Enabling ATI Dashboard Actions for a User

https://campus.barracuda.com/doc/96771712/

The **ADVANCED > Admin Access Control** page, **Administrator Roles** section, allows you to grant action permission(s) to the user on the Active Threat Intelligence (ATI) dashboard. For example, if "Exempting Client Fingerprint Policy" is enabled, the user is allowed to add a client fingerprint to the exempted list on the ATI dashboard. If disabled, the user will not see the actionable link on the ATI dashboard.

> The user can perform the “Exempting Client Fingerprint Policy” action or any other action on the ATI dashboard only if the corresponding service is configured with **Read** and **Write** permissions.

- **Allow All** – User is allowed to perform all actions related to the ATI dashboard if the corresponding service(s) are configured with **Read** and **Write** permissions.
- **Deny All** – User is allowed to view the configuration on the ATI dashboard if the corresponding service(s) are configured with the **Read** permission.