

****

**One Identity Manager**

**Solution Accelerator**

**SIEM integration**

Any questions regarding this document should be directed to:

Serkan Cetin

Technical Director, APJ

M: +61 402 929 266

E: serkan.cetin@oneidentity.com

November 3, 2023

Table of Contents

[1 Introduction 3](#_Toc149950545)

[2 How it works 4](#_Toc149950546)

[2.1 Technical description 4](#_Toc149950547)

[2.2 CEF events and activities 5](#_Toc149950548)

[2.3 Extensibility 7](#_Toc149950549)

[3 Package contents 8](#_Toc149950550)

[3.1 Table scripts 9](#_Toc149950551)

[4 Installation instructions 10](#_Toc149950552)

[4.1 SIEM configuration 10](#_Toc149950553)

[4.1.1 Log samples 10](#_Toc149950554)

1. Introduction

Identity Manager provides organizations centralized visibility and control over identity lifecycle events, providing for automation for identity lifecycle management tasks and governance over user access to applications and data. Utilizing the rules and workflows defined in Identity Manager, organizations can detect policy violations, high-risk users, and proactively prevent policy violations. Security operations team can benefit from obtaining this visibility within monitoring tools and SIEM platforms, allowing for the further analysis and correlation of identity events with other sources to detect suspicious activity within the network and application environments.

This solution accelerator provides the capability to integrate Identity Manager with SIEM platforms using the Common Event Format (CEF) standard. CEF is a standardized logging format developed by ArcSight (now MicroFocus), and widely used and supported by SIEM platforms, including Microsoft Sentinel and Splunk.

Utilizing CEF as the standard for logging simplifies the process of integrating Identity Manager with SIEM platforms, with natively available parsing of CEF logs within the SIEM platforms, thus reducing the time and effort often associated with building custom data connectors or parsing rules.

Refer to the CEF standard documentation published by MicroFocus for further details on the CEF standard and message format: <https://www.microfocus.com/documentation/arcsight/arcsight-smartconnectors-8.4/pdfdoc/cef-implementation-standard/cef-implementation-standard.pdf>

1. How it works

The below diagram provides a high-level illustration of how the CEF logging within Identity Manager is designed and implemented within this solution accelerator.

A group of white rectangular boxes with text

Description automatically generated

* 1. Technical description

A script has been added to the OnSaved table scripts for each table which has the events we are interested in. The OnSaved scripts are used to call a function which generates and stores a CEF message.

For example, on the Person table, the OnSaved script includes the following script which is triggered when an identity records security risk flag is set.



The table scripts calls the function “CCC\_CEFMessageBuilder”, which constructs a CEF message. A second function “CCC\_CEFMessageWriter” is called to store the message as a record in the table “CCC\_CEFMessages”.

A process orchestration task, scheduled for every 15 mins, is run to send the messages within the CEFMessages table to the SIEM platform. If the message was sent, the record in CEFMessages is updated to indicate that the record has been sent. If there is an error (i.e.: due to network comms), the record remains unsent, and the error messages are also stored in this table for review by an administrator.

* 1. CEF events and activities

The CEF standard includes an approach to define event class ID’s and corresponding activity names. These activity ID’s and names can be used as part of correlation rules, dashboards or reporting within the SIEM platform, and is a way to categorise or group the events. The following mapping has been defined to standardize these within Identity Manager.

|  |  |  |
| --- | --- | --- |
| Event class ID | Activity name | Comments |
| 01 | Authentication successful | Logging of successful authentication events |
| 02 | Authentication failed | Logging of failed authentication events |
| 03 | Insert object | Generic logging of insert operations for any object type. |
| 04 | Update object | Generic logging of update operations for any object type. |
| 05 | Delete object | Generic logging of delete operations for any object type. |
| 10 | Access request submitted | Logging of access requests submitted. This can be configured for either all entitlements (products) published on the IT Shop, or alternatively be selective to only log high-risk or privileged entitlements. |
| 11 | Access request approved | Logging of access requests approved. This can be configured for either all entitlements (products) published on the IT Shop, or alternatively be selective to only log high-risk or privileged entitlements. |
| 12 | Access request granted | Logging of access requests granted (assigned). This can be configured for either for all entitlements (products) published on the IT Shop, or alternatively be selective to only log high-risk or privileged entitlements. |
| 13 | Access request denied | Logging of access requests denied. This can be configured for either all entitlements (products) published on the IT Shop, or alternatively be selective to only log high-risk or privileged entitlements. |
| 14 | Access request approval granted despite recommendation to deny | Logging of cases where an approver has decided to approve an access request where the recommendation provided by Identity Manager was to deny. |
| 20 | Access review approved | Logging of access review (attestation) approvals. This can also be configured for all attestation cases or be selective for specific attestation cases (i.e.: attestation cases where the employee has a risk score above 0.7). |
| 21 | Access review denied | Logging of access review (attestation) deny decisions. This can also be configured for all attestation cases or be selective for specific attestation cases (i.e.: attestation cases where the employee has a risk score above 0.7). |
| 22 | Access review approval granted despite recommendation to deny | Logging of cases where an approver has decided to approve an access review case where the recommendation provided by Identity Manager was to deny. |
| 30 | Compliance rule violation detected | Logging of new compliance violations detected. |
| 31 | Exception approval granted for compliance rule violation | Logging of exception approvals granted for a compliance violation. |
| 32 | Exception approval denied for compliance rule violation | Logging of exception approvals denied for a compliance violation. |
| 40 | Security risk triggered on an identity | Logging of a security risk flag triggered for an identity. |
| 41 | Security risk flag on an identity has been unchecked | Logging of a security risk flag unchecked (removed) from an identity. |

* 1. Extensibility

The CEF logging mechanism and mapping has been designed to be extendable. The mapping information is stored within the table CCC\_CEFEventClassIDs.

It is recommended to continue using the same structure and grouping if these are to be extended as described below:

* 00 – 09: system events or generic events
* 10 – 19: Activities related to Access Requests and IT Shop
* 20 – 29: Activities related to Access review cases and attestations
* 30 – 39: Activities related to compliance rule violations and compliance rules
* 40 – 49: Activities related to security risks triggered, or high-risk users and objects

This may be further enhanced over time, and submissions are welcome to define additional CEF event ID and activity mappings to be included as part of this solution.

1. Package contents

The following lists the contents of the transport package:

**Schema extensions:**

* New tables:
  + CCC\_CEFEventClassIDs
  + CCC\_CEFMessages

**Configuration parameters:**

* Custom\Syslog
* Custom\Syslog\HostnameOrIP
* Custom\Syslog\Port
* Custom\Syslog\Protocol
* Custom\Syslog\RetentionDays

**Scripts:**

* CCC\_CEF\_MessageBuilderWriter, contains 2 functions:
  + CCC\_CEFMessageBuilder
  + CCC\_CEFMessageWriter
* CCC\_CEF\_SendSyslogMessage, contains 2 functions:
  + CCC\_GetCEFMessages2Send
  + CCC\_SendSyslogMessage

**Process orchestration:**

* CCC\_ProcessCEFMessages on the table CCC\_CEFMessages
* CCC\_CleanUpCEFMessages on the table CCC\_CEFMessages

**Schedule:**

* Process CEF messages
* Cleanup CEF messages
  1. Table scripts

Table scripts are required which will create the log message when an object is saved in the table. These have not been included within a transport package to prevent the possibility of overriding any existing customer defined scripts that may already exist on tables. The table scripts are provided within the attached file, CEF\_TableScripts.vb. The file includes sample scripts which can be used as is or be further configured to only trigger for select objects, events or in specific conditions.

* DialogJournal – OnSaved script
* Person – OnSaved script
* PersonWantsOrg – OnSaved script
* AttestationCase - OnSaved script
* PersonInBaseTree – OnSaved script

1. Installation instructions

Install and perform the following steps:

1. Import the transport package CEF\_Solution\_Accelerator\_v1.zip. This transport package has been created as a single cumulative update containing the entire solution.
2. Add the table on save scripts required.
3. Set the values for syslog host, port and protocol in the configuration parameters.
4. The default schedule has been set to run every 15 mins and is initially deactivated. Enable the schedule and edit if required.
   1. SIEM configuration

The receiving SIEM platform needs to be enabled to accept CEF logs. Refer to the documentation of the SIEM platform for configuring the CEF data collector.

* + 1. Log samples

The following are sample CEF messages generated by this solution:

1. Security risk flag (IsSecurityIncident) triggered on a Person object.

CEF:0|One Identity|Identity Manager|9.2|41|Security risk flag on identity has been unchecked|3|deviceCustomDate1=10/30/2023 10:42:10 AM deviceCustomDate1Label=System\_Timestamp duser=SERKANC msg=A security risk has been removed for identity Serkan Cetin (SERKANC)

1. Access request submitted for a product.

CEF:0|One Identity|Identity Manager|9.2|10|Access request submitted|5|deviceCustomDate1=12/30/1899 12:00:00 AM deviceCustomDate1Label=System\_Timestamp msg=User Serkan Cetin (SCETIN) has submitted an access request for AD Domain Administrators

1. Access request has been approved.

CEF:0|One Identity|Identity Manager|9.2|12|Access request granted|5|deviceCustomDate1=10/31/2023 4:26:40 AM deviceCustomDate1Label=System\_Timestamp msg=User Serkan Cetin (SCETIN) access request for AD Domain Administrators has been granted

1. Examples of how the CEF data can be used within the SIEM environments
   1. Reporting

Having the One Identity Manager (IDM) data will allow security operators, analysts, auditors, etc. to run queries and reports either solely against the IDM data or across objects which would search all of the SIEM data for that object; including that of IDM.

* 1. Part of correlation rule processing

SIEM correlation rules are normally used for incident detections, such as threats or anomalous behaviour. By having the IDM data as part of the SIEM event data, those correlation rules will have more in-depth views of a particular area or use case being monitored.

For example, a rule may look for unusual access right changes followed by uses of those rights by an unknown device in a specific region of the world.

* 1. General security investigations

SIEM (along with SOAR) is central to investigating security incidents. By having events from One Identity Manager, it will allow the research team to have access to key information such as:

* Who had access to this system at the time of a breach?
* How did they get that access?
* Who approved it?
  1. Enabling ITDR

Identity Threat Detection and Response is an important use case that every enterprise works to enable accurately and efficiently. With data from One Identity Manager, this is yet another source of information that can lead to rapid threat detection.

As a side note, the “Response” may be feeding events back to One Identity Manager to take actions such as disabling an account, resetting a password or any other access right type of action. This is *not* part of this solution accelerator, but it is an action that One Identity Manager allows as a part of its integration capabilities.

1. Sample Screen Shots of One Identity Manager Data in Microsoft Sentinel

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated