



okta

OKTA, INC. SERVICE-SPECIFIC TERMS

These Service-Specific Terms (the “SSTs”) are between Okta and Customer. By executing an Order Form that references the SSTs or by otherwise accepting them, Customer agrees to the SSTs and will use the Service in compliance with them. The SSTs are intended to supplement the Master Services Agreement (“Agreement”) between Okta and Customer, to which the SSTs are incorporated therein. Capitalized terms used in the SSTs not otherwise defined herein have the meanings given to them in the Agreement.

1. General Terms (last updated November 18, 2025).

1.1. Okta may update or modify the SSTs from time to time effective when updated on okta.com/legal.

2. Highly Regulated Identity (“HRI Service”) (last updated August 15, 2025).

2.1. HRI Service is only offered as an add-on SKU for Enterprise Plans.

2.2. Notwithstanding anything to the contrary in the Agreement, Customer may submit to the HRI Service Customer Data that is considered personal financial data or other similarly regulated personal data, such as bank account numbers (collectively, “Regulated Data”), solely for Customer’s business purposes, provided that Customer agrees:

- a) to only submit Regulated Data as part of the HRI Service in accordance with the Documentation,
- b) that Regulated Data will not include any government identifiers or Social Security numbers, any payment card or other data subject to the Payment Card Industry Data Security Standard, any other personal data that is considered “special” or “sensitive” under applicable Laws, or any protected health information subject to the Health Insurance Portability and Accountability Act except as Okta otherwise agrees in writing, and
- c) that Customer is solely responsible for ensuring that its use of the HRI Service in connection with Non-Okta Applications (as defined in the Agreement) complies with all Laws applicable to Customer’s services and products.

3. Client-Initiated Backchannel Authentication (“CIBA Service”) (last updated November 18, 2025).

3.1. The CIBA Service is included in Enterprise Plans and only includes notification channels for Auth0 Guardian App and SDK.

3.2. Notwithstanding anything to the contrary in the Agreement, Customer may submit to the CIBA Service Customer Data that is considered Regulated Data, solely for Customer’s business purposes, provided that Customer agrees:

- a) to only submit Regulated Data as part of the CIBA Service in accordance with the Documentation,
- b) that Regulated Data will not include any government identifiers or Social Security numbers, any payment card or other data subject to the Payment Card Industry Data Security Standard, any other personal data that is considered “special” or “sensitive” under applicable Laws, or any protected health information subject to the Health Insurance Portability and Accountability Act except as Okta otherwise agrees in writing, and
- c) that Customer is solely responsible for ensuring that its use of the CIBA Service in connection with Non-Okta Applications (as defined in the Agreement) complies with all Laws applicable to Customer’s services and products.

4. Enterprise MFA Factors (last updated August 15, 2025).

4.1. Enterprise MFA Factors is included in B2C & B2B Professional, as well as all Enterprise Plans.

4.2. Enterprise MFA Factors includes second factor support for Auth0 Guardian, SMS, Email, Voice and others as updated. SMS and Voice for MFA is charged separately by carriers supported by Auth0. Details are listed at <https://auth0.com/docs/multifactor-authentication>.

5. Adaptive MFA (last updated October 20, 2025).

5.1. Adaptive MFA is only offered as an add-on SKU for Enterprise Plans. Custom Device Remembrance is included in Adaptive MFA.

5.2. Adaptive MFA provides Adaptive MFA Enterprise MFA factors, and Adaptive MFA Triggers. SMS for MFA is charged separately by carriers supported by Auth0; details are listed at <https://auth0.com/docs/attack-protection>, <https://auth0.com/docs/multifactor-authentication> and <https://auth0.com/docs/mfa/adaptive-mfa>.

5.3. Customer is solely responsible for any diminishment in security posture caused by adjusting their device remembrance time period to a period of time longer than Okta’s standard recommended setup.

6. Attack Protection Package (last updated November 18, 2025).

6.1. Attack Protection Package is only offered as an add-on SKU for Enterprise Plans.

6.2. Attack Protection Package enhances attack protection and security measures by increasing Tenant Access Control list beyond core plan entitlements and enabling the Credential Guard and Bot Detection functionality; additional usage details are listed at <https://auth0.com/docs/attack-protection>.



7. Token Vault (last updated November 18, 2025).

7.1. Token Vault is included in all Auth0 plans.

7.2. Connected Accounts is a feature of Token Vault.

7.3. Connected account deletion only removes the external provider's access and refresh tokens from token vault, but does not automatically revoke tokens from Customer's external provider. Customer is responsible for manually revoking the tokens from Customer's external provider.

8. Auth0 for AI Agents add-on SKU (last updated November 18, 2025).

8.1. Auth0 for AI Agents add-on SKU is only offered for Enterprise and Growth Plans.

8.2. Auth0 for AI Agents increases Customer's Token Vault number of connected apps beyond core plan entitlements and expands notification channels for CIBA flows.

8.3. For the Auth0 for AI Agents add-on SKU, CIBA includes SMS, Email, Voice, and other notification channels for CIBA flows as updated. SMS is charged separately by carriers supported by Auth0. Details are listed at <https://auth0.com/docs/multifactor-authentication>.

9. Public Performance Burst (last updated November 18, 2025).

9.1. The Public Performance Burst offering is only offered as an add-on SKU for Enterprise Plans that enhances an existing Public Cloud deployment.

9.2. This add-on SKU only extends the Authentication API request limits and does NOT apply to the Management API or other endpoints that are rate-limited outside the scope of the Authentication API.

10. Private Performance Burst Azure (last updated December 18, 2025).

10.1. Private Performance Burst Azure SKU is only available to Enterprise Private Cloud Customers and includes a single geographical deployment of the Private Performance Burst Environment in the United States, Canada, Mexico, or Europe.

10.2. This SKU also includes one development environment that provides a low capacity, non-production environment hosted within a single region in the Auth0 dedicated cloud Service, and is intended for development or testing environments only. Customers have no guaranteed RPS in the development environment.

10.3. This add-on SKU only extends the Authentication API request limits and does not apply to the Management API or other endpoints that are rate-limited outside the scope of the Authentication API.

11. Private Performance Burst Azure International (last updated December 18, 2025).

11.1. Private Performance Burst Azure International SKU is only available to Enterprise Private Cloud Customers and includes a single geographical deployment of the Private Performance Burst Environment outside of the United States, Canada, Mexico, and Europe.

11.2. This SKU also includes one development environment that provides a low capacity, non-production environment hosted within a single region in the Auth0 dedicated cloud Service, and is intended for development or testing environments only. Customers have no guaranteed RPS in the development environment.

11.3. This add-on SKU only extends the Authentication API request limits and does not apply to the Management API or other endpoints that are rate-limited outside the scope of the Authentication API.

12. Private Performance Burst Geo HA Azure (last updated December 18, 2025).

12.1. This SKU is an add-on to the Private Performance Burst Azure SKU and allows for a geographically redundant failover to be deployed in the United States, Canada, Mexico, or Europe.

12.2. The Performance Multiple subscribed to for this SKU must align with the base deployment subscribed to for the Private Performance Burst Azure SKU.

13. Private Performance Burst Geo HA Azure International (last updated December 18, 2025).

13.1. This SKU is an add-on to the Private Performance Burst Azure International SKU, and allows for a geographically redundant failover to be deployed outside the United States, Canada, Mexico, and Europe.

13.2. The Performance Multiple subscribed to for this SKU must align with the base deployment subscribed to for the Private Performance Burst Azure International SKU.