Barracuda Cloud-to-Cloud Backup

Data Protection and Security
# TABLE OF CONTENTS

**Overview** ................................................................................................................. 3

1. **Deployment Model** ............................................................................................. 3
   1.1 CCB Service Deployment Model ........................................................................... 3

2. **Product Security** ................................................................................................. 3
   2.1 CCB Access Controls ........................................................................................... 3
   2.2 Data Transmission and Storage ............................................................................ 3

3. **Data Center Location** .......................................................................................... 3
   3.1 Data Locations ....................................................................................................... 3
Overview
This document describes product security measures and data storage policies that are specific to the Barracuda Cloud-to-Cloud Backup (CCB) product.

1. Deployment Model

1.1 CCB Service Deployment Model
The CCB Service utilizes Barracuda’s cloud infrastructure and is delivered to customers in a Software-as-a-Service (SaaS) model.

2. Product Security

2.1 CCB Access Controls
CCB provides the following features to give customers flexibility to limit access to their CCB account:

- IP login restrictions can be set for each user who has access to CCB. Those restrictions prevent access to the hosted user interface from an IP address outside the range specified.
- Customers use the Barracuda Cloud Control interface to access and manage their CCB accounts. The Barracuda Cloud Control supports Multifactor Authentication. More information about this feature is available here: https://campus.barracuda.com/product/cloudcontrol/doc/69960137/multi-factor-authentication-in-barracuda-cloud-control

2.2 Data Transmission and Storage
- CCB secures data transfers using HTTPS. Before data is stored in the Barracuda Cloud, CCB breaks protected files down into parts that are variable in size and fingerprints those parts for analysis, comparison and deduplication. Those parts are AES 256-bit symmetrically encrypted, are written into storage at the Barracuda Cloud in an encrypted state, and remain encrypted until requested for restore.

3. Data Center Location

3.1 Data Locations
Barracuda maintains a network of cloud-scale datacenters by geographic location around the globe and requires that each meets defined security requirements. The cloud infrastructure for CCB is deployed in the following geographical regions: Customer data is stored in the respective region where the customer is located. Any transfer of customer data outside the regions will be done in compliance with the GDPR and applicable local privacy laws. Barracuda’s Privacy Policy and Privacy Shield certification are located at: https://www.barracuda.com/company/legal/privacy.

- United States of America: infrastructure deploys in this region stores data for all customers in the United States, as well as any region not specifically configured to send data to an available local location.
- United Kingdom: stores data for all customers in the United Kingdom, Europe, Middle East and Africa.
- Canada: stores data for all customers in Canada
- Germany: stores data for all customers in Germany, Austria, Belgium, Netherlands, and Luxembourg.
- Australia: stores data for all customers in Australia.
- Japan: stores data for all customers in Japan.