



Pulse Policy Secure

802.1X Authentication with Cisco Switch on Windows Configuration Guide

Published Date	August 2019
Document Version	3.2

Pulse Secure, LLC
2700 Zanker Road, Suite 200 San Jose, CA 95134
www.pulsesecure.net

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

802.1X Authentication with Cisco Switch

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.”

Introduction

This example describes a phased approach to deploy IEEE 802.1x port-based authentication with Cisco Switch on Windows platform to provide secure and role based access control using Pulse Policy Secure.

Figure: Overview



Configuration

The goal is to provide secure and role based access control using ACLs on Cisco Switch through PPS.

- Configuring Authentication Server
- Updating Default Realm
- Updating Default Sign-in Policy
- Creating a Host Checker Policy
- Creating User Role
- Creating a new RADIUS Client
- Configuring RADIUS Return Attribute Policies
- Configuring 802.1X Connections
- Configuring Cisco Switch

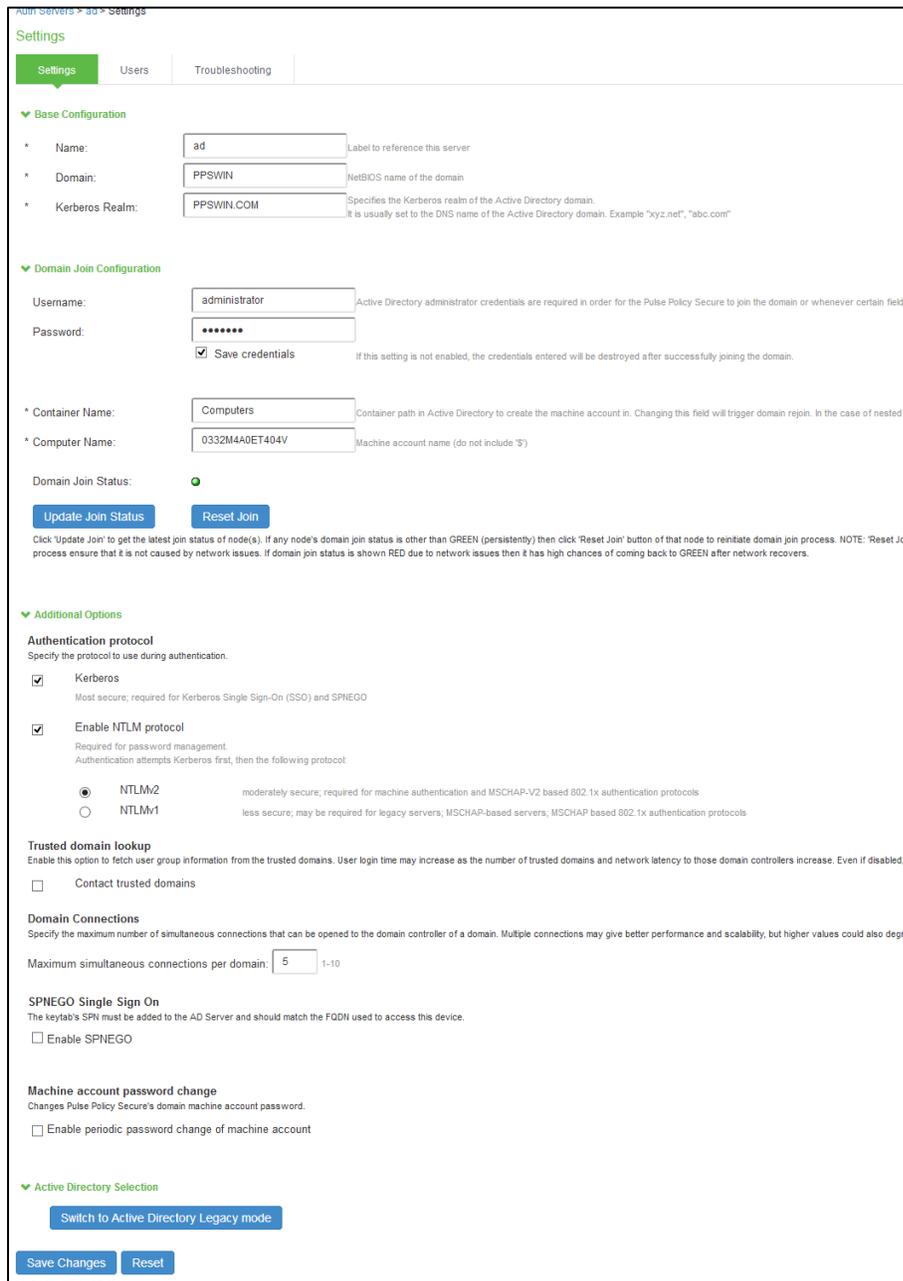
Configuring Authentication Server

Create a new AD Authentication server, select **Authentication > Auth.Servers**. For example, Select AD server from the drop down and Click **New Server**.

Figure 1: Authentication Server



The AD configuration page is shown below.



This screenshot displays the 'Settings' page for an authentication server. The page is divided into several sections:

- Base Configuration:** Includes fields for 'Name' (set to 'ad'), 'Domain' (set to 'PPSWIN'), and 'Kerberos Realm' (set to 'PPSWIN.COM').
- Domain Join Configuration:** Includes fields for 'Username' (set to 'administrator') and 'Password' (masked with dots). A checkbox for 'Save credentials' is checked. Below these are fields for 'Container Name' (set to 'Computers') and 'Computer Name' (set to '0332M4A0ET404V'). A 'Domain Join Status' indicator shows a green circle. There are 'Update Join Status' and 'Reset Join' buttons.
- Additional Options:**
 - Authentication protocol:** 'Kerberos' and 'Enable NTLM protocol' are checked. Under 'Enable NTLM protocol', 'NTLMv2' is selected.
 - Trusted domain lookup:** 'Contact trusted domains' is unchecked.
 - Domain Connections:** 'Maximum simultaneous connections per domain' is set to 5.
 - SPNEGO Single Sign On:** 'Enable SPNEGO' is unchecked.
 - Machine account password change:** 'Enable periodic password change of machine account' is unchecked.
- Active Directory Selection:** A button labeled 'Switch to Active Directory Legacy mode' is present.

At the bottom of the page, there are 'Save Changes' and 'Reset' buttons. A small asterisk indicates required fields.

Updating Default Realm

1. Select **User Realms > User > General**.
2. Under Authentication, select the AD as the authentication server.
3. Click **Save Changes**.

Figure 2: Realm

Pulse Secure System Authentication Administrators **Users** Endpoint Policy Maintenance Wizards

User Realms > Users > General

General

General Authentication Policy Role Mapping

* Name: Label to reference this realm

Description:

When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Specify the server to use for authenticating users.

User Directory/Attribute: Specify the server to use for authorization.

Accounting: Specify the server to use for Radius accounting.

Device Attributes: Specify the server to use for device authorization.

Dynamic policy evaluation

Enable dynamic policy evaluation

Session Migration

Session Migration

Other Settings

Authentication Policy: Password restrictions
Role Mapping: Host Checker restrictions
1 Rule

* indicates required field

Updating Default Sign-in Policy

1. Select **Authentication > Signing In > Sign-in Policies**.
2. Add Available Realms as **Users**, Authentication protocol set as **802.1X**.
3. Click **Save Changes**.

Figure 3: Sign-in Policy

Pulse Secure System **Authentication** Administrators Users Endpoint Policy Maintenance Wizards Pulse Policy Secure

Signing In > Sign-in Policies > */

User type: Users Administrators

Sign-in URL: */ Format: <host>/<path>/. Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: Default Sign-In Page To create or manage pages, see Sign-in pages.

Authentication realm

Specify what realms will be available when signing in.

Delete

<input type="checkbox"/>	Available realms	Authentication protocol set	
<input type="checkbox"/>	Cert Auth	- Not applicable -	<input type="button" value="Add"/>
<input type="checkbox"/>	Users	802.1X	

If more than one realm appears above, Odyssey Access Client or the Policy Secure sign-in page will ask the user to choose. Other endpoints cannot choose a realm; the Policy Secure will assign the first suitable realm from the list. If no realms appear above, sign-in will fail.

User may specify the realm name as a Username suffix
When this option is selected, the Username suffix will be used to specify a realm

Remove realm suffix before passing to authentication server
When this option is selected, the username suffix will be stripped from the Username prior to authenticating with an authentication server

Fail if suffix does not match any of the realms
When this option is selected, the user should provide one of the realm as suffix. If not, the user will be denied sign-in.

Configure Guest Settings

Use this sign-in policy for Guest and Guest admin to use specific pages.

Configure SignIn Notifications

Pre-Auth Sign-in Notification

Post-Auth Sign-in Notification

Creating a Host Checker Policy

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Under Policies, Click **New** and enter a policy name and click **Continue**.

Endpoint Security > Host Checker > New Host Checker Policy

New Host Checker Policy

Host Checker

*Policy Name: Firewall Policy Continue >> Cancel

* indicates required field

3. Under Rule Settings, select the rule type as **Predefined Firewall** and click **Add**.

Endpoint Security > Host Checker Policy

Host Checker Policy

Use this restriction to limit this policy to users whose workstations are running host-checking software.

Policy Name: Firewall Policy

Windows Mac Linux Solaris

Rule Settings

Predefined: Firewall Add Delete

4. Enter the rule name and specify the criteria for compliance and click **Save Changes**.

Configuration > Host Checker Policy > Add Predefined Rule : Firewall

Add Predefined Rule : Firewall

Rule Type: Firewall

*Rule Name: rule

*Criteria

Require any supported product.

Require specific products/vendors

Require any supported product from a specific vendor.

Available Vendors: adaware, Agnitum Ltd., AhnLab, Inc., ALLIT Service, LLC., Arcabit

Selected Vendors: Microsoft Corporation

Require specific products

Optional

Monitor this rule for change in result

Note: Enabling this option will report change in compliance for this rule to the Pulse Policy Secure immediately. The client component requires additional computing cycles to report change in compliance immediately. We strongly recommend that this option be enabled for rules that are dynamic in nature, for example a rule for RTP check provided by AntiVirus software. For other rules the host checker update frequency should be used to get periodic health checks from endpoints.

Remediation

Click on the remediation column headers to see the list of Firewalls supporting remediation

10 records per page Search:

Product Name	Turn On Firewall	
Windows Firewall (10.x)	<input type="checkbox"/>	
Windows Firewall (6.x)	<input type="checkbox"/>	

← Previous 1 Next →

Powered by OPSVAT

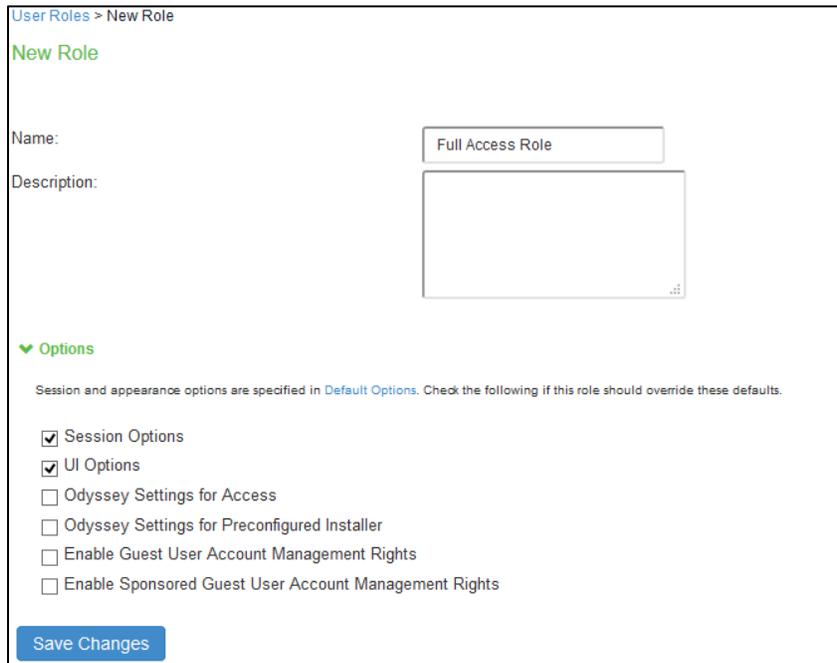
Save Changes Cancel

* indicates required field

Creating User Roles

1. Select **Users > User Roles > New User Role**.
2. Enter a name. For example, Full Access Role, Limited Access Role.
3. Click **Save Changes**.

Figure 4: User Role



The screenshot shows the 'New Role' configuration page. At the top, there is a breadcrumb trail 'User Roles > New Role' and a green heading 'New Role'. Below this, there are two input fields: 'Name:' with the text 'Full Access Role' and 'Description:' which is currently empty. A green section header 'Options' is followed by a note: 'Session and appearance options are specified in [Default Options](#). Check the following if this role should override these defaults.' Below the note are five checkboxes: 'Session Options' (checked), 'UI Options' (checked), 'Odyssey Settings for Access' (unchecked), 'Odyssey Settings for Preconfigured Installer' (unchecked), 'Enable Guest User Account Management Rights' (unchecked), and 'Enable Sponsored Guest User Account Management Rights' (unchecked). At the bottom left, there is a blue 'Save Changes' button.

4. Select **User Roles > <Full Access Role> > General > Restrictions > Host Checker**. Add the Firewall Policy restriction created earlier in [Creating a Host Checker Policy](#) for Full Access Role. Click **Save Changes**.

User Roles > Full Access Role > General > Restrictions > Host Checker

Host Checker

General Agent Agentless

Overview Restrictions Session Options UI Options

Source IP Browser Certificate Host Checker

Allow all users (Host Checker not required)
 Allow users whose workstations meet the requirements specified by these Host Checker policies:

Available Policies:

- Demo-SCCM-Policy
- Firewall
- test

Add -> Remove

Selected Policies:

- Firewall Policy

Allow access to the role if any ONE of the selected policies is passed.

To manage Host Checker policies, see the [Host Checker](#) configuration page.

Save Changes

For Limited Access Role, ensure that the Host Checker not required option is not selected.

User Roles > Limited Access Role > General > Restrictions > Host Checker

Host Checker

General Enterprise Onboarding Agent Agentless

Overview Restrictions Session Options UI Options

Source IP Browser Certificate Host Checker

Allow all users (Host Checker not required)
 Allow users whose workstations meet the requirements specified by these Host Checker policies:

Available Policies:

- antivirus

Add -> Remove

Selected Policies:

-

Allow access to the role if any ONE of the selected policies is passed.

To manage Host Checker policies, see the [Host Checker](#) configuration page.

Save Changes

5. Set Role Mapping rules. Select **User Realms > Users > Role Mapping > New Rule**

Figure 5: Role Mapping Rule

User Realms > Users > Role Mapping > Role Mapping Rule

Role Mapping Rule

Rule based on: Username

* Name:

▼ Rule if username...

is If more than one username should match, enter one username per line. You can use * wildcards.

▼ then assign these roles

Available Roles:

- Guest Admin
- Guest Sponsor
- Guest Wired Restricted
- LimitedAccessRole
- Quarantine role

Selected Roles:

- Full Access Role
- Limited Access Role

Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

*Indicates required field

Once the role mapping roles are configured the following screen is displayed.

Figure 6: Completed Role Mapping Rules

User Realms > Users > Role Mapping

Role Mapping

General Authentication Policy **Role Mapping**

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

<input type="checkbox"/>	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/>	1. username is "*"	→ Full Access Role and Limited Access Role	rule1	

When more than one role is assigned to a user:

- Merge settings for all assigned roles
- User must select from among assigned roles
- User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

Creating a new RADIUS Client

Add the Switch as RADIUS client

1. Select **Endpoint Policy > Network Access > RADIUS Client**.
2. Enter the name.
3. Enter the IP address of the Switch.
4. Select the make/model as Cisco Systems.
5. Select the default location group.
6. Click **Save Changes**.

Shared Secret will be used in the Cisco/RADIUS configuration.

Figure 7: RADIUS client

The screenshot shows the configuration page for a RADIUS Client named 'Cisco'. The breadcrumb trail is 'Network Access > RADIUS Client > Cisco'. The page title is 'Cisco'. Under the 'RADIUS Client' section, there are several fields: 'Name' (Cisco), 'Description' (empty), 'IP Address' (1), 'IP Address Range' (1), 'Shared Secret' (masked with dots), 'Make/Model' (Cisco Systems), 'Key Wrap' (unchecked), and 'Location Group' (Default). Below this is the 'Dynamic Authorization Support' section with 'Support Disconnect Messages' and 'Support CoA Messages' both unchecked. A 'Save Changes' button is at the bottom left. A small asterisk indicates required fields.

Network Access > RADIUS Client > Cisco

Cisco

▼ RADIUS Client

* Name: Cisco Label to reference this RADIUS Client.

Description:

* IP Address: 1 IP Address of this RADIUS Client.

* IP Address Range: 1 Number of IP Addresses for this RADIUS Client

* Shared Secret: ***** RADIUS shared secret

* Make/Model: Cisco Systems To manage make/model, see the [RADIUS Vendor](#)

Key Wrap Key Wrap (Support for RFC 6218)

* Location Group: Default To manage groups, see the [Location Group](#)

▼ Dynamic Authorization Support

Support Disconnect Messages Disconnect Message Support

Support CoA Messages Change of Authorization Message Support

Save Changes

* Indicates required field

Configuring RADIUS Return Attribute Policies

Define Radius Return Attribute policy based on ACL for different roles.

1. Set RADIUS return attributes. Select **Endpoint Policy > Network Access > RADIUS Return Attribute Policies**. Click **New Policy**.
2. Under RADIUS Attributes tab, select the check box for **Return Attribute**. Select appropriate Vendor Specific Attribute as Return Attribute. In the Value field, define the ACL/Firewall Filter. For example, Return Attribute is *Filter-Id* and Value as *compliant.in*.

Figure 8: RADIUS Return Attribute Policy

The screenshot shows the Pulse Secure web interface for configuring a RADIUS Return Attribute Policy. The breadcrumb trail is "Network Access > RADIUS Return Attributes Policies > full_access_policy". The page title is "full_access_policy".

General

* Name: full_access_policy
Description: [Empty text area]

Location Group

Specify the Location Group for which this policy applies.

Available Location Groups: Guest, Cert Auth, Guest Wired, SCCM-Location
Selected Location Groups: Default

RADIUS Attributes

Open port
 VLAN: [Empty field] (1 - 4094)
 Return Attribute

Return Attribute	Radius Auth Server Attribute Value	Auth Server Catalog Attribute Value	Value	
Filter-Id	-none-	-none-	[Empty field]	Add
<input type="checkbox"/> Filter-Id	-none-	-none-	compliant.in	

Add Session-Timeout attribute with value equal to the session lifetime
 Add Termination-Action attribute with value equal 1

Interface

Specify the interface which endpoints on this VLAN use to connect to the Pulse Policy Secure

Automatic (use configured VLANs)
 Internal
 External

Roles

Policy applies to ALL roles
 Policy applies to SELECTED roles
 Policy applies to all roles OTHER THAN those selected below

Available roles: Compliant Role, FullAccessRole, Guest Admin, Guest Sponsor, Guest Wired Restricted
Selected roles: Full Access Role

NOTE: changes to this page will cause all L2 clients to drop their connections and reconnect.

Save Changes Save as Copy

* indicates required field

Similarly define a remediation policy with Return Attribute as *Filter-Id* and Value as *noncompliant.in*.

Figure 9: RADIUS Return Attribute Policy

The screenshot shows the Pulse Secure web interface for configuring a RADIUS Return Attribute Policy. The breadcrumb trail is "Network Access > RADIUS Return Attributes Policies > rem_policy". The page title is "rem_policy".

General

* Name: Required: Label to reference this policy.
 Description:

Location Group

Specify the Location Group for which this policy applies.

Available Location Groups:
 Selected Location Groups:

RADIUS Attributes

Open port
 VLAN: (1 - 4094)
 Return Attribute:

Return Attribute	Radius Auth Server Attribute Value	Auth Server Catalog Attribute Value	Value	
<input type="text" value="Filter-Id"/>	<input type="text" value="-none-"/>	<input type="text" value="-none-"/>	<input type="text"/>	<input type="button" value="Add"/>
<input type="checkbox"/> <input type="text" value="Filter-Id"/>	<input type="text" value="-none-"/>	<input type="text" value="-none-"/>	<input type="text" value="noncompliant.in"/>	

Add Session-Timeout attribute with value equal to the session lifetime
 Add Termination-Action attribute with value equal 1

Interface

Specify the interface which endpoints on this VLAN use to connect to the Pulse Policy Secure

Automatic (use configured VLANs)
 Internal
 External

Roles

Policy applies to ALL roles
 Policy applies to SELECTED roles
 Policy applies to all roles OTHER THAN those selected below

Available roles:
 Selected roles:

NOTE: changes to this page will cause all L2 clients to drop their connections and reconnect.

* indicates required field

The following example shows the Filter-Id radius attribute policy for Cisco Switches.

Figure 10: RADIUS Return Attributes: Filter-Id

RADIUS Return Attributes Policies

Return Attributes | Request Attributes | Attribute Logging

Show policies that apply to: All roles [Update]

A RADIUS return attributes policy specifies the return list attributes to send to an 802.1X network access device, such as which VLAN endpoints must use to access the network. If no policy applies, Open Port is the default action.

[New Policy...] [Duplicate] [Delete...] [Up] [Down] [Save Changes]

Policy	Attributes	Location Group	Interface	Applies to role
1. full_access_policy	Filter-Id=compliant.in	Default	N/A	Full Access Role
2. rem_policy	Filter-Id=noncompliant.in	Default	N/A	Limited Access Role

Keyboard shortcuts:
Use "<" and ">" keys to move selected items up and down (remember to click Save Changes after rearranging the list). Use Ctrl+Plus and Ctrl-Minus to expand and collapse all items.

The following example shows RADIUS return attribute used to send the VLAN ID. In the below example, VLAN 65 is sent for Full Access Role and VLAN 60 for Limited Access Role.

RADIUS Return Attributes

Return Attributes | Request Attributes | Attribute Logging

Show policies that apply to: All roles [Update]

A RADIUS return attributes policy specifies the return list attributes to send to an 802.1X network access device, such as which VLAN endpoints must use to access the network. If no policy applies, Open Port is the default action.

[New Policy...] [Duplicate] [Delete...] [Up] [Down] [Save Changes]

Policy	ACL Settings	Attributes	Location Group	Interface	Applies to role
1. Full Access Policy	N/A	Tunnel-Type=13 Tunnel-Medium-Type=6 Tunnel-Private-Group-ID=65	All location groups	N/A	Full Access Role
2. Limited Access Policy	N/A	Tunnel-Type=13 Tunnel-Medium-Type=6 Tunnel-Private-Group-ID=60	All location groups	N/A	Limited Access Role

The following example shows the Cisco-AVPair radius attribute policy for Cisco Switches.

Note:

- When using VSAs there is no need to configure ACL/Firewall filters in the switches. These are managed by PPS and access control entries (ACEs) will be applied on the switches after User Authentication.
- VLAN change using CoA is not supported with Cisco Switches. It is recommended to use RADIUS disconnect for VLAN change.

Figure 11: RADIUS Return Attributes: Cisco-AVPair

Network Access > RADIUS Return Attributes Policies

RADIUS Return Attributes Policies

RADIUS Dictionary | RADIUS Vendor | Location Group | RADIUS Client | **RADIUS Attributes** | Network Infrastructure Device | SNMP Enforcement Policies

Return Attributes | Request Attributes | Attribute Logging

Show policies that apply to: All roles

A RADIUS return attributes policy specifies the return list attributes to send to an 802.1X network access device, such as which VLAN endpoints must use to access the network. If no policy applies, Open Port is the default action.

<input type="checkbox"/>	<input type="checkbox"/>	Policies	Attributes	Location Group	Interface	Applies to role
<input type="checkbox"/>	1.	full_access_with_AV_Pair	Cisco-AVPair=ip.inacl#161=permit ip any any	Default	N/A	Full Access Role
<input type="checkbox"/>	2.	rem_policy_with_AV_pair	Cisco-AVPair=ip.inacl#161=permit ip any host 10.10.10.5 Cisco-AVPair=ip.inacl#161=deny ip any host 10.10.10.5 Cisco-AVPair=ip.inacl#161=permit udp any eq bootpc any Cisco-AVPair=ip.inacl#161=permit udp any any eq domain Cisco-AVPair=ip.inacl#161=deny ip any any	Default	N/A	Limited Access Role

Configuring 802.1X Connections

1. Select Users > Pulse Secure Client > Connections. Click Default.

Figure 12: Connections

Pulse Secure Client > Connections > Default

Default

Name:

Description:

Owner: pps.ppswin.com
 Last Modified: 2019-01-23 10:53:41 UTC
 Server ID: 0320M8R509EC0ILE

Options

Name	Value
Allow saving logon information Enables the Save settings checkbox in the certificate trust and password prompts.	<input checked="" type="checkbox"/>
Allow user connections Allows user to create connections via the Pulse UI.	<input checked="" type="checkbox"/>
Always-on Pulse Client Prevents end users from circumventing Pulse connections. This option will disable all configuration settings that allow the end user to disable or remove Pulse connections, services or software.	<input type="checkbox"/>
Display Splash Screen Controls whether the splash screen is displayed when Pulse starts.	<input checked="" type="checkbox"/>
Dynamic certificate trust Controls whether users may accept to trust unknown certificates.	<input checked="" type="checkbox"/>
Dynamic connections Allows connections to be deployed automatically from devices.	<input checked="" type="checkbox"/>
EAP Fragment Size Maximum number of bytes in an EAPoL message from the client for 802.1x connections. Range: 450 - 3000 bytes	<input type="text" value="1400"/>
Enable captive portal detection Pulse will attempt to detect the presence of a captive portal hotspot. Only applies to Connect Secure and Policy Secure (L3) connections.	<input type="checkbox"/>
Enable embedded browser for authentication Pulse will use embedded browser for saaml, custom sign-in or token based authentication.	<input type="checkbox"/>
Enable embedded browser for captive portal Pulse will use an embedded web browser for captive portal pages. Only applies when captive portal detection is enabled.	<input type="checkbox"/>
FIPS mode enabled Deploy client with Federal Information Processing Standard enabled.	<input type="checkbox"/>
Prevent caching smart card PIN Enabling this will ensure the smart card PIN value is not cached by the client process.	<input type="checkbox"/>
VPN only access When Pulse client connects to a PCS having lock down mode enabled, it will enter lock-down mode and won't let any traffic flow through unless a Locked-down VPN connection is in connected state. User is allowed to connect or disconnect any connection. User is allowed to add any new connection/server URI. User is allowed to delete a connection if the connection is not locked down.	<input type="checkbox"/>
Wireless suppression Disconnect all wireless interfaces when a wired interface gets connected to a network. Applies to all wireless connections (not just those managed by Pulse).	<input type="checkbox"/>

Connections

10 records per page Search:

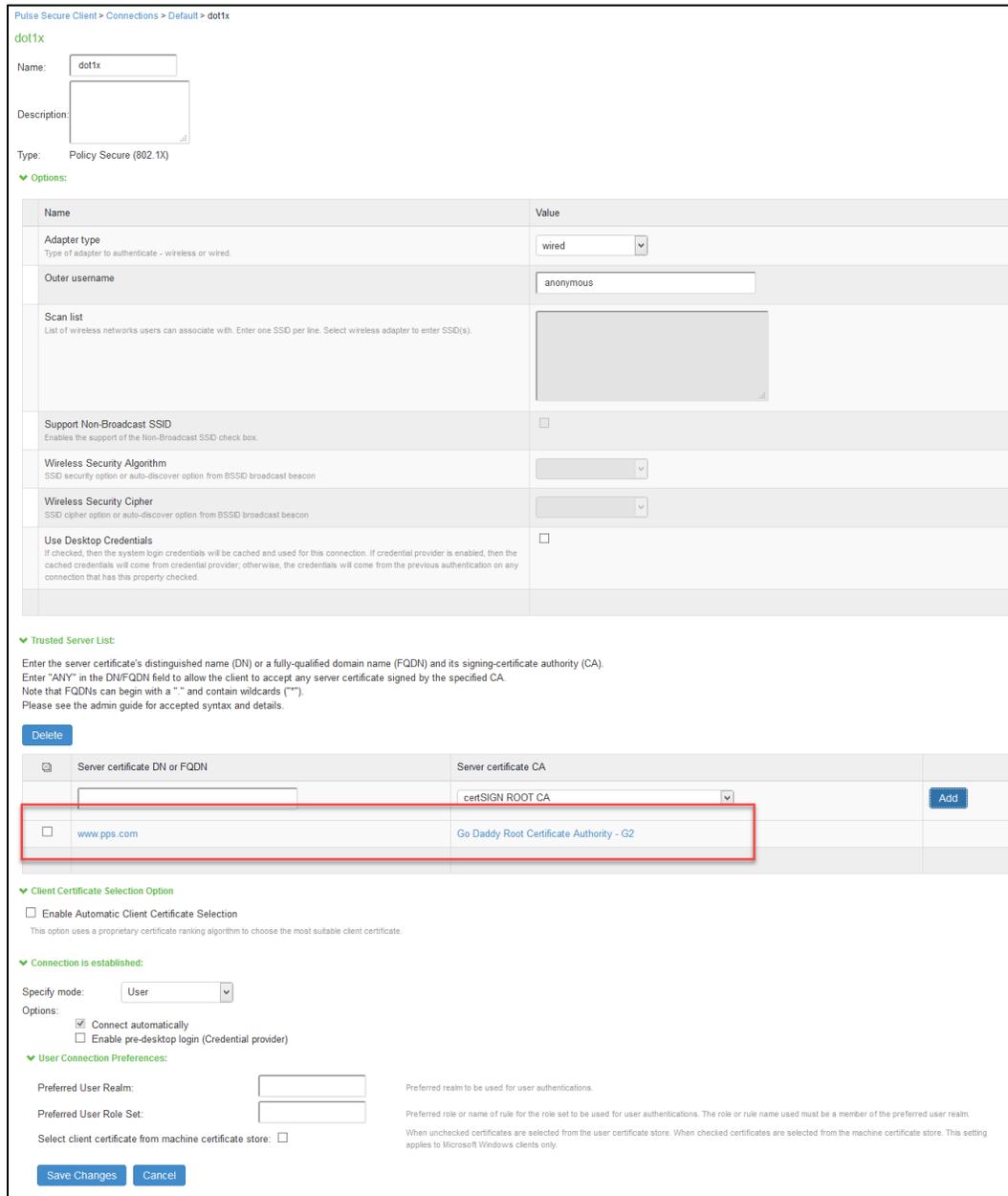
	Name	Type	Description
<input type="checkbox"/>	1. PPS	Connect Secure or Policy Secure (L3)	Default server connection
<input type="checkbox"/>	2. dot1x	Policy Secure (802.1X)	

1

- Under Connections, Click **New** to create a **New Pulse Secure Connection**.
Ensure that you have the valid device certificate to avoid certificate warnings at Pulse Client.

 Note: The configuration mentioned is only for User mode connections.

Figure 13: Pulse Secure Connection



The screenshot shows the configuration page for a connection named 'dot1x'. The 'Name' field is 'dot1x' and the 'Type' is 'Policy Secure (802.1X)'. Under 'Options', the 'Adapter type' is set to 'wired', 'Outer username' is 'anonymous', and 'Scan list' is empty. There are checkboxes for 'Support Non-Broadcast SSID', 'Use Desktop Credentials', and 'Client Certificate Selection Option'. The 'Trusted Server List' table contains one entry: 'www.pps.com' with 'Server certificate CA' set to 'Go Daddy Root Certificate Authority - G2'. At the bottom, there are fields for 'Preferred User Realm', 'Preferred User Role Set', and a checkbox for 'Select client certificate from machine certificate store'. 'Save Changes' and 'Cancel' buttons are at the bottom.

- Enter name and select Type as Pulse Secure (802.1X).
- Click **Save Changes**.

Configuring Cisco Switch

CLI command to configure 802.1X on Cisco 3850. The switch configuration varies for each switch type. Run the show run command on your switch to ensure that your access interface connections are set up.

```
# Interface configuration.
interface GigabitEthernet1/0/7
  switchport access vlan 60
  switchport mode access
  authentication periodic
  authentication timer reauthenticate server
  authentication event server dead action authorize
  access-session port-control auto
  dot1x pae authenticator
  spanning-tree portfast
end

# Specify the server group for authentication, authorization and accounting.
aaa authentication dot1x default group <group-name>
aaa authorization network default group <group-name>
aaa accounting dot1x default start-stop group <group-name>

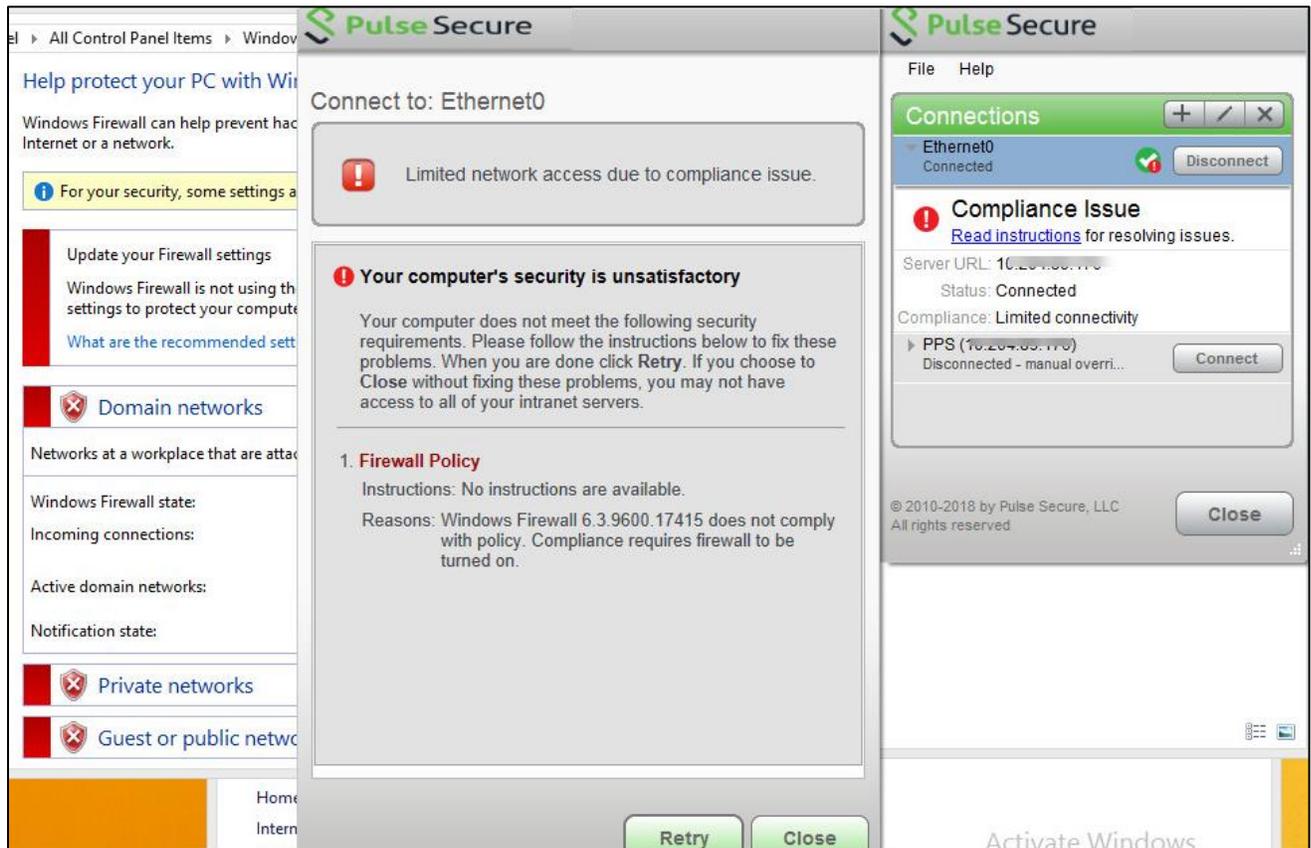
# Configure the PPS as radius server.
radius server <PPS-Server-name>
  address ipv4 <PPS-IP Address> auth-port 1812 acct-port 1813
  key psecure
  radius-server attribute 44 extend-with-addr
  radius-server attribute 6 on-for-login-auth
  radius-server attribute 8 include-in-access-req
  radius-server attribute 25 access-request include
  radius-server retransmit 1

# Create the server group which will be used for AAA.
# Add PPS as server in the server group.
aaa group server radius <group-name>
  server name <PPS-Server-name>

# ACL configuration
ip access-list extended compliant
  permit ip any any
ip access-list extended uncompliant
  deny ip any host <Resource-IP-Address1>
  deny ip any host <Resource-IP-Address2>
  permit ip any any
```

Results

Authenticate devices using 802.1X using Pulse Client. For example, in the above configuration scenario, users will be assigned Limited access role if the Host Checker compliance fails. A sample screenshot of users trying to access the network using Pulse Client on windows platform is shown below.



You can verify the active users table to view the session details of the user. The user gets a limited access role.

	User	Realm	Roles	Signed in	Signed in IP	MAC Address	Device Details	Agent Type	Agent Version	Endpoint Security Status
<input type="checkbox"/>	admin	Admin Users	Administrators	2019/1/23 15:45:36	██████████			Windows 8.1 FireFox		Not Applicable
<input type="checkbox"/>	PPSWINuser	Users	Limited Access Role	2019/1/23 15:50:51	██████████	00:50:55:14:55:1f		Windows 8.1 Pulse Secure	9.0.2.1421	Partially Compliant (Logs)

For troubleshooting you can verify the user access logs.

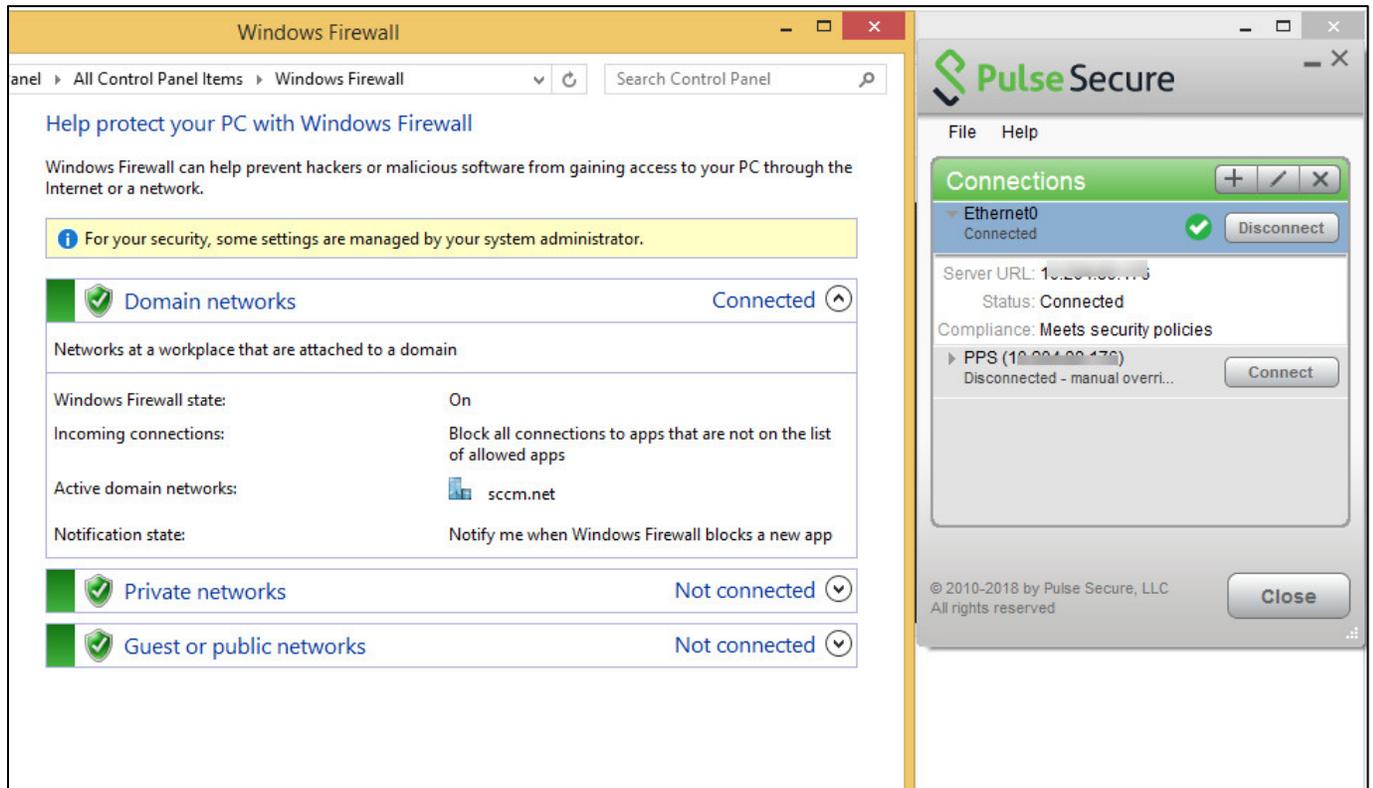
The screenshot shows the Pulse Secure System interface with a log table. The table has columns for Severity, ID, and Message. The third row is highlighted with a red box, showing a message where the Filter-ID is noncompliant.

Severity	ID	Message
Info	ACT30610	2019-01-23 15:50:51 - [127.0.0.1] PPSWUser(Users)[Limited Access Role] - Cisco.Start,Unknown,
Info	EAM24805	2019-01-23 15:50:51 - [127.0.0.1] PPSWUser(Users)[Limited Access Role] - RADIUS authentication accepted for PPSWUser(realm 'Users') from location-group 'Default' and attributes are: NAS-IP-Address = 10.10.10.2,NAS-Port = 50113,NAS-Port-Type = 15
Info	EAM24636	2019-01-23 15:50:51 - [127.0.0.1] PPSWUser(Users)[Limited Access Role] - User assigned RADIUS attribute(s) (Filter-Id='noncompliant')
Info	AUT24414	2019-01-23 15:50:51 - [127.0.0.1] PPSWUser(Users)[Limited Access Role] - Agent login succeeded for PPSWUser(Users) from 00-50-56-bf-55-4f with Pulse-Secure/9.0.2.1421 (Windows 8.1) Pulse/9.0.2.1421.
Info	AUT24804	2019-01-23 15:50:51 - [127.0.0.1] PPSWUser(Users)[Limited Access Role] - Host Checker policy 'Firewall Policy' failed on host ' address '00-50-56-BF-55-4F' for user 'PPSWUser' reason 'Rule-rule:Windows Firewall 6.3.9600.17415 does not comply with policy. Compliance requires firewall to be turned on:'

Verify the Switch for the applied Filter-Id. In the below example, Filter-Id applied is noncompliant.

```
Interface: GigabitEthernet1/0/13
  IIF-ID: 0x19C91A80
  MAC Address: 0050.56bf.554f
  IPv6 Address: Unknown
  IPv4 Address: Unknown
  User-Name: anonymous
  Status: Authorized
  Domain: DATA
  Oper host mode: multi-host
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: 0A190FCA0000029B7A2669E1
  Acct Session ID: 0x0000000f
  Handle: 0x6d00000f
  Current Policy: POLICY_Gi1/0/3
Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
  Security Policy: Should Secure
  Security Status: Link Unsecured
Server Policies:
  Filter-ID: noncompliant
Method status list:
  Method      State
  dot1x      Authc Success
```

The user turns ON the Windows Firewall and the Host Checker policy passes and the user connection is successfully established.



You can verify the active users table to view the session details of the user.

Figure 14: Active Users- Full Access Role

The image shows the Pulse Secure web interface. At the top, there is a navigation bar with 'PulseSecure' logo and menu items: 'System', 'Authentication', 'Administrators', 'Users', 'Endpoint Policy', 'Maintenance', 'Wizards'. Below the navigation bar, there is a breadcrumb 'Status > Active Users' and a sub-header 'Active Users'. There are tabs for 'Activity', 'Overview', 'Active Users' (selected), 'Device Profiles', and 'Admin Notification'. Below the tabs, there is a search field 'Show users named: *' and a 'Show 200 users' button. There are also buttons for 'Delete Session...', 'Delete All Sessions...', 'Refresh Roles', and 'Disable All Users...'. Below this, it says 'Number of Users: 2'. The main content is a table with the following columns: 'User', 'Realm', 'Roles', 'Signed in', 'Signed in IP', 'MAC Address', 'Device Details', 'Agent Type', 'Agent Version', and 'Endpoint Security Status'. The table contains two rows of data.

User	Realm	Roles	Signed in	Signed in IP	MAC Address	Device Details	Agent Type	Agent Version	Endpoint Security Status
admin	Admin Users	.Administrators	2019/1/23 15:45:36	170.04.15.40			Windows 8.1 FireFox		Not Applicable
PPSWINuser	Users	Full Access Role, Limited Access Role	2019/1/23 15:50:51	10.20.100.170	00-30-30-0F-35-4F		Windows 8.1 Pulse Secure	9.0.2.1421	Fully Compliant (Logs) Passed Policies: Firewall Policy Failed Policies: N/A Eliminated Roles: N/A

For troubleshooting you can verify the user access logs.

Figure 15: User Access Logs for compliant role.

Severity	ID	Message
Info	ACT30610	2019-01-23 16:17:35 - [10.00.0007] PPSWUser(Users)[Full Access Role, Limited Access Role] - Cisco,Start,Unknown,
Info	EAM24805	2019-01-23 16:17:35 - [10.00.0001] PPSWUser(Users)[Full Access Role, Limited Access Role] - RADIUS authentication accepted for PPSWUser (realm 'Users') from location-group 'Default' and attributes are: NAS-IP-Address = 10.00.0002,NAS-Port = 50113,NAS-Port-Type = 15
Info	EAM24638	2019-01-23 16:17:35 - [10.00.0007] PPSWUser(Users)[Full Access Role, Limited Access Role] - User assigned RADIUS attribute(s) (Filter-ID=compliant.in)
Info	ACT30610	2019-01-23 16:17:35 - [10.00.0007] PPSWUser(Users)[Full Access Role, Limited Access Role] - Cisco,Stop,Unknown,
Info	COA24753	2019-01-23 16:17:35 - [10.00.0007] PPSWUser(Users)[Full Access Role, Limited Access Role] - Session Deletion Disconnect Message sent to RADIUS Client Cisco for agent at 00-50-56-bf-55-4f has succeeded.
Info	AUT23524	2019-01-23 16:17:34 - [10.00.0007] PPSWUser(Users)[Full Access Role, Limited Access Role] - Roles for user PPSWUser on host 10.00.0007 changed from <Limited Access Role> to <Full Access Role, Limited Access Role> during policy reevaluation.
Info	AUT24803	2019-01-23 16:17:34 - [10.00.0007] PPSWUser(Users)[Limited Access Role] - Host Checker policy 'Firewall Policy' passed on host '10.00.0007' address '00-50-56-BF-55-4F' for user 'PPSWUser'.
Info	AUT24803	2019-01-23 16:17:34 - [10.00.0007] PPSWUser(Users)[Limited Access Role] - Host Checker policy 'Demo-SCCM-Policy' passed on host '10.00.0007' address '00-50-56-BF-55-4F' for user 'PPSWUser'.
Info	AUT24804	2019-01-23 16:17:13 - [10.00.0007] PPSWUser(Users)[Limited Access Role] - Host Checker policy 'Firewall Policy' failed on host '10.00.0007' address '00-50-56-BF-55-4F' for user 'PPSWUser' reason 'Rule-rule:Windows Firewall 8.3.9600.17415 does not comply with policy. Compliance requires firewall to be turned on.'

Verify the Switch for change of Filter-ID to compliant.

```

Interface: GigabitEthernet1/0/13
  IIF-ID: 0x11BB48C9
  MAC Address: 0050.56bf.554f
  IPv6 Address: Unknown
  IPv4 Address: Unknown
  User-Name: anonymous
  Status: Authorized
  Domain: DATA
  Oper host mode: multi-host
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: 0A190FCA0000029C7A2CAD96
  Acct Session ID: 0x00000010
  Handle: 0x1a000010
  Current Policy: POLICY_Gi1/0/3
Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
  Security Policy: Should Secure
  Security Status: Link Unsecured
Server Policies:
  Filter-ID: compliant
Method status list:
  Method      State
  dot1x      Authc Success
  
```

Appendix

CLI commands on Cisco Switch running 15.2.

```
#show configuration
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname myswitch
boot-start-marker
boot-end-marker
enable password Cisco
username admin privilege 15 secret 5 $1$mUVx$5lNk8ibYzrj4fyRtVPhb91
aaa new-model
aaa group server radius radiusgroup
  server name radiusserver
aaa authentication login default local
aaa authentication enable default enable
aaa authentication dot1x default group radiusgroup
aaa authorization network default group radiusgroup
aaa authorization auth-proxy default group radiusgroup
aaa accounting send stop-record authentication failure
aaa accounting update newinfo
aaa accounting identity default start-stop broadcast group radiusgroup
aaa accounting network default start-stop group radiusgroup
aaa server radius dynamic-author
  client 10.209.126.152 server-key 12345
  port 3799
  auth-type all
  ignore session-key
  ignore server-key
aaa session-id common
clock timezone IST 5 30
switch 1 provision ws-c2960x-24pd-l
ip dhcp snooping
ip domain-name pps.local
crypto pki trustpoint TP-self-signed-3051400704
```

```
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3051400704
revocation-check none
rsakeypair TP-self-signed-3051400704
crypto pki certificate chain TP-self-signed-3051400704
certificate self-signed 01 nvram:IOS-Self-Sig#1.cer
dot1x system-auth-control
dot1x test timeout 30
service-template webauth-global-inactive
  inactivity-timer 3600
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  voice vlan
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
  match result-type aaa-timeout
  match authorization-status authorized
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
  match result-type aaa-timeout
  match authorization-status unauthorized
class-map type control subscriber match-all DOT1X
  match method dot1x
class-map type control subscriber match-all DOT1X_FAILED
  match method dot1x
  match result-type method dot1x authoritative
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
  match authorizing-method-priority gt 20
class-map type control subscriber match-all DOT1X_NO_RESP
  match method dot1x
  match result-type method dot1x agent-not-found
class-map type control subscriber match-all DOT1X_TIMEOUT
  match method dot1x
  match result-type method dot1x method-timeout
class-map type control subscriber match-all MAB
  match method mab
```

```
class-map type control subscriber match-all MAB_FAILED
  match method mab
  match result-type method mab authoritative
policy-map type control subscriber POLICY_Gi1/0/2
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x priority 10
  event authentication-failure match-first
    5 class DOT1X_FAILED do-until-failure
      10 terminate dot1x
      20 authenticate using mab priority 20
    10 class DOT1X_NO_RESP do-until-failure
      10 terminate dot1x
      20 authenticate using mab priority 20
    20 class MAB_FAILED do-until-failure
      10 terminate mab
      20 authentication-restart 60
    40 class always do-until-failure
      10 terminate dot1x
    20 terminate mab
      30 authentication-restart 60
  event agent-found match-all
    10 class always do-until-failure
      10 terminate mab
      20 authenticate using dot1x priority 10
  event authentication-success match-all
    10 class always do-until-failure
      10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
policy-map type control subscriber POLICY_Gi1/0/3
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x priority 10
  event authentication-failure match-first
    5 class DOT1X_FAILED do-until-failure
      10 terminate dot1x
      20 authenticate using mab priority 20
    10 class DOT1X_NO_RESP do-until-failure
      10 terminate dot1x
```

```

20 authenticate using mab priority 20
20 class MAB_FAILED do-until-failure
  10 terminate mab
20 authentication-restart 60
40 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
event agent-found match-all
  10 class always do-until-failure
  10 terminate mab
  20 authenticate using dot1x priority 10
event authentication-success match-all
  10 class always do-until-failure
  10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
interface FastEthernet0
no ip address
interface GigabitEthernet1/0/1
interface GigabitEthernet1/0/2
description #####GUEST_ACCESS#####
switchport mode access
switchport port-security
authentication periodic
access-session host-mode single-host
access-session port-control auto
mab
dot1x pae authenticator
dot1x timeout tx-period 10
service-policy type control subscriber POLICY_Gi1/0/2
interface GigabitEthernet1/0/3
description #####802.1x#####
switchport mode access
switchport port-security
authentication periodic
authentication timer reauthenticate 43200
access-session host-mode single-host
access-session port-control auto
mab

```

```
dot1x pae authenticator
dot1x timeout tx-period 10
service-policy type control subscriber POLICY_Gi1/0/3
interface GigabitEthernet1/0/4
switchport access vlan 60
switchport mode access
authentication periodic
authentication timer reauthenticate server
access-session port-control auto
dot1x pae authenticator
spanning-tree portfast
interface GigabitEthernet1/0/5
interface Vlan1
ip address 10.209.216.96 255.255.255.0
ip default-gateway 10.209.126.254
ip http server
ip http secure-server
ip access-list extended PERMIT-ALL
permit ip any any
ip access-list extended RESTRICT-ALL
deny  udp any any eq domain
deny  ip any host 10.209.126.152
permit ip any any
ip radius source-interface Vlan1
!
snmp-server community public RO
snmp-server community private RW
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 30 tries 3
!
radius server radiusserver
address ipv4 10.209.226.152 auth-port 1812 acct-port 1813
key 12345
no vstack
line con 0
```

```
line vty 0 4
  transport input ssh
line vty 5 15
  transport input ssh
end
```