okta

OKTA INC.

INFORMATION SECURITY DOCUMENTATION FOR OKTA ACCESS GATEWAY

(last updated August 22, 2024)

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 on-premise Okta Access Gateway software product and software updates or modifications ("Updates") to the foregoing (collectively, the "Software").

- Okta has commissioned a third-party review of the Software's code base, to verify the identity of third-party (including open source) components that are included in the Software. Okta commissions third-party reviews from time to time, as necessary in its discretion, to perform additional reviews of the Software's code base, if and to the extent that the Software is updated.

- If Okta elects to make any Updates available to customers, it may use a third-party platform provider, such as 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 Software. 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 penetration testing of the Software at least once annually.

Free Trials or Purchased Early Access Services.

Okta's services that are labeled 'Free Trial' or 'Purchased Early Access' may employ lesser or different security measures than those described in this document.

Usage Data.

Okta processes the data derived from the usage of its products and services, including data regarding service configurations and applications utilized in connection with the hosted Service, support data, operational data, log data and the performance results for the hosted Service ("Usage Data"). Okta may process Usage Data as outlined in the Data Processing Addendum ("DPA"), which is publicly available at https://www.okta.com/trustandcompliance, and for legitimate business purposes, such as to: (i) analyze application usage trends; (ii) detect, investigate, and combat fraud and cyber-attacks; (iii) detect, investigate, and combat security incidents, and other such deceptive, fraudulent or malicious behavior against Okta or its customers, including taking measures to improve Okta's overall security posture; (iv) improve service and product functionality; (v) retain and/or employ another service provider or contractor; and (vi) undertake any other specific business purpose authorized by the Customer. Okta may disclose Usage Data publicly and to other entities, and when doing so, will adhere to any applicable confidentiality obligations. Okta may retain, use, and disclose Usage Data in the normal course of business that is (i) deidentified when disclosed; or (ii) disclosed on an aggregated basis; for example, Okta may make available to the public information showing trends about the general use of the hosted service. For clarity, Okta owns Usage Data, which does not include Customer Data.