ESET Protect Integration

ESET PROTECT allows you to efficiently manage ESET products across workstations and servers within a networked environment, supporting up to 50,000 devices from a single centralized platform. Through the ESET PROTECT Web Console, you can seamlessly deploy ESET solutions, manage tasks, enforce security policies, monitor system health, and swiftly address any issues or threats on remote devices.

Data streams

The ESET PROTECT integration collects three types of logs: Detection, Device Task and Event.

Detection is used to retrieve detections via the ESET Connect - Incident Management.

Device Task is used to retrieve device tasks via the ESET Connect - Automation.

Event is used to retrieve Detection, Firewall, HIPS, Audit, and ESET Inspect logs using the Syslog Server.

Requirements:

- Elastic Agent must be installed

Setup

To collect data from ESET Connect, follow the below steps:

1. Create API User Account (*Refer to How to Create an API User Account below*)
2. Retrieve the username and password generated during the creation of an API user account.
3. Retrieve the region from the ESET Web Console URL.

To collect data from ESET PROTECT via Syslog, follow the below steps:

1. Follow the steps to configure syslog server (*Refer to How to Configure Syslog Server*).
   - Set the format of the payload to **JSON**.
   - Set the format of the envelope to **Syslog**.
   - Set the minimal log level to **Information** to collect all data.

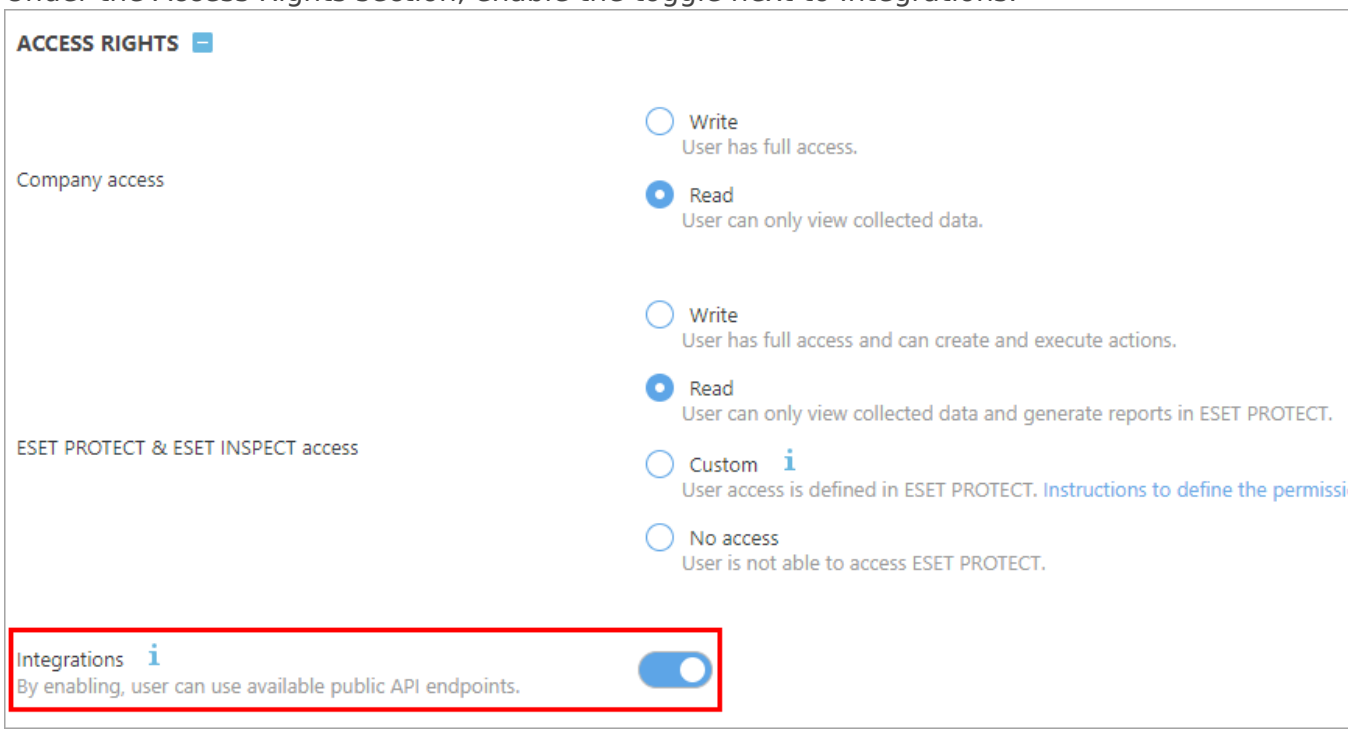
- Select all checkboxes to collect logs for all event types.
- Enter the **IP Address** or **FQDN** of the Elastic Agent that is running the integration in the Destination IP field.

How to Create an API User Account:

For ESET Business Account and ESET MSP Administrator 2

Follow the steps below to create the dedicated API user account:

1. Log in as Superuser (or Root) to your ESET Business Account or ESET MSP Administrator 2.
2. Navigate to User management and create a new user.
3. Under the Access Rights section, enable the toggle next to Integrations.



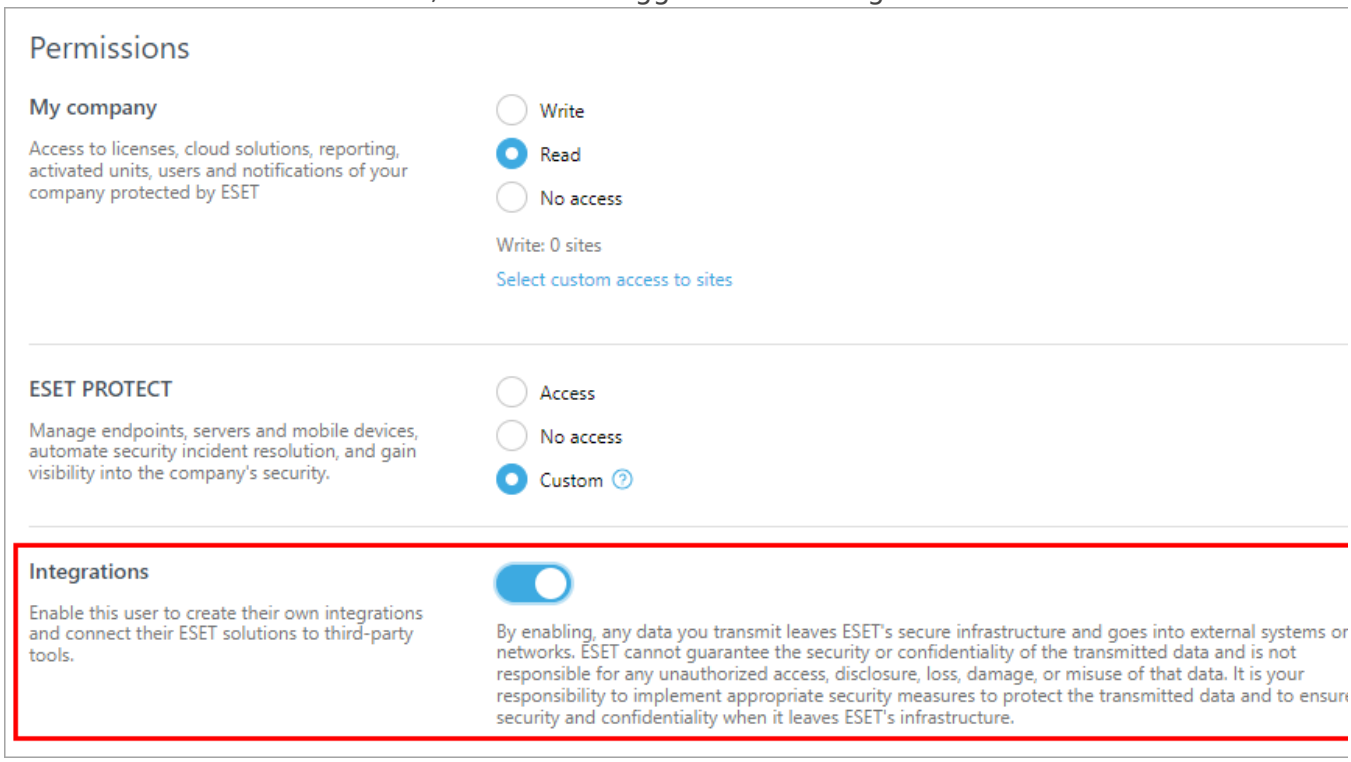
4. Click Create to apply the changes.
5. The new user receives an invitation email and must finish the account activation process.

For ESET PROTECT Hub

Follow the steps below to create the dedicated API user account:

1. Log in as a Superuser to your ESET PROTECT Hub account.
2. Navigate to Users and add a new user.

3. Under the Permissions section, enable the toggle next to Integrations.



4. Click Next and then click Create to apply the changes.
5. The new user receives an invitation email and must finish the account activation process.

How to Configure Syslog Server

If you have a Syslog server running in your network, you can Export logs to Syslog to receive certain events (Detection Event, Firewall Aggregated Event, HIPS Aggregated Event, etc.) from client computers running ESET Endpoint Security.

To enable the Syslog server:

1. Click More > Settings > Syslog and click the toggle next to Enable Syslog sending.
2. Specify the following mandatory settings:

- Format of payload: **JSON**, **LEEF** or **CEF**
- Format of envelope of the log: **BSD** (specification), **Syslog** (specification)
- Minimal log level: **Information**, **Warning**, **Error** or **Critical**
- Event type of logs: Select the type of logs you want to include **(Antivirus, HIPS, Firewall , Web protection, Audit Log, Blocked files, ESET Inspect alerts).**
- **Destination IP or FQDN of TLS-compatible syslog server:** IPv4 address or hostname of the destination for Syslog messages
- **Validate CA Root certificates of TLS connections:** Click the toggle to enable the certificate validation for the connection between your Syslog server and ESET PROTECT. After enabling the validation, a new text field will be displayed where you can copy and paste the required certificate chain. The server certificate must meet the following requirements:

- The whole certificate chain in PEM format is uploaded and saved in the Syslog export configuration (this includes root CA, as there are no built-in trusted certificates)
- Your Syslog server's certificate provides a Subject Alternative Name extension (DNS=/IP=), in which at least one record corresponds to the FQDN/IP hostname configuration.

> You need the certification authority version 3 (and later) with the Basic Constraints certificate extension to pass the validation.
>
> The validation of TLS connections applies only to the certificates. Disabling the validation does not affect the TLS settings of ESET PROTECT.

After making the applicable changes, click **Apply settings**. The configuration becomes effective in 10 minutes.

> The regular application log file is constantly being written to. Syslog only serves as a medium to export certain asynchronous events, such as notifications or various client computer events.

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.

Revision #3
Created 27 November 2024 05:04:49 by David Napoleon Romanillos
Updated 27 November 2024 05:51:39 by Aldion Pueblos