

# Interfacing with Cisco ISE

ENG-010562

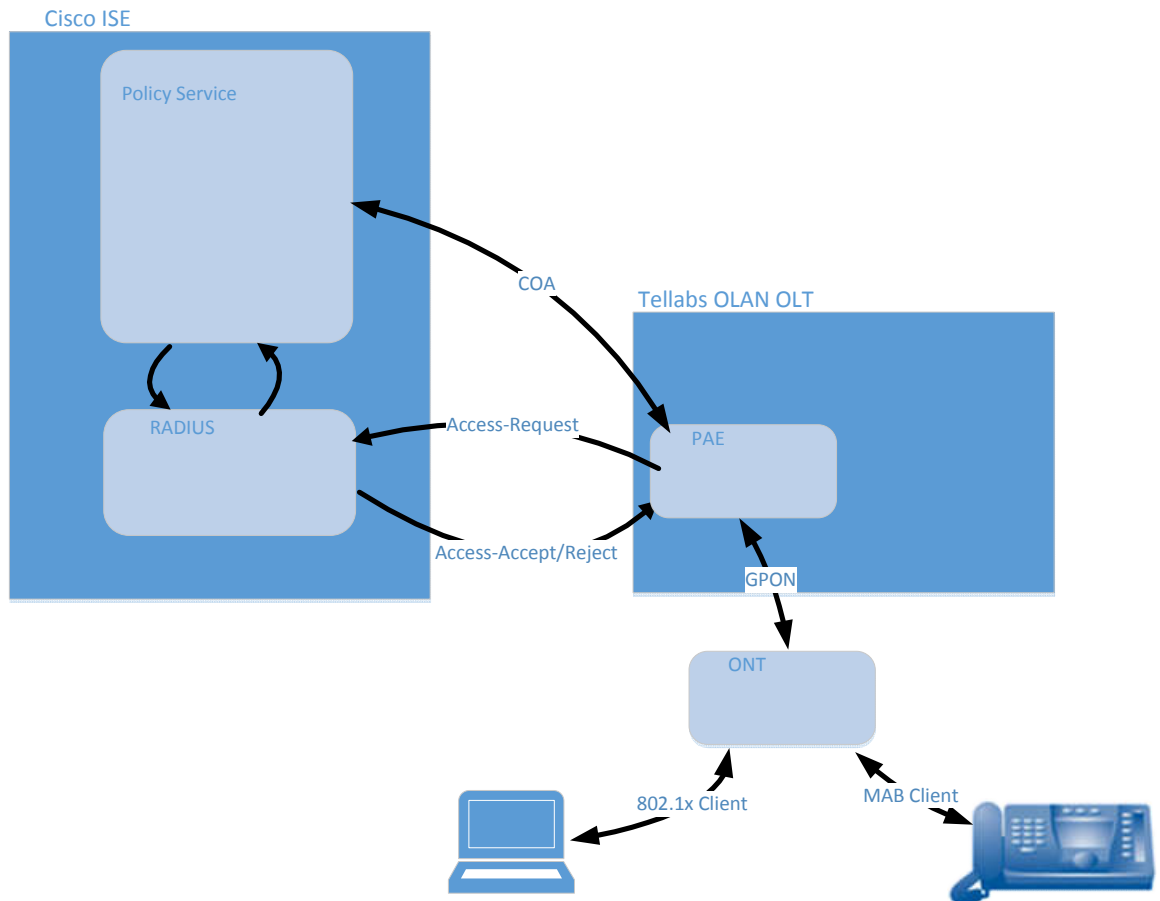
## Introduction

Cisco ISE is a software package providing policy management to control network access. The purpose of this document is to explain how to configure and administer the Tellabs OLAN system to interface with Cisco ISE.

## Applies To

This document applies to all Tellabs OLAN systems running OLT SR29.2 and EMS SR30.0 or above. Earlier releases do not fully support Cisco ISE and are limited to simple access via 802.1x.

## Enforcing Policy on OLAN using Cisco ISE



Cisco ISE, or Identity Services Engine is an application that is able to characterize systems that are discovered on the network and apply policies based on rule sets. This allows more consistent application

of policy across the network. It also allows application of policy based on the user login or device type which allows for dynamic configuration and allocation of resources in real time.

The Tellabs OLAN system has added support for integration with Cisco ISE in the SR29.2 and above releases. OLT Releases prior to SR29.2 can be used, but only for simple 802.1x and granting of access to the network. Also since OLT SR29.2 added support for MAB authentication for phones and 802.1x authentication for PCs on the same port, it is typically best to have OLT SR29.2 or above.

The OLAN PAE or Port Authentication Entity interfaces with Cisco ISE for two different protocols:

- **RADIUS** – Remote Authentication Dial In User Service. This interface allows a switch to transparently forward credentials from a user to the RADIUS server for authentication. The RADIUS Server will either grant access via an Access Accept or Access Reject. Radius also supports a mechanism to pass back the name of the policy to apply to the port via the FILTER-ID attribute.
- **COA** – Change of Authorization is an extension to the RADIUS protocol to allow additional updates to a port. RADIUS suffers from only being triggered by authentication requests and cannot send updates in real time to the port. COA allows updates of the port in real time.

COA which is in SR29.2 and above supports the following messages for additional control:

- **Session Re-authentication** – Force re-authentication of a port.
- **Session Termination** – Allows terminating a user immediately from the network. RADIUS only can terminate a user when it attempts to re-authenticate after the re-authentication timeout.
- **Session Termination with Port Shutdown** – Terminate a session and shut off the port afterwards. This prevents further access after the session is terminated from that port. Admin is required to manually admin the port up before it can be used again. This can be used in highly secure areas to prevent further attempts to access the port.
- **Session Termination with Port Bounce** – Terminate the session and disable/re-enable the port to restart authentication and restart with a new session.
- **Session Policy Push** – COA can push a new policy to a port at any time using the Session Policy Push. This allows changes to take effect immediately rather than waiting for the next re-authentication attempt from the Port.
- **Session Re-authentication with rerun** – Force Re-authentication with the configured authentication method from the beginning. This is not supported by Tellabs in the current release.
- **Session Re-authentication with last** – Force Re-authentication using the last successful method of authentication. This is not supported by the Tellabs system in the current release.

Additional general information on RADIUS authentication, support and configuration can be found in the AppNote ENG-010428 Configuring Policy Via RADIUS Authentication. This document explains the basic operation of RADIUS and how to use RADIUS to distribute policy via the RADIUS FILTER-ID attribute.

The following table outlines the Tellabs OLAN product support for Cisco ISE Features:

	Tellabs
Session Termination	✓
Session Termination with port bounce	✓
Session Termination with port shutdown	✓
Session re-authentication	✓
Session re-authentication with rerun	-
Session re-authentication with last	-
Session Policy Push CoA	✓
URL Redirect (Dynamic)	✓
802.1x/MAB	✓
Profiler without CoA	✓
Profiler with CoA	✓
Posture	✓
Guest/BYOD	✓

### Cisco ISE Configuration for Tellabs OLAN

Cisco ISE documentation should always be consulted first to get the latest up to date information about configuration of ISE features. This example configuration shows one example of how to configure ISE to interoperate with Tellabs OLAN. This section only details configuration of components that are unique to Tellabs OLAN. It does not cover full configuration of Cisco ISE and Cisco manuals and documentation should be consulted for Cisco ISE configuration.

### Load Tellabs RADIUS Dictionaries

In later versions of Cisco ISE, the Tellabs Dictionary will be included with the ISE install. If your Cisco ISE instance does not include the Tellabs RADIUS Dictionary will need to be loaded. You can determine if the Tellabs Dictionary is loaded by looking at:

Policy->Policy Elements-> Dictionaries,

then expand the System Folder->Radius-> and double click on RADIUS Vendors, look for Tellabs

## RADIUS Vendors

<input type="checkbox"/>	Name	Vendor ID	Description
<input type="checkbox"/>	Airespace	14179	Dictionary for Vendor Airespace
<input type="checkbox"/>	Alcatel-Lucent	800	Dictionary for Vendor Alcatel-Lucent
<input type="checkbox"/>	Aruba	14823	Dictionary for Vendor Aruba
<input type="checkbox"/>	Brocade	1588	Dictionary for Vendor Brocade
<input type="checkbox"/>	Cisco	9	Dictionary for Vendor Cisco
<input type="checkbox"/>	Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM
<input type="checkbox"/>	Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000
<input type="checkbox"/>	H3C	25506	Dictionary for Vendor H3C
<input type="checkbox"/>	HP	11	Dictionary for Vendor HP
<input type="checkbox"/>	Juniper	2636	Dictionary for Vendor Juniper
<input type="checkbox"/>	Microsoft	311	Dictionary for Vendor Microsoft
<input type="checkbox"/>	Motorola-Symbol	388	Dictionary for Vendor Motorola-Symbol
<input type="checkbox"/>	Ruckus	25053	Dictionary for Vendor Ruckus
<input type="checkbox"/>	Tellabs	1397	Dictionary for Vendor Tellabs
<input type="checkbox"/>	WISPr	14122	Dictionary for Vendor WISPr

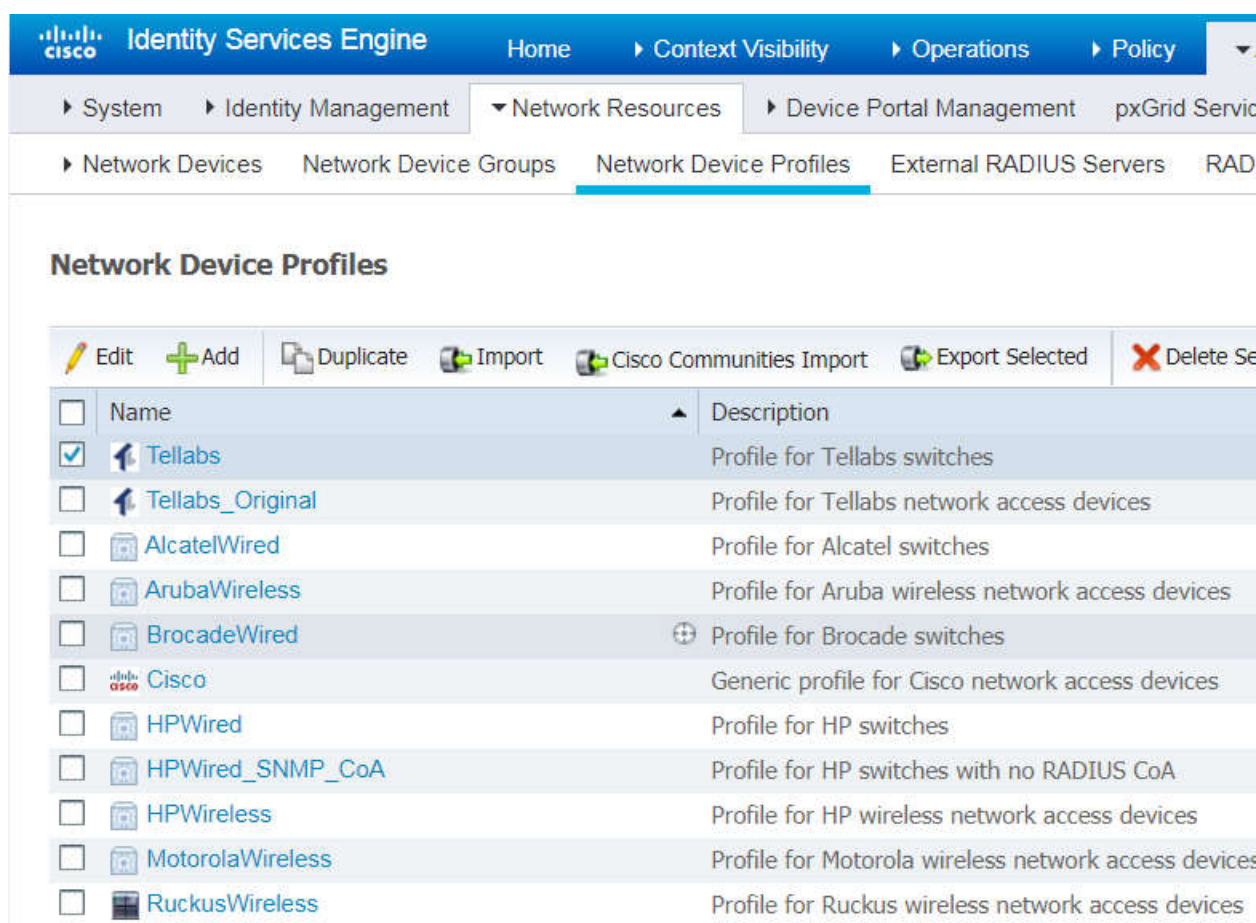
If the Tellabs entry is missing, then the Tellabs ISE Dictionary will need to be added. It can be downloaded from the Application notes section of the Tellabs Website.

Click on the Import button, choose the dictionary.tellabs file that was downloaded and add it to Cisco ISE. You should then see the Tellabs dictionary listed.

### Creation of Network Device Profile for Tellabs OLAN

ISE should first be configured to add a Network Device Profile for Tellabs. Tellabs OLAN is being added to the Cisco ISE and in future releases of ISE this step should not be necessary. Additionally, the Tellabs Application Notes site has a sample Tellabs Profile XML file that can be used to import.

The Tellabs Network Device File can be imported into Cisco ISE using the following procedure: Administration-> Network Resources -> Network Device Profiles -> Import using the file "Tellabs-ISE-Network-Device-Profile.xml" downloaded from the Application Notes site.



The screenshot displays the Cisco Identity Services Engine (ISE) interface, specifically the "Network Device Profiles" section. The navigation menu at the top includes "Home", "Context Visibility", "Operations", and "Policy". The main navigation bar shows "System", "Identity Management", "Network Resources", "Device Portal Management", and "pxGrid Services". The "Network Resources" menu is expanded, showing "Network Devices", "Network Device Groups", "Network Device Profiles", "External RADIUS Servers", and "RADIUS Servers".

### Network Device Profiles

Actions: Edit, Add, Duplicate, Import, Cisco Communities Import, Export Selected, Delete Selected

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

If you need to manually add the Network Device Profile, it can be added via: **Administration->Network Resources->Network Device Profiles** menu using the Add button.


[Network Device Profile List > Tellabs](#)

### Network Device Profile

* Name	<input type="text" value="Tellabs"/>
Description	<input type="text" value="Profile for Tellabs switches"/>
Icon	<input type="button" value="Change icon..."/> <input type="button" value="Set To Default"/> ⓘ
Vendor	<input type="text" value="Cisco"/>
<b>Supported Protocols</b>	
RADIUS	<input checked="" type="checkbox"/>
TACACS+	<input type="checkbox"/>
TrustSec	<input type="checkbox"/>
RADIUS Dictionaries	<input type="text" value="Cisco x Tellabs x"/>

Update the following fields in the Main section of the profile:

- **Name:** The profile should be named Tellabs.
- **Description:** Profile for Tellabs Devices
- **Icon:** Update with Tellabs icon.
- **Vendor:** Other
- **Supported Protocols:** RADIUS
- **RADIUS Dictionaries:** Add Cisco, and Add Tellabs

The Tellabs Icon  is included here for use in the profile definition:



Tellabs\_Icon.jpg

(Right Click, Packager Shell Object->Activate Contents, then save it or download this file from the Application Notes Section of the web site.)

Then update the following fields within the Templates Section:

▼ Authentication/Authorization

▼ Flow Type Conditions

Wired MAB detected if the following condition(s) are met :

Radius:NAS-Port-Type	=	Ethernet	-	+
Radius:Service-Type	=	Call Check	-	+

Wireless MAB detected if the following condition(s) are met :

Radius:NAS-Port-Type	=	Wireless - IEEE 802.11	-	+
Radius:Service-Type	=	Call Check	-	+

Wired 802.1x detected if the following condition(s) are met :

Radius:NAS-Port-Type	=	Ethernet	-	+
Radius:Service-Type	=	Framed	-	+

Wireless 802.1x detected if the following condition(s) are met :

Radius:NAS-Port-Type	=	Wireless - IEEE 802.11	-	+
Radius:Service-Type	=	Framed	-	+

Wired Web Authentication detected if the following condition(s) are met :

Radius:NAS-Port-Type	=	Ethernet	-	+
Radius:Service-Type	=	Login	-	+

Wireless Web Authentication detected if the following condition(s) are met :

Radius:NAS-Port-Type	=	Wireless - IEEE 802.11	-	+
Radius:Service-Type	=	Login	-	+

- Authentication / Authorization
  - Check Wired MAB detected if the following conditions are met:
    - **RADIUS: NAS-Port-Type** = Ethernet
    - **RADIUS: Service Type** = Call Check
  - Wireless MAB/802.1X is unchecked as the wireless devices handle MAB and OLAN only acts as transport not as the PAE.
  - Wired 802.1x detected if the following conditions are met
    - **RADIUS: NAS-Port-Type** = Ethernet
    - **RADIUS: Service-Type** = Framed
  - Wireless 802.1x is handled by the Wireless AP and is left unchecked.

- Wired Web Authentication is checked and the following attributes set:
  - **RADIUS: NAS-Port-Type** = Ethernet
  - **RADIUS: Service-Type** = Login
- Wireless Web is provided transparently and is not a portion of the Tellabs Device Profile and would be addressed by the Device Profile of the wireless devices.

- Host Lookup (MAB)

- ▼ **Attribute Aliasing**

- SSID

- ▼ **Host Lookup (MAB)**

- Process Host Lookup
      - Via PAP/ASCII
        - Check Password
        - Check Calling-Station-Id equals MAC Address
      - Via CHAP
        - Check Password
        - Check Calling-Station-Id equals MAC Address
      - Via EAP-MD5
        - Check Password
        - Check Calling-Station-Id equals MAC Address

- Check Process Host Lookup
  - Via PAP/ASCII
    - Uncheck Check Password
    - Check Check Calling-Station-ID equals MAC Address
  - Leave CHAP unchecked
  - Via EAM-MD5
    - Uncheck Check Password
    - Check Check Calling-Station-ID equals MAC Address

- Permissions

- ▼ **Permissions**

- Set VLAN**
    - IETF 802.1X Attributes
    - Unique Attributes
  - Set ACL**



- Check Set VLAN
  - Select IETF 802.1X Attributes
- Check Set ACL
  - Select **RADIUS:Filter-ID**

- CoA

**▼ Change of Authorization (CoA)**

CoA by

\* Default CoA Port  (i)

\* Timeout Interval  seconds (i)

\* Retry Count  (i)

Send Message-Authenticator

**Disconnect**

RFC 5176

<input type="text" value="Radius:Acct-Terminate-Cause"/>	=	<input type="text" value="Admin Reset"/>	-	+
<input type="text" value="Radius:Calling-Station-ID"/>	=	<input type="text" value="0"/>	-	+

Port Bounce

<input type="text" value="Radius:Acct-Terminate-Cause"/>	=	<input type="text" value="Admin Reset"/>	-	+
<input type="text" value="Radius:Calling-Station-ID"/>	=	<input type="text" value="0"/>	-	+
<input type="text" value="Tellabs:Tellabs-AVPair"/>	=	<input type="text" value="subscriber:command=bounce-hos"/>	-	+

Port Shutdown

<input type="text" value="Radius:Acct-Terminate-Cause"/>	=	<input type="text" value="Admin Reset"/>	-	+
<input type="text" value="Radius:Calling-Station-ID"/>	=	<input type="text" value="0"/>	-	+
<input type="text" value="Tellabs:Tellabs-AVPair"/>	=	<input type="text" value="subscriber:command=disable-hos"/>	-	+

**Re-authenticate**

Basic

<input type="text" value="Radius:Calling-Station-ID"/>	=	<input type="text" value="0"/>	-	+
<input type="text" value="Tellabs:Tellabs-AVPair"/>	=	<input type="text" value="subscriber:command=reauthentic"/>	-	+

**Rerun**

Radius:Calling-Station-ID	=	0
Tellabs:Tellabs-AVPair	=	subscriber:command=reauthentici
Tellabs:Tellabs-AVPair	=	subscriber:reauthenticate-type=re

**Last**

Radius:Calling-Station-ID	=	0
Tellabs:Tellabs-AVPair	=	subscriber:command=reauthentici
Tellabs:Tellabs-AVPair	=	subscriber:reauthenticate-type=la

**CoA Push**

RFC 5176

Radius:Calling-Station-ID	=	0
---------------------------	---	---

- Set to COA by RADIUS
  - **CoA Port:** CoA Port is configurable and must agree with the Tellabs Network Device setting. The default on Cisco ISE is 1700 (and for ISE versions 2.0, 2.1, 2.2, 2.3 MUST be 1700 when you have a distributed Cisco ISE Instance with PANs and PSNs due to an ISE issue). The default in the standard and on Tellabs equipment is 3799.
  - **Timeout Interval 5**
  - **Retry count 2**
  - Enable **Send Message-Authenticator**
- Check Disconnect
  - Check RFC5176
  - Add **RADIUS:Calling-Station-ID=0**
  - Add **RADIUS:Acct-Terminate-Cause=Admin Reset**
- Check Port Bounce
  - **Radius:Acct-Terminate-Cause = Admin Reset**
  - **Radius:CallingStation-ID=0**
  - **Tellabs:Tellabs-AVPair=subscriber:command=bounce-host-port**
- Check Port Shutdown
  - **Radius:Acct-Terminate-Cause = Admin Reset**
  - **Radius:Calling-Station-ID=0**
  - **Tellabs:Tellabs-AVPair=subscriber:command=disable-host-port**
- Re-authenticate
  - Check Basic
    - Add **Radius:Calling-Station-ID=0**
    - **Tellabs:Tellabs-AVPair= subscriber:command=reauthenticate**

- COA Push
  - Check RFC5176
  - Add Radius:Calling-Station-ID=0
- Redirect

▼ 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

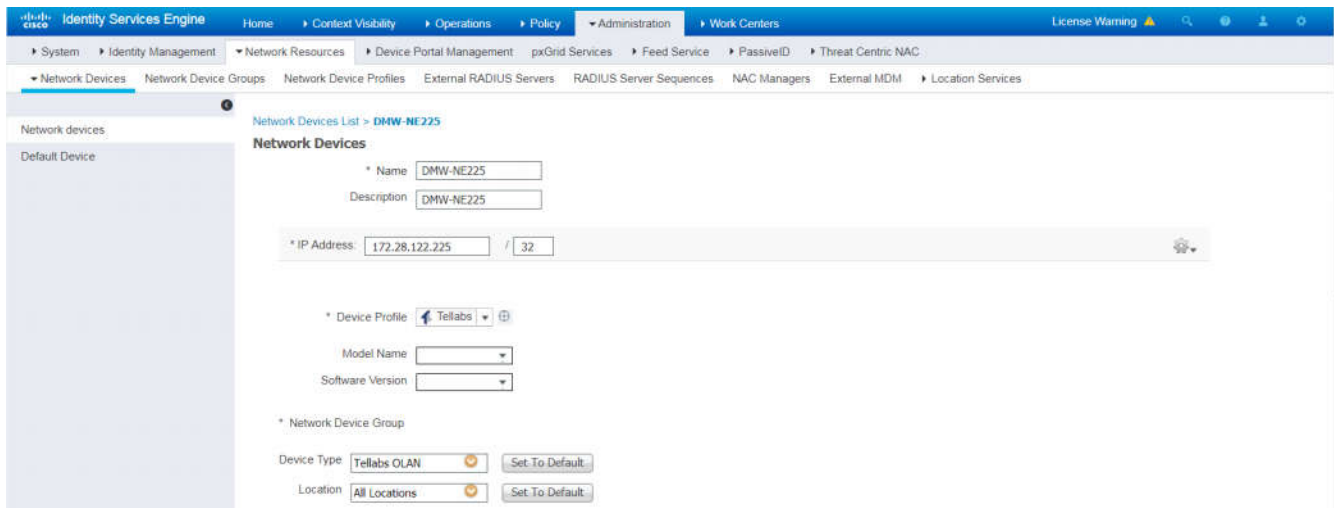
SSID

- Accept all the defaults
  - **Type:** Dynamic URL
  - **Cisco:** cisco-av-pair: url-redirect=\${URL}
  - **Select Session ID** in the Dynamic URL Parameter
  - **Client IP Address:** Blank
  - **Client MAC Address:** client\_mac
  - **Originating URL:** redirect
  - **Session ID:** sessionId
  - **SSID:** wlan

### Creation of Network Device for Tellabs OLAN

The Creation of a Network Device will allow Cisco ISE and the Tellabs OLT to communicate for the purposes of authorizing users via the RADIUS interface. A Network Device needs to be created for each OLAN OLT. Creation of a network device is done from the menu:

Administration->Network Resources->Network Devices->Add



- **Name:** Enter the logical name of the OLT here.
- **Description:** Enter the description of the OLT.
- **IP Address:** Enter the management IP of the Tellabs OLT.
- **Device Profile:** Select the Tellabs Network Device Profile created earlier.
- **Model Name:** Leave Blank
- **Software Version:** Leave Blank
- **Location:** Set as appropriate to allow access at the appropriate locations.
- **Device Type:** Set as Tellabs OLAN

Then enter the RADIUS Authentication Settings:

**RADIUS Authentication Settings**

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

CoA Port

- **Radius Checkbox:** Check the radius checkbox to enable a RADIUS interface to the Tellabs OLT.
- **Shared Secret:** Enter the RADIUS secret/pre-shared key that will also be entered into the Tellabs OLT and used for authentication of RADIUS requests.
- **Enable Key Wrap:** Leave Unchecked.
- **Key Encryption Key:** Leave blank.
- **Message Authenticator Key:** Leave blank
- **Key Input Format:** Key can be entered in either ASCII or Hex.
- **CoA Port:** CoA Port is configurable and must agree with the Tellabs Network Device Profile's setting. The default on Cisco ISE is 1700 (and for ISE versions 2.0, 2.1, 2.2, 2.3 MUST be 1700 when you have a distributed Cisco ISE Instance with PANs and PSNs due to an ISE issue). The default in the standard and on Tellabs equipment is 3799.

▼ SNMP Settings

\* SNMP Version

\* SNMP RO Community

SNMP Username

Security Level

Auth Protocol

Auth Password

Privacy Protocol

Privacy Password

\* Polling Interval  seconds (Valid Range 600 to 86400 or zero)

Link Trap Query

MAC Trap Query

\* Originating Policy Services Node

The SNMP settings are optional. At this time Cisco ISE does not make effective use of Tellabs SNMP Data for profiling purposes.

- **SNMP Version:** 2c.
- **SNMP RO Community:** Type in the community string that was configured on the EMS on the SNMP interface.
- **SNMP Username/Security Level/Passwords:** Not needed in SNMP2c (note if SNMPv3 selected, this is required).
- **SNMP Polling Interval:** Set to desired polling interval, recommend that minimum value is 600 seconds.
- **Link Trap Query:** Check This.
- **MAC Trap Query:** Check This.
- **Originating Policy Services Note:** Select the name of the Cisco ISE PSN instance, in this case it was named CiscoISE.

### Creation of Network Device Type Tellabs OLAN

Under the Administration->Network Resources->Network Device Groups->All Device Types add a network Device Group for Tellabs OLAN:

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Network Devices **Network Device Groups** Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

**Network Device Groups**

Selected 0 | Total 3

Edit Add Duplicate Delete Show All

Name	Type	Description
<input type="checkbox"/> Cisco Switch	Device Type	Cisco Switches
<input type="checkbox"/> Tellabs OLAN	Device Type	Tellabs OLAN
<input type="checkbox"/> WLC	Device Type	Wireless LAN Controller

Network Device Groups > All Device Types > **Tellabs OLAN**

**Network Device Groups**

\* Name

Description

\* Type

Then add all the Tellabs OLAN OLTs that are in the network to this Network Device Group:

**Network Device Groups**

\* Name

Description

\* Type

**Group's Network Devices**

Selected 0 | Total 5

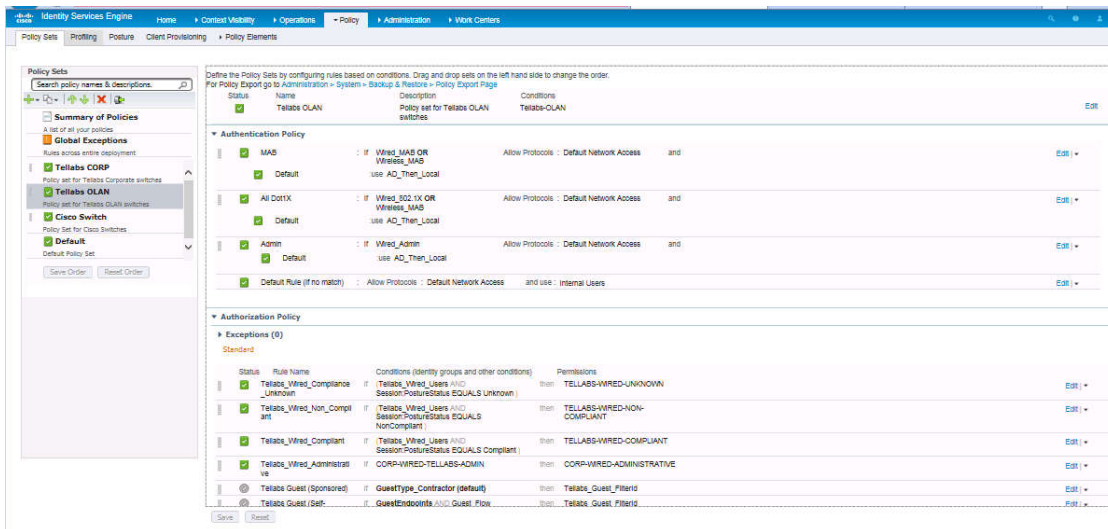
+ Add Move Remove to root type Show All

Name	IP/Mask	Description
<input type="checkbox"/> CORP-1150	10.50.0.50/32	CORP-1150
<input type="checkbox"/> CORP-1150-SECONDARY	172.28.128.92/32	CORP-1150-SECONDARY
<input type="checkbox"/> DMW-NE146	172.28.125.146/32	DMW Tellabs OLAN 1134
<input type="checkbox"/> DMW-NE56	172.28.125.56/32	DMW Tellabs OLAN 1150
<input type="checkbox"/> DMW_NE21	172.28.126.21/32	DMW Tellabs OLAN 1134

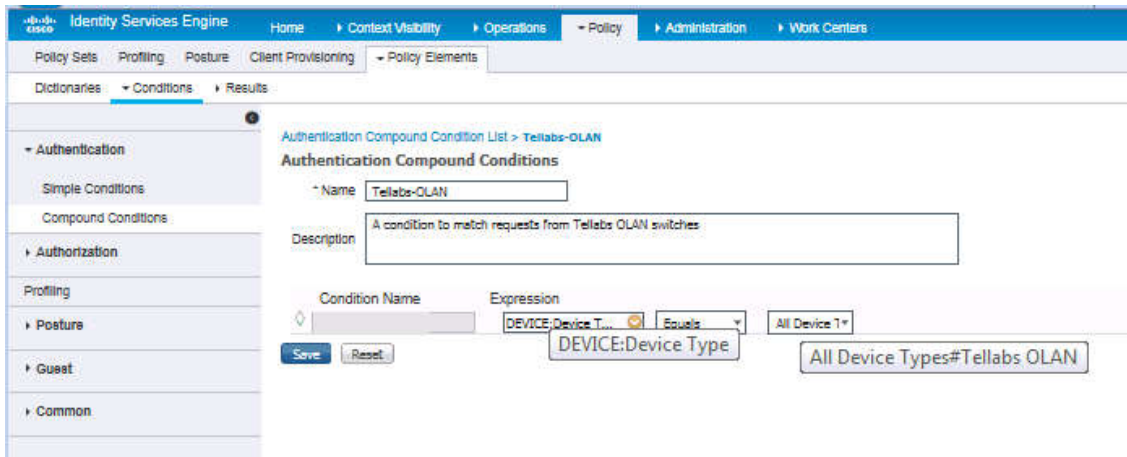
**Add Policy Set**



This section will demonstrate how to create a Policy Set that references the Network Device Group that we just created. This allows you to associate a Policy Set with a specific Tellabs OLT Instance which was specified above in the Network Device's Device Type. This allows separate treatment of policy for Tellabs OLAN and more specifically for specific OLT Instances. This is located under Policy -> Policy Sets.



Under the Policy -> Elements -> Condition -> Authentication -> Compound Conditions add an Authorization Compound Condition for Tellabs-OLAN.



**Example Authorization Profiles with Filter-ID**

This section will give several Authorization Profiles examples which demonstrate two different mechanisms for using Filter-ID to configure the Service Profile on a UNI port of an ONT attached to the Tellabs OLT.

This Authorization Profile will give an example of selecting a specific service profile on the Tellabs OLAN System.

Authorization Profiles > Tellabs-FilterID-Match-Example

### Authorization Profile

Name:

Description:

Access Type:

Network Device Profile:

Service Template:

Track Movement:

Passive Identity Tracking:

---

**Common Tasks**

DACL Name

ACL (Filter-ID)

VLAN

Voice Domain Permission

---

**Advanced Attributes Settings**

=

=

---

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
 Session-Timeout = 3600  
 Termination-Action = RADIUS-Request  
 Filter-ID = TLAB:PROFILE-MATCH=DATA  
 Filter-ID = TLAB:PROFILE-ACL=TELLABS-PERMIT-ALL

- Name: Name of the Authorization Profile.
- Description: Enter a description of the profile.
- Access Type: Select Access Accept
- Network Device Profile: Tellabs
- Advanced Attributes Setting
  - Add RADIUS:Filter-ID=TLAB:PROFILE-MATCH=<Service Profile Name> where in this example the service profile name to be communicated to the Tellabs OLT needs to be with DATA for a successful profile match. As an example, it might match to Service profile DATA-VLAN2995 that is in the NAC profile on the port.
    - PROFILE-SVC does an exact match.

- PROFILE-MATCH will look for a profile that has the MATCH phrase at the beginning.
- PROFILE-ACL will add an ACL Profile to the selected Service Profile so that proper ACLs will be enforced on the line.

With this Authorization profile when a port is authorized, it will send back an Access-Accept message with a MATCH PROFILE name of DATA and find the Service profile DATA-VLAN2995 as a match. This will properly configure the port with all the proper service profile attributes.

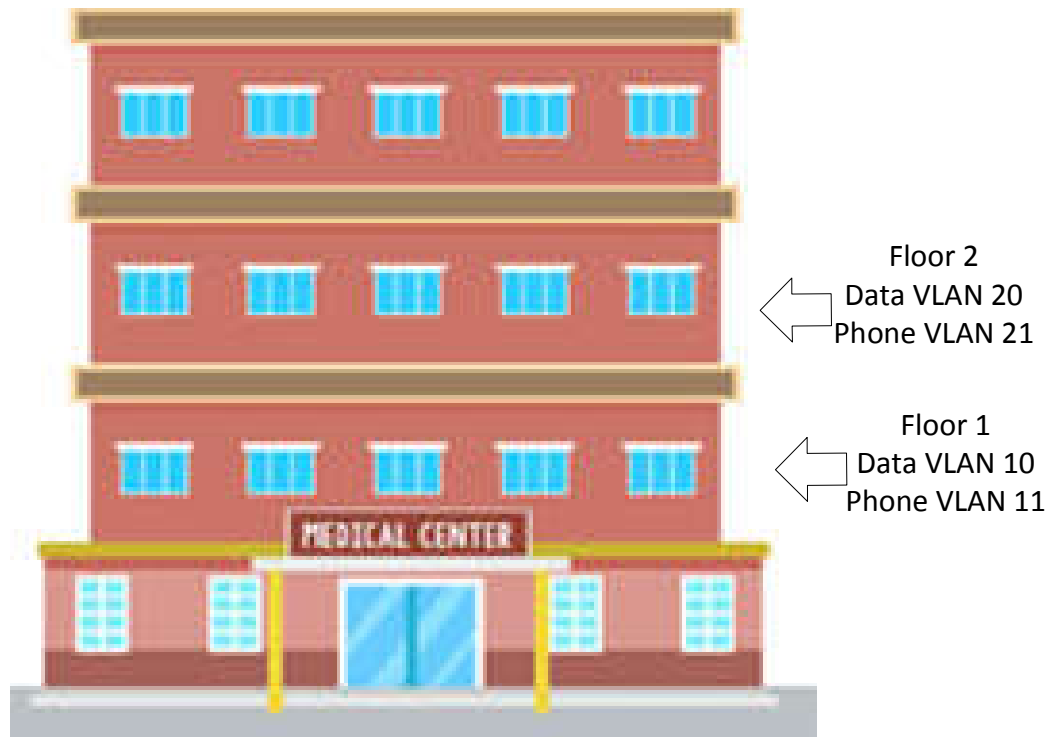
### Using Service Profile-Match for Generic Policies

The Tellabs OLAN system supports a vendor specific extension of the Filter-ID field to allow a more generic method for configuring the system. This Filter-ID extension causes the system to do a search of the profiles assigned to a port and look for a prefix match. The system will then assign the profile to the Ethernet port. This allows for much more generic rules in RADIUS and policy engines like Cisco ISE to remove knowledge of specific VLAN IDs.

The syntax for this is as follows:

TLAB:PROFILE-MATCH=<Service Profile Name Prefix>

Where <Service Profile Name Prefix> is the substring you want to match at the beginning of the profile name. Then the service profiles would all be named based on their logical function rather than the specific profile for that port. (ex. Camera, Data, Guest, Printer, Security, Video, Voice).



You might have for each floor of a building two VLANs, one for Data, and one for phones. These VLANs are specific to a geographic location, but logically there is a phone and data VLAN per floor.

In the EMS, all ports on the first floor would be assigned with a NAC profile with all VLANs used on that floor.

**Create Ethernet Port NAC Profile**

Profile Name: Floor1

Maximum Managed MACs: 16

Access Violation

Auto Disable      Auto Re-Enable Timeout (sec): 300

Default VLAN

Enable Default VLAN

Service Profile: Data-Floor1

Guest VLAN

Enable Guest VLAN      Startup Delay (sec): 90

Service Profile: 110-1002

MAC Bypass

Enable MAC Bypass      Startup Delay (sec): 30

Auth Method: PAP (MAC as Credentials)

Username:      Password:     

PAE Dynamic Service

Enable PAE Dynamic Service

Enable Filter ID       Enable Tunnel

Enable Egress VLAN ID

Authorization Failure

Apply      Cancel

Then assign floor 1 profiles to a NAC profile which you assign to ALL the ports on floor 1. You can multi-click the profiles by <Ctrl> clicking them.

**Create Ethernet Port NAC Profile**

Profile Name: Floor1

Maximum Managed MACs: 16

Access Violation:  Auto Disable, Auto Re-Enable Timeout (sec): 300

Default VLAN:  Enable Default VLAN

Service Profile: PRINTER-NV802, PROD-1131-data-200, Phone-Floor1, Phone-Floor2, QOS-Port01-XCN01

Guest VLAN:  Enable Guest VLAN, Startup Delay (sec): 90

Service Profile: 100M\_100M, 110-10, 110-100, 110-1001, 110-1002

MAC Bypass:  Enable MAC Bypass, Startup Delay (sec): 30

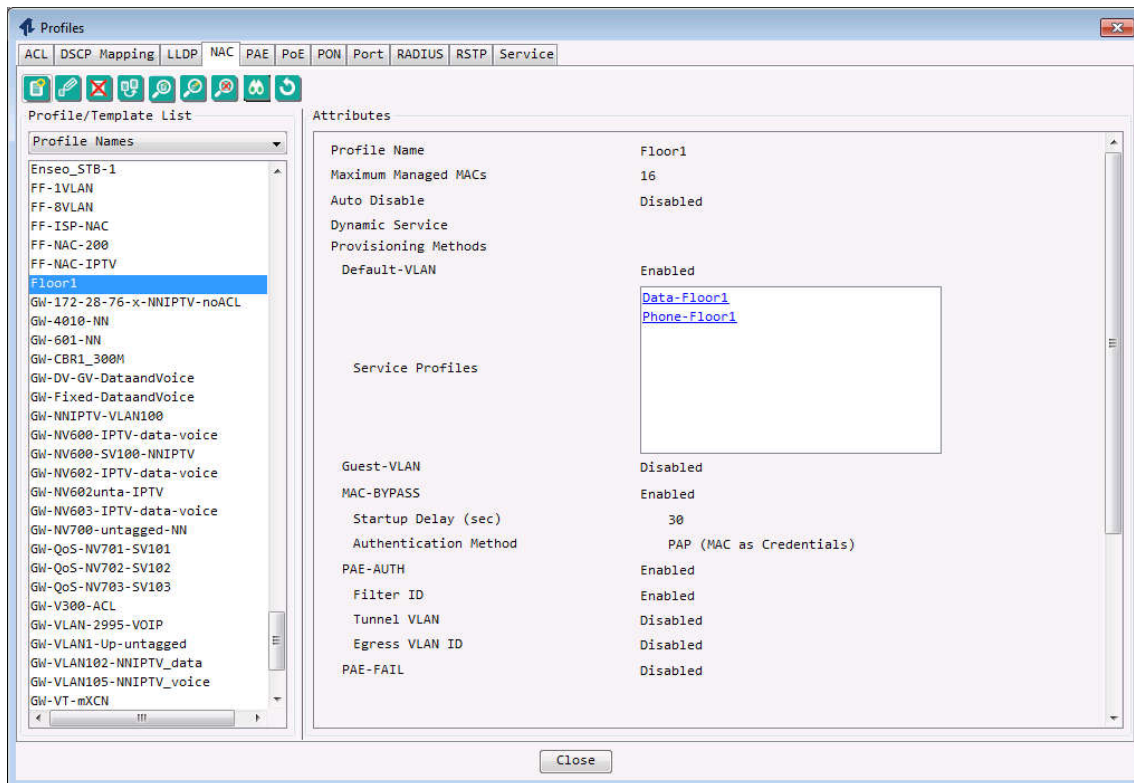
Auth Method: PAP (MAC as Credentials)

Username: , Password:

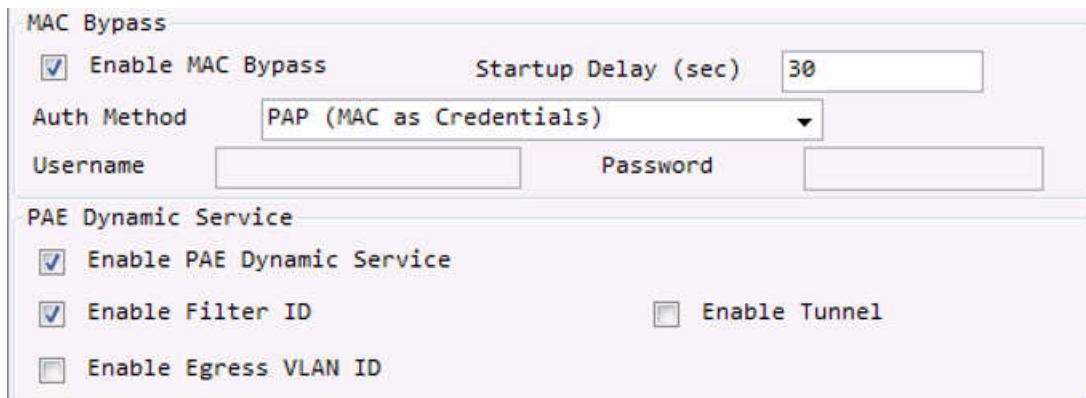
PAE Dynamic Service:  Enable PAE Dynamic Service,  Enable Filter ID,  Enable Tunnel,  Enable Egress VLAN ID

Authorization Failure

Apply Cancel



Enable either MAC Bypass (typically used for phones, printers, etc that don't properly handle 802.1x), and/or PAE Dynamic Service. This will enable 802.1x on the port. If you have a PC and phone sharing the port, you may need both enabled. Please consult the AppNote on RADIUS for further guidance on detailed settings.



Ports									
UNI	UNI Status	PON	Voice	Voice Status					
AID	User Label	NAC Profile	Port	PoE	RSTP	PAE	LLDP	Admin State	
ETH1-4-1-1-1		Floor1	Corp-Long-Hold-Time	PoE_Enabled	CORP_RSTP_ENABLED	CORP-PAE-Enabled	LLDP-PoE-Trim	Enabled	

Then from RADIUS you can just return a filter ID of either:

- TLAB:PROFILE-MATCH=Data
- Or TLAB:PROFILE-MATCH=Phone

The system will search for these prefixes for a match within the profiles assigned in the default VLAN section of the NAC profile.

The user (or MAB MAC) will be authenticated to RADIUS. The Filter ID will be returned that corresponds with that user. When the service profile reaches the OLAN system, it will search the port for a match on the beginning of the profile name and apply the profile that matches. If it does not match, no action is taken and the port remains without access.

### Configuring Cisco ISE to use Profile Match

This section will illustrate how to create an Authorization Profile that supports a Profile Match operation. This is located under Policy -> Policy Elements -> Results -> Authorization Profile.



Authorization Profiles > Tellabs-FilterID-Match-Example

**Authorization Profile**

Name:

Description:

Access Type:

Network Device Profile:

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

- DACL Name
- ACL (Filter-ID)
- VLAN
- Voice Domain Permission

Advanced Attributes Settings

=

=

Attributes Details

```

Access Type = ACCESS_ACCEPT
Session-Timeout = 3600
Termination-Action = RADIUS-Request
Filter-ID = TLAB:PROFILE-MATCH=DATA
Filter-ID = TLAB:PROFILE-ACL=TELLABS-PERMIT-ALL
    
```

Authorization Profile attributes:

- Name: Enter Profile Name.
- Description: Enter Profile Description.
- Access Type: ACCESS\_ACCEPT
- Network Device Profile: Select previously created Tellabs Network Device Profile.
- Leave common tasks unchecked.
- Advanced Attributes Settings
  - RADIUS:Filter-ID=TLAB:PROFILE-MATCH=DATA

- o PROFILE-ACL will add an ACL Profile to the selected Service Profile so that proper ACLs will be enforced on the line.

This will cause the OLT to look at all profiles configured in the Default VLAN section of the NAC profile and find one that begins with the string "DATA", when it finds a match, that profile will be assigned. If there is no match found, the MAC/802.1x device will not be connected to the network.

**Allowed Protocols for Authentication**

Tellabs supports all the allowed protocols defined in the current Default Network Access Profile and the default profile can be used. This is located at Policy -> Policy Elements -> Authentication -> Allowed Protocols -> Default Network Access

Allowed Protocols Services List > Default Network Access

**Allowed Protocols**

Name: Default Network Access

Description: Default Allowed Protocol Service

▼ Allowed Protocols

**Verifying Selected Profile for a Port or Logged in User**

You can verify the Service Profile that was assigned to a port in the Radius Accept-Accept message by looking at the Dynamic Services menu item on an Ethernet Port.

Ports									
UNI   UNI Status   PON   Voice   Voice Status									
AID	User Label	NAC Profile	Port	PoE	RSTP	PAE	LLDP	Admin State	
ETH1-4-1-1-1	Floor1	Corp-Long-Hold-Time		PoE_Enabled	CORP_RSTP_ENABLED	CORP-PAE-Enabled	LLDP-PoE-Trim	Enabled	
ETH1-4-1-1	Property		t	default	default	default	default	Disabled	
ETH1-4-1-1	Dynamic Services		t	default	default	default	default	Disabled	
ETH1-4-1-1	Profile and Admin State		t	default	default	default	default	Disabled	

The dynamic services tab will show you the network VLAN that is assigned to the port from the services profile, and the service profile that was selected. In this case Radius returned the profile name: DATA and matched a profile named "DATA-NV2995" as the profile to be assigned to the port. This will be updated dynamically based on whatever is returned from Radius.

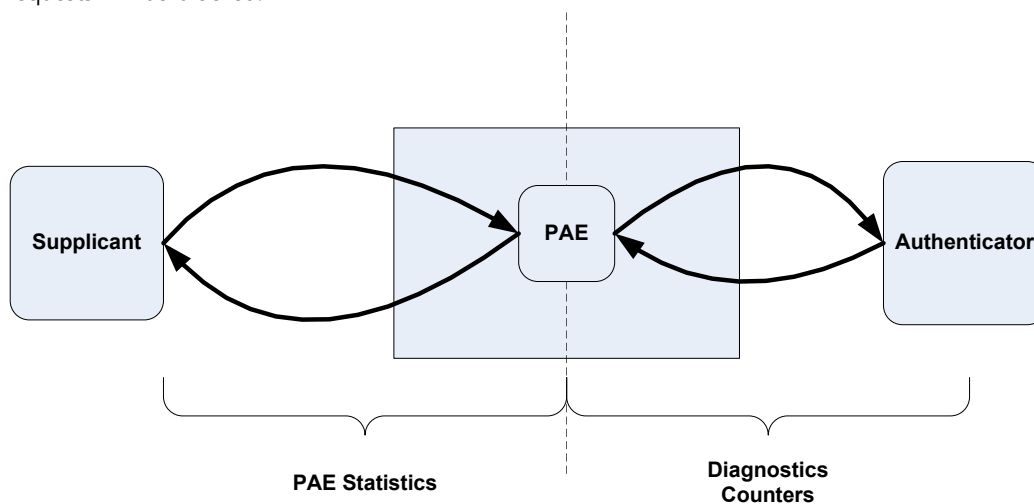
The screenshot shows the 'Ethernet Port Services' configuration window with the 'Dynamic Services' tab selected. It displays a table with the following data:

NE IP Address	NE Target Ide...	AID	Network Vlan	Network Vlan...	Subscriber Vlan	Service Profile Name
172.28.125.146	DMW-1134-125.146	ETH1-1-1-2-4	2995	N/A	untagged	DATA-NV2995

At the bottom of the window, it indicates 'Unique VLAN Count: 1' and has 'Refresh' and 'Close' buttons.

### Troubleshooting Radius Requests

The first thing to remember about the radius requests is they will all go up the Management VLAN. Ensure that you have a route from the management VLAN to the Radius server. If not, the EAPOL requests will be blocked.



There are two types of statistics for diagnosing what is going on with Radius authentication. The PAE Statistics will cover the exchanges between the supplicant (end device) and the OLT for 802.1x. The Diagnostics tab will contain the counters associated with the Radius Authentication exchange.

You can also use the PAE Counters to understand what is going on with the exchange between the supplicant (end device), the OLT, and the Radius Server.

You can get statistics for the PAE by going to the Ports View, right clicking on the port, and selecting PAE Property from the right click menu.

AID	User Label	NAC Profile	Port	PoE	RSTP	PAE	LLDP	Admin State
ETH1-1-1-2-1		DMW-CORP-...	Corp-Long-Hold-Time	DMW-CORP...	DMW-CORP-RSTP-...	CORP-PAE-Enabled	Corporate-L...	Enabled
ETH1-1-1-2-2		DMW-CORP-...	Corp-Long-Hold-Time	DMW-CORP...	DMW-CORP-RSTP-...	CORP-PAE-Enabled	Corporate-L...	Enabled
ETH1-1-1-2-3		DMW-CORP-...	Corp-Long-Hold-Time	DMW-CORP...	DMW-CORP-RSTP-...	CORP-PAE-Enabled	Corporate-L...	Enabled
ETH1-1-1-2-4		DMW-CORP-...	Corp-Long-Hold-Time	DMW-CORP...	DMW-CORP-RSTP-...	CORP-PAE-Enabled	Corporate-L...	Enabled

The Status Tab will give you the high level state of the Authentication Process:

Authenticator PAE State lets you know what the current state of the PAE State Machine

- **Initialize** - Generally a transient state. Can occur when the RADIUS server denies authentication, the port's MAC is inoperable, or the state machine is initializing. Other transient states include Disconnected, Connecting, Authenticating, Aborting, and Held. If any of these states are not transient, contact your next level of support.
- **Authenticated and Force Authentication** - These states allow traffic to flow.
- **Force Unauthentication** - blocks all traffic on the port.

The Backend Authentication State lets you know what is going on within the authentication process: Displays the back-end authentication state received from the RADIUS server. Possible values are:

- **Request** - The RADIUS server received an authentication request.
- **Response** - The RADIUS server has sent an authentication response.
- **Success** - RADIUS authentication succeeded.
- **Fail** - RADIUS authentication failed.
- **Timeout** - Communication with the RADIUS server timed out.
- **Idle** - Following its initialization, the authenticator PAE is idle. It hasn't sent any authorization requests yet.
- **Initializing** - The authenticator PAE is initializing.

The Authentication Controlled Port status lets you know whether the port is currently Authorized or Unauthorized.

The Statistics Tab can be consulted to get more information to troubleshoot a connection.

Configuration	
NE IP Address	172.28.125.146
NE Target Identifier	DMW-1134-125.146
AID	ETH1-1-1-2-4
Available MAC	28-D2-44-24-02-A7

Received Frame Counter	
EAPOL	21
EAPOL Start	1
EAPOL Logoff	0
EAP Resp/Id	2
EAP Response	18
Invalid EAPOL	0
EAP length error	0

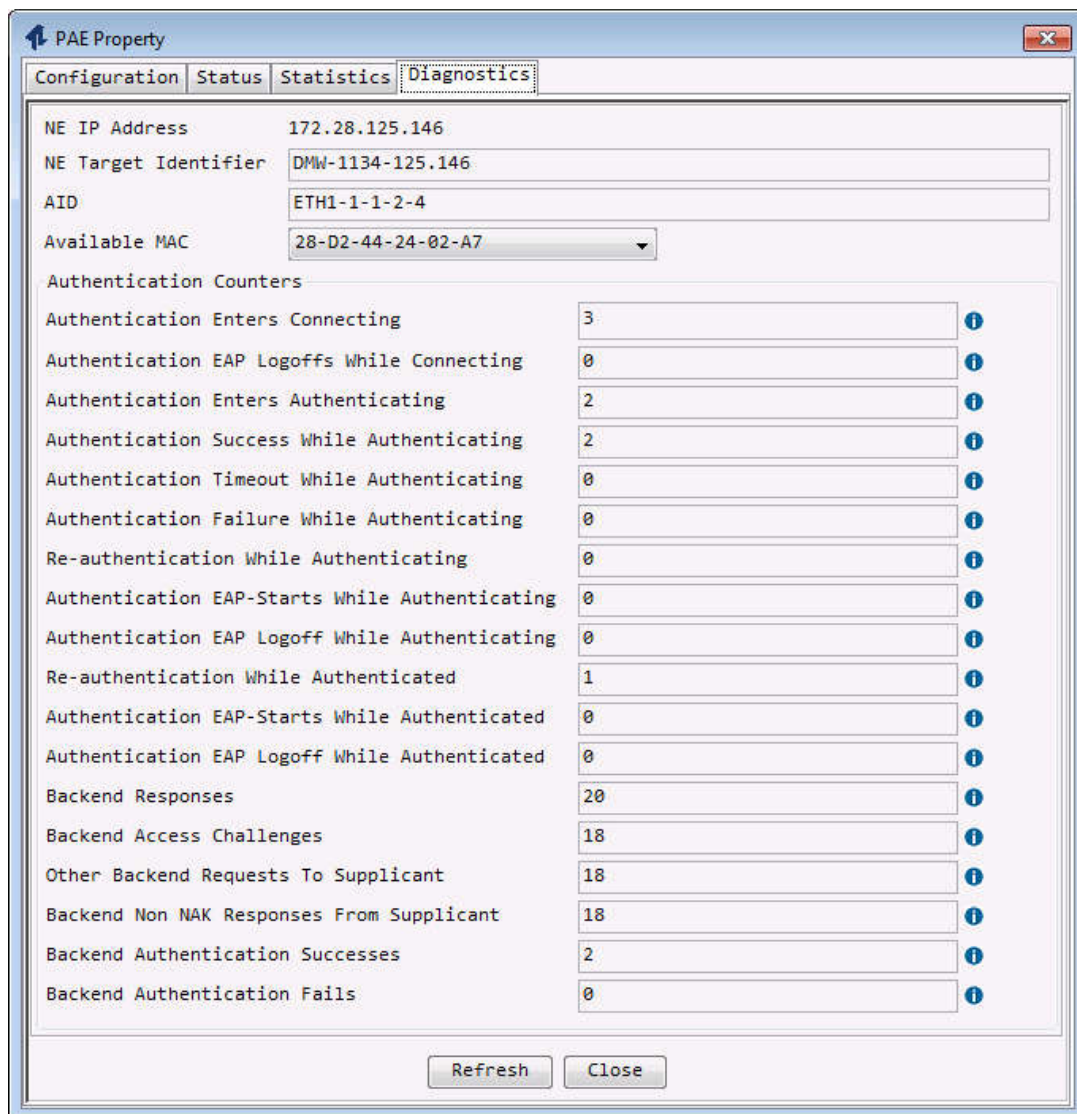
Transmitted Frame Counter	
EAPOL	23
EAP Req/Id	3
EAP Request	20

Last EAPOL Frame Information	
Version	01
Source	28-D2-44-24-02-A7

If the Received EAPOL counter is incrementing it means the OLT received EAPOL requests from the attached device on the port and is forwarding them to the Radius server. If the EAPOL counters are zero, then no requests have been received from the end device. The first message sent from the Supplicant is EAPOL Start, so this counter should be at least 1 if a request has been received. If this counter is zero, ensure that 802.1x is enabled, and that the correct PAE profile is assigned to the port. Please note these counters are reset on every run of the state machine and the MAC will be zeroed when the state machine starts over.

The Diagnostics Tab will give the results of the Radius / Authenticator exchanges between the OLT and RADIUS. The most important counter to watch is the "Backend Authentication Successes" and "Fails" as this will indicate whether the authenticator is allowing the supplicant access or not.



**Other Applicable AppNotes**

The following application notes should be consulted for further information relevant to RADIUS implementation on the Tellabs OLAN OLT:

- ENG-010428 Configuring Policy via Radius Authentication
- ENG-010466 Multiple Radius Authentication Domains

**Summary**

The above configuration outlines Tellabs specific configuration. Outside of those elements the configuration should follow typical Cisco ISE configuration rules.

**Technical Assistance**

For further support, please contact the Tellabs 24/7 Technical Assistance Center (TAC) .

Take the next step. Contact Tellabs today.



+1.800.690.2324(24hrs) 18583 N. Dallas Pkwy  
All other countries Dallas, TX 75287  
+1 630 798 9900 U.S.A  
www.tellabs.com



© 2015, Tellabs Access, LLC. All rights reserved.

TELXXXX 1/15