DYNAMIC SEGMENTATION WITH CISCO ISE

CONTENTS
Dynamic Segmentation With Cisco ISE ........................................................................................................ 1
Requirements ........................................................................................................................................ 1
Overview ............................................................................................................................................. 1
Adding a Device TO ISE .......................................................................................................................... 2
Adding The User Role VSA to the HP Dictionary ..................................................................................... 5
Using the HP-User-Role VSA ................................................................................................................... 9
Verification ........................................................................................................................................... 11

REQUIREMENTS
- Aruba Mobility Controller
- Aruba Switch (2930M/F, 3810M, 5400)
- Cisco ISE

OVERVIEW
Dynamic Segmentation with an Aruba Switch allows us to leverage User Roles. These User Roles are
applied to devices which allows policy to be applied based on the User Role rather than an IP address.
The User Role can be applied to a device in one of two ways, either using Local User Roles (LUR)
locally defined on the switch, or using Downloadable User Roles (DUR) centrally defined in ClearPass
and downloaded by the switch.

To support User-Based Tunneling (UBT), both methods utilize a “Secondary Role” which is the role
assigned at the controller for policy enforcement. User Roles are assigned dynamically based on device
authentication/authorization using a AAA Server.

In order to use User Roles with Cisco ISE, they must be defined locally on the switch. This document will
cover Local User Roles with Cisco ISE.
ADDING A DEVICE TO ISE

Description
This section will go over adding a device into Cisco ISE.

Navigate to Work Centers > BYOD > Network Devices. Click Add.
Enter the IP address, RADIUS shared secret, and Model of the switch
Switch Configuration
Pointing the switch to ISE Server

```
radius-server host <Radius-IP> dyn-authorization
radius-server host <Radius-IP> time-window 0
radius-server key < KEY-STR>
tunneled-node-server
  controller-ip <Controller-IP>
  mode role-based
aaa port-access authenticator <Ports>
aaa port-access authenticator active
aaa authorization user-role enable
```

Configuring the Local User Role on the switch

This is the User Role that will be referenced throughout this document. The Secondary Role is manually configured on the Controller and is referenced here within the local role. The VLAN-ID, user role and secondary role will need to be changed to fit your environment.

```
aaa authorization user-role name "ISE-LOCAL"
  vlan-id 101
  tunneled-node-server-redirect secondary-role "adminuser"
exit
```

Controller Configuration

```
vlan 101
interface vlan 101
  ip address <IP-Address> <Subnet-Mask>
  ip helper-address <DHCP-Server-IP>
user-role adminuser
  access-list session global-sacl
  access-list session apprf-adminuser-sacl
  access-list session allowall
```
ADDING THE USER ROLE VSA TO THE HP DICTIONARY

Description
This section will guide you through how to add the User Role Dictionary to Cisco. The HP-User-Role VSA is used to call the Local User Role which has already been pre-configured on the switch. This step can be skipped if the “HP-User-Role” VSA is already present in ISE.

1. To add the dictionary navigate to Policy>Policy Elements then click the “Radius” folder and navigate to the “HP” dictionary within the Radius Vendors Folder.
2. Click Dictionary Attributes then click add
3. After clicking add dictionary attribute enter the information below then click Submit.

Attribute name: “HP-User-Role”
Data type: “String”
Direction: “Both”
ID: “25”
4. The “HP-User-Role” should now appear.
USING THE HP-USER-ROLE VSA

Description
This section will go over how to use the HP-User-Role VSA in a Policy Set in ISE, however this will not cover how to create a policy set in ISE.

1. Now that the HP-User-Role VSA is defined in ISE, it can now be used. Navigate to Policy>Policy Sets and edit a policy for your environment. In this case we will use “User01 Policy”.

2. Under the “Policy Set” edit the “Authorization Policy”. Click the “+” symbol under profiles.
3. Once the new standard profile appears name the “Standard Profile” In this case it is named “ISE-LOCAL”. Change the Network Device Profile needs to be changed to “HPWired”.

In the “Advanced Attributes” section, the “HP-User-Role” VSA needs to be selected. The HP-User-Role” Located HP>HP-User-Role.

Once the “HP-User-Role” VSA is selected. Enter the name of the Local User Role that the switch has in its configuration. In this case it is also called “ISE-Local”.

4. Now that the profile is created, it needs to be selected so it can be used.
5. The final result should look similar to the image below. Devices are now ready to be authenticated.

VERIFICATION

The switch should show the devices authenticated with the proper local role.
ISE will show that the User Role Was applied to the switch
The result should also show the name of the “Local User Role” at the bottom.