Mandiant

DUO INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to Duo to ensure compliance with security policies and regulations
- Collects authentication, telephony, and administrator log events generated by Duo to test the efficacy and configuration of security controls using Security Validation jobs

This feature is released as a Public Preview.
Pre-GA products and features are available "as is" and might have limited support. For more information, please contact your TSC, your CSM, or go to **Support.** (https://docs.mandiant.com/home/mandiant-support-cases)

API Calls

API	Usage
`/admin/v1/info/summary`	Retrieve account summary information to verify connectivity and authentication settings
`/admin/v2/logs/authentication`	Retrieve authentication log events from Duo
`/admin/v1/logs/telephony`	Retrieve telephony log events from Duo
`/admin/v1/logs/administrator`	Retrieve administrator log events from Duo

Supported Versions

Duo Admin API v1 and v2

Before You Begin

To configure this integration, you need the following from your Duo Admin Panel:

- The API hostname of your Duo instance
- An integration key (used as the **Client Id**)
- A secret key (used as the **Client Secret**)

For more information about generating Admin API credentials and configuring permissions to read logs, see the **Duo Admin API documentation** (https://duo.com/docs/adminapi#logs).

Configure Security Validation

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

   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/help/msv-proxy-rules).
5. Enter the **Host** for the Duo API instance.
6. Enter a **Port** value. The default is **443**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

7. Enter the **Client Id** and **Client Secret** values for your Duo Admin API application.
8. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
9. Optional: Select **Verify Ssl** if you want this verification done for requests to an upstream server.
10. Optional: Select one or more of the following log types to collect events from Duo:
    - **Enable Authentication Log**
    - **Enable Telephony Log**
    - **Enable Administrator Log**
11. 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. If supported by your integration, configure correlation queries:
        i. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
        ii. Modify the **Correlation Query Interval**, if necessary (minutes).
    d. 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.

    e. Select **Save Suspicious Events**.
    f. Modify the **Event Time Adjustment** (seconds). The default is **0**.
    g. 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.
12. 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/help/msv-managing-

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

integrations).

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.