



Micro Focus Security ArcSight Connectors

SmartConnector for Microsoft Windows Event Log – Native: Powershell

Supplemental Configuration Guide

Document Release Date: July 24, 2019

Software Release Date: July 24, 2019

Legal Notices

Copyright Notice

© Copyright 2010-2019 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.

US. 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 US registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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://communitysoftwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs |

Revision History

| Date | Description |
|------------|---|
| 06/19/2019 | First edition of this Configuration Guide, for initial support of ttthese events. |

Contents

| | |
|--|----|
| SmartConnector for Microsoft Windows EventLog – Native: Powershell | 6 |
| Product Overview | 6 |
| Configure Auditing for Specific Powershell Objects | 6 |
| Connector Installation and Configuration | 8 |
| Collect Events from the Event Log | 8 |
| General Mappings | 8 |
| Windows PowerShell Mappings | 9 |
| Event 400, 403 | 9 |
| Event 500, 501 | 9 |
| Event 600 | 10 |
| Event 800 | 11 |
| Windows Microsoft-Windows-PowerShell/Operational Mappings | 11 |
| Event 4100 | 11 |
| Event 4103 | 12 |
| Event 4104 | 13 |
| Event 4105 | 13 |
| Event 8193 | 13 |
| Event 8194 | 14 |
| Event 8195 | 14 |
| Event 8196, 12039 | 14 |
| Event 8197 | 14 |
| Event 24577 | 14 |
| Event 24579 | 15 |
| Event 24580 | 15 |
| Event 24581 | 15 |
| Event 24582 | 15 |
| Event 24583 | 15 |
| Event 24584 | 15 |
| Event 24592 | 16 |
| Event 24593 | 16 |
| Event 24594 | 16 |
| Event 24595 | 16 |
| Event 24596 | 16 |
| Event 24597 | 17 |
| Event 24598 | 17 |
| Event 24599 | 17 |
| Event 40961 | 17 |

| | |
|-----------------------------------|----|
| Event 40962 | 18 |
| Event 53249 | 18 |
| Event 53250 | 18 |
| Event 53504 | 18 |
| Send Documentation Feedback | 19 |

SmartConnector for Microsoft Windows Event Log – Native: Powershell

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

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

Product Overview

PowerShell is a task-based command-line shell and scripting language built on .NET. PowerShell helps system administrators and power-users rapidly automate tasks that manage operating systems (Linux, macOS, and Windows) and processes.

PowerShell commands let you manage computers from the command line. PowerShell providers let you access data stores, such as the registry and certificate store, as easily as you access the file system. PowerShell includes a rich expression parser and a fully developed scripting language.

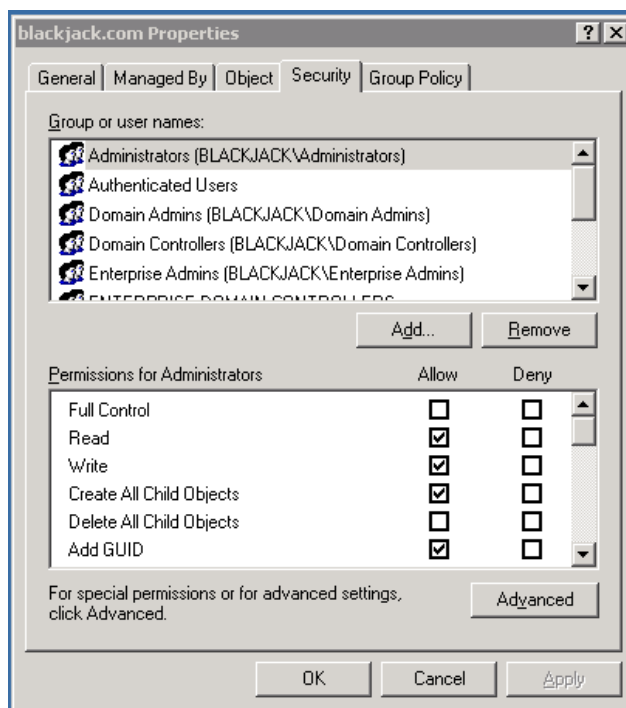
As it is widely used by the black hat community for initial access and further lateral movement within an enterprise, it is critical to properly collect and parse Windows Powershell logs. This would open the doors to writing correlation and hunt/search tools to find the APT's and other advanced threats.

Configure Auditing for Specific Powershell Objects

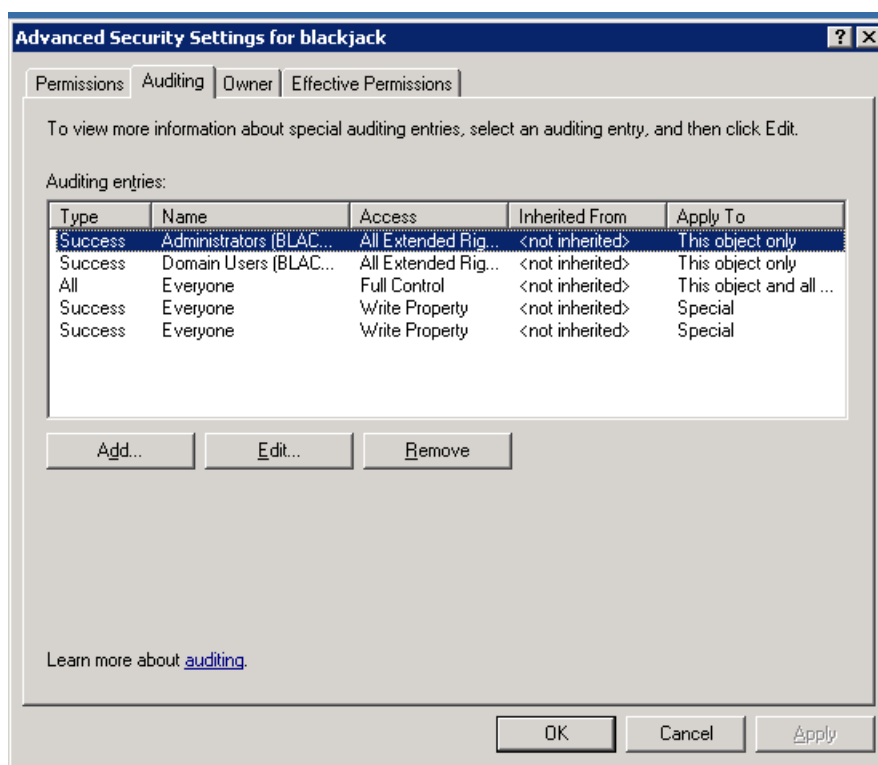
After you configure an audit policy setting, you can configure auditing for specific objects, such as users, computers, organizational units, or groups, by specifying both the types of access and the users whose access you want to audit.

To configure auditing for specific Powershell objects (steps may vary for differing Windows operating systems):

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Powershell Users and Computers**.
2. Verify that **Advanced Features** is selected on the **View** menu (the command has a checkmark beside it).
3. Right-click on the Powershell object you want to audit (**blackjack.com** in the example) and select **Properties**.



- Click the **Security** tab, then click the **Advanced** button; **Advanced Security Settings** for the object is displayed. Click the **Auditing** tab.



- To add an object, click **Add**.

6. Either enter the name of either the user or the group whose access you want to audit in the **Enter the object name to select** box, then click **OK**, or browse the list of names and then double-click either the user or the group whose access you want to audit.
7. Click to select either the **Successful** checkbox or the **Failed** checkbox for the actions you want to audit, then click **OK**. Click **OK** on the next two windows to exit.

Connector Installation and Configuration

Follow the installation and configuration procedures in the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Native*, selecting **Microsoft Windows Event Log – Native** as the connector to be configured.

Collect Events from the Event Log

To set up the connector to collect application events:

1. From \$ARCSIGHT_HOME\current\bin, double-click **runagentsetup.bat**.
2. Select **Modify Connector** on the window displayed and click **Next**.
3. Select **Modify connector parameters** and click **Next**.
4. Select **Navigate to the Modify table parameters** window.
5. Click **Next** to update the parameters; when you receive the successful update message, click **Next**.
6. Select **Exit** and click **Next** to exit the configuration wizard.
7. Restart the connector for your changes to take effect.

For more information about application event support, see the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Native*.

General Mappings

| ArcSight Field | Vendor Field |
|----------------|--------------|
| Device Vendor | 'Microsoft' |
| Device Product | 'PowerShell' |

Windows PowerShell Mappings

Event 400, 403

| ArcSight Field | Vendor Field |
|----------------------------|--|
| Name | 'Engine state is changed' |
| Message | 'Engine state is changed from,%2,'to,%1 |
| File Hash | %1 |
| Old FileHash | %2 |
| Device Custom Number 2 | SequenceNumber(Sequence Number) |
| Device Custom String 4 | All of (Host Name: 'HostName,', Host Version: 'HostVersion,', Host ID: 'HostId')(Host Information) |
| Request Client Application | HostApplication |
| Old File Id | RunspaceId |
| Device Custom Number 1 | PipelineId(Pipeline ID) |
| File Name | CommandName |
| File Type | CommandType |
| Old File Name | ScriptName |
| File Path | CommandPath |
| File Permission | CommandLine |
| Source NT Domain | UserId |
| Source User Name | UserId |

Event 500, 501

| ArcSight Field | Vendor Field |
|----------------------------|--|
| Name | 'Command State' |
| Message | 'Command "%1," is %2 |
| Device Custom Number 2 | SequenceNumber(Sequence Number) |
| Device Custom String 4 | All of (Host Name: 'HostName,', Host Version: 'HostVersion,', Host ID: 'HostId')(Host Information) |
| Request Client Application | HostApplication |

| ArcSight Field | Vendor Field |
|------------------------|-------------------------|
| Old File Id | RunspaceId |
| Device Custom Number 1 | PipelineId(Pipeline ID) |
| File Name | CommandName |
| File Type | CommandType |
| Old File Name | ScriptName |
| File Path | CommandPath |
| File Permission | CommandLine |
| Source NT Domain | UserId |
| Source User Name | UserId |

Event 600

| ArcSight Field | Vendor Field |
|----------------------------|---|
| Name | 'Provider State' |
| Message | 'Provider "%1," is "%2' |
| Device Custom Number 2 | SequenceNumber(Sequence Number) |
| Device Custom String 4 | All of (Host Name: ',HostName,', Host Version: ',HostVersion,', Host ID: ',HostId')(Host Information) |
| Request Client Application | HostApplication |
| Old File Id | RunspaceId |
| Device Custom Number 1 | PipelineId(Pipeline ID) |
| File Name | CommandName |
| File Type | CommandType |
| Old File Name | ScriptName |
| File Path | CommandPath |
| File Permission | CommandLine |
| Source NT Domain | UserId |
| Source User Name | UserId |

Event 800

| ArcSight Field | Vendor Field |
|----------------------------|---|
| Name | 'Pipeline execution details for command line' |
| Message | 'Pipeline execution details for command line: ;%1 |
| Device Custom String 1 | %3(Details) |
| Device Custom Number 2 | SequenceNumber(Sequence Number) |
| Device Custom String 4 | All of (Host Name: ;HostName,', Host Version: ;HostVersion,', Host ID: ;HostId)(Host Information) |
| Request Client Application | HostApplication |
| Old File Id | RunspaceId |
| Device Custom Number 1 | PipelineId(Pipeline ID) |
| Old File Name | ScriptName |
| File Permission | CommandLine |
| Source NT Domain | UserId |
| Source User Name | UserId |
| | |

Windows Microsoft-Windows-PowerShell/Operational Mappings

Event 4100

| ArcSight Field | Vendor Field |
|----------------------------|--|
| Name | 'Error Message' |
| Device Custom String 1 | UserData(User Data) |
| Device Severity | Severity |
| Device Custom String 4 | All of (Host Name: ;Host Name,', Host Version: ;Host Version,', Host ID: ;Host Id)(Host Information) |
| Request Client Application | HostApplication |
| Old File Id | RunspaceId |
| Device Custom Number 1 | PipelineId(Pipeline ID) |

| ArcSight Field | Vendor Field |
|------------------------|-----------------------------------|
| File Name | CommandName |
| File Type | CommandType |
| Old File Name | ScriptName |
| File Permission | CommandLine |
| Device Custom Number 2 | SequenceNumber(Sequence Number) |
| Source NT Domain | User |
| Source User Name | User |
| Device Custom String 6 | Connected User(Connected User) |
| Request Context | Shell ID |
| Message | Error Message,'Recommended Action |
| Reason | Fully Qualified Error ID |

Event 4103

| ArcSight Field | Vendor Field |
|----------------------------|--|
| Name | 'Command Invocation' |
| Message | Payload |
| Device Custom String 1 | UserData(User Data) |
| Device Severity | Severity |
| Device Custom String 4 | All of (Host Name: ',Host Name,', Host Version: ',Host Version,', Host ID: ',Host Id')(Host Information) |
| Request Client Application | HostApplication |
| Old File Id | RunspaceId |
| Device Custom Number 1 | PipelineId(Pipeline ID) |
| File Name | Command Name |
| File Type | Command Type |
| Old File Name | Script Name |
| File Path | Command Path |
| File Permission | Command Line |
| Device Custom Number 2 | SequenceNumber(Sequence Number) |
| Source NT Domain | User |

| ArcSight Field | Vendor Field |
|------------------------|--------------------------------|
| Source User Name | User |
| Device Custom String 6 | Connected User(Connected User) |
| Request Context | Shell ID |

Event 4104

| ArcSight Field | Vendor Field |
|------------------------|---|
| Name | 'Creating Scriptblock text' |
| Message | 'Creating Scriptblock text(,MessageNumber,' of ',MessageTotal,\');ScriptBlockText |
| Device Custom Number 1 | MessageNumber(Message Number) |
| Device Custom Number 2 | Message Total |
| File Name | ScriptBlockText |
| File Path | Path |

Event 4105

| ArcSight Field | Vendor Field |
|----------------|--|
| Name | 'Started invocation of ScriptBlock' |
| Message | 'Started invocation of ScriptBlock ID',ScriptBlockId |
| File ID | ScriptBlockId |
| Old File ID | RunspaceId |

Event 8193

| ArcSight Field | Vendor Field |
|------------------------|--|
| Name | 'Creating Runspace object' |
| Message | 'Creating Runspace object Instance Id:',param1 |
| Device Custom String 5 | param1(Instance Id) |

Event 8194

| ArcSight Field | Vendor Field |
|------------------------|--|
| Name | 'Creating RunspacePool object' |
| Message | 'Creating RunspacePool object Instance Id:',InstanceId |
| Device Custom String 5 | param1(Instance Id) |
| Device Custom Number 1 | MaxRunspaces(Max Runspaces) |
| Device Custom Number 2 | MinRunspaces(Min Runspaces) |

Event 8195

| ArcSight Field | Vendor Field |
|----------------|------------------------|
| Name | 'Opening RunspacePool' |
| Message | 'Opening RunspacePool' |

Event 8196, 12039

| ArcSight Field | Vendor Field |
|----------------|---|
| Name | 'Modifying activity Id and correlating' |
| Message | 'Modifying activity Id and correlating' |

Event 8197

| ArcSight Field | Vendor Field |
|----------------|------------------------------------|
| Name | 'Runspace state changed' |
| Message | 'Runspace state changed to',param1 |
| Device Action | param1 |

Event 24577

| ArcSight Field | Vendor Field |
|----------------|---|
| Name | 'Windows PowerShell ISE has started to run script file' |
| Message | 'Windows PowerShell ISE has started to run script file ',FileName |
| File Path | FileName |

Event 24579

| ArcSight Field | Vendor Field |
|----------------|--|
| Name | 'Windows PowerShell ISE is stopping the current command' |
| Message | 'Windows PowerShell ISE is stopping the current command' |

Event 24580

| ArcSight Field | Vendor Field |
|----------------|---|
| Name | 'Windows PowerShell ISE is resuming the debugger' |
| Message | 'Windows PowerShell ISE is resuming the debugger' |

Event 24581

| ArcSight Field | Vendor Field |
|----------------|---|
| Name | 'Windows PowerShell ISE is stopping the debugger' |
| Message | 'Windows PowerShell ISE is stopping the debugger' |

Event 24582

| ArcSight Field | Vendor Field |
|----------------|---|
| Name | 'Windows PowerShell ISE is stepping into debugging' |
| Message | 'Windows PowerShell ISE is stepping into debugging' |

Event 24583

| ArcSight Field | Vendor Field |
|----------------|---|
| Name | 'Windows PowerShell ISE is stepping over debugging' |
| Message | 'Windows PowerShell ISE is stepping over debugging' |

Event 24584

| ArcSight Field | Vendor Field |
|----------------|---|
| Name | 'Windows PowerShell ISE is stepping out of debugging' |
| Message | 'Windows PowerShell ISE is stepping out of debugging' |

Event 24592

| ArcSight Field | Vendor Field |
|----------------|--|
| Name | 'Windows PowerShell ISE is enabling all breakpoints' |
| Message | 'Windows PowerShell ISE is enabling all breakpoints' |

Event 24593

| ArcSight Field | Vendor Field |
|----------------|---|
| Name | 'Windows PowerShell ISE is disabling all breakpoints' |
| Message | 'Windows PowerShell ISE is disabling all breakpoints' |

Event 24594

| ArcSight Field | Vendor Field |
|----------------|--|
| Name | 'Windows PowerShell ISE is removing all breakpoints' |
| Message | 'Windows PowerShell ISE is removing all breakpoints' |

Event 24595

| ArcSight Field | Vendor Field |
|------------------------|---|
| Name | 'Windows PowerShell ISE is setting the breakpoint' |
| Message | 'Windows PowerShell ISE is setting the breakpoint at line #: 'CurrentLine,' of file 'FileName |
| Device Custom Number 3 | CurrentLine(Current Line) |
| File Path | FileName |

Event 24596

| ArcSight Field | Vendor Field |
|------------------------|--|
| Name | 'Windows PowerShell ISE is removing the breakpoint' |
| Message | 'Windows PowerShell ISE is removing the breakpoint on line #: 'CurrentLine,' of file 'FileName |
| Device Custom Number 3 | CurrentLine(Current Line) |
| File Path | FileName |

Event 24597

| ArcSight Field | Vendor Field |
|------------------------|--|
| Name | 'Windows PowerShell ISE is enabling the breakpoint' |
| Message | 'Windows PowerShell ISE is enabling the breakpoint on line #: 'CurrentLine,' of file 'FileName |
| Device Custom Number 3 | CurrentLine(Current Line) |
| File Path | FileName |

Event 24598

| ArcSight Field | Vendor Field |
|------------------------|---|
| Name | 'Windows PowerShell ISE is disabling the breakpoint' |
| Message | 'Windows PowerShell ISE is disabling the breakpoint on line #: 'CurrentLine,' of file 'FileName |
| Device Custom Number 3 | CurrentLine(Current Line) |
| File Path | FileName |

Event 24599

| ArcSight Field | Vendor Field |
|------------------------|--|
| Name | 'Windows PowerShell ISE has hit a breakpoint' |
| Message | 'Windows PowerShell ISE has hit a breakpoint on line #: 'CurrentLine,' of file 'FileName |
| Device Custom Number 3 | CurrentLine(Current Line) |
| File Path | FileName |

Event 40961

| ArcSight Field | Vendor Field |
|----------------|-------------------------------------|
| Name | 'PowerShell console is starting up' |
| Message | 'PowerShell console is starting up' |

Event 40962

| ArcSight Field | Vendor Field |
|----------------|--|
| Name | 'PowerShell console is ready for user input' |
| Message | 'PowerShell console is ready for user input' |

Event 53249

| ArcSight Field | Vendor Field |
|------------------------|---|
| Name | 'Scheduled Job started' |
| Message | 'Scheduled Job';ScheduledJobDefName,' started at ;StartTime |
| Device Custom String 1 | ScheduledJobDefName(Scheduled Job Name) |
| Start Time | Start Time |

Event 53250

| ArcSight Field | Vendor Field |
|------------------------|--|
| Name | 'Scheduled Job completed' |
| Message | 'Scheduled Job';ScheduledJobDefName,' completed at ;StopTime,' with state ;State |
| Device Custom String 1 | ScheduledJobDefName(Scheduled Job Name) |
| End Time | StopTime |
| Device Action | State |

Event 53504

| ArcSight Field | Vendor Field |
|------------------------|---|
| Name | 'Windows PowerShell has started an IPC listening thread' |
| Message | 'Windows PowerShell has started an IPC listening thread on process: ;param1,' in AppDomain: ;param2 |
| Destination Process Id | param1 |
| Device Custom String 1 | param2(App Domain) |

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)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!