



Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft ADFS Logs

Supplemental Configuration Guide

Document Release Date: December 18, 2020

Software Release Date: December 18, 2020

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Copyright Notice

© Copyright 2010-2020 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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:

[ArcSight Product Documentation on the Micro Focus Security Community](#)

Support

Contact Information

| | |
|---------------------------------------|---|
| Phone | A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information |
| Support Web Site | https://softwaresupport.softwaregrp.com/ |
| ArcSight Product Documentation | https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs |

Revision History

| Date | Description |
|------------|---|
| 12/18/2020 | First edition of this Configuration Guide, for initial support of these events. |

Contents

| | |
|--|----|
| SmartConnector for Microsoft Windows Event Log – Native: Microsoft ADFS Logs | 6 |
| Product Overview | 6 |
| Configuring Microsoft ADFS Logs | 6 |
| Installing and Configuring the Connector | 7 |
| Mappings for Microsoft ADFS Logs | 7 |
| General | 7 |
| Event 299 | 7 |
| Event 300 | 7 |
| Event 307 | 8 |
| Event 403 | 8 |
| Event 404 | 9 |
| Event 405 | 9 |
| Event 406 - Windows Server 2016 | 10 |
| Event 406 - Windows Server 2019 | 10 |
| Event 410 | 11 |
| Event 411 | 11 |
| Event 412 | 12 |
| Event 413 | 12 |
| Event 418 | 13 |
| Event 420 | 13 |
| Event 424 | 13 |
| Event 431 | 14 |
| Event 512 | 14 |
| Event 513 | 15 |
| Event 515 | 15 |
| Event 516 | 15 |
| Event 1102 | 16 |
| Event 1200 | 16 |
| Event 1201 | 16 |
| Event 1202 | 16 |
| Event 1203 | 17 |
| Event 1204 | 17 |
| Event 1205 | 17 |
| Event 1206 | 17 |
| Event 1210 | 17 |

| | |
|---|----|
| Common Mappings for Events - 1200, 1201, 1202, 1203, 1204, 1205, 1206, and 1210 | 17 |
| Send Documentation Feedback | 19 |

SmartConnector for Microsoft Windows Event Log – Native: Microsoft ADFS Logs

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft ADFS Logs and its event mappings to ArcSight data fields.

Supported Versions:

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides main mappings for the Windows Event Log SmartConnectors. The field mappings listed in this document are specifically for Microsoft Remote Access.

Product Overview

Active Directory Federation Service (ADFS) is a software component in Windows Server 2012, Windows Server 2016, and Windows Server 2019. It contains Active Directory, Federation Server, Federation Server Proxy, and ADFS Web Server.

ADFS provides the following services:

- **Single Sign-On (SSO):** ADFS provides SSO authorization to users who want to access applications in different networks or organizations. It provides SSO access to internet-facing applications or services.
- **Identity Federation (Identity Management):** This provides the digital identity to the users and allows to centralize it. This helps to maintain security and rights across security and enterprise boundaries.

Configuring Microsoft ADFS Logs

For information about Microsoft's ADFS events logs, see <https://adfshelp.microsoft.com/AdfsEventViewer/GetAdfsEventList> in the Microsoft TechNet Library.

Installing and Configuring the Connector

Follow the installation and configuration procedures in the [SmartConnector for MS Windows Event Log – Native SmartConnector \(WiNC\)](#) configuration guide, selecting **Microsoft Windows Event Log – Native** as the connector to be configured. During installation, select **true** for the **Security Logs** field for system events to be collected. It enables ADFS Auditing (Security) events to be captured.

Mappings for Microsoft ADFS Logs

General

| ArcSight Field | Vendor Field |
|----------------|-----------------|
| Device Product | 'ADFS Auditing' |
| Device Vendor | 'Microsoft' |

Event 299

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Destination DNS Domain | %3 (Relying Party) |
| Device Custom String 1 | %2 (Activity ID) |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 4 | %1 (Instance ID) |
| Device Custom String 4 Label | "Instance ID" |
| Message | __concatenate("A token was successfully issued for the relying party ",%3) |
| Name | "A token was successfully issued for relying party" |

Event 300

| ArcSight Field | Vendor Field |
|------------------------------|-------------------|
| Device Custom String 1 | %1 (Activity ID) |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 5 | %2 (Request type) |
| Device Custom String 5 Label | "Request Type" |

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Device Custom String 6 | %3 (Exception details) |
| Device Custom String 6 Label | "Exception details" |
| Message | "The Federation Service failed to issue a token as a result of an error during processing of the WS-Trust request" |
| Name | "Federation Service failed to issue a token as a result of an error" |
| Source Nt Domain | __extractNTDomain(%3) |
| Source User Name | __extractNTUser(%3) |

Event 307

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Device Custom String 4 | %1 |
| Device Custom String 4 Label | "Instance ID" |
| Name | "Federation service configuration was changed" |
| Source Nt Domain | __extractNTDomain(%3) |
| Source User Name | __extractNTUser(%3) |

Event 403

| ArcSight Field | Vendor Field |
|------------------------------|------------------|
| Destination Address | %9 (Local IP) |
| Destination Dns Domain | %14 |
| Destination Port | %8 (Local Port) |
| Device Custom Date 1 | %3 |
| Device Custom Date 1 Label | "Request Time" |
| Device Custom Number 1 | %11 |
| Device Custom Number 1 Label | "Content Length" |
| Device Custom String 1 | %2 |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 4 | %1 |
| Device Custom String 4 Label | "Instance ID" |
| Device Custom String 6 | %16 |

| | |
|------------------------------|--|
| Device Custom String 6 Label | "Proxy DNS name" |
| End Time | %3 |
| Name | "An HTTP request was received" |
| Old File Hash | __concatenate("Through Proxy:",%15) |
| Old File Id | __concatenate("Caller Identity:",%12) |
| Old File Type | __concatenate("Certificate Identity:",%13) |
| Request Client Application | %10 (User Agent) |
| Request Method | %5 (HTTP Method) |
| Request Url File Name | %6 (Url Absolute Path) |
| Request Url Query | %7 (Query string) |
| Source Address | %4 |
| Start Time | %3 |

Event 404

| ArcSight Field | Vendor Field |
|------------------------------|-----------------------------------|
| Device Custom Date 1 | %3 |
| Device Custom Date 1 Label | "Response Time" |
| Device Custom String 1 | %2 |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 4 | %1 |
| Device Custom String 4 Label | "Instance ID" |
| Device Custom String 5 | %5 |
| Device Custom String 5 Label | "Status Description" |
| End Time | %3 |
| Event Outcome | %4 |
| Name | "An HTTP response was dispatched" |

Event 405

| ArcSight Field | Vendor Field |
|------------------------|--------------|
| Destination Host Name | %3 |
| Device Custom String 1 | %1 |

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Device Custom String 1 Label | "Activity ID" |
| Message | __concatenate("Password change succeeded for following user:;",%2) |
| Name | "Password change succeeded" |
| Source Nt Domain | __extractNTDomain(%2) |
| Source User Name | __extractNTUser(%2) |

Event 406 - Windows Server 2016

| ArcSight Field | Vendor Field |
|------------------------------|---|
| Destination Host Name | %3 |
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Message | __concatenate("Password change failed for following user:;",%2) |
| Name | "Password change failed" |
| Reason | %4 |
| Source Nt Domain | __extractNTDomain(%2) |
| Source User Name | __extractNTUser(%2) |

Event 406 - Windows Server 2019

| ArcSight Field | Vendor Field |
|------------------------------|---|
| Destination Host Name | %4 |
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 4 | %3 |
| Device Custom String 4 Label | "Device Certificate" |
| Message | __concatenate("Password change failed for following user:;",%2) |
| Name | "Password change failed" |
| Reason | %5 |
| Source Address | %6 |
| Source Nt Domain | __extractNTDomain(%2) |
| Source User Name | __extractNTUser(%2) |

Event 410

| ArcSight Field | Vendor Field |
|------------------------------|---|
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 4 | %3 |
| Device Custom String 4 Label | "Client Application" |
| Device Custom String 5 | %13 |
| Device Custom String 5 Label | "Proxy" |
| Device Custom String 6 | %11 |
| Device Custom String 6 Label | "Forwarded Client IP" |
| Name | "Following request context headers present" |
| Old File Id | __concatenate(%6,"%",%7) |
| Request Client Application | %5 |
| Request Url File Name | %9 |
| Source Address | %15 |
| Source Translated Address | __regexToken(%11) |

Event 411

| ArcSight Field | Vendor Field |
|------------------------------|---------------------------|
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 4 | %2 |
| Device Custom String 4 Label | "Token Type" |
| Device Custom String 5 | %3 |
| Device Custom String 5 Label | "Error message" |
| Device Custom String 6 | %4 |
| Device Custom String 6 Label | "Exception details" |
| Name | "Token validation failed" |
| Reason | __regexToken(%3) |

| ArcSight Field | Vendor Field |
|------------------|------------------|
| Request Url | %2 |
| Source Address | %5 |
| Source User Name | __regexToken(%3) |

Event 412

| ArcSight Field | Vendor Field |
|------------------------------|---|
| Destination Dns Domain | %4 |
| Device Custom String 1 | %2 |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 4 | %1 |
| Device Custom String 4 Label | "Instance ID" |
| Device Custom String 6 | %3 |
| Device Custom String 6 Label | "Token type" |
| Message | __concatenate("A token of type ",%3," for relying party ",%4," was successfully authenticated") |
| Name | "A token for relying party was successfully authenticated" |

Event 413

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Destination Dns Domain | %5 |
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Name | "An error occurred during processing of a token request" |
| Old File Hash | __concatenate("Caller:",%2) |
| Old File Id | __concatenate("Device identity:",%6) |
| Old File Name | __concatenate("Act as User:",%4) |
| Source Address | %7 |
| Source User Name | __extractNTUser(%3) |

Event 418

| ArcSight Field | Vendor Field |
|----------------|--|
| File Hash | %4 |
| File Name | %2 |
| Name | "Trust between federation server proxy and service was successfully renewed" |
| Old File Hash | %3 |
| Source Address | %1 |

Event 420

| ArcSight Field | Vendor Field |
|------------------|--|
| File Hash | %4 |
| File Name | %3 |
| Name | "Trust between federation server proxy and service was successfully established" |
| Source Address | %2 |
| Source User Name | __extractNTUser(%1) |
| Source Nt Domain | __extractNTDomain(%1) |

Event 424

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 6 | %5 |
| Device Custom String 6 Label | "Inner exception" |
| File Hash | %2 |
| File Name | %3 |
| Name | "The federation server proxy was not able to authenticate the client certificate presented in the request" |
| Source Address | %4 |

Event 431

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 4 | %5 |
| Device Custom String 4 Label | "Token Type" |
| Device Custom String 5 | %4 |
| Device Custom String 5 Label | "Request Type" |
| Device Custom String 6 | %6 |
| Device Custom String 6 Label | "Signature Algorithm" |
| File Size | %2 |
| File Type | %3 |
| Name | "An active request was received at STS with RST" |

Event 512

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Device Custom Date 1 | __concatenate(%5, " ", %6) |
| Device Custom Date 1 Label | "Last Bad Password Attempt" |
| Device Custom Number 1 | %4 |
| Device Custom Number 1 Label | "Bad Password Count" |
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Message | __concatenate("The account for the following user ", %2, " is locked out. A login attempt is being allowed due to the system configuration") |
| Name | "The account for the following user is locked out" |
| Source Address | %3 |
| Source Nt Domain | __extractNTDomain(%2) |
| Source User Name | __extractNTUser(%2) |

Event 513

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 6 | %4 |
| Device Custom String 6 Label | "Exception details" |
| Name | "The Artifact REST service failed to return an artifact as a result of an error during processing" |
| Request Url | %3 |
| Source Address | %2 |

Event 515

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Event Outcome | "This account may be compromised" |
| Message | __concatenate("The following user ",%2," account was in a locked out state and the correct password was just provided. This account may be compromised") |
| Name | "The following user account was in a locked out state and the correct password was just provided" |
| Source Address | %3 |
| Source Nt Domain | __extractNTDomain(%2) |
| Source User Name | __extractNTUser(%2) |

Event 516

| ArcSight Field | Vendor Field |
|------------------------------|-----------------------------|
| Device Custom Date 1 | __concatenate(%5," ",%6) |
| Device Custom Date 1 Label | "Last Bad Password Attempt" |
| Device Custom Number 1 | %4 |
| Device Custom Number 1 Label | "Bad Password Count" |

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Name | "The following user account has been locked out due to too many bad password attempts" |
| Source Address | %3 |
| Source Nt Domain | __extractNTDomain(%2) |
| Source User Name | __extractNTUser(%2) |

Event 1102

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 5 | %4 |
| Device Custom String 5 Label | "Additional details" |
| Name | "The Federation Service authorized a request to one of the REST endpoints" |
| Request Url | %3 |
| Source Address | %2 |

Event 1200

| ArcSight Field | Vendor Field |
|----------------|---|
| Name | "The Federation Service issued a valid token" |

Event 1201

| ArcSight Field | Vendor Field |
|----------------|--|
| Name | "The Federation Service failed to issue a valid token" |

Event 1202

| ArcSight Field | Vendor Field |
|----------------|---|
| Name | "The Federation Service validated a new credential" |

Event 1203

| ArcSight Field | Vendor Field |
|----------------|--|
| Name | "The Federation Service failed to validate a new credential" |

Event 1204

| ArcSight Field | Vendor Field |
|----------------|--------------------------|
| Name | "A password was changed" |

Event 1205

| ArcSight Field | Vendor Field |
|----------------|---|
| Name | "A password change was attempted, but failed" |

Event 1206

| ArcSight Field | Vendor Field |
|----------------|---|
| Name | "A Sign Out request was successfully processed" |

Event 1210

| ArcSight Field | Vendor Field |
|----------------|--|
| Name | "An extranet lockout event has occurred" |

Common Mappings for Events - 1200, 1201, 1202, 1203, 1204, 1205, 1206, and 1210

| ArcSight Field | Vendor Field |
|--------------------------|----------------------|
| Application Protocol | AuthProtocol |
| Destination Dns Domain | RelyingParty |
| Destination Host Name | __regexToken(Server) |
| Destination Service Name | __regexToken(Server) |
| Device Custom Date 1 | LastBadAttempt |

| ArcSight Field | Vendor Field |
|------------------------------|--|
| Device Custom Date 1 Label | "Last Bad Attempt" |
| Device Custom Number 1 | __oneOfLong(CurrentBadPasswordCount) |
| Device Custom Number 1 Label | "Current Bad Password Count" |
| Device Custom Number 2 | __oneOfLong(ConfigBadPasswordCount) |
| Device Custom Number 2 Label | "Config Bad Password Count" |
| Device Custom String 1 | %1 |
| Device Custom String 1 Label | "Activity ID" |
| Device Custom String 5 | ForwardedIpAddress |
| Device Custom String 5 Label | "Forwarded Ip Address" |
| Device Custom String 6 | AuditType |
| Device Custom String 6 Label | "Audit Type" |
| Device Domain | NetworkLocation |
| Device External Id | DeviceId |
| Device Process Name | ClaimsProvider |
| Event Outcome | AuditResult |
| Old File Hash | __concatenate("SSO Binding Validation Level:",SSOBindingValidationLevel) |
| Old File Name | __concatenate("Device Auth:",DeviceAuth) |
| Old File Path | __concatenate("Primary Auth:",PrimaryAuth) |
| Old File Type | __concatenate("Failure Type:",FailureType) |
| Reason | ErrorCode |
| Request Client Application | UserAgentString |
| Source Address | IpAddress |
| Source Nt Domain | __extractNTDomain(UserId) |
| Source Translated Address | __regexToken(ForwardedIpAddress) |
| Source User Name | __extractNTUser(UserId) |

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 Supplemental Configuration Guide (Connectors 8.1.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!