portnox™

WHITE PAPER

# 802.1X Authentication Is Simpler Than You Think

Examination of a new and simple way of implementing 802.1x for stronger authentication

## Executive Summary

The following whitepaper presents existing challenges with the IEEE 802.1X standard for port-based Network Access Control (NAC) and authentication, suggesting that much of the frustration centers on deployment, the complexity of integration, the need for expensive hardware, and issues authorizing access based on level of device compliance. It then presents some of the benefits that 802.1X authentication affords, such as integrated management, ease of use in setting access permissions and enhanced security that is not based on pre-shared keys (PSKs). With both the challenges and benefits in mind, the whitepaper presents Portnox CLEAR – a turn-key solution for 802.1X from the cloud that maximizes the benefits and applications of the authentication standard.

## The Pain of 802.1X Authentication

The 802.1X standard for authenticating access to wired and wireless networks has met with a good deal of scrutiny in recent years. While 802.1X was considered a success when initially implemented on wired networks, with the shift to wireless networks, the growth of the geo-distributed organizations and the proliferation of internet-connected devices, the tides of opinion shifted, casting 802.1X in a negative light due to the difficulty and sheer expense of implementation.

Deployment of 802.1X is the main pain point as it requires support from RADIUS/AD servers at every location, making authentication available only when devices are physically present in the office, and requiring manual configuration of endpoints with an agent. This makes the implementation of 802.1X daunting, often taking systems administrators and engineers weeks to configure (and even more if a user repository is not already in place). This can take even longer (and cost much more) if being implemented in a geo-distributed organization that needs continually authenticate endpoints. As a result, deployment of 802.1X authentication protocols often feel like more of a headache than a help.

## So Why Reconsider 802.1X?

Aside from implementation woes, 802.1X remains the one of the best ways to authenticate devices because of its continuous and direct communication with the authenticating, as opposed to pre/post scanners or other less secure authentication solutions that expose the network to vulnerabilities (see more below).

### Here's why:

#### 1. Ease of Management

Unlike other authentication methods that use pre-shared keys (PSKs), which are difficult to control and can result in unauthorized access if not properly managed, 802.1X depends on certificates (WEP) and/or user credentials to grant access. These certificates/credentials can be effectively managed from the server, and the method uses existing backend infrastructure, simplifying implementation and policy administration. 802.1X is a highly integrated solution across all pillars of authentication: PKI and credential management, as well as automated management of access based on information from user repositories.

#### 2. Ease of Use

Despite the myth that 802.1X is more demanding of end users than other authentication solutions due to dependence on an agent, all it requires is that end users enter their credentials when promoted by the wired/wireless supplicant. This prompt is issued once, unless passwords or certificates have been altered. Group policies automatically configure the end user's device for connection based on their specific group permissions. 802.1X allows for full end-to-end provisioning, automating deployment, management and troubleshooting tasks.

#### 3. Security

02.1X is one of the best methods for secure authentication of devices because authentication keys are individual and not shared like PSKs. Contextual information on users can be retrieved from the authentication server, such as roles like "Staff" or "Visitor". Role assignment makes it possible to devise specific access policies (known as Role Based Access Control), and it's possible to track individual users, removing them from the network if they pose a threat.

## 802.1X Delivered as a Cloud Service

Armed with knowledge of the benefits of 802.1X, Portnox CLEAR was created to offer a solution that addresses the biggest pain point – deployment and implementation – delivering 802.1X authentication as a software-defined cloud service without compromising on security.

- **No Physical Deployment or Network Hardware:** Portnox CLEAR introduces hyper-availability of 802.1X authentication, eliminating geo-redundancies and addressing business continuity needs by offering secure access to the network from every location for geo-distributed organizations. An appliance-free, limitless deployment is made possible for the cloud agile enterprise. The solution answers the challenges faced by companies after a merger or acquisition bridging the IT implementation gaps by making 802.1X readily accessible at all times.
- **Automation of Policy Enforcement:** Portnox CLEAR allows for automated full end-to-end provisioning and configuration, including the deployment of agents and management of network access and security policies. Using information from the supplicant and the authentication server, Portnox CLEAR characterizes device risk with the help of contextual device information called a "Risk Score". Risk Scores are used to grant or deny access based on compliance with network and cloud access policies, such as geolocation, time of access, active applications, security posture, patching status, and more. With Risk Scores, it's easier to identify, characterize and address issues with malicious devices, automatically limiting or blocking access, if needed.
- **No Post Scanners or Logs:** In an effort to simplify 802.1X deployment, some security vendors offer post scanners or log referencing to extend 802.1X across geolocations and endpoints. However, these solutions are inherently insecure as they scan for vulnerabilities only after the device has connected to the network, making it difficult to carry out remediation. By taking 802.1X to the cloud, Portnox CLEAR eliminates the necessity for post scanners and logs, keeping the network secure and closing a major window of vulnerability for the organization.

## Conclusion – It Can Be That Simple

Though many security professionals have knowledge of 802.1X's strengths, deployment on wireless networks has presented significant implementation barriers. By delivering 802.1X as a cloud service, Portnox CLEAR radically simplifies 802.1X deployment without compromising on security, making it an essential solution for enterprises invested in the cloud computing, geo-distribution and enterprise mobility.

To summarize, obtaining the benefits of 802.1X authentication without the headache of on-premise deployment or compromising on security is what Portnox CLEAR is all about.

**Find out more to radically simplify your 802.1X deployment here:**
https://www.portnox.com/portnox-clear/

**Contact Us**

Americas: usinfo@portnox.com | +1.855.476.7866
Europe: dotell@portnox.com | +44.1273.256325

www.portnox.com

www.twitter.com/portnox
www.facebook.com/portnox
www.linkedin.com/company/2526271/
www.youtube.com/portnox