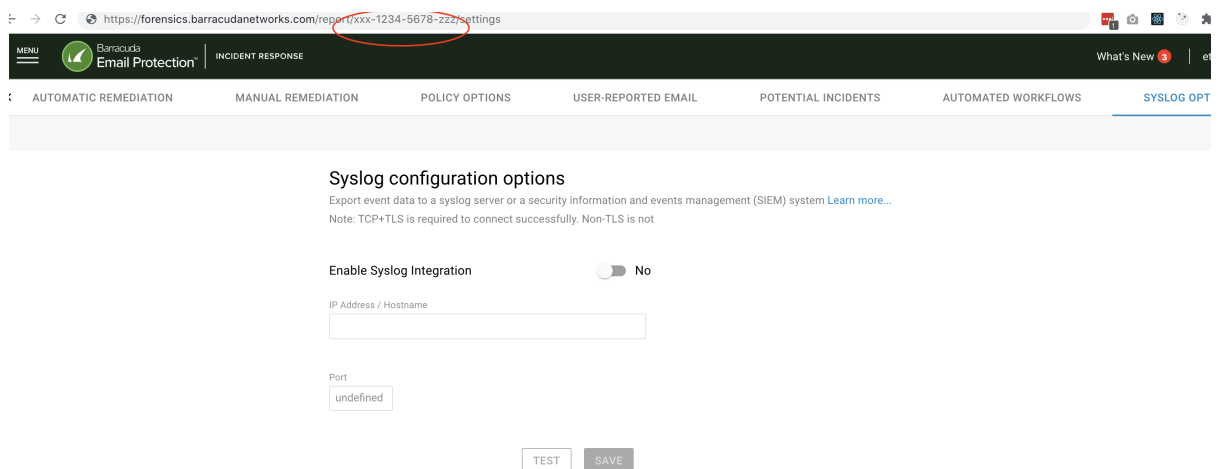


Integrating Barracuda Incident Response

<https://campus.barracuda.com/doc/96767773/>

Set up the Syslog

1. Sign in to **Barracuda Incident Response**.
2. On menu in the top left, click **Settings**.
3. Click the **Syslog Options** tab.
4. Toggle **Enabled** to on.
5. In **IP Address/Hostname**, enter `barracuda-forensics.skout-build.com`.
6. In **Port**, enter **6514**.
7. Click **Save**.
8. While still in the Incident Response app, in your browser's location bar, take note of the UUID Portion of the URL. For example:
 - If the url is **`https://forensics.barracudanetworks.com/report/xxxx-1234-5678-abcd-zzzz/dashboard`** , then the `xxxx-1234-5678-abcd-zzzz` portion is the id.



9. In **Barracuda XDR dashboard**, click **Administration > Integrations > Barracuda Incident Response**.
10. In **Tenant ID**, enter the id.
11. Check the **Enabled** box.
12. Click **Save**.

Set Up the API (Optional)

The second step is setting up the API, so that you can create incidents directly from Barracuda XDR Dashboard. This step is optional and not used by the SOC.

1. Create a Client ID and Client Secret. Log in to the **Barracuda Token Service** at <https://login.bts.barracudanetworks.com/register>. If you are not currently logged into **Barracuda Cloud Control (BCC)**, you must log in using your BCC user credentials before you are redirected to the **Barracuda Token Service**.
2. Click **Add Application** in the top right.
3. On the **Add Application** page, in the **Application Details** section, fill in the **Application name**. In the **Application Scope** section, select following the account level checkboxes:
 - **Email Gateway Defense**
 - **Incident Response**
4. Click **Add Application** to register your application.
5. On the **Application Details** page, you can copy your **Client ID** and **Client Secret** to the clipboard and enter these values into the appropriate fields on **Administration > Integrations > Barracuda Incident Response**. The Client Secret is only available to copy for 15 minutes. However, you can reset it at any time.

If you want to confirm that the integration works correctly, contact the Barracuda Incident Response team and request that they generate a test event.

Figures

1. 1.png

© 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.