



Micro Focus Security ArcSight Connectors

SmartConnector for Amazon Web Services CloudTrail

Configuration Guide

March 19, 2020

Configuration Guide

SmartConnector for Amazon Web Services CloudTrail

March 19, 2020

Copyright © 2015 – 2020 Micro Focus or one of its affiliates.

Legal Notices

Micro Focus

The Lawn

22-30 Old Bath Road

Newbury, Berkshire RG14 1QN

UK

<https://www.microfocus.com>.

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:

<https://community.microfocus.com/t5/ArcSight-Product-Documentation/ct-p/productdocs>

Revision History

Date	Description
02/21/2020	Added support for AWS Trusted Advisor.
02/21/2020	Added these new sections in the document: Terms Introduction, Related AWS Services, Understanding Data Collection, and Configuring a Trail in CloudTrail.
01/16/2020	Added support for Amazon Inspector.
01/16/2020	Added support for Amazon WAF and WAF-Regional.
01/16/2020	Added support for SecurityHub.
01/16/2020	Added support for AWS CloudFormation.
06/25/2018	Added support for Amazon GuardDuty. Added properties:amazon_cloudtrail.services.include' and 'amazon_cloudtrail.services.exclude'
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. Common fields for other services are supported but specific fields are not supported at this time.

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.

Terms Introduction

This section helps you understand the definitions of important and standard terms used in this document.

- **Trails:** A trail is a configuration that enables you to deliver CloudTrail events to an Amazon S3 bucket, CloudWatch Logs, and CloudWatch Events. You can use a trail to filter CloudTrail events you want to deliver, encrypt your CloudTrail event log files with an AWS KMS key, and set up Amazon SNS notifications for log file delivery.
- **CloudTrail Events:** An event in CloudTrail is the record of activities in an AWS account. These activities include actions taken by a user, role, or a service that CloudTrail monitors. CloudTrail events provide a history of both API and non-API account activities made through AWS Management Console, AWS SDKs, command line tools, and other AWS services. There are two types of events you can log in CloudTrail: management events and data events. By default, CloudTrail logs management events, but not data events.



Both management events and data events use the same CloudTrail JSON log format.

Related AWS Services

The following services are used in conjunction with CloudTrail Events:

- **CloudTrail:** enables you to capture all AWS API calls made by users and/or services. Whenever an API request is made within your environment AWS CloudTrail can track that

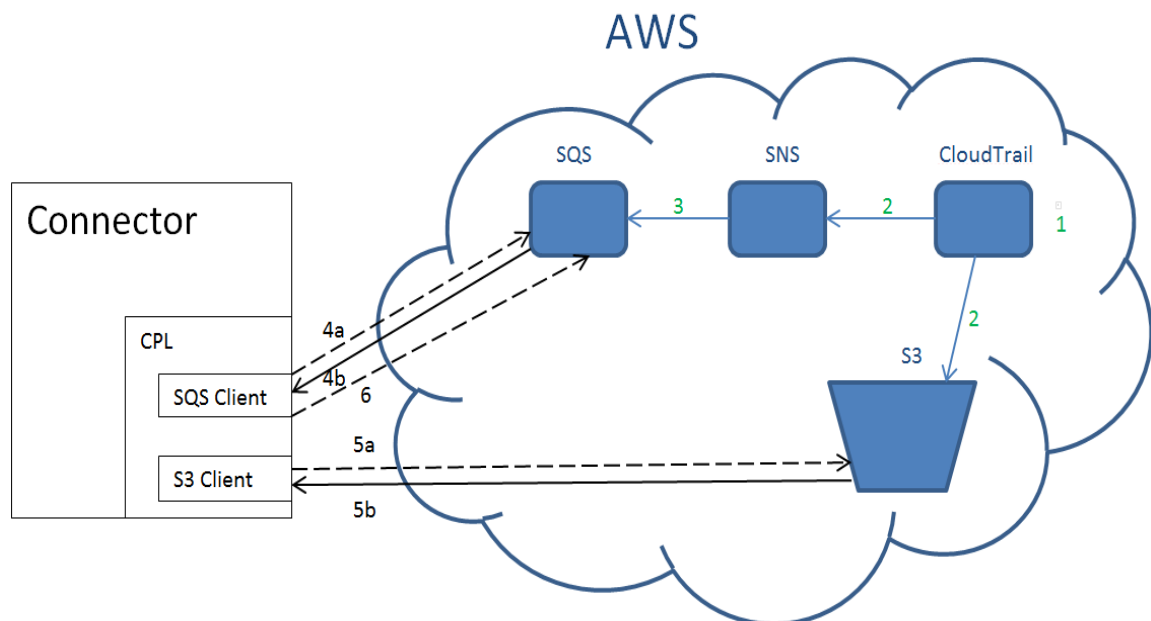
request with a host of metadata, record it in a Log, and then send the same to AWS S3 for storage where you can view the historical data of your API calls.

- **S3 (Amazon Simple Storage Service):** a cloud storage service to store internet data. You must create a bucket in one of the AWS Regions to upload your data (for example: photos, videos, documents, etc.). You can then upload any number of objects to the bucket.
- **SQS (Amazon Simple Queue Service):** a fully managed service that works with serverless systems, microservices, and distributed architectures. It has the capability of sending, storing and receiving messages at scale without dropping message data.
- **SNS (Amazon Simple Notification Service):** When you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon SNS. Using the information collected by CloudTrail, you can determine the request made to Amazon Simple Notification Service (SNS).

when you subscribe an Amazon SQS queue to an Amazon SNS topic, you can publish a message to the topic and Amazon SNS sends an Amazon SQS message to the subscribed queue. The Amazon SQS message contains the subject and message that were published to the topic along with metadata about the message in a JSON document.

Understanding Data Collection

This section provides an overview of the AWS Cloud Trail connector design to understand the data collection flow.



1 - The CloudTrail captures API action and creates a log entry.

2 - The CloudTrail periodically (~5min) dumps a Gzipped JSON log file into the S3 bucket of your choice and sends a notification to the SNS.

3 - The SQS queue receives an SNS notification and queues up an action.

4a and 4b - The connector (through the CPL) pulls the SQS queue and receives an SQS message which has instruction to retrieve the newly delivered CloudTrail log file.

5a and 5b - The connector (through the CPL) pulls the log file from the S3 bucket for parsing.

6 - The connector (through the CPL) deletes an SQS message.

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.

Configure a Trail in CloudTrail

For more information about creating a trail, see Amazon Web Services documentation at: <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-a-trail-using-the-console-first-time.html>

Note:

- Enable **Send SNS notification for every log file delivery**.
- Currently, the connector collects CloudTrails logs for these AWS services: **AWS, SignIn, CloudTrail, EC2, IAM, and KMS**.

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

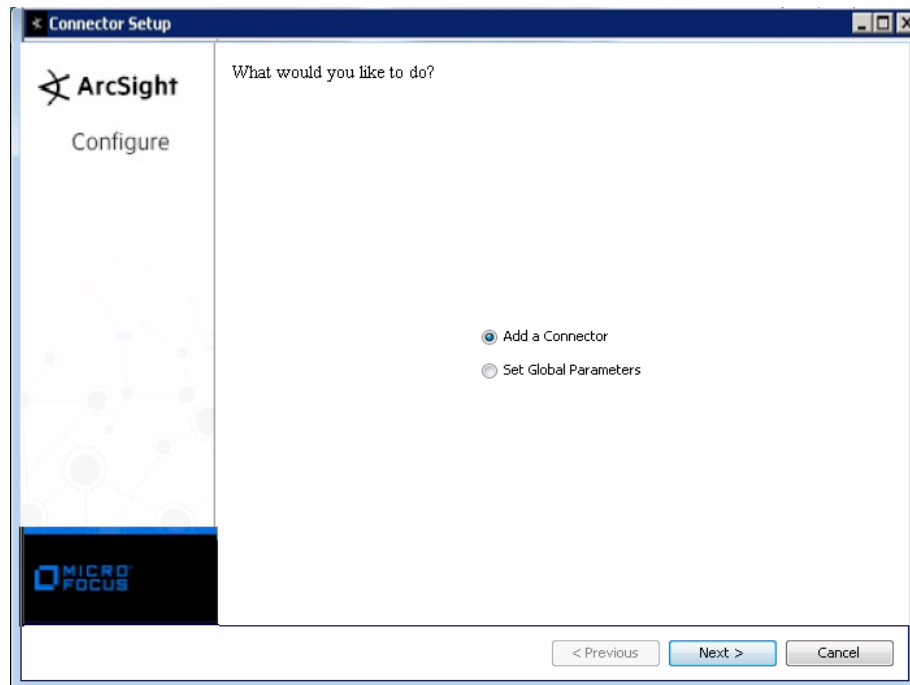
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 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.

Parameter	Setting
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**.

Connector Setup

ArcSight

Configure

Enter the parameter details

Proxy Host

Proxy Port

Proxy User Name

Proxy Password

AWS Access Key

AWS Secret Key

AWS SQS URL

AWS SQS Region

AWS SQS Visibility Timeout 60

AWS SQS Max Received Count 3

AWS S3 Region

< Previous Next > Cancel

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 Floating Point 1	eventVersion

ArcSight ESM Field	Device-Specific Field
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	All of (eventName, One of ('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	eventName
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
Request Method	eventType
Source Address	sourceIPAddress
Source Process Name	userIdentity->invokedBy
Source User ID	userIdentity->Accountid
Source User Name	UserIdentity->UserName

Amazon Web Services Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	additionalEventData
Device Custom String 4	additionalEventData
Device Custom String 5	additionalEventData
Device Custom String 6	additionalEventData
Device Event Class ID	All of (eventName, responseElements)
Event Outcome	responseElements
Old File Permission	All of ('consoleLogin:', responseElements)

CloudFormation Service Common Mappings for SmartConnector 7.14.1

ArcSight ESM Field	Device-Specific Field
--------------------	-----------------------

ArcSight ESM Field	Device-Specific Field
Destination User ID	recipientAccountid
Device Custom Floating Point 1	eventVersion
Device Domain	awsRegion
Device Event Class ID	All of(eventName, One of('!Success','!Failure'))
Device Payload ID	eventid
Device Product	eventSource
Device Vendor	'Amazon'
Event Outcome	One of('Success','Failure')
Message	errorMessage
Name	eventName
Reason	errorCode
Request Client Application	userAgent
Request Cookies	requestID
Request Method	eventType
Source Address	sourceIPAddress

CloudFormation Service CancelUpdateStack Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname

CloudFormation Service CancelUpdateStack Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	notificationarns
deviceCustomString5	parameters
deviceCustomString6	capabilities
fileId	stackId
requestUrl	templateurl

CloudFormation Service DeleteStack Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname

CloudFormation Service DescribeStackDriftDetectionStatus Operation Mappings

ArcSight ESM Field	Device-Specific Field
fileId	stackdriftdetectionId

CloudFormation Service DescribeStackEvents Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname

CloudFormation Service DescribeStackResource Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname

CloudFormation Service DescribeStackResourceDrifts Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname

CloudFormation Service DescribeStackResources Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname

CloudFormation Service DescribeStacks Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname

CloudFormation Service DetectStackDrift Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname
fileId	stackdriftdetectionId

CloudFormation Service DetectStackResourceDrift Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname
sourceUserId	logicalResourceId

CloudFormation Service EstimateTemplateCost Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	parameters
deviceCustomString5	templateurl
requestUrl	url

CloudFormation Service GetStackPolicy Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname

CloudFormation Service GetTemplate Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname

CloudFormation Service GetTemplateSummary Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname
deviceCustomString5	parameters
deviceCustomString6	capabilities
message	description
reason	capabilitiesreason

CloudFormation Service ListStackResources Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname

CloudFormation Service ListStacks Operation Mappings

ArcSight ESM Field	Device-Specific Field
requestContext	stackstatusfilter

CloudFormation Service UpdateStack Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	stackname
deviceCustomString5	parameters
deviceCustomString6	capabilities
fileId	notificationarns
oldFileId	useprevioustemplate

CloudFormation Service ValidateTemplate Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	capabilities
deviceCustomString5	parameters

ArcSight ESM Field	Device-Specific Field
deviceCustomString6	templateurl
message	description
reason	capabilitiesreason

SecurityHub Service Common Mappings for SmartConnector 7.14.1

ArcSight ESM Field	Device-Specific Field
Destination User ID	recipientAccountid
Device Custom Floating Point 1	eventVersion
Device Domain	awsRegion
Device Event Class ID	All of(eventName, One of('!Success','!Failure'))
Device Payload ID	eventid
Device Product	eventSource
Device Vendor	'Amazon'
Event Outcome	One of('Success','Failure')
Message	errorMessage
Name	EventName
Reason	errorCode
Request Client Application	userAgent
Request Cookies	RequestID
Request Method	eventType
Source Address	sourceIPAddress

SecurityHub Service AcceptInvitation Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Accept Invitation)
oldFileHash	invitationId
oldFileType	masterId

SecurityHub Service BatchDisableStandards Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Batch Disable Standards)
deviceCustomString3	standardsinput
deviceCustomString5	standardsstatus
deviceCustomString6	standardssubscriptionarn
fileId	standardssubscriptionarns
fileType	standardsarn

SecurityHub Service BatchEnableStandards Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Batch Enable Standards)
deviceCustomString3	standardsinput
deviceCustomString5	standardsstatus
deviceCustomString6	standardssubscriptionarn
fileId	standardssubscriptionrequests
fileType	standardsarn

SecurityHub Service CreateInsight Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Create Insight)
deviceCustomString3	groupbyattribute
deviceCustomString5	insightarn
deviceCustomString6	name
requestContext	filters

SecurityHub Service CreateMembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Create Members)
deviceCustomString3	accountdetails
reason	result
sourceUserId	accountId

SecurityHub Service DeclineInvitations Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Decline Invitations)
deviceCustomString3	accountIds
deviceCustomString5	unprocessedAccounts
sourceUserId	accountIds
sourceUserName	unprocessedAccounts

SecurityHub Service DeleteInsight Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action>Delete Insight)
deviceCustomString3	requestinsightarn
deviceCustomString5	responseinsightarn

SecurityHub Service DeleteInvitations Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Delete Invitations)
deviceCustomString3	accountIds
deviceCustomString5	unprocessedAccounts
sourceUserId	accountIds
sourceUserName	unprocessedAccounts

SecurityHub Service DeleteMembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Delete Members)
deviceCustomString3	accountIds
deviceCustomString5	unprocessedAccounts
sourceUserId	accountIds
sourceUserName	unprocessedAccounts

SecurityHub Service DescribeActionTargets Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Describe Action Targets)
deviceCustomString3	actiontargetarns
deviceCustomString5	actiontargets

SecurityHub Service DisableSecurityHub Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Disable Security Hub)

SecurityHub Service DisassociateFromMasterAccount Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Disassociate From Master Account)

SecurityHub Service DisassociateMembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Disassociate Members)
deviceCustomString3	accountIds
deviceCustomString5	unprocessedAccounts
sourceUserId	accountIds
sourceUserName	unprocessedAccounts

SecurityHub Service EnableSecurityHub Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Enable Security Hub)

SecurityHub Service GetEnabledStandards Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Get Enabled Standards)
deviceCustomString3	standardsinput
deviceCustomString5	standardsstatus
deviceCustomString6	standardssubscriptionarn
fileId	standardssubscriptionarns
fileType	standardsarn

SecurityHub Service GetFindings Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Get Findings)
deviceCustomNumber1	maxresults
deviceCustomString3	sortcriteria
deviceCustomString6	findings
requestContext	filters

SecurityHub Service GetInsightResults Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Get Insight Results)
deviceCustomString3	insightarn
deviceCustomString6	insightresults

SecurityHub Service GetInsights Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Get Insights)
deviceCustomNumber1	maxresults
deviceCustomString3	insightarns
deviceCustomString6	insights

SecurityHub Service GetInvitationsCount Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Get Invitations Count)

ArcSight ESM Field	Device-Specific Field
deviceCustomNumber1	invitationsCount

SecurityHub Service GetMasterAccount Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Get Master Account)

SecurityHub Service GetMembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Get Members)

SecurityHub Service InviteMembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Invite Members)
deviceCustomString3	accountIds
deviceCustomString5	unprocessedAccounts
sourceUserId	accountIds
sourceUserName	unprocessedAccounts

SecurityHub Service ListMembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,List Members)

SecurityHub Service UpdateInsight Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceAction	One of (action,Update Insight)
deviceCustomString3	groupbyattribute
deviceCustomString5	insightarn
deviceCustomString6	name
requestContext	filters

WAF-Regional Associate Web ACL Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,__,stringConstant("Associate Web ACL"),action)
Device Custom String 5	webACLId
Device Custom String 5 Label	"Web ACL ID"
Device Custom String 6	ResourceArn

ArcSight ESM Field	Device-Specific Field
Device Custom String 6 Label	"Resource Arn"

WAF-Regional Create Byte Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Byte Match Set"),action)
Device Custom String 3	byteMatchSet
Device Custom String 3 Label	"Byte Match Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF-Regional Create Geo Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Geo Match Set"),action)
Device Custom String 3	geoMatchSet
Device Custom String 3 Label	"Geo Match Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF-Regional Create IPSet Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	ipSet
Device Action	__ifThenElse(action,___stringConstant("Create IPSet"),action)
Device Custom String 3	ipSet
Device Custom String 3 Label	"IPSet"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF-Regional Create Rate Based Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Rate Based Rule"),action)
Device Custom Number 1	rateLimit
Device Custom Number 1 Label	"Rate Limit"
Device Custom String 3	metricName
Device Custom String 3 Label	"Metric Name"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Old File Hash	rateKey
Old File Name	rule
Old File Path	tags
Request Context	requestName

WAF-Regional Create Regex Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Regex Match Set"),action)
Device Custom String 3	regexMatchSet
Device Custom String 3 Label	"Regex Match Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF-Regional Create Regex Pattern Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Regex Pattern Set"),action)
Device Custom String 3	regexPatternSet
Device Custom String 3 Label	"Regex Pattern Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF-Regional Create Rule Group Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Rule Group"),action)
Device Custom String 3	metricName
Device Custom String 3 Label	"Metric Name"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Old File Name	ruleGroup
Old File Path	tags
Request Context	requestName

WAF-Regional Create Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Rule"),action)
Device Custom String 3	metricName
Device Custom String 3 Label	"Metric Name"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Old File Name	rule
Old File Path	tags
Request Context	requestName

WAF-Regional Create Size Constraint Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Size Constraint Set"),action)
Device Custom String 3	sizeConstraintSet
Device Custom String 3 Label	"Size Constraint Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF-Regional Create Sql Injection Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Sql Injection Match Set"),action)

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	sqlInjectionMatchSet
Device Custom String 3 Label	"Sql Injection Match Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF-Regional Create Web ACL Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Create Web ACL"), action)
Device Custom String 3	metricName
Device Custom String 3 Label	"Metric Name"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Old File Name	webACL
Old File Path	tags
Request Context	requestName

WAF-Regional Create Xss Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Create Xss Match Set"), action)
Device Custom String 3	xssMatchSet
Device Custom String 3 Label	"Xss Match Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF-Regional Delete Byte Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Byte Match Set"), action)
Device Custom String 3	byteMatchSetId
Device Custom String 3 Label	"Byte Match Set ID"
Device Custom String 5	requestChangeToken

ArcSight ESM Field	Device-Specific Field
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Delete Geo Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Geo Match Set"), action)
Device Custom String 3	geoMatchSetId
Device Custom String 3 Label	"Geo Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Delete IPSet Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete IPSet"), action)
Device Custom String 3	ipSetId
Device Custom String 3 Label	"IPSet ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Delete Logging Configuration Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Logging Configuration"), action)
Device Custom String 3	resourceArn
Device Custom String 3 Label	"Resource Arn"

WAF-Regional Delete Permission Policy Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Permission Policy"), action)
Device Custom String 3	resourceArn
Device Custom String 3 Label	"Resource Arn"

WAF-Regional Delete Rate Based Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Rate Based Rule"),action)
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Delete Regex Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Regex Match Set"),action)
Device Custom String 3	regexMatchSetId
Device Custom String 3 Label	"Regex Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Delete Regex Pattern Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Regex Pattern Set"),action)
Device Custom String 3	regexPatternSetId
Device Custom String 3 Label	"Regex Pattern Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Delete Rule Group Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Rule Group"),action)
Device Custom String 3	ruleGroupId
Device Custom String 3 Label	"Rule Group ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken

ArcSight ESM Field	Device-Specific Field
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Delete Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Rule"),action)
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Delete Size Constraint Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Size Constraint Set"),action)
Device Custom String 3	sizeConstraintSetId
Device Custom String 3 Label	"Size Constraint Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Delete Sql Injection Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Sql Injection Match Set"),action)
Device Custom String 3	sqlInjectionMatchSetId
Device Custom String 3 Label	"Sql Injection Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Delete Web ACL Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Web ACL"),action)
Device Custom String 3	webACLId
Device Custom String 3 Label	"Web ACL ID"

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Delete Xss Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Xss Match Set"), action)
Device Custom String 3	xssMatchSetId
Device Custom String 3 Label	"Xss Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Disassociate Web ACL Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Disassociate Web ACL"), action)
Device Custom String 6	resourceArn
Device Custom String 6 Label	"Resource Arn"

WAF-Regional Get Byte Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Byte Match Set"), action)
Device Custom String 5	byteMatchSetId
Device Custom String 5 Label	"Byte Match Set ID"
Device Custom String 6	byteMatchSet
Device Custom String 6 Label	"Byte Match Set"

WAF-Regional Get Change Token Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Change Token"), action)
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Get Change Token Status Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Change Token Status"), action)
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF-Regional Get Geo Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Geo Match Set"), action)
Device Custom String 5	geoMatchSetId
Device Custom String 5 Label	"Geo Match Set ID"
Device Custom String 6	byteMatchSet
Device Custom String 6 Label	"Geo Match Set"

WAF-Regional Get IPSet Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get IPSet"), action)
Device Custom String 5	iPSetId
Device Custom String 5 Label	"IPSet ID"
Device Custom String 6	iPSet
Device Custom String 6 Label	"IPSet"

WAF-Regional Get Logging Configuration Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Logging Configuration"), action)
Device Custom String 5	resourceArn
Device Custom String 5 Label	"Resource Arn"
Device Custom String 6	loggingConfiguration
Device Custom String 6 Label	"Logging Configuration"

WAF-Regional Get Permission Policy Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Permission Policy"), action)
Device Custom String 5	resourceArn
Device Custom String 5 Label	"Resource Arn"
Device Custom String 6	policy

ArcSight ESM Field	Device-Specific Field
Device Custom String 6 Label	"Policy"

WAF-Regional Get Rate Based Rule Managed Keys Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Get Rate Based Rule Managed Keys"),action)
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"
Old File Hash	managedKeys

WAF-Regional Get Rate Based Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Get Rate Based Rule"),action)
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 6	rule
Device Custom String 6 Label	"Rule"

WAF-Regional Get Regex Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Get Regex Match Set"),action)
Device Custom String 5	regexMatchSetId
Device Custom String 5 Label	"Regex Match Set ID"
Device Custom String 6	regexMatchSet
Device Custom String 6 Label	"Regex Match Set"

WAF-Regional Get Regex Pattern Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Get Regex Pattern Set"),action)
Device Custom String 5	regexPatternSetId
Device Custom String 5 Label	"Regex Pattern Set ID"
Device Custom String 6	regexPatternSet
Device Custom String 6 Label	"Regex Pattern Set"

WAF-Regional Get Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Rule"), action)
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 6	rule
Device Custom String 6 Label	"Rule"

WAF-Regional Get Rule Group Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Rule Group"), action)
Device Custom String 5	ruleGroupId
Device Custom String 5 Label	"Rule Group ID"
Device Custom String 6	ruleGroup
Device Custom String 6 Label	"Rule Group"

WAF-Regional Get Sampled Requests Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Sampled Requests"), action)
Device Custom Date 1	requestStartTime
Device Custom Date 1 Label	"Response Start Time"
Device Custom Date 2	requestEndTime
Device Custom Date 2 Label	"Response End Time"
Device Custom Number 1	maxItems
Device Custom Number 1 Label	"Max Items"
Device Custom Number 2	populationSize
Device Custom Number 2 Label	"Population Size"
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 6	webAclId
Device Custom String 6 Label	"Web Acl ID"
End Time	responseEndTime
Request Context	sampledRequests
Start Time	requestStartTime

WAF-Regional Get Size Constraint Set Mappings

ArcSight ESM Field	Device-Specific Field
--------------------	-----------------------

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Size Constraint Set"), action)
Device Custom String 5	sizeConstraintSetId
Device Custom String 5 Label	"Size Constraint Set ID"
Device Custom String 6	sizeConstraintSet
Device Custom String 6 Label	"Size Constraint Set"

WAF-Regional Get Sql Injection Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Sql Injection Match Set"), action)
Device Custom String 5	sqlInjectionMatchSetId
Device Custom String 5 Label	"Sql Injection Match Set ID"
Device Custom String 6	sqlInjectionMatchSet
Device Custom String 6 Label	"Sql Injection Match Set"

WAF-Regional Get Web ACL For Resource Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Web ACL For Resource"), action)
Device Custom String 3	webACLSummary
Device Custom String 3 Label	"Web ACL Summary"
Device Custom String 6	resourceArn
Device Custom String 6 Label	"Resource Arn"

WAF-Regional Get Web ACL Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Web ACL"), action)
Device Custom String 5	webACLId
Device Custom String 5 Label	"Web ACL ID"
Device Custom String 6	webACL
Device Custom String 6 Label	"Web ACL"

WAF-Regional Get Xss Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Xss Match Set"), action)
Device Custom String 5	xssMatchSetId
Device Custom String 5 Label	"Xss Match Set ID"
Device Custom String 6	xssMatchSet

ArcSight ESM Field	Device-Specific Field
Device Custom String 6 Label	"Xss Match Set"

WAF-Regional List Activated Rules In Rule Group Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Activated Rules In Rule Group"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	activatedRules
Device Custom String 3 Label	"Activated Rules"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"
Old File Hash	ruleGroupId

WAF-Regional List Byte Match Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Byte Match Sets"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	byteMatchSets
Device Custom String 3 Label	"Byte Match Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List Geo Match Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Geo Match Sets"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	geoMatchSets
Device Custom String 3 Label	"Geo Match Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List IPSets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List IPSets"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	ipSets
Device Custom String 3 Label	"IPSets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List Logging Configurations Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Logging Configurations"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	loggingConfigurations
Device Custom String 3 Label	"Logging Configurations"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List Rate Based Rules Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Rate Based Rules"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	rules
Device Custom String 3 Label	"Rules"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List Regex Match Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Regex Match Sets"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	regexMatchSets
Device Custom String 3 Label	"Regex Match Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List Regex Pattern Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Regex Pattern Sets"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	regexPatternSets
Device Custom String 3 Label	"Regex Pattern Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List Resources For Web ACL Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Resources For Web ACL"), action)
Device Custom String 3	resourceType
Device Custom String 3 Label	"Resource Type"
Device Custom String 5	webACLId
Device Custom String 5 Label	"Web ACL ID"
Device Custom String 6	resourceArns
Device Custom String 6 Label	"Resource Arns"

WAF-Regional List Rule Groups Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Rule Groups"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	ruleGroups
Device Custom String 3 Label	"Rule Groups"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List Rules Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Rules"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	rules
Device Custom String 3 Label	"Rules"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List Size Constraint Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Size Constraint Sets"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	sizeConstraintSets
Device Custom String 3 Label	"Size Constraint Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List Sql Injection Match Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Sql Injection Match Sets"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	sqlInjectionMatchSets
Device Custom String 3 Label	"Sql Injection Match Sets"

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List Subscribed Rule Groups Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("List Subscribed Rule Groups"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	ruleGroups
Device Custom String 3 Label	"Rule Groups"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List Tags For Resource Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("List Tags For Resource"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	resourceARN
Device Custom String 3 Label	"Resource ARN"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"
Request Context	tagInfoForResource

WAF-Regional List Web ACLs Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("List Web ACLs"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	webACLs
Device Custom String 3 Label	"Web ACLs"
Device Custom String 5	requestNextMarker

ArcSight ESM Field	Device-Specific Field
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional List Xss Match Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Xss Match Sets"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	xssMatchSets
Device Custom String 3 Label	"Xss Match Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF-Regional Put Logging Configuration Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Put Logging Configuration"), action)
Device Custom String 5	requestLoggingConfiguration
Device Custom String 5 Label	"Request Logging Configuration"
Device Custom String 6	responseLoggingConfiguration
Device Custom String 6 Label	"Response Logging Configuration"

WAF-Regional Put Permission Policy Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Put Permission Policy"), action)
Device Custom String 3	resourceArn
Device Custom String 3 Label	"Resource Arn"
Device Custom String 6	policy
Device Custom String 6 Label	"Policy"

WAF-Regional Tag Resource Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Tag Resource"), action)
Device Custom String 3	resourceArn
Device Custom String 3 Label	"Resource Arn"

ArcSight ESM Field	Device-Specific Field
Old File Path	tags

WAF-Regional Untag Resource Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Untag Resource"),action)
Device Custom String 3	resourceArn
Device Custom String 3 Label	"Resource Arn"
Old File Hash	tagKeys

WAF-Regional Update Byte Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Update Byte Match Set"),action)
Device Custom String 3	byteMatchSetId
Device Custom String 3 Label	"Byte Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF-Regional Update Geo Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Update Geo Match Set"),action)
Device Custom String 3	geoMatchSetId
Device Custom String 3 Label	"Geo Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF-Regional Update IPSet Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Update IPSet"),action)
Device Custom String 3	ipSetId
Device Custom String 3 Label	"IPSet ID"
Device Custom String 5	requestChangeToken

ArcSight ESM Field	Device-Specific Field
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF-Regional Update Rate Based Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Rate Based Rule"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF-Regional Update Regex Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Regex Match Set"), action)
Device Custom String 3	regexPatternSetId
Device Custom String 3 Label	"Regex Pattern Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF-Regional Update Regex Pattern Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Regex Pattern Set"), action)
Device Custom String 3	regexMatchSetId
Device Custom String 3 Label	"Regex Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken

ArcSight ESM Field	Device-Specific Field
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF-Regional Update Rule Group Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Rule Group"), action)
Device Custom String 3	ruleGroupId
Device Custom String 3 Label	"Rule Group ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF-Regional Update Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Rule"), action)
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF-Regional Update Size Constraint Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Size Constraint Set"), action)
Device Custom String 3	sizeConstraintSetId
Device Custom String 3 Label	"Size Constraint Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF-Regional Update Sql Injection Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Update Sql Injection Match Set"),action)
Device Custom String 3	sqlInjectionMatchSetId
Device Custom String 3 Label	"Sql Injection Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF-Regional Update Web ACL Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Update Web ACL"),action)
Device Custom String 3	webACLId
Device Custom String 3 Label	"Web ACL ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF-Regional Update Xss Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Update Xss Match Set"),action)
Device Custom String 3	xssMatchSetId
Device Custom String 3 Label	"Xss Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Create Byte Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Byte Match Set"),action)
Device Custom String 3	byteMatchSet
Device Custom String 3 Label	"Byte Match Set"
Device Custom String 5	requestChangeToken

ArcSight ESM Field	Device-Specific Field
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF Create Geo Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,__,stringConstant("Create Geo Match Set"),action)
Device Custom String 3	geoMatchSet
Device Custom String 3 Label	"Geo Match Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF Create IPSet Mappings

ArcSight ESM Field	Device-Specific Field
Destination Address	ipSet
Device Action	__ifThenElse(action,__,stringConstant("Create IPSet"),action)
Device Custom String 3	ipSet
Device Custom String 3 Label	"IPSet"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF Create Rate Based Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,__,stringConstant("Create Rate Based Rule"),action)
Device Custom Number 1	rateLimit
Device Custom Number 1 Label	"Rate Limit"
Device Custom String 3	metricName
Device Custom String 3 Label	"Metric Name"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken

ArcSight ESM Field	Device-Specific Field
Device Custom String 6 Label	"Response Change Token"
Old File Hash	rateKey
Old File Name	rule
Old File Path	tags
Request Context	requestName

WAF Create Regex Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Regex Match Set"),action)
Device Custom String 3	regexMatchSet
Device Custom String 3 Label	"Regex Match Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF Create Regex Pattern Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Regex Pattern Set"),action)
Device Custom String 3	regexPatternSet
Device Custom String 3 Label	"Regex Pattern Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF Create Rule Group Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Rule Group"),action)
Device Custom String 3	metricName
Device Custom String 3 Label	"Metric Name"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Old File Name	ruleGroup

ArcSight ESM Field	Device-Specific Field
Old File Path	tags
Request Context	requestName

WAF Create Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Create Rule"), action)
Device Custom String 3	metricName
Device Custom String 3 Label	"Metric Name"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Old File Name	rule
Old File Path	tags
Request Context	requestName

WAF Create Size Constraint Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Create Size Constraint Set"), action)
Device Custom String 3	sizeConstraintSet
Device Custom String 3 Label	"Size Constraint Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF Create Sql Injection Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Create Sql Injection Match Set"), action)
Device Custom String 3	sqlInjectionMatchSet
Device Custom String 3 Label	"Sql Injection Match Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF Create Web ACL Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Web ACL"),action)
Device Custom String 3	metricName
Device Custom String 3 Label	"Metric Name"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Old File Name	webACL
Old File Path	tags
Request Context	requestName

WAF Create Xss Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Create Xss Match Set"),action)
Device Custom String 3	xssMatchSet
Device Custom String 3 Label	"Xss Match Set"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	requestName

WAF Delete Byte Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Byte Match Set"),action)
Device Custom String 3	byteMatchSetId
Device Custom String 3 Label	"Byte Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF Delete Geo Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Geo Match Set"),action)
Device Custom String 3	geoMatchSetId

ArcSight ESM Field	Device-Specific Field
Device Custom String 3 Label	"Geo Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF Delete IPSet Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete IPSet"), action)
Device Custom String 3	ipSetId
Device Custom String 3 Label	"IPSet ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF Delete Logging Configuration Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Logging Configuration"), action)
Device Custom String 3	resourceArn
Device Custom String 3 Label	"Resource Arn"

WAF Delete Permission Policy Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Permission Policy"), action)
Device Custom String 3	resourceArn
Device Custom String 3 Label	"Resource Arn"

WAF Delete Rate Based Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Rate Based Rule"), action)
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken

ArcSight ESM Field	Device-Specific Field
Device Custom String 6 Label	"Response Change Token"

WAF Delete Regex Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Regex Match Set"), action)
Device Custom String 3	regexMatchSetId
Device Custom String 3 Label	"Regex Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF Delete Regex Pattern Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Regex Pattern Set"), action)
Device Custom String 3	regexPatternSetId
Device Custom String 3 Label	"Regex Pattern Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF Delete Rule Group Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Rule Group"), action)
Device Custom String 3	ruleGroupId
Device Custom String 3 Label	"Rule Group ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF Delete Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Rule"), action)
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF Delete Size Constraint Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Size Constraint Set"),action)
Device Custom String 3	sizeConstraintSetId
Device Custom String 3 Label	"Size Constraint Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF Delete Sql Injection Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Sql Injection Match Set"),action)
Device Custom String 3	sqlInjectionMatchSetId
Device Custom String 3 Label	"Sql Injection Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF Delete Web ACL Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Delete Web ACL"),action)
Device Custom String 3	webACLId
Device Custom String 3 Label	"Web ACL ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF Delete Xss Match Set Mappings

ArcSight ESM Field	Device-Specific Field
--------------------	-----------------------

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Xss Match Set"), action)
Device Custom String 3	xssMatchSetId
Device Custom String 3 Label	"Xss Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF Get Byte Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Byte Match Set"), action)
Device Custom String 5	byteMatchSetId
Device Custom String 5 Label	"Byte Match Set ID"
Device Custom String 6	byteMatchSet
Device Custom String 6 Label	"Byte Match Set"

WAF Update Xss Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Xss Match Set"), action)
Device Custom String 3	xssMatchSetId
Device Custom String 3 Label	"Xss Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Update Web ACL Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Web ACL"), action)
Device Custom String 3	webACLId
Device Custom String 3 Label	"Web ACL ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Update Size Constraint Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Size Constraint Set"), action)
Device Custom String 3	sqlInjectionMatchSetId
Device Custom String 3 Label	"Sql Injection Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Update Size Constraint Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Size Constraint Set"), action)
Device Custom String 3	sizeConstraintSetId
Device Custom String 3 Label	"Size Constraint Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Update Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Rule"), action)
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Update Rule Group Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Rule Group"), action)
Device Custom String 3	ruleGroupId
Device Custom String 3 Label	"Rule Group ID"
Device Custom String 5	requestChangeToken

ArcSight ESM Field	Device-Specific Field
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Update Regex Pattern Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Update Regex Pattern Set"),action)
Device Custom String 3	regexMatchSetId
Device Custom String 3 Label	"Regex Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Update Regex Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Update Regex Match Set"),action)
Device Custom String 3	regexPatternSetId
Device Custom String 3 Label	"Regex Pattern Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Update Rate Based Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Update Rate Based Rule"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken

ArcSight ESM Field	Device-Specific Field
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Update IPSet Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update IPSet"), action)
Device Custom String 3	ipSetId
Device Custom String 3 Label	"IPSet ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Update Geo Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Geo Match Set"), action)
Device Custom String 3	geoMatchSetId
Device Custom String 3 Label	"Geo Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Update Byte Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Byte Match Set"), action)
Device Custom String 3	byteMatchSetId
Device Custom String 3 Label	"Byte Match Set ID"
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"
Request Context	updates

WAF Untag Resource Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Untag Resource"), action)
Device Custom String 3	resourceArn
Device Custom String 3 Label	"Resource Arn"
Old File Hash	tagKeys

WAF Tag Resource Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Tag Resource"), action)
Device Custom String 3	resourceArn
Device Custom String 3 Label	"Resource Arn"
Old File Hash	tags

WAF Put Permission Policy Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Put Permission Policy"), action)
Device Custom String 3	resourceArn
Device Custom String 3 Label	"Resource Arn"
Device Custom String 6	policy
Device Custom String 6 Label	"Policy"

WAF Put Logging Configuration Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Put Logging Configuration"), action)
Device Custom String 5	requestLoggingConfiguration
Device Custom String 5 Label	"Request Logging Configuration"
Device Custom String 6	responseLoggingConfiguration
Device Custom String 6 Label	"Response Logging Configuration"

WAF List Xss Match Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Xss Match Sets"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	xssMatchSets
Device Custom String 3 Label	"Xss Match Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List Web ACLs Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Web ACLs"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	webACLs
Device Custom String 3 Label	"Web ACLs"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List Tags For Resource Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Tags For Resource"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	resourceARN
Device Custom String 3 Label	"Resource ARN"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"
Request Context	tagInfoForResource

WAF List Subscribed Rule Groups Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Subscribed Rule Groups"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	ruleGroups
Device Custom String 3 Label	"Rule Groups"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker

ArcSight ESM Field	Device-Specific Field
Device Custom String 6 Label	"Response Next Marker"

WAF List Sql Injection Match Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("List Sql Injection Match Sets"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	sqlInjectionMatchSets
Device Custom String 3 Label	"Sql Injection Match Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List Size Constraint Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("List Size Constraint Sets"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	sizeConstraintSets
Device Custom String 3 Label	"Size Constraint Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List Rules Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("List Rules"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	rules
Device Custom String 3 Label	"Rules"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List Rule Groups Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("List Rule Groups"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	ruleGroups
Device Custom String 3 Label	"Rule Groups"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List Regex Pattern Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("List Regex Pattern Sets"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	regexPatternSets
Device Custom String 3 Label	"Regex Pattern Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List Regex Match Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("List Regex Match Sets"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	regexMatchSets
Device Custom String 3 Label	"Regex match Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List Rate Based Rules Mappings

ArcSight ESM Field	Device-Specific Field
--------------------	-----------------------

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,__,stringConstant("List Rate Based Rules"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	rules
Device Custom String 3 Label	"Rules"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List Logging Configurations Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,__,stringConstant("List Logging Configurations"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	loggingConfigurations
Device Custom String 3 Label	"Logging Configurations"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List IPSets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,__,stringConstant("List IPSets"),action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	ipSets
Device Custom String 3 Label	"IPSets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List Geo Match Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,__,stringConstant("List Geo Match Sets"),action)
Device Custom Number 1	limit

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1 Label	"Limit"
Device Custom String 3	geoMatchSets
Device Custom String 3 Label	"Geo Match Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List Byte Match Sets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Byte Match Sets"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	byteMatchSets
Device Custom String 3 Label	"Byte Match Sets"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"

WAF List Activated Rules In Rule Group Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Activated Rules In Rule Group"), action)
Device Custom Number 1	limit
Device Custom Number 1 Label	"Limit"
Device Custom String 3	activatedRules
Device Custom String 3 Label	"Activated Rules"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"
Old File Hash	ruleGroupId

WAF Get Xss Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Xss Match Set"), action)
Device Custom String 5	xssMatchSetId
Device Custom String 5 Label	"Xss Match Set ID"

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	xssMatchSet
Device Custom String 6 Label	"Xss Match Set"

WAF Get Web ACL Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Web ACL"), action)
Device Custom String 5	webACLId
Device Custom String 5 Label	"Web ACL ID"
Device Custom String 6	webACL
Device Custom String 6 Label	"Web ACL"

WAF Get Sql Injection Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Sql Injection Match Set"), action)
Device Custom String 5	sqlInjectionMatchSetId
Device Custom String 5 Label	"Sql Injection Match Set ID"
Device Custom String 6	sqlInjectionMatchSet
Device Custom String 6 Label	"Sql Injection Match Set"

WAF Get Size Constraint Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Size Constraint Set"), action)
Device Custom String 5	sizeConstraintSetId
Device Custom String 5 Label	"Size Constraint Set ID"
Device Custom String 6	sizeConstraintSet
Device Custom String 6 Label	"Size Constraint Set"

WAF Get Sampled Requests Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Sampled Requests"), action)
Device Custom Date 1	requestStartTime
Device Custom Date 1 Label	"Response Start Time"
Device Custom Date 2	requestEndTime
Device Custom Date 2 Label	"Response End Time"
Device Custom Number 1	maxItems
Device Custom Number 1 Label	"Max Items"

ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	populationSize
Device Custom Number 2 Label	"Population Size"
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 6	webAclId
Device Custom String 6 Label	"Web Acl ID"
End Time	responseEndTime
Request Context	sampledRequests
Start Time	requestStartTime

WAF Get Rule Group Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Rule Group"), action)
Device Custom String 5	ruleGroupId
Device Custom String 5 Label	"Rule Group Id"
Device Custom String 6	ruleGroup
Device Custom String 6 Label	"Rule Group"

WAF Get Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Rule"), action)
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule Id"
Device Custom String 6	rule
Device Custom String 6 Label	"Rule"

WAF Get Regex Pattern Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Regex Pattern Set"), action)
Device Custom String 5	regexPatternSetId
Device Custom String 5 Label	"Regex Pattern Set ID"
Device Custom String 6	regexPatternSet
Device Custom String 6 Label	"Regex Pattern Set"

WAF Get Regex Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Regex Match Set"), action)

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	regexmatchSetId
Device Custom String 5 Label	"Regex Match Set ID"
Device Custom String 6	regexMatchSet
Device Custom String 6 Label	"Regex Match Set"

WAF Get Rate Based Rule Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Rate Based Rule"), action)
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 6	rule
Device Custom String 6 Label	"Rule"

WAF Get Rate Based Rule Managed Keys Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Rate Based Rule Managed Keys"), action)
Device Custom String 3	ruleId
Device Custom String 3 Label	"Rule ID"
Device Custom String 5	requestNextMarker
Device Custom String 5 Label	"Request Next Marker"
Device Custom String 6	responseNextMarker
Device Custom String 6 Label	"Response Next Marker"
Old File Hash	managedKeys

WAF Get Permission Policy Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Permission Policy"), action)
Device Custom String 5	resourceArn
Device Custom String 5 Label	"Resource Arn"
Device Custom String 6	policy
Device Custom String 6 Label	"Policy"

WAF Get Logging Configuration Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Get Logging Configuration"), action)
Device Custom String 5	resourceArn

ArcSight ESM Field	Device-Specific Field
Device Custom String 5 Label	"Resource Arn"
Device Custom String 6	loggingConfiguration
Device Custom String 6 Label	"Logging Configuration"

WAF Get IPSet Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Get IPSet"),action)
Device Custom String 5	iPSetId
Device Custom String 5 Label	"IPSet ID"
Device Custom String 6	iPSet
Device Custom String 6 Label	"IPSet"

WAF Get Geo Match Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Get Geo Match Set"),action)
Device Custom String 5	geoMatchSetId
Device Custom String 5 Label	"Geo Match Set ID"
Device Custom String 6	byteMatchSet
Device Custom String 6 Label	"Geo Match Set"

WAF Get Change Token Status Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Get Change Token Status"),action)
Device Custom String 5	requestChangeToken
Device Custom String 5 Label	"Request Change Token"
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

WAF Get Change Token Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Get Change Token"),action)
Device Custom String 6	responseChangeToken
Device Custom String 6 Label	"Response Change Token"

Inspector Add Attributes To Findings Mappings

ArcSight ESM Field	Device-Specific Field
--------------------	-----------------------

ArcSight ESM Field	Device-Specific Field
Device Action	<code>__ifThenElse(action, __stringConstant("Add Attributes To Findings"), action)</code>
Device Custom String 3	attributes
Device Custom String 3 Label	"Attributes"
Device Custom String 5	failedItems
Device Custom String 5 Label	"Failed Items"
Device Custom String 6	findingArns
Device Custom String 6 Label	"Finding Arns"

Inspector Create Assessment Target Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	<code>__ifThenElse(action, __stringConstant("Create Assessment Target"), action)</code>
Device Custom String 3	assessmentTargetArn
Device Custom String 3 Label	"Assessment Target Arn"
Device Custom String 5	assessmentTargetName
Device Custom String 5 Label	"Assessment Target Name"
Device Custom String 6	resourceGroupArn
Device Custom String 6 Label	"Resource Group Arn"

Inspector Create Assessment Template Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	<code>__ifThenElse(action, __stringConstant("Create Assessment Template"), action)</code>
Device Custom Number 1	durationInSeconds
Device Custom Number 1 Label	"Duration In Seconds"
Device Custom String 3	requestAssessmentTargetArn
Device Custom String 3 Label	"Request Assessment Target Arn"
Device Custom String 5	responseAssessmentTargetName
Device Custom String 5 Label	"Response Assessment Target Arn"
Device Custom String 6	assessmentTemplateName
Device Custom String 6 Label	"Assessment Template Name"
Old File ID	userAttributesForFindings
Request Context	rulesPackageArns

Inspector Create Exclusions Preview Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	<code>__ifThenElse(action, __stringConstant("Create Exclusions Preview"), action)</code>
Device Custom String 5	previewToken
Device Custom String 5 Label	"Preview Token"

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	assessmentTemplateArn
Device Custom String 6 Label	"Assessment Template Arn"

Inspector Create Resource Group Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Create Resource Group"), action)
Device Custom String 5	resourceGroupTags
Device Custom String 5 Label	"Resource Group Tags"
Device Custom String 6	resourceGroupArn
Device Custom String 6 Label	"Resource Group Arn"

Inspector Delete Assessment Run Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Assessment Run"), action)
Device Custom String 5	assessmentRunArn
Device Custom String 5 Label	"Assessment Run Arn"

Inspector Delete Assessment Target Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Assessment Target"), action)
Device Custom String 6	assessmentTargetArn
Device Custom String 6 Label	"Assessment Target Arn"

Inspector Delete Assessment Template Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Delete Assessment Template"), action)
Device Custom String 5	assessmentTemplateArn
Device Custom String 5 Label	"Assessment Template Arn"

Inspector Describe Assessment Runs Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Describe Assessment Runs"), action)
Device Custom String 3	assessmentRuns
Device Custom String 3 Label	"Assessment Runs"

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	failedItems
Device Custom String 5 Label	"Failed Items"
Device Custom String 6	assessmentRunArns
Device Custom String 6 Label	"Assessment Run Arns"

Inspector Describe Assessment Targets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Describe Assessment Targets"),action)
Device Custom String 3	assessmentTargets
Device Custom String 3 Label	"Assessment Targets"
Device Custom String 5	failedItems
Device Custom String 5 Label	"Failed Items"
Device Custom String 6	assessmentTargetArns
Device Custom String 6 Label	"Assessment Target Arns"

Inspector Describe Assessment Templates Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Describe Assessment Templates"),action)
Device Custom String 3	assessmentTemplates
Device Custom String 3 Label	"Assessment Templates"
Device Custom String 5	failedItems
Device Custom String 5 Label	"Failed Items"
Device Custom String 6	assessmentTemplateArns
Device Custom String 6 Label	"Assessment Template Arns"

Inspector Describe Cross Account Access Role Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Describe Cross Account Access Role"),action)
Device Custom Date 1	registeredAt
Device Custom Date 1 Label	"Registered Time"
Device Custom String 3	valid
Device Custom String 3 Label	"valid"
Device Custom String 5	roleArn
Device Custom String 5 Label	"Role Arn"

Inspector Describe Exclusions Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Describe Exclusions"), action)
Device Custom String 3	exclusions
Device Custom String 3 Label	"Exclusions"
Device Custom String 5	failedItems
Device Custom String 5 Label	"Failed Items"
Device Custom String 6	exclusionArns
Device Custom String 6 Label	"Exclusion Arns"

Inspector Describe Findings Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Describe Findings"), action)
Device Custom String 3	findings
Device Custom String 3 Label	"Findings"
Device Custom String 5	failedItems
Device Custom String 5 Label	"Failed Items"
Device Custom String 6	findingArns
Device Custom String 6 Label	"Finding Arns"

Inspector Describe Resource Groups Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Describe Resource Groups"), action)
Device Custom String 3	resourceGroups
Device Custom String 3 Label	"Resource Groups"
Device Custom String 5	failedItems
Device Custom String 5 Label	"Failed Items"
Device Custom String 6	resourceGroupArns
Device Custom String 6 Label	"Resource Group Arns"

Inspector Describe Rules Packages Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Describe Rules Packages"), action)
Device Custom String 3	rulesPackages
Device Custom String 3 Label	"Rules Packages"
Device Custom String 5	failedItems
Device Custom String 5 Label	"Failed Items"
Device Custom String 6	rulesPackageArns
Device Custom String 6 Label	"Rules Package Arns"

Inspector Get Assessment Report Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Get Assessment Report"),action)
Device Custom String 5	assessmentRunArn
Device Custom String 5 Label	"Assessment Run Arn"
Event Outcome	status
Old File Name	reportType
Old File Type	reportFileFormat
Request Url	Url

Inspector Get Exclusions Preview Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Get Exclusions Preview"),action)
Device Custom Number 1	maxResults
Device Custom Number 1 Label	"Max Results"
Device Custom String 3	previewToken
Device Custom String 3 Label	"Preview Token"
Device Custom String 5	assessmentTemplateArn
Device Custom String 5 Label	"Assessment Template Arn"
Device Custom String 6	exclusionPreviews
Device Custom String 6 Label	"Exclusion Previews"
Event Outcome	previewStatus
Old File Name	responseNextToken
Old File Type	requestNextToken

Inspector Get Telemetry Metadata Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("Get Telemetry Metadata"),action)
Device Custom String 5	assessmentRunArn
Device Custom String 5 Label	"Assessment Run Arn"
Device Custom String 6	telemetryMetadata
Device Custom String 6 Label	"Telemetry Metadata"

Inspector List Assessment Run Agents Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,___stringConstant("List Assessment Run Agents"),action)
Device Custom Number 1	maxResults

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1 Label	"Max Results"
Device Custom String 5	assessmentRunArn
Device Custom String 5 Label	"Assessment Run Arn"
Device Custom String 6	assessmentRunAgents
Device Custom String 6 Label	"Assessment Run Agents"
Old File Name	responseNextToken
Old File Type	requestNextToken
Request Context	Filter

Inspector List Assessment Runs Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Assessment Runs"), action)
Device Custom Number 1	maxResults
Device Custom Number 1 Label	"Max Results"
Device Custom String 5	assessmentRunArns
Device Custom String 5 Label	"Assessment Run Arns"
Device Custom String 6	assessmentTemplateArns
Device Custom String 6 Label	"Assessment Template Arns"
Old File Name	responseNextToken
Old File Type	requestNextToken
Request Context	Filter

Inspector List Assessment Targets Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Assessment Targets"), action)
Device Custom Number 1	maxResults
Device Custom Number 1 Label	"Max Results"
Device Custom String 6	assessmentTargetArns
Device Custom String 6 Label	"Assessment Target Arns"
Old File Name	responseNextToken
Old File Type	requestNextToken
Request Context	Filter

Inspector List Assessment Templates Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Assessment Templates"), action)
Device Custom Number 1	maxResults

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1 Label	"Max Results"
Device Custom String 6	assessmentTargetArns
Device Custom String 6 Label	"Assessment Target Arns"
Old File Name	responseNextToken
Old File Type	requestNextToken
Request Context	Filter

Inspector List Event Subscriptions Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,__stringConstant("List Event Subscriptions"),action)
Device Custom Number 1	maxResults
Device Custom Number 1 Label	"Max Results"
Device Custom String 5	subscriptions
Device Custom String 5 Label	"Subscriptions"
Device Custom String 6	resourceArn
Device Custom String 6 Label	"Resource Arn"
Old File Name	responseNextToken
Old File Type	requestNextToken

Inspector List Exclusions Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,__stringConstant("List Exclusions"),action)
Device Custom Number 1	maxResults
Device Custom Number 1 Label	"Max Results"
Device Custom String 5	exclusionArns
Device Custom String 5 Label	"Exclusion Arns"
Device Custom String 6	assessmentRunArn
Device Custom String 6 Label	"Assessment Run Arn"
Old File Name	responseNextToken
Old File Type	requestNextToken

Inspector List Findings Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,__stringConstant("List Findings"),action)
Device Custom Number 1	maxResults
Device Custom Number 1 Label	"Max Results"
Device Custom String 5	findingArns
Device Custom String 5 Label	"Finding Arns"
Device Custom String 6	assessmentRunArns

ArcSight ESM Field	Device-Specific Field
Device Custom String 6 Label	"Assessment Run Arns"
Old File Name	responseNextToken
Old File Type	requestNextToken
Request Context	filter

Inspector List Rules Packages Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Rules Packages"), action)
Device Custom Number 1	maxResults
Device Custom Number 1 Label	"Max Results"
Device Custom String 6	rulesPackageArns
Device Custom String 6 Label	"Rules Package Arns"
Old File Name	responseNextToken
Old File Type	requestNextToken

Inspector List Tags For Resource Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("List Tags For Resource"), action)
Device Custom String 5	tags
Device Custom String 5 Label	"Tags"
Device Custom String 6	resourceArn
Device Custom String 6 Label	"Resource Arn"

Inspector Preview Agents Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Preview Agents"), action)
Device Custom Number 1	maxResults
Device Custom Number 1 Label	"Max Results"
Device Custom String 5	agentPreviews
Device Custom String 5 Label	"Agent Previews"
Device Custom String 6	previewAgentsArn
Device Custom String 6 Label	"Preview Agents Arn"
Old File Name	responseNextToken
Old File Type	requestNextToken

Inspector Register Cross Account Access Role Mappings

ArcSight ESM Field	Device-Specific Field
--------------------	-----------------------

ArcSight ESM Field	Device-Specific Field
Device Action	<code>__ifThenElse(action, __stringConstant("Register Cross Account Access Role"), action)</code>
Device Custom String 6	<code>roleArn</code>
Device Custom String 6 Label	<code>"Role Arn"</code>

Inspector Remove Attributes From Findings Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	<code>__ifThenElse(action, __stringConstant("Remove Attributes From Findings"), action)</code>
Device Custom String 3	<code>findingArns</code>
Device Custom String 3 Label	<code>"Finding Arns"</code>
Device Custom String 5	<code>failedItems</code>
Device Custom String 5 Label	<code>"Failed Items"</code>
Device Custom String 6	<code>attributeKeys</code>
Device Custom String 6 Label	<code>"Attribute Keys"</code>

Inspector Set Tags For Resource Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	<code>__ifThenElse(action, __stringConstant("Set Tags For Resource"), action)</code>
Device Custom String 5	<code>tags</code>
Device Custom String 5 Label	<code>"Tags"</code>
Device Custom String 6	<code>resourceArn</code>
Device Custom String 6 Label	<code>"Resource Arn"</code>

Inspector Start Assessment Run Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	<code>__ifThenElse(action, __stringConstant("Start Assessment Run"), action)</code>
Device Custom String 3	<code>assessmentTemplateArn</code>
Device Custom String 3 Label	<code>"Assessment Template Arn"</code>
Device Custom String 5	<code>assessmentRunName</code>
Device Custom String 5 Label	<code>"Assessment Run Name"</code>
Device Custom String 6	<code>assessmentRunArn</code>
Device Custom String 6 Label	<code>"Assessment Run Arn"</code>

Inspector Stop Assessment Run Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	<code>__ifThenElse(action, __stringConstant("Stop Assessment Run"), action)</code>

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	assessmentRunArn
Device Custom String 6 Label	"Assessment Run Arn"
Event Outcome	stopAction

Inspector Subscribe To Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Subscribe To Event"), action)
Device Custom String 3	event
Device Custom String 3 Label	"Event"
Device Custom String 5	resourceArn
Device Custom String 5 Label	"Resource Arn"
Device Custom String 6	topicArn
Device Custom String 6 Label	"Topic Arn"

Inspector Unsubscribe From Event Mappings

ArcSight ESM Field	Device-Specific Field
Device Action __ifThenElse(action, __stringConstant("Unsubscribe To Event"), action)	A
Device Custom String 3	event
Device Custom String 3 Label	"Event"
Device Custom String 5	resourceArn
Device Custom String 5 Label	"Resource Arn"
Device Custom String 6	topicArn
Device Custom String 6 Label	"Topic Arn"

Inspector Update Assessment Target Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action, __stringConstant("Update Assessment Target"), action)
Device Custom String 3	assessmentTargetArn
Device Custom String 3 Label	"Assessment Target Arn"
Device Custom String 5	resourceGroupArn
Device Custom String 5 Label	"Resource Group Arn"
Device Custom String 6	assessmentTargetName
Device Custom String 6 Label	"Assessment Target Name"

Simple Cloud Storage Service (S3) Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	requestParameters

ArcSight ESM Field	Device-Specific Field
Destination User ID	resources->accountId
Destination User Privileges	requestParameters
Device Custom String 4	additionalEventData
Device Custom String 5	requestParameters
Device Custom String 6	requestParameters
File Hash	All of('encoding-type:', requestParameters)
File Name	resources->arn
File Path	requestParameters
Old File Permission	resources->type
Request Context	All of('SSEApplied:', additionalEventData)
Request Cookies	RequestId

Amazon Identity and Access Management Service (IAM) Mappings

ArcSight ESM Field	Device-Specific Field
Destination User Name	requestParameters
File Path	requestParameters
Request Cookies	RequestId

Key Management Service (KMS) Mappings

ArcSight ESM Field	Device-Specific Field
Destination Custom Number 1	requestParameters
Request Cookies	RequestId

Elastic Compute Cloud Service (EC2) Mappings

ArcSight ESM Field	Device-Specific Field
Request Cookies	RequestId

GuardDuty Service Common Mappings for SmartConnector 7.9.0

ArcSight ESM Field	Device-Specific Field
Destination User ID	recipientAccountid
Device Custom Floating Point 1	eventVersion
Device Domain	awsRegion
Device Event Class ID	All of(eventName, One of('!Success','!Failure'))
Device Payload ID	eventid
Device Product	eventSource
Device Vendor	'Amazon'
Event Outcome	One of('Success','Failure')
Message	errorMessage

ArcSight ESM Field	Device-Specific Field
Name	EventName
Reason	errorCode
Request Client Application	userAgent
Request Cookies	RequestID
Request Method	eventType
Source Address	sourceIPAddress

GuardDuty Service Acceptinvitation Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
Old File Hash	invitationId
Old File ID	detectorId
Old File Type	masterId

GuardDuty Service Archivefindings Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File ID	detectorId
Request Cookies	findingIds

GuardDuty Service Createdetector Operation Mappings

ArcSight ESM Field	Device-Specific Field
Destination Translated Port	enable
Device Action	action
File Hash	version
Old File ID	detectorId

GuardDuty Service Createipset Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File ID	detectorId
Old File Path	location
Old File Size	activate
Request Client Application	format
Request Url	name
Source Host Name	ipSetId

GuardDuty Service Createmembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
Destination user Name	accountDetails
Device Action	action
File Hash	version
Old File ID	detectorId
Source Host Name	ipSetId

GuardDuty Service Createsamplefindings Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File ID	detectorId
Request Context	findingTypes

GuardDuty Service Createthreatintelset Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File ID	detectorId
Old File Path	location
Old File Size	activate
Request Client Application	format
Request Url	name
Source Service Name	threatIntelSetId

GuardDuty Service Declineinvitations Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Source User Name	unprocessedAccounts
Source User Privileges	accountIds

GuardDuty Service Deletedetector Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version

ArcSight ESM Field	Device-Specific Field
Old File ID	detectorId

GuardDuty Service Deleteinvitations Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Source User Name	unprocessedAccounts
Source User Privileges	accountIds

GuardDuty Service Deleteipset Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File ID	detectorId
Source Host Name	ipSetId

GuardDuty Service Deletemembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File ID	detectorId
Source User Name	unprocessedAccounts
Source User Privileges	accountIds

GuardDuty Service Deletethreatintelset Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File ID	detectorId
Source Service Name	threatIntelSetId

GuardDuty Service Disassociatefrommasteraccount Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File ID	detectorId

GuardDuty Service Disassociatemembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File ID	detectorId
Source User Name	unprocessedAccounts
Source User Privileges	accountIds

GuardDuty Service Getdetector Operation Mappings

ArcSight ESM Field	Device-Specific Field
Destination Dns Domain	serviceRole
Device Action	action
Device Custom Date 2	createdAt
File Hash	version
Old File ID	detectorId
Old File Modification Time	updatedAt
Source Process Name	status

GuardDuty Service Getfindings Operation Mappings

ArcSight ESM Field	Device-Specific Field
Application Protocol	protocol
Bytes In	portProbeAction_blocked
Crypto Signature	remotelp_org
Destination Address	ipAddressV4
Destination Dns Domain	iamInstanceProfile_arn
Destination Host Name	countryCode
Destination NT Domain	One Of(attributeName,countryName)
Destination Port	remotePort
Destination Service Name	remotePortName
Destination Translated Port	archived
Destination User Id	iamInstanceProfile_id
Destination User Name	localPortName
Destination User Privileges	remotelp_cityName
Device Action	actionType
Device Custom Date 1	eventFirstSeen
Device Custom Date 2	eventLastSeen
Device Custom Floating Point 1	confidence
Device Custom Floating Point 2	geoLocation_lat
Device Custom Floating Point 3	geoLocation_lon
Device Custom Floating Point 4	remotelp_lat
Device Custom Number 1	blocked

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	networkInterfaces
Device Custom String 2	productCodes
Device Custom String 3	tags
Device Custom String 4	portProbeDetails
Device Direction	connectionDirection
Device Event Category	organization_asnOrg
Device External Id	id
Device Facility	One Of(title,detectorId)
Device Inbound Interface	resourceRole
Device Outbound Interface	userFeedback
Device Payload Id	remotelp_lon
Device Severity	severity
Event Outcome	organization_org
External Id	remotelp_asnOrg
File Create Time	updatedAt
File Hash	instanceState
File Id	remotelp_countryName
File Name	remotelp_ipAddressV4
File Path	remotelp_asn
File Permission	resourceType
File Type	instanceType
Message	description
Old File Create Time	createdAt
Old File Hash	cityName
Old File Id	One Of(detectorId,accessKeyId)
Old File Name	imageId
Old File Path	partition
Old File Permission	principalId
Old File Type	instanceId
Reason	organization_isp
Request Client Application	type
Request Context	callerType
Request Cookies	findingIds
Request Method	api
Request URL	remotelp_isp
Source Dns Domain	One Of(orderBy,arn,domain)
Source Host Name	platform
Source NT Domain	organization_asn
Source Port	localPort
Source Process Name	availabilityZone
Source Service Name	serviceName
Source User Id	accountId
Source User Name	username

ArcSight ESM Field	Device-Specific Field
Source User Privileges	userType
Start Time	launchTime

GuardDuty Service Getfindingsstatistics Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
File ID	criterion
Old File ID	detectorId
Old File Name	countBySeverity
Request Method	findingStatisticTypes

GuardDuty Service Getinvitationscount Operation Mappings

ArcSight ESM Field	Device-Specific Field
Bytes In	invitationsCount
Device Action	action
File Hash	version

GuardDuty Service Getipset Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File ID	detectorId
Old File Path	location
Request Client Application	format
Request URL	name
Source Host Name	ipSetId
Source Process Name	status

GuardDuty Service Getmembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File ID	detectorId
Source Dns Domain	members
Source User Name	unprocessedAccounts
Source User Privileges	accountIds

GuardDuty Service Getthreatintelset Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File ID	detectorId
Old File Path	location
Request Client Application	format
Request URL	name
Source Process Name	status
Source Service Name	threatIntelSetId

GuardDuty Service Invitemembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Message	message
Old File Id	detectorId
Source User Name	unprocessedAccounts
Source User Privileges	accountIds

GuardDuty Service Listdetectors Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File Name	detectorIds

GuardDuty Service Listfindings Operation Mappings

ArcSight ESM Field	Device-Specific Field
Destination NT Domain	attributeName
Device Action	action
File Id	criterion
Old File Name	detectorId
Request Cookies	findingIds
Source Dns Domain	orderBy

GuardDuty Service Listinvitations Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
Device Event Category	invitations

ArcSight ESM Field	Device-Specific Field
File Hash	version

GuardDuty Service Listipsets Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File Id	detectorId
Source User Id	threatIntelSetIds

GuardDuty Service Listmembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	onlyAssociated
File Id	version
Old FileId	detectorId
Source Dns Domain	members

GuardDuty Service Listthreatintelsets Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File Id	detectorId
Source User Id	threatIntelSetIds

GuardDuty Service Startmonitoringmembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File Id	detectorId
Source User Name	unprocessedAccounts
Source User Privileges	accountIds

GuardDuty Service Stopmonitoringmembers Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File Id	detectorId

ArcSight ESM Field	Device-Specific Field
Source User Name	unprocessedAccounts
Source User Privileges	accountIds

GuardDuty Service Unarchivefindings Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File Id	detectorId
Request Cookies	findingIds

GuardDuty Service Updatedetector Operation Mappings

ArcSight ESM Field	Device-Specific Field
Destination Translated Port	enable
Device Action	action
File Hash	version
Old File Id	detectorId

GuardDuty Service Updatefindingsfeedback Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
Device Facility	comments
File Hash	version
Old File Id	detectorId
Reason	feedback
Request Cookies	findingIds

GuardDuty Service Updateipset Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File Id	detectorId
Old File Path	location
Old File Size	activate
Request Url	name
Source Host Name	ipSetId

GuardDuty Service Updatethreatintelset Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	action
File Hash	version
Old File Id	detectorId
Old File Path	location
Old File Size	activate
Request Url	name
Source Service Name	threatIntelSetId

GuardDuty Service Unsupported Operation Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	requestParameters
Device Custom String 2	responseElements

Trusted Advisor Add Attachments To Set Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Add Attachments to Set"
Device Custom Date 1	expiryTime
Device Custom Date 1 Label	"Expiry Time"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 3	attachments
Device Custom String 3 Label	"Attachments"
File ID	attachmentSetId

Trusted Advisor Add Communication To Case Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Add Communication to Case"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 3	result
Device Custom String 3 Label	"Result"
Device Custom String 5	ccEmailAddresses
Device Custom String 5 Label	"Cc Email Address"
Device Custom String 6	communicationBody
Device Custom String 6 Label	"Communication Body"

ArcSight ESM Field	Device-Specific Field
File ID	attachmentSetId
Old File ID	caseld

Trusted Advisor Create Case Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Create Case"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 3	language
Device Custom String 3 Label	"Language"
Device Custom String 5	ccEmailAddresses
Device Custom String 5 Label	"Cc Email Address"
Device Custom String 6	communicationBody
Device Custom String 6 Label	"Communication Body"
Device Severity	severityCode
File ID	attachmentSetId
File Type	issueType
Old File Id	caseld
Old File Type	"Category Code: "categoryCode
Request Context	subject
Source Service Name	serviceCode

Trusted Advisor Describe Attachment Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Describe Attachment"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 3	data
Device Custom String 3 Label	"Data"
File ID	attachmentId
File Name	fileName

Trusted Advisor Describe Cases Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__stringConstant("Describe Cases")

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	afterTime
Device Custom Date 1 Label	"After Time"
Device Custom Date 2	beforeTime
Device Custom Date 2 Label	"Before Time"
Device Custom Number 1 Label	__ifThenElse(maxResults,,"Max Results")
Device Custom Number 1	maxResults
Device Custom String 1	requestParameters
Device Custom String 1 Label	__stringConstant("Request Parameters")
Device Custom String 2	responseElements
Device Custom String 2 Label	__stringConstant("Response Elements")
Device Custom String 3	language
Device Custom String 3 Label	__ifThenElse(language,,"Language")
Device Custom String 5	nextToken
Device Custom String 5 Label	__ifThenElse(nextToken,,"Next Token")
Device Custom String 6	cases
Device Custom String 6 Label	__ifThenElse(cases,,"Cases")
File ID	"Display ID: "displayId
File Type	"Include Communications: "includeCommunications
Old File ID	caseIdList
Old File Type	"Include Resolved Cases: "includeResolvedCases

Trusted Advisor Describe Communications Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Describe Communications"
Device Custom Date 1	afterTime
Device Custom Date 1 Label	"After Time"
Device Custom Date 2	beforeTime
Device Custom Date 2 Label	"Before Time"
Device Custom Number 1	maxResults
Device Custom Number 1 Label	"Max Results"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 5	nextToken
Device Custom String 5 Label	"Next Token"
Device Custom String 6	communications
Device Custom String 6 Label	"Communications"
Old File ID	caseId

Trusted Advisor Describe Services Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Describe Services"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 3	language
Device Custom String 3 Label	"Language"
Device Custom String 5	serviceCodeList
Device Custom String 5 Label	"Service Code List"
Device Custom String 6	services
Device Custom String 6 Label	"Services"

Trusted Advisor Describe Severity Levels Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Describe Severity Levels"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 3	language
Device Custom String 3 Label	"Language"
Device Custom String 5	severityLevels
Device Custom String 5 Label	"Severity Levels"

Trusted Advisor Describe Check Refresh Statuses Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Describe Trusted Advisor Check Refresh Statuses"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 5	statuses
Device Custom String 5 Label	"Statuses"
Device Custom String 6	checkIds
Device Custom String 6 Label	"Check IDs"

Trusted Advisor Describe Check Result Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Describe Trusted Advisor Check Result"

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	timestamp
Device Custom Date 1 Label	"TimeStamp"
Device Custom Floating Point 2	estimatedMonthlySavings
Device Custom Floating Point 2 Label	"Estimated Monthly Savings"
Device Custom Floating Point 3	estimatedPercentMonthlySavings
Device Custom Floating Point 3 Label	"Estimated Percent Monthly Savings"
Device Custom Floating Point 4	resourcesSuppressed
Device Custom Floating Point 4 Label	"Resources Suppressed"
Device Custom Number 1	resourcesFlagged
Device Custom Number 1 Label	"Resources Flagged"
Device Custom Number 2	resourcesIgnored
Device Custom Number 2 Label	"Resources Ignored"
Device Custom Number 3	resourcesProcessed
Device Custom Number 3 Label	"Resources Processed"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 3	language
Device Custom String 3 Label	"Language"
Device Custom String 5	status
Device Custom String 5 Label	"Status"
Device Custom String 6	checkId
Device Custom String 6 Label	"Check ID"
Old File Type	"Flagged Resources: ",flaggedResources

Trusted Advisor Describe Checks Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Describe Trusted Advisor Checks"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 3	language
Device Custom String 3 Label	"Language"
Device Custom String 5	checks
Device Custom String 5 Label	"Checks"

Trusted Advisor Describe heck Summaries Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Describe Trusted Advisor Check Summaries"

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 5	checkIds
Device Custom String 5 Label	"Check IDs"
Device Custom String 6	summaries
Device Custom String 6 Label	"Summaries"

Trusted Advisor Refresh Check Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Refresh Trusted Advisor Check Mappings"
Device Custom Number 1	millisUntilNextRefreshable
Device Custom Number 1 Label	"Milliseconds Until Next Refreshable"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 5	checkId
Device Custom String 5 Label	"Check ID"
Device Custom String 6	status
Device Custom String 6 Label	"Status"

Trusted Advisor Resolve Case Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Resolve Case"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"Response Elements"
Device Custom String 5	initialCaseStatus
Device Custom String 5 Label	"Initial Case Status"
Device Custom String 6	finalCaseStatus
Device Custom String 6 Label	"Final Case Status"
Old File ID	caseId

Unsupported Services Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Id	recipientAccountId

ArcSight ESM Field	Device-Specific Field
Device Custom Floating Point 1	eventVersion
Device Custom String 1	requestParameters
Device Custom String 2	responseElements
Device Custom String 4	additionalEventData
Device Domain	awsRegion
Device Event Class Id	All of (eventName, One of ('!Success','!Failure'))
Device Payload Id	eventId
Device Product	eventSource
Device Vendor	Amazon
Event Outcome	One of('Success','Failure')
Message	errorMessage
Name	eventName
Reason	errorCode
Request Client Application	userAgent
Request Cookies	requestID
Request Method	eventType
Source Address	sourceIPAddress