

Integrating SentinelOne

<https://campus.barracuda.com/doc/96767922/>

To integrate SentinelOne, do the following procedures:

- To configure Syslog forwarding from SentinelOne EPP
- To find your SentinelOne Site token
- To set up Barracuda XDR Dashboard

To configure Syslog forwarding from SentinelOne EPP

1. In address bar of a browser, enter the SentinelOne Management Console URL provided by the SentinelOne support team (For example, <https://<DomainName>.sentinelone.net/dashboard>, where <DomainName> is the domain name of your SentinelOne account).
2. Log in to the SentinelOne Management Console as an Administrator.
3. If you are a Site or Account Admin, you must select a **Site** to open **Settings**.
 This configuration is done by site. You can only integrate one site per XDR Dashboard.
4. Click **Settings**.
5. Click **Notifications**.
6. In the **Syslog** column, ensure all Syslog settings are selected. (See the sample screenshot below.)

| Notification Types | ADMINISTRATIVE NOTIFICATIONS | Email | Syslog |
|------------------------|--|--------------------------------|-------------------------------------|
| | | No Recipients, SMTP configured | Syslog configured |
| Administrative | Notification recipients modified | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Custom Rules | Agent logging aborted | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Device Control | Agent UI settings modified | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Firewall Control | Anti tampering modified | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Locations | Auto decommission configuration modified | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Malware | Auto decommission days modified | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Mitigation | Configuration action modified | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Operations | Deep Visibility setting modified | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Remote Shell | Agent Disabled/Enabled | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Threat Management | Network quarantine modified | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Exclusions / Blacklist | Maintenance window settings modified | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

7. In the SentinelOne Management Console, click **Settings** > **Integrations** > **Syslog**. Ensure **Formatting** is set to **CEF2**.

Host

Your syslog host

sentinel-us-ingest.skou...

:

6514

TLS

☒ Use TLS secure connection

Certificate

Optional for TLS authentication and privacy:

- To force server authentication: Upload the certificate used to sign the server certificate. For a self-signed certificate, this is the server certificate itself. In other scenarios it is the CA's certificate.
- To let the Syslog server enforce client authentication: Upload the server-approved client certificate (.crt or .pem) and the client key.

Server certificate

Upload

?

Client certificate

Upload

?

Client key

Upload

Formatting

Information format

CEF2

▼

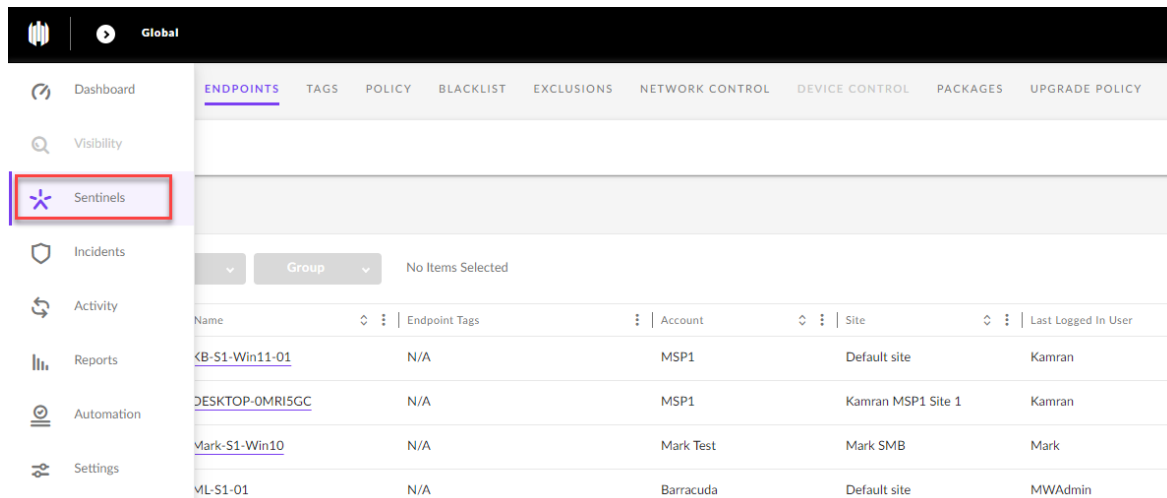
[Add SIEM Token](#)

8. In **Your syslog host**, enter the following:
 - US: sentinel-us-ingest.skout-build.com
 - EU: sentinel-eu-ingest.skout-build.com
9. In the textbox, after the ":", type 6514.
10. Check the **Use TLS Secure Connection** box.
11. Click **Test**.
12. Click **Save**.

Notify Barracuda XDR that you have configured Syslog forwarding.

To find your SentinelOne site ID

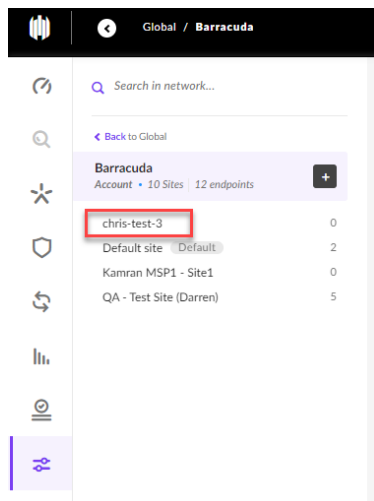
1. In a web browser, navigate to `https://<DomainName>.sentinelone.net/dashboard`, where <DomainName> is the domain name of your SentinelOne account.
2. In the left navigation bar, click **Sentinels**.



The screenshot shows the Barracuda XDR dashboard. In the left sidebar, the 'Sentinels' menu item is highlighted with a red box. The main content area displays a table of endpoints with columns: Name, Endpoint Tags, Account, Site, and Last Logged In User. The table contains four rows of data.

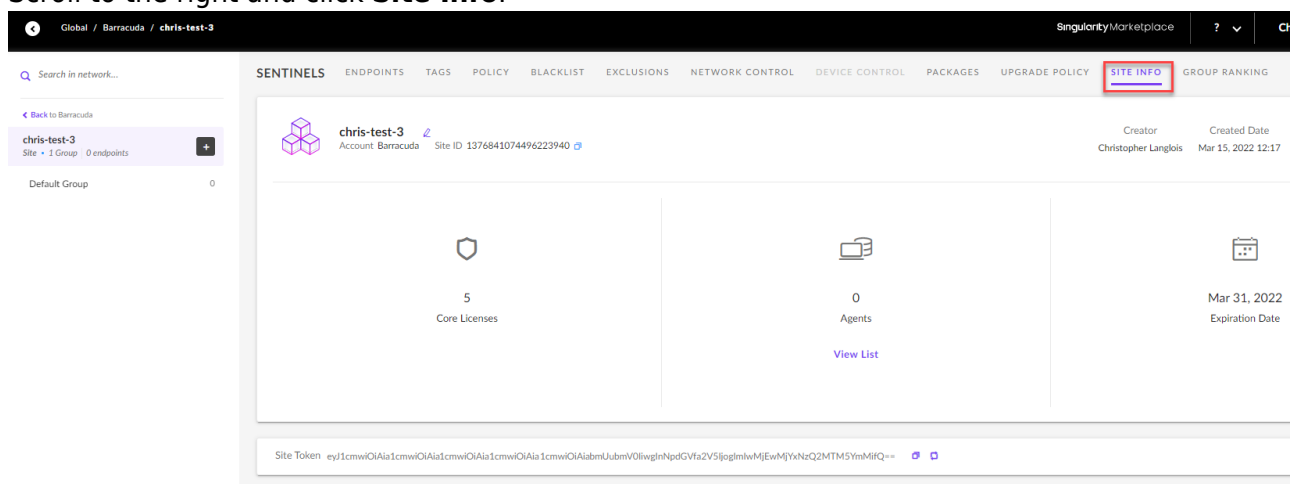
| Name | Endpoint Tags | Account | Site | Last Logged In User |
|-----------------|---------------|-----------|--------------------|---------------------|
| KB-S1-Win11-01 | N/A | MSP1 | Default site | Kamran |
| DESKTOP-0MRI5GC | N/A | MSP1 | Kamran MSP1 Site 1 | Kamran |
| Mark-S1-Win10 | N/A | Mark Test | Mark SMB | Mark |
| ML-S1-01 | N/A | Barracuda | Default site | MWAdmin |

3. Click the name of the site.



The screenshot shows the Barracuda XDR dashboard. In the left sidebar, the 'Sentinels' menu item is highlighted with a red box. The main content area displays a list of sites for the 'Barracuda' account. The list includes 'chris-test-3', 'Default site', 'Kamran MSP1 - Site1', and 'QA - Test Site (Darren)'.

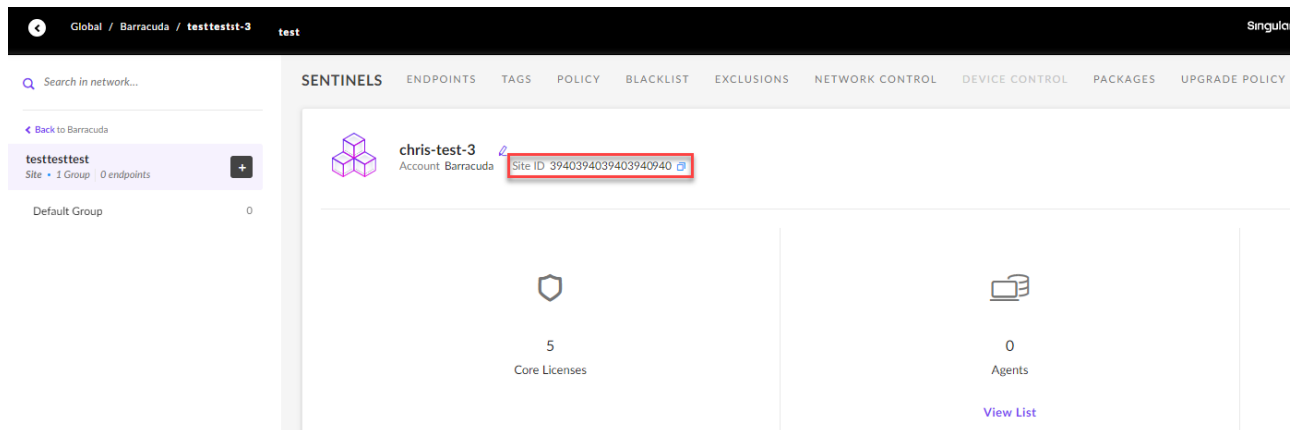
4. Scroll to the right and click **Site Info**.



The screenshot shows the Barracuda XDR dashboard. In the top navigation bar, the 'Site Info' tab is highlighted with a red box. The main content area displays the 'Site Info' page for 'chris-test-3'. The page shows the site ID, creator, created date, and a list of core licenses and agents.

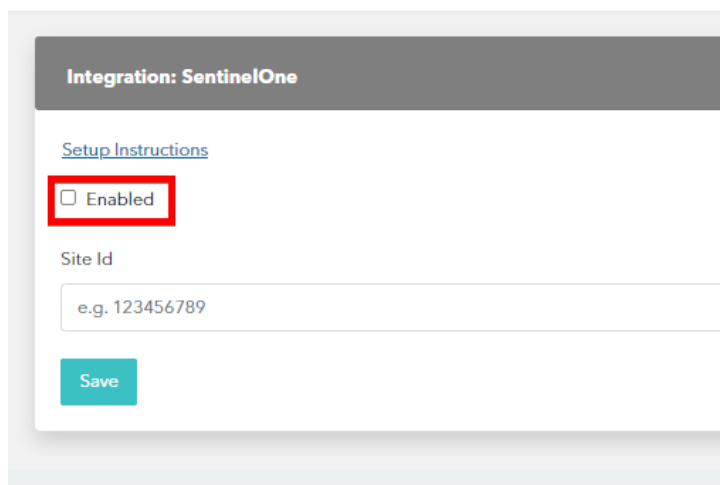
| Core Licenses | Agents | Expiration Date |
|---------------|--------|-----------------|
| 5 | 0 | Mar 31, 2022 |

5. Copy the site ID to use in the *To set up Barracuda XDR Dashboard* procedure, below.



To set up Barracuda XDR Dashboard

1. In **Barracuda XDR Dashboard**, click **Administration > Integrations**
2. On the **SentinelOne** card, click **Setup**.
3. Select **Enabled**.



4. In the **Site Id** field, paste the **Site ID** you copied in the previous procedure.
5. Click **Save**.

Figures

1. sentinelone-setup-1.png
2. sentinelone-setup-2.png
3. Sentinels.png
4. SelectSite.png
5. SiteInfo.png
6. SiteID.png
7. chrome_u6ndjwaqca.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.