Pulse Policy Secure

Getting Started Guide

Document Version	2.0
Published	December 2018

Pulse Secure, LLC

2700 Zanker Road, Suite 200 San Jose, CA 95134

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

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

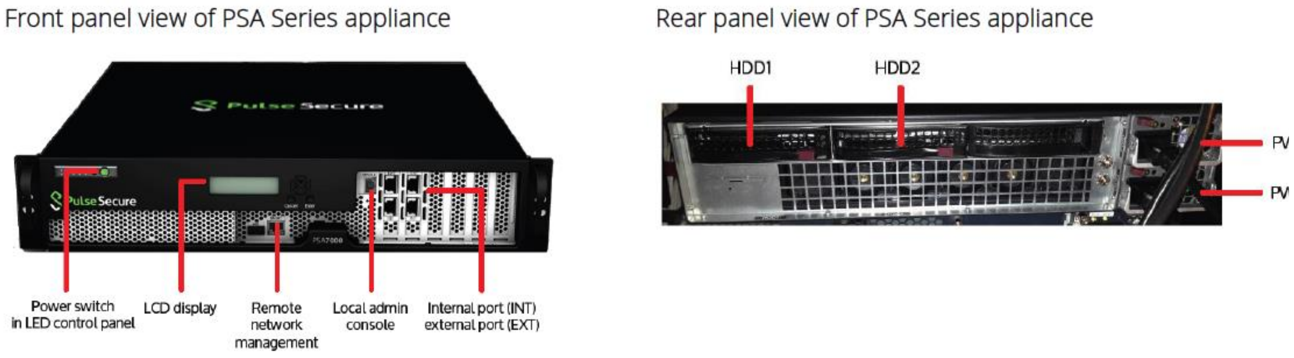
Note: After installing and setting up Pulse Policy Secure, refer to the Initial Configuration task guide in the administrator Web console to install the most current Pulse Policy Secure software, license your Pulse Policy Secure appliance, and create a test user to verify user accessibility. To test 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



Front panel view of PSA Series appliance

Rear panel view of PSA Series appliance

Power switch in LED control panel
LCD display
Remote network management
Local admin console
Internal port (INT) external port (EXT)
HDD1
HDD2
PV
PV

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 1: Device Status LEDs

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

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.)

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

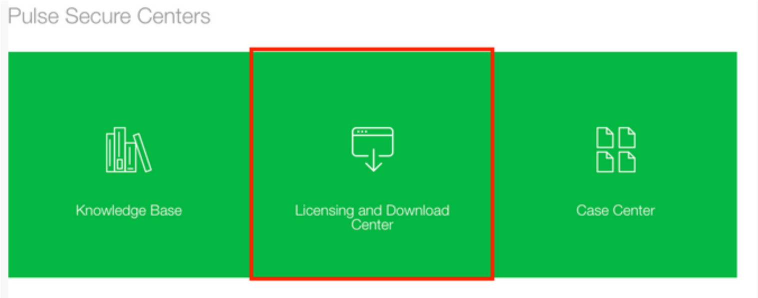
Pulse Policy Secure software and Pulse Policy Secure software include a Pulse Secure Licensing and Software Download Center @ https://my.pulsesecure.net that lets you to configure a Pulse Policy Secure appliance as a license server. This license server allows administrators to view all configured systems 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.

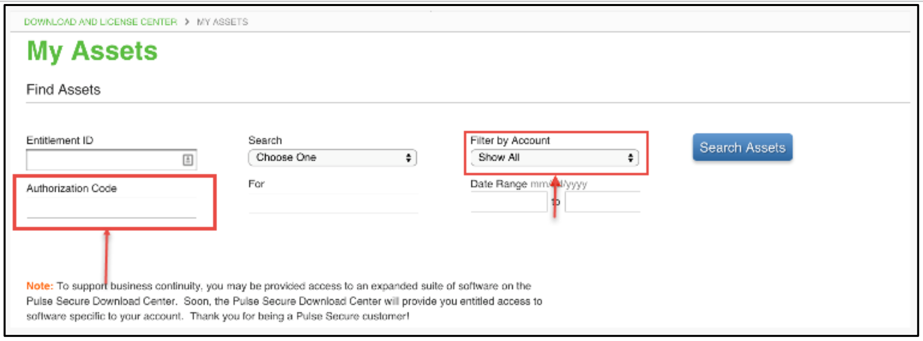
Obtain Licenses

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**
2. Under Pulse Secure Centers, click on **Licensing and Download Center.**

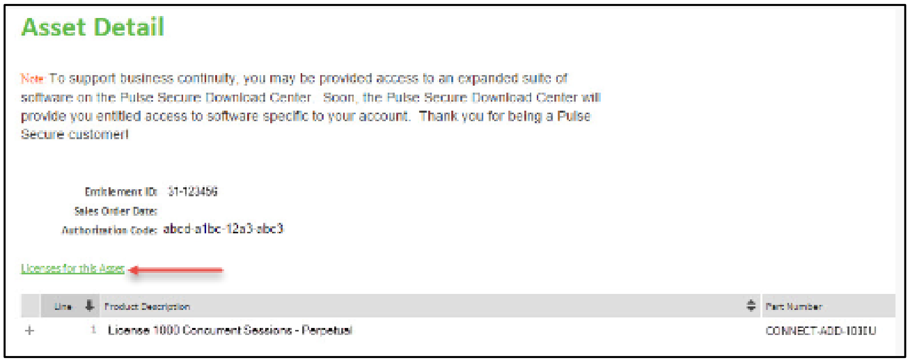


3. From the My Assets page, select **Show All** from the Filter by Account drop-down list.



Note: To support business continuity, you may be provided access to an expanded suite of software on the Pulse Secure Download Center. Soon, the Pulse Secure Download Center will provide you entitled access to software specific to your account. Thank you for being a Pulse Secure customer!

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.

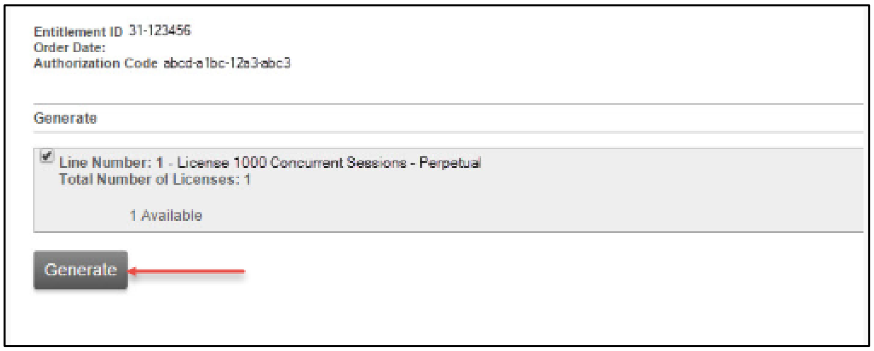


Note: To support business continuity, you may be provided access to an expanded suite of software on the Pulse Secure Download Center. Soon, the Pulse Secure Download Center will provide you entitled access to software specific to your account. Thank you for being a Pulse Secure customer!

Entitlement ID: 31-123456
Sales Order Date:
Authorization Code: abcd-a1bc-12a3-abc3

	Line	Product Description	Part Number
+	1	License 1000 Concurrent Sessions - Perpetual	CONNECT-ADD-1000U

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

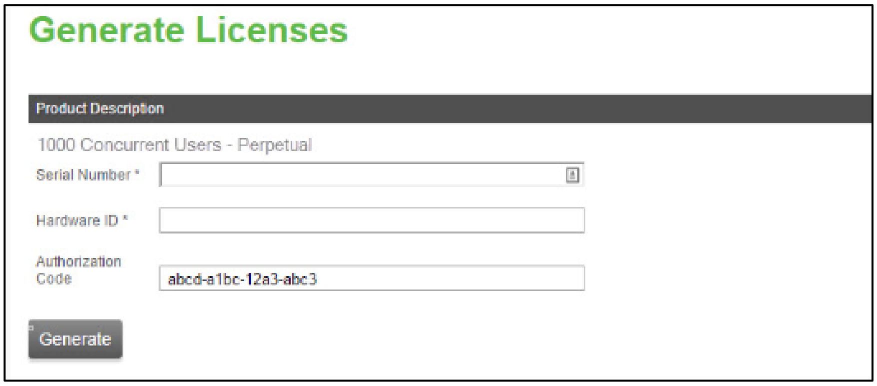


Entitlement ID 31-123456
Order Date:
Authorization Code abcd-a1bc-12a3-abc3

☑ Line Number: 1 - License 1000 Concurrent Sessions - Perpetual
Total Number of Licenses: 1

1 Available

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



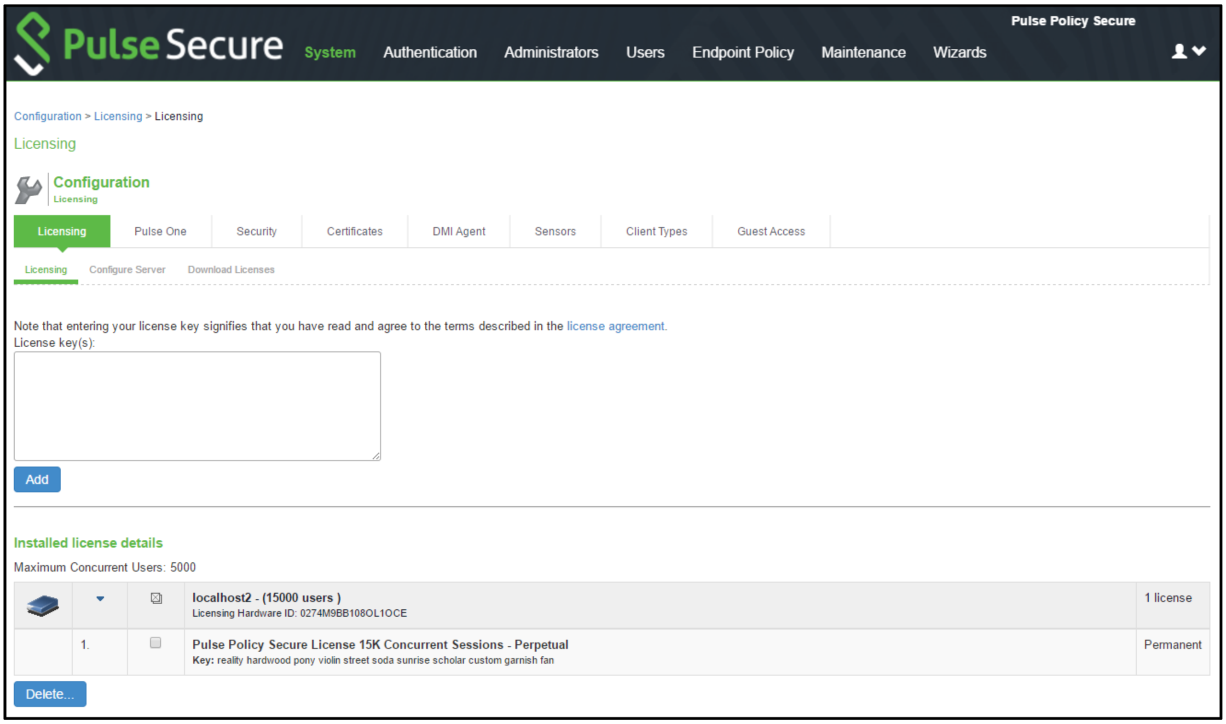
1000 Concurrent Users - Perpetual

Authorization Code: abcd-a1bc-12a3-abc3

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**.

Figure 2: Pulse Policy Secure License



Note that entering your license key signifies that you have read and agree to the terms described in the license agreement.

License key(s):

Installed license details

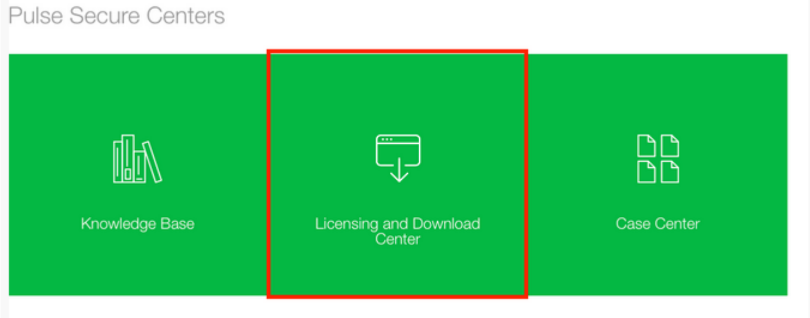
Maximum Concurrent Users: 5000

		☒	**localhost2 - (15000 users)** Licensing Hardware ID: 0274M9BB108OL1OCE	1 license
	1.	□	**Pulse Policy Secure License 15K Concurrent Sessions - Perpetual** **Key:** reality hardwood pony violin street soda sunrise scholar custom garnish fan	Permanent

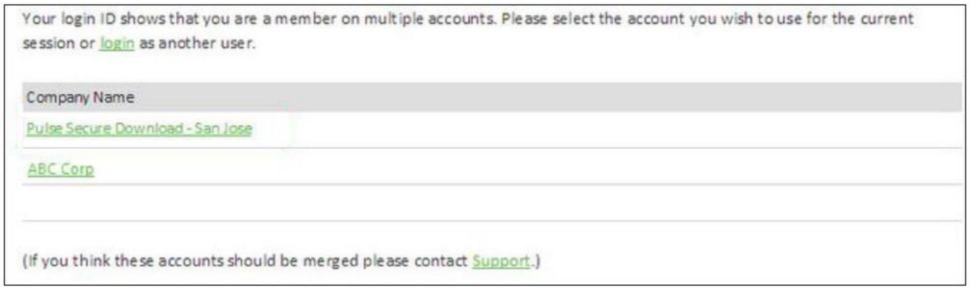
For details about types of licenses, license keys and license management, refer to **PCS/PPS License Management Guide**.

Download Software

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



3. Select the account you want to use.

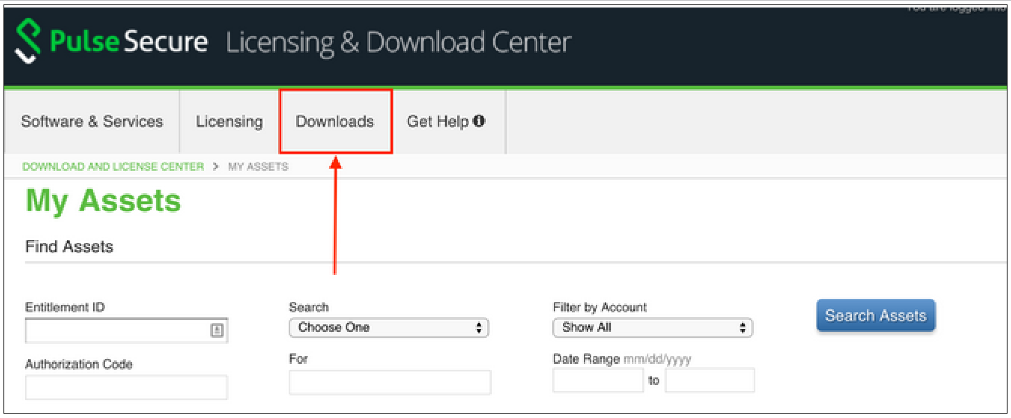


Your login ID shows that you are a member on multiple accounts. Please select the account you wish to use for the current session or login as another user.

Company Name
Pulse Secure Download - San Jose
ABC Corp

(If you think these accounts should be merged please contact Support.)

4. In the Pulse Secure Licensing & Download Center page, select the **Downloads** tab.



Pulse Secure Licensing & Download Center
Software & Services
Licensing
Downloads
Get Help
DOWNLOAD AND LICENSE CENTER > MY ASSETS
Search Assets

My Assets

Find Assets

Entitlement ID

Authorization Code

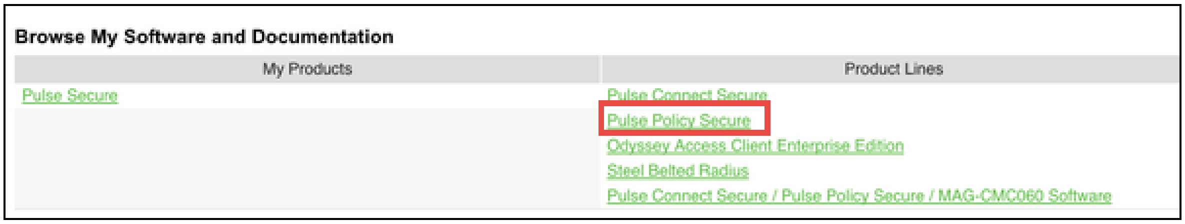
Search: Choose One

For

Filter by Account: Show All

Date Range mm/dd/yyyy to

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.



Browse My Software and Documentation

My Products	Product Lines
Pulse Secure	Pulse Connect Secure Pulse Policy Secure Odyssey Access Client Enterprise Edition Steel Belted Radius Pulse Connect Secure / Pulse Policy Secure / MAG-CMC060 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:

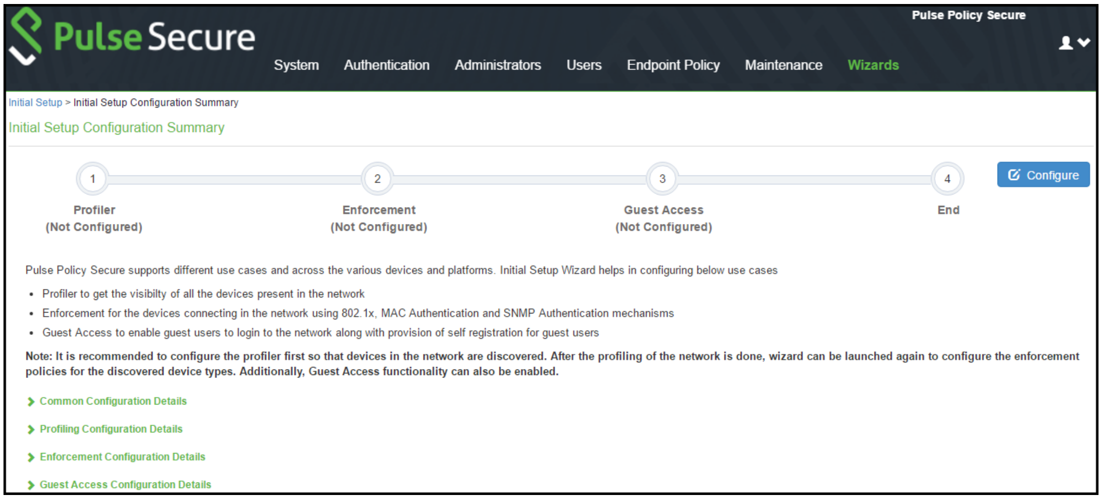
- Step 1: Basic Settings
- Step 2: Configuring Profiling for Network Visibility
- Step 3: Configuring Layer 2 Enforcement
- Step 4: Configure Guest Authentication

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



Pulse Policy Secure supports different use cases and across the various devices and platforms. Initial Setup Wizard helps in configuring below use cases

- Profiler to get the visibilty of all the devices present in the network
- Enforcement for the devices connecting in the network using 802.1x, MAC Authentication and SNMP Authentication mechanisms
- Guest Access to enable guest users to login to the network along with provision of self registration for guest users

Note: It is recommended to configure the profiler first so that devices in the network are discovered. After the profiling of the network is done, wizard can be launched again to configure the enforcement policies for the discovered device types. Additionally, Guest Access functionality can also be enabled.

Common Configuration Details
Profiling Configuration Details
Enforcement Configuration Details
Guest Access Configuration Details

Step 1: Basic Settings

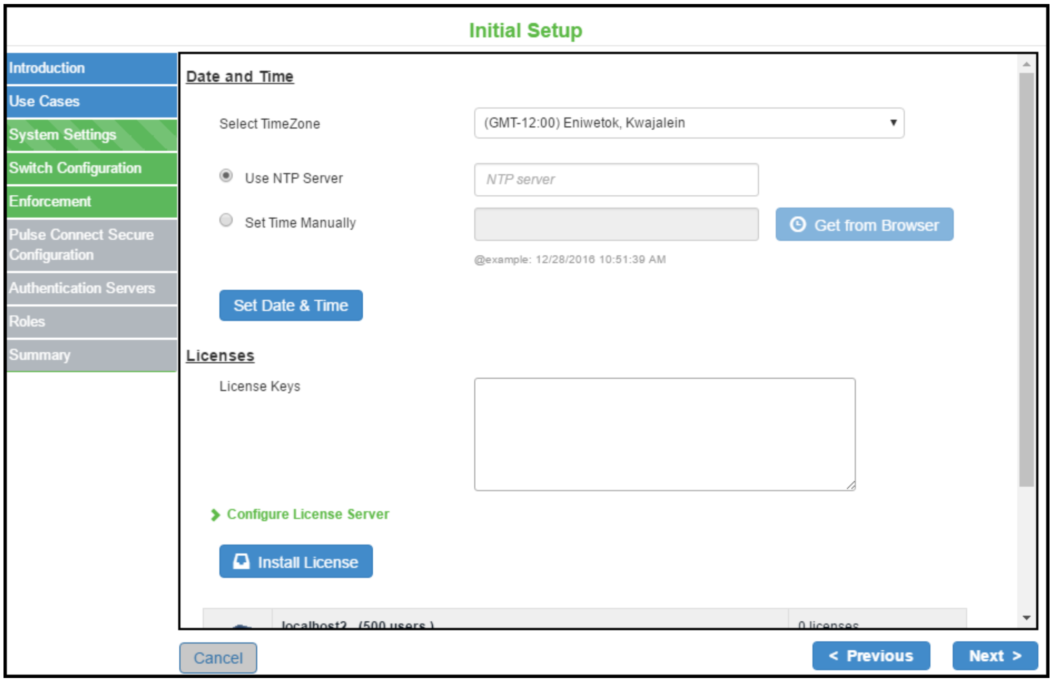
This section covers the following topics:

- 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



Initial Setup

Date and Time

Select TimeZone: (GMT-12:00) Eniwetok, Kwajalein

● Use NTP Server — NTP server

○ Set Time Manually

@example: 12/28/2016 10:51:39 AM

Licenses

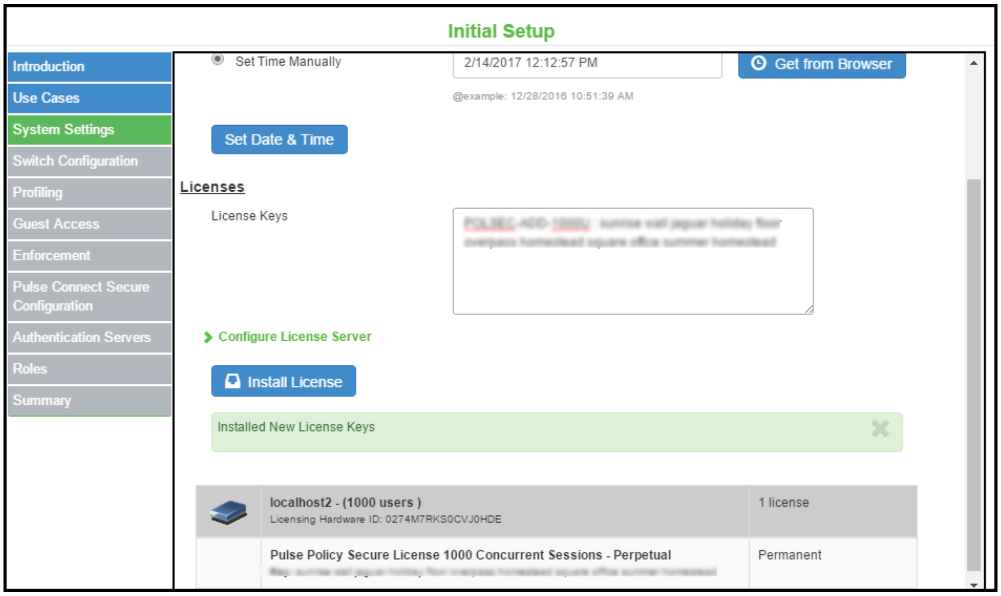
License Keys

localhost2 (500 users) 0 licenses

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



● Set Time Manually 2/14/2017 12:12:57 PM

@example: 12/28/2016 10:51:39 AM

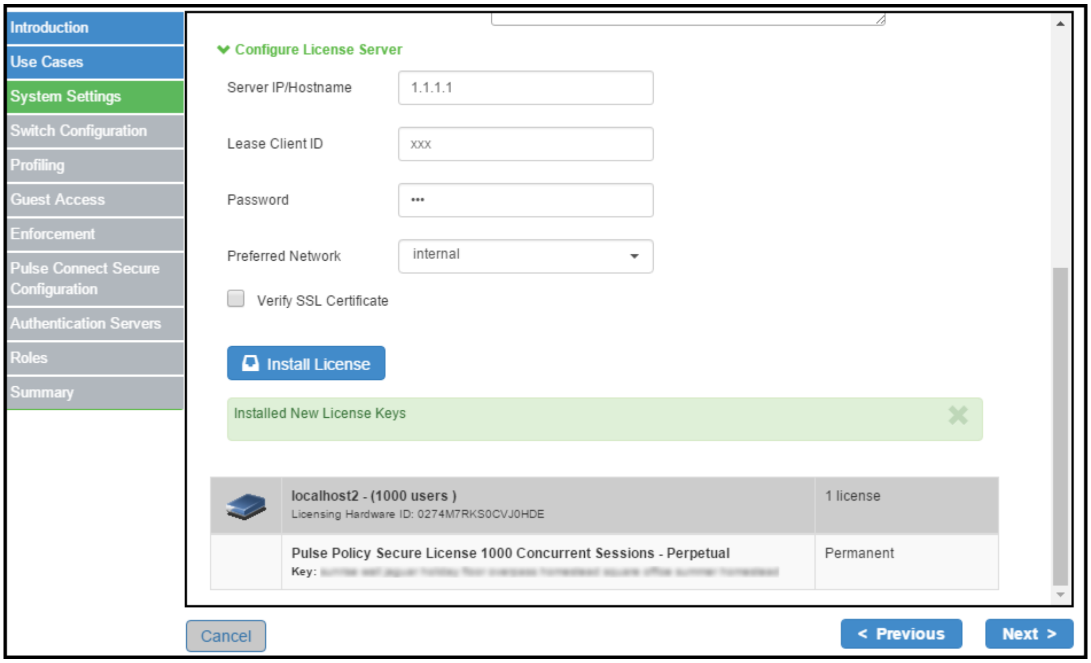
Licenses

License Keys [redacted]

Installed New License Keys ✖

	localhost2 - (1000 users) Licensing Hardware ID: 0274M7RKS0CVJ0HDE	1 license
	Pulse Policy Secure License 1000 Concurrent Sessions - Perpetual [redacted]	Permanent

Figure 6: License Server



Server IP/Hostname 1.1.1.1

Lease Client ID xxx

Password •••

Preferred Network internal

□ Verify SSL Certificate

Installed New License Keys ✖

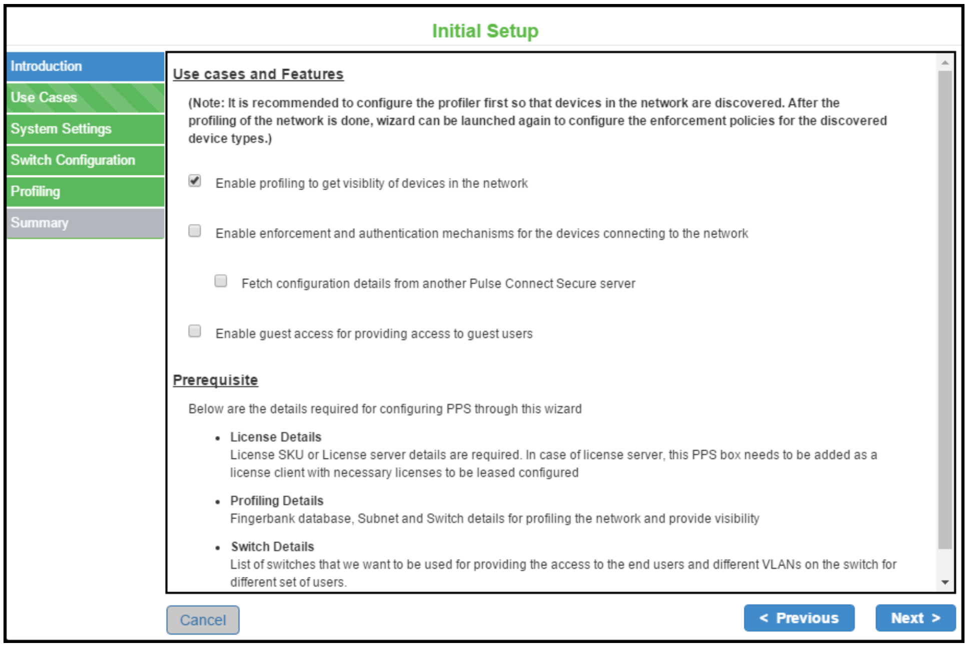
	localhost2 - (1000 users) Licensing Hardware ID: 0274M7RKS0CVJ0HDE	1 license
	Pulse Policy Secure License 1000 Concurrent Sessions - Perpetual Key: [redacted]	Permanent

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



Use cases and Features

(Note: It is recommended to configure the profiler first so that devices in the network are discovered. After the profiling of the network is done, wizard can be launched again to configure the enforcement policies for the discovered device types.)

☑ Enable profiling to get visiblity of devices in the network

☐ Enable enforcement and authentication mechanisms for the devices connecting to the network

☐ Fetch configuration details from another Pulse Connect Secure server

☐ Enable guest access for providing access to guest users

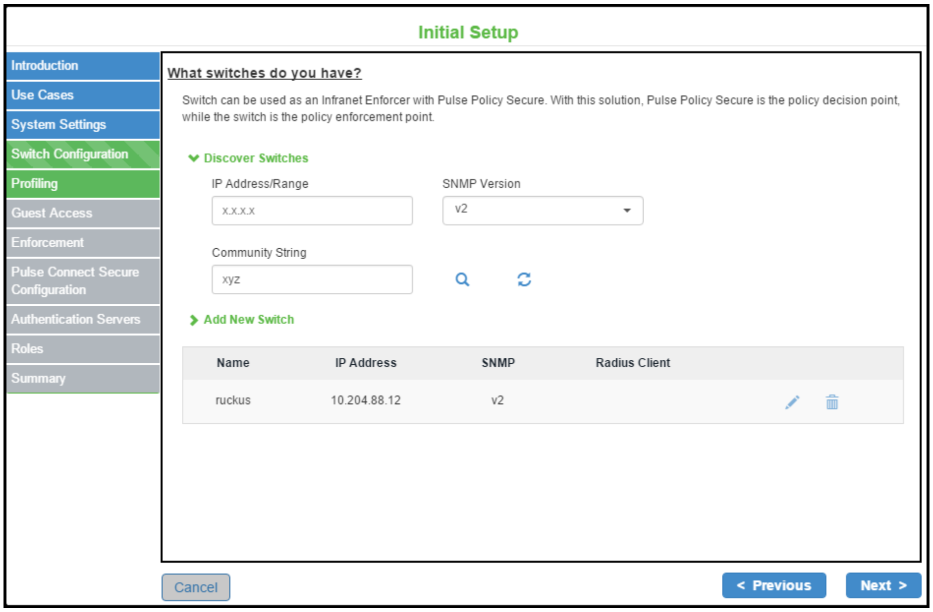
Prerequisite

Below are the details required for configuring PPS through this wizard

- **License Details**
  License SKU or License server details are required. In case of license server, this PPS box needs to be added as a license client with necessary licenses to be leased configured
- **Profiling Details**
  Fingerbank database, Subnet and Switch details for profiling the network and provide visibility
- **Switch Details**
  List of switches that we want to be used for providing the access to the end users and different VLANs on the switch for different set of users.

Discover SNMP v2/v3 devices.

Figure 8: Initial Setup Configuration Page- Discover Switch SNMPv2



What switches do you have?

Switch can be used as an Infranet Enforcer with Pulse Policy Secure. With this solution, Pulse Policy Secure is the policy decision point, while the switch is the policy enforcement point.

IP Address/Range: x.x.x.x

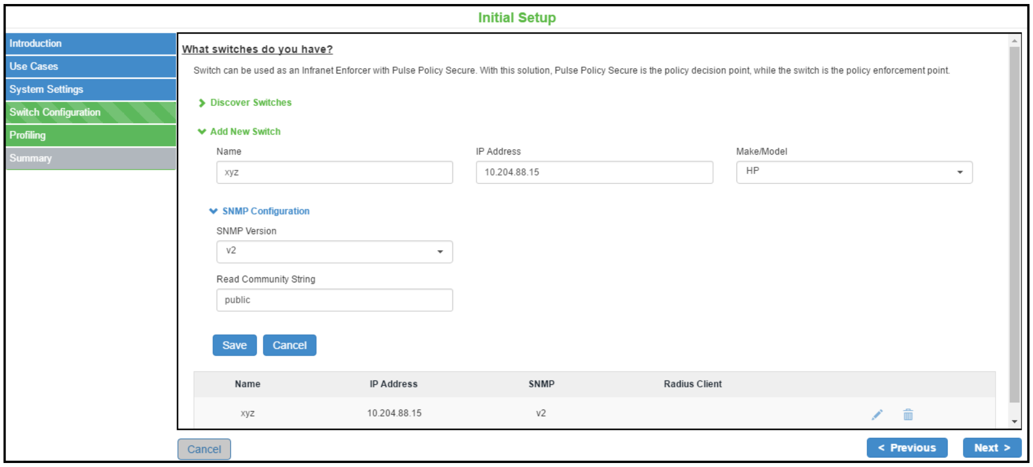
SNMP Version: v2

Community String: xyz

Name	IP Address	SNMP	Radius Client
ruckus	10.204.88.12	v2	

Add the SNMP v2/v3 Switch

Figure 9: Initial Setup Configuration Page- Add Switch SNMPv2



What switches do you have?

Switch can be used as an Infranet Enforcer with Pulse Policy Secure. With this solution, Pulse Policy Secure is the policy decision point, while the switch is the policy enforcement point.

Name: xyz

IP Address: 10.204.88.15

Make/Model: HP

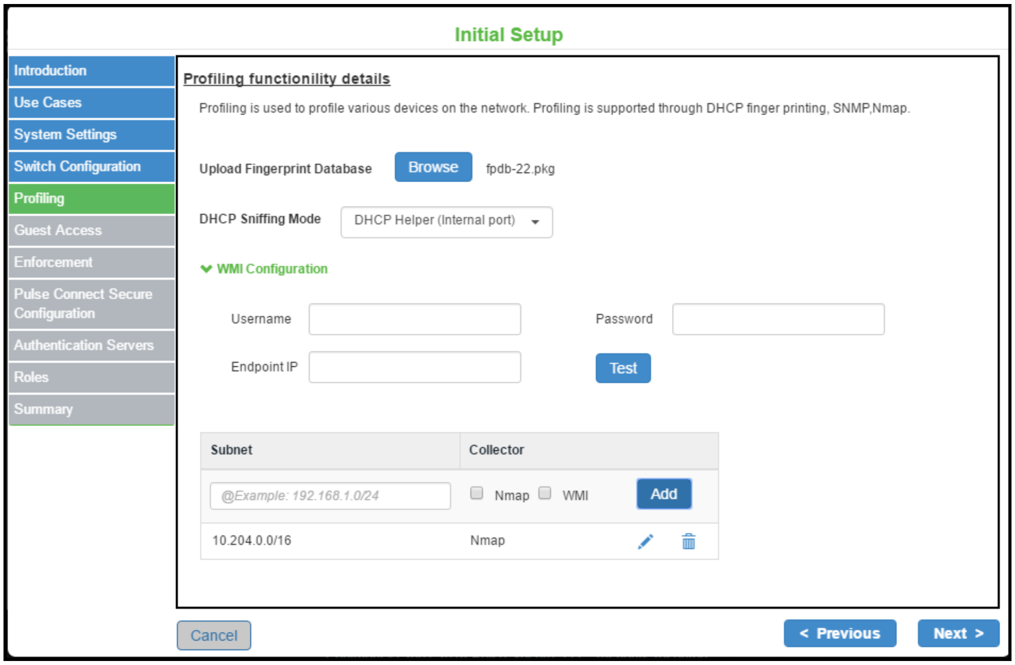
SNMP Version: v2

Read Community String: public

Name	IP Address	SNMP	Radius Client
xyz	10.204.88.15	v2	

Upload the fingerprint database.

Figure 10: Initial Setup Configuration Page – Fingerprint database



Profiling functionility details

Profiling is used to profile various devices on the network. Profiling is supported through DHCP finger printing, SNMP,Nmap.

Upload Fingerprint Database: fpdb-22.pkg

DHCP Sniffing Mode: DHCP Helper (Internal port)

Username:

Password:

Endpoint IP:

Subnet	Collector
@Example: 192.168.1.0/24	□ Nmap □ WMI
10.204.0.0/16	Nmap

Step 3: Configuring Layer 2 Enforcement

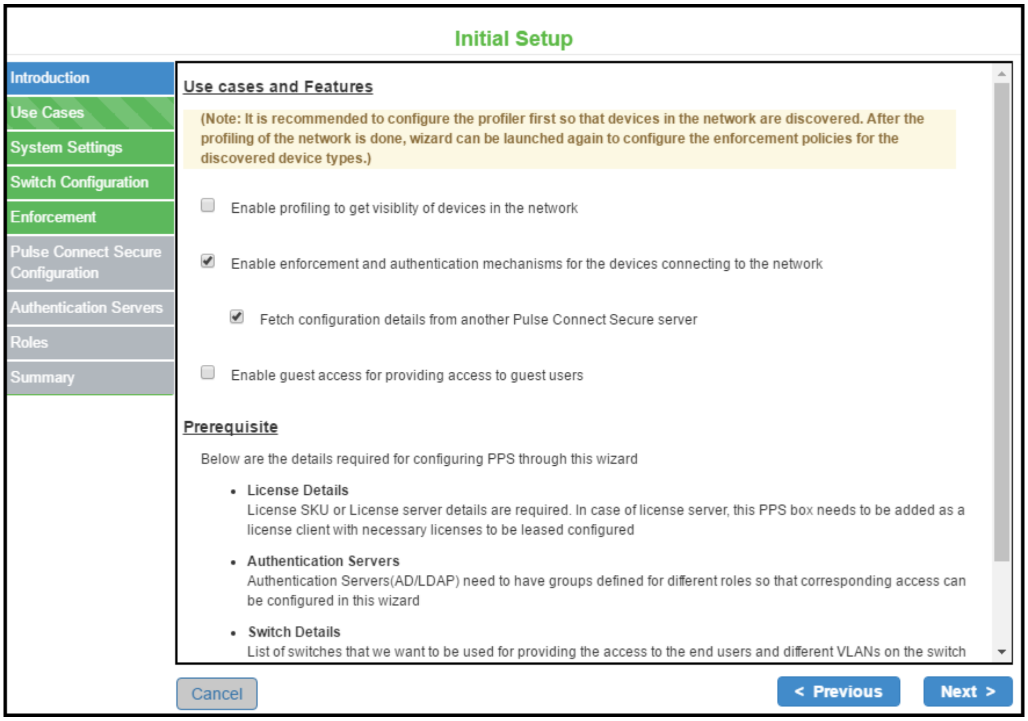
Layer 2 enforcement means controlling network access at the point where the user attaches to the network. In a wired network, this control is at the switch port; in a wireless network the control is at the wireless access point. The network access control is accomplished through 802.1X authentication 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



Use cases and Features

(Note: It is recommended to configure the profiler first so that devices in the network are discovered. After the profiling of the network is done, wizard can be launched again to configure the enforcement policies for the discovered device types.)

□ Enable profiling to get visiblity of devices in the network

☑ Enable enforcement and authentication mechanisms for the devices connecting to the network

☑ Fetch configuration details from another Pulse Connect Secure server

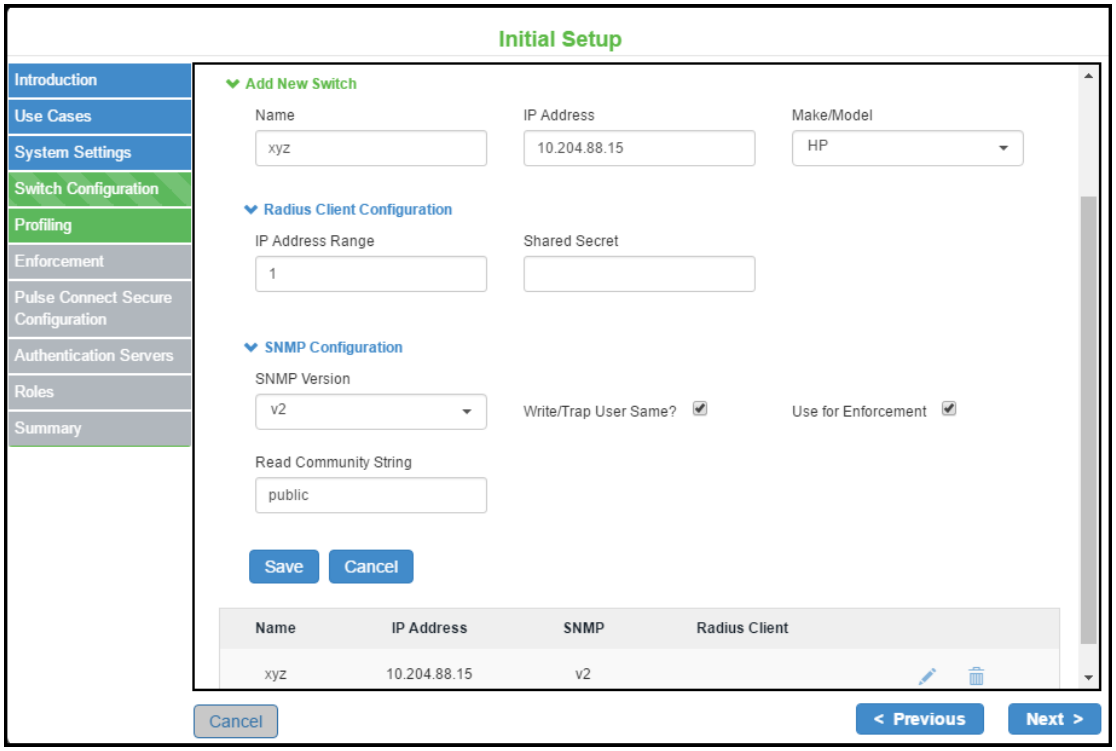
□ Enable guest access for providing access to guest users

Prerequisite

Below are the details required for configuring PPS through this wizard

- **License Details**
  License SKU or License server details are required. In case of license server, this PPS box needs to be added as a license client with necessary licenses to be leased configured
- **Authentication Servers**
  Authentication Servers(AD/LDAP) need to have groups defined for different roles so that corresponding access can be configured in this wizard
- **Switch Details**
  List of switches that we want to be used for providing the access to the end users and different VLANs on the switch

Figure 12: Add Switch – SNMPv2



Add New Switch

Name: xyz

IP Address: 10.204.88.15

Make/Model: HP

Radius Client Configuration

IP Address Range: 1

Shared Secret:

SNMP Configuration

SNMP Version: v2

Write/Trap User Same? ☑

Use for Enforcement ☑

Read Community String: public

Name	IP Address	SNMP	Radius Client
xyz	10.204.88.15	v2	

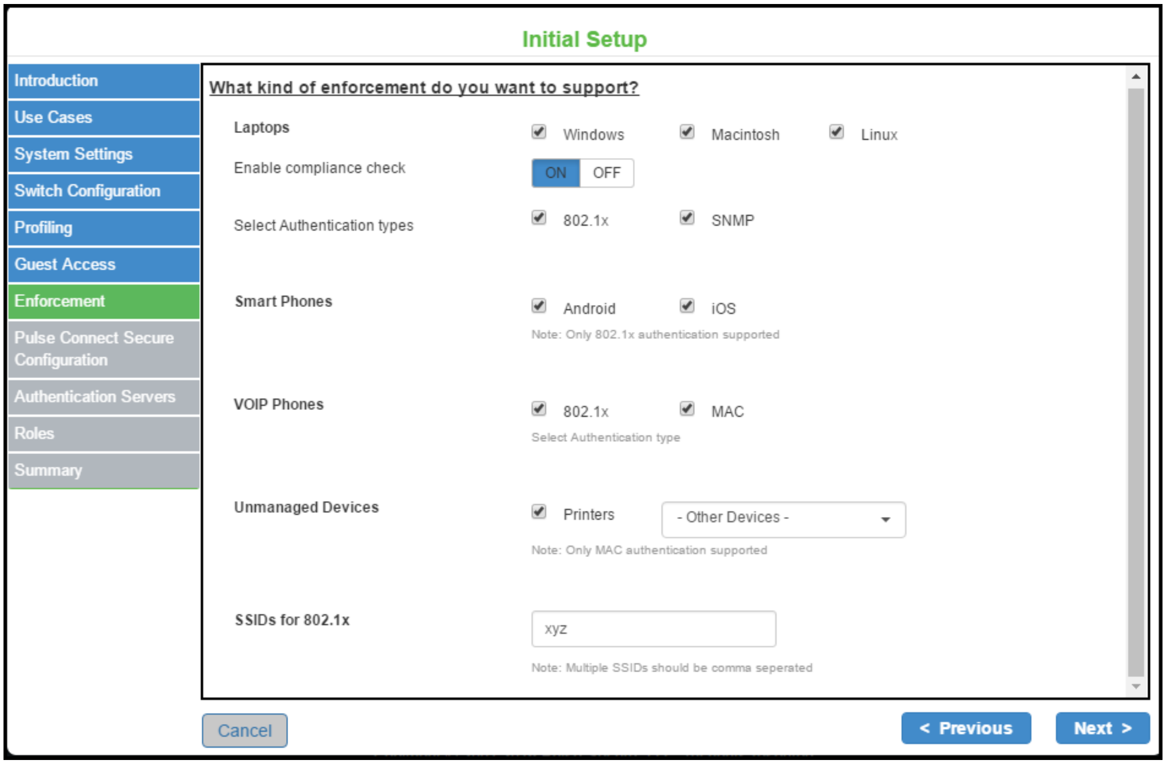
Configure the enforcement for devices, which includes laptops, smart phones, VOIP phones, and unmanaged devices.

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

Table 2: Enforcement

Device Type	Platforms	Authentication Type	Additional Support
Laptops	- Windows - MAC - Linux	- 802.1X - SNMP	Host Checker
Smart phones	- Android - iOS	802.1X	NA
VOIP phones	NA	- 802.1X - MAC	NA
Unmanaged devices	NA	MAC	NA

Figure 13: Initial Setup Layer2 Enforcement



What kind of enforcement do you want to support?

Laptops: ☑ Windows ☑ Macintosh ☑ Linux

Enable compliance check: ON OFF

Select Authentication types: ☑ 802.1x ☑ SNMP

Smart Phones: ☑ Android ☑ iOS

Note: Only 802.1x authentication supported

VOIP Phones: ☑ 802.1x ☑ MAC

Select Authentication type

Unmanaged Devices: ☑ Printers - Other Devices -

Note: Only MAC authentication supported

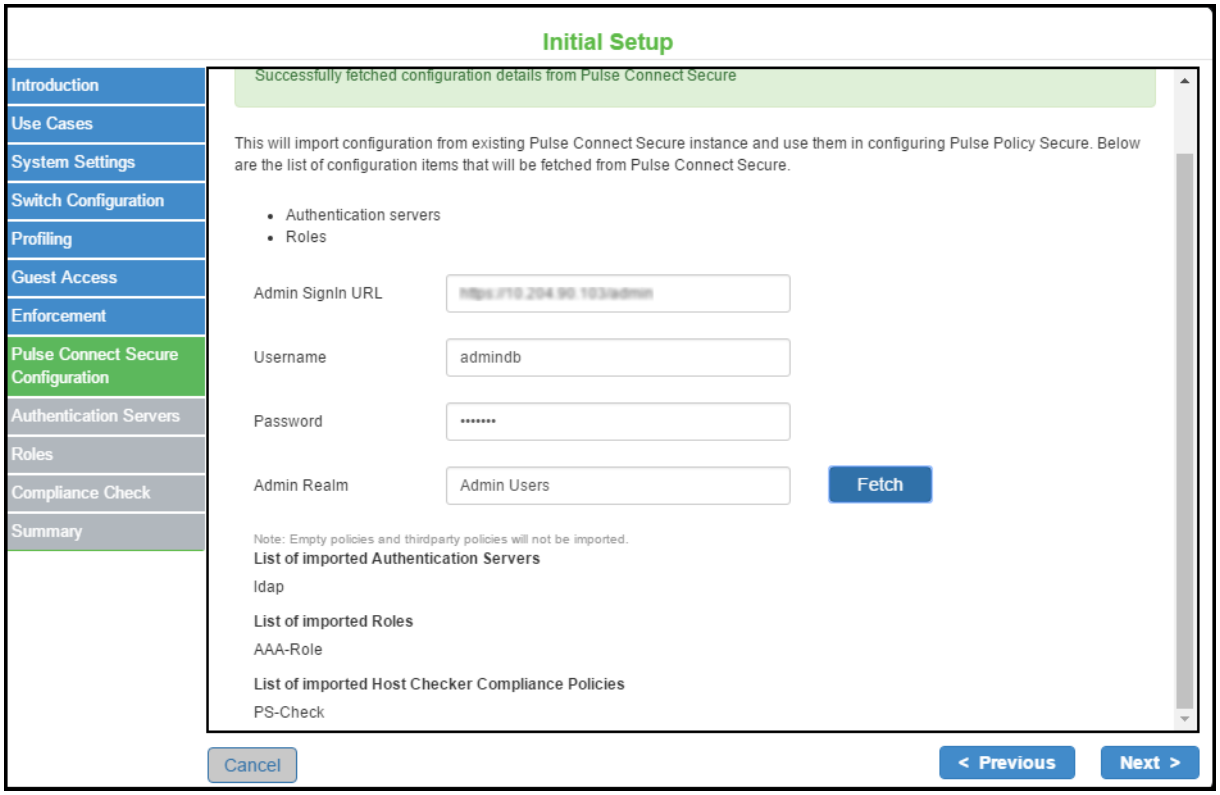
SSIDs for 802.1x: xyz

Note: Multiple SSIDs should be comma seperated

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.

Figure 14: Importing configuration from Pulse Connect Secure



Successfully fetched configuration details from Pulse Connect Secure

This will import configuration from existing Pulse Connect Secure instance and use them in configuring Pulse Policy Secure. Below are the list of configuration items that will be fetched from Pulse Connect Secure.

- Authentication servers
- Roles

Admin SignIn URL: [redacted]

Username: admindb

Password: •••••••

Admin Realm: Admin Users

Note: Empty policies and thirdparty policies will not be imported.

List of imported Authentication Servers

ldap

List of imported Roles

AAA-Role

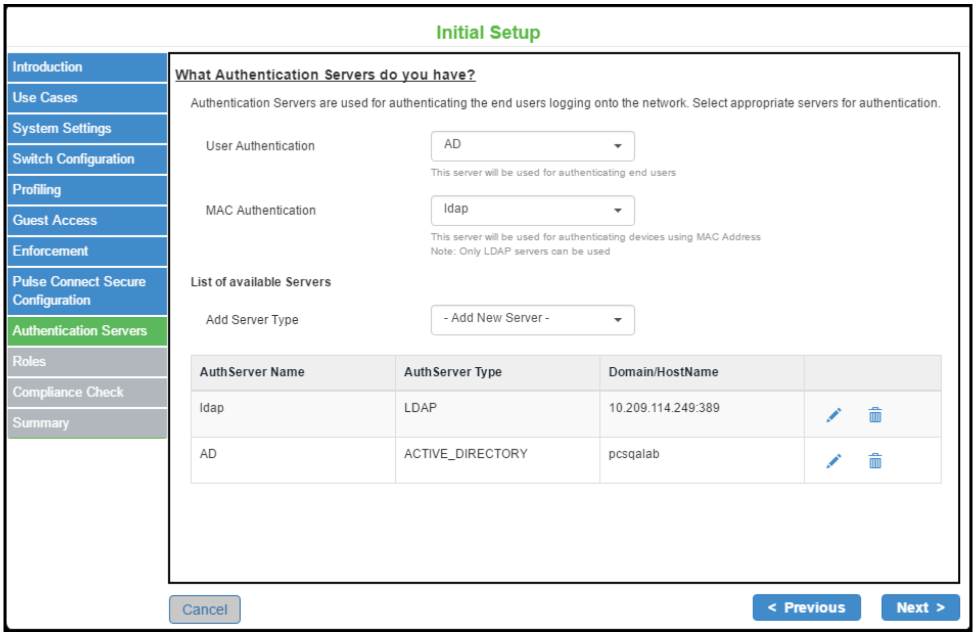
List of imported Host Checker Compliance Policies

PS-Check

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



What Authentication Servers do you have?

Authentication Servers are used for authenticating the end users logging onto the network. Select appropriate servers for authentication.

User Authentication: AD

This server will be used for authenticating end users

MAC Authentication: ldap

This server will be used for authenticating devices using MAC Address
Note: Only LDAP servers can be used

List of available Servers

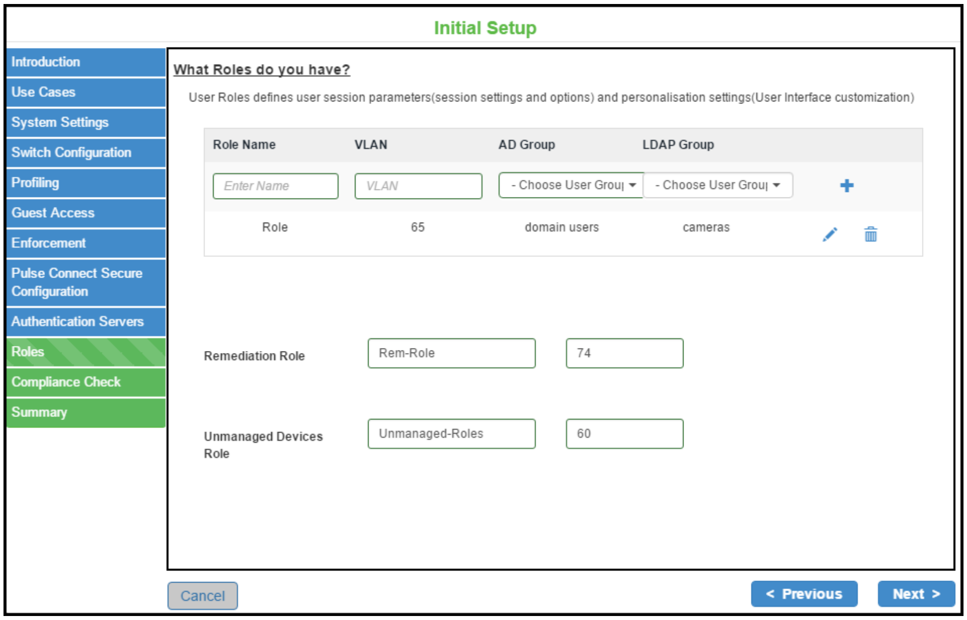
Add Server Type: - Add New Server -

AuthServer Name	AuthServer Type	Domain/HostName	
ldap	LDAP	10.209.114.249:389	
AD	ACTIVE_DIRECTORY	pcsqalab	

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



What Roles do you have?

User Roles defines user session parameters(session settings and options) and personalisation settings(User Interface customization)

Role Name	VLAN	AD Group	LDAP Group	
Enter Name	VLAN	- Choose User Grou	- Choose User Grou	+
Role	65	domain users	cameras	

Remediation Role: Rem-Role 74

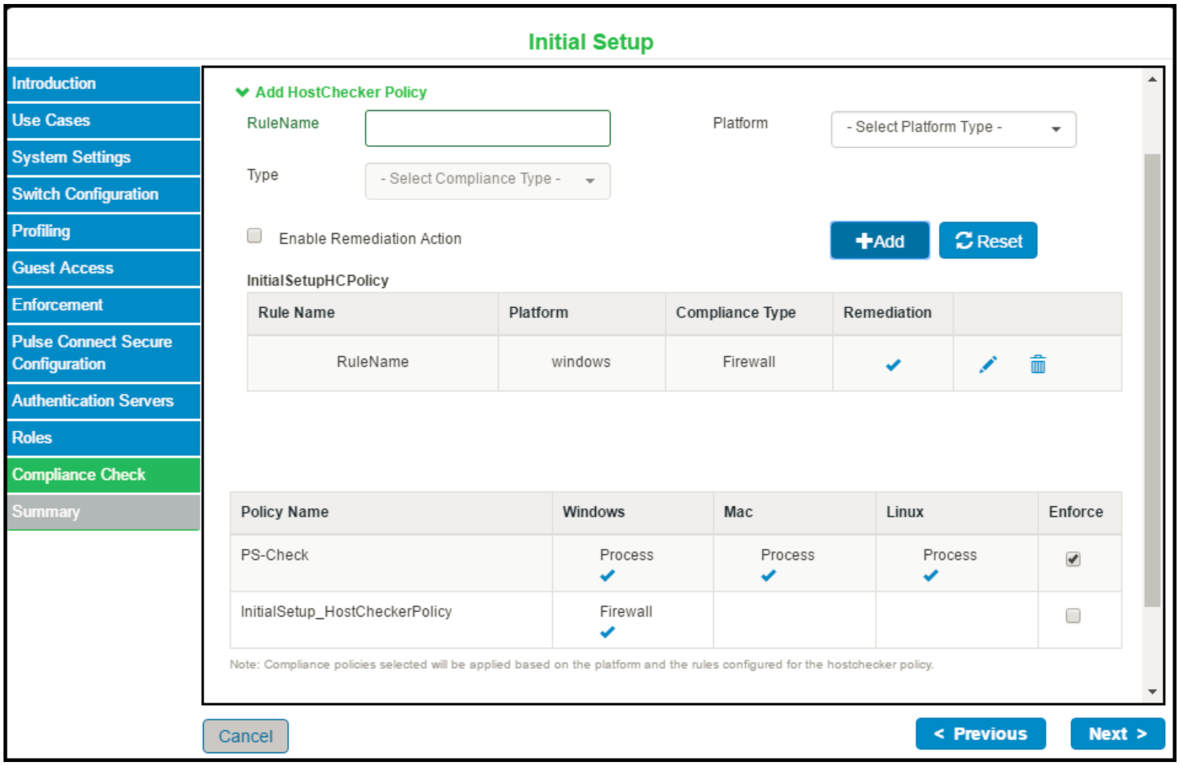
Unmanaged Devices Role: Unmanaged-Roles 60

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



Add HostChecker Policy

RuleName

Platform: - Select Platform Type -

Type: - Select Compliance Type -

☐ Enable Remediation Action

InitialSetupHCPolicy

Rule Name	Platform	Compliance Type	Remediation	
RuleName	windows	Firewall	✓	

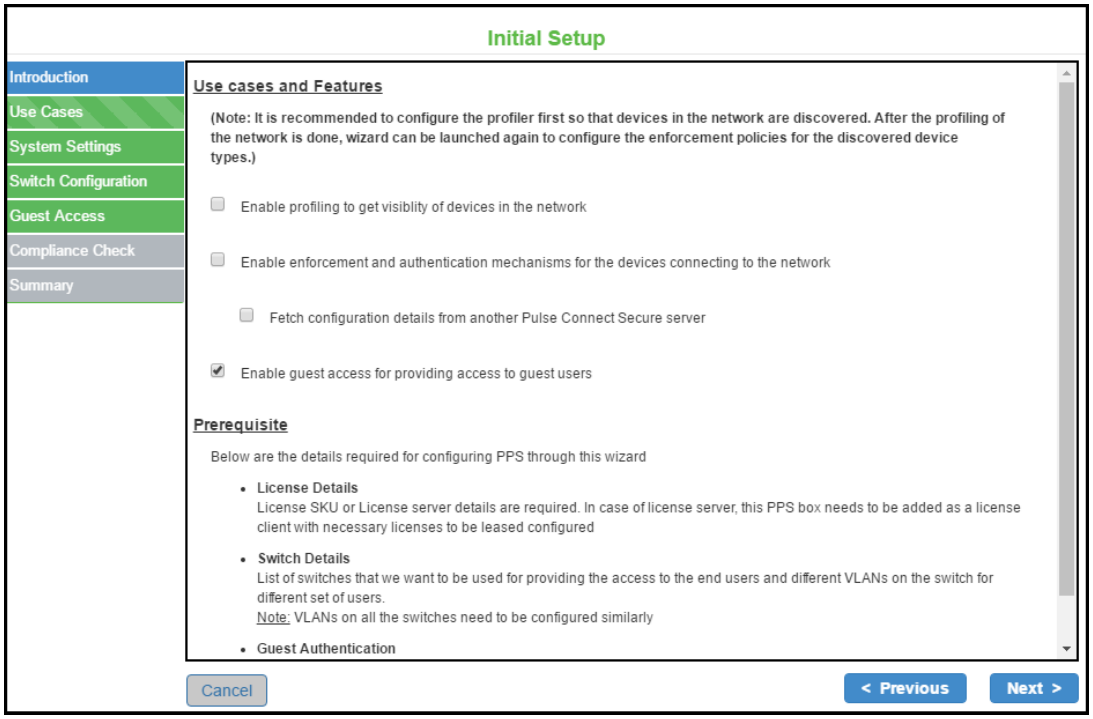
Policy Name	Windows	Mac	Linux	Enforce
PS-Check	Process ✓	Process ✓	Process ✓	☑
InitialSetup_HostCheckerPolicy	Firewall ✓			☐

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



Use cases and Features

(Note: It is recommended to configure the profiler first so that devices in the network are discovered. After the profiling of the network is done, wizard can be launched again to configure the enforcement policies for the discovered device types.)

☐ Enable profiling to get visiblity of devices in the network

☐ Enable enforcement and authentication mechanisms for the devices connecting to the network

☐ Fetch configuration details from another Pulse Connect Secure server

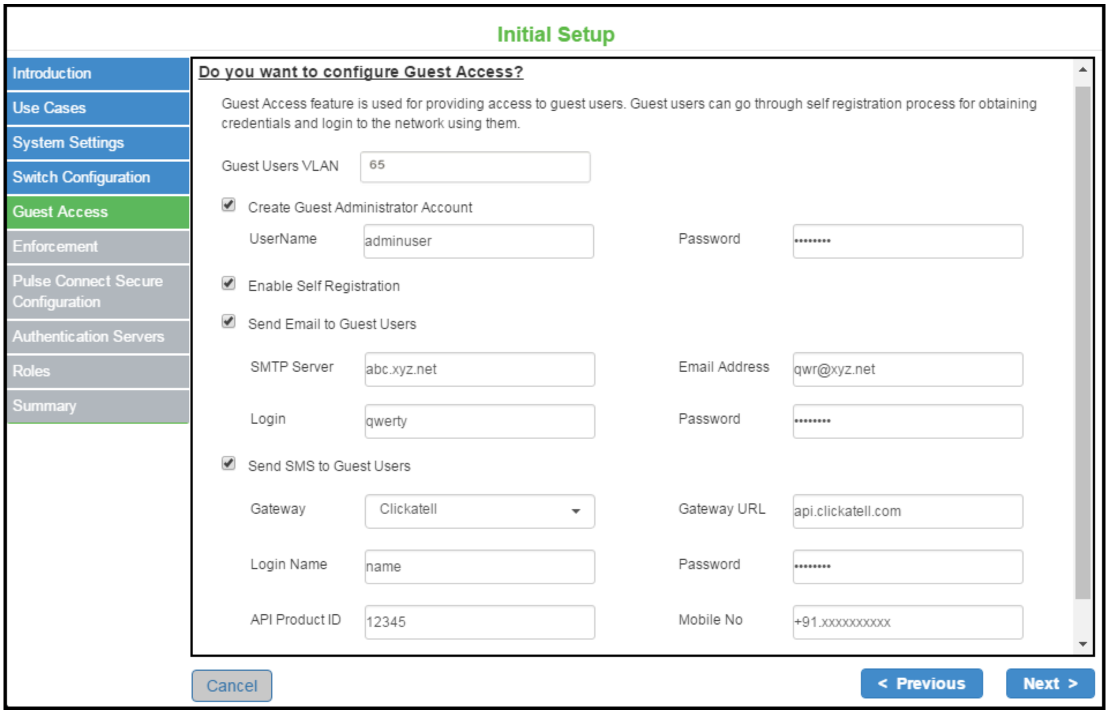
☑ Enable guest access for providing access to guest users

Prerequisite

Below are the details required for configuring PPS through this wizard

- **License Details**
  License SKU or License server details are required. In case of license server, this PPS box needs to be added as a license client with necessary licenses to be leased configured
- **Switch Details**
  List of switches that we want to be used for providing the access to the end users and different VLANs on the switch for different set of users.
  Note: VLANs on all the switches need to be configured similarly
- **Guest Authentication**

Figure 19: Initial Setup Guest Configuration



Do you want to configure Guest Access?

Guest Access feature is used for providing access to guest users. Guest users can go through self registration process for obtaining credentials and login to the network using them.

Guest Users VLAN: 65

☑ Create Guest Administrator Account

UserName: adminuser Password: ••••••••

☑ Enable Self Registration

☑ Send Email to Guest Users

SMTP Server: abc.xyz.net Email Address: qwr@xyz.net

Login: qwerty Password: ••••••••

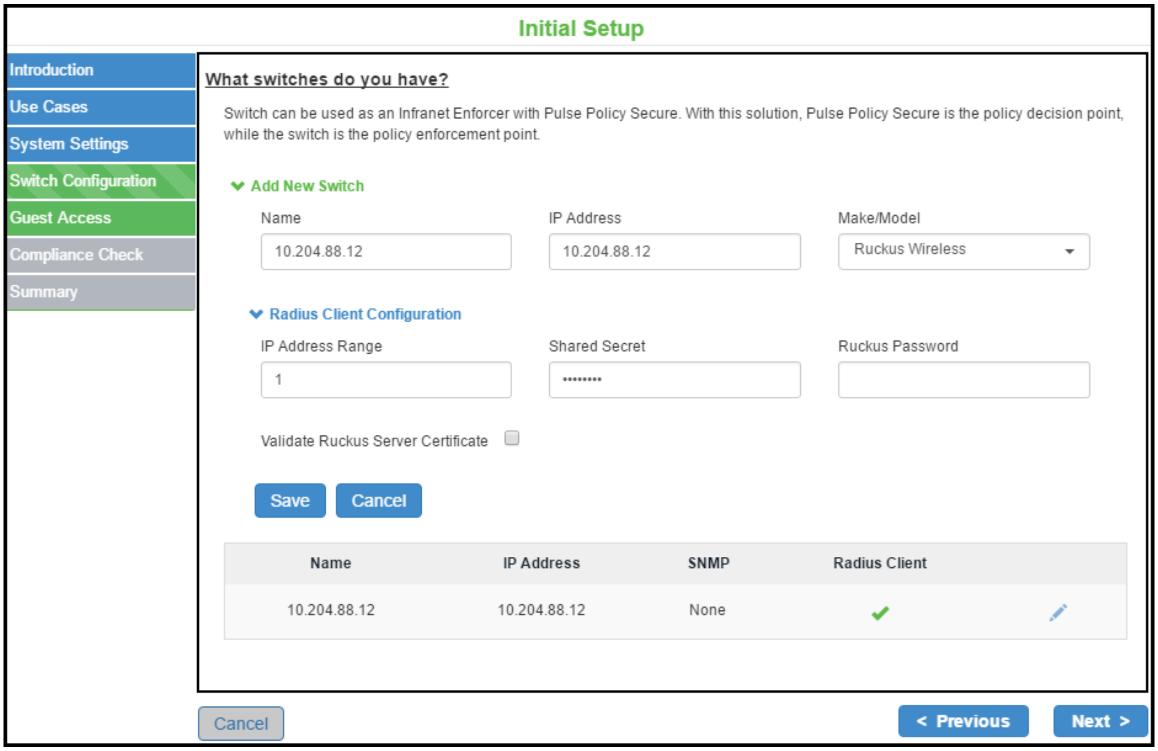
☑ Send SMS to Guest Users

Gateway: Clickatell Gateway URL: api.clickatell.com

Login Name: name Password: ••••••••

API Product ID: 12345 Mobile No: +91.xxxxxxxxxx

Figure 20: Initial Setup Guest Configuration- Add switch



What switches do you have?

Switch can be used as an Infranet 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:

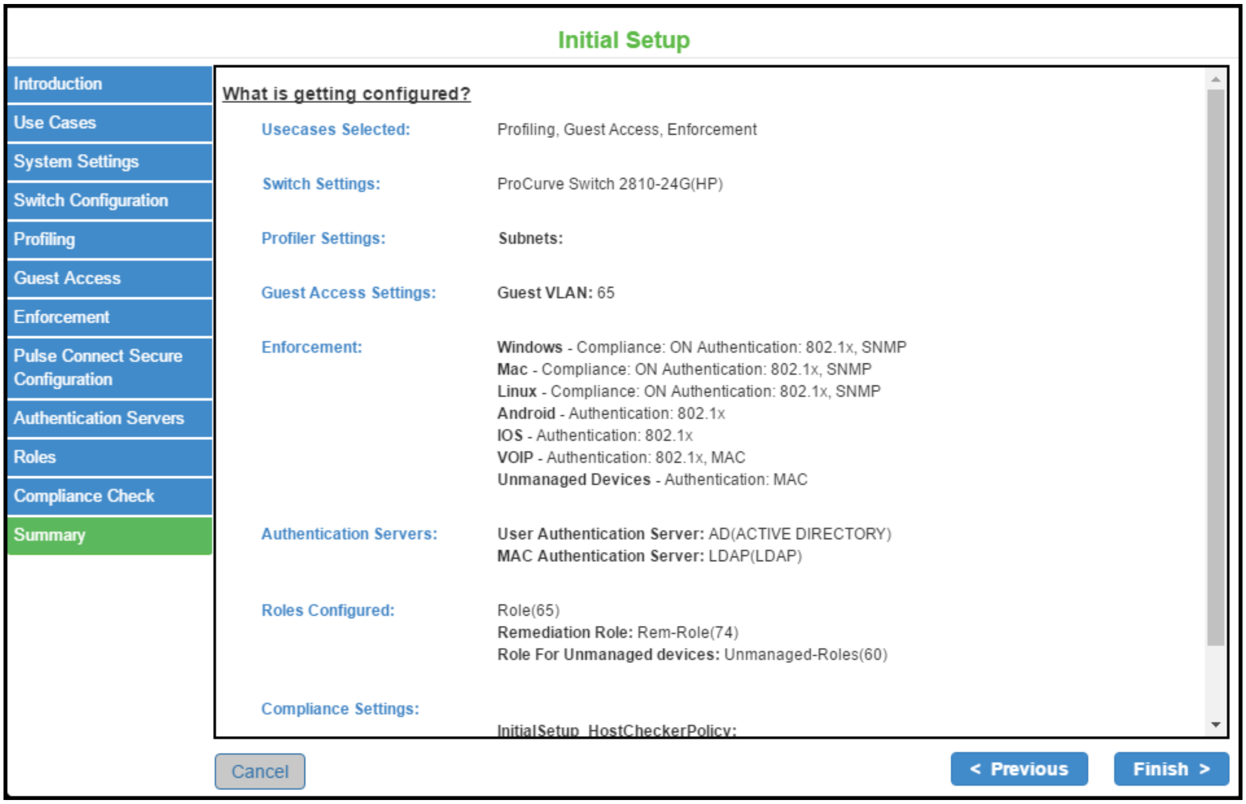
Validate Ruckus Server Certificate □

Name	IP Address	SNMP	Radius Client	
10.204.88.12	10.204.88.12	None	✓	✎

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



What is getting configured?

Usecases Selected: Profiling, Guest Access, Enforcement

Switch Settings: ProCurve Switch 2810-24G(HP)

Profiler Settings: **Subnets:**

Guest Access Settings: **Guest VLAN:** 65

Enforcement:
Windows - Compliance: ON Authentication: 802.1x, SNMP
Mac - Compliance: ON Authentication: 802.1x, SNMP
Linux - Compliance: ON Authentication: 802.1x, SNMP
Android - Authentication: 802.1x
IOS - Authentication: 802.1x
VOIP - Authentication: 802.1x, MAC
Unmanaged Devices - Authentication: MAC

Authentication Servers:
User Authentication Server: AD(ACTIVE DIRECTORY)
MAC Authentication Server: LDAP(LDAP)

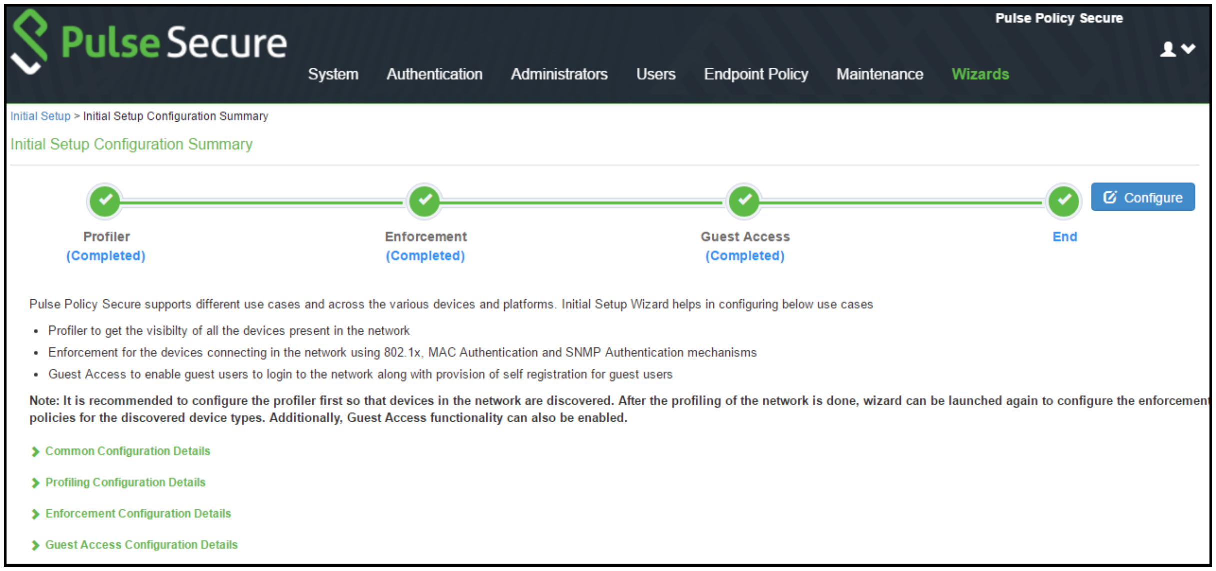
Roles Configured:
Role(65)
Remediation Role: Rem-Role(74)
Role For Unmanaged devices: Unmanaged-Roles(60)

Compliance Settings:

InitialSetup_HostCheckerPolicy:

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



Initial Setup > Initial Setup Configuration Summary

Initial Setup Configuration Summary

Pulse Policy Secure supports different use cases and across the various devices and platforms. Initial Setup Wizard helps in configuring below use cases

- Profiler to get the visibilty of all the devices present in the network
- Enforcement for the devices connecting in the network using 802.1x, MAC Authentication and SNMP Authentication mechanisms
- Guest Access to enable guest users to login to the network along with provision of self registration for guest users

Note: It is recommended to configure the profiler first so that devices in the network are discovered. After the profiling of the network is done, wizard can be launched again to configure the enforcement policies for the discovered device types. Additionally, Guest Access functionality can also be enabled.

› Common Configuration Details

› Profiling Configuration Details

› Enforcement Configuration Details

› Guest Access Configuration Details

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.

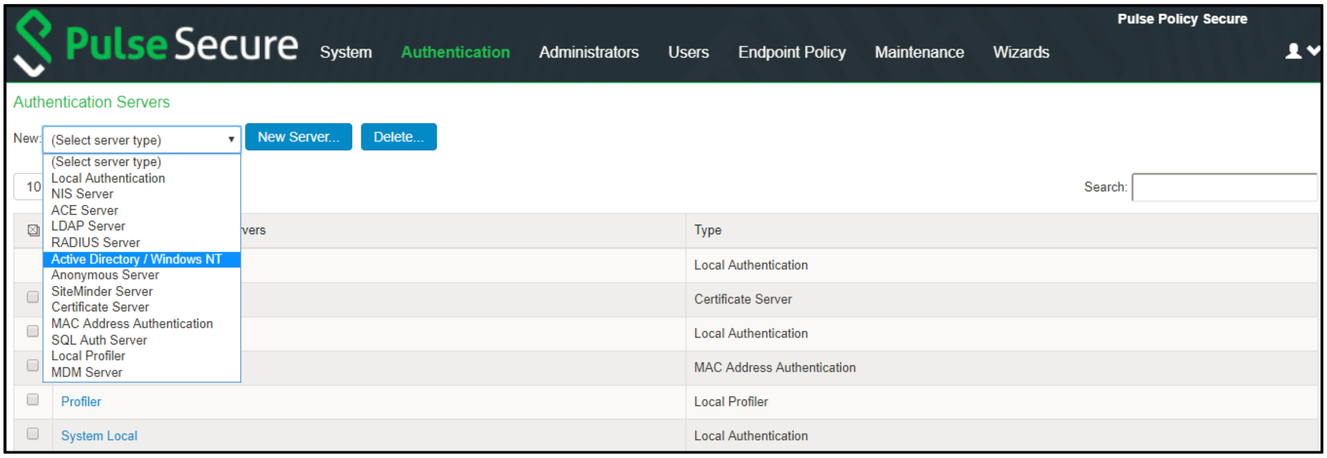
Navigate to System > Reports > Devices Discovery to start seeing devices with static IP addresses on the network. Profiler will periodically poll the switches to ensure that new devices get profiled as they connect to the network.

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



Authentication Servers

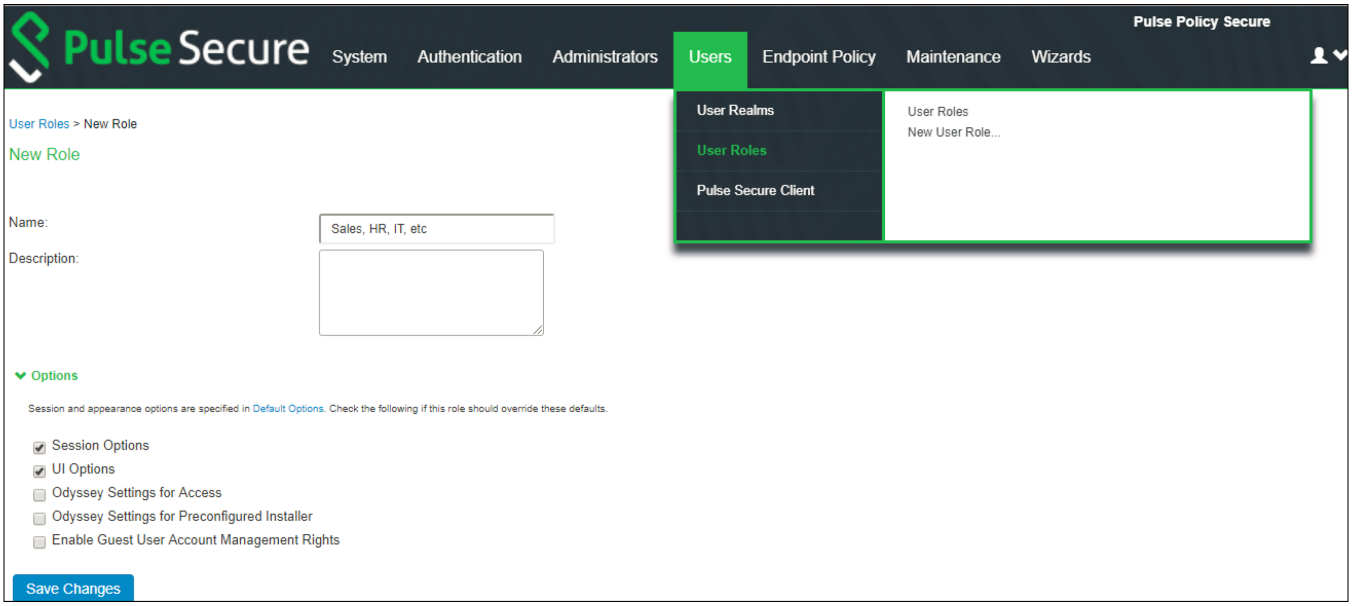
New: (Select server type)

(Select server type)
Local Authentication
NIS Server
ACE Server
LDAP Server
RADIUS Server
Active Directory / Windows NT
Anonymous Server
SiteMinder Server
Certificate Server
MAC Address Authentication
SQL Auth Server
Local Profiler
MDM Server

	...vers	Type
		Local Authentication
□		Certificate Server
□		Local Authentication
□		MAC Address Authentication
□	Profiler	Local Profiler
□	System Local	Local Authentication

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

Figure 24: User Role Configuration



User Roles > New Role

New Role

Name: Sales, HR, IT, etc

Description:

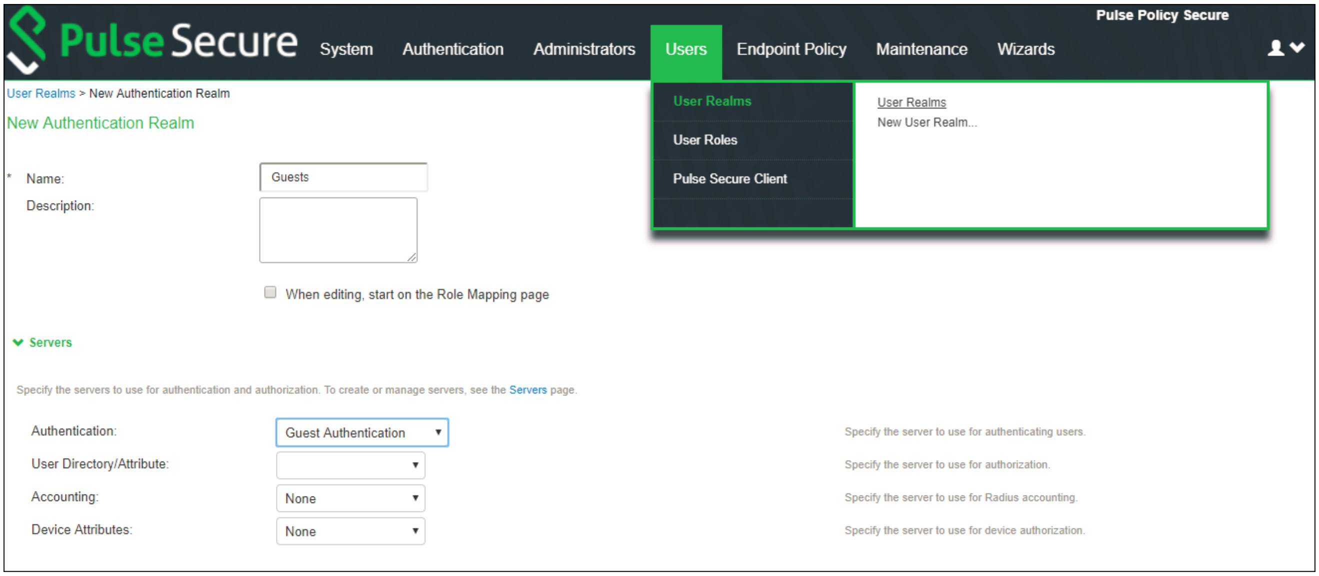
Options

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

3. To configure user realm, navigate to Users > User Realms and create a new realm or edit a realm you have already created.

Figure 25: User Realm Configuration



User Realms > New Authentication Realm

New Authentication Realm

* Name:	Guests
Description:	

□ When editing, start on the Role Mapping page

Servers

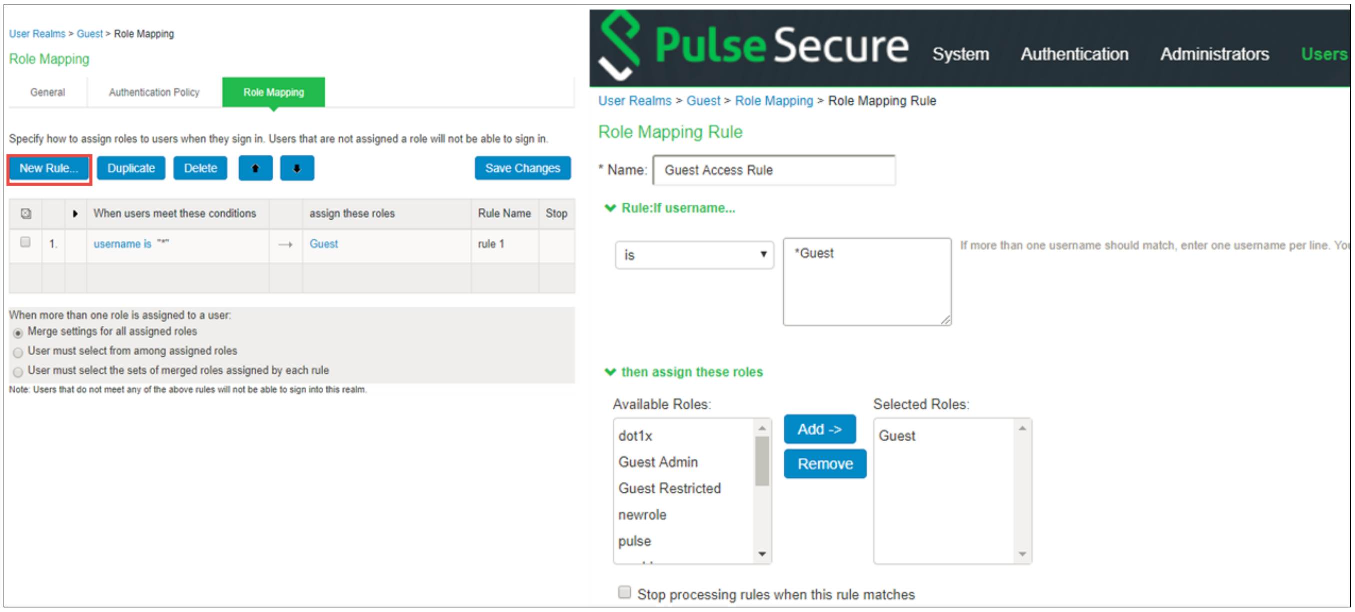
Specify the servers to use for authentication and authorization. To create or manage servers, see the Servers page.

Authentication:	Guest Authentication	Specify the server to use for authenticating users.
User Directory/Attribute:		Specify the server to use for authorization.
Accounting:	None	Specify the server to use for Radius accounting.
Device Attributes:	None	Specify the server to use for device authorization.

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.

Figure 26: Create Role Mapping Rule



User Realms > Guest > Role Mapping

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.

			When users meet these conditions		assign these roles	Rule Name	Stop
□	1.		username is "*"	→	Guest	rule 1	

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.

User Realms > Guest > Role Mapping > Role Mapping Rule

Role Mapping Rule

* Name: Guest Access Rule

Rule:If username...

is | *Guest | If more than one username should match, enter one username per line. Yo

then assign these roles

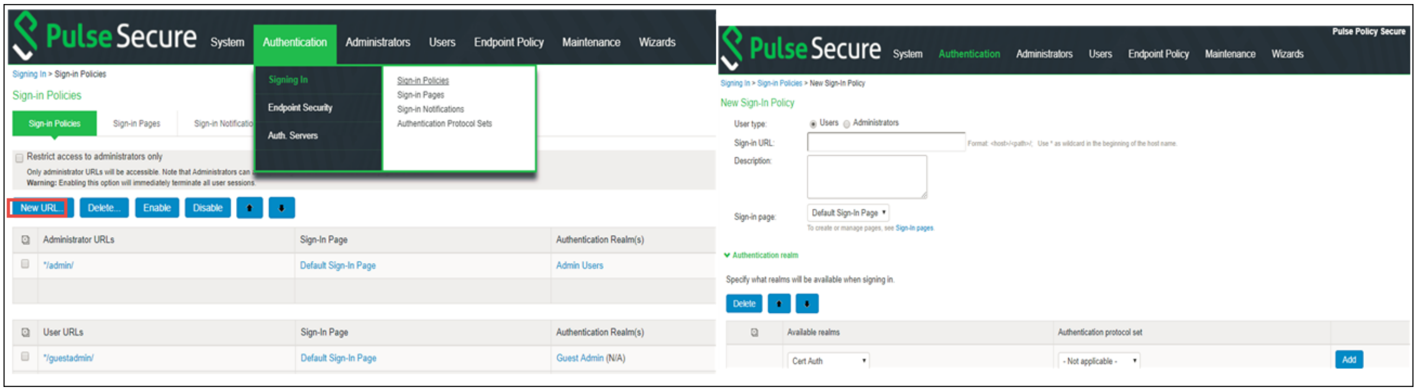
Available Roles: dot1x, Guest Admin, Guest Restricted, newrole, pulse

Selected Roles: Guest

□ Stop processing rules when this rule matches

5. To configure sign-in policy, navigate to Authentication > Signing In > Sign-In Policies and complete the configuration.

Figure 27: Configure Sign-in Policy



Signing In > Sign-in Policies

Sign-in Policies

□ Restrict access to administrators only

Only administrator URLs will be accessible. Note that Administrators can

Warning: Enabling this option will immediately terminate all user sessions.

□	Administrator URLs	Sign-In Page	Authentication Realm(s)
□	*/admin/	Default Sign-In Page	Admin Users

□	User URLs	Sign-In Page	Authentication Realm(s)
□	*/guestadmin/	Default Sign-In Page	Guest Admin (N/A)

Signing In > Sign-in Policies > New Sign-In Policy

New Sign-In Policy

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.

□	Available realms	Authentication protocol set	
	Cert Auth	- Not applicable -	Add

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**