FORCEPOINT

Forcepoint DLP and AWS Security Hub

Integration Guide

Michael Nevin
Mattia Maggioli
31 March 2020
Public

Version	Date	Author	Notes
0.1	15 December 2019	Michael Nevin	First draft
0.2	19 December 2019	Mattia Maggioli	Review
0.3	1 January 2020	Michael Nevin	Update
0.4	21 January 2020	Mattia Maggioli	Review
0.5	30 January 2020	Jonathan Knepher	Review
0.6	17 February 2020	Mattia Maggioli	Removed references to ARN
0.7	23 March 2020	Neelima Rai	Added troubleshooting chapter
0.8	31 March 2020	Mattia Maggioli	Updated references and file name after ASFF format update on 13 March 2020

Summary

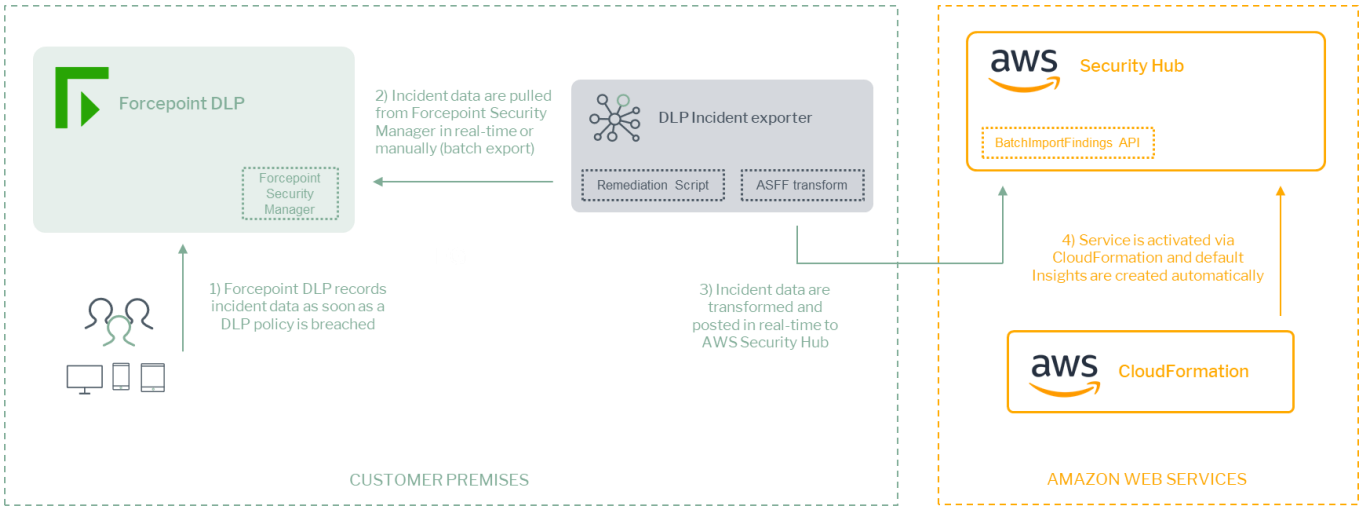
This guide provides step by step instructions to configure Forcepoint DLP and AWS Security Hub to export DLP incidents, transform data across different formats, and ingest them into AWS Security Hub.

The code and instructions provided enable system administrators to:

- Export incident data from Forcepoint DLP automatically in real-time or manually for batch exports
- Transform incident data into the ASFF format required by AWS Security Hub
- Ingest the data as “Findings” into AWS Security Hub and visualize events in groups as “Insights”

This interoperability enables customers to use AWS Security Hub as SIEM tool for incident data provided by Forcepoint DLP, and to correlate incident events with other Findings from multiple sources including AWS workloads.

A description of the workflow between the components involved in this POC is depicted in this diagram:



Caveats

The integration described in this document is tested with the following product versions:

- Forcepoint DLP with Forcepoint Security Manager 8.5.x
- AWS Security Hub – API schema 2018-10-08 with ASFF format update on 12 March 2020

Implementation

The solution described in this chapter requires the following files available at this link:

https://frcpnt.com/dlp-securityhub-latest

- fp-dlp-exporter-aws-azure-v1.1.zip

The archive **fp-dlp-exporter-aws-azure-v1.1.zip** contains all files necessary to setup and run all the services which enable the integration between Forcepoint DLP and AWS Security Hub:

- **FSM DB connection:** provides real-time export of DLP incidents, extracted from the database of Forcepoint Security Manager
- **Incident XML transformation:** provides manual and batch export capabilities via the remediation script feature available in Forcepoint Security Manager

The solution allows for customizable levels of granularity (High, Medium, and Low severity levels) and performs the transformation and upload tasks, with minimal impact on the underlying storage.

We suggest deploying the solution on the machine which hosts Forcepoint Security Manager, the instructions provided in this document are based on this scenario. The machine hosting the Forcepoint Security Manager will be referenced in the rest of this document by the name "**FSM**".

The following software will be automatically installed by the **install.bat** script provided inside **fp-dlp-exporter-aws-azure-v1.1.zip**:

- Nssm 2.24

using the following command

START /WAIT powershell -command "[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-WebRequest "https://nssm.cc/release/nssm-2.24.zip" -Method Get -OutFile .\Resources\nssm.zip"

Step 1 – Unpack DLP Incident Exporter and setup AWS Security Hub

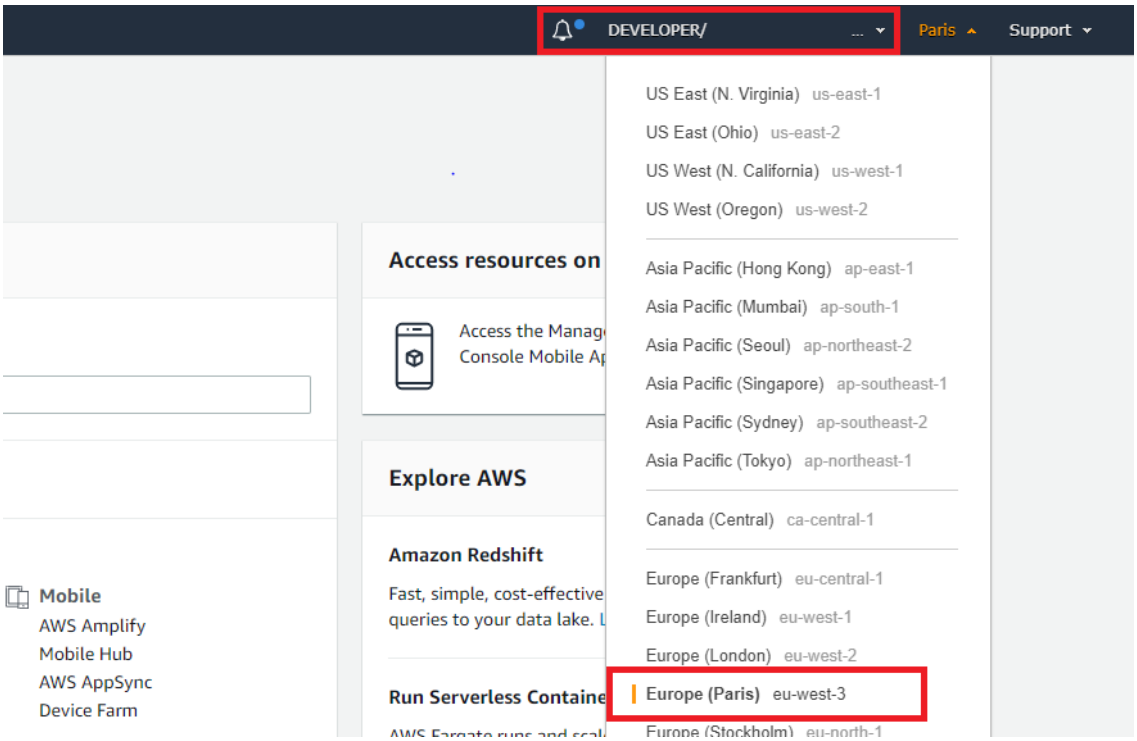
Interoperability with AWS Security Hub requires the activation of the service within AWS and the creation of credentials that will be used to send data using the **BatchImportFinding** API. If both requirements are already satisfied skip to Step 2.

Step 1.1 – Activate Security Hub using a CloudFormation template

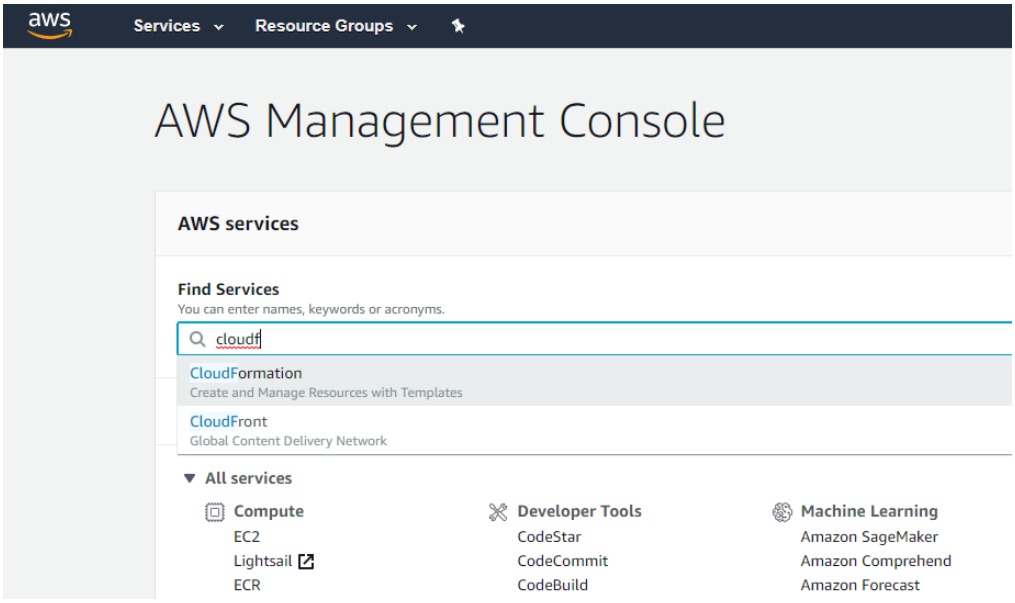
1. Login to the FSM machine and unzip **fp-dlp-exporter-aws-azure-v1.1.zip** into **C:\fp-dlp-exporter-aws-azure-v1**
2. Browse to AWS and from the header of the Management Console select the **AWS Region**

where you want to activate Security Hub, for performance we suggest picking a region close to the logs source

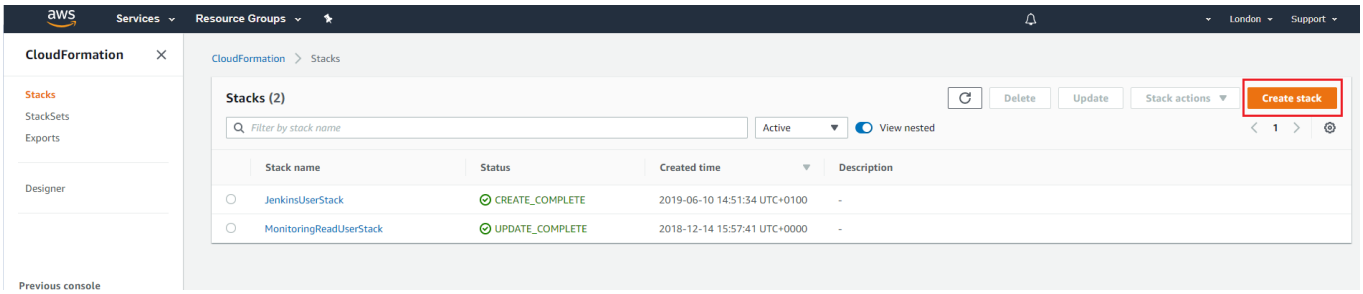
3. Take note of the region code (e.g. **eu-west-3**) next to the region name since this will be necessary in Step 2 of this guide



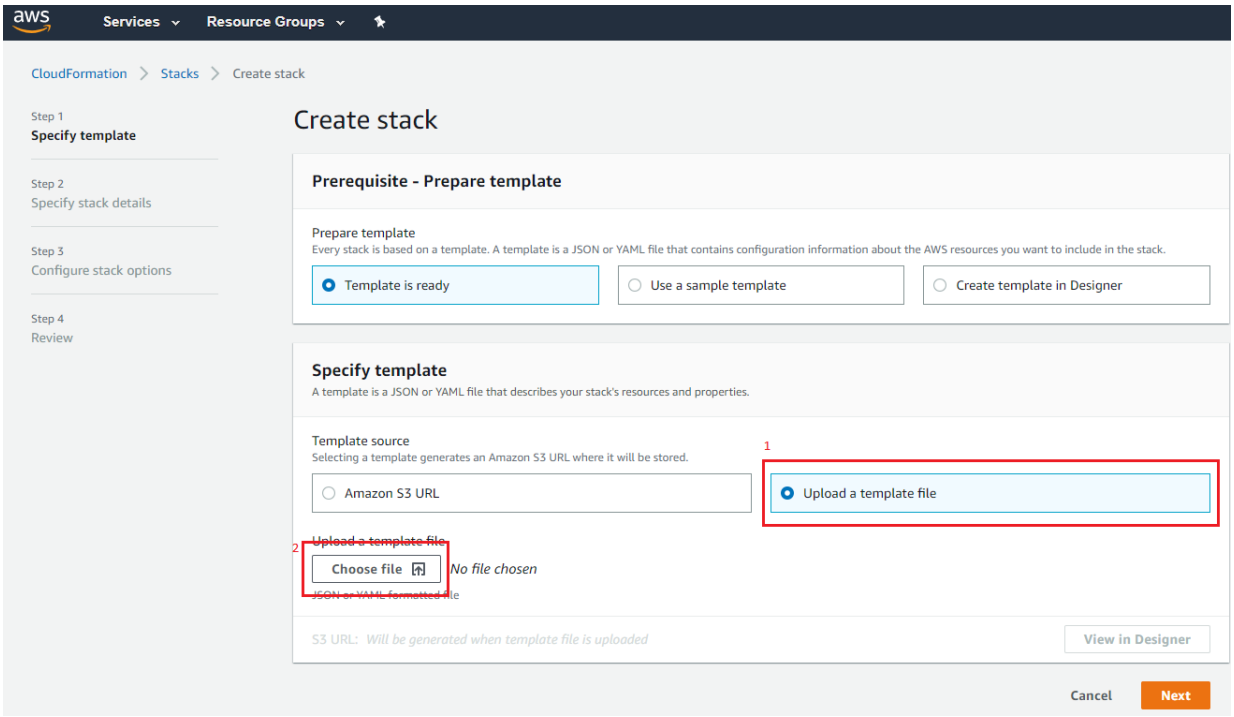
4. In the AWS Management Console, search for “cloudformation”, it will suggest some options as you type: click **CloudFormation** from the drop-down list



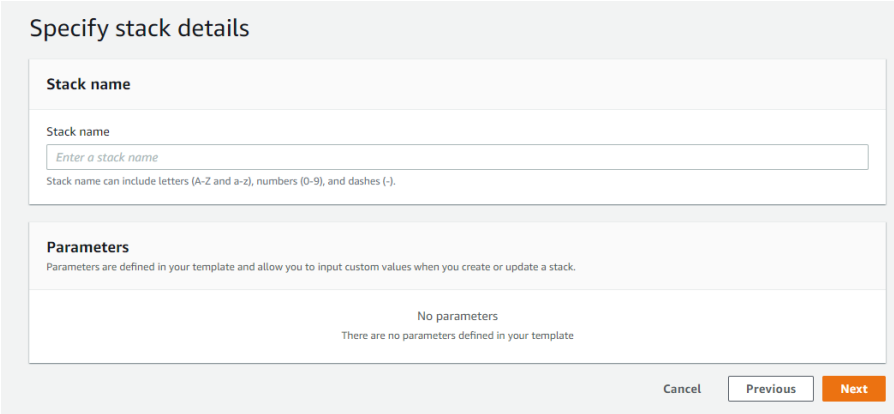
5. In the CloudFormation console click **Create stack** in the top right corner



6. In the next page select **Upload a template file**, click **Choose file** and navigate to the **EnableSecurityHub.json** located in **C:\fp-dlp-exporter-aws-azure-v1\CloudFormationTemplate**



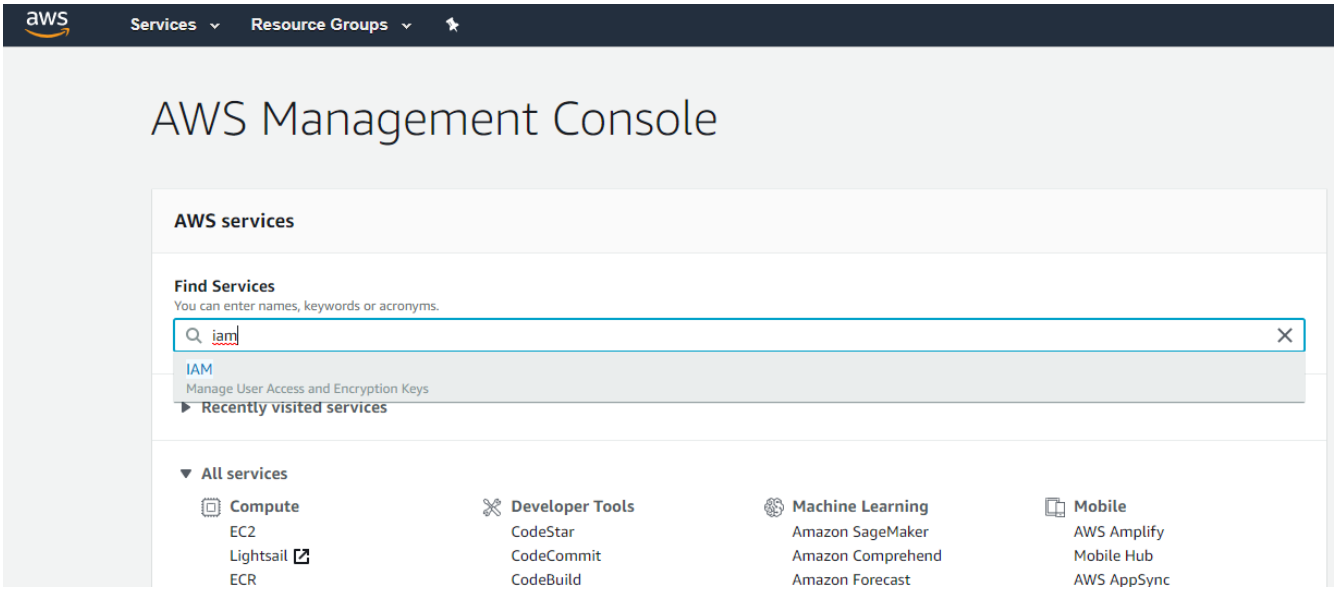
7. Click **Next** once the file is uploaded, enter a name for the new stack and then click **Next, Next** again and in the last page **Create stack**



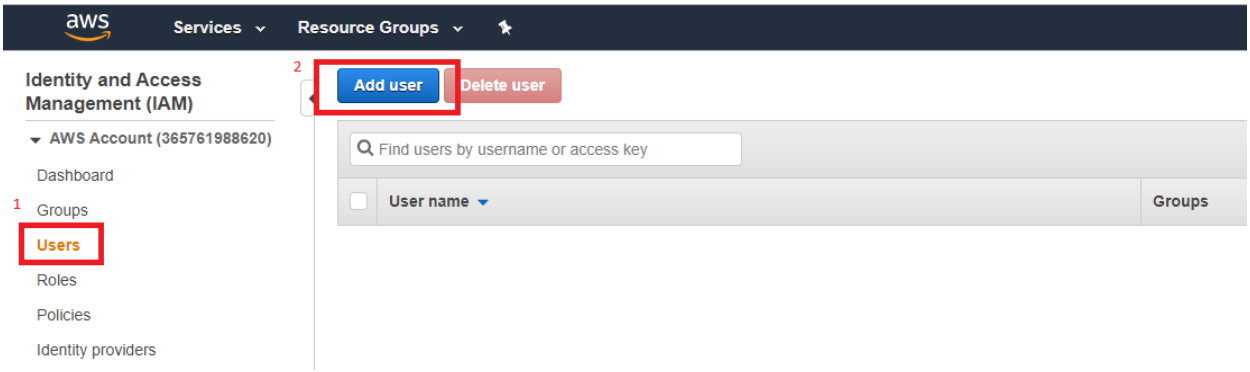
One that is complete, return to the AWS Management Console and search for “Security Hub”, it will be enabled and ready for use.

Step 1.2 – Create an IAM user that has access to Security Hub

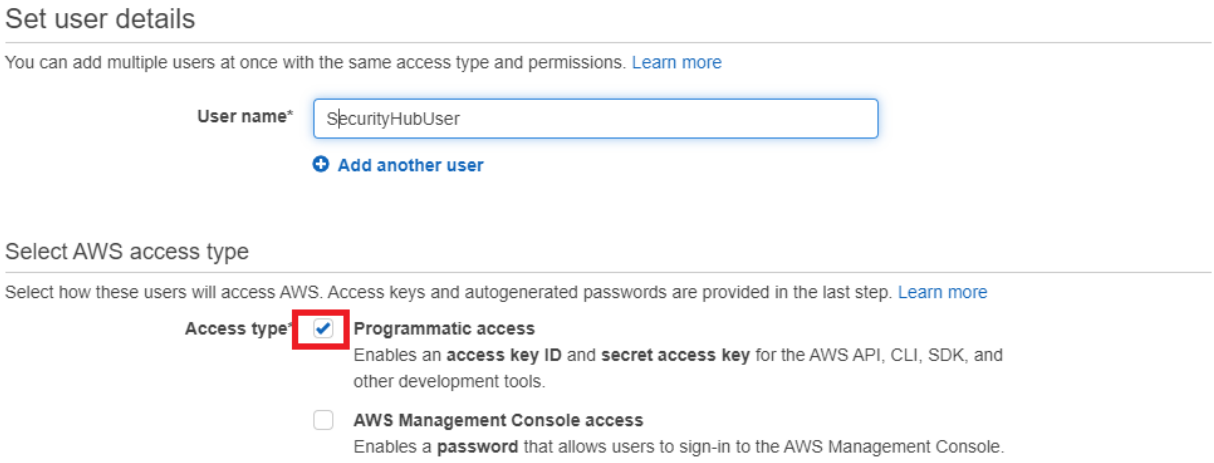
1. From the AWS Management Console type “iam” in the search area and select it form the drop-down list



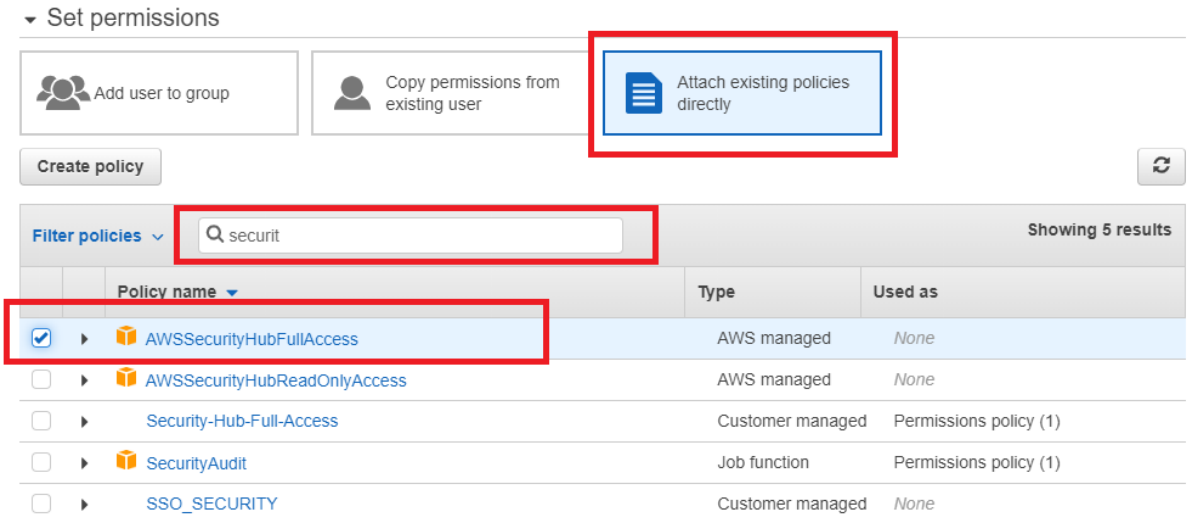
2. Select **Users** from the navigation pane on the left then click **Add user**



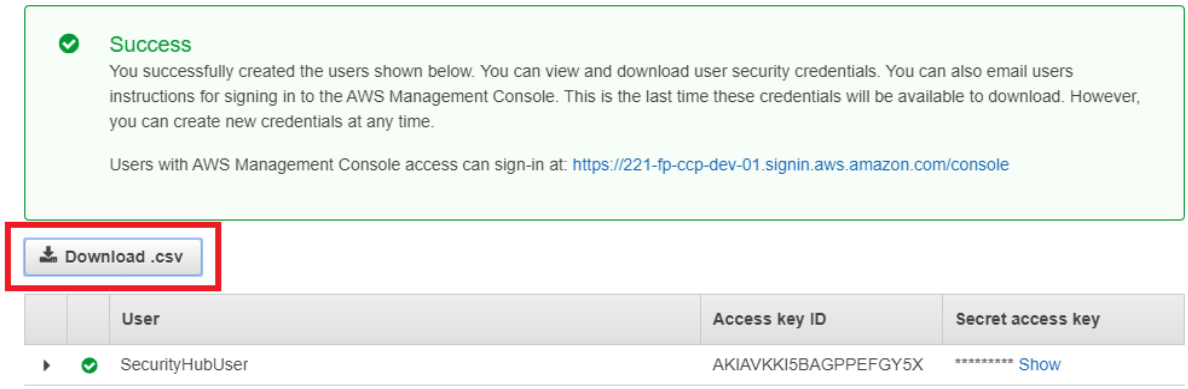
3. Enter a name for the new user and make sure to select the option **Programmatic access**, then click **Next: Permissions**



4. Select **Attach existing policies directly**, search for **AWSSecurityHUBFullAccess** and tick the box next to it then click **Next: Tags**. Since no tags are needed by our integration package click **Next: Review** then **Create User**.



5. Click **Download .csv** and store the file in a secure location: this will be needed in the next chapter of this guide.



Step 2 – Installing the DLP Incident Exporter

1. If not already done at step 1.1, login to the FSM machine and unzip **fp-dlp-exporter-aws-azure-v1.1.zip** into **C:\fp-dlp-exporter-aws-azure-v1**
2. Move to **C:\fp-dlp-exporter-aws-azure-v1**, open **config.json** with a text editor and add/edit the settings that will be used by the **DLP Incident Exporter**: values that require changing are highlighted with red font color in the following example:

```
{
  "AwsAccountId": "0123456789",
  "aws_access_key_id": "123ABC123ABC123ABC",
  "aws_secret_access_key": " abc123abc123abc123abc123abc123abc123abc123abc123",
  "region_name": "eu-west-1",
  "file_location": "/XMLFileCopy ",
  "HIGH": true,
  "MEDIUM": false,
  "LOW": false,
  "Database_Connection":
          {
             "Server": "sqlserver-hostname",
             "Database": "wbsn-data-security",
             "Trusted_Connection": "yes",
             "UID": "username",
             "PWD": "password"
          },
  "LogName": "ForcepointDLPEvents"
}
```

Once **config.json** is edited with all necessary values, double click **install.bat** to run it: the installer will display a few messages as it progresses through the installation steps.

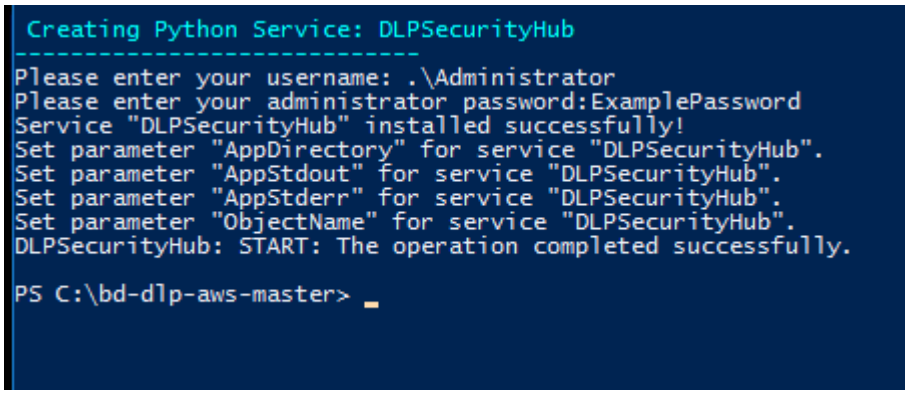
3. The installer will pause at **Creating Service: DLPExporter** and wait for user input:

   - **Please enter your username:** enter the username of an account with administrator access to the FSM machine. Username must be entered according to the format

     DOMAIN\username if using a domain account
     .\username if using a local account

   - **Please enter your administrator password:** enter the password of the account with administrator access

   Once both values are entered the installer will progress until a successful completion.



Once completed, the **DLP Incident Exporter** will run as a service on the FSM machine and DLP incidents will be exported to AWS Security Hub automatically.

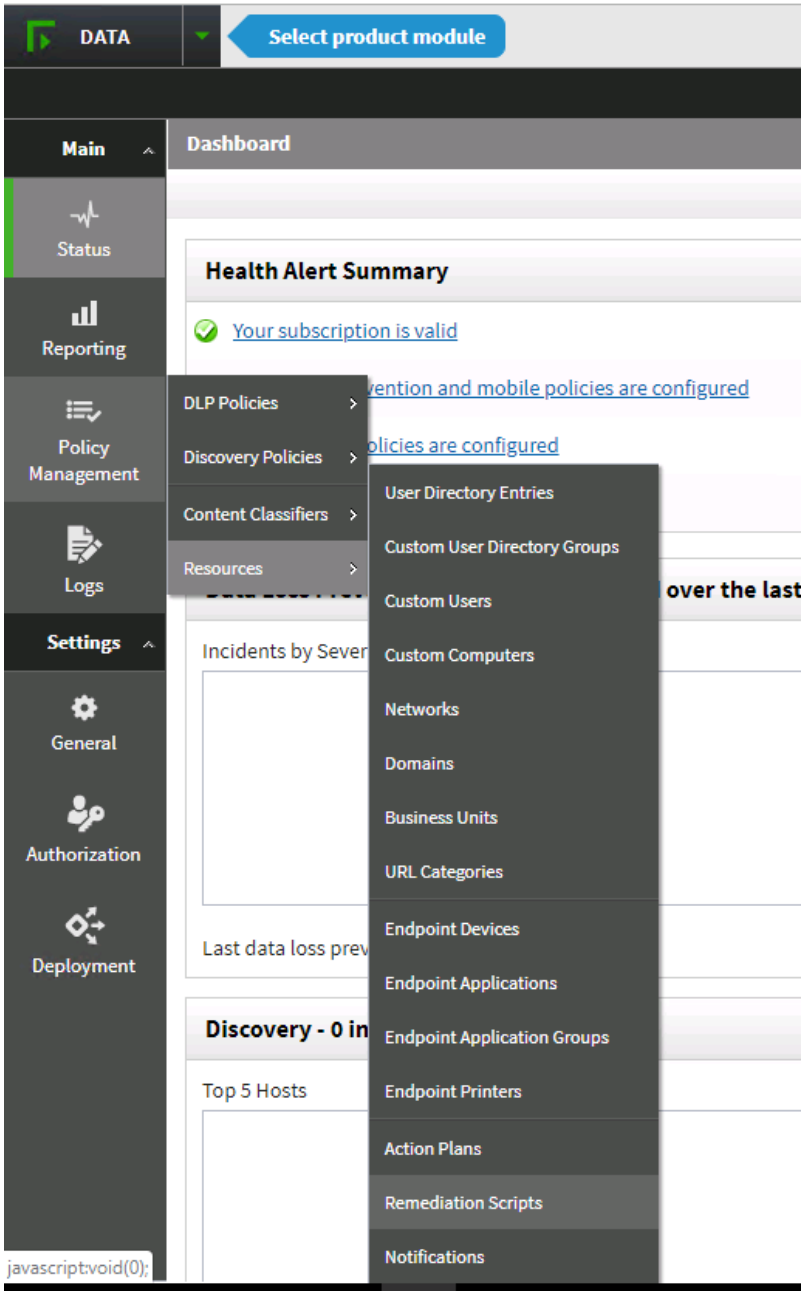
Appendix A - Description of config.json settings

PARAMETER	DESCRIPTION	CHANGE REQUIRED
AwsAccountId	ID of the AWS account used to post data into AWS Security Hub using the BatchImportFinding API	YES
aws_access_key_id	Located inside the .csv file downloaded as explained in step 1.2 of this document	YES
aws_secret_access_key	Located inside the .csv file downloaded as explained in step 1.2 of this document	
region_name	The AWS Region where Security Hub was activated at step 1.1	YES
file_location	Location used by the **DLP Incident Exporter** to store XML files with incident data before upload to AWS. Used when log export is done using the manual method based on remediation script	NO
HIGH **MEDIUM** **LOW**	These parameters allow filtering of DLP incidents, uploading only logs whose severity matches the levels set to TRUE.	YES
Database_Connection	These parameters are needed to connect to the SQL database used by Forcepoint Security Manager to store data of DLP incidents. **Server**: hostname or IP address of the SQL database **Database**: name of the database hosting the FSM data **Trusted_Connection**: only “yes” or “no” are possible • yes - if it is a trusted connection • no - if username and password will be used to connect **UID**: username used to login to the database **PWD**: password used to login to the database	YES
LogName	Name of the file storing logs of the DLP Incident Exporter	NO

Appendix B - Manual export of DLP incidents

The integration package provides also a method to export DLP incidents manually, either one by one or in batches, using a **Remediation Script**.

8. Login into the **FSM** machine, then login into the web interface of **Forcepoint Security Manager**
9. Using the left navigation bar, go to **Policy Management** > **Resources** > **Remediation Scripts**



10. Select **New…** from the top left corner and from the drop-down menu select **Incident Management Script**
11. Name the remediation script you are about to import, click **Choose file** and navigate to **C:\fp-dlp-exporter-aws-azure-v1\Remediation_script**, select **runScript.bat**
12. Click **Additional Files** to reveal **Choose File**: select the zip file **CopyFiles.zip** and click **OK** once done

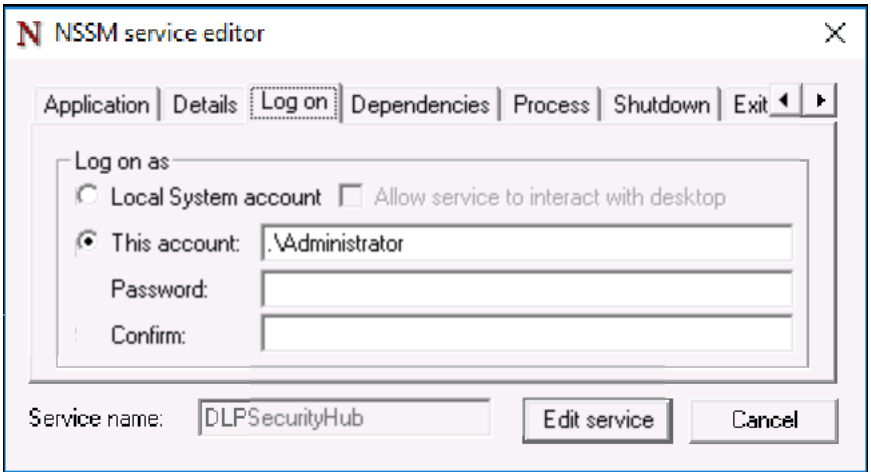
Now that the script is imported, DLP incidents can be exported simply using this Remediation Script selecting one or multiple DLP incidents from the **Reporting** area of Forcepoint Security Manager.

Appendix C – Service scripts

The **DLP Incident Exporter** service is managed by the NSSM tool.

Navigate to **C:\fp-dlp-exporter-aws-azure-v1\ServiceScripts**. There are four scripts provided.

PARAMETER	DESCRIPTION
changePassword	This script opens the UI of NSSM to provide an easy way to change or update the password. The password is editable from the **Log on** tab of NSSM (see below)
removeService	This script will remove the **DLPExporter** service from the server and stop it from running
restart	Restarts the **DLPExporter** service
stopService	Stops the **DLPExporter** service (Note this has not removed the service only stopped it from running)



Appendix D – Logs of DLP Incident Exporter

Logs of **DLP Incident Exporter** operations are stored into **C:\fp-dlp-exporter-aws-azure-v1\dlpLogger**.

Example message

DLPSecurityHub - INFO - 2019-12-13 17:56:35.055756 : Database Connection established

Log structure

Service Name	Message Type	Date and time	message
DLPSecurityHub	INFO DEBUG CRITICAL ERROR WARNING	2019-12-13 17:56:35.055756	Database Connection established

Troubleshooting

Follow these steps to identify issues impacting the normal operation of the integration described in this document.

Validate the prerequisites

Make sure the prerequisites described in the **Summary** chapter are all satisfied:

- Check the versions of Forcepoint DLP with Forcepoint Security Manager and 3rd party products/services in use are listed as compatible

  Forcepoint DLP with Forcepoint Security Manager 8.5.x
  Amazon web services Security Hub – API schema 2018-10-08

- Verify the integration component is hosted on a Windows 10 or Windows Server machine
- User must have administrator access to the Windows machine in order to run and complete the installation successfully. Username and password will be requested at the time of install.
- The machine running the **DLPExporter** must have network connectivity to the SQL server
- Check the user has permissions to **Invoke-WebRequest** and **Expand-Archive** in Powershell

Check network connectivity

Make sure firewalls or other security appliances are not impacting the network connectivity necessary for the operation of all components involved into this integration:

- Check the windows machine has network connectivity to AWS:

  The user can check this from the logs created in **C:\fp-dlp-exporter-aws-azure-v1\logs** in the log file named **ForcepointDLPEvents**

  and check the log file has a message similar to below:

  2020-02-28 13:09:34 - DLPExporter - INFO - AWS is configured on

- Check the windows machine has network connectivity to the SQL server:

  The user can check this from the logs created in **C:\fp-dlp-exporter-aws-azure-v1\logs** in the log file named **ForcepointDLPEvents**

  and check the log file has a message similar to below:

  2020-02-28 13:06:06 - DLPExporter - INFO - Database Connection established

Check all components are configured and running properly

Make sure the products and services involved into this integration are configured as expected and they

are running:

- Check SQL connectivity: If you get messages similar to below, that means you either have no SQL connectivity or are entering wrong credentials:

  2020-02-28 13:04:21 - DLPExporter - ERROR - [08001] [Microsoft][ODBC SQL Server Driver][DBNETLIB]SQL Server does not exist or access denied. (17) (SQLDriverConnect); [08001] [Microsoft][ODBC SQL Server Driver][DBNETLIB]ConnectionOpen (Connect()). (53)
  Traceback (most recent call last):
  File "DLPExporter.py", line 135, in <module>
  KeyboardInterrupt
  [18468] Failed to execute script DLPExporter
  2020-02-28 13:09:35 - DLPExporter - ERROR - [28000] [Microsoft][ODBC SQL Server Driver][SQL Server]Login failed for user 'g'. (18456) (SQLDriverConnect); [28000] [Microsoft][ODBC SQL Server Driver][SQL Server]Login failed for user 'g'. (18456)

- In case the user provided wrong credentials for SQL server connection, you can follow the following steps:

  1. Go to C:\fp-dlp-exporter-aws-azure-v1 and edit the configs.json file to add the correct SQL Server connection credentials
  2. Go back to C:\fp-dlp-exporter-aws-azure-v1\ServiceScripts and double click on restart script. This will restart the DLPExporter
  3. Check the ForcepointDLPEVents log in C:\fp-dlp-exporter-aws-azure-v1\logs and see if the database connection is established.

- The install.bat file should only be run once. If anything goes wrong, you need to go back to the Service scripts to make changes.
- If a wrong password for the administrator account was entered during the first run of the **install.bat** file to install DLPExporter, use the following the steps to change it:

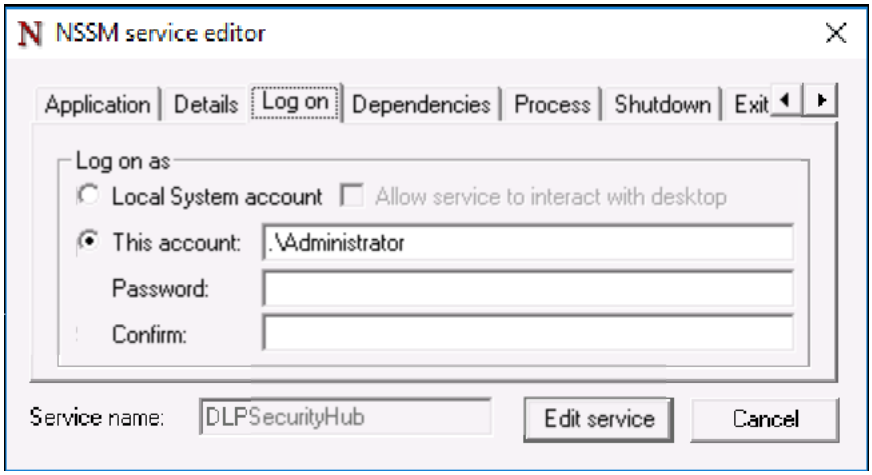
```
 Creating required directories
-----------------------------


 Creating Service: DLPExporter[0m
-----------------------------
Please enter your username: example
Please enter your administrator password: example
Service "DLPExporter" installed successfully!
Set parameter "AppDirectory" for service "DLPExporter".
Set parameter "AppStdout" for service "DLPExporter".
Set parameter "AppStderr" for service "DLPExporter".
Failed to look up the SID for username example!
LsaLookupNames(): No mapping between account names and security IDs was done.

Failed to look up the SID for username example!
LsaLookupNames(): No mapping between account names and security IDs was done.

Failed to grant the "Log on as a service" right to account example!
Error setting parameter "ObjectName" for service "DLPExporter"!
DLPExporter: START: The operation completed successfully.
Press any key to continue . . .
```

1. Go to **C:\fp-dlp-exporter-aws-azure-v1\ServiceScripts** and double click on **changePassword** script. A window will pop up where the user can enter the correct password



2. Go back to C:\fp-dlp-exporter-aws-azure-v1\ServiceScripts and double click on restart script. This will restart the DLPExporter.

- If the **install.bat** file was run multiple times, the **DLPExporter** service might still be running in the background (even if **removeService** script was run afterwards). Follow the steps below in order to remove the service completely:

1. Open the cmd prompt as administrator.
2. Go to the **C:\fp-dlp-exporter-aws-azure-v1\Resources** folder
3. Execute the command: **nssm**
4. Execute the command: **nssm stop DLPExporter**

5. Execute the command: **nssm remove DLPExporter confirm**
6. Execute the command: **nssm status DLPExporter**