Portnox CLEAR

Quick Start Guide

What is Portnox CLEAR?

Portnox CLEAR is a cloud-delivered network access control solution providing actionable network visibility and risk management of endpoints in any location, on or off campus. CLEAR delivers continuous risk monitoring of all endpoints – IoT, BYOD and managed devices, across wired, wireless and virtual networks.

As a cloud-delivered solution, CLEAR is always running the most updated version with the latest features and capabilities. The solution authenticates devices by various repositories and goes deep into the security posture of the endpoint. The network access is granted based on user/device's identity or certificate, as well as a device's risk profile.

How Portnox CLEAR Works

1 Initial account setup for the enterprise is done online within a few minutes and then any endpoint, in any location is on-boarded to the Portnox CLEAR account by using a corporate email or a **domain** directory* identity (on-prem Active Directory, Azure AD, G Suite or Okta UD).

2 Each account is assigned to a group based on company policies. CLEAR's groups define which networks (Wireless, Wired, VPN) the account (and its devices) has access to, and from here on out CLEAR will automatically keep track and manage all associated identities.

3 The CLEAR engine assigns the following policies:

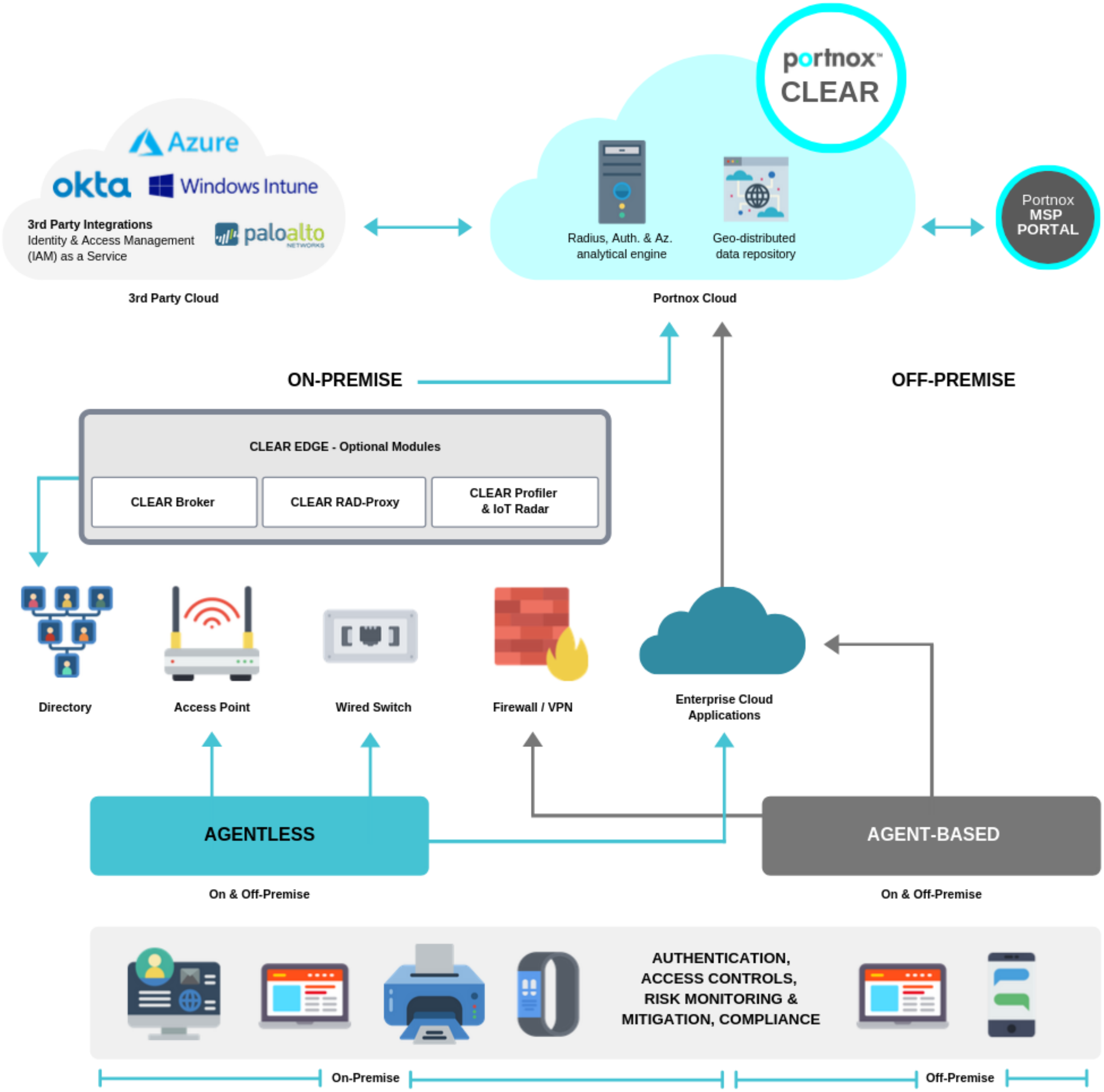
- Access Control Policy: Allow / Deny Access or assign VLAN / ACL upon successful authentication, authentication failure, risk policy violation and blocking by Admin

- Risk Assessment and Remediation Policies: requires a lightweight AgentP on endpoints. Supported with OS X, Windows, Linux, iOS and Android

4 All authentication, authorization and enforcement events are immediately reflected by the real-time Alerts

Open LDAP is supported as well

Portnox CLEAR Architecture

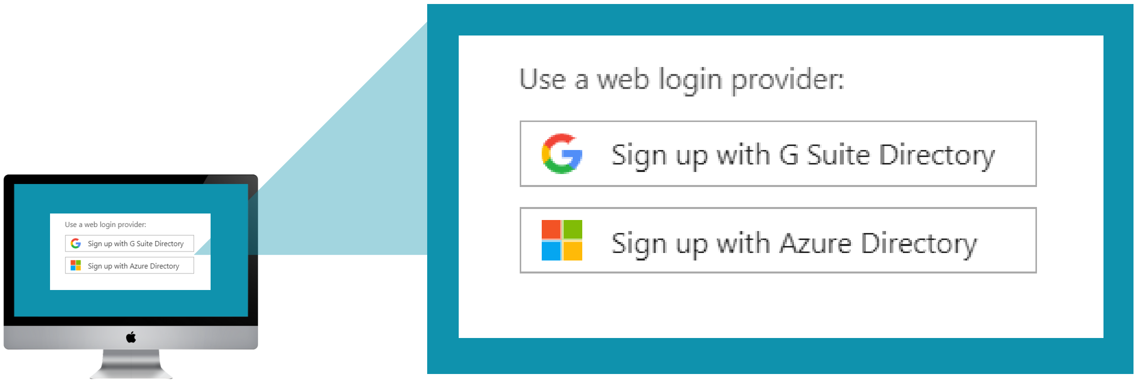


Setting Up Portnox CLEAR

Follow these seven 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 or visit our support portal at https://www.portnox.com/support/

1 Create Your CLEAR account

- Navigate to https://clear.portnox.com/ and click **Sign Up**
- 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.
- You will receive back a Welcome email. **Click the activation link in the email.**
- In addition, we support sign up by SSO using G Suite or Azure Directory identity

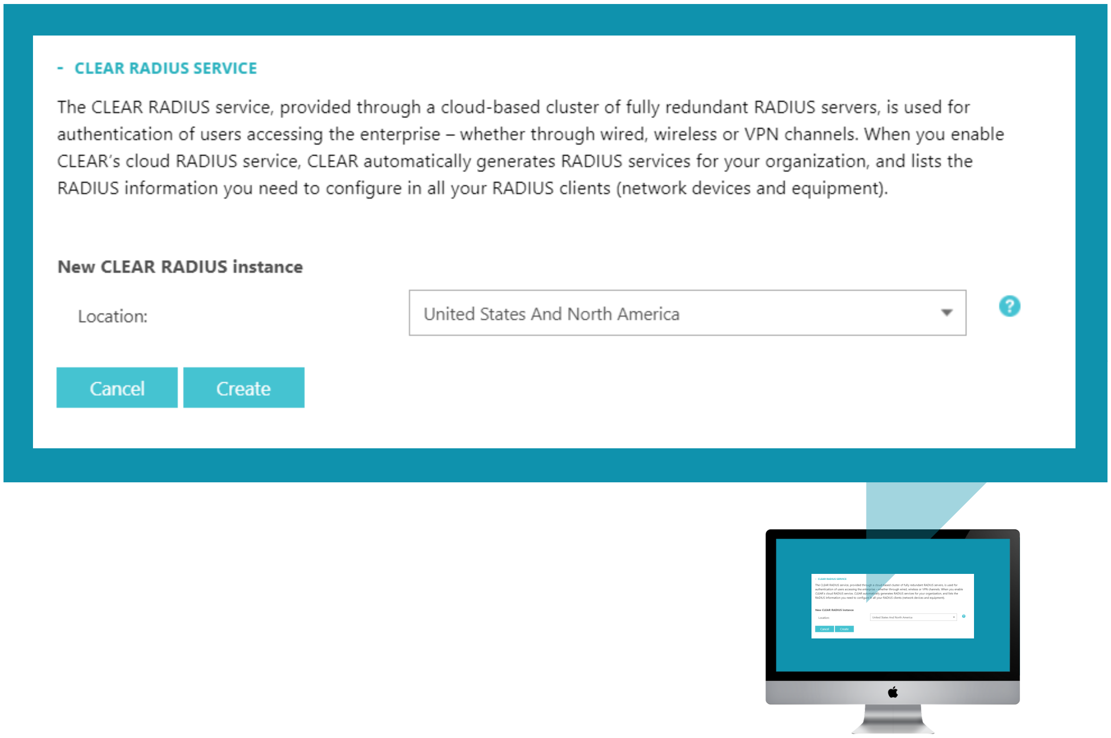

Use a web login provider:
Sign up with G Suite Directory
Sign up with Azure Directory

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:

- Hit Create new **CLEAR RADIUS instance**, chose the Radius instance according to your geo-location, press **Create**



- CLEAR RADIUS SERVICE

The CLEAR RADIUS service, provided through a cloud-based cluster of fully redundant RADIUS servers, is used for authentication of users accessing the enterprise – whether through wired, wireless or VPN channels. When you enable CLEAR's cloud RADIUS service, CLEAR automatically generates RADIUS services for your organization, and lists the RADIUS information you need to configure in all your RADIUS clients (network devices and equipment).

New CLEAR RADIUS instance

Location: United States And North America

- Click on your newly created RADIUS server to view details which you will need when configuring your RADIUS clients, devices and equipment in Steps 4a, 4b, 4c and/or 7.

3 Directory Integration as Authentication Repository

! Directory Integration is required for:

- Network Authentication by Directory Identities
- Endpoints on-boarding via AgentP enrollment or Agelessness Self-Onboarding
- Directory Identities mapping for Policies assignment Network Access restriction

To enable your site for Portnox Directory integration, simply refer to the guides below:

- **On-prem or Azure AD:** https://portnox.box.com/v/adbroker
- **G Suite Directory:** https://portnox.app.box.com/v/GSUITECLEARIntegration
- **Okta Universal Directory:** https://portnox.box.com/v/OKTADirectoryCLEARIntegration

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.

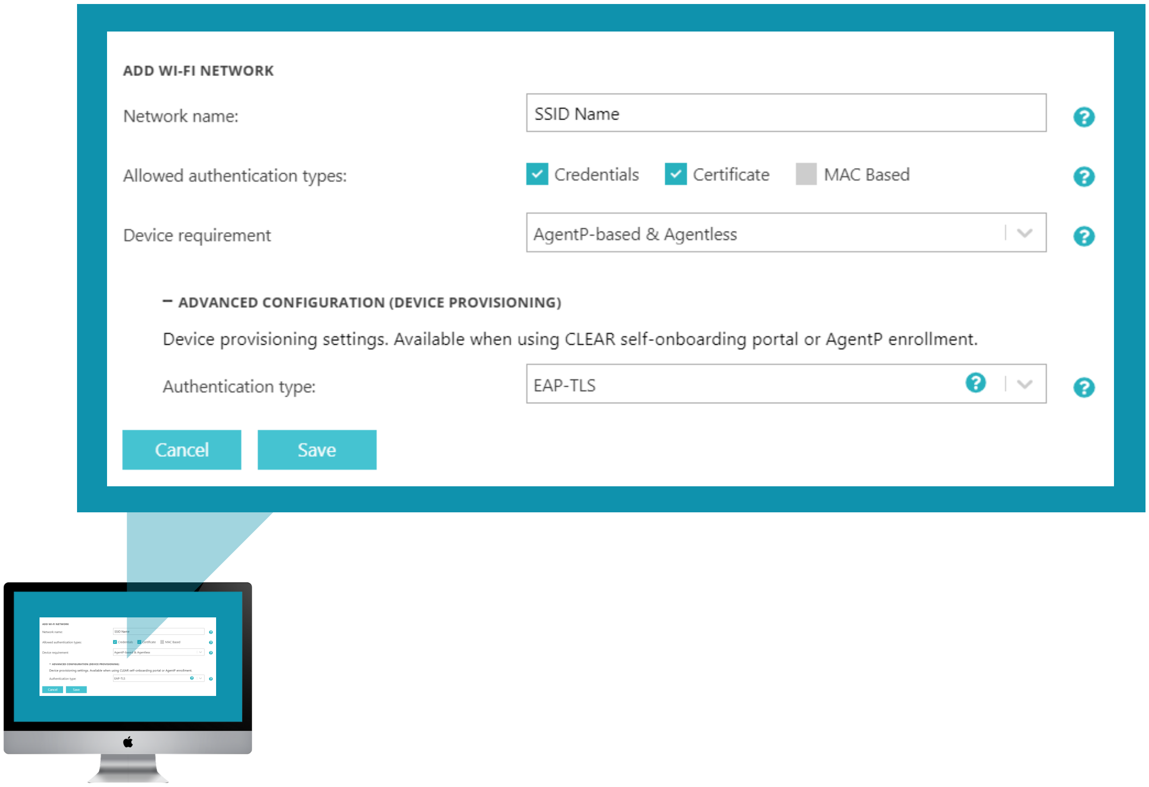
4a. CLEAR for Wireless Access Control

Perform the following for every WiFi network you plan to protect with CLEAR:

- Navigate in the portal to Groups. Edit the Default group or create new security groups (Step 5). Whether you are creating or editing a group, in **Group Settings > 802.1X WIRELESS NETWORK ACCESS**, click **Add WiFi network** and specify:

4a. CLEAR for Wireless Access Control (Continued)

- The SSID of the network you wish to secure.
- The allowed authentication type(s)
- The Device requirement: Agent-based & Agentless, Agent-based only or Agentless only
- Expand “ADVANCED CONFIGURATION (DEVICE
- PROVISIONING)” to select the desired authentication type for devices’ provisioning. Note: a single Certificate authentication selection allows EAP-TLS provisioning only. Device provisioning is irrelevant for MAC Based Authentication type
- Click Save



ADD WI-FI NETWORK

Network name:	SSID Name
Allowed authentication types:	☑ Credentials ☑ Certificate □ MAC Based
Device requirement	AgentP-based & Agentless

– ADVANCED CONFIGURATION (DEVICE PROVISIONING)

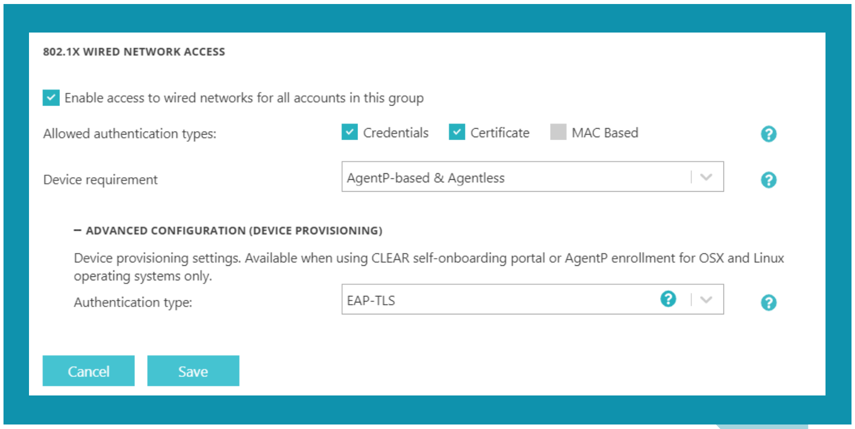
Device provisioning settings. Available when using CLEAR self-onboarding portal or AgentP enrollment.

Authentication type:	EAP-TLS

- Configure your WLAN 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 here for a configuration example.

4b. CLEAR for Wired Access Control

- Navigate in the portal to Groups. Edit the Default group or create new security groups (Step 5). Whether you are creating or editing a group, in **Group Settings > 802.1X WIRED NETWORK ACCESS** and specify:
  - The allowed auhentication type(s)
  - The Device requirement: Agent-based &
  - Agentless, Agent-based only or Agentless only
  - Expand "ADVANCED CONFIGURATION (DEVICE
  - PROVISIONING)" to select the desired authentication type for devices'
  - provisioning.
  - Note: device provisioning for wired connection is applicable for OSX and Linux operating systems only
  - Click Save



802.1X WIRED NETWORK ACCESS

☑ Enable access to wired networks for all accounts in this group

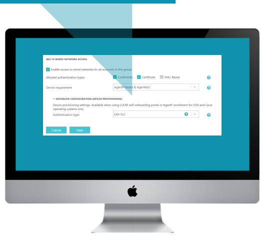
Allowed authentication types: ☑ Credentials ☑ Certificate □ MAC Based

Device requirement: AgentP-based & Agentless

– ADVANCED CONFIGURATION (DEVICE PROVISIONING)

Device provisioning settings. Available when using CLEAR self-onboarding portal or AgentP enrollment for OSX and Linux operating systems only.

Authentication type: EAP-TLS

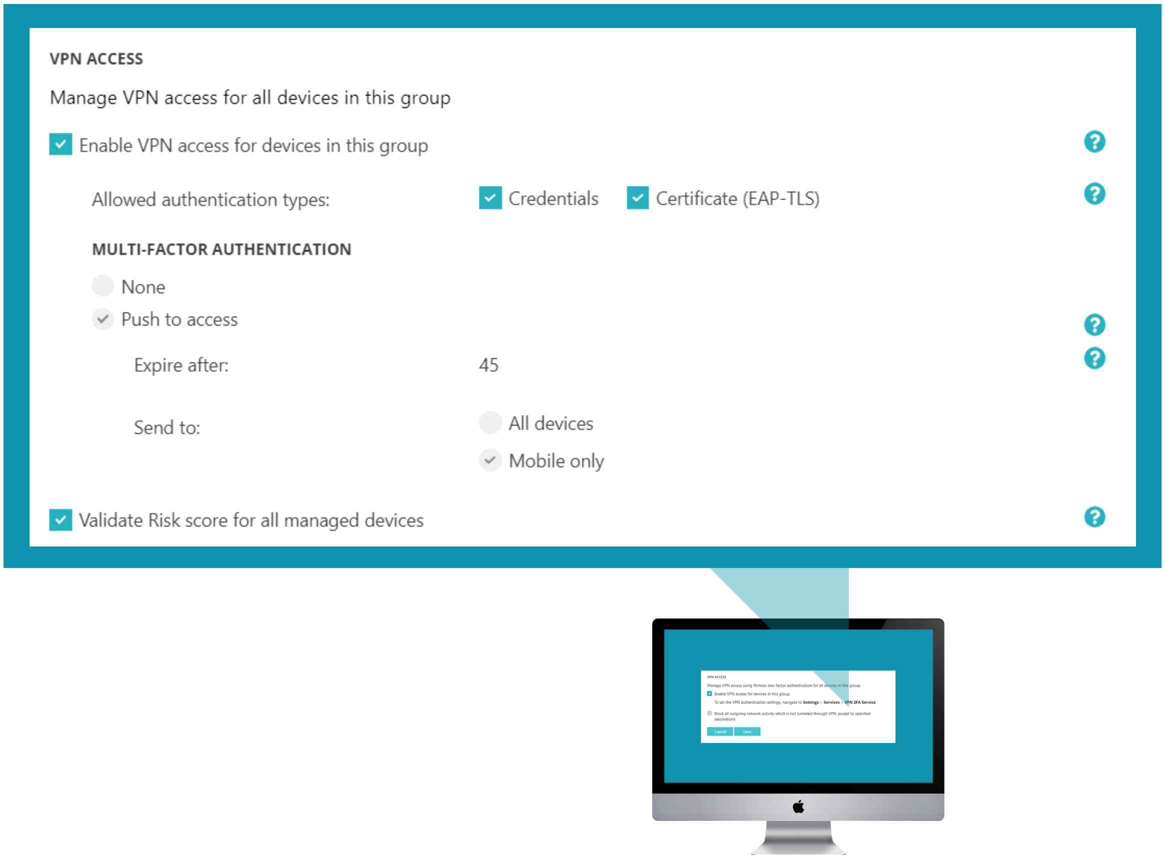


4c. CLEAR for VPN Access Control

- Navigate in the portal to **Groups**. Edit the Default group or create new security groups (Step 5). Whether you are creating or editing a group, in **Group Settings** check the **Enable VPN access for devices in this group** checkbox.

4c. CLEAR for VPN Access Control (Continued)

- Select the Allowed Authentication Type(s)
- Set the desired Multi-factor authentication type:
  - **None** – Portnox CLEAR does not provide Strong authentication; it is up to the organization to provide this
  - **Push-To-Access** – Push notifications to AgentP device for user to approve connection.
    - All Devices – Local AgentP authorizes VPN connection of the client
    - Mobile only – External AgentP app on iOS or Android devices authorizes VPN access for computers



VPN ACCESS

Manage VPN access for all devices in this group

☑ Enable VPN access for devices in this group

Allowed authentication types: ☑ Credentials ☑ Certificate (EAP-TLS)

MULTI-FACTOR AUTHENTICATION

○ None

✓ Push to access

Expire after: 45

Send to: ○ All devices ✓ Mobile only

☑ Validate Risk score for all managed devices

- 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 here for a VPN Gateway configuration example.

5 Define CLEAR Security Groups (Optional)

- Assign end-users to groups either manually - CLEAR / Contractors or MAC-based accounts - or by mapping the Directory (on-prem Active Directory, Azure AD, G Suite or Okta UD) groups to CLEAR security groups. If this is an on-prem Active Directory, you must deploy the Portnox™ Active Directory Broker (Step 3) if you haven't done so already. Note that automatic agentless accounts onboarding upon successful authentication requires checking the "Enable automatic LDAP-based device onboarding" box at **Group Settings > Automatic Device Onboarding**

- Assign to security groups the access control, risk and remediation policies you define in the portal's Policies page.

6 On-Board Users / Devices

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

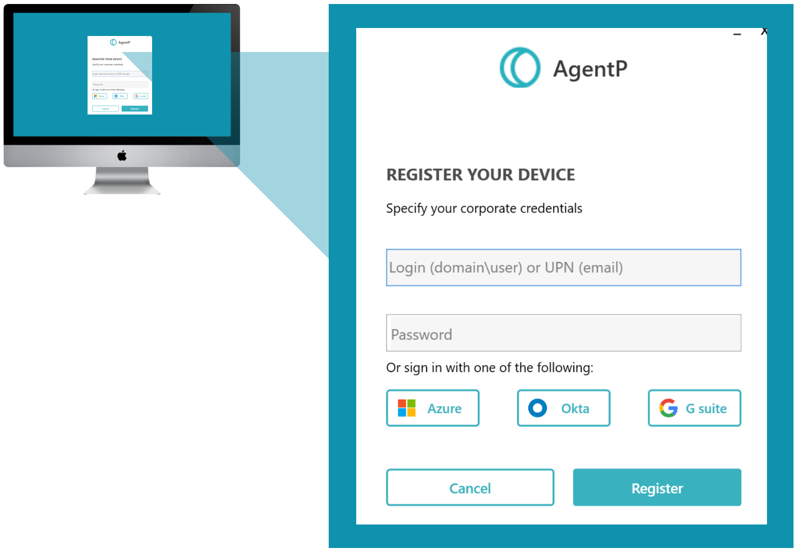
6a. Portnox AgentP Enrollment

For corporate and BYOD devices, AgentP enrollment supports the most feature-rich use of CLEAR, including continuous risk monitoring, risk-based access controls, remediation, certificates distribution (for credentials-free authentications) and automated credential management.

- 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, OS X and Linux – Click the link: https://clear.portnox.com/agentinstall

6a. Portnox AgentP Enrollment (Continued)

- 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 identity if the organization deployed and configured a Portnox™ Active Directory Broker (Step 3) AgentP supports enrollment using federated services (MFA) with Azure, Okta and G Suite



AgentP

REGISTER YOUR DEVICE

Specify your corporate credentials

Or sign in with one of the following:

6b. Portnox Agentless & IoT Device On-Boarding

The options below are to support on-boarding 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 identity (on-prem Active Directory, Azure AD, G Suite or Okta UD), if the organization deployed and configured a Portnox™ on-prem Active Directory Broker (Step 3)

6b. Portnox Agentless & IoT Device On-Boarding (Continued)

- 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

! AgentP is mandatory for continuous risk monitoring, risk-based access controls and remediation.

- Self-onboarding. In this case, you must:
  - Go to **Settings > Services > CLEAR General Settings > Self On-Boarding**, and check the **Allow self on-boarding by end-users** option.
  - Send users the URL of a self on-boarding 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 (on-prem Active Directory, Azure AD, G Suite or Okta UD), if the organization deployed and configured a Portnox™ on-prem Active Directory Broker (Step 3)

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

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™

About Portnox

Portnox provides simple to deploy, operate and maintain network security, visibility and access control solutions. Portnox software can be deployed on-premises, as a SaaS/cloud-delivered service, or in hybrid mode. It is agentless and is vendor agnostic, allowing organizations to maximize their existing network and cybersecurity investments. Hundreds of enterprises around the world rely on Portnox for network visibility, cybersecurity policy enforcement and regulatory compliance. The company has been recognized for its innovations by Info Security Products Guide, Cyber Security Excellence Awards, IoT Innovator Awards, Computing Security Awards, Best of Interop ITX, Cyber Defense Magazine and more. Portnox has offices in the U.S., Europe and Asia.

www.portnox.com // clearsupport@portnox.com