NG SIEM - Microsoft Exchange Server

Overview

The Microsoft Exchange Server integration for Elastic enables you to monitor Exchange Server installations by collecting and indexing server log data into Elasticsearch. With Kibana, you can visualize, search, and alert on Exchange activity in real time.

This integration is part of the Elastic integrations library and is deployed via Elastic Agent. It is designed for on-premises Exchange Server environments (versions 2013, 2016, and 2019) and supports the following log streams:

- Exchange HTTPProxy Logs
- Exchange IMAP4 / POP3 Logs
- Exchange Message Tracking Logs
- Exchange SMTP Logs (Send/Receive)

Prerequisite

Before setting up the integration, ensure the following components are in place:

- **Exchange Server Requirements**
  - Microsoft Exchange Server 2013, 2016, or 2019
  - Local or remote access to Exchange log directories
  - Administrative privileges to enable SMTP protocol logging (if required)
  - Windows Server 2012 R2 or later

Permissions

The Elastic Agent service account (or the user running Filebeat) must have read access to the Exchange log directories. Default log paths require local administrator or at minimum read access to:

- C:\Program Files\Microsoft\Exchange Server\V15\Logging\
- C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\

Log Streams and File Paths

The integration collects the following log streams. Below are the default file paths for Exchange Server V15 (2013/2016/2019):

Enabling SMTP Protocol Logging

SMTP Send and Receive logs are not enabled by default on Exchange Server. Follow these steps to enable them using the Exchange Management Shell (EMS).

Enable SMTP Send Logging (Hub Transport)

- Open the Exchange Management Shell as Administrator.
- Run the following command to enable protocol logging for the Hub Send connector:

Set-TransportService -Identity <ServerName> -SendProtocolLogPath "C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Hub\ProtocolLog\SmtpSend" -SendProtocolLogMaxAge 30.00:00:00 -SendProtocolLogMaxDirectorySize 250MB

- Enable protocol logging on the Send connector:
  - **Set-SendConnector -Identity "<ConnectorName>" -ProtocolLoggingLevel Verbose**
- Enable SMTP Receive Logging (Frontend Transport)

- Run the following command to enable logging on the Frontend Receive connector:
  - **Set-ReceiveConnector -Identity "<ServerName>\<ConnectorName>" -ProtocolLoggingLevel Verbose**

- Verify that the log path is configured:
  - **Get-TransportService <ServerName> | Select ReceiveProtocolLogPath**

Verify SMTP Logging is Active

After enabling, you can verify log files are being written to the configured path. Wait a few minutes for mail flow to generate entries, then check the directory for new .LOG files.

Enable SMTP Receive Logging (Frontend Transport)

- Run the following command to enable logging on the Frontend Receive connector:
  - Set-ReceiveConnector -Identity "<ServerName>\<ConnectorName>" -ProtocolLoggingLevel Verbose

- Verify that the log path is configured:
  - Get-TransportService <ServerName> | Select ReceiveProtocolLogPath

Verify SMTP Logging is Active

After enabling, you can verify log files are being written to the configured path. Wait a few minutes for mail flow to generate entries, then check the directory for new .LOG files.

Log Stream	Default File Path	Notes
HTTPProxy	...\Logging\HttpProxy\{ECP,OWA,EWS,RPC}*.LOG	Enabled by default
IMAP4	...\Logging\Imap4*.LOG	Enabled by default
POP3	...\Logging\Pop3*.LOG	Enabled by default
Message Tracking	...\TransportRoles\Logs\MessageTracking*.LOG	Enabled by default
SMTP Send	...\TransportRoles\Logs\Hub\ProtocolLog\SmtpSend*.LOG	Must be enabled manually
SMTP Receive	...\TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpReceive*.LOG	Must be enabled manually

Elastic Fleet Configuration

With the Azure application registered, the next step is to configure Elastic Fleet to deploy the Microsoft Exchange Server integration.

> **To enable log collection from the Microsoft Entra ID, provide the following information to CyTech Support:**

Collect Microsoft Exchange Server Logs from file

- Exchange HTTPProxy Logs
  - Paths: eg: C:\Program Files\Microsoft\Exchange Server\V15\Logging\HttpProxy**.LOG

Exchange Server IMAP4 POP3 Logs

- Collect Exchange Server IMAP4 POP3 logs
  - Paths: C:\Program Files\Microsoft\Exchange Server\V15\Logging\Imap4\IMAP*.LOG
  - Paths: C:\Program Files\Microsoft\Exchange Server\V15\Logging\Pop3\POP*.LOG

Exchange Messagetracking Logs

- Collect Exchange Messagetracking logs
  - Paths: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking*.LOG

Exchange SMTP logs

- Collect Exchange SMTP logs
  - Paths: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Hub\ProtocolLog\SmtpSend*.LOG
  - Paths: C:\Program Files\Microsoft\ExchangeServer\V15\TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpReceive*.LOG

Conclusion

The Microsoft Exchange Server integration for Elastic is a practical and well-structured solution for organizations that need visibility into their on-premises email infrastructure. By leveraging Elastic Agent to collect and index Exchange log data — covering HTTPProxy, IMAP4/POP3, Message Tracking, and SMTP streams — teams gain centralized observability without having to build custom pipelines from scratch.

The integration's strength lies in its alignment with the Elastic Common Schema (ECS), which makes Exchange logs immediately searchable and compatible with Kibana's pre-built dashboards and alerting tools. This significantly reduces the time-to-value for security and operations teams who need to monitor mail flow, detect anomalies, or audit user activity.

That said, it does require some upfront effort — particularly around enabling SMTP protocol logging manually on the Exchange side and ensuring Elastic Agent has proper file system access. Organizations running non-standard Exchange installations will also need to adjust default file paths accordingly.

Overall, it's a solid community-supported integration that fits well into broader SIEM or observability strategies built on the Elastic Stack. For teams already invested in Elastic, adding Exchange Server monitoring is a natural and low-friction extension of their existing setup.

Revision #1
Created 5 March 2026 07:24:50
Updated 12 March 2026 07:25:35