Mandiant

EXABEAM ANALYTICS INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validate that security tools are writing log events to Exabeam Analytics to ensure compliance with security policies and regulations
- Collect events generated by security tools that write to Exabeam Analytics to test the efficacy and configuration of security controls using Security Validation jobs

Use this document to configure the integration using one of the following methods:

- MSI (Supported and recommended for new integration configurations)
- Legacy (Supported for existing integration configurations)

Configure MSI Integration

This method is the recommended approach for configuring new integrations in Security Validation.

API Calls

API	Usage
`/api/auth/login`	Log in and retrieve a session cookie from Exabeam Analytics
`/api/auth/logout`	Log out of Exabeam Analytics session
`/uba/api/user/{username}/timeline/entities/all`	Retrieve events for a specific user from Exabeam Analytics

Supported Versions

Exabeam Advanced Analytics i54

Before You Begin

To configure this integration, you need:

- A valid username and password for a user with permissions to use the API endpoints described in the previous step
- The hostname or IP address of your Exabeam Analytics instance

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Exabeam Analytics**.

   You can add this as either a Direct or Remote Integration.
3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** **(https://docs.mandiant.com/home/msv-proxy-rules)**.
5. For the **Host**, enter the hostname of your Exabeam Analytics instance.
6. Enter a **Port** value. The default is **443**.
7. Change the **HttpProtocols** to use for requests. (**Https** or **Http**.)
8. Enter the **Username** and **Password** for the account with permissions to use the API endpoints.
9. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The

default is **30** (seconds).

10. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
11. Optional: Modify the **Field Map** values, as necessary.

    - Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
    - When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

12. Optional: Expand **Advanced options** and update the information as necessary.
    a. Update **Query Time** and **Delay Time**.

    The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

    If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

    b. Update **Query Interval** (seconds).
    c. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    d. Modify the **Correlation Query Interval**, if necessary (minutes).
    e. Select **Discover network devices automatically**, the default and recommended option.

    If unselected, reported events won't include product information for any matching network security technology.

    f. Select **Save Suspicious Events**.
    g. Modify the **Event Time Adjustment** (seconds). The default is **0**.
    h. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

13. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click ⋮ **> Test** to verify that:
   - The Director can communicate with the integration host on the port and protocol specified.

- The integration credentials are valid and working.

For more information on setting up queries, see **Manage Integrations** (https://docs.mandiant.com/home/msv-managing-integrations).

Configure Legacy Integration

> This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** (https://docs.mandiant.com/home/msv-integrations-overview).

This integration is remote capable.

Update Exabeam Advanced Analytics

Identify or create credentials to access Exabeam Advanced Analytics with read access, at minimum. The Validation Platform uses the Exabeam user profile to query for events, so it is important that you identify an Exabeam user profile with the appropriate permissions.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Authentication login	/api/auth/login?username=:username&password=:password
Authentication logout	/api/auth/logout
Get user sessions	/uba/api/user/:username/timeline/entities/all
Get details from a specific session	/uba/api/session/:session_id/info

The Director time must be synchronized in order to successfully make API calls. Discrepancies in time will result in test query failure and missed events.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the hostname/IP used to access Exabeam Advanced Analytics.
- Identify the Port used for Exabeam Advanced Analytics communication (this defaults to 8484).
- Identify whether the protocol is HTTP or HTTPS for connections to the Exabeam Advanced Analytics port.
- Obtain the username and password of an Exabeam account with appropriate access permissions; or, obtain an API token from the Exabeam Portal.

For older versions of Exabeam Analytics (i51 and older), use username/password authentication. For newer versions of Exabeam Analytics (i52 and newer), use the API Token authentication.

Configuration

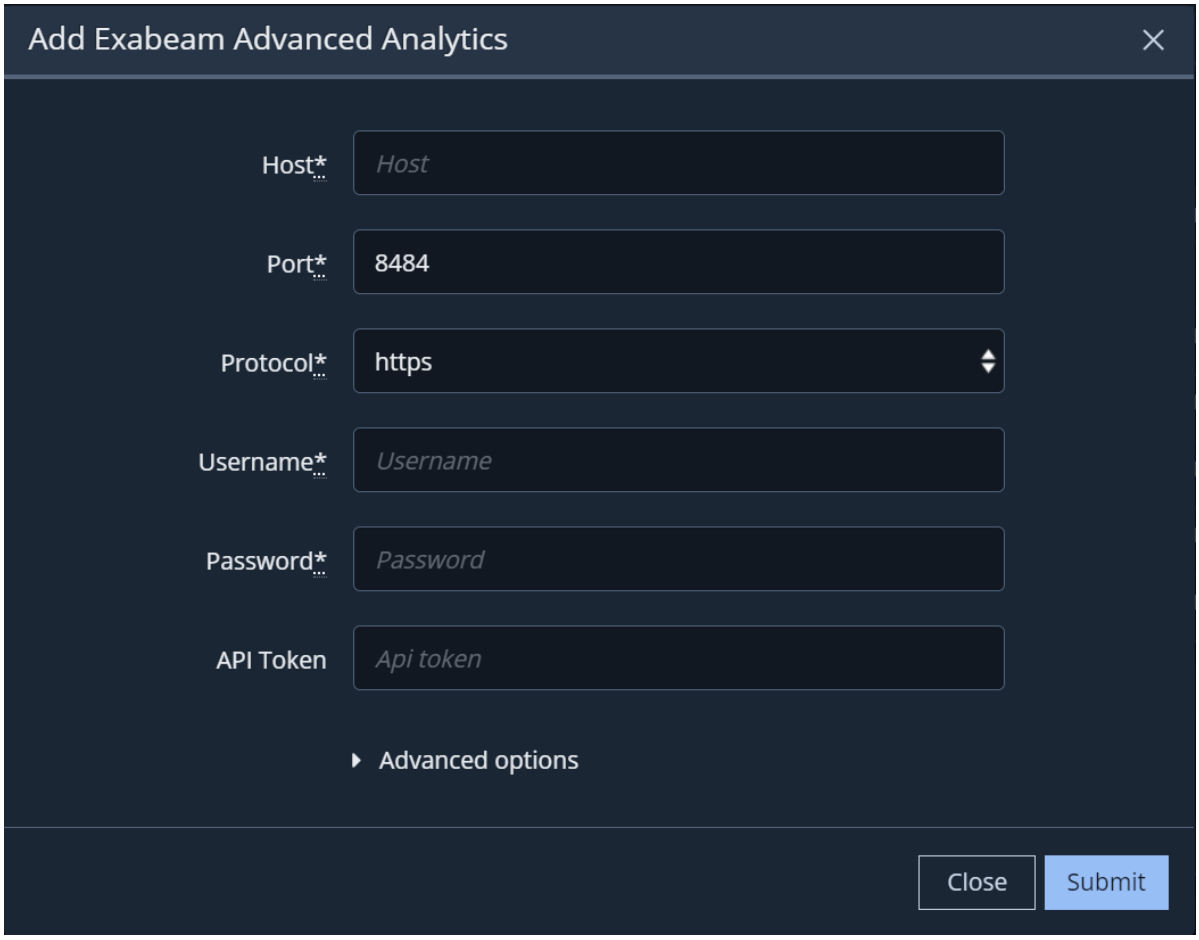
TO ADD THE EXABEAM ADVANCED ANALYTICS INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Exabeam Advanced Analytics**.
3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.

   If you are authenticating your Exabeam account with Domain Logon (Active Directory), you must enter the username in lower case. For example, the username `ExampleUserName` would need to be entered as `exampleusername`.

4. Expand **Advanced options** and update the information if necessary.
5. Click **Submit**.

You must select the Exabeam user profile when running an Action in order for the Action to be recognized by Exabeam queries.



Set up Proxy Assignment

If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. For information on setting up your proxy rules, see **Proxy Rules (https://docs.mandiant.com/home/msv-proxy-rules)**.

Verify connectivity

TO VERIFY CONNECTIVITY TO EXABEAM ADVANCED ANALYTICS

Click **Test** to verify that:

- The Director can communicate with the Exabeam host on the port and protocol specified.
- The Exabeam credentials are valid and working.