Security and Compliance

https://campus.barracuda.com/doc/78156017/

You must enable security and compliance to protect the contents of your cloud service account. Barracuda Cloud Security Guardian checks for anomalies, like critical ports that are left open to the public or users who are administrators, but do not use multi-factor authentication.

Policies are based on the standardized Center for Internet Security (CIS) AWS and Azure Foundations Benchmarks. A default security policy that includes all of the CIS rules is provided during installation. You can create additional security policies based on the CIS rules and add your own user-defined attributes.

Enabling security and compliance is usually part of the Getting Started process. If you did not complete it at that time, follow the steps described in Enabling Security and Compliance.

After you have enabled security and compliance, create policies. Refer to Creating Policies for Security and Compliance.