
Micro Focus Security ArcSight SmartConnectors

SmartConnector for Amazon Web Services S3 Configuration Guide

Document Release Date: July 31, 2020

Software Release Date: July 31, 2020



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 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/ct-p/productdocs

Revision History

Date	Description
07/24/2020	First edition of this guide. Added support for Cisco Umbrella (ver 1 & 2) - DNS Logs

Contents

SmartConnector for Amazon Web Services S3	5
Product Overview	5
Understanding Data Collection	6
S3 Approach - Poll Approach (Recommended for Vendor Managed S3 Buckets)	6
SQS Approach - Notification Approach (Recommended for Customer Managed S3 Buckets)	6
Setting up an AWS Account	7
Creating a Group with Users Added	8
Log Retrieval Configuration	9
S3 Approach - Poll Approach (Recommended for Vendor Managed S3 Buckets)	9
SQS Approach - Notification Approach (Recommended for Customer Managed S3 Buckets)	9
Creating an S3 bucket and Configure it to Receive logs	9
Creating an SQS queue to poll and Configure S3 to send Events to SQS on a new Object	10
Install the SmartConnector	11
Prepare to Install Connector	11
Install Core Software	11
Set Global Parameters (optional)	12
Select Connector and Add Parameter Information	14
Complete Installation and Configuration	16
Run the SmartConnector	16
Device Event Mapping to ArcSight Fields	17
Cisco Umbrella DNS Logs Mappings to ArcSight Fields	18
Troubleshooting	18
Send Documentation Feedback	20

SmartConnector for Amazon Web Services S3

This guide provides information for installing the SmartConnector for Amazon Web Services S3 and configuring the device for event collection from an AWS S3 bucket. Currently, only Cisco Umbrella DNS Logs are supported but it is expected to support more events from different vendors in the future.

However, the connector can support other log sources available in an AWS S3 bucket. One connector instance can support one log source. To support multiple log sources, install multiple instances of the AWS S3 connector and provide specific configurations. With parser updates, the connector can support extended events of existing log sources or a complete new log source.

The supported log formats are:

- CSV
- Json
- Regex
- Key, value pair

Product Overview

Amazon Web Services (AWS) is a collection of remote computing services (also called web services) that make up a cloud computing platform offered by Amazon which provides online services for other websites or client-side applications.

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. You must create a bucket in one of the AWS regions to upload your data. You can then upload any number of objects to the bucket.

Amazon Simple Queue Service (SQS) is a fully managed service that works with serverless systems, micro-services, and distributed architectures. It has the capability of sending, storing and receiving messages at scale without dropping message data.

Understanding Data Collection

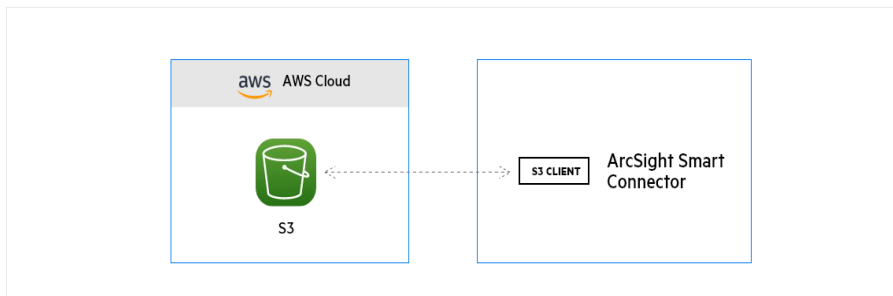
The following diagram provides a high-level overview on the data collection flow. With the SmartConnector for AWS S3, you can choose one of the two approaches below to collect events from an S3 bucket.

S3 Approach - Poll Approach (Recommended for Vendor Managed S3 Buckets)

When choosing this approach, the connector will directly enumerate an S3 bucket for the new files. This approach is recommended when logs are stored in the vendor's AWS S3 bucket with limited access.

Process Flow

1. A file is enumerated from a specified folder in S3.
2. The log files are collected from S3.
3. The log files are processed.
4. The connector will continue to collect only new and unprocessed files.



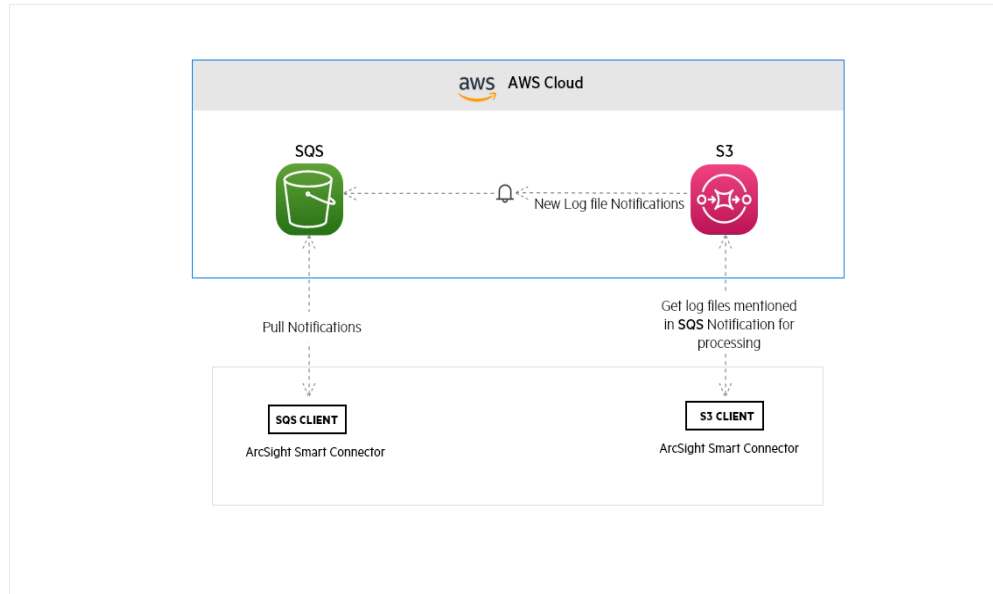
SQS Approach - Notification Approach (Recommended for Customer Managed S3 Buckets)

When choosing this approach, the connector will poll SQS for S3 notifications and collect log files from an S3 bucket. This approach is recommended when users have control over the AWS account with permissions to create SQS and configure S3 notifications to SQS.

Process Flow

1. AWS S3 is configured to send notifications from a new file to SQS.
2. The connector reads the SQS notifications.

3. Based on the SQS notifications, the log files are collected from the S3 bucket.
4. The log files are processed.
5. The SQS messages are deleted.



Setting up an AWS Account

Follow the instructions below if you are using an access key/secret key as credentials. If you are using an EC2 role-based credentials, you must use an IAM role with AmazonS3ReadOnlyAccess and AmazonSQSFullAccess policies, instead.

1. Create an Amazon Web Services account.
2. From the Welcome to Amazon Web Services window, click **Launch Management Console**.
3. From the Amazon Web Services menu < Administration & Security, select **Identity & Access Management**.
4. On the left side of the console, go to **Dashboard** and select Groups.
5. Create a new group with permissions to access the logs stored in S3 through the API.
6. Click **Create New Group** and enter a **Group Name**, for example, arcsightgroup.
7. Click **Next** to attach two policies to the group.
8. Select the **AmazonS3ReadOnlyAccess** and **AmazonSQSFullAccess** checkboxes policies of the arcsightgroup and click **Next**.
The connector can now download logs.
9. Click **Create Group**.

Creating a Group with Users Added

To create new users to be added to a group:

1. Return to the Amazon Web Services console. On the left pane, go to **Dashboard**.
2. Select **Users** and click **Create New Users**.
Create a user to access the logs stored in S3 through the API.
3. Enter the user name, for example, arcsight2.
4. Select the **Generate an Access Key** check box for each user and click **Create**.
A confirmation window is displayed.
5. Click the **Download Credentials** and save the .csv file.
Download the Access Key ID and Secret Access Key. You will need them while installing the connector.
6. Click **Close** and return to the **Dashboard**.
7. Under **Dashboard**, select **Groups** and click the arcsightgroup previously created.
8. Click **Add Users to Group**.
9. Select the check boxes next to the users previously created, and click **Add Users**.

AWS Credentials

In the configuration window, you can enter the AWS access key and AWS secret key. These parameters are optional and will be used if provided. Otherwise, the Default Credential Provider Chain is used, instead. The Default Credential Provider Chain searches for credentials in the following order, as documented by [Class Default AWS Credentials Provider Chain](#).

1. In the environment variables: AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY (These recommended since they are recognized by all the AWS SDKs and CLI except for .NET), or AWS_ACCESS_KEY and AWS_SECRET_KEY (only recognized by Java SDK).
2. In the Java system properties: aws.accessKeyId and aws.secretKey.
3. In the **Web Identity Token Credentials**, from the environment or container
4. In the default **Credential Profiles** file, the (~/.aws/credentials) is shared by all AWS SDKs and the AWS CLI.
5. Credentials delivered through the Amazon EC2 container service if AWS_CONTAINER_CREDENTIALS_RELATIVE_URI" environment variable is set and security manager has permission to access the variable.
6. In the instance **Profile Credentials**, through the Amazon EC2 metadata service.

Log Retrieval Configuration

S3 Approach - Poll Approach (Recommended for Vendor Managed S3 Buckets)

Users with customer-managed S3 buckets may also choose the S3 Approach setup, although, this approach is highly recommended for users with vendor-managed S3 buckets.

- If your bucket is vendor-managed, note the AWS credentials (access key and secret key, the S3 bucket name, the S3 folder name and the S3 region).
 - To enable logging Cisco Umbrella logs to a Cisco-managed S3 Bucket, see, [Enable Logging to a Cisco-managed S3 Bucket](#).
- If you manage the AWS account and the S3 bucket:
 - Set up an AWS account and create an Identity and Access Management (IAM) user or role.
 - Create an S3 bucket and configure it to receive logs.

Note: S3 buckets can be encrypted or non-encrypted.

You can also consider using this approach if the service provider (in this case, Cisco Umbrella), manages the AWS account and as a user you are not authorized to create AWS resources.

SQS Approach - Notification Approach (Recommended for Customer Managed S3 Buckets)

1. Set up an AWS account and create an Identity and Access Management (IAM) user or role.
2. Create an S3 bucket and configure it to receive logs.
3. Create an SQS queue and configure S3 to send events to SQS on new object creation.

Creating an S3 bucket and Configure it to Receive logs

To create a new S3 bucket:

1. Log in to the AWS Management Console and open the **Amazon S3** console.
2. Click **Create bucket**.
3. In the **Create bucket** dialog box, enter the **Bucket Name** of your S3 bucket, for example, arcsights3.
4. Accept or edit the default value settings in the other fields.
5. Click **Create**.

Your new S3 bucket is now listed under the S3 bucket names.

The configuration to receive DNS logs may change based on the device.

For Cisco Umbrella, see [Enable Logging to Your Own S3 Bucket](#).

Creating an SQS queue to poll and Configure S3 to send Events to SQS on a new Object

To create a new queue:

1. Log in to the **AWS Management** Console and open the **Amazon SQS** console.
2. Click **Create New Queue**.
3. In the **Create New Queue** dialog box, enter the **Bucket Name** of your S3 bucket, for example, arcsightQueue.
4. Accept or edit the default value settings of the other fields.
5. Click **Create Queue**.

Your new queue is now listed under the queue names.

6. Select the Queue created.
 - a. Click **Permissions**.
 - b. Click **Add permission**.
 - c. From **Select Effect**, click **Allow**.
 - d. Enter Principal.
 - e. Select Actions: Delete Message, Receive Message, and Send Message.
 - f. Click **Add Permission**.

To configure S3 to send events to SQS on a new object, see [Amazon Documentation](#).

1. Log in to the **AWS Management** Console and open the **Amazon S3** console.
2. Select the S3 bucket created to receive logs.
3. Click **Properties** and select **Events**.
4. In the Events dialog, add a notification:
 - a. Enter the notification Name
 - b. Click **Events < All objects create events**.

This option is triggered when the events are sent to SQS, for example, all object create events on a specific prefix.

- c. Enter a **prefix** (the folder name to receive device logs).
- d. Select **Send to as SQS Queue**.
- e. Select the **SQS queue** created above.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the Administrator's Guide as well as the Installation and Configuration guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the ArcSight Management Center Administrator's Guide for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the SmartConnector Product and Platform Support document, available from the Micro Focus SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction

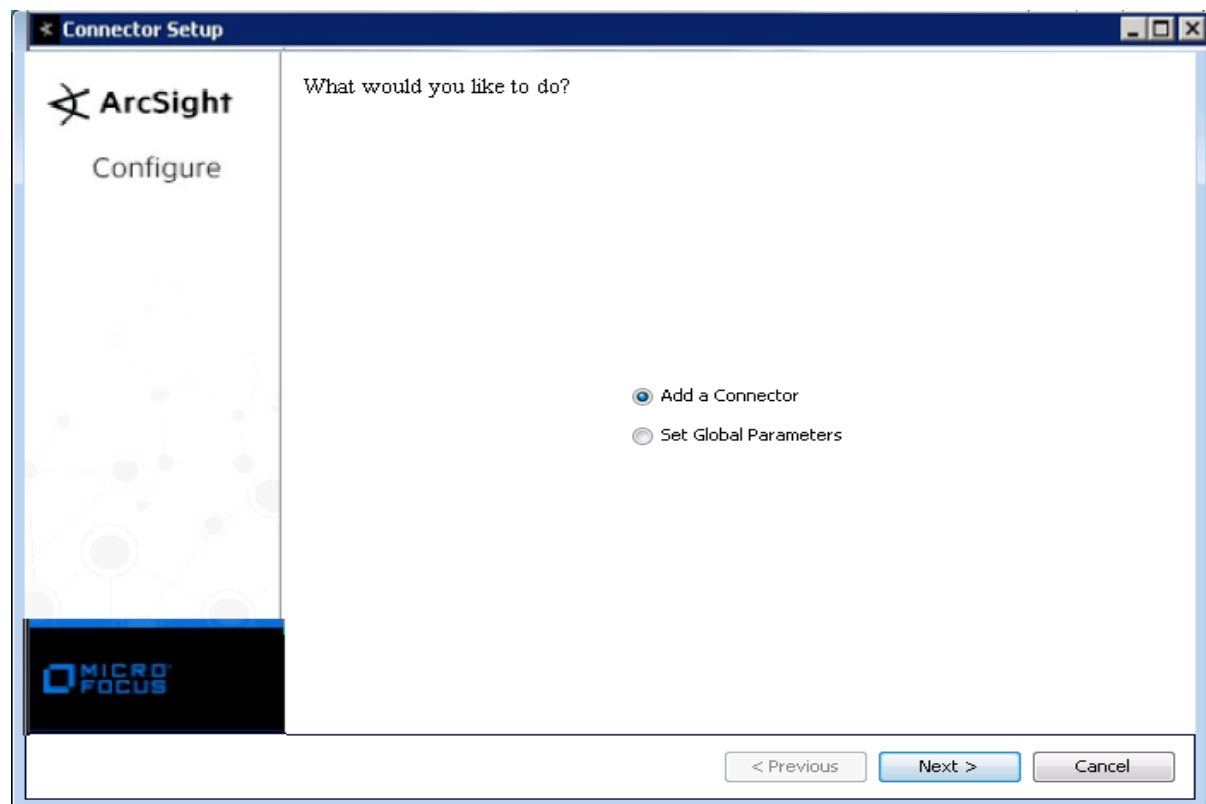
Choose Install Folder

Choose Shortcut Folder

Pre-Installation Summary

Installing...

3. When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4
The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the Micro Focus SecureData Architecture Guide for more information.	
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypted	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
2. Select **Amazon Web Services S3** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Details
Log Type	Enter Log Type, the default option is CiscoUmbrella-DnsLogs.
Proxy Host	Enter the proxy host IP address or name. This value is required to configure the proxy.
Proxy Port	Enter the proxy port. This value is required to configure the proxy.
Proxy User Name	Enter the proxy user name. This value is optional for additional proxy authentication. If you enter proxy user name, you must also enter a proxy password.
Proxy Password	Enter the password for the proxy user specified in the Proxy User Name field. This value is optional for additional proxy authentication. This field is required only if you have specified a proxy user name.

Parameter	Details
AWS Access Key	Enter the AWS access key. This is optional and will be used if provided. If not, the Default Credential Provider Chain will be used. For more information, see "AWS Credentials" on page 8 .
AWS Secret Key	Enter the AWS secret key. This is optional and will be used if provided. If not, the Default Credential Provider Chain will be used. For more information, see "AWS Credentials" on page 8 .
Polling Approach	For S3: provide the S3 bucket name, S3 folder name and S3 region details. For SQS: provide SQS URL, SQS region and S3 region.
AWS S3 Bucket Name	Enter the name of the AWS S3 bucket that will be sending logs out.
AWS S3 Folder Name	Enter the folder name in which the logs appear. For example: AWS S3 > bucket-name > folder-name
AWS S3 Region	Choose the S3 region code.
AWS SQS Region	Choose SQS the region code.
AWS SQS URL	The SQS URL from which AWS S3 notifications are pulled.

- The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.
- Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and Password should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click Next.
- Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.
- If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.
2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.
3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.
4. Click **Next** on the summary window.
5. To complete the installation, choose **Exit** and click **Next**.

For instructions about upgrading the connector or modifying parameters, see the SmartConnector User Guide.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the ArcSight SmartConnector User Guide.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file

`$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Performance Tuning

By default, the connector application maximum heap size is set to 256MB. If users with higher system configurations, expect higher EPS, update the changes below to improve the performance.

1. Stop the connector.
2. Increase heap size to perform more in memory operations. For more information, see [Increase Memory Size for XML Reports](#).
 - a. To increase the memory size for stand-alone connectors from the command line, change the following line in


```
$ARCSIGHT_HOME\current\bin\scripts\connectors.bat (Windows)
```

```
$ARCSIGHT_HOME/current/bin/scripts/connectors.sh (Linux)
```

```
ARCSIGHT_MEMORY_OPTIONS=" -Xms256m -Xmx256m "
```

 to


```
ARCSIGHT_MEMORY_OPTIONS=" -Xms1024m -Xmx1024m "
```
 - b. To increase the memory size for connectors being run as a service, change the following lines in `user/agent/agent.wrapper.conf` from:


```
wrapper.java.initmemory=256 wrapper.java.maxmemory=256
```

 to


```
wrapper.java.initmemory=1024 wrapper.java.maxmemory=1024
```
3. To increase the memory size for connectors managed by the Connector Appliance/ArcSight Management Center, the heap size can be set using a container level command.


```
<Install path>\current\user\agent\agent.properties
```

 Existing: `awsthreadcount=1`
 New: `awsthreadcount=5`
4. Start the connector.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the ArcSight Console User's Guide for more information about the ArcSight data fields.

Cisco Umbrella DNS Logs Mappings to ArcSight Fields

ArcSight Field	Vendor Field
Device Vendor	Cisco
Device Product	Umbrella
Start Time	DateTime
Device Custom String 2	Policy Identity
Device Custom String 3	Identities
Source Address	InternalIp
Source Translated Address	ExternalIp
Device Action	Action
Device Custom String 1	QueryType
Name	ResponseCode: Action
Device Custom String 6	ResponseCode
Destination Dns Domain	Domain
Device Custom String 5	Categories
Device Severity	ResponseCode
Device Event Class Id	ResponseCode: Action

Troubleshooting

1. Agent is configured but not generating event.
 - a. Check for errors in <Install path>\current\logs\agent.log.
 - b. If any errors related to AWS permissions are found, refer to ["Log Retrieval Configuration" on page 9](#)
2. When using the SQS approach, the configuration may be completed without any errors displayed on the configuration window, even if the IAM user does not have the required permissions. Post-configuration, the IAM user will not be able to process any events.
 In this case, the installer does not control and/or validate the S3 bucket details.
 Check for errors in <Install path>\current\logs\agent.log.

If any errors related to AWS permissions are found, see ["Log Retrieval Configuration" on page 9](#)

3. When noticing frequent AWS API calls, checking for new S3 files or SQS Messages:
 - a. If a specific interval was defined to receive new files, set the time interval in connector configuration.
`<Install path>\current\user\agent\agent.properties`
 - b. Replace `pollingfrequencyinsec=10` for `pollingfrequencyinsec=<Defined new file arrival interval in seconds>`
4. When using the S3 approach, how to re-process the log files?
 - a. Stop running agent.
 - b. Clear the `<Install path>\current\user\agent\ageantdata` folder to discard the intermediate state.
 - c. Restart agent.
5. When a file is deleted or the connector is restarted, SQS notifications can get into flight mode.
 - a. S3 must be configured to send events to SQS on new object creation. The connector will only delete SQS only if the message is successfully processed.
6. Agent setup pops the following message "Enter valid AWS Credentials and parameters to retrieve AWS logs."
 - a. Ensure you are using valid AWS credentials with valid permissions. For more information, see ["Log Retrieval Configuration" on page 9](#).
 - b. If using the SQS approach, make sure these values are correct:
AWS SQS URL
AWS SQS Region
AWS S3 region
 - c. If using the S3 approach, make sure these values are correct:
AWS S3 bucket name
AWS S3 folder name
AWS S3 region

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 Configuration Guide (SmartConnectors 8.0.0)

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!