Setting Default Remediation Options

https://campus.barracuda.com/doc/91982264/

You will likely be creating many incidents using the wizard. This article describes how you can set default values in the wizard, so you do not have to choose them each time you go through the wizard. You can, however, change these values each time you run the wizard. For more information on the wizard, refer to Creating an Incident.

Before describing the defaults, here is a brief overview of the two types of remediation:

- **Manual Remediation** – *You* create and remediate an incident by performing a search with the wizard, as described in Creating an Incident.
- **Automatic Remediation** – *The system* creates and remediates certain incidents automatically, without your involvement. For more information, including which types of threats can be remediated automatically, see Automatic Remediation.

To set default remediation options:

1. Log into Barracuda Forensics & Incident Response.
2. In the upper-right corner of the **Incidents** page, click the settings icon to open the Default Remediation Options dialog.
   There are two levels of options, available on two tabs – **Remediation Defaults** and **Policy Options**.
3. Select the **Remediation Defaults** tab. You can set defaults for both Manual and Automatic Remediation.
4. In the **Manual Remediation** section, set the following defaults for your organization. The first two options have recommended values. The others do not.
   - **Delete emails from users' mailboxes** – **Recommended value: Yes**. If you choose not to delete, suspicious or malicious emails remain in users' inboxes. This option must be selected to enable continuous remediation in the next field.
   - **Enable continuous remediation for incidents** – **Recommended value: Yes**. Enable if you want the system to locate and delete emails matching your search criteria for 72 hours past the original deletion time. *The symbol on this field indicates that its default setting is used both for manual and automatic remediation.*
     You must enable the **Delete emails** option to use this option. For more information, see Continuous Remediation.
   - **Send an email alert to the recipient** – Enable if you want to alert the email recipient when they are affected by an incident. Optionally, click **Customize Alert** to use your own text in email notifications. Note that your customized text will be used for both manual and automatic remediation. Save your customized text or revert to the default text.
     The symbol on this field indicates that its default setting is used both for manual and automatic remediation.
   - **Send an email alert to the security team** – Enable if you want to alert your organization's security team for each incident. If you enable this option, you must specify

the default security team email here. *Should you choose to enable Automatic Remediation, it uses the same email address you specify here.*

5. In the **Automatic Remediation** section, select whether you want to enable automatic remediation for your organization. *Note that the fields marked with symbols above are also used for automatic remediation.*
6. Select the **Policy Options** tab. Note that options on this tab affect *both* manual and automatic remediation.
   Consider enabling the following options:
   - **Add a sender policy to Block|Quarantine emails** – Select this option to add a sender policy within your Barracuda Email Security Service account which will either block or quarantine future emails. Choose whether to block by all unique senders (individual addresses) or by all unique domains (each entire unique domain) associated with a new incident.
     This feature requires a Barracuda Email Security Service account. For more information on sender policies in Barracuda Email Security Service, refer to Sender and Recipient Analysis.
   - **Block all user web traffic for domains contained in links** – Select this option to add a DNS filtering block exception within your Barracuda Content Shield account. This will block all users in your organization from accessing links associated with an incident you created.
     This feature requires a Barracuda Content Shield account. For more information on DNS filtering block exceptions, refer to Barracuda Forensics & Incident Response and DNS Filtering With Barracuda Content Shield.
7. Click **Save**.

Figures