MICRO FOCUS®

Micro Focus Security ArcSight Connectors

SmartConnector for Amazon Web Services CloudTrail

Configuration Guide

April 16, 2018

Configuration Guide

SmartConnector for Amazon Web Services CloudTrail

April 16, 2018

Revision History

Date	Description
04/16/2018	Added mapping for 'Source Process Name' event. Removed mappings for: 'Request Cookies', 'File Name' and 'Device Custom String 4'.
11/15/2017	Added mapping for 'Device Receipt Time' event in place of 'Start Time' event.
10/17/2017	Updated descriptions for AWS SQS Region and AWS S3 Region. Added encryption parameters to Global Parameters.
07/15/2017	Noted that the connector can also be configured with S3 buckets that are encrypted.
05/15/2017	Added support for event collection from Key Management Service (KMS). The connector can now use EC2 role-based access.
11/30/2016	Updated parameter descriptions for AWS regions. Updated installation procedure for setting preferred IP address mode.
06/30/2015	Initial release of this connector.

SmartConnector for Amazon Web Services CloudTrail

This guide provides information for installing the SmartConnector for Amazon Web Services CloudTrail and configuring the connector for event collection. Event collection from Amazon Identity and Access Management (IAM), Elastic Compute Cloud (EC2), Key Management Service (KMS), and CloudTrail is supported.

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.com, which provides online services for other web sites or client-side applications. AWS CloudTrail records API calls for your account and delivers log files. The recorded information includes the API caller identity, the time of the API call, the source IP address of the caller, the request parameters, and the response returned by the service.

For complete information about AWS CloudTrail, search for Amazon Web Services CloudTrail to access Amazon documentation.

CloudTrail Log Retrieval Configuration

To set up the connector to retrieve events:

■ Set up an AWS account and create an Identity and Access Management (IAM) user or role

■ Configure CloudTrail to create an S3 bucket and SNS topic

> S3 buckets can be encrypted or non-encrypted.

■ Create an SQS queue for the connector to poll and subscribe the queue to the SNS topic

Set up an AWS Account and Create a Group with Users Added

Follow the instructions in this section only if you are using access key/secret key as credentials. If you are using EC2 role-base credentials, then you must use an IAM role with `AmazonS3ReadOnlyAccess` and `AmazonSQSFullAccess` policies instead.

1   Acquire an Amazon Web Services account.

2   Click **Launch Management Console** from the Welcome to Amazon Web Services window.

3   From the Amazon Web Services menu, under **Administration & Security**, select **Identity & Access Management**.

4   Under **Dashboard** on the left side of the console window, select **Groups**.

5   You will create a new group with permissions to access the CloudTrail logs through the API. Select the **Create New Group** tab and then enter a **Group Name** for example, **arcsightgroup**.

6   Click **Next Step** to attach two policies to the group.

7   Select the checkboxes for **AmazonS3ReadOnlyAccess** and **AmazonSQSFullAccess** policies to the **arcsightgroup**. This lets the connector download the logs.

8   Click **Next Step** and then click **Create Group**.

9   To create new users to add to the group, return to the Amazon Web Services console. Under **Dashboard** in the left pane, select **Users**; then click the **Create New Users** tab. You need to create a user to be used to access the CloudTrail logs through the API.

10   Enter the user name (for example **arcsight2**). Make sure the checkbox for **Generate an access key for each user** is checked. Click **Create**.

11   When the user is created, a confirmation window displays. Make sure you click the **Download Credentials** button and save the .csv file. This is the only chance you will have to download the Access Key ID and Secret Access Key. You will use these when installing the connector.

12   Click **Close** to return to the **Dashboard**.

13   Select **Groups** under **Dashboard** and click the **arcsightgroup** (created in step 5 above).

14   Click **Add Users to Group**.

15   Select the checkbox next to the users (created in step 10 above) and click **Add Users**.

Configure CloudTrail

In this section, you will create a new S3 bucket and a new SNS topic.

To configure CloudTrail for the first time:

1   From the console, select the **CloudTrail** icon from the **Administration & Security** portion of the menu.

2   Create a new bucket, for example named **arcsightbucket2**.

   a)   For **Create a new S3 bucket?**, select **Yes**.

   b)   For **S3 Bucket***, enter a name for the bucket, for example, **arcsightbucket2**.

   c)   Select a **Log file prefix**, such as **arcsight**.

   d)   For **SNS notification for every log file delivery?**, select **Yes**.

   e)   Enter a name for the **SNS Topic (new)***, such as **arcsight**.

   Note the **AWS S3 Region** name in the browser address URL to use later when installing.

Create and Subscribe an SQS Queue

To create a new queue and subscribe the queue to a topic:

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 a name for the queue (for example, **arcsightQueue**) in the **Queue Name** field. Accept or edit the default value settings for the remaining fields.

4   Click **Create Queue**. Your new queue appears in the list of queues.

5   Select the new queue.

     Note the **AWS SQS Region** and **AWS SQS URL** in the browser address URL to use later when installing.

6   Select **Subscribe Queue to SNS Topic** from **Queue Actions**.

7   From the **Choose a Topic** list, select the **arcsight** topic you created in the **Configure CloudTrail** section and click **Subscribe**.

8   In the **Topic Subscription Result** dialog, click **OK**.

AWS Credentials for Connector Configuration

The connector configuration window lets you specify 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, which looks for credentials in the following order, as documented by Amazon.

1   In the environment variables: `AWS_ACCESS_KEY_ID` and `AWS_SECRET_ACCESS_KEY`.

2   In the Java system properties: `aws.accessKeyId` and `aws.secretKey`.

3   In the default credential profiles file. The location of this file varies by platform.

4   In the instance profile credentials, which exist within the instance metadata associated with the IAM role for the EC2 instance.

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:
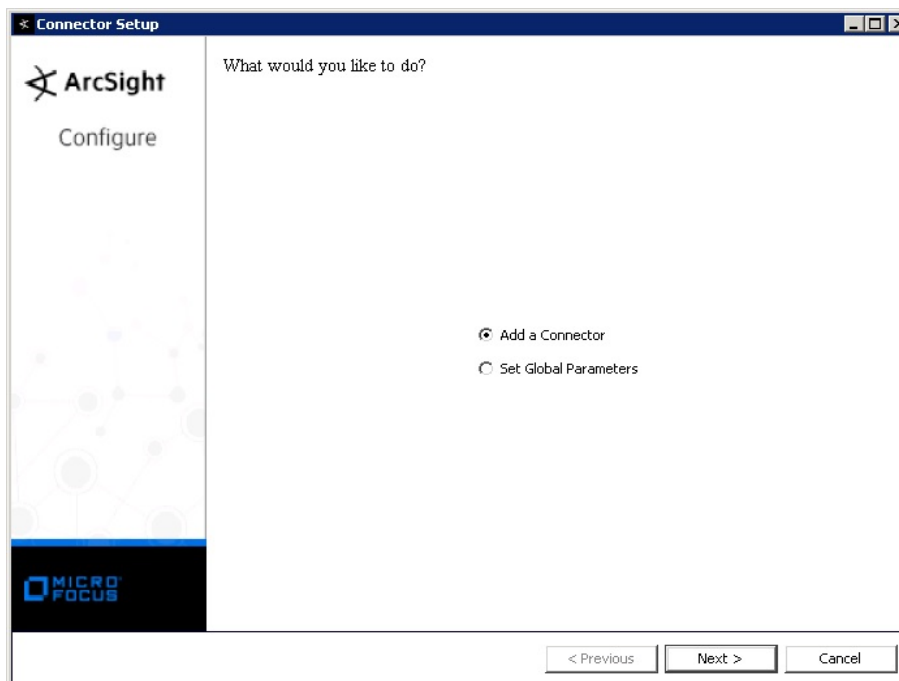
Set Global Parameters (optional)

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.

Parameter	Setting
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 Encrypt	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 CloudTrail** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Proxy Host	Enter the proxy host IP address or name. This value is required for proxy configuration.
Proxy Port	Enter the proxy port. This value is required for proxy configuration.
Proxy User Name	Enter the proxy user name. This value is optional for additional proxy authentication. If you specify a proxy user name, you must also specify 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.
AWS Access Key	Enter the AWS access key. This is optional and will be used if provided. Otherwise the default credential provider chain will be used. See "AWS Credentials for Connector Configuration" for more information.
AWS Secret Key	Enter the AWS secret key. This is optional and will be used if provided. Otherwise the default credential provider chain will be used. See "AWS Credentials for Connector Configuration" for more information.
AWS SQS URL	Enter the SQS URL from which you want to pull the CloudTrail notification.
AWS SQS Region	Enter the SQS region code (for example, us-east-1). You can find the region information in the browser address box of the SQS page.
AWS SQS Visibility Timeout	Enter a time period in seconds during which Amazon SQS prevents other consuming components from receiving and processing that message.
AWS SQS Max Received Count	Enter the maximum retries for an SQS message.
AWS S3 Region	Enter the S3 region code (for example, us-east-1). You can find the region information in the browser address box of the S3 page.

Select a Destination

1 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*.

2 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**.

3 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.

4 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.

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.

Amazon Web Services Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User ID	recipientAccountid
Device Custom Date 1	userIdentity->sessionContext->attributes->creationDate
Device Custom Date 1 Label	'creationDate'
Device Custom Floating Point 1	eventVersion
Device Custom String 1	requestParameters
Device Custom String 2	responseElements
Device Custom String 3	userIdentity->sessionContext->attributes->mfaAuthenticated
Device Domain	awsRegion
Device Event Class ID	Both (eventName, one of (errorCode,('Success', 'Failure'))
Device Payload ID	eventid
Device Product	eventSource
Device Receipt Time	eventTime
Device Vendor	'Amazon'
Event Outcome	one of (errorCode, ('Success', 'Failure'))
File ID	userIdentity->principalid
File Path	userIdentity->arn
File Permission	userIdentity->accessKeyId
File Type	userIdentity->Type
Message	errorMessage
Name	Event Name
Old File Hash	userIdentity->SessionIssuer->AccountId
Old File ID	userIdentity->SessionIssuer->principalId
Old File Name	userIdentity->SessionIssuer->UserName
Old File Path	userIdentity->SessionIssuer->arn
Old File Type	userIdentity->SessionIssuer->Type
Reason	errorCode
Request Client Application	userAgent
Source Address	sourceIPAddress
Source Process Name	userIdentity->invokedBy
Source User ID	userIdentity->Accountid
Source User Name	UserIdentity->UserName