

# Fehlerbehebung und Aktivierung von NVM für XDR-Analysen

## Inhalt

---

### [Einleitung](#)

#### [Voraussetzungen](#)

##### [Anforderungen](#)

##### [Verwendete Komponenten](#)

#### [XDR-Analysen NVM-Datenflüsse](#)

##### [NVM-Datenflüsse - XDR-Analysen](#)

##### [NVM-Sensorstatus](#)

##### [NVM-Org-ID](#)

##### [NVM Data Lake-Bereitstellungsstatus](#)

##### [Debuggen](#)

#### [Beobachtungen und Warnungen](#)

##### [NVM-Warnungen](#)

##### [NVM-Warmmeldungseinstellungen](#)

##### [NVM-Beobachtungen](#)

##### [Hinweise zur NVM-Erkennung](#)

#### [Schlussfolgerung](#)

---

## Einleitung

In diesem Dokument wird die Fehlerbehebung bei Cisco XDR-Analysen für Cisco Xtended Detection and Response (XDR)/Network Visibility Module (NVM) beschrieben.

## Voraussetzungen

Aktives XDR-Analyseportal mit XDR-Integration

## Anforderungen

Ausführung des XDR-Analytics-Kontos mit einer einzigen XDR-Integration

## Verwendete Komponenten

- XDR-Analysen
- XDR
- NVM-Sensor
- Sicherer Client (Version 5.0+)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## XDR-Analysen NVM-Datenflüsse

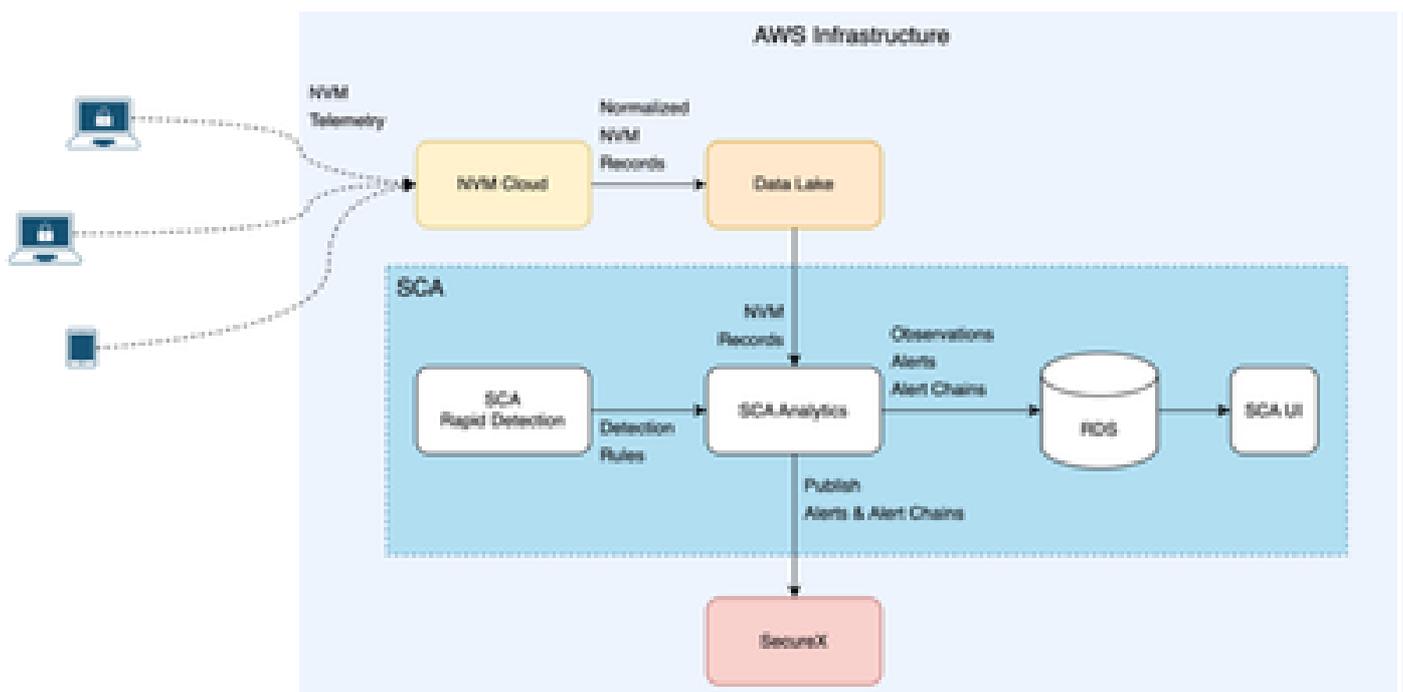
XDR Analytics nutzt jetzt NVM-Telemetrie

Die Telemetrie wird von der NVM-Komponente des Cisco Secure Client generiert.

Die NVM bietet eine verbesserte Netzwerktransparenz, einschließlich des Benutzerverhaltens, der Netzwerkkommunikation und der Prozesse, wodurch der Zeitaufwand für die Vorfalluntersuchung reduziert wird und Lücken in der Endpunkttransparenz geschlossen werden.

<https://docs.xdr.security.cisco.com/Content/Help-Resources/nvm-resources.htm>

### NVM-Datenflüsse - XDR-Analysen



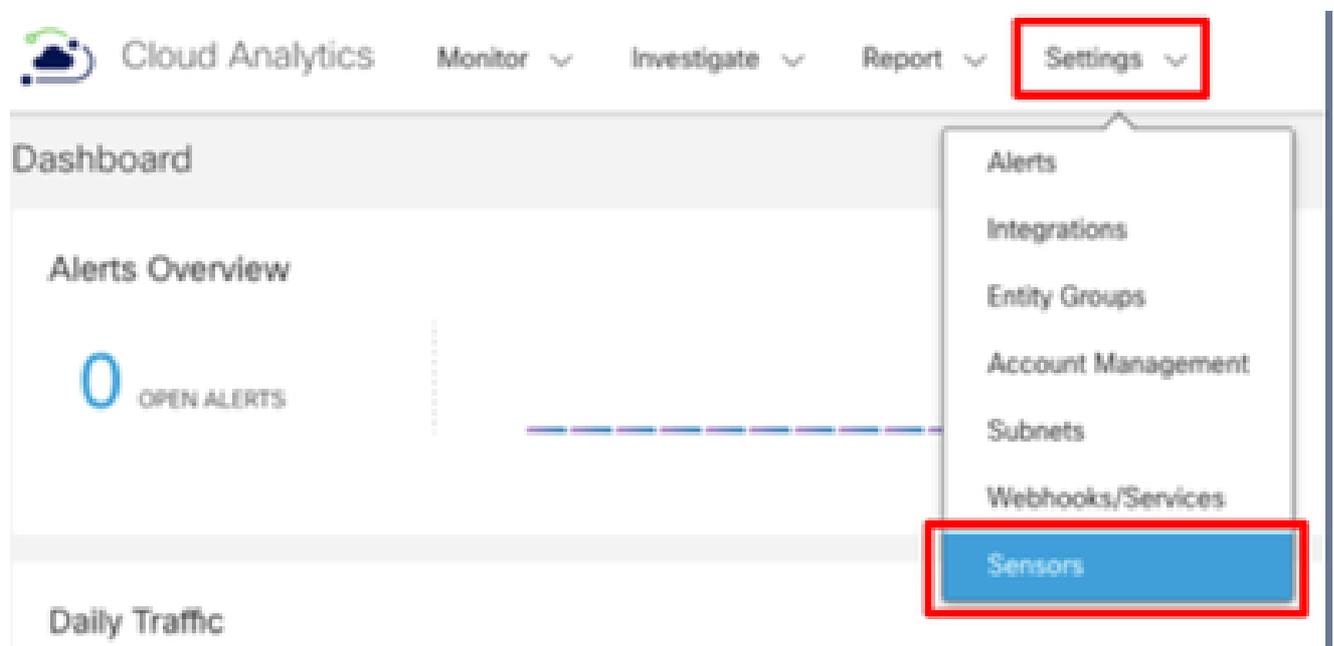
- Wir empfehlen stets, die aktuellen Versionen von Secure Client zu verwenden. Für diesen Workflow ist Secure Client Version 5.0 oder höher erforderlich:  
[https://www.cisco.com/c/en/us/td/docs/security/vpn\\_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html](https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html)
- Aktualisieren Sie Ihr System auf die aktuelle Version von Secure Client und Deployment Profile: <https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm>
- NVM Cloud verarbeitet das Telemetriematerial und stellt es für die Erfassung zur Verfügung. Data Lake nimmt die Telemetriedaten auf und normalisiert sie für eine effiziente

Speicherung.

- XDR Analytics verarbeitet NVM-Datensätze in regelmäßigen Abständen (10 Minuten), um Erkennungen zu generieren - Beobachtungen und Warnungen
- Schnelle Erkennung ermöglicht schnelles Hinzufügen einfacher Beobachtungen und Warnungen mithilfe von Konfigurationen
- XDR-Analytik korreliert Warnungen mit Angriffsketten (ehemals Warnketten)
- Benutzer können Warn- und Angriffsketten auf XDR veröffentlichen.

## NVM-Sensorstatus

- Sicherstellen, dass der NVM-Sensor erstellt wurde:- Navigieren Sie im XDR-Analyse-Dashboard zu "Einstellungen > Sensoren".



- Bestätigen Sie anschließend, dass der NVM-Sensor in der Sensorliste verfügbar ist.

Sensors Sensors

No filters have been applied

Sensor Name Sensor Type Sensor Status

NVM Sensors

NVM Delete



Warnung: Dem XDR-Analytikportal muss maximal ein einzelner XDR-Tenant/eine einzelne Organisation zugeordnet sein.

## NVM-Org-ID

- Vergewissern Sie sich, dass die NVM-Clients die gleiche im API-Endpoint angezeigte Organisations-ID aufweisen:

<https://XDR Analytics PORTAL URL/api/v3/integrations/securex/orgs/>

```
pretty print 
{"meta":{"total":1000,"next_page":0,"offset":0,"prev_page":0,"total_count":1},"objects":[{"org_url":"https://xdr.analytics.com","org_name":"Cisco"}]}
```

## NVM Data Lake-Bereitstellungsstatus

- Die API-Endpunkte, um sicherzustellen, dass der Datensee ordnungsgemäß integriert ist, kann die Zuordnung mithilfe dieses API-Endpunkts bestätigt werden: [https://XDR Analytics Portal URL/api/v3/integrations/securex/orgs/onboard\\_datalake/](https://XDR Analytics Portal URL/api/v3/integrations/securex/orgs/onboard_datalake/)

```
pretty print 
"Datalake provisioned successfully"
```

- Alle Benutzer, denen Zugriff über das Portal gewährt wird, können diese Endpunkte erreichen (Portal-Administratoren, TAC, Techniker)

## Debuggen

- Debugging-Antwortcodes:

Antwortcode	Aktion erforderlich
DataLake erfolgreich bereitgestellt	Validierung von NVM-Flows über die Ereignisanzeige
Datensee kann nicht bereitgestellt werden, keine XDR-Organisation erkannt	XDR und XDR Analytics mit einem Klick integrieren
Datenpakete können nicht bereitgestellt werden. Mehrere XDR-Organisationen wurden erkannt.	TAC-Unterstützung kontaktieren

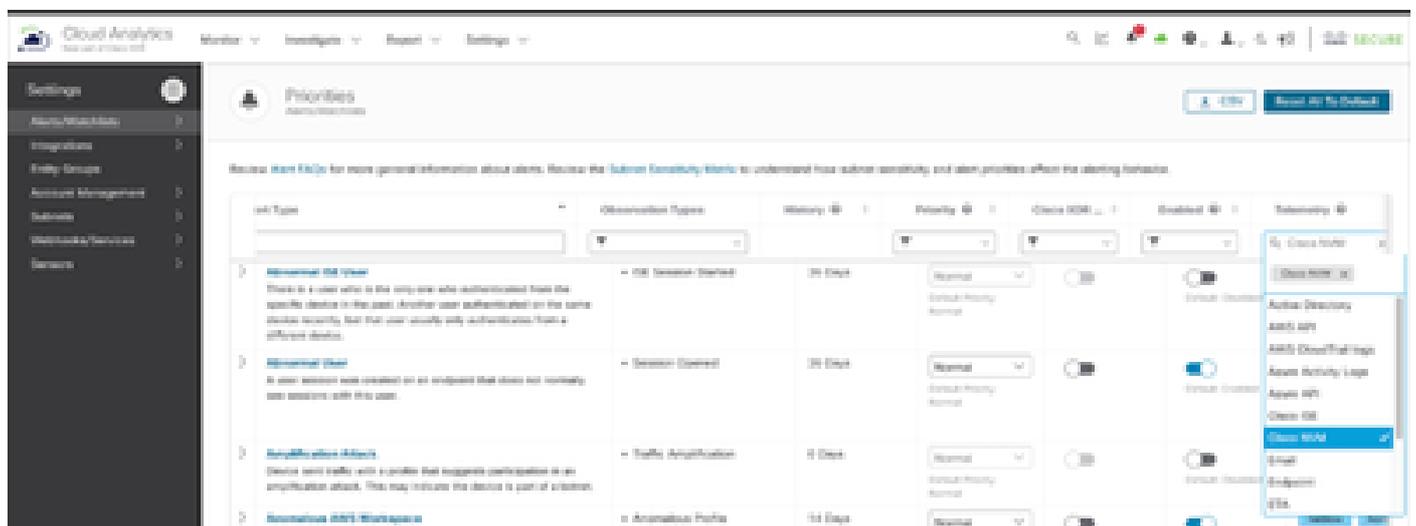
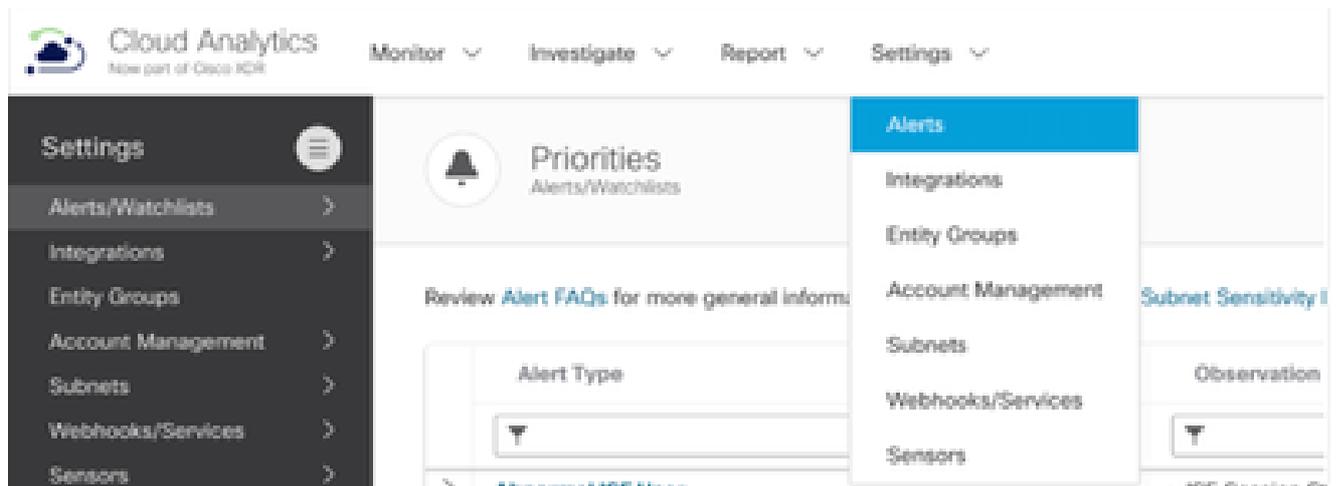
- Wenn einer dieser Schritte fehlschlägt, führen Sie das Secure Client Diagnostics And Reporting Tool (DART) über die Secure Client-Schnittstelle aus, um das Problem zu diagnostizieren (fordern Sie DART immer als Administrator an).

[Sammeln Sie DART-Pakete für sichere Clients](#)

# Beobachtungen und Warnungen

## NVM-Warnungen

- Anmeldung beim XDR Analytics-Portal
- Einstellungen > Warnmeldungen Telemetrie > Cisco NVM
- Telemetrie > Cisco NVM



## NVM-Warmeldungseinstellungen

**Priorities** Clear Reset All

Review [Alert FAQs](#) for more general information about alerts. Review the [Subnet Sensitivity Matrix](#) to understand how subnet sensitivity and alert priorities affect the alerting behavior.

Alert Type	History	Priority	Enabled	Published to Sentinel	Sensitivity
<b>LDAP Connection from Suspicious Process</b> The device was detected running a non-standard LDAP process. This might indicate a credential theft attempt.	0 Days	Normal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Close All</a>
<b>Malicious Process Detected</b> A process running has a hash matching one in a list of known malicious process hashes.	0 Days	Normal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Close All</a>
<b>Metasploit Executed</b> Execution of the offensive tool Metasploit has been detected in endpoint or endpoint telemetry.	0 Days	Normal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Close All</a>
<b>Port 8888: Connections from multiple sources</b> Multiple devices transferred files to a host serving on a file port. This might indicate an exfiltration attempt.	0 Days	Normal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Close All</a>
<b>Potential Persistence Attempt</b> The device was detected applying known persistence mechanisms like establishing background processes used for network access or running applications from network shares.	0 Days	Normal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Close All</a>
<b>Potential System Process Impersonation</b> A process with a name that looks like a common process has been executed indicating process impersonation.	0 Days	Normal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Close All</a>
<b>SMB2001: Connection to multiple destinations</b> The host has transferred files into multiple destination hosts using SMB and connected to those hosts using RDP. This could indicate lateral movement.	1 Day	Normal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Close All</a>
<b>Suspicious Process Path</b> A process was executed on an endpoint from a directory that shouldn't have executables.	0 Days	Normal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">Close All</a>

## NVM-Beobachtungen

- Verdächtige Endpunktaktivität
- XDR Analytics-Portal
- Überwachen > Beobachtungen
- Ausgewählte Beobachtung
- Filtern verdächtiger Endpunktaktivitäten

**Cloud Analytics** Monitor Investigate Report Settings

**Observations**

Highlights

Types

By Device

**Selected Observation**

### Selected Observation

Observations

---

#### Persistent External Server observation

Observation Type: Persistent External Server

Observation Type\*

- Q Suspi
- ISE Suspicious Activity
- Suspicious Endpoint Activity**
- Suspicious Network Activity
- Suspicious SMB Activity

Search

Filter by source name, sha1, raw

## Hinweise zur NVM-Erkennung

- NVM erfasst nur Prozesse und Flow-Daten, mit denen eine Netzwerkverbindung besteht.
- NVM ist so konfiguriert, dass Flow-Daten standardmäßig nur am Ende des Flow gemeldet werden

## Schlussfolgerung

Diese Schritte helfen Ihnen, durch XDR-Analysen zu navigieren, um Beobachtungen und Warnungen mithilfe von NVM-Informationen zu aktivieren und den Workflow zu beheben.

## 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.