# Microsoft Sentinel and Entrust KeyControl Vault

## Integration Guide

2024-05-22

Member of
Microsoft Intelligent
Security Association

Microsoft Security

# Table of Contents

# Chapter 1. Introduction

This document describes the integration of Microsoft Sentinel (SIEM Ingest Syslog and CEF) with Entrust KeyControl.

## 1.1. Documents to read first

This guide describes how to configure CEF and Syslog collection to Microsoft Sentinel from the Entrust KeyControl Vault servers.

To install and configure the Entrust KeyControl cluster on Microsoft Azure, see Entrust KeyControl Azure Installation

To install and configure the Entrust KeyControl server on prem, see KeyControl Installation and Upgrade Guide.

Also refer to the documentation and set-up process for Microsoft Sentinel in the Microsoft Sentinel online documentation.

## 1.2. Requirements

- Entrust KeyControl Vault version 10.2 or later

  An Entrust KeyControl license is required for the on prem installation. You can obtain this license from your Entrust KeyControl Vault and account team or through Entrust KeyControl Vault customer support.

- Microsoft Azure subscription

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

## 1.3. High-availability considerations

Entrust KeyControl Vault uses an active-active deployment, which provides high-availability capability to manage encryption keys. Entrust recommends this deployment configuration. In an active-active cluster, changes made to any KeyControl node in the cluster are automatically reflected on all nodes in the cluster. For information about Entrust KeyControl, see the Entrust KeyControl Vault Product Overview.

## 1.4. Product configuration

The integration between Microsoft Sentinel and Entrust KeyControl Vault has been successfully tested in the following configurations:

| Product | Version |
| --- | --- |
| Entrust KeyControl Vault | 10.2 |
| Log Forwarder Machine | Ubuntu 20.04 |

# Chapter 2. Procedures

The following steps summarize the deployment steps of the Microsoft Sentinel and Entrust KeyControl:

1. Deploy a Entrust KeyControl Vault cluster
2. Install the log forwarder machine
3. Enable Syslog Server on KeyControl
4. Set up Microsoft Sentinel
5. Set up data connectors
6. Test Microsoft Sentinel

This integration will require the Log Forwarder setup showcased here: https://learn.microsoft.com/en-us/azure/sentinel/cef-syslog-ama-overview?tabs=forwarder.

See Microsoft's recommendations on network best practices at https://learn.microsoft.com/en-us/azure/security/fundamentals/network-best-practices.

## 2.1. Deploy a Entrust KeyControl Vault cluster

Microsoft Sentinel supports a deployment of a KeyControl cluster on Microsoft Azure or on an on prem deployment. An Azure deployment of KeyControl was tested for this integration.

For the steps on deploying a KeyControl cluster on Azure, see Entrust KeyControl Azure Installation.

For the steps on deploying a KeyControl cluster on prem, see Entrust KeyControl OVA Installation.

## 2.2. Install the log forwarder machine

The data connectors cannot directly be connected to KeyControl. A log forwarder machine is required to act as a Syslog server for KeyControl and will forward the log to Microsoft Sentinel.

For more information on Log Forwarder machine requirements, see the **Log forwarder prerequisites** section at https://learn.microsoft.com/en-us/azure/sentinel/connect-cef-syslog-ama?tabs=syslog%2Cportal.

Set up `/etc/hosts` on the Linux forwarder VM. Edit `/etc/hosts` and add the hostname and IP address of the Linux forwarder machine.

## 2.3. Enable Syslog Server on KeyControl

1. Sign in to the Entrust KeyControl Vault Server web user interface:
    a. Use your browser to access the IP address of the server.
    b. Sign in with Security Admin privileges.
2. Navigate to **Appliance Management**.
3. In the top menu bar, select **Settings**.
4. In the **System Settings** section, select **Syslog Server**.
5. On the **Syslog Server Settings** page, specify the options you want to use.

| | |
|---|---|
| **State** | **ENABLED** |
| **Protocol** | **TCP** or **UDP** |
| **TLS Authentication List** | One of the options |
| **Log Format** | **CEF** |
| **Server List** | Hostname of the Linux forwarder machine and port 514 |
| **CA Certificate** | Upload a CA certificate if you are using x509/certvalid or x509/name |
| **Client Certificate** | Upload a client certificate if you are using x509/certvalid, x509/name, or x509/fingerprint |

See Entrust KeyControl documentation on Syslog Server Settings for more information: https://docs.hytrust.com/DataControl/10.2/Online/Content/Books/Admin-Guide/KC-System-Config/Syslog-Server.html.

## 2.4. Set up Microsoft Sentinel

To install and configure Microsoft Sentinel on Azure, follow the installation and setup instructions at Microsoft online documentation.

## 2.5. Set up data connectors

To set up the connection to the log forwarder through Syslog via AMA or Common Event Format (CEF) via AMA, or both, follow https://learn.microsoft.com/en-us/azure/sentinel/connect-cef-syslog-ama?tabs=syslog%2Cportal.

## 2.6. Test Microsoft Sentinel

At this point, Microsoft Sentinel should be monitoring logs that are forwarded from KeyControl through the Log Forwarder machine. These logs can be viewed by running simple queries.

1. Go to **Microsoft Sentinel**.
2. Select your instance.
3. Under **General**, select **Logs**.
4. Run the following queries to get the logs from each **Data connector** source.
    - For a list of the CEF logs:

      ```
      CommonSecurityLog
      ```

    - For a list of the Syslogs:

      ```
      Syslog
      ```

      It can take up to 30 minutes for KeyControl logs to appear in Log Analytics after setting up the **Data connectors**.

# Chapter 3. Additional resources and related products

## 3.1. KeyControl

## 3.2. Entrust products

## 3.3. nShield product documentation