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

Pulse Secure, Pulse and Steel-Belted Radius are registered trademarks of Pulse Secure, LLC in the United States and other countries. The Pulse Secure Logo, the Pulse logo, and PulseE are trademarks of Pulse Secure, LLC. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

Products made or sold by Pulse Secure or components thereof might be covered by one or more of the following patents that are owned by or licensed to Pulse Secure: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Pulse Policy Secure Getting Started Guide for PSA Series Appliances
Revision History
2018—Revised for Pulse Policy Secure

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. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.
# Table of Contents

**INSTALLATION, CONFIGURATION AND START-UP PROCEDURE** ................................................................. 4  
**INTRODUCTION TO PULSE POLICY SECURE** ......................................................................................... 4  
  Step 1: Installing the Hardware .............................................................................................................. 5  
  Step 2: Performing Basic Setup using Serial Console .......................................................................... 6  
  Step 3: Downloading Pulse Policy Secure Software and License .......................................................... 7  

**PULSE POLICY SECURE CONFIGURATION** ......................................................................................... 11  

**INITIAL SETUP WIZARD CONFIGURATION** ....................................................................................... 11  
  **STEP 1: BASIC SETTINGS** .................................................................................................................. 12  
  Step 1.1: Configuring System Date and Time ......................................................................................... 12  
  Step 1.2: Configuring License ............................................................................................................... 13  
  **STEP 2: CONFIGURING PROFILING FOR NETWORK VISIBILITY** .................................................. 14  
  **STEP 3: CONFIGURING LAYER 2 ENFORCEMENT** ....................................................................... 16  
  Step 3.1: Importing Configurations from Pulse Connect Secure ........................................................... 18  
  Step 3.2: Configure Authentication Server ........................................................................................... 19  
  Step 3.3: Define the Roles and the AD/LDAP group ........................................................................... 19  
  Step 3.4: Configure Compliance Check ............................................................................................... 19  
  **STEP 4: CONFIGURE GUEST AUTHENTICATION** .............................................................................. 21  
  **STEP 5: VERIFICATION AND TROUBLESHOOTING** .................................................................... 23  

**MANUAL INITIAL CONFIGURATION** ................................................................................................. 24  
  **STEP 1: CONFIGURING PULSE SECURE PROFILER** ...................................................................... 24  
  Step1.1: Discover devices using DHCP ............................................................................................... 24  
  Step1.2: Discover devices using SNMP ................................................................................................ 24  
  **STEP 2: CONFIGURING PPS** ............................................................................................................ 25  

**REQUESTING TECHNICAL SUPPORT** ............................................................................................... 27  
  **OPENING A CASE WITH PSGSC** .................................................................................................... 27
Installation, Configuration and Start-Up Procedure

Thank you for choosing Pulse Policy Secure, one of the leading network and access control (NAC) and BYOD solution for enterprises.

Introduction to Pulse Policy Secure

Pulse Policy Secure is a network access control (NAC) solution which provides network access only to authorized and secured users and devices. It protects your network and guards mission critical applications and sensitive data through comprehensive NAC management, visibility, and monitoring.

You can install Pulse Policy Secure and start configuring your system using the following easy steps:

- **Step 1: Installing the Hardware**
- **Step 2: Performing Basic Setup using Serial Console**
- **Step 3: Downloading Pulse Policy Secure Software and License**

**Note:** After installing and setting up Pulse Policy Secure, refer to the Initial Configuration task guide in the administrator Web console to install the most current Pulse Policy Secure software, license your Pulse Policy Secure appliance, and create a test user to verify user accessibility. To test initial setup and continue configuring Pulse Policy Secure, refer to the “Initial Verification and Key Concepts” section of the Pulse Policy Secure Administration Guide.

To download a PDF version of the Pulse Policy Secure Administration Guide and other related documents, go to the Pulse Policy Secure Product Documentation page at: https://www.pulsesecure.net/techpubs/pulse-policy-secure/pps.
Step 1: Installing the Hardware

The PSA Series appliances chassis can be mounted in a rack for secure storage and use.

Figure 1: PSA Series Appliances

For unpacking instructions, mounting instructions, and precautions, refer to the appliance's Hardware Guides at: https://www.pulsesecure.net/techpubs/pulse-appliances.

Next, connect the included cables and power on the PSA Series appliances following these steps:

1. On the front panel:
   a. Connect an Ethernet cable from one of the Ethernet ports on the device to a Gigabit switch port set to 1000BaseTX. DO NOT use auto-select on either port.
      Once you apply power to the device, the port uses two LEDs to indicate the connection status.
   b. Connect a laptop or external monitor and keyboard to the appliance.

2. On the rear panel, plug the power cord into the AC receptacle. There is no on/off switch on Pulse Policy Secure.
   Once you plug the power cord into the AC receptacle, Pulse Policy Secure powers up.

Hardware installation is complete after you rack-mount the appliance and connect the power, network, and serial cables. The next step is to connect to the appliance's serial console as described in “Step 2: Performing Basic Setup".
Device Status LED Behavior

Startup takes approximately one minute to complete. If you want to turn the device off and on again, we recommend you wait a few seconds between shutting it down and powering it back up.

There are three device status LEDs located on the front panel:

- Power
- Hard disk access
- Information/Fault

Table 1 lists the name, color, status, and description of each device status LED.

<table>
<thead>
<tr>
<th>Name</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POWER</td>
<td>Green</td>
<td>Off</td>
<td>Device is not receiving power</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On Steady</td>
<td>Device is receiving power</td>
</tr>
<tr>
<td>HARD DISK ACCESS</td>
<td>Yellow</td>
<td>Off</td>
<td>Hard disk is idle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blinking</td>
<td>Hard disk is being accessed</td>
</tr>
<tr>
<td>FAULT</td>
<td>Red</td>
<td>Off</td>
<td>Device is operating normally</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Slow blinking</td>
<td>Power supply fault</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fast blinking</td>
<td>Fan failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Solid</td>
<td>Thermal failure</td>
</tr>
</tbody>
</table>

Step 2: Performing Basic Setup using Serial Console

After the initial boot up, you need to enter basic network and machine information through the serial console to make the appliance accessible to the network.

During this basic setup process, you also define the appliance to act as a Pulse Connect Secure. You can switch this to act as a Pulse Policy Secure device at any time by reconfiguring the appliance.

Note: Installation process may take up to 20 minutes.

To do the basic set up:

1. Configure a console terminal or terminal emulation utility running on a computer, such as HyperTerminal or PuTTY, to use these serial connection parameters. These defaults are usually set already, but check them if there are connection problems:
   - 9600 bits per second
   - 8-bit no parity (8N1)
   - 1 stop bit
   - No flow control
2. Connect the terminal or laptop to the serial cable plugged in to the appliance's console port and press Enter until you are prompted by the initialization script.
3. Enter y to proceed and then y to accept the license terms (or r to read the license first).
4. Follow the directions in the serial console and enter the machine information for which you are prompted, including the:
   - IP address of the internal port (you configure the external port through the administrator Web console after initial configuration)
   - Network mask
   - Default gateway address
   - Primary DNS server address
   - Secondary DNS server address (optional)
   - Default DNS domain name (for example, acmegizmo.com)
- WINS server name or address (optional)
- Administrator username
- Administrator password
- REST API Access
- Common machine name (for example, connect.acmegizmo.com)
  Organization name (for example, Acme Gizmo, Inc.)

ℹ️ **Note:** Pulse Policy Secure uses the common machine and organization names to create a self-signed digital certificate for use during product evaluation and initial setup.

We strongly recommend that you import a signed digital certificate from a trusted certificate authority (CA) before deploying Pulse Policy Secure for production use.

5. In a browser, enter the machine’s IP address followed by “/admin” to access the administrator sign-in page. The URL is in the format: https://a.b.c.d/admin, where a.b.c.d is the machine’s IP address you entered in step 4.

6. When prompted with the security alert to proceed without a signed certificate, click Yes. When the administrator sign-in page appears, you have successfully connected your Pulse Policy Secure appliance to the network.

7. On the sign-in page, enter the administrator user name and password you created in step 4 and then click Sign In. The administrator Web console opens to the System > Status > Overview page.

### Step 3: Downloading Pulse Policy Secure Software and License

Pulse Policy Secure software and Pulse Policy Secure software include a Pulse Secure Licensing and Software Download Center @ [https://my.pulsesecure.net](https://my.pulsesecure.net) that lets you configure a Pulse Policy Secure appliance as a license server. This license server allows administrators to view all configured systems and lease licenses to the other appliances in the network as needed.

Alternatively, you can install and manage licenses directly on each device and eliminate the license server entirely. Your company’s needs and requirements dictate which configuration is best for you.

#### Obtain Licenses

You must access the Pulse Secure Licensing and Software Download Center at https://my.pulsesecure.net, provide your licensing hardware ID and serial number to obtain your license keys, and sign in to the admin console to enter the license keys you receive from Pulse Secure.

1. Log in to [https://my.pulsesecure.net](https://my.pulsesecure.net)
2. Under Pulse Secure Centers, click on **Licensing and Download Center**.

3. From the My Assets page, select **Show All** from the Filter by Account drop-down list.
4. In the **Authorization Code** field, enter your authorization code that you have received by mail, in the Right To Use (RTU) certificate, when the device/license was purchased.

5. Click **Licenses** for this asset.

6. Click **Generate** to generate license keys for the selected license.

7. Enter the serial number and hardware ID for the device the license applies to and click **Generate**.

---

**Apply License Keys**

To enter the license keys for your appliance, to view their expiration dates, or to delete them, navigate to **System > Configuration > Licensing tab**.
For details about types of licenses, license keys and license management, refer to **PCS/PPS License Management Guide**.

**Download Software**

1. Log in to [https://my.pulsesecure.net](https://my.pulsesecure.net)
2. Under Pulse Secure Centers, click on **Licensing and Download Center**.
3. Select the account you want to use.
4. In the Pulse Secure Licensing & Download Center page, select the **Downloads** tab.
5. At the bottom of the screen, under Browse My Software and Documentation, click Pulse Secure.

6. From Product Lines, click Pulse Policy Secure. This will download the latest Pulse Policy Secure software.

After you install Pulse Policy Secure and perform basic setup, you are ready to install the most current Pulse Policy Secure software, license Pulse Policy Secure, verify accessibility, and complete the configuration process:

- To install the most current Pulse Policy Secure software, license your Pulse Policy Secure and create a test user to verify user accessibility, follow the task guide embedded in the administrator Web console.
Pulse Policy Secure Configuration

- Initial Setup Wizard Configuration
- Manual Initial Configuration

Initial Setup Wizard Configuration

PPS comes with an inbuilt initial setup wizard, which allows you to easily configure the following:

- Step 1: Basic Settings
- Step 2: Configuring Profiling for Network Visibility
- Step 3: Configuring Layer 2 Enforcement
- Step 4: Configure Guest Authentication

You can launch the initial setup wizard using:

- Select Wizards > Initial Wizard > Configure
- Select Wizards > Initial Wizard > Configuration Summary

The below figure shows the configuration summary page for a fresh installation.

Figure 3: Initial Setup Configuration Summary Page
Step 1: Basic Settings

This section covers the following topics:

- Step 1.1: Configuring System Date and Time
- Step 1.2: Configuring License

Step 1.1: Configuring System Date and Time

The time synchronization between PPS and another component is very critical. You can easily configure the system date and time using the initial setup wizard. The system date and time can be configured manually or you can configure a network time protocol (NTP) server. It is recommended to use a public NTP server for time synchronization.

Figure 4: Initial Setup Configuration Page
Step 1.2: Configuring License

Configure the license either manually by entering the license key or through the License Server.

Figure 5: Configure License Manually

Figure 6: License Server
Step 2: Configuring Profiling for Network Visibility

Note: You must procure and install Profiler license for profiler functionality.

Pulse Secure Profiler dynamically identifies and classifies endpoints across managed and unmanaged endpoint devices, so that access to network and resources can be controlled based on the type of the device. It also helps you to get visibility so that necessary security policies for corporate access, BYOD, and guest access can be enforced.

**Figure 7: Initial Setup Configuration Page- Profiling**

Discovered SNMP v2/v3 devices.

**Figure 8: Initial Setup Configuration Page- Discover Switch SNMPv2**

Add the SNMP v2/v3 Switch
Upload the fingerprint database.

**Figure 10: Initial Setup Configuration Page – Fingerprint database**
Step 3: Configuring Layer 2 Enforcement

Layer 2 enforcement means controlling network access at the point where the user attaches to the network. In a wired network, this control is at the switch port; in a wireless network the control is at the wireless access point. The network access control is accomplished through 802.1X authentication protocol (implemented on the switch or wireless AP) in conjunction with RADIUS return attributes to control switch or AP operation such as VLAN assignment and filtering.

The following enforcements are supported for the devices connecting to the network.

- 802.1X
- MAC Authentication
- SNMP

**Note:** Profiling is enabled by default when you enable enforcement and authentication.

**Figure 11: Initial Setup Layer2 Enforcement**

![Initial Setup Layer2 Enforcement](image-url)
Configure the enforcement for devices, which includes laptops, smart phones, VOIP phones, and unmanaged devices.

**Note:** If profiling is enabled the device platform types are automatically enabled.

### Table 2: Enforcement

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Platforms</th>
<th>Authentication Type</th>
<th>Additional Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptops</td>
<td>• Windows</td>
<td>• 802.1X</td>
<td>Host Checker</td>
</tr>
<tr>
<td></td>
<td>• MAC</td>
<td>• SNMP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Linux</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart phones</td>
<td>• Android</td>
<td>802.1X</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>• iOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VOIP phones</td>
<td>NA</td>
<td>• 802.1X</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MAC</td>
<td></td>
</tr>
<tr>
<td>Unmanaged devices</td>
<td>NA</td>
<td>MAC</td>
<td>NA</td>
</tr>
</tbody>
</table>
Step 3.1: Importing Configurations from Pulse Connect Secure

The existing configurations in PCS can be imported to PPS for quickly configuring the PPS device.
Step 3.2: Configure Authentication Server

The initial setup wizard supports AD and LDAP authentication servers for user authentication. LDAP is supported for device authentication based on MAC address. Configure the required authentication server for user authentication and machine authentication.

Figure 15: Authentication Server

![Authentication Server](image)

Step 3.3: Define the Roles and the AD/LDAP group.

You can reuse the roles imported from PCS and then configure the VLAN and group information.

Figure 16: Authentication Server- LDAP

![Authentication Server- LDAP](image)

Step 3.4: Configure Compliance Check

PPS offers a variety of endpoint host checks to ensure compliance, including predefined checks for third-party endpoint security software including anti-virus, firewall, anti-malware/anti-spyware applications.

**Note:** You can reuse the compliance policies from PCS.
**Figure 17: Compliance Check**

![Initial Setup Diagram]

- **Add HostChecker Policy**
  - **Rule Name**: [Field]
  - **Platform**: [dropdown]
  - **Type**: [dropdown]

- **Enable Remediation Action**
  - [Add] [Reset]

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Platform</th>
<th>Compliance Type</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>RuleName</td>
<td>windows</td>
<td>Firewall</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Windows</th>
<th>Mac</th>
<th>Linux</th>
<th>Enforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS-Check</td>
<td>Process</td>
<td></td>
<td>Process</td>
<td></td>
</tr>
<tr>
<td>InitialSetup_HostCheckerPolicy</td>
<td>Firewall</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: Compliance policies selected will be applied based on the platform and the rules configured for the hostchecker policy.*
Step 4: Configure Guest Authentication

Guest access feature on PPS enables guest users to access the network through a self-registration process. The guest users self-register for network access from their device. Upon successful registration, the guest users are notified with the user credentials and other details through SMS or email.

**Figure 18: Initial Setup Guest Configuration**

![Initial Setup Guest Configuration](image1)

**Figure 19: Initial Setup Guest Configuration**

![Initial Setup Guest Configuration](image2)
Figure 20: Initial Setup Guest Configuration - Add switch

**What switches do you have?**
Switch can be used as an Intranet Enforcer with Pulse Policy Secure. With this solution, Pulse Policy Secure is the policy decision point, while the switch is the policy enforcement point.

- **Add New Switch**
  - Name: 10.204.88.12
  - IP Address: 10.204.88.12
  - Make/Model: Ruckus Wireless

- **RADIUS Client Configuration**
  - IP Address Range: 1
  - Shared Secret: ********
  - Ruckus Password:

Validate Ruckus Server Certificate: Yes

Save

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>SNMP</th>
<th>RADIUS Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.204.88.12</td>
<td>10.204.88.12</td>
<td>None</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Step 5: Verification and Troubleshooting

The wizard captures the summary of the configurations before proceeding with enabling the corresponding use case on PPS. If needed you can modify the required configurations before completing the configuration.

Figure 21: Summary

![Summary](image1)

The below figure shows the final configuration summary page. You can verify the common configuration, profiling, enforcement, guest access configuration details.

Figure 22: Configuration Summary

![Configuration Summary](image2)
Manual Initial Configuration

This section describes in brief about the Pulse Policy Secure configuration manually. For details, refer to the Pulse Policy Secure Administration Guide.

Step 1: Configuring Pulse Secure Profiler

Note: You must procure and install Profiler license for profiler functionality.

Pulse Policy Secure includes a built-in device Profiler that can automatically detect and classify all devices on the network using DHCP-fingerprinting, SNMP discovery and HTTP-UA fingerprinting.

Once you are logged in to the web-based Admin Console, configure the in-built Profiler using the steps shown below.

1. Navigate to Authentication > Auth Servers page.
2. Select Local Profiler from the server type drop-down and click New Server.
3. Enter a name for the Auth. server.
4. Click Browse and upload the device fingerprints package.
5. Click Save Changes to save the configuration settings. Please be patient; this operation may take a few minutes to complete.

Step1.1: Discover devices using DHCP

Devices on the network that have DHCP-based IP addresses are automatically profiled by the Profiler as they connect to the network. However, to enable this type of profiling, you need to ensure that all the DHCP requests are forwarded to the internal port of the Pulse Policy Secure – this configuration needs to be done on one or more switches in your network.

Configure DHCP relay on switches to forward DHCP packets to Pulse Policy Secure. See Profiler Deployment Guide for more information.

Navigate to System > Reports > Devices Discovery to start seeing devices on the network. The discovery process may take from a few minutes to a few hours depending on the network.

Step1.2: Discover devices using SNMP

To discovery and profile devices with static IP addresses, you need to add one or more SNMP-enabled switches in the SNMP management page of the web based Admin Console.

1. Select Authentication > Auth Servers > [Local Profiler]. Set the SNMP Poll interval to 5 mins. Click on Save Changes.
2. Click on the SNMP Device link in the help text for SNMP Poll Interval. Enter information about the switch. If SNMP switch is only used for Profiling endpoints, do not select the SNMP Enforcement check box.
3. Save the changes. The SNMP Device Configuration table should get updated with the new switch information. Status should be GREEN.
4. Wait for 15 minutes for the new polling interval to take effect, or restart services using Maintenance > System > Platform > Restart Services button so the new configuration is active immediately after restart.

Navigate to System > Reports > Devices Discovery to start seeing devices with static IP addresses on the network. Profiler will periodically poll the switches to ensure that new devices get profiled as they connect to the network.
Step 2: Configuring PPS

The following steps are involved in the Pulse Policy Secure configuration.

1. To create an Authentication Server (for example, Active Directory Standard Mode) configuration, navigate to Authentication > Auth. Servers and complete the configuration.

   Figure 23: Auth. Server Configuration

2. To configure user role, navigate to Users -> User Roles -> New Role and create a new role.

   Figure 24: User Role Configuration

3. To configure user realm, navigate to Users > User Realms and create a new realm or edit a realm you have already created.
4. To create role mapping rule, navigate to Users > User Realms > <select user> > Role Mapping and complete the configuration.

Note: Role-mapping rules can be defined to place users in Roles based on many different attributes, such as username, certificate, device attributes from Profiler or a batch of custom expressions. The Roles will define the level of access to different features and resources available on the network.

5. To configure sign-in policy, navigate to Authentication > Signing In > Sign-In Policies and complete the configuration.
Once you complete the basic configurations, you can explore more on PPS functionality.

For example:

- PPS can be used as a standalone RADIUS server.
- It can also be used for SNMP enforcement, MAC address authentication along with 802.1X.
- Layer 3 enforcement with a Juniper Network SRX, Palo Alto Networks next generation firewall, Check Point firewall, or Fortinet Firewall.

Refer the Pulse Policy Secure Administration Guide for more details.

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, then file a ticket with PSGSC.

- Product warranties—For product warranty information, visit https://www.pulsesecure.net
- Find product documentation: https://www.pulsesecure.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: https://www.pulsesecure.net/support

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at https://www.pulsesecure.net/support.
- Call Phone: 1-844-751-7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see https://www.pulsesecure.net/support