



Pulse Policy Secure: RADIUS Server Management Guide

Published

June 2020

Document Version

1.3

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

© 2020 by Pulse Secure, LLC. All rights reserved.

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.

Pulse Policy Secure: RADIUS Server Management Guide

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 <http://www.pulsesecure.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

RADIUS SERVER MANAGEMENT.....	1
RADIUS SERVER OVERVIEW.....	1
HOW TO ENABLE RADIUS SERVER.....	2
RADIUS FEATURES ADDED WITH A RADIUS LICENSE.....	2
SUPPORTED EAP TYPES	3
CONFIGURING A RADIUS SERVER	3
UPGRADING FROM A PS-PROFILERRADIUS-SM/MD/LG LICENSE TO PULSE POLICY SECURE	8
802.1X DEPLOYMENT USING PPS.....	11
SCENARIO 1: CORPORATE LAPTOP ON WIRED/WIRELESS NETWORK AND PERSONAL DEVICE ON WIRELESS NETWORK (CORPORATE ACCESS).....	11
SCENARIO 2: GUEST USERS ON WIRED/WIRELESS CONNECTIONS (ONLY INTERNET ACCESS)	12
SCENARIO 3: UNMANAGEABLE DEVICES ON WIRED/WIRELESS CONNECTIONS	13
SCENARIO 4: CORPORATE LAPTOP CONNECTING VIA PULSE SECURE CLIENT THROUGH THE INTERNAL FIREWALL	13
SCENARIO 5: CONTRACTORS CONNECT TO BUSINESS APPLICATIONS VIA CAPTIVE PORTAL/WEB AUTHENTICATION	14

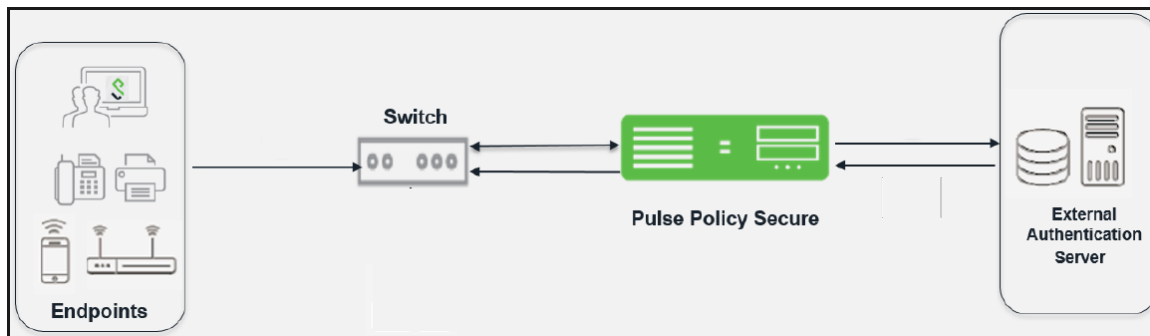
RADIUS Server Management

RADIUS Server Overview

RADIUS is an industry-standard protocol for providing authentication, authorization and accounting services.

- **Authentication** - Authentication is the process of verifying a user's identity and associating additional information (attributes) to the user's login session.
- **Authorization** - Authorization is the process of determining whether the user is allowed on the network and of controlling network access values based on a defined security policy.
- **Accounting** - Accounting is the process of generating log files that record session statistics to be used for billing, system diagnosis and usage planning.
- The following figure illustrates a simple RADIUS Environment.

Figure 1 Pulse Policy Secure Deployment as a RADIUS Server



A RADIUS-based remote access environment typically involves the following four types of components:

- **Access Client** - An access client is a user who initiates a network connection. An access client might be a user dialing in to a service provider network, a router at a small office or home office connecting to an enterprise network to provide network access, or a wireless client connecting to an 802.1X access point.
- **Network Access Device (NAD)** - A network access device (NAD), also called a RADIUS client, is a device that recognizes and processes connection requests from outside the network edge. A NAD can be a wireless access point, a modem pool, a network firewall, or any other device that authenticates users.
- **RADIUS Server** - The RADIUS server (in this case, the Pulse Policy Secure) matches data from the authentication and authorization request with information in a trusted database. If a match is found and the user's credentials are correct, the RADIUS server sends an Access-Accept message to the NAD. If a match is not found or if a problem is found with the user's credentials, the server returns an Access-Reject message. The NAD then establishes or terminates the user's connection. The NAD might also forward accounting information to the RADIUS server to document the transaction, and the RADIUS server might store or forward this information as needed to support billing for the services provided.

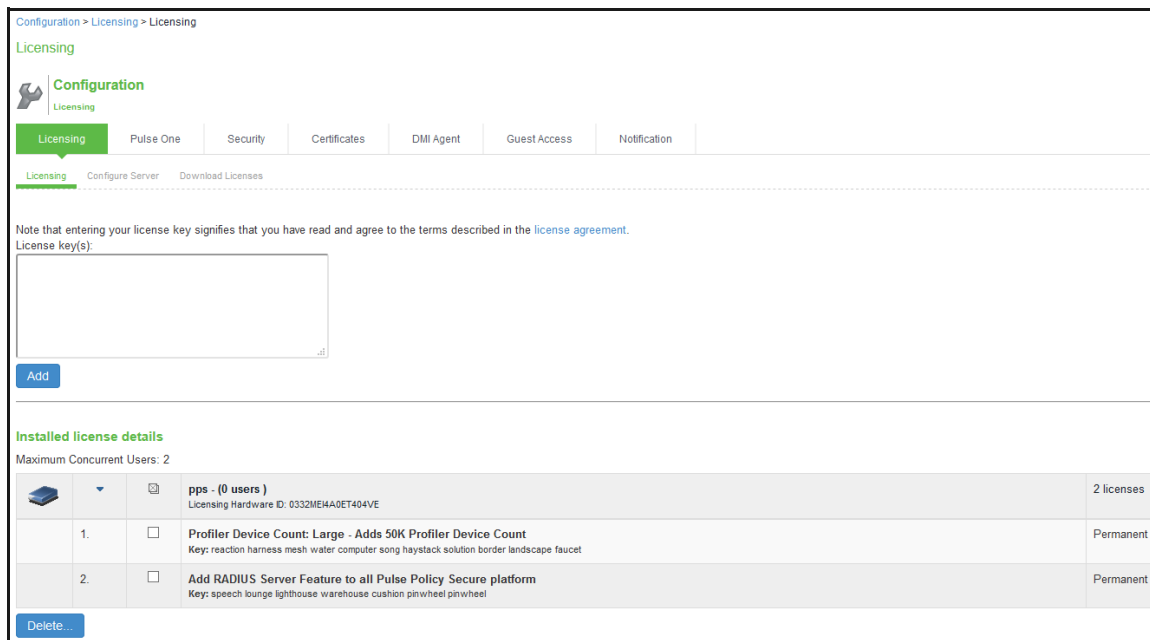
- Back-end Authentication Server - In some networks, a back-end authentication server, such as RSA or SecurID (an LDAP database) stores the information against which the authentication request is compared. In some cases, the back-end server passes information to the RADIUS server, which determines whether a match exists. In other cases, the matching is performed on the back-end server, which then passes 'accept' or 'reject' result to the RADIUS server.

How to enable RADIUS Server

A RADIUS license allows you to use the Pulse Policy Secure as a RADIUS server. Apply the PS-PROFILER-RADIUS-SM/MD/LG license to get the RADIUS server capability.

Note: The POLSEC license also enables RADIUS functionality.

To apply initial license or to upgrade license, select **System > Configuration > Licensing** in the left navigation pane.



The screenshot shows the 'Licensing' configuration page in the Pulse Policy Secure interface. The page has a breadcrumb trail: Configuration > Licensing > Licensing. Below the breadcrumb, there are tabs for 'Configuration', 'Licensing', 'Pulse One', 'Security', 'Certificates', 'DMI Agent', 'Guest Access', and 'Notification'. The 'Licensing' tab is active. Underneath, there are sub-tabs: 'Licensing', 'Configure Server', and 'Download Licenses'. A note states: 'Note that entering your license key signifies that you have read and agree to the terms described in the license agreement.' Below this is a text input field for 'License key(s)' and an 'Add' button. The 'Installed license details' section shows 'Maximum Concurrent Users: 2'. A table lists installed licenses:

Icon	License Name	License Key	Duration
	pps - (0 users) Licensing Hardware ID: 0332ME4A0ET404VE		2 licenses
1.	<input type="checkbox"/>	Profiler Device Count: Large - Adds 50K Profiler Device Count Key: reaction harness mesh water computer song haystack solution border landscape faucet	Permanent
2.	<input type="checkbox"/>	Add RADIUS Server Feature to all Pulse Policy Secure platform Key: speech lounge lighthouse warehouse cushion pinwheel pinwheel	Permanent

At the bottom left of the table is a 'Delete...' button.

As a RADIUS server, the Pulse Policy Secure receives the endpoint connection request, authenticates the user, and returns the configuration parameters required to provision the connection using RADIUS attributes. The Pulse Policy Secure can also serve as a proxy client to external RADIUS servers to offload authentication requests.

Note: You can upgrade to a fully functional PPS at any time in addition to an endpoint user license.

RADIUS Features added with a RADIUS License

When RADIUS server license is applied, the applicable Pulse Policy Secure screens become available. You can access most of the RADIUS configuration pages from the Network Access menu available in PPS category.

The following table describes the features available on the main RADIUS configuration pages:

Feature	Description
RADIUS Dictionary	The RADIUS server uses dictionary files to store lists of RADIUS attributes, to parse authentication and accounting requests and generate responses.
RADIUS Vendor	Vendor-specific dictionary files help for complete connections. The RADIUS server supports large number of NADs that use vendor-specific dictionary files.
Location Group	RADIUS location groups allow you to assign a sign-in policy to a user based on the NAD through which the user is connecting.
RADIUS Client	A RADIUS client is a network device or software application that contacts the RADIUS server to authenticate a user or to record accounting information about a network connection.
RADIUS Attributes	<ul style="list-style-type: none"> • Return Attributes: RADIUS return attributes specify the return list attributes to an 802.1X NAD. • Request Attributes: RADIUS request attributes enforce the ability to process authentication requests based on information in the RADIUS packet before a connection can be authenticated. You assign RADIUS request attribute policies as a realm restriction. • Attribute Logging: RADIUS attribute logging allows you to enable or disable authentication reporting for RADIUS authentication events.

Supported EAP Types

The RADIUS server supports all EAP types and supplicants supported by the full-feature PPS product except EAP-JUAC. EAP-JUAC is the proprietary protocol used by the clients. For a list of supported authentication protocols, see RADIUS Server.

Configuring a RADIUS Server

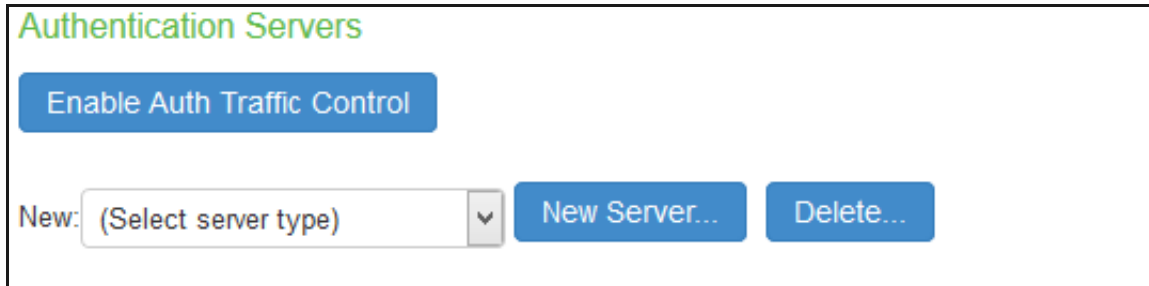
This topic describes the features that are enabled when the PS-PROFILER-RADIUS-SM/MD/LG license is applied.

Follow the below mentioned steps to configure a RADIUS server:

1. Configure an Authentication Server

Authentication and authorization servers authenticate user credentials and determine user privileges within the system. PPS is preconfigured with one local authentication server (System Local) to authenticate users and one local authentication server (Administrators) to authenticate administrators. You must add users either to the local authentication server or to external authentication servers.

Figure 2 Authentication Server



The configuration page is shown below.

Settings

Settings | Users | Troubleshooting

Base Configuration

- Name: Label to reference this server
- Domain: NetBIOS name of the domain
- Kerberos Realm: Specifies the Kerberos realm of the Active Directory domain. It is usually set to the DNS name of the Active Directory domain. Example "xyz.net", "abc.com"

Domain Join Configuration

- Username: Active Directory administrator credentials are required in order for the Pulse Policy Secure to join the domain or whenever certain fields
- Password:
 - Save credentials If this setting is not enabled, the credentials entered will be destroyed after successfully joining the domain.
- Container Name: Container path in Active Directory to create the machine account in. Changing this field will trigger domain rejoin. In the case of nested co
- Computer Name: Machine account name (do not include "?")

Domain Join Status: ●

Click 'Update Join' to get the latest join status of node(s). If any node's domain join status is other than GREEN (persistently) then click 'Reset Join' button of that node to reinitiate domain join process. NOTE: 'Reset Join' process ensure that it is not caused by network issues. If domain join status is shown RED due to network issues then it has high chances of coming back to GREEN after network recovers.

Additional Options

Authentication protocol
Specify the protocol to use during authentication.

- Kerberos
Most secure; required for Kerberos Single Sign-On (SSO) and SPNEGO
- Enable NTLM protocol
Required for password management. Authentication attempts Kerberos first, then the following protocol:
 - NTLMv2 moderately secure; required for machine authentication and MSCHAP-V2 based 802.1x authentication protocols
 - NTLMv1 less secure; may be required for legacy servers; MSCHAP-based servers; MSCHAP based 802.1x authentication protocols

Trusted domain lookup
Enable this option to fetch user group information from the trusted domains. User login time may increase as the number of trusted domains and network latency to those domain controllers increase. Even if disabled, p

Contact trusted domains

Domain Connections
Specify the maximum number of simultaneous connections that can be opened to the domain controller of a domain. Multiple connections may give better performance and scalability, but higher values could also degrad

Maximum simultaneous connections per domain: 1-10

SPNEGO Single Sign On
The keytab's SPN must be added to the AD Server and should match the FQDN used to access this device.

Enable SPNEGO

Machine account password change
Changes Pulse Policy Secure's domain machine account password.

Enable periodic password change of machine account

Active Directory Selection

2. Define an Authentication Realm

Authentication realms contain policies specifying conditions the user or administrator must meet to sign in to the Pulse Policy Secure. When configuring an authentication realm, you must create rules to map users to roles and specify which server (or servers) the Pulse Policy Secure must use to authenticate and authorize realm members.

Figure 3 Authentication Realm

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

User Realms > Users > 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

3. Define Sign-In Policy

A sign-in policy defines which URL and realm(s) that the user will have access to. This is configured in Signing-in > Sign-in Policies > New URL. Select a Sign-in URL (Example: */radius), a sign-in page, and choose an available realm with an authentication protocol set.

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: To create or manage pages, see [Sign-in pages](#).

Authentication realm

Specify what realms will be available when signing in.

[Delete](#) [↑](#) [↓](#)

	Available realms	Authentication protocol set	
<input type="checkbox"/>	<input type="text" value="Cert Auth"/>	<input type="text" value="- Not applicable -"/>	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 signin policy for Guest and Guest admin to use specific pages.

Configure SignIn Notifications

Pre-Auth Sign-in Notification

Post-Auth Sign-in Notification

[Save Changes](#)

4. Create User Role

Roles define user session parameters or agent options. The Pulse Policy Secure is preconfigured with one user role (Users) and two administrator roles (Administrators and Read-Only).

Figure 4 User Role

User Roles > New Role

New Role

Name:

Description:

▼ Options

Session and appearance options are specified in [Default Options](#). Check the following if this role should override these defaults.

- Session Options
- UI Options
- Odyssey Settings for Access
- Odyssey Settings for Preconfigured Installer
- Enable Guest User Account Management Rights
- Enable Sponsored Guest User Account Management Rights

5. Create a RADIUS Client

Select **Endpoint Policy > Network Access > RADIUS Client > New RADIUS Client**. Enter a name for the policy, the IP address of the client, an IP address range (optional), the shared secret, the make/model of your client, and your location group.

Figure 5 RADIUS Client

The screenshot shows the 'RADIUS Client' configuration page for a client named 'Cisco'. The page includes the following fields and options:

- Name:** Cisco (required field)
- Description:** (empty text area)
- IP Address:** (empty text field)
- IP Address Range:** 1 (required field)
- Shared Secret:** (password field)
- Make/Model:** Cisco Systems (dropdown menu)
- Key Wrap:** (checkbox, unchecked)
- Location Group:** Default (dropdown menu)
- Dynamic Authorization Support:**
 - Support Disconnect Messages: (checked)
 - Support CoA Messages: (unchecked)
 - Dynamic Authorization Port: 3799 (text field)

A 'Save Changes' button is located at the bottom left. A note at the bottom left states '* indicates required field'.

6. Configure RADIUS Return Attribute Policies

Define specific return attributes to your switch and/or access point. It is often used to assign client to a specific VLAN. Select Endpoint Policy > Network Access > RADIUS Return Attribute Policies. Click New Policy. Enter the policy name, assign a location group, assign the attributes to be returned from a list, specify the interface and the user role.

Figure 6 RADIUS Return Attribute Policy

The screenshot shows the 'RADIUS Return Attributes' configuration page. It includes a navigation bar with tabs for RADIUS Dictionary, RADIUS Vendor, Location Group, RADIUS Client, RADIUS Attributes (selected), Network Infrastructure Device, and SNMP Enforcement Policies. Below the navigation bar, there are sections for 'Return Attributes', 'Request Attributes', and 'Attribute Logging'. A dropdown menu shows 'Show policies that apply to: All roles' with an 'Update' button. A note explains that a RADIUS return attributes policy specifies the return list attributes to send to an 802.1X network access device. Below this, there are buttons for 'New Policy', 'Duplicate', 'Delete', and 'Save Changes'. A table lists the configured policies:

	Policies	ACL Settings	Attributes	Location Group	Interface	Applies to role
<input type="checkbox"/>	1. full_access_policy	N/A	VLAN=64	Default	N/A	Full access role
<input type="checkbox"/>	2. rem_policy	N/A	VLAN=65	Default	AUTO	Limited Access role

Upgrading from a PS-PROFILERRADIUS-SM/MD/LG License to Pulse Policy Secure

To upgrade from a PS-PROFILERRADIUS-SM/MD/LG license to a full-featured PPS system, add a valid POLSEC user license to the system. Once the license is added, all PPS features become available. Profiler license has to be applied separately for network visibility.

After upgrading to PPS, review the system configuration. For example, for realms and roles, more features are available now. Default settings are automatically assigned to those features after the upgrade, and make sure that those default settings are appropriate for your system. Also, authentication protocol sets can support EAP-JUAC after you add the PPS license. Therefore, consider updating configured authentication protocols sets to include EAP-JUAC for concurrent user sessions.

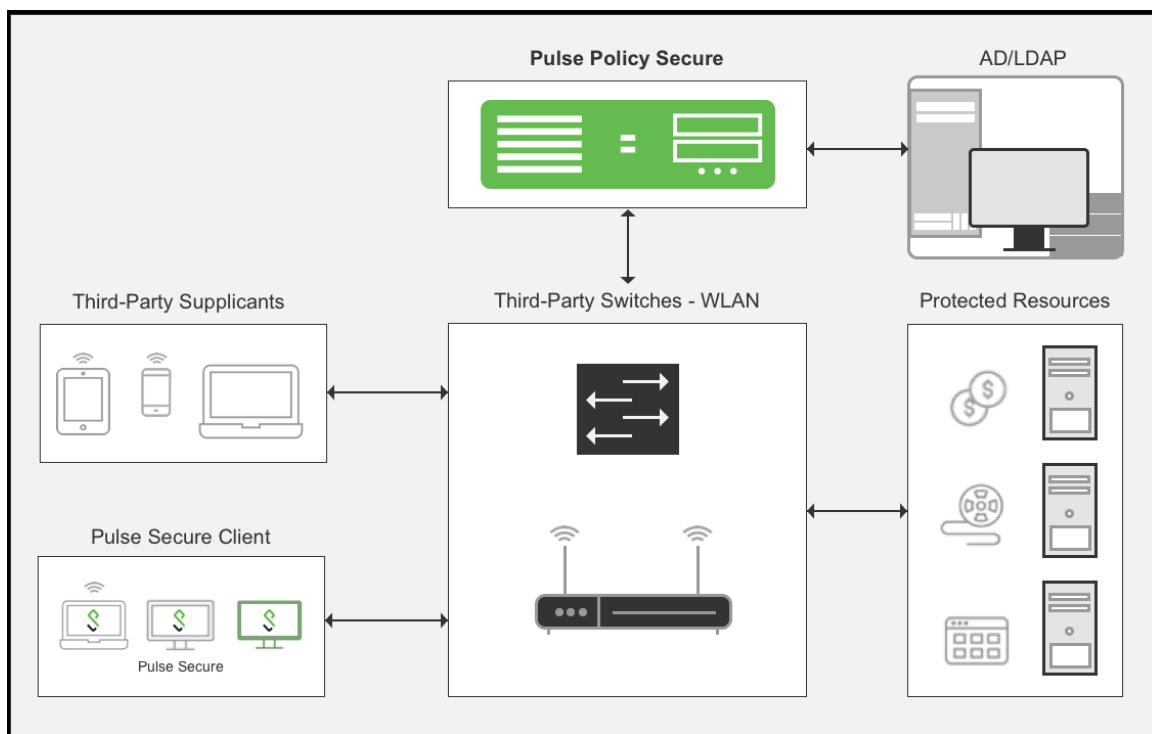
802.1X Deployment using PPS

PPS supports a variety of 802.1X open standard based NAC deployments which increases transparency and offers true customer choice.

Pulse Secure's focus is on allowing users to simply and securely connect, and ensuring a consistently high quality of experience. End user intervention is minimized at every step, making the process easy even as it becomes more secure.

Scenario 1: Corporate Laptop on Wired/Wireless Network and personal device on Wireless Network (Corporate Access)

Figure 7 Access Control at Layer 2 (802.1X)



In our first scenario, an employee, Joe, wants to access the office network resources using his corporate laptop by connecting to either corporate wired or wireless network. Joe may also want to access the Internet on his personal mobile phone using office wireless network while he is away from the laptop.

When Joe's corporate laptop is connected to the office wired/wireless network, it is connected to a Switch/WLC that is 802.1X enabled. User authentication is done by exchanging the credentials in an encrypted TLS tunnel (EAP-TTLS). Host Checker information is collected by the Pulse client and then sent to PPS inside a proprietary EAP-JUAC protocol. PPS first performs a host check to ensure that Joe's laptop is healthy and complies with the corporate security policies. If Joe's device is deemed healthy and compliant. If not, Joe's device may be quarantined and could be subject to automatic or manual remediation, depending on the situation or issue. Once Joe's device passes the host check, PPS communicates with AD server for authentication and

authorization. Based on the User Role assigned to Joe in AD, the PPS sends the RADIUS attributes back to the Switch. The attributes could be a VLAN ID, a filter ID (ACL), or other attributes. The Switch port is opened, and Joe has access to network resources. After getting the access to the network, Pulse client installed on Joe's laptop creates a L3 connection directly with PPS and periodically monitors the device health and provides this information to the PPS. If Joe's laptop becomes non-compliant at any point, Pulse Secure client shares this information with the PPS and server either disconnects the device by sending RADIUS disconnect or quarantines it by sending RADIUS CoA depending on the corporate policy.

In the personal mobile phone scenario, the process works a little differently. As the device is owned by Joe, the entire 802.1X authentication process is done using the mobile phone's native 802.1X supplicant. In this scenario, the WLC acts as the authenticator and the PPS server functions as the RADIUS server. The PPS receives the authentication and authorization information from the backend AD server, and pushes the appropriate policy rules to the WLAN controller. The compliance check can be done using integration with MDM/EMM such as Pulse WorkSpace (PWS), Airwatch, MobileIron, and Microsoft Intune.

How does Pulse Secure Client add value when compared with native/third-party 802.1X supplicant?

Host Check Prior to Authentication (Pre-admission Control)

In the first scenario, the Pulse Secure client delivered a full host check, before Joe could enter his credentials. Pulse Secure host checker functionality includes patch assessment/remediation, check for viruses, malware, and other threats before switch or WLAN controller ports are opened. This allows IT admin to ensure that an infected device has no connectivity to the Dynamic Host Configuration Protocol (DHCP) server or any other resource in the data center or on the network prior to the completion of host check. Pulse Secure provides these capabilities via a proprietary EAP-JUAC plug-in.

Layer 2 and Layer 3 Access Control via SSO

Using Pulse Secure client, the enterprise users can deploy 802.1X based access control such as VLAN or filter assignments at Layer 2, and provide more granular Layer 3-based access control through next-generation firewalls (For example, Juniper SRX, Checkpoint, Fortinet or Palo Alto Networks Firewall). Once the PPS authenticates the user, these credentials are cached on the Pulse Secure client. Once the Switch/WLAN controller opens the port and the device is part of the corporate domain appropriate to the user's role, the relevant resource access policies for the user will be pushed to the firewall to access protected resources. This entire process is transparent to the end user, and can be achieved with a single sign-on (SSO) from the end user's perspective.

Scenario 2: Guest Users on Wired/Wireless Connections (Only Internet Access)

In this scenario, Lisa, a guest user needs Internet access by connecting to either wired switch port or wireless access point.

When Lisa launches a web browser, the Switch or WLAN controller sends an HTTP redirect to PPS, also called a captive portal. PPS launches an authentication page to Lisa's browser through the captive portal solution. Once the user enters the guest credentials, the PPS authenticates the user locally and sends appropriate access control rules to the Switch or WLAN controller. In this case, the guest user role limits Lisa's access only to Internet and access to other corporate resources is restricted.

Scenario 3: Unmanageable Devices on Wired/Wireless Connections

This scenario occurs when an unmanageable device such as an IP enabled phone, printer, or fax machine is connected to the network. If PPS is deployed the device simply connects to a Switch port, joins the domain, and starts providing services to the network.

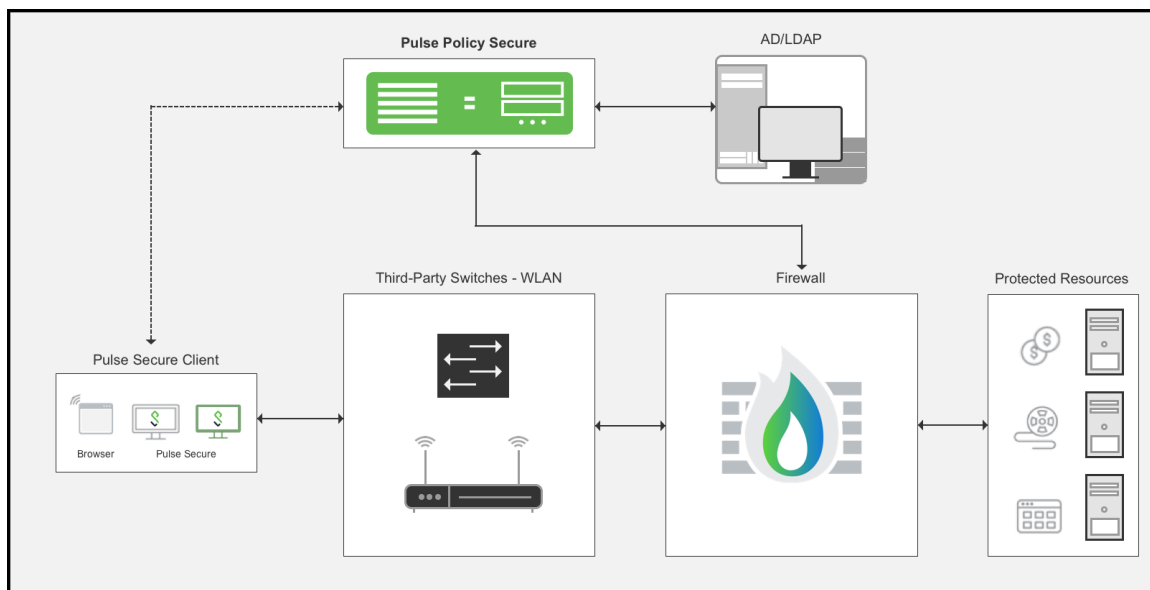
When unmanageable devices are connected, a Media Access Control (MAC) request comes to PPS from the Switch or WLAN device. The PPS authenticates the unmanageable device through the MAC authentication bypass (MAB) mechanism.

In addition, PPS pushes appropriate access control rules to Switches, WLAN controllers, and next-generation firewalls (For example, Juniper SRX, Checkpoint, or Palo Alto Networks Firewall) based on device profiling through Pulse Profiler. Security is achieved using standard-based Lightweight Directory Access Protocol (LDAP) between the PPS and unmanageable third-party devices.

See [MAC Address Authentication with Profiler configuration guide](#) for more details.

Scenario 4: Corporate Laptop Connecting via Pulse Secure Client through the Internal Firewall

Role Based Access Control at Firewall



In this scenario, Pat, a marketing employee, is connecting from his office to access the Business Objects applications that he is authorized to access.

In this scenario, Pat is trying to access a mission critical application protected by a firewall. The administrator can create an access policy, tying user roles to policy—for example, only users in a marketing role can access the Business Objects networked application. Note that this policy is created during initial setup configuration.

The first step is to perform a full host check to ensure that the device meets corporate policy. Next, the PPS talks to the AD server to perform authentication and authorization. When AD confirms that Pat is part of the marketing organization, and the role is pushed to the firewall along with the device IP. The firewall maps Pat to a specific resource access policy based on this role information and enables to access the applications.

The integration between PPS and third-party next-generation firewalls (Currently supported are Juniper SRX Series, Palo Alto Networks Firewall, Check Point Firewall, and Fortinet) built security ecosystem for heterogeneous networks. When combined with PPS, the firewall becomes identity-aware to enforce application security policies per user and role basis, and meets compliance regulations. This delivers fine grained access control that is easily managed from a central location. It also enables IT admin to extend NAC BYOD at the perimeter level to offer end-to-end secure access.

Scenario 5: Contractors Connect to Business Applications via Captive Portal/Web Authentication

In this scenario, Dave, a contractor who doesn't have the Pulse Secure client on his device, needs to get access to the Internet and some protected applications from inside the corporate office.

In this scenario, Dave's access to the Internet from the corporate office is protected through a Firewall. As we have seen in the previous scenario, user roles are sent from PPS to the firewall. The administrator has created an access policy for contractors, allowing them access only to the Internet and a few restricted applications.

When Dave launches his browser, the request comes to the firewall, which does an HTTP redirect to the PPS. Before authentication, a host check is performed to ensure that Dave's device meets minimum corporate security standards. PPS hosts a login page on the browser and asks Dave to authenticate. Dave presents his credentials, and PPS pushes an access control list to the firewall. Dave is now allowed to access Internet and gets access to a few corporate applications.

All firewall policies can be constructed with user and role information. For example, a user within the "Sales" role can access sales data, as opposed to a user within the "Engineering" role who can access a build server.