Forcepoint

Email Security Cloud

Getting started with SIEM Integration

Revision A

Contents

Introduction

Administrators using Forcepoint Web Security Cloud or Forcepoint Email Security Cloud have the option to download reporting data for use by a third-party Security Information and Event Management (SIEM) solution.

Once you have enabled SIEM logging in the Forcepoint Cloud Security Gateway Portal, also referred to as the cloud portal, you can schedule a regular process to download the logs and save them to a location of your choice. Logs stored by Forcepoint are retained in the cloud service for 14 days.

Important

Standard reporting data is retained for 90 days and can be accessed through standard and custom reports; SIEM logs, once enabled, are retained for 14 days.

Follow the steps in this paper to set up and use SIEM logging. See:

1) *Setting up SIEM integration*, provides step-by-step instructions for setting up SIEM logging in the cloud portal, accessing the log files, and understanding the sample download script.

2) *Schedule log file download for Forcepoint storage*, describes the issues you must be aware of when downloading the logs, and how to schedule the download process when Forcepoint storage has been selected.

3) *File format definition for SIEM logging*, describes the contents of a log file, with examples.

If you encounter unexpected issues while setting up SIEM logging, see *Troubleshooting SIEM logging using Forcepoint storage*.

Related concepts

Schedule log file download for Forcepoint storage on page 5
File format definition for SIEM logging on page 7
Troubleshooting SIEM logging using Forcepoint storage on page 7

Related tasks

Setting up SIEM integration on page 3

Setting up SIEM integration

SIEM logging permissions are available by default. To set up SIEM logging in the cloud portal:

Steps

1) *Create a new administrator contact for Forcepoint storage*.
   We strongly recommend that the log download process has its own user name and password to gain access to the Forcepoint Web Security Cloud service. This keeps the process separate from your other administration tasks and enables you to establish longer password expiration policies.

2) *Enable SIEM logging*.

3) *Schedule log file download for Forcepoint storage*.

Related concepts
Enable SIEM logging on page 4
Schedule log file download for Forcepoint storage on page 5

Related tasks
Create a new administrator contact for Forcepoint storage on page 3

Create a new administrator contact for Forcepoint storage

To create the new contact:

Steps

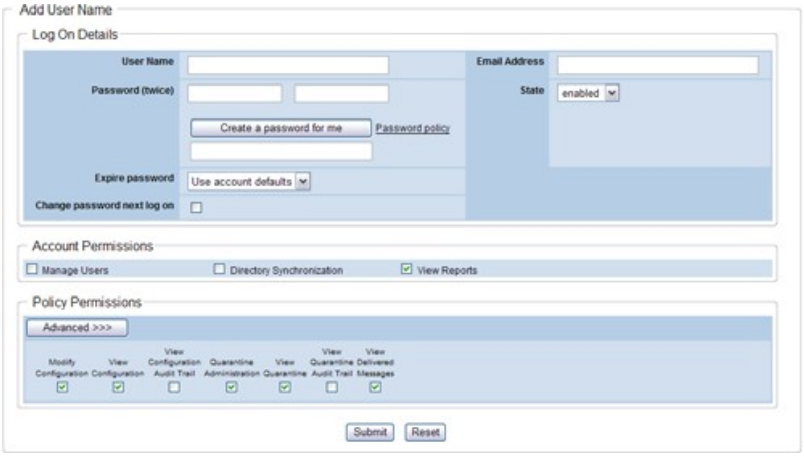
1) In the cloud portal, on the main toolbar, click **Account**, then select **Contacts**.

2) Under the Contacts list, click **Add**.

3) Enter identifying information for the new contact in the **First name** and **Surname** fields. For example, “SIEM” and “Logging.”

4) Click **Submit**.

5) Click the link provided to supply a **User name** for the account.



6) Enter a password for the contact. It must conform to the password policy on the main Contacts page.

7) Enter a password expiration date for the contact. To avoid having to regularly update it, this should be different than the regular account settings; it should span a longer period. The maximum period is 365 days.

8) Under **Account Permissions**, check the **Log Export** box, and any other permissions you want to give this user. You can act as an administrator from this logon.

Note

If you give this contact only the **Log Export** permission and nothing else, the user name and password cannot be used to log on to the cloud portal. Although log on permissions are not needed to run the download script, the **View Reports** permission is the minimum permission a user needs to be able to log on.

Minimum permissions should be given to this user. The user password is needed to run the script and is viewable in plain text. For that reason, it is recommended that this user not be one with permissions to modify reports or account policies.

9) Click **Submit**.

Enable SIEM logging

Use the **Account** > **SIEM Storage** page of the cloud portal to configure the storage options for SIEM output generated on the **Reporting** > **Account Reports** > **SIEM Integration** page. See Configuring SIEM Storage for details.

The **Reporting** > **Account Reports** > **SIEM Integration** page is used to format reporting data for use by a third-party SIEM tool and enable the generation of the log files.

Note

The option to export data cannot be set to **ON** unless a valid storage option has been configured on **Account** > **SIEM Storage**.

The option is automatically set to **OFF** if:

- **Forcepoint** storage is enabled but no logs have been downloaded for 30 days.
- **Bring your own** storage is enabled but no SIEM data could be forwarded to the active bucket for 14 days.

Multiple emails are sent prior to disabling the export option.

See Exporting data to a third-party SIEM tool in Help for details on formatting the data.

Using Bring your own storage

The output generated by the export process is forwarded to the active AWS S3 bucket listed on the SIEM Storage page. Files are assigned names using the format `web|email_<accountid>_<timestamp>_<server>_<timestamp>.csv.gz`, and will use any prefix values defined for the bucket.

Using Forcepoint storage

To get the formatted SIEM data to your network when Forcepoint storage has been selected as the Storage type on the SIEM Storage page, you can either use the sample Perl script included in the zip file linked at the top of the SIEM integration page, or create a script of your own. The account used to run this script is the one created in *Create a new administrator contact for Forcepoint storage*.

See Running the SIEM log file download script for Forcepoint Storage in Help for details on formatting the data and downloading and using the script.

Related tasks

Create a new administrator contact for Forcepoint storage on page 3

Schedule log file download for Forcepoint storage

Once you have run an initial download and determined the parameters you want to use in your script, set up a scheduled service to run automatic downloads.

We recommend that you download the log files at least once a day. To avoid periods of high network traffic, select a random time for the download (for example, somewhere between 10 and 50 minutes past the hour).

Scheduling on Windows

Before scheduling downloads from the cloud service, make sure that the Windows Task Scheduler service is started. To check this:

1) Open the Windows **Services** tool.

2) Scroll down to **Task Scheduler**.
   a) If the status is **Started**, you need do nothing.

b) Otherwise, click **Start** or **Resume** to start the service.

To schedule the log file download:

Steps

1) Open the Windows **Scheduled Tasks** tool.

2) Select **Add/Create Scheduled Task**.

3) Work through the Scheduled Task Wizard. Note that the steps involved may differ for each Windows version.
   a) The network user name and password you provide is not the user name and password you set up in the cloud portal.

   b) The following settings are required as part of Actions to successfully run the download script:
      i) Program: `<full path>\perl.exe`.

      ii) Additional Arguments: `<full path>\log_export_siem_v2_0.pl --cfgfile <full path>\log_export_siem.cfg`

      iii) Start in: enter the full path to the script.

   c) Mark the **Open the properties....** checkbox, then click **Finish**.

4) Define the task:
   a) To run as the user defined in *Create a new administrator contact for Forcepoint storage*, using the password defined for that user.

   b) To download the file to a designated local destination.

5) Click **OK**.

Related tasks
Create a new administrator contact for Forcepoint storage on page 3

Scheduling on Linux

Create a cron job to schedule your script to run at the times you want. For more information in Linux, see `man cron` and `man crontab`.

File format definition for SIEM logging

The log files downloaded from the cloud service are comma-separated value (CSV) files. Each file contains multiple lines, with one request per line.

Each line includes the reporting record attributes selected using the cloud portal. Attribute and Metric selection options are determined by the data type selected (Web Security or Email Security) and the number of columns is limited to 35 for Web Security and 25 for Email security log data.

Filters defined in the cloud portal are applied to the reporting data before it is exported.

Limitations

The following limitations apply when data is sent to a SIEM integration.

- When name changes are made to policies, custom categories, groups, or other configuration settings that have been selected for inclusion in the SIEM data, there is a short delay before the new name is included. The entity is listed as an ID number during the delay period.
- Backlog files created when processing issues occur will be processed starting with the oldest file when processing recovers.
- If the Advanced Malware Detection for Web module is used, AMD generated data is not forwarded correctly to the SIEM output.
- Encryption for AWS S3 buckets is not supported.

Troubleshooting SIEM logging using Forcepoint storage

Your download script attempts to connect to the cloud service to download SIEM logs at an interval that you configure. If your script is unable to make the connection, or if it is unable to retrieve the log files after connecting, the following problems may occur:

- The cloud service stores log files for only 14 days. After that period, the files are deleted, and cannot be recovered. When this occurs, your organization is no longer able to access and analyze web activity recorded in those logs.
- Depending on the volume of Internet activity that your organization sends through the cloud service, log files may grow quickly. If your script is unable to download log files for a day or more, the bandwidth required to download the files and the disk space required to store them may be substantial.

To address this issue:

- Check that your scheduling service (**Windows Task Scheduler**, or **crontab** on Linux) is running. If you are using **Windows Task Scheduler**, check that it is using your most recent network password to run the task.
- Your script may be prevented from accessing the cloud service due to network problems, either affecting Internet or internal network connections. Use a browser or the ping utility to verify that the machine running the script can connect to the Internet.
- If the script is connecting to the cloud service but cannot retrieve log records, verify that there is not a problem with the cloud service. Check the administrative email address associated with your SIEM logging account.
- Check that your cloud service password has not expired.

If you do not download logs for a period of 7 days, an email is sent to all administrative contacts with Log Export permission enabled, and all policy administrators where full traffic logging is enabled for the policy, notifying them that data has not yet been downloaded. At 13 days, a different email warns that data may be lost; it is deleted at 14 days. Further notifications are sent after 21 days to warn that the process will be disabled if not used. After 30 days you will be notified that SIEM logging has been deactivated and reporting logs are no longer being generated for your account.

Published 14 February 2024