



Pulse Policy Secure

Multi Factor Authentication with Duo

Configuration Guide

Product Release	9.0R1
Document	1.0
Published	May 2018

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.

Multi Factor Authentication with Duo

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.”

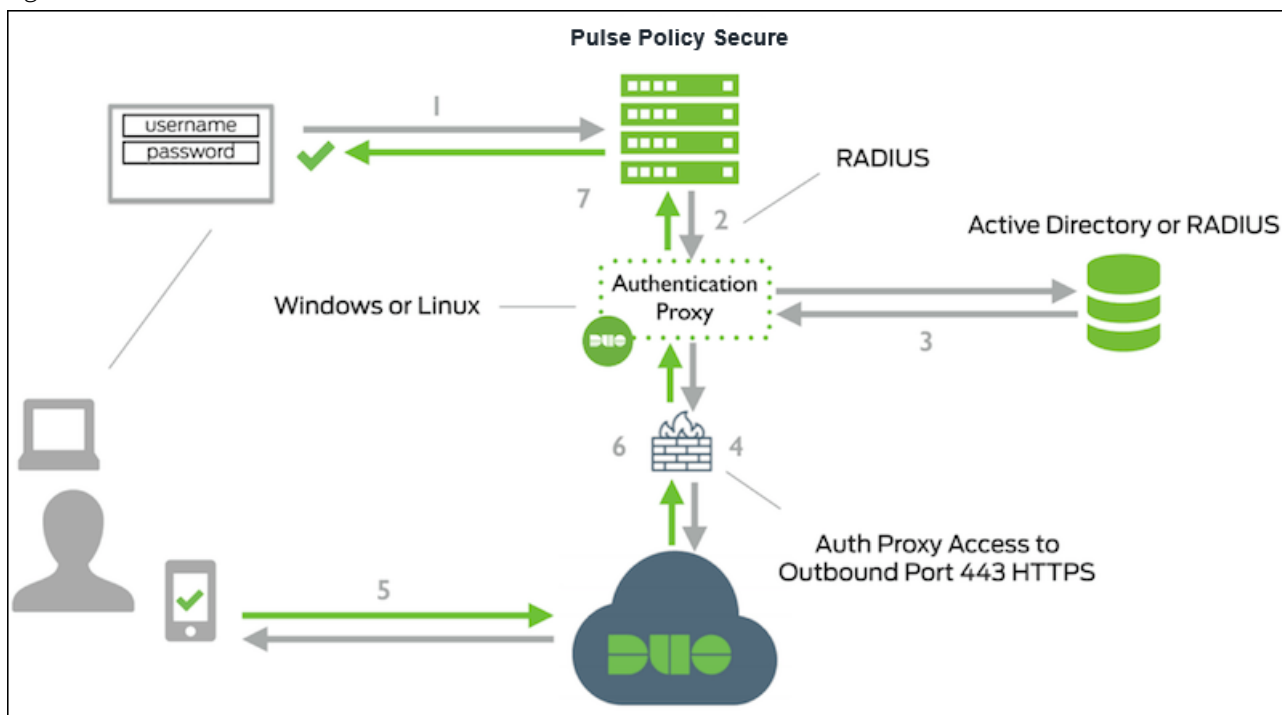
Introduction

Multi-factor authentication (MFA) adds a layer of security that allows companies to protect against the leading cause of data breach, which happens through compromised credentials. The MFA adds additional security where users must provide extra information or factors for authentication before accessing corporate applications, networks, and servers.

PPS integration with Duo security adds two-factor authentication to PPS login. It uses a combination of primary username and password along with secondary authentication based on push-notification approval to a mobile device or phone call or other supported authentication methods through Duo Security.

This document explains how PPS integrates with Duo Security to add two-factor authentication to PPS login.

Figure 1: Overview



1. Primary authentication is initiated to PPS.
2. PPS sends authentication request to Duo Security's authentication proxy.
3. Primary authentication is performed using Active Directory or RADIUS.
4. Duo authentication proxy connection is established to Duo Security over TCP port.
5. Secondary authentication through Duo Security's service.
6. Duo authentication proxy receives authentication response.
7. PPS access is granted.

Configuration

The goal is to configure two-factor authentication using RADIUS/AD as a Primary authentication server with Duo Security as a Secondary authentication server. It explains how to integrate MFA solution into the existing 802.1X connections and how-to setup the MFA realm.

This use case involves the following configuration:

- [Configuring Duo RADIUS Proxy](#)
- [Configuring Duo Security](#)
- [Configuring PPS](#)

Configuring Duo RADIUS Proxy

1. Install the [Duo Authentication Proxy](#) on Windows or Linux server and configure the authproxy.cfg file.

Location of the configuration file.

```
Windows (64-bit): C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg  
Linux: /opt/duoauthproxy/conf/authproxy.cfg
```

2. Configure the Proxy for Primary Authentication.

If you have only RADIUS authentication server for primary authentication, then modify the authproxy.cfg file with below command. For example:

```
[radius_client]  
host=1.2.3.4  
secret=radiusclientsecret
```

If you have want to use Active Directory for primary authentication, then modify the authproxy.cfg file with below command. For example:

```
[ad_client]  
host=1.2.3.4  
host_2=1.2.3.5  
service_account_username=duoservice  
service_account_password=password1  
search_dn=DC=example,DC=com  
security_group_dn=CN=DuoVPNUsers,OU=Groups,DC=example,DC=com
```

3. Setup the Authentication Proxy to work with PPS.

Example configuration for AD.

```
[radius_server_auto]  
ikey=DXXXXXXXXXXXXXXXXXXXXX  
skkey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
api_host=api-XXXXXXX.duosecurity.com  
radius_ip_1=5.6.7.8  
radius_secret_1=radiussecret1  
client=ad_client  
port=1812  
failmode=safe
```

Configuring Duo Security

1. Signup for a Duo account. Log in to the [Duo Admin Panel](#) and navigate to Applications.
2. Click Protect an Application and locate Juniper UAC (Older name for Pulse Policy Secure) in the applications list. Click Protect this Application to get your integration key, secret key, and API hostname.
3. Add the RADIUS server in PPS.
4. Configure a user realm in PPS.

Note: This configuration applies to a RADIUS based MFA solution with Duo Security configured as a Secondary authentication server.

Configuring PPS

The configuration involves adding a RADIUS Server profile and then configuring a user realm.

1. From the PPS Admin console, navigate to **Authentication > Auth. Servers**.
2. Select **RADIUS Server** from the **Auth Server Type** list, click **New Server**.
3. In the **Name** field, enter **Duo-Proxy-RADIUS**.
4. Under the **Primary Server** section, enter the following information:
 - a. The IP address of your Duo Authentication Proxy.
 - b. The RADIUS secret shared with your Duo Authentication Proxy.
 - c. 1812 (or whichever port specified in your authproxy.cfg file).

Figure 2: RADIUS server

The screenshot shows the Pulse Secure Admin console interface for configuring a new RADIUS server. The breadcrumb trail is 'Auth Servers > New RADIUS Server'. The main heading is 'New RADIUS Server'. The configuration form includes the following fields:

- *Name:** Duo_Proxy_RADIUS (Label to reference this server.)
- NAS-Identifier:** (Name of the device as known to RADIUS server)
- Primary Server** (expanded section):
 - *RADIUS Server:** 1.2.3.4 (Name or IP address)
 - *Authentication Port:** 1812
 - *Shared Secret:** (masked with dots)
 - *Accounting Port:** 1813 (Port used for RADIUS accounting, if applicable)
 - NAS IPv4/IPv6 Address:** (IPv4/IPv6 address)
 - *Timeout:** 30 seconds
 - *Retries:** 0
- Users authenticate using tokens or one-time passwords

5. Configure User Realm for the Duo RADIUS server, navigate to **Users > User Realms** select **Duo-Proxy-RADIUS** (or whatever you named your new RADIUS server) in the Authentication drop-down.

Figure 3: Authentication Realm

The screenshot shows the Pulse Secure web interface for configuring a User Realm. The breadcrumb trail is "User Realms > Duo_Users > General". The "General" tab is active, with sub-tabs for "General", "Authentication Policy", and "Role Mapping".

Name: Duo_Users (Label to reference this realm)

Description: [Empty text area]

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:	<input type="text" value="Duo_Proxy_RADIUS"/>	Specify the server to use for authenticating users.
User Directory/Attribute:	<input type="text" value="Same as above"/>	Specify the server to use for authorization.
Accounting:	<input type="text" value="None"/>	Specify the server to use for Radius accounting.
Device Attributes:	<input type="text" value="None"/>	Specify the server to use for device authorization.
RADIUS Proxy:	<input type="radio"/> Proxy Outer Authentication <input type="radio"/> Proxy Inner Authentication <input checked="" type="radio"/> Do not proxy	Proxy EAP messages to the Authentication server.

6. Click **Save Changes**.

Conclusion

You should now be able to properly authenticate devices based on the primary and secondary authentication server.

For troubleshooting you can verify the user access logs.

Figure 4: User Access Logs

The screenshot shows the Pulse Secure web interface. The top navigation bar includes: System, Authentication, Administrators, Users, Endpoint Policy, Maintenance, and Wizards. The breadcrumb trail is: Log/Monitoring > User Access > Logs. The main content area is titled 'User Access Logs' and includes a filter bar with options: Events, User Access (selected), Admin Access, Sensors, Client Logs, SNMP, Statistics, and Advanced Settings. Below the filter bar, there are tabs for Log, Settings, and Filters. The main content area displays a table of log entries with columns for Severity, ID, and Message. The table shows two entries: one for 'Agent login succeeded' and one for 'Primary authentication successful'.

Severity	ID	Message
Info	AUT24414	2017-11-27 16:19:27 - ic - [172.21.16.210] kajalr(Users)[Users] - Agent login succeeded for kajalr@leers from [172.21.16.210] with Pulse-Secure/8.2.6.977 (Windows 10) Pulse/5.2.6.977.
Info	AUT24326	2017-11-27 16:19:27 - ic - [172.21.16.210] kajalr(Users)[] - Primary authentication successful for kajalr@Duo-Proxy from 172.21.16.210