FORESCOUT

Forescout

Forescout Data Source Onboarding Guide - For Government

Contact Information

Forescout Technologies, Inc.
2400 Dallas Pkwy, Suite 230, Plano, TX 75093
https://www.forescout.com/support-hub/
Toll-Free (US): 1-866-377-8773
Tel (Intl): 1-708-237-6591

About the Documentation

- Refer to the Documentation Portal for additional technical documentation: https://docs.forescout.com/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

Table of Contents

Forescout Data Source Onboarding Overview

The Forescout Data Source Onboarding Guide provides information on Data Source device configuration and data telemetry onboarding for both customer environments and the Forescout Cloud product.

> **CAUTION:**
> This reference is frequently updated but may not reflect the latest information about the configuration of third-party (non-Forescout) hardware and software devices. Always ensure that you are using the latest vendor documentation for your specific product and product version when performing configuration procedures.

Intended Audience: Security Engineers.

Connector Note: This configuration reference assumes the Forescout Cloud Connector you will be using has been provisioned and deployed either on-premises or hosted by Forescout. If you are unsure whether or not the Connector for the Data Source you are adding has been deployed, contact your Forescout sales representative. For detailed information about Connector provisioning and configuration, see the Forescout Cloud Connector Deployment and Configuration Guide.

What is a Forescout Data Source?

A Data Source is any customer entity that sends data to Forescout Cloud, which typically consists of logged event data. For simplicity's sake, an entity that acts as a source or provider of logs shall be referred to in this guide as a device. This could be a server, a network appliance, a cloud service or an endpoint. Examples of functions of devices that can act as a Data Source for Forescout Cloud include the following:

- Endpoint Security & EDR
- Email Security
- Network Security
- Cloud Services
- Infrastructure & Authentication
- Enrichment Solutions
- Application Logs
- Other Log Sources

When the customer-side Data Source device and Forescout Cloud are correctly configured so that the device's targeted data logs can be retrieved and filtered (ingested) by Forescout Cloud, the resulting actionable intelligence is referred to as **Telemetry**.

What is a Forescout Cloud Connector?

A Forescout Data Source Connector is a small utility that establishes a secure connection between a Data Source and Forescout Cloud for the purpose of ingesting raw log data. A Connector can be deployed on-premise at the customer site or it can be hosted by Forescout. The Connector deployment environment, combined with the nature of the Data Source device or service itself, determines the transport configuration settings for the successful ingestion of log files. This manual assumes the Connector you will be using has been provisioned and deployed either on-premise or hosted by Forescout. If you are unsure whether or not the Connector for the Data Source you are adding has been deployed, contact your Forescout sales representative.

For detailed information about Connector provisioning and configuration, see the Forescout Cloud Connector Deployment and Configuration Guide.

What is Loggify?

Loggify is a filtering tool that Forescout developed to transform Data Source log records after they have been ingested into the platform. Loggify parses, cleans, normalizes, and enriches raw logs. It is a critical process that empowers Forescout's Threat Detection Engine to automatically extract Suspicious Entities that pose or expose a potential cybersecurity risk. You may see reference to Loggify in this documentation but there is no need for customers to configure the tool in any way.

How to successfully onboard a Forescout eyeAlert Data Source

To retrieve logs from a source of data that you want Forescout eyeAlert to use in threat detection and management, you need to clearly understand the type of product you have and the method Forescout eyeAlert uses to successfully process the information it receives.

Successful log ingestion requires the completion of the following high-level steps:

1. Find the vendor of the Data Source product you are onboarding in the Data Source Product Index.

2. Find the reference page for your specific Data Source product, and note which method Forescout eyeAlert uses to ingest logs (Push or Pull).

3. Configure your Data Source product as instructed by its specific reference page. When available, the reference page for your product suggests vendor online documentation sites that you can use to guide configuration.

4. Configure Forescout eyeAlert to receive (Push) or retrieve (Pull) targeted logs for ingestion.

The following topics explain the onboarding process. If this is the first time you are onboarding a data source, be sure to read all of the topics below in their entirety.

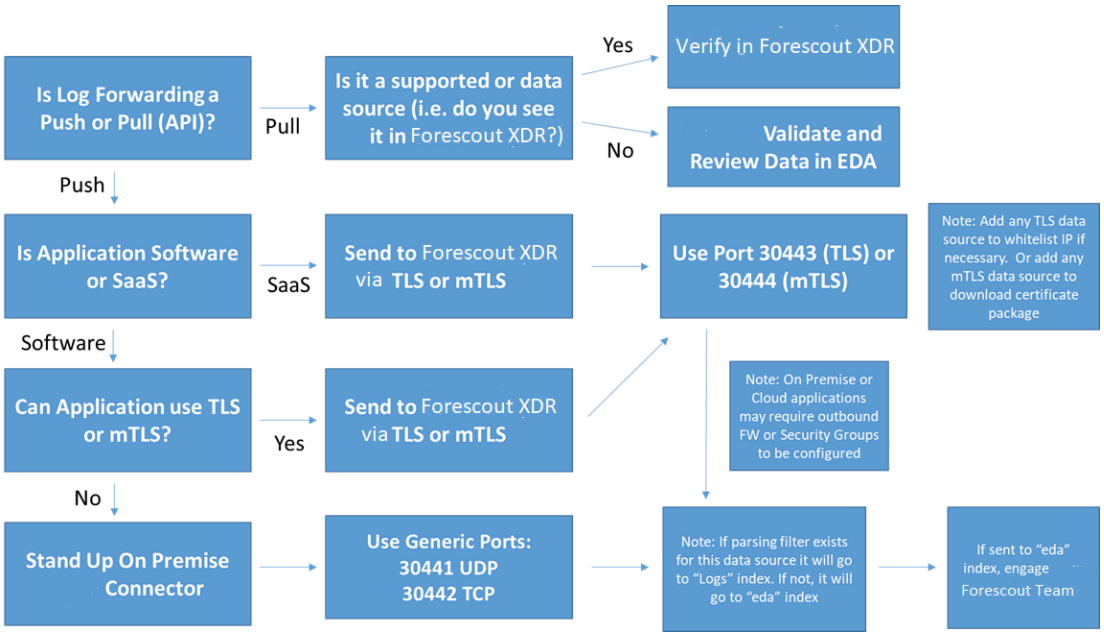
- Forescout Data Source Onboarding Decision Quick Reference
  Note:
  The Quick Reference is a snapshot of the various decision points that flow towards the successful onboarding of logs from a Data Source product. This reference is a useful key for pinpointing the type of log retrieval that must be used for your particular Data Source, but only the page specific to your product in the Data Source Vendor and Product Index provides details that are unique to your product. In addition, more detailed guidance is often necessary (especially for Pull-based Data Source log retrieval).
- The First Question to Answer - Push or Pull?
- Push-based Data Source Onboarding
- Pull-based Data Source Onboarding

Forescout Data Source Onboarding Decision Quick Reference

The Connector deployment environment, combined with the nature of the Data Source device or service itself, determines the transport configuration settings for the successful ingestion of log files. For example, is the Connector deployment environment on-premises or is it a cloud-based SAAS service? Is the Data Source an application software product that supports TLS and can send to a hosted Forescout eyeAlert Connector? The answers to these questions determine the required configurations for successful log ingestion.

The flow chart below provides a general mapping of the decisions you must make about the characteristics of your Data Source product to ensure successful onboarding of raw logs. We recommend that all Forescout eyeAlert users review this quick reference. For those who have a lot of confidence with how to configure their product and Forescout eyeAlert, the quick reference below may be all that you need to configure a Push-based Data Source.

For those who are not sure about configuring their Data Source and/or the Forescout eyeAlert UI, we recommend that you read the following topic: The First Question to Answer - Push or Pull?.



The First Question to Answer - Push or Pull?

Once you have found the reference page for your specific Data Source product in the Data Source Product Index, the first question to answer is which method Forescout eyeAlert uses to ingest logs - Push or Pull. This topic explains the two types of log ingestion.

Push-based Data Sources

Push-based Data Source logs are forwarded from the customer's network or cloud environment to a Forescout-hosted or on-premise Connector over a pre-defined port. Push-based data sources do not require custom security and authentication configuration on the Connector side, but the transport protocol selection and configuration does depend on whether the Connector deployment environment is on-premise or hosted. The following are a few examples of Push-based Data Sources:

- Deep Security

- Deep Discovery Inspector/Analyzer
- Apex Central

Pull-based Data Sources

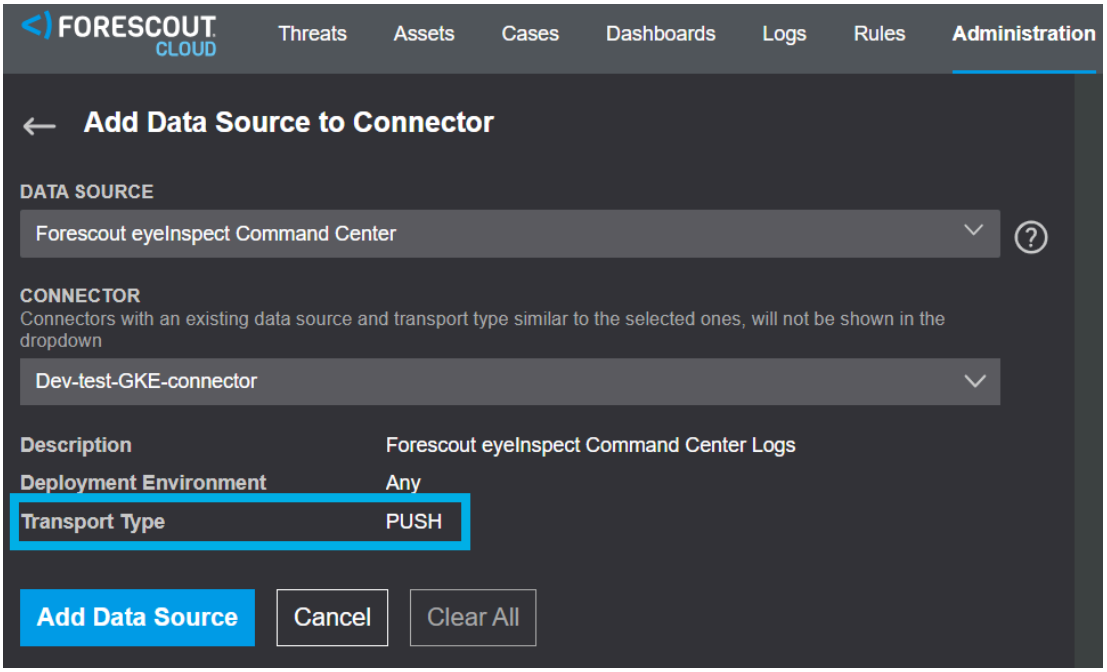
Pull-based Data Source logs are retrieved from the customer's network or cloud environment by a custom-designed application (typically called a "puller") deployed on a Forescout-hosted or on-premise Connector. The Connector uses the puller application to actively connect to a customer device or cloud environment and continuously or periodically retrieve data. As such, pull-based Data Sources require the configuration of authentication and connection parameters that are unique to each vendor and/or device (e.g., username/password, server URL, connection string, etc.). The following are examples of Forescout eyeAlert Pull-based Data Sources:

- Salesforce
- Active Directory Entities
- Google Pubsub

How to Determine which Log Retrieval Method the Data Source Supports

The fastest way to determine whether the Data Source you are onboarding uses the Push method or the Pull method is to reference the specific page for your Data Source product in the Data Source Product Index.

Another method is to go to the Forescout eyeAlert UI, click **Administration** > **Data Sources** > **+ Add Data Source**, select your Data Source from the **Data Source** dropdown, and look at the displayed "Transport Type" as shown below.



For detailed Push-based Data Source onboarding guidance, click here.

For detailed Pull-based Data Source onboarding guidance, click here.

Push-based Data Source Onboarding

Push-based Data Source log retrieval is actually very straightforward if you understand the product type you are onboarding, the transport protocols it supports, and the log format Forescout eyeAlert requires for successful processing. Log transport to Forescout eyeAlert must be secure and/or encrypted to ensure security, regardless of the product type you are using.

Use the Specific Reference Page for your Data Source Product

All Push-based Data Source devices supported by Forescout eyeAlert have a specific reference page in the Data Source Product Index. Find the reference page and take note of the following: targeted logs, the preferred log format, available sources of vendor information and final configuration instructions to help you configure your product.

- **Suggested Information Sources**: Provides links to suggested information sources - typically a Vendor documentation portal or customer resource center - so that you can find specific instructions about configuring your Data Source product using the specified reference information.
- **Targeted Logs**: Specifies the log types that Forescout eyeAlert targets for ingestion.
- **Preferred Log Format**: This is key - to successfully process logs, Forescout specifies a particular log format which is typically CEF. If no format information is present, configure Syslog as the log format.
- **Forescout eyeAlert Configuration Procedure**: Links you to the procedure to configure Forescout TDR to receive the Pushed Data Source logs.

What Transport Protocols Does Your Data Source Product Support? Is it SaaS or On-Premises?

All log transfers to Forescout eyeAlert must be encrypted unless they are directed via UDP and TCP to specific ports on an on-premises Forescout eyeAlert Connector.

When your Data Source product is a **SAAS service**, it will always send logs to a hosted Forescout eyeAlert connector via the TLS or mTLS protocols. Data Source SAAS products never use UDP or TCP to forward logs to Forescout eyeAlert. In terms of SAAS products, very few support mTLS, so in most cases a SAAS product will send logs to Forescout eyeAlert in the specified format over TLS. The use of TLS requires that you "allow-list" the incoming IP (the source IP for the logs that are being sent) when you configure Forescout eyeAlert to receive the logs. Allow-listing is not required if your SAAS product supports mTLS.

When your Data Source Product is an **on-premises application**, it must send logs to specific ports via UDP and TCP. The TLS protocol is preferred, but is only valid if logs are sent to a hosted connector. Logs are never sent to a on-premises Connector using the TLS protocol. The use of TLS requires that you "allow-list" the incoming IP (the source IP for the logs that are being sent) when you configure Forescout eyeAlert to receive the logs.

Many on-premises applications do not support the TLS protocol or can't send logs to a hosted connector via TLS. In such cases, logs are received by Forescout eyeAlert over UDP or TCP on specific ports.

Configure Your Data Source to Push to an On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)

When you have finished reviewing the specific reference page for your Data Source product in the Data Source Product Index, configure your product to forward logs to the ports specified below. The index with note any unique configurations for both Hosted or On-Premises connectors on the specific page for your Data Source product.

On Premise-Connector Deployments

- If you are using TCP, push the data logs to Forescout eyeAlert Network port 30442.
- If you are using UDP, push the data logs to Forescout eyeAlert Network port 30441.

No further required configuration is required in the Forescout eyeAlert UI. Once the device begins sending logs in the specified format to the ports specified above, the Data Source and its data log ingestion statistics should appear in the "Discovered" category on the Data Sources screen under the Forescout eyeAlert **Administration** tab.

Hosted Connector Deployments

For hosted Connector deployments:

- If you are using TLS, push the data logs to Forescout eyeAlert Network port 30443.
- If you are using mTLS, push the data logs to Forescout eyeAlert Network port 30444.

When you are finished configuring your Push-based Data Source, if you are using a connector hosted by Forescout eyeAlert click here to configure Forescout eyeAlert to receive the logs.

Pull-based Data Source Onboarding

Due to the dynamic nature of Pull-based Data Source configuration, the steps required to successfully onboard logs can vary between specific vendor, specific product, and the requirements of the Forescout eyeAlert "Puller" application that has been specifically designed to receive the logs. You have been provided with the best possible available information to configure your pull-based Data Source in small configuration manuals that are specific to the product you want to onboard.

Find your vendor and product in the Data Source Product Index and follow the provided instructions while referencing the product configuration documentation that has been provided by your vendor.

The manual for your Data Source uses the best available information at the time of writing to configure your product. It provides specific configuration information needed to configure the Forescout eyeAlert "Puller" that has been specifically designed for your product (often interfacing with a product API).

Configuring Forescout eyeAlert to Receive Logs Pushed to a Hosted Connector

Complete this procedure to configure Forescout eyeAlert to receive logs pushed to a Hosted Connector after all prerequisites have been completed.

1. On the **Configurations** panel, use the **TRANSPORT SECURITY PROTOCOL** drop-down to select the transport security protocol for the Data Source.
    - TLS (default port 30443)
    - mTSL (default port 30444)
2. Enter the appropriate port number in the **PORT** field (the default port value will appear by default).
3. If the selected transport security protocol is TLS, in the **CIDR ALLOW-LIST** field enter a comma-separated list of the source IPs and/or CIDR ranges of the sending device(s) – for example: 1.2.3.4/32.
4. Select the preferred **TIME ZONE** from the dropdown.
5. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
6. Click the **Download Server Certificate** (TLS) or **Download Certificate Bundle** (mTLS) button.

    Note:

    Client Certificate Installation -

    If mTLS is the selected communication protocol, ensure that you install the Client Certificate appropriately as described by the vendor documentation for the Data Source.

    Note:
    Server Certificates expire after three years from the day of the initial configuration. As the three-year point from initial configuration approaches, ensure that you complete this procedure to renew the Client Certificate before it expires to ensure no interruption to log ingestion.
7. On the **Add Data Source to Connector** panel, click **Apply**.
    The UI will indicate whether the deployment has been successful.

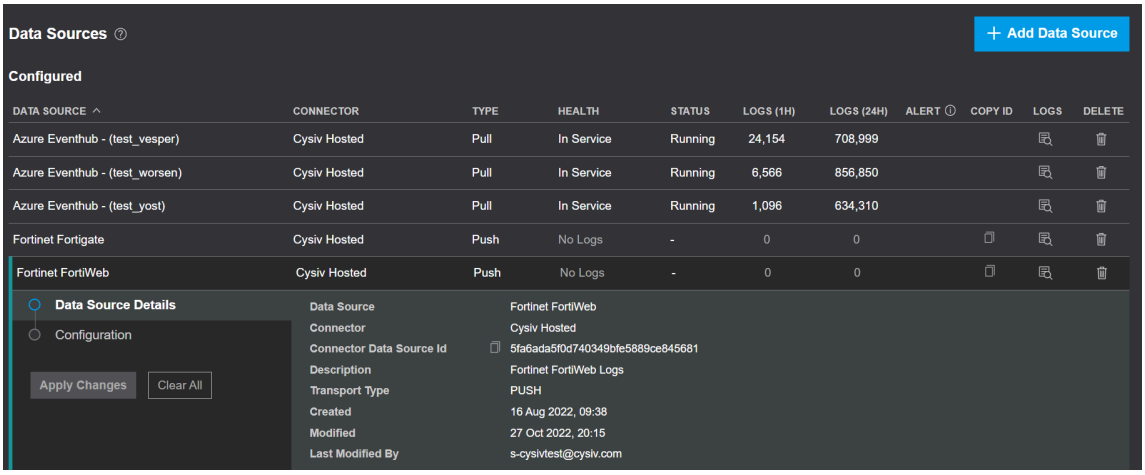
Data Source Server Certificate Expiry and Replacement

Push-based Data Sources that use a hosted Connector have a Client Certificate that is downloaded during the initial ingestion configuration procedure. The Client Certificate is only valid for three years from the day of the initial configuration. If the client certificate expires, logs will stop being ingested.

To renew a client certificate for Push-based Data Sources that use a hosted Connector, complete the following procedure:

1. Log in to Forescout eyeAlert and select **Data Sources** from the **Administration** menu.

2. Locate the Data Source you are updating in the list of **Configured Data Sources** and click on it.



3. Click **Configuration.**
4. Click the **Download Certificate Bundle** button.
5. Extract and install the Client Certificate as required and described by the applicable vendor documentation for the Data Source you are renewing.

Data Source Product Index

The Data Source Product Vendor Index is the source that specifically pinpoints the information you need to send logs from a Data Source product to Forescout eyeAlert and have them successfully processed. The index is organized by vendor and product based on ingestion method, as follows:

Push- and Pull-based Data Source Product Vendors

This section of the index organizes push-based Data Sources by vendor and product. Select your Data Source vendor below:

1password

This manual is under construction.

Abnormal Security

Abnormal Security™ provides protection against attacks that target human behavior, including socially-engineered threats, vendor fraud, and cloud account takeovers.

To add Abnormal Security to Forescout eyeAlert as a Data Source, use the following settings when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source.

Key Data Source Product Configuration and Authentication Requirements

To onboard logs from this Data Source, you will need to have the following credential information on-hand when configuring Forescout eyeAlert:

- API URL
- Authentication Token

Suggested Information Sources for Data Source Product Configuration

Abnormal Security provides a knowledgebase here.

Note:
The reference links above are suggestions only. To ensure accuracy, be sure to use the latest official documentation provided by the vendor of your Data Source product type and version.

Target Data Logs

Forescout currently targets Hosts logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON format when configuring your Data Source to make logs available for ingestion by Forescout eyeAlert.

Configure Forescout eyeAlert to Retrieve the Data Source Logs

See Configuring Forescout eyeAlert to Receive Abnormal Security Logs.

Note:

When you have finished configuring Forescout eyeAlert and the Data Source has been successfully integrated you can use the API access token to send requests to the Abnormal API from any HTTP client.

For details on each Abnormal REST API endpoint, see the Abnormal API documentation in SwaggerHub. SwaggerHub lists and describes all available Abnormal API endpoints, and enables you to test API calls to each endpoint.

To generate the cURL commands associated with the endpoints you would like to use, you must add SwaggerHub IPs to the IP Safelist, as outlined by the vendor documentation. For a full list of SwaggerHub IP addresses, see SwaggerHub IP Addresses.

Configuring Forescout eyeAlert to Receive Abnormal Security Logs

Data Source Name – Abnormal Security

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > + Add Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the API URL.
2. Enter the Authentication Token.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is *21600* (6 hours).
4. Enter a value in seconds into the No Flow Alert Threshold field. The value determines how long the system will wait before alerting on absence of logs.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as *2592000*.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. Click the **Add Data Source** button.

The UI will indicate whether the deployment has been successful.

Absolute

This series of topics presents Data Source products provided by Absolute Software™, as follows:

Absolute SIEM Connector (Push)

Absolute SIEM Connector (Push)

Absolute SIEM Connector collects logged events from multiple software programs and store them in a central repository for consolidated reporting and analysis. Organizations can then monitor security events across their system for incident response, forensics, and regulatory compliance.

To add Adobe Experience Manager to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Adobe provides a public documentation portal here.

Target Data Logs

Forescout currently processes Firewall Traffic Reports.

- AEM Java logs
- HTTP Request logs
- HTTP Access logs
- Apache HTTPD Web Server Access logs
- Apache HTTPD Web Server Error Logs
- Dispatcher Logs

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Admin by Request

Admin By Request provides end users a way to request administrator access for their currently logged in user account.

To add Admin by Request™ to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Pull mechanism and the Admin by Request API to ingest logs.

Key Data Source Product Configuration and Authentication Requirements

To onboard logs from this Data Source, you will need to have the following credential information on-hand when configuring Forescout eyeAlert:

- API URL
- API Key

Suggested Information Sources for Data Source Product Configuration

Admin by Request provides a resource center here.

Admin by Request provides an API overview here.

Note:
The reference links above are suggestions only. To ensure accuracy, confirm that you are using the latest official documentation provided by the vendor of your Data Source product.

Target Data Logs

Forescout currently targets the following log types for ingestion:

- Inventory
- Audit
- System

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON format when configuring your Data Source to make logs available for ingestion by Forescout eyeAlert.

Configure Forescout eyeAlert to Retrieve the Data Source Logs

See Configuring Forescout eyeAlert to Receive Admin by Request Logs.

Configuring Forescout eyeAlert to Receive Admin by Request Logs

Data Source Name – Admin by Request

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > + Add Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the API URL.
2. Enter the API Key.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is *86400* (24 hours).
4. Enter a value in seconds into the No Flow Alert Threshold field. The value determines how long the system will wait before alerting on absence of logs. The default is 129600 seconds.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 15 days expressed in seconds as *1296000*.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. Click the **Add Data Source** button.

The UI will indicate whether the deployment has been successful.

Adobe

This series of topics presents supported Data Source products provided by Adobe™, as follows:

Adobe Experience Manager

Adobe Experience Manager

Adobe™ Experience Manager™ (AEM) is a comprehensive content management solution for building websites, mobile apps, and forms.

This manual is under construction.

Aiven

This series of topics covers all Data Source products offered by Aiven™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Aiven Elasticsearch (Pull)

Aiven Elasticsearch (Push)

Aiven™ Elasticsearch™ is a proprietary Data Source based on the open source Elasticsearch. To add Aiven Elasticsearch to Forescout eyeAlert as a Data Source, ensure you use the following settings when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Aiven provides a user documentation portal here.

Target Data Logs

Forescout currently processes Firewall Traffic Reports.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Akamai

This series of topics covers all products offered by Akamai™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Akamai Datastream (Push)

Akamai Technologies, Inc. is a content delivery network (CDN), cybersecurity, and cloud service company, providing web and Internet security services. To add Akamai DataStream to Forescout eyeAlert as a Data Source, complete the following tasks:

To add Amazon GuardDuty to Forescout eyeAlert as a Data Source, consult your vendor documentation to ensure the following settings are used:

Log Retrieval Method

Push the logs to an AWS S3 bucket. Then pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic in the *Forescout Cloud Connector Configuration Guide*.

Instructions and/or Suggested Information Sources

Akamai provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

When the logs have been successfully pushed to the S3 Bucket, pull the logs into Forescout TDR from the S3 Bucket by referencing this topic.

Amazon

This series of topics covers all products offered by Amazon™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

AWS Cloudtrail (Push)

AWS CloudWatch (Pull)

AWS Kinesis (Pull)

AWS Guardduty (Push)

AWS Load Balancer (Push)

AWS S3 Access (Push)

AWS SecurityHub (Push)

AWS Storage Bucket (Push)

AWS VPC (Push)

AWS WAF (Push)

AWS Cloudtrail (Push)

CloudTrail™ is a service offered by Amazon™ that captures a log of all API calls for an AWS account and its services. CloudTrail enables continuous monitoring and post-incident forensic investigations of AWS by providing an audit trail of all activities across an AWS infrastructure. All CloudTrail logs files are stored in a dedicated S3 (Simple Storage Service) bucket, which is similar to a file folder and stores data and metadata objects. To add this Data Source to Forescout eyeAlert, consult with your Amazon product documentation to ensure the following settings are used:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Amazon provides a user documentation portal here.

Target Data Logs

Forescout currently processes the following security logs:

- Public S3 Buckets Logs
- S3 Bucket Downloads Logs
- Launch Instances Logs
- Open Security Group Access Logs
- Modification to IAM Logs
- Impossible Travel Logs
- Authentication Failures Logs (Brute Force Detection)

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Data Source Product Index.

AWS Kinesis (Pull)

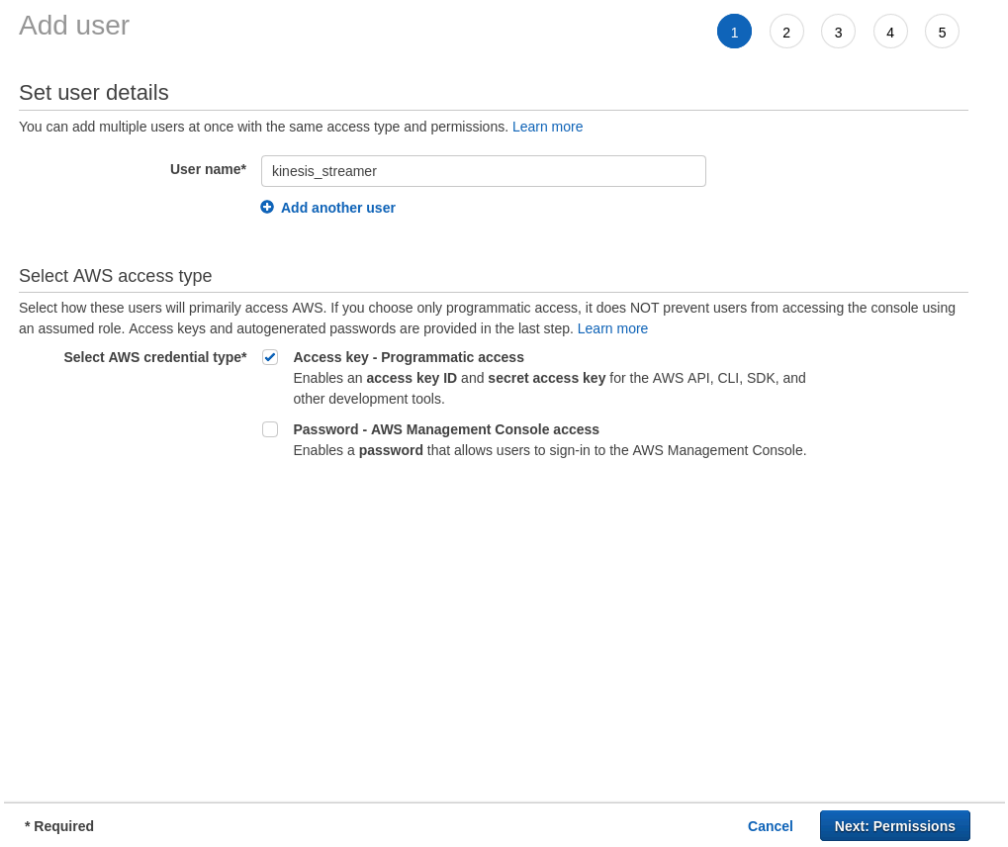
To add AWS Kinesis to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the AWS Kinesis Data Source in the Forescout eyeAlert UI

AWS Kinesis Customer-Side Configuration Prerequisites

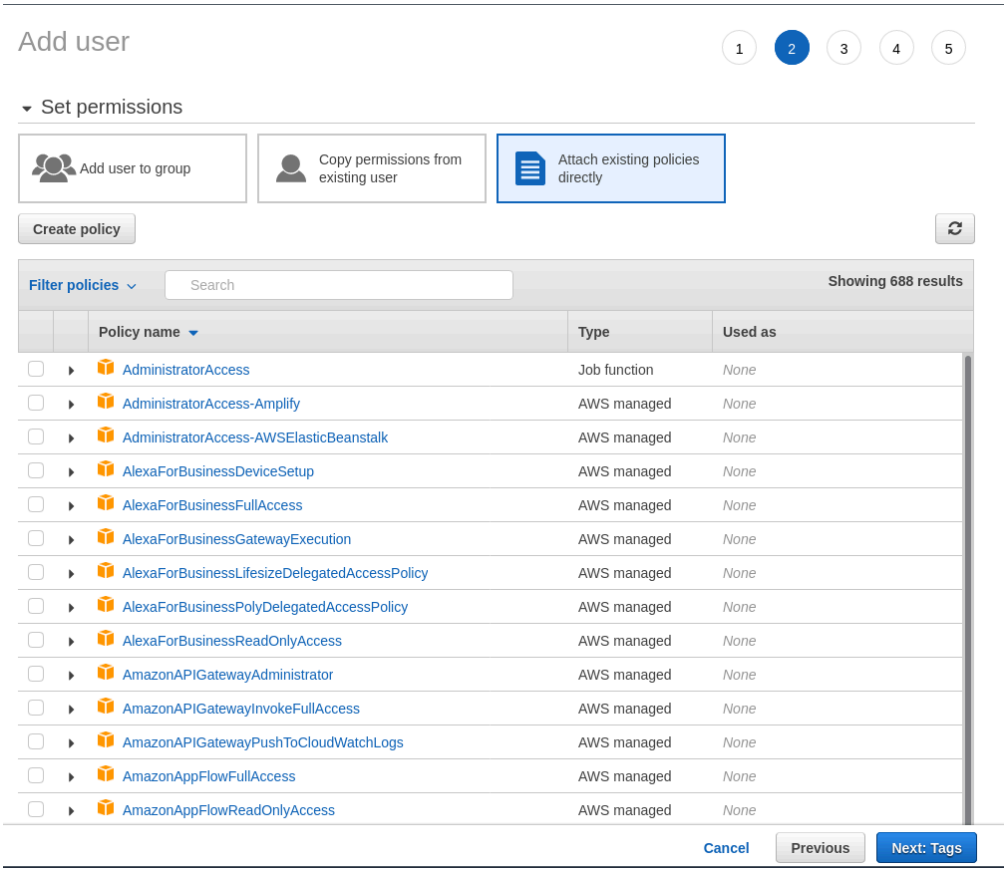
Forescout eyeAlert uses the pull mechanism to ingest logs from this Data Source. The following procedure for configuring AWS Kinesis for Forescout eyeAlert log ingestion is based on vendor documentation located here.

1. Log in to the AWS console using the root account.
2. Go to AWS IAM.
3. Go to **`Users`** in the sidebar on the left.
4. Click on **`Add user`**.
5. Give the user a username, and enable the checkbox **Access Key - Programmatic**



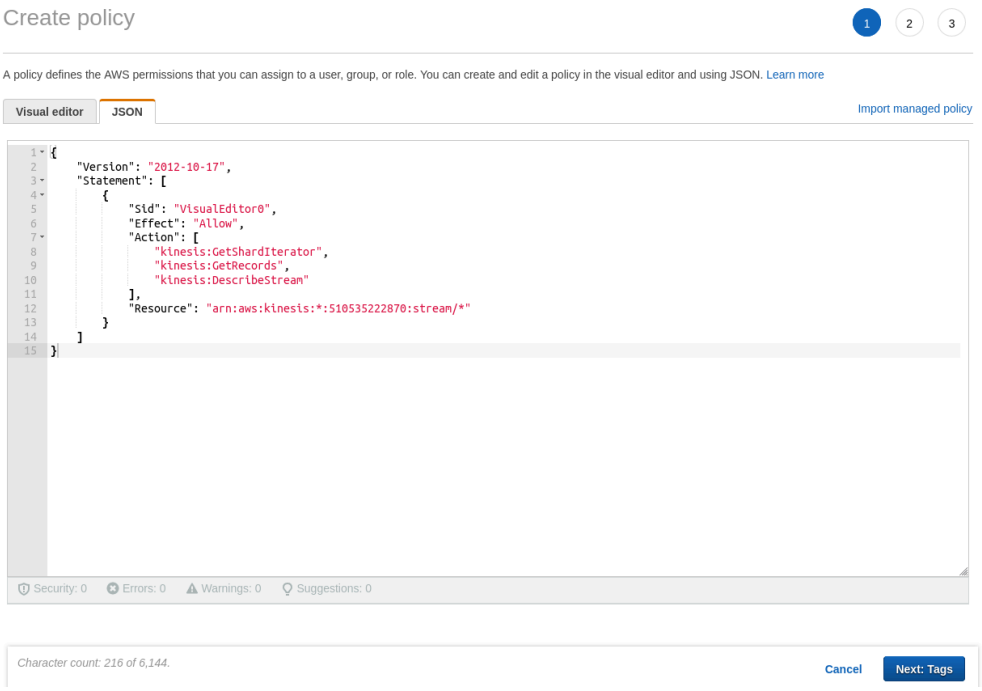
Access.

6. Click **Next**.
7. On the permissions page, click on **Attach existing policies directly**.

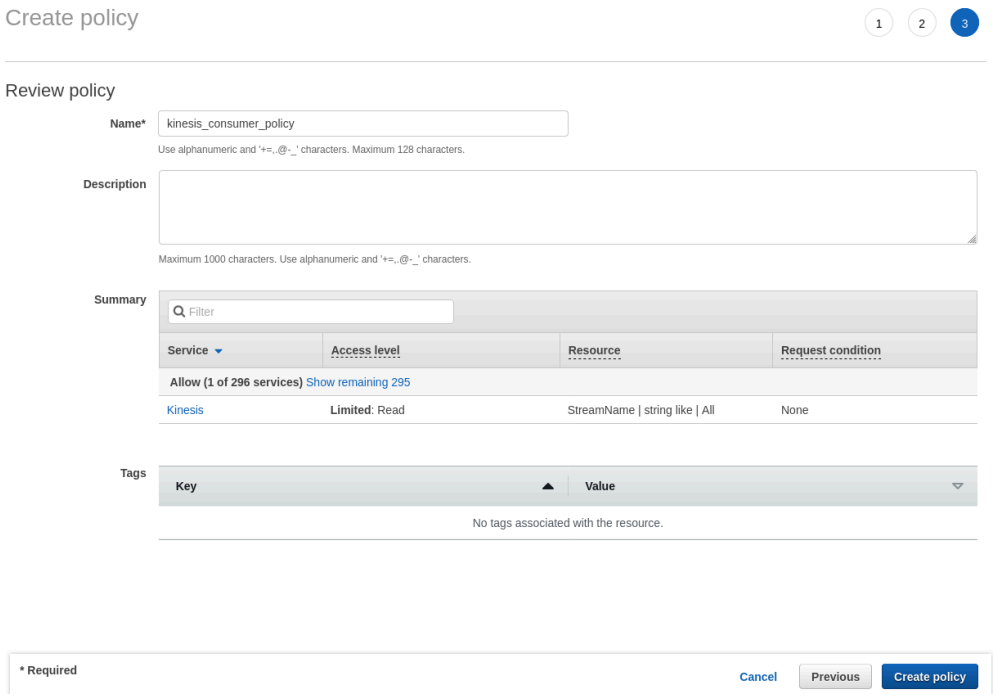


8. Choose **JSON** and paste the following, so that puller user has access to get records from kinesis.

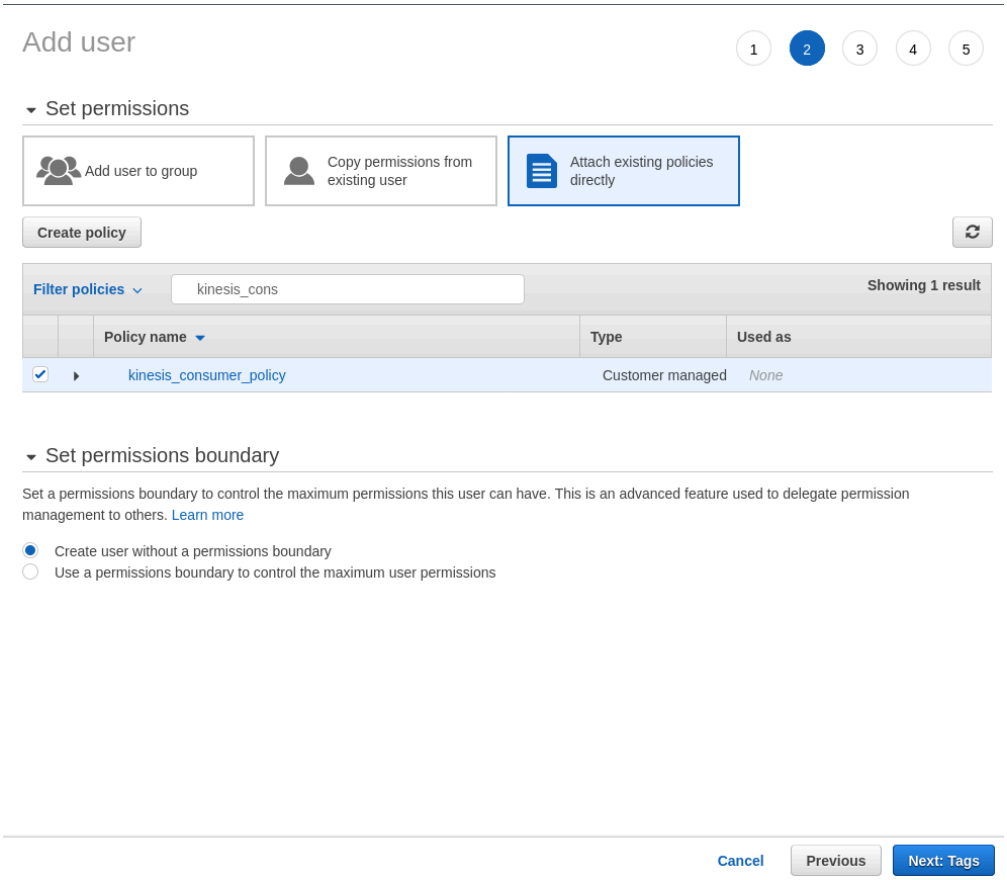
   { "Version": "2012-10-17", "Statement": [{ "Sid": "VisualEditor0", "Effect": "Allow", "Action": ["kinesis:GetShardIterator", "kinesis:GetRecords", "kinesis:DescribeStream"], "Resource": "arn:aws:kinesis:*:510535222870:stream/*" }] }



9. Go through the rest of the steps clicking **Next** and **Create**.



10. Search for created policy as the following.



11. Go through the rest of the steps clicking Next and Create.

12. Download the user credentials and use the **Access key ID** and **Secret access key** to be used in puller UI configuration.
13. Proceed now to Selecting the AWS Kinesis Data Source.

Selecting the AWS Kinesis Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive AWS Kinesis Logs

Data Source Name – AWS Kinesis

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the Kinesis **USER ACCESS KEY ID.**
2. Enter the **USER SECRET ACCESS KEY**.
3. Enter the **KINESIS REGION**.
4. Enter the **KINESIS STREAM NAME**.
5. Enter the **DATA RETENTION** period in minutes - 0.
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
7. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

AWS GuardDuty (Push)

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts, workloads, and data stored in Amazon S3.It process and analyses data fromVPC Flow Logs, AWS CloudTrail management event logs, CloudTrail S3 data event logs, and DNS logs.It uses threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning to identify unexpected and potentially unauthorized and malicious activities such as escalations of privileges, uses of exposed credentials, and communication with malicious IP addresses or domains.

To add Amazon GuardDuty to Forescout eyeAlert as a Data Source, consult your vendor documentation to ensure the following settings are used:

Log Retrieval Method

Push the logs to an AWS S3 bucket. Then pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic in the *Forescout Cloud Connector Configuration Guide*.

Instructions and/or Suggested Information Sources

Amazon provides a user documentation portal here.

Target Data Logs

Forescout currently processes the following log types for ingestion:

- EC2 finding type
- S3 finding type
- IAM finding type

Log Format Necessary for Forescout eyeAlert Retrieval

Use the default flow log record format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

When the logs have been successfully pushed to the S3 Bucket, pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic in the Forescout Cloud Connector Configuration Guide.

AWS Load Balancer (Push)

AWS™ Load Balancer™ serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability of your application. You add one or more listeners to your load balancer.

To add the AWS Load Balancer Data Source to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Push the logs to an AWS S3 bucket. Then pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic in the *Forescout Cloud Connector Configuration Guide*.

Instructions and/or Suggested Information Sources

Amazon provides a user documentation portal here.

Target Data Logs

Forescout currently processes access logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON log record format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

When the logs have been successfully pushed to the S3 Bucket, pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic.

AWS S3 Access (Push)

The Amazon™ Simple Storage Service™ (S3) is a cloud storage service. This Data Source is for ingesting server access log files from Amazon S3. To add AWS S3 Access toForescout XDR as a Data Source, consult with your user documentation to ensure the following settings are used in configuring your device:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Amazon provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

AWS SecurityHub (Push)

Security Hub collects security data from across AWS accounts, services, and supported third-party partner products and helps you analyze your security trends and identify the highest priority security issues. When you enable Security Hub, it begins to consume, aggregate, organize, and prioritize findings from AWS services that you have enabled, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie. You can also enable integrations with AWS partner security products. Those partner products can then also send findings to Security Hub. See Product integrations in AWS Security Hub. Security Hub also generates its own findings by running continuous, automated security checks based on AWS best practices and supported industry standards. See Security standards and controls in AWS Security Hub.

To add AWS SecurityHub to Forescout eyeAlert as a Data Source, consult your vendor documentation to ensure the following settings are used:

Log Retrieval Method

Push the logs to an AWS S3 bucket. Then pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic in the *Forescout Cloud Connector Configuration Guide*.

Instructions and/or Suggested Information Sources

Amazon provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format if possible, or the default format if CEF is not available.

Configure Forescout eyeAlert to Receive the Data Source Logs

When the logs have been successfully pushed to the S3 Bucket, pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic in the Forescout Cloud Connector Configuration Guide.

AWS Storage Bucket (Push)

Amazon™ Simple Storage Service™ stores objects that are organized into AWS S3 buckets and identified within each bucket by a unique, user-assigned key. All requests are authorized using an access control list associated with each bucket and object. The bucket is basically a secure cloud-based folder for storing files. When data logs are stored in an AWS bucket, they can be ingested by Forescout eyeAlert and used to automatically alert the SOC to Suspicious Entities, and by Forescout's SOC Security Analysts in the analysis and resolution of Security Incidents. Certain Data Sources require specific configurations for S3 bucket pulling.

To use an AWS Storage Bucket to pull logs for a particular Data Source, see this topic in the *Forescout Cloud Connector Configuration Guide*.

AWS VPC (Push)

Amazon™ Virtual Private Cloud™ enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS. **AWS VPC Flow Logs**enable you to capture information about the network traffic moving to and from network interfaces within your VPC. You can use VPC Flow Logs as a centralized, single source of information to monitor different network aspects of your VPC. VPC Flow logging gives security engineers a history of high-level network traffic flows within entire VPCs, subnets, or specific network interfaces (ENIs). This makes VPC Flow Logs a useful source of information for detection teams focused on collecting network instrumentation across large groups of instances.

To add AWS VPC to Forescout eyeAlert as a Data Source, consult your vendor documentation to ensure the following settings are used:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Amazon provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud activity logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the default flow log record format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

AWS WAF (Push)

AWS™ WAF™ (Amazon Web Services Web Application Firewall) is a web application firewall that helps protect web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources.

To add the AWS WAF Data Source to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Push the logs to an AWS S3 bucket. Then pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic in the *Forescout Cloud Connector Configuration Guide*.

Instructions and/or Suggested Information Sources

Amazon provides a user documentation portal here.

Target Data Logs

Forescout currently processes access logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON log record format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

When the logs have been successfully pushed to the S3 Bucket, pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic in the *Forescout Cloud Connector Configuration Guide*.

AWS SecurityHub (Push)

Security Hub collects security data from across AWS accounts, services, and supported third-party partner products and helps you analyze your security trends and identify the highest priority security issues. When you enable Security Hub, it begins to consume, aggregate, organize, and prioritize findings from AWS services that you have enabled, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie.

You can also enable integrations with AWS partner security products. Those partner products can then also send findings to Security Hub. See Product integrations in AWS Security Hub. Security Hub also generates its own findings by running continuous, automated security checks based on AWS best practices and supported industry standards. See Security standards and controls in AWS Security Hub. To add AWS SecurityHub to Forescout XDR as a Data Source, complete the following tasks:

Log Retrieval Method

Push the logs to an AWS S3 bucket. Then pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic in the *Forescout Cloud Connector Configuration Guide*.

Instructions and/or Suggested Information Sources

Amazon provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format if possible, or the default format if CEF is not available.

Configure Forescout eyeAlert to Receive the Data Source Logs

When the logs have been successfully pushed to the S3 Bucket, pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic in the *Forescout Cloud Connector Configuration Guide*.

AWS CloudWatch (Pull)

Amazon™ CloudWatch™ is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers.

CloudWatch provides data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.

CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications, and services that run on AWS and on-premises servers.

To add AWS CloudWatch to Forescout eyeAlert as a Data Source, consider the following information and references:

Log Retrieval Method

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source.

Key Data Source Product Configuration and Authentication Requirements

To onboard logs from this Data Source, you will need to have the following credential information on-hand when configuring Forescout eyeAlert:

- User Access Key ID
- User Secret Access Key
- API Gateway Host
- API Gateway URI
- API Gateway Region
- Log Group Name Prefixes

Suggested Information Sources for Data Source Product Configuration

Amazon provides the following information sources related to establishing the necessary setup for accurate log ingestion:

- AWS Services that send logs to CloudWatch: Enable logging from AWS services - Amazon CloudWatch Logs.

- AWS API Gateway logs: Set up CloudWatch logging for REST APIs in API Gateway - Amazon API Gateway.
- AWS Lambda: Log and monitor Node.js Lambda functions - AWS Lambda.
- GetLogEvents: GetLogEvents - Amazon CloudWatch Logs.
- DescribeLogGroups: DescribeLogGroups - Amazon CloudWatch Logs.
- DescribeLogStreams: DescribeLogStreams - Amazon CloudWatch Logs.
- Signing requests: Create a signed AWS API request - AWS Identity and Access Management.

Note:
The reference links above are suggestions only. To ensure accuracy, be sure to use the latest official documentation provided by the vendor of your Data Source product type and version.

Target Data Logs

AWS CloudWatch supports logging from a myriad of Amazon services which are listed by Amazon here. Forescout currently targets logs from Amazon API Gateway, AWS CloudTrail, and AWS Lambda.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON or CLF format when configuring your Data Source to make logs available for ingestion by Forescout eyeAlert.

Configure Forescout eyeAlert to Retrieve the Data Source Logs

See Configuring Forescout eyeAlert to Receive AWS CloudWatch Logs.

Configuring Forescout eyeAlert to Receive AWS CloudWatch Logs

Data Source Name – AWS Cloudwatch

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

Select Data Sources under the Administration menu and click + Add Data Source.

Select the AWS CloudWatch Data Source from the drop down menu, select a connector, and fill in the Configurations form on the right side of the view as follows:

1. Enter the **USER ACCESS KEY ID**.
2. Enter the **USER SECRET ACCESS KEY**.
3. Enter the **API GATEWAY HOST**.
4. Enter the **API GATEWAY URI**.
5. Enter the **API GATEWAY REGION**.
6. Enter the **GROUP NAME PREFIX**.
7. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 600 seconds.
8. In the **NOTES** field, enter any comments about the deployment you want preserved for

later reference.
9. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
10. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Anomali

This series of topics covers all products offered by Anomali™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Anomali ThreatStream Filter (Push)

Anomali Threatstream Filter (Pull)

Anomali™ ThreatStream™ automates the threat intelligence collection and management lifecycle to speed detection, streamline investigations and increase analyst productivity. ThreatStream easily integrates into existing security infrastructure to operationalize threat intelligence and improve organizational efficiencies. To add Anomali ThreatStream to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Anomali ThreatStream Filter Data Source in the Forescout eyeAlert UI

Target Data Logs

Forescout currently ingests Marking-definition and Indicator logs for ingestion:

- **Marking-definition:**The marking-definition object represents a specific marking. Data markings typically represent handling or sharing requirements for data and are applied in the***object_marking_refs***and***granular_markings***properties on STIX Objects, which reference a list of IDs for marking-definition objects.

  Two marking definition types are defined in this specification:

  - **TLP**: to capture TLP markings
  - **Statement:** to capture text marking statements.
  - In addition, it is expected that the FIRST **I**nformation **E**xchange **P**olicy (IEP) will be included in a future version once a machine-usable specification for it has been defined.
  - **Indicator:**Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity. For example, an Indicator may be used to represent a set of malicious domains and use the STIX Patterning Language to specify these domains. Relationships from the Indicator can describe the malicious or suspicious behavior that it directly detects (Malware, Tool, and Attack Pattern). In addition, it may also imply the presence of a Campaigns, Intrusion Sets, and Threat Actors, etc.

Anomali ThreatStream Customer-Side Configuration Prerequisites

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source. On the appropriate device or software application:

- **Add new user**
    - In the top navigation bar, click **Setting** and then **User Admin**.
    - Click **Add User**.
    - Enter the email address for the new user. The domain must match the domain of your organization.
    - Select the permissions you want to give the new user.
    - Click **Add**.
- **Configure a site:** The Sites tab enables you to configure and manage communication between ThreatStream and external TAXII sources to which you have access. Configuring a Site on ThreatStream involves authenticating to a Discovery URL for the site. After you have configured a TAXII server site, you can poll data from available collections on the server.
    - In the top navigation bar, click **Settings** and then **TAXII**.
    - Under Sites, click **Actions > Add Site**.
    - Enter a meaningful Name for the site.
    - Select a TAXII Version. You can select TAXII 1.1, TAXII 2.0, or TAXII 2.1.
    - Enter the Discovery URL.
    - **(Optional)** Select required authentication methods.
        - If you will use SSL Verification from the site, select Use Site SSL Verification.
        - If the site uses basic authentication, select Basic Authentication and enter your credentials for the site.
        - If the site requires an SSL Two-Way Certificate, select SSL Two-Way Certificate and upload your certificate.
    - Click **Add Site**. ThreatStream will now discover available TAXII feeds on the site.
- **Configuring Push Collections**
    - In the top navigation bar, click **Settings** and then **TAXII**.
    - Under **Sites**, locate the TAXII server of interest and click to expand the site details.

- Click **Push Collections**.
- Click **New**.
- Under **Collection Name**, select the collection on the TAXII server to which you want to push.
- Enter an **Interval** to specify the cadence at which ThreatStream will push data to the collection.
- Enter a **Start From** date. This specifies the furthest timestamp you want to be polled. Click **Now** to use the current date and time.
- Select a **Saved Search** to specify the data you want to push to the collection.
- If required, enter your **Subscription ID**.
- To save the configuration and push data to the collection, click **Save and Run Now.**

During the procedure to configure Forescout eyeAlert to ingest logs from this source, the following information will be required:

- `username` of the user created in the previous steps.
- `password` of the user created in the previous steps.
- `api_url`: This field varies based on the TAXII server version

Selecting the Anomali ThreatStream Data Source

1. Log in to Forescout eyeAlert and click the **Administration** tab.
2. Select **Data Sources**.
3. Click the **+ Data Source** button.
4. Click the **DATA SOURCE** dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR** dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Anomali ThreatStream Logs

Data Source Name – Anomalie ThreatStream Filter

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration* > *Data Sources* > *+Data Source* > *Add Data Source to Connector* – *Configurations* (right-panel)

1. Enter the **API URL**.
2. Enter **USERNAME**.
3. Enter the **PASSWORD**.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 86400.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Apache

This series of topics covers all products offered by Apache™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Apache Access Web Server (Push)

Apache Access Web Server (Push)

The Apache Web Server™ delivers requested files after a visitor enters a domain name into the browser. A web server acts a middleman between the server and client machine pulling content from each user request and delivering it to the web. The web server processes files in different programming languages and converts them into static HTML files to be able to serve them in the browser.

To add this Data Source to Forescout eyeAlert as a Data Source, use your vendor documentation to ensure the following settings are used:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Apache provides a user documentation portal here. These additional sources of information may also be helpful:

- Apache Log Documentation - https://httpd.apache.org/docs/current/mod/mod_log_config.html
- Ultimate Guide to Logging - https://www.loggly.com/ultimate-guide/access-and-error-logs/
- Apache Module mod_log_config - http://httpd.apache.org/docs/2.4/mod/

mod_log_config.html
- Apache Log Files - https://httpd.apache.org/docs/2.4/logs.html
- Apache Access Log in CEF:

Target Data Logs

Forescout currently processes the following logs:

Access Logs – the logs are typically located in the directory /var/log:

- /var/log/apache/access.log
- /var/log/apache2/access.log
- /var/log/httpd/access.log

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format if possible, and Syslog if not, when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Area 1 Security

This series of topics covers all products offered by Area 1 Security™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Area 1 Horizon

Area 1 Horizon (Pull)

Area 1™ Horizon™, a cloud-based service, stops phishing attacks across all traffic vectors including email, web, or network. Phishing attacks remain the primary cybersecurity threat and Area 1 has been introduced to reduce the gap between phishing baits leading to massive damage and the need for a new, advanced platform to address them. To add Area 1 Horizon to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Area 1 Security Data Source in the Forescout eyeAlert UI

Target Data Logs

Forescout targets the Alert Endpoint logs via the Alerts Endpoint API for ingestion.

Area 1 Security Customer Side Configuration Prerequisites

Forescout supports the pull mechanism for the Area 1 Security Data Source.

When configuring Forescout eyeAlert to receive Area 1 Security log files, you will need to main values: public key and private key.

In order to get them from Area1 Security portal, follow the next steps:

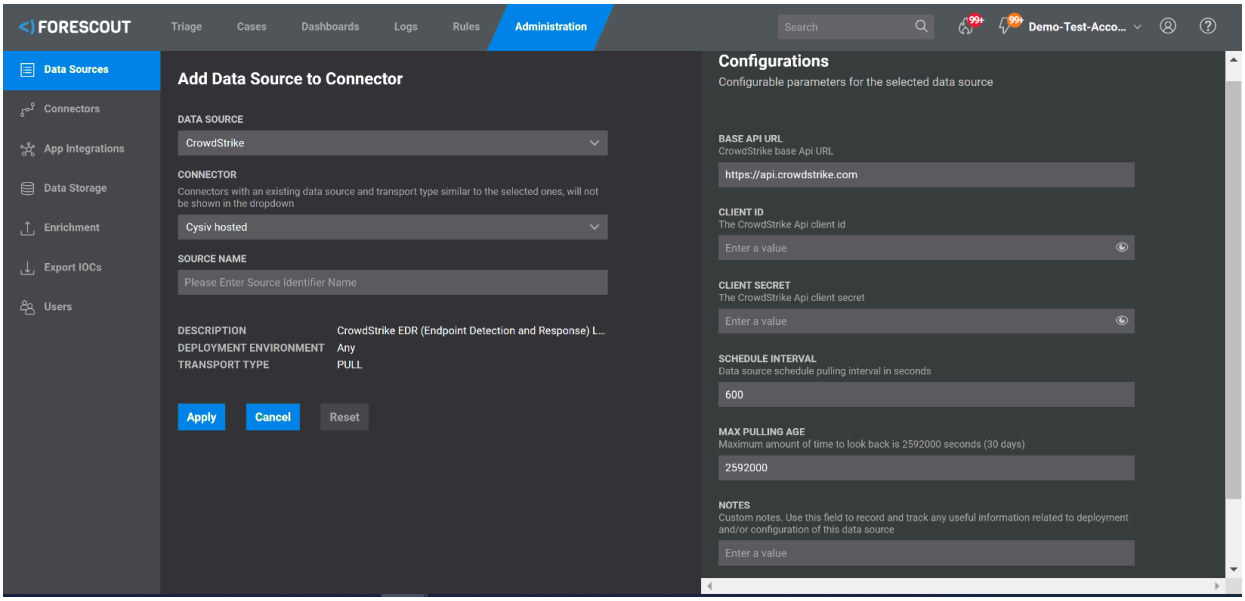
1- You need to have access to the Area1 Horizon portal.

2- Navigate to the **Service Accounts** tab, and click **+ Add Service Account**.

The service account will generate public and private keys for you which can be added to Forescout eyeAlert portal. You will input these keys during the procedure to configure Forescout eyeAlert to receive Area 1 Security log files. Proceed now to Selecting the Area 1 Security Data Source.

Selecting the Area 1 Security Data Source Selecting a New Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Select your Data Source from the dropdown.



The available configuration options will vary depending on the Data Source type and Connector deployment method. The example shown above is of a CrowdStrike EDR™ Data Source where logs are pulled by a Connector that is hosted by Forescout.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout TDR to Receive Area 1 Security Log Files

Data Source Name – Area 1 Security

Log Retrieval Method – Pull

Connector Deployment Environment – Any

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **PUBLIC KEY**.
2. Enter the **PRIVATE KEY**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 900.
4. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
5. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
7. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Armorblox

This series of topics covers all products offered by Armorblox™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Armorblox Data Source (Pull)

Armorblox Data Source (Pull)

Armorblox™ helps organizations communicate more securely over email and other cloud office applications with the power of Natural Language Understanding. The Armorblox platform connects over APIs and analyzes thousands of signals to understand who users are, what they do, and how they communicate. With this context, Armorblox can stop advanced email attacks like business email compromise, and also help organizations stay compliant by protecting their sensitive data from falling into the wrong hands. To add Armorblox to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Armorblox Data Source in the Forescout eyeAlert UI

Target Data Logs

Forescout currently targets Incident and Activity logs for this Data Source.

Armorblox Customer Side Configuration Prerequisites

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source. To configure Armorblox for Forescout eyeAlert pull ingestion, complete the following procedure:

Create new API key:

1. Log into your Armorblox portal with your credentials.
2. In the portal, click **Settings**.
3. In the **Settings** view, click **API Keys.**
4. Click **Create API Key**.
5. Specify a descriptive name so that you know the purpose of this key for future reference.
6. Click **Create**, and copy the API key displayed in the modal. The key is only displayed once.
7. Save the API key securely.

In the procedure to configure Forescout eyeAlert to ingest the logs, you will need to provide the Tenant ID and API Key.

Selecting the Armorblox Data Source

1. Log in to Forescout eyeAlert and click the **Administration** tab.
2. On the Administration screen, click the **Data Sources** tab.
3. Click the **+ Data Source** button.
4. Click the **DATA SOURCE** dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR** dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME** field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout TDR to Receive Area 1 Security Log Files

Data Source Name – Area 1 Security

Log Retrieval Method – Pull

Connector Deployment Environment – Any

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **PUBLIC KEY**.

2. Enter the **PRIVATE KEY**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 900.
4. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
5. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
7. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Aruba

This series of topics covers all products offered by Aruba™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Aruba OS (Push)

Aruba SD-WAN (Push)

Aruba SD-WAN (Push)

Aruba SD-WAN enables customers to build a unified WAN edge. A Software-defined Wide Area Network (SD-WAN) is a virtual WAN architecture that allows enterprises to leverage any combination of transport services – including MPLS, LTE and broadband internet services – to securely connect users to applications.

To add Aruba SD-WAN to Forescout eyeAlert as a Data Source, complete the following tasks:

Target Data Logs

Forescout currently targets the Alarm logs for ingestion.

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Aruba Networks provides a user documentation portal here.

Target Data Logs

Forescout currently processes Alarm logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS

or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Aruba OS (Push)

ArubaOS™ is the network operating system for Aruba Mobility Masters, Mobility Controllers and controller-managed campus access points (APs). To add Aruba OS to Forescout eyeAlert as a Data Source, refer to your vendor documentation to ensure the following settings are used:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Aruba Networks provides a user documentation portal here.

Target Data Logs

Forescout currently targets the following log types for ingestion:

- Aruba Logs
- Deletion of Key Logs
- System Logs
- Failure Logs

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Asterisk

This series of topics covers all products offered by Asterix™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Asterisk VOIP (Push)

Asterisk VOIP (Push)

Asterisk is an open source framework for building communications applications, and "turns an ordinary computer into a communications server". Asterisk powers IP PBX systems, VoIP gateways, conference servers and other custom solutions. It is used by small businesses, large businesses, call centers, carriers and government agencies, worldwide. To add Asterisk VoIPto Forescout eyeAlert as a Data Source, ensure to use the following settings when configuring your Data Source:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Asterix provides a user documentation portal here.

Target Data Logs

Forescout currently targets the following log types for ingestion:

- Invalid Account ID
- Failed ACL match
- Invalid Challenge/Response
- Invalid Password
- Successful Authentication
- Invalid formatting of Request
- Session Limit Reached (such as a call limit)
- Memory Limit Reached
- Maximum Load Average Reached
- Request Not Allowed
- Request Not Supported
- Authentication Method Not Allowed

- `In dialog message from unexpected host`
- `User login banned`
- `Fail2ban blocking event`

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format if possible, or the Syslog format if not, when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Auth0

This series of topics covers all products offered by Auth0™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Auth0 Data Source (Pull)

Auth0 Data Source (Pull)

Auth0™is a flexible, drop-in solution to add authentication and authorization services to your applications.You can connect any application (written in any language or on any stack) to Auth0 and define the identity providers you want to use (how you want your users to log in). Based on your app's technology, choose one of our SDKs (or call our API), and hook it up to your app. Now each time a user tries to authenticate, Auth0 will verify their identity and send the required information back to your app. To add Auth0 to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Auth0 Data Source in the Forescout eyeAlert UI

Target Data Logs

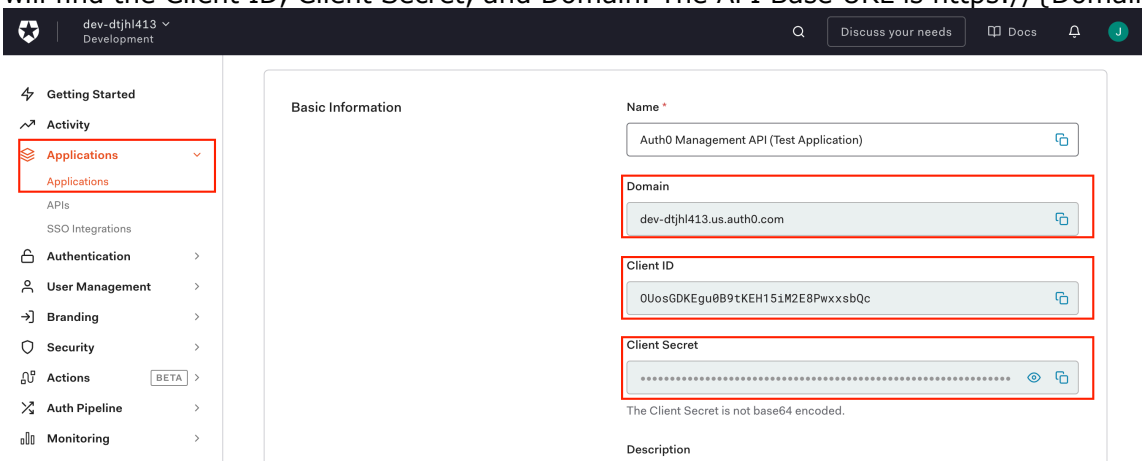
Forescout targets event logs that can be pulled through the Management API Logs Endpoint

Auth0 Customer-Side Configuration Prerequisites

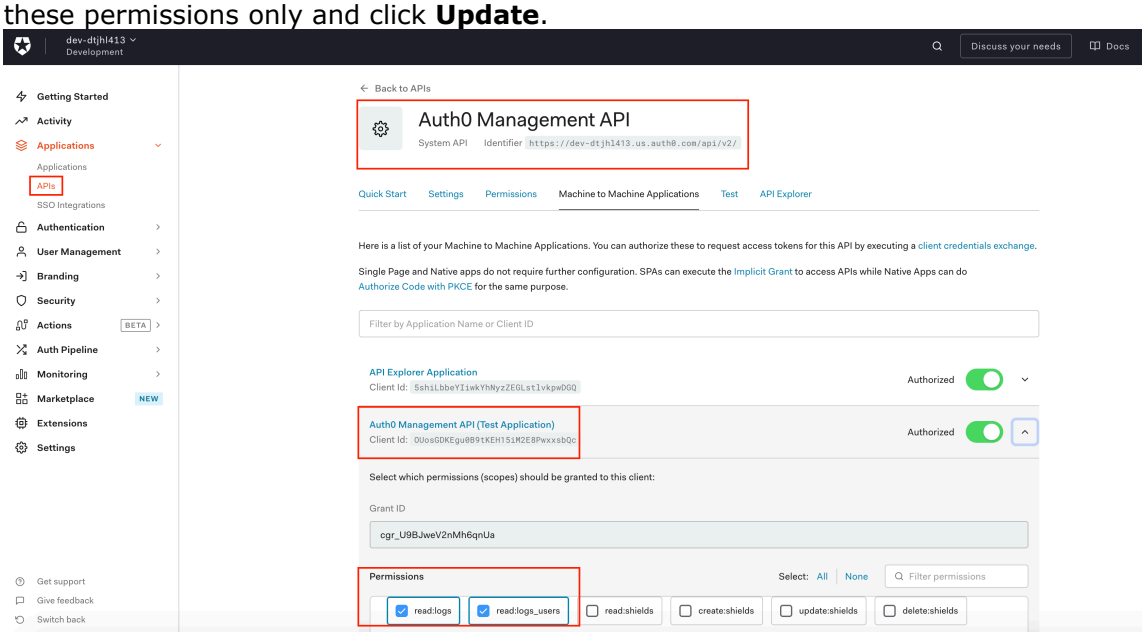
At the end of this section, take note of the following fields because their values must be provided during the procedure to configure Forescout eyeAlert to receive Auth0 logs:

- Client ID
- Client Secret
- API Base URL

1. Create and Authorize a Machine-to-Machine Application.
2. When the application is created, go to the Settings tab of your Application, and there you will find the Client ID, Client Secret, and Domain. The API Base URL is https://{Domain}.



3. Ensure that the API has only the permissions it needs. The Forescout puller only needs to use endpoint/api/v2/logs/which uses permissions "read:logs":and "read:logs_user". Select these permissions only and click **Update**.



4. Proceed now to Selecting the Auth0 Data Source.

Selecting the Auth0 Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).

5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed now to Configuring Forescout eyeAlert to Receive Auth0 Logs.

Configuring Forescout TDR to Receive Auth0 Logs

Data Source Name – Auth0

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **API BASE URL**.
2. Enter the Auth0 API client id into the **CLIENT ID** field.
3. Enter the Auth0 API client secret into the **CLIENT SECRET** field.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 300.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Avast

This series of topics covers all products offered by Avast™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Avast Antivirus (Push)

Avast Antivirus (Push)

Avast™is a family of cross-platform internet security applications developed by Avast for Microsoft Windows, macOS, Android and iOS.To add Avast Antivirus to Forescout eyeAlert as a Data Source, ensure you use the following settings when configuring your product.

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Avast provides a user documentation portal here.

Target Data Logs

Forescout currently targets the following the following log types for ingestion:

- Information
- Warning
- Error

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Barracuda

This series of topics covers all products offered by Barracuda™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Barracuda Cloudgen (Push)

Barracuda ESS (Push)

Barracuda ESG (Push)

Barracuda WAF (Push)

Barracuda WSG (Push)

Barracuda Cloudgen (Push)

Barracuda™ CloudGen™ Firewall is a family of physical, virtual, and cloud-based appliances that protect and enhance dispersed network infrastructures.To add Barracuda CloudGen Firewall to Forescout eyeAlert as a Data Source, use the following settings when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Barracuda provides a user documentation portal here.

Target Data Logs

Forescout currently targets system processes, box services, and configured services such as Forwarding Firewall, Event, Authentication, Cloud, Config, System, etc. Logging is processed according to system and service settings.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Barracuda ESS (Push)

Barracuda™ Email Security Service™ is a cloud-based email security service that protects both inbound and outbound emails against the latest spam, viruses, worms, phishing, and denial of service attacks. Barracuda Cloud Control is a comprehensive cloud-based web interface that enables administrators to monitor and configure Barracuda services. To add Barracuda ESS to Forescout eyeAlert as a Data Source, ensure to use the following settings when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Barracuda provides a user documentation portal here.

Target Data Logs

Forescout eyeAlert currently processes email security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Barracuda ESG (Push)

Barracuda™ Email Security Gateway™ is a hardware appliance that protects both inbound and

outbound emails against the latest spam, viruses, worms, phishing, and denial of service attacks.

To add Barracuda ESG to Forescout eyeAlert as a Data Source, use the following settings when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Barracuda provides a user documentation portal here.

Target Data Logs

Forescout currently processes email security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert.

See Configuring Forescout eyeAlert to Receive Logs Pushed to a Hosted Connector for the procedure to configure Forescout eyeAlert to receive the logs.

Barracuda WAF (Push)

Barracuda™ Web Application Firewall™ is a part of Barracuda Cloud Application Protection, an integrated platform that brings a set of interoperable solutions and capabilities together to provide application security.

To add Barracuda WAF to Forescout eyeAlert as a Data Source, ensure you use the following settings when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Barracuda provides a user documentation portal here.

Target Data Logs

Forescout currently processes the following log types for ingestion:

-
- Web Firewall logs
- Access logs
- Audit logs

- System logs
- Network Firewall logs

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic.

Barracuda WSG (Push)

Barracuda™ Web Security Gateway™ includes spyware, malware, and virus protection with a policy and reporting engine. Features are focused on helping organizations adapt to emerging requirements like social-network regulation, remote filtering, and visibility into SSL-encrypted traffic.

To add Barracuda WSG to Forescout eyeAlert as a Data Source, use the following settings when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Barracuda provides a user documentation portal here.

Target Data Logs

Forescout currently processes web security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert.

See Configuring Forescout eyeAlert to Receive Logs Pushed to a Hosted Connector for the procedure to configure Forescout eyeAlert to receive the logs.

BeyondTrust

This series of topics covers all products offered by BeyondTrust™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

BeyondTrust Priveleged Access (Push)

BeyondTrust BeyondInsight (Push)

BeyondTrust Priveleged Access (Push)

To add BeyondTrust Privelege Access to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

BeyondTrust provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

BeyondTrust BeyondInsight (Push)

To add BeyondTrust BeyondInsight to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

BeyondTrust provides a user documentation portal here.

Target Data Logs

Forescout currently targets the following log types for ingestion:

- Login (1)
- Logout (2)
- Add (3)
- Edit (4)
- Delete (5)
- Read (6)

- Assign (11)
- Managed
- Requestor
- System
- Administrator
- Domainmanagement
- Test

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

BIND

This series of topics covers all products offered by BIND™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

BIND DNS (Push)

Berkeley Internet Name Domain™ (BIND) is a Domain Name System (DNS) server. To add this Data Source to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

BIND provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Box

This series of topics covers all products offered by Box™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Box Data Source

Box Data Source

Box™ is a content management platform that centralizes content online, allowing users to control their own content so they can securely share files and folders.

To add Box™ to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source.

Key Data Source Product Configuration and Authentication Requirements

To onboard logs from this Data Source, you will need to have the following credential information on-hand when configuring Forescout eyeAlert:

- API URL

  Note:
  Use the API URL applicable for your region.

- SERVICE ACCOUNT KEY

Note:

When configuring Box, ensure the following options are selected:

- Write all files and folders stored in Box
- Manage users
- Manage groups
- Manage enterprise properties

Suggested Information Sources for Data Source Product Configuration

Box provides documentation here.

Target Data Logs

Forescout currently targets Application logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON format when configuring your Data Source to make logs available for ingestion by Forescout eyeAlert.

Configure Forescout eyeAlert to Retrieve the Data Source Logs

See Configuring Forescout eyeAlert to Receive Box Data Source Logs.

Configuring Forescout eyeAlert to Receive Box Data Source Logs

Data Source Name – Box

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > + Add Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the**API URL** – use the appropriate URL for your region.
2. Enter the **SERVICE ACCOUNT KEY**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is *7200* or 24 hours.

4. Enter your desired value for **NO FLOW ALERT THRESHOLD**, which is the time to wait before alerting on absence of logs in seconds (default is Schedule Interval + 1 hour or 10800).

5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as *604800* or 7 days.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.

7. Select the appropriate **TIME ZONE**.

8. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is *Pulling* for periodic retrieval of target data logs.
9. Click the **Apply** button.

Carbon Black

This series of topics covers all products offered by Carbon Black™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Carbon Black EDR (Push)

Carbon Black Cloud (Push)

Carbon Black EDR (Push)

VMware™ Carbon Black Enterprise™ EDR is an advanced threat hunting and incident response solution that delivers continuous visibility for top security operations centers (SOCs) and incident response (IR) teams. Enterprise EDR is delivered through the VMware Carbon Black Cloud, a next-generation endpoint protection platform that consolidates security in the cloud using a single agent, console and dataset. It employs a listening component called a sensor that listens to every process running including changes to the file system and registries.

To add Carbon Black EDR to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

VMWare provides a user documentation portal for Carbon Black EDR here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Carbon Black Cloud (Push)

VMware™ Carbon Black Cloud™ is a software as a service (SaaS) solution that provides next-generation anti-virus (NGAV), endpoint detection and response (EDR), advanced threat hunting, and vulnerability management within a single console using a single sensor. It consists of multiple products (VMware Carbon Black Cloud Endpoint, VMware Carbon Black Cloud Enterprise EDR and VMware Carbon Black Cloud Audit & Remediation).

To add Carbon Black Cloud to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

VMware provides a user documentation portal for Carbon Black Cloud here.

Target Data Logs

Forescout currently processes endpoint and alert logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Cato Networks

This series of topics covers all products offered by Cato Networks™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Cato Networks Data Source

Cato Networks Data Source (Pull)

Cato Networks™ uses a full enterprise-grade network security stack natively built into the Cato SASE Cloud to inspect all WAN and Internet traffic. Security layers include an application-aware next-generation firewall-as-a-Service (FWaaS), secure web gateway with URL filtering (SWG), standard and next-generation anti-malware (NGAM), IPS-as-a-Service (IPS), and Cloud Access Security Broker (CASB). Cato can further secure your network with a comprehensive Managed Threat Detection and Response (MDR) service to detect compromised endpoints. All layers scale to decrypt and inspect all customer traffic, without the need for sizing, patching, or upgrading of appliances and other point solutions. Security policies and events are managed using the self-service Cato Management Application.

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Cato Networks Data Source in the Forescout eyeAlert UI

Target Data Logs

Forescout eyeAlert currently ingests Events Feeds: The eventsFeed query helps you analyze events generated by activities related to networking, security, Sockets, Cato Clients, and more. The event data that this query returns is similar to the Analytics > Event Discovery window in the Cato Management Application.

Cato Networks Customer Side Configuration Prerequisites

Forescout uses the pull mechanism to ingest logs from this Data Source. To configure the Cato Networks for Forescout eyeAlert log ingestion, complete the following procedure:

1. Log in to your Cato Networks **Editors Account**.

2. Record the **Account ID** that appears in the Cato Networks URL to a temporary text file. If you have multiple account IDs you wish to monitor, repeat this step for each. For example, if your Account ID is "1234" then the URL should look like: https://www.catonetworks.com/#!/1234/topology.

3. Open the **Navigation Menu** and click **Administration** > **API Management**.

4. Enter the **Name** of the key and click **Apply**. If the API key has been successfully added a window will appear displaying the new API key.

5. Click the **Copy Icon** to copy your API key and ensure you **Save** it to a secure location. Once you close the window you can no longer access the value of the API key.

6. Click **Ok** to close the API window.

7. On the **API Management** page click the **Event Feed Enabled** toggle to enable your

account to send events to the Cato API servers.

Once this procedure has been completed, proceed to Selecting the Cato Networks Data Source.

Selecting the Cato Networks Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Cato Networks Logs

Data Source Name – Cato Networks

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations (right-panel)

1. Enter the **API KEY.**
2. Enter the **ACCOUNT ID.**
3. Enter the CrowdStrike API client secret into the **CLIENT SECRET** field.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 60.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 86400.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Check Point

This series of topics covers all products offered by Check Point™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Check Point Network Security (Push)

Check Point Network Security (Push)

Check Point™ provides cyber security solutions for clouds and networks. The CheckPoint Smart Center centralizes many functions.

To add CheckPoint to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Check Point provides a customer support portal here.

Target Data Logs

Forescout currently processes security and audit logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF (preferred) or the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Cisco

This series of topics covers all products offered by Cisco™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Cisco ACL (Push)

Cisco ASA (Push)

Cisco Core Switch (Push)

Cisco ESA (Push)

Cisco Firepower (Push)

Cisco-ACL (Push)

The Cisco™ ACL logging feature allows you to monitor ACL flows and to log dropped packets on an interface. When the ACL logging feature is configured, the system monitors ACL flows and logs dropped packets and statistics for each flow that matches the deny conditions of the ACL entry. Statistics and dropped-packet logs are generated for each flow.A flow is defined by the source interface, protocol, source IP address, source port, destination IP address, and destination port values. The statistics maintained for a matching flow is the number of denies of the flow by the ACL entry during the specified time interval.

To add Cisco ACL to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Cisco provides a possible starting point with its community portal here. The following information sources may also be useful:

- Understanding Access Control List Logging
- Configure Commonly Used IP ACLs
- IOS ACL Logging Knobs and Process Switching
- Security Configuration Guide: Access Control Lists, Cisco IOS Release 15S
- Configuring IP Access Lists
- Cisco Nexus 5500 Series NX-OS Quality of Service Configuration Guide, Release 7.x, Chapter: Configuring ACL Logging
- Configuring ACL Logging

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you

should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Cisco ASA (Push)

The Cisco™ Adaptive Security Appliance (ASA) Firewall is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. To add Cisco ASA Firewall to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Cisco provides a user documentation roadmap here.

Target Data Logs

Forescout currently processes a series of relevant Syslog messages.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Cisco Core Switch (Push)

Cisco™ Core Switch™ is a managed switch that is positioned at the backbone or physical core of the network. Some of the switches with this functionality are Cisco Catalyst 6800, 6500, 9*** series, 3850 fiber series and Meraki aggregation switches. To add the Cisco Core Switch Data Source to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Cisco provides a user documentation portal here.

Target Data Logs

Forescout currently processes emergencies, alerts, critical, errors, warnings, notifications, informational, and debugging logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Cisco ESA (Push)

Cisco™ Email Security Appliance™ is an email security gateway product. It is designed to detect and block a wide variety of email-borne threats, such as malware, spam, and phishing attempts. Because so many of today's attacks occur through email messages, having an email security gateway has become a necessity for most organizations.

To add Cisco ESA to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Cisco provides a user documentation portal here.

Target Data Logs

Forescout currently processes targets text mail and consolidated event logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Cisco Firepower (Push)

Cisco Firepower Threat Defense (FTD) is an integrative software image combining CISCO ASA and FirePOWER features into one hardware- and software-inclusive system.To add Cisco Firepower to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Cisco provides a user documentation portal here.

Target Data Logs

Forescout currently processes the following logs for ingestion:

- 106023
- 106100
- 305011
- 302013
- 302014
- 302015
- 302016
- 302021
- 106006
- 106007
- 106016
- 313001
- 313004

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Cisco IOS (Push)

Cisco IOS (Internetwork Operating System) is a proprietary operating system that runs on Cisco Systems routers and switches. The core function of Cisco IOS is to enable data communications between network nodes. To add Cisco IOS to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Cisco provides a user documentation portal here.

Target Data Logs

Forescout currently processes network security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Cisco ISE (Push)

Cisco™ Identity Services Engine™ (Cisco ISE) is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can then use that information to make proactive governance decisions by tying identity to various network elements including access switches, wireless LAN controllers (WLCs), Virtual Private Network (VPN) gateways, and data center switches.

To add Cisco ISE to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Cisco provides a user documentation portal here.

Target Data Logs

Forescout currently processes the following log types for ingestion:

- Failed Attempts
- Administrative and Operational Audit
- Threat Centric NAC

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS

or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Cisco Meraki (Push)

Cisco™ Meraki™ is a unified management solution that allows users to control their network from a centralized dashboard. It has a feature called EventTracker that amasses and examines logs generated by Meraki Firewall where administrators can monitro IDS alerts, VPN sessions, web traffic, user behavior and system activity.

To add the Cisco Meraki Data Source to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Cisco provides a user documentation portal here.

Target Data Logs

Forescout currently processes targets URL, flows, security events, air marshal, and appliance events.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Cisco Meraki Identity (Pull)

The Cisco™ Meraki Identity™ (CrowdStrike™ Hosts™) is developed as an "API First Platform", so as new features are released, corresponding API functionality is added to help automate and control any newly added functionality.

To add Cisco Meraki Identity™ to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source.

Key Data Source Product Configuration and Authentication Requirements

To onboard logs from this Data Source, you will need to have the following credential information

on-hand when configuring Forescout eyeAlert:

- API URL
- API KEY

Note:
To generate an API Key with Cisco Meraki Identity you must have a Dashboard Administrator account.

Suggested Information Sources for Data Source Product Configuration

Cisco provides a documentation portal for general Meraki administration here.

Cisco provides a developer documentation portal for the Meraki Dashboard API here.

Note:
The reference links above are suggestions only. To ensure accuracy, confirm that you are using the latest official documentation provided by the vendor of your Data Source product to ensure accuracy.

Target Data Logs

Forescout currently targets the following log types for ingestion:

- Air Marshall Logs
- Security Events Logs
- Network Events Logs

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON format when configuring your Data Source to make logs available for ingestion by Forescout eyeAlert.

Configure Forescout eyeAlert to Retrieve the Data Source Logs

See Configuring Forescout eyeAlert to Receive Cisco Meraki Identity Logs

Configuring Forescout eyeAlert to Receive Cisco Meraki Identity Logs

Data Source Name – Cisco Meraki Identity

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > + Add Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **API URL** – the default value is *https://api.meraki.com/api/v1*.
2. Enter the API Key value into the **API Key** field.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in

seconds – the default value is 5 minutes or *600*.
4. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default and maximum being 30 days expressed in seconds as *2592000*.
5. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is *Pulling*for periodic retrieval of target data logs.
7. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Cisco Secure Email (Push)

Cisco™ Secure Email™ (formerly Email Security Appliance and **Cisco IronPort**) provides advanced threat defense capabilities that detect, block, and remediate threats in incoming email.

To add the Cisco Secure Email Data Source to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Cisco provides a user documentation portal here.

Target Data Logs

Forescout currently processes Text Mail, CLI Audit, GUI, HTTP, Anti-Spam, Anti-Virus, and Audit logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic.

Cisco Sourcefire (Push)

The Cisco™ Sourcefire™ Next-Generation IPS integrates real-time contextual awareness, intelligent security automation, and unprecedented performance with industry-leading network intrusion prevention.To addCisco Sourcefire to Forescout eyeAlert as a Data Source, complete the following tasks:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Cisco provides a user documentation portal here.

Target Data Logs

Forescout currently processes network security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Cisco Secure Endpoint (Pull)

Cisco Secure Endpoint (Formally Advanced Malware Protection (AMP)) is a cloud-managed endpoint security solution that provides advanced protection against viruses, malware, and other cyber-threats by detecting, preventing, and responding to threats. To add Cisco Secure Endpoint to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Cisco Secure Endpoint in the Forescout eyeAlert UI

Target Data Logs

The following logs are relevant for Forescout eyeAlert ingestion:

- Events
- Vulnerabilities

Cisco Secure Endpoint Customer Side Configuration Prequisites

Forescout eyeAlert uses the pull mechanism to ingest logs from this Data Source. To configure Cisco Secure Endpoint to send logs to command you need to determine and/or generate a client ID and API Key and then input this information during the procedure to configure command to receive the logs.

To generate a Client ID and API Key:

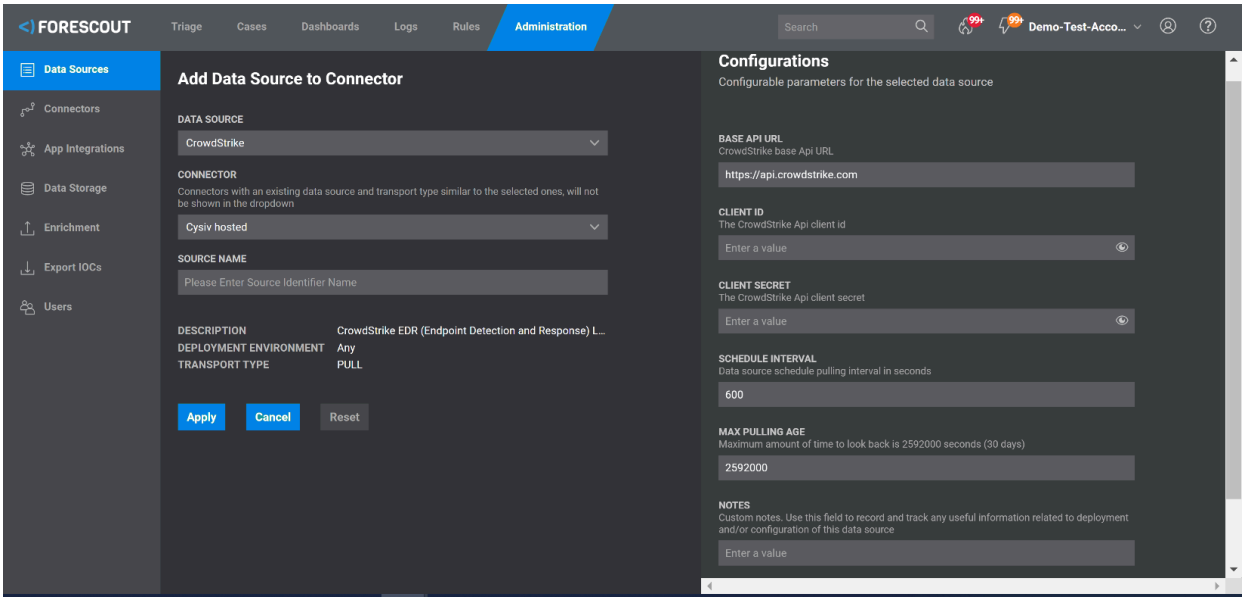
1. Log in to your AMP for Endpoints Console.
2. Go to **Accounts** > **API Credentials**.
3. Click New API Credential to generate an API Key and Client ID.

Proceed now to Cisco Secure Endpoint - Selecting the New Data Source.

Selecting the Cisco Secure Endpoint Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.

1. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
2. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
3. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.



The available configuration options will vary depending on the Data Source type and Connector deployment method. The example shown above is of a CrowdStrike EDR™ Data Source where logs are pulled by a Connector that is hosted by Forescout.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Cisco Secure Endpoint Logs

Data Source Name – Cisco Secure Endpoint

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the Cisco Secure Endpoint **CLIENT ID**.
2. Enter the Cisco Secure **API KEY**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 300.
4. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 86400.
5. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
7. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Cisco WLC (Push)

Cisco™ WLC™ is a wireless lan controller used to gain control over your routers, switches, firewalls, gateways and other devices. Monitoring Cisco WLC helps you determine the performance and efficiency of every device and its associated peripherals.

To add the Cisco WLC to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Cisco provides a user documentation portal here.

Target Data Logs

Forescout currently processes network security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS

or mTLS)?" in the Push-based Data Source Onboarding topic.

Citrix

This series of topics covers all products offered by Citrix™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Citrix Netscaler (Push)

Citrix Netscaler (Push)

Citrix™ Netscaler™ is an application deliver controller (ADC). To add Citrix Netscaler to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Citrix provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

CloudFlare

This series of topics covers all products offered by Cloudflare™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

CloudFlare Security Product (Push)

CloudFlare Security Product (Push)

CloudFlare™ is a content delivery network (CDN) - a geographically distributed network of proxy servers and their data centers. It provides cybersecurity services like DDoS protection, rate limiting, and bot management.

To add CloudFlare to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

CloudFlare provides a user documentation portal here.

Target Data Logs

Forescout currently targets Firewall Traffic Reports.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Cofense

This series of topics covers all products offered by Cofense™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Cofense Intelligence

Cofense Intelligence (Pull)

Cofense Intelligence™ is a cyber security service designed to help enterprises stop dangerous malware and phishing attacks. It uses proprietary methods to automatically identify top threats to an enterprise, and provides customers with actionable intelligence, tools, and coaching to respond to attacks. To add Cofense Intelligence to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Cofense Intelligence Data Source in the Forescout eyeAlert UI

Cofense Intelligence Customer Side Configuration Prequisites

Forescout eyeAlert uses the pull mechanism in conjunction with the Cofense Intelligence API. Documentation explaining how to configure the Cofense Intelligence API is available to Cofense customer only here.

During the procedure to configure Forescout eyeAlert to receive Cofense Intelligence logs, it is assumed that the Cofense API has been correctly configured. The following information will be required during the procedure:

- API USERNAME
- API PASSWORD

Proceed now to Selecting the Cofense Intelligence Data Source.

Selecting the Cofense Intelligence Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to Configuring Forescout eyeAlert to Receive Cofense Intelligence Logs.

Configuring Forescout eyeAlert to Receive Cofense Intelligence Logs

Data Source Name – Cofense Intelligence

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **API USERNAME**.
2. Enter the **API PASSWORD**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 900.
4. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
7. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

CrowdStrike

This series of topics covers Data Source products offered by CrowdStrike that are supported by Forescout eyeAlert.

CrowdStrike Falcon Data Replicator (Push)

CrowdStrike™ Falcon™ Data Replicator™ (Push)

The CrowdStrike™ Falcon™ Data Replicator™ can be used to push logs to an endpoint, such as an S3 bucket or Forescout eyeAlert.

To add CrowdStrike Falcon Data Replicator to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Push the logs to an AWS S3 bucket. Then pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic in the *Forescout Cloud Connector Configuration Guide*.

Instructions and/or Suggested Information Sources

CrowdStrike provides a resource center here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

When the logs have been successfully pushed to the S3 Bucket, pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic.

CrowdStrike™ Falcon™ Identity Protection™ (Push)

CrowdStrike™ Falcon™ Identity Protection™ consists of Falcon Zero Trust, which enable frictionless Zero Trust security with real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics, and Falcon Identity Threat Detection, which is for organizations that want only identity-based threat incident alerts and threat hunting without analytics or automatic prevention.

To add CrowdStrike Falcon Identity Protection to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

CrowdStrike provides a resource center here.

Target Data Logs

Forescout currently targets the following log types for ingestion:

- System Notifications
- System Audit Log
- Incidents

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout TDR.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

CrowdStrike Hosts (Pull)

The CrowdStrike™ Falcon Platform™ (CrowdStrike™ Hosts™) is developed as an "API First Platform", so as new features are released, corresponding API functionality is added to help automate and control any newly added functionality.

To add CrowdStrike™ Hosts™ to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source.

Key Data Source Product Configuration and Authentication Requirements

To onboard logs from this Data Source, you will need to have the following credential information on-hand when configuring Forescout eyeAlert:

- BASE API URL
- CLIENT ID
- CLIENT SECRET

Note:
To define a CrowdStrike API client you must be designated the "Falcon Administrator" role to view, create, or modify API clients or keys. Secrets are only shown when a new API Client is created or when it is reset.

Suggested Information Sources for Data Source Product Configuration

CrowdStrike provides a resource center here.

CrowdStrike provides access to Swagger for API documentation purposes and to simplify the development process. Each CrowdStrike cloud environment has a unique Swagger page. Please refer to the CrowdStrike OAuth2-Based APIs documentation for your cloud environment.

Note:
The reference links above are suggestions only. To ensure accuracy, confirm that you are using the latest official documentation provided by the vendor of your Data Source product to ensure accuracy.

Target Data Logs

Forescout currently targets Hosts logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON format when configuring your Data Source to make logs available for ingestion by Forescout eyeAlert.

Configure Forescout eyeAlert to Retrieve the Data Source Logs

See Configuring Forescout eyeAlert to Receive CrowdStrike Hosts Logs.

Configuring Forescout eyeAlert to Receive CrowdStrike Hosts Logs

Data Source Name – CrowdStrike Hosts

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > + Add Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **BASE API URL** – the default value is*https://api.crowdstrike.com*.
2. Enter the CrowdStrike API client id into the **CLIENT ID** field.
3. Enter the CrowdStrike API client secret into the **CLIENT SECRET** field.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is *600*.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as *2592000*.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is *Pulling* for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Crowdstrike Replicator AWS Bucket (Pull)

Refer to "AWS Storage Bucket" in the Forescout Cloud Data Source Connector Configuration Guide.

CrowdStrike EDR (Pull)

CrowdStrike Endpoint Detection and Response (EDR)is a cybersecurity solution that detects and mitigates cyber threats by continuously monitoring endpoint devices and analyzing endpoint data. To add CrowdStrike EDR to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configuring Forescout eyeAlert to Receive CrowdStrike EDR Data Logs.

CrowdStrike offers the following primary APIs:

- **Falcon Streaming API**provides data through a streaming HTTP connection. An HTTPS connection is opened between a consumer client and the Falcon Streaming API, and new events are sent as they occur. Crowdstrike also offers the SIEM connector client to simplify ingestion and enable conversion into syslog formats.
- **Falcon Data Replicator API**provides a means to pull raw event data from a Threat Graph, and once the data is pulled it can be ingested, transformed, and analyzed.
- **Falcon Threat Graph API**provides insight into the relationships between indicators of compromise (IOCs), devices, and processes. These relationships can be visualized using tools such as Maltego.
- **Falcon Query API** offers a series of HTTPS REST APIs that operate according to a standard request-response model. Responses are formatted in JSON.

CrowdStrike EDR Customer-Side Prerequisites

Crowdstrike must be properly configured using one of two methods as follows:

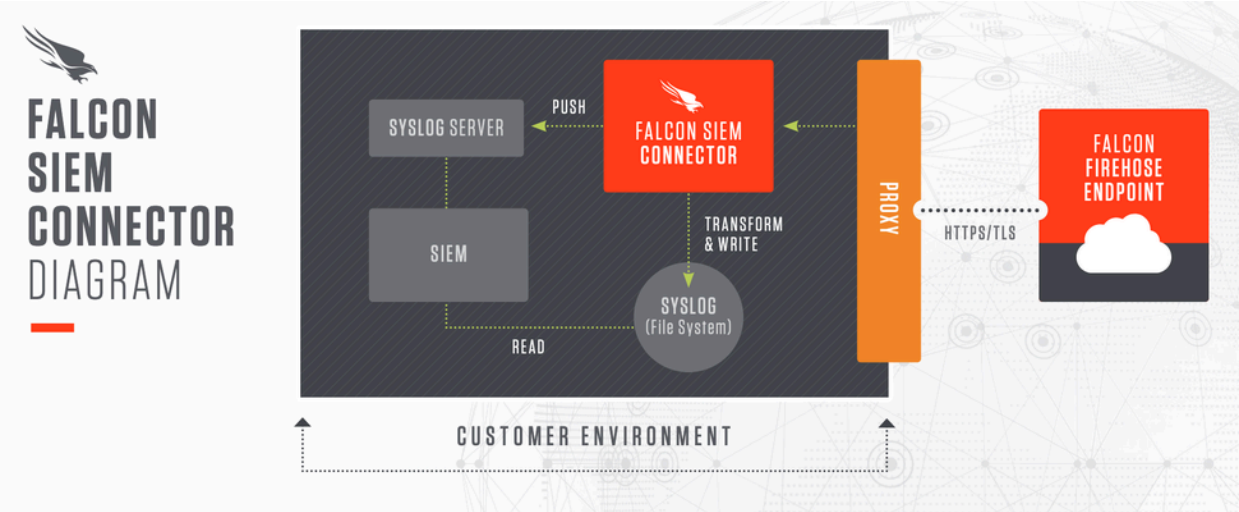
- Falcon SIEM Connector and Falcon Streaming API
- Falcon Data Replicator (FDR)

Using the Falcon SIEM Connector with the Falcon Streaming API

This method is easier to set up and supports small to medium-sized deployments. The Falcon SIEM Connector streamlines the process of connecting to the CrowdStrike Falcon Streaming API and importing the data into external SIEMs and other log management tools by doing the following:

- Transforming Falcon Streaming API data into a format that a SIEM can consume.
- Maintaining the connection to the CrowdStrike Falcon Streaming API (FireHose EndPoint) and your SIEM.
- Managing the data-stream pointer to prevent data loss.

The SIEM connector allows you to choose how to pass data to a Syslog server or third party SIEM, as shown by the following diagram:



To define a CrowdStrike API client, you must be designated with the Falcon Administrator role to view, create, or modify API clients or keys. Secrets are only shown when a new API Client is created or when it is reset.

1. When logged into the Falcon UI, navigate to **Support** > **API Clientsand Keys**. From there you can view existing clients, add new API clients, or view the audit log.
2. Click "Add new API Client" you will be prompted to give a descriptive name and select the appropriate API scopes.
3. Click **Save**, and you will be presented with the **Client ID** and **Client Secret**. The secret will only be shown once and should be stored in a secure place. If the Client Secret is lost, a reset must be performed and any applications relying on the Client Secret will need to be updated with the new credentials.

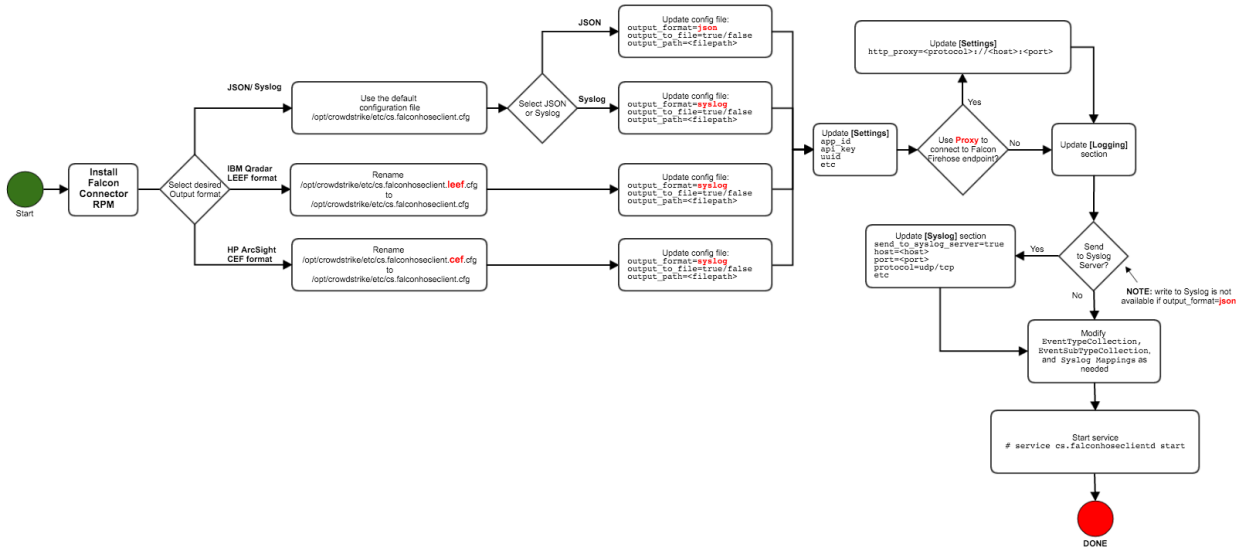
You will want to select all of the options for the API scope, with "READ" permissions:

API SCOPES

	Read	Write
Custom IOA rules	☐	☐
Detections	☐	☐
Device control policies	☐	☐
Hosts	☐	☐
Actors (Falcon X)	☐	—
Indicators (Falcon X)	☐	—
Reports (Falcon X)	☐	—
Firewall management	☐	☐
Host groups	☐	☐
Incidents	☐	☐

Save the **Client ID** and **Client Secret** - you will need them during the procedure to configure Forescout eyeAlert to ingest the logs.

The following flow diagram can assist with output selection and configuration (the "Notes" field in the Forescout eyeAlert UI can be used while configuring a new Data Source or Connector to record your configuration choices for later reference):



Target Data Logs

The SIEM Connector can output log data to a local file (the SIEM and other tools must read from the file directly) or to a Syslog Server, and includes the following event types:

- Falcon Host Detection Summary
- Falcon Host Authentication Log
- Falcon Host Detect Status Update Logs
- Customer IOC Detect Event
- Hash Spreading Event

Using the Falcon Data Replicator (FDR)

Event data can be forwarded to Forescout eyeAlert by placing it in an AWS S3 bucket, and the data can be pulled from this location. Once the raw event data is flowing into the bucket, the TDR Connector application is responsible for retrieving log data from the S3 bucket.

Data Replicator API is not installable on its own, It is a part of CrowdStrike's Falcon Suite. The process to create it goes as follows:

1. Before enabling the Falcon Data Replicator be sure to review the technical support feature guide to gain a fuller understanding of the requirements. Once you have the fuller understanding, you can proceed with those steps.

2. Contact CrowdStrike to create an S3 bucket.

   At your request they will create a CrowdStrike managed Amazon Web Services (AWS) S3 bucket for short term storage purposes as well as a SQS (simple queue service) account for monitoring changes to the S3 bucket. This S3 bucket has a 7 day retention policy by default, because data is intended to be pulled out of it for longer term retention.

3. Pull Data from the created S3 Bucket.

   Once support creates your bucket and queue, it is your responsibility to pull the raw event data from the bucket. The Simple Queue Service (SQS) simplifies this process by

publishing any file changes to the S3 bucket. You can leverage a script to monitor the SQS account for published changes, thus removing the tedious need to scan for directory and files changes.

Target Data Logs

The following event types can be captured from CrowdStrike using the Falcon Data Replicator method:

- Detection Summary Events
- User Activity Audit Events
- Authorization Activity Audit Events

CrowdStrike provides details about the FDR method here.

Selecting the CrowdStrike EDR Data Source

Selecting the CrowdStrike EDR Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Configuring Forescout eyeAlert to Receive CrowdStrike EDR Data Logs

The configuration procedure you should follow depends on which CrowdStrike Data Source type/ method you are using:

- Configuring CrowdStrike using The Falcon Streaming API Method
- Configuring CrowdStrike using the Falcon Data Replicator Method

Configuring Forescout eyeAlert to Receive CrowdStrike EDR Logs Using the Falcon Streaming API Method

Data Source Name – CrowdStrike EDR

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > + Add Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the**BASE API URL**– the default value is*https://api.crowdstrike.com*.
2. Enter the CrowdStrike API client id into the **CLIENT ID** field.
3. Enter the CrowdStrike API client secret into the **CLIENT SECRET** field.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is *600*.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as *2592000*.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is *Pulling* for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Configuring Forescout eyeAlert To Receive CrowdStrike EDR Logs Using the Falcon Data Replicator Method

See AWS Storage Bucket in the *Forescout Cloud Connector Deployment and Configuration Guide* for instructions about pulling logs from an AWS S3 Bucket.

CyberArk

This series of topics covers all products offered by CyberArk™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

CyberArk EPM (Pull)

CyberArk PAM (Push)

CyberArk EPM (Pull)

CyberArk™ Endpoint Privilege Manager™ (EPM) enforces least privilege and allows organizations to block and contain attacks at the endpoint, reducing the risk of information being stolen or encrypted and held for ransom. A combination of privilege security, application control and credential theft prevention reduces the risk of malware infection.

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the CyberArk EPM Data Source in the Forescout eyeAlert UI

Target Data Logs

The following logs are relevant for Forescout eyeAlert ingestion:

- **Get detailed raw events ⮚ Supported**

This method enables users to retrieve raw events from EPM, according to filters.

There are some adjustable query parameters along with the filters in the body.

The result is a JSON object which its structure contains: array of events, filteredCount, returnedCount and nextCursor (Optional).

- **Get policy audit raw event details ⍰Supported**

  This method enables users to retrieve policy audit raw events from EPM, according to filters.

  More about policy audits: tools that give the Set Administrator an in-depth look at policy usage.

CyberArk EPM Customer Side Configuration Prequisites

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source. To configure the Data Source to send logs to Forescout eyeAlert for ingestion and addition to the telemetry pool, complete the following procedure:

1. **Create a new user:** Account administrator

   a. In the Account Management page, go to **Create > Create User** to create an administrator account.

      i. For **Account administrator**, select **View only** (The user can only view the set and its properties).

   b. Click **Next** then, for each set, select the role for this user. A single user can manage multiple sets with different roles.

   c. Click **Finish.**

Proceed now to Selecting the CyberArk EPM Data Source**.**

Selecting the CyberArk EPM Data Source

1. Log in to Forescout TDR and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout TDR to Receive Cyberark EPM Logs

Data Source Name – Cyberark EPM

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **AUTHENTICATION SERVICE URL** for CyberArk EPM account.
2. Enter the **USERNAME** for your CyberArk EPM account.
3. Enter the **PASSWORD** for your CyberArk EPM account.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 600.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 1 day expressed in seconds as 86400.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful

CyberArk PAM (Push)

CyberArk™ is a security software company focused on eliminating cyber threats using insider privileges to attack the heart of the enterprise. CyberArk includes features that secure, maintain, and monitor privileged accounts across the global organization either on-premises or in the cloud.

To add CyberArk to Forescout TDR as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout TDR uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

CyberArk provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout TDR Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout TDR to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout TDR, and for information about configuring Forescout TDR to receive the logs.

Cylance

This series of topics covers all products offered by Cylance™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Cylance Data Source (Pull)

Cylance Data Source (Pull)

This manual is under construction.

Darktrace

This series of topics covers all products offered by Darktrace™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Darktrace DCIP (Push)

Darktrace DCIP (Push)

Darktrace is a Cyber AI platform for threat detection and response across cloud, email, industrial, and the network.

To add Darktrace to Forescout eyeAlert as a Data Source, use the following settings when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Darktrace provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for

information about configuring Forescout eyeAlert to receive the logs.

Dell

This series of topics covers all products offered by Dell™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Dell Data Domain(Push)

Dell Isilon (Push)

Dell Data Domain

This manual is under construction.

Dell Isilon

This manual is under construction.

Duo

This series of topics covers all products offered by Duo™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Duo Security

Duo Security (Pull)

Duo Security™ is a user-centric access security platform that provides two-factor authentication, endpoint security, remote access solutions and more to protect sensitive data at scale for all users, all devices and all applications.To add Duo Security to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Duo Security Data Source in the Forescout eyeAlert UI

Target Data Logs

The following logs are relevant for Forescout eyeAlert ingestion:

- **Authentication Logs** - Returns a paged list of authentication log events ranging from the last 180 days up to as recently as two minutes before the API request.
- **Authentication Logs (Legacy v1)** - The v2 authentication logs endpoint provides new filtering and querying capabilities unavailable in the legacy v1 handler, like the ability to filter on users, groups, applications, authentication results, factors, and time ranges. Consider migrating to the new handler.
- **Administrator Logs** - Returns a list of administrator log events. Only the 1000 earliest events will be returned.
- **Telephony Logs** - Returns a list of telephony log events. Only the 1000 earliest events

will be returned.
- **Offline Enrollment Logs** - Returns a list of Duo Authentication for Windows Logon offline enrollment events ranging from the last 180 days up to as recently as two minutes before the API request.

Duo Security Customer Side Configuration Prequisites

Forescout eyeAlert uses the pull mechanism to retrieve Duo Security data logs. To configure Duo Security to have data logs pulled by Forescout eyeAlert follow these steps:

1. Log in to the Duo Admin Panel and navigate to **Applications**.
2. Click **Protect an Application** and locate the entry for **Admin API** in the applications list. C
3. Click **Protect** to the far-right to configure the application and get your **integration key**, **secret key**, and **API hostname**. You'll need this information to complete your setup. See Protecting Applications for more information about protecting applications in Duo and additional application options.
4. Ensure that you enable the **Grant read log** permission.
5. The following table lists the other permissions that must be granted to the Admin API application:

Permission	Details
Grant administrators	The Admin API application can read information about, create, update, and delete Duo administrators and administrative units.
Grant read information	The Admin API application can read information about the Duo customer account's utilization.
Grant applications	The Admin API application can read information about, create, update, and delete Duo applications (referred to as "integrations" in the API).
Grant settings	The Admin API application can read and change global Duo account settings.
Grant read log	The Admin API application can read authentication, offline access, telephony, and administrator action log information.
Grant read resource	The Admin API application can read information about resource objects such as end users and devices.
Grant write resource	The Admin API application can create, update, and delete resource objects such as end users and devices.

6. Proceed to Selecting the Duo Security Data Source.

Selecting the Duo Security Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select

will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Duo Security Data Logs

Data Source Name – Duo Security

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration* > *Data Sources* > *+Data Source* > *Add Data Source to Connector – Configurations* (right-panel)

1. Enter the Duo Security **API HOSTNAME**.
2. Enter the Duo Security **SECRET KEY**.
3. Enter the Duo Security **INTEGRATION KEY**.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 900.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 7 days expressed in seconds as 604800.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

ESET

This series of topics covers all products offered by ESET™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

ESET Endpoint Security (Push)

ESET Protect Cloud (Push)

ESET Endpoint Security (Push)

ESET™ Endpoint Security™, a component of the Endpoint Protection Platform™ (EPP), is a security

solution deployed on company devices to prevent cyber attacks, detect malicious activity, and provide instant remediation capabilities, and includes the ability to detect and address fileless malware that exists only in memory.

To add ESET Endpoint Security to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

ESET Endpoint Security provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

ESET Protect Cloud (Push)

ESET™ PROTECT Cloud™ enables you to manage ESET products on workstations and servers in a networked environment with up to 50,000 devices from one central location. Using the ESET PROTECT Cloud Web Console, you can deploy ESET solutions, manage tasks, enforce security policies, monitor system status and quickly respond to problems or threats on remote computers.

To add ESET Protect Cloud to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

ESET Protect Cloud provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

ExtraHop

This series of topics covers all products offered by ExtraHop™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

ExtraHop Reveal(x) (Push)

ExtraHop Reveal(x) (Push)

ExtraHop Reveal(x)™ network detection and response automatically discovers and classifies every transaction, session, device, and asset in an enterprise.

To add ExtraHop Reveal(x) to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

ExtraHop Reveal (x) provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

F5 Networks

This series of topics covers all products offered by F5 Networks™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

F5 Big IP (Push)

F5 BigIP Syslog (Push)

F5 Big IP (Push)

The F5™ BIG-IP™ product family comprises hardware, modularized software, and virtual appliances that run the F5 TMOS operating system. Depending on the appliance selected, one or more BIG-IP product modules can be added.

To add F5 Big IP to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

F5 (Networks) BigIP provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or CEF format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

F5 BigIP Syslog (Push)

The F5™ BIG-IP™ product family comprises hardware, modularized software, and virtual appliances that run the F5 TMOS operating system. Depending on the appliance selected, one or more BIG-IP product modules can be added.

To add F5 Big IP to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

F5 Networks provides a user documentation portal here.

Target Data Logs

Forescout eyeAlert processes network security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout processes these ogs in JSON format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

F5 Distributed Cloud (Push)

F5 Distributed Cloud™ services are SaaS-based security, networking, and application management services that can be deployed across multi-cloud, on-premises, and edge locations

To add F5 Distributed Cloud to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

F5 Networks provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or CEF format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

F5 Networks (Push)

F5™ Inc. focuses on the delivery, security, performance, and availability of web applications, including the availability of computing, storage, and network resources.

F5's BIG-IP product family comprises hardware, modularized software, and virtual appliances that run the F5 TMOS operating system. Depending on the appliance selected, one or more BIG-IP product modules can be added.

To add F5 Networks to Forescout eyeAlert as a Data Source, ensure the following settings are used

when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

F5 Networks provides a user documentation portal here.

Target Data Logs

Forescout currently processes the following log types:

- Application Security Manager Violations events
- Application Security Manager Brute Force and Scraping events
- Advanced Firewall Manager events
- Network DoS Protection events
- Protocol Security events
- DNS events
- Local Traffic Manager messages

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in CEF format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Fidelis

This series of topics covers all products offered by Fidelis™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Fidelis Endpoint

Fidelis Endpoint (Pull)

Fidelis Endpoint is designed for mature security operations seeking expert level visibility, advanced detection and investigation features, open threat intelligence feeds, and automated playbooks and scripts for detection and response against known and unknown advanced cyber threats. It provides incident responders with direct, remote access into an endpoint’s disk, files and processes, to more quickly mitigate threats found on an asset.To add Fidelis Endpoint to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Fidelis Endpoint Data Source in the Forescout eyeAlert UI

Target Data Logs

The following logs are targeted for ingestion by Forescout eyeAlert:

- Alerts
- Events

Fidelis Endpoint Customer Side Configuration Prerequisites

Forescout eyeAlert uses the pull mechanism to ingest logs from this Data Source the Fidelis instance. Fidelis offers an API endpoint for each tenant, and there are APIs for each of the log types Forescout eyeAlert supports. The logs are then forwarded from the puller to Forescout eyeAlert. During the procedure to configure Forescout eyeAlert to receive Fidelis Endpoint logs you will be prompted to enter the following information from your Fidelis Endpoint configuration and account:

- FIDELIS SERVER DOMAIN
- USERNAME
- PASSWORD

Fidelis Endpoint Selecting the New Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed now to Configuring Forescout eyeAlert to Receive Fidelis Endpoint Logs.

Configuring Forescout eyeAlert to Receive Fidelis Endpoint Logs

Data Source Name – Fidelis Endpoint

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector –*

Configurations (right-panel)

1. Enter the **FIDELIS SERVER DOMAIN**.
2. Enter the **USERNAME**.
3. Enter the **PASSWORD**.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 300.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Forcepoint

This series of topics covers all products offered by Forcepoint™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Forcepoint Websense (Push)

Forecepoint NGFW (Push)

Forcepoint Websense (Push)

Forcepoint™ Websense™ software prevents employees from viewing inappropriate or malicious content, or leaking confidential data.

To add Forcepoint Websense to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

ForcePoint Websense provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you

should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Forecepoint NGFW (Push)

Forcepoint™ NGFW™ comprises several functions, including Zero Trust network access controls, Advanced Malware Detection and Protection (AMDP), and an intrusion prevention system.

To add Forcepoint NGFW to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

ForcePoint provides a user documentation portal here.

Target Data Logs

Forescout currently processes network security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Forescout

This series of topics covers all products offered by Forescout™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

eyeInspect Command Center (Push)

Forescout CyberMDX (Push)

Forescout eyeSight (Push)

Forescout Threatintel (coming soon)

Forescout eyeInspect Command Center (Push)

Forescout™ eyeInspect™ is an Network Domain Security (NDS) tool that works exceptionally well with OT focused deployments. It uses network data and asset-inventory data to trigger alerts on anomalous traffic. Forescout eyeInspect provides in-depth device visibility for OT/ICS networks and enables effective, real-time management of operational and cyber risks.

To add Forescout™ eyeInspect™ to Forescout TDR as a Data Source, note the following information and complete the following procedures:

Log Retrieval Method

Forescout TDR uses the Push mechanism to ingest logs from this Data Source.

Target Data Logs

Forescout currently processes network security logs.

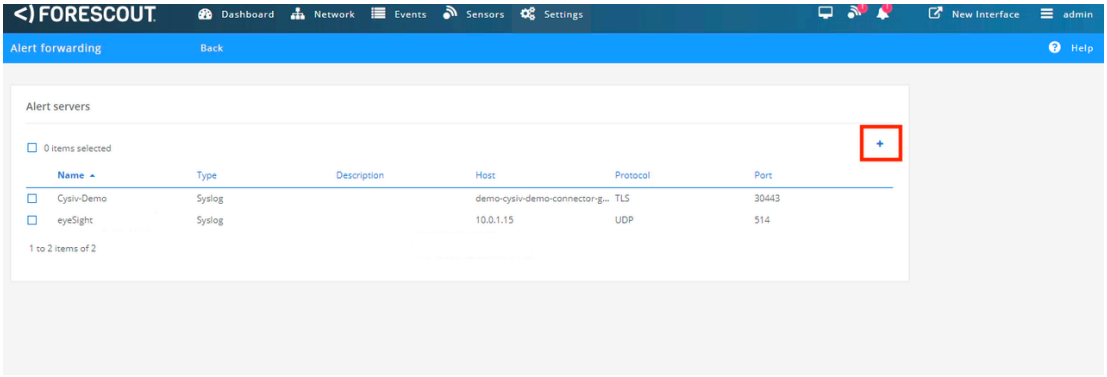
Log Format Necessary for Forescout TDR Retrieval

Forescout currently processes logs in CEF format.

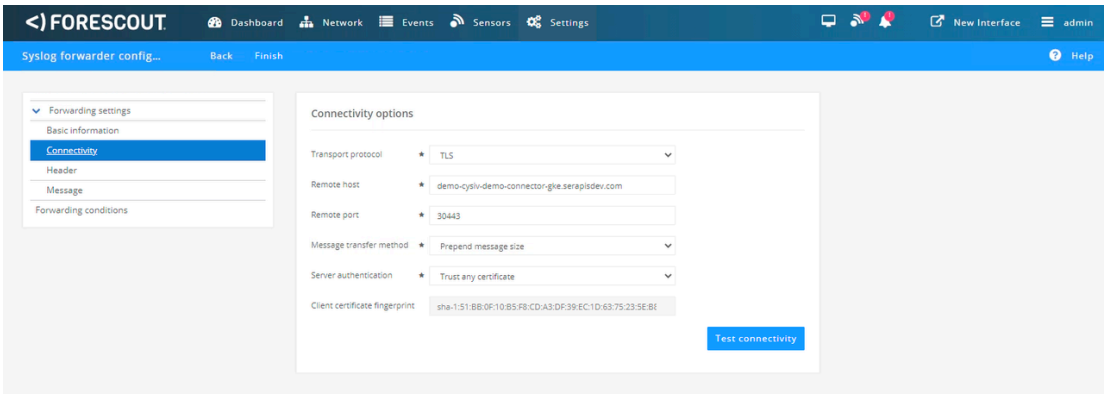
Configure Forescout eyeInspect Command Center

Complete the following steps to configure Forescout eyeInspect Command Center to push logs to Forescout TDR.

1. Log into the Forescout eyeInspect Command Center web portal as an administrator.
2. Once logged in, navigate to general settings.
3. Select the option for "Alert Forwarding".
4. Use the "+" sign in the top right corner to create a new forwarding configuration.



5. Under connectivity, select TLS for the protocol, give it the domain for the Forescout eyeAlert instance, select port 30443, and also select "Prepend message size" and "Trust any certificate", as shown here:



6. Under the message section, paste the following in for the message:

```
{tsFormattedRFC5424}
CEF:0|Forescout|CommandCenter|{sdVersion}|{typeId}|{name}|{severityNum}|ca
t=alert externalId={alertId} caseId={caseId} caseName={caseName}
rt={tsFormatted} smac={srcMac} dmac={dstMac} src={srcIp} dst={dstIp}
spt={srcPort} dpt={dstPort} shost={srcHostName} dhost={dstHostName}
proto={l4Proto} app={l7Proto} in={upDataLength} out={downDataLength}
deviceDirection={streamDir} deviceExternalId={sensorName}
cs1Label=ProfileModule cs1={profModName} cs2Label=FEAState cs2={feaState}
cn1Label=AggrAlerts cn1={feaAlertCount} deviceCustomDate1Label=FEAStart
deviceCustomDate1={feaStartMillisec} cn2Label=FEADurationSec
cn2={feaDurationSec} cs3Label=FieldPath cs3={fieldPath} cs4Label=FieldVal
cs4={fieldVal} cs5Label=ExpVals cs5={expFieldVals} cs6Label=Labels
cs6={labels} msg={desc}


0
```

Note:
The `0` character MUST be on a separate/new line. The reason for that is it will trigger Forescout to include the `\n` between logs (and then the `0` gets prepended to the next log) so that we have a way to split the logs. The `0` has to be there because Forescout uses a trim function and will remove the new line if you do not have a character after the new line. Other characters, like punctuation, will cause other errors wherein our pipeline will stop recognizing the log format as CEF.

Configure Forescout TDR to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic.

Forescout CyberMDX (Push)

CyberMDX™ is an IoT security leader dedicated to protecting the quality care of health delivery worldwide. CyberMDX provides cloud-based cyber security solutions that support the advancement of The Internet of Medical Things. The CyberMDX platform integrates with SIEM solutions by

generating alerts whenever a new cyber vulnerability, threat, or compliance case is detected.

To add CyberMDX to Forescout TDR as a Data Source, ensure the following values are used when configuring your product:

Log Retrieval Method

Forescout TDR uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Forescout provides a user documentation portal here.

Target Data Logs

Forescout currently processes alert logs.

Log Format Necessary for Forescout TDR Retrieval

Forescout currently processes logs in CEF.

Configure Forescout TDR to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout TDR, and for information about configuring Forescout TDR to receive the logs.

Forescout eyeSight (Push)

To integrate Forescout eyeSight with Forescout eyeAlert, please refer to Integrating the Forescout Cloud Data Exchange Plugin with Forescout Cloud in the *Forescout Cloud Administration Guide*.

Fortinet

This series of topics covers all products offered by Fortinet™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Fortinet FortiClient EMS (Push)

Fortinet FortiWeb (Push)

Fortinet FortiGate (Push)

Fortinet FortiMail (Push)

Fortinet Fortiwifi (Push)

Fortinet FortiClient EMS (Push)

Fortinet™ FortiClient™ Endpoint Management Server is a security management solution that enables scalable and centralized management of multiple endpoints (computers).

To add Fortinet FortiClient EMS to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Fortinet FortiClient EMS provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Fortinet FortiWeb (Push)

Fortinet™ FortiWeb™ Web Application Firewall, protects your business-critical web applications from attacks that target known and unknown vulnerabilities. The FortiWifi™ line of wireless security gateways add a built-in 802.11a/b/g wireless access point to the enterprise-level, multi-threat protection of FortiGate appliances. They provide network, content, and application protection for wired and wireless networks.

To add Fortinet FortiWeb EMS to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Fortinet FortiWeb EMS provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS

or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Fortinet FortiGate (Push)

The Fortinet™ FortiGate™ Next Generation Firewall (NGFW) protects an organization from external threats, maintaining security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection. Fortinet NGFWs meet the performance needs of highly scalable, hybrid IT architectures, enabling organizations to reduce complexity and manage security risks.

To add Fortinet FortiGate to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Fortinet provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Fortinet FortiMail (Push)

Fortinet™ FortiMail™ helps your organization prevent, detect, and respond to email-based threats including spam, phishing, malware, zero-day threats, impersonation, and Business Email Compromise (BEC) attacks.

To add Fortinet FortiMail to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Fortinet provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Fortinet Fortiwifi (Push)

Fortinet™ WAF™ (Web Application Firewall), protects your business-critical web applications from attacks that target known and unknown vulnerabilities.

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Fortinet provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic.

Gitlab

This series of topics covers all products offered by Gitlab™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Gitlab Data Source (Push)

Gitlab Data Source (Push)

GitLab™ is a web-based Git repository for devops that provides free open and private repositories, issue-following capabilities, and wikis.

To add GitLab™ to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Gitlab provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic.

Google

This series of topics covers Data Source products provided by Google that are supported by Forescout eyeAlert.

Google Security Command Center (Push)

Google Pub/Sub Streaming (Pull)

Google Workspace Formerly G Suite (Pull)

Google Storage Bucket (Push)

Google Security Command Center (Push)

The Google Cloud Security Command Center is the security and risk management platform for Google Cloud, and comes with the following built-in services for customers subscribed to the Premium tier:

- Security Health Analytics
- Web Security Scanner
- Event Threat Detection
- Container Threat Detection

To add Google Security Command Center (Push) to Forescout TDR as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout TDR uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Google provides a user documentation portal here.

Target Data Logs

Forescout currently targets Web Security Scanner and Event Threat Detection logs for ingestion.

- **Web Security Scanner** logs are results from scans of computers and application engines for common web vulnerabilities.
- **Event Threat Detection**

Log Format Necessary for Forescout TDR Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout TDR.

Configure Forescout TDR to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout TDR, and for information about configuring Forescout TDR to receive the logs.

Google Pub/Sub Streaming (Pull)

Google™ Pub/Sub™ is a fully managed real-time messaging service that allows you to send and receive messages between independent applications. For customers that have configured logs that push to a Pub/Sub queue, Forescout eyeAlert can subscribe to the queue and pull logs for retrieval.

To use Google Pub/Sub to pull logs for a particular Data Source, see Google Pub/Sub Streaming (Pull) in the *Forescout Cloud Data Source Connector Configuration Guide*.

Google Workspace Formerly G Suite (Pull)

Google™ Workspace™, formerly G Suite, is a collection of cloud computing, productivity and collaboration tools, software and products developed by Google. G Suite includes Gmail, Hangouts, Calendar, and Currents for communication; Drive for storage; Docs, Sheets, Slides, Keep, Forms, and Sites for productivity and collaboration; and, depending on the plan, an Admin panel and Vault for managing users and the services. It also includes the digital interactive whiteboard Jamboard. To add Google Storage Bucket to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Google Workspace Data Source in the Forescout eyeAlert UI

Target Data Logs

The following logs are relevant and supported by Forescout eyeAlert for ingestion:

- Chrome
- Google Drive
- Login
    - Login activity events
    - Login audit log

Google Workspace Customer Side Configuration Prerequisites

Forescout TDR uses the Google Workspace Reports API and Alert Center API for log ingestion using the PULL mechanism, which requires the use of an authorized email account with the Administrator Reports privilege enabled. For example, a super administrator typically has this privilege. Forescout recommends creating a new user (i.e., Forescout-reports@domain.com) and granting the new user the Administrator Reports privilege because the Connector's "puller" will access the data by using a service account that needs to act as this user while accessing the log data (covered in procedure 1 below).

There are two procedures below - select the procedure that applies to you. Procedure one is for configuring Google Workspace with Forescout TDR for the first time, and procedure two is for Forescout TDR accounts that have already integrated with the Google Workspace Reports API (but not the Alert Center API).

Procedure 1 - Configuring Google Workspace to Integrate with Forescout TDR for the First Time

Note: The steps below are drawn from external sources and may not represent the latest information. After the detailed procedure, a high-level task list is provided with references to vendor documentation in the event that the specific steps change over time. If you encounter problems, see the high level task list and vendor documentation references.

1. Make sure you are in the right project.
2. We need an authorized email to access any API of interest (authorized email: an email that has the administrator privileges enabled). A super administrator has this privilege.
    a. Create a new user (authorized email: Forescout-forwarder@domain.com).
        i. Go to Admin console Home page.
        ii. From the menu on the left, choose **Directory** → **Users**.
        iii. Click **Add new user**.
        iv. Fill the required data then press **Add new user (make sure to save the password that will show on the screen to be used later)**.
    b. Grant the new user you just created **Admin privileges** to the APIs of interest through adding a **custom admin role** following this page: create a custom administrator role.
        i. Go to the Admin console Home page.
        ii. From the menu on the left, choose **Account** → **Admin roles**.
        iii. Click **Create new role**.
        iv. Enter a name and, optionally, a description for the role and click **Continue**.
        v. From the **Privilege Name** list, check boxes to select each privilege that you want users with this role to have.
            1. To allow the role to access the **Reports API**, type "**reports**" in the search bar and check the box that will appear.
            2. To allow the role to access the **Alert Center API**, type "**alert center**" in the search bar and check the box that will appear (you can either choose **full access** or **view access**, both of the will work).

   c. Assign the custom role you just created to the user you just created.
      i. Go to the Admin console Home page.
      ii. Go to Users, click on the user you just created.
      iii. Scroll down until you find **Admin roles and privileges**, click on **Assign Roles**.
      iv. Look for the role you created earlier and assign it to the user (turn it on).
      v. Click **Save**.
   d. **Alternatively**, the authorized email can be and super admin email, or any user email that has the admin privileges for the APIs we need to support. However it's favorable to create the new email because the puller will access the data by using a service account that needs to impersonate this user while accessing the data.
3. **For each API we need to support**, Activate **API** service for this project:
   a. Go to Google API Console.
   b. From the menu on the left, choose **Library** → Search for the required API and choose it → Click **Enable**.
      i. For **Reports API**, search for "**Admin SDK API**".
      ii. For **Alert Center API**, search for "**Alert Center API**".
4. Create the service account (if you already have a service account, you can skip this step):
   a. Go to Google API Console.
   b. Choose **Credentials** (from the left menu).
   c. Click **CREATE CREDENTIALS** → **Service account** (no specific **permissions / users access** are needed for the service account while creating it).
5. Create a JSON key to the newly create service account:
   a. Go to Google API Console.
   b. Choose **Credentials** (from the left menu).
   c. Open the service account you created in the previous step.
   d. Take note of the Client ID (copy and paste it somewhere as you will need it inthe next step).
   e. Click **Keys** → **ADD KEY** → **Create new key** (Choose **JSON**) → Save (and keep the JSON file to use later when configuring the puller in Forescout TDR UI).
6. Delegate domain-wide authority to your service account:
   a. Go to Admin console Home page.
   b. From the menu on the left, **Security** → **Access and Data control** → **API controls**.
   c. In the **Domain wide delegation** pane, select **Manage Domain Wide Delegation**.
   d. Click **Add new**.
   e. In the **Client ID** field, enter the client ID obtained from the service account creation steps above (the service account Unique ID).
   f. In the **OAuth Scopes** field, enter the following values (only add the values corresponding to the APIs you want to be supported):
      i. **Reports API**: https://www.googleapis.com/auth/admin.reports.audit.readonly
      ii. **Alert Center API**: https://www.googleapis.com/auth/apps.alerts
   g. Click **Authorize**.
7. While configuring the puller in Forescout TDR UI, you'll need to add:
   a. service_acc_key: Copy the JSON object from the JSON key file that we downloaded earlier.
   b. authorized_user_email: Add a user email that have access to the APIs (either Forescout-forwarder@domain.com like in our case earlier, or use any user email that has admin reports and alerts privileges, or one who is a super administrator).
   c. Check the ⍰ Enable pulling logs from alert center API checkbox.
8. If needed: check these common errors while debugging the puller (related to a missing setup step while configuring the admin reports privilege, or creating the service account key).

High-level Reference (in case the granular steps above grow stale)

1. Follow the steps mentioned in the Reports API: Prerequisites page: Set up a new project in the Google API Console, and activate **Reports API** service for this project.

2. Follow the steps mentioned in the Alert Center API: Prerequisites page: Set up a new project in the Google API Console, and activate **Alert Center API** service for this project.

3. Follow the steps mentioned in the Perform G Suite Domain-Wide Delegation of Authority page: Create the service account and its credentials, then delegate domain-wide authority to your service account.

4. While configuring a Google Workspace data source in the Forescout TDR UI: Add the `email of the service account`, and Add the JSON object from the `private key file` (in JSON format) that you get after performing step 2.

Procedure 2 - Updating an Existing Google Workspace-Forescout TDR Integration to use the Alert Center API

1. We need an authorized email to access any API of interest (authorized email: an email that has the administrator privileges enabled). A super administrator has this privilege.
    a. Update the user authorized email used for the Forescout TDR integration (it is created in the procedure above) and grant it Admin privileges to the new API(s) of interest through editing the custom admin role you created previously.
        i. Go to Admin console Home page.
        ii. From the menu on the left, go to **Account** → **Admin roles**.
        iii. Click the custom role that you want to edit (the one you created previously in the "Configuring Google Workspace for the first time" section).
        iv. Choose an action:
            1. To edit the name or description of the role, click Edit Role Info and make the changes.
            2. To edit the privileges associated with the role, click Privileges and check the boxes to select each privilege that you want users with this role to have.
                a. To add Alert center API, type "alert center" in the search bar and check the box that will appear (you can either choose full access or view access, both of the will work).
        v. Click **Save**.
2. For each API we need to support, Activate API service for this project:
    a. Go to Google API Console.
    b. From the menu on the left, choose Library → Search for the required API and choose it → Click Enable.
        i. For Alert Center API, search for "Alert Center API".
3. Delegate domain-wide authority to your service account:
    a. From your G Suite domain's Admin console, go to **Main menu** → **Security** → **Access and Data control** → **API controls**.
    b. In the **Domain wide delegation** pane, select **Manage Domain Wide Delegation**.
    c. For the API client already being used, click **Edit**.
    d. In the **OAuth Scopes** field, add the following extra value:
        i. **Alert Center API**: https://www.googleapis.com/auth/apps.alerts
    e. Click **Authorize**.

Google Workspace Selecting a New Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed next to Configuring Forescout eyeAlert to Receive Google Workspace Data Logs.

Configuring Forescout TDR to Receive Google Workspace Data Logs

Data Source Name – Google Workspace

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the Google **SERVICE ACCOUNT KEY**.
2. Enter the **AUTHORIZED USER EMAIL** account address that has access to reports in the Google Admin Console.
3. If you are collecting Alert Center API logs, click the "Enable pulling logs from alert center API" checkbox.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 300.
5. Enter the **MAX PULLING AGE** value, which is the maximum age of a log file that will be pulled, in seconds – the default is 1000.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Enter the number of **PULLER EXECUTOR REPLICAS**.
9. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Google Storage Bucket (Push)

The Google™ Storage Bucket refers to Google Storage™, which stores objects (originally limited to 100 GiB, currently up to 5 TiB) that are organized into buckets (as S3 does), with each object identified within each bucket by a unique, user-assigned key. All requests are authorized using an access control list associated with each bucket and object. The bucket is basically a secure cloud-based folder for storing files.

To use a Google Storage Bucket to pull logs for a particular Data Source, refer to Google Storage Bucket in the *Forescout Cloud Data Source Connector Configuration Guide*.

Google Security Command Center Puller (Pull)

The Google Cloud Security Command Center is the security and risk management platform for Google Cloud, and comes with the following built-in services for customers subscribed to the Premium tier:

- Security Health Analytics
- Web Security Scanner
- Event Threat Detection
- Container Threat Detection

To add Google Security Forescout eyeAlert Center to Forescout eyeAlert as a Data Source, complete the following task:

1. Review the Customer-Side Configuration Prerequisites and Configure Data Logs for Discovery by Forescout eyeAlert..
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Google Security Forescout eyeAlert Center - Puller Data Source in the Forescout eyeAlert UI.

Target Data Logs

Forescout currently targets Web Security Scanner and Event Threat Detection logs for ingestion.

- **Web Security Scanner** logs are results from scans of computers and application engines for common web vulnerabilities.
- **Event Threat Detection** logs indicate detected threats within the Google Cloud environment, including some of the most common container attacks such as suspicious binaries, suspicious libraries, and reverse shell.

Google Security Command Center Customer Side Configuration Prerequisites (Pull)

Forescout eyeAlert can receive logs from Google Security Forescout eyeAlert Center using either the push or pull method. The following references are relevant to configuring Google Security Forescout eyeAlert Center, with steps for the recommended push and pull methods provided below:

- Security Forescout eyeAlert Center API | Google Cloud

- Web Security Scanner API | Security Forescout eyeAlert Center | Google Cloud
- Exporting Security Forescout eyeAlert Center data | Google Cloud
- Access control | Security Forescout eyeAlert Center | Google Cloud
- Accessing Security Forescout eyeAlert Center using an SDK | Google Cloud
- Listing security findings using the Security Forescout eyeAlert Center API

Note: Successful completion of this procedure requires collaboration with a Forescout Solution Architect to configure the Forescout puller.

The following procedure, which is based on the Google Cloud documentation located here, details how to configure the Google Security Forescout eyeAlert Center Data Source to for direct pulling of logs into Forescout TDR (as opposed to pushing logs to Pub/Sub and then pulling them into Forescout eyeAlert). When you complete the below configuration procedure, the Forescout eyeAlert side of the configuration must be completed by a Forescout Solution Architect or Data Engineer.

1. Navigate to **IAM & Admin** service.
2. Choose **Service Accounts** from the menu.
3. Click on **+ Create Service Account** button.
    a. First step: Enter the required data.
    b. Second step: Choose role**Security Center Findings Viewer**from**Security Center**then click**continue.**
    c. Third step: Leave this blank and click **Done**.

    You should be navigated to**APIs & Services**in**Credentials**menu.
4. Choose the created account service from the list.
5. Navigate to the **KEYS** sub-menu.
6. Click on **ADD KEY, Create New Key.**
7. Choose **JSON** Key type then click **CREATE.**
8. Download the JSON file, which should look like this:

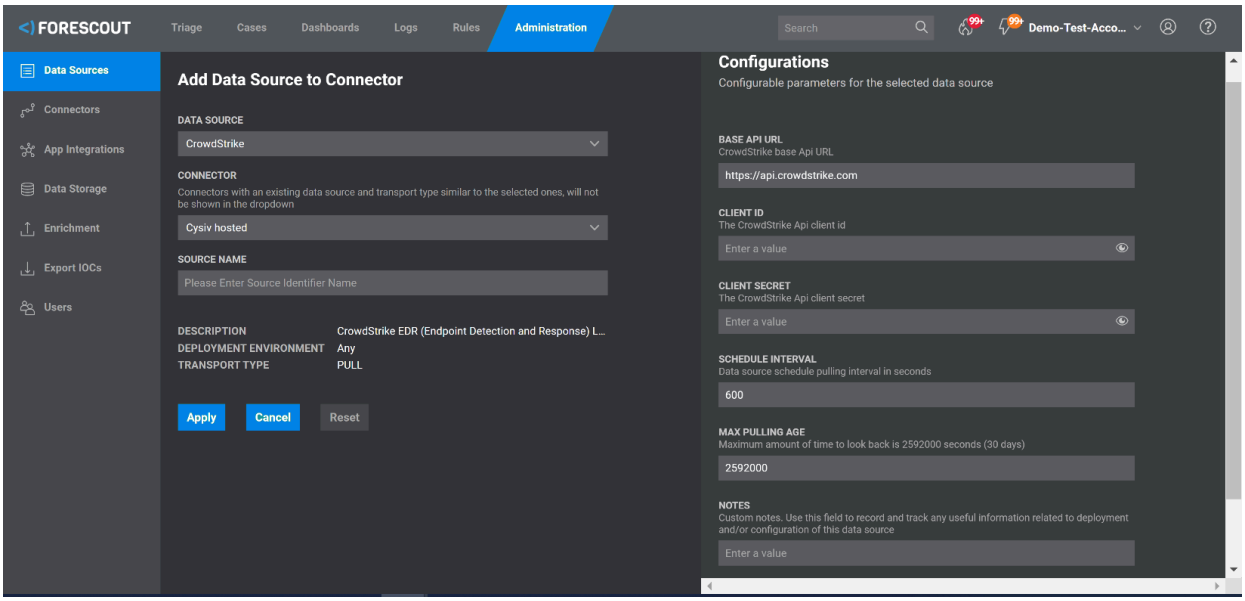
    { "type": "service_account", "project_id": "project_id", "private_key_id": "e3**********", "private_key": "-----BEGIN PRIVATE KEY-----\n**********\n-----END PRIVATE KEY-----\n", "client_email": "*******@*****.iam.gserviceaccount.com", "client_id": "11**********", "auth_uri": "https://accounts.google.com/o/oauth2/auth", "token_uri": "https://oauth2.googleapis.com/token", "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs", "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/*******%40*********.iam.gserviceaccount.com" }
9. Proceed to Selecting the Google Security Forescout eyeAlert Center Puller Data Source.

Selecting the Google Security Command Center Puller Data Source (Pull)

1. Log in to Forescout XDR and click the**Administration**tab.

2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.

1. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
2. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
3. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.



The available configuration options will vary depending on the Data Source type and Connector deployment method. The example shown above is of a CrowdStrike EDR™ Data Source where logs are pulled by a Connector that is hosted by Forescout.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the XDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout TDR to Receive Google Security Command Center Puller Logs (Pull)

Data Source Name – Google Security Forescout TDR Center - Puller

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration* > *Data Sources* > *+Data Source* > *Add Data Source to Connector* – *Configurations* (right-panel)

1. Enter the **SERVICE ACCOUNT KEY** – the Google service account key (JSON format) which is connected to the Findings API.
2. Enter the **ORGANIZATION ID**.
3. Enter the **SOURCE ID –** leaving it empty will pull all sources for the organization ID**.**
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 300.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Hillstone Networks

This series of topics covers all products offered by Hillstone Networks™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

SCVPN

SCVPN

This manual is under construction.

IBM

This series of topics covers all products offered by IBM™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

IBM iSeries (Push)

IBM Datapower (Push)

IBM iSeries (Push)

The IBM iSeries™ is a midrange server designed for small businesses and departments in large enterprises.

To add IBM iSeries to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

IBM iSeries provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

IBM Datapower (Push)

To add IBM Datapower to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

IBM Datapower provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

iBoss

This series of topics covers all products offered by iBoss™ that can be used as a Data Source for

Forescout TDR log ingestion.

iBoss SWG (Push)

iBoss SWG (Push)

The iBoss™ Secure Web Gateway™ (SWG) platform includes detailed logs that include username, device name, group, source IP address, URL, timestamp and a large number of attributes needed to correlate cloud use information to specific users and devices. This allows IT administrators to quickly locate problems such as infected devices or risky users which results in faster remediation and less downtime. The logs are stored in iboss cloud and automatically backed-up to ensure data is always available when needed while eliminating the need for tape backup to preserve web logs.

To add iBoss SWG to Forescout TDR as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Push the logs to an AWS S3 bucket. Then pull the logs into Forescout TDR from the S3 Bucket by referencing this topic in the Forescout Cloud Connector Configuration Guide.

Instructions and/or Suggested Information Sources

iBoss SWG provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud security logs.

Log Format Necessary for Forescout TDR Retrieval

Forescout currently processes logs in Structured (CSV), JSON or Syslog format.

Configure Forescout TDR to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout TDR, and for information about configuring Forescout TDR to receive the logs.

Imperva

This series of topics covers all products offered by Imperva™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Imperva SecureSphere (Push)

Imperva WAF (Push)

Imperva Jsonar (coming soon)

Imperva SecureSphere (Push)

IMPERVA SecureSphere™ - Database activity monitoring (DAM) identifies and reports unauthorized behavior without severely impacting operations or productivity. To add Imperva SecureSphereto Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Imperva™ WAF™ (Web Application Firewall) protects web applications from online attacks and comes in two variants:

- On-Premise WAF (SecureSphere): SecureSphere Web Application Security solutions protect Web applications from cyber attacks.
- Cloud WAF (Incapsula): Imperva Incapsula is a cloud-based application delivery service that includes web security, DDoS protection, CDN, and load balancing.

To add Imperva WAF to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Imperva provides a user documentation portal here.

Target Data Logs

Forescout currently targets System Event for Auditing logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Imperva WAF (Push)

Imperva™ WAF™ (Web Application Firewall) protects web applications from online attacks and comes in two variants:

- On-Premise WAF (SecureSphere): SecureSphere Web Application Security solutions protect Web applications from cyber attacks.
- Cloud WAF (Incapsula): Imperva Incapsula is a cloud-based application delivery service that includes web security, DDoS protection, CDN, and load balancing.

To add Imperva WAF to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Imperva provides a user documentation portal here.

Target Data Logs

Forescout currently targets the following logs for ingestion:

- **Security logs:** Provide a detailed alert for each suspicious event detected by the Imperva proxy while protecting your network throughout its globally distributed network. All logs include the account ID and site ID references, which enables drill down into each individual customer/site.
- **Access logs S**pecify every request and response sent between your customers and the Imperva proxy. This is all the traffic that would have been sent between end-users and your origin server, including traffic that Imperva served from its cache.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Intsights

This series of topics covers all products offered by Intsights™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Intsights Data Source

IntSights Data Source (Pull)

IntSights™ is a cybersecurity protection and intelligence platform designed to neutralize cyberattacks outside the wire by monitoring an enterprise’s external digital profile across the open, deep, and dark web to identify emerging threats and orchestrate proactive response. To add IntSightsto Forescout eyeAlert as a Data Source, complete the following tasks:

On-premise Connector Deployment Environment

1. Review the Customer-Side Configuration Prerequisites and Configure Data Logs for Discovery by Forescout eyeAlert.

Hosted Connector Deployment Environment

1. Review the Customer-Side Configuration Prerequisites.

2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the IntSights Data Source in the Forescout eyeAlert UI.

Target Data Logs

Forescout currently targets alert and threat logs.

Intsights Customer Side Configuration Prerequisites

Forescout eyeAlert obtains IntSight logs using the pull mechanism and IntSight's REST API. The REST API is located at https://api.intsights.com/. Only IntSight users are authorized to access the API configuration documentation located on IntSight's documentation portal here. When you logged in, search for the online version of the information contained in the *IntSights External Threat Protection Suite User Guide* for your specific product(s). **Additional information is available for Forescout employees** here.

Using the appropriate API configuration documentation, do the following:

- Authenticate using **Basic-Authentication.**
- When making a request, use your **Account-IDand API key** for the basic authentication. You will also need to enter these during the procedure to configure Forescout eyeAlert to receive IntSights logs.
- If you need to obtain your account ID and API key, visit the IntSights cloud platform UI from the **Subscription** page.

Proceed now to Selecting the IntSights Data Source.

Selecting the Intsights Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Insights Data Logs

Data Source Name – IntSights

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration* > *Data Sources* > *+Data Source* > *Add Data Source to Connector* – *Configurations* (right-panel)

1. Enter your IntSights **ACCOUNT ID**.
2. Enter your IntSights **API Key**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 300.
4. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
5. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
6. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

ISAC

This series of topics covers all products offered by ISAC™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

ISAC Threat Intelligence

ISAC Threat Intelligence (Pull)

This is a Threat intelligence feed from ISAC, generally using TAXII format.

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the ISAC Threat Intelligence Data Source in the Forescout eyeAlert UI

Target Data Logs

The following logs are relevant for Forescout eyeAlert ingestion:

- Marking-definition
- Identity
- Indicator

ISAC Threat intelligence Customer Side Configuration Prerequisites

Forescout eyeAlert uses the Pull mechanism to ingest logs form this Data Source. The following three pieces of information are required to configure Forescout eyeAlert to receive the logs:

- A URL for the CyTaxii server.
- A Username for the account (Usually looks like a GUID)

- A password for the provided username

When you have located and secured this information, proceed to Selecting the ISAC Threat Intelligence Data Source.

Selecting the ISAC Threat Intelligence Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to Configuring Forescout eyeAlert to Receive ISAC Threat Intelligence Logs to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive ISAC Threat Intelligence Logs

Data Source Name – ISAC Threat Intelligence

Log Retrieval Method – Pull

Connector Deployment Environment – ISAC Threat Intelligence

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **API.**
2. Enter the **USERNAME**.
3. Enter the **PASSWORD**.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 86400.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Jamf

This series of topics covers all products offered by Jamf™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Jamf Protect (Push)

Jamf Protect (Push)

Jamf™ Protect™ is an enterprise endpoint security solution for the Mac. it create custom detections that protect computers with real-time monitoring for suspicious and unwanted activities, while measuring computers against the Center for Internet Security (CIS) benchmarks with security insights.

To add Jamf Protect to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Push the logs to an AWS S3 bucket. Then pull the logs into Forescout eyeAlert from the S3 Bucket by referencing this topic in the *Forescout Cloud Connector Configuration Guide*.

Instructions and/or Suggested Information Sources

Jamf provides a user documentation portal here.

Target Data Logs

Forescout currently targets the following logs for ingestion:

- Alerts: Alerts are all detections from Jamf Protect that have been reported. These detections come from Analytics and Threat Prevention database matches.
- Unified logs

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON format when configuring your Data Source to send logs to the S3 bucket.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Juniper

This series of topics covers all products offered by Juniper™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Juniper Firewall (Push)

Juniper Pulse Secure (Push)

Juniper Firewall (Push)

The Juniper™ Firewall Logs Data Source refers to Juniper Firewall vSRX™, a virtual security appliance that provides security and networking services at the perimeter or edge in virtualized private or public cloud environments. Juniper Firewall vSRX runs as a virtual machine (VM) on a standard x86 server. Juniper Firewall vSRX is built on the juniper operating system (Junos OS).

Juniper Firewall vSRX runs as a virtual machine and provides an extensive guide to installing vSRX in a virtual machine. The guide provides instructions for most cloud providers, and includes a guide for installing vSRX on your local machine using various kinds of hypervisors.

Once you have access to the firewall host, there are two main modes: the operational mode, which you enter automatically when you log in, and the configuration mode which you need to configure your firewall.

To add Juniper Firewall Logs to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring their product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Juniper provides a user documentation portal here.

Target Data Logs

Forescout currently targets the following Intrusion Detection and Prevention (IDP) and Real-Time Screen logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Juniper Pulse Secure (Push)

Juniper™ Pulse Connect Secure™ gives employees, partners and customers secure and controlled access to corporate data and applications. The applications include file servers, web servers, native messaging, e-mail clients, and hosted servers outside your trusted network.

To add Juniper Pulse Secure to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Juniper provides a user documentation portal here.

Target Data Logs

Forescout currently targets events, user access, and admin access logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Juniper ScreenOS Firewall (Push)

Juniper™ ScreenOS Firewall™ , formerly known as **Juniper NetScreen Firewall**, is real-time firewall hardware among a series of security devices that you can access through your local internet, or through the Juniper web console.

To add Juniper ScreenOS Firewall to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Juniper provides a user documentation portal here.

Target Data Logs

Forescout currently processes event logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Kemp

This series of topics covers all products offered by Kemp Technologies™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

KEMP Load Balancer (Push)

KEMP Load Balancer (Push)

The KEMP™ Load Balancer™ supports content switching, which is sometimes referred to as URL switching. This allows the Load Balancer to direct specific requests to specific Real Servers based on the contents of the requested URL.

To add Kemp Load Balancer to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Kemp provides a user documentation portal here.

Target Data Logs

Forescout currently processes load balancer logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout XDR to receive the logs.

KnowBe4

This series of topics covers all products offered by KnowB4™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

KnowBe4 PhishER (Push)

KnowBe4 PhishER (Push)

KnowBe4's **PhishER**is a Security Orchestration, Automation, and Response (SOAR) platform that manages emails that your users report as suspicious.

To add KnowBe4 PhishER to Forescout eyeAlert as a Data Source, ensure the following settings are

used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

KnowBe4 provides a user documentation portal here.

Target Data Logs

Forescout currently processes email security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Kaspersky

This series of topics covers all products offered by Kaspersky™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Kaspersky Security Center

Kaspersky Security Center (Push)

Kaspersky Security Center™ is designed for centralized execution of basic administration and maintenance tasks in an organization's network. The application provides the administrator access to detailed information about the organization's network security level; it allows configuring all the components of protection built using Kaspersky Lab applications.

To add Kaspersky Security Center to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Kaspersky provides individual PDF manuals online for specific versions of its product. Please reference the appropriate user manual for your product version.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout currently targets general event logs for ingestion.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the topic Push-based Data Source Onboarding.

Lepide

This series of topics covers all products offered by Lepide™ that can be used as a Data Source for log ingestion.

Lepide Security Center

Lepide Security Center

This manual is under construction.

Linux

This series of topics covers all products offered by Linux™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

CentOS Linux (Push)

RHEL Linux (Push)

Ubuntu Linux (Push)

SSH Logs (Push)

CentOS Linux (Push)

To add CentOS Linux to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

CentOS Linux provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout currently targets the following log types for ingestion:

- **Authentication logs (/var/log/secure):**Keep authentication logs for both successful or failed logins, and authentication processes.
- **Cron logs (/var/log/cron):** Keeps a record of Cron-related messages (cron jobs). Like when the cron daemon started a job.
- **System logs (/var/log/messages):** Shows general messages and info regarding the system. Basically a data log of all activity throughout the global system. Everything that happens on Red Hat-based systems, like CentOS or Rhel, will go in messages.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

RHEL Linux (Push)

Red Hat™ Enterprise Linux™ is an enterprise Linux operating system.

To add RHEL Linux to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

RHEL Linux provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout currently targets the following log types for ingestion:

1- Authentication logs (/var/log/secure) (supported): Keep authentication logs for both successful or failed logins, and authentication processes.

2- Cron logs (/var/log/cron) (supported): keeps a record of crond-related messages (cron jobs). Like when the cron daemon started a job.

3- System logs (/var/log/messages) (supported): Shows general messages and info regarding the system. Basically a data log of all activity throughout the global system. Know that everything that happens on Redhat-based systems, like CentOS or Rhel, will go in messages.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for

information about configuring Forscout XDR to receive the logs.

Ubuntu Linux (Push)

Ubuntu is a complete Linux operating system, freely available with both community and professional support.

To add Ubuntu Linux to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Ubuntu Linux provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout currently targets the following log types for ingestion:

- **System logs (/var/log/syslog) (supported):** Shows general messages and info regarding the system. Basically a data log of all activity throughout the global system.
- **Authentication logs (/var/log/auth.log) (supported):** Keep authentication logs for both successful or failed logins, and authentication processes.
- **Cron logs (/var/log/cron) (supported):**

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout XDR to receive the logs.

SSH Logs (Push)

SSH, or Secure Shell, is a network protocol that allows for secure communication between a client and a server over an unsecured network. SSH is commonly used to access remote servers for command execution, file transfers, and system management.

To ensure security and proper management, logging SSH activities is crucial. SSH logs can help system administrators monitor access, diagnose issues, and detect unauthorized attempts to access systems.

To add Linux SSH Logs to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

There are no external references available from Linux for configuration. Common locations for SSH logs on Linux systems include:

- **/var/log/auth.log**: This is the default location for SSH authentication logs on many Linux distributions like Ubuntu, Debian, and others that use the syslog system.
- **/var/log/secure**: This is the default location for SSH authentication logs on CentOS, RHEL, Fedora, and other distributions that use the rsyslog system.
- **/var/log/messages**: On some systems, SSH authentication logs might also be found in the main system log file.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout currently targets logs related to closed connections and option deprecation.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout eyeAlert to receive the logs.

ManageEngine

This series of topics covers all products offered by ManageEngine™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

ADAudit Plus (Push)

ADManager Plus (Push)

ADAudit Plus (Push)

To add ADAudit Plus™ to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

ManageEngine provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout currently targets Audit logs for ingestion, which record the details of any AD Management task you perform using your AD Manager Plus. The Audit Log is an effective tracking tool which helps in tracing down events like Reset Password, Delete Users, Create/Modify Users, etc.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

ADManager Plus (Push)

To add ADManager Plus™ to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

ManageEngine provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout currently targets Audit logs for ingestion, which record the details of any AD Management task you perform using your AD Manager Plus. The Audit Log is an effective tracking tool which helps in tracing down events like Reset Password, Delete Users, Create/Modify Users, etc.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

McAfee

This series of topics covers all products offered by McAfee™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

McAfee EPO Puller (Pull)

McAfee EPO Puller (Pull)

The McAfee® ePolicy Orchestrator® (McAfee® ePO™) platform enables centralized policy management and enforcement for your endpoints and enterprise security products such as McAfee Client Proxy. McAfee Client Proxy is available on-premises and from the cloud. To add McAfee to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the McAfee ePO (puller) Data Source in the Forescout eyeAlert UI

Target Data Logs

Forescout currently targets Threat Event and DLP Endpoint incident logs for ingestion.

McAfee EPO Puller Customer Side Configuration Prerequisites

Forescout eyeAlert uses the pull mechanism to ingest logs from this Data Source. The following procedure is derived from reference material located here:

1. **Create user account (reference)** — Click **Invite User**, type the email address of the person you want to invite, then click **Invite**. An invitation is sent to the new user with instructions on how to activate themselves as a user and create a password. The invitation is valid for seven days.
    a. From MVISION ePO, select **Menu** → **Configuration** → **Users & Roles**.
    b. Next to **Users**, click **Invite User**.
    c. Type the first name, last name, and the email address of the user you want to invite to create an account.
    d. Click **Invite**.
2. **Create role(reference)** with permissions and assign it to the user.
    a. From MVISION ePO, select **Menu** → **Configuration** → **Users & Roles**.
    b. Next to Roles, click **Add Role**.
    c. In the Role Name field, type the name of the role you want to create.
    d. From the Unassigned Permissions list, select the `Reporting` permission to assign it to the role.
    e. Click **Save Changes**. The details show which permissions are assigned to the selected role.
    f. Click **Edit Assignments** to view the **User Assignments** pane.

g. In the **User Assignments** pane, select the users for whom you want to assign the selected role.

h. Click **Save Changes**.

3. **Get`lient_id`(reference)**.

   a. Log in to MVISION.

   b. Go to the following pageSupport.

   c. Save the `client_id` for reference later.

Ensure you retain the following information for the procedure to configure Forescout eyeAlert to receive the logs:

- username
- password
- client_id
- url, which should be one of the values in the table below. Based on your region.

Region	URL
United States	arevents.mvision.mcafee.com
Singapore	areventssgp.mvision.mcafee.com
Frankfurt	areventsfrk.mvision.mcafee.com
Sydney	areventssyd.mvision.mcafee.com

Proceed now to Selecting the McAfee ePO (puller) Data Source.

Selecting the McAfee EPO Puller Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive McAfee EPO Puller Logs

Data Source Name – McAfee ePO (puller)

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration* > *Data Sources* > *+Data Source* > *Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **API URL**.
2. Enter the appropriate McAfee ePO **USERNAME**.
3. Enter the password into the **PASSWORD** field.
4. Enter the client id into the **CLIENT ID** field.
5. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 120 (2 minutes).
6. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being one hour expressed in seconds as 3600.
7. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
8. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
9. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

McAfee EPO (Push)

The McAfee® ePolicy Orchestrator® (McAfee® ePO™) platform enables centralized policy management and enforcement for your endpoints and enterprise security products such as McAfee Client Proxy. McAfee Client Proxy is available on-premises and from the cloud.

To add McAfee EPO to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

McAfee EPO provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout currently targets Threat Event and DLP Endpoint incident logs for ingestion.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout XDR to receive the logs.

McAfee IDS (Push)

McAfee (Network Security Platform) is a combination of network appliances and software that detects and prevents intrusions, denial of service (DoS) and distributed denial of service (DDoS) attacks, and network misuse.

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

No publicly-available documentation site for this product was found.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout currently targets Threat Event and DLP Endpoint incident logs for ingestion.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic.

Microsoft

This series of topics covers all products offered by Microsoft™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Active Directory Entities (Pull)

Advanced Threat Analytics (Push)

Azure (Pull)

IIS Web Access (Push)

Microsoft Graph Security Alerts (Pull)

Microsoft Defender ATP (coming soon)

Microsoft Defender for Endpoint (Pull)

Microsoft Defender Identity (coming soon)

Active Directory Entities (Pull)

The Active Directory Entities™ Data Source employs a puller application (TDR Connector) that connects to customer's Office 365 account and queries for entities (user/computer) and entries. The collected information is forwarded to Forescout eyeAlert in JSON format over TCP using TLS encryption and is enriched in Elasticsearch. These logs can be used by Forescout's Threat Detection Engine to automatically alert the SOC to Suspicious Entities, and by Forescout's SOC Security Analysts in the analysis and resolution of Security Incidents. To add this Data Source to Forescout eyeAlert, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Active Directory Entities Data Source in the Forescout eyeAlert UI.

Active Directory Entities Customer Side Configuration Prequisites

The following customer-side conditions must be met for a successful deployment:

Forescout's LDAP Collector currently supports Simple and NTLM authentication methods. SASL GSSAPI/KERBEROS is not supported. SSL (port 636) should be enabled by setting the LdapCollector.secureCollection flag to True in the configuration yaml file. This is the default setting, but if it is disabled insecure communication with the LDAP server will commence over port 389.

Publicly-available instructions on how to configure Active Directory Domain Services are located here.

For Forescout-only instructions on provisioning, click here.

Active Directory Entities Selecting a New Data Source

1. Log in to Forescout TDR and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout TDR to Receive Active Directory Entities Logs

Data Source Name – Active Directory Entities

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **LDAP HOST** URL.
2. Enter the **QUERY USERNAME**– this is the username without the domain name.
3. Enter the **PASSWORD** that will be used for authentication.
4. *Enter the* **BASE DN** – *the Base domain name.*
5. Enter the **SUBDIRECTORY SEARCH** – Specifies the AD forest location and type of entities that should be retrieved - To retrieve users and computers, enter: (|(objectCategory=CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com)(objectCategory
6. Enter the **CLIENT AUTHENTICATION METHOD** – The default is "simple".
7. Enable the **SECURE CONNECTION** checkbox to use SSL over port 636 (leaving it disabled will use uns-secure TCP over port 389.
8. The **LDAP SEARCH ATTRIBUTES** field can be used to limit the types of returned entity attributes – the default is ALL.
9. Use the SCHEDULE INTERVAL field to specify the pull interval schedule in seconds, with the default being 43200 (i.e., 12 hours).
10. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
11. Click the **Apply**.

The UI will indicate whether the deployment has been successful.

Advanced Threat Analytics (Push)

Microsoft Advanced Threat Analytics (ATA)™ is an on-premises platform helps protect your enterprise from multiple types of advanced targeted cyber attacks and insider threats. It leverages a proprietary network parsing engine to capture and parse network traffic of multiple protocols (Kerberos, DNS, RPC, NTLM, and others) for authentication and information gathering.

To add IIS Web Access to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Microsoft provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout eyeAlert currently processes Health Alerts and Security Alerts logs for ingestion.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Azure (Pull)

This series of topics covers all Data Sources offered by Microsoft™ under the Azure™ product line that can be used as a Data Source for Forescout eyeAlert log ingestion.

- Azure Active Directory v2.0 (Pull)
- Azure Active Directory Entities (Pull)
- Azure ATP (Pull)
- Azure Event Hub (Pull)

Azure Active Directory v2.0 (Pull)

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatisMicrosoft Azure Active Directoryis a system in Microsoft Azure that enables the identity management to configure accessibility of users and groups to services and resources. It shares the same name with a similar directory service found in Windows Server, but Azure Active Directory is not a replacement of the on-premises local directory service. Azure AD is based on Active Directory but incorporates different features such as providing identity as a service (IDaaS).To add Azure Active Directory v2.0 to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Azure Active Directory 2.0 Data Source in the Forescout eyeAlert UI

Target Data Logs

The following logs are relevant for Forescout XDR log ingestion:

- **Device:** Represents a device registered in the organization. Devices are created in the cloud using the Device Registration Service or by Intune. They're used by conditional access policies for multi-factor authentication. These devices can range from desktop and laptop machines to phones and tablets.
- **User:** Represents an Azure Active Directory (Azure AD) user account. This resource is an

open type that allows other properties to be passed in.

- **Group:** Represents an Azure Active Directory (Azure AD) group, which can be a Microsoft 365 group, or a security group. This resource is an open type that allows other properties to be passed in.

Azure Active Directory v2.0 Customer Side Configuration Prequisites

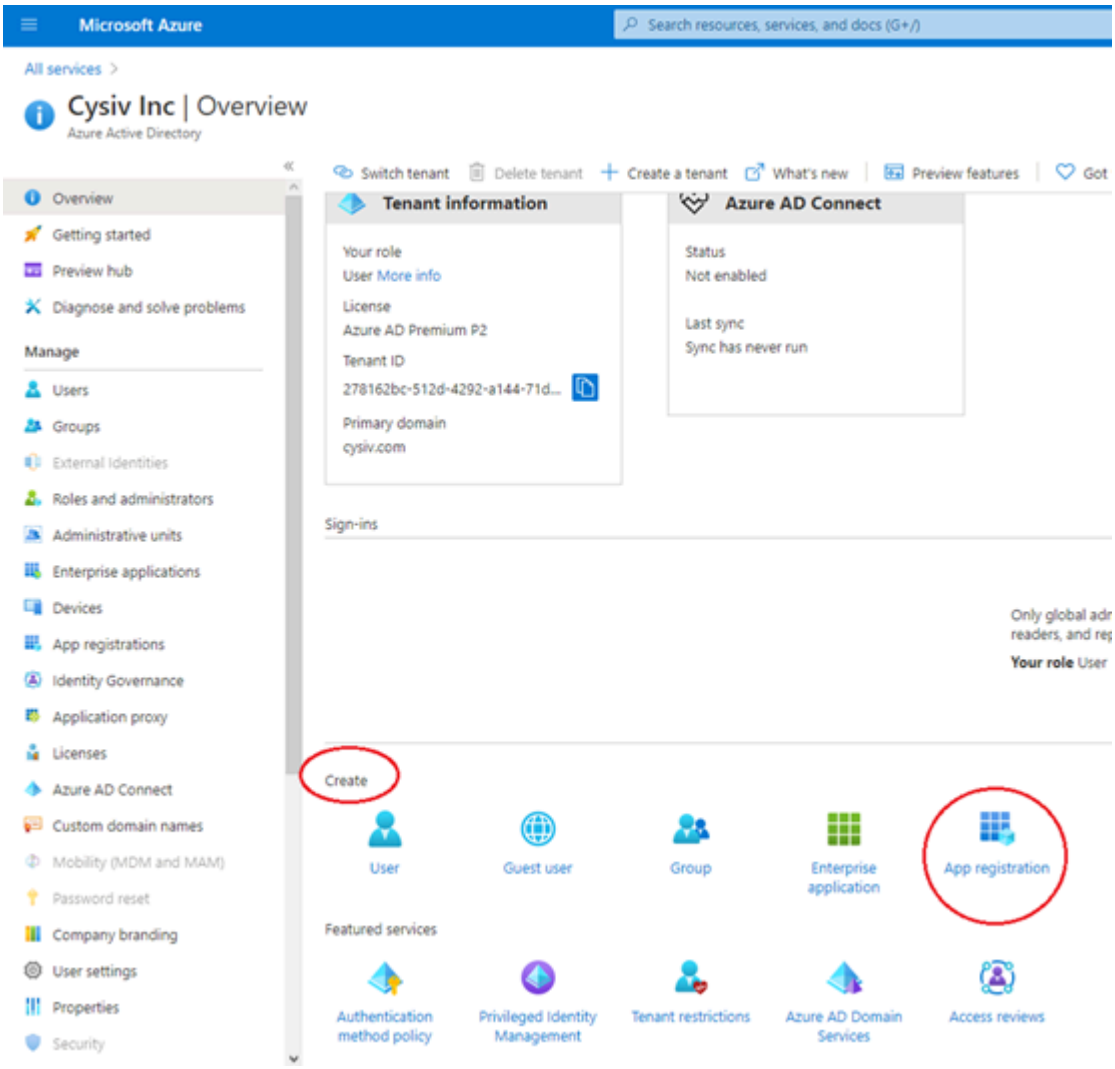
Forescout eyeAlert uses the "Pull" mechanism to ingest logs from this Data Source. The Azure Active Directory 2.0 puller connects with your Office 365 account and queries for user entries. The collected information is forwarded to Forescout eyeAlert in JSON format over TCP using TLS encryption and is enriched in Elasticsearch.

Complete the following procedure to configure Azure Active Directory 2.0 for log ingestion by Forescout eyeAlert:

1. Log in to your Azure AD account and navigate to **AzureActive Directory**. Under the “Create” section click on **App Registration**.

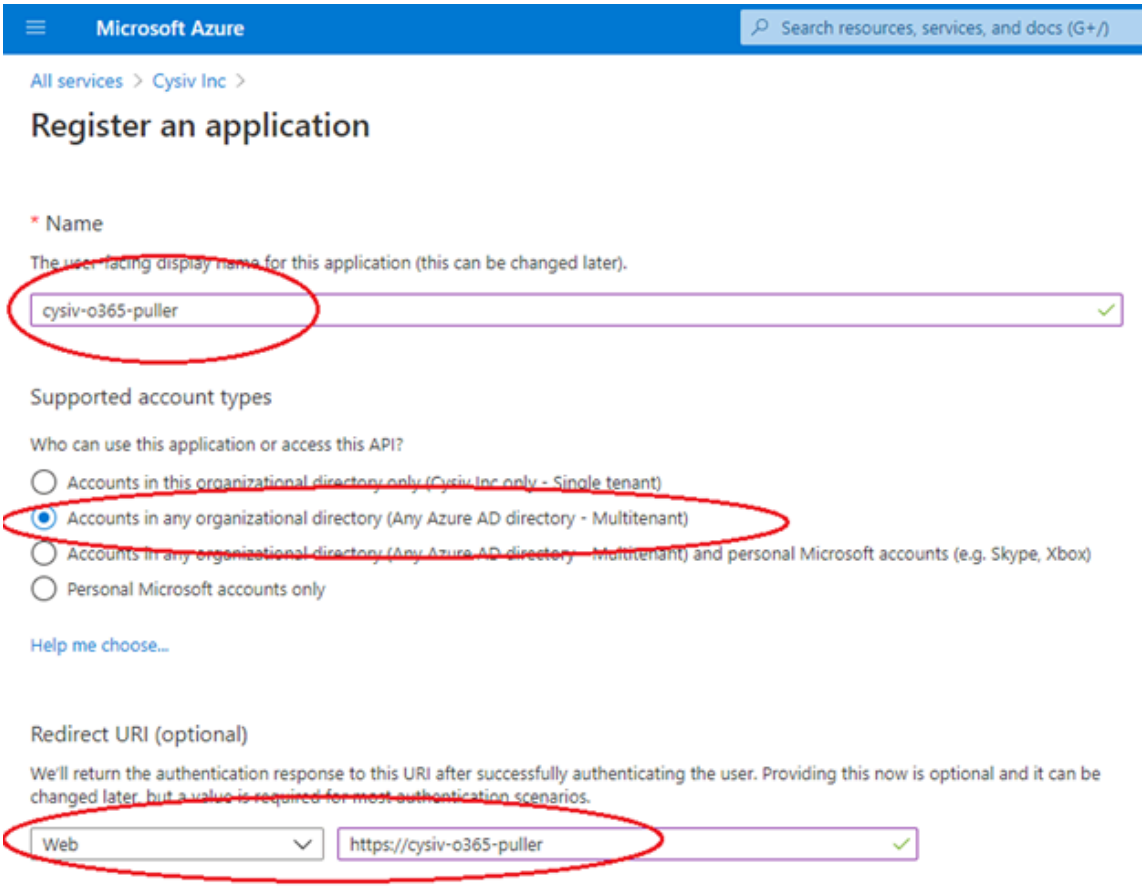
2. In the **Register an Application** screen, input a name of your choice, (i.e., forescout-o365-ad-puller).
3. Select the “Accounts in any organizational directory (Any Azure AD directory – Multitenant)” option.

4. Under the “Redirect URI (Optional)” section, leave “Web” selected, and input a URL, which matches the name you’ve chosen (i.e., https://forescout-o365-puller).



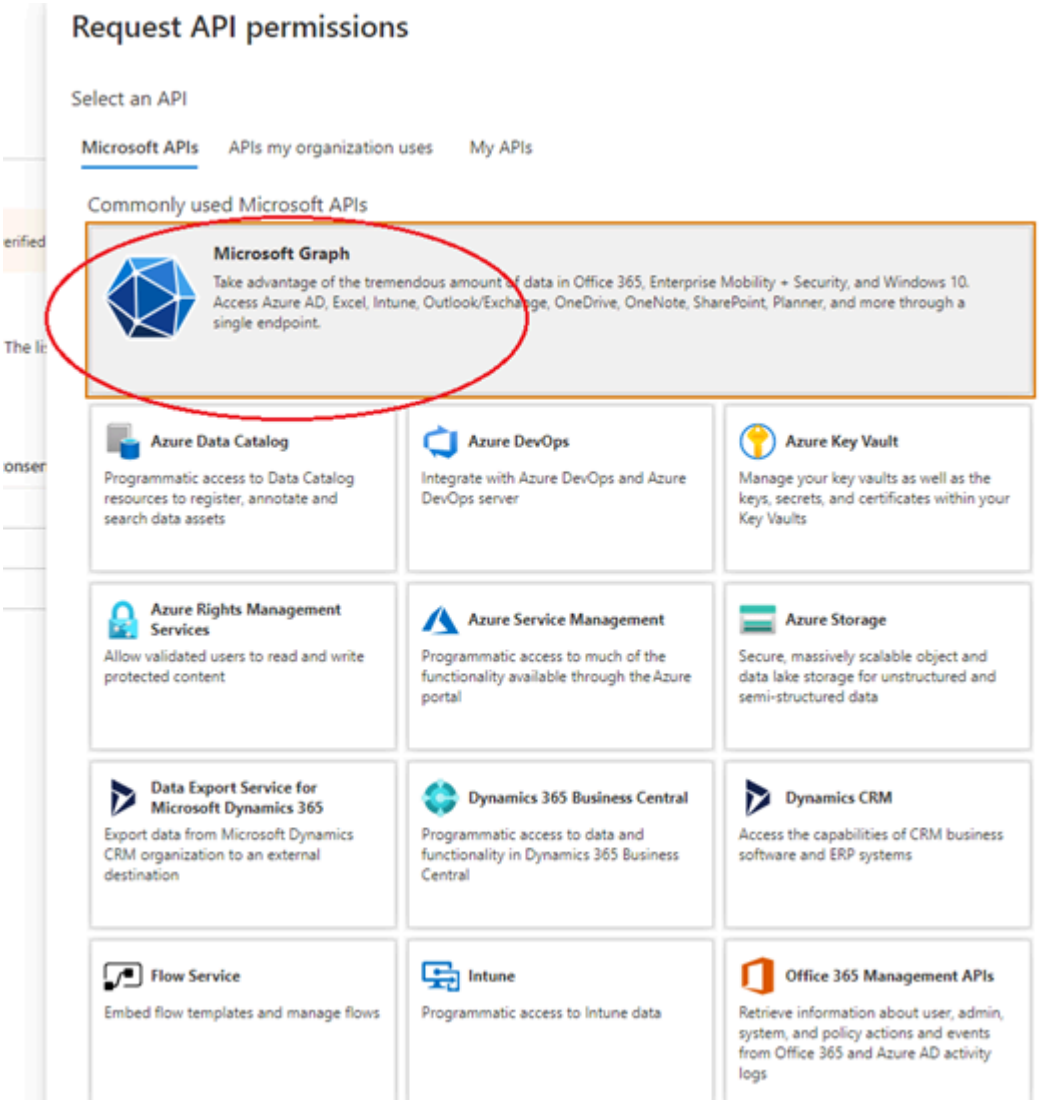
5. Click on the **Register** button.

6. Once the registration is complete, you will be presented with a screen that lists “Essentials” parameters: Application ID, Tenant ID, Object ID, etc. Ensure you copy the “Application (client) ID”. This is the Client Id which will be used for authentication. You should see a Call APIs section:



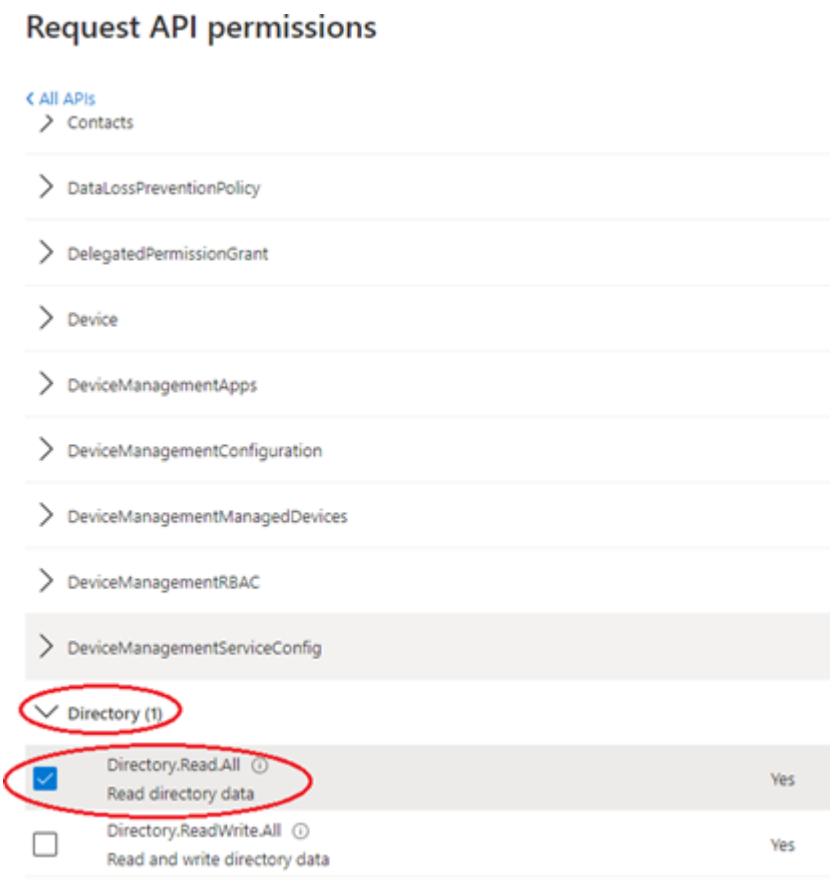
7. Click the **View API Permissions** button.
8. Click the **Add a Permission** option.

9. Click the **Microsoft Graph** box.



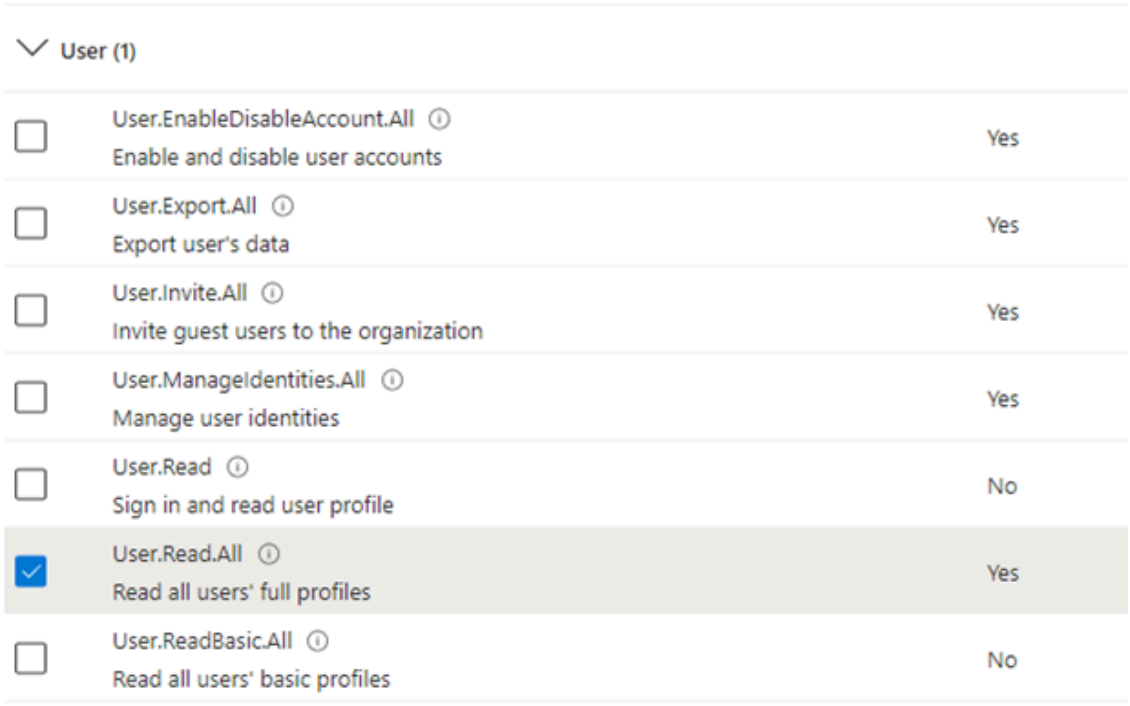
10. Click on the **Application Permissions** box.
11. Search for "directory" to find the **Directory** section and expand it.

12. Select the **Directory.Read.All** checkbox.

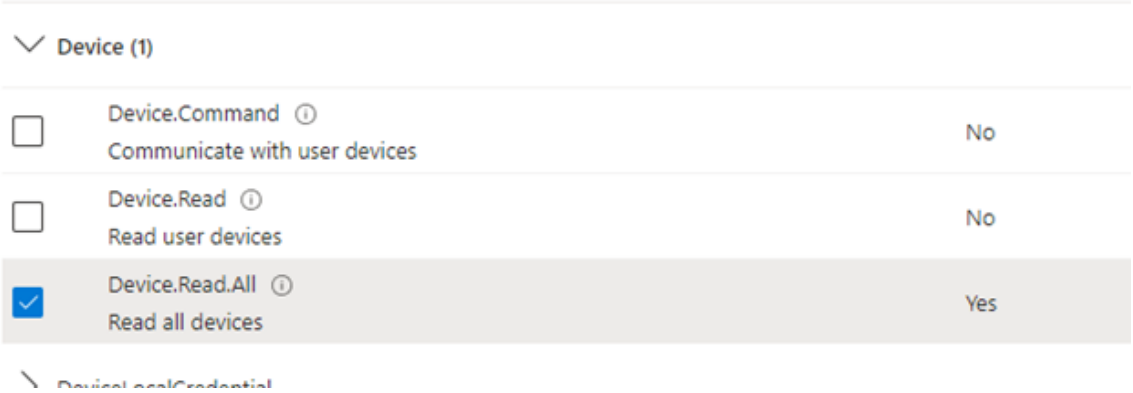


13. Search for "group" to find the **Group** section and expand it.
14. Select the **Group.Read.All** checkbox.

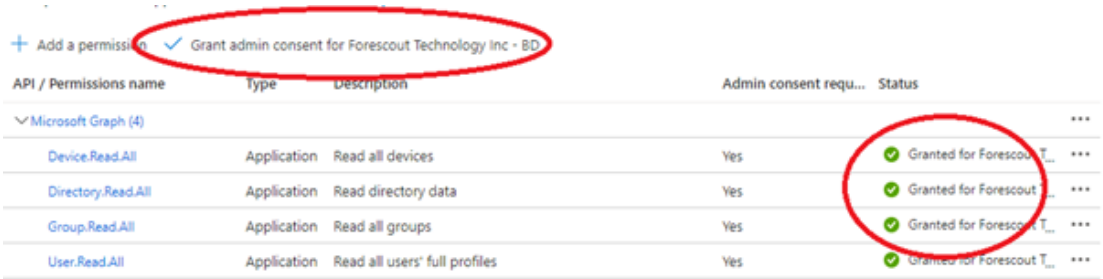
15. Find and expand the **User** section.
16. Select the **User.Read.All** checkbox.



17. Search for "device" to find the **Device** section and expand it.
18. Select the **Device.Read.All** checkbox.



19. Click **Add Permissions**.
20. Ensure you click on the **Grant admin consent...** button



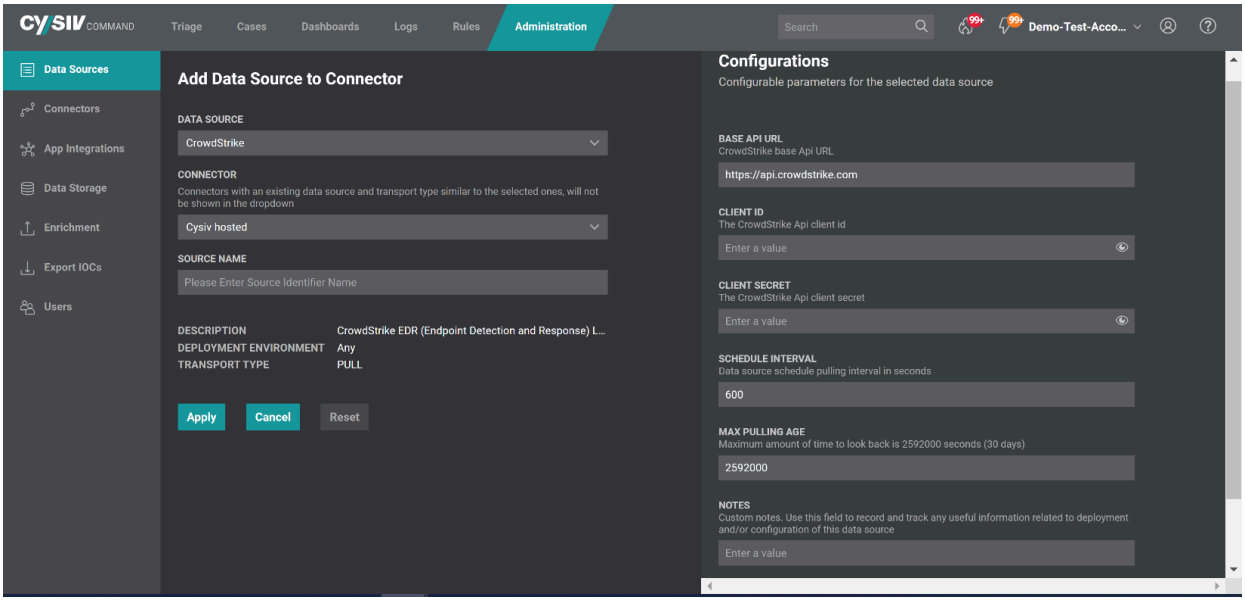
21. Click on **Certificates & secrets** (from the left-hand panel).
22. Click on "New Client Secret".
23. Add a Description (your choice).
24. Select "Expires" and select the "In 2 years" bullet.
25. Click **Add**.

26. Once added, make sure you COPY the "Value" field, and keep the Secret key value safe, as Forescout will need this key.

Selecting the Azure Active Directory v2.0 Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.

1. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
2. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
3. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.



The available configuration options will vary depending on the Data Source type and Connector deployment method. The example shown above is of a CrowdStrike EDR™ Data Source where logs are pulled by a Connector that is hosted by Forescout.

For the pull-based Data Source you are adding, the configuration parameters you should enter on

the right side of the window are typically specific to the vendor and device type. These settings are required to allow the Forescout Cloud Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Azure Active Directory v2.0 Logs

Data Source Name – Azure Active Directory v2.0

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **TENANT.**
2. Enter the **CLIENT ID**.
3. Enter the **CLIENT SECRET**.
4. Choose whether to enable Fetching Users, Devices, and Groups data and select the appropriate checkboxes.
5. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 10800.
6. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 7 days expressed in seconds as 604800.
7. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
8. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
9. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Azure Active Directory Entities (Pull)

The Azure™ Active Directory Entities Data Source is an LDAP puller that connects to a customer's Azure AD server and queries for entities (user/computer) and entries. The collected information is forwarded to Forescout eyeAlert in JSON format over TCP using TLS encryption and is enriched in Elasticsearch. To add this Data Source to Forescout eyeAlert, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Active Directory Entities Data Source in the Forescout eyeAlert UI .

Azure Active Directory Entities Customer Side Configuration Prerequisites

The following customer-side conditions must be met for a successful deployment:

Office 365 AD puller configuration assumes that the Connector cluster has already been

provisioned: Forescout collector certificates have been deployed and stored on the cluster under a secret named log-certs.

The certificates are required by Office 365 AD puller in order to communicate with Forescout eyeAlert via TLS.

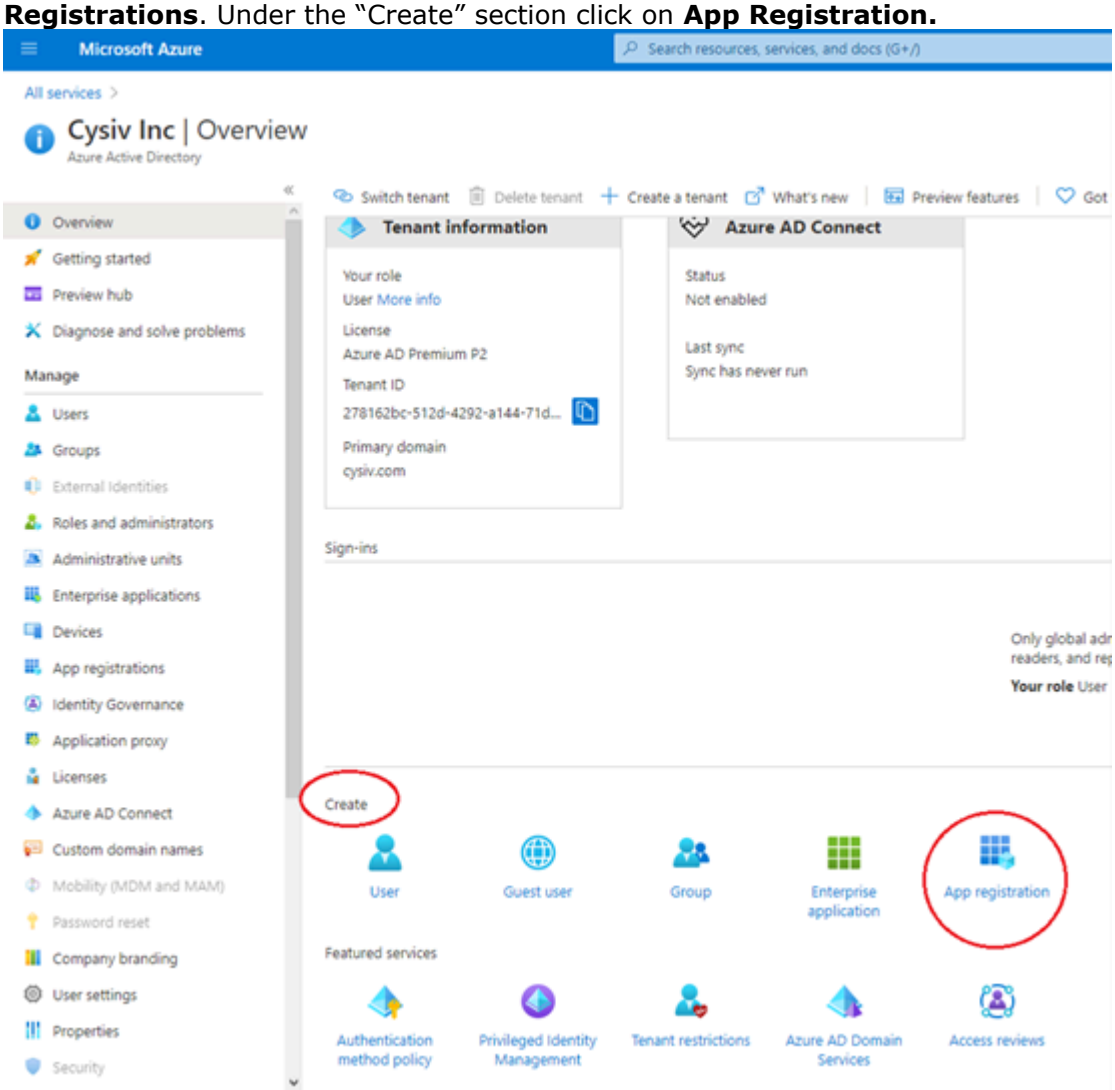
Customer-Side Azure AD Configuration Steps

Caution: These steps are provided for guidance purposes only, and should only be performed after consulting with the Forescout Security Engineer. Consult the vendor documentation for your specific product and version for the latest procedural steps.

Office 365 AD puller must be authorized by MS Azure AD using client credentials.

To generate client credentials, the app must be registered in customer's Azure AD account.

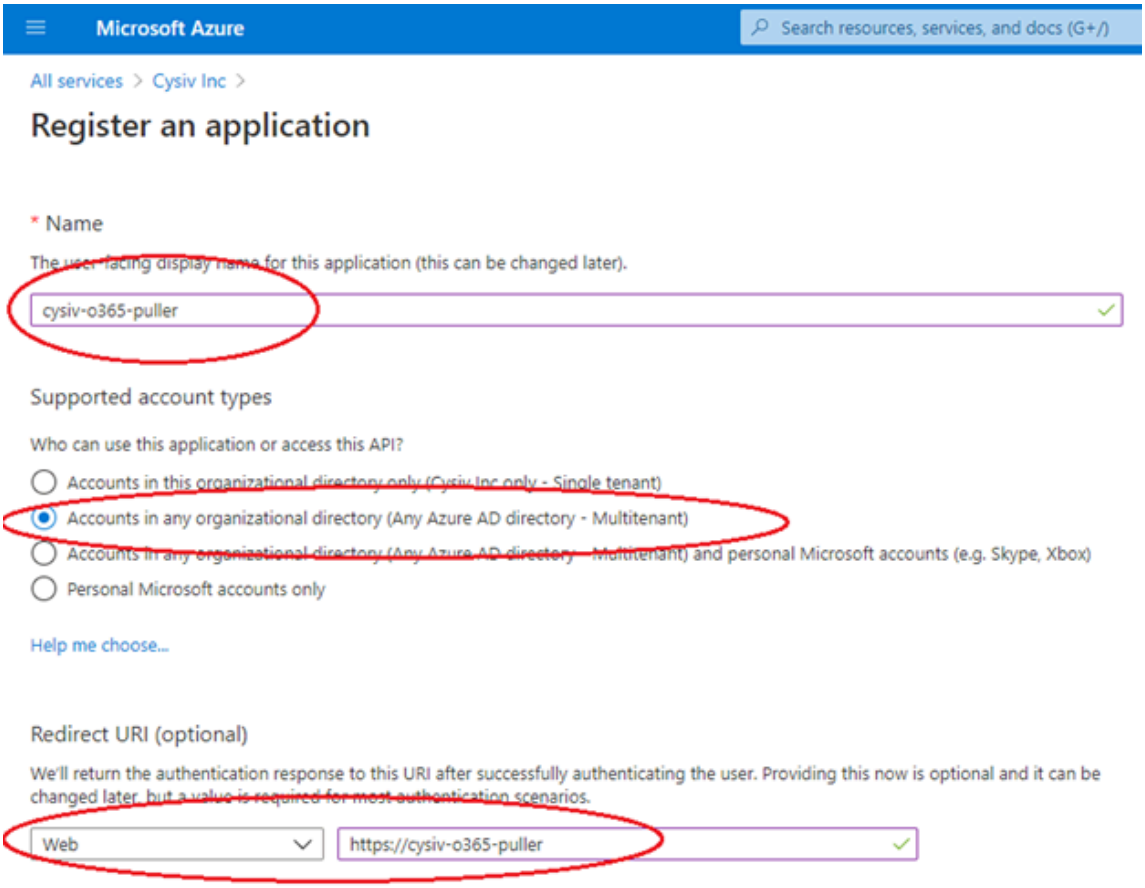
1. Login to your Azure AD account and navigate to **Azure Active Directory → App Registrations**. Under the "Create" section click on **App Registration.**



2. Under the Register an Application screen, input a "Name" (of your choice, i.e. Forescout-o365-ad-puller).

3. Select the "Accounts in any organizational directory (Any Azure AD directory – Multitenant)" option.

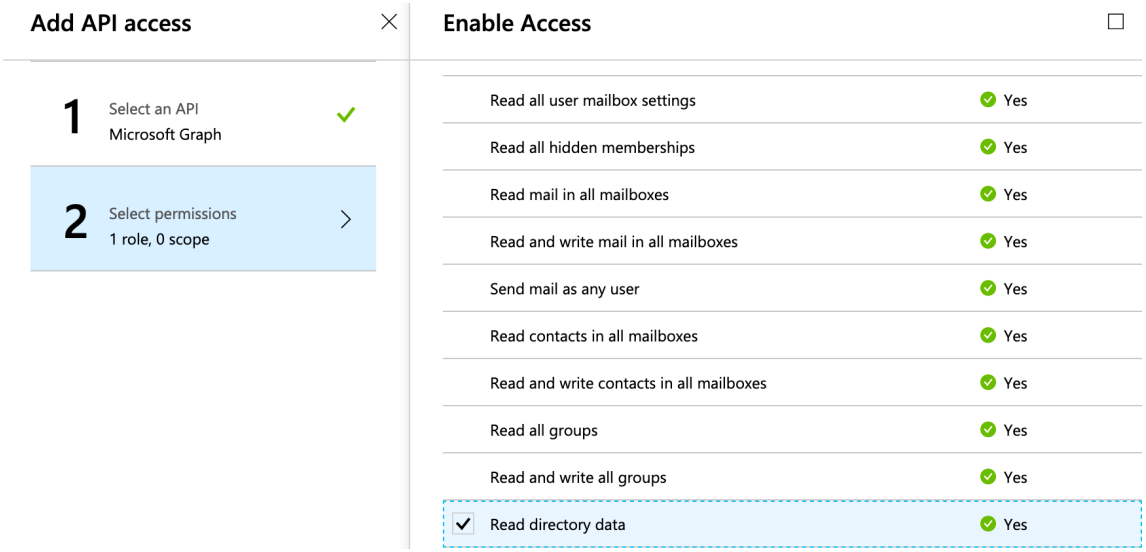
4. Under the "Redirect URI (Optional)" section, leave "Web" selected, and input a URL, which matches the name you've chosen (i.e., https://Forescout-o365-puller).



5. Click on the **Register** button.

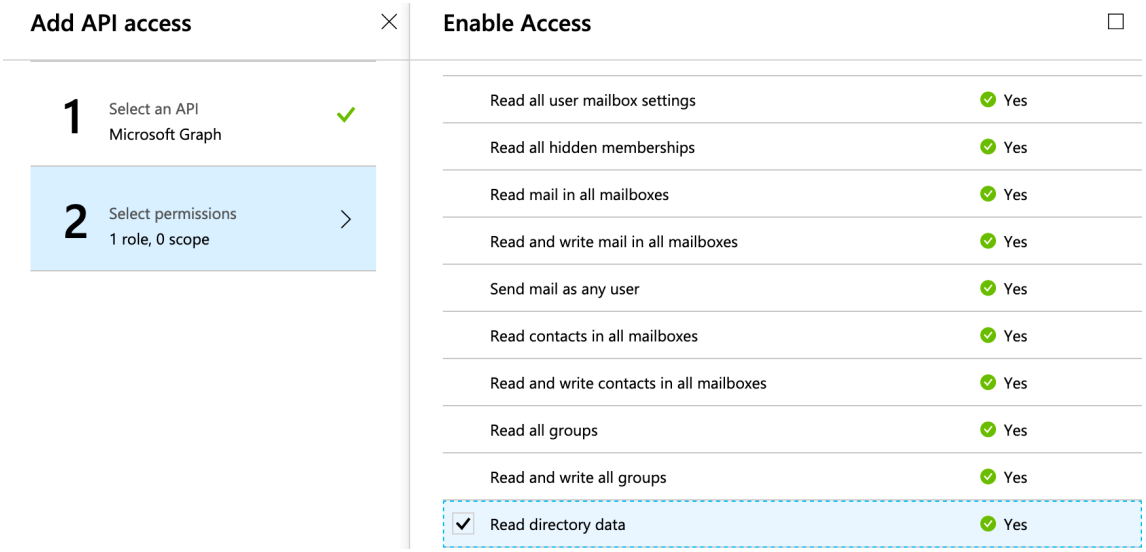
6. Once the registration is complete, you will be presented with a screen which lists Essential parameters - Application ID, Tenant ID, Object ID, etc. Ensure you copy the Application (client) ID. This is the Client Id which will be used for authentication.

   You should see a **Call APIs** section, with the **View API permissions** button



Click on View API POe

7. Click on **View API Permissions**.



8. Click on the **Add a permission** option and then click **Yes**.
9. Click on the **Application Permissions** box.
10. Scroll down to find the **Directory** section and expand it.
11. Select the **Directory.Read.All** checkbox.
12. Click on **Add Permissions**. You will have to ensure that the permission is granted (by an Administrator).
13. Click on **Certificates & secrets** (from the left-hand panel).

14. Click on **New Client Secret**.

15. Add a Description (your choice).
16. Select **Expires In 2 years** bullet.
17. Click add.

18. Once added, make sure you COPY the **Value** field, and keep the Secret key value safe.

This will need to be set as the Client Secret when configuring the data source in **Forescout eyeAlert.**

19. Proceed next to Active Directory Entities - Selecting a New Data Source.

Selecting the New Data Source for Azure Active Directory

1. Log in to Forescout eyeAlert and click the **Administration** tab.
2. On the Administration screen, click the **Data Sources** tab.
3. Click the **+ Data Source** button.
4. Click the **DATA SOURCE** dropdown and select the Data Source you are adding from the list.
5. Click the **CONNECTOR** dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".

For the Data Source you are adding, the configuration parameters you should enter on the right side of the window depend on whether the log retrieval method is Push or Pull (determined by the Data Source device type) and whether the Connector deployment environment is on-premise or hosted.

Proceed to Configuring Forescout eyeAlert to Receive Azure Active Directory Entities Data Logs.

Configuring Forescout eyeAlert to Receive Azure Active Directory Entities Data Logs

Data Source Name – Azure Active Directory Entities

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **CLIENT ID** that will be used for authentication.
2. Enter the **TENANT** name or tenant ID that be used for authentication.
3. Enter the **CLIENT SECRET that will be used for authentication.**
4. Enter any relevant **SEARCH ATTRIBUTES -** with Azure you can specify precise attributes or default to **ALL.**
5. Enter the **SCHEDULE INTERVAL** in seconds (the default is 43200 or 12 hours).
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
7. Click the **Apply** button.

TActive Directory Entites Data Logshe UI will indicate whether the deployment has been successful.

Azure ATP (Pull)

Azure™ Advanced Threat Protection (ATP) is a cloud-based security solution that leverages your on-premise Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. To add this

Data Source to Forescout eyeAlert, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Azure ATP Data Source in the Forescout eyeAlert UI

Target Data Logs

The following logs, which are available in CEF format, can be used by Forescout's Threat Detection Engine to automatically alert the SOC to Suspicious Entities, and by Forescout's SOC Security Analysts in the analysis and resolution of Security Incidents:

- Account enumeration reconnaissance
- Data exfiltration over SMB
- Honeytoken activity
- Malicious request of Data Protection API master key
- Network-mapping reconnaissance (DNS)
- Reconnaissance using directory services queries
- Remote code execution attempt
- Remote code execution over DNS
- Security principal reconnaissance (LDAP)
- Suspected brute force attack (LDAP)
- Suspected brute force attack (Kerberos, NTLM)
- Suspected DCSync attack (replication of directory services)
- Suspected Golden Ticket usage (encryption downgrade)
- Suspected Golden Ticket usage (non-existent account)
- Suspected Golden Ticket usage (ticket anomaly)
- Suspected Golden Ticket usage (time anomaly)
- Suspected Golden Ticket usage (forged authorization data)
- Suspected identity theft (Pass-the-Hash)
- Suspected identity theft (Pass-the-Ticket)
- Suspected NTLM authentication tampering
- Suspected Over-Pass-the-Hash attack (encryption downgrade)
- Suspected Skeleton Key attack (encryption downgrade)
- Suspicious authentication failures
- Suspicious communication over DNS
- Suspicious domain controller promotion (potential DcShadow attack)
- Suspicious additions to sensitive groups
- Suspicious replication of directory services
- Suspicious replication request (potential DcShadow attack)
- Suspicious service creation
- Suspicious VPN Connection
- Suspected WannaCry ransomware attack
- Suspected brute force attack (SMB)
- Suspected use of Metasploit hacking framework
- Suspected overpass-the-hash attack (Kerberos)

Azure ATP Customer Side Configuration Prerequisites

Use of Azure ATP service requires and registration with the Azure ATP Portal. The Azure ATP logs are ingestion by Forescout eyeAlert via integration with Syslog.

- To understand more about Azure ATP architecture, click here.
- For the Microsoft QuickStart guide to creating an Azure ATP instance, click here.

- For the Microsoft guide to integrating Azure ATP with Syslog, click here.

When pushing data logs to Forescout eyeAlert, ensure the following:

On Premise-Connector Deployments

- If you are using TLS, push the data logs to Forescout eyeAlert Network port 30443.
- If you are using TCP, push the data logs to Forescout eyeAlert Network port 30442.
- If you are using UDP, push the data logs to Forescout eyeAlert Network port 30441.

No further required configuration is required in the Forescout eyeAlert UI. Once the device begins sending logs in the specified format to the ports specified above, the Data Source and its data log ingestion statistics should appear in the "Discovered" category on the Data Sources screen under the Forescout eyeAlert **Administration** tab.

Hosted Connector Deployments

For hosted Connector deployments:

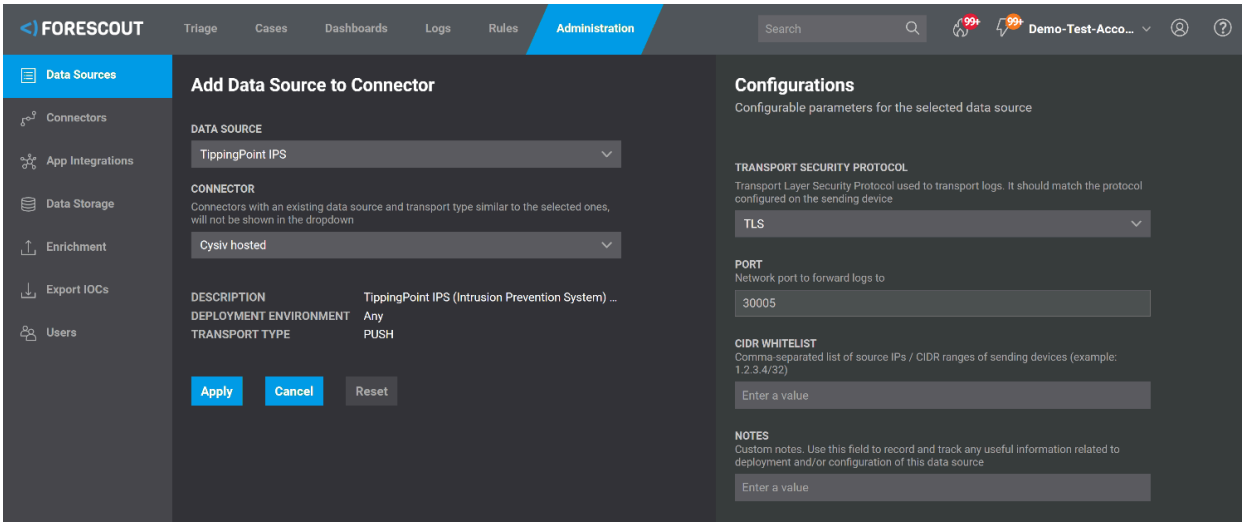
- If you are using TLS, push the data logs to Forescout eyeAlert Network port 30443.
- If you are using mTLS, push the data logs to Forescout eyeAlert Network port 30444.

When the Connector deployment environment is hosted, some configuration within the Forescout eyeAlert UI is required to establish a secure connection to the Connector Forescout has deployed on its own premises. Proceed now to Selecting the New Data Source.

Azure ATP Selecting the New Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.

1. Click the**DATA SOURCE**dropdown and select the Data Source you are adding from the list.
2. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named “Forescout hosted”.



The available configuration options will vary depending on the Data Source type and Connector deployment method. The example shown above is of a TippingPoint IPS™ Data Source where logs are pushed to a Connector that is hosted by Forescout.

For the Data Source you are adding, the configuration parameters you should enter on the right side of the window depend on whether the log retrieval method is Push or Pull (determined by the Data Source device type) and whether the Connector deployment environment is on-premise or hosted.

Proceed to Configuring Forescout eyeAlert to Receive Azure ATP Data Logs.

Configuring Forescout eyeAlert to Receive Azure ATP Data Logs

1. On the**Configurations**panel, use the**TRANSPORT SECURITY PROTOCOL**drop-down to select the transport security protocol for the Data Source.

- TLS (default port 30443)
- mTLS (default port 30444)

1. Enter the appropriate port number in the **PORT** field (the default port value will appear by default).
2. If the selected transport security protocol is TLS, in the **CIDR ALLOW-LIST** field enter a comma-separated list of the source IPs and/or CIDR ranges of the sending device(s) – for example: 1.2.3.4/32.
3. Select the preferred **TIME ZONE** from the dropdown.
4. In the **NOTES**field, enter any comments about the deployment you want preserved for later reference.

5. Click the **Download Server Certificate** (TLS) or **Download Certificate Bundle** (mTLS) button.

   Note on Client Certificate Installation: If mTLS is the selected communication protocol, ensure that you install the Client Certificate appropriately as described by the vendor documentation for the Data Source. **Note on Client Certificate Expiry:** Server Certificates expire after three years from the day of the initial configuration. As the three-year point from initial configuration approaches, ensure that you complete this procedure to renew the Client Certificate before it expires to ensure no interruption to log ingestion.

6. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Azure Event Hub (Pull)

Using Azure™ Event Hubs, you can log information obtained for Network Security Groups to get network-level logging information. To use Azure Eventhub to pull logs for a particular Data Source, see Microsoft Azure Event Hubs in the *Forescout Cloud Data Source Connector Configuration Guide*.

IIS Web Access (Push)

Internet Information Services™ (IIS) is an extensible web server software created by Microsoft for use with the Windows NT family. IIS supports HTTP, HTTP/2, HTTPS, FTP, FTPS, SMTP and NNTP and has been an integral part of the Windows NT family since Windows NT 4.0.

To add IIS Web Access to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

IIS provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout eyeAlert currently targets IIS Access Logs.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Microsoft Graph Security Alerts (Pull)

Microsoft™ Graph™ is a reporting feature of Microsoft Office 365. It provides a unified programmability model that can be used to access the tremendous amount of data in Microsoft 365, Windows 10, and Enterprise Mobility + Security. To add Microsoft Graph Security Alerts to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Microsoft Defender Data Source in the Forescout eyeAlert UI

Target Data Logs

Forescout targets Microsoft Graph alert logs for ingestion.

Microsoft Graph Customer Side Configuration Prerequisites

The Microsoft Graph API is used to pull different logs from different Microsoft data sources.

Configuring the Graph API in Forescout eyeAlert require three parameters: API Url, client ID and client secret.

To get these values please follow the same steps as the customer-side configuration for the Office 365 Management APIs, but at step 5 select "Microsoft Graph" instead of "Office 365 Management APIs". See the Microsoft Graph permission reference for information about the permissions you need.

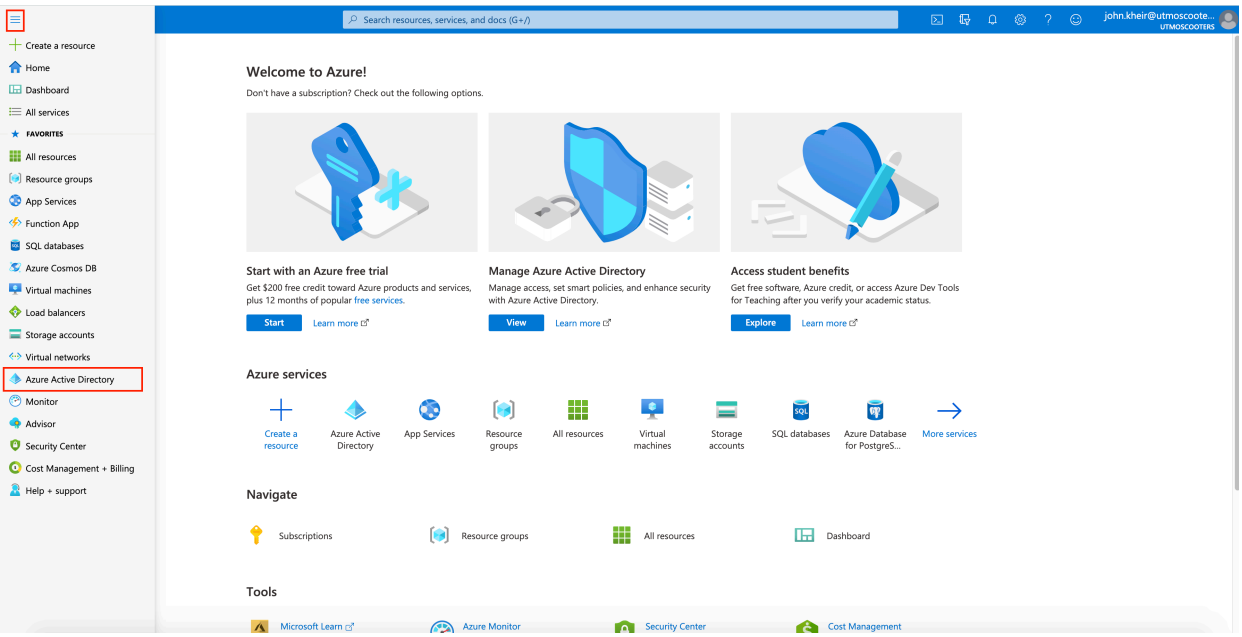
This procedure is based on the detailed Microsoft procedures located here.

Caution: These steps are provided for guidance purposes only, and should only be performed after consulting with the Forescout Security Engineer. Consult the vendor documentation for your specific product and version for the latest procedural steps.

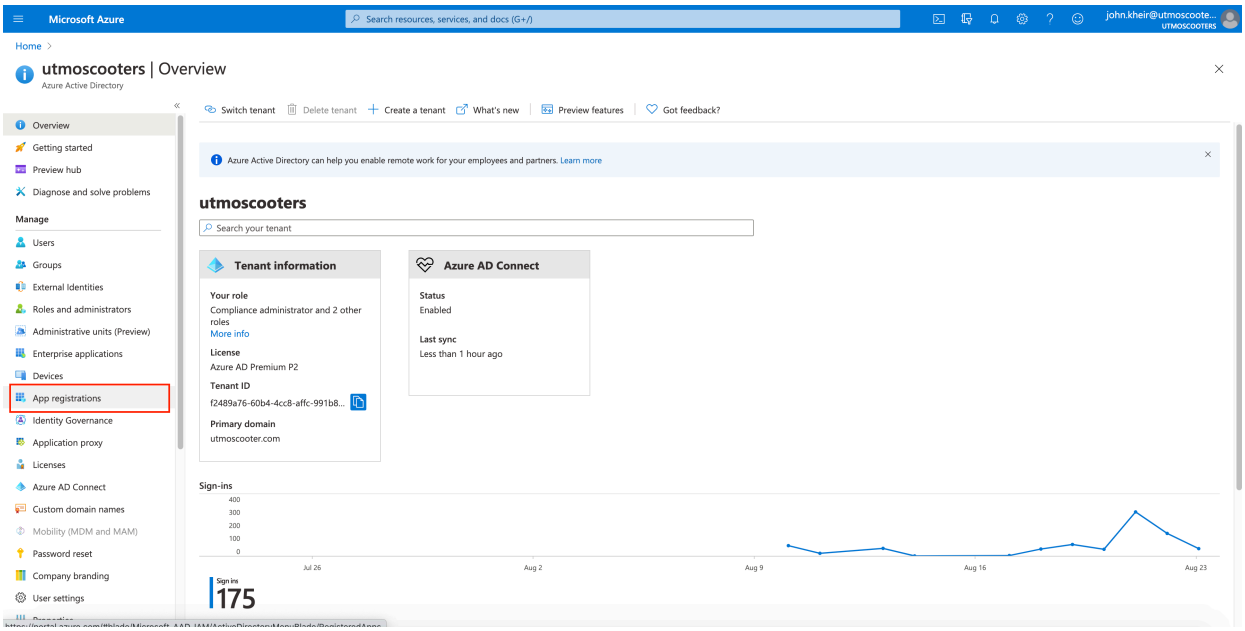
You should take note of the following information that will be required during the Forescout eyeAlert Data Source configuration procedure:

- The API URL
- Client ID
- Tenant ID
- Client Secret
- Content Types

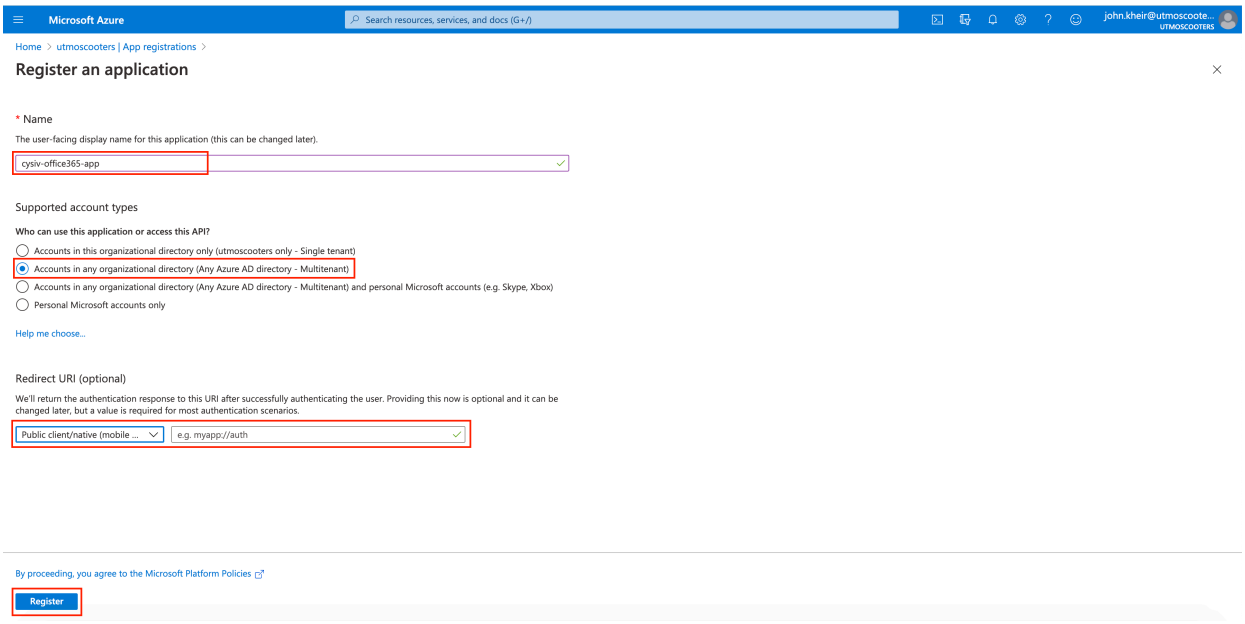
1- Go to Azure Management portal. Then in the left navigation panel, choose "**Azure Active Directory".**



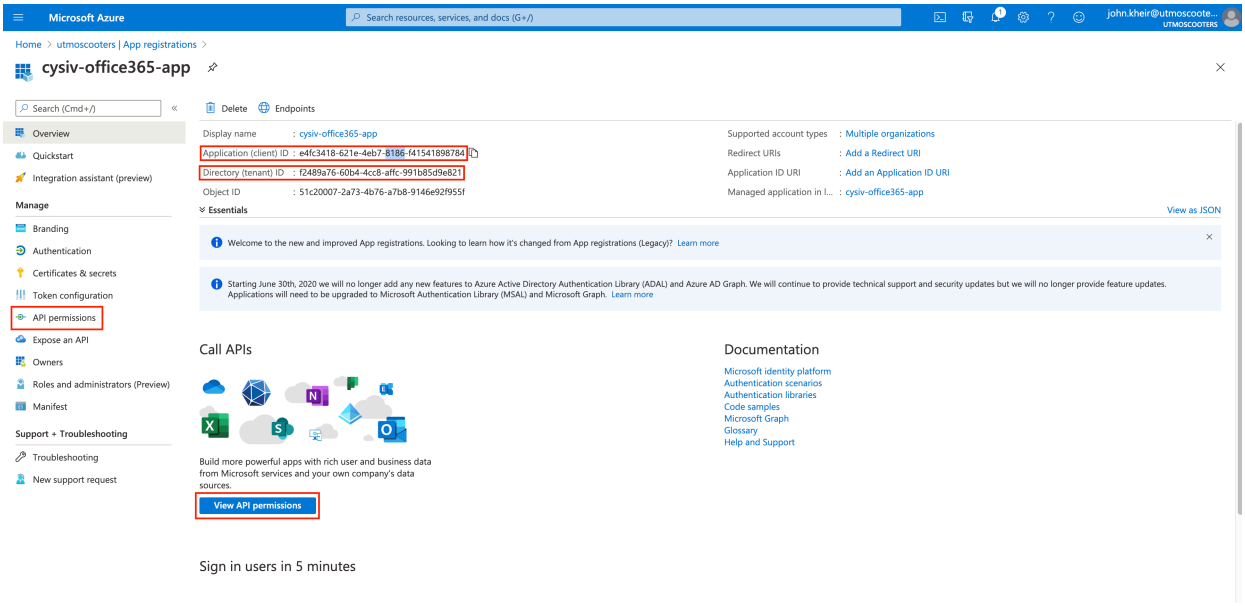
2- Choose **"App registration"**to register a new application.



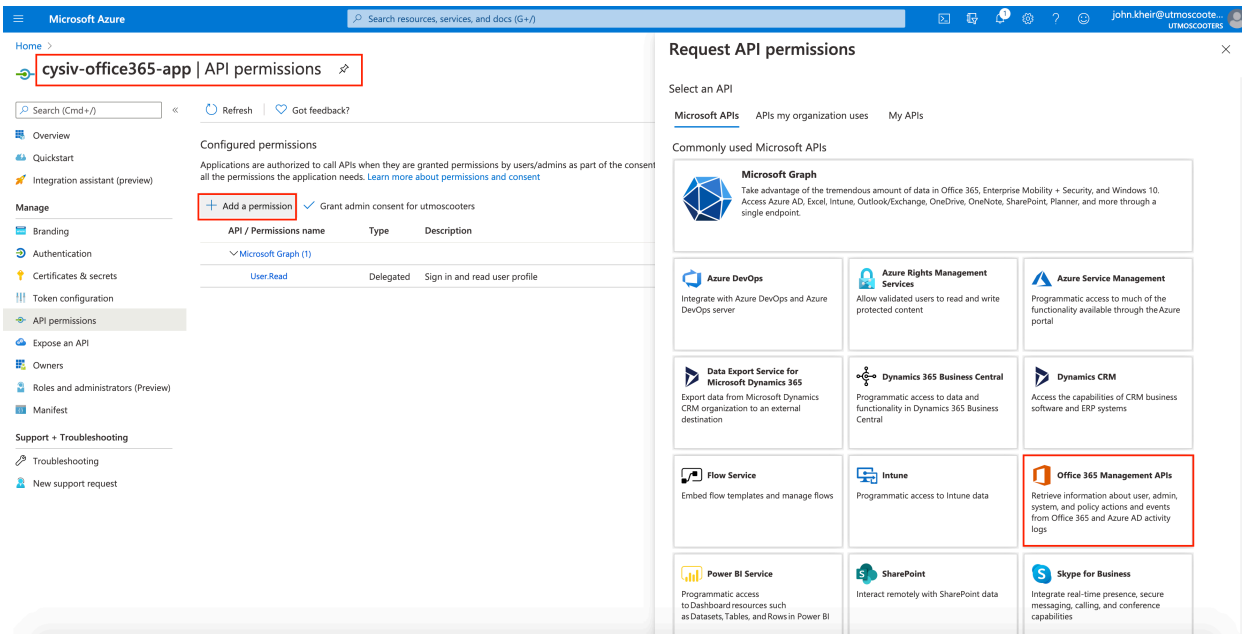
3- Add a name for the app, Choose the multi tenant option as shown in the figure. Then choose public client/native without adding a rediret URL. Then press register. Once the app has been registered, you will be redirected to the app page to complete the configuration.



4- On the app age, you will find the **client ID** and the **tenant ID**. In the left-hand navigation panel, click API permission to set the permissions needed for the office365 management API.

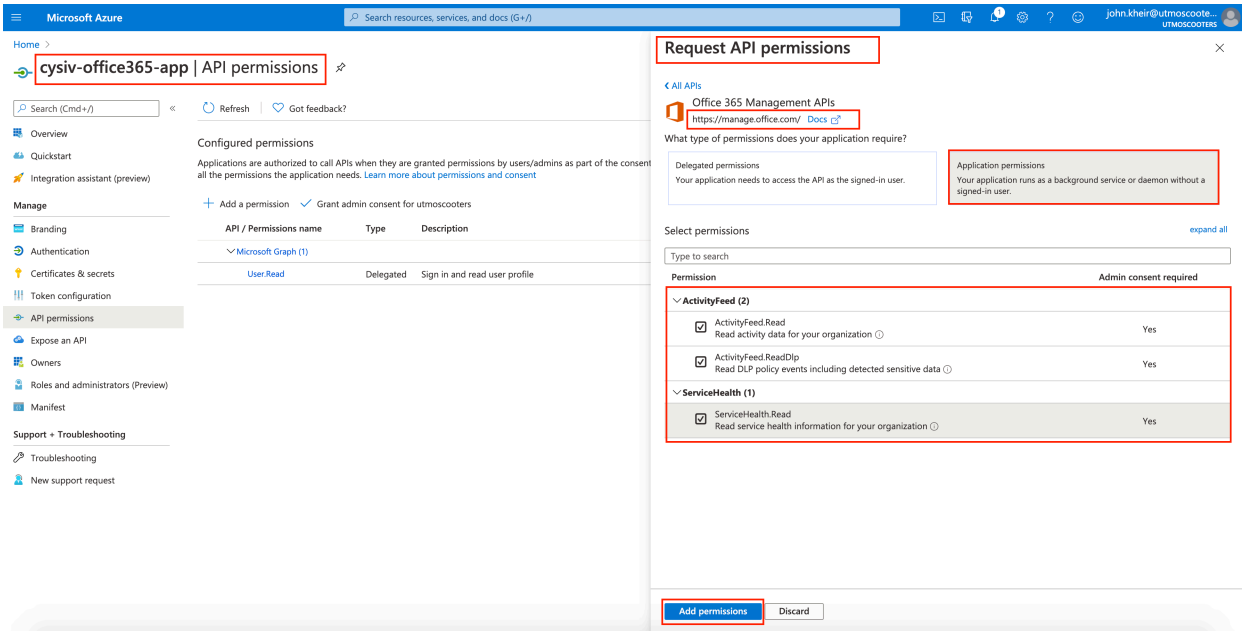


5- Press "Add a permission." Then a box called "Request API permissions" will appear. Choose "Microsoft Graph".

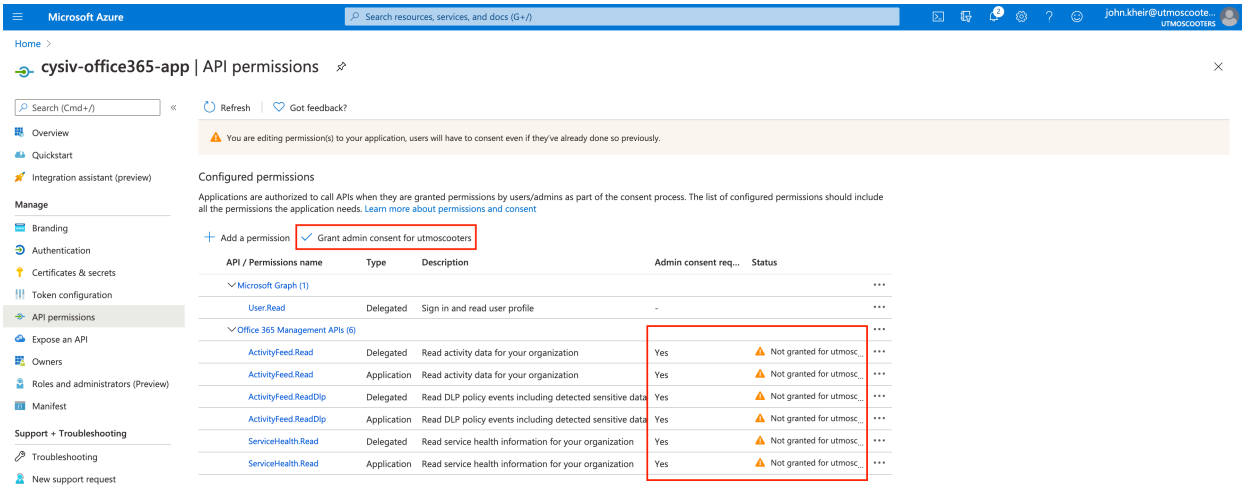


6- In the "**Request API permissions**" box, you will find the **api_url.** In this case the **api_url** is "https://manage.office.com".

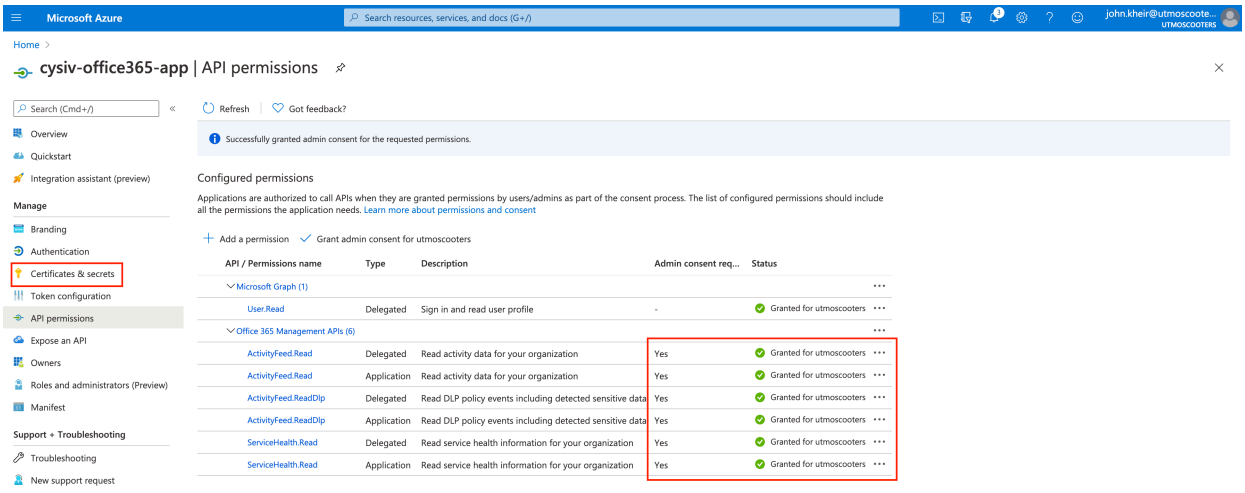
Then select **"Application permissions"** and check all the activity feed and service health permissions. Please select the same permissions for "**Delegated Permissions"** option. Then click **"Add permissions"**.



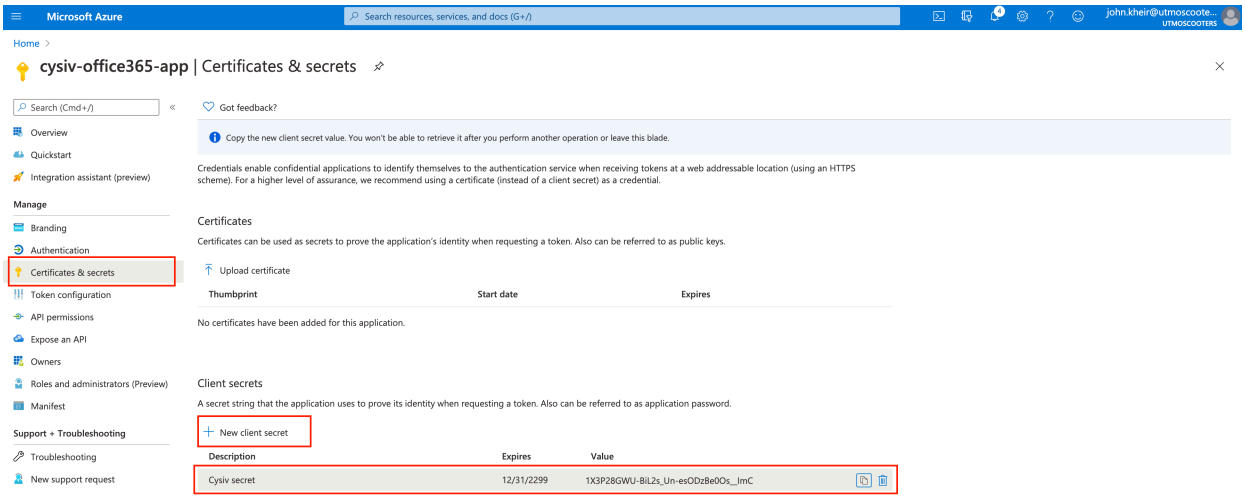
7- Once you have added the permissions, you will need an admin consent to grant these permissions. if "**Grant admin consent for ....**"button is enabled, then the signed in user has admin permission and can grant access. Click "**Grant admin consent for ....**" then grant access.



Once access is granted, you should see the following screen:



8-In the certificates and secrets page: Choose **"+ New client Secret"**. Add a name for it and choose expiration date **"Never"**then click **yes**. Once it is created, make sure to copy the secret as it will not be visible later on.



Two final notes:

1. Make sure audit log search is turned on. You have to be assigned the Audit Logs role in Exchange Online to turn audit log search on or off in your Microsoft 365 organization. By default, this role is assigned to the Compliance Management and Organization Management role groups on the **Permissions** page in the Exchange admin center. If you are not assigned to one of the previous roles explained, you will not be able to view audit log search page in Security & Compliance Center

2. Make sure you are subscribed to certain content types. Not sure how to do this from the UI but I did it using the following python script: If you will use the following script please provide client_id, client_secret, tenant_id, api_url and content types you want to subscribe

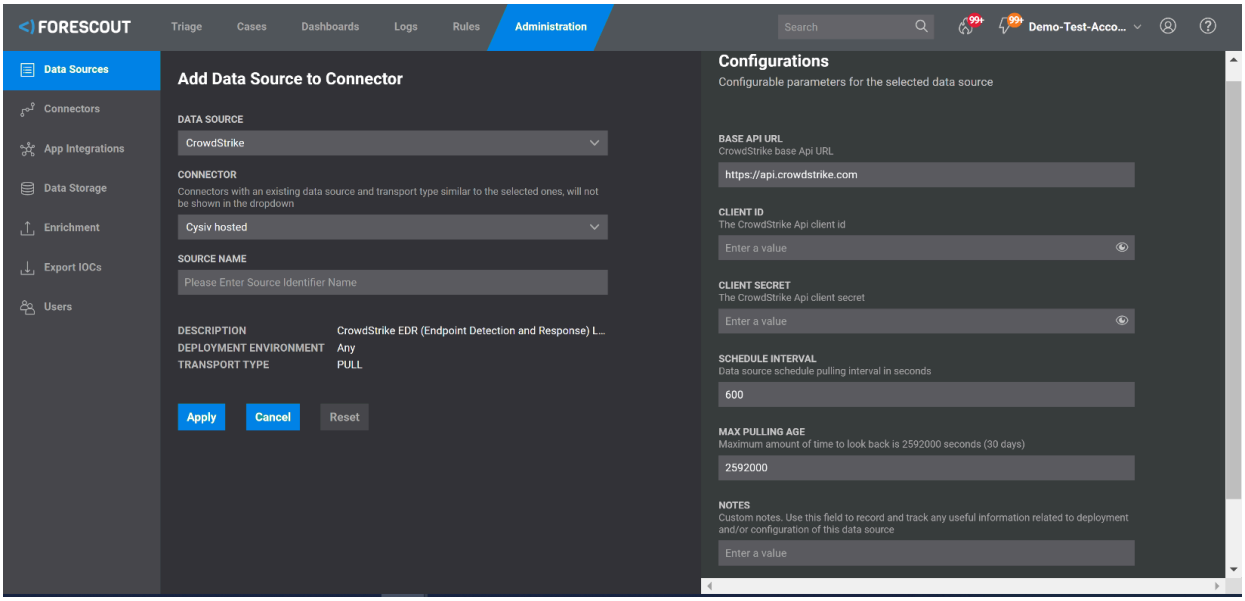
to before running it.

To run the script copy paste the code into subscribe.py for instance then python subscribe.py

Microsoft Graph Selecting a New Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.

1. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
2. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
3. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.



The available configuration options will vary depending on the Data Source type and Connector deployment method. The example shown above is of a CrowdStrike EDR™ Data Source where logs are pulled by a Connector that is hosted by Forescout.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Microsoft Graph Data Logs

Data Source Name – Microsoft Graph Security Alerts

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration* > *Data Sources* > *+Data Source* > *Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **CLIENT ID** that will be used for authentication.
2. Enter the **CLIENT SECRET** that will be used for authentication.
3. Enter the **TENANT ID** that will be used for authentication.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value 30 minutes expressed as 1800.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000. The size of this value affects
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Microsoft Defender for Endpoint (Pull)

Microsoft Defender For Endpoint™ is a Microsoft security product that is designed to help organizations detect and respond to security threats. It also allows you to manage multiple devices for each user. Licensing is user-based, so new devices per user can be added as needed. To add Microsoft Defender Endpoint to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Microsoft Defender Endpoint Data Source in the Forescout eyeAlert UI

Target Data Logs

Forescout currently targets generic alert logs for ingestion.

Microsoft Defender Endpoint Customer Side Configuration Prerequisites

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source in JSON format using a SIEM REST API. Before calling Microsoft Defender for Endpoint to pull alerts, the SIEM integration application in Azure Active Directory (AAD) must be enabled - instructions and

additional information are located here. You must generate a Client ID, Tenant ID, and Secret ID - instructions for how to do this are located here.

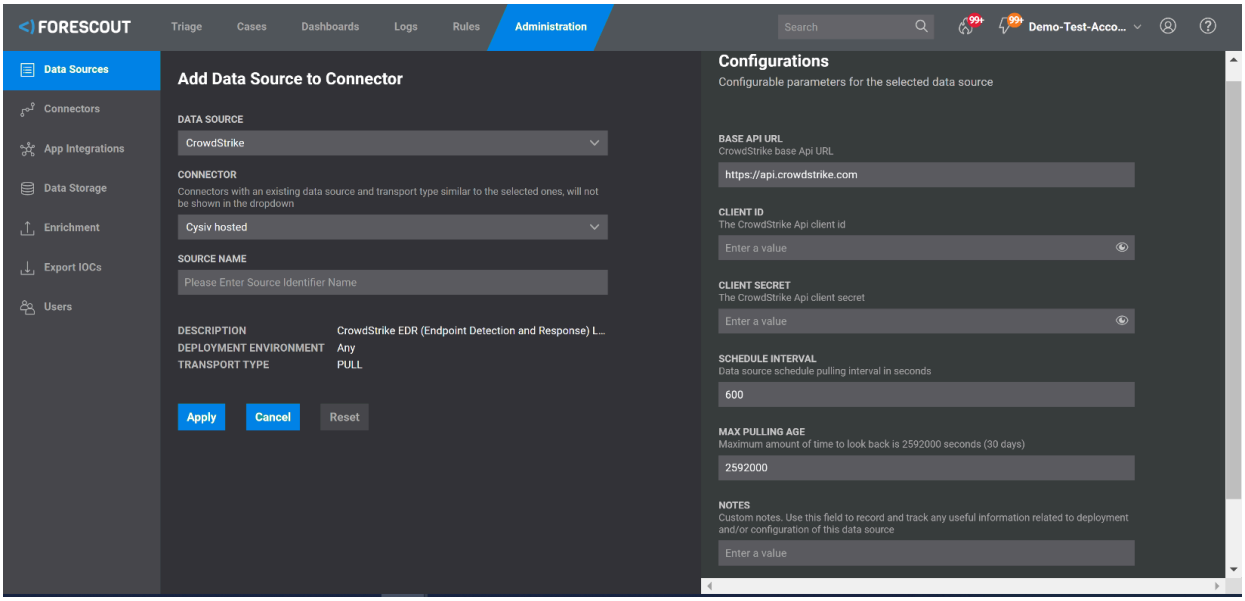
In the procedure to configure Forescout eyeAlert to receive the logs, you will need to provide the Client ID, Tenant ID, and Secret ID.

When the tasks are complete, proceed to Selecting the Microsoft Defender Endpoint Data Source.

Selecting the Microsoft Defender Endpoint Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.

1. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
2. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
3. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.



The available configuration options will vary depending on the Data Source type and Connector

deployment method. The example shown above is of a CrowdStrike EDR™ Data Source where logs are pulled by a Connector that is hosted by Forescout.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Microsoft Defender ATP Data Logs

Data Source Name – Microsoft Defender

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the**ENDPOINT URL**– be sure to use the alerts endpoint URL applicable to your region.
2. Enter the **CLIENT ID** that will be used for authentication.
3. Enter the **TENANT ID** that will be used for authentication.
4. Enter the **CLIENT SECRET** that will be used for authentication.
5. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 720.
6. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
7. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
8. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
9. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Microsoft™ Office 365™ Management APIs (Pull)

The Microsoft™ Office 365™ Management APIs provide a single extensibility platform for all Office 365 customers' and partners' management tasks, including service communications, security, compliance, reporting, and auditing. All of the Office 365 Management APIs are consistent in design and implementation with the current suite of Office 365 REST APIs, using common industry-standard approaches, including OAuth v2, OData v4, and JSON. Like the other Office 365 APIs, applications are registered in Azure Active Directory, giving developers a consistent way to authenticate and authorize their apps.

To add Microsoft Office 365 Management APIs to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.

2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Microsoft Defender Data Source in the Forescout eyeAlert UI

Target Data Logs

Forescout targets activity logs - click here for the full field reference.

Microsoft Office 365 Management APIs Customer Side Configuration Prerequisites

Forescout eyeAlert pulls logs using the Office 365 Management APIs. The Office 365 Management Activity API aggregates actions and events into tenant-specific content blobs, which are classified by the type and source of the content they contain. Currently, these content types are supported:

- Audit.AzureActiveDirectory
- Audit.Exchange
- Audit.SharePoint
- Audit.General (includes all other workloads not included in the previous content types)
- DLP.All (DLP events only for all workloads)

Pulling logs requires rights access to Management APIs, which uses Azure AD to provide authentication services to grant rights for application access. The following four tasks must be completed (a detailed step-by-step guide follows this summary):

1. **Register your application in Azure AD**. To allow your application access to the Office 365 Management APIs, you need to register your application in Azure AD. This allows you to establish an identity for your application and specify the permission levels it needs to access the APIs.

2. **Get Office 365 tenant admin consent**. An Office 365 tenant admin must explicitly grant consent to allow your application to access their tenant data by means of the Office 365 Management APIs. The consent process is a browser-based experience that requires the tenant admin to sign in to the **Azure AD consent UI** and review the access permissions that your application is requesting, and then either grant or deny the request. After consent is granted, the UI redirects the user back to your application with an authorization code in the URL. Your application makes a service-to-service call to Azure AD to exchange this authorization code for an access token, which contains information about both the tenant admin and your application. The tenant ID must be extracted from the access token and stored for future use.

3. **Request access tokens from Azure AD**. Using your application's credentials as configured in Azure AD, your application requests additional access tokens for a consented tenant on an ongoing basis, without the need for further tenant admin interaction. These access tokens are called app-only tokens because they do not include information about the tenant admin.

4. **Call the Office 365 Management APIs**. The app-only access tokens are passed to the Office 365 Management APIs to authenticate and authorize your application.

Forescout eyeAlert-Specific Step Guide

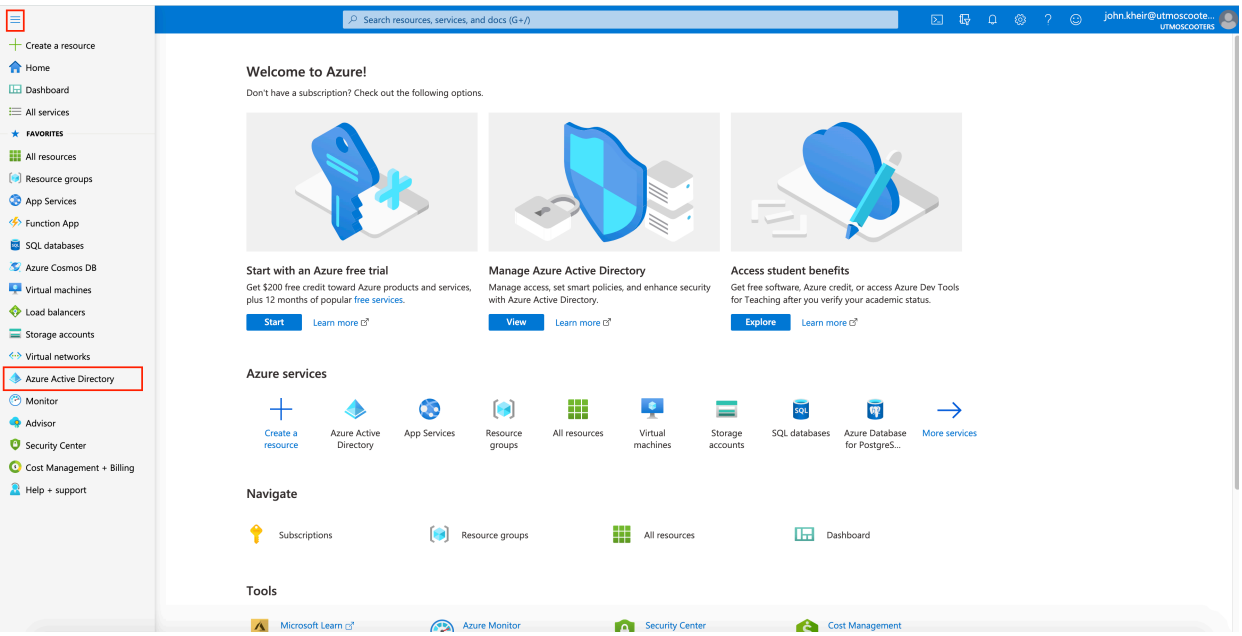
This procedure is based on the detailed Microsoft procedures located here.

Caution: These steps are provided for guidance purposes only, and should only be performed after consulting with the Forescout Security Engineer. Consult the vendor documentation for your specific product and version for the latest procedural steps.

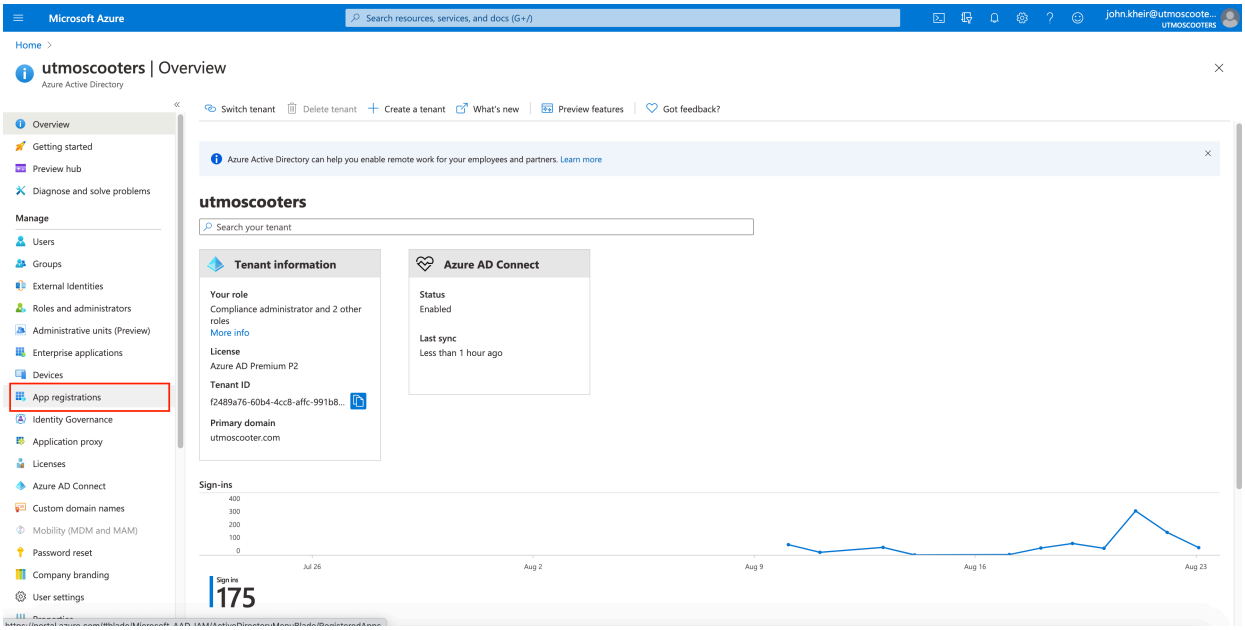
You should take note of the following information that will be required during the Forescout eyeAlert Data Source configuration procedure:

- The API URL
- Client ID
- Tenant ID
- Client Secret
- Content Types

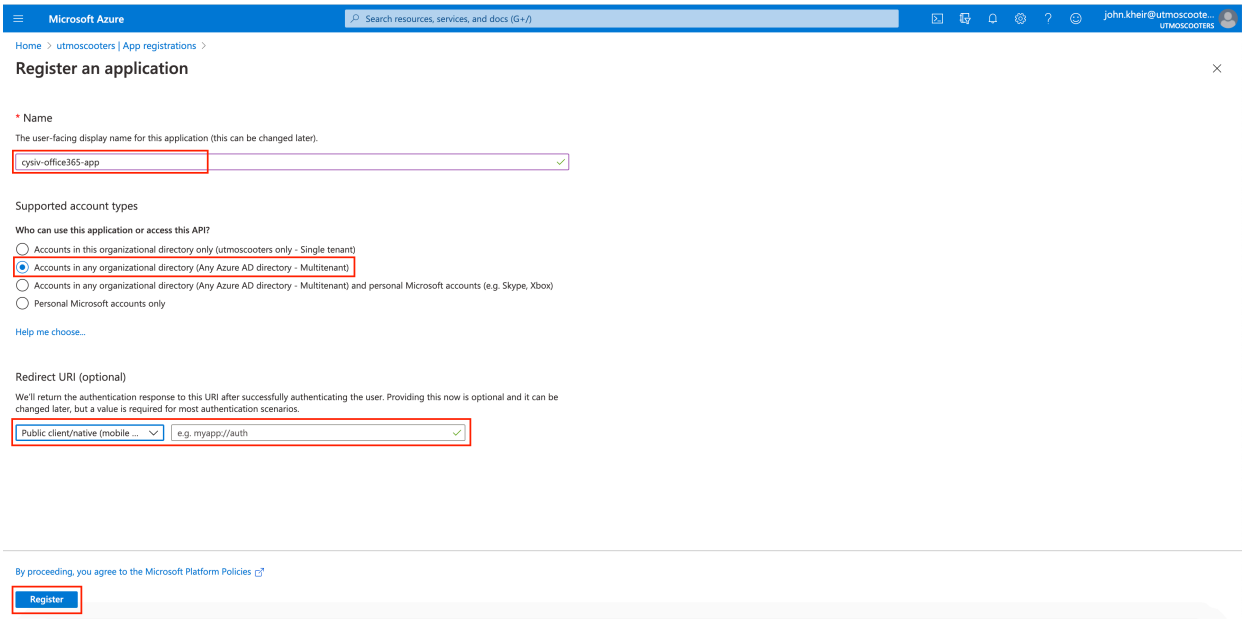
1- Go to Azure Management portal. Then in the left navigation panel, choose "**Azure Active Directory".**



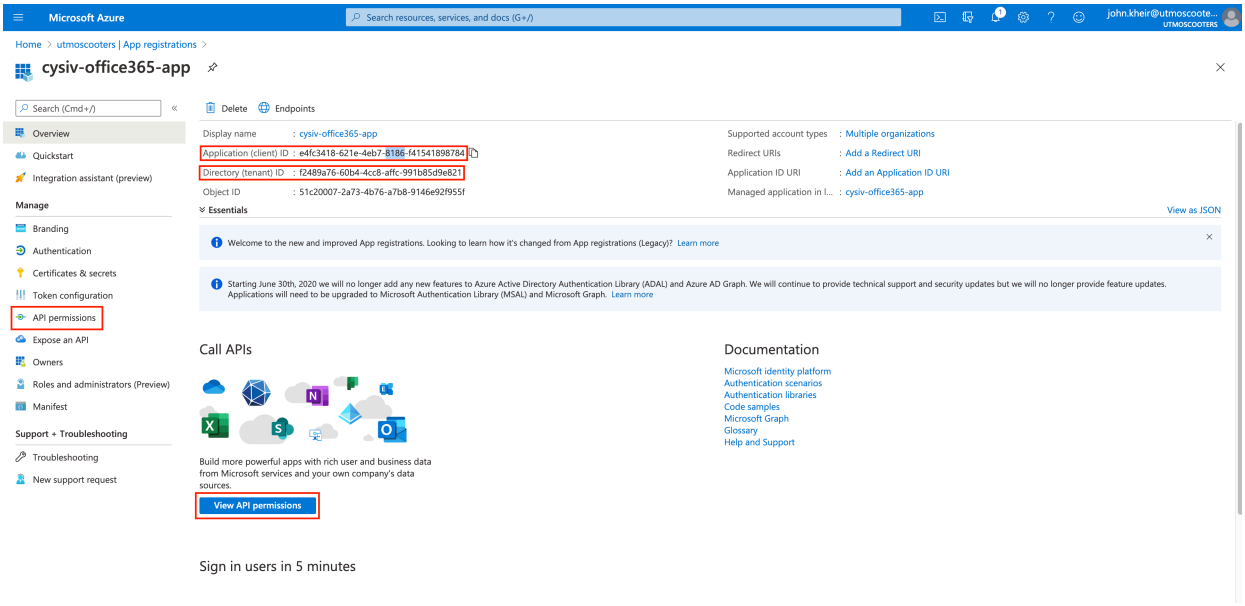
2- Choose **"App registration"**to register a new application.



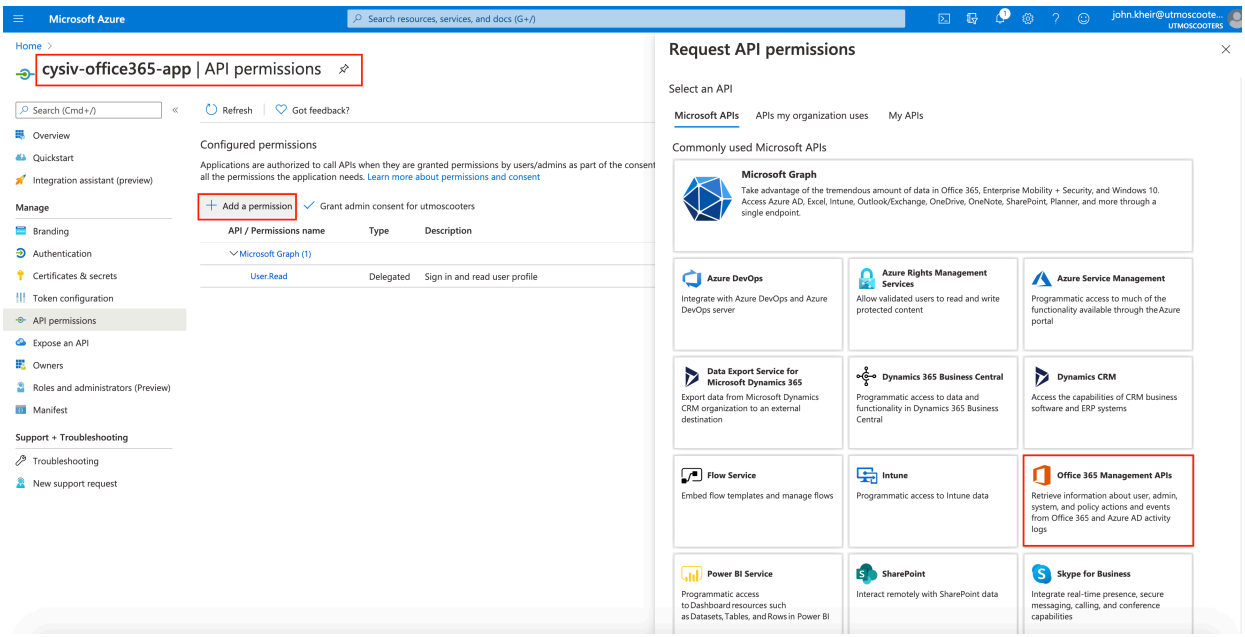
3- Add a name for the app. Choose the multi tenant option as shown in the figure. Then choose public client/native without adding a rediret URL and click register. Once the app has been registered, you will be redirected to the app page to complete the configuration.



4- On the app age, you will find the **client ID** and the **tenant ID**. In the left-hand navigation panel, click API permission to set the permissions needed for the office365 management API.

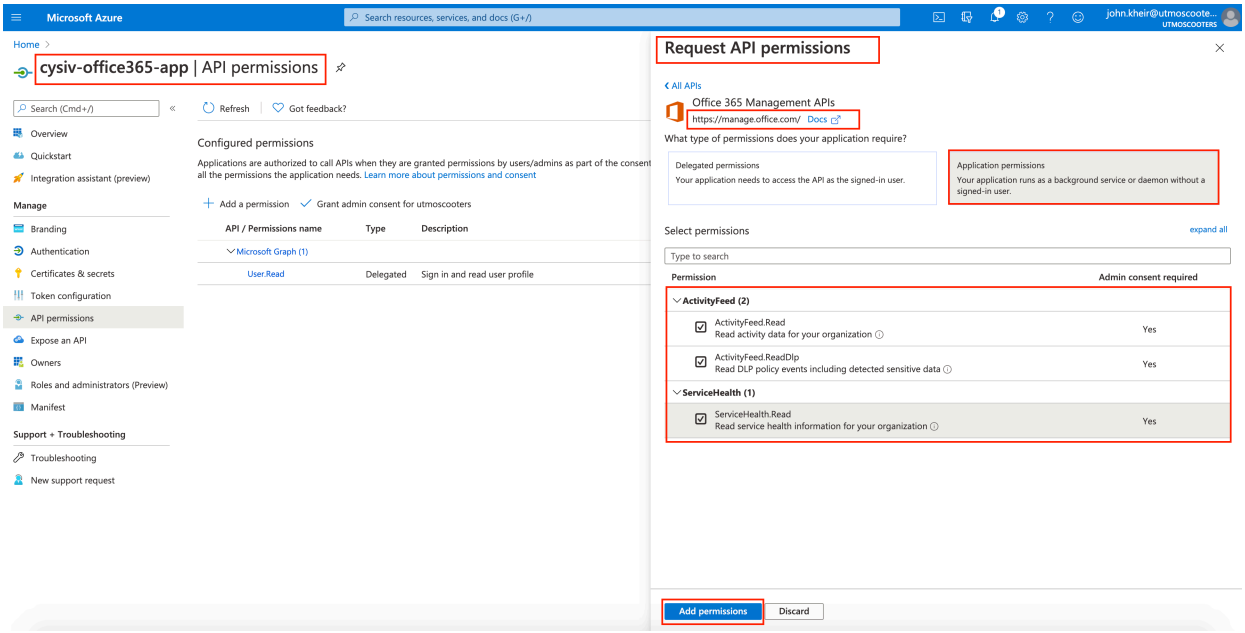


5- Press "Add a permission." Then a box called "Request API permissions" will appear. Choose "Office365 Management APIs".

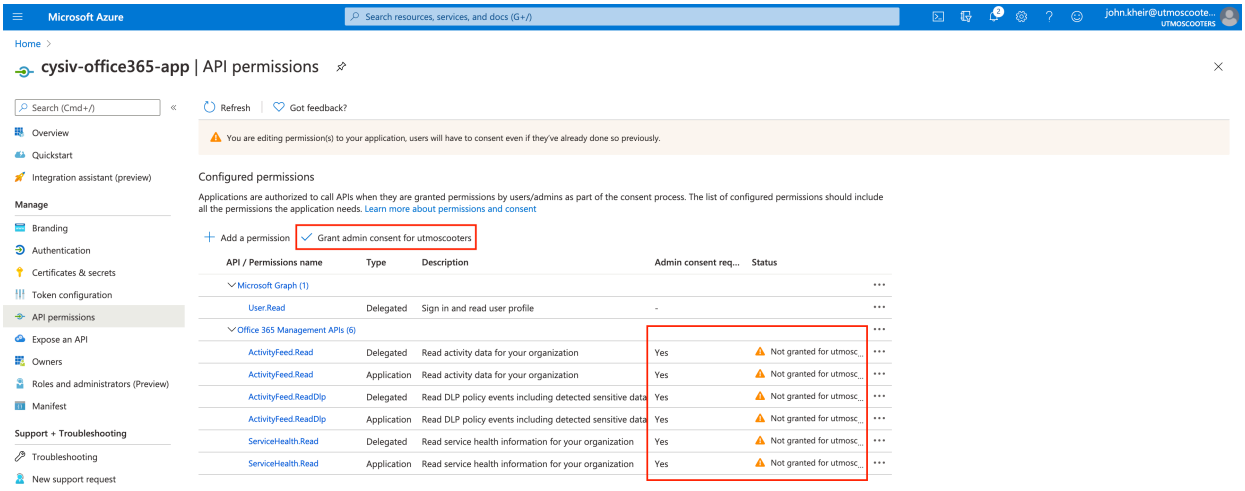


6- In the "**Request API permissions**" box, you will find the **api_url.** In this case the **api_url** is "https://manage.office.com".

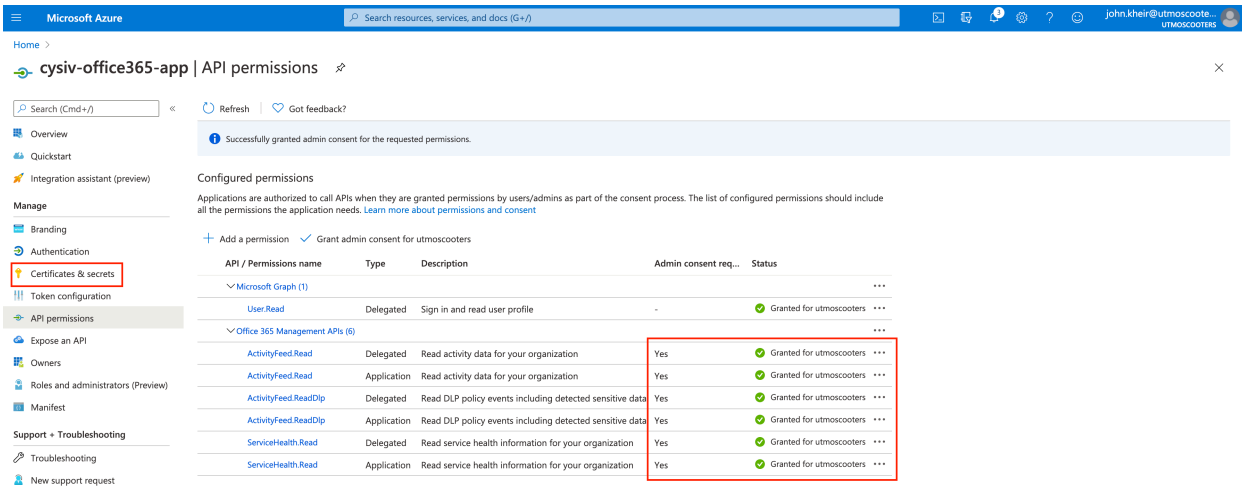
Then select **"Application permissions"** and check all the activity feed and service health permissions. Please select the same permissions for "**Delegated Permissions"** option. Then click **"Add permissions"**.



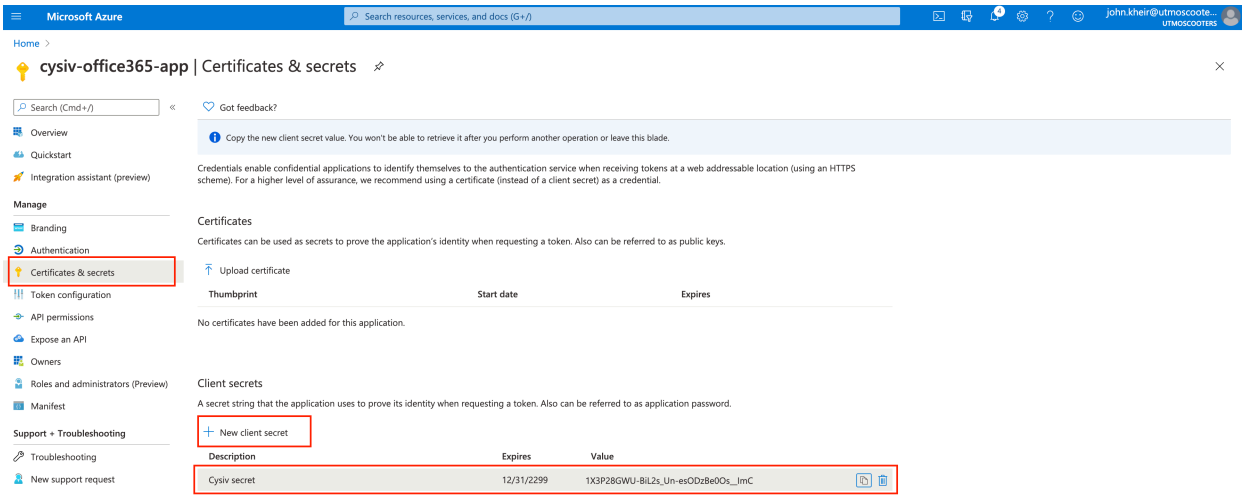
7- Once you have added the permissions, you will need an admin consent to grant these permissions. if "**Grant admin consent for ....**"button is enabled, then the signed in user has admin permission and can grant access. Click "**Grant admin consent for ....**" then grant access.



Once access is granted, you should see the following screen:



8-In the certificates and secrets page: Choose **"+ New client Secret"**. Add a name for it and choose expiration date **"Never"**then click **yes**. Once it is created, make sure to copy the secret as it will not be visible later on.



Two final notes:

1. Make sure audit log search is turned on. You have to be assigned the Audit Logs role in Exchange Online to turn audit log search on or off in your Microsoft 365 organization. By default, this role is assigned to the Compliance Management and Organization Management role groups on the **Permissions** page in the Exchange admin center. If you are not assigned to one of the previous roles explained, you will not be able to view audit log search page in Security & Compliance Center

2. Make sure you are subscribed to certain content types. Not sure how to do this from the UI but I did it using the following python script: If you will use the following script please provide client_id, client_secret, tenant_id, api_url and content types you want to subscribe

to before running it.

To run the script copy paste the code into subscribe.py for instance then python subscribe.py

Selecting the Microsoft Office 365 Management APIs Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.

1. Click the **DATA SOURCE** dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
2. Click the **CONNECTOR** dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
3. If applicable, enter the source identifier name into the **SOURCE NAME** field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

The available configuration options will vary depending on the Data Source type and Connector deployment method.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Microsoft Office 365 Management APIs Logs

Data Source Name – Microsoft Office 365 Management APIs

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **APIURL** – be sure to use the alerts endpoint URL applicable to your region.
2. Enter the **CLIENT ID** that will be used for authentication.
3. Enter the **TENANT ID** that will be used for authentication.
4. Enter the **CLIENT SECRET** that will be used for authentication.
5. Enter the relevant **CONTENT TYPES** - these are Tenant-specific content blobs, which are classified by the type and source of the content they contain. This value is a comma-separated string. Values supported are: 'Audit.SharePoint,Audit.Exchange,Audit.AzureActiveDirectory,Audit.General,DLP.All'. Please

only use content types to which you are subscribed.
6. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 900.
7. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 7 days expressed in seconds as 86400.
8. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
9. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
10. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Microsoft Cloud App Security (Pull)

Microsoft™ Cloud App Security™(MCAS) is a Cloud Access Security Broker (CASB) that operates on multiple clouds. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services. To add Microsoft Cloud App Security to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Microsoft Cloud App Security Data Source in the Forescout eyeAlert UI

Target Data Logs

According to the Generic SIEM integration document provided by MCAS, there are two main logs that can be pulled which are alerts and activities.

Activities comes from the apps connected to your MCAS. The activity log can be filtered to enable you to find specific activities. You create policies based on the activities and then define what you want to be alerted about and act on. You are able to search for activities performed on certain files. The type of activities and the information we get for each activity depends on the app and what kind of data the app can provide.

Alerts are the entry points to understanding your cloud environment more deeply. Alerts have two main types: built-in and custom alerts.

A description of the alert types can also be found here.

Microsoft Cloud App Security Customer Side Configuration Prerequisites

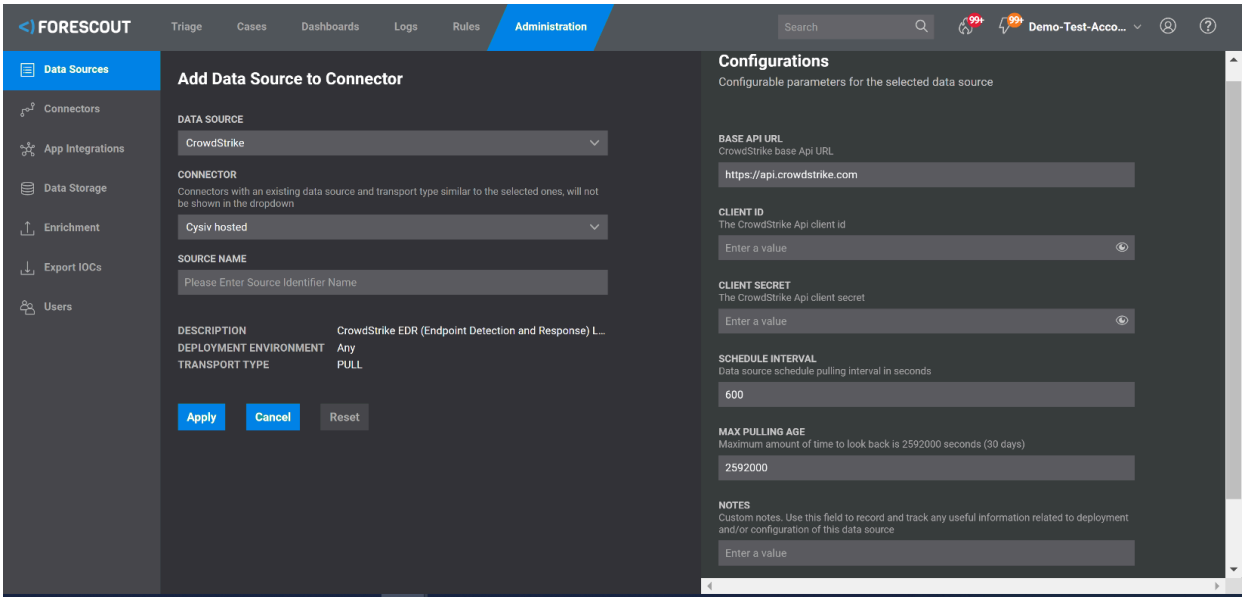
Forescout eyeAlert can obtain logs from Microsoft Cloud App Security using the pull mechanism. Forescout has created a "puller" to support obtaining data logs through the pull mechanism, and this has been developed by integrating theMCAS REST API.

During the procedure to configure Forescout eyeAlert to retrieve Microsoft Cloud App Security data logs you will be asked to enter the authorization token and API URL. To be able to get both, please sign in to theMCAS portal, then follow theinstructionson how to get authenticated.

Selecting the Microsoft Cloud App Security Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.

1. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
2. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
3. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.



The available configuration options will vary depending on the Data Source type and Connector deployment method. The example shown above is of a CrowdStrike EDR™ Data Source where logs are pulled by a Connector that is hosted by Forescout.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Microsoft Cloud App Security Data Logs

Data Source Name – Microsoft Cloud App Security

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **API URL**.
2. Enter the **AUTHENTICATION TOKEN**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 600.
4. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
5. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
6. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Windows Events (Push)

This manual is under construction.

Windows Sysmon (Push)

This manual is under construction.

Mimecast

This series of topics covers all products offered by Mimecast™ that can be used as a Data Source for Forescout XDR log ingestion.

Mimecast Data Source

Mimecast Data Source

Mimecast is a set of cloud services designed to provide protection against email-borne threats such as malicious URLs, malware, impersonation attacks. To add Mimecast to Forescout XDR as a Data Source, complete the following tasks:

To add Mimecast to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Mimecast provides a customer resource portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

The following logs are relevant for Forescout XDR ingestion:

- SIEM Logs.
- Targeted Threat Protection URL Protect.
- Targeted Threat Protection Attachment Protect.
- Targeted Threat Protection Impersonation Protect.
- Audit Events.
- DLP Logs.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

MongoDB

This series of topics covers all products offered by MongoDB™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

MongoDB-Atlas

MongoDB Atlas (Pull)

MongoDB Atlas™ is a fully-managed cloud database that handles all the complexity of deploying, managing, and healing your deployments on the cloud service provider of your choice (AWS , Azure, and GCP). MongoDB Atlas is the best way to deploy, run, and scale MongoDB in the cloud. With Atlas, you'll have a MongoDB database running with just a few clicks, and in just a few minutes.

To add MongoDB-Atlas to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the MongoDB-Atlas Data Source in the Forescout eyeAlert UI

Target Data Logs

Forescout eyeAlert targets Event and Monitoring logs for ingestion.

MongoDB Atlas Customer Side Configuration Prerequisites

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source. The following procedure configures MongoDB-Atlas for Forescout eyeAlert log ingestion, which will produce the following information required for the procedure to configure Forescout eyeAlert to receive the logs:

- private_key
- public_key
- group_id

First you need to generate the key pair used in authentication and add the used IP to the API access list, based on the official documentation:

1. Navigate to the Access Manager page for your organization.
    a. If it is not already displayed, select your desired organization from the Organizations menu in the navigation bar.
    b. Click **Access Manager** in the sidebar, or click **Access Manager** in the navigation bar, then click your organization.
2. Click the ***API Keys*** tab.
3. Enter the ***API Key Information***.
    a. Enter a **Description**.
    b. In the **Organization Permissions** menu, select the new role or roles for the API key.
4. Click ***Next***.
5. Copy and save the ***Public Key***.
6. Copy and save the ***Private Key***.
7. Add an ***API Access List Entry***.
    a. Click **Add Access list Entry**.
    b. Enter an IP address from which you want Atlas to accept API requests for this API Key.

    You can also click **Use Current IP Address** if the host you are using to access Atlas also will make API requests using this API Key.
    c. Click **Save**.
8. Click ***Done***.

To retrieve your project ID (GROUP-ID):

1. Navigate to the Settings page for your project.
2. If it is not already displayed, select the organization that contains your desired project from the **Organizations** menu in the navigation bar.
    a. If it is not already displayed, select your desired project from the **Projects** menu in the navigation bar.
    b. Next to the **Projects** menu, expand the **Options** menu, then click **Project Settings**.
3. Copy the string listed under the ***Project ID*** heading.

Notes:

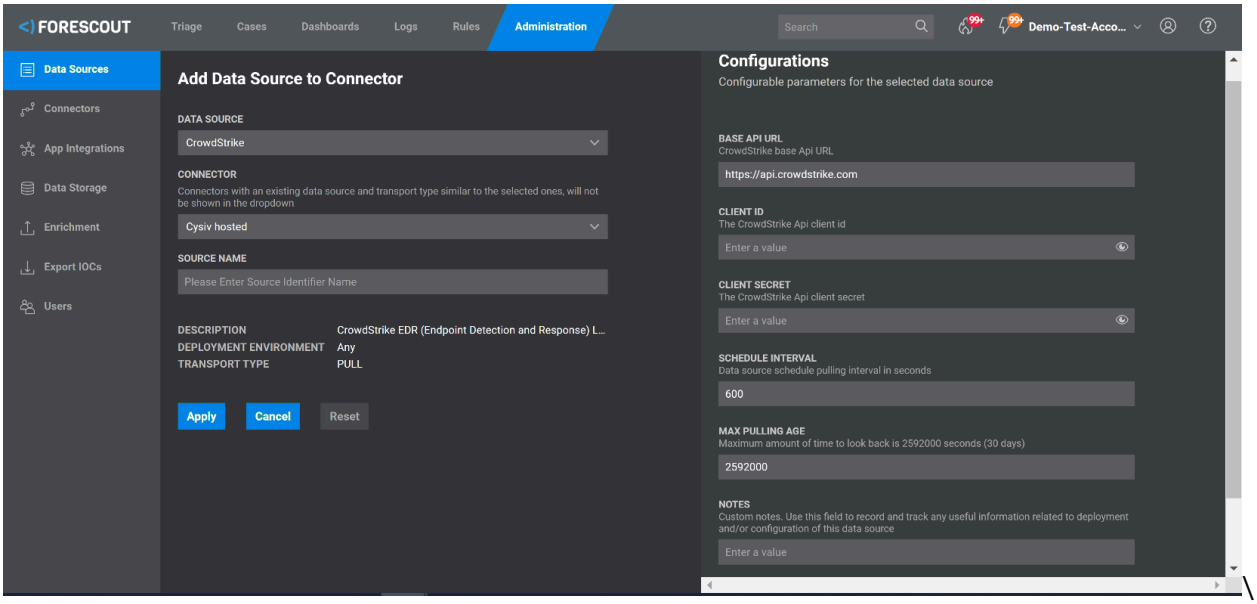
- Audit logs are only available if you have enabled Database Auditing for an Atlas project.
- Process and audit logs are updated from the cluster backend infrastructure every five minutes and contain log data from the previous five minutes. If you are polling the API for log files, polling every five minutes is recommended.
- **Rate Limiting:** Certain resources limit how many requests they can process per minute. For these resources, Atlas allows up to 100 requests per minute *per project*. API keys belong to an organization, but can be granted access multiple projects. If you made 110 requests in one minute, the last 10 requests will be rejected and you will hav to repeat these requests

Proceed to the next section.

Selecting the MongoDB Atlas Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.

1. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
2. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
3. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.



The available configuration options will vary depending on the Data Source type and Connector deployment method. The example shown above is of a CrowdStrike EDR™ Data Source where logs are pulled by a Connector that is hosted by Forescout.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive MongoDB Atlas Logs

Data Source Name – MongoDB-Atlas

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration* > *Data Sources* > *+Data Source* > *Add Data Source to Connector* – *Configurations* (right-panel)

1. Enter the **PROJECT ID.**
2. Enter the **Public Key**.
3. Enter the **Private Key**.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 600.
5. Enter the LAG INTERVAL in seconds - the default value is 600.
6. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
7. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
8. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
9. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Netgate

This series of topics covers all products offered by Netgate™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Netgate PfSense (Push)

Netgate PfSense (Push)

Netgate™ is a free network firewall distribution, based on the FreeBSD operating system with a custom kernel and including third-party free software packages for additional functionality.

To add Netgate PfSense to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Netgate provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout currently targets Firewall Traffic Reports.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Netskope

This series of topics covers all products offered by Netskope™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Netskope Data Source

Netscope Data Source (Pull)

Netskope™ is a Cloud Access Security Broker (CASB) to address cloud service risks, enforce security policies, and comply with regulations, even when cloud services are beyond their perimeter and out of their direct control. To add Netskope to Forescout TDR as a Data Source,

complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Netskope Data Source in the Forescout eyeAlert UI

Target Data Logs

Forescout targets Alert and Events logs for ingestion.

Netskope Customer Side Configuration Prerequisites

Forescout eyeAlert uses the pull mechanism to ingest logs from this Data Source. The following procedure is modified from vendor documentation located here. To be able to integrate an instance with Forescout eyeAlert, we need a Base API URL and authentication token.

1. For the Netskope integration, Forescout simply needs the API token along with your Netskope tenant URL (i.e. https://customer.eu.goskope.com).

2. Netskope REST APIs use an auth token to make authorized calls to the API. The token can be generated or revoked in the Netskope UI by going to **Settings** > **Tools** > **Rest API v1.**

3. To set the token expiration, click on the pencil icon next to the **Expiration** date.

   Note: Please set the expiration to NEVER.

Once Netskope has been appropriately configured, proceed to the next section to select the Data Source in the Forescout eyeAlert UI. Additional reference points are available here.

Selecting the Netskope Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Netskope Logs

Data Source Name – Netskope

Log Retrieval Method – Pull

Connector Deployment Environment – Any

UI Location – *Administration* > *Data Sources* > *+Data Source* > *Add Data Source to Connector* – *Configurations* (right-panel)

1. Enter the **API URL**.
2. Enter the **AUTHENTICATION TOKEN**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 60.
4. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 7 days expressed in seconds as 86400.
5. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
7. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

NetIQ

This series of topics covers Data Source products offered by NetIQ that are supported by Forescout eyeAlert.

NetIQ Change Guardian (Push)

NetIQ Change Guardian (Push)

NetIQ Change Guardian is a privileged user activity and change monitoring solution that helps with responding to potential threats in real time. Change Guardian provides alerts about unauthorized access and changes to critical files systems.

These alerts hold security information such as who performed the action, what action was performed, when and where the action was taken, and whether the activity was authorized.

To add NetIQ Change Guardian to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

NetIQ provides a user guide here.

Target Data Logs

Forescout currently processes network security logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Okta

This series of topics covers all products offered by Okta™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Okta Identity

Okta Identity (Pull)

Okta™ provides secure connections between people and your applications on any device through an identity management service built for the cloud. Okta Identity Cloud provides secure identity management with, among other things, Single Sign-On, Multi-factor Authentication, and Lifecycle Management (Provisioning). To add Identity to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Okta Identity Data Source in the Forescout eyeAlert UI

Target Data Logs

The following logs are relevant for Forescout eyeAlert ingestion:

- System Logs and Reports
- SIEM Integrations
- API Integrations

Okta Identity Customer Side Configuration Prerequisites

Reference this link and use the table below to configure the specific Okta Data Source parameters. Also reference this link to create a Token, as this information as well as the API URL will be needed during the procedure to configure Forescout eyeAlert to receive Okta Identity logs.

Log Source type	Okta
Protocol Configuration	Okta REST API
IP or Hostname	oktaprise.okta.com
Authentication Token	A single authentication token that is generated by the Okta console and must be used for all API transactions.

Log Source type	Okta
Use Proxy	When a proxy is configured, all traffic for the log source travels through the proxy for JSA to access Okta. Configure the **Proxy IP or Hostname**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.
Automatically Acquire Server Certificate(s)	If you select **Yes** from the list, JSA downloads the certificate and begins trusting the target server.
Recurrence	You can specify when the log source collects data. The format is M/H/D for Months/Hours/Days. The default is 1 M.
EPS Throttle	The maximum limit for the number of events per second.

Proceed to the next section to select the Okta Identity Data Source in Forescout eyeAlert.

Selecting the Okta Identity Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Okta Identity Logs

Data Source Name – Okta Identity

Log Retrieval Method – Pull

Connector Deployment Environment – On-Premise or Hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **API URL**.
2. Enter the **ACCESS TOKEN**.
3. Enter the **LIMIT** value.

4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 300.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

OneLogin

This series of topics covers Data Source products offered by OneLogin™ that are supported by Forescout eyeAlert.

OneLogin API (Pull)

OneLogin API (Pull)

This manual is under construction.

OpenText

This series of topics covers all products offered by OpenText™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Voltage SecureData

Voltage SecureData

This manual is under construction.

OpenVPN

This series of topics covers all products offered by OpenVPN™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

OpenVPN Data Source (Push)

OpenVPN Data Source (Push)

OpenVPN™ is a virtual private network (VPN) system that implements techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It implements both client and server applications.

To add OpenVPN Data Source to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

OpenVPN provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Oracle

This series of topics covers all products offered by Oracle™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Oracle HCM (Pull)

Oracle Cloud (Pull)

Oracle FineGrain Audit Logs

Oracle Cloud Infrastructure (Pull)

Oracle Cloud (Pull)

This manual is under contruction.

Oracle Cloud Infrastructure (Pull)

Oracle Cloud Infrastructure™ (OCI) is a platform of cloud services that enable you to build and run a wide range of applications. It offers IaaS, PaaS, SaaS, and Data as a Service (DaaS) capabilities in a single platform. With OCI, Oracle has welded an array of compute, storage, database, networking, and platform services geared towards the enterprise, including small and medium-sized ones.

To add Oracle Cloud Infrastructure to Forescout eyeAlert as a Data Source, ensure the following setting are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source.

Key Data Source Product Configuration and Authentication Requirements

OCI requires a somewhat complex configuration to make logs available for pull retrieval by Forescout eyeAlert. Use your vendor documentation to perform the necessary configurations to complete the following high level steps:

1. **Create an OCI Compartment:** Create and name a compartment, and optionally associate it with an existing parent compartment.

2. **Configure Logs:** Create a log group and associate it with the compartment you created in step 1. Select the "Enable Service Log" option, associate it with the compartment you created in step 1, and configure log categories as appropriate.

3. **Create and Configure Oracle Streaming Service:** Create a Stream and associate it with the compartment you created in step1

4. **Create a Service Connector Hub:** You must create a service connector hub for reading logs from logging and send data to the Oracle Streaming Service. When configuring the source and target connection, select the compartment you created in step 1.

5. **Configure Kafka Consumer:** Create a Kafka consumer from IBM QRadar console. When configuring, do not select the *Use Client Authentication* option. Also, add the server certificate to the location (`/opt/qradar/conf/trusted_certificates/`) in `.der` format

To onboard logs from this Data Source, you will need to have the following credential information on-hand when configuring Forescout eyeAlert:

- **KAFKA SERVERS**: Comma-separated list of brokers that run in a Kafka Cluster. If you have multiple brokers(servers), Use 'host:port1,host2:port2'

- **SASL USER NAME**: SASL username used for authentication.

- **SASL PASSWORD**: SASL password used for authentication.

- **CONSUMER GROUP**: A consumer group is a set of consumers which cooperate to consume data from some topics.

- **TOPIC NAMES**: Comma-separated list of topics names to consume from.

Suggested Information Sources for Data Source Product Configuration

Oracle provides a help center here, and has procedural help articles on OCI logging and Python configuration .

Note:
The reference links above are suggestions only. To ensure accuracy, confirm that you are using the latest official documentation provided by the vendor of your Data Source product to ensure accuracy.

Target Data Logs

Forescout currently targets Audit and Service logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON format when configuring your Data Source to make logs available for ingestion by Forescout eyeAlert.

Configure Forescout eyeAlert to Retrieve the Data Source Logs

See Configuring Forescout eyeAlert to Retrieve Oracle Cloud Infrastructure Logs

Configuring Forescout eyeAlert to Retrieve Oracle Cloud Infrastructure Logs

Data Source Name – Oracle Cloud Infrastructure

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration* > *Data Sources* > + *Add Data Source* > *Add Data Source to Connector* – *Configurations* (right-panel)

1. Enter a comma-separated list of Kafka brokers that run in the cluster in the **KAFKA SERVERS** field. If you have multiple brokers(servers), use 'host:port1,host2:port2'.
2. Enter the appropriate value in the **SASL USER NAME** field.
3. Enter the appropriate value in the **SASL PASSWORD** field.
4. Enter the appropriate value in the **CONSUMER GROUP** field.
5. Enter a comma-separated list of Topic names to consume from in the **TOPIC NAMES** field.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is *Pulling*for periodic retrieval of target data logs.
8. Click the **Apply** button.

Oracle FineGrain Audit Logs

This manual is under construction.

Oracle HCM (Pull)

Natively built for the cloud, Oracle™ Fusion Cloud™ Human Capital Management™ is a complete solution connecting every human resource process from hire to retire. This provides a consistent experience across devices, enables one source of truth for HR data to improve decision-making, and empowers you with market-leading innovation to address your needs today and into the future. This page focuses on Sign in - Sign out REST API. Through this API we get users activities regarding their sign-in & sign-out attempts only in the last seven days.

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Oracle HSM Data Source in the Forescout eyeAlert UI

Oracle HCM Customer Side Configuration Prerequisites

Forescout eyeAlert uses the pull mechanism via the Oracle HSM Sign in - Sign out REST API to ingest logs from this Data Source. To configure Oracle HSM for log ingestion by Forescout eyeAlert:

First, create a new Oracle HSM user by completing the following procedure, which has been

referenced from vendor information located here:

1. In the Security Console, click the **Users** tab.
2. On the User Accounts page, click the **Add User Account** button.
3. From the **Associated Person Type** list, select **Worker** to link this account to a worker record in HCM. Otherwise, leave it as **None**.
4. In the **Account Information** section, change the default settings if you don't want the account to be active or unlocked.
5. Fill in the **User Information** section:
    a. Select the user category that you want to associate the user with. The user category includes a password policy and a rule that determines how the user name is automatically generated.
    b. Enter the user's first name only if the rule from the selected user category makes use of the first name or the first name initial to generate user names.
    c. Enter a password that conforms to the password policy from the selected user category.
6. In the Roles section, click the**Add Role**button.
7. Search for the role that you want to assign to the user and the click**Add Role Membership**button. The role is added to the list of existing roles.
8. Repeat the previous step to add more roles if required, or just click**Done**.
9. Click the**Add Auto-Provisioned Roles**button to add any roles that the user is eligible for, based on role provisioning rules. If nothing happens, that means there aren't any roles to autoprovision.
10. In the Roles table, click the**Assignable**check box for any role that can be delegated to another user. The**Auto-Provisioned**column displays a tick mark if the user has roles that were assigned through autoprovisioning.
11. Click the**Delete**icon to unassign any role.
12. Click**Save and Close**.

Next, grant the new user access to the Sign in - Sign out API, by completing the following procedure, which has been referenced from vendor information located here:

1. In the Setup and Maintenance work area, open the task **Manage Administrator Profile Values**.
2. Search the following **Profile Option Code**:

    ASE_ADVANCED_USER_MANAGEMENT_SETTING
3. In the**Profile Value**drop-down list, select**Yes**.
4. Click Save and Close.

Proceed now to Selecting the Oracle HSM Data Source.

1.

Selecting the Oracle HCM Data Source

1. Log in to Forescout eyeAlert and click the **Administration** tab.
2. On the Administration screen, click the **Data Sources** tab.
3. Click the **+ Data Source** button.
4. Click the **DATA SOURCE** dropdown and select the Data Source you are adding from the list.
5. Click the **CONNECTOR** dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".

For the Data Source you are adding, the configuration parameters you should enter on the right side of the window depend on whether the log retrieval method is Push or Pull (determined by the Data Source device type) and whether the Connector deployment environment is on-premise or hosted. Proceed to Configuring Forescout eyeAlert to Receive Oracle HSM Logs.

Configuring Forescout TDR to Receive Oracle HCM Logs

Data Source Name – Oracle HCM

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **API URL**.
2. Enter the username into the **USERNAME** field.
3. Enter the password into the **PASSWORD** field.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 43200.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 3600.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

PaloAlto

This series of topics covers all products offered by PaloAlto™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

PAN-OS (Push)

PAN-OS® is the software that runs all Palo Alto Networks® next-generation firewalls.

To add PAN-OS to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

PAN-OS provides a user documentation portal here.

Log Format Necessary for Forescout TDR Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout TDR.

Target Data Logs

The supported log formats are Syslog, CEF, and JSON. There is a list of standard fields of each log type that Palo Alto Networks firewalls can forward to an external server, as well as the severity levels, custom formats, and escape sequences. Those logs are Traffic Log, Threat Logs, HIP Match Logs, Config Logs, System Logs; however, Forescout is currently focused on Threat and Wildfire Logs.

- Threat Log Fields: record traffic that matches spyware, vulnerability, or virus signature or a DoS attack that matches the thresholds configured for a port scan or host sweep activity on the firewall.
- WildFire Logs: WildFire Submissions log entries include the firewall Action for the sample (allow or block), the WildFire verdict for the submitted sample, and the severity level of the sample

Configure Forescout TDR to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout TDR, and for information about configuring Forescout TDR to receive the logs.

PaloAlto Cortex XDR (Push)

Cortex XDR™ applies machine learning at cloud scale to rich network, endpoint, and cloud data, so you can quickly find and stop targeted attacks, insider abuse, and compromised endpoints. Cortex XDR apps consume and correlate data from the Cortex Data Lake to reveal threat causalities and timelines.

To add PaloAlto Cortex XDR to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout TDR uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

PaloAlto Cortex XDR provides a user documentation portal here.

Log Format Necessary for Forescout TDR Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout TDR.

Configure Forescout TDR to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout TDR, and for information about configuring Forescout TDR to receive the logs.

Prisma Cloud (Pull)

Prism Cloud™is an API-based cloud service that connects to your cloud environments in just minutes and aggregates volumes of raw configuration data, user activity information, and network traffic to analyze and produce concise and actionable insights.

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Prisma Cloud Data Source in the Forescout eyeAlert UI

Target Data Log Types

Forescout eyeAlert currently targets Prisma Cloud alert logs

Prisma Cloud Customer Side Configuration Prerequisites

This section assumes Prisma Cloud has been successfully installed by the customer. Once Prisma Cloud is up and running, it must be connected to your cloud infrastructure. Please check the following onboarding options for how to connect your cloud infrastructure to Prisma Cloud:

- Cloud Account Onboarding
- Onboard Your AWS Account
- Onboard Your Azure Subscription
- Onboard Your Google Cloud Platform (GCP) Account
- Onboard Your Alibaba Cloud Account

Configuring Prisma Cloud for the Forescout TDR Log Puller

Prisma Cloud supports pull mechanism. Palo alto provides a very well-written API reference. This API reference include the API links that should be called during making Rest API calls. The API URL for the Prisma Cloud service varies depending on the cluster on which your tenant is deployed. To access Primsa Cloud Rest API, you need to have an access key. Once you have an access key, you need to obtain a JWT which will be used for every Prisma Cloud REST API request.

Prisma Cloud Selecting the New Data Source

1. Log in to Forescout TDR and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout TDR to Receive Prisma Cloud Logs

Data Source Name – Prisma Cloud

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or Hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **API URL**.
2. Enter the **ACCESS KEY ID** that will be used for authentication.
3. Enter the **SECRET KEY** that will be used for authentication.
4. Enter the **BASE DN** – *the Base domain name.*
5. Enter the **SCHEDULE INTERVAL** which specifies the Data Source pulling interval schedule in seconds with the default being 720 (two hours).
6. Enter the **MAX PULLING AGE** in seconds - the default is 604800 (1 month).
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Ping Identity

This series of topics covers all products offered by Ping Identity™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

PingIdentity™ PingFederate™ (Push)

PingIdentity™ PingFederate™ (Push)

PingIdentity™ PingFederate™ is an enterprise identity bridge. It enables outbound and inbound solutions for single sign-on (SSO), federated identity management, customer identity and access management, mobile identity security, API security, and social identity integration. Browser-based SSO extends employee, customer, and partner identities across domains without passwords using standard identity protocols such as SAML, WS-Federation, WS-Trust, OAuth and OpenID Connect, and SCIM.

To add PingFederate to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

PingIdentity PingFederate provides a user documentation portal here.

Target Data Logs

Forescout currently targets server event log files for ingesting security audit logs: In CEF format and syslog format. These logs record a subset of transaction log information with additional details at runtime, intended to facilitate security auditing and regulatory compliance.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout XDR to receive the logs.

Proofpoint

This series of topics covers data sources offered by Proofpoint that are supported by Forescout eyeAlert.

Proofpoint Threat Response (Push)

Proofpoint PoD (Pull)

Proofpoint Threat Response Auto-Pull (Push)

Proofpoint™ Threat Response Auto-Pull™ (TRAP) enables messaging and security administrators to analyze emails and move malicious or unwanted emails to quarantine, after delivery. It follows forwarded mail and distribution lists and creates an auditable activity trail.

To add Proofpoint Threat Response Auto-Pull to Forescout TDR as a Data Source, complete the following tasks:

Log Retrieval Method

Forescout TDR uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Proofpoint explains how to access their documentation resources here.

Target Data Logs

Forescout currently processes incidents logs.

Log Format Necessary for Forescout TDR Retrieval

Use the CEF format if possible, or the Syslog format if not, when configuring your Data Source to send logs to Forescout TDR.

Configure Forescout TDR to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout TDR, and for information about configuring Forscout XDR to receive the logs.

Proofpoint PoD (Pull)

Proofpoint on Demand™ (PoD) delivers Proofpoint's unified email security and data loss prevention features as a SaaS (Software-as-a-Service) solution. Based on the same platform that powers Proofpoint Messaging Security Gateway™ appliances, Proofpoint on Demand offers protection against both inbound and outbound email-borne threats without requiring the installation of on-premises hardware or software. To add Proofpoint POD to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Proofpoint POD Data Source in the Forescout eyeAlert UI

Target Data Logs

The following logs are relevant for Forescout TDR ingestion:

- ProofpointPOD_message_CL
- ProofpointPOD_maillog_CL

Proofpoint POD Customer Side Configuration Prerequisites

Public access to Proofpoint configuration documentation is limited and requires authorized credentials. Additional documentation is available for Forescout employees only here under "External References". Ensure that you have configured the product for pulling by Forescout eyeAlert and have the following pieces of information on hand during the procedure to configure Forescout eyeAlert to receive Proofpoint POD logs:

- Authorization Token
- Cluster ID

Proceed to Selecting the Proofpoint POD Data Source.

Selecting the ProofPoint POD Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout TDR to Receive Proofpoint Pod Logs

Data Source Name – Proofpoint POD

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **AUTHORIZATION TOKEN.**
2. Enter the Proofpoint API cluster id into the **CLUSTER ID** field.
3. Select the preferred **TIME ZONE** from the dropdown.

4. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
5. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Streaming for continuous retrieval of target data logs.
6. Click the **Apply** button.CThe UI will indicate whether the deployment has been successful.

Proofpoint Threat Response (Pull)

Proofpoint Threat Response™ orchestrates and automates incident response. The platform surrounds security alerts with contextual data to help security teams prioritize and execute response actions.

To add Proofpoint Threat Response to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source.

Key Data Source Product Configuration and Authentication Requirements

To onboard logs from this Data Source, you will need to have the following credential information on-hand when configuring Forescout eyeAlert:

- API URL
- API KEY

Note:

The API authorization key must have the following characteristics:

- The date range must be less than or equal to 30 days.
- The API cannot be called by specifying only *created_before* or only *closed_before*; an *after* date range parameter must be specified.
- The API client must specify ***created_after*** or ***closed_after*** for any API call.

Note:
You must allow-list the ip you are using to pull the logs.

Suggested Information Sources for Data Source Product Configuration

Proofpoint provides integration documentation here.

Note:
The reference links above are suggestions only. To ensure accuracy, confirm that you are using the latest official documentation provided by the vendor of your Data Source product to ensure accuracy.

Target Data Logs

Forescout currently targets Incidents logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON format when configuring your Data Source to make logs available for ingestion by Forescout eyeAlert.

Configure Forescout eyeAlert to Retrieve the Data Source Logs

See Configuring Forescout eyeAlert to Receive Proofpoint Threat Response Data Logs.

Configuring Forescout eyeAlert to Receive Proofpoint Threat Response Data Logs

Data Source Name – Proofpoint Threat Response

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **API URL** .
2. Enter the **API KEY**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 300.

4. Enter the desired value into the **NO FLOW ALERT THRESHOLD** - the default is the value of the schedule interval plus one hour.

5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Proofpoint Targeted Attack Protection (Pull)

Proofpoint™ Targeted Attack Protection™ (TAP) detects, analyzes and blocks advanced threats before they reach your inbox. This includes ransomware and other advanced email threats delivered through malicious attachments and URLs. To add ProofPoint TAP to Forescout TDR as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the ProofPoint TAP Data Source in the Forescout eyeAlert UI

Proofpoint TAP Customer Side Configuration Prerequisites

- Log retrieval requires use of the Proofpoint SIEM API.
- Retain the following information items because they will be referenced in the Forescout TDR UI procedure to add this Data Source:
- Proofpoint TAP SIEM API URL
- Principal key
- Secret Key
- Estimate of logs rate per second

ProofPoint Tap Selecting a New Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to Selecting the New Data Source.

Configuring Forescout TDR to Receive Proofpoint Tap Data Logs

Data Source Name – Proofpoint TAP

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **TAP SIEM API URL** – the default value is https://tap-api-v2.proofpoint.com/v2/siem/all.
2. Enter the Proofpoint TAP service **PRINCIPAL KEY**.
3. Enter the Proofpoint TAP service **SECRET KEY**.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 600.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 12 hours expressed in seconds as 43200.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for

later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Pure

This series of topics covers Data Source products offered by Pure that are supported by Forescout eyeAlert.

Pure Storage (Push)

Pure Storage (Push)

This manual is under construction.

Qualys

This series of topics covers all products offered by Qualys™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Qualys Data Source

Qualys Data Source (Pull)

Qualys™ enables the automatic inventory of all known and unknown assets in a global IT infrastructure – on prem, endpoints, clouds, containers, mobile, OT and IoT. Qualys scans report on analyzed threats and device misconfigurations that present cybersecurity vulnerabilities. To add Qualys to Forescout eyeAlert as a Data Source, complete the following tasks:

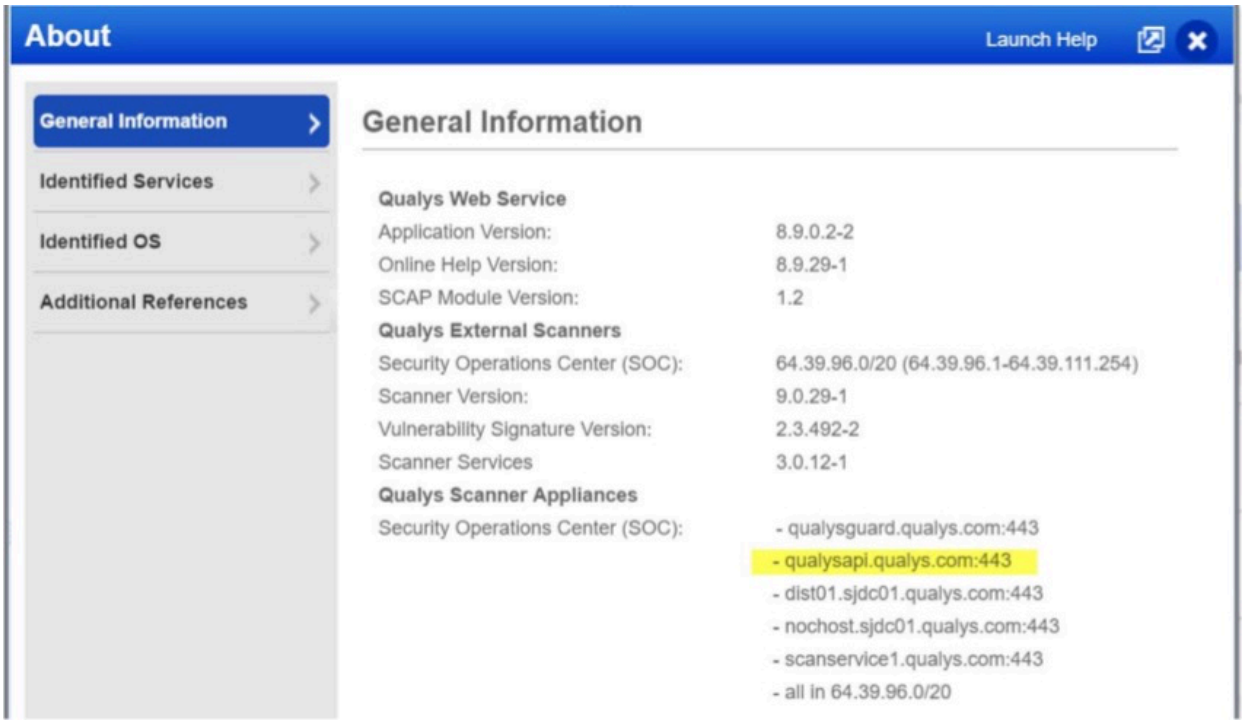
1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Qualys Data Source in the Forescout eyeAlert UI

How Forescout Uses Qualys

When Forescout's Data Science team creates an Indicator or Detection rule, the Qualys scan report can be queried using the host entity information to provide further insight for analysis of the possible threat.

Qualys Customer Side Configuration Prerequisites

To setup the API, log in to your Qualys account and go to Help > About. You'll see information under Security Operations Center (SOC). Here is an example:



Please notice that each account has a different API URL - they are not always the same.

Reference the Qualys API guide for detailed documentation and retrieve and note for future reference the **API URL**.

Qualys Selecting New Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Qualys Data Logs

Data Source Name – Qualys

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **API URL**– the default value is qualysapi.qualys.com.
2. Enter the Qualys **USERNAME**.
3. Enter the Qualys **PASSWORD**.
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 43200 (12 hours).
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 24 hours expressed in seconds as 86400.
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
7. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Redhat

This series of topics covers all products offered by Redhat™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Redhat Openshift (Push)

Redhat Openshift (Push)

To add Redhat Openshift to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Redhat provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format if possible, or Syslog if not, when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you

should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout XDR to receive the logs.

Rsyslog

This series of topics covers all products offered by RSYSLOG™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Rsyslog Custom Configuration (Push)

Rsyslog Custom Configuration (Push)

Rsyslog is a system for log processing. It offers high-performance, security features and a modular design. While it started as a regular syslogd, rsyslog has evolved into a kind of swiss army knife for logging. Rsyslog accepts data from different types of source (systems/applications) and outputs it into multiple formats:

- accept inputs from a wide variety of sources,
- transforms them,
- and output the results to diverse destinations.

Rsyslog has a strong enterprise focus but also scales down to small systems. It supports, among others, MySQL, PostgreSQL, failover log destinations, ElasticSearch, syslog/tcp transport, fine grain output format control, high precision timestamps, queued operations and the ability to filter on any message part.

To add Rsyslog custom configuration to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Rsyslog provides access to user documentation here.

Target Data Logs

Forescout currently processes Rsyslogd logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format if possible, or the Rsyslog format if not, when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout XDR to receive the logs.

Rubrik

This series of topics covers Data Source products offered by Rubrik that are supported by Forescout eyeAlert.

Rubrik Polaris (Push)

Rubrik Polaris (Push)

Rubrik Polaris, a SaaS platform, operationalizes all data situated in your distributed environment into a metadata framework and organizes all your business information to make it discoverable and usable.

To add Rubrik Polaris to Forescout eyeAlert as a Data Source, complete the following tasks:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Rubrik provides a user documentation portal here.

Target Data Logs

Forescout currently processes various log types.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format if possible, or the Syslog format if not, when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic and use port range 30001-30004 as the port destination for logs.

Sailpoint

This series of topics covers all products offered by Sailpoint™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Sailpoint IdentityIQ (Push)

Sailpoint IdentityIQ (Push)

SailPoint IdentityIQ™ is an identity and access management (IAM) solution for enterprise customers that delivers automated access certifications, policy management, access request and provisioning, password management, and identity intelligence. IdentityIQ has a flexible connectivity model that simplifies the management of applications running on-premise or in the cloud.

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Sailpoint provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout eyeAlert currently processes identity and access management logs.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding .

Salesforce

This series of topics covers all products offered by Salesforce™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Salesforce CRM (Pull)

Salesforce CRM (Pull)

Salesforce™ is an online solution for Customer Relationship Management (CRM). To add Salesforce to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Salesforce Data Source in the Forescout eyeAlert UI

Salesforce Customer Side Configuration Prerequisites

Note the following information items for later reference in the Forescout eyeAlert UI procedure:

- Consumer key
- Consumer secret
- Security token
- Username and password
- Whether the Salesforce environment being connected to is a sandbox environment or not
- Estimate of logs rate per second

Reference the Salesforce API guide for detailed documentation.

Salesforce Selecting a New Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.

3. Click the **+ Data Source**button.

4. Click the **DATA SOURCE** dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR** dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME** field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to Select the New Data Source.

Configuring Forescout eyeAlert to Receive Salesforce Data Logs

Data Source Name – Salesforce

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the Salesforce connected application **CONSUMER KEY**.
2. Enter the Salesforce connected **CONSUMER SECRET**.
3. Enter the **SECURITY TOKEN** of the customer Salesforce API service account.
4. Enter the **USERNAME** of the customer Salesforce API service account.
5. Enter the **PASSWORD** of the customer Salesforce API service account.
6. Enter the Salesforce **TOPICS**, separated by comma.
7. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
8. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Streaming for continuous retrieval of target data logs.
9. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

SAP

This series of topics covers all products offered by SAP™ that can be used as a Data Source for

Forescout eyeAlert log ingestion.

SAP BTP

This manual is under construction.

To add CrowdStrike™ Hosts™ to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source.

Key Data Source Product Configuration and Authentication Requirements

To onboard logs from this Data Source, you will need to have the following credential information on-hand when configuring Forescout eyeAlert:

- **AUTHENTICATION URL**: Used to generate an API token.
- **AUDIT LOGS URL**: Use to retrieve audit data from SAP BTP.
- **CLIENT ID**: The client ID that will be used for authentication.
- **CLIENT SECRET**: Client secret that will be used for authentication.

Suggested Information Sources for Data Source Product Configuration

SAP BTP provides a public help center here.

Note:
The reference links above are suggestions only. To ensure accuracy, confirm that you are using the latest official documentation for your product version provided by product vendor to ensure accuracy.

Target Data Logs

Forescout currently targets network security logs for ingestion and processing.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON format when configuring your Data Source to make logs available for ingestion by Forescout eyeAlert.

Configure Forescout eyeAlert to Retrieve the Data Source Logs

Configuring Forescout eyeAlert to Receive SAP BTP Logs.

Configuring Forescout eyeAlert to Receive SAP BTP Logs

Data Source Name – SAP BTP

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration* > *Data Sources* > *+ Add Data Source* > *Add Data Source to Connector* – *Configurations* (right-panel)

1. Enter the **AUTHENTICATION URL** .
2. Enter the appropriate value into the **AUDIT LOGS URL** field.
3. Enter the appropriate value into the **CLIENT ID** field.
4. Enter the appropriate value into the **CLIENT SECRET** field.
5. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is *3600* or 1 hour.
6. Enter a value in seconds between 3900 and 608400 into the **NO FLOW ALERT THRESHOLD**, which specifies the time to wait before alerting on absence of logs.
7. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as *2592000*.
8. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
9. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is *Pulling* for periodic retrieval of target data logs.
10. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Sentinel One

This series of topics covers Data Source products offered by Sentinel One that are supported by Forescout eyeAlert.

SentinelOne Deep Visibility (Pull)

SentinelOne Endpoint Security (Push)

SentinelOne Deep Visibility (Pull)

SentinelOne™ Deep Visibility™ empowers users with rapid threat hunting capabilities thanks to SentinelOne's Storylines technology. Each autonomous SentinelOne Agent builds a model of its endpoint infrastructure and real-time running behavior. The Storyline ID is an ID given to a group of related events in this model. When you find an abnormal event that seems relevant, use the Storyline ID to quickly find all related processes, files, threads, events and other data with a single query.To add SentinelOne Deep Visibilityto Forescout eyeAlert as a Data Source, complete the following tasks:

On-premise Connector Deployment Environment

1. Review the Customer-Side Configuration Prerequisites and Configure Data Logs for Discovery by Forescout eyeAlert.

Hosted Connector Deployment Environment

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the IntSights Data Source in the Forescout eyeAlert UI.

Target Data Logs

S1 Deep Visibility gives out messages on a pub/sub architecture. Those messages are parsable into JSON format. Forescout currently targets the following event types from the logs:

- File Modification
- File Creation
- File Deletion
- Process Creation
- Process Exit
- Process Termination
- Dns Query
- TCPv4 Connection
- TCPv4 Listen
- Http Request
- Registry Key Security Changed
- Registry Value Modified
- Registry Value Delete
- Scheduled Task Update
- Scheduled Task Start
- Scheduled Task Trigger

SentinelOne™ Deep Visibility™ Customer Side Configuration Prerequisites

Forescout TDR obtains SentinelOne Deep Visibility EDR logs using the pull mechanism. Only SentinelOne Deep Visibility users are authorized to access the documentation portal, but some guidance is provided here.**Additional information is available for Forescout employees** here.

Deep Visibility logs are not obtained via a RESTful API like most. To get the EDR events from the SentinelOne instance, a message broker called Hermes, which is an abstraction of a message broker that uses Apache Kafka. You do require credentials to be able to subscribe to the message broke to listen to the events. They are the same as any other pub/sub consumer:

- **topic_name:** The name of the topic the events will be published on by the broker
- **consumer_user_name:** Consumer user name.
- **consumer_password:** Consumer password.
- **broker_dns:** DNS address of the Kafka broker.
- **broker_dns_port:** Port that the messages will be emitted on.
- **group_id:** An ID for the consumer group this consumer will join.

Once the client (message consumer) has created a connection to the message broker channel, the message consumer, which in this case is Forescout TDR, needs to poll the broker for new messages. The broker in turn sends back all logs that were created in that specified time period, or in the number of messages we specify.

During the procedure to configure Forescout TDR to receive SentinelOne Deep Visibility logs, in addition to the values listed above you will be prompted to enter the following information:

- Kafka Topic Name
- Consumer Group ID

- Consumer Username
- Consumer Password

Proceed now to Selecting the SentinelOne Deep Visibility Data Source.

Selecting the SentinelOne Deep Visibility Data Source

1. Log in to Forescout TDR and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout TDR to Receive SentnelOne Deep Visibility Logs

Data Source Name – SentinelOne Deep Visibility

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter your **Kafka Topic Name.**
2. Enter your **Consumer Group ID**.
3. Enter your **Consumer Group Username**.

4. Enter your **Consumer Password**.

5. Enter the **Maximum Number of Messages**, with the default being 10.
6. Enter the **Timeout value**, with the default being 60 seconds.
7. Enter the **Broker DNS** address.
8. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
9. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Sentinel One End Point Security (Push)

Sentinel One™ End Point Security™ is an EDR (Endpoint Detection and Response) tool. EDR tools are typically deployed on endpoints. They collect data from endpoints, analyze the data to reveal potential cyber threats and issues and, if a threat is found, typically the end-user is immediately prompted with preventive list of actions.

To add Sentinel One End Point Security to Forescout TDR as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout TDR uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Sentinel One provides a resource center here.

Target Data Logs

Forescout currently processes event logs.

Log Format Necessary for Forescout TDR Retrieval

Use the CEF2 format when configuring your Data Source to send logs to Forescout TDR.

Configure Forescout TDR to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout TDR, and for information about configuring Forscout XDR to receive the logs.

SonicWall

This series of topics covers all products offered by SonicWall™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

SonicWall Firewall (Push)

Sonicwall SMA (Push)

SonicWall Firewall (Push)

SonicWall™ Firewall™ covers a spectrum of devices and virtual firewalls for different ranges of businesses, from small companies to large enterprises. The main function of the SonicWall Firewall is to prevent unauthorized access outside the private network. SonicWall also can be deployed to protect endpoints over the cloud infrastructure and also hybrid-cloud projects.

To add SonicWall to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

SonicWall provides a user documentation portal here.

Target Data Logs

Forescout currently processes standard Syslog or ArcSight (CEF) logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF or Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout XDR to receive the logs.

Sonicwall SMA (Push)

SonicWall Secure Mobile Access (SMA) is a unified secure access gateway that enables organizations to provide access to any application, anytime, from anywhere and any devices, including managed and unmanaged. SonicWall's SMA allows administrators to provision secure mobile access and identity-based privileges.

To add SonicWall SMA to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

SonicWall provides a user documentation portal here.

Target Data Logs

Forescout currently processes system message logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for

information about configuring Forscout XDR to receive the logs.

Snare

This series of topics covers all products offered by SonicWall™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Snare Syslog

Snare Syslog (Push)

Snare is a log collection and management solution, providing Snare Agents to ingest logs from different sources and Snare Central to store and archive log data. Snare Agents output events in tab-delimited records commonly referred to as Snare format, and can use syslog over TCP or UDP as the transport.

To add Snare Syslog to Forescout TDR as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout TDR uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

No publicly-available documentation source could be found.

Target Data Logs

Forescout currently targets various log types for ingestion.

Log Format Necessary for Forescout TDR Retrieval

Use the Syslog in SNARE format when configuring your Data Source to send logs to Forescout TDR.

Configure Forescout TDR to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic and send the logs to destination port range 30000-30006.

Sophos

This series of topics covers all products offered by Sophos™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Sophos Endpoint (Pull)

Sophos Firewall (Push)

Sophos UTM (Push)

Sophos Endpoint (Pull)

Sophos™ Endpoint™ is an endpoint protection product that combines antimalware, web and application control, device control and other touch points. To add Sophos to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Sophos Data Source in the Forescout eyeAlert UI

Customer Side Configuration Prerequisites

The following configuration must be in place to retrieve logs:

- The logs are pulled (HTTPs REST) based on the schedule interval (e.g: 1 minutes)
    - Log format: JSON
    - Log Transport: TCP
    - Logs have timestamp in UTC
- Review the Sophos API documentation to configure the SIEM API. Make note of the following information items for reference during the Forescout eyeAlert UI procedure:
    - SIEM API URL
    - Authorization key
    - x-API-key
    - Estimate of logs rate per second

Selecting the Sophos Endpoint Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to Selecting the New Data Source.

Configuring Forescout eyeAlert to Receive Sophos Endpoint Logs

Data Source Name – Sophos

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration* > *Data Sources* > *+Data Source* > *Add Data Source to Connector* – *Configurations* (right-panel)

1. Enter the **SIEM API URL**– the default value is https://api5.central.sophos.com/gateway/siem/v1/events.
2. Enter the Sophos **AUTHORIZATION** request header setting.
3. Enter the Sophos **API KEY**(API request header key).
4. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 600.
5. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 24 hours expressed in seconds as 86400.
6. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
7. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
8. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Sophos Firewall (Push)

Sophos™ SG/XG Firewall™ allows customers to manage their firewall, respond to threats, and monitor what's happening on the network.

To add Sophos Firewall to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Sophos Firewall provides an online help portal here.

Target Data Logs

Forescout currently processes the following log types for ingestion:

- Firewall
- IPS
- AntiVirus
- Anti Spam
- Content Filtering
- Event
- WAF

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout XDR to receive the logs.

Sophos UTM (Push)

Sophos™UTM™ is a unified threat management solution that employs machine learning and behavioral analysis to detect known and unknown malware with a focus on accurately identifying evasive ransomware and targeted attacks.

To add Sophos UTM to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Sophos Firewall provides an online help portal here.

Target Data Logs

Forescout currently processes firewall logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout XDR to receive the logs.

Squid

This series of topics covers all products offered by Squid™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Squid Proxy (Push)

Squid™ is a caching and forwarding HTTP web proxy. It has a wide variety of uses, including speeding up a web server by caching repeated requests, caching web, DNS and other computer network lookups for a group of people sharing network resources, and aiding security by filtering traffic.

To add Squid Proxy to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

No secure and public sites of documentation were available.

Target Data Logs

Squid creates multiple log files which offers access information alongside the system configuration errors and resource consumption (eg, memory, disk space) which is helpful mostly for debugging purposes.

- **access.log**

  Most log file analysis program are based on the entries in *access.log*.

  The log file format can be customized to a large extend (defined by the logformat directive), and there are multiple default formats which are build-in (squid, common, combined, referrer, useragent). By default, Squid will log in its native log file format (squid).

- **hierarchy.log**

  This log file exists for Squid-1.0 only which is not available for new installations. And for Squid 1.1 and later, this information was moved into access.log.

- **squid.out**

  If Squid was being run from the RunCache script, a file squid.out contains the Squid startup times, and also all fatal errors.

- **cache.log**

  The cache.log file contains the debug and error messages that Squid generates. From the area of automatic log file analysis, the cache.log file does not have much to offer. Usually this file will be used for automated error reports, when programming Squid, testing new features, or searching for reasons of a perceived misbehaviour, etc.

- **useragent.log**

  This log file contains information about the distribution of browsers of the clients, and is only maintained if it's been specifically configured for that, which is not recommended for a loaded production squid.

- **store.log**

  The store.log file covers the objects currently kept or removed from storage. As a kind of transaction log it is usually used for debugging purposes. The store.log file may be of interest to log file analysis which looks into the objects on the disks and the time they spend there, or how many times a hot object was accessed, However, the Squid developers recommend to treat store.log primarily as a debug file, and so should we, unless there are a clear reason for that.

- **icap_log**

ICAP log files record ICAP transaction summaries, one line per transaction. It's needed to be enabled.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout XDR to receive the logs.

Stormshield

This series of topics covers Data Source products offered by Stormshield that are supported by Forescout eyeAlert.

Stormshield Firewall (Push)

Stormshield Firewall (Push)

Stormshield Firewall™, also known as SNS firewall, is a security solution to protect corporate networks from cyber attacks. It includes real-time protection (intrusion prevention and detection, application control, antivirus, etc.), control and supervision (URL filtering, IP geolocation, vulnerability detection, etc.) and content filtering (anti spam, anti spyware, anti phishing, etc.).

To add Stormshield Firewall as a Data Source, ensure you use the following settings when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Stormshield provides an online help portal here.

Target Data Logs

Forescout currently processes the following log types for ingestion:

- Filter Policy
- Alarms
- Network Connections
- Application Connections
- Vulnerability Manager
- System Events
- Administration
- IPSec VPN
- Statistics
- SMTP Proxy
- POP3 Proxy

- FTP Proxy
- HTTP Proxy
- SSL Proxy
- Authentication
- SSL VPN
- Sandboxing
- Router Statistics
- Filter Statistics

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in Push-based Data Source Onboarding.

SUSE

This series of topics covers all products offered by SUSE™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

SUSE Linux (Push)

SUSE Linux (Push)

SUSE Linux™ is a computer operating system developed by SUSE. It is built on top of the free and open-source Linux kernel and is distributed with system and application software from other open-source projects.

To add SUSE Linux to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

SUSE Linux provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout XDR to receive the logs.

Symantec

This series of topics covers all products offered by Symantec™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Symantec Email Security (Pull)

Symantec Endpoint Protection (Push)

Symantec ProxySG Bluecoat (Push)

Symantec WSS (Pull)

Symantec Email Security (Pull)

Symantec™ Email Security™ is a cloud email security service that filters unwanted messages and protects your mailboxes from targeted attacks. To add Symantec Email Security to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Symantec Email Security Data Source in the Forescout eyeAlert UI

Target Data Logs

The following logs are relevant for Forescout TDR ingestion:

- Email logs
- Click logs

Symantec Email Security Customer Side Configuration Prerequisites

Forescout eyeAlert uses the pull mechanism to ingest logs from this data source, and supports the JSON format. For guidance, see the following vendor documentation:

- Deployment guide: https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/email-security/email-security-cloud/generated-pdfs/EmailServices_DeploymentGuide.pdf
- Data feeds API guide: https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/email-security/email-security-cloud/generated-pdfs/Data-Feeds-API-Guide-Email-Security.cloud.pdf

Once configured, there are a couple of parameters that need to be provided for Forescout to be able to successfully pull data from the instance:

- username
- password

Both are used with basic authentication with the Symantec Cloud API. The API URL is the same for all instances as it is shared by all. https://datafeeds.emailsecurity.symantec.com/all. Once the

necessary information and configurations have been completed, proceed to Selecting the Symantec Email Security Data Source.

Selecting the Symantec Email Security Data Source

1. Log in to Forescout TDR and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout TDR to Receive Symantec Email Security Logs

Data Source Name – Symantec Email Security

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **USERNAME**.
2. Enter the **PASSWORD**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 300.
4. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 15 minutes expressed in seconds as 900.
5. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
7. Click the **Add Data Source** button.

The UI will indicate whether the deployment has been successful.

Symantec Endpoint Protection (Push)

Symantec™ Endpoint Protection™, developed by Broadcom Inc., is a security software suite that

consists of anti-malware, intrusion prevention and firewall features for server and desktop computers. It has the largest market-share of any product for endpoint security. It provides a complete all-round end point protection system to the end-user.

To add Symantec Endpoint Protection to Forescout TDR as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout TDR uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Broadcom, which acquired Symantec, provides a user documentation portal here.

Target Data Logs

Forescout currently processes the following log types for ingestion:

- Policy logs
- Agent Activity logs
- Agent System logs
- Agent Security logs
- Agent Traffic logs
- Agent Behavior logs
- Agent Scan logs
- Agent Risk logs
- Agent Proactive Detection logs (SONAR)
- HIPS Activity logs

Log Format Necessary for Forescout TDR Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout TDR.

Configure Forescout TDR to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout TDR, and for information about configuring Forscout XDR to receive the logs.

Symantec ProxySG Bluecoat (Push)

Symantec™ ProxySG™ sits between users and their interactions with the Internet, and inspects content to identify malicious payloads to then filter, strip, block or replace web content to mitigate risks and prevent data loss (DLP).

To add Symantec ProxySG to Forescout TDR as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout TDR uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Broadcom, which acquired Symantec, provides a user documentation portal here.

Target Data Logs

Forescout currently processes network security logs for ingestion.

Log Format Necessary for Forescout TDR Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout TDR.

Configure Forescout TDR to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic.

Symantec WSS (Pull)

Symantec Web Security Service (WSS) is a cloud-delivered network security service that enforces comprehensive internet security and data compliance policies, regardless of location or device.Symantec Web Security Service delivers a broad set of advanced capabilities—including a secure web gateway (SWG), software defined perimeter, anti-virus scanning, sandboxing, web isolation, data loss prevention (DLP), and email security.To add Symantec WSS to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Symantec WSS Data Source in the Forescout eyeAlert UI

Target Data Logs

Forescout currently targets access logs for ingestion.

Symantec WSS Customer Side Configuration Prerequisites

To ingest logs from this Data Source, Forescout uses the pull mechanism and the Broadcom Web Security Service Sync API described in vendor documentation here**,** which allows a web client to obtain recently hardened log data from the cloud by downloading the current hour in smaller up-to-the-minute segments.Follow the vendor instructions located here to generate **Username** and **Password** API credentials, which will be used during the procedure to configure Forescout eyeAlert to receive the logs.

Additional Notes

1. Symantec ProxySG (formerly Blue Coat ProxySG)can forward its logs to Symantec WSS as

well (for a hosted reporting service).
2. If you use Symantec ProxySG in this manner, pages 17 and 28 of vendor documentation here explains how to use the ProxySG appliance upload client and the upload schedule to control the delay of the logs being in WSS. This might affect the logs available for the puller from the WSS's side.

Once the API credentials have been successfully generated, record the information and proceed to Selecting the Symantec WSS Data Source.

Selecting the Symantec WSS Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to Configuring Forescout eyeAlert to Receive Symantec WSS Logs..

Configuring Forescout TDR to Receive Symantec WSS Logs

Data Source Name – Symantec WSS

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **USERNAME**.
2. Enter the **PASSWORD**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 300.
4. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 15 minutes expressed in seconds as 900.
5. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
7. Click the **Add Data Source** button.

The UI will indicate whether the deployment has been successful.

Synology

This series of topics covers all products offered by Synology™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Synology NAS (Push)

Synology NAS (Push)

Synology is a company specializing in Network Attached Storage (NAS) device. NAS is an intelligent storage device connected to your home or office network. You can store all your family and colleagues' files on the NAS, from important documents to precious photos, music and video collections. By using a web browser or mobile apps, you can access files and use various services provided by the NAS via the Internet.

To add Synology NAS to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your Data Source:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Synology provides a Knowledge Center here.

Target Data Logs

Forescout currently processes Connection, System and WinFileService logs for ingestion..

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Sysdig

This series of topics covers all products offered by Sysdig™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Sysdig Secure (Push)

Sysdig Secure (Push)

Sysdig™ Secure™is part of Sysdig's container intelligence platform. Sysdig uses a unified platform to deliver security, monitoring, and forensics in a container and microservices-friendly architecture. Sysdig Secure takes a services-aware approach to runtime security and forensics and brings together deep container visibility with Docker and Kubernetes integration to block threats more effectively.

To add Sysdig Secure to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your Data Source:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Sysdig provides a user documentation portal here.

Target Data Logs

Forescout currently processes policy event logs.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forscout XDR to receive the logs.

Tanium

This series of topics covers all products offered by Tanium™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Tanium Data Source (Push)

Tanium Data Source (Push)

Tanium is a feature-packed endpoint management and endpoint security platform designed to strengthen and optimize an organization's cybersecurity efforts. The platform gives security teams the tools they need to fortify existing security gaps or completely overhaul their cybersecurity environments, providing complete threat response capabilities from a single endpoint agent.

To add Tanium to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Tanium provides a resource center here.

Target Data Logs

Forescout currently processes Palo Alto Network Wildfire, and Tanium Audit Source, Comply, Reputation, Threat Response, and Asset logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Tenable

This series of topics covers all products offered by Tenable™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Tenable SC

Tenable.io (Pull)

Tenable.sc (Pull)

Tenable.sc is a comprehensive vulnerability analysis solution that provides complete visibility into the security posture of the IT infrastructure. It consolidates and evaluates vulnerability data from across the entire IT infrastructure, illustrates vulnerability trends over time, and assesses risk with actionable context for effective remediation prioritization.

To add Tenable SC to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Tenable SC Data Source in the Forescout eyeAlert UI

Tenable.sc Customer Side Configuration Prerequisites

The following credentials will be necessary to configure command to receive Tenable SC logs:

- API URL
- ACCESS KEY
- QUERY ID
- CLIENT SECRET
- SCHEDULE INTERVAL

Proceed now to Selecting the Tenable SC Data Source.

Selecting the Tenable SC Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed now to Configuring Forescout eyeAlert to Receive Tenable SC Logs.

Configuring Forescout eyeAlert To Receive Tenable SC Logs

Data Source Name – Tenable SC

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the **API URL**.
2. Enter the **Access Key**.
3. Enter the **Query ID**.
4. Enter the **Client Secret**.
5. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 43200.
6. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
7. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
8. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
9. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Tenable.io (Pull)

Tenable.ioIs a cloud-based vulnerability management for complete visibility into the assets and vulnerabilities in the organization.

The platform is designed to support and visualize elastic IT assets, such as containers and web apps. Tenable offers pre-built integrations and allows developers to build new integrations quickly in order to improve their vulnerability management program. To add Tenable.io to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the tenable.io Data Source in the Forescout eyeAlert UI

Target Data Logs

Forescout currently targets the ingestion of vulnerability-related logs.

Tenable.io Customer Side Configuration Prerequisites

Forescout eyeAlert uses the push mechanism to ingest logs from this Data Source. For additional information beyond the procedure presented below, please see Tenable API Get Started. To set up access to Tenable.io API:

1. Verify that you have a valid user account with appropriate permissions by logging into Tenable.io.
2. Generate the API keys for the account. For more information, see Generate API Keys in the Tenable.io Vulnerability Management User Guide.
    a. In the upper-left corner, click the menu button.

       The left navigation plane appears.

        i. In the left navigation plane, click **Settings**.

           The **Settings** page appears.

        ii. Click the **My Account** tile.

            The **My Account** page appears, where you can view and update your account details.

    b. Click the **API Keys** tab.

       The **API Keys** section appears.

    c. Click **Generate**.

       The **Generate API Keys** window appears with a warning.

    d. Review the warning and click **Generate**.

The API keys must be assigned the access role of Administrator to be able to use the export API function (used for pulling the logs).

Selecting the Tenable IO Data Source

1. Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Tenable IO Logs

Data Source Name – Tenable.io

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration* > *Data Sources* > *+Data Source* > *Add Data Source to Connector* – *Configurations* (right-panel)

1. Enter the **Access Key**.
2. Enter the **Secret Key**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 300.
4. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 604800.
5. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
7. Click the **Apply** button.

Taxii

This series of topics covers all products offered by Taxii™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Taxii Data Source

Taxii Data Source

This manual is under construction.

Taxii2 Data Source

This manual is under construction.

Thinkst

This series of topics covers all products offered by Thinkst™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Thinkst Canary (Push)

Thinkst Canary™ is a deception technology that augments security programs with high fidelity detection points that can be spread across environments. To add Thinkst Canary to Forescout eyeAlert as a Data Source, complete the following tasks:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Thinkst provides a resource center here.

Target Data Logs

Forescout currently processes incident logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog or Rsyslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Trellix

This series of topics covers all products offered by Trellix™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

FireEye

This manual is under construction.

Trend Micro

This series of topics covers all products offered by Trend Micro™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Trend Micro Apex Central (Push)

Trend Micro™ Apex Central™ is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Configuration is managed through Trend Micro™ Control Manager™, a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Control Manager web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

To add Trend Micro Apex Central to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Trend Micro Apex Central provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Trend Micro Deep Discovery Analyzer (Push)

Trend Micro™ Deep Discovery Analyzer™ is a turnkey appliance that uses virtual images of endpoint configurations to analyze and detect targeted attacks.

To add Trend Micro Deep Discovery Analyzer to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Trend Micro Deep Discovery Analyzer provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Trend Micro Deep Discovery Inspector (Push)

Trend Micro™ Deep Discovery Inspector™ is a physical or virtual network appliance that monitors 360-degrees of your network to create complete visibility into all aspects of targeted attacks, advanced threats and ransomware.

To add Trend Micro Deep Discovery Inspector to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Trend Micro Deep Discovery Inspector provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

For information about data log types and field mapping, see Deep Discovery Inspector Reference Information

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Trend Micro Deep Discovery Detector (Push)

Trend Micro™ Deep Discovery Director™ is a management solution that enables the following:

- Centralized deployment of hotfixes, critical patches, firmware, and Virtual Analyzer images.
- Configuration replication.
- Log aggregation.
- Realtime threat detection monitoring and correlation
- Threat intelligence management and sharing

To add Trend Micro Deep Discovery Detector to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Trend Micro Deep Discovery Detector provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout currently targets the following logs for ingestion:

- CEF Virtual Analyzer Logs: Deny List Transaction Events
- CEF Threat Logs
- CEF Disruptive Application Logs
- CEF Web Reputation Logs
- CEF Detection Logs: Email Detection Logs
- CEF Detection Logs: Attachment Detection Logs
- CEF Detection Logs: URL Detection Logs

- CEF Message Tracking Logs
- CEF Virtual Analyzer Analysis Logs: File Analysis Events

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Trend Micro Deep Security Manager (Push)

Trend Micro™ Deep Security Manager™ provides advanced server security for physical, virtual, and cloud servers.

To add Trend Micro Deep Security Manager to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Trend Micro Deep Security Manager provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Deep Security has various modules that produce the following data logs relevant for Forescout eyeAlert ingestion:

- Anti-malware
- Firewall
- IPS
- IM
- LI
- Web Reputation Logs

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Trend Micro Deep Security Reference Information and CIM Field Mapping

The following tables provide information about data log types and fields:

Anti-malware logs:

DS CEF Logs	Name	data_type	Description	Examples
cn1	host_id	Long	The agent computer's internal unique identifier.	cn1=1
cn2	file_size	Long	The size of the quarantine file. This extension is included only when the "direct forward" from agent /appliance is selected.	cn2=100
cs3	file_path	String	The path of the spyware item. This field is only for spyware detection events.	cs3=C:\test\atse_samples\SPYW
cs4	resource_type	String	For example, if there's a spyware file named spy.exe that creates a registry run key to keep its persistence after system reboot, there will be two items in the spyware report: the item for spy.exe has cs4=10 (Files and Directories), and the item for the run key registry has cs4=11 (System Registry).	cs4=10
cs5	risk_level	String	Risk level values:	cs5=25
cs6	container	String	The image name of the Docker container, container name, and container ID where the malware was detected.	cs6=ContainerImageName | Cor
filePath	file_path	String	The location of the malware file.	filePath=C:\\Users\\Mei\\Deskto

act	action	String	The action performed by the Anti-Malware engine. Possible values are: Deny Access, Quarantine, Delete, Pass, Clean, Terminate, and Unspecified.	act=Clean
msg	Message	String	The type of scan. Possible values are: Realtime, Scheduled, and Manual.	msg=Realtime
dvc	dvc_ip4	IP	The IPv4 address for cn1.	dvc=10.1.144.199
dvchost	dvc_host	String	The hostname or IPv6 address for cn1.	dvchost=www.example.com
TrendMicroDsBehaviorRuleID	rule_id	Long	The behavior monitoring rule ID for internal malware case tracking.	BehaviorRuleID=CS913
TrendMicroDsBehaviorType	detection_type	String	The type of behavior monitoring event detected.	BehaviorType=Threat-Detection
TrendMicroDsTags	event_tags	String	Deep Security event tags assigned to the event	TrendMicroDsTags=suspicious
TrendMicroDsTenant	tenant	String	Deep Security tenant	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	tenant_id	Long	Deep Security tenant ID	TrendMicroDsTenantId=0
TrendMicroDsMalwareTarget	target_obj	String	The file, process, or registry key (if any) that the malware was trying to affect. If the malware was trying to affect more than one, this field will contain the value "Multiple."	TrendMicroDsMalwareTarget=C:\
TrendMicroDsMalwareTargetCount	target_count	String	The number of target files.	TrendMicroDsMalwareTargetCou
TrendMicroDsMalwareTargetType	target_type	String	The type of system resource	TrendMicroDsMalwareTargetType

			that this malware was trying to affect, such as the file system, a process, or Windows registry.	
TrendMicroDsProcess	proc_name	String	Process Name	TrendMicroDsProcess= abc.exe
TrendMicroDsFileMD5	file_hash_md5	String	The MD5 hash of the file	TrendMicroDsFileMD5=1947A1B
TrendMicroDsFileSHA1	file_hash_sha1	String	The SHA1 hash of the file	TrendMicroDsFileSHA1=5AD084
TrendMicroDsFileSHA256	file_hash_sha256	String	The SHA256 hash of the file	TrendMicroDsFileSHA256=25F23
TrendMicroDsDetectionConfidence	confidence	INT	Indicates how closely (in %) the file matched the malware model	TrendMicroDsDetectionConfidenc
TrendMicroDsRelevantDetectionNames	Probable Threat Type	String	Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats(separate by semicolon";")	TrendMicroDsRelevantDetectionN
Severity	severity_level	String	The severity of the event. 1 is the least severe; 10 is the most severe.	sev=6
Category	event_category	String	Category	cat=Anti-Malware
Name	event_name	String	Event name	name=SPYWARE_KEYL_ACTIVE
Description	event_description	String	Event description. Anti-Malware uses the event name as the description.	desc=SPYWARE_KEYL_ACTIVE

App Control Logs

CEF	CIM Name	data_type	Description	Examples
cn1	host_id	String	The agent computer's internal unique identifier.	cn1=2

cs1	reason	String	The reason why application control performed the specified action, such as "notWhitelisted" (the software did not have a matching rule, and application control was configured to block unrecognized software).	cs1=notWhitelisted
cs2	file_hash_sha1	String	If it was calculated, the SHA-1 hash of the file.	cs2=156F4CB711FDBD668943711F853FB6DA89
cs3	file_hash_md5	String	If it was calculated, the MD5 hash of the file.	cs3=4E8701AC951BC4537F8420FDAC7EFBB5
act	action	String	The action performed by the Application Control engine. Possible values are: Blocked, Allowed.	act=blocked
dvc	dvc_ip4	String	The IPv4 address for cn1.Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.)	dvc=10.1.1.10
dvchost	dvc_host	String	The hostname or IPv6 address for cn1.	dvchost=www.example.com
suid	user_id	String	The account ID number of the user name.	suid=0
suser	user_name	String	The name of the user account that installed the software on the protected computer.	suser=root
TrendMicroDsTenant	tenant	String	Deep Security tenant name.	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	tenant_id	String	Deep Security tenant ID number.	TrendMicroDsTenantId=0

fileHash	file_hash_sha256	String	The SHA 256 hash that identifies the software file.	fileHash=E3B0C44298FC1C149AFBF4C8996FB92
filePath	file_path	String	The location of the malware file.	filePath=/bin/my.jar
fsize	file_size	String	The file size in bytes.	fsize=16
aggregationType	aggregation_type	String	An integer that indicates how the event is aggregated: 0: The event is not aggregated, 1: The event is aggregated based on file name, path, and event type., 2: The event is aggregated based on event type.	aggregationType=2
repeatCount	event_count	String	The number of occurrences of the event. Non-aggregated events have a value of 1. Aggregated events have a value of 2 or more.	repeatCount=4
Severity	severity_level	String	The severity of the event. 1 is the least severe; 10 is the most severe.	sev=6
Category	event_category	String	Category	cat=AppControl
Name	event_name	String	Event name	name=blocked
Description	event_description	String	Event description. Application Control uses the action as the description.	desc=blocked

Firewall Logs

CEF Extension Field	CIM name	Data_type	Description	Examples
act	action	String		act=Log
cn1	host_id	String	The agent computer's	cn1=113

			internal unique identifier.	
cnt	event_count	String	The number of times this event was sequentially repeated.	cnt=8
cs2	tcp_flags	String		cs2=0x10 ACK
cs3	fragmentation_bits	String		cs3=DF MF
cs4	icmp_type	String	(For the ICMP protocol only) The ICMP type and code, delimited by a space.	cs4=11 0
dmac	dst_mac	String	MAC address of the destination computer's network interface.	dmac= 00:0C:29:2F:09:B3
dpt	dst_port	String	(For TCP and UDP protocol only) Port number of the destination computer's connection or session.	dpt=80
dst	dst_ip4	String	IP address of the destination computer.	dst=192.168.1.102
in	bytes_in	String	(For inbound connections only) Number of inbound bytes read.	in=137
out	bytes_out	String	(For outbound connections only) Number of outbound bytes read.	out=216
proto	protocol	String	Name of the transport protocol used.	proto=tcp
smac	src_mac	String	MAC address of the source computer's network interface.	smac= 00:0E:04:2C:02:B3
spt	src_port	String	(For TCP and UDP protocol only) Port number of the source	spt=1032

			computer's connection or session.	
src	src_ip4	String	The packet's source IP address at this event.	src=192.168.1.105
TrendMicroDsFrameType	frame_type	String	Connection ethernet frame type.	TrendMicroDsFrameType=IP
TrendMicroDsPacketData	packet_data	String	The packet data, represented in Base64.	TrendMicroDsPacketData=AFB...
dvc	dvc_ip4	String	The IPv4 address for cn1.	dvc=10.1.144.199
dvchost	dvc_host	String	The hostname or IPv6 address for cn1.	dvchost=exch01.example.com
TrendMicroDsTags	event_tags	String	Deep Security event tags assigned to the event	TrendMicroDsTags=suspicious
TrendMicroDsTenant	tenant	String	Deep Security tenant	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	tenant_id	String	Deep Security tenant ID	TrendMicroDsTenantId=0
sev	severity_level	String	The severity of the event. 1 is the least severe; 10 is the most severe.	sev=5
cat	event_category	String	Category	cat=Firewall
name	event_name	String	Event name	name=Remote Domain Enforcement (Split Tunnel)
desc	event_description	String	Event description. Firewall events use the event name as the description.	desc=Remote Domain Enforcement (Split Tunnel)

IM Events:

CEF Extension Field	CIM	data_type	Description	Examples
act	action	String	The action detected by the integrity rule. Can contain: created,	act=created

			updated, deleted or renamed.	
cn1	host_id	Long	The agent computer's internal unique identifier.	cn1=113
filePath	file_path	String	The integrity rule target entity. May contain a file or directory path, registry key, etc.	filePath=C:\WINDOWS\system32\drivers\etc\hosts
suser	user_name	String	Deep Security Manager administrator's account.	suser=MasterAdmin
sproc	src_proc	String	The name of the event's source process.	sproc=C:\\Windows\\System32\\notepad.exe
msg	event_description	String	(For "renamed" action only) A list of changed attribute names.	msg=lastModified,sha1,size
oldfilePath	Old target entity	String	(For "renamed" action only) The previous integrity rule target entity to capture the rename action from the previous target entity to the new, which is recorded in the filePath field.	oldFilePath=C:\WINDOWS\system32\logfiles\ds_agent.log
dvc	dvc_ip4	String	The IPv4 address for cn1.	dvc=10.1.144.199
dvchost	dvc_host	String	The hostname or IPv6 address for cn1.	dvchost=www.example.com
TrendMicroDsTags	event_tags	String	Deep Security event tags assigned to the event	TrendMicroDsTags=suspicious
TrendMicroDsTenant	tenant	String	Deep Security	TrendMicroDsTenant=Primary

			tenant	
TrendMicroDsTenantId	tenant_id	Long	Deep Security tenant ID	TrendMicroDsTenantId=0
sev	severity_level	String	The severity of the event. 1 is the least severe; 10 is the most severe.	sev=8
cat	event_category	String	Category	cat=Integrity Monitor
name	event_name	String	Event name	name=Microsoft Windows - System file modified
desc	event_description	String	Event description. Integrity Monitoring uses the event name as the description.	desc=Microsoft Windows - System file modified

IPS Events

CEF Extension Field	CIM Field	data_type	Description	Examples
act	action	String	(IPS rules written before Deep Security version 7.5 SP1 could additionally perform Insert, Replace, and Delete actions. These actions are no longer performed. If an older IPS Rule is triggered which still attempts to perform those actions, the event will indicate that the rule was applied in detect-only mode.)	act=Block
cn1	host_id	String	The agent computer's internal unique identifier.	cn1=113

cn3	packet_location	String	Position within packet of data that triggered the event.	cn3=37
cnt	event_count	String	The number of times this event was sequentially repeated.	cnt=8
cs1	Intrusion Prevention Filter Note	String	(Optional) A note field which can contain a short binary or text note associated with the payload file. If the value of the note field is all printable ASCII characters, it will be logged as text with spaces converted to underscores. If it contains binary data, it will be logged using Base-64 encoding.	cs1=Drop_data
cs2	tcp_flags	String	(For the TCP protocol only) The raw TCP flag byte followed by the URG, ACK, PSH, RST, SYN and FIN fields may be present if the TCP header was set.	cs2=0x10 ACK
cs3	fragmentation_bits	String		cs3=DF
cs4	icmp_type	String	(For the ICMP protocol only) The ICMP type and code stored in	cs4=11 0

			their respective order delimited by a space.	
cs5	stream_location	String	Position within stream of data that triggered the event.	cs5=128
dmac	dst_mac	String	Destination computer network interface MAC address.	dmac= 00:0C:29:2F:09:B3
dpt	dst_port	String	(For TCP and UDP protocol only) Destination computer connection port.	dpt=80
dst	dst_ip4	String	Destination computer IP Address.	dst=192.168.1.102
xff	http_header _x_forward_for	String	The IP address of the last hub in the X-Forwarded-For header.	xff=192.168.137.1
in	bytes_in	String	(For inbound connections only) Number of inbound bytes read.	in=137
out	bytes_out	String	(For outbound connections only) Number of outbound bytes read.	out=216
proto	protocol	String	Name of the connection transport protocol used.	proto=tcp
smac	src_mac	String	Source computer network interface MAC address.	smac= 00:0E:04:2C:02:B3

spt	src_port	String	(For TCP and UDP protocol only) Source computer connection port.	spt=1032
src	src_mac	String	Source computer IP Address. This is the IP of the last proxy server, if it exists, or the client IP. See also the xff field.	src=192.168.1.105
TrendMicroDsFrameType	frame_type	String	Connection ethernet frame type.	TrendMicroDsFrameType=IP
TrendMicroDsPacketData	packet_data	String	The packet data, represented in Base64.	TrendMicroDsPacketData=R0VUIC9zP3...
dvc	dvc_ip4	String	The IPv4 address for cn1.	dvc=10.1.144.199
dvchost	dvc_host	String	The hostname or IPv6 address for cn1.	dvchost=www.example.com
TrendMicroDsTags	event_tags	String	Deep Security event tags assigned to the event	TrendMicroDsTags=Suspicious
TrendMicroDsTenant	tenant	String	Deep Security tenant name	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	tenant_id	String	Deep Security tenant ID	TrendMicroDsTenantId=0
sev	severity_level	String	The severity of the event. 1 is the least severe; 10 is the most severe.	sev=10
cat	event_category	String	Category	cat=Intrusion Prevention
name	event_name	String	Event name	name=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities
desc	event_description	String	Event description.	desc=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities

			Intrusion Prevention events use the event name as the description.	

LI Logs

CEF Extension Field	CIM	data_types	Description	Examples	Index Searchable (Y/N)
cn1	host_id	String	The agent computer's internal unique identifier.	cn1=113	N
cs1	rub_rule_name	String	The Log Inspection sub-rule which triggered this event.	cs1=Multiple Windows audit failure events	Y
duser	dst_user	String	(If parse-able username exists) The name of the target user initiated the log entry.	duser=(no user)	Y
fname	target_obj	String	The Log Inspection rule target entity. May contain a file or directory path, registry key, etc.	fname=C:\Program Files\CMS\logs\server0.log	Y
msg	event_description	String	Details of the Log Inspection event. May contain a verbose description of the detected log event.	msg=WinEvtLog: Application: AUDIT_FAILURE(20187): pgEvent: (no user): no domain: SERVER01: Remote login failure for user 'xyz'	Y
shost	src_host	String	Source computer hostname.	shost=webserver01.corp.com	Y
src	src_ip4	String	Source computer IP address.	src=192.168.1.105	Y
dvc	dvc_ip4	String	The IPv4	dvc=10.1.144.199	Y

			address for cn1.		
dvchost	dvc_host	String	The hostname or IPv6 address for cn1.	dvchost=www.example.com	Y
TrendMicroDsTags	event_tags	String	Deep Security event tags assigned to the event	TrendMicroDsTags=suspicious	N
TrendMicroDsTenant	tenant	String	Deep Security tenant	TrendMicroDsTenant=Primary	Y
TrendMicroDsTenantId	tenant_id	String	Deep Security tenant ID	TrendMicroDsTenantId=0	Y
sev	severity_level	String	The severity of the event. 1 is the least severe; 10 is the most severe.	sev=3	
cat	event_category	String	Category	cat=Log Inspection	
name	event_name	String	Event name	name=Mail Server - MDaemon	
desc	event_description	String	Event description.	desc=Server Shutdown	

WRS Events:

CEF Extension Field	CIM Field	Data_type	Description	Examples
cn1	host_id	Long	The agent computer's internal unique identifier.	cn1=1
request	request_url	String	The URL of the request.	request=http://www.example.com/index.php
msg	scan_type	String	The type of action. Possible values are: Realtime, Scheduled, and Manual.	msg=Realtime
dvc	dvc_ip4	String	The IPv4 address for cn1.	dvc=10.1.144.199
dvchost	dvc_host	String	The hostname or IPv6 address for cn1.	dvchost=www.example.com
TrendMicroDsTags	event_tags	String	Deep Security	TrendMicroDsTags=suspicious

			event tags assigned to the event	
TrendMicroDsTenant	tenant	String	Deep Security tenant	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	tenant_id	Long	Deep Security tenant ID	TrendMicroDsTenantId=0
sev	severity_level	String	The severity of the event. 1 is the least severe; 10 is the most severe.	sev=6
cat	event_category	String	Category	cat=Web Reputation
name	event_name	String	Event name	name=WebReputation
desc	event_description	String	Event description. Web Reputation uses the event name as the description.	desc=WebReputation

CIM Mapping Fields:

Name	**data_type**	**Description**	**Example**
data_source	String	Data source name	data_source: trendmicro_deepsecurity_logs
data_source_category	String	category of the data source	data_source_category: endpoint_security_logs If Firewall, IPS the
host_id	Long	The agent computer's internal unique identifier.	cn1=1
file_size	Long	The size of the quarantine file. This extension is included only when the "direct forward" from agent /appliance is selected.	cn2=100
file_path	String	The path of the spyware item. This field is only for spyware detection events.	cs3=C:\test\atse_samples\SPYW_Test_Virus.exe
resource_type	String	For example, if there's a spyware file named spy.exe	cs4=10

		that creates a registry run key to keep its persistence after system reboot, there will be two items in the spyware report: the item for spy.exe has cs4=10 (Files and Directories), and the item for the run key registry has cs4=11 (System Registry).	
risk_level	String	Risk level values:	cs5=25
container_name	String	The image name of the Docker container, container name, and container ID where the malware was detected.	cs6=ContainerImageName | ContainerName | ContainerID
action	String	The action performed by the Anti-Malware engine. Possible values are: Deny Access, Quarantine, Delete, Pass, Clean, Terminate, and Unspecified.	act=Clean
dvc_ip4	IP	The IPv4 address for cn1.	dvc=10.1.144.199
dvc_host	String	The hostname or IPv6 address for cn1.	dvchost=www.example.com
rule_id	Long	The behavior monitoring rule ID for internal malware case tracking.	BehaviorRuleID=CS913
detection_type	String	The type of behavior monitoring event detected.	BehaviorType=Threat-Detection
event_tags	String	Deep Security event tags assigned to the	TrendMicroDsTags=suspicious

		event	
tenant	String	Deep Security tenant	TrendMicroDsTenant=Primary
tenant_id	Long	Deep Security tenant ID	TrendMicroDsTenantId=0
target_obj	String	The file, process, or registry key (if any) that the malware was trying to affect. If the malware was trying to affect more than one, this field will contain the value "Multiple."	TrendMicroDsMalwareTarget=C:\\Windows\\System32\\cmd.exe
target_count	String	The number of target files.	TrendMicroDsMalwareTargetCount=3
target_type	String	The type of system resource that this malware was trying to affect, such as the file system, a process, or Windows registry.	TrendMicroDsMalwareTargetType=File System
proc_name	String	Process Name	TrendMicroDsProcess= abc.exe
file_hash	String	The MD5 hash of the file	TrendMicroDsFileMD5=1947A1BC0982C5871FA3768CD025453E
confidence	INT	Indicates how closely (in %) the file matched the malware model	TrendMicroDsDetectionConfidence=95
threat_type	String	Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats(separate by semicolon";")	TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ran
severity_level	String	The severity of the event. 1 is the least severe; 10 is the most	sev=6

		severe.	
event_description	String	Event description. Anti-Malware uses the event name as the description.	event_description=installation of feature 'im' started
user_id	INT	The account ID number of the user name.	suid=0
user_name	String	The name of the user account that installed the software on the protected computer, or the source user which made connection.	suser=root
aggregation_type	INT	An integer that indicates how the event is aggregated: 0: The event is not aggregated, 1: The event is aggregated based on file name, path, and event type., 2: The event is aggregated based on event type.	aggregationType=2
event_count	INT	The number of occurrences of the event. Non-aggregated events have a value of 1. Aggregated events have a value of 2 or more.	repeatCount=4
tcp_flags	String		cs2=0x10 ACK
fragmentation_bits	String		cs3=DF MF
icmp_type	String	(For the ICMP protocol only) The ICMP type and code, delimited by a space.	cs4=11 0
dst_mac	String	MAC address of the destination computer's network interface.	dmac= 00:0C:29:2F:09:B3

dst_ip4	String	IP address of the destination computer.	dst=192.168.1.102
dst_port	Int	Destination port int the connection	dst_port=80
bytes_in	INT	(For inbound connections only) Number of inbound bytes read.	in=137
bytes_out	INT	(For outbound connections only) Number of outbound bytes read.	out=216
protocol	String	Name of the transport protocol used.	proto=tcp
src_mac	String	MAC address of the source computer's network interface.	smac= 00:0E:04:2C:02:B3
src_port	INT	(For TCP and UDP protocol only) Port number of the source computer's connection or session.	spt=1032
src_ip4	String	The packet's source IP address at this event.	src=192.168.1.105
frame_type	String	Connection ethernet frame type.	TrendMicroDsFrameType=IP
packet_data	String	The packet data, represented in Base64.	TrendMicroDsPacketData=AFB...
prior_file_path	String	(For "renamed" action only) The previous integrity rule target entity to capture the rename action from the previous target entity to the new, which is recorded in the filePath field.	oldFilePath=C:\WINDOWS\system32\logfiles\ds_agent.log
packet_location	Long	Position within	cn3=37

		packet of data that triggered the event.	
event_count	INT	The number of times this event was sequentially repeated.	cnt=8
http_x_forward_header	String	The IP address of the last hub in the X-Forwarded-For header.	xff=192.168.137.1
sub_rule_name	String	The Log Inspection sub-rule which triggered this event.	cs1=Multiple Windows audit failure events
dst_user	String	(If parse-able username exists) The name of the target user initiated the log entry.	duser=(no user)
url	String	The URL of the request.	url=http://www.example.com/index.php
scan_type	String	The type of action. Possible values are: Realtime, Scheduled, and Manual.	msg=Realtime
event_type	String	Type of the event, like firewall , IPS, anti-malware event	event_type=anti-malware
rule_name	String	Name of the rule which triggered the event. It could be the IPS/ Firewall/LI/IM rule name	rule_name= Microsoft Windows Events

Trend Micro Email Security (Push)

Trend Micro™ Email Security™ is an enterprise-class solution that delivers continuously updated protection to stop phishing, ransomware, Business Email Compromise (BEC) scams, spam and other advanced email threats before they reach your network. It provides advanced protection for Microsoft™ Exchange Server, Microsoft Office 365, Google™ Gmail, and other cloud or on-premises email solutions.

Using Trend Micro Email Security, mail administrators set up policies to handle email messages based on the threats detected. For example, administrators can remove detected malware from incoming messages before they reach the corporate network or quarantine detected spam and

other inappropriate messages.

Furthermore, Trend Micro Email Security delivers Email Continuity against planned or unplanned downtime events, which allows end users to continue sending and receiving email messages in the event of an outage.

To add Trend Micro Email Security to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Trend Micro Email Security provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Target Data Logs

Forescout currently targets the following log types]:

- Detection
- Audit
- Tracking

TippingPoint IPS (Push)

The Trend Micro™ TippingPoint IPS™ is an aspect of the Trend Micro Tipping Point Threat Protection System™ (TPS), which is a powerful network security platform that offers comprehensive threat protection against known and undisclosed vulnerabilities with high accuracy. TPS provides industryleading coverage across different threat vectors from advanced threats like malware and phishing with extreme flexibility and high performance. The TPS uses a combination of technologies, including deep packet inspection, threat reputation, URL reputation, and advanced malware analysis on a flow-by-flow basis—to detect and prevent attacks on the network. The TPS enables enterprises to take a proactive approach to security, providing comprehensive contextual awareness and deeper analysis of network traffic.

To add TippingPoint IPS to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

TippingPoint IPS provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

The following SNMP trap data is relevant for Forescout eyeAlert ingestion:

- Intrinsic Network HA trap
- Transparent Network HA
- Zero-Power HA
- Device-Wide Congestion Thresholds
- TippingPoint: Tier 3 Congestion Thresholds
- TippingPoint: System Resources Notifications

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Trend Micro IWSVA (Push)

The Trend Micro™ InterScan Web Security Virtual Appliance™ (IWSVA) is a highly scalable and reliable web security solution that includes virus protection for HTTP and FTP traffic. IWSVA delivers best-in-class HTTP and FTP virus scanning features that leverage the administration, policy, and centralized management of Trend Micro's Enterprise Protection Strategy.

To add Trend Micro IWSVA to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Trend Micro IWSVA provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

Forescout currently targets the following logs for ingestion:

- Event Perf. (Performance events)
- Event SysEvent
- Auditing Logs

- URL Access Logs
- Virus Logs
- Spyware Logs
- C&C callback Logs
- URL blocking Logs
- Performance Logs
- System event Logs
- Audit Logs
- FTP get Logs
- FTP put Logs

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Trend Micro™ Vulnerability Protection (Push)

Trend Micro™ Vulnerability Protection provides reinforces endpoint protection by supplementing desktop anti-malware and threat security with proactive virtual patching. A high-performance engine monitors traffic for new specific vulnerabilities using host-based intrusion prevention system (IPS) filters as well as zero-day attack monitoring.

To add Trend Micro Vulnerability Protection to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Trend Micro Vulnerability Protection provides a user documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Target Data Logs

The following logs are relevant for Forescout eyeAlert ingestion:

- Firewall Events
- Intrusion Prevention

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Trend Micro Worry Free (Pull)

Trend Micro™ Worry Free™ is designed for busy, overburdened IT staff wearing multiple hats. It is a cloud-based protection with automatic updates. It has optimized user interface for ease of use. It also provides a centralized console for endpoint, mobile, and extended detection and response (XDR). To add Trend Micro Worry Free to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Trend Micro Worry Free Data Source in the Forescout eyeAlert UI.

Target Data Logs

The following logs are relevant for Forescout eyeAlert ingestion:

- Web Reputation
- Spyware/Grayware
- Behavior Monitoring
- Virus
- Data Loss Prevention

Trend Micro Worry Free Customer Side Configuration Prerequisites

Forescout eyeAlert ingests logs from this Data Source using the pull mechanism, which uses the Log Forwarder API in WFBS-SVC. The following procedure is derived from the vendor documentation located here, and will configure the Trend Micro Worry Free Data Source for Forescout eyeAlert log ingestion:

1. Send a request for access to the Log Forwarder API to the Trend Micro WFBS-SVC Technical Support team. Send the request along with your WFBS-SVC Activation Code/s by contacting Trend Micro Technical Support.
2. WFBS-SVC Technical Support team will send the Cloud Services Platform Integration (CSPI) key pair, which is required to setup Log Forwarder. The key pair is (ACCESS_TOKEN, SECRET_KEY).
3. Once this key pair is obtained the log forwarder API can be activated.

The following information is required for the procedure to configure Forescout eyeAlert to ingest logs from this Data Source:

- Access Token
- Secret Key

When the required configurations have been implemented, proceed to Selecting the Trend Micro Worry Free Data Source.

Selecting the Trend Micro Worry Free Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.

3. Click the **+ Data Source**button.
4.
5. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
6. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
7. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert to Receive Trend Micro Worry Free Logs

Data Source Name – Trend Micro Worry Free

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations (right-panel)

1. Enter the **ACCESS TOKEN**.
2. Enter the **SECRET KEY**.
3. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 600.
4. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
5. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
6. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
7. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Trend Micro Worry Free Reference Information and CIM Field Mapping

The following external references relate to this Data Source:

- Worry-Free Suites: Multi-Device, Endpoint, Email Protection + XDR | Trend Micro

- Installation guide for Worry-Free Business Security 9.0
- Install and upgrade videos - Worry-Free Business Security
- Enable Log Forwarder API - Worry-Free Business Security Services

Trend Micro XDR (Pull)

Trend Micro™ XDR™is cross-layered detection and response. XDR collects and automatically correlates data across multiple security layers – email, endpoint, server, cloud workloads, and network – so threats can be detected faster and security analysts can improve investigation and response times. To add Trend Mirco XDR to Forescout eyeAlert as a Data Source, complete the following tasks:

1. Review the Customer-Side Configuration Prerequisites.
2. Select the Data Source in the Forescout eyeAlert UI.
3. Configure the Trend Micro XDR Data Source in the Forescout eyeAlert UI

Target Data Logs

Trend Micro XDR supports the pull mechanism. The XDR admin should assign some detection models. These models are used to control the types of alerts that Trend Micro XDR triggers. Forescout eyeAlert supports ingestion of all types of alerts.

Trend Micro XDR Customer Side Configuration Prerequisites

The key piece of information required to configure Forescout eyeAlert to receive Trend Micro XDR data logs is the authentication token. To configure Trend Micro XDR for Forescout eyeAlert data log retrieval complete the following steps:

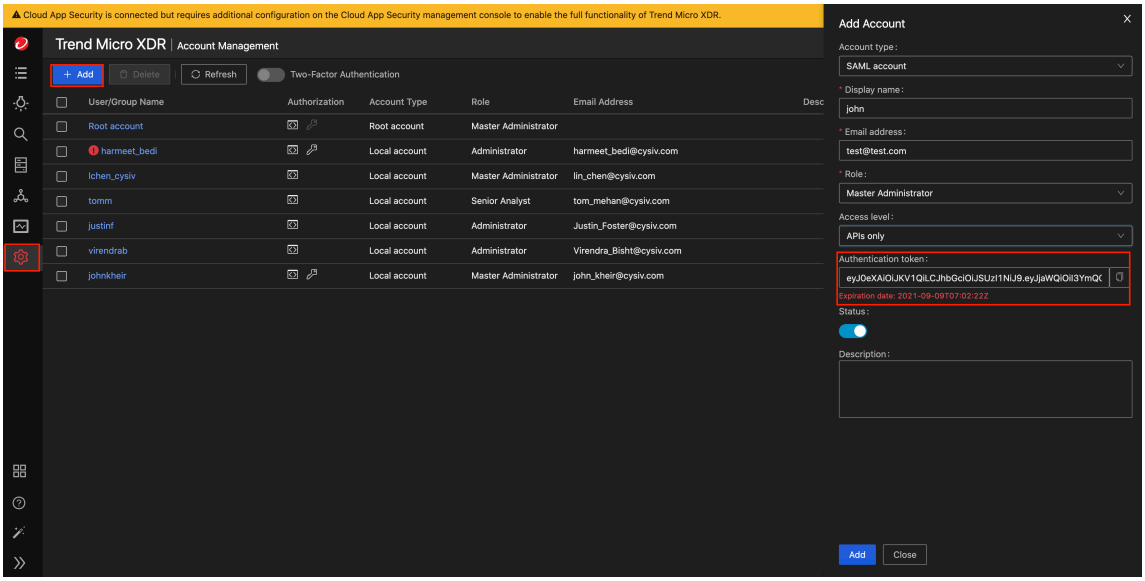
The Trend Micro XDR co

nsole automatically generates an authentication token for each account with API access.

1. On the Trend Micro XDR console, go to **Administration** > **Account Management**.
2. Click **+ Add**.
3. Add your information, then copy the authentication token and securely store it.

   The authentication token displays only when the Access level is either Trend Micro XDR console and APIs or APIs only.

   By default, an authentication token expires one year after creation. However, a Master Administrator can delete and re-generate a token at any time.



Selecting the Trend Micro XDR Data Source

1. Log in to Forescout eyeAlert and click the**Administration**tab.
2. On the Administration screen, click the **Data Sources**tab.
3. Click the **+ Data Source**button.
4. Click the**DATA SOURCE**dropdown and select the Data Source Name you are adding from the list (Forescout supports multiple Data Source types from the same vendor – be sure to select the correct name from the list).
5. Click the **CONNECTOR**dropdown and select the Connector you are using for the Data Source. When deploying a Connector in a hosted environment, the Connector you select will typically be named "Forescout hosted".
6. If applicable, enter the source identifier name into the **SOURCE NAME**field. This optional field is used to specify the unique name of the custom puller application in cases where a single Connector is used to "pull" the log data of a specific Data Source type from multiple environments – for example, a sandbox environment vs. staging or production.

For the pull-based Data Source you are adding, the configuration parameters you should enter on the right side of the window are typically specific to the vendor and device type. These settings are required to allow the TDR Connector with installed custom puller application to retrieve the target data logs securely.

Proceed to the next section to configure and apply your new Data Source.

Configuring Forescout eyeAlert To Receive Trend Micro XDR Data Logs

Data Source Name – Trend Micro XDR

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration > Data Sources > +Data Source > Add Data Source to Connector – Configurations* (right-panel)

1. Enter the Trend Micro XDR **AUTHENTICATION TOKEN**.
2. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is 300.
3. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as 2592000.
4. The **PULLER EXECUTOR TYPE** field displays the operating mode of the Data Source, which in this case is Pulling for periodic retrieval of target data logs.
5. Click the **Apply** button.

The UI will indicate whether the deployment has been successful.

Vedere Labs

This Data Source is related to Vedere Labs Threat Intelligence and for Forescout internal use only.

VMware

This series of topics covers all products offered by VMware™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

VMWare vCenter (Push)

VMWare vSphere (Push)

Aruba SD-WAN (Push)

VMWare vSphere (Push)

VMWare vCenter (Push)

VMware™ vCenter™ is software that allows you to control multiple Virtual Machines from one centralized place with SSO in details.

To add VMware vCenter to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Vmware provides a user documentation portal here.

Target Data Logs

Forescout currently processes load balancer logs.

- procstate: Supported process state logs (look)
- eam: Supported Health reports for the ESX agent monitor extension and connectivity logs to vCenter Server.
- lookupsvc-localhost_access : Supported VMware Lookup Service.

- vpxd: Supported The main vCenter Server logs. Includes all vSphere Client and web services, connections, and events.(look)
- vpxd-main: Supported
- analytics : Supported VMware Analytics Service.
- analytics-runtime: Supported
- envoy-access: Supported VMware Envoy Proxy
- vapi-endpoint: Supported VMware vAPI Endpoint provides a single point of access to vAPI services.
- vlcm: Supported VMware vCenter Lifecycle API
- vsan-health-main: Supported VMware VSAN Health Service
- wcpsvc: Supported Workload Control Plane
- vmcad: Supported VMware Certificate Service
- vcha-main: Supported VMware vCenter High Availability (replication of files)
- observability-main: Supported VMware VCSA Observability Service
- sca: Supported Manages service configurations
- sca-vmon.std: Supported
- sps: Supported Profile-Driven Storage Service (checked for connection errors)
- vstats: VMware vStats Service
- vdtc: VMware vSphere Distrubuted Tracing Collector
- perfcharts-localhost_access: Supported Performance Charts
- certificatemanagement-svcs: Supported VMware Certificate Management Service
- cis-license: Supported VMware Licensing Service
- content-library: Supported VMware Content Library Service
- vmon:Supportedmanages the lifecycle of Platform Services Controller and vCenter Server. Exposes APIs and CLIs to third-party applications (look)
- applmgmt:SupportedHandles appliance configuration
- vmafdd: Supported VMware Authentication Framework daemon (look) provides a client-side framework for vmdir authentication and serves

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

VMWare vSphere (Push)

To add VMware vSphere™ to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Vmware provides a user documentation portal here.

Target Data Logs

Forescout currently processes the following log types:

- hostd
- vpxa
- vmkernel
- vmkwarning
- kmxa
- esxtokend
- vsansystem
- VSANMGMTSVC
- Rhttpproxy
- Fdm

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

VMWare SD-WAN (Push)

VMware SD-WAN™ is a cloud network service solution enabling sites to quickly deploy Enterprise grade access to legacy and cloud applications over both private networks and Internet broadband.

To add WMWare SD-WAN to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Vmware provides a user documentation portal here.

Target Data Logs

Forescout currently processes event logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

VMWare vSphere ESXi (Push)

VMWare vSphere ESXi™ is a Type-1 hypervisor that runs on host computers to manage the execution of virtual machines, allocating resources to the virtual machines as needed.

To add VMWare vSphere ESXi to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Vmware provides a user documentation portal here.

Target Data Logs

Forescout currently processes the following log types for ingestion:

- hostd
- vpxa
- vmkernel
- vmkwarning
- kmxa
- esxtokend
- vsansystem
- VSANMGMTSVC
- Rhttpproxy
- Fdm

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

WatchGuard

This series of topics covers all products offered by WatchGuard™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

WatchGuard Firewall (Push)

WatchGuard™ Firewall™ offers traditional intrusion prevention, gateway antivirus, application control, spam prevention, and URL filtering, and more advanced services for protecting against

evolving malware, ransomware, and data breaches. Each security service is delivered as an integrated solution within a Firebox appliance.

To add WatchGuard Firewall to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

WatchGuard provides a technical documentation portal here.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Wazuh

This series of topics covers all products offered by Wazuh™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Wazuh Security Platform (Push)

Wazuh is a free and open source platform used for threat prevention, detection, and response. It is capable of protecting workloads across on-premises, virtualized, containerized, and cloud-based environments. Wazuh solution consists of an endpoint security agent, deployed to the monitored systems, and a management server, which collects and analyzes data gathered by the agents.

To add Wazuh to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Wazuh provides a user documentation portal here.

Target Data Logs

Forescout currently targets OSSET logs - OSSEC is an open-source, host-based intrusion detection system (HIDS) that performs log analysis, integrity checking, Windows registry monitoring, rootkit

detection, time-based alerting, and active response. It's the application to install on your server if you want to keep an eye on what's happening inside it.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the Syslog format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Wiz

This series of topics covers all products offered by Wiz™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Wiz.io (Pull)

This manual is under construction.

Workday

Workday™ Security™ is an enterprise management platform, which offers services related to payroll, human resources, and applicant tracking.

To add Workday™ Security™ to Forescout eyeAlert as a Data Source, use the following settings when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Pull mechanism to ingest logs from this Data Source.

Key Data Source Product Configuration and Authentication Requirements

To onboard logs from this Data Source, you will need to have the following credential information on-hand when configuring Forescout eyeAlert:

- Tenant Hostname
- Tenant Name
- Token URL
- Client ID
- Client Secret
- Refresh Token

Suggested Information Sources for Data Source Product Configuration

Workday provides documentation on enabling activity logging with the REST API here.

Note:
The reference links above are suggestions only. To ensure accuracy, be sure to use the latest official documentation provided by the vendor of your Data Source product type and version.

Target Data Logs

Forescout currently targets cloud activity logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON format when configuring your Data Source to make logs available for ingestion by Forescout eyeAlert.

Configure Forescout eyeAlert to Retrieve the Data Source Logs

See Configuring Forescout eyeAlert to Receive Workday Security Logs.

Configuring Forescout eyeAlert to Receive Workday Security Logs

Data Source Name – Workday Security

Log Retrieval Method – Pull

Connector Deployment Environment – On-premise or hosted

UI Location – *Administration* > *Data Sources* > + *Add Data Source* > *Add Data Source to Connector* – *Configurations* (right-panel)

1. Enter the Tenant Hostname.
2. Enter the Tenant Name.
3. Enter the Token URL.
4. Enter the Client ID.
5. Enter the Client Secret.
6. Enter the data source pulling interval schedule into the **SCHEDULE INTERVAL** field in seconds – the default value is *300* (5 minutes).
7. Enter a value in seconds into the No Flow Alert Threshold field. The value determines how long the system will wait before alerting on absence of logs.
8. The **MAX PULLING AGE** field is where you can specify how far back in time records can be pulled, with the default being 30 days expressed in seconds as *2592000*.
9. In the **NOTES** field, enter any comments about the deployment you want preserved for later reference.
10. Click the **Add Data Source** button.

The UI will indicate whether the deployment has been successful.

Zscaler

This series of topics covers all products offered by Zscaler™ that can be used as a Data Source for Forescout eyeAlert log ingestion.

Zscaler Cloud (Push)

Zscaler™ Cloud™ offers a private network connection to its clients for security operations.

To add Zscaler™ Cloud™ to Forescout eyeAlert as a Data Source, ensure the following settings are used:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Zscaler provides a user documentation portal here.

Target Data Logs

Forescout currently processes cloud activity logs for ingestion.

Log Format Necessary for Forescout eyeAlert Retrieval

Use the CEF format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic.

Zscaler ZPA (Push)

Zscaler™ ZPA™ Public Service Edge (formerly ZPA ZEN or ZPA Broker). The ZIA Public Service Edge inspects all internet/cloud traffic for malware and enforces security, compliance, and firewall policies.

To add Zscaler ZPA to Forescout eyeAlert as a Data Source, ensure the following settings are used when configuring your product:

Log Retrieval Method

Forescout eyeAlert uses the Push mechanism to ingest logs from this Data Source.

Instructions and/or Suggested Information Sources

Zscaler provides a user documentation portal here.

Target Data Logs

Forescout currently targets the following log types for ingestion:

- User Activity
- User Status

- App Connector Status
- Browser Access

Log Format Necessary for Forescout eyeAlert Retrieval

Use the JSON format when configuring your Data Source to send logs to Forescout eyeAlert.

Configure Forescout eyeAlert to Receive the Data Source Logs

See "Configure Your Data Source - On-Premises Connector (TCP or UDP) or Hosted Connector (TLS or mTLS)?" in the Push-based Data Source Onboarding topic to see the protocol and port you should configure your Data Source to use when sending logs to Forescout eyeAlert, and for information about configuring Forescout eyeAlert to receive the logs.

Miscellaneous Data Sources

This section of the index covers non-standard Data Sources used for specialized use cases, and documents the following:

- Custom Logs
- Diagnostic Tools and Utilities
- Forescout Sensor Beta
- Forescout Preparsed Logs
- Forescout Raw Logs
- Generic Syslog
- Generic Syslog for Custom DB
- Loggify Format Logs
- Microsoft DNS Debug
- Sanitized EDA Logs
- Sanitized Logs
- Strongswan

Custom Logs

This Data Source is a push-based Data Source for customer logs produced by Forescout and Forescout Customers.

Diagnostic Tools and Utilities

The following Data Sources are used to diagnose and troubleshoot Data Source log ingestion and to provide an alternate data point for investigating and confirming incidents:

- Backend Services
- Forescout Diagnostic
- Metricbeat
- Unknown Raw Logs
- Connector Metrics

- Unknown Raw Logs

Backend Services

This Data Source is used by Forescout for internal maintenance.

Forescout Diagnostic

This Data Source is used by Forescout for internal diagnostics.

Metricbeat

This Data Source requires the participation of a Forescout Cloud deployment representative.

Unknown Raw Logs

This Data Source is used to process unknown raw logs and is typically used for troubleshooting by Forescout.

Connector Metrics

This manual is under construction.

Forescout Sensor Beta

This is a guide to the installation and configuring of Microsoft Windows Sysmon and the Forescout Sensor. This section provides an overview of the Forescout Sensor and its architecture, and Microsoft™ Windows™ Sysmon™.

NOTE: During beta, it is strongly recommended that deployment of the Forescout Sensor be done with the assistance of your Forescout technical representative.

To deploy the Forescout Sensor, complete the following task list:

1. Read the overview information below.
2. Review the Network Firewall Requirements for the Forescout Sensor.
3. Optional - follow the instructions for How to Install and Configure Sysmon to work with the Forescout Sensor and Forescout eyeAlert.
4. Sensor installation option 1 (**requires Forescout participation**) - How to Install and Configure the Forescout Sensor.
5. Sensor installation option 2 (**requires Forescout participation**) - Creating an Intune Deployment Package.

Forescout Sensor Overview

The Forescout Sensor is a Windows system service that monitors system activity, gathering events of interest and forwarding them to a Forescout Collector. The Sensor includes the following capabilities:

- Collection and forwarding of system activity related to:
    - DNS queries and responses

    - File activity
    - NTFS alternate data stream activity
    - Network activity, correlated with DNS responses
    - Process activity
    - Session activity (logon/logoff, RDP connect/disconnect, lock/unlock
    - URL access
- Windows event log forwarding comparable to Winlogbeat. Unlike Winlogbeat, Analytic and Debug channels can be monitored and forwarded by way of a direct ETW subscription.
- Event enrichment using:
    - The geo-location of the machine (via Windows system APIs) at the time of the event
    - The geo-location of remote network connections (by looking up the remote IP in a local database)
    - File hashes, PE details for process and DLL binaries, and Authenticode signature details
    - Volume and file system details for file events, including the vendor, serial number, and type (removable, fixed, network) of the volume
- Event filtering to avoid sending unwanted data to the TDR Connector
- Control of Windows audit and group policy settings, similar what can be done via group policy or the AuditPol.exe utility
- Remote management of the Sensor's configuration
- Optional automatic updates to the Sensor software
- Optional installation of Sysmon and control of the Sysmon configuration

Sysmon Overview

System Monitor (Sysmon) is a Windows system service and device driver from the Sysinternals team at Microsoft. It can be used to supplement the event collection capabilities of the Sensor, and its configuration can be remotely administered via the Sensor.

If Sysmon is installed, it can provide insight into certain kinds of system activity not monitored by the Sensor, including:

- Loading of drivers with their signatures and hashes
- Opens for raw read access of disks and volumes
- Changes in file creation time to understand when a file was really created. Modification of file create timestamps is a technique commonly used by malware to cover its tracks.
- Registry modification activity
- Events from early in the boot process to capture activity made by even sophisticated kernel-mode malware.

Forescout Sensor Architecture

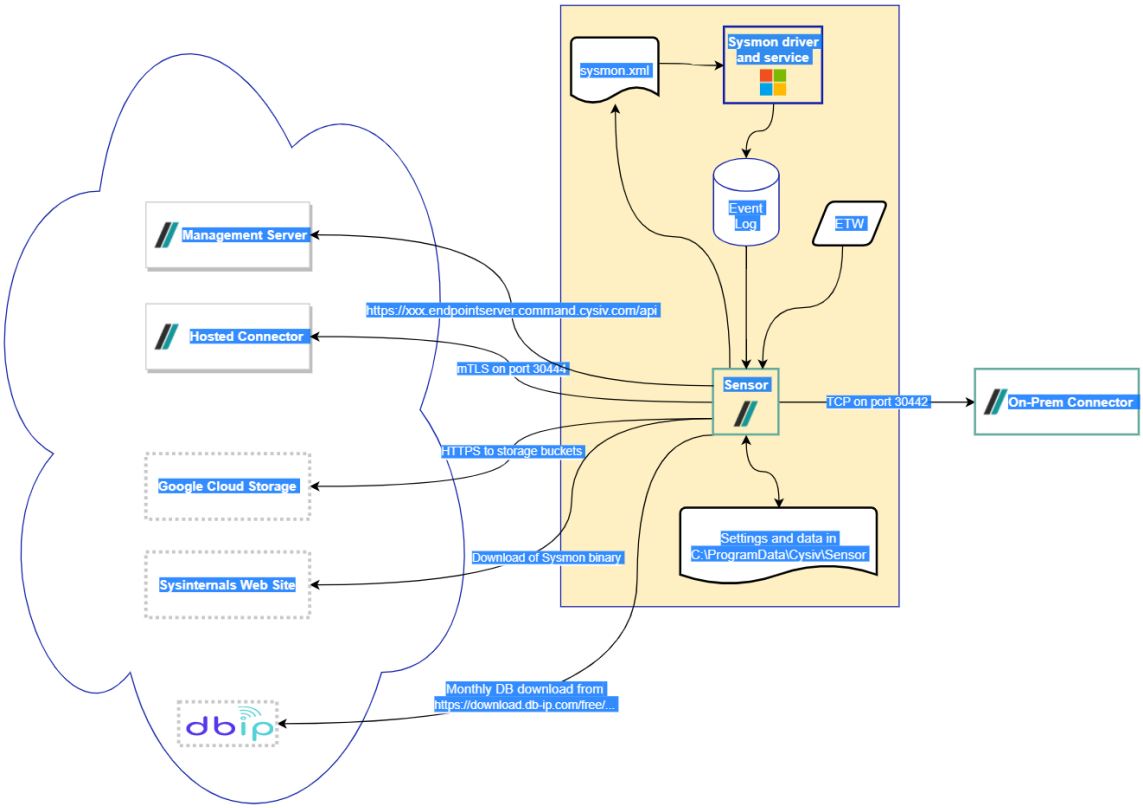
The Forescout Sensor and Sysmon both run as system services on any Windows machine running Windows 10 version 1703 or newer or Windows Server 2012 or newer. Sysmon also installs a device driver. Both applications run automatically at system startup and monitor activity. Sysmon writes its events to the local Windows Event Log, the Sensor queues its events internally and sends them in batches to the TDR Connector. If the system is offline or the Connector is unreachable, the Sensor will store events on disk and send them when connectivity to the Connector is restored.

The Sensor communicates with a management server to get its configuration information and to send some basic system-level metadata to the server. By default, it communicates with the server

once every 15 minutes, although this interval can be altered via a config setting.

It will also communicate with the TDR Connector, either a hosted instance running in the cloud or an on-prem instance. Configuration settings received from the server tell the Sensor how to reach the Connector. If the configuration specifies both on-prem and hosted Connectors, the Sensor will attempt to send its event data to the on-prem Connector and switch to the hosted Connector only if the on-prem Connector is unavailable. If the system's network settings change (ex. connecting to a different WiFi network, getting a different IP address, rebooting), the Sensor will try the on-prem Connector again.

The following diagram provides a high-level view of the components and network connections used by the Forescout Sensor:



Forescout Sensor Network Firewall Requirements

The Sensor makes the following network connections and therefore requires the indicated ports to be open for TCP connections:

- WAN port 443 (HTTPS) between machines running the Sensor and the management server. The DNS name and IP of the management server will depend upon the region in which the customer's tenant resides.
- WAN port 443 (HTTPS) between machines running the Sensor and the DB-IP web site. The Sensor downloads a copy of the "IP to City Lite" database from this site and refreshes it once a month. This is used to enrich network events with the geo-location of remote public IPs.

- WAN port 443 (HTTPS) between machines running the Sensor and the download.sysinternals.com web site. This is only required if the Sensor is configured to automatically download and install Sysmon.
- WAN port 443 (HTTPS) between machines running the Sensor and the Google Cloud Storage web site storage.googleapis.com. The Sensor can be configured to check a storage bucket for updates to its software. It can also be configured to upload diagnostic information to a storage bucket. For customers that do not wish to ALLOW-LIST all of Google's public IPs, Forescout will be offering an option to proxy this traffic through a Forescout-controlled hostname and IP address.
- WAN port 30444 (for mTLS) between machines running the Sensor and the tenant-specific Forescout Hosted Connector.
- LAN port 30442 (for TCP) between machines running the Sensor and the on-prem XDR Connector host.

In addition to the above requirements, it may be necessary to configure firewalls and/or proxies to allow HTTP access to `www.ssl.com`, `crls.ssl.com`, and `ocsps.ssl.com`. This is only required if the Sensor is configured to update its software by periodically checking a Cloud Storage bucket for new versions. If this feature is enabled, the Sensor will validate the digital signature on the software update package, which may require making HTTP requests to check for certificate revocation. Revocation checking is enabled by default, but can be disabled by Forescout personnel using the Sensor's management server to set the `SelfUpdate:SkipUpdateSignatureRevocationCheck` configuration option to `true`.

If the Sensor software is being updated through other means (ex. Intune), then no exceptions are required for `ssl.com` subdomains.

How to Install and Configure the Forescout Sensor

NOTE: During beta, it is strongly recommended that deployment of the Forescout Sensor be done with the assistance of your Forescout technical representative.

Installing the Sensor involves running a single command, but it requires some customer-specific information:

- The URL of the Forescout endpoint management server.
- The customer's tenant ID with the Forescout endpoint management server (this value is typically the same as the customer's tenant ID with Forescout TDR).

Forescout personnel can obtain the full command-line required to install the Sensor by signing into the endpoint management server for the customer's tenant ID and navigating to the "Endpoints" page. The **Add Endpoint** button on that page will display the command line with the appropriate tenant ID and URL values filled in.

To run the installer interactively (it will display a user-interface and show progress etc.) the command line is:

CysivSensor-x.y.z.exe TENANTID=TID SERVERURL=https://mgmtsrv.host.name/api

For a silent install (no user-interface), the command line to use is:

CysivSensor-x.y.z.exe /install /quiet TENANTID=TID SERVERURL=https://mgmtsrv.host.name/api

where:

- ***x.y.z***: is the version of the Sensor to be installed
- ***TID***: is the customer's tenant ID. It is in the form of a GUID.
- ***mgmtsrv.host.name***: is the fully qualified hostname of the management server for the tenant. As with other Forescout services, there are multiple instances of the management server running in different regions of the world.

A full example might look something like the following:

CysivSensor-0.9.44.exe /install /quiet TENANTID=cd0b918d-fb08-46ef-8a0e-3783005d4e3f SERVERURL=https://uc1.endpointserver.command.Forescout.com/api

The silent install option should be used with endpoint deployment tools such as Microsoft Intune. An MSI version of the installer is available for tools that require it, but Forescout recommends using the EXE installer where possible.

The equivalent command-line for an MSI deployment is:

```
msiexec.exe /l* CysivSensorInstall.log /i CysivSensor-x.y.z.msi
                    TENANTID=TID SERVERURL=https://mgmtsrv.host.name/api
```

for an interactive install and:

```
msiexec.exe /l* CysivSensorInstall.log /i CysivSensor-x.y.z.msi /qn
                    TENANTID=TID SERVERURL=https://mgmtsrv.host.name/api
```

for a silent install.

NOTE: whether running the EXE installer interactively or in a deployment script, it's important to understand that the installer is a Windows graphical application, so "shell" applications like PowerShell and cmd.exe will NOT wait for the installer to finish before showing the next prompt or executing the next command in a script. To ensure that the shell waits for the installer to complete, use the following techniques:

PowerShell: add

```
|
                    Write-Host
```

to the end of the command to force PowerShell to wait for the installer to complete:

```
&
                    C:\full\path\to\CysivSensor-x.y.z.exe /install /quiet
TENANTID=TID
                    SERVERURL=https://mgmtsrv.host.name/api | Write-Host
```

cmd.exe: add

```
start /wait
```

at the beginning of the command to force cmd.exe to wait for the installer to complete:

```
start /wait
                    C:\full\path\to\CysivSensor-x.y.z.exe /install /quiet
TENANTID=TID
                    SERVERURL=https://mgmtsrv.host.name/api
```

Deployment tools such as Intune typically do not use a shell application to run the installer, so the highlighted options are not required.

Validating the Installation

The simplest way to check to see if installation of the Sensor on a machine named "LAPTOP-1" in the Windows domain or workgroup "CUSTOMER" is to check the management server's **Endpoints** page to see if "CUSTOMER\LAPTOP-1" appears in the list. The Sensor enrolls with the management server immediately after it is installed. Assuming there are no network connectivity issues, enrollment should happen right away.

If the machine does not appear in the management server's list of endpoints, check the following using an administrative PowerShell session:

- Ensure that the Sensor's Windows service is running. Run Get-Service CysivSensor and check that the status is "Running". If it is not running, contact Forescout Support for assistance.
- If the service is running, check the Sensor's logs to see what prevented it from enrolling with the management server.

  Run notepad.exe C:\ProgramData\Forescout\Sensor\logs\sensorYYYYMMDD.log where YYYYMMDD is the current date and check the file for network-related errors such as "connection refused", "no such host", or timeout errors. Those indicate that either the hostname given in the SERVERURL is incorrect or that a firewall is blocking the connection.

  If the SERVERURL or the TENANTID value was mistyped, run the following command to configure the Sensor with the correct value:

  & 'C:\Program Files (x86)\Forescout\Sensor\Reset-Sensor.ps1' -ServerURL https://mgmtsrv.host.name/api -TenantId TID

How to Install and Configure Sysmon

Forescout recommends that Sysmon be installed on all monitored endpoints in addition to the Sensor. Once Sysmon is installed, the Sensor and its remote management console can be used to set and update the Sysmon configuration.

Installing Sysmon via the Forescout Sensor

With Forescout Sensor v0.9.50 and later, Sysmon can be automatically installed or updated by the Sensor if its configuration setting Sysmon:InstallSysmon is true. By default, this setting is `false`, but it can be changed by Forescout personnel using the Sensor's management server. Customers for whom this is set to `true` must be made aware that Sysmon will be installed and that they are subject to the Sysinternals Software License Terms.

Installing Sysmon Manually

Forescout recommends that Sysmon be installed on all monitored endpoints in addition to the Sensor. Once Sysmon is installed, the Sensor and its remote management console can be used to set and update the Sysmon configuration. Installation of Sysmon involves the following steps:

1. Download the current version of Sysmon from https://download.sysinternals.com/files/Sysmon.zip
2. Extract the contents of the ZIP file. This will yield the following files:
    a. Eula.txt – the Sysmon license agreement
    b. Sysmon.exe – the 32-bit binary
    c. Sysmon64.exe – the 64-bit binary
3. Using an administrative account, run Sysmon.exe or Sysmon64.exe as appropriate for the edition of Windows installed on the host using the following command-line:
    a. Sysmon[64].exe -i -accepteula
4. Confirm that Sysmon is installed and running by executing the following command from an administrative account:
    a. Sysmon[64].exe -c

If Sysmon is installed, you'll see some details about the Sysmon configuration along with "No rules installed". If it is not installed, you'll see the message "Sysmon is not installed on this computer".

Removing Sysmon

To uninstall Sysmon, run the following command in console:

C:\Windows\Sysmon[64].exe -u

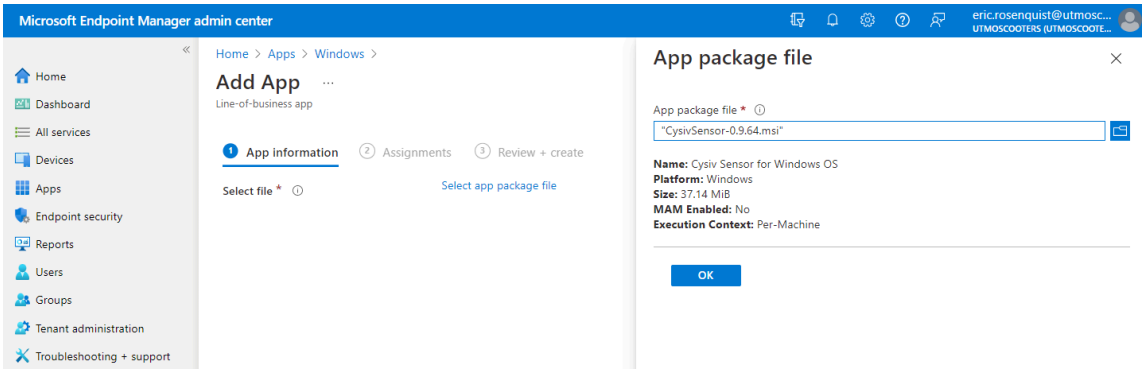
Creating an Intune Deployment Package

NOTE: During beta, it is strongly recommended that deployment of the Forescout Sensor be done with the assistance of your Forescout technical representative.

The MSI installer for the Sensor can be used to create an Intune "Line of business" deployment package in Microsoft's Endpoint Manager.

1. In the Microsoft Endpoint Manager web console, navigate to **App | All Apps** and then click on **Add** to create a new deployment package.
2. Select "Line-of-business app" as the app type and click the [Select] button.

3. Click on "Select app package file" and then click on the folder icon. Select the CysivSensor .msi file from your local system and click [OK].

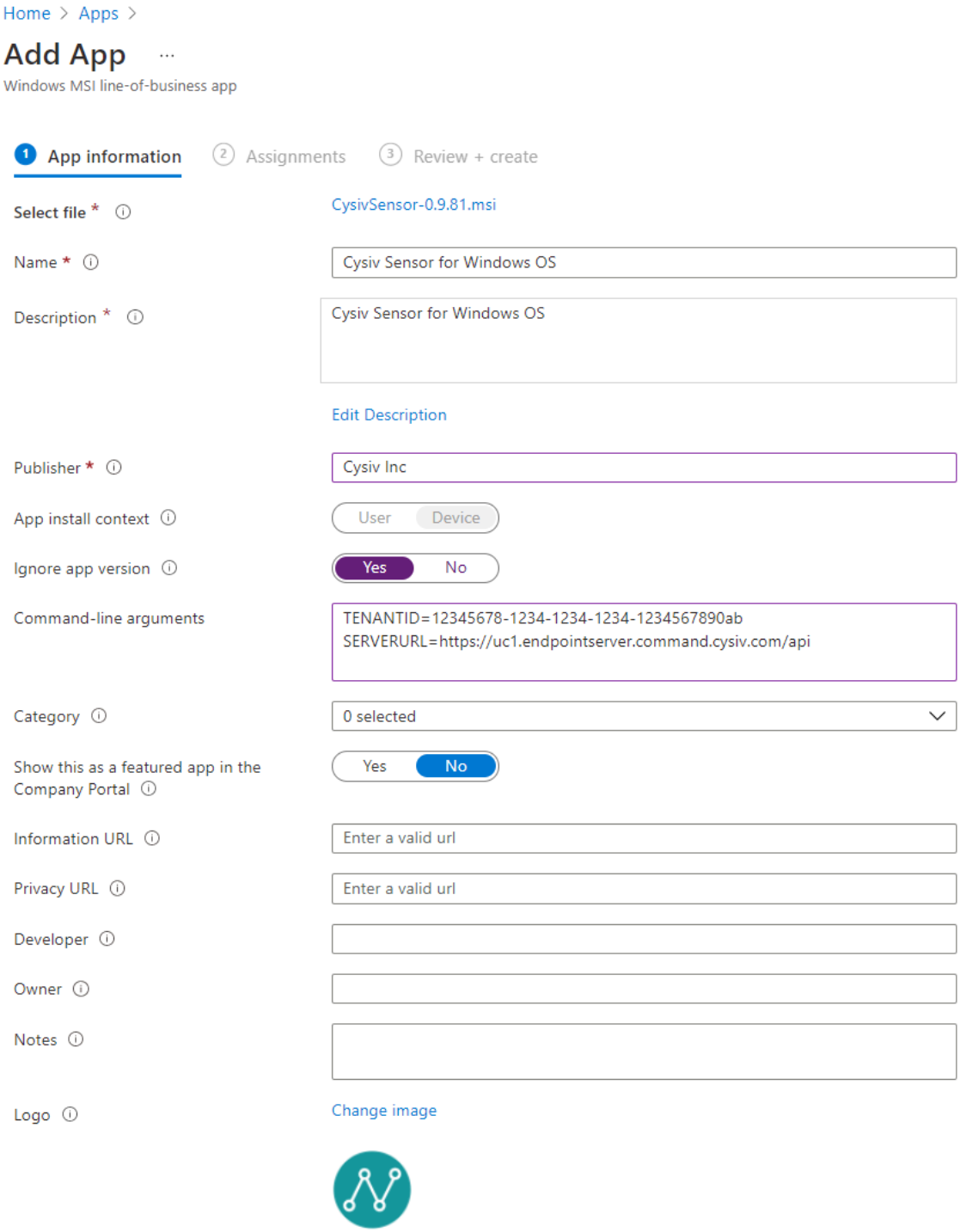


4. In the**App Information**screen, put "Forescout Inc" in the vendor name and optionally fill in the other fields. The version number should be filled in automatically from the`.msi`file - do not change it.
5. Set**Ignore app version**to**Yes**, otherwise Intune will report errors if the Sensor updates itself to a newer version.
6. For the **Forescout eyeAlert-line arguments**, add

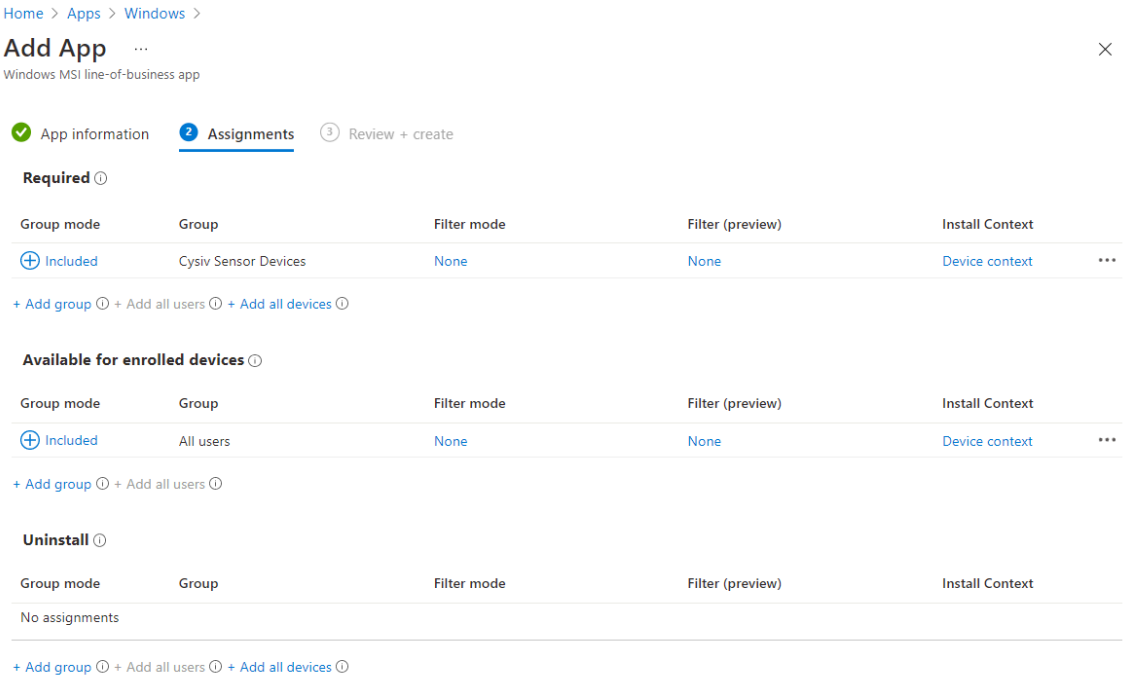
   ```
   TENANTID=TID
                        SERVERURL=https://mgmtsrv.host.name/api
   ```

   to the end of the Install command, where `TID`is a customer-specific tenant ID and the SERVERURL value is region-specific. These values are supplied by Forescout personnel.

7. Add the Forescout logo - a suitable Forescout logo file can be found here.



8. On the**Assignments**screen, determine which machines should have the Sensor installed and configure the settings accordingly. In the screen capture below, any machine that is a member of the security group named "Forescout Sensor Devices" will automatically have the package installed. If you want the app to be visible in the Company Portal, select "Add all users" in the "Available for enrolled devices" section.



9. Finally, review the information displayed on the **Review + create**screen and click [Create] if no changes are required. After a few minutes, the App should appear in the Endpoint Manager's list of Apps; deployment to machines matching the "Required" criteria will follow according to normal Intune scheduling.

How to Remove the Forescout Sensor

If a deployment tool such as Intune was used to install the Sensor, it should be used to remove it as well. If it was manually installed, it can be removed in one of several ways:

- By running the exact same CysivSensor-x.y.z.exe package used for the installation and selecting [Uninstall] in the user interface. Using an older or newer version of the package won't work; a newer version will upgrade the current version, and an older version will detect that a newer version is already installed and abort.
- By running the exact same CysivSensor-x.y.z.exe package used for the installation and using the /uninstall command-line option. For example: CysivSensor-x.y.z.exe /uninstall or CysivSensor-x.y.z.exe /uninstall /quiet

NOTE: if the Sensor is configured to update its software automatically, it's likely that the installer package originally used for the installation won't work since it will be older than the currently installed version. See below for alternative techniques.

- If the original EXE package used for the install is not available or if the Sensor has updated itself to a newer version, it can be removed in the following ways:
    - From the Windows "Apps & features" section of Windows Settings.
    - By running the following command from an administrative PowerShell 5 session (NOTE – this does *not* work from PowerShell Core, a.k.a. pwsh, a.k.a. PowerShell version 6 or higher):

```
Get-Package -Provider Programs
                                -IncludeWindowsInstaller -Name
'Forescout*Sensor*' -ErrorAction
                                Ignore | Uninstall-Package
```

- If an EXE installer was used, you can use the following command to locate and run the stub in the Package Cache folder:

```
& (Get-ChildItem
                                'C:\ProgramData\Package
Cache\*\CysivSensor*.exe').FullName
                                /uninstall /quiet
```

- If an MSI installer was used, you can use one of the following commands to find the correct GUID and then run msiexec to remove the Sensor:

  64-bit OS:

```
& msiexec.exe /X
                                ((Get-ItemProperty
                                HKLM:\SOFTWARE\WOW6432Node\
Microsoft\Windows\CurrentVersion\Uninstall\*
                                | Where-Object -Property
DisplayName -like

'Forescout*Sensor*').UninstallString.Replace("MsiExec.exe /I",
                                ""))
```

  32-bit OS:

```
& msiexec.exe /X
                                ((Get-ItemProperty
                                HKLM:\SOFTWARE\Microsoft\
Windows\CurrentVersion\Uninstall\* |
                                Where-Object -Property
DisplayName -like

'Forescout*Sensor*').UninstallString.Replace("MsiExec.exe /I",
                                ""))
```

Forescout Preparsed Logs

A Data Source used by Forescout for internal investigation, setup and configuration.

Forescout Raw Logs

A catch-all Data Source used by Forescout to process EDR logs for internal investigation, setup and configuration.

Generic Syslog

This manual is under construction.

Generic Syslog for Custom DB

This manual is under construction.

Loggify Format Logs

This Data Source is for Forescout internal use.

Microsoft DNS Debug

This Data Source is used by Forescout internally for troubleshooting investigations.

Sanitized EDA Logs

This Data Source is for Forescout internal use.

Sanitized Logs

This Data Source is for Forescout internal use.

Strongswan

This Data Source is for Forescout internal use only.