opentext™

ArcSight SmartConnectors

Software Version: 8.4.x

Installation Guide for ArcSight Content and Context Updates

Document Release Date: 2023
Software Release Date: 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

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.

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

Installation Guide for ArcSight Content and Context Updates

Installation Guide for ArcSight Content and Context Updates

This guide provides information to install the ArcSight Content and Context updates.

> **Note**: From May 2023 onwards, the ArcSight Context-GeoLocation & Vulnerability Signature updates and ArcSight Content-Categorization updates will be a monthly release.

Content AUP 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 might 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.

Context Update also known as ArcSight Context-GeoLocation & Vulnerability Signature Updates is delivered through ESM and Logger SKUs. Context updates are based on the following 3 factors which changes in every release:

- Vulnerability Signatures: Every single ArcSight release provides additional context as part of the event enrichment process and lets ESM leverage this data as it analyzes the barrage of IDS and other security alerts available for popular products like Snort, Juniper, TippingPoint, etc.
- Sensor Signatures: The term signature refers to signatures, rules, and filters. Customers use IPS systems to monitor networks for suspicious traffic. Mostly a set of filters or rules, which is commonly known as signatures, is designed to identify various types of network events. Signatures are often associated with vulnerabilities. ArcSight collects this information and stores it in the categorization database. Vulnerabilities are mapped to a signature. From a signature, one can find the associated vulnerabilities.
- `ipdataV6`: We have a redistribution license for Maxmind DB, which is a third-party geolocation database that is updated every week. The MaxMind and the geolocation information are distributed via a binary data file known as `ipdataV6.mmdb`.

> **Important**: Every information submitted to MaxMind is subjected to modifications as they have the final destination to introduce the modifications on DB's that they provide to build the Context Builds. Every correction is reviewed by MaxMind to ensure that is accurate and complies with their policies which might take 2-3 weeks. No requests are accepted for changing anonymous proxy or VPN IP addresses.

Installation Guide for ArcSight Content 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.

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.

Installing ArcSight Content-Categorization Updates

Important: Micro Focus recommends the customers to use this AUP Content version on the latest release of SmartConnectors.

Note: ArcSight Content Updates are packaged in the form of AUP files. To obtain the updated files, navigate to https://softwaresupport.softwaregrp.com/ and log in using the **user ID** and **password**.

Applying on ESM

To apply a new Content AUP:

1. Log in to an ESM machine.
2. Copy the **.aup** file to **ARCSIGHT_HOME\updates\** directory.
3. SmartConnectors registered to this ArcSight Enterprise Security Manager downloads the file, and generates an audit event once completed.

The ArcSight Enterprise Security Manager finds the new content and pushes it to the SmartConnectors. When the updates occurs, each of the affected SmartConnectors triggers an audit event to ArcSight Enterprise Security Manager.

Applying on ArcMC

To apply Content AUP:

1. Copy the downloaded Content AUP file to the machine that is used to connect to the browser-based interface.
2. Log in to the browser-based interface for ArcSight Management Center, from the computer where the AUP file is downloaded.
3. Click **Administration** > **Repositories**.
4. Click **Content AUP** from the left panel.
5. Click **Upload** from the right panel.

6. Click **Browse** and **Select** the file you downloaded.
7. Click **Submit** to add the specified file to the repository and send it to all the applicable connectors.

Modified Signatures

There is a list of signatures within which the categorization gets modified. Every Content AUP release might not contain any modified signatures and this changes with every release. The user can find these signatures in the Release Notes.

Installing ArcSight Context-GeoLocation & Vulnerability Signature Updates

Applying and Verifying Context Updates on ArcSight ESM

1. Make a note of the md5 checksum generated for the files, as the values change with every release. The updated values are provided along with the mappings for every release. For detailed description, click Release Notes for 2022 Context Updates.
2. Copy the .zip file over to the **$ARCSIGHT_HOME/config/server** directory on ESM.
3. Unzip the file in **$ARCSIGHT_HOME/config/server**, and replace the existing files with the unzipped files.
4. Remove the **.new** file extension.
5. Verify the md5 checksum values for the files.
6. ESM renames files from previous releases with a timestamp appended to their names. These files are saved in the same directory as the unzipped files.
7. To verify if the updates are successfully applied on the ArcSight Enterprise Security Manager, check the timestamped files from the last release.
8. Verify that the three new files are unzipped. The ArcSight Enterprise Security Manager will use the new files until the next release update. These file names are present in the Release Notes.

Note: Restarting the manager is not required with this version.

Important: Make sure to check the Release Notes for the specified version of ArcSight Enterprise Security Manager for the updates to work properly.

For more information on this process, see ESM Administrator's Guide.

Applying on Logger

1. Log in to **ArcSight Logger**.
2. Navigate to **Configuration** > **Import Content**.
3. Click **Choose File**.
4. **Locate** the specific file name.

5. Click **Import**. A message will be acknowledging the request.
6. Verify that the new file named `ipdataV6.mmdb` was imported to `<loggerInstallation>/config/logger/server/`.

   When new release files are imported to Logger, the old files are automatically renamed in the following format:

   `ipdataV6_year-month.mmbd`.

> **Note**: ArcSight Logger stores a maximum of 4 geolocation files by default. The Logger search panel uses the latest imported file.

For more information on this process, see the Logger Administrator's Guide.

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 Installation Guide for ArcSight Content and Context Updates (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!