opentext™

ArcSight SmartConnectors

Software Version: 8.4.x

Release Notes for ArcSight Content AUP-Categorization Updates 2023

Document Release Date: 2023
Software Release Date: 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Release Notes for ArcSight Content AUP-Categorization Updates 2023

This guide provides information for all the monthly Release Updates for **ArcSight Content AUP-Categorization for the year 2023**.

Note: From May 2023 onwards, the ArcSight Content AUP-Categorization updates will be a monthly release.

Content AUP which is also known as ArcSight Content-Categorization Updates is delivered as Patch and is available through ArcSight SmartConnectors License SKU. Customers who are still on legacy ArcSight product structure who have not migrated to ArcSight Standard Edition license structure may obtain the AUP updates through most current version of core product downloads. There is a list of signatures within which the categorization gets modified which changes with every release.

For instructions about installing the Content AUP updates on ESM and ArcMC, see Installation Guide for Content AUP and Context Updates.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- Technical Requirements Guide for SmartConnector, which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- Installation and User Guide for SmartConnectors, which provides detailed information about installing SmartConnectors.
- Configuration Guides for ArcSight SmartConnectors, which provides information about configuring SmartConnectors to collect events from different sources.
- Configuration Guide for SmartConnector Load Balancer, which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors 8.4.

Release Notes for ArcSight Content AUP-Categorization Updates 2023

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, contact Open Text Support for Micro Focus products.

October 2023 Updates

Data Sources with New Signatures and Categorizations

- Cisco ISE 1
- Juniper IDP Content Version 3641
- Microsoft DNS Trace Log
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1705
- TippingPoint SMS IPS DV9832
- Trellix Endpoint Security 10.7.0

Modified Signatures

This release contains no Modified Signatures.

File Name

ArcSight-9199-ConnectorContent.aup

For instructions about installing the Content AUP updates on ESM and ArcMC, see Installation Guide for Content AUP and Context Updates.

September 2023 Updates

Data Sources with New Signatures and Categorizations

- Amazon CloudTrail
- Juniper IDP Content Version 3635
- McAfee Network Security Manager 11.10.9.4
- Microsoft DNS Trace Log
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1691
- TippingPoint SMS IPS DV9828
- Trellix Endpoint Security 10.7.0

Modified Signatures

This release contains no Modified Signatures.

File Name

ArcSight-9198-ConnectorContent.aup

For instructions about installing the Content AUP updates on ESM and ArcMC, see Installation Guide for Content AUP and Context Updates.

August 2023 Updates

Data Sources with New Signatures and Categorizations

- Cisco Cisco ISE 1
- IBM X-Force XPU 4212.12221
- Juniper IDP Content Version 3622
- McAfee Network Security Manager 11.10.8.1
- Microsoft Windows
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1659
- TippingPoint SMS IPS DV9814

Modified Signatures

Device Event Class ID: `Microsoft-Windows-Security-Auditing:4768`

OLD: `/Host/Operating System,/Authentication/Verify,,/Operating System,/Normal,/Success,Source`

NEW: `/Host/Operating System,/Authentication/Verify,,/Operating System,/Informational/Warning,/Failure,Source`

File Name

ArcSight-9159-ConnectorContent.aup

For instructions about installing the Content AUP updates on ESM and ArcMC, see Installation Guide for Content AUP and Context Updates.

July 2023 Updates

Data Sources with New Signatures and Categorizations

- Juniper IDP Content Version 3614
- McAfee Network Security Manager 11.10.7.1
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 2983
- Symantec Network Security 7100 1639
- TippingPoint SMS IPS DV9807
- UNIX syslog

Modified Signatures

This release contains no Modified Signatures.

File Name

ArcSight-9129-ConnectorContent.aup

For instructions about installing the Content AUP updates on ESM and ArcMC, see Installation Guide for Content AUP and Context Updates.

June 2023 Updates

Data Sources with New Signatures and Categorizations

- Juniper IDP Content Version 3604
- McAfee Network Security Manager 11.10.6.1
- Microsoft SharePoint 2010
- Microsoft Windows
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1621
- TippingPoint SMS IPS DV9800
- UNIX syslog

Modified Signatures

This release contains no Modified Signatures.

File Name

ArcSight-9126-ConnectorContent.aup

For instructions about installing the Content AUP updates on ESM and ArcMC, see Installation Guide for Content AUP and Context Updates.

May 2023 Updates

Data Sources with New Signatures and Categorizations

- Juniper IDP Content Version 3596
- Microsoft System or Application Event
- McAfee Network Security Manager 11.10.5.1
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1597
- TippingPoint SMS IPS DV9788

Modified Signatures

This release contains no Modified Signatures.

File Name

ArcSight-9088-ConnectorContent.aup

For instructions about installing the Content AUP updates on ESM and ArcMC, see Installation Guide for Content AUP and Context Updates.

April 2023 Updates

R2

Data Sources with New Signatures and Categorizations

- Juniper IDP Content Version 3592
- McAfee Network Security Manager 11.9.4.3
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1587
- TippingPoint SMS IPS DV9784

Modified Signatures

This release contains no Modified Signatures.

File Name

ArcSight-9086-ConnectorContent.aup

R1

Data Sources with New Signatures and Categorizations

- Juniper IDP Content Version 3585
- McAfee Network Security Manager 11.9.4.1
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1577
- TippingPoint SMS IPS DV9780
- Palo Alto Networks PAN-OS 10.0.8

Modified Signatures

This release contains no Modified Signatures.

File Name

ArcSight-9055-ConnectorContent.aup

For instructions about installing the Content AUP updates on ESM and ArcMC, see Installation Guide for Content AUP and Context Updates.

March 2023 Updates

R2

Data Sources with New Signatures and Categorizations

The following data sources have new signatures and categorizations:

- Juniper IDP Content Version 3581
- McAfee Network Security Manager 11.9.3.3
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1563
- TippingPoint SMS IPS DV9773

Modified Signatures

This release contains no Modified Signatures.

File Name

ArcSight-9044-ConnectorContent.aup

R1

Data Sources with New Signatures and Categorizations

The following data sources have new signatures and categorizations:

- Juniper IDP Content Version 3576
- McAfee Network Security Manager 11.9.2.5
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1554
- TippingPoint SMS IPS DV9767

Modified Signatures

This release contains no Modified Signatures.

File Name

ArcSight-9025-ConnectorContent.aup

For instructions about installing the Content AUP updates on ESM and ArcMC, see Installation Guide for Content AUP and Context Updates.

February 2023 Updates

R2

Data Sources with New Signatures and Categorizations

The following data sources have new signatures and categorizations:

- Cisco Router 15.4
- HPE iLO 4
- Juniper IDP Content Version 3574
- McAfee Network Security Manager 11.9.2.2
- Oracle 10.x
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1548
- TippingPoint SMS IPS DV9763

Modified Signatures

The following signatures have been modified:

McAfee - Network Security Manager

Intruvert - IntruShield

McAfee - IntruShield

- **Device Event Class ID**: `0x40410200`

OLD: ,,,/IDS/Network,,,Source

NEW:
/Host/Application/Service,/Communicate/Query,/Exploit/Vulnerability,/IDS/Network,/Compromise,/Attempt,Source

- **Device Event Class ID**: `0x4040ff00`

OLD: ,,,/IDS/Network,,,Source

NEW:
/Host/Application/Service,/Communicate/Query,/Exploit/Vulnerability,/IDS/Network,/Compromise,/Attempt,Source

- **Device Event Class ID**: `0x4028ab00`

OLD: ,,,/IDS/Network,,,Source

NEW:
/Host/Application,/Communicate/Query,/Exploit/Vulnerability,/IDS/Network,/Compromise,/Attempt,Source

- **Device Event Class ID**: `0x452afd00`

OLD:
/Host/Application,/Communicate/Query,/Code,/IDS/Network,/Compromise,/Attempt,Source

NEW: /Host/Application/Service,/Communicate/Query,/Code/Application Command,/IDS/Network,/Compromise,/Attempt,Source

File Name

ArcSight-9016-ConnectorContent.aup

R1

Data Sources with New Signatures and Categorizations

The following data sources have new signatures and categorizations:

- Juniper IDP Content Version 3570
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1539

Modified Signatures

This release contains no Modified Signatures.

File Name

ArcSight-9006-ConnectorContent.aup

For instructions about installing the Content AUP updates on ESM and ArcMC, see Installation Guide for Content AUP and Context Updates.

January 2023 Updates

R2

Data Sources with New Signatures and Categorizations

The following data sources have new signatures and categorizations:

- Cisco IronPort
- Juniper IDP Content Version 3565
- McAfee Network Security Manager 10.9.41.3
- Microsft SQL Server 2000
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1526
- TippingPoint SMS IPS DV9756
- VMWare ESX

Modified Signatures

This release contains no Modified Signatures.

File Name

ArcSight-8991-ConnectorContent.aup

R1

Data Sources with New Signatures and Categorizations

The following data sources have new signatures and categorizations:

- IBM X-Force XPU 4212.12221
- Juniper IDP Content Version 3562
- McAfee Network Security Manager 10.9.41.1
- Microsoft SQL Server 2000
- Microsoft AD FS
- Palo Alto Networks PAN-OS 10.0.8

- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1520
- TippingPoint SMS IPS DV9751

Modified Signatures

This release contains no Modified Signatures.

File Name

ArcSight-8981-ConnectorContent.aup

For instructions about installing the Content AUP updates on ESM and ArcMC, see Installation Guide for Content AUP and Context Updates.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes for ArcSight Content AUP-Categorization Updates 2023 (SmartConnectors 8.4.x)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!