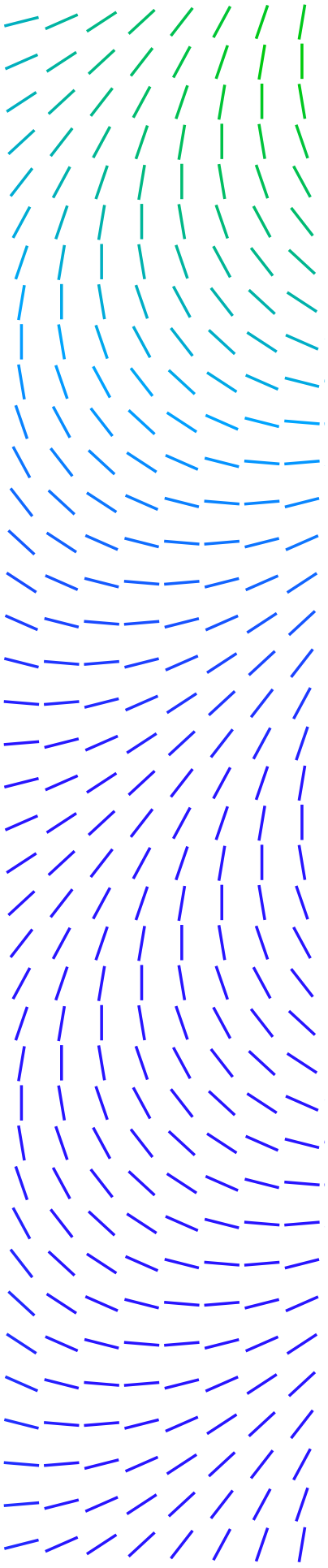
USER GUIDE



Getting Started with Trellix and Amazon Security Lake

Trellix

Table of Contents

Introduction

Amazon Security Lake

Amazon Security Lake is a data lake for security logs, built in the customer's account. It's backed by an Amazon S3 bucket and organizes data as a set of Lake Formation tables. Amazon Security Lake is designed to optimize the cost of storing and querying massive security log sources, while maintaining good query performance and compatibility with a wide variety of analytic infrastructure. Amazon Security Lake customers retain low-level ownership of their data. Amazon Security Lake also delivers of a set of core AWS- native security logs, minimizing costs and maximizing performance.

How the integration works using Trellix XDR

As an open platform that seamless integrates across hundreds of solutions, the Trellix integration with Amazon Security Lake allows customers to easily connect data across their organization and share insights across differing vendor products more cost effectively.

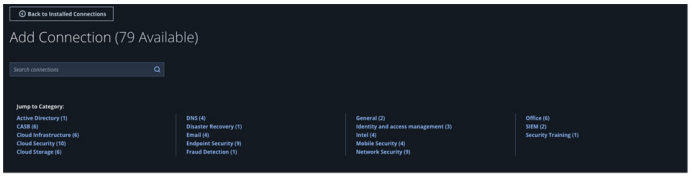
Customers can augment their Amazon Security Lake with the 1000+ sources of security events in Trellix XDR, getting complete detection and response capabilities for their AWS environments by correlating the risks and providing customers with the necessary playbooks to respond to a risk in a timely manner.

Trellix Helix Integration with Amazon Security Lake

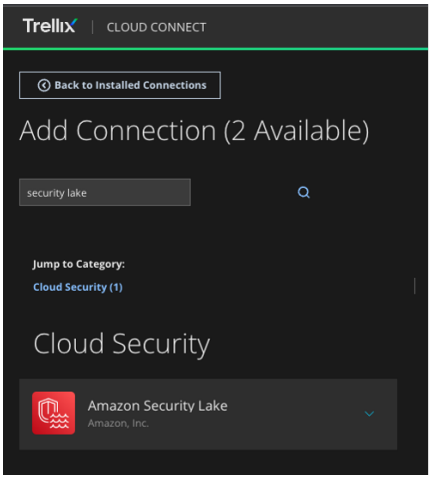
How to Enable Trellix Helix Integration with Amazon Security Lake in Minutes

Navigate to the Trellix Helix Cloud Connect portal:

1. Select **Configure > Cloud Connect** to open the Cloud Connect page.
2. Click **Add Connection**.
3. Locate the connection under **Cloud Security**



   - **As a subscriber:** Select **Amazon Security Lake Tile under Cloud Security**



This Trellix integration will forward any files found in a given (Amazon Security Lake) S3 bucket to Trellix Helix. You can restrict which files are sent by setting the optional prefix filter below. To install:

1. Ensure that the correct Helix instance is selected in the drop-down.
2. Log into your AWS account (https://console.aws.amazon.com) in a different browser tab.
3. In the region you want to subscribe to Trellix XDR, go to the AWS SNS Console and create a topic named "trellix-xdr". The topic can be standard (not FIFO).
4. Click the "Create topic" button and copy the ARN of this topic and paste it in the form below in Cloud Connect under the "SNS topic" field.
5. In Trellix Helix Cloud Connect portal, enter "Amazon Security Lake" in the search bar and choose the entry under the "Cloud Security" category.

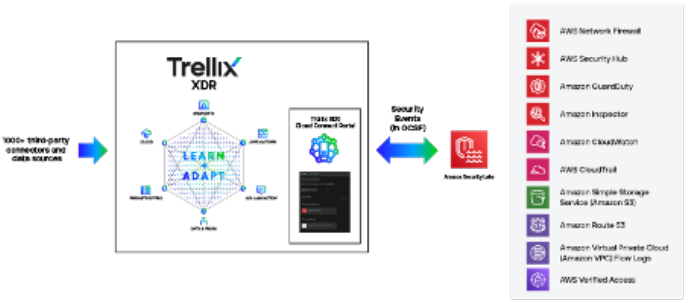
6. In the other browser tab, go to the Amazon Security Lake console and click the "Regions" menu item.
7. For each region listed, you will need to create this Trellix integration in Cloud Connect. You may choose to create a rollup region and use just that region.
8. In the Amazon Security Lake console for this region, find the corresponding bucket name and enter it in the "AWS bucket to monitor" field in Cloud Connect, along with the region in the "AWS region name" field.
9. In the Amazon Security Lake console, click on "Subscribers," then click the "Create subscriber" button.
10. Enter "Trellix" as the Subscriber name.
11. Enter "Trellix XDR" as the description.
12. Choose all or specific log sources.
13. Choose "S3" as the data access method.
14. Under "Subscriber credentials" enter 264756907367 as the Account ID. Enter the unique external ID generated in the instructions in the form below for the external ID in the Amazon Security Lake Console.
15. Under "Notification details" choose "Subscription endpoint" and enter the SNS topic ARN you created earlier as the Subscription endpoint.
16. Click "Create" in the Amazon Security Lake Console.
17. In the Amazon Security Lake console list of subscribers, click on the newly-created subscriber. Copy the AWS role ID and paste it in the Cloud Connect field for "S3 Access Role."
18. Click "Submit" in Cloud Connect below, and the integration setup will generate a CloudFormation template. The CloudFormation template adds necessary permissions for Trellix to subscribe to the SNS topic and for AWS EventBridge to publish to the SNS topic. Run that template in the same AWS account and region, and the setup will be complete.

Troubleshooting

Ensure the CloudFormation template executes successfully. It is valid for 24 hours after being created.

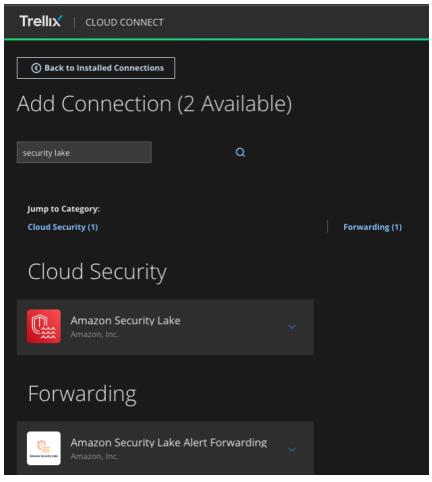
You can use the Helix Cloud Connect console to view integration status, including latest event times.

How to use Trellix as a Source

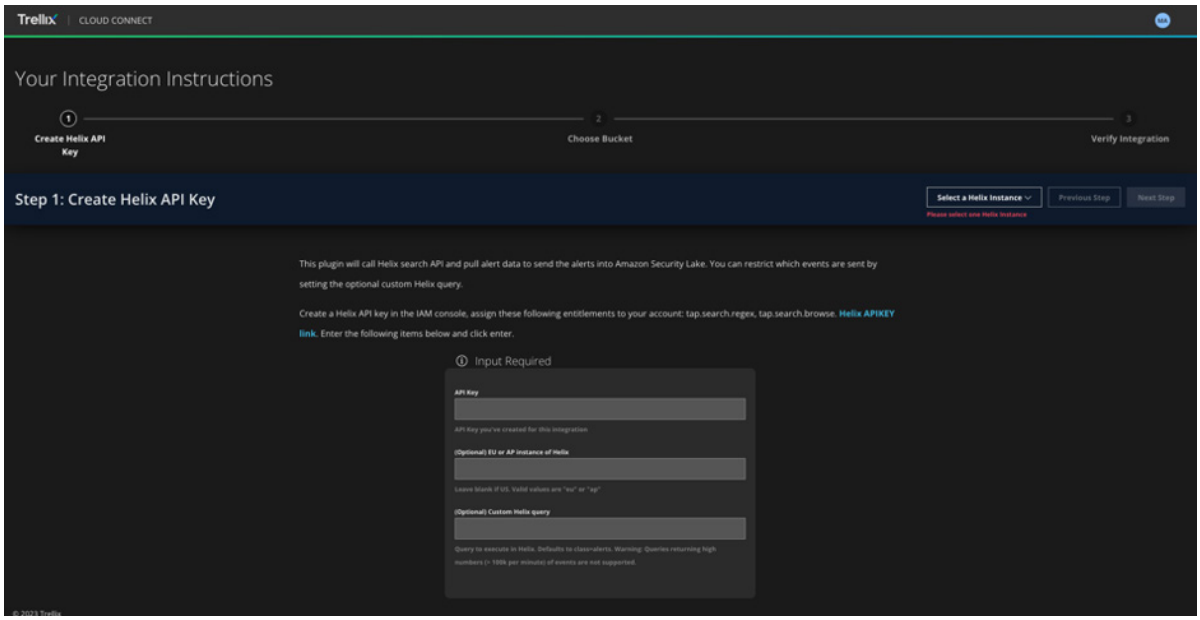


As a Source (to send security events from Trellix XDR into Amazon Security Lake): Select Amazon Security Lake Alert Forwarding

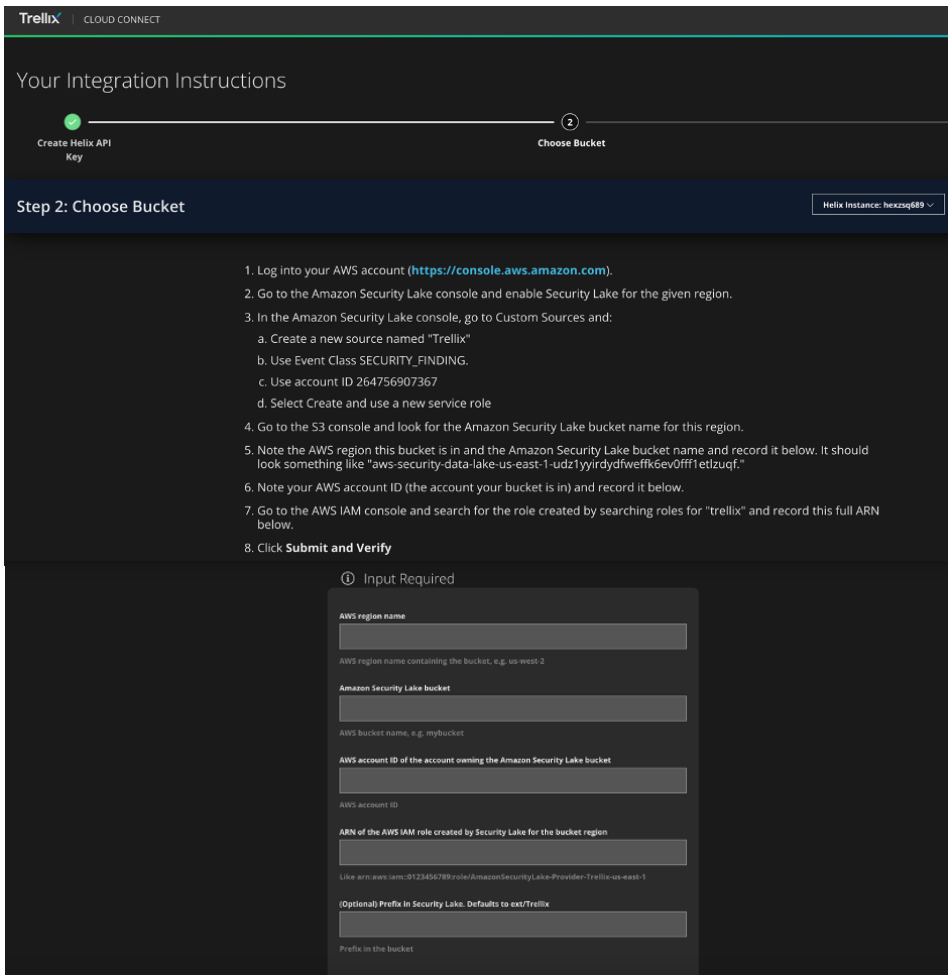
1. Select **Configure > Cloud Connect** to open the Cloud Connect page.
2. Click **Add Connection**.
3. Locate the connection under **Cloud Security**
4. Click on the **Amazon Security Lake Alert Forwarding Tile**



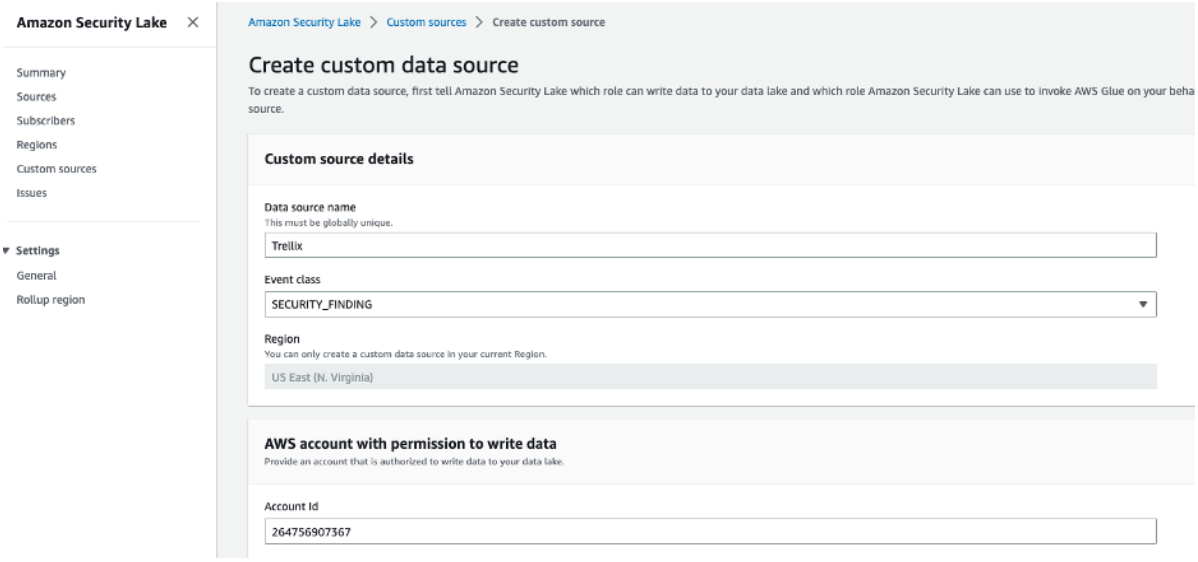
You will see Helix authentication configuration screen.



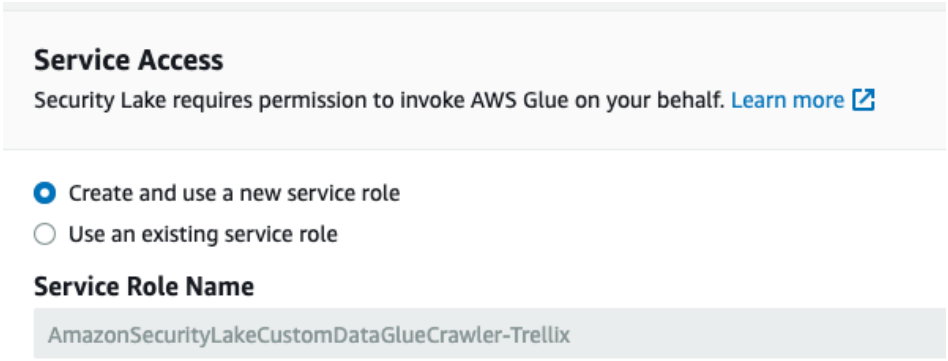
5. Configure Amazon Security Bucket Lake S3 bucket location



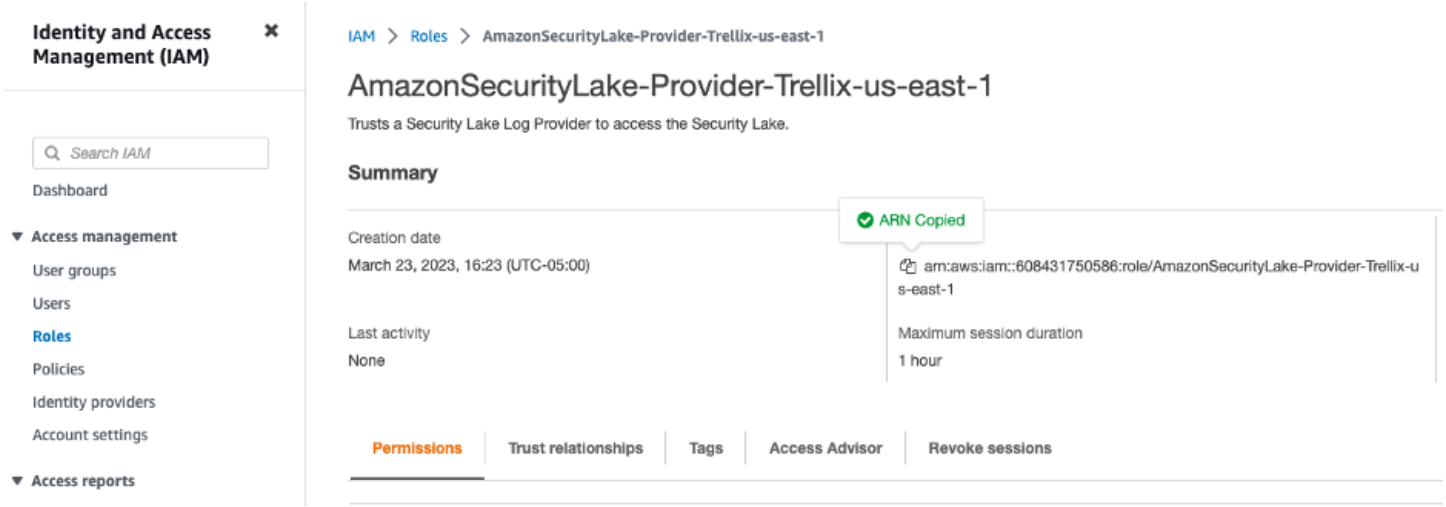
6. Go to Amazon Security Lake console and Create custom source
7. Add Trellix info and set event class to SECURITY_FINDING



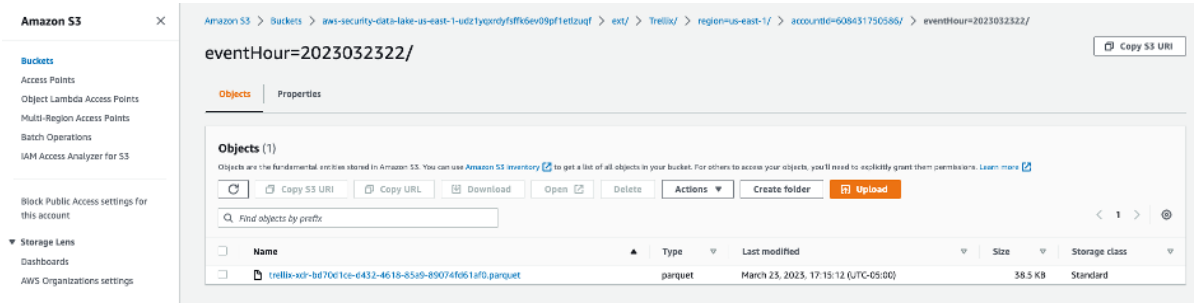
8. Create and use a new service role



9. Find AWS IAM role created by the Amazon Security Lake console



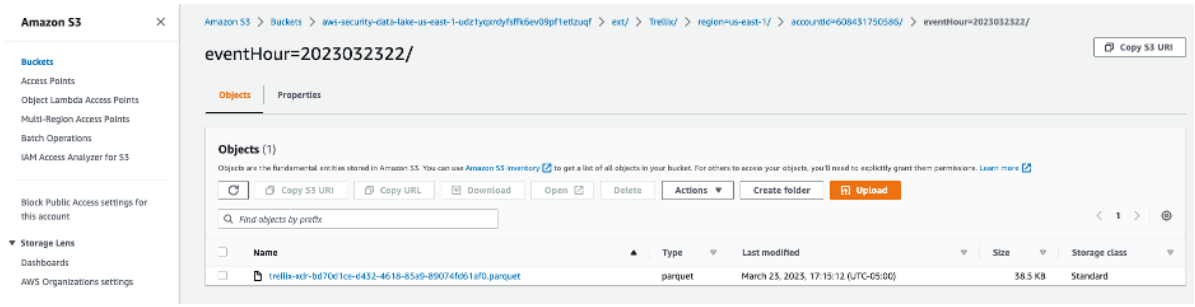
Events in Security Lake



Example fields from a Trellix finding:


```
{
  "activity_id": 1,
  "activity_name": "Generate",
  "category_name": "Findings",
  "category_uid": 2,
  "class_name": "Security Finding",
  "class_uid": 2001,
  "confidence": 100,
  "data": "{\"__metadata__\": {\"customer_id\": \"foo\"}}",
  "message": null,
  "severity": null,
  "severity_id": null,
  "status": null,
  "status_id": -1,
  "state": null,
  "state_id": 1,
  "time": null,
  "timezone_offset": 0,
  "type_name": "Security Finding: Generate",
  "type_uid": 200101,
  "metadata": {
    "logged_time": -2208988800.0,
    "original_time": null,
    "labels": [],
    "product": {
      "lang": "en",
      "name": "Trellix XDR",
      "uid": "trellix_xdr",
      "feature": {
        "uid": null,
        "name": "XDR"
      },
      "vendor_name": "Trellix",
      "version": "1.0.0"
    },
    "profiles": []
  },
  "finding": {
    "title": null,
    "uid": "26c7c83d-0aad-411b-88ee-52343ff22064",
    "types": [],
    "src_url": "https://apps.fireeye.com/helix/id/foo/alerts/None",
    "remediation": {
      "desc": "If this IP address is tied to your network via any observables attached to this event, take immediate steps to find the related device on your network and remove the infection seen from external threat intelligence",
      "kb_articles": null
    },
    "product_uid": "ssc_malware_dns_sinkhole",
    "last_seen_time": 1668535199948,
    "desc": null
  },
  "resources": [],
  "observables": []
}
```


Example objects saved to S3:



OCSF Maintenance

Trellix will handle the OSCF maintenance on behalf of the customer.

Basic Troubleshooting

Ensure the CloudFormation template executes successfully. It is valid for 24 hours after being created.

You can use the Helix Cloud Connect console to view integration status, including latest event times.

Trellix Customer Support Process

You can request assistance from Trellix Customer Support directly from Trellix Helix. To use this feature, you can click the Chat icon at the top-right of any Helix page and select **Customer Support**. A chat window will open and connect you directly to a Trellix customer support engineer.

Trellix Support

Trellix Product Documentation

Trellix Product Documentation