AQUILA - Varonis (DLP) Integration

Purpose

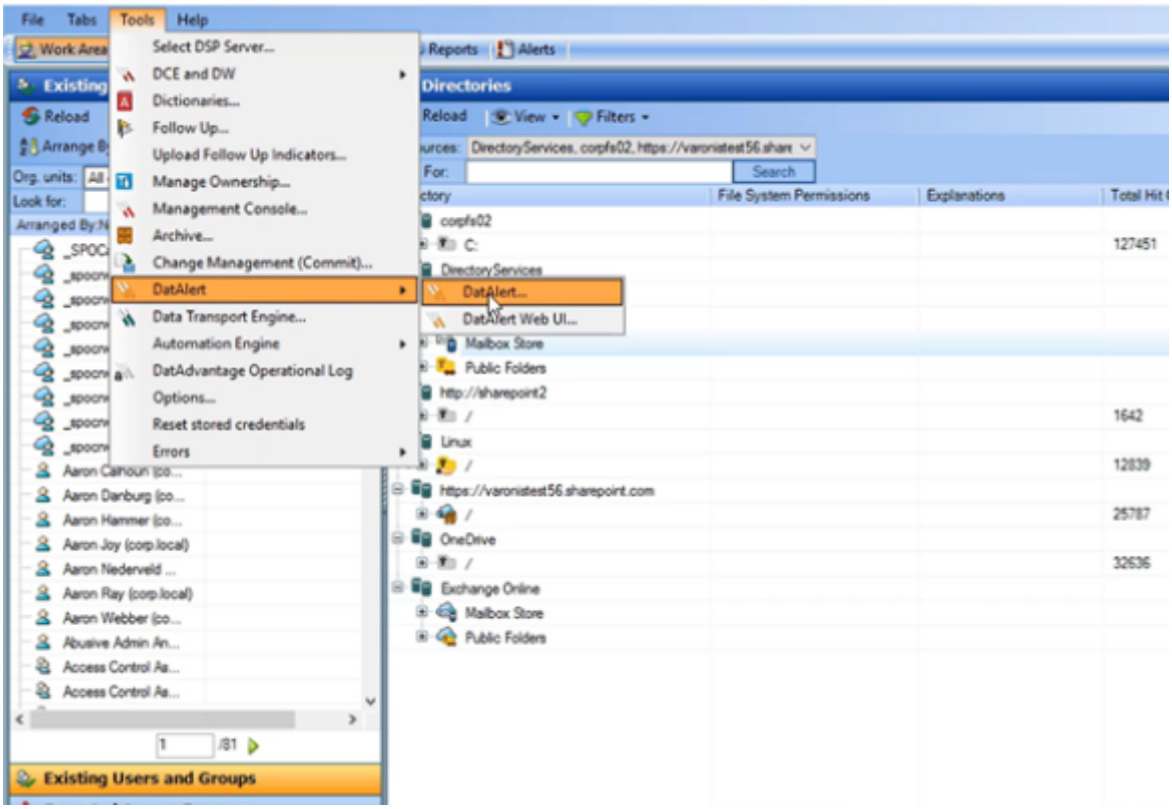
This document outlines the procedure to integrate **Varonis DatAlert** or **DatAdvantage** with a SIEM platform using **Syslog (CEF)**. The integration provides visibility into sensitive data access, permissions changes, and threat alerts.

Prerequisites

- Admin access to **Varonis DatAlert Console**
- IP address and port of your **SIEM/syslog collector**
- Network/firewall access from Varonis to SIEM (UDP or TCP port open)
- (Optional) CEF parsing support in your SIEM

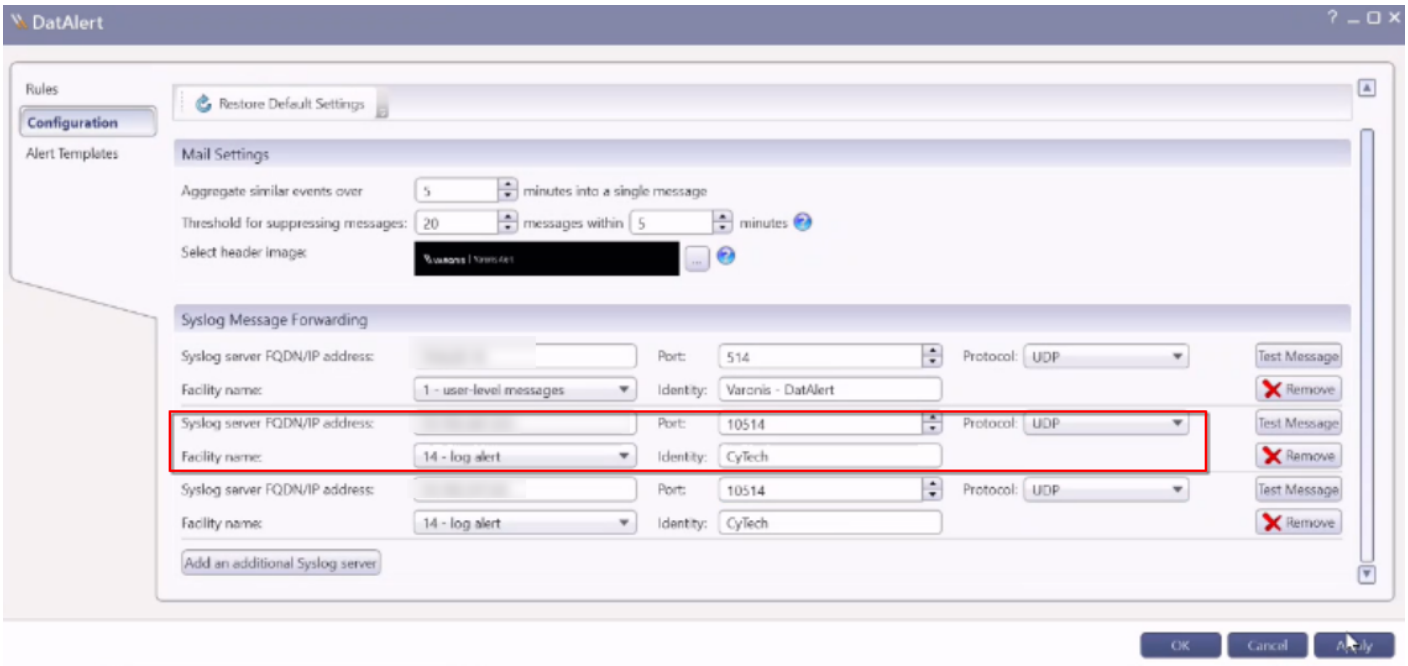
Step 1: Configure Varonis DatAlert for Syslog forwarding

1. Log in to your **Varonis UI** using admin credentials.
2. In Data Advantage, Navigate to:
   Tools → DatAlert → Select DatAlert.



3. Now, select **Configuration.**
4. In **Syslog Message Forwarding**,

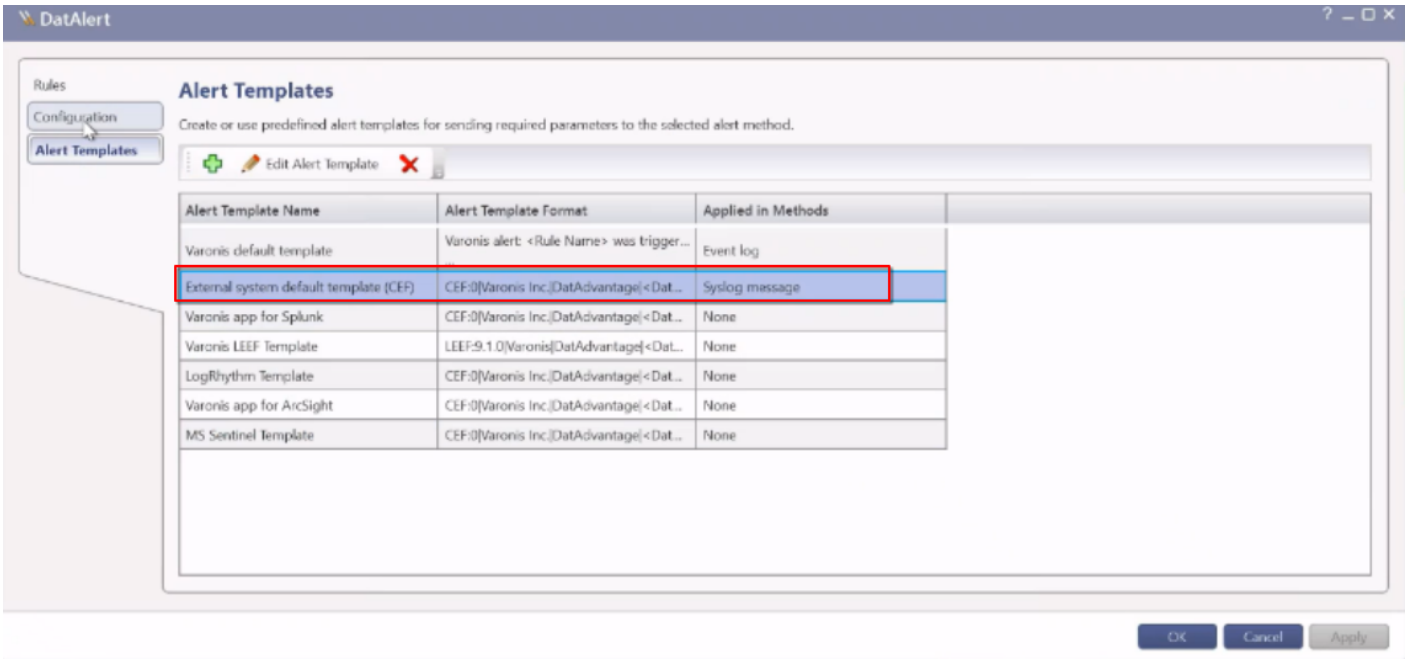
- **Syslog Message IP Address:** AQUILA log collector IP
- **Port: 10514** (if the port has already been used, you can set another one)
- **Transport protocol:** Choose **UDP** or **TCP** (if not already an option; some Varonis versions infer it)
- **Facility name:** Choose a different facility.

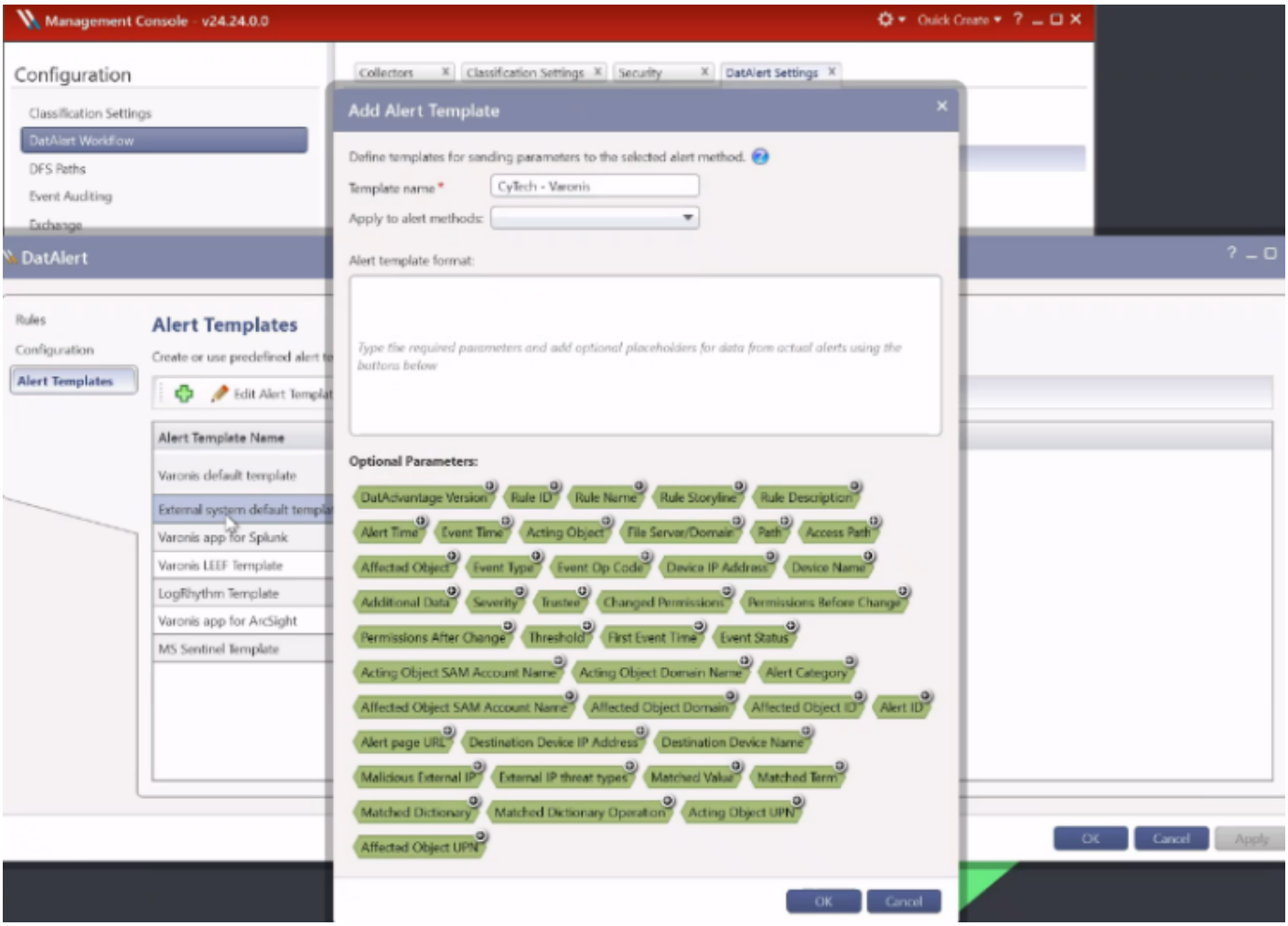


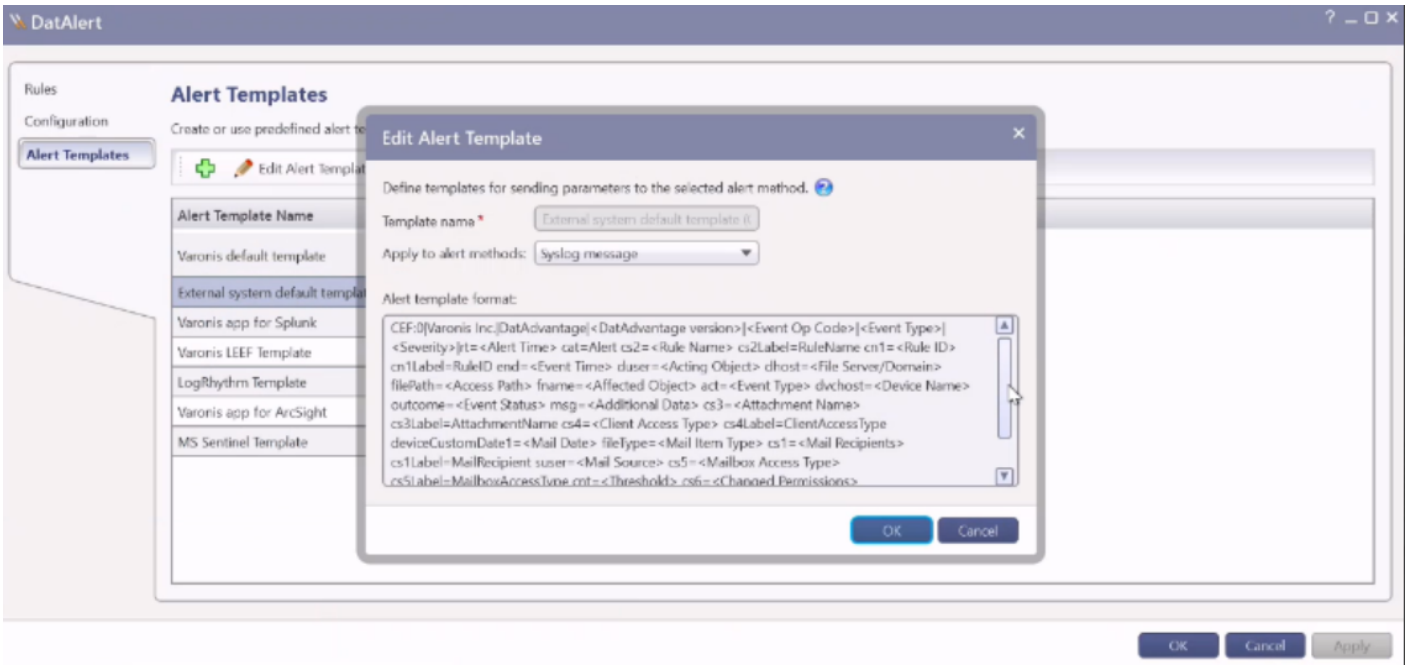
5. Click **Apply.**

Step 2: Create Alert Template in Varonis DatAlert

1. In **DatAlert**, select **Alert Templates**.
2. Click on the **Green Plus** sign to add a New Alert Template.
   - In the Template name, select the **'External system default template (CEF)'**
   - In the Apply to alert methods, select the **'Syslog message'**
3. Click **OK.**


DatAlert
Rules
Configuration
Alert Templates
Alert Templates
Create or use predefined alert templates for sending required parameters to the selected alert method.
Edit Alert Template
Alert Template Name
Alert Template Format
Applied in Methods
Varonis default template
Varonis alert: <Rule Name> was trigger...
Event log
External system default template (CEF)
CEF:0|Varonis Inc.|DatAdvantage|<Dat...
Syslog message
Varonis app for Splunk
CEF:0|Varonis Inc.|DatAdvantage|<Dat...
None
Varonis LEEF Template
LEEF:9.1.0|Varonis|DatAdvantage|<Dat...
None
LogRhythm Template
CEF:0|Varonis Inc.|DatAdvantage|<Dat...
None
Varonis app for ArcSight
CEF:0|Varonis Inc.|DatAdvantage|<Dat...
None
MS Sentinel Template
CEF:0|Varonis Inc.|DatAdvantage|<Dat...
None
OK
Cancel
Apply


Management Console - v24.24.0.0
Quick Create
Configuration
Classification Settings
DatAlert Workflow
DFS Paths
Event Auditing
Exchange
Collectors
Classification Settings
Security
DatAlert Settings
Add Alert Template
Define templates for sending parameters to the selected alert method.
Template name *
CyTech - Varonis
Apply to alert methods:
Alert template format:
Type the required parameters and add optional placeholders for data from actual alerts using the buttons below
Optional Parameters:
DatAdvantage Version
Rule ID
Rule Name
Rule Storyline
Rule Description
Alert Time
Event Time
Acting Object
File Server/Domain
Path
Access Path
Affected Object
Event Type
Event Op Code
Device IP Address
Device Name
Additional Data
Severity
Trustee
Changed Permissions
Permissions Before Change
Permissions After Change
Threshold
First Event Time
Event Status
Acting Object SAM Account Name
Acting Object Domain Name
Alert Category
Affected Object SAM Account Name
Affected Object Domain
Affected Object ID
Alert ID
Alert page URL
Destination Device IP Address
Destination Device Name
Malicious External IP
External IP threat types
Matched Value
Matched Term
Matched Dictionary
Matched Dictionary Operation
Acting Object UPN
Affected Object UPN
OK
Cancel
DatAlert
Rules
Configuration
Alert Templates
Alert Templates
Alert Template Name
Varonis default template
External system default templa
Varonis app for Splunk
Varonis LEEF Template
LogRhythm Template
Varonis app for ArcSight
MS Sentinel Template
OK
Cancel
Apply



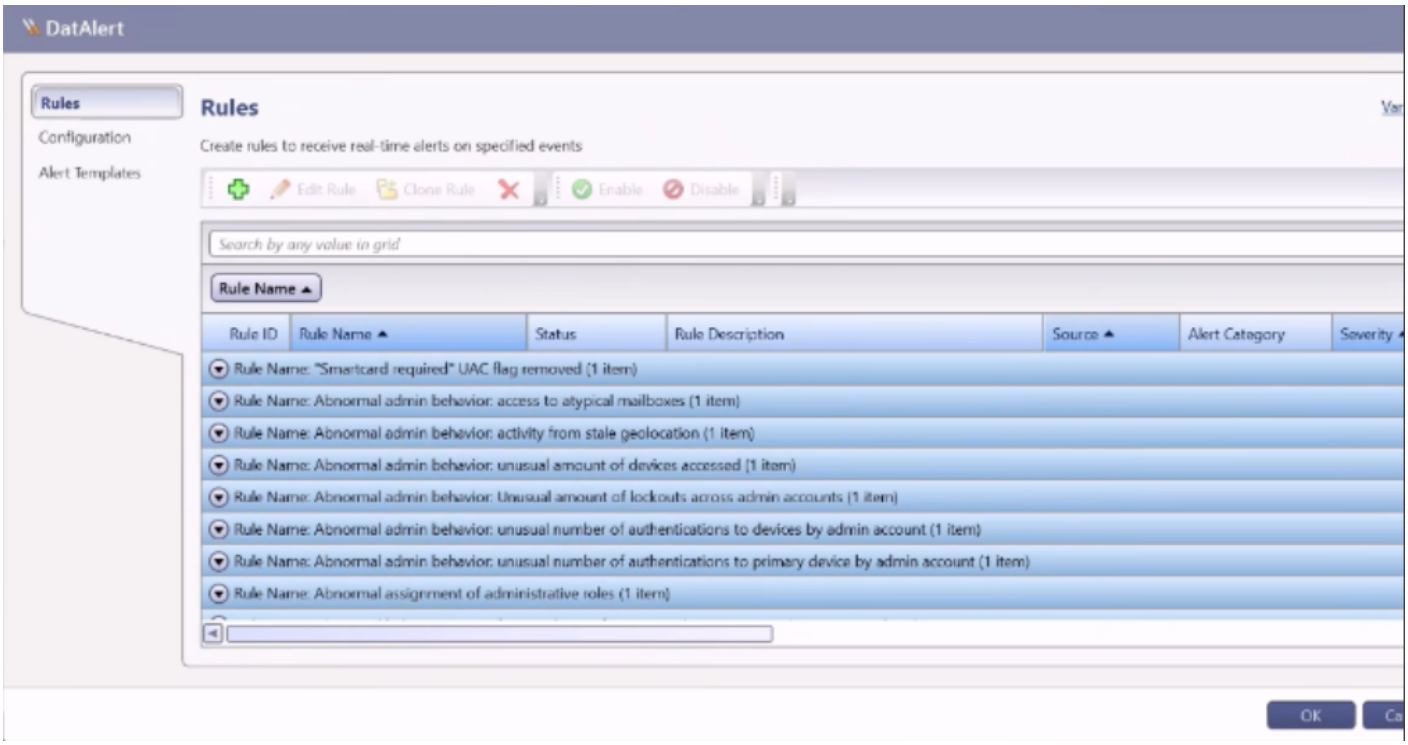
Step 3: Configuring alerts for single or multiple rules

To select the Syslog alert method for a single rule:

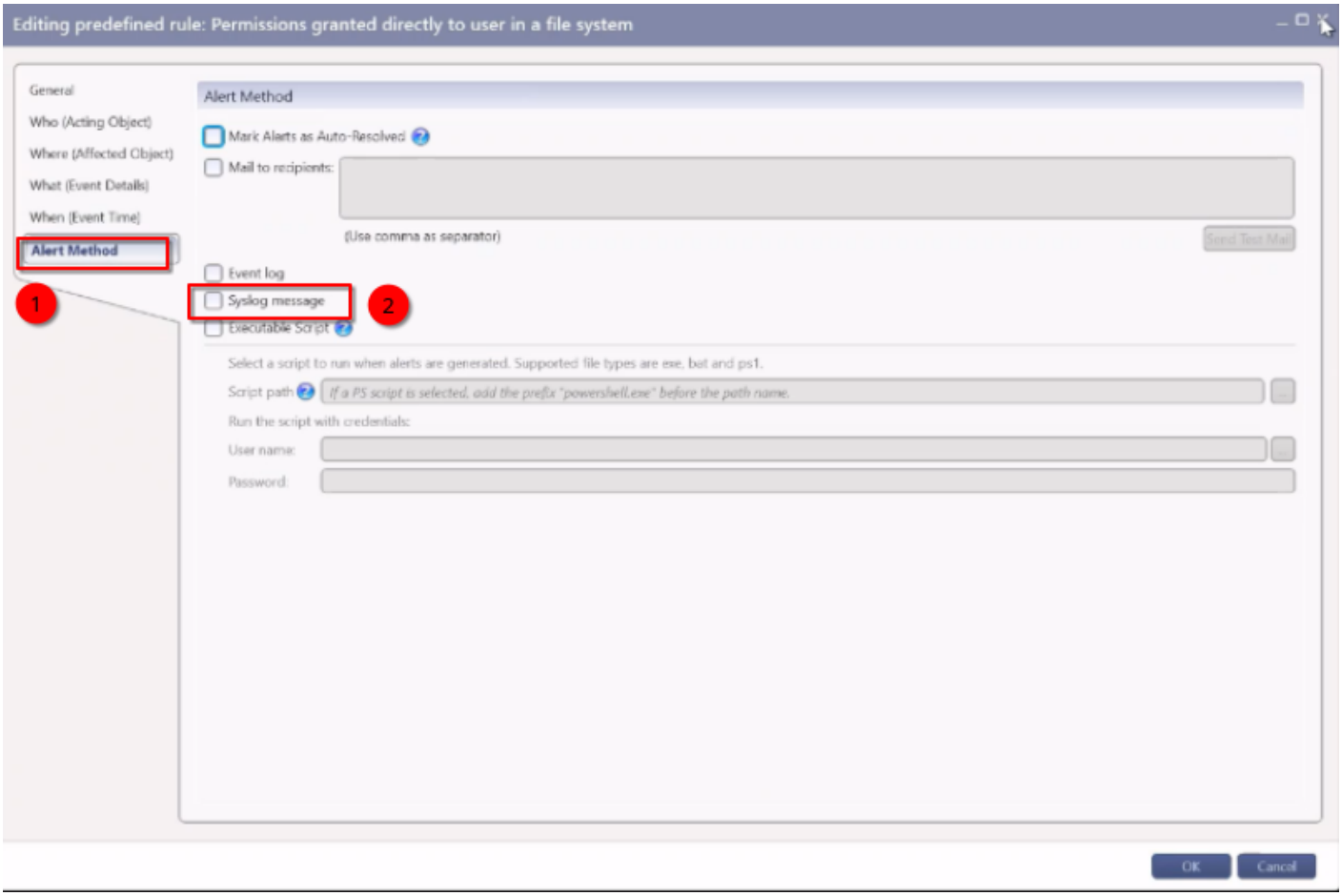
1. From the DatAlert rules table, select the **rule**, then click **Edit Rule**. The rule editing menu appears.
2. From the left menu, select **Alerts Method**. The “**Alert Method**” window appears.
3. Select **Syslog message**.
4. Click **OK**.

To select the Syslog alert method for multiple rules:

1. From the DatAlert rules table, select the **rules**, then click **Edit Rule**. The rule editing menu appears and just "control A" to select all rules.



1. From the left menu, select **Alerts Method**. The "**Alert Method**" window appears, and its contents are disabled for selection.
2. Click the **edit** icon for the Syslog message option, then click the checkbox next to **Syslog message**.
3. Click **OK**.



Please provide the following information to CyTech Support:

- **Port Address**
- **Protocol (TCP or UDP)**

If you need further assistance, kindly contact our support at ***support@cytechint.com*** *for prompt assistance and guidance.*

Revision #5
Created 19 June 2025 07:34:35
Updated 19 June 2026 14:06:48 by Richmond Abella