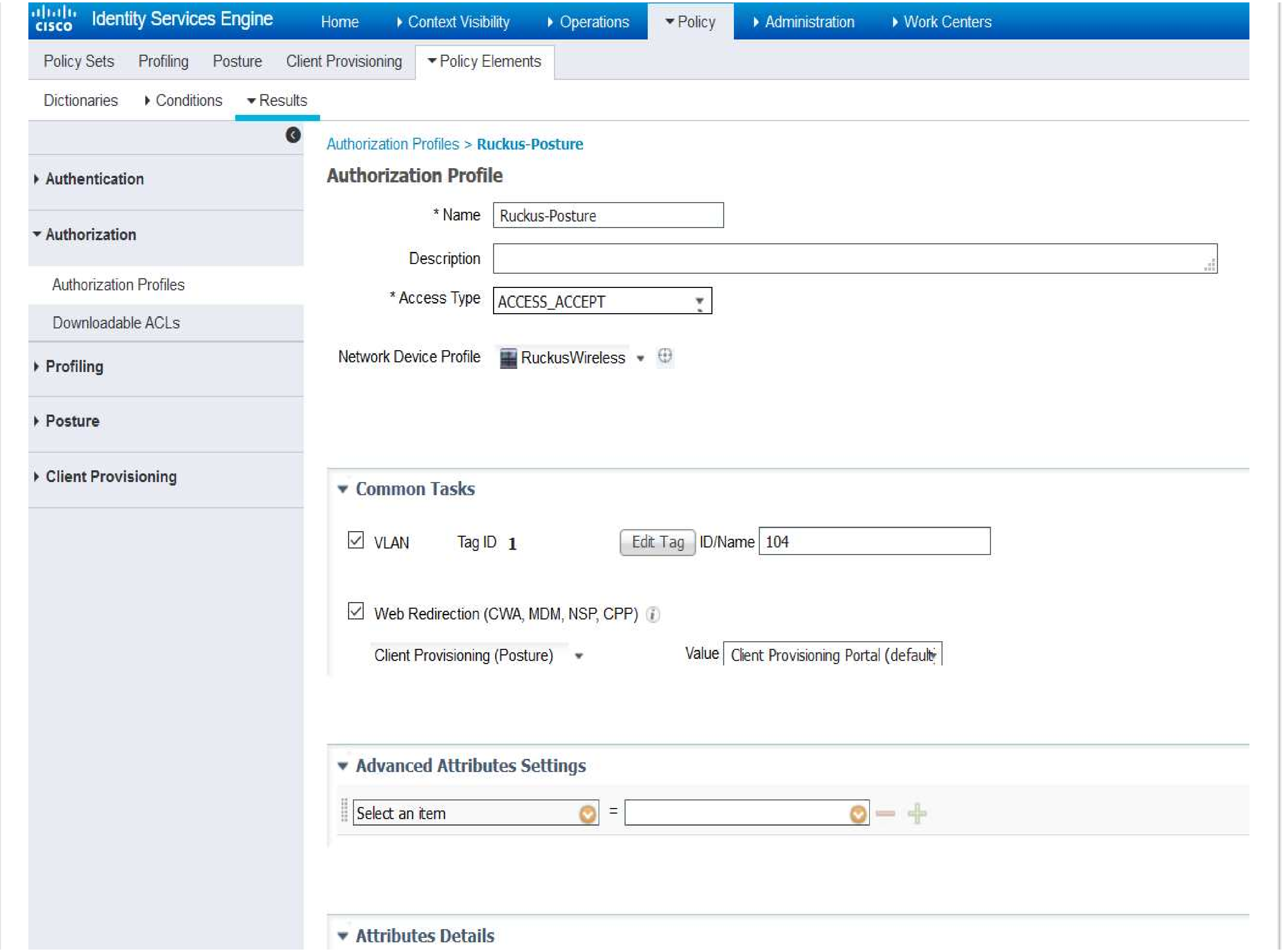
Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT

3.3.2 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. '**Ruckus**-Posture')
Step 4	Select **'ACCESS_ACCEPT'** in Access Type option
Step 5	Select under Network Device Profile **'RuckusWireless'**
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.



Authorization Profiles > Ruckus-Posture

Authorization Profile

* Name: Ruckus-Posture

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: RuckusWireless

Common Tasks

☑ VLAN Tag ID 1 Edit Tag ID/Name 104

☑ Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) Value Client Provisioning Portal (default)

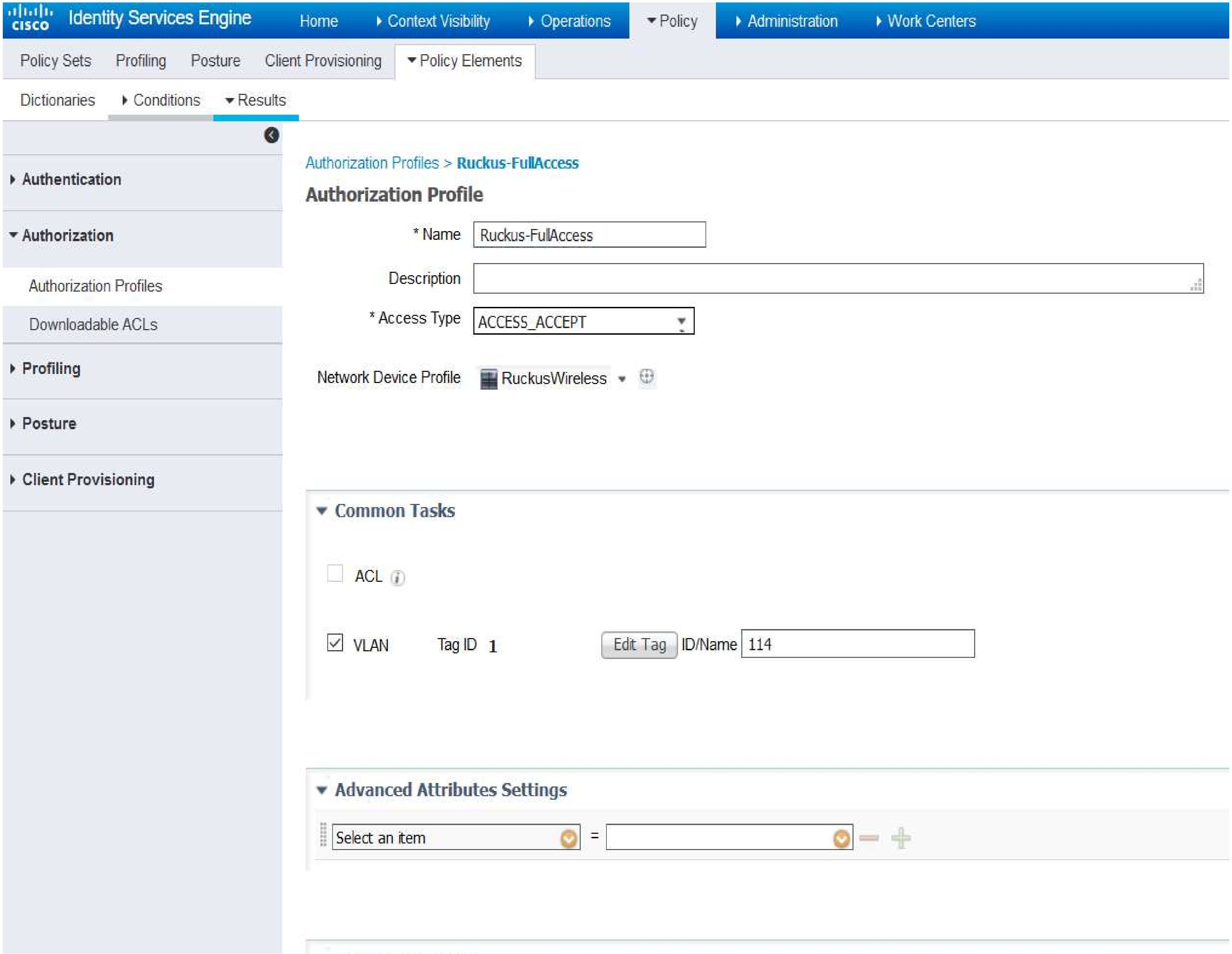
Advanced Attributes Settings

Select an item =

Attributes Details

3.3.3 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. ‘**Ruckus-FullAccess’**)
Step 4	Select **‘ACCESS_ACCEPT’** in Access Type option
Step 5	Select under Network Device Profile **‘RuckusWireless’**
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.



Authorization Profiles > **Ruckus-FullAccess**

Authorization Profile

* Name: Ruckus-FullAccess

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: RuckusWireless

Common Tasks

□ ACL

☑ VLAN Tag ID 1 ID/Name 114

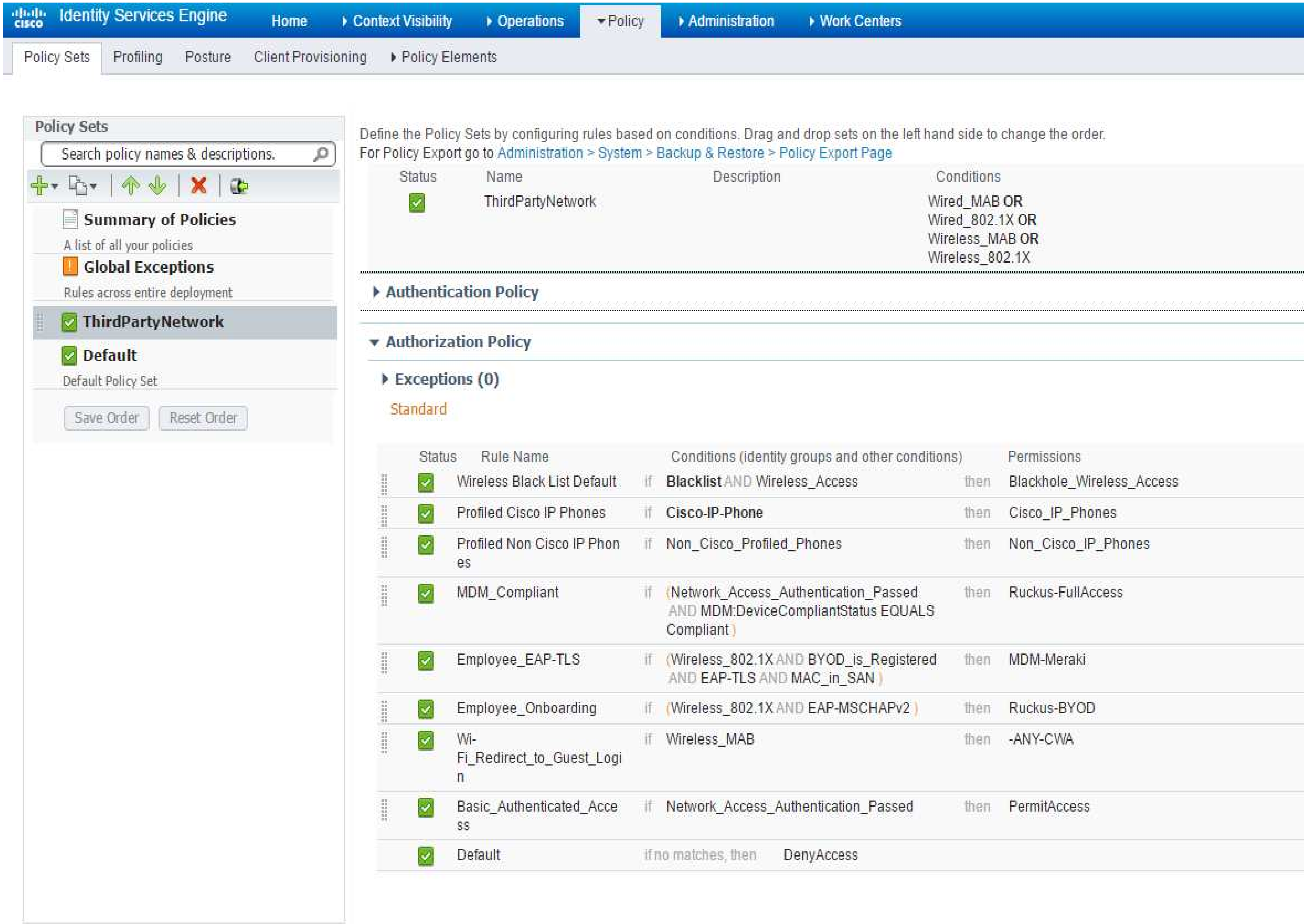
Advanced Attributes Settings

Select an item =

3.4 Identity Services Engine 2.1 Authorization policy Configuration

3.4.1 Create authorization rule in policy sets

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
✓	ThirdPartyNetwork		Wired_MAB OR Wired_802.1X OR Wireless_MAB OR Wireless_802.1X

Authentication Policy

Authorization Policy

Exceptions (0)

Standard

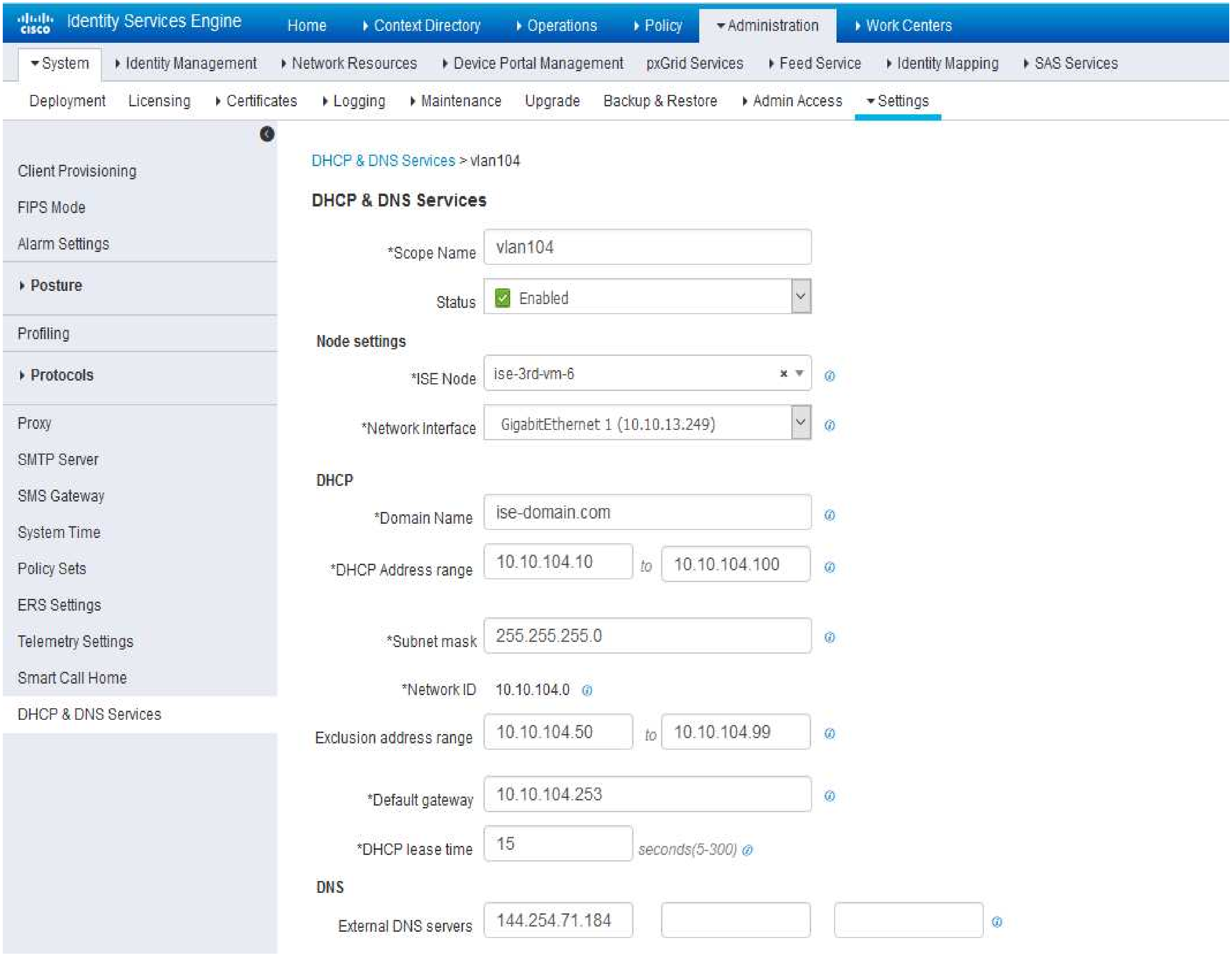
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	Blacklist AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones
✓	MDM_Compliant	if	(Network_Access_Authentication_Passed AND MDM:DeviceCompliantStatus EQUALS Compliant)	then	Ruckus-FullAccess
✓	Employee_EAP-TLS	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then	MDM-Meraki
✓	Employee_Onboarding	if	(Wireless_802.1X AND EAP-MSCHAPv2)	then	Ruckus-BYOD
✓	Wi-Fi_Redirect_to_Guest_Login	if	Wireless_MAB	then	-ANY-CWA
✓	Basic_Authenticated_Access	if	Network_Access_Authentication_Passed	then	PermitAccess
✓	Default	if no matches, then	DenyAccess		

3.5 Configuring the DHCP/DNS services in ISE for Auth VLAN flow

The Auth VLAN flow designated to third party device which doesn't support URL-redirection option.

How Auth VLAN flow works:

1. The guest endpoint connects to the network device.
2. The device sends Radius/MAB request to ISE.
3. ISE runs the MAB Authentication/Authorization policy
4. ISE stores the Guest Portal details on the user session on Session cache.
5. ISE responds with the Radius Access carrying the Guest VLAN name.
6. The guest endpoint obtains network access.
7. The endpoint broadcasts a DHCP request and obtains a client IP address and the ISE sinkhole DNS IP address from the ISE DHCP service.
8. Endpoint browser sends a DNS query and receives the ISE's IP address.
9. Endpoint HTTP/S request is directed to the ISE box.
10. ISE maps the client IP address to the MAC address using DHCP query.
11. ISE searches the user session by the MAC address, extracts the Guest portal details and builds the portal URL
12. ISE responses with HTTP 301/Moved providing the guest portal URL.
13. The endpoint browser redirects to the Guest portal page.
14. The client authenticates in Guest portal
15. ISE issues a CoA request with authorization details.
16. Endpoint obtains an access to the corporate network
17. Endpoint receives an IP address from the enterprise DHCP.



DHCP & DNS Services

*Scope Name: vlan104

Status: ☑ Enabled

Node settings

*ISE Node: ise-3rd-vm-6

*Network Interface: GigabitEthernet 1 (10.10.13.249)

DHCP

*Domain Name: ise-domain.com

*DHCP Address range: 10.10.104.10 to 10.10.104.100

*Subnet mask: 255.255.255.0

*Network ID: 10.10.104.0

Exclusion address range: 10.10.104.50 to 10.10.104.99

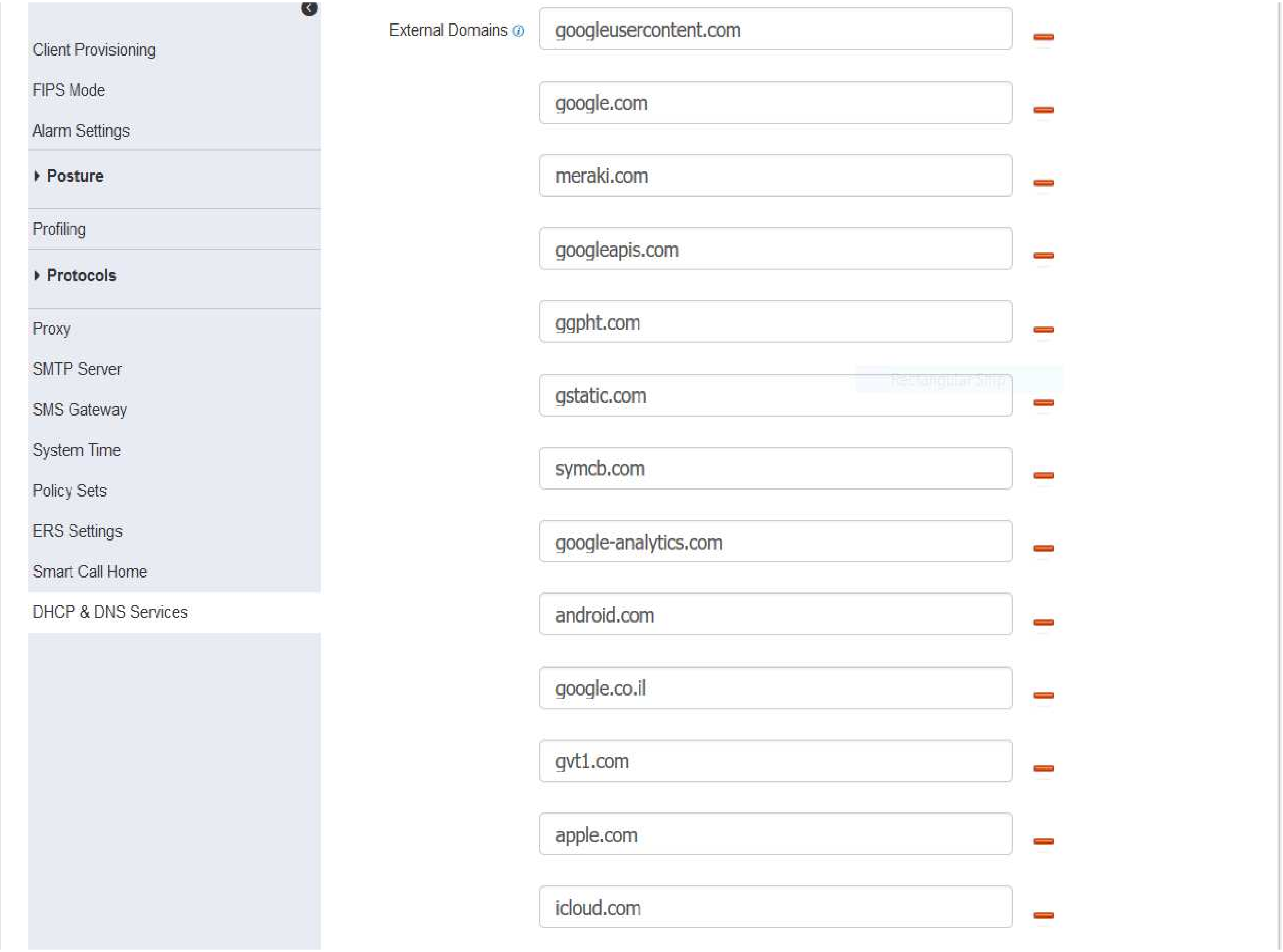
*Default gateway: 10.10.104.253

*DHCP lease time: 15 seconds(5-300)

DNS

External DNS servers: 144.254.71.184

To access Google play and MDM Meraki server, please add the following domains in 'External Domans' option:



External Domains

- googleusercontent.com
- google.com
- meraki.com
- googleapis.com
- ggpht.com
- gstatic.com
- symcb.com
- google-analytics.com
- android.com
- google.co.il
- gvt1.com
- apple.com
- icloud.com

3.6 Ruckus ZD1200 Configurations:

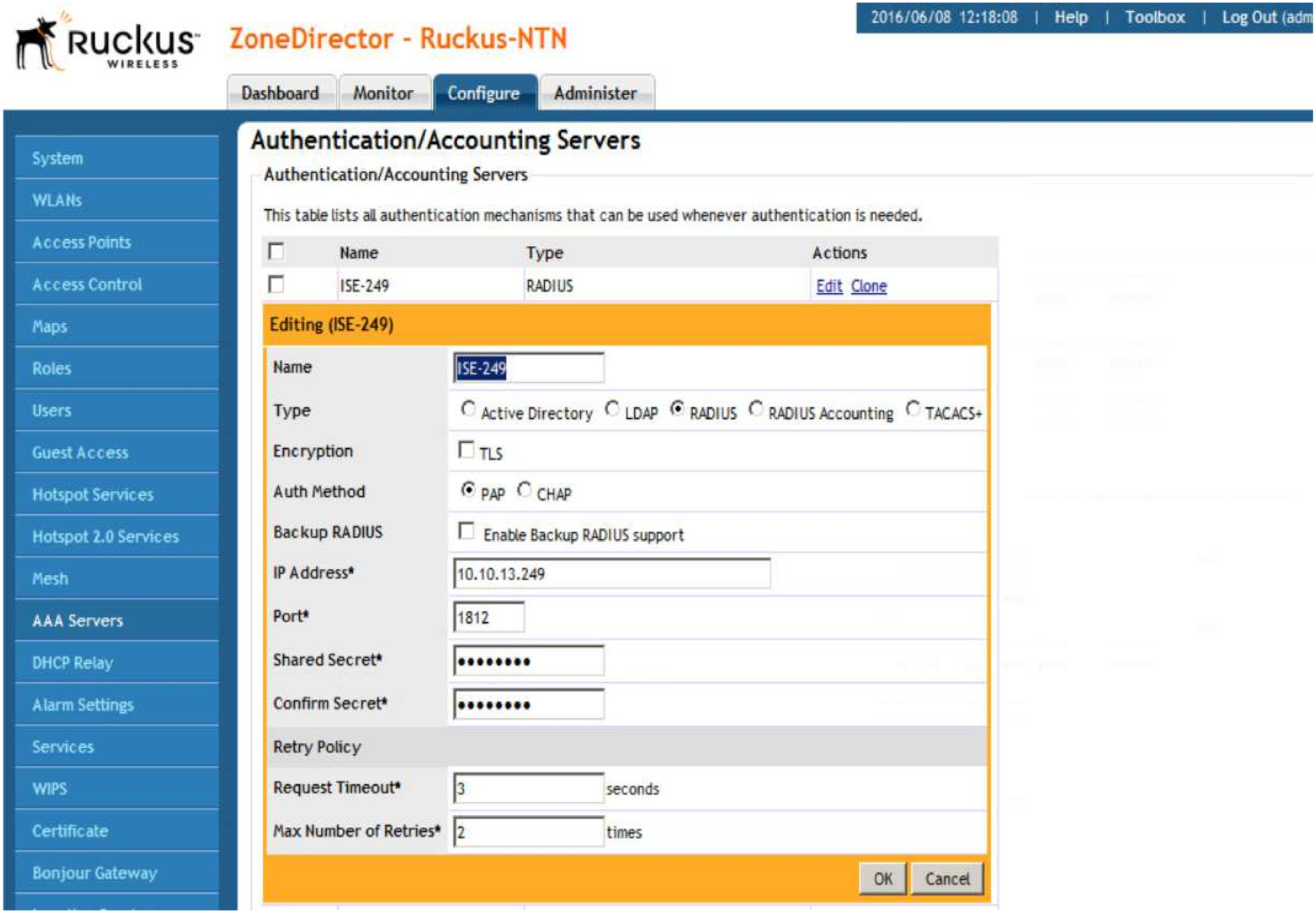
*The Radius CoA option is enabled by default.

*I used default configuration of ZD except the AAA Servers and SSID pages.

Here you can find info how to configure the AAA Servers and SSID pages:

Ruckus 1200 AAA Servers configuration:

RADIUS configuration for authentication



Authentication/Accounting Servers

Authentication/Accounting Servers

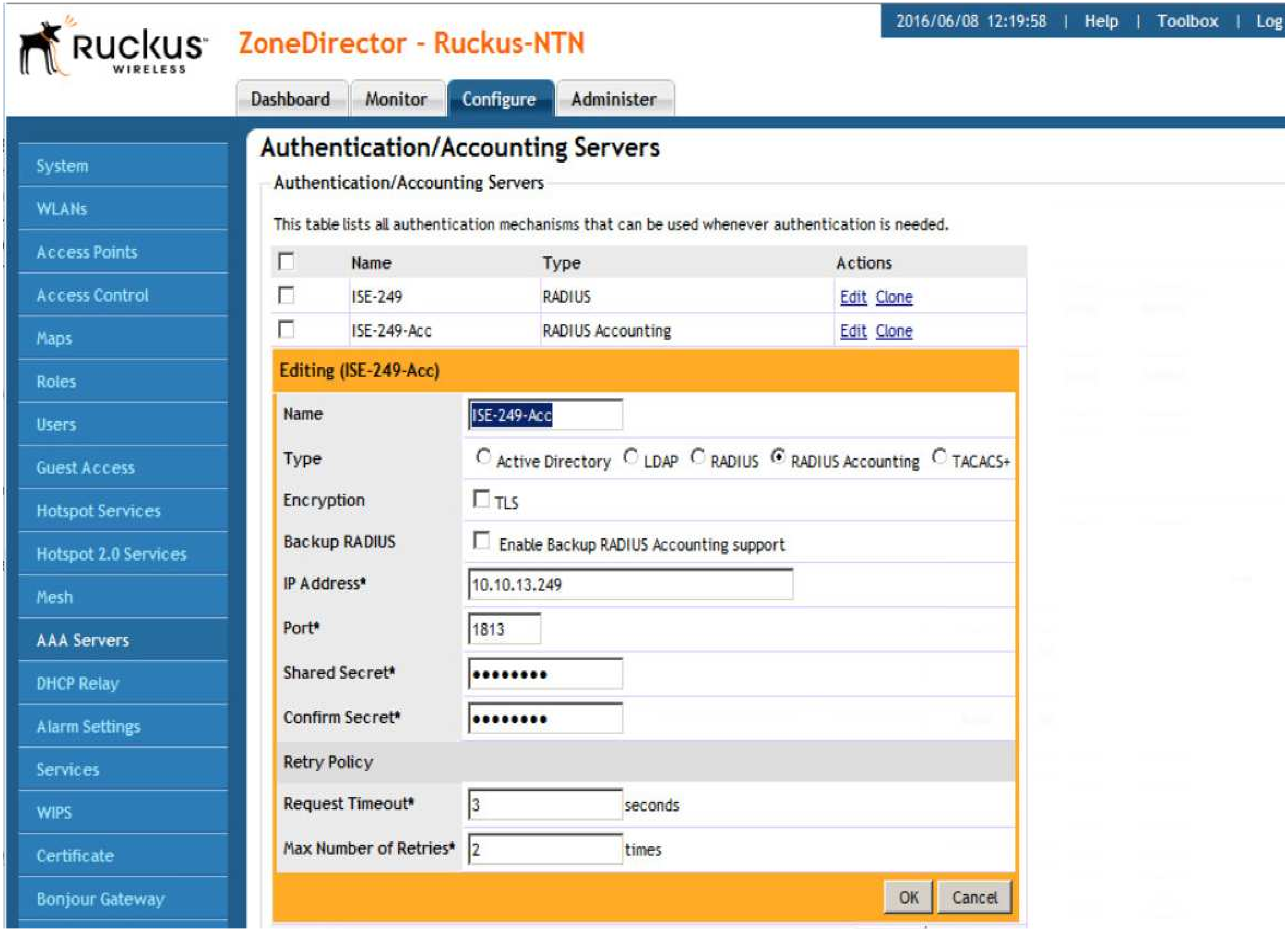
This table lists all authentication mechanisms that can be used whenever authentication is needed.

□	Name	Type	Actions
□	ISE-249	RADIUS	Edit Clone

Editing (ISE-249)

Name	ISE-249
Type	○ Active Directory ○ LDAP ● RADIUS ○ RADIUS Accounting ○ TACACS+
Encryption	□ TLS
Auth Method	● PAP ○ CHAP
Backup RADIUS	□ Enable Backup RADIUS support
IP Address*	10.10.13.249
Port*	1812
Shared Secret*	••••••••
Confirm Secret*	••••••••
Retry Policy	
Request Timeout*	3 seconds
Max Number of Retries*	2 times

RADIUS configuration for accounting:



Authentication/Accounting Servers

Authentication/Accounting Servers

This table lists all authentication mechanisms that can be used whenever authentication is needed.

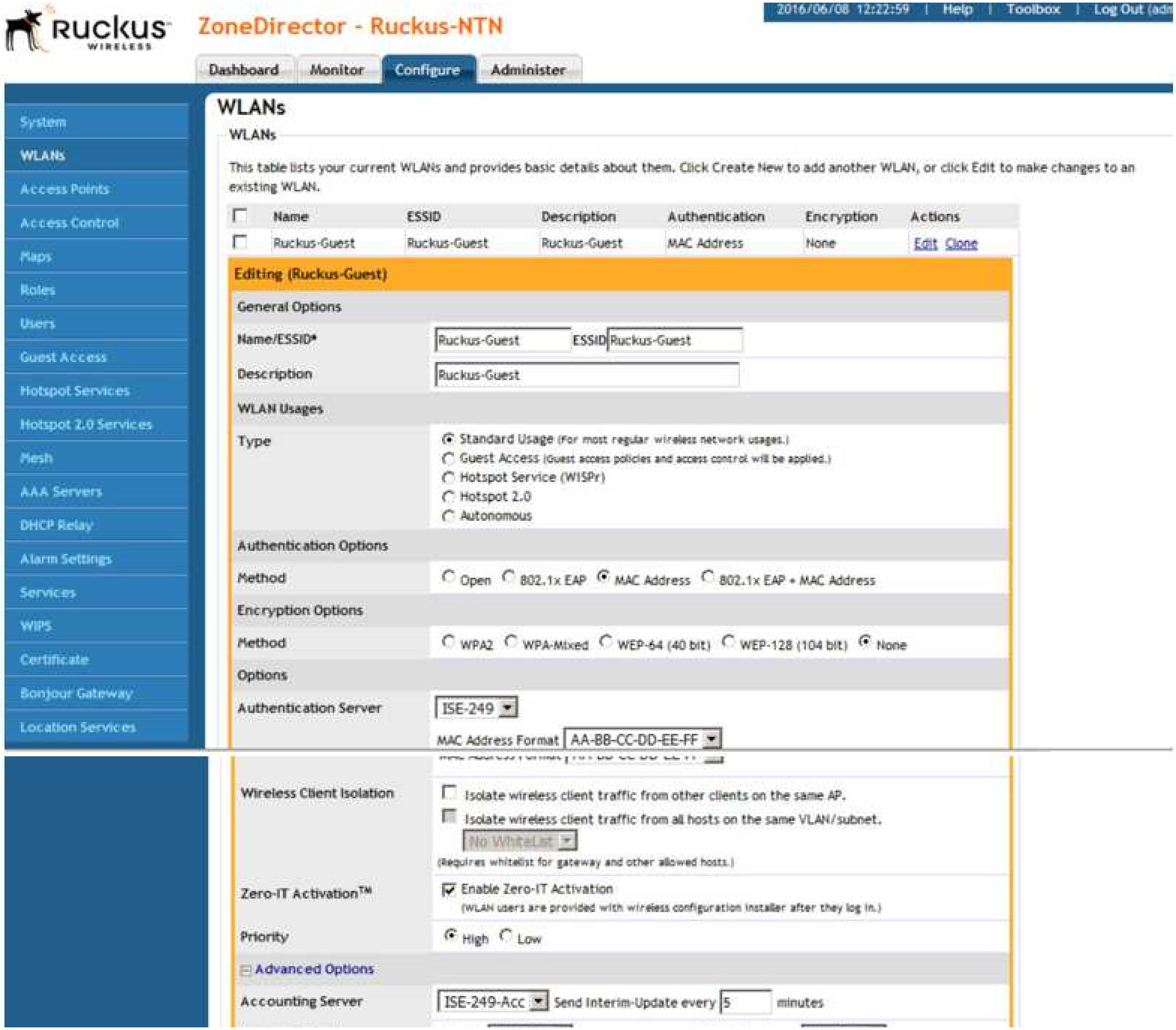
□	Name	Type	Actions
□	ISE-249	RADIUS	Edit Clone
□	ISE-249-Acc	RADIUS Accounting	Edit Clone

Editing (ISE-249-Acc)

Name	ISE-249-Acc
Type	○ Active Directory ○ LDAP ○ RADIUS ● RADIUS Accounting ○ TACACS+
Encryption	□ TLS
Backup RADIUS	□ Enable Backup RADIUS Accounting support
IP Address*	10.10.13.249
Port*	1813
Shared Secret*	••••••••
Confirm Secret*	••••••••
Retry Policy	
Request Timeout*	3 seconds
Max Number of Retries*	2 times

OK Cancel

Guest SSID configuration:



WLANs

WLANs

This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN, or click Edit to make changes to an existing WLAN.

□	Name	ESSID	Description	Authentication	Encryption	Actions
□	Ruckus-Guest	Ruckus-Guest	Ruckus-Guest	MAC Address	None	Edit Clone

Editing (Ruckus-Guest)

General Options

Name/ESSID* Ruckus-Guest ESSID Ruckus-Guest

Description Ruckus-Guest

WLAN Usages

Type
● Standard Usage (For most regular wireless network usages.)
○ Guest Access (Guest access policies and access control will be applied.)
○ Hotspot Service (WISPr)
○ Hotspot 2.0
○ Autonomous

Authentication Options

Method ○ Open ○ 802.1x EAP ● MAC Address ○ 802.1x EAP + MAC Address

Encryption Options

Method ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ● None

Options

Authentication Server ISE-249

MAC Address Format AA-BB-CC-DD-EE-FF

Wireless Client Isolation
□ Isolate wireless client traffic from other clients on the same AP.
□ Isolate wireless client traffic from all hosts on the same VLAN/subnet.
No WhiteList
(Requires whitelist for gateway and other allowed hosts.)

Zero-IT Activation™ ☑ Enable Zero-IT Activation
(WLAN users are provided with wireless configuration installer after they log in.)

Priority ● High ○ Low

⊟ Advanced Options

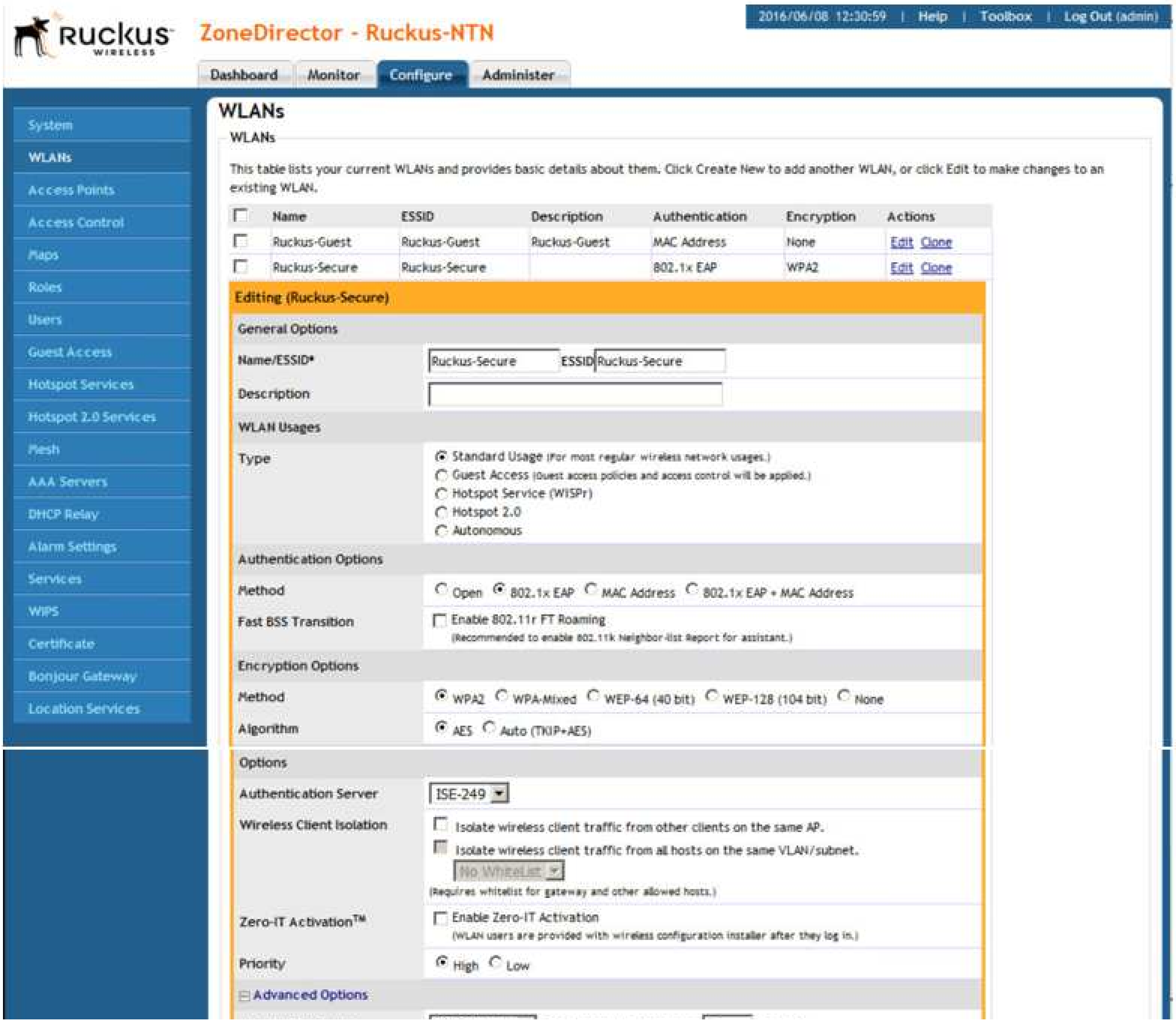
Accounting Server ISE-249-Acc Send Interim-Update every 5 minutes

---

Notes: Guest flow will not work using this gear, the reason that is the device doesn't send 'Class' attribute as prat of accouting request.CSCuz81959-Some 3rd party NADs are not sending "Class" attribute in account-request

----

Secure (dot1x/EAP) SSID configuration:



WLANs

WLANs

This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN, or click Edit to make changes to an existing WLAN.

□	Name	ESSID	Description	Authentication	Encryption	Actions
□	Ruckus-Guest	Ruckus-Guest	Ruckus-Guest	MAC Address	None	Edit Clone
□	Ruckus-Secure	Ruckus-Secure		802.1x EAP	WPA2	Edit Clone

Editing (Ruckus-Secure)

General Options

Name/ESSID* Ruckus-Secure ESSID Ruckus-Secure

Description

WLAN Usages

Type
● Standard Usage (For most regular wireless network usages.)
○ Guest Access (Guest access policies and access control will be applied.)
○ Hotspot Service (WISPr)
○ Hotspot 2.0
○ Autonomous

Authentication Options

Method ○ Open ● 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address

Fast BSS Transition □ Enable 802.11r FT Roaming
(Recommended to enable 802.11k Neighbor-list Report for assistant.)

Encryption Options

Method ● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ○ None

Algorithm ● AES ○ Auto (TKIP+AES)

Options

Authentication Server ISE-249

Wireless Client Isolation
□ Isolate wireless client traffic from other clients on the same AP.
□ Isolate wireless client traffic from all hosts on the same VLAN/subnet.
No WhiteList
(Requires whitelist for gateway and other allowed hosts.)

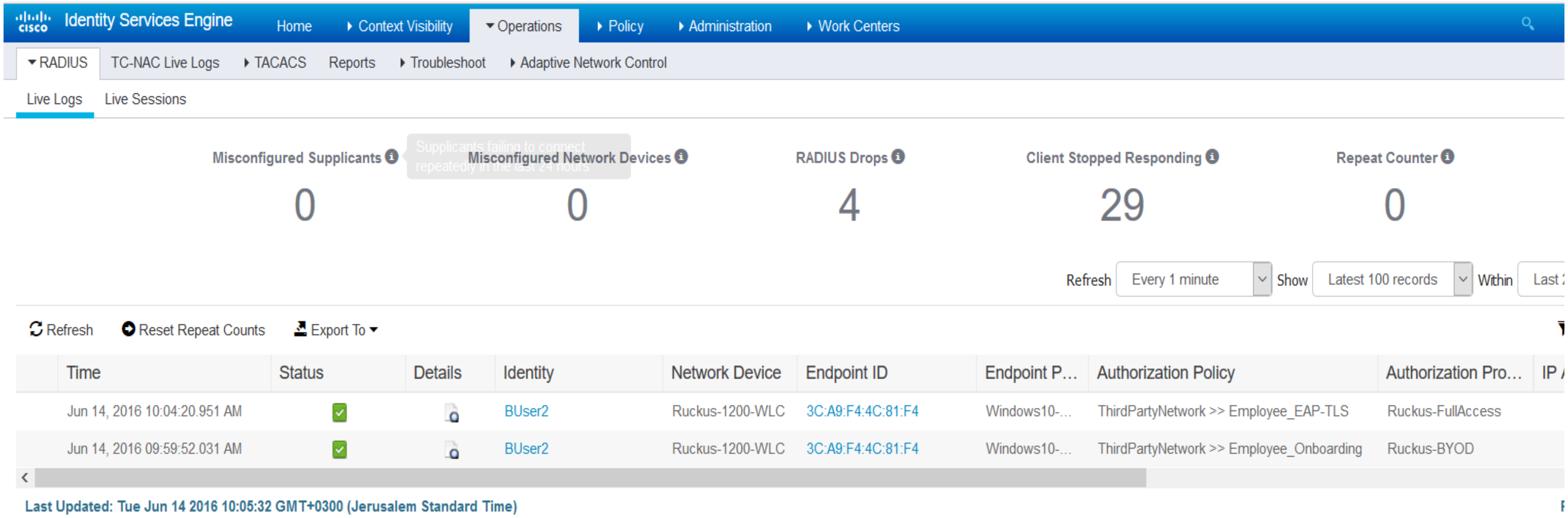
Zero-IT Activation™ □ Enable Zero-IT Activation
(WLAN users are provided with wireless configuration installer after they log in.)

Priority ● High ○ Low

⊟ Advanced Options

3.7 Verify

3.7.1 MnT report:



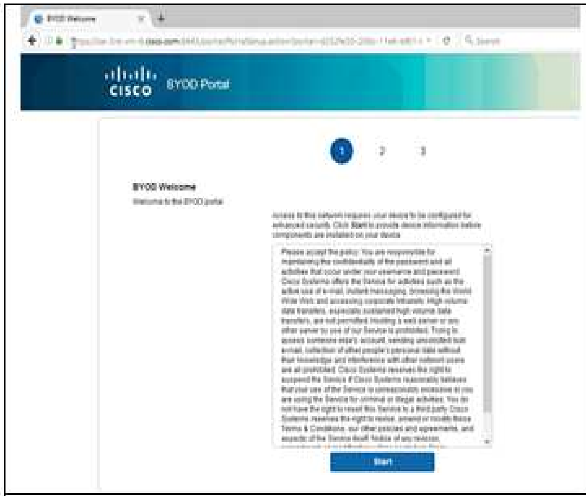
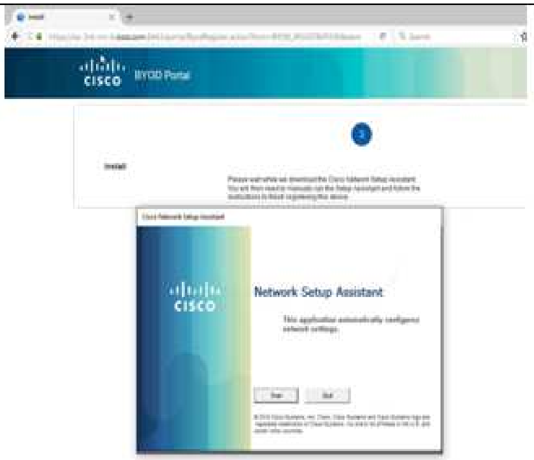
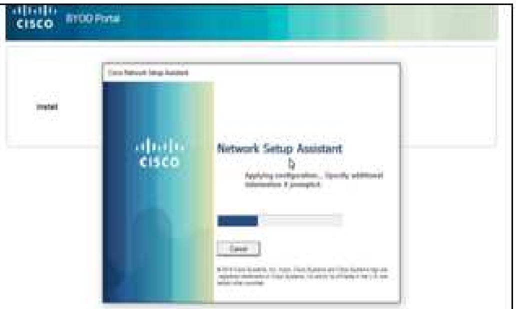
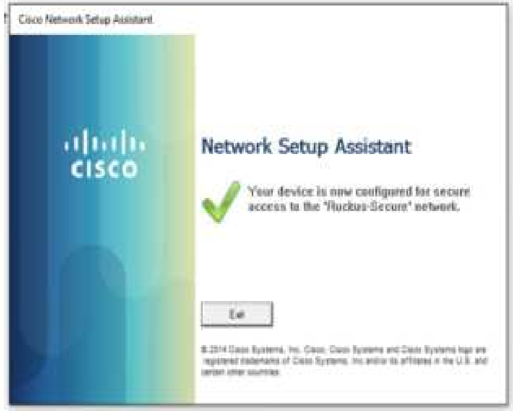
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	4	29	0

Refresh: Every 1 minute Show: Latest 100 records Within: Last

Time	Status	Details	Identity	Network Device	Endpoint ID	Endpoint P...	Authorization Policy	Authorization Pro...	IP
Jun 14, 2016 10:04:20.951 AM	✓		BUser2	Ruckus-1200-WLC	3C:A9:F4:4C:81:F4	Windows10-...	ThirdPartyNetwork >> Employee_EAP-TLS	Ruckus-FullAccess	
Jun 14, 2016 09:59:52.031 AM	✓		BUser2	Ruckus-1200-WLC	3C:A9:F4:4C:81:F4	Windows10-...	ThirdPartyNetwork >> Employee_Onboarding	Ruckus-BYOD	

Last Updated: Tue Jun 14 2016 10:05:32 GMT+0300 (Jerusalem Standard Time)

3.7.2 BYOD flow on Windows

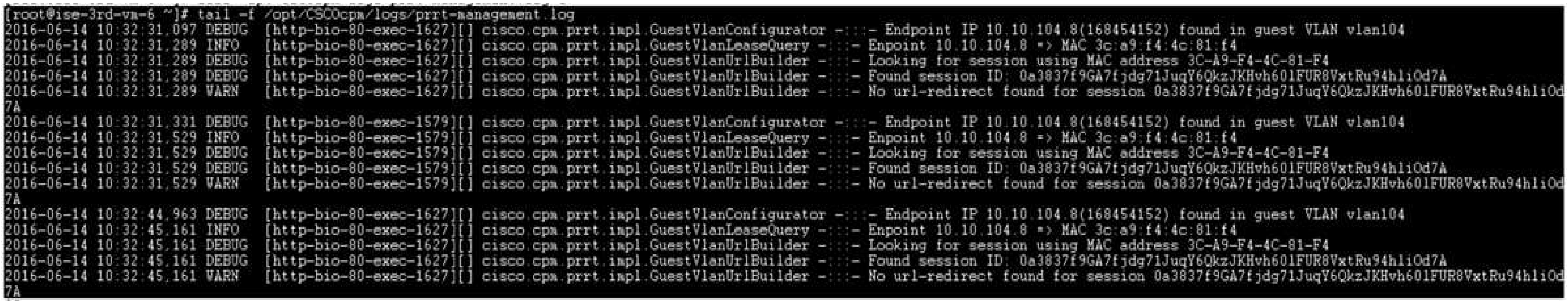
 BYOD Welcome Welcome to the BYOD portal Access to this network requires your device to be configured for enhanced security. Click Start to provide device information before components are installed on your device. Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision,	 Install Please wait while we download the Cisco Network Setup Assistant. You will then need to manually run the Setup Assistant and follow the instructions to finish registering this device. Cisco Network Setup Assistant Network Setup Assistant This application automatically configures network settings.	 Install Cisco Network Setup Assistant Network Setup Assistant Applying configuration... Specify additional information if prompted.
	 Cisco Network Setup Assistant Network Setup Assistant Your device is now configured for secure access to the 'Ruckus-Secure' network. © 2014 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.	

3.8 Troubleshoot

3.8.1 the endpoint is connected and it got the BYOD authz profile but when opening the endpoint's browser it doesn't display the BYOD portal:

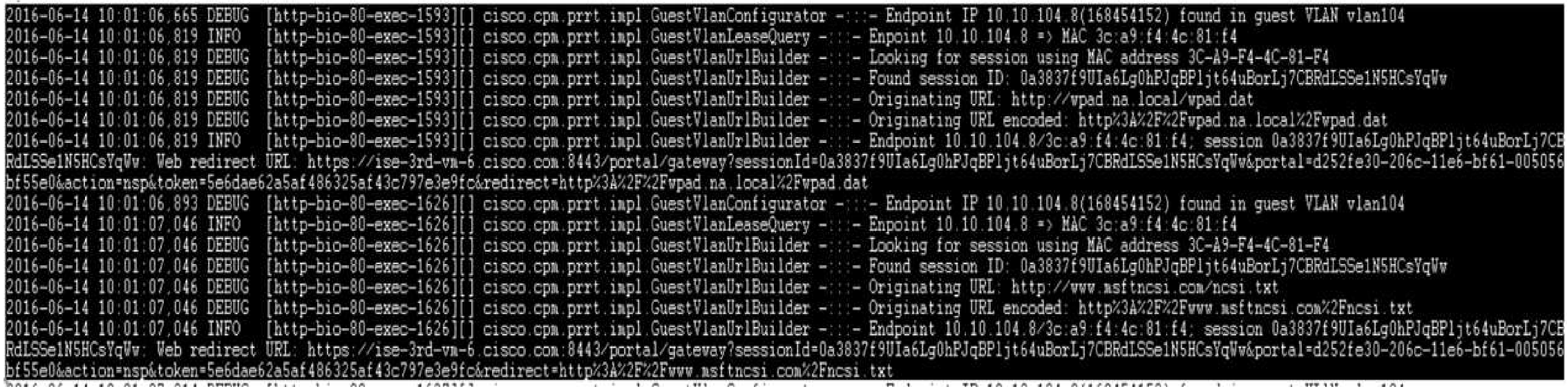
Please the the prrt-management.log after changing it to debug mode if url-redirect found for session.

if you see this log, it means the url-redirect not found for this session:



```
[root@ise-3rd-vm-6 ~]# tail -f /opt/CSCOcpm/logs/prrt-management.log
2016-06-14 10:32:31,097 DEBUG  [http-bio-80-exec-1627][] cisco.cpm.prrt.impl.GuestVlanConfigurator -:::- Endpoint IP 10.10.104.8(168454152) found in guest VLAN vlan104
2016-06-14 10:32:31,289 INFO   [http-bio-80-exec-1627][] cisco.cpm.prrt.impl.GuestVlanLeaseQuery -:::- Enpoint 10.10.104.8 => MAC 3c:a9:f4:4c:81:f4
2016-06-14 10:32:31,289 DEBUG  [http-bio-80-exec-1627][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Looking for session using MAC address 3C-A9-F4-4C-81-F4
2016-06-14 10:32:31,289 DEBUG  [http-bio-80-exec-1627][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Found session ID: 0a3837f9GA7fjdg71JuqY6QkzJKHvh601FUR8VxtRu94hliOd7A
2016-06-14 10:32:31,289 WARN   [http-bio-80-exec-1627][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- No url-redirect found for session 0a3837f9GA7fjdg71JuqY6QkzJKHvh601FUR8VxtRu94hliOd
7A
2016-06-14 10:32:31,331 DEBUG  [http-bio-80-exec-1579][] cisco.cpm.prrt.impl.GuestVlanConfigurator -:::- Endpoint IP 10.10.104.8(168454152) found in guest VLAN vlan104
2016-06-14 10:32:31,529 INFO   [http-bio-80-exec-1579][] cisco.cpm.prrt.impl.GuestVlanLeaseQuery -:::- Enpoint 10.10.104.8 => MAC 3c:a9:f4:4c:81:f4
2016-06-14 10:32:31,529 DEBUG  [http-bio-80-exec-1579][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Looking for session using MAC address 3C-A9-F4-4C-81-F4
2016-06-14 10:32:31,529 DEBUG  [http-bio-80-exec-1579][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Found session ID: 0a3837f9GA7fjdg71JuqY6QkzJKHvh601FUR8VxtRu94hliOd7A
2016-06-14 10:32:31,529 WARN   [http-bio-80-exec-1579][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- No url-redirect found for session 0a3837f9GA7fjdg71JuqY6QkzJKHvh601FUR8VxtRu94hliOd
7A
2016-06-14 10:32:44,963 DEBUG  [http-bio-80-exec-1627][] cisco.cpm.prrt.impl.GuestVlanConfigurator -:::- Endpoint IP 10.10.104.8(168454152) found in guest VLAN vlan104
2016-06-14 10:32:45,161 INFO   [http-bio-80-exec-1627][] cisco.cpm.prrt.impl.GuestVlanLeaseQuery -:::- Enpoint 10.10.104.8 => MAC 3c:a9:f4:4c:81:f4
2016-06-14 10:32:45,161 DEBUG  [http-bio-80-exec-1627][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Looking for session using MAC address 3C-A9-F4-4C-81-F4
2016-06-14 10:32:45,161 DEBUG  [http-bio-80-exec-1627][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Found session ID: 0a3837f9GA7fjdg71JuqY6QkzJKHvh601FUR8VxtRu94hliOd7A
2016-06-14 10:32:45,161 WARN   [http-bio-80-exec-1627][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- No url-redirect found for session 0a3837f9GA7fjdg71JuqY6QkzJKHvh601FUR8VxtRu94hliOd
7A
```

you see this log when the url-redirection found for session:



```
2016-06-14 10:01:06,665 DEBUG  [http-bio-80-exec-1593][] cisco.cpm.prrt.impl.GuestVlanConfigurator -:::- Endpoint IP 10.10.104.8(168454152) found in guest VLAN vlan104
2016-06-14 10:01:06,819 INFO   [http-bio-80-exec-1593][] cisco.cpm.prrt.impl.GuestVlanLeaseQuery -:::- Enpoint 10.10.104.8 => MAC 3c:a9:f4:4c:81:f4
2016-06-14 10:01:06,819 DEBUG  [http-bio-80-exec-1593][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Looking for session using MAC address 3C-A9-F4-4C-81-F4
2016-06-14 10:01:06,819 DEBUG  [http-bio-80-exec-1593][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Found session ID: 0a3837f9UIa6Lg0hPJqBPljt64uBorLj7CBRdLSSe1N5HCsYqWw
2016-06-14 10:01:06,819 DEBUG  [http-bio-80-exec-1593][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Originating URL: http://wpad.na.local/wpad.dat
2016-06-14 10:01:06,819 DEBUG  [http-bio-80-exec-1593][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Originating URL encoded: http%3A%2F%2Fwpad.na.local%2Fwpad.dat
2016-06-14 10:01:06,819 INFO   [http-bio-80-exec-1593][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Endpoint 10.10.104.8/3c:a9:f4:4c:81:f4; session 0a3837f9UIa6Lg0hPJqBPljt64uBorLj7CB
RdLSSe1N5HCsYqWw: Web redirect URL: https://ise-3rd-vm-6.cisco.com:8443/portal/gateway?sessionId=0a3837f9UIa6Lg0hPJqBPljt64uBorLj7CBRdLSSe1N5HCsYqWw&portal=d252fe30-206c-11e6-bf61-005056
bf55e0&action=nsp&token=5e6dae62a5af486325af43c797e3e9fc&redirect=http%3A%2F%2Fwpad.na.local%2Fwpad.dat
2016-06-14 10:01:06,893 DEBUG  [http-bio-80-exec-1626][] cisco.cpm.prrt.impl.GuestVlanConfigurator -:::- Endpoint IP 10.10.104.8(168454152) found in guest VLAN vlan104
2016-06-14 10:01:07,046 INFO   [http-bio-80-exec-1626][] cisco.cpm.prrt.impl.GuestVlanLeaseQuery -:::- Enpoint 10.10.104.8 => MAC 3c:a9:f4:4c:81:f4
2016-06-14 10:01:07,046 DEBUG  [http-bio-80-exec-1626][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Looking for session using MAC address 3C-A9-F4-4C-81-F4
2016-06-14 10:01:07,046 DEBUG  [http-bio-80-exec-1626][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Found session ID: 0a3837f9UIa6Lg0hPJqBPljt64uBorLj7CBRdLSSe1N5HCsYqWw
2016-06-14 10:01:07,046 DEBUG  [http-bio-80-exec-1626][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Originating URL: http://www.msftncsi.com/ncsi.txt
2016-06-14 10:01:07,046 DEBUG  [http-bio-80-exec-1626][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Originating URL encoded: http%3A%2F%2Fwww.msftncsi.com%2Fncsi.txt
2016-06-14 10:01:07,046 INFO   [http-bio-80-exec-1626][] cisco.cpm.prrt.impl.GuestVlanUrlBuilder -:::- Endpoint 10.10.104.8/3c:a9:f4:4c:81:f4; session 0a3837f9UIa6Lg0hPJqBPljt64uBorLj7CB
RdLSSe1N5HCsYqWw: Web redirect URL: https://ise-3rd-vm-6.cisco.com:8443/portal/gateway?sessionId=0a3837f9UIa6Lg0hPJqBPljt64uBorLj7CBRdLSSe1N5HCsYqWw&portal=d252fe30-206c-11e6-bf61-005056
bf55e0&action=nsp&token=5e6dae62a5af486325af43c797e3e9fc&redirect=http%3A%2F%2Fwww.msftncsi.com%2Fncsi.txt
```

3.8.2 issue: i can't to whitelist domains or get ip address using Auth VLAN:

1. login to ISE as root
2. enable DNS logs (named) using this cli "rndc querylog"
3. watch the logs using "tail -f /var/log/messages"

Everyone's Tags: tz:scim:639231261 View All (1)