Portnox + Okta

SSO integration for Portnox's
NAC-as-a-Service solution.

okta

Portnox CLEAR, our cloud-delivered NAC-as-a-Service solution, integrates with Okta for improved identity and access management (IAM). This integration helps to simplify and secure identity management processes for new and existing CLEAR customers who already rely on Okta for single sign-on (SSO).

Understanding the benefits.

The Portnox-Okta integration offers several distinct use case benefits for organizations, including:

SSO & multi-factor authentication (MFA)
Portnox admins can now perform SSO and optionally use Okta MFA to access the Portnox admin console.

End-user self-onboarding
End-users can simplify the Portnox self-onboarding process for various endpoints by using their Okta credentials for SSO.

Network authentication synchronization
Admins can synchronize network authentication and access segmentation with pre-determined Okta groups.

Risk-based application access
Portnox risk scoring can be leveraged as part of the decision-making process to grant or deny access to certain cloud apps.

Questions?

We want to hear from you! Send us a note at **support@portnox.com**.

Simple & secure.

Out-of-the-Box SAML Integration – Enjoy an easy and secure self-onboarding process together with simplified identity management.

Radius-as-a-Service Authentication – Avoid the overhead and complications of on-premises equipment. Keep things simple with cloud-delivery.

Simplified Guest & BYOD Access – Grant access for managed devices and restrict access based on endpoint risk policies for all devices.

Real-Time Risk Assessment – Continuously monitor and deal with all endpoints based on your organization's security policies.

Flexible Access Controls – Use built-in parameters such as geo-location, known threats, open ports, security posture and more to determine access together with SSO credentials.

Enhanced Security Intelligence – Gain contextual insights on all devices and strengthen your overall understanding of risks to corporate data stored on applications and network components.

Automated Enforcement – Take action automatically for remediation such as quarantining or disconnecting rouge or suspicious devices, or those lacking the latest security patches and software updates.