

---

**opentext™**

# ArcSight User Behavior Monitoring

Software Version: 24.3

**Release Notes**

## Legal Notices

Open Text Corporation

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

### Copyright Notice

Copyright 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

### Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

## Support

### Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
Support Web Site	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
ArcSight Product Documentation	<a href="https://www.microfocus.com/documentation/arcSight/">https://www.microfocus.com/documentation/arcSight/</a>

# Contents

- What's New ..... 4
- Updated Content ..... 10
- ESM Requirements ..... 11
- Downloading and Verifying the Installation Files ..... 12
- Publication Status ..... 13
  - Contact Information ..... 13
- Send Documentation Feedback ..... 14

# What's New

ArcSight User Behavior Monitoring (UBM) 24.3 introduces new content including rules, pattern discovery profiles, an integration command, and supporting resources to help you monitor user activity. This release specifically introduces a Federation Services folder of new Active Directory Federation Services (AD FS) content that monitors your AD FS environment.

Resource Type	Resource Name	Description	Location
Pattern Discovery Profile	Removable Media - Hostname to Media	Identifies patterns in removable media activity. By default, patterns will be identified when the set of two or more media and host involved on data transfer of at least two files.	/All Profiles/ArcSight Solution/UBM/User Activity Monitoring
Field Set	Remote Logon Activity	Contains fields required to monitor remote logon activity.	/All Field Sets/ArcSight Solutions/UBM/User Activity Monitoring/Login Events
Filter	Remote Desktop Logon Events	Captures Microsoft Windows 4624 events where the Logon Type is 10.  Logon Type 10 is when a user logs on to a computer remotely using Terminal Services or Remote Desktop.	/All Filters/ArcSight Solutions/UBM/User Activity Monitoring/Login Events
Active Channel	Remote Login Events	Displays Microsoft Windows 4624 events where the Logon Type is 10.  Logon Type 10 is when a user logs on to a computer remotely using Terminal Services or Remote Desktop.	/All Active Channels/ArcSight Solutions/UBM/User Activity Monitoring/Login Events
Rule	Possible Data Theft Through Removable Media from the Same Machine  T1052.001	Detects possible data exfiltration via removable media from the same actor on a specific machine.	/All Rules/ArcSight Solutions/UBM/User Activity Monitoring/Removable Media Activity
Rule	Potential Data Theft Through Removable Media across Multiple Machines  T1052.001	Detects possible data exfiltration from the same actor across multiple machines.	/All Rules/ArcSight Solutions/UBM/User Activity Monitoring/Removable Media Activity

Resource Type	Resource Name	Description	Location
Pattern Discovery Profile	Logins - Failed - GeoCountry to User	Identifies patterns related to failed login by countries. By default, patterns will be identified when the same set of one or more accounts have failed logins from two or more different attacker countries and target IPs combinations.	/All Profiles/ArcSight Solutions/UBM/User Activity Monitoring
Rule	Information Leakage from Database T1213	Detects information leakage from a database.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity/Information Leakage
Rule	Data Manipulated T1565	Detects attempts to insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data.	/All Rules/Real-time Rules/UBM/Suspicious Activity/General Security/Data Manipulated
Rule	Consecutive Unsuccessful Logins to Same Actor from different Countries T1110	Detects sets of three consecutive unsuccessful logins to the same actor from three different countries.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity/General Security
Rule	Consecutive Unsuccessful Logins to Same Actor from different IPs T1110	Detects set of three consecutive unsuccessful logins to the same actor from three different IPs.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity/General Security
Rule	Silver Ticket Attack Detected T1558.002	Detects silver ticket attacks. A silver ticket forges authentication tickets that the system creates when an attacker steals a user's password from Active Directory (AD). This ticket is used to forge ticket-granting service tickets, allowing unauthorized access to targeted resources.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity/General Security
Rule	Golden Ticket Attack Detected T1558.001	Detects golden ticket attacks. A golden ticket attack occurs when an attacker tries to access a domain through user data stored in the Microsoft Active Directory (AD). This allows attackers to bypass authentication, gaining access to the AD and its resources.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity/General Security

Resource Type	Resource Name	Description	Location
Rule	Pass-the-Hash Attack Detected T1550.002	Detects if Pass-the-Hash (PtH) attack detected.	/All Rules/ArcSight Foundation/User Behavior Monitoring/ Suspicious Activity
Rule	Successful Brute Force Account Login T1110	Detects each time a user logs in successfully after multiple unsuccessful attempts in a short time.  This rule depends on an entry in the active list: Brute Force Attempts.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity
Rule	Unsuccessful Brute Force Login Attempts T1110	Detects multiple unsuccessful logins to the account in a short time.  This rule adds an entry to the active list: Brute Force Attempts.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity
Rule	Possible LSASS Memory Dumping T1003.001	Detects when ProcDumps or MiniDumps via rundll32 are used to dump the memory space of Lsass.exe.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity/General Security
Rule	Possible Data Exfiltration T1041	Detects transfers of suspicious amounts of data to any host outside the network.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity/Network Based Anomaly Detection
Rule	Possible Data Exfiltration to External Website via PowerShell T1041	Detects possible data exfiltration to external website via PowerShell.	/All Rules/ArcSight Solutions/UBM/ Suspicious Activity/ Information Leakage
Rule	Attempted Bypass of MFA T1111	Detects attempts to bypass MFA.  Adversaries may target multi-factor authentication (MFA) mechanisms to gain access to credentials that can be used to access systems, services, and network resources.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity
Rule	Possible Scrapping of Outlook Inbox via PowerShell T1114.001	Detects possible scrapping of outlook inbox via PowerShell.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity/ Information Leakage

Resource Type	Resource Name	Description	Location
Rule	Possible Automated Collection via PowerShell T1119	Detects possible automated collection of files by PowerShell.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity/Information Leakage
Rule	Multiple MITRE Techniques Against the Same Actor	Detects sets of three MITRE ATT&CK Techniques against the same actor.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity/General Security
Pattern Discovery Profile	MITRE ATT&CK Activity - Department and MITRE Techniques	Identifies patterns related to MITRE Techniques by Department. By default, patterns will be identified when the same set of three or more MITRE Techniques and Triggered rules of at least two different departments.	/All Profiles/ArcSight Solutions/UBM/Suspicious Activity
Rule	Multiple Systems Logged into by Same User in a Short Time T1078.002	Detects each time a user logs in successfully into multiple systems in a short time.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity/General Security
Rule	Consecutive Unsuccessful Logins into Same Machine by Different Users T1078.002	Detects consecutive unsuccessful logins into same machine by different users in a short time.	/All Rules/Real-time Rules/UBM/Suspicious Activity/General Security
Rule	Multiple MITRE Techniques Against the Same Department	Detects sets of three MITRE ATT&CK Techniques against specific department.	/All Rules/ArcSight Solutions/UBM/Suspicious Activity/General Security
Pattern Discovery Profile	MITRE ATT&CK Activity - Users and MITRE Techniques	Identifies patterns related to MITRE Techniques by users. By default, patterns will be identified when the same set of three or more MITRE Techniques and Triggered rules of at least two different users.	/All Profiles/ArcSight Solutions/UBM/Suspicious Activity

Resource Type	Resource Name	Description	Location
Report	Actors	Offers comprehensive insights into actors registered on ESM.  It includes: <ul style="list-style-type: none"> <li>• A detailed listing of actors categorized by their identity management identifiers.</li> <li>• A speedometer chart illustrating the current availability status of actors within ESM.</li> <li>• A bar chart showcasing the distribution of actors across different identity management identifiers.</li> </ul>	/All Reports/ArcSight Solutions/UBM/Overview
Integration Command	User Lookup on Dark Website	Identifies if a user's email address is available on the dark web.	/All Integration Commands/ArcSight Solutions/UBM/External
Rule	Error During Token Validation  T1087.002	Detects errors that occur during token validations.	/All Rules/ArcSight Solutions/UBM/Federation Services
Dashboard	ADFS Health Check Status	Displays the top AD FS Health error and failure events.  Before running this dashboard, ensure the following data monitors are enabled: <ul style="list-style-type: none"> <li>• AD FS Health</li> <li>• AD FS Health Check Events - Bar Chart</li> </ul>	/All Dashboards/ArcSight Solutions/UBM/Federation Services
Filter	ADFS Health Errors and Failures	Filters for AD FS error or failure events.	/All Filters/ArcSight Solutions/UBM/Federation Services
Data Monitor	ADFS Health Check	Shows the top AD FS Health error and failure events.	/All Data Monitors/ArcSight Solutions/UBM/Federation Services
Data Monitor	ADFS Health Check Events - Bar Chart	Shows the top AD FS Health error and failure events on bar chart format.	/All Data Monitors/ArcSight Solutions/UBM/Federation Services
Active Channel	Monitor Successful MFA Token Validation	Displays successful MFA token validation events.	/All Active Channels/ArcSight Solutions/UBM/Federation Services

Resource Type	Resource Name	Description	Location
Field Set	Monitor Successful MFA Token Validation	Contains fields to monitor successful MFA token validation events.	/All Field Sets/ArcSight Solutions/UBM/Federation Services
Filter	Successful MFA Token Validation	Captures events when an MFA token is successfully validated.	/All Filters/ArcSight Solutions/UBM/ Federation Services
Rule	Multiple Token Validations Failed by User in a Short Time T1078.002	Detects when a token validation fails multiple times from the same user.	/All Rules/ArcSight Solutions/UBM/Federation Services
Rule	Extranet Lockout Event has Occurred T1110	Detects extranet lockout events. Extranet Lockout is a security feature that enables AD FS to stop authenticating malicious user accounts from outside the organization's network (extranet) for a specific period of time. This prevents the account from being locked out of the Active Directory, striking a balance between security and productivity.	/All Rules/ArcSight Solutions/UBM/Federation Services
Rule	Multiple Password Change Attempts Failed T1110.002	Detects when a user fails multiple password change attempts in a short time.	/All Rules/ArcSight Solutions/UBM/Federation Services

# Updated Content

ArcSight User Behavior Monitoring (UBM) updated the Threat Score Overview dashboard to support drill-downs and provide even better information about actor events in your environment. You can find this dashboard here: [/All Dashboards/ArcSight Solutions/UBM/Overview](#).

# ESM Requirements

Requires ArcSight ESM 7.7 or later.

# Downloading and Verifying the Installation Files

To download and verify the signature of your downloaded files:

1. Log in to the host where you want to begin the installation process.
2. Change to the directory where you want to download the installer files.
3. Download the product solution package .arb file: ArcSight-SolutionPackage-UBM-24.3.0.0.x.arb. from the [OpenText Downloads](#) website along with their associated signature files (\*.sig).



**Tip:** Evolving security needs imply the renewal of certificates for the signature verification procedure. To ensure a successful verification of your product signature, download the latest public keys file before proceeding with the verification process (step 1 of the Get the Public Keys procedure).

Open Text provides a digital public key that is used to verify that the software you downloaded from the Open Text software entitlement site is indeed from Open Text and has not been tampered with by a third party. For more information and instructions on validating the downloaded software, visit the [Open Text Code Signing site](#). If you discover a file does not match its corresponding signature (.sig), attempt the download again in case there was a file transfer error. If the problem persists, please contact Open Text Customer Support.

4. Begin the [installation or upgrade](#).

# Publication Status

Released: July 2024

Updated: Friday, June 21, 2024

## 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](mailto:MFI-Documentation-Feedback@opentext.com).

For specific product issues, contact [OpenText Customer Care](#).

# 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 (User Behavior Monitoring 24.3)**

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](mailto:MFI-Documentation-Feedback@opentext.com).

We appreciate your feedback!