



Micro Focus Security ArcSight Logger

Software Version: 1.0.0.0

SolarWinds IOC Activity

Document Release Date: January 25, 2021

Software Release Date: January 25, 2021

Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2021 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/ct-p/productdocs

Contents

Overview	5
Installation and Uninstallation	5
Installing the SolarWinds IOC Activity Content Package	5
Configuring the Lookup File	5
SolarWinds IOC Activity Content Package Resources	6
Send Documentation Feedback	7

Overview

The SolarWinds IOC Activity is a content package which leverages ArcSight Logger to detect any communication between your organization and SolarWinds SUNBURST IOC.

Installation and Uninstallation

Installing the SolarWinds IOC Activity Content Package

The complete process of setting up the SolarWinds IOC Activity Content Package includes Configuring the lookup files and then installing the content.

Configuring the Lookup File

The SolarWinds IOC by IP Address Search is based on monitoring the following Sunburst IPs:

`solarwinds_ips.csv`

In order to configure Logger to monitor and download this file, follow the instructions below:

1. In Logger, select Configuration > Lookup Files > Add. Then, in the dialog box, enter the following values for the lookup file.

Name: ips

File Location: On Logger

Path and File: <location of the solarwinds_ips.csv file>>

Schedule: One time only

2. Save your changes.

To Install the SolarWinds IOC Activity Content Package:

1. Download the installer file `Solarwinds_IOC_Activity_1.0.0.0.xml.gz` to a secure network location.
2. In **Logger**, select **Configuration > Import Content**.
3. Search for the file `Solarwinds_IOC_Activity_1.0.0.0.xml.gz`.

The Content Package and the resources are installed.

To Uninstall the SolarWinds IOC Activity Content Package:

To uninstall the dashboard:

1. Select **Dashboards > Malicious Activity Dashboard**.
2. Click **Tools > Delete Dashboard**.
3. Click **Yes** to confirm changes.

To uninstall saved searches:

1. Select **Configuration > Saved Searches**.
2. For each SolarWinds saved search, click the **Remove** icon.
3. Click **Yes** to confirm changes.

SolarWinds IOC Activity Content Package Resources

Resource	Type	Description
Solarwinds IOC by Host Name	Saved Search	Displays any communication between your organization and SolarWinds IOC domains
Solarwinds IOC by IP Address	Saved Search	Displays any communication between your organization and SolarWinds IOC IPs

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 SolarWinds IOC Activity (Logger 1.0.0.0)

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!