

DYNAMIC SEGMENTATION WITH CISCO ISE

CONTENTS

Dynamic Segmentation With Cisco ISE	1
Requirments.....	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.

Network Devices

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> 2930M-Dynamic	10.128.1.6/32	HPWired	All Locations	All Device Types	Dyn-Segmentation using Local roles
<input type="checkbox"/> 9300-F1-SW0...	1.93.3.101/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/> 9300-F2-SW0...	1.93.4.101/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/> 9300-S1-SW01	172.25.2.1/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/> 9300-S2-SW01	172.25.1.1/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/> 9300-S2-SW02	172.25.1.2/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/> 9500-CRE-S...	1.95.1.101/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/> 9500-DIS-SW...	1.95.2.101/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/> BLUE-3850	20.85.85.85/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/> Dis-9500	10.6.4.52/32	Cisco	All Locations	All Device Types	

Enter the IP address, RADIUS shared secret, and Model of the switch

Overview ▸ Identities Identity Groups **Network Devices** Ext Id Sources ▸ Client Provisioning ▸ Portals & C

[Network Devices List](#) > [New Network Device](#)

Network Devices

* Name

Description

IP Address ▾ * IP : /

● IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

☒ **RADIUS Authentication Settings**

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required ☐

Shared Secret

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.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The left sidebar shows the navigation tree with categories like Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. Under Policy Elements, the 'Dictionaries' tab is selected, showing a list of dictionaries including Network Condition, NMAP, NMAPExtension, Normalised Radius, PassiveID, Posture, PROFILER, and Radius. The 'Radius' folder is expanded, showing a list of vendors including IETF, RADIUS Vendors, Airespace, Alcatel-Lucent, Aruba, Aruba_Wired, Brocade, Cisco, Cisco-BBSM, Cisco-VPN3000, H3C, HP, Juniper, and Microsoft. The 'HP' dictionary is selected, and the configuration page is displayed. The configuration page has two tabs: 'Dictionary' and 'Dictionary Attributes'. The 'Dictionary' tab is active, showing the following fields:

- * Dictionary Name: HP
- Description: Dictionary for Vendor HP
- * Vendor ID: 11
- Vendor Attribute Type Field Length: 1
- Vendor Attribute Size Field Length: 1

 At the bottom of the configuration page are 'Save' and 'Reset' buttons.

2. Click Dictionary Attributes then click add

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities Id Groups Ext Id Sources Network Resources Policy Elements Policy Sets Troubleshoot Reports Settings **Dictionaries**

Dictionaries

Network Condition

NMAP

NMAPEExtension

Normalised Radius

PassiveID

Posture

PROFILER

Radius

IETF

RADIUS Vendors

Airspace

Alcatel-Lucent

Aruba

Aruba_Wired

Brocade

Cisco

Cisco-BBSM

Cisco-VPN3000

H3C

HP

Juniper

Microsoft

Motorola-Symbol

Ruckus

WISPr

Session

SNMP

SXP

TACACS

TC-NAC

Threat

TrustSec

User

Dictionaries > ... > RADIUS Vendors > HP

Dictionary Dictionary Attributes

Dictionary Attributes

+ Add Edit Delete

<input type="checkbox"/>	Name	Number	Type	Direction	Description	Predefined
<input type="checkbox"/>	HP-Bandwidth-Max-Egr...	48	UINT32	BOTH	Attribute HP-Bandwidth-Max-Egr...	NO
<input type="checkbox"/>	HP-Bandwidth-Max-Ingr...	46	UINT32	BOTH	Attribute HP-Bandwidth-Max-Ingr...	NO
<input type="checkbox"/>	HP-Capability-Advert	255	OCTET_STRING	BOTH	Attribute HP-Capability-Advert	NO
<input type="checkbox"/>	HP-Command-Exception	3	UINT32	BOTH	Attribute HP-Command-Exception	NO
<input type="checkbox"/>	HP-Command-String	2	STRING	BOTH	Attribute HP-Command-String	NO
<input type="checkbox"/>	HP-Cos	40	STRING	BOTH	Attribute HP-Cos	NO
<input type="checkbox"/>	HP-Egress-VLAN-Name	65	STRING	BOTH	Attribute HP-Egress-VLAN-Name	NO
<input type="checkbox"/>	HP-Egress-VLANID	64	UINT32	BOTH	Attribute HP-Egress-VLANID	NO
<input type="checkbox"/>	HP-Management-Proto...	26	UINT32	BOTH	Attribute HP-Management-Protocol	NO
<input type="checkbox"/>	HP-Nas-Filter-Rule	61	STRING	BOTH	Attribute HP-Nas-Filter-Rule	NO
<input type="checkbox"/>	HP-Nas-Rules-IPv6	63	UINT32	BOTH	Attribute HP-Nas-Rules-IPv6	NO
<input type="checkbox"/>	HP-Port-Auth-Mode-Dot...	13	UINT32	BOTH	Attribute HP-Port-Auth-Mode-Dot1x	NO
<input type="checkbox"/>	HP-Port-Client-Limit-Do...	10	UINT32	BOTH	Attribute HP-Port-Client-Limit-Dot...	NO
<input type="checkbox"/>	HP-Port-Client-Limit-MA	11	UINT32	BOTH	Attribute HP-Port-Client-Limit-MA	NO
<input type="checkbox"/>	HP-Port-Client-Limit-WA	12	UINT32	BOTH	Attribute HP-Port-Client-Limit-WA	NO
<input type="checkbox"/>	HP-Privilege-Level	1	UINT32	BOTH	Attribute HP-Privilege-Level	NO
<input checked="" type="checkbox"/>	HPE-Port-MA-Port-Mode	14	UINT32	BOTH	words	NO

- After clicking add dictionary attribute enter the information below then click Submit.

Attribute name: "HP-User-Role"

Data type: "String"

Direction: "Both"

ID: "25"

The screenshot shows the Aruba configuration interface. The top navigation bar includes links for Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, and PassiveID. Below this is a secondary navigation bar with links for Overview, Identities, Id Groups, Ext Id Sources, Network Resources, Policy Elements, Policy Sets, Troubleshoot, Reports, Settings, and Dictionaries. The 'Dictionaries' section is active, and the breadcrumb trail shows 'Dictionaries > ... > RADIUS Vendors > HP'. The 'Dictionary Attributes' tab is selected. On the left, a tree view shows the hierarchy of dictionaries, with 'HP' selected under 'RADIUS Vendors'. The main form contains the following fields:

- * Attribute Name: HP-User-Role
- Description: (empty text box)
- * Data Type: STRING (dropdown menu)
- Enable MAC option: ☐
- * Direction: BOTH (dropdown menu)
- * ID: 25 (text box) (0-255)
- Allow Tagging: ☐
- Allow multiple instances of this attribute in a profile: ☐

At the bottom of the form are 'Submit' and 'Cancel' buttons.

4. The “HP-User-Role” should now appear.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Dictionary Attributes

Dictionary Attributes

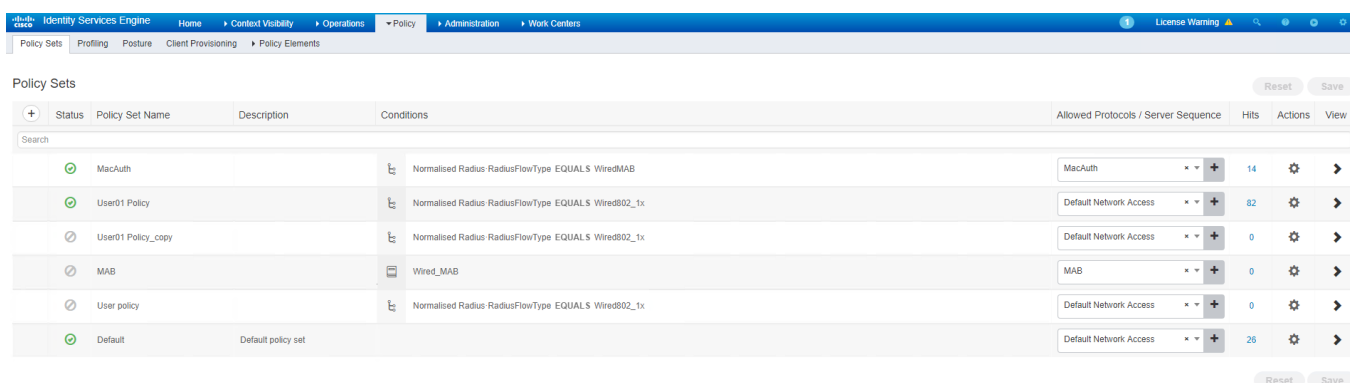
Name	Number	Type	Direction	Description	Predefined
HP-Bandwidth-Max-Egr...	48	UINT32	BOTH	Attribute HP-Bandwidth-Max-Egr...	NO
HP-Bandwidth-Max-Ingr...	46	UINT32	BOTH	Attribute HP-Bandwidth-Max-Ingr...	NO
HP-Capability-Advert	255	OCTET_STRING	BOTH	Attribute HP-Capability-Advert	NO
HP-Command-Exception	3	UINT32	BOTH	Attribute HP-Command-Exception	NO
HP-Command-String	2	STRING	BOTH	Attribute HP-Command-String	NO
HP-Cos	40	STRING	BOTH	Attribute HP-Cos	NO
HP-Egress-VLAN-Name	65	STRING	BOTH	Attribute HP-Egress-VLAN-Name	NO
HP-Egress-VLANID	64	UINT32	BOTH	Attribute HP-Egress-VLANID	NO
HP-Management-Proto...	26	UINT32	BOTH	Attribute HP-Management-Protocol	NO
HP-Nas-Filter-Rule	61	STRING	BOTH	Attribute HP-Nas-Filter-Rule	NO
HP-Nas-Rules-IPv6	63	UINT32	BOTH	Attribute HP-Nas-Rules-IPv6	NO
HP-Port-Auth-Mode-Dot...	13	UINT32	BOTH	Attribute HP-Port-Auth-Mode-Dot1x	NO
HP-Port-Client-Limit-Do...	10	UINT32	BOTH	Attribute HP-Port-Client-Limit-Dot...	NO
HP-Port-Client-Limit-MA	11	UINT32	BOTH	Attribute HP-Port-Client-Limit-MA	NO
HP-Port-Client-Limit-WA	12	UINT32	BOTH	Attribute HP-Port-Client-Limit-WA	NO
HP-Privilege-Level	1	UINT32	BOTH	Attribute HP-Privilege-Level	NO
HP-User-Role	25	STRING	BOTH		NO
HPE-Port-MA-Port-Mode	14	UINT32	BOTH	words	NO

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.

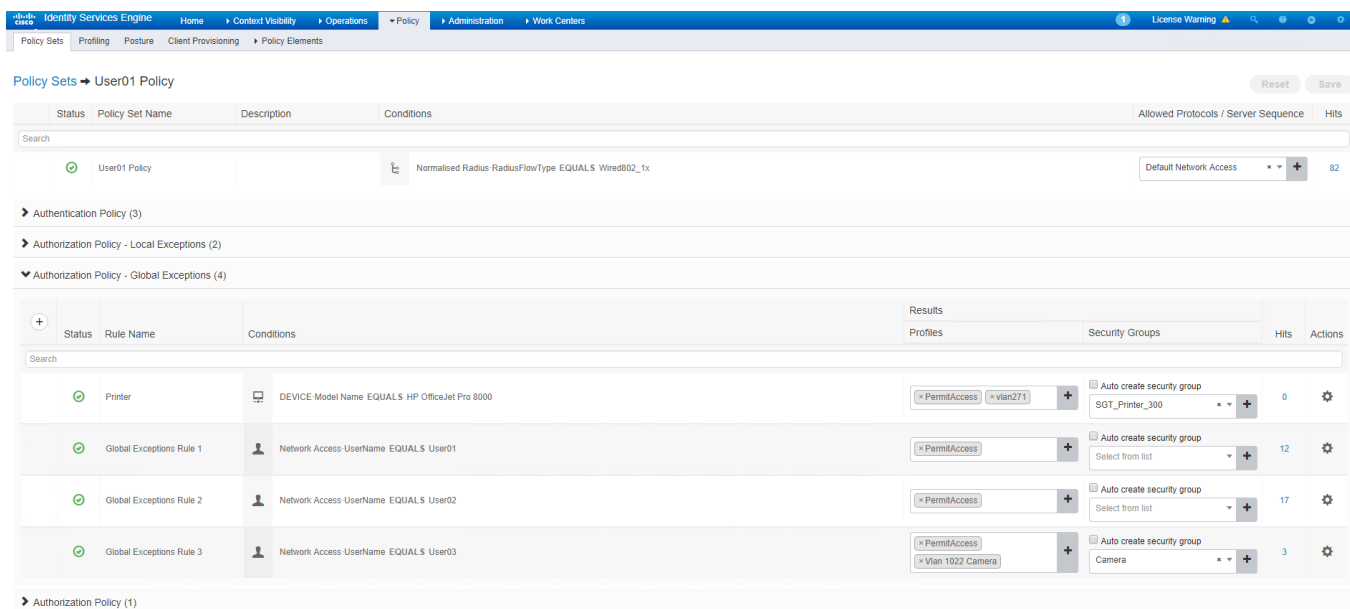
1. Now that the HP-User-Role VSA is defined in ISE, it can now be used. Navigate to Policy > Policy Sets and edit a policy for your environment. In this case we will use “User01 Policy”.



The screenshot shows the 'Policy Sets' page in the ISE GUI. The table lists several policy sets, including MacAuth, User01 Policy, User01 Policy_copy, MAB, User policy, and Default. The 'User01 Policy' is highlighted, showing its conditions as 'Normalised Radius RadiusFlowType EQUALS Wired802_1x' and its allowed protocols as 'Default Network Access' with 82 hits.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	MacAuth		Normalised Radius RadiusFlowType EQUALS WiredMAB	MacAuth	14	⚙️	➔
✓	User01 Policy		Normalised Radius RadiusFlowType EQUALS Wired802_1x	Default Network Access	82	⚙️	➔
⚙️	User01 Policy_copy		Normalised Radius RadiusFlowType EQUALS Wired802_1x	Default Network Access	0	⚙️	➔
⚙️	MAB		Wired_MAB	MAB	0	⚙️	➔
⚙️	User policy		Normalised Radius RadiusFlowType EQUALS Wired802_1x	Default Network Access	0	⚙️	➔
✓	Default	Default policy set		Default Network Access	26	⚙️	➔

2. Under the “Policy Set” edit the “Authorization Policy”. Click the “+” symbol under profiles



The screenshot shows the 'Authorization Policy' configuration page for 'User01 Policy'. It displays a list of rules, including 'Printer', 'Global Exceptions Rule 1', 'Global Exceptions Rule 2', and 'Global Exceptions Rule 3'. The 'Printer' rule is highlighted, showing its conditions as 'DEVICE-Model Name EQUALS HP OfficeJet Pro 8000' and its results as 'PermitAccess' and 'vlan271'.

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
✓	Printer	DEVICE-Model Name EQUALS HP OfficeJet Pro 8000	PermitAccess, vlan271	Auto create security group SOT_Printer_300	0	⚙️
✓	Global Exceptions Rule 1	Network Access-UserName EQUALS User01	PermitAccess	Auto create security group Select from list	12	⚙️
✓	Global Exceptions Rule 2	Network Access-UserName EQUALS User02	PermitAccess	Auto create security group Select from list	17	⚙️
✓	Global Exceptions Rule 3	Network Access-UserName EQUALS User03	PermitAccess, Vlan 1022 Camera	Auto create security group Camera	3	⚙️

5. The final result should look similar to the image below. Devices are now ready to be authenticated.

Policy Sets → User01 Policy

Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	User01 Policy		Normalised Radius RadiusFlowType EQUALS Wired802_tx	Default Network Access	82

Authentication Policy (3)

Authorization Policy - Local Exceptions (2)

Authorization Policy - Global Exceptions (4)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Printer	DEVICE Model Name EQUALS HP OfficeJet Pro 8000	*PermitAccess *vlan271	Auto create security group SOT_Printer_300	0	
✓	Global Exceptions Rule 1	Network Access UserName EQUALS User01	*ISE-LOCAL *PermitAccess	Auto create security group Select from list	12	
✓	Global Exceptions Rule 2	Network Access UserName EQUALS User02	*ISE-LOCAL *PermitAccess	Auto create security group Select from list	17	
✓	Global Exceptions Rule 3	Network Access UserName EQUALS User03	*PermitAccess *Vlan 1022 Camera	Auto create security group Camera	3	

VERIFICATION

The switch should show the devices authenticated with the proper local role.

```
172.16.8.5 - PuTTYNG
name "VLAN1001"
ip address 10.111.100.1 255.255.255.0
exit
spanning-tree Trk1 priority 4

Aruba-3810M-48G-PoEP-1-slot(eth-15-16)#
Aruba-3810M-48G-PoEP-1-slot(eth-15-16)# show port acc
Ambiguous input: port
Aruba-3810M-48G-PoEP-1-slot(eth-15-16)# show port acces
Ambiguous input: port
Aruba-3810M-48G-PoEP-1-slot(eth-15-16)# show port-access clients
Downloaded user roles are preceded by *

Port Access Client Status

Port  Client Name  MAC Address      IP Address      User Role      Type
-----
VLAN
-----
15    user01        a0cec8-02a948    n/a             ISE-LOCAL      8021X
101
16    user02        0050b6-79bdac    n/a             ISE-LOCAL      8021X
101

Aruba-3810M-48G-PoEP-1-slot(eth-15-16)#
```

ISE will show that the User Role Was applied to the switch

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers 1 License Warning

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Live Logs Live Sessions

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

Refresh Every 30 seconds Show Latest 50 records W

Refresh Reset Repeat Counts Export To

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
Jul 24, 2018 06:17:53.087 PM			0	user01	A0:CE:C8:02:A9:48	Microsoft-Workstation	User01 Policy >> Catch All	User01 Policy >> Global Exceptions Rule 1	ISE-LOCAL,PermitAccess
Jul 24, 2018 06:17:53.087 PM			0	user01	A0:CE:C8:02:A9:48	Microsoft-Workstation	User01 Policy >> Catch All	User01 Policy >> Global Exceptions Rule 1	ISE-LOCAL,PermitAccess
Jul 24, 2018 06:17:52.182 PM			0	user02	00:50:B6:79:BD:AC	Unknown	User01 Policy >> Catch All	User01 Policy >> Global Exceptions Rule 2	ISE-LOCAL,PermitAccess
Jul 24, 2018 06:17:52.182 PM			0	user02	00:50:B6:79:BD:AC	Unknown	User01 Policy >> Catch All	User01 Policy >> Global Exceptions Rule 2	ISE-LOCAL,PermitAccess

The result should also show the name of the “Local User Role” at the bottom.

Cisco Identity Services Engine	
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384
TLSType	TLSv1.2
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:Profiled:Workstation
Model Name	2930M
Software Version	16.05
Network Device Profile	HPWired
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
RADIUS Username	user01
NAS-Identifier	Aruba-3810M-48G-PoEP-1-slot
Device IP Address	10.128.1.6
Called-Station-ID	70:10:6F:8F:24:00

Result	
State	ReauthSession:0a06041eHDbm8k/qZT/79k5vh1qaB5jx3T1mzg7bZDfxVkhizls
Class	CACS:0a06041eHDbm8k/qZT/79k5vh1qaB5jx3T1mzg7bZDfxVkhizls:ISE220M4/319414502/238571
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Base license consumed
HP-User-Role	ISE-LOCAL