

# Konfigurieren eines FireSIGHT-Systems zum Senden von Warnmeldungen an einen externen Syslog-Server

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Senden von Intrusion Alerts](#)

[Statusbenachrichtigungen senden](#)

[Teil 1: Syslog-Warnung erstellen](#)

[Teil 2: Warnungen für die Integritätsüberwachung erstellen](#)

[Versenden von Auswirkungsmarkierungen, Erkennung von Ereignissen und Malware-Warnungen](#)

## Einleitung

Ein FireSIGHT-System bietet zwar verschiedene Ansichten von Ereignissen innerhalb der Webschnittstelle, Sie können jedoch externe Ereignisbenachrichtigungen konfigurieren, um die konstante Überwachung kritischer Systeme zu vereinfachen. Sie können ein FireSIGHT-System so konfigurieren, dass Sie Warnmeldungen per E-Mail, SNMP-Trap oder Syslog erhalten, wenn eine der folgenden Funktionen generiert wird. In diesem Artikel wird beschrieben, wie Sie ein FireSIGHT Management Center konfigurieren, um Warnungen an einen externen Syslog-Server zu senden.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zu Syslog und FireSIGHT Management Center verfügen. Außerdem muss der Syslog-Port (der Standardwert ist 514) in der Firewall zugelassen sein.

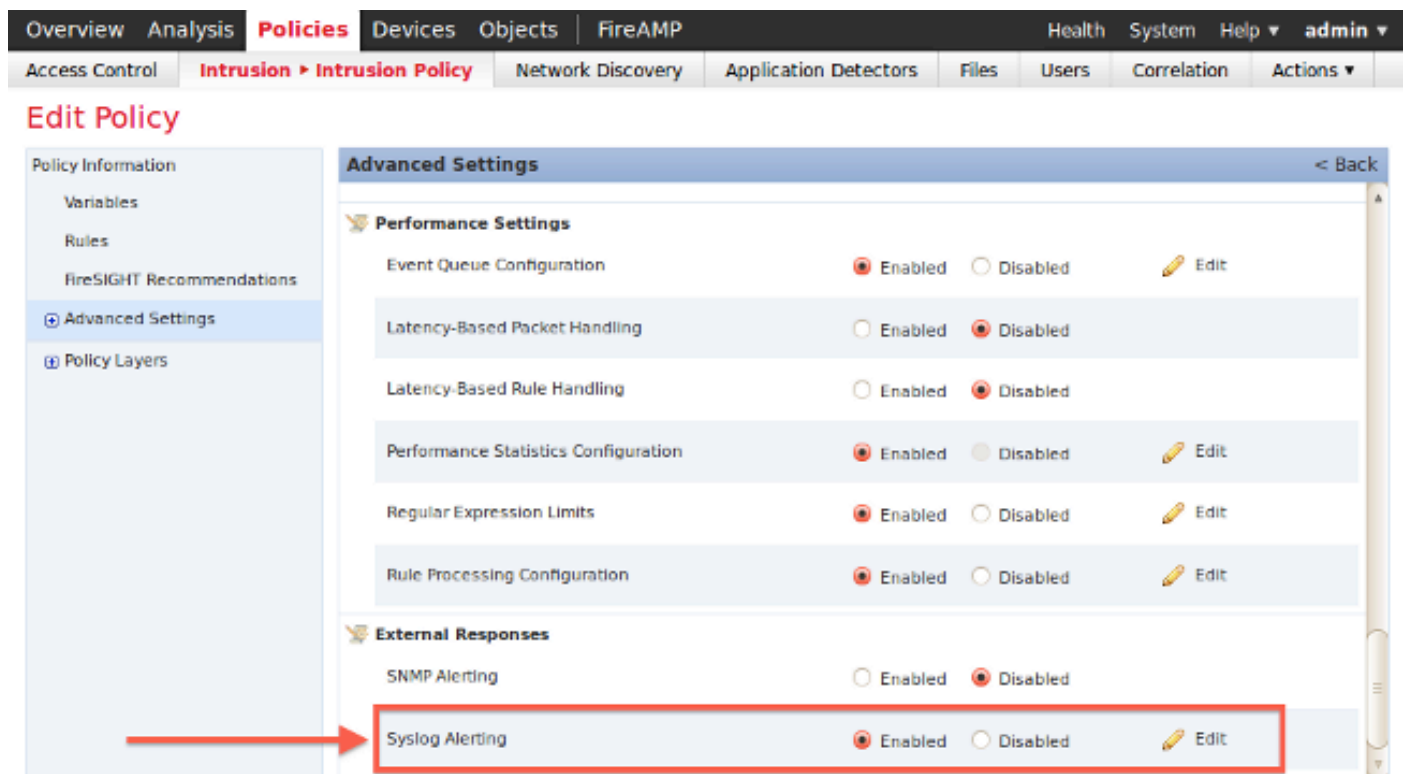
### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Softwareversion 5.2 oder höher.

**Vorsicht:** Die Informationen in diesem Dokument werden von einer Appliance in einer bestimmten Laborumgebung erstellt und mit einer gelöschten (Standard-) Konfiguration gestartet. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

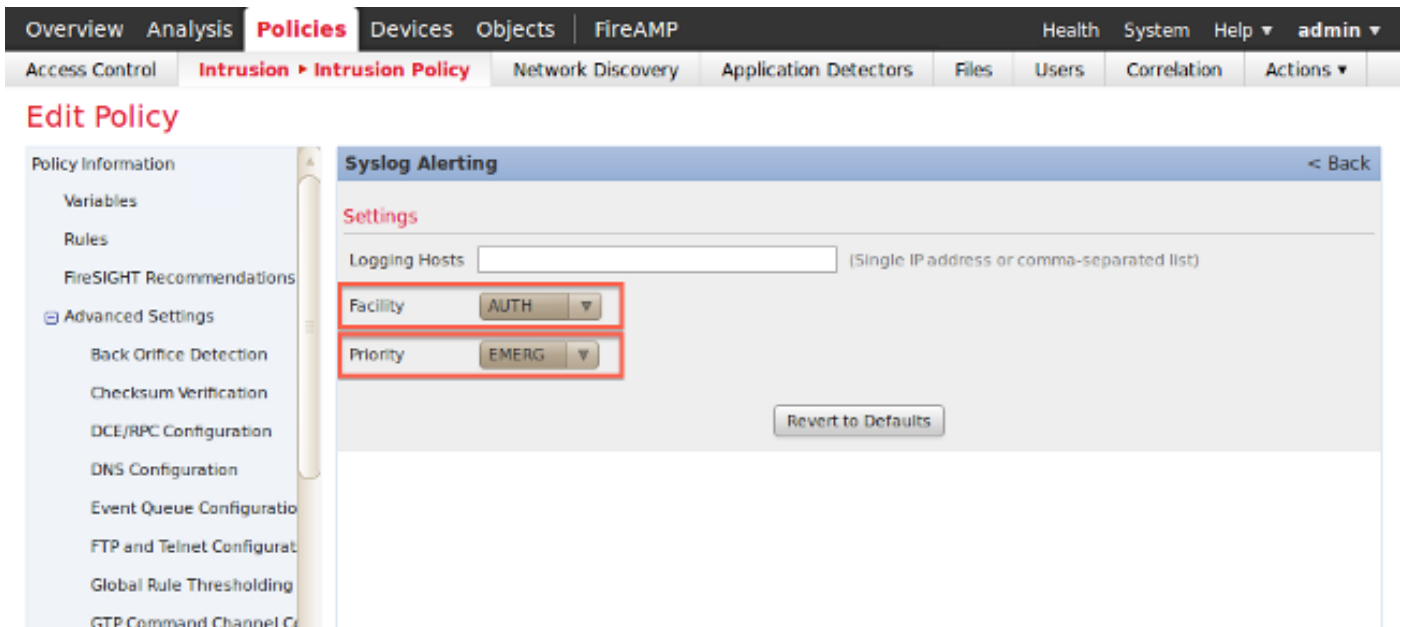
## Senden von Intrusion Alerts

1. Melden Sie sich bei der Web-Benutzeroberfläche Ihres FireSIGHT Management Center an.
2. Navigieren Sie zu **Policies > Intrusion > Intrusion Policy**.
3. Klicken Sie neben der Richtlinie, die Sie anwenden möchten, auf **Bearbeiten**.
4. Klicken Sie auf **Erweiterte Einstellungen**.
5. Suchen Sie in der Liste nach **Syslog Alerting**, und setzen Sie diese auf **Enabled**.



The screenshot shows the 'Edit Policy' page in the FireSIGHT Management Center. The navigation bar at the top includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'FireAMP', 'Health', 'System', 'Help', and 'admin'. The breadcrumb trail is 'Access Control > Intrusion > Intrusion Policy'. The left sidebar shows 'Policy Information' with sub-items: 'Variables', 'Rules', 'FireSIGHT Recommendations', 'Advanced Settings', and 'Policy Layers'. The main content area is titled 'Advanced Settings' and contains two sections: 'Performance Settings' and 'External Responses'. The 'Performance Settings' section includes: 'Event Queue Configuration' (Enabled), 'Latency-Based Packet Handling' (Disabled), 'Latency-Based Rule Handling' (Disabled), 'Performance Statistics Configuration' (Enabled), 'Regular Expression Limits' (Enabled), and 'Rule Processing Configuration' (Enabled). The 'External Responses' section includes: 'SNMP Alerting' (Disabled) and 'Syslog Alerting' (Enabled). The 'Syslog Alerting' row is highlighted with a red box, and a red arrow points to it from the left sidebar.

6. Klicken Sie rechts neben **Syslog Alerting** auf **Edit**.
7. Geben Sie die IP-Adresse Ihres Syslog-Servers in das Feld **Protokollierungshosts** ein.
8. Wählen Sie im Dropdown-Menü eine entsprechende **Fazilität** und einen **Schweregrad**. Diese können auf den Standardwerten belassen werden, es sei denn, ein Syslog-Server ist so konfiguriert, dass er Warnungen für eine bestimmte Einrichtung oder einen bestimmten Schweregrad akzeptiert.



9. Klicken Sie auf **Policy Information** oben links in diesem Bildschirm.

10. Klicken Sie auf die Schaltfläche **Änderungen bestätigen**.

11. Wenden Sie Ihre Zugriffsrichtlinien erneut an.

**Anmerkung:** Verwenden Sie diese Richtlinie für Sicherheitsrisiken in der Zugriffskontrollregel, damit die Warnungen generiert werden. Wenn keine Zugriffskontrollregel konfiguriert ist, legen Sie diese Zugriffskontrollrichtlinie so fest, dass sie als Standardaktion der Zugriffskontrollrichtlinie verwendet wird, und wenden Sie die Zugriffskontrollrichtlinie erneut an.

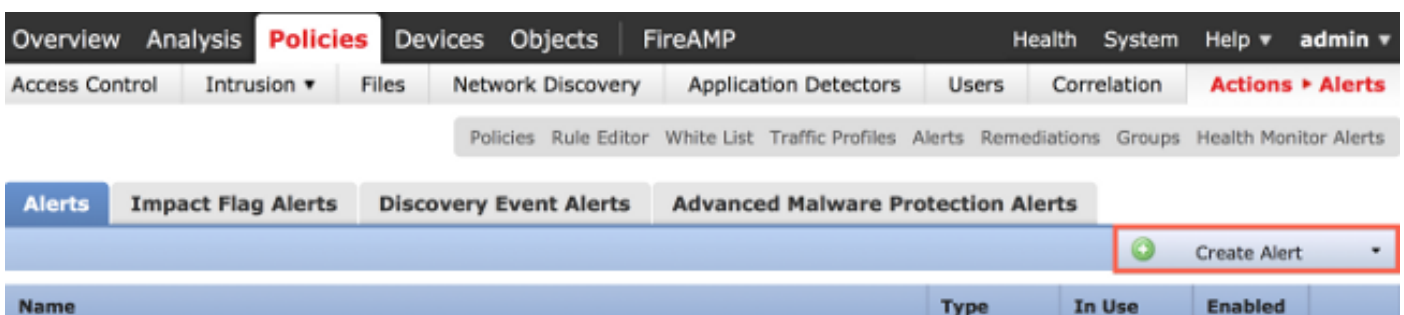
Wenn nun ein Angriffsereignis für diese Richtlinie ausgelöst wird, wird auch eine Warnung an den Syslog-Server gesendet, der für die Angriffsrichtlinie konfiguriert ist.

## Statusbenachrichtigungen senden

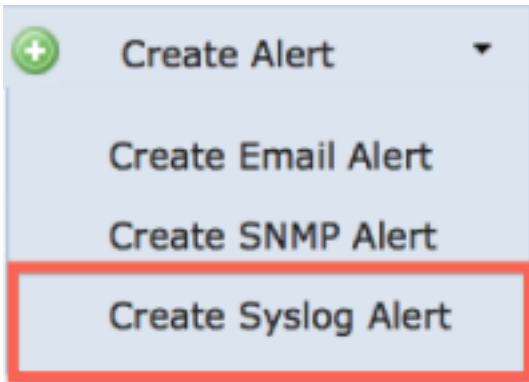
### Teil 1: Syslog-Warnung erstellen

1. Melden Sie sich bei der Web-Benutzeroberfläche Ihres FireSIGHT Management Center an.

2. Navigieren Sie zu **Richtlinien > Aktionen > Warnmeldungen**.



3. Wählen Sie **Create Alert** (Warnung erstellen) auf der rechten Seite der Webschnittstelle aus.



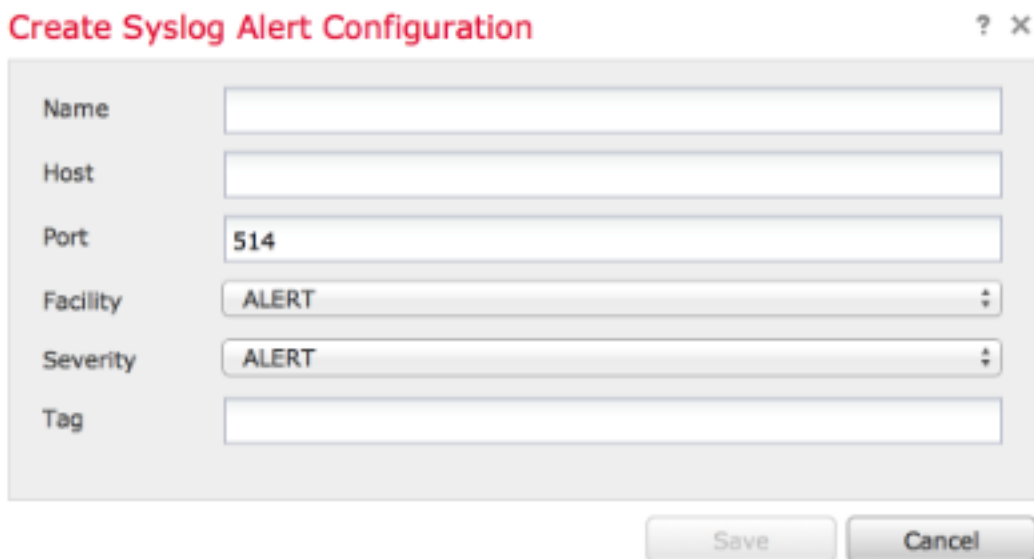
4. Klicken Sie auf **Syslog-Warnung erstellen**. Ein Popup-Fenster für die Konfiguration wird angezeigt.

5. Geben Sie einen Namen für die Warnung ein.

6. Geben Sie die IP-Adresse Ihres Syslog-Servers in das Feld **Host** ein.


7. Ändern Sie den Port bei Bedarf für Ihren Syslog-Server (der Standardport ist 514).

8. Wählen Sie eine geeignete **Anlage** und einen geeigneten **Schweregrad**.

A screenshot of a dialog box titled 'Create Syslog Alert Configuration'. The dialog has a title bar with a question mark and a close button. It contains several input fields: 'Name' (empty), 'Host' (empty), 'Port' (514), 'Facility' (ALERT), 'Severity' (ALERT), and 'Tag' (empty). Below the fields are two buttons: 'Save' and 'Cancel'.

9. Klicken Sie auf die Schaltfläche **Speichern**. Sie kehren zur Seite **Richtlinien > Aktionen > Warnmeldungen** zurück.

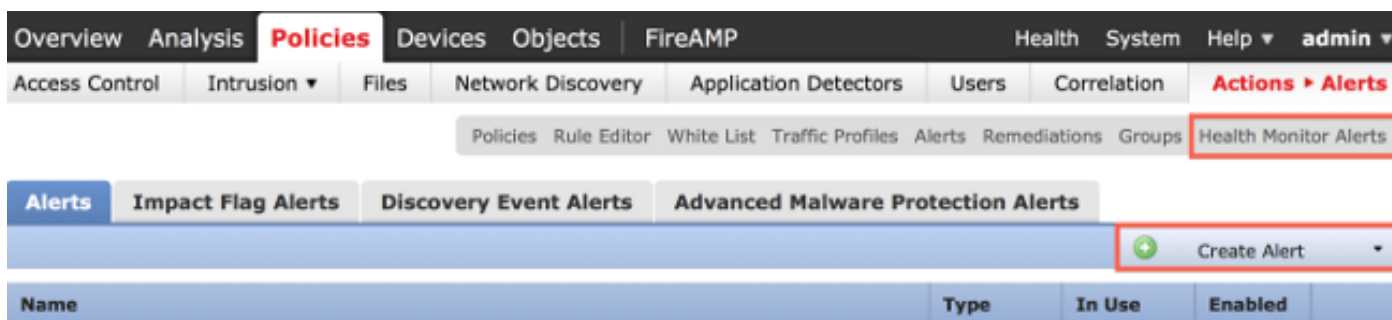
10. Aktivieren Sie die Syslog-Konfiguration.

<span style="float: right;">+ Create Alert</span>			
Type	In Use	Enabled	
Syslog	In Use	<input checked="" type="checkbox"/>	 

## Teil 2: Warnungen für die Integritätsüberwachung erstellen

Die folgende Anweisung beschreibt die Schritte zum Konfigurieren von **Systemüberwachungswarnungen**, die die soeben erstellte Syslog-Warnung verwenden (im vorherigen Abschnitt):

1. Gehen Sie zu **Richtlinien > Aktionen > Warnungen**, und wählen Sie **Warnmeldungen der Integritätsüberwachung**, die sich am oberen Seitenrand befindet.



The screenshot shows the 'Policies' tab in the FireSIGHT Management Center. The navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'FireAMP'. The 'Alerts' section is active, with sub-tabs for 'Impact Flag Alerts', 'Discovery Event Alerts', and 'Advanced Malware Protection Alerts'. A 'Create Alert' button is highlighted with a red box. Below the navigation, a table header is visible with columns for 'Name', 'Type', 'In Use', and 'Enabled'.

2. Geben Sie der Warnmeldung einen Namen.

3. Wählen Sie einen **Schweregrad** (halten Sie die STRG-TASTE gedrückt und klicken Sie darauf, um mehr als einen Schweregrad auszuwählen).

4. Wählen Sie in der Spalte **Module** die Integritätsmodule aus, für die Sie Warnungen an den Syslog-Server senden möchten (z. B. Festplattennutzung).

5. Wählen Sie eine zuvor erstellte Syslog-Warnung in der Spalte **Alerts (Warnungen)**.

6. Klicken Sie auf die Schaltfläche **Speichern**.

## Versenden von Auswirkungsmarkierungen, Erkennung von Ereignissen und Malware-Warnungen

Sie können auch ein FireSIGHT Management Center konfigurieren, um Syslog-Warnungen für Ereignisse mit einer bestimmten Auswirkungsmarkierung, bestimmten Arten von Erkennungsereignissen und Malware-Ereignissen zu senden. Dazu müssen Sie [Teil 1: Erstellen Sie eine Syslog-Warnung](#), und konfigurieren Sie dann die Art von Ereignissen, die Sie an den Syslog-Server senden möchten. Sie können dies tun, indem Sie auf die Seite **Richtlinien >**

**Aktionen > Warnmeldungen** navigieren und dann eine Registerkarte für den gewünschten Warnungstyp auswählen.

The screenshot shows a web-based interface for network security management. At the top, there is a navigation bar with tabs for Overview, Analysis, Policies (highlighted in red), Devices, Objects, and FireAMP. On the right side of this bar, there are links for Health, System, Help, and a user profile for 'admin'. Below this, a secondary navigation bar contains various functional areas: Access Control, Intrusion, Files, Network Discovery, Application Detectors, Users, Correlation, and Actions > Alerts (highlighted in red). A sub-menu for Alerts is open, showing options: Policies, Rule Editor, White List, Traffic Profiles, Alerts, Remediations, Groups, and Health Monitor Alerts. Below this, a specific Alerts sub-menu is visible with three tabs: Alerts, Impact Flag Alerts, Discovery Event Alerts, and Advanced Malware Protection Alerts (highlighted with a red box). To the right of these tabs is a '+ Create Alert' button. At the bottom, the start of a table is visible with columns for Name, Type, In Use, and Enabled.

Name	Type	In Use	Enabled
------	------	--------	---------

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.