Juniper with Cisco Identity Services Engine 2.X / Multi-Auth Configuration with Phone and PC using Dynamic VLAN assignment

Chad Mitchell CCIE#44090 - chadmi@cisco.com May 8, 2018

Testing Network Access Device Info

****

```
root@JUNIPER-EX4200-48T> show version
fpc0:
--------------------------------------------------------------------------
Hostname: JUNIPER-EX4200-48T
Model: ex4200-48t
Junos: 15.1R6.7
JUNOS EX  Software Suite [15.1R6.7]
JUNOS FIPS mode utilities [15.1R6.7]
JUNOS Online Documentation [15.1R6.7]
JUNOS EX 4200 Software Suite [15.1R6.7]
JUNOS Web Management Platform Package [15.1R6.7]

{master:0}
root@JUNIPER-EX4200-48T>
```

Network Access Device Configuration

****

With Juniper switches the standard allows us to specify either a VLAN name or number for assignment. In this testing, the name specified in the “set vlans” command will be sent via ISE for the dynamic assignment of the Voice and Data VLANs. VLAN numbers can be used as well but leveraging a standardized naming structure across all switches and VLANs can simplify ISE configuration.

The default MAB protocol used on this device and version was EAP-MD5. The device also does support PAP but must be manually specified by using the “pap” operator in the “mac-radius authentication-protocol” command below if desired. Specifying PAP will make the MAB request look similar to a Cisco device MAB so you must ensure that the Juniper device is specified as such using the Network Device Profile and adding that as a condition to the Policy Set decision process.

802.1X on this device and version does not send a RADIUS Service-Type therefore the only matching we can do to differentiate 802.1X from MAB is to look at the Authentication Protocol as shown in the Authentication policy below.

Juniper Device Configuration

ISE Relevant Configuration only

```
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members INTERNAL
set ethernet-switching-options voip interface ge-0/0/0.0 vlan VOICE
!
set protocols dot1x authenticator authentication-profile-name 8021x-auth
set protocols dot1x authenticator interface ge-0/0/0.0 supplicant multiple
set protocols dot1x authenticator interface ge-0/0/0.0 retries 3
set protocols dot1x authenticator interface ge-0/0/0.0 quiet-period 300
set protocols dot1x authenticator interface ge-0/0/0.0 transmit-period 5
set protocols dot1x authenticator interface ge-0/0/0.0 mac-radius authentication-protocol eap-md5
set protocols dot1x authenticator interface ge-0/0/0.0 reauthentication 3600
set protocols dot1x authenticator interface ge-0/0/0.0 server-timeout 5
set protocols dot1x authenticator interface ge-0/0/0.0 maximum-requests 3
set protocols dot1x authenticator interface ge-0/0/0.0 server-reject-vlan INTERNAL
set protocols dot1x authenticator interface ge-0/0/0.0 server-fail permit
set protocols dot1x authenticator interface ge-0/0/0.0 server-fail-voip vlan-name VOICE
!
set access radius-server 10.99.10.15 port 1812
set access radius-server 10.99.10.15 dynamic-request-port 3799
set access radius-server 10.99.10.15 secret "$9$IaocSeN-wgaUylwgoaUD9AtOEc"
set access radius-server 10.99.10.15 timeout 5
set access radius-server 10.99.10.15 retry 3
set access radius-server 10.99.10.15 source-address 10.99.254.14
!
set access profile 8021x-auth authentication-order radius
set access profile 8021x-auth radius authentication-server 10.99.10.15
set access profile 8021x-auth radius accounting-server 10.99.10.15
set access profile 8021x-auth accounting order radius
!
set vlans INTERNAL vlan-id 252
set vlans VOICE vlan-id 3
```

****

****

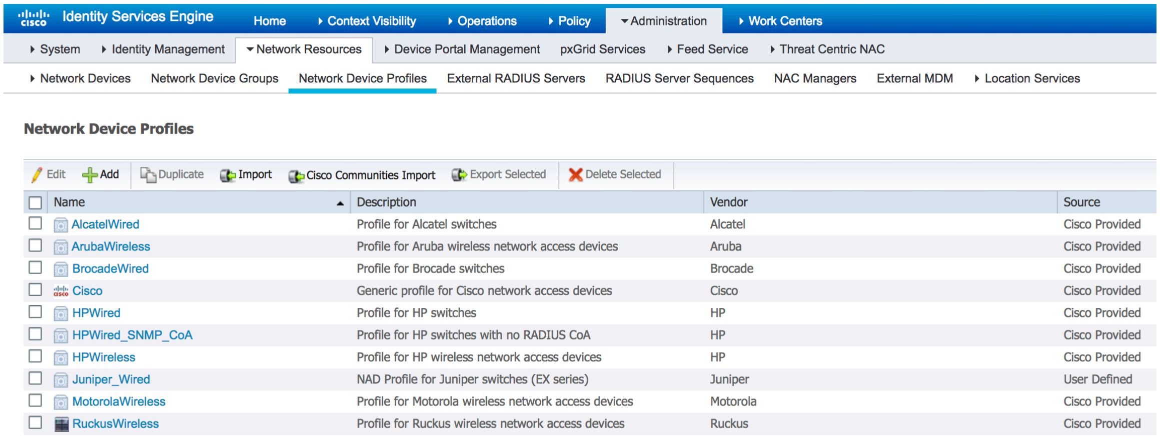
ISE Configuration

Network Device Profile Configuration

Cisco ISE 2.X comes with many pre-imported Network Device Profiles on the system. The Juniper Network Device Profile is not one of those that at this time. Cisco ISE allows the import of profiles in XML format to enable integration with any 802.1X network device. Juniper switching devices have been tested with Cisco ISE by the BU and the Network Device Profile is provided at the link below.

https://communities.cisco.com/docs/DOC-64547

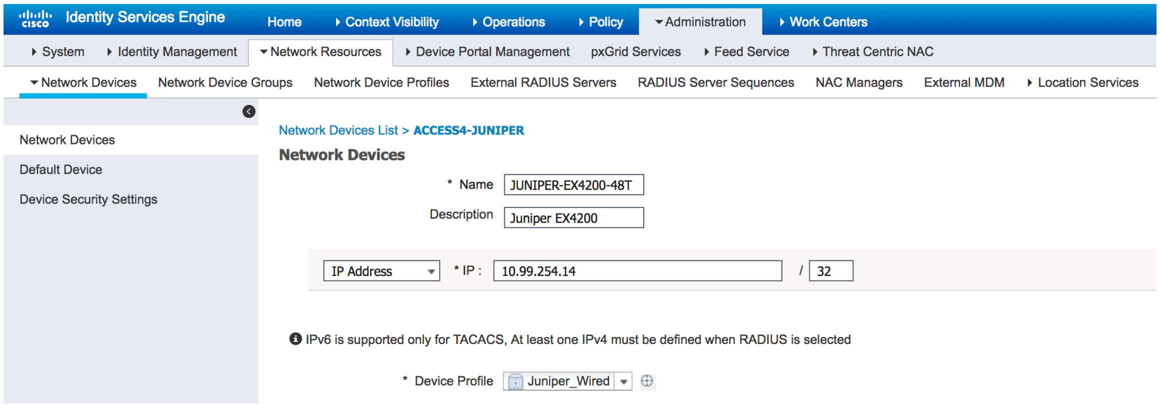
To import the Network Device Profile in ISE you must navigate to Administration > Network Resources > Network Device Profiles and click "Import" at the top of the table. You will also see the "Cisco Communities Import" button which will direct you to the link above. Once imported you should see the "Juniper_Wired" profile listed as shown.



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
□	Juniper_Wired	NAD Profile for Juniper switches (EX series)	Juniper	User Defined
□	MotorolaWireless	Profile for Motorola wireless network access devices	Motorola	Cisco Provided
□	RuckusWireless	Profile for Ruckus wireless network access devices	Ruckus	Cisco Provided

Now that the Network Device Profile is imported we can add the switch to the Network Device database and specify it as a Juniper_Wired device. Navigate to Administration > Network Resources > Network Devices and add a new device as shown. Note the "Device Profile" selected at the bottom of the capture.



Network Devices List > ACCESS4-JUNIPER

Network Devices

* Name: JUNIPER-EX4200-48T

Description: Juniper EX4200

IP Address * IP : 10.99.254.14 / 32

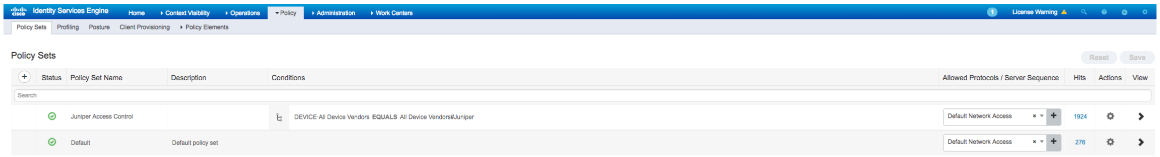
IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected

* Device Profile: Juniper_Wired

The device is now added to the database correctly as a Juniper device and we can now setup the policy for AAA functions for this device.

Policy Set Configuration

Navigate to Policy > Policy Sets and click the plus sign in the top left corner to create a new Policy Set. For the Policy Set configuration I recommend using a dedicated Policy Set specific to Juniper NAD RADIUS connections. This can easily be done by creating a new Policy Set and using the Device Vendor group as the condition to use the Policy Set as shown below.

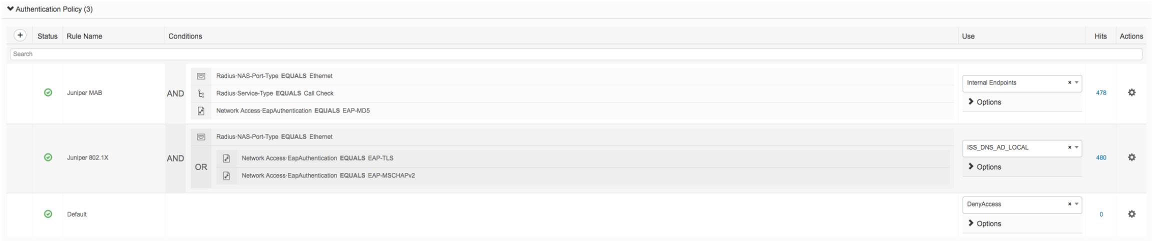


Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Juniper Access Control		DEVICE·All Device Vendors **EQUALS** All Device Vendors#Juniper	Default Network Access	1924	⚙	›
✓	Default	Default policy set		Default Network Access	276	⚙	›

Authentication Policy

Next is to setup the Authentication Policy under the newly created Policy Set. In this example we will only use two rules with the default being a DenyAccess result. The Network Device Profile that was imported earlier does allow the default Wired_MAB and Wired_802.1X conditions to be used to specify the difference in authentication, however in this example I wanted to be more absolute and defined on what is matching for 802.1X and MAB. The Juniper MAB policy is matching NAS Port Type as Ethernet and Service Type as Call Check. It is also requiring that the MAB Authentication EAP type is EAP-MD5 which we discussed earlier. This rule is pointing to Internal Endpoints. The Juniper 802.1X policy is only looking for NAS Port Type from RADIUS however I am also specifying that the EAP Authentication protocol must be either EAP-TLS OR EAP-MSCHAPv2 and referencing the Identity Source Sequence that has a Certificate Authentication Profile as for DNS name extraction from the certificate and/or Active Directory authentication.



Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Juniper MAB	AND Radius·NAS-Port-Type **EQUALS** Ethernet Radius·Service-Type **EQUALS** Call Check Network Access·EapAuthentication **EQUALS** EAP-MD5	Internal Endpoints	478	⚙
✓	Juniper 802.1X	AND Radius·NAS-Port-Type **EQUALS** Ethernet OR Network Access·EapAuthentication **EQUALS** EAP-TLS Network Access·EapAuthentication **EQUALS** EAP-MSCHAPv2	ISS_DNS_AD_LOCAL	480	⚙
✓	Default		DenyAccess	0	⚙

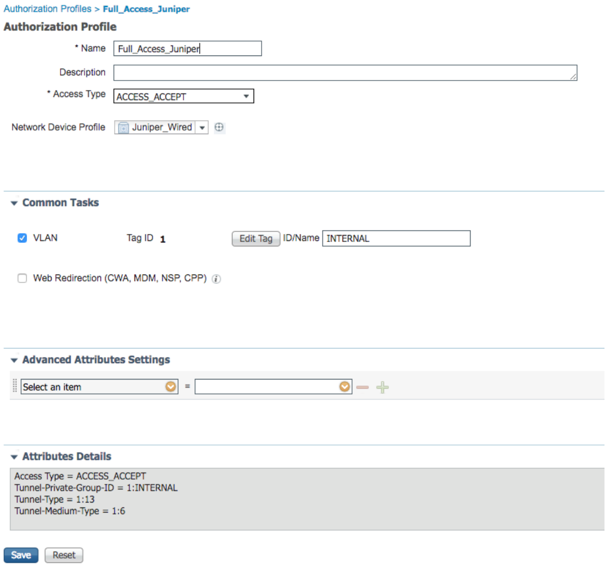
Save the Policy Set Configuration at this time.

Authorization Profiles

Before we configure the Authorization Policy we must setup the Authorization Profiles that we will assign based on successful AuthC and AuthZ. Navigate to Policy > Policy Elements > Results > Authorization > Authorization Profiles and click Add to create a new Profile.

First we will create the Full Access profile for successful 802.1X authenticated PCs. This profile will send an ACCESS_ACCEPT as well as the desired VLAN name in this example. See example below.

> *Note: The Network Device Profile of Juniper_Wired OR Any must be selected to properly send to a Juniper_Wired designated NAD.*



Authorization Profiles > Full_Access_Juniper

Authorization Profile

* Name: Full_Access_Juniper

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Juniper_Wired

Common Tasks

☑ VLAN   Tag ID 1   Edit Tag   ID/Name: INTERNAL

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

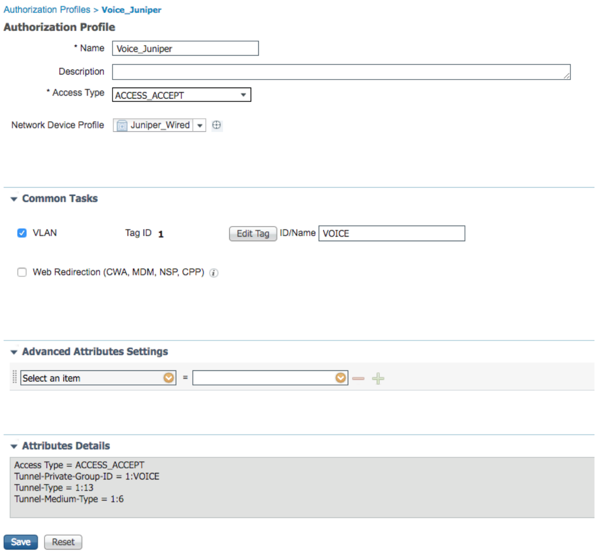
Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:INTERNAL
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
```

Repeat for Voice MAB devices and all other AuthZ Profiles you may need in your environment.



Authorization Profiles > Voice_Juniper

Authorization Profile

* Name: Voice_Juniper

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Juniper_Wired

Common Tasks

☑ VLAN   Tag ID 1   Edit Tag   ID/Name: VOICE

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

Advanced Attributes Settings

Select an item =

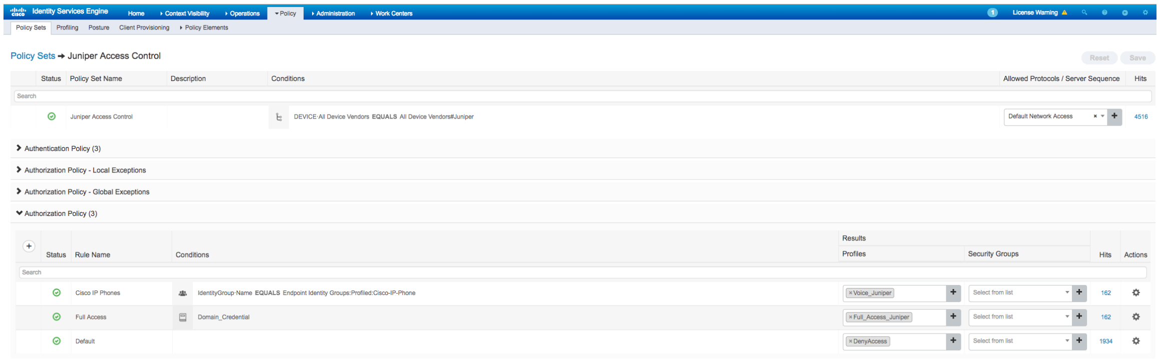
Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:VOICE
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
```

Authorization Policy

Now that the AuthC Policy and AuthZ Profiles are built we can complete the ISE configuration with the Authorization Policy. Navigate to the Policy Set that you created earlier and expand the Authorization Policy section.

We will have a simple policy here in the example. One rule for profiled Cisco IP Phones and another for authenticated domain machine/user credentials. Each of these will be accompanied with the Authorization Profile we just built. See the example below.



Policy Sets → Juniper Access Control

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Juniper Access Control		DEVICE·All Device Vendors **EQUALS** All Device Vendors#Juniper	Default Network Access	4516

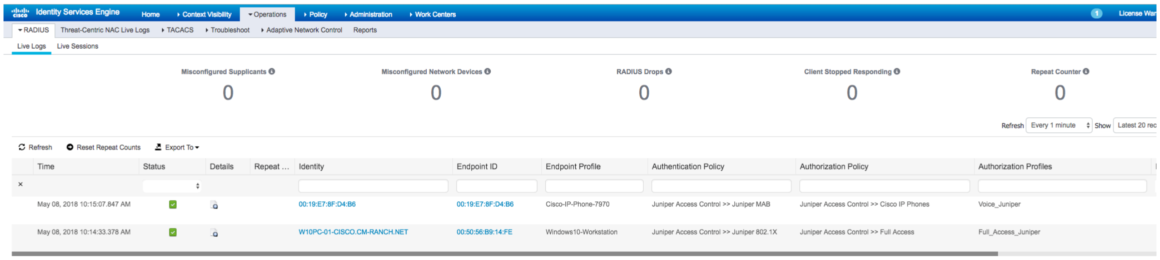
- Authentication Policy (3)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (3)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
✓	Cisco IP Phones	IdentityGroup·Name **EQUALS** Endpoint Identity Groups:Profiled:Cisco-IP-Phone	Voice_Juniper	Select from list	162	⚙
✓	Full Access	Domain_Credential	Full_Access_Juniper	Select from list	162	⚙
✓	Default		DenyAccess	Select from list	1934	⚙

Now we can connect the devices and verify successful authentication to the network.

Verification

To verify we will look first at the live logs on ISE and will see that the phone and PC have authenticated successfully and ISE has applied the correct AuthZ profiles.



Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 0

Refresh Every 1 minute

Show Latest 20 rec

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
May 08, 2018 10:15:07.847 AM	✓			00:19:E7:8F:D4:B6	00:19:E7:8F:D4:B6	Cisco-IP-Phone-7970	Juniper Access Control >> Juniper MAB	Juniper Access Control >> Cisco IP Phones	Voice_Juniper
May 08, 2018 10:14:33.378 AM	✓			W10PC-01-CISCO.CM-RANCH.NET	00:50:56:B9:14:FE	Windows10-Workstation	Juniper Access Control >> Juniper 802.1X	Juniper Access Control >> Full Access	Full_Access_Juniper

Second on the switch we can run the “show dot1x interface ge0/0/0.0 detail” command and see that the phone session has the VOICE VLAN assigned and the PC has the INTERNAL VLAN assigned as we configured it.

```
root@JUNIPER-EX4200-48T> show dot1x interface ge-0/0/0.0 detail
ge-0/0/0.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 300 seconds
  Transmit period: 5 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Mac Radius Authentication Protocol: EAP-MD5
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 5 seconds
  Maximum EAPOL requests: 3
  Guest VLAN member: not configured
  Number of connected supplicants: 2
    Supplicant: 0019e78fd4b6, 00:19:E7:8F:D4:B6
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Mac Radius
      Authenticated VLAN: VOICE
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3538 seconds
    Supplicant: host/W10PC-01-CISCO.CM-RANCH.NET, 00:50:56:B9:14:FE
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Radius
      Authenticated VLAN: INTERNAL
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3503 seconds

{master:0}
root@JUNIPER-EX4200-48T>
```