

Understanding the Audit Log

<https://campus.barracuda.com/doc/90446527/>

The Audit Log is available only for Barracuda Email Security Service accounts. It is not available with Barracuda Cloud Protection Layer.

The Audit Log provides a record of all changes made to Barracuda Email Security Service by administrators, end users, and Barracuda Networks Support. This can help both the Administrator and Barracuda Networks Support to track down the reason for a particular behavior. For example, the Audit Log shows which user added a domain to an allow list.

The Audit Log contains data for the last 14 days.

The Audit Log is located under **Dashboard > Audit Log** and contains the following information:

- **Date/Time** – When the action occurred.
- **User** – Email and IP address of the user who performed the action. Displayed value is Barracuda Networks Support if action was taken by a Barracuda Networks Support Representative.
- **Scope** – Describes what is affected by the action. Actions include (creating, changing, or deleting):
 - **Account** – Affects Account Settings, Domains, Marking Messages, Allow Lists.
 - **Domain** – Affects Domain Settings, Users, Allow Lists.
 - **User** – Affects User Settings.
- **Details** – Basic information about the action.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.