



Okta Access Gateway: Early Access Program / Security & Privacy Documentation (effective July 31, 2019)

Okta's Commitment to Security & Privacy

Okta is committed to achieving and preserving the trust of our customers, by providing a comprehensive security and privacy program that carefully considers data protection matters across our suite of products and services.

This documentation describes the security-related and privacy-related practices that Okta follows for the software and services branded as 'Okta Access Gateway: Early Access Program' (collectively, the "Services").

- Okta has commissioned a third-party review of the Services' code base, to identify all third-party (including open source) components that are included in the Service. Okta commissions third-party reviews from time to time, as necessary, to perform additional reviews of the Services' code base, if and to the extent that the Services are updated.
- If Okta elects to make any updates and/or upgrades to the Services available to customers (collectively, "Updates"), it may use a third-party platform provider, Amazon Web Services, to assist in doing so.
- Prior to being distributed or otherwise made available to customers, any Updates will be scanned to identify and remediate the Open Web Application Security Project's top ten application vulnerabilities, to the extent applicable to the Services. As of the drafting date of this document, those application vulnerabilities include: injection; broken authentication, sensitive data exposure, XML External Entities; broken access control; security misconfigurations; cross-site scripting; insecure deserialization; using components with known vulnerabilities; and insufficient logging and monitoring.
- Okta will perform comprehensive security testing of the Services at least once annually.