Okta Access Gateway

Security & Privacy Documentation

(effective October 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 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.

Language

The governing language of this Okta Access Gateway Security and Privacy Documentation is English. Any Japanese language version of this Okta Access Gateway Security and Privacy Documentation is for reference purposes only. If there is any conflict between the English and Japanese version, the English version shall prevail.

Okta Access Gateway の

セキュリティおよびプライバシーに関する文書

(2019 年 10 月 31 日発効)

Okta のセキュリティおよびプライバシーへの取り組み

Okta は、お客様の信頼を獲得し、維持するために尽力するものであり、一連の製品およびサービス全体を通じたデータ保護問題を慎重に考慮した包括的なセキュリティおよびプライバシープログラムを提供する。

本文書では、オンプレミスの Okta Access Gateway ソフトウェア製品およびそのソフトウェアアップデートまたは変更（「アップデート」）について（総称して「本ソフトウェア」）、Okta が従うセキュリティ関連およびプライバシー関連の慣行について説明する。

- Okta は本ソフトウェアに含まれるサードパーティ製（オープンソースを含む）コンポーネントの身元を確認するために、本ソフトウェアのコードベースの第三者レビューを委託している。Okta は、本ソフトウェアがアップデートされた場合、その範囲で、本ソフトウェアのコードベースの追加レビューを行うために、必要に応じて随時第三者レビューを委託する。

- Okta がアップデートをお客様に提供することを選択した場合、Amazon Web Services などの第三者プラットフォームプロバイダを利用してアップデート提供の支援を得ることができる。

- お客様に配布またはその他の方法で提供される前に、アップデートはスキャンされ、Open Web Application Security Project のアプリケーション脆弱性トップ 10 を特定し、本ソフトウェアに適用のある範囲で修正される。本文書の作成日現在、これらのアプリケーション脆弱性には、インジェクション、認証の破損、機密データの公開、XML 外部エンティティ、アクセス制御の破損、セキュリティ設定の誤り、クロスサイトスクリプティング、安全でない逆シリアル化、既知の脆弱性を持つコンポーネントの使用、および不十分なログおよび監視が含まれる。

- Okta は、少なくとも年に 1 回、本ソフトウェアの侵入テストを実施する。

言語

本 Okta Access Gateway のセキュリティおよびプライバシーに関する文書の準拠言語は英語である。本 Okta Access Gateway のセキュリティおよびプライバシーに関する文書の日本語版はすべて参照のみを目的としている。英語版と日本語版との間に矛盾がある場合、英語版が優先される。