portnox™
CLEAR

Quick Start Guide

December 14, 2016

What is Portnox CLEAR

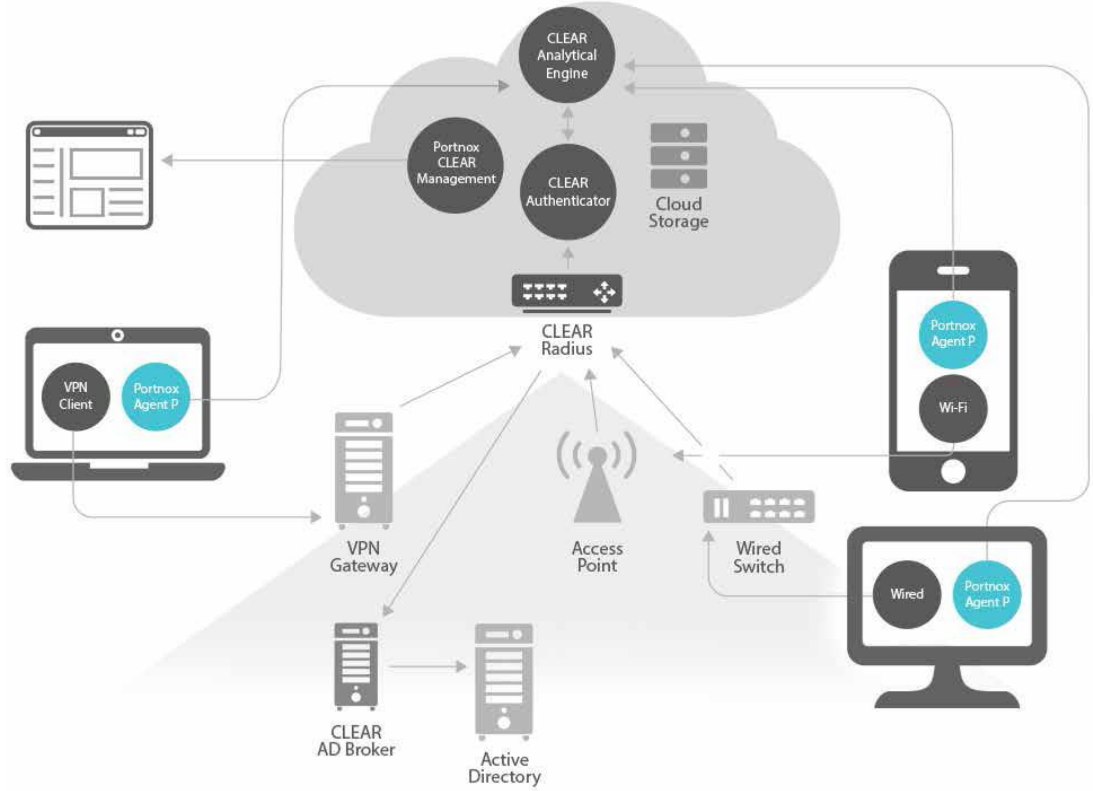
Portnox CLEAR is a cloud-based continuous monitoring and risk-based access control solution for devices accessing the corporate network.
It performs real-time monitoring and analysis of hundreds of end-user device parameters: configurations, applications, activities, vulnerabilities, and anomalies. It then performs risk assessment and makes an access-control decision.
CLEAR also provides network visibility and discovery and enables answering various questions about the connected device, such as: which software is installed and patched, which processes are running, which peripheral devices are or were attached, with which other devices is it communicating, etc.
The solution consists of a cloud-based analytic engine, RADIUS in the cloud, and a light-weight agent installed on end-devices.

How Portnox CLEAR works

1. A light-weight agent called Portnox AgentP is installed on each end-device. AgentP continuously gathers and sends device risk-state data to the CLEAR analytical engine. All data stored with CLEAR is protected using strong encryption measures.
2. Each device is on-boarded to Portnox CLEAR based on an organizational email identity or optionally on an organizational domain identity (Active Directory or Open LDAP), and is assigned to a defined CLEAR group.

   Note that CLEAR also support onboarding and authentication of devices without AgentP.

3. Portnox CLEAR groups define which networks (WiFi, wired, VPN) the device may access, and automatically manages all associated connection credentials.
4. The engine continuously calculates a security risk score for each AgentP device, which determines whether (and where) the device may connect to the corporate network. The corporate administrator can fine-tune the risk score calculation by modifying the security risk policies of security groups.
5. When an end-device attempts to connect to the corporate network, the CLEAR Radius in the cloud:
   - Verifies the device was on-boarded and the credentials are correct.
   - Verifies access location/type (wireless, wired, VPN)
   - Makes an access decision based on the device's current risk score: Allow, Deny, or Allow with Alert.
6. If access is denied, CLEAR sends a security alert to the CLEAR admin and to the end user.



Setting Up Portnox CLEAR

Follow these simple steps to configure, enable and start gaining the continuous device monitoring and access control values of CLEAR. Should you encounter any problems or have questions, we are available to help, just drop us an email to clearsupport@portnox.com.

Step 1. Create your CLEAR account

a. Navigate to https://clear.portnox.com/ and click **Get Started**.

b. Submit your information in the Registration page. When providing an email address, provide one with the same email domain as that of the users who will be registering for the service. No public email addresses are allowed, such as @gmail.com, @hotmail.com, etc.

c. You will receive back a Welcome email. Click the activation link in the email.

If you plan to use CLEAR only for continuous risk monitoring with no access control, skip to Step 6a.

Step 2. Configure RADIUS for CLEAR access control

CLEAR supports RADIUS access controls across wireless, wired and VPN. To enable RADIUS access controls, go to **Settings** > **Services** and expand **CLEAR RADIUS Service**. Then:

a. Click **Edit**, and check the **Enable Cloud RADIUS** checkbox.

b. Note the RADIUS server details which you will need when configuring your RADIUS clients, devices and equipment in Steps 4a, 4b, 4c and/or 7.

Step 3. Active Directory (Open LDAP) Integration

Active Directory/LDAP Integration is REQUIRED if any of the following are true:

- You will use Portnox CLEAR to authentication wired/wireless access via Active Directory/LDAP (Steps 4a and 4b)
- You will use Portnox CLEAR for VPN access control (Step 4c)
- You want user onboarding & management via the organizational user repository (as opposed to email)

To enable your site for Portnox Active Directory/Open LADP integration, simply follow the steps below:

a. In the CLEAR portal, navigate to **Settings** > **Services** > **Directory Integration Service**, and enter the details of the organization's Domain Controller.

b. Download the Portnox™ Active Directory Broker found at **Settings** > **Services** > **Directory Integration Service** and install it in the organization on a domain-joined machine.

c. Make sure that machine has outgoing internet connection over HTTPS to ports 8081 and 443.

Step 4. Configure the network access layers that will use CLEAR

CLEAR supports all your network access layers. Follow the steps below for those access layers you want to support with CLEAR.

Step 4a. CLEAR for Wireless access control

Perform the following for every Wi-Fi network you plan to protect with CLEAR:

a. Navigate in the portal to **Settings** > **Groups**. Edit the default "Unassigned" group or create new security groups (Step 5). Whether you are creating or editing a group, in **Group Settings** click **Add Wi-Fi network** and specify:

- The SSID of the network you wish to secure.
- The Authentication type IEEE802.1X PWD.
- The Authentication Encryption type as defined on your Wi-Fi equipment.

b. Configure your Wi-Fi network equipment to use CLEAR's RADIUS server – whose details you noted down in Step 2 – for device authentication. See the Knowledge Base in the Portnox support site for a Wi-Fi configuration example.

Step 4b. CLEAR for Wired access control

a. Navigate in the portal to **Settings** > **Groups**. Edit the default "Unassigned" group or create new security groups (Step 5). Whether you are creating or editing a group, in **Group Settings** > **Access to Wired Networks** do the following:

- Check the **Enable wired access using 802.1x authentication for devices in this group** checkbox.
- Optionally, check also the **Enable Dynamic VLAN Assignment for devices in this group** checkbox, and specify a VLAN ID.

b. Define 802.1x authentication on your wired switch, using the CLEAR RADIUS server details you noted down in Step 2.

Step 4c. CLEAR for VPN access control

a. in the CLEAR portal under **Settings** > **Services** > **VPN 2FA Service**:

- In **Primary Authentication Factor**, select **Enable validation of user credentials against user repositories**.
- In **Strong Authentication Factor**, select one of the following:
  - **None –** Portnox CLEAR does not provide Strong authentication; it is up to the organization to provide this
  - **One Time Password (OTP) –** AgentP serves as a soft token for OTP generation
  - **Portnox AgentP –** Portnox CLEAR calls back the specific AgentP on the device requesting access, to verify that the device is the one it claims to be

b. Navigate in the portal to **Settings** > **Groups**. Edit the default "Unassigned" group or create new security groups (Step 5). Whether you are creating or editing a group, in **Group Settings** check the **Enable VPN access using Portnox two-factor authentication for devices in this group** checkbox.

c. Define RADIUS authentication on your VPN Gateway using the CLEAR RADIUS server details you noted down in Step 2. See the Knowledge Base in the Portnox support site for a VPN Gateway configuration example.

Step 5. Define CLEAR Security Groups (Optional)

a. Assign end-users to groups either manually, or by mapping Active Directory/LDAP groups to CLEAR security groups. If the latter, you must deploy the Portnox™ Active Directory Broker (Step 3) if you haven't done so already.

b. Assign to security groups the risk policies you define in the portals Policies page.

Step 6. Onboard Users/Devices

Portnox CLEAR supports several methods of onboarding devices/users depending on your need and the type of device (user, IoT). Follow the steps below based on your specific need and environment.

Step 6a. Portnox AgentP Enrollment

For corporate and BYOD devices, AgentP enrollment supports the most feature-rich use of CLEAR, including continuous risk monitoring, risk-based access controls and automated credential management.

a. Download the AgentP that corresponds to the device's OS:

- iOS (iPhone and iPad) – Search for the Portnox AgentP App on App Store, or click the link: https://itunes.apple.com/us/app/portnox-agentp/id861819015?mt=8
- Android – Search for the Portnox AgentP App on Google Play, or click the link: https://play.google.com/store/apps/details?id=com.portnox.agentp&hl=en
- Windows and OS X – Click the link: https://clear.portnox.com/agentinstall

b. Install AgentP on the device and enroll. The user can create either:

- A Portnox CLEAR account, using his corporate email; or
- A Directory account based on the user's domain identity (Active Directory or Open LDAP), if the organization deployed and configured a Portnox™ Active Directory Broker (Step 3)

Step 6b. Portnox Agentless & IoT Device Onboarding

The options below are to support onboarding of user devices without AgentP and of devices that cannot support an agent such as printers, VoIP and other internet-of-things (IoT) devices.

- CLEAR admin onboarding. In this case, create user accounts using **Create new account** in the Portal's **Devices** page. You can create the following types of user accounts:
  - A Portnox CLEAR account, based on a user's corporate email
  - A Directory account based on the user's domain identity (Active Directory or Open LDAP), if the organization deployed and configured a Portnox**™** Active Directory Broker (Step 3)
  - A MAC-based account, based on a device's MAC address. Intended mainly for Internet of Things devices
  - A Contractor account, based on a user's non-corporate email

! Note that security risk assessment and scoring cannot be performed for non-AgentP devices.

- Self-onboarding. In this case, you must:
  a. Go to **Settings** > **Services** > **CLEAR General Settings** > **On-boarding**, and check the **Allow self-onboarding by end-user** option.
  b. Send users the URL of a self-onboarding site, where each user can create either:
    - A Portnox CLEAR account, using his corporate email; or
    - A Directory account based on the user's domain identity (Active Directory or Open LDAP), if the organization deployed and configured a Portnox**™** Active Directory Broker (Step 3)

! Note that security risk assessment and scoring cannot be performed for non-AgentP devices.

Step 7. Guest Access Management (Optional)

Portnox CLEAR supports several methods of onboarding and managing your guest network access. Download the *Guest Network Management Guide* from the CLEAR portal for configuration guidelines.

! Technical questions or issues? Email: clearsupport@portnox.com

Purchase CLEAR or license cost questions? Email: clearsales@portnox.com

portnox™ CLEAR

For further information please visit us at: portnox.com