MACMON NAC WHITEPAPER

Integration von macmon NAC mit Flowmon ADS

Integration von macmon NAC mit Flowmon ADS

Inhalt

Version: 1.5

Über Progress und Flowmon ADS:

Progress ist ein internationaler Anbieter von Netzwerk- und Sicherheitslösungen und bietet mit **Flowmon**, als Teil des Progress-Produktportfolios, eine Lösung zur Überwachung von Netzwerk-Infrastrukturen und Auswertung der ermittelten Daten an.

1 Anwendungsfälle

Noch besser als Datenströme zu beobachten ist es, eine automatische Anomalie-Erkennung im Einsatz zu haben, die nicht nur die Netzwerkadministratoren benachrichtigt, sondern auch Maßnahmen gegen eine angehende Bedrohung ergreift.

1.1 macmon isoliert schadhafte Endgeräte, die von Flowmons Verhaltensanalyse erkannt wurden

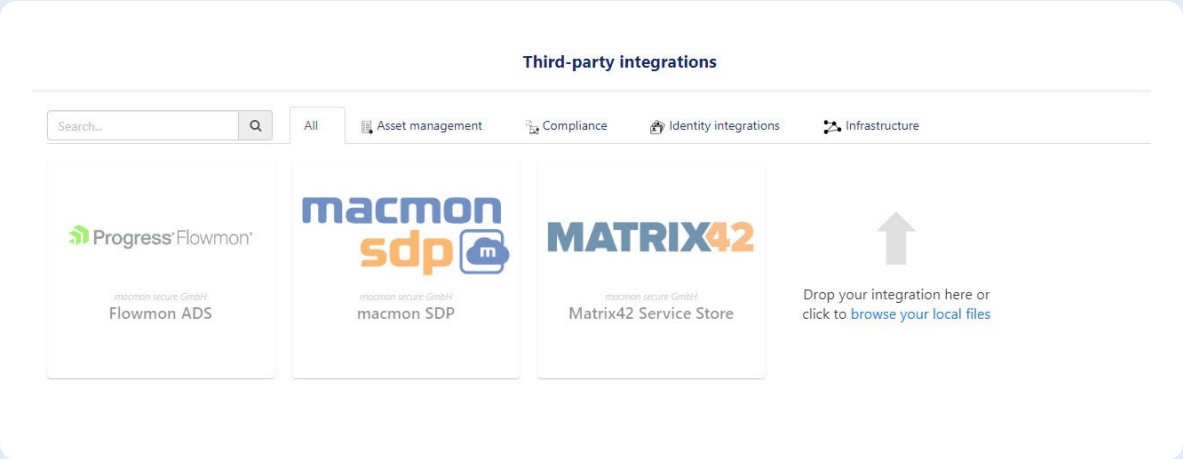
Flowmon ADS nutzt eine fortgeschrittene Künstliche Intelligenz für seine Engine zur Verhaltensanalyse, die verdächtige Netzwerkströme entdeckt, die von einem infizierten Endgerät stammen oder dorthin gehen. Solche Netzwerkströme könnten unter anderem aus Malware-Kommunikation, Botnetz-Aktivitäten oder in gängigen Netzwerkprotokollen versteckten Daten bestehen. Informationen betref-fend des Systemzustands eines Endgeräts wird dann an die **macmon** Compliance API weitergegeben, um das Endgerät zu isolieren und, wenn konfiguriert, den Netzwerkadministrator zu benachrichtigen.

1.2 macmon erlaubt granulare Behandlung verschiedener Ereignisse

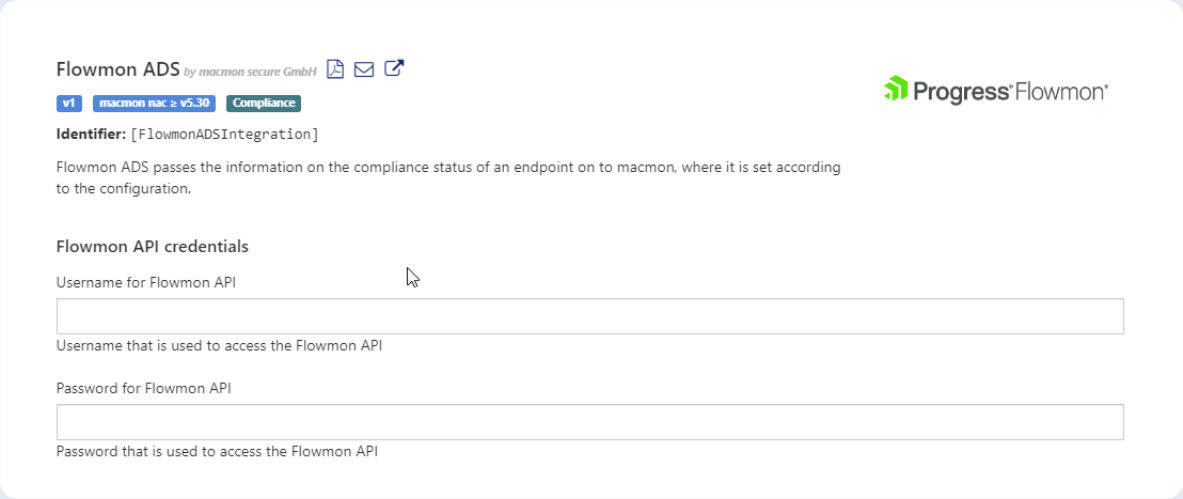
In **Flowmons** *Anomaly Detection System* (Flowmon ADS) können Netzwerkadministatoren verschiedene Anomalie- und Bedrohungsmuster verschiedenen Prioritätsstufen zuordnen. Diese Prioritätsstufen können verschiedenen Compliance-Status in **macmon** zugewiesen werden, um auf Bedrohungslagen verschiedenen Schweregrads angemessen und effektiv reagieren zu können.

2 Konfiguration von macmon NAC

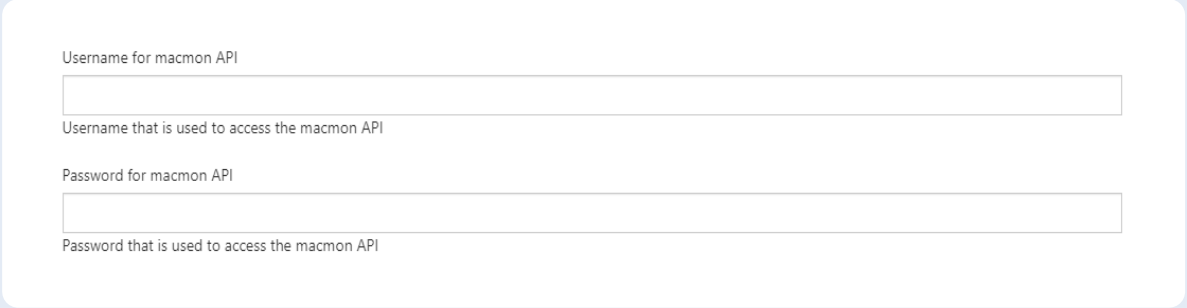
Die Konfiguration wird über die Web-GUI vorgenommen. Wählen Sie dazu bitte *Integrationen*. Für eine bessere Übersicht wählen sie anschließend den Tab *Compliance*.



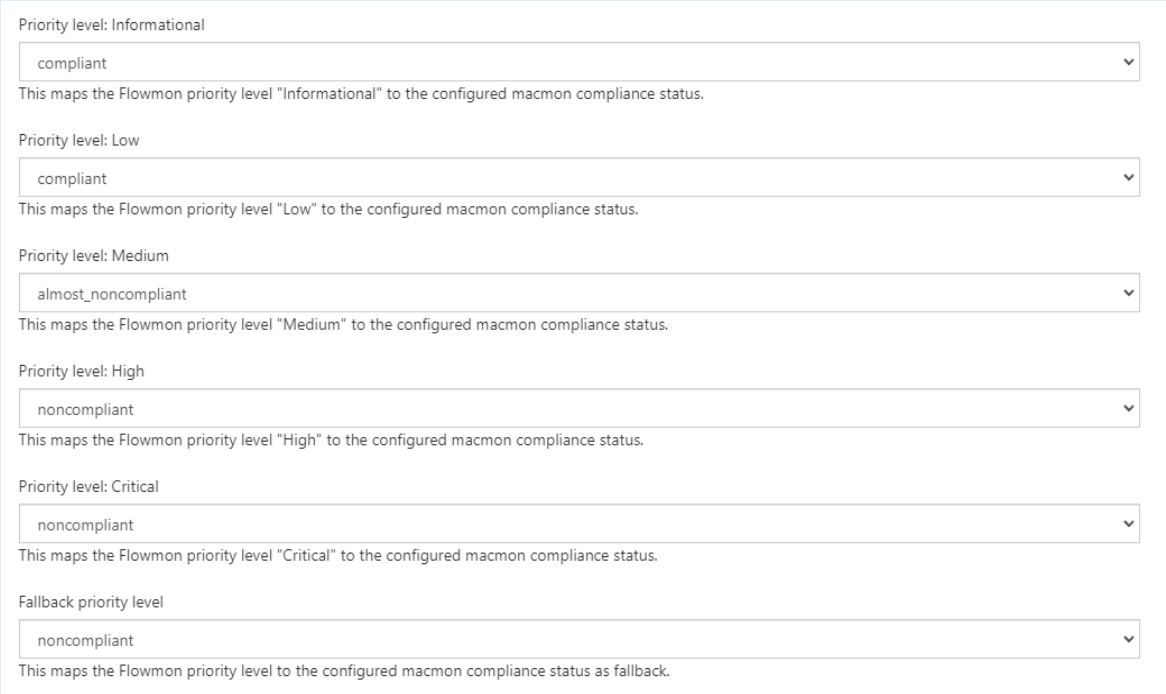
1. Nachdem Sie die Kachel Flowmon – Flowmon ADS angeklickt haben, erscheint die Detailansicht mit dem Konfigurationsformular. Geben Sie hier zunächst die Zugangsdaten ein, die nötig sind, um sich mit der **Flowmon** API zu verbinden.



Geben Sie ebenfalls die Zugangsdaten für die **macmon** *API* ein, über die der Endpoint-Compliance-Status gesetzt werden soll.



2. Weisen Sie den fünf **Flowmon**-Prioritätslevel *Informational*, *Low*, *Medium*, *High* und *Critical* jeweils einen **macmon**-Compliance-Status *compliant*, *almost_noncompliant*, *noncompliant* von **macmon** zu.

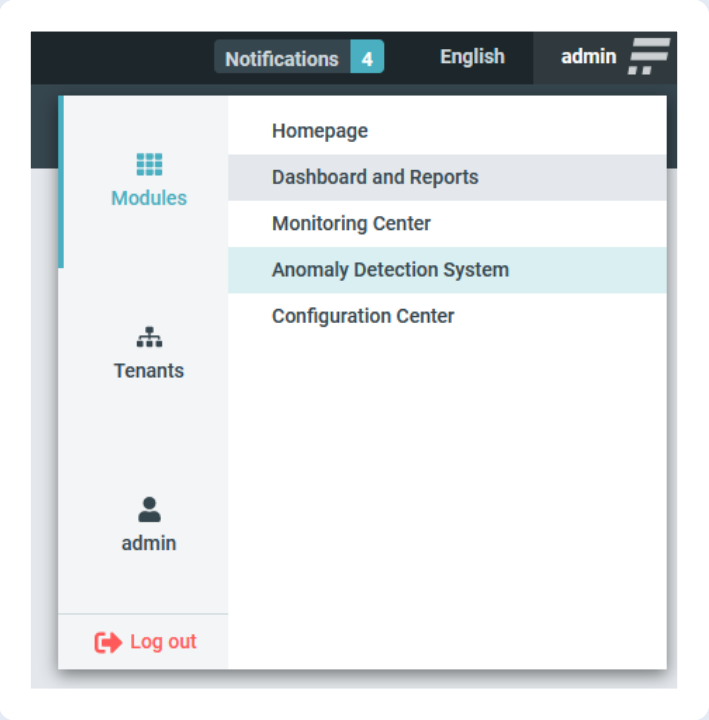


3. In den vorangegangenen Schritten wurde ein Konfigurationsskript erstellt, das sie nun herunterladen und abspeichern können. Der Import des Skriptes und die Konfiguration in Ihrer **Flowmon-Installation** erfolgt im nächsten Schritt (siehe nächsten Abschnitt Konfiguration von Flowmon).

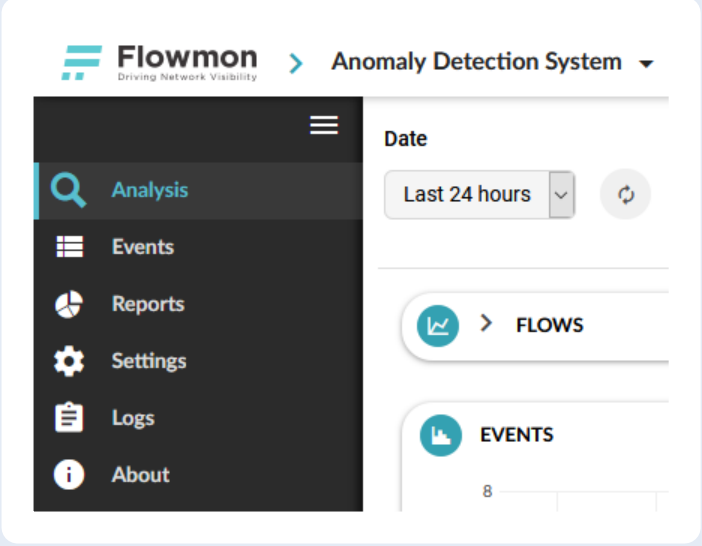
3 Konfiguration von Flowmon

Es sind nur wenige Schritte nötig, um das Skript für die **macmon**-Integration in **Flowmon** zu aktivieren. Stellen Sie sicher, dass Sie die vorherigen Schritte abgeschlossen und das heruntergeladene Skript **macmon**-*integration.sh* in einem Verzeichnis abgespeichert haben, welches sie einfach wiederfinden können.

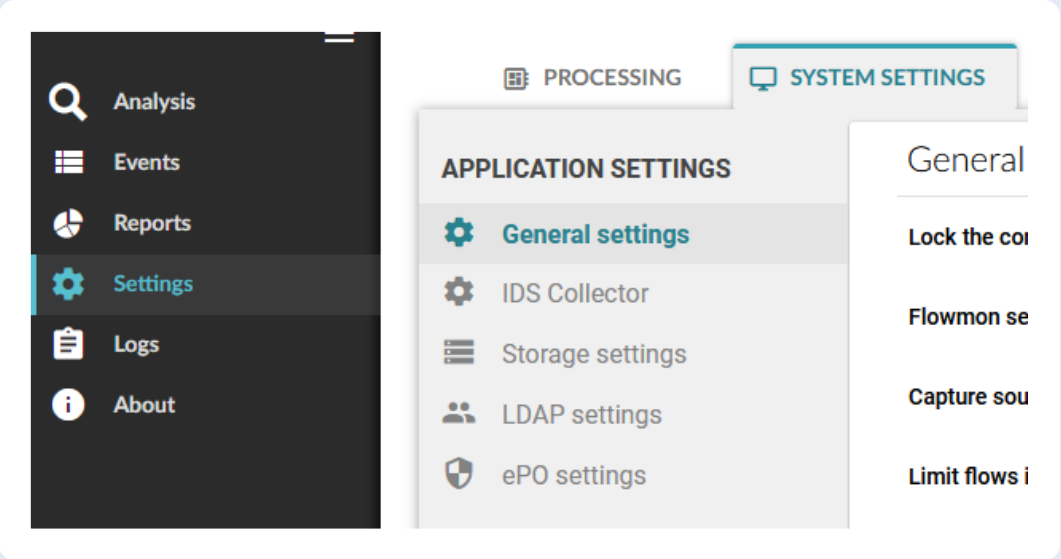
1. Gehen Sie zum **Flowmon-Dashboard** und tippen Sie auf Ihren Benutzernamen in der oberen rechten Ecke. Dort tippen Sie auf *Anomaly Detection System*.



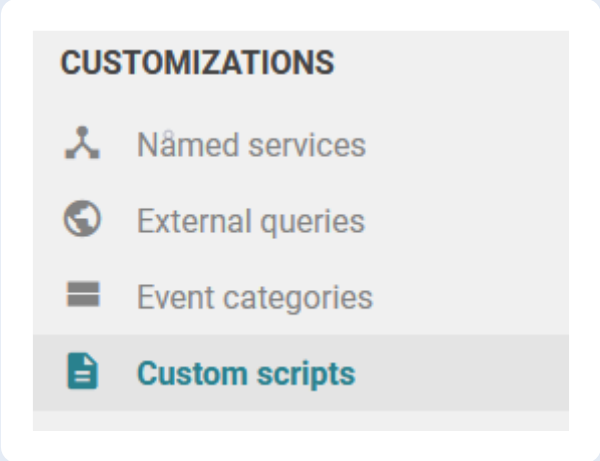
2. Tippen Sie auf *Settings* in der linken Navigationsleiste.



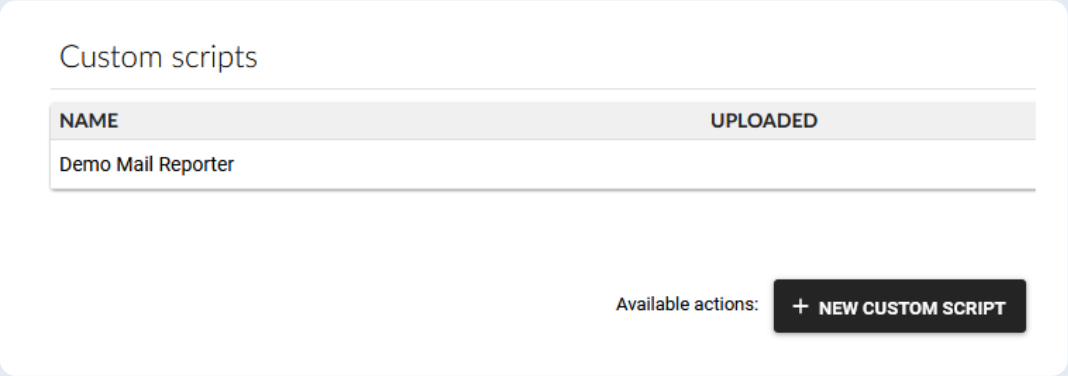
3. Tippen Sie auf den Reiter *System Settings* in der Mitte des Bildschirms.



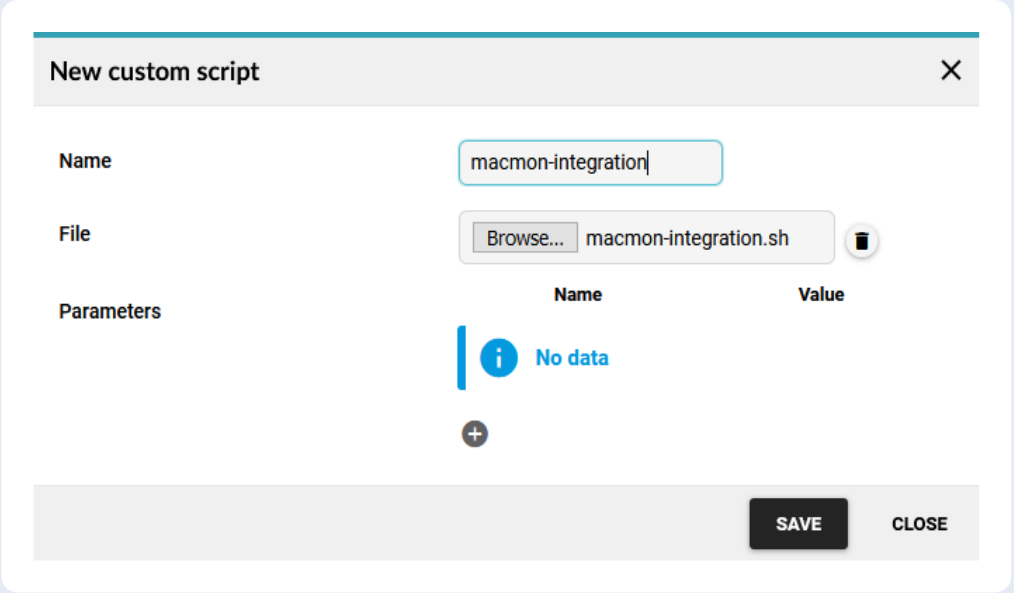
4. Tippen Sie auf *Custom scripts* in der seitlichen Leiste.



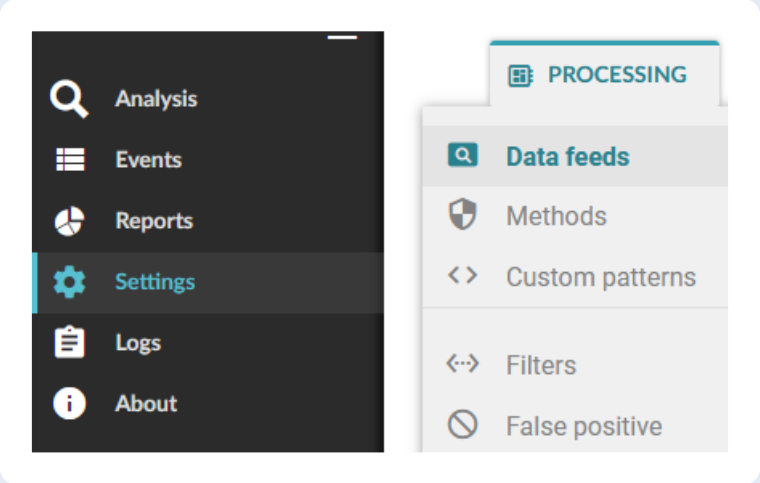
5. Tippen Sie auf den Button *New Custom Script*.



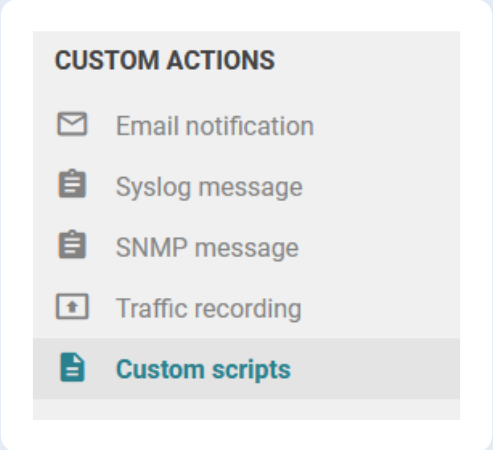
6. Geben Sie im Feld *Name* einen Namen ein, der Ihrem gewöhnlichen Namensschema am besten entspricht. Tippen Sie auf den Button *Durchsuchen* oder *Browse* und wählen Sie das Script **macmon**-*integration.sh* aus. Tippen Sie danach auf den Button *Save*, um das Script auf Ihr **Flowmon**-System zu laden.



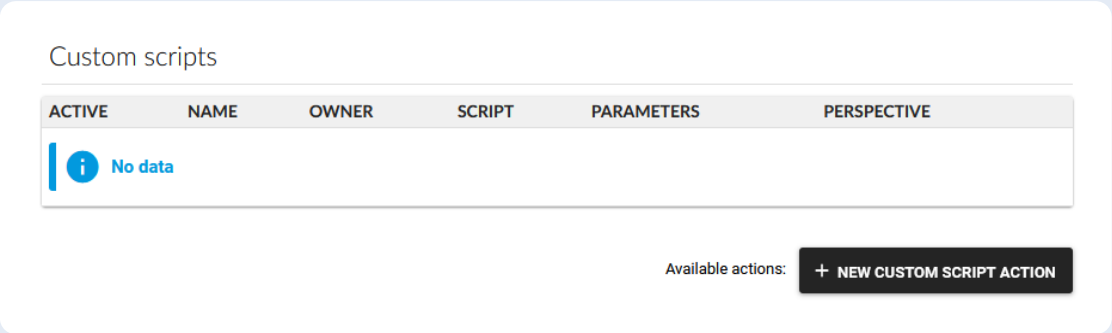
7. Tippen Sie auf den Reiter *Processing*.



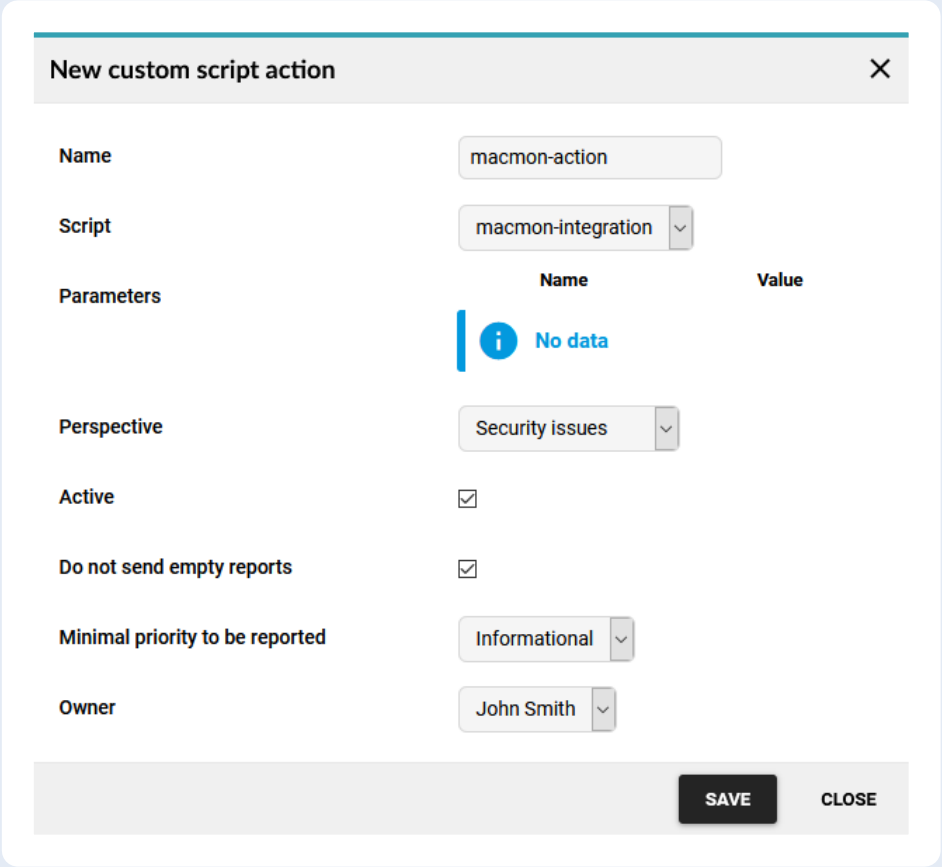
8. Tippen Sie auf *Custom scripts* in der seitlichen Leiste.



9. Tippen Sie auf den Button *New Custom Script Action*, um eine neue Script-Action zu erstellen.



10. Geben Sie im Feld *Name* einen Namen ein, der Ihrem gewöhnlichen Namensschema am besten entspricht. Im Dropdown-Menü *Script* wählen Sie den Namen von **Schritt 6** aus.
Im Dropdown-Menü *Perspective* wählen Sie *Security issues*. Setzen Sie den Haken bei *Active* und wählen Sie bei *Minimal priority to be reported* die minimale Priority-Stufe in der Meldungen an **macmon** übertragen werden sollen. Tippen Sie auf den Button *Save*, um die Integration zu aktivieren.



Sie sind fertig. Die Integration läuft bereits und überträgt Ereignisse an Ihr **macmon**-System.

Kontakt zu Flowmon

Firemenzentrale Europa

Progress Software Europe BV
Prins Alexanderplein 12
Rotterdam, 3067 GC
EMEA Headquarters

Website: https://www.flowmon.com/en
Telefon: +31-10-286-5700