Trellix

Trellix and AWS Verified Access

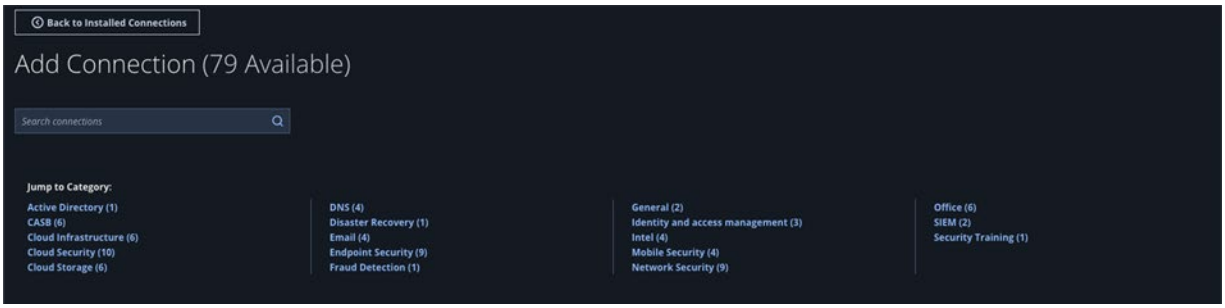
Trellix supports AWS Verified Access provides visibility into a customer's per application configurations to see when policies are set and changed. This makes it incredibly easy for SOC analysts to correlate security threats seen across their ecosystem with key configuration settings and changes in a customer's AWS environment and can help provide crucial and timely information for a customer's Zero Trust architecture.

Trellix Helix integrates metadata from AWS Verified Access to enable customers greater visibility across their AWS infrastructure. Integrating Verified Access and Trellix helps assist analysts with security investigation, such as correlating a compromised endpoint to a user whose credentials might have been compromised and could affect their AWS accounts.

How to Enable Trellix Helix Integration with AWS Verified Access

Navigate to the Trellix Helix CloudConnect portal:

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



Select AWS Verified Access Tile listed under Cloud Security

Click the arrow to expand the connection information.

- Select View Install (see below) Steps or click Print Installation Steps to see a summary of the steps you must perform to install the integration. Click Exit Preview Mode when you are ready to begin the installation.

- Select Install to open a wizard that guides you through the installation.

Integration Steps

This Helix integration will forward any files found in a given (AWS Access Verified) bucket to Helix. You can restrict which files are sent by setting the optional prefix filter below.

1. Ensure that the correct Helix instance is selected in the drop-down.
2. Log into your AWS account (https://console.aws.amazon.com).
3. Go to the S3 console and look for the (AWS Access Verified) bucket name that you want to send into Helix.
4. Note the AWS region this bucket is in and the AWS Access Verified bucket name, and record it below.
5. Click **Submit and Verify**, which will generate a Cloudformation template for you.
6. **IMPORTANT!!!** If there is an existing notification configuration on the bucket, the template will fail unless you set OverwriteExistingConfig to 1. This will remove the existing configuration, so ensure that is acceptable first.

Regular Expression matches are against full S3 file path (excluding Access Verified). You can add multiple line separated regular expressions.
Example Regular Expressions (only one of the Allow or Deny is allowed)
^.*very_useful_log.*$ - Matches file paths containing very_useful_log
^.*useful_log|very_useful_log.*$ - Matches file paths containing useful_log or very_useful_log
^.*tar\.gz$ - Matches only tar.gz extensions

Trouble Shooting

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.

Helix Customer Support Chat

You can request assistance from Trellix Customer Support directly from 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 Customer Support

Documentation:

Helix Documentation