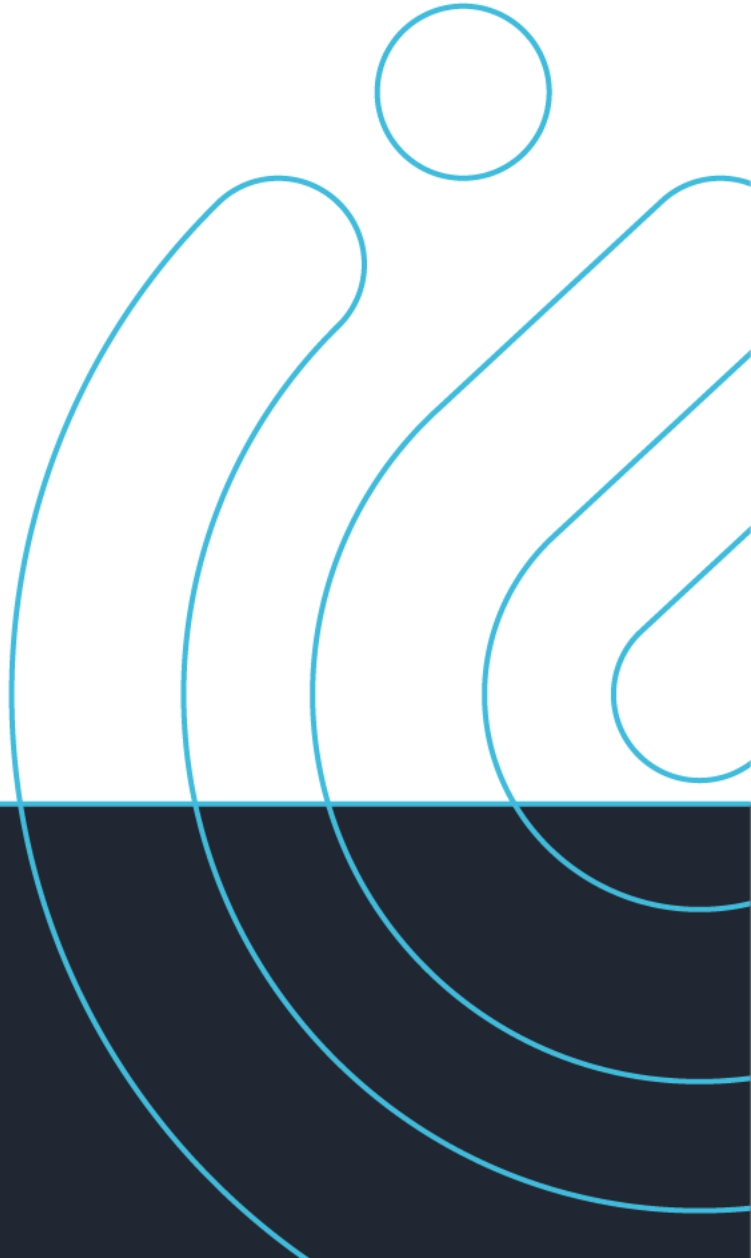
RELEASE NOTES

ClearSkies™

SIEM

Version 6.5.2 / June 2022

"Unlock the Intelligence of Your Data"



ClearSkies™

Table of Contents

Overview

This version release of ClearSkies™ SIEM includes features and enhancements that empower organizations and MSSPs, of any size, in any industry, to effectively anticipate, respond, swiftly recover, and adapt to the emerging threats and vulnerabilities of a dynamically expanding and unpredictable threat landscape.

What's New in v6.5.2

Several new features, functionality enhancements and bug fixes are introduced in this ClearSkies™ SIEM version 6.5.2, including:

- **Marketplace**: improvements include:
  - Expanded data enrichment possibilities with support for new 3rd-party integrations ("FortiGuard" Threat Intelligence, "ManageEngine ServiceDesk Plus" Ticketing, "Microsoft Intune Logs" Log).
  - Enhanced 3rd-party integration connection testing to include application testing.
- **Help**: Improved help guides user experience, through direct linking with Marketplace.
- **Other Enhancements**: Enriched effectiveness and usage of existing functionality.

Important Notes

No special considerations applicable for this version.

New Features

Enhancements

A number of enhancements were made for improved functionality and user experience.

"ServiceModules"

Marketplace

- **Supported Integrations**
  - "Fortiguard" Threat Intelligence 3rd-party integration now supported.
  - "ManageEngine ServiceDesk Plus" Ticketing 3rd-party integration now supported.
  - "Microsoft Intune Logs" Log 3rd-party integration now supported.
  - New Supported 3rd-party integrations Banner slides increased to display the 7 latest additions.

- **Configured Integrations**
  - "Test Connection" capability in 3rd-party configuration windows enhanced to test not only the network connection, but also the parameters of the configuration form (e.g. credentials).
  - New "Method" column introduced displaying the type of method of log collection for enhanced overview.
  - New "Collection Method" field introduced under the 3rd-party integration configuration pop-up window displaying the type of method of log collection for enhanced configuration.

- **Configuration Guides**
  - Configuration guides grid redesigned to include the "Vendor", "Type", "Product", "Date Published", "Created by", "Collection Method" and "Action" columns for simplified overview over the documentation for available 3rd-party integrations.
  - Configuration guides now linked to Help allowing you to select and immediately navigate to selected guides.

ClearSkies™ Endpoint

- **Management**
  - "Network Connections" and "DNS Queries" events toggle buttons introduced when enabling "Behavioral Log Data" in "LogSources" of the "Policy" editing/creating window of the "Policies" tab enhancing the configuration of Behavioral LogSources.
  - New "Office Macro Command Execution" malicious activity introduced in "Activity Configuration" of the "Policy" editing/creating window of the "Policies" tab detecting micro command execution by Microsoft Office Products.

Threat Intelligence

- **Threat Anticipation**
  - Additional Asset information for assets registered into SIEM included in the "Basic Information" section under the "Properties" tab of the "Local" page for improved overview.

Reports

- **Create**
  - Report Templates not applicable to specific projects will not be displayed in "Log Data Reports" tab enhancing reporting.

“General”

Widgets

- New “Search” field introduced in the Widgets Sidebar Menu allowing for quick and easy search through the available widgets by text.
- “Successful attempts based on Active Directory (24 hours)” and “Failed attempts based on Active Directory (24 hours)” widgets redesigned for enhanced reporting overview.
- Widgets Menu design enhanced for improved readability.
- Minor UI changes completed in the Widgets Left Sidebar improving user experience.

SWP

- Code optimization performed on our analytical and machine learning models enhancing performance and accuracy of results.

“TopMenu”

Help

- “Help” TopMenu item redesigned to group documentation under two distinct categories, “SWP Management” and “Configuration Guides”.

Bug fixes

This version resolves a number of stability and performance issues identified.

New Supported Products and Versions

Vendor	Product	Product Category	Product Version	Type of Collection	What's New
Oracle	Oracle Cloud	Web Application Firewall	–	API	Product support
VMWare	vSAN	Audit	7.0.2, 7.0.3	Syslog	Product support
Cisco	Meraki Events	Network Management	16.16	Syslog	Version support
Cisco	Meraki Flows	Connection Monitoring	16.16	Syslog	Version support
Cisco	Meraki Security Events	IDS – IPS	16.16	Syslog	Version support
Fortinet	Fortigate Access Control CEF	Access Control	6.2.9, 6.4.6, 7.0.1, 7.0.3, 7.0.4, 7.0.5	Syslog (CEF)	Version support
Fortinet	Fortigate Antivirus CEF	Anti Virus	6.2.9, 6.4.6, 7.0.1, 7.0.3, 7.0.4, 7.0.5	Syslog (CEF)	Version support
Fortinet	Fortigate Application Control CEF	Application Control	6.2.9, 6.4.6, 7.0.1, 7.0.3, 7.0.4, 7.0.5	Syslog (CEF)	Version support
Fortinet	Fortigate DLP CEF	Data Loss Prevention	6.2.9, 6.4.6, 7.0.1, 7.0.3, 7.0.4, 7.0.5	Syslog (CEF)	Version support
Fortinet	Fortigate DNS CEF	DNS	6.2.9, 6.4.6, 7.0.1,	Syslog (CEF)	Version support

			7.0.3, 7.0.4, 7.0.5		
Fortinet	Fortigate Email Filter CEF	Email Gateway	6.2.9, 6.4.6, 7.0.1, 7.0.3, 7.0.4, 7.0.5	Syslog (CEF)	Version support
Fortinet	Fortigate Firewall CEF	Firewall	6.2.9, 6.4.6, 7.0.1, 7.0.3, 7.0.4, 7.0.5	Syslog (CEF)	Version support
Fortinet	Fortigate IPS CEF	IDS – IPS	6.2.9, 6.4.6, 7.0.1, 7.0.3, 7.0.4, 7.0.5	Syslog (CEF)	Version support
Fortinet	Fortigate System CEF	Audit	6.2.9, 6.4.6, 7.0.1, 7.0.3, 7.0.4, 7.0.5	Syslog (CEF)	Version support
Fortinet	Fortigate VOIP CEF	Telephony	6.2.9, 6.4.6, 7.0.1, 7.0.3, 7.0.4, 7.0.5	Syslog (CEF)	Version support
Fortinet	Fortigate WAF CEF	Application Firewall	6.2.9, 6.4.6, 7.0.1, 7.0.3, 7.0.4, 7.0.5	Syslog (CEF)	Version support
Fortinet	Fortigate Web Filter CEF	Web Gateway	6.2.9, 6.4.6, 7.0.1, 7.0.3, 7.0.4, 7.0.5	Syslog (CEF)	Version support
Barracuda	Web Application Firewall	Application Firewall	10.1.1.015	Syslog (CEF)	Version support
Sophos	Sophos Firewall Event	Audit	18.0.3 MR-3	Syslog	Version support

Sophos	Sophos Email Filtering	Email Gateway	18.0.3 MR-3	Syslog	Version support
Sophos	Sophos XG Firewall	Firewall	18.0.3 MR-3	Syslog	Version support
Sophos	Sophos System Health	Health Status	18.0.3 MR-3	Syslog	Version support
Sophos	Sophos IDS – IPS	IDS – IPS	18.0.3 MR-3	Syslog	Version support
Sophos	Sophos XG Web Filtering	Web Gateway	18.0.3 MR-3	Syslog	Version support