Forescout

Method 1: Network logs forwarding

The Network logs forwarding page ("Settings" > "System Settings" > "Network logs forwarding") allows users to enable and configure the forwarding of Network Logs to a third-party solution by means of syslog messages. The pages and configuration steps required to enable forwarding of Network Logs are exactly the same as those described for Alerts. The only difference lies in the semantics adopted when users un-tick the "always active" checkbox in the alert forwarding conditions, but leave the conditions "tree" empty. For Alerts, this results in all alerts being forwarded, whereas for Network Logs, this results in no log begin forwarded. The rationale is that Alerts are important events that are generally desirable to be forwarded to an analyst, whereas Network Logs are useful additional intelligence for context and threat hunting. This choice of default behavior is to prevent user mistakes in the configuration of eyeInspect to impact their monitoring capabilities. Pre-set messages for CEF, LEEF and JSON (Splunk) are available also for Network Logs forwarding.

Source: *https://docs.forescout.com/bundle/eyeinspect-user-guide-v5-5-0/page/gitdoc-eyeinspect/eyeInspect/eyeInspect_User_Guide/network-logs-forwarding.html*

Configure the plugin receiver port

Configure the Syslog plugin port for receiving syslog events for each Forescout Platform device configured as a syslog server (receiver of wireless events and/or switch events) in the management interface. Each device receives syslog events sent from managed, individual network devices.

To configure the port for receiving syslog events:

1. Select Tools > Options.
2. From the Options pane, select Syslog.
3. Select the Receive From tab and specify this information:
   Source Type
   IP Address
   Specify the syslog server IP address.
   UDP Port
   - Cisco Meraki: Specify the port number that you configured for the syslog server port in the Meraki Dashboard. Cisco Meraki only supports using UDP

protocol for sending syslog events.
- Ruckus SmartZone: Specify the port number that you configured the syslog server port and protocol in the Ruckus SmartZone Web GUI
- Arista CloudVision WiFi: Arista CloudVision WiFi only supports using port 514 for sending syslog events.

TCP Port
: Prisma Access: Specify port 514.

Use TLS
: Optional. Select this checkbox to instruct Forescout Platform to encrypt communication with the syslog sources. For required certificates when using "Receive From" syslog servers, refer to: Certificate Management in the Syslog Plugin Configuration Guide.

4. Select Apply > Yes.
5. Repeat steps 4–8 for each device configured as a syslog server in the management interface.

Verify the plugin is running

Verify that the Syslog plugin is running in all of the Forescout Platform devices that are configured in the management interface as syslog servers (In the Console, select Options > Modules and expand the Core Extensions module entry).

If the plugin is not running in all of these Forescout Platform devices, select Syslog > Start.

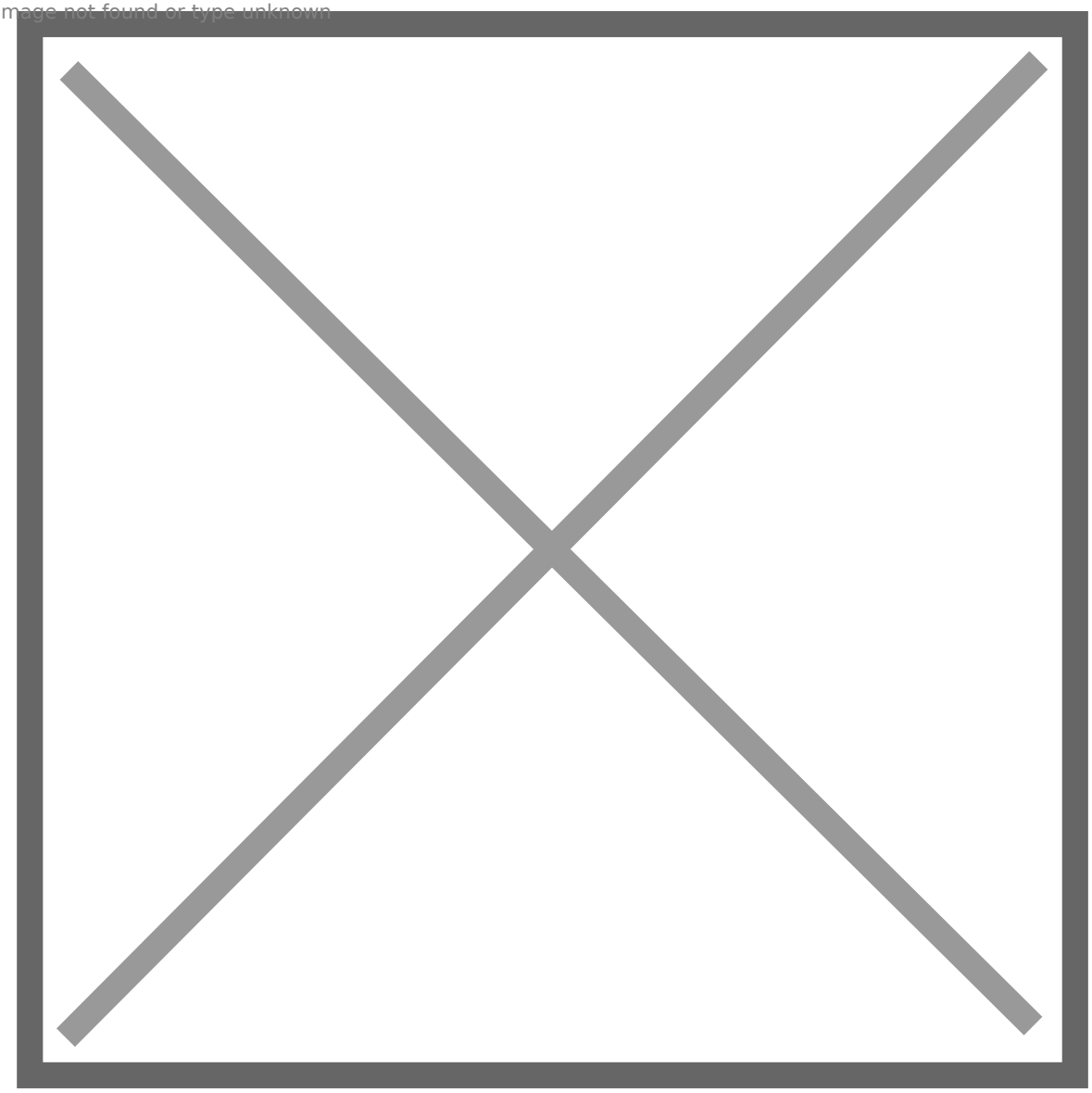
Source: *https://docs.forescout.com/bundle/network-cntrlr-1-2-8-h/page/c-syslog-plugin-configuration-p-d1e1407.html*

Method 2: Generate an API key for application integration

To generate an API key for your custom application to query ingested log telemetry and other sources of data, complete the following procedure:

1. In Forescout Cloud Console, select **Integrations** under the **Administration** menu.
2. Click the **Generate API Key** button next to the category of your application - **IoT/OT** or **SIEM**.
   The **Generate API Key** configuration screen appears.

Image not found or type unknown



3. Select a time for the API key to expire or select "Never Expires".
4. Select users to receive Email notifications about the API key generation and expiry date.
5. Click the **Generate** button and copy the API key that appears. This API key is unique and non-retrievable once the window is closed. Store the key in a secure location now; it will be needed by the application with which you are integrating.
   When generating an API key for Risk Sharing applications, the configuration screen will display the API endpoint URL needed to communicate with the API.

Source: *https://docs.forescout.com/bundle/forescout-cloud-administration-guide/page/gitdoc-cloud/Cloud/forescout-cloud-administration-guide/generate_an_api_key_for_application_integration.html*

Revision #2
Created 16 January 2025 09:27:22 by Richmond Abella
Updated 16 January 2025 09:54:17 by Richmond Abella