

Evo SSO Service Description

Barracuda sells products and services through channel partners to end users that use the products and services in their own business. For customers that purchase the Evo single sign-on service offering (the “**Service**” or “**SSO**”) from a Barracuda authorized channel partner, your use of the Service is subject to this Service Description and the [Barracuda Legal Terms and Conditions](#) (unless you have a negotiated agreement with Barracuda, in which case the negotiated agreement will apply).

Barracuda also sells the Service to managed service providers (“**MSP**”) for their use in connection with the managed services the MSP provides to its end customers. Such sale and use of the Service is subject to this Service Description and the MSP’s agreement with Barracuda under which the MSP purchases the Services. When an MSP provides its end customer with direct access to the Service, the MSPs pass through to their end customers the Barracuda Customer Terms and Conditions (which incorporate this Service Description).

The applicable governing terms and conditions document and this Service Description together are referred to as the “**Agreement.**” This Service Description will govern if there is any conflict with other documents. For clarity, the Global DPA will take precedence over any other document that is a part of the Agreement as to the subject matter addressed in the Global DPA. Customers that purchase from an authorized channel partner and MSPs who purchase the Service are collectively referred to as the “**Customer.**” References to the “end customer” means the entity that benefits from use of the Service, regardless of purchasing methodology. Any capitalized terms used but not defined below have the meanings in the Agreement.

Contents

[OVERVIEW..... 1](#)

[UNIT OF MEASURE AND LIMITATIONS2](#)

[SERVICE LEVEL AGREEMENT \(“SLA”\)2](#)

[DATA PROTECTION AND SECURITY3](#)

[BARRACUDA IQ™ – ARTIFICIAL INTELLIGENCE \(“AI”\)5](#)

[CUSTOMER PROVIDED THIRD PARTY SOFTWARE5](#)

[BARRACUDA PROVIDED THIRD PARTY SOFTWARE5](#)

[END OF SALE AND END OF SUPPORT5](#)

OVERVIEW

The Service gives Customers the ability to easily login to multiple web applications and websites with one set of credentials. The Service gives an easy, simple experience for users to log into multiple web applications without having to remember their credentials. It is a brandable experience, which means there is better security adoption, and a lower risk of breach. MSP employees can manage the Service via a single platform across all of their Customers, enabling them to have a standardized and programmatic approach to implementing and provisioning web login security at scale.

UNIT OF MEASURE AND LIMITATIONS

The Service is sold on a per seat basis. For Services sold on a per seat basis, Customer must maintain a 1:1 ratio between users and licenses to the Service. Per seat licenses may be transferred from 1 user to another so long as the 1st user completely stops using the Service.

A customer's use of the Service may be subject to additional or different restrictions as specified in the applicable Barracuda quote (for example, without limitation, the quote may limit users to a particular number of logins per year).

SERVICE LEVEL AGREEMENT ("SLA")

Barracuda makes the following two commitments to Customers in connection with use of a paid subscription to the Service that has not been suspended for any reason.

1. Use of SSO. Subject to the Exceptions stated below, Barracuda agrees that Customers will be able to authenticate and access their connected applications through the Service at least 99.9% of the time each calendar month.

2. Web Access. Subject to the Exceptions stated below, Barracuda agrees that Customers will be able to access the dashboard for the Service at least 99.9% of the time each calendar month.

Exceptions. The above commitments are subject to the following exceptions: (a) planned downtime or emergency maintenance for the Service; and (b) any unavailability caused by force majeure events, actions/inactions by persons other than Barracuda and its contractors, third party products or services used with the Service, outages that are less than 5 continuous minutes in duration, Internet, hosting or platform service provider failure or delay, denial of service attack, use of the Service in violation of the Barracuda Legal Terms and

Conditions, or use of Service that is not in accordance with Documentation (collectively “Exceptions”).

Any Service-impacting condition that you experience must be reported within 24 hours to Barracuda Networks Support, and, if required by Barracuda, you must provide Barracuda Networks Support with access to your Service account. For calculating the amount of excess downtime, over the relevant Barracuda commitment, the downtime does not begin until you report the Service-impacting condition to Barracuda Networks Support.

Barracuda publishes Service status updates at <https://status.barracuda.com>.

DATA PROTECTION AND SECURITY

Data Privacy Terms. Barracuda’s [Global DPA](#) provides both Barracuda’s and its customers’ rights and obligations regarding the processing of Customer Personal Data (as defined in the DPA) in connection with Barracuda’s products and services. Barracuda’s customers can electronically sign the DPA via our [Trust Center](#). For more information about how Barracuda processes personal data as a data controller, please review our [Privacy Notice](#).

Cross-Border Data Transfer. Barracuda operates worldwide. When Barracuda receives or transfers personal data it does so in accordance with local data protection laws, like the GDPR, for example. Where required, Barracuda adopts approved cross-border data transfer mechanisms including the EU’s Standard Contractual Clauses incorporated into our Global DPA. For personal data transfers to the United States, Barracuda is self-certified under the US Department of Commerce Data Privacy Framework, and its certification can be found [here](#).

Access Control. Barracuda personnel may only access customer data to assist with a support issue, when requested by the MSP or Customer. Barracuda also employs privilege identify management (“PIM”), which means that someone can request elevated permissions and it is only for a set duration. For example, if a customer reaches out to Barracuda support and it is deemed necessary for Barracuda personnel to access the customer’s environments, the Barracuda technical support engineer must obtain the customer’s consent and a one-time approval from the customer and only then will access be granted to address the issue in the customer’s environment.

For customers whose data is stored at rest in any non-US data center location, please see Barracuda’s discussion regarding the [2018 US CLOUD Act](#).

Data Retention During Subscription Period. Barracuda retains the data processed by the Service for as long as the Customer's subscription remains active, in order to provide the

Service's privilege-control, elevation, and reporting functionality. Elevation requests and related endpoint and local-administrator records are retained for the duration of the subscription to support these functions. Sign-in and session records are retained on a rolling basis of approximately 30 days, and operational and diagnostic logs are retained for up to 180 days. The Service does not archive Customer data on the Customer's behalf. Retention of Customer Personal Data is further governed by the Global DPA.

Data Center Security and Data Residency. The Service is offered on the AWS cloud infrastructure. The data center provider's compliance documentation is at

AWS Trust Center: [Customer Trust & Security - AWS Trust Center](#)

The storage locations for customer data used for the Service are set forth below. Barracuda stores customer data at rest in the region the customer or its representative selects at the time of initial Service configuration. Once a customer selects a storage location, the customer data will not be stored or failed over outside the region in which the customer selected.

Americas

- AWS Region – US East-1 (N. Virginia)
- AWS Region – US East-2 (Ohio)

Back Ups and Disaster Recovery. For Barracuda's AWS environment, the company maintains a comprehensive data backup policy to support business continuity and disaster recovery best practices. Data backups are taken daily.

Data Transmission. Data is encrypted in transmission and at rest.

Subscription Termination and Data Export. Barracuda generally stores customer data for 30 days post termination or expiration of a subscription to allow additional time for the customer to manually export its data or renew the subscription. After this 30-day retention period, Barracuda will fully disable the account and commence deletion of all customer data (including Customer Personal Data), including any cached or backup copies. Notwithstanding the foregoing, Barracuda may retain security, audit, and elevation event records, and any data it is required to retain to comply with legal obligations, for a longer period, in accordance with the Global DPA and applicable law.

This Service does not archive or store data on Customer's behalf.

Upon termination, the Service will stop backing up customer data. The Service allows customers to export or restore their data at any time. Barracuda will retain customer data in

the Service for up to 30 days to give customers the opportunity to export or restore their data. After the 30-day period, Barracuda will begin the data deletion process and will have no obligation to maintain or provide any customer data and will have no liability resulting from destruction of the customer data.

BARRACUDA IQ™ – ARTIFICIAL INTELLIGENCE (“AI”)

No Use of AI. The Service does not use AI.

No High-Risk AI Systems. The Service is not intended for use in situations that would cause the Service to be considered “High-risk AI” under the EU AI Act. Customers must not use the Service in a manner that would subject Barracuda to obligations applicable to High-risk AI. Barracuda may terminate the customer’s applicable subscriptions to the Service if it violates this obligation. Barracuda has no responsibility for customers’ use of the Service in situations considered “High-risk AI.”

CUSTOMER PROVIDED THIRD PARTY SOFTWARE

In situations where Customer wishes to use third-party software to interoperate with the Service, Customer grants Barracuda permission to allow the third party and its provider to access customer data and information about Customer’s usage of the third-party product or service as appropriate for the interoperation of that third party product or service with the Service. Customer is responsible for ensuring that it has sufficient rights under applicable law to such third-party software to grant the rights to Barracuda to allow Barracuda to perform its obligations for the Customer.

BARRACUDA PROVIDED THIRD PARTY SOFTWARE

Barracuda provides third party software for use with this Service. Customer’s use of the Barracuda-provided third-party software listed below is subject to the third party’s terms and is not subject to the Agreement.

END OF SALE AND END OF SUPPORT

See the Barracuda [End of Sale and End of Support Policy](#) on the Trust Center. Nothing in this section limits Barracuda’s ability to make changes required to comply with applicable law, address a material security risk, or avoid substantial economic or material technical burdens. This section does not apply to pre-general availability Services.