Email Security Agent - Configuration & Usage Guide

1. Introduction

The **Email Security Agent** automates the investigation of suspicious emails by querying your Microsoft Sentinel and Defender data, analyzing email content for psychological triggers, and checking URLs against threat intelligence.

2. Prerequisites

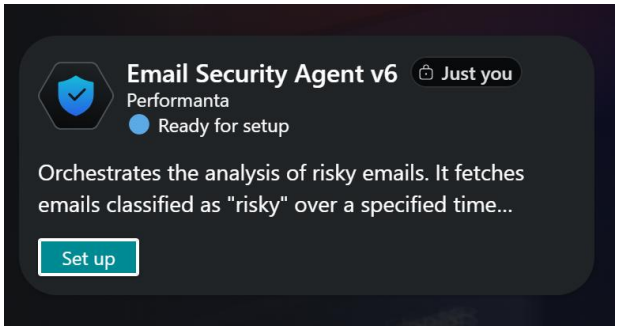
Before configuring or running the agent, ensure you have the following information available from your Azure Portal. The agent requires these details to locate your security data:

1. **Workspace Name:** The name of your Microsoft Sentinel / Log Analytics workspace.
2. **Tenant ID:** Your Azure Active Directory (Entra ID) Tenant GUID.
3. **Subscription Name:** The name of the Azure Subscription hosting the workspace.
4. **Resource Group Name:** The name of the Resource Group hosting the workspace.

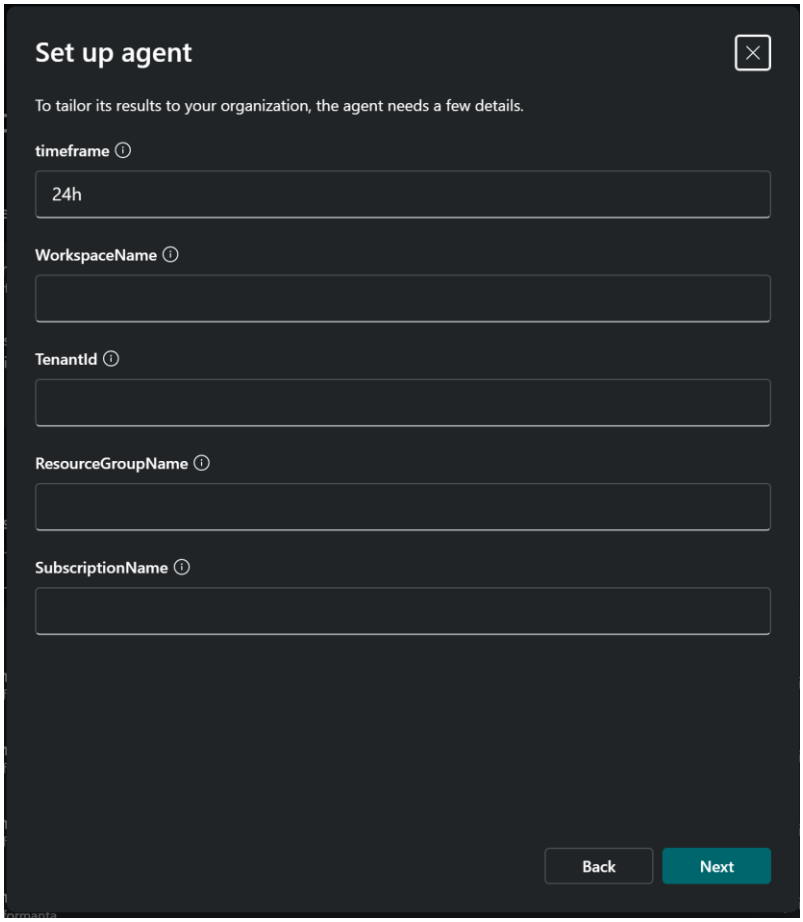
Note: The user account running this agent must have at least **Reader** permissions on the Sentinel Workspace to fetch incidents.

3. Installation & Configuration

1. **Add the agent:**
    - Find Performanta Email Security Agent in the Microsoft Security Store
    - Click on “Set up”



    - Grant any necessary permissions
    - Sign in with a user that has all necessary access
    - Configure the agent with the Timeframe to investigate, Workspace Name, Tenant ID, Resource Group Name, and Subscription Name

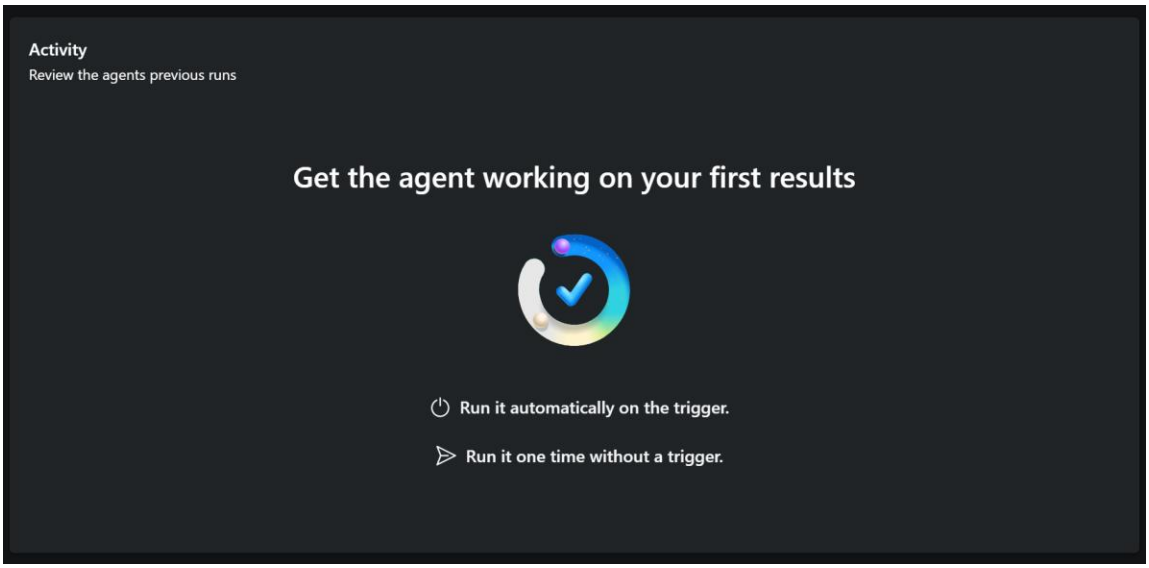


- Once configuration is finished, you may go to the agent and run manually, or set up to run on a schedule.

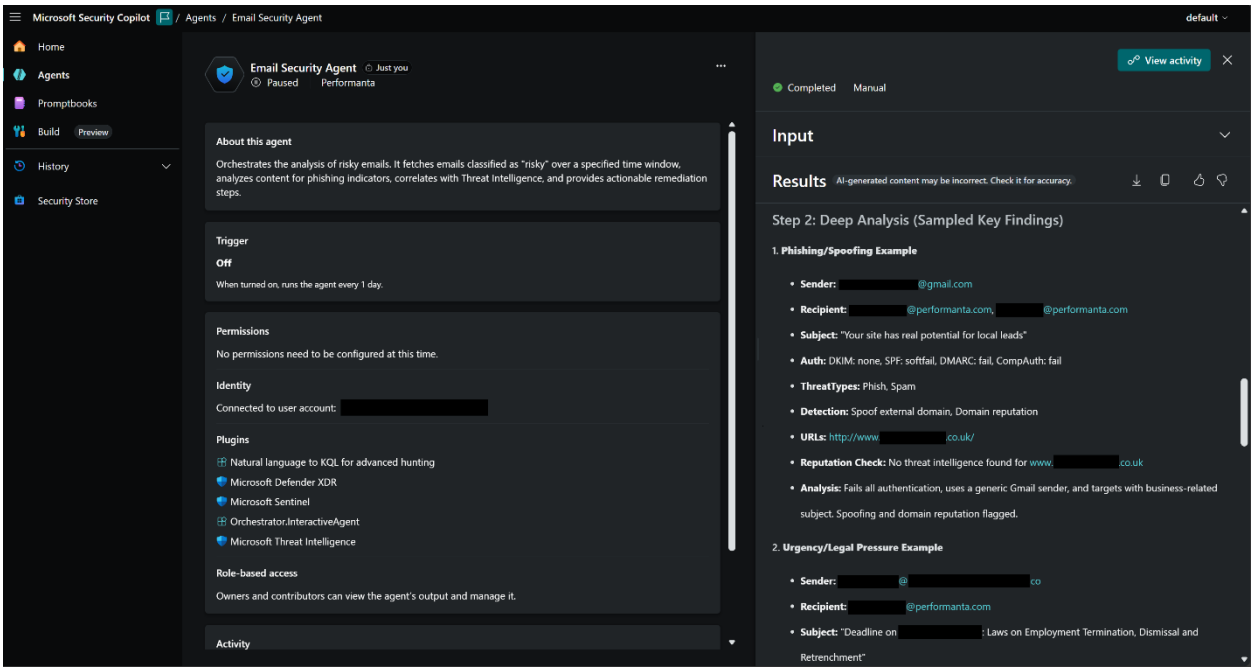
Running the Agent

Once you have configured the agent, you will be able to select “Go to agent” where you will have the option of either enabling it to run on the trigger (once every 24 hours), or manually initiate a single run.

- To enable the agent to run on the trigger (scheduled once every 24 hours), simply click “Run it automatically on the trigger.”
- To manually run the agent one time, select “Run it one time without a trigger. Then review the inputs, and click “Submit”



You will see the output of the agent as in the following example



Understanding the Output

The agent will process the data and return a full analysis of every risky email it investigated, followed by a structured report comprising four key sections:

1. **Verdict:**
    - **[Benign]:** No threats detected.
    - **[Suspicious]:** Anomalies found (e.g., mismatched headers, unusual language) but no known malicious IoCs.

    - **[Malicious]:** Confirmed threats (e.g., known bad domains, blatant credential harvesting).
2. **Executive Summary:** A high-level overview suitable for management, explaining *why* the verdict was reached (e.g., *"Email identified as a BEC attempt due to urgent language requesting wire transfer and a spoofed domain."*).
3. **MITRE ATT&CK Mapping:** Technical categorization of the threat (e.g., *Technique T1566.001: Spearphishing Attachment*).
4. **Action Plan:** A prioritized list of steps you should take immediately.
    - *Example:* "Block sender domain @example.com."
    - *Example:* "Reset password for user: john.doe@company.com."

5. Troubleshooting

Issue: "No incidents found"

- **Cause:** The agent cannot find data matching the criteria.
- **Fix:**
    1. Verify that your Sentinel Workspace has actual email alerts generated within the requested timeframe.
    2. Check your **Settings** configuration. If the WorkspaceName, ResourceGroupName, TenantID, or SubscriptionName is misspelled, the agent will query the wrong location.

Issue: "Authorization Failed" or "Access Denied"

- **Cause:** The user context lacking permissions.
- **Fix:** Ensure the user account logged into Security Copilot has Microsoft Sentinel Reader or Contributor access to the Resource Group specified in the settings.