Okta + NGINX

Simplify, Secure, and Fine-Tune Access to Applications and APIs

You've invested in NGINX for application delivery and its versatility as a load balancer, web server, API gateway, and more. Now, it's possible to fully leverage that investment by dramatically improving your application access management and API access management. Security and development teams tired of sacrificing accessibility for security can now simplify sign-in for end users, and enable sophisticated, policy-driven authentication and fine-grained, scopes-driven access to apps and APIs, all secured by best-in-class multifactor authentication. Here's how.

Okta, the leading independent provider of identity for the enterprise, now integrates with NGINX, the revolutionary application delivery solution, to simultaneously simplify application access for end users and deliver an unprecedented level of control to the IT team, all while keeping authentication and access more secure than ever. Okta's comprehensive solution lets access to applications behind NGINX be fine-tuned and driven by policy, while Okta's Multi-Factor Authentication (MFA) ensures that users are who they say they are, and Okta's Single Sign-On (SSO) makes sure the process is easy for authorized end users.

Together, Okta + NGINX let you secure your apps, regardless of where they live, and secure your APIs.

How Okta + NGINX Help You Secure Your Apps

Okta's best-in-class identity solutions combine with NGINX's best-in-class application delivery capabilities to provide enterprises with nuanced gatekeeping, where access can be both secure and

conditional—based on policy settings, like a user's department, seniority, or geographic location.

- Apply Okta's SSO to resources, even those behind the firewall, keeping log-in simple for authorized end users
- Apply Okta MFA protection to on-prem or legacy apps that don't natively support it
- Use Okta and NGINX to "translate" an OIDC token into headers that downstream apps can consume
- Mint tokens that include user attributes, allowing customized user experiences and access control
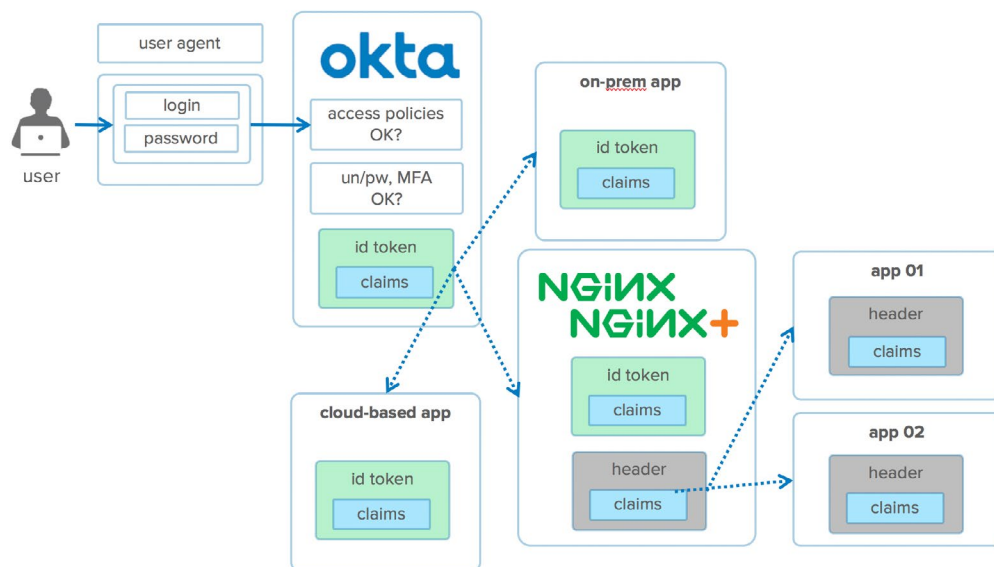
How Okta + NGINX Help You Securely Manage Your APIs

- Managing API endpoints with this integration gives your team robust tools to carefully define access and protect those endpoints through specialized access tokens, secured by identity management and powered by defined scopes

- Identity-based authentication through OIDC and OAuth mints access tokens that can include scopes, like "read only" or "admin access", based on a user's group membership or network location (for example)

- Okta can restrict access until MFA verifies the login attempt and the access policies, before minting an ID token

- APIs can restrict access to endpoints until they can validate that token and ensure the access is within any included scopes

Okta integrated with NGINX and NGINX Plus arms enterprises to take the next step in access management, enabling secure, sophisticated, policy-driven access to applications and APIs.

- Apply conditional access tokens without complicating authentication for end users

- Manage developers' API access with the same policy-driven access

- Provide best-in-class MFA protection for enterprise resources behind the firewall

- Use Okta as your cloud-based authentication and authorization server to give you the combined power of security and ease of use
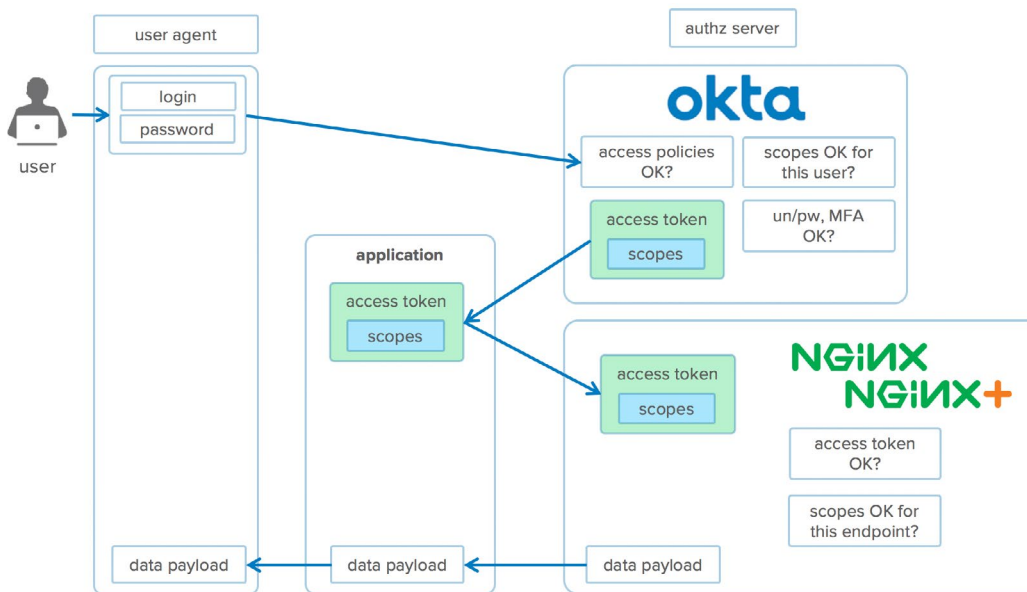
Okta integrates both with NGINX Open Source and with NGINX Plus, the commercial version supported by NGINX, Inc. Both systems natively support OIDC for authentication and can validate tokens for API access management.

For more information on this integration, go to okta.com/partners/nginx
If you have questions, please contact our sales team at okta.com/contact-sales