Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

SmartConnector for Amazon Web Services CloudTrail

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

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

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

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.

The supported log sources are:

- Cloud Formation
- Guard Duty
- Security Hub
- Lambda Trusted Advisor
- Inspector
- WAF & WAF Regional

Common fields for other services are supported, but specific fields are not supported at this time.

This guide provides a high level overview of ArcSight SmartConnectors for the Cloud.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectorss to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

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.

Note: 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:

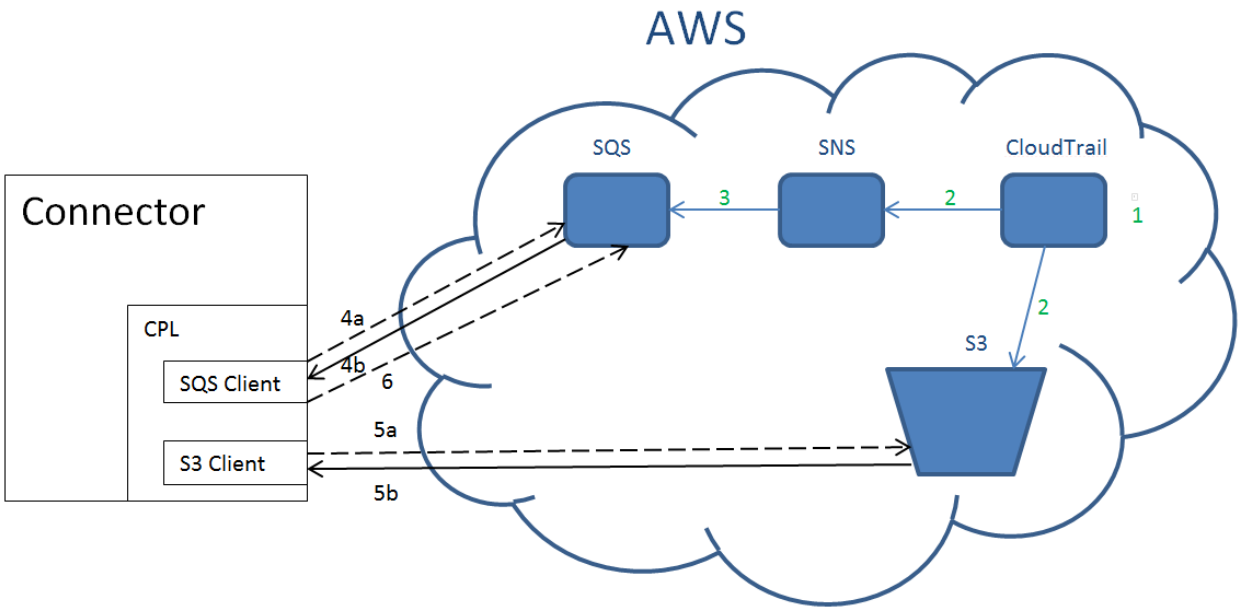
- **CloudTrail:** enables you to capture all AWS API calls made by users and/or services. Whenever an API request is made within your environment AWS CloudTrail can track that request with a host of metadata, record it in a Log, and then send the same to AWS S3 for storage where you can view the historical 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.

Configuring AWS CloudTrail to Retrieve Events

To set up the connector to retrieve events:

1. Set up an AWS account.
2. Create an Identity and Access Management (IAM) user or role.
3. Configure CloudTrail to create an S3 bucket and an SNS topic.

   Note: S3 buckets can be encrypted or non-encrypted.
4. Create an SQS queue for the connector to poll and subscribe the queue to the SNS topic.

Setting up an AWS Account and Creating a Group with Users Added

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

1. Log in to the Amazon Web Services account.
2. Click **Launch Management Console** from the Welcome to Amazon Web Services window.
3. From the Amazon Web Services menu, click **Administration & Security** > **Identity & Access Management**.
4. Under **Dashboard** on the left side of the console window, select **Groups**.
5. Click the **Create New Group** tab to create a new group with permissions to access the CloudTrail logs through API, and then enter a **Group Name** (For example: arcsightgroup).
6. Click **Next Step** to attach two policies to the group.
7. Select the check boxes for **AmazonS3ReadOnlyAccess** and **AmazonSQSFullAccess** policies to the **arcsightgroup**. This enables the connector to download logs.
8. Click **Next Step**, 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 **Generate an access key for each user** check box is selected. 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. You must download the **Access Key ID** and **Secret Access Key** now. You will use these when installing the connector.
12. Click **Close** to return to the **Dashboard**.
13. Select **Groups** under **Dashboard**, then click **arcsightgroup** you created in step 5.
14. Click **Add Users to Group**.
15. Select the check box next to the users you created in step 10 and click **Add Users**.

Configuring CloudTrail

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

To configure CloudTrail:

1. In the console, from the **Administration & Security**menu, select the **CloudTrail** icon.
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**.
   f. Note the **AWS S3 Region** name in the browser address URL to use later when installing.

Creating a Trail in CloudTrail

For information about creating a trail, see Amazon Web Services documentation.

Note:

- Enable **Send SNS notification for every log file delivery**.
- Currently, the connector collects CloudTrails logs for these AWS services: Cloud Formation, Guard Duty, Security Hub, Lambda Trusted Advisor, Inspector, and WAF & WAF Regional

Creating and Subscribing an SQS Queue

To create an SQS 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**. The **Create New Queue** dialog box is displayed.
3. In the **Queue Name** field, enter a name of the queue (For example: **arcsightQueue**). 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 queue you created.
6. Note the **AWS SQS Region** and **AWS SQS URL** in the browser address URL to use later when installing.
7. Select **Subscribe Queue to SNS Topic** from **Queue Actions**.
8. From the **Choose a Topic** list, select the **arcsight** topic you created in the **Configure CloudTrail** section and click **Subscribe**.
9. In the **Topic Subscription Result** dialog, click **OK**.

Specifying AWS Credentials to Configure the Connector

The connector configuration window allows you to 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 that 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.

Installing the SmartConnector

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

Preparing to Install Connector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on ArcSight Documentation for instructions.

Before installing the SmartConnector, ensure that you have the following:

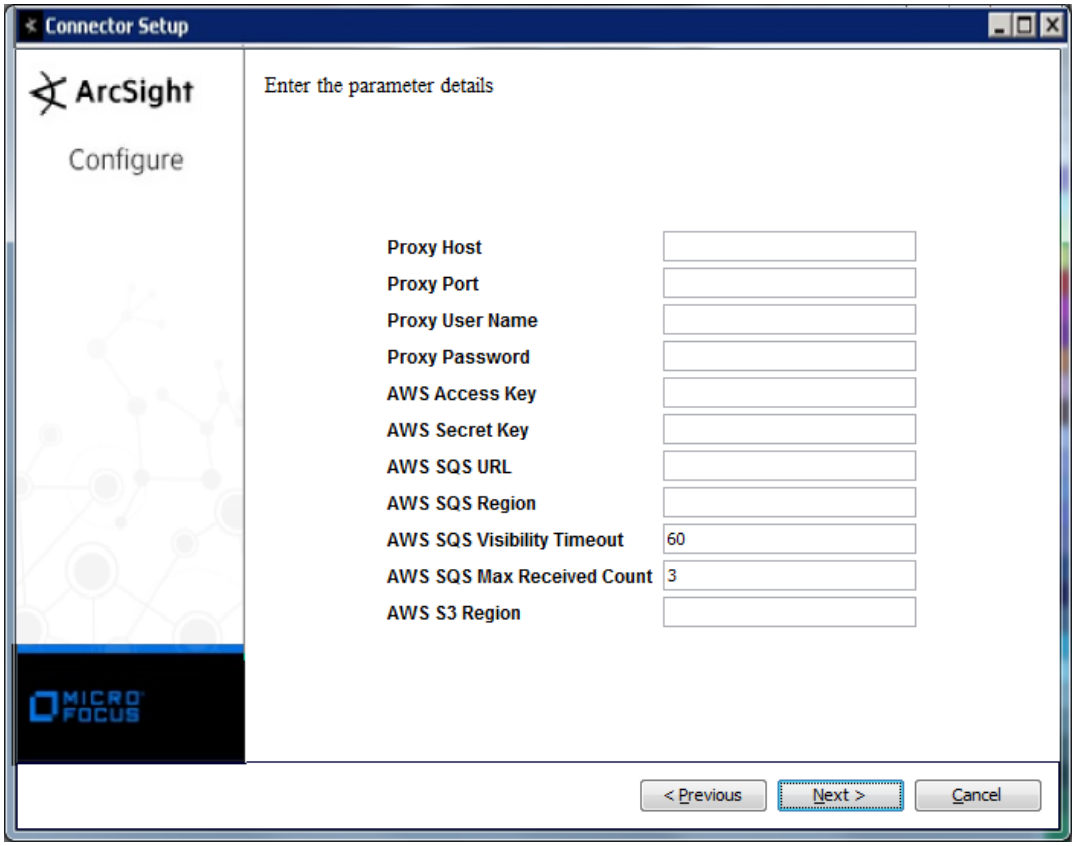
- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the AWS CloudTrail connector. For detailed installation steps or for manual installation steps, see SmartConnector Installation and User Guide.

To install and configure the AWS CloudTrail connector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant Global Parameters, when prompted.
4. From the **Type** drop-down list, select **Amazon Web Services CloudTrail** as the type of connector, then click **Next**.
5. Enter the parameter details, then click **Next**:



Parameters	Description
Avro File Storage Path	The path to the location where the Avro files will be stored.
File Rotation Interval (Sec)	The desired file rotation interval, in seconds. The default value is 3,600 seconds (one hour). The maximum value is 36000 seconds (10 hour).
Number of Events in a File	The number of events that can be stored in each Avro file. The maximum number is 10000.
Proxy Host	If proxy is enabled for your machine, the IP address or host name of the proxy server for HTTPS connection.
Proxy Port	If proxy is enabled for your machine, the port number of the proxy server for HTTPS connection.
Proxy User Name	If proxy is enabled for your machine, the user name for the proxy server. This value is optional for additional proxy authentication. If you enter the proxy user name, you must provide the proxy password.
Proxy Password	If proxy is enabled for your machine, the password for the proxy server user.
Amazon Access Key	The access key that is used to access Amazon S3.
Amazon Secret Key	The secret key that is used to access Amazon S3.

Parameters	Description
Amazon S3 Bucket Name	The name of Amazon S3 bucket that is created on the Amazon account to which the Avro output files will be sent.
Amazon S3 Bucket Folder Name	The name of the folder in the Amazon S3 bucket. This is an optional field. **Note**: If the folder is not present in the Amazon S3 bucket, then it will be automatically created with the name specified in this field.
Amazon S3 Region Code	The Amazon S3 region code in which the Amazon S3 bucket was created on Amazon account with the name specified in the **Amazon S3 Bucket Name** field.

Note: To use the Default Credential Provider Chain for **Amazon Access Key** and **Amazon Secret Key**, see AWS Credentials.

6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. 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.
9. Select whether you want to run the connector as a service or in the standalone mode.
10. Complete the installation.
11. Run the SmartConnector.

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

Modifying Amazon S3 Default Parameters

You can use the following default parameters to refine or elaborate the way the Connector works with Amazon S3 as destination.

To modify the Amazon S3 default parameters:

1. Go to `ArcSight_home>\config\agent\agent.default.properties` file.
2. Copy the property line that you want to modify to your `agent.properties` file.
3. Modify the values of the following parameters as required:

Parameter	Description
transport.avroawss3.file.s3done.retention.days=5	The number of days for which the generated Avro output file that was successfully sent to the Amazon S3 destination will be retained. Modify this parameter to increase the maximum number of days for which the Avro output file will be retained.
transport.avroawss3.file.event.max.limit=10000	The maximum number of events to be available in the generated Avro output file. Modify this parameter to increase the number of events to be saved in the Avro output file.
transport.avroawss3.file.upload.interval.minutes=5	The time interval (in minutes) at which the generated Avro output files will be sent to the Amazon S3 destination. Modify this parameter to increase the time interval between the Avro output files.

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
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

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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	usepreviousetemplate

CloudFormation Service ValidateTemplate Operation Mappings

ArcSight ESM Field	Device-Specific Field
deviceCustomString3	capabilities
deviceCustomString5	parameters
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)
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

ArcSight ESM Field	Device-Specific Field
Device Custom String 5 Label	"Web ACL ID"
Device Custom String 6	ResourceArn
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"

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"
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"

ArcSight ESM Field	Device-Specific Field
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)
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
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

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 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

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 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-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"
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 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

ArcSight ESM Field	Device-Specific Field
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
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

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"
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"

ArcSight ESM Field	Device-Specific Field
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
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
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"
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"

ArcSight ESM Field	Device-Specific Field
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"
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 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
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"
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
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
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"

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"
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"

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"
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
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
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"

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"
Old File Name	ruleGroup
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"

ArcSight ESM Field	Device-Specific Field
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
Device Custom String 3 Label	"Geo 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 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
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

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 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"
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

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 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 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"

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"
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"

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"
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
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"
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
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
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
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"
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"
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)
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
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
Device Action	__ifThenElse(action,,__stringConstant ("Add Attributes To Findings"),action)
Device Custom String 3	attributes

ArcSight ESM Field	Device-Specific Field
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	__ifThenElse(action,,__stringConstant ("Create Assessment Target"),action)
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	__ifThenElse(action,,__stringConstant ("Create Assessment Template"),action)
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	__ifThenElse(action,,__stringConstant ("Create Exclusions Preview"),action)
Device Custom String 5	previewToken
Device Custom String 5 Label	"Preview Token"
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"
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

ArcSight ESM Field	Device-Specific Field
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"

ArcSight ESM Field	Device-Specific Field
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
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
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

ArcSight ESM Field	Device-Specific Field
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
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

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

Inspector Remove Attributes From Findings Mappings

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

Inspector Set Tags For Resource Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,,__stringConstant ("Set 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 Start Assessment Run Mappings

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

Inspector Stop Assessment Run Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	__ifThenElse(action,,__stringConstant ("Stop Assessment Run"),action)
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
Destination User ID	resources->accountId
Destination User Privileges	requestParameters
Device Custom String 4	additionalEventData
Device Custom String 5	requestParameters

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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
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

ArcSight ESM Field	Device-Specific Field
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	remoteIp_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	remoteIp_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	remoteIp_lat
Device Custom Number 1	blocked
Device Custom String 1	networkInterfaces
Device Custom String 2	productCodes
Device Custom String 3	tags

ArcSight ESM Field	Device-Specific Field
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	remoteIp_lon
Device Severity	severity
Event Outcome	organization_org
External Id	remoteIp_asnOrg
File Create Time	updatedAt
File Hash	instanceState
File Id	remoteIp_countryName
File Name	remoteIp_ipAddressV4
File Path	remoteIp_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

ArcSight ESM Field	Device-Specific Field
Request URL	remoteIp_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 Translated Address	remoteIp_ipAddressV4
Source User Id	accountId
Source User Name	username
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
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

ArcSight ESM Field	Device-Specific Field
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
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"

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	communicationBody
Device Custom String 6 Label	"Communication Body"
File ID	attachmentSetId
Old File ID	caseId

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	languaage
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	caseId
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")
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 Number1	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")

ArcSight ESM Field	Device-Specific Field
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"
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"

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 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"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"Request Parameters"

ArcSight ESM Field	Device-Specific Field
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

ArcSight ESM Field	Device-Specific Field
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
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

Lambda Add Layer Version Permission Mappings

ArcSight ESM Field	Device-Specific Field
Destination Dns Domain	requestOrganizationId
Destination Nt Domain	requestPrincipal
Destination User Privileges	requestAction
Device Action	"Add Layer Version Permission"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Old File Id	responseRevisionId
Old File Permission	statement
Source Process Name	requestLayerName

Lambda Add Permission Mappings

ArcSight ESM Field	Device-Specific Field
Destination User Privileges	requestAction
Device Action	"Add Permission"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 6	sourceArn
Device Custom String 6 Label	"Source Arn"
File Name	functionName
Old File Permission	statement
Source Nt Domain	requestPrincipal
Source User Id	sourceAccount

Lambda Create Alias Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Create Alias"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	responseFunctionVersion
Device Custom String 3 Label	"Response Function Version"
Device Custom String 5	aliasArn
Device Custom String 5 Label	"Alias Arn"
File Name	requestFunctionName
Old File Hash	responseDescription
Old File Id	revisionId
Old File Name	responseName
Old File Type	responseRoutingConfig

Lambda Create Event Source Mapping Mappings

ArcSight ESM Field	Device-Specific Field
Additional Data	bisectBatchOnFunctionError
Device Action	"Create Event Source Mapping"
Device Custom Number 1	maximumRecordAgeInSeconds
Device Custom Number 1 Label	"Maximum Record Age In Seconds"
Device Custom Number 2	responseBatchSize
Device Custom Number 2 Label	"Response Batch Size"
Device Custom Number 3	responseMaximumBatchingWindowInSeconds
Device Custom Number 3 Label	"Response Maximum Batching Window In Seconds"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	destinationConfig
Device Custom String 3 Label	"Destination Config"
Device Custom String 6	responseEventSourceArn
Device Custom String 6 Label	"Response Event Source Arn"
File Id	functionArn
File Modification Time	lastModified
File Name	requestFunctionName
File Type	state
Old File Hash	maximumRetryAttempts
Old File Id	uuid
Old File Name	lastProcessingResult
Old File Path	stateTransitionReason
Old File Type	parallelizationFactor

Lambda Create Function Mappings

ArcSight ESM Field	Device-Specific Field
Additional Data	stateReasonCode
Additional Data	lastUpdateStatusReasonCodeA
Additional Data	lastUpdateStatus
Additional Data	lastUpdateStatusReason
Additional Data	responseTracingConfi
Additional Data	responseVpcConfig
Additional Data	responseDeadLetterConfig
Device Action	"Create Function"
Device Custom Number 2	responseMemorySize
Device Custom Number 2 Label	"Response Memory Size"
Device Custom Number 3	responseTimeout
Device Custom Number 3 Label	"Response Timeout"

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	responseHandler
Device Custom String 3 Label	"Response Handler"
Device Custom String 5	masterArn
Device Custom String 5 Label	"Master Arn"
Device Custom String 6	version
Device Custom String 6 Label	"Function Version"
File Hash	codeSha256
File Id	functionArn
File Modification Time	lastModified
File Name	responseFunctionName
File Path	responseLayers
File Permission	responseKMSKeyArn
File Size	codeSize
File Type	state
Old File Hash	responseDescription
Old File Id	revisionId
Old File Name	responseEnvironment
Old File Path	stateReason
Old File Permission	responseRole
Old File Type	responseRuntime

Lambda Delete Alias Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Delete Alias"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
File Name	requestFunctionName
Old File Name	name

Lambda Delete Event Source Mapping Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Delete Event Source Mapping"
Device Custom Number 1	maximumRecordAgeInSeconds
Device Custom Number 2	responseBatchSize
Device Custom Number 2 Label	"Maximum Record Age In Seconds"
Device Custom Number 2 Label	"Response Batch Size"
Device Custom Number 3	responseMaximumBatchingWindowInSeconds
Device Custom Number 3 Label	"Response Maximum Batching Window In Seconds"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	destinationConfig
Device Custom String 3 Label	"Destination Config"
Device Custom String 6	responseEventSourceArn
Device Custom String 6 Label	"Response Event Source Arn"
File Id	functionArn
File Modification Time	lastModified
File Type	State
Old File Hash	maximumRetryAttempts
Old File Id	uuid
Old File Name	lastProcessingResult
Old File Path	stateTransitionReason
Old File Type	parallelizationFactor

Lambda Delete Function Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Delete Function"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
File Name	requestFunctionName

Lambda Delete Function Concurrency Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Delete Function Concurrency"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
File Name	requestFunctionName

Lambda Delete Function Event Invoke Config Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Delete Function Event Invoke Config"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
File Name	requestFunctionName

Lambda Delete Layer Version Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Delete Layer Version"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Source Process Name	layerName

Lambda Delete Provisioned Concurrency Config Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Delete Provisioned Concurrency Config"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
File Name	requestFunctionName

Lambda Get Account Settings Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Get Account Settings"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 5	accountLimit
Device Custom String 5 Label	"Account Limit"
Device Custom String 6	accountUsage
Device Custom String 6 Label	"Account Usage"

Lambda Get Alias Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Get Alias"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	responseFunctionVersion
Device Custom String 3 Label	"Response Function Version"
Device Custom String 5	aliasArn
Device Custom String 5 Label	"Alias Arn"
File Name	requestFunctionName
Old File Hash	responseDescription
Old File Id	revisionId
Old File Name	responseName
Old File Type	responseRoutingConfig

Lambda Get Event Source Mapping Mappings

ArcSight ESM Field	Device-Specific Field
Additional Data	bisectBatchOnFunctionError
Device Action	"Get Event Source Mapping"
Device Custom Number 1	maximumRecordAgeInSeconds
Device Custom Number 2	responseBatchSize
Device Custom Number 2 Label	"Maximum Record Age In Seconds"
Device Custom Number 2 Label	"Response Batch Size"
Device Custom Number 3	responseMaximumBatchingWindowInSeconds
Device Custom Number 3 Label	"Response Maximum Batching Window In Seconds"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	destinationConfig
Device Custom String 3 Label	"Destination Config"
Device Custom String 6	responseEventSourceArn
Device Custom String 6 Label	"Response Event Source Arn"
File Id	functionArn
File Modification Time	lastModified
File Type	state
Old File Hash	maximumRetryAttempts
Old File Id	uuid
Old File Name	lastProcessingResult
Old File Path	stateTransitionReason
Old File Type	parallelizationFactor

Lambda Get Function Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Get Function"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	configuration
Device Custom String 3 Label	"Configuration"
Device Custom String 5	tags
Device Custom String 5 Label	"Tags"
Device Custom String 6	code
Device Custom String 6 Label	"Code"
File Name	requestFunctionName
Old File Hash	concurrency

Lambda Get Function Concurrency Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Get Function Concurrency"
Device Custom Number 1	reservedConcurrentExecutions
Device Custom Number 1 Label	"Reserved Concurrent Executions"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
File Name	requestFunctionName

Lambda Get Function Configuration Mappings

ArcSight ESM Field	Device-Specific Field
Additional Data	stateReasonCode
Additional Data	lastUpdateStatusReasonCode
Additional Data	lastUpdateStatus
Additional Data	lastUpdateStatusReason
Additional Data	responseTracingConfig
Additional Data	responseVpcConfig
Additional Data	responseDeadLetterConfig
Device Action	"Get Function Configuration"
Device Custom Number 2	responseMemorySize
Device Custom Number 2 Label	"Response Memory Size"
Device Custom Number 3	responseTimeout
Device Custom Number 3 Label	"Response Timeout"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	responseHandler
Device Custom String 3 Label	"Response Handler"
Device Custom String 5	masterArn
Device Custom String 5 Label	"Master Arn"
Device Custom String 6	version
Device Custom String 6 Label	"Function Version"
File Hash	codeSha256
File Id	functionArn
File Modification Time	lastModified
File Name	requestFunctionName
File Path	responseLayers
File Permission	responseKMSKeyArn
File Size	codeSize
File Type	state
Old File Hash	responseDescription
Old File Id	revisionId
Old File Name	responseEnvironment
Old File Path	stateReason
Old File Permission	responseRole
Old File Type	responseRuntime

Lambda Get Function Event Invoke Config Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Get Function Event Invoke Config"
Device Custom Number 1	maximumEventAgeInSeconds
Device Custom Number 1 Label	Maximum Event Age In Seconds
Device Custom Number 2	maximumRetryAttempts
Device Custom Number 2 Label	Maximum Retry Attempts
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	destinationConfig
Device Custom String 3 Label	"Destination Config"
Field Id	functionArn
File Modification Time	lastModified
File Name	requestFunctionName

Lambda Get Layer Version Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Get Layer Version"
Device Custom Date 1	createdDate
Device Custom Date 1 Label	"Created Date"
Device Custom Number 1	version
Device Custom Number 1 Label	"Version"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	layerVersionArn
Device Custom String 3 Label	"Layer Version Arn"
Device Custom String 5	layerArn
Device Custom String 5 Label	"Layer Arn"
Device Custom String 6	licenseInfo
Device Custom String 6 Label	"License Info"
Old File Hash	description
Old File Name	content
Old File Type	compatibleRuntimes
Source Process Name	requestLayerName

Lambda Get Layer Version By Arn Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Get Layer Version By Arn"
Device Custom Date 1	createdDate
Device Custom Date 1 Label	"Created Date"
Device Custom Number 1	version
Device Custom Number 1 Label	"Version"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	layerVersionArn
Device Custom String 3 Label	"Layer Version Arn"
Device Custom String 5	layerArn
Device Custom String 5 Label	"Layer Arn"
Device Custom String 6	licenseInfo
Device Custom String 6 Label	"Get Layer Version By Arn"
Old File Hash	description
Old File Name	content
Old File Type	compatibleRuntimes

Lambda Get Layer Version Policy Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Get Layer Version Policy"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 6	policy

ArcSight ESM Field	Device-Specific Field
Device Custom String 6 Label	"Policy"
Old File Id	revisionId
Source Process Name	requestLayerName

Lambda Get Policy Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Get Policy"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 6	policy
Device Custom String 6 Label	"Policy"
File Name	requestFunctionName
Old File Id	revisionId

Lambda Get Provisioned Concurrency Config Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Get Provisioned Concurrency Config"
Device Custom Number 1	allocatedProvisionedConcurrentExecutions
Device Custom Number 1 Label	"Allocated Provisioned Concurrent Executions"
Device Custom Number 2	availableProvisionedConcurrentExecutions
Device Custom Number 2 Label	"Available Provisioned Concurrent Executions"
Device Custom Number 3	requestedProvisionedConcurrentExecutions
Device Custom Number 3 Label	"Requested Provisioned Concurrent Executions"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
File Modification Time	lastModified
File Name	requestFunctionName
File Type	status
Old File Path	statusReason

Lambda Invoke Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Invoke"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	functionError
Device Custom String 3 Label	"Function Error"
Device Custom String 5	executedVersion
Device Custom String 5 Label	"Executed Version"
Device Custom String 6	responsePayload
Device Custom String 6 Label	"Response Payload"
File Name	requestFunctionName
Old File Hash	logResult
Old File Id	statusCode

Lambda Invoke Async Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Invoke Async"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
File Name	requestFunctionName
Old File Id	status

Lambda List Aliases Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"List Aliases"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	nextMarker
Device Custom String 3 Label	"Next Marker"
Device Custom String 5	aliases
Device Custom String 5 Label	"Aliases"
File Name	requestFunctionName

Lambda List Event Source Mappings Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"List Event Source Mappings"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	nextMarker
Device Custom String 3 Label	"Next Marker"
Device Custom String 6	eventSourceMappings
Device Custom String 6 Label	"Event Source Mappings"
File Name	requestFunctionName

Lambda List Function Event Invoke Configs Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"List Function Event Invoke Configs"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	nextMarker
Device Custom String 3 Label	"Next Marker"
Device Custom String 6	functionEventInvokeConfigs
Device Custom String 6 Label	"Function Event Invoke Configs"

Lambda List Functions Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"List Functions"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	nextMarker
Device Custom String 3 Label	"Next Marker"
Device Custom String 6	functions
Device Custom String 6 Label	"Functions"

Lambda List Layers Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"List Layers"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	nextMarker
Device Custom String 3 Label	"Next Marker"
Device Custom String 6	layers
Device Custom String 6 Label	"Layers"

Lambda List Layer Versions Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"List Layer Versions"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	nextMarker
Device Custom String 3 Label	"Next Marker"
Device Custom String 6	layerVersions
Device Custom String 6 Label	"Layer Versions"
Old File Type	requestCompatibleRuntime
Source Process Name	requestLayerName

Lambda List Provisioned Concurrency Configs Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"List Provisioned Concurrency Configs"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	nextMarker

ArcSight ESM Field	Device-Specific Field
Device Custom String 3 Label	"Next Marker"
Device Custom String 6	provisionedConcurrencyConfigs
Device Custom String 6 Label	"Provisioned Concurrency Configs"

Lambda List Tags Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"List Tags"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 5	tags
Device Custom String 5 Label	"Tags"

Lambda List Versions by Function Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"List Versions By Function"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	nextMarker
Device Custom String 3 Label	"Next Marker"
Device Custom String 5	versions
Device Custom String 5 Label	"Versions"
File Name	requestFunctionName

Lambda Publish Layer Version Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Publish Layer Version"
Device Custom Date 1	createdDate
Device Custom Date 1 Label	"Created Date"
Device Custom Number 1	version
Device Custom Number 1 Label	"Version"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	layerVersionArn
Device Custom String 3 Label	"Layer Version Arn"
Device Custom String 5	layerArn
Device Custom String 5 Label	"Layer Arn"
Device Custom String 6	responseLicenseInfo
Device Custom String 6 Label	"Response License Info"
Old File Hash	responseDescription
Old File Name	responseContent
Old File Type	responseCompatibleRuntimes
Source Process Name	requestLayerName

Lambda Publish Version Mappings

ArcSight ESM Field	Device-Specific Field
Additional Data	stateReasonCode
Additional Data	lastUpdateStatusReasonCode
Additional Data	lastUpdateStatus
Additional Data	lastUpdateStatusReason
Additional Data	responseTracingConfig

ArcSight ESM Field	Device-Specific Field
Additional Data	responseVpcConfig
Additional Data	responseDeadLetterConfig
Device Action	"Function Version"
Device Custom Number 2	responseMemorySize
Device Custom Number 2 Label	"Response Memory Size"
Device Custom Number 3	responseHandler
Device Custom Number 3 Label	"Response Handler"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	layerVersionArn
Device Custom String 3 Label	"Layer Version Arn"
Device Custom String 5	masterArn
Device Custom String 5 Label	"Master Arn"
Device Custom String 6	version
Device Custom String 6 Label	"Function Version"
File Hash	codeSha256
File Id	functionArn
File Modification Time	lastModified
File Name	responseFunctionName
File Path	responseLayers
File Permission	responseKMSKeyArn
File Size	codeSize
File Type	state
Old File Hash	responseDescription
Old File Id	revisionId
Old File Name	responseEnvironment
Old File Path	stateReason
Old File Permission	responseRole
Old File Type	responseRuntime

Lambda Put Function Concurrency Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	reservedConcurrentExecutions
Device Custom Number 1 Label	"Reserved Concurrent Executions"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
File Name	requestFunctionName

Lambda Put Function Event Invoke Config Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Put Function Event Invoke Config"
Device Custom Number 1	maximumEventAgeInSeconds
Device Custom Number 1 Label	Maximum Event Age In Seconds
Device Custom Number 2	maximumRetryAttempts
Device Custom Number 2 Label	Maximum Retry Attempts
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	destinationConfig
Device Custom String 3 Label	"Destination Config"
File Id	functionArn
File Modification Time	lastModified
File Name	requestFunctionName

Lambda Put Provisioned Concurrency Config Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Put Provisioned Concurrency Config"
Device Custom Number 1	allocatedProvisionedConcurrentExecutions
Device Custom Number 1 Label	"Allocated Provisioned Concurrent Executions"
Device Custom Number 2	availableProvisionedConcurrentExecutions
Device Custom Number 2 Label	"Available Provisioned Concurrent Executions"
Device Custom Number 3	requestedProvisionedConcurrentExecutions
Device Custom Number 3 Label	"Requested Provisioned Concurrent Executions"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
File Modification Time	lastModified
File Name	requestFunctionName
File Type	status
Old File Path	statusReason

Lambda Remove Layer Version Permission Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Remove Layer Version Permission"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Old File Id	revisionId
Source Process Name	layerName

Lambda Remove Permission Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Remove Permission"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
File Name	requestFunctionName
Old File Id	revisionId

Lambda Tag Resource Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Tag Resource"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 5	tags
Device Custom String 5 Label	"Tags"
File Id	arn

Lambda Untag Resource Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Untag Resource"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	tagKeys
Device Custom String 5 Label	"Tag Keys"
File Id	arn

Lambda Update Alias Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Update Alias"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	responseFunctionVersion
Device Custom String 3 Label	"Response Function Version"
Device Custom String 5	aliasArn
Device Custom String 5 Label	"Alias Arn"
File Name	requestFunctionName
Old File Hash	responseDescription
Old File Id	revisionId
Old File Name	responseName
Old File Type	responseRoutingConfig

Lambda Update Event Source Mapping Mappings

ArcSight ESM Field	Device-Specific Field
Additional Data	bisectBatchOnFunctionError
Device Action	"Update Event Source Mapping"
Device Custom Number 1	maximumRecordAgeInSeconds
Device Custom Number 1 Label	"Maximum Record Age In Seconds"
Device Custom Number 2	responseBatchSize
Device Custom Number 2 Label	"Response Batch Size"

ArcSight ESM Field	Device-Specific Field
Device Custom Number 3	responseMaximumBatchingWindowInSeconds
Device Custom Number 3 Label	"Response Maximum Batching Window In Seconds"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	destinationConfig
Device Custom String 3 Label	"Destination Config"
Device Custom String 6	responseEventSourceArn
Device Custom String 6 Label	"Response Event Source Arn"
Field Id	functionArn
File Modification Time	lastModified
File Name	requestFunctionName
File Type	state
Old File Hash	maximumRetryAttempts
Old File Id	uuid
Old File Name	lastProcessingResult
Old File Path	stateTransitionReason
Old File Type	parallelizationFactor

Lambda Update Function Code Mappings

ArcSight ESM Field	Device-Specific Field
Additional Data	stateReasonCode
Additional Data	lastUpdateStatusReasonCode
Additional Data	lastUpdateStatus
Additional Data	lastUpdateStatusReason
Additional Data	responseTracingConfig
Additional Data	responseVpcConfig
Additional Data	responseDeadLetterConfig

ArcSight ESM Field	Device-Specific Field
Device Action	"Update Function Code"
Device Custom Number 2	responseMemorySize
Device Custom Number 2 Label	"Response Memory Size"
Device Custom Number 3	responseTimeout
Device Custom Number 3 Label	"Response Timeout"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	responseHandler
Device Custom String 3 Label	"Response Handler"
Device Custom String 5	masterArn
Device Custom String 5 Label	"Master Arn"
Device Custom String 6	version
Device Custom String 6 Label	"Function Version"
File Hash	codeSha256
File Id	functionArn
File Modification Time	lastModified
File Name	responseFunctionName
File Path	responseLayers
File Permission	responseKMSKeyArn
File Size	codeSize
File Type	state
Old File Hash	responseDescription
Old File Id	revisionId
Old File Name	responseEnvironment
Old File Path	stateReason
Old File Type	responseRuntime

Lambda Update Function Configuration Mappings

ArcSight ESM Field	Device-Specific Field
Additional Data	stateReasonCode
Additional Data	lastUpdateStatusReasonCode
Additional Data	lastUpdateStatus
Additional Data	lastUpdateStatusReason
Additional Data	responseTracingConfig
Additional Data	responseVpcConfig
Additional Data	responseDeadLetterConfig
Device Action	"Update Function Configuration"
Device Custom Number 2	responseMemorySize
Device Custom Number 2 Label	"Response Memory Size"
Device Custom Number 3	responseTimeout
Device Custom Number 3 Label	"Response Timeout"
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	responseHandler
Device Custom String 3 Label	"Response Handler"
Device Custom String 5	masterArn
Device Custom String 5 Label	"Master Arn"
Device Custom String 6	version
Device Custom String 6 Label	"Function version"
File Hash	codeSha256
File Id	functionArn
File Modification Time	lastModified
File Name	responseFunctionName
File Path	responseLayers
File Permission	responseKMSKeyArn
File Size	codeSize

ArcSight ESM Field	Device-Specific Field
File Type	state
Old File Id	revisionId
Old File Name	responseEnvironment
Old File Path	stateReason
Old File Permission	responseRole
Old File Type	responseRuntime

Lambda Update Function Event Invoke Config Mappings

ArcSight ESM Field	Device-Specific Field
Device Action	"Update Function Event Invoke Config"
Device Custom Number 1	maximumEventAgeInSeconds
Device Custom Number 1 Label	Maximum Event Age In Seconds
Device Custom Number 2	maximumRetryAttempts
Device Custom Number 2 Label	Maximum Retry Attempts
Device Custom String 1	requestParameters
Device Custom String 1 Label	"requestParameters"
Device Custom String 2	responseElements
Device Custom String 2 Label	"responseElements"
Device Custom String 3	destinationConfig
Device Custom String 3 Label	"Destination Config"
Field Id	functionArn
File Modification Time	lastModified
File Name	requestFunctionName

Troubleshooting

Certificate Issue while Integrating Connector with Third-party Application

Because of SNI, the following certificate exception might be displayed while configuring the connector with third-party application:

```
Error[1]: RemoteException: cause[javax.net.ssl.SSLHandshakeException: PKIX
path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target
```

Workaround: To fix this issue, see Certificate Issue while Integrating Connector with Third-party Application.

AWS CloudTrail connector latency in 'processLog' and 'processSource'

AWS CloudTrail connector takes more than expected time to process the 'processLog' and 'processSource'. As a result, a large number of messages wait in the SQS queue resulting in performance issues.

Workaround: To resolve this issue, the following default parameters have been introduced in the `agent.properties` file:

- **awsfilterevent:** By default, the value of this parameter is set to false in the `agent.properties` file. If you want to filter events, set **awsfilterevent** to **true** and add `include` and `exclude` services for the following parameters:

  ```
  amazon_cloudtrail.services.exclude=
  ```

  ```
  amazon_cloudtrail.services.include=
  ```

- **awsthreadcount:** By default, the value of this parameter is set to 10 in the `agent.properties` file.

Note: You can change the value of this parameter if required, but it is not recommended to increase the number of threads. Before changing any value in the file, you must stop the connector and restart it once you save the modified value.

If you want to increase the number of threads, you must increase the memory for the connector as follows:

- If you run the connector as a standalone, perform the following steps:
  a. Go to the `..\current\bin\scripts` directory and open the `connectors.bat` file.
  b. In line 22, you can change the value of **ARCSIGHT_MEM_OPTIONS**.

     The connector uses only 256 MB for **Xms** and **Xmx** parameters. You can increase the connector's memory to the desired value. However, you can set it either to 1024 MB or 2048 MB.
  c. Click **Save**.
- If you run the connector as a service, perform the following additional steps:
  a. Go to the `..\current\user\agent` directory and open the `agent.wrapper.conf` file.
  b. Modify the values for **wrapper.java.initmemory** and **wrapper.java.maxmemory** properties as required. However, you can set it either to 1024 MB or 2048 MB.
  c. Click **Save**.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on SmartConnector for Amazon Web Services CloudTrail (SmartConnectors 8.3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!