# ExtraHop 9.6
# Leitfaden für die Admin-Benutzeroberfläche von ExtraHop Trace

Weitere Informationen finden Sie unter https://docs.extrahop.com.

Veröffentlicht: 2024-04-10

ExtraHop Networks
Seattle, WA 98101
877-333-9872 (US)
+44 (0)203 7016850 (EMEA)
+65-31585513 (APAC)
www.extrahop.com

# Inhaltsübersicht

# Einführung in die ExtraHop Trace Admin UI

Der ExtraHop Trace Admin UI Guide enthält detaillierte Informationen zu den Administratorfunktionen und Funktionen der ExtraHop Trace-Appliance.

Darüber hinaus bietet dieses Handbuch einen Überblick über die globale Navigation und Informationen zu den Steuerelementen, Feldern und Optionen, die in den Einstellungen der Trace-Administration verfügbar sind.

Nachdem Sie Ihre Trace-Appliance bereitgestellt haben, lesen Sie die Checkliste für die Nachverfolgung nach der Bereitstellung.

Wir freuen uns über Ihr Feedback. Bitte teilen Sie uns mit, wie wir dieses Dokument verbessern können. Senden Sie Ihre Kommentare oder Vorschläge an documentation@extrahop.com.

## Unterstützte Browser

Die folgenden Browser sind mit allen ExtraHop-Systemen kompatibel. Wenden Sie die von Ihrem Browser bereitgestellten Barrierefreiheits- und Kompatibilitätsfunktionen an, um über technische Hilfsmittel auf Inhalte zuzugreifen.

- Firefox
- Google Chrome
- Microsoft Edge
- Safari

**Wichtig:** Internet Explorer 11 wird nicht mehr unterstützt. Wir empfehlen Ihnen, die neueste Version aller unterstützten Browser zu installieren.

# Status und Diagnose

Die Status und Diagnose Dieser Abschnitt enthält Metriken und Protokolldaten zum aktuellen Status des ExtraHop-Packetstores und ermöglicht es Systemadministratoren, den allgemeinen Systemzustand einzusehen.

**Gesundheit**

Stellt Kennzahlen zur Betriebseffizienz des ExtraHop-Packetstores bereit.

**Audit-Protokoll**

Ermöglicht das Anzeigen von Daten zur Ereignisprotokollierung und das Ändern der Syslog-Einstellungen.

**Fingerabdruck**

Bietet die einzigartige Hardware Fingerabdruck für den ExtraHop Packetstore.

**Unterstützungsskripte**

Ermöglicht das Hochladen und Ausführen von Support-Skripten.

**Ausnahmedateien**

Aktiviert oder deaktiviert die ExtraHop Packetstore-Ausnahmedateien.

## Gesundheit

Die Gesundheit Diese Seite bietet eine Sammlung von Metriken, mit denen Sie den Betrieb der Trace-Appliance überprüfen können.

Die Metriken auf dieser Seite können Ihnen helfen, Probleme zu beheben und festzustellen, warum die ExtraHop-Appliance nicht wie erwartet funktioniert.

**System**

Meldet die folgenden Informationen über die CPU-Auslastung des Systems und die Festplattenlaufwerke.

**CPU-Benutzer**

Zeigt den Prozentsatz der CPU-Auslastung an, der dem Trace-Appliance-Benutzer zugeordnet ist.

**CPU-System**

Zeigt den Prozentsatz der CPU-Auslastung an, der der Trace-Appliance zugeordnet ist.

**CPU im Leerlauf**

Zeigt den Prozentsatz der CPU-Leerlaufzeit an, der der Trace-Appliance zugeordnet ist.

**CPU-IO**

Zeigt den Prozentsatz der CPU-Auslastung an, der mit den I/O-Funktionen der Trace-Appliance verknüpft ist.

**Status des Dienstes**

Meldet den Status der ExtraHop Packetstore-Systemdienste.

**Ex-Admin**

Zeigt die Uhrzeit an, zu der der ExtraHop Packetstore-Webportaldienst gestartet wurde.

**exconfig**

Zeigt die Uhrzeit an, zu der der ExtraHop Packetstore-Konfigurationsdienst gestartet wurde.

**ausnehmen**

Zeigt die Uhrzeit an, zu der der ExtraHop-Packetstore-Erfassungsdienst gestartet wurde.

**Schnittstellen**

Meldet den Status der ExtraHop Packetstore-Netzwerkschnittstellen.

**RX-Pakete**

Zeigt die Anzahl der Pakete an, die vom ExtraHop-Packetstore auf der angegebenen Schnittstelle empfangen wurden.

**RX-Fehler**

Zeigt die Anzahl der empfangenen Paketfehler auf der angegebenen Schnittstelle an.

**RX-Drops**

Zeigt die Anzahl der empfangenen Pakete an, die auf der angegebenen Schnittstelle verworfen wurden.

**TX-Pakete**

Zeigt die Anzahl der Pakete an, die vom ExtraHop-Packetstore auf der angegebenen Schnittstelle übertragen wurden.

**TX-Fehler**

Zeigt die Anzahl der übertragenen Paketfehler auf der angegebenen Schnittstelle an.

**TX Drops**

Zeigt die Anzahl der übertragenen Pakete an, die auf der angegebenen Schnittstelle verworfen wurden.

**RX-Bytes**

Zeigt die Anzahl der Byte an, die der ExtraHop-Paketspeicher auf der angegebenen Schnittstelle empfangen hat.

**TX-Bytes**

Zeigt die Anzahl der Byte an, die vom ExtraHop-Packetstore auf der angegebenen Schnittstelle übertragen wurden.

**Partitionen**

Meldet den Status und die Verwendung von ExtraHop Packetstore-Komponenten. Die Konfigurationseinstellungen für diese Komponenten werden auf der Festplatte gespeichert und auch dann beibehalten, wenn der Packetstore ausgeschaltet wird.

**Name**

Zeigt die ExtraHop-Packetstore-Einstellungen an, die auf der Festplatte gespeichert sind.

**Optionen**

Zeigt die Lese- und Schreiboptionen für die auf der Festplatte gespeicherten Einstellungen an.

**Größe**

Zeigt die Größe der identifizierten Komponente in Gigabyte an.

**Nutzung**

Zeigt den Speicherverbrauch für jede der Komponenten als Menge und als Prozentsatz des gesamten Festplattenspeichers an.

## Audit-Protokoll

Das Audit-Log enthält Daten über den Betrieb Ihres ExtraHop-Systems, aufgeschlüsselt nach Komponenten. Das Audit-Log listet alle bekannten Ereignisse nach Zeitstempel in umgekehrter chronologischer Reihenfolge auf.

Wenn Sie ein Problem mit dem ExtraHop-System haben, lesen Sie das Audit-Log, um detaillierte Diagnosedaten einzusehen, um festzustellen, was das Problem verursacht haben könnte.

## Fingerabdruck

Fingerabdrücke helfen dabei, Appliances vor Machine-in-the-Middle-Angriffen zu schützen, indem sie eine eindeutige Kennung bereitstellen, die beim Verbinden von ExtraHop-Appliances verifiziert werden kann.

Wenn Sie eine Explore- oder Trace-Appliance mit einer Discover-Appliance oder Command-Appliance verbinden, stellen Sie sicher, dass der angezeigte Fingerabdruck genau dem Fingerabdruck entspricht, der auf der Beitritts - oder Kopplungsseite angezeigt wird.

Wenn die Fingerabdrücke nicht übereinstimmen, wurde die Kommunikation zwischen den Geräten möglicherweise abgefangen und verändert.

## Unterstützungsskripte

ExtraHop Support stellt möglicherweise ein Support-Skript bereit, das eine spezielle Einstellung anwenden, eine kleine Anpassung am ExtraHop-System vornehmen oder Hilfe beim Fernsupport oder bei erweiterten Einstellungen bieten kann. Die Administrationseinstellungen ermöglichen es Ihnen, Support-Skripte hochzuladen und auszuführen.

### Führen Sie das Standard-Support-Skript aus

Das Standard-Supportskript sammelt Informationen über den Status des ExtraHop-Systems zur Analyse durch den ExtraHop-Support.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Status und Diagnose auf **Unterstützungsskripte**.
3. klicken **Standard-Support-Skript ausführen**.
4. klicken **Lauf**.
   Wenn das Skript abgeschlossen ist, Ergebnisse des Support-Skripts Seite erscheint.
5. Klicken Sie auf den Namen des Diagnosesupportpakets, das Sie herunterladen möchten. Die Datei wird am Standard-Download-Speicherort auf Ihrem Computer gespeichert.
   Senden Sie diese Datei, normalerweise mit dem Namen `diag-results-complete.expk`, zum ExtraHop Support.

   Die `.expk` Die Datei ist verschlüsselt und der Inhalt ist nur für den ExtraHop-Support sichtbar. Sie können jedoch das herunterladen `diag-results-complete.manifest` Datei, um eine Liste der gesammelten Dateien anzuzeigen.

### Führen Sie ein benutzerdefiniertes Support-Skript aus

Wenn Sie vom ExtraHop Support ein benutzerdefiniertes Support-Skript erhalten, gehen Sie wie folgt vor, um eine kleine Anpassung am System vorzunehmen oder erweiterte Einstellungen vorzunehmen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Status und Diagnose Abschnitt, klicken **Unterstützungsskripte**.
3. klicken **Benutzerdefiniertes Support-Skript ausführen**.
4. klicken **Wählen Sie Datei**, navigieren Sie zu dem Diagnosesupport-Skript, das Sie hochladen möchten, und klicken Sie dann auf **Offen**.
5. klicken **Upload** um die Datei auf dem ExtraHop-System auszuführen.
   Der ExtraHop Support bestätigt, dass das Support-Skript die gewünschten Ergebnisse erzielt hat.

## Ausnahmedateien

Ausnahmedateien sind eine Kerndatei der im Speicher gespeicherten Daten. Wenn Sie die Einstellung Ausnahmedatei aktivieren, wird die Kerndatei auf die Festplatte geschrieben, wenn das System unerwartet stoppt oder neu gestartet wird. Diese Datei kann dem ExtraHop Support helfen, das Problem zu diagnostizieren.

- Klicken Sie **Ausnahmedateien aktivieren** oder **Ausnahmedateien deaktivieren** um das Speichern von Ausnahmedateien zu aktivieren oder zu deaktivieren.

# Netzwerk-Einstellungen

Der Abschnitt Netzwerkeinstellungen enthält die folgenden konfigurierbaren Netzwerkverbindungseinstellungen.

**Konnektivität**

Konfigurieren Sie Netzwerkverbindungen.

**SSL Zertifikat**

Generieren Sie ein selbstsigniertes Zertifikat und laden Sie es hoch.

**Benachrichtigungen**

Richten Sie Warnmeldungen per E-Mail und SNMP-Traps ein.

Die Trace-Appliance verfügt über zwei 10/100/1000BaseT-Netzwerkanschlüsse und vier 10-GbE-SFP+-Netzwerkanschlüsse. Standardmäßig ist der Gb3-Port als Management-Port konfiguriert und erfordert eine IP-Adresse. Port 5 ist die Standard-Monitor- (oder Capture-) Schnittstelle.

Bevor Sie mit der Konfiguration der Netzwerkeinstellungen beginnen, stellen Sie sicher, dass ein Netzwerk-Patchkabel den Gb3-Port der Trace-Appliance mit dem Verwaltungsnetzwerk verbindet. Weitere Informationen zur Installation einer Trace-Appliance finden Sie in der Leitfaden zur Bereitstellung der ExtraHop Trace-Appliance oder kontaktieren ExtraHop-Unterstützung für Hilfe.

Spezifikationen, Installationsanleitungen und weitere Informationen zu Ihrer Appliance finden Sie in der vollständigen ExtraHop-Dokumentation unter docs.extrahop.com.

## Stellen Sie eine Verbindung zu ExtraHop Cloud Services her

ExtraHop Cloud Services bietet Zugriff auf die Cloud-basierten Dienste von ExtraHop über eine verschlüsselte Verbindung. Die Dienste, mit denen Sie verbunden sind, werden durch Ihre Systemlizenz bestimmt.

Nachdem die Verbindung hergestellt wurde, werden Informationen zu den verfügbaren Diensten auf der Seite ExtraHop Cloud Services angezeigt.

- Durch das Teilen von Daten mit dem ExtraHop Machine Learning Service können Sie Funktionen aktivieren , die das ExtraHop-System und Ihre Benutzererfahrung verbessern.
  - Aktivieren Sie den AI-Suchassistenten, um Geräte mit Benutzeraufforderungen in natürlicher Sprache zu finden, die zur Produktverbesserung mit ExtraHop Cloud Services geteilt werden. Sehen Sie die Häufig gestellte Fragen zum AI-Suchassistenten für weitere Informationen.
  - Melden Sie sich für Expanded Threat Intelligence an, damit der Machine Learning Service Daten wie IP-Adressen und Hostnamen anhand der von CrowdStrike bereitgestellten Bedrohungsinformationen, gutartigen Endpunkten und anderen Informationen zum Netzwerkverkehr überprüfen kann. Sehen Sie die Häufig gestellte Fragen zu erweiterten Bedrohungsinformationen für weitere Informationen.
  - Tragen Sie Daten wie Datei-Hashes und externe IP-Adressen zur Collective Threat Analysis bei, um die Erkennungsgenauigkeit zu verbessern. Sehen Sie die Häufig gestellte Fragen zur kollektiven Gefahrenanalyse für weitere Informationen.
- Der ExtraHop Update Service ermöglicht automatische Aktualisierungen von Ressourcen auf dem ExtraHop-System, wie z. B. Ransomware-Paketen.
- Mit ExtraHop Remote Access können Sie Mitgliedern des ExtraHop-Account-Teams und dem ExtraHop-Support erlauben, sich mit Ihrem ExtraHop-System zu verbinden, um Hilfe bei der Konfiguration zu erhalten. Sehen Sie die Häufig gestellte Fragen zum Fernzugriff für weitere Informationen über Benutzer mit Fernzugriff.

**Video:** Sehen Sie sich die entsprechende Schulung an: Stellen Sie eine Verbindung zu ExtraHop Cloud Services her

**Bevor Sie beginnen**

- Reveal (x) 360-Systeme werden automatisch mit den ExtraHop Cloud Services verbunden. Möglicherweise müssen Sie jedoch Zugriff über Netzwerkfirewalls zulassen.
- Sie müssen die entsprechende Lizenz auf dem ExtraHop-System anwenden, bevor Sie eine Verbindung zu ExtraHop Cloud Services herstellen können. Sehen Sie die Häufig gestellte Fragen zur Lizenz für weitere Informationen.
- Sie müssen eingerichtet haben oder System- und Zugriffsadministrationsrechte um auf die Administrationseinstellungen zuzugreifen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Netzwerkeinstellungen auf **ExtraHop Cloud-Dienste** .
3. Klicken Sie **Allgemeine Geschäftsbedingungen** um den Inhalt zu lesen.
4. Lesen Sie die Allgemeinen Geschäftsbedingungen und aktivieren Sie dann das Kontrollkästchen.
5. Klicken Sie **Stellen Sie eine Verbindung zu ExtraHop Cloud Services her**.

   Nachdem Sie eine Verbindung hergestellt haben, wird die Seite aktualisiert und zeigt Status- und Verbindungsinformationen für jeden Dienst an.
6. Optional: Wählen Sie im Abschnitt Machine Learning Service eine oder mehrere erweiterte Funktionen aus:
   - Aktiviere den AI Search Assistant, indem du auswählst **Ich bin damit einverstanden, den KI-Suchassistenten zu aktivieren und Suchanfragen in natürlicher Sprache an ExtraHop Cloud Services zu senden**. (NDR-Modul erforderlich)
   - Aktivieren Sie Expanded Threat Intelligence, indem Sie **Ich bin damit einverstanden, IP-Adressen, Domainnamen, Hostnamen, Datei-Hashes und URLs an ExtraHop Cloud Services zu senden**.
   - Aktivieren Sie die kollektive Bedrohungsanalyse, indem Sie **Ich bin damit einverstanden, Domainnamen, Hostnamen, Datei-Hashes und externe IP-Adressen zu ExtraHop Cloud Services beizutragen**.

Wenn die Verbindung fehlschlägt, liegt möglicherweise ein Problem mit Ihren Firewallregeln vor.

## Konfigurieren Sie Ihre Firewall-Regeln

Wenn Ihr ExtraHop-System in einer Umgebung mit einer Firewall eingesetzt wird, müssen Sie den Zugriff auf ExtraHop Cloud Services öffnen. Für Reveal (x) 360-Systeme, die mit selbstverwalteten Systemen verbunden sind Sensoren, müssen Sie auch den Zugang zum ExtraHop Cloud Recordstore öffnen.

### Offener Zugang zu Cloud-Diensten

Für den Zugriff auf ExtraHop Cloud Services benötigen Sie Sensoren muss in der Lage sein, DNS-Abfragen für *.extrahop.com aufzulösen und über die IP-Adresse, die Ihrer entspricht, auf TCP 443 (HTTPS) zuzugreifen Sensor Lizenz:

- 35.161.154.247 (Portland, Vereinigte Staaten von Amerika)
- 54.66.242.25 (Sydney, Australien)
- 52.59.110.168 (Frankfurt, Deutschland)

### Offener Zugang zu Cloud Recordstore

Für den Zugriff auf den ExtraHop Cloud Recordstore benötigen Sie Sensoren muss in der Lage sein, auf ausgehendes TCP 443 (HTTPS) zu diesen vollqualifizierten Domainnamen zuzugreifen:

- `bigquery.googleapis.com`
- `bigquerystorage.googleapis.com`

- `oauth2.googleapis.com`
- `www.googleapis.com`
- `www.mtls.googleapis.com`
- `iamcredentials.googleapis.com`

Sie können auch die öffentlichen Leitlinien von Google zu folgenden Themen lesen Berechnung möglicher IP-Adressbereiche für googleapis.com.

Zusätzlich zur Konfiguration des Zugriffs auf diese Domänen müssen Sie auch die globale Proxyserver-Einstellungen.

## Stellen Sie über einen Proxy eine Verbindung zu ExtraHop Cloud Services her

Wenn Sie keine direkte Internetverbindung haben, können Sie versuchen, über einen expliziten Proxy eine Verbindung zu ExtraHop Cloud Services herzustellen.

**Bevor Sie beginnen**
Überprüfen Sie, ob Ihr Proxyanbieter so konfiguriert ist, dass er Machine-in-the-Middle (MITM) ausführt, wenn SSH über HTTP CONNECT zu localhost:22 getunnelt wird. ExtraHop Cloud Services stellt einen verschlüsselten inneren SSH-Tunnel bereit, sodass der Datenverkehr für die MITM-Inspektion nicht sichtbar ist. Es wird empfohlen, eine Sicherheitsausnahme zu erstellen und die MITM-Prüfung für diesen Datenverkehr zu deaktivieren.

**Wichtig:** Wenn Sie MITM auf Ihrem Proxy nicht deaktivieren können, müssen Sie die Zertifikatsvalidierung in der Konfigurationsdatei des ExtraHop-Systems deaktivieren, in der das ExtraHop-System ausgeführt wird. Weitere Informationen finden Sie unter Zertifikatsvalidierung umgehen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerk-Einstellungen Abschnitt, klicken **Konnektivität**.
3. Klicken **ExtraHop Cloud-Proxy aktivieren**.
4. Geben Sie den Hostnamen für Ihren Proxyserver ein, z. B. `Proxyhost`.
5. Geben Sie den Port für Ihren Proxyserver ein, z. B. `8080`.
6. Optional: Geben Sie bei Bedarf einen Benutzernamen und ein Passwort für Ihren Proxyserver ein.
7. Klicken **Speichern**.

## Zertifikatsvalidierung umgehen

Einige Umgebungen sind so konfiguriert, dass verschlüsselter Datenverkehr das Netzwerk nicht ohne Überprüfung durch ein Gerät eines Drittanbieters verlassen kann. Dieses Gerät kann als SSL/TLS-Endpunkt fungieren, der den Datenverkehr entschlüsselt und erneut verschlüsselt, bevor die Pakete an ExtraHop Cloud Services gesendet werden.

Wenn eine Appliance über einen Proxyserver eine Verbindung zu ExtraHop Cloud Services herstellt und die Zertifikatsvalidierung fehlschlägt, deaktivieren Sie die Zertifikatsvalidierung und versuchen Sie erneut, die Verbindung herzustellen. Die durch die Authentifizierung und Verschlüsselung des ExtraHop-Systems gebotene Sicherheit stellt sicher, dass die Kommunikation zwischen Geräten und ExtraHop Cloud-Diensten nicht abgefangen werden kann.

**Hinweis:** Das folgende Verfahren setzt Vertrautheit mit der Änderung der laufenden ExtraHop-Konfigurationsdatei voraus.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Geräteeinstellungen Abschnitt, klicken **Config ausführen**.
3. Klicken **Konfiguration bearbeiten**.

4. Fügen Sie die folgende Zeile am Ende der laufenden Konfigurationsdatei hinzu:

```
"hopcloud": { "verify_outer_tunnel_cert": false }
```

5. Klicken **Aktualisieren**.
6. Klicken **Änderungen anzeigen und speichern**.
7. Überprüfen Sie die Änderungen und klicken Sie auf **Speichern**.
8. Klicken **Erledigt**.

## Konnektivität

Die Seite Konnektivität enthält Steuerelemente für Ihre Appliance-Verbindungen und Netzwerkeinstellungen.

**Status der Schnittstelle**

Auf physischen Appliances wird ein Diagramm der Schnittstellenverbindungen angezeigt, das basierend auf dem Portstatus dynamisch aktualisiert wird.

- Der blaue Ethernet-Port dient der Verwaltung
- Ein schwarzer Ethernet-Port weist auf einen lizenzierten und aktivierten Port hin, der derzeit ausgefallen ist.
- Ein grüner Ethernet-Port zeigt einen aktiven, verbundenen Port an
- Ein grauer Ethernet-Port weist auf einen deaktivierten oder nicht lizenzierten Port hin.

**Netzwerkeinstellungen**

- Klicken Sie **Einstellungen ändern** um einen Hostnamen für Ihre ExtraHop-Appliance hinzuzufügen oder DNS-Server hinzuzufügen.

**Proxy-Einstellungen**

- Aktiviere eine globaler Proxy um eine Verbindung zu einer ExtraHop Command-Appliance herzustellen
- Aktiviere eine Cloud-Proxy um eine Verbindung zu ExtraHop Cloud Services herzustellen

**Einstellungen für die Bond-Schnittstelle**

- Erstellen Sie eine Bond-Schnittstelle um mehrere Schnittstellen zu einer logischen Schnittstelle mit einer einzigen IP-Adresse zu verbinden.

**Schnittstellen**

Sehen und konfigurieren Sie Ihre Verwaltungs- und Überwachungsoberflächen. Klicken Sie auf eine beliebige Schnittstelle, um die Einstellungsoptionen anzuzeigen.

- Erfassen Sie den Datenverkehr von NetFlow- und sFlow-Geräten
- Paketweiterleitung mit RPCAP

**Netskope-Einstellungen**

- Netskope-Paketaufnahme aktivieren auf Ihrem Sensor, um Geräte über eine Netskope-Integration zu erkennen und zu überwachen.

### Eine Schnittstelle konfigurieren

1. In der Netzwerkeinstellungen Abschnitt, klicken Sie **Konnektivität**.
2. In der Schnittstellen Abschnitt, klicken Sie auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
3. Auf dem Netzwerkeinstellungen für die Schnittstelle *<interface number>* Seite, wählen Sie eine der folgenden Optionen aus der **Schnittstellen-Modus** Dropdownliste:

| Option | Beschreibung |
|---|---|
| **Deaktiviert** | Die Schnittstelle ist deaktiviert. |

| Option | Beschreibung |
| --- | --- |
| **Überwachung (nur Empfang)** | Überwacht den Netzwerkverkehr. |
| **Verwaltung** | Verwaltet den ExtraHop-Sensor. |
| **Management + Flow-Ziel** | Verwaltet den ExtraHop-Sensor und erfasst den Verkehr, der von einem weitergeleitet wird Flussnetz.<br>**Hinweis:** Wenn du aktivierst NetFlow auf dem EDA 1100 müssen Sie Interface 2 deaktivieren. Diese Sensoren können NetFlow und Kabeldaten nicht gleichzeitig verarbeiten. |
| **Verwaltung + RPCAP/ERSPAN/VXLAN/GENEVE Target** | Verwaltet den ExtraHop-Sensor und erfasst den von einem Paketweiterleiter weitergeleiteten Verkehr, ERSPAN*, VXLAN** oder GENEVE***.<br>Während die 10-GbE-Management+-Erfassungsschnittstellen auf diesem Sensor Verwaltungsfunktionen mit Geschwindigkeiten von 10 Gbit/s ausführen können, ist die Verarbeitung von Datenverkehr wie ERSPAN, VXLAN und GENEVE auf 1 Gbit/s begrenzt.<br>**Hinweis:** In Umgebungen mit asymmetrischem Routing neben den Hochleistungsschnittstellen gelangen Ping-Antworten möglicherweise nicht an den Absender zurück. |
| **Leistungsstarkes ERSPAN/VXLAN/GENEVE-Ziel** | Erfasst den von ERSPAN*, VXLAN** oder GENEVE*** weitergeleiteten Datenverkehr. Dieser Schnittstellenmodus ermöglicht es dem Port, mehr als 1 Gbit/s zu verarbeiten. Stellen Sie diesen Schnittstellenmodus ein, wenn der ExtraHop-Sensor über einen 10-GbE-Anschluss verfügt. Für diesen Schnittstellenmodus müssen Sie nur eine IPv4-Adresse konfigurieren. |

*Das ExtraHop-System unterstützt die folgenden ERSPAN-Implementierungen:

- ERSPAN Typ I
- ERSPAN Typ II
- ERSPAN Typ III
- Transparentes Ethernet-Bridging. ERSPAN-ähnliche Kapselung, die häufig in virtuellen Switch-Implementierungen wie dem VMware VDS und Open vSwitch zu finden ist.

**Virtual Extensible LAN (VXLAN) -Pakete werden auf dem UDP-Port 4789 empfangen.

***Generic Network Virtualization Encapsulation (GENEVE) -Pakete werden auf dem UDP-Port 6081 empfangen. Informationen zur Konfiguration von Geneve-gekapseltem Datenverkehr, der von einem AWS Gateway Load Balancer (GWLB) weitergeleitet wird, der als VPC Traffic Mirroring-Ziel fungiert, finden Sie in der AWS-Dokumentation.

**Hinweis:** Für Amazon Web Services (AWS) -Bereitstellungen mit einer Schnittstelle müssen Sie auswählen **Verwaltung + RPCAP/ERSPAN/VXLAN/GENEVE Target** für Interface 1. Wenn Sie zwei Schnittstellen konfigurieren, müssen Sie auswählen **Verwaltung +**

**RPCAP/ERSPAN/VXLAN/GENEVE Target** für Interface 1 und **Verwaltung + RPCAP/ERSPAN/VXLAN/GENEVE Target** für Interface 2.

**Hinweis:** Bei Azure-Bereitstellungen unterstützen einige Instanzen, auf denen ältere NICs ausgeführt werden, möglicherweise den Hochleistungs-ERSPAN-/VXLAN-/GENEVE-Zielmodus nicht.

4. Optional: Wählen Sie eine Schnittstellengeschwindigkeit aus. **Automatisch aushandeln** ist standardmäßig ausgewählt. Sie sollten jedoch manuell eine Geschwindigkeit auswählen, wenn sie von Ihrem Sensor, Netzwerk-Transceiver und Netzwerk-Switch unterstützt wird.
   - **Automatisch aushandeln**
   - **10 Gbit/s**
   - **25 Gbit/s**
   - **40 Gbit/s**
   - **100 Gbit/s**

   **Wichtig:** Wenn Sie die Schnittstellengeschwindigkeit ändern auf **Automatisch aushandeln**, Sie müssen den Sensor möglicherweise neu starten, bevor die Änderung wirksam wird.
5. Optional: Wählen Sie einen FEC-Typ (Forward Error Correction). Wir empfehlen Auto-Negotiate, das für die meisten Umgebungen optimal ist.

   • **Automatisch aushandeln:** Aktiviert automatisch entweder RS-FEC oder Firecode FEC oder deaktiviert FEC basierend auf den Funktionen der verbundenen Schnittstellen.

   • **RS-FEC:** Aktiviert immer Reed-Solomon FEC.

   • **Firecode:** Aktiviert immer Firecode (FC) FEC, auch bekannt als BaseR FEC.

   • **Deaktiviert:** Deaktiviert FEC.
6. DHCPv4 ist standardmäßig aktiviert. Wenn Ihr Netzwerk DHCP nicht unterstützt, können Sie das löschen DHCPv4 Kontrollkästchen, um DHCP zu deaktivieren und dann eine statische IP-Adresse, eine Netzmaske und ein Standard-Gateway einzugeben.

   **Hinweis:** Nur eine Schnittstelle sollte mit einem Standard-Gateway konfiguriert werden. Statische Routen konfigurieren wenn Ihr Netzwerk das Routing über mehrere Gateways erfordert.
7. Konfigurieren Sie den TCP-Health-Check-Port. Diese Einstellung ist nur für Hochleistungsschnittstellen konfigurierbar und wird benötigt, wenn GENEVE-Datenverkehr von einem AWS Gateway Load Balancer (GWLB) aufgenommen wird. Der Wert der Portnummer muss mit dem in AWS konfigurierten Wert übereinstimmen. Weitere Informationen finden Sie unter Weiterleiten von geneve-gekapseltem Datenverkehr von einem AWS Gateway Load Balancer.
8. Optional: Aktiviere IPv6.

   Weitere Hinweise zur Konfiguration von IPv6 finden Sie unter IPv6 für eine Schnittstelle aktivieren.
9. Optional: Fügen Sie manuell Routen hinzu.
10. Klicken Sie **Speichern**.

**Schnittstellendurchsatz**
ExtraHop Sensor Die Modelle EDA 6100, EDA 8100 und EDA 9100 sind für die Erfassung von Datenverkehr ausschließlich über 10GbE-Ports optimiert.

Die Aktivierung der 1-GbE-Schnittstellen für die Überwachung des Datenverkehrs kann sich je nach ExtraHop auf die Leistung auswirken Sensor. Sie können diese zwar optimieren Sensoren Um den Datenverkehr sowohl an den 10-GbE-Ports als auch an den drei 1-GbE-Ports ohne Verwaltungszugang gleichzeitig zu erfassen, empfehlen wir, dass Sie sich an den ExtraHop-Support wenden, um Unterstützung zu erhalten, um einen verringerten Durchsatz zu vermeiden.

**Hinweis:** Die Sensoren EDA 6200, EDA 8200, EDA 9200 und EDA 10200 sind nicht anfällig für einen reduzierten Durchsatz, wenn Sie 1GbE-Schnittstellen für die Überwachung des Datenverkehrs aktivieren.

| ExtraHop Fühler | Durchsatz | Einzelheiten |
|---|---|---|
| VON 910 | Standarddurchsatz von 40 Gbit/s | Wenn die 1-GbE-Schnittstellen, die nicht zur Verwaltung gehören, deaktiviert sind, können Sie bis zu vier der 10-GbE-Schnittstellen für einen kombinierten Durchsatz von bis zu 40 Gbit/s verwenden. |
| VON 810 | Standarddurchsatz von 20 Gbit/s | Wenn die 1-GbE-Schnittstellen, die nicht zur Verwaltung gehören, deaktiviert sind, können Sie entweder eine oder beide der 10-GbE-Schnittstellen verwenden, um einen kombinierten Durchsatz von bis zu 20 Gbit/s zu erzielen. |
| VON 610 | Standarddurchsatz von 10 Gbit/s | Wenn die 1-GbE-Schnittstellen, die nicht zur Verwaltung gehören, deaktiviert sind, beträgt der maximale kombinierte Gesamtdurchsatz 10 Gbit/s. |
| VON 310 | Standarddurchsatz von 3 Gbit/s | Keine 10GbE-Schnittstelle |
| VON 100 | Standarddurchsatz von 1 Gbit/s | Keine 10GbE-Schnittstelle |

**Stellen Sie eine statische Route ein**

**Bevor Sie beginnen**
Sie müssen DHCPv4 deaktivieren, bevor Sie eine statische Route hinzufügen können.

1. Auf dem Oberfläche bearbeiten Seite, stellen Sie sicher, dass **IPv4-Adresse** und **Netzmaske** Felder sind vollständig und gespeichert, und klicken Sie auf **Routen bearbeiten**.
2. In der Route hinzufügen Abschnitt, geben Sie einen Netzwerkadressbereich in CIDR-Notation in das **Netzwerk** Feld und IPv4-Adresse in der **Über IP** Feld und dann klicken **Hinzufügen**.
3. Wiederholen Sie den vorherigen Schritt für jede Route, die Sie hinzufügen möchten.
4. klicken **Speichern**.

**IPv6 für eine Schnittstelle aktivieren**

1. In der Netzwerk-Einstellungen Abschnitt, klicken **Konnektivität**.
2. In der Schnittstellen Klicken Sie im Abschnitt auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
3. Auf dem Netzwerkeinstellungen für die Schnittstelle *<interface number>* Seite, wählen **IPv6 aktivieren**. Die IPv6-Konfigurationsoptionen werden unten angezeigt **IPv6 aktivieren**.
4. Optional: Konfigurieren Sie IPv6-Adressen für die Schnittstelle.
   - Um IPv6-Adressen automatisch über DHCPv6 zuzuweisen, wählen Sie **DHCPv6 aktivieren**.

     **Hinweis:** Wenn diese Option aktiviert ist, wird DHCPv6 zur Konfiguration der DNS-Einstellungen verwendet.
   - Um IPv6-Adressen automatisch über die automatische Konfiguration von statusfreien Adressen zuzuweisen, wählen Sie eine der folgenden Optionen aus Automatische Konfiguration von statusfreien Adressen Liste:

     **MAC-Adresse verwenden**

     Konfiguriert die Appliance für die automatische Zuweisung von IPv6-Adressen auf der Grundlage der MAC-Adresse der Appliance.

**Verwenden Sie eine stabile Privatadresse**

Konfiguriert die Appliance so, dass sie automatisch private IPv6-Adressen zuweist, die nicht auf Hardwareadressen basieren. Diese Methode ist in RFC 7217 beschrieben.

- Um manuell eine oder mehrere statische IPv6-Adressen zuzuweisen, geben Sie die Adressen in das Feld Statische IPv6-Adressen Feld.

5. Um die Appliance in die Lage zu versetzen, Informationen zum rekursiven DNS-Server (RDNSS) und zur DNS-Suchliste (DNSSL) entsprechend den Routerankündigungen zu konfigurieren, wählen Sie **RDNSS/ DNSSL**.
6. klicken **Speichern**.

## Globaler Proxyserver

Wenn Ihre Netzwerktopologie einen Proxyserver benötigt, damit Ihr ExtraHop-System entweder mit einem Konsole oder mit anderen Geräten außerhalb des lokalen Netzwerks können Sie Ihr ExtraHop-System so einrichten, dass es eine Verbindung zu einem Proxyserver herstellt, den Sie bereits in Ihrem Netzwerk haben. Für den globalen Proxyserver ist keine Internetverbindung erforderlich.

**Hinweis:** Pro ExtraHop-System kann nur ein globaler Proxyserver konfiguriert werden.

Füllen Sie die folgenden Felder aus und klicken Sie auf **Speichern** um einen globalen Proxy zu aktivieren.

- **Hostname :** Der Hostname oder die IP-Adresse für Ihren globalen Proxyserver.
- **Hafen :** Die Portnummer für Ihren globalen Proxyserver.
- **Nutzername :** Der Name eines Benutzers, der privilegierten Zugriff auf Ihren globalen Proxyserver hat.
- **Passwort :** Das Passwort für den oben angegebenen Benutzer.

## ExtraHop Cloud-Proxy

Wenn Ihr ExtraHop-System nicht über eine direkte Internetverbindung verfügt, können Sie über einen Proxy-Server, der speziell für die Konnektivität von ExtraHop-Cloud-Diensten vorgesehen ist, eine Verbindung zum Internet herstellen . Pro System kann nur ein Proxy konfiguriert werden.

Füllen Sie die folgenden Felder aus und klicken Sie auf **Speichern** um einen Cloud-Proxy zu aktivieren.

- **Hostname :** Der Hostname oder die IP-Adresse für Ihren Cloud-Proxyserver.
- **Hafen :** Die Portnummer für Ihren Cloud-Proxyserver.
- **Nutzername :** Der Name eines Benutzers, der Zugriff auf Ihren Cloud-Proxyserver hat.
- **Passwort :** Das Passwort für den oben angegebenen Benutzer.

## Bond-Schnittstellen

Sie können mehrere Schnittstellen auf Ihrem ExtraHop-System zu einer einzigen logischen Schnittstelle verbinden, die eine IP-Adresse für die kombinierte Bandbreite der Mitgliedsschnittstellen hat. Verbindungsschnittstellen ermöglichen einen größeren Durchsatz mit einer einzigen IP-Adresse. Diese Konfiguration wird auch als Link-Aggregation, Port-Channeling, Linkbündelung, Ethernet-/Netzwerk-/NIC-Bonding oder NIC-Teaming bezeichnet. Bond-Schnittstellen können nicht in den Überwachungsmodus versetzt werden.

**Hinweis:** Wenn Sie die Einstellungen der Bond-Schnittstelle ändern, verlieren Sie die Konnektivität zu Ihrem ExtraHop-System. Sie müssen Änderungen an Ihrer Netzwerk-Switch-Konfiguration vornehmen, um die Konnektivität wiederherzustellen. Die erforderlichen Änderungen hängen von Ihrem Switch ab. Wenden Sie sich an den ExtraHop-Support, um Unterstützung zu erhalten, bevor Sie eine Bond-Schnittstelle erstellen.

- Bonding ist nur auf Management- oder Management +-Schnittstellen konfigurierbar.
- Port-Channeling auf den ExtraHop-Sensoren werden keine Anschlüsse zur Verkehrsüberwachung unterstützt.

Schnittstellen, die als Mitglieder einer Bond-Schnittstelle ausgewählt wurden, sind nicht mehr unabhängig konfigurierbar und werden angezeigt als Deaktiviert (Bond-Mitglied) im Abschnitt Schnittstellen der Seite Konnektivität. Nachdem eine Bond-Schnittstelle erstellt wurde, können Sie keine weiteren Mitglieder hinzufügen oder vorhandene Mitglieder löschen. Die Bond-Schnittstelle muss zerstört und neu erstellt werden.

- Erstellen Sie eine Bond-Schnittstelle
- Modifizieren Sie eine Bond-Schnittstelle
- Zerstöre eine Bond-Schnittstelle

**Erstellen Sie eine Bond-Schnittstelle**
Sie können eine Bond-Schnittstelle mit mindestens einem Schnittstellenmitglied und bis zu der Anzahl von Mitgliedern erstellen, die für die Bindung verfügbar sind.

1. klicken **Bond-Schnittstelle erstellen**.
2. Konfigurieren Sie die folgenden Optionen:

   • **Mitglieder:** Aktivieren Sie das Kontrollkästchen neben jeder Schnittstelle, die Sie in das Bonding einbeziehen möchten. Es werden nur Ports angezeigt, die derzeit für eine Bond-Mitgliedschaft verfügbar sind.

   • **Einstellungen übernehmen von:** Wählen Sie die Schnittstelle mit den Einstellungen aus, die Sie auf die Bond-Schnittstelle anwenden möchten. Die Einstellungen für alle nicht ausgewählten Schnittstellen gehen verloren.

   • **Art der Anleihe:** Geben Sie an, ob eine statische oder eine dynamische Verbindung über IEEE 802.3ad Link Aggregation (LACP) erstellt werden soll.

   • **Hash-Richtlinie:** Geben Sie die Hash-Richtlinie an. Die **Schicht 3+4** Die Richtlinie gleicht die Verteilung des Datenverkehrs gleichmäßiger auf die Schnittstellen aus. Diese Richtlinie entspricht jedoch nicht vollständig den 802.3ad-Standards. Die **Schicht 2+3** Die Richtlinie verteilt den Datenverkehr weniger gleichmäßig und entspricht den 802.3ad-Standards.
3. klicken **Erstellen**.

Aktualisieren Sie die Seite, um die anzuzeigen Bond-Schnittstellen Abschnitt. Jedes Bond-Interface-Mitglied, dessen Einstellungen nicht in der **Einstellungen übernehmen von** Drop-down-Menüs werden angezeigt als **Deaktiviert ( Bondmitglied)** in der Schnittstellen Abschnitt.

**Einstellungen der Bond-Schnittstelle ändern**
Nachdem eine Bond-Schnittstelle erstellt wurde, können Sie die meisten Einstellungen so ändern, als ob es sich bei der Bond-Schnittstelle um eine einzelne Schnittstelle handeln würde.

1. In der Netzwerk-Einstellungen Abschnitt, klicken **Konnektivität**.
2. In der Bond-Schnittstellen Klicken Sie im Abschnitt auf die Bond-Schnittstelle, die Sie ändern möchten.
3. Auf dem Netzwerkeinstellungen für Bond Interface Seite <interface number>, ändern Sie die folgenden Einstellungen nach Bedarf:

   • **Mitglieder :** Die Schnittstellenmitglieder der Bond-Schnittstelle. Mitglieder können nicht geändert werden, nachdem eine Bond-Schnittstelle erstellt wurde. Wenn Sie die Mitglieder ändern müssen, müssen Sie die Bond-Schnittstelle zerstören und neu erstellen.

   • **Bond-Modus:** Geben Sie an, ob eine statische oder eine dynamische Verbindung über IEEE 802.3ad Link Aggregation (LACP) erstellt werden soll.

   • **Schnittstellenmodus :** Der Modus der Bond-Mitgliedschaft. Eine Bond-Schnittstelle kann sein **Verwaltung** oder **Management+RPCAP/ERSPAN-Ziel** nur.

   • **DHCPv4 aktivieren :** Wenn DHCP aktiviert ist, wird automatisch eine IP-Adresse für die Bond-Schnittstelle abgerufen.

   • **Hash-Richtlinie:** Geben Sie die Hash-Richtlinie an. Die **Schicht 3+4** Die Richtlinie sorgt für eine gleichmäßigere Verteilung des Datenverkehrs auf die Schnittstellen, entspricht jedoch nicht vollständig

den 802.3ad-Standards. Die **Schicht 2+3** Die Richtlinie verteilt den Datenverkehr weniger gleichmäßig, entspricht jedoch den 802.3ad-Standards.

- **IPv4-Adresse :** Die statische IP-Adresse der Bond-Schnittstelle. Diese Einstellung ist nicht verfügbar, wenn DHCP aktiviert ist.
- **Netzmaske :** Die Netzwerk-Netzmaske für die Bond-Schnittstelle.
- **Tor :** Die IP-Adresse des Netzwerk-Gateways.
- **Strecken :** Die statischen Routen für die Bond-Schnittstelle. Diese Einstellung ist nicht verfügbar, wenn DHCP aktiviert ist.
- **IPv6 aktivieren :** Aktivieren Sie die Konfigurationsoptionen für IPv6.

4. klicken **Speichern**.

**Zerstöre eine Bond-Schnittstelle**
Wenn eine Bond-Schnittstelle zerstört wird, kehren die einzelnen Schnittstellenmitglieder der Bond-Schnittstelle zur unabhängigen Schnittstellenfunktionalität zurück. Eine Mitgliedsschnittstelle wird ausgewählt, um die Schnittstelleneinstellungen für die Bond-Schnittstelle beizubehalten, und alle anderen Mitgliedsschnittstellen sind deaktiviert. Wenn keine Mitgliedsschnittstelle ausgewählt wurde, um die Einstellungen beizubehalten, gehen die Einstellungen verloren und alle Mitgliedsschnittstellen sind deaktiviert.

1. In der Netzwerk-Einstellungen Abschnitt, klicken **Konnektivität**.
2. In der Bereich Bond-Schnittstellen, klicken Sie auf das Rote **X** neben der Schnittstelle, die Sie zerstören möchten.
3. Auf dem Zerstöre die Bond-Schnittstelle <interface number>Seite, wählen Sie die Mitgliederschnittstelle aus, auf die Sie die Einstellungen der Bond-Schnittstelle verschieben möchten. Nur die Mitgliedsschnittstelle, die ausgewählt wurde, um die Bond-Schnittstelleneinstellungen beizubehalten, bleibt aktiv, und alle anderen Mitgliedsschnittstellen sind deaktiviert.
4. klicken **Zerstören**.

## Benachrichtigungen

Das ExtraHop-System kann Benachrichtigungen über konfigurierte Alarme per E-Mail, SNMP-Traps und Syslog-Exporte an Remote-Server senden. Wenn eine E-Mail-Benachrichtigungsgruppe angegeben ist, werden E-Mails an die Gruppen gesendet, die der Alarm zugewiesen sind.

### E-Mail-Einstellungen für Benachrichtigungen konfigurieren

Sie müssen einen E-Mail-Server und einen Absender konfigurieren, bevor das ExtraHop-System Warnmeldungen oder geplante Berichte senden kann.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken Sie **Benachrichtigungen**.
3. klicken **E-Mail-Server und Absender**.
4. In der SMTP-Server In diesem Feld geben Sie die IP-Adresse oder den Hostnamen für den SMTP-Mailserver für ausgehende E-Mails ein. Der SMTP-Server sollte der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse eines Postausgangsservers sein, auf den vom ExtraHop-System aus zugegriffen werden kann. Wenn der DNS-Server eingerichtet ist, kann der SMTP-Server ein FQDN sein, andernfalls müssen Sie eine IP-Adresse eingeben.
5. In der SMTP-Anschluss In diesem Feld geben Sie die Portnummer für die SMTP-Kommunikation ein. Port 25 ist der Standardwert für SMTP und Port 465 ist der Standardwert für SSL/TLS-verschlüsseltes SMTP.
6. Wählen Sie in der Dropdownliste Verschlüsselung eine der folgenden Verschlüsselungsmethoden aus:

- **Keine**. Die SMTP-Kommunikation ist nicht verschlüsselt.
- **SSL/TLS**. Die SMTP-Kommunikation wird über das Secure Socket Layer/Transport Layer Security-Protokoll verschlüsselt.
- **STARTTLS**. Die SMTP-Kommunikation wird über STARTTLS verschlüsselt.

7. In der Adresse des Absenders der Warnung Feld, geben Sie die E-Mail-Adresse für den Absender der Benachrichtigung ein.

   **Hinweis:** Die angezeigte Absenderadresse wird möglicherweise vom SMTP-Server geändert. Wenn Sie beispielsweise über einen Google SMTP-Server senden, wird die Absender-E-Mail in den für die Authentifizierung angegebenen Benutzernamen geändert, anstatt in die ursprünglich eingegebene Absenderadresse.

8. Optional: Wählen Sie die SSL-Zertifikate validieren Kontrollkästchen, um die Zertifikatsvalidierung zu aktivieren. Wenn Sie diese Option auswählen, wird das Zertifikat auf dem Remote-Endpunkt anhand der Stammzertifikatsketten validiert, die vom Trusted Certificates Manager angegeben wurden. Beachten Sie, dass der Hostname, der in dem vom SMTP-Server vorgelegten Zertifikat angegeben ist, mit dem in Ihrer SMTP-Konfiguration angegebenen Hostnamen übereinstimmen muss. Andernfalls schlägt die Überprüfung fehl. Darüber hinaus müssen Sie auf der Seite Vertrauenswürdige Zertifikate konfigurieren, welchen Zertifikaten Sie vertrauen möchten. Weitere Informationen finden Sie unter Fügen Sie Ihrem ExtraHop-System ein vertrauenswürdiges Zertifikat hinzu
9. In der Absenderadresse melden In diesem Feld geben Sie die E-Mail-Adresse ein, die für den Versand der Nachricht verantwortlich ist. Dieses Feld gilt nur, wenn geplante Berichte von einer Command-Appliance oder Reveal (x) 360 gesendet werden.
10. Wählen Sie die SMTP-Authentifizierung aktivieren Markieren Sie das Kontrollkästchen und geben Sie dann die Anmeldedaten für das SMTP-Server-Setup in das Nutzername und Passwort Felder.
11. Optional: klicken **Einstellungen testen**, geben Sie Ihre E-Mail-Adresse ein, und klicken Sie dann auf **Senden**. Sie sollten eine E-Mail-Nachricht mit dem Betreff erhalten `ExtraHop Test Email`.
12. klicken **Speichern**.

**Nächste Schritte**
Nachdem Sie bestätigt haben, dass Ihre neuen Einstellungen erwartungsgemäß funktionieren, speichern Sie Ihre Konfigurationsänderungen durch Systemneustart- und Shutdown-Ereignisse, indem Sie die Running Config-Datei speichern.

## Eine neue E-Mail-Adresse für Benachrichtigungen auf einer Explore- oder Trace-Appliance hinzufügen

Sie können Systemspeicherwarnungen an einzelne Empfänger senden. Benachrichtigungen werden unter den folgenden Bedingungen gesendet:

- Eine physische Festplatte befindet sich in einem heruntergekommenen Zustand.
- Eine physische Festplatte weist eine steigende Anzahl von Fehlern auf.
- (Nur Explore-Appliance) Ein virtuelles Laufwerk befindet sich in einem heruntergestuften Zustand.
- (Nur Explore-Appliance) Ein registrierter Explore-Knoten fehlt im Cluster. Der Knoten ist möglicherweise ausgefallen oder er ist ausgeschaltet.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerk-Einstellungen Abschnitt, klicken **Benachrichtigungen**.
3. Unter Benachrichtigungen, klicken **E-Mail-Adressen**.
4. In der **E-Mail-Adresse** Textfeld, geben Sie die E-Mail-Adresse des Empfängers ein.
5. klicken **Speichern**.

## Konfigurieren Sie die Einstellungen, um Benachrichtigungen an einen SNMP-Manager zu senden

Der Zustand des Netzwerk kann über das Simple Network Management Protocol (SNMP) überwacht werden. SNMP sammelt Informationen, indem es Geräte im Netzwerk abfragt. SNMP-fähige Geräte können auch Warnmeldungen an SNMP-Managementstationen senden. SNMP-Communities definieren die Gruppe , zu der Geräte und Verwaltungsstationen, auf denen SNMP ausgeführt wird, gehören, was angibt, wohin Informationen gesendet werden. Der Community-Name identifiziert die Gruppe.

**Hinweis:** Die meisten Organisationen verfügen über ein etabliertes System zur Erfassung und Anzeige von SNMP-Traps an einem zentralen Ort, der von ihren Betriebsteams überwacht werden kann. Beispielsweise werden SNMP-Traps an einen SNMP-Manager gesendet, und die SNMP-Managementkonsole zeigt sie an.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken Sie **Benachrichtigungen**.
3. Unter Benachrichtigungen, klicken **SNMP**.
4. Auf dem SNMP-Einstellungen Seite, in der **SNMP-Monitor** Feld, geben Sie den Hostnamen für den SNMP-Trap-Empfänger ein.

   Trennen Sie mehrere Hostnamen durch Kommas.
5. In der **SNMP-Gemeinschaft** Feld, geben Sie den SNMP-Community-Namen ein.
6. In der **SNMP-Anschluss** Geben Sie in dieses Feld die SNMP-Portnummer für Ihr Netzwerk ein, die vom SNMP-Agent verwendet wird, um auf den Quellport im SNMP-Manager zu antworten.

   Der Standard-Antwortport ist `162`.
7. Optional: klicken **Einstellungen testen** um zu überprüfen, ob Ihre SNMP-Einstellungen korrekt sind.

   Wenn die Einstellungen korrekt sind, sollten Sie in der SNMP-Protokolldatei auf dem SNMP-Server einen Eintrag sehen, der diesem Beispiel ähnelt, wobei `192.0.2.0` ist die IP-Adresse Ihres ExtraHop-Systems und `192.0.2.255` ist die IP-Adresse des SNMP-Servers:

   Eine ähnliche Antwort wie in diesem Beispiel wird angezeigt:

   ```
   Connection from UDP: [192.0.2.0]:42164->[ 192.0.2.255]:162
   ```
8. Klicken Sie **Speichern**.

### Laden Sie die ExtraHop SNMP MIB herunter

SNMP stellt keine Datenbank mit Informationen bereit, die ein SNMP-überwachtes Netzwerk meldet. SNMP-Informationen werden durch MIBs (Management Information Bases) von Drittanbietern definiert, die die Struktur der gesammelten Daten beschreiben.

Sie können die ExtraHop MIB-Datei aus den Administrationseinstellungen des Systems herunterladen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Gehe zum Netzwerkeinstellungen Abschnitt und klick **Benachrichtigungen**.
3. Unter Benachrichtigungen, klicken **SNMP**.
4. Unter SNMP MIB, klicken Sie auf **ExtraHop SNMP MIB herunterladen**.
   Die Datei wird normalerweise am Standardspeicherort für den Download Ihres Browsers gespeichert.

## Systembenachrichtigungen an einen Remote-Syslog-Server senden

Mit der Syslog-Exportoption können Sie Warnungen von einem ExtraHop-System an jedes Remote-System senden, das Syslog-Eingaben zur Langzeitarchivierung und Korrelation mit anderen Quellen empfängt.

Für jedes ExtraHop-System kann nur ein Remote-Syslog-Server konfiguriert werden.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerk-Einstellungen Abschnitt, klicken **Benachrichtigungen**.
3. Geben Sie im Feld Ziel die IP-Adresse des Remote-Syslog-Servers ein.
4. Wählen Sie im Dropdownmenü Protokoll **TCP** oder **UDP**. Diese Option gibt das Protokoll an, über das die Informationen an Ihren Remote-Syslog-Server gesendet werden.
5. Geben Sie im Feld Port die Portnummer für Ihren Remote-Syslog-Server ein. Standardmäßig ist dieser Wert auf 514 festgelegt.
6. Klicken **Einstellungen testen** um zu überprüfen, ob Ihre Syslog-Einstellungen korrekt sind. Wenn die Einstellungen korrekt sind, sollten Sie in der Syslog-Log-Datei auf dem Syslog-Server einen Eintrag sehen, der dem folgenden ähnelt:

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```
7. Klicken **Speichern**.
8. Optional: Ändern Sie das Format von Syslog-Meldungen.

   Standardmäßig entsprechen Syslog-Meldungen nicht RFC 3164 oder RFC 5424. Sie können Syslog-Meldungen jedoch so formatieren, dass sie konform sind, indem Sie die laufende Konfigurationsdatei ändern.

   a) Klicken **Admin**.
   b) Klicken **Config ausführen (ungespeicherte Änderungen)**.
   c) Klicken **Konfiguration bearbeiten**.
   d) Füge einen Eintrag hinzu unter `syslog_notification` wo der Schlüssel ist `rfc_compliant_format` und der Wert ist entweder `rfc5424` oder `rfc3164`.

      Das `syslog_notification` Der Abschnitt sollte dem folgenden Code ähneln:

      ```
      "syslog_notification": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "rfc_compliant_format": "rfc5424"
      }
      ```
   e) Klicken **Aktualisieren**.
   f) Klicken **Erledigt**.
9. Optional: Ändern Sie die Zeitzone, auf die in den Syslog-Zeitstempeln verwiesen wird.

   Standardmäßig verweisen Syslog-Zeitstempel auf die UTC-Zeit. Sie können Zeitstempel jedoch so ändern, dass sie auf die ExtraHop-Systemzeit verweisen, indem Sie die laufende Konfigurationsdatei ändern.

   a) Klicken **Admin**.
   b) Klicken **Config ausführen (ungespeicherte Änderungen)**.
   c) Klicken **Konfiguration bearbeiten**.
   d) Füge einen Eintrag hinzu unter `syslog_notification` wo der Schlüssel ist `syslog_use_localtime` und der Wert ist `true`.

      Das `syslog_notification` Der Abschnitt sollte dem folgenden Code ähneln:

      ```
      "syslog_notification": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "syslog_use_localtime": true
      }
      ```
   e) Klicken **Aktualisieren**.

f) Klicken **Erledigt**.

**Nächste Schritte**
Nachdem Sie sich vergewissert haben, dass Ihre neuen Einstellungen erwartungsgemäß funktionieren, behalten Sie Ihre Konfigurationsänderungen bei Systemneustart- und Shutdown-Ereignissen bei, indem Sie die laufende Konfigurationsdatei speichern.

## SSL-Zertifikat

SSL-Zertifikate bieten eine sichere Authentifizierung für das ExtraHop-System.

Sie können ein selbstsigniertes Zertifikat für die Authentifizierung anstelle eines von einer Zertifizierungsstelle signierten Zertifikats angeben. Beachten Sie jedoch, dass ein selbstsigniertes Zertifikat einen Fehler in der Client Browser, der meldet, dass die signierende Zertifizierungsstelle unbekannt ist. Der Browser stellt eine Reihe von Bestätigungsseiten bereit, um dem Zertifikat zu vertrauen, auch wenn das Zertifikat selbst signiert ist. Selbstsignierte Zertifikate können auch die Leistung beeinträchtigen, da sie das Zwischenspeichern in einigen Browsern verhindern. Wir empfehlen Ihnen, eine Anfrage zur Zertifikatsignierung von Ihrem ExtraHop-System aus zu erstellen und stattdessen das signierte Zertifikat hochzuladen.

**Wichtig:** Beim Ersetzen eines SSL-Zertifikats wird der Webserverdienst neu gestartet. Getunnelte Verbindungen von Discover-Appliances zu Command-Appliances gehen verloren, werden dann aber automatisch wiederhergestellt.

### Laden Sie ein SSL-Zertifikat hoch

Sie müssen eine PEM-Datei hochladen, die sowohl einen privaten Schlüssel als auch entweder ein selbstsigniertes Zertifikat oder ein Zertifikat einer Zertifizierungsstelle enthält.

**Hinweis:** Die.pem-Datei darf nicht passwortgeschützt sein.

**Hinweis:** Du kannst auch Automatisieren Sie diese Aufgabe über die REST-API.

1. In der Netzwerk-Einstellungen Abschnitt, klicken **SSL Zertifikat**.
2. klicken **Zertifikate verwalten** um den Abschnitt zu erweitern.
3. klicken **Wählen Sie Datei** und navigieren Sie zu dem Zertifikat, das Sie hochladen möchten.
4. klicken **Offen**.
5. klicken **hochladen**.

### Generieren Sie ein selbstsigniertes Zertifikat

1. In der Netzwerkeinstellungen Abschnitt, klicken **SSL-Zertifikat**.
2. klicken **Zertifikate verwalten** um den Abschnitt zu erweitern.
3. klicken **Erstellen Sie ein selbstsigniertes SSL-Zertifikat basierend auf dem Hostnamen** .
4. Auf dem Zertifikat generieren Seite, klicken **OK** um das selbstsignierte SSL-Zertifikat zu generieren.

**Hinweis:** Der Standard-Hostname ist `extrahop`.

### Erstellen Sie eine Zertifikatsignieranforderung von Ihrem ExtraHop-System aus

Eine Certificate Signing Request (CSR) ist ein codierter Textblock, der an Ihre Zertifizierungsstelle (CA) weitergegeben wird, wenn Sie ein SSL-Zertifikat beantragen. Die CSR wird auf dem ExtraHop-System generiert, auf dem das SSL-Zertifikat installiert wird, und enthält Informationen , die im Zertifikat enthalten sein werden, z. B. den allgemeinen Namen (Domänenname), die Organisation, den Ort und das Land. Die CSR enthält auch den öffentlichen Schlüssel, der im Zertifikat enthalten sein wird. Die CSR wird mit dem privaten Schlüssel aus dem ExtraHop-System erstellt, wodurch ein Schlüsselpaar entsteht.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Netzwerkeinstellungen auf **SSL Zertifikat**.
3. klicken **Zertifikate verwalten** und dann klicken **Exportieren einer Zertifikatsignieranforderung (CSR)**.
4. In der Betreff Alternative Namen Geben Sie in diesem Abschnitt den DNS-Namen des ExtraHop-Systems ein. Sie können mehrere DNS-Namen und IP-Adressen hinzufügen , die durch ein einziges SSL-Zertifikat geschützt werden sollen.
5. In der Betreff Abschnitt, füllen Sie die folgenden Felder aus. Nur der **Gemeinsamer Name** Feld ist erforderlich.

| Feld | Beschreibung | Beispiele |
|---|---|---|
| Gemeinsamer Name | Der vollqualifizierte Domänenname (FQDN) des ExtraHop-Systems . Der FQDN muss mit einem der alternativen Subject Names übereinstimmen. | *.example.com<br>discover.example.com |
| E-mail-Adresse | Die E-Mail-Adresse des Hauptansprechpartners für Ihre Organisation. | webmaster@example.com |
| Organisatorische Einheit | Die Abteilung Ihrer Organisation, die das Zertifikat bearbeitet. | IT-Abteilung |
| Organisation | Der offizielle Name Ihrer Organisation. Dieser Eintrag sollte nicht abgekürzt werden und Suffixe wie Inc, Corp oder LLC enthalten. | Beispiel, Inc. |
| Ort/Stadt | Die Stadt, in der sich Ihre Organisation befindet. | Seattle |
| Bundesstaat/Provinz | Das Bundesland oder die Provinz, in dem Ihre Organisation ansässig ist. Dieser Eintrag sollte nicht abgekürzt werden. | Washington |
| Landesvorwahl | Der zweibuchstabige ISO-Code für das Land, in dem Ihre Organisation ansässig ist. | UNS |

6. klicken **Exportieren**. Die CSR-Datei wird automatisch auf Ihren Computer heruntergeladen.

**Nächste Schritte**
Senden Sie die CSR-Datei an Ihre Zertifizierungsstelle (CA), um die CSR signieren zu lassen. Wenn Sie das SSL-Zertifikat von der CA erhalten haben, kehren Sie zurück zur SSL Zertifikat Öffnen Sie die Administrationseinstellungen und laden Sie das Zertifikat in das ExtraHop-System hoch.

**Hinweis** Wenn Ihre Organisation verlangt, dass die CSR einen neuen öffentlichen Schlüssel enthält, ein selbstsigniertes Zertifikat generieren um vor der Erstellung der CSR neue Schlüsselpaare zu erstellen.

# Vertrauenswürdige Zertifikate

Mit vertrauenswürdigen Zertifikaten können Sie SMTP-, LDAP-, HTTPS- ODS- und MongoDB-ODS-Ziele sowie Splunk-Recordstore-Verbindungen von Ihrem ExtraHop-System aus validieren.

## Fügen Sie Ihrem ExtraHop-System ein vertrauenswürdiges Zertifikat hinzu

Ihr ExtraHop-System vertraut nur Peers, die ein Transport Layer Security (TLS) -Zertifikat vorlegen, das mit einem der integrierten Systemzertifikate und allen von Ihnen hochgeladenen Zertifikaten signiert ist. SMTP-, LDAP-, HTTPS-ODS- und MongoDB-ODS-Ziele sowie Splunk-Recordstore-Verbindungen können mit diesen Zertifikaten validiert werden.

**Bevor Sie beginnen**
Sie müssen sich als Benutzer mit Setup- oder System- und Zugriffsadministrationsrechten anmelden , um vertrauenswürdige Zertifikate hinzuzufügen oder zu entfernen.

Beim Hochladen eines benutzerdefinierten vertrauenswürdigen Zertifikats muss ein gültiger Vertrauenspfad vom hochgeladenen Zertifikat zu einem vertrauenswürdigen, selbstsignierten Stammzertifikat vorhanden sein, damit das Zertifikat vollständig vertrauenswürdig ist. Laden Sie entweder die gesamte Zertifikatskette für jedes vertrauenswürdige Zertifikat hoch oder stellen Sie (vorzugsweise) sicher, dass jedes Zertifikat in der Kette in das System für vertrauenswürdige Zertifikate hochgeladen wurde.

**Wichtig:** Um den integrierten Systemzertifikaten und allen hochgeladenen Zertifikaten zu vertrauen, müssen Sie bei der Konfiguration der Einstellungen für den externen Server auch die SSL-/TLS- oder STARTTLS-Verschlüsselung und die Zertifikatsvalidierung aktivieren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerk-Einstellungen Abschnitt, klicken **Vertrauenswürdige Zertifikate**.
3. Optional: Das ExtraHop-System wird mit einer Reihe von integrierten Zertifikaten geliefert. Wählen **Trust System-Zertifikate** wenn Sie diesen Zertifikaten vertrauen möchten, und klicken Sie dann auf **Speichern**.
4. Um Ihr eigenes Zertifikat hinzuzufügen, klicken Sie auf **Zertifikat hinzufügen** und fügen Sie dann den Inhalt der PEM-codierten Zertifikatskette in die Zertifikat Feld
5. Geben Sie einen Namen in das Name Feld und Klick **Hinzufügen**.

# Zugriffs-Einstellungen

Im Abschnitt Zugriffseinstellungen können Sie Benutzerkennwörter ändern, das Support-Konto aktivieren, lokale Benutzer und Benutzergruppen verwalten, die Remoteauthentifizierung konfigurieren und den API-Zugriff verwalten.

## Passwörter

Benutzer mit Rechten für die Administrationsseite können das Passwort für lokale Benutzerkonten ändern.

- Wählen Sie einen beliebigen Benutzer aus und ändern Sie sein Passwort
  - Sie können nur Passwörter für lokale Benutzer ändern. Sie können die Passwörter für Benutzer, die über LDAP oder andere Remote-Authentifizierungsserver authentifiziert wurden, nicht ändern.

Weitere Informationen zu Rechten für bestimmte Benutzer und Gruppen der Administrationsseite finden Sie in der Nutzer Abschnitt.

## Ändern Sie das Standardkennwort für den Setup-Benutzer

Es wird empfohlen, das Standardkennwort für den Setup-Benutzer auf dem ExtraHop-System zu ändern, nachdem Sie sich zum ersten Mal angemeldet haben. Um Administratoren daran zu erinnern, diese Änderung vorzunehmen, erscheint ein blaues Symbol **Passwort ändern** Schaltfläche oben auf der Seite, während der Setup-Benutzer auf die Administrationseinstellungen zugreift. Nachdem das Setup-Benutzerkennwort geändert wurde, wird die Schaltfläche oben auf der Seite nicht mehr angezeigt.

**Hinweis:** Das Passwort muss mindestens 5 Zeichen lang sein.

1. In der Einstellungen für die Verwaltung, klicken Sie auf das Blaue **Standardkennwort ändern** knopf. Die Passwortseite wird ohne das Dropdownmenü für Konten angezeigt. Das Passwort wird nur für den Setup-Benutzer geändert.
2. Geben Sie das Standardkennwort in das Altes Passwort Feld.
3. Geben Sie das neue Passwort in das Neues Passwort Feld.
4. Geben Sie das neue Passwort erneut ein in Passwort bestätigen Feld.
5. klicken **Speichern**.

## Zugang zum Support

Support-Konten bieten dem ExtraHop-Supportteam Zugriff, um Kunden bei der Behebung von Problemen mit dem ExtraHop-System zu unterstützen.

Diese Einstellungen sollten nur aktiviert werden, wenn der ExtraHop-Systemadministrator das ExtraHop-Supportteam um praktische Unterstützung bittet.

### SSH-Schlüssel generieren

Generieren Sie einen SSH-Schlüssel, damit der ExtraHop-Support eine Verbindung zu Ihrem ExtraHop-System herstellen kann, wenn Fernzugriff wird konfiguriert durch ExtraHop Cloud-Dienste .

1. In der Zugriffs-Einstellungen Abschnitt, klicken **Zugang zum Support**.
2. klicken **SSH-Schlüssel generieren**.
3. klicken **SSH-Schlüssel generieren**.

4. Kopieren Sie den verschlüsselten Schlüssel aus dem Textfeld und senden Sie den Schlüssel per E-Mail an Ihren ExtraHop-Ansprechpartner.
5. klicken **Erledigt**.

### Den SSH-Schlüssel neu generieren oder widerrufen

Um den SSH-Zugriff auf das ExtraHop-System mit einem vorhandenen SSH-Schlüssel zu verhindern, können Sie den aktuellen SSH-Schlüssel widerrufen. Ein neuer SSH-Schlüssel kann bei Bedarf auch neu generiert werden.

1. In der Zugriffs-Einstellungen Abschnitt, klicken **Zugang zum Support**.
2. klicken **SSH-Schlüssel generieren**.
3. Wählen Sie eine der folgenden Optionen:
   - klicken **SSH-Schlüssel neu generieren** und dann klicken **Regenerieren**.

     Kopieren Sie den verschlüsselten Schlüssel aus dem Textfeld und senden Sie den Schlüssel per E-Mail an Ihren ExtraHop-Ansprechpartner. Klicken Sie dann auf **Erledigt**.
   - klicken **SSH-Schlüssel widerrufen** um den SSH-Zugriff auf das System mit dem aktuellen Schlüssel zu verhindern.

## Nutzer

Auf der Seite Benutzer können Sie den lokalen Zugriff auf die ExtraHop-Appliance steuern.

### Fügen Sie ein lokales Benutzerkonto hinzu

Durch Hinzufügen eines lokalen Benutzerkonto können Sie Benutzern direkten Zugriff auf Ihr ExtraHop-System gewähren und ihre Rechte entsprechend ihrer Rolle in Ihrer Organisation einschränken.

Weitere Informationen zu Standardsystembenutzerkonten finden Sie unter Lokale Benutzer.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Zugriffs-Einstellungen Abschnitt, klicken **Nutzer**.
3. klicken **Nutzer hinzufügen**.
4. In der Personenbezogene Daten Abschnitt, geben Sie die folgenden Informationen ein:

   • Anmelde-ID : Der Benutzername, mit dem sich Benutzer am Sensor anmelden, der keine Leerzeichen enthalten darf. Zum Beispiel `Adalovelace`.

   • Vollständiger Name : Ein Anzeigename für den Benutzer, der Leerzeichen enthalten kann. Zum Beispiel `Ada Lovelace`.

   • Passwort : Das Passwort für dieses Konto.

   **Hinweis** Auf Sensoren und Konsolen muss das Passwort den Kriterien entsprechen, die von globale Passwortrichtlinie. In ExtraHop-Plattenläden und Packetstores müssen Passwörter mindestens 5 Zeichen lang sein.

   • Bestätigen Sie das Passwort : Geben Sie das Passwort erneut aus dem Passwort Feld.
5. Wählen Sie im Abschnitt Authentifizierungstyp die Option Lokal aus.
6. In der Benutzertyp Wählen Sie im Abschnitt die Art der Rechte für den Benutzer aus.
   - System- und Zugriffsadministrationsrechte ermöglichen vollen Lese- und Schreibzugriff auf das ExtraHop-System, einschließlich der Administrationseinstellungen.
   - Mit eingeschränkten Rechten können Sie aus einer Teilmenge von Rechten und Optionen auswählen.

     **Hinweis** Weitere Informationen finden Sie in der Benutzerrechte Abschnitt.

7. klicken **Speichern**.

**Hinweis:**
- Um die Einstellungen für einen Benutzer zu ändern, klicken Sie in der Liste auf den Benutzernamen, um die Bearbeiten Benutzerseite.
- Um ein Benutzerkonto zu löschen, klicken Sie auf das rote **X** Ikone. Wenn Sie einen Benutzer von einem Remote-Authentifizierungsserver wie LDAP löschen, müssen Sie auch den Eintrag für diesen Benutzer auf dem ExtraHop-System löschen.

## Benutzer und Benutzergruppen

Benutzer können auf drei Arten auf das ExtraHop-System zugreifen: über eine Reihe vorkonfigurierter Benutzerkonten, über lokale Benutzerkonten, die auf der Appliance konfiguriert sind, oder über Remote-Benutzerkonten, die auf vorhandenen Authentifizierungsservern wie LDAP, SAML, Radius und TACACS+ konfiguriert sind.

**Video:** Sehen Sie sich die entsprechenden Schulungen an:

- Benutzerverwaltung
- Benutzergruppen

### Lokale Benutzer

In diesem Thema geht es um Standard- und lokale Konten. siehe Fernauthentifizierung um zu lernen, wie man Remote-Konten konfiguriert.

Die folgenden Konten sind standardmäßig auf ExtraHop-Systemen konfiguriert, erscheinen jedoch nicht in der Namensliste auf der Benutzerseite. Diese Konten können nicht gelöscht werden und Sie müssen das Standardkennwort bei der ersten Anmeldung ändern.

**Einrichten**

Dieses Konto bietet volle System-Lese- und Schreibrechte für die browserbasierte Benutzeroberfläche und die ExtraHop-Befehlszeilenschnittstelle (CLI). Auf physischem Sensoren, das Standardkennwort für dieses Konto ist die Service-Tag-Nummer auf der Vorderseite der Appliance. Auf virtuellem Sensoren, das Standardpasswort ist `default`.

**Schale**

Die `shell` Das Konto hat standardmäßig Zugriff auf nicht administrative Shell-Befehle in der ExtraHop-CLI. Bei physischen Sensoren ist das Standardkennwort für dieses Konto die Service-Tag-Nummer auf der Vorderseite der Appliance. Bei virtuellen Sensoren lautet das Standardkennwort `default`.

**Hinweis:** Das standardmäßige ExtraHop-Passwort für eines der Konten, wenn es in Amazon Web Services (AWS) und Google Cloud Platform (GCP) bereitgestellt wird, ist die Instanz-ID der virtuellen Maschine.

### Nächste Schritte

- Fügen Sie ein lokales Benutzerkonto hinzu

### Fernauthentifizierung

Das ExtraHop-System unterstützt die Fernauthentifizierung für den Benutzerzugriff. Mithilfe der Remoteauthentifizierung können Unternehmen, die über Authentifizierungssysteme wie LDAP (z. B. OpenLDAP oder Active Directory) verfügen, allen oder einem Teil ihrer Benutzer die Möglichkeit geben, sich mit ihren vorhandenen Anmeldedaten am System anzumelden.

Die zentralisierte Authentifizierung bietet die folgenden Vorteile:

- Synchronisation von Benutzerkennwörtern.
- Automatische Erstellung von ExtraHop-Konten für Benutzer ohne Administratoreingriff.
- Verwaltung von ExtraHop-Privilegien auf der Grundlage von Benutzergruppen.
- Administratoren können allen bekannten Benutzern Zugriff gewähren oder den Zugriff einschränken, indem sie LDAP-Filter anwenden.

### Nächste Schritte

- Konfigurieren Sie die Remote-Authentifizierung über LDAP
- Konfigurieren Sie die Remote-Authentifizierung über SAML
- Konfiguration der Fernauthentifizierung über TACACS+
- Konfigurieren Sie die Remoteauthentifizierung über RADIUS

### Entfernte Benutzer

Wenn Ihr ExtraHop-System für die SAML- oder LDAP-Fernauthentifizierung konfiguriert ist, können Sie ein Konto für diese Remote-Benutzer erstellen. Durch die Vorkonfiguration von Konten auf dem ExtraHop-System für Remote-Benutzer können Sie Systemanpassungen mit diesen Benutzern teilen, bevor sie sich anmelden.

Wenn Sie sich bei der Konfiguration der SAML-Authentifizierung für die automatische Bereitstellung von Benutzern entscheiden, wird der Benutzer bei der ersten Anmeldung automatisch zur Liste der lokalen Benutzer hinzugefügt. Sie können jedoch ein SAML-Remotebenutzerkonto auf dem ExtraHop-System erstellen, wenn Sie einen Remote-Benutzer bereitstellen möchten, bevor sich dieser Benutzer am System angemeldet hat. Rechte werden dem Benutzer vom Anbieter zugewiesen. Nachdem der Benutzer erstellt wurde, können Sie ihn zu lokalen Benutzergruppen hinzufügen.

### Nächste Schritte

- Konto für einen Remote-Benutzer hinzufügen

### Benutzergruppen

Benutzergruppen ermöglichen es Ihnen, den Zugriff auf gemeinsam genutzte Inhalte nach Gruppen statt nach einzelnen Benutzern zu verwalten. Benutzerdefinierte Objekte wie Activity Maps können mit einer Benutzergruppe geteilt werden, und jeder Benutzer, der der Gruppe hinzugefügt wird, hat automatisch Zugriff. Sie können eine lokale Benutzergruppe erstellen, die Remote- und lokale Benutzer umfassen kann. Wenn Ihr ExtraHop-System für die Fernauthentifizierung über LDAP konfiguriert ist, können Sie alternativ Einstellungen für den Import Ihrer LDAP-Benutzergruppen konfigurieren.

- klicken **Benutzergruppe erstellen** um eine lokale Gruppe zu erstellen. Die Benutzergruppe wird in der Liste angezeigt. Aktivieren Sie dann das Kontrollkästchen neben dem Namen der Benutzergruppe und wählen Sie Benutzer aus der **Benutzer filtern...** Drop-down-Liste. klicken **Benutzer zur Gruppe hinzufügen**.
- (nur LDAP) Klicken Sie **Alle Benutzergruppen aktualisieren** oder wählen Sie mehrere LDAP-Benutzergruppen aus und klicken Sie auf **Benutzer in Gruppen aktualisieren**.
- klicken **Benutzergruppe zurücksetzen** um alle geteilten Inhalte aus einer ausgewählten Benutzergruppe zu entfernen. Wenn die Gruppe auf dem Remote-LDAP-Server nicht mehr existiert, wird die Gruppe aus der Benutzergruppenliste entfernt.
- klicken **Benutzergruppe aktivieren** oder **Benutzergruppe deaktivieren** um zu kontrollieren, ob ein Gruppenmitglied auf geteilte Inhalte für die ausgewählte Benutzergruppe zugreifen kann.
- klicken **Benutzergruppe löschen** um die ausgewählte Benutzergruppe aus dem System zu entfernen.
- Sehen Sie sich die folgenden Eigenschaften für aufgelistete Benutzergruppen an:

  **Name der Gruppe**

  Zeigt den Namen der Gruppe an. Um die Mitglieder der Gruppe anzuzeigen, klicken Sie auf den Gruppennamen.

  **Typ**

  Zeigt Lokal oder Remote als Art der Benutzergruppe an.

  **Mitglieder**

  Zeigt die Anzahl der Benutzer in der Gruppe an.

  **Geteilter Inhalt**

  Zeigt die Anzahl der vom Benutzer erstellten Objekte an, die mit der Gruppe gemeinsam genutzt werden.

**Status**

Zeigt an, ob die Gruppe auf dem System aktiviert oder deaktiviert ist. Wenn der Status ist `Disabled`, wird die Benutzergruppe bei der Durchführung von Mitgliedschaftsprüfungen als leer betrachtet. Die Benutzergruppe kann jedoch weiterhin angegeben werden, wenn Inhalte geteilt werden.

**Mitglieder aktualisiert (nur LDAP)**

Zeigt die Zeit an, die seit der Aktualisierung der Gruppenmitgliedschaft vergangen ist. Benutzergruppen werden unter den folgenden Bedingungen aktualisiert:

- Standardmäßig einmal pro Stunde. Die Einstellung für das Aktualisierungsintervall kann auf der **Fernauthentifizierung** > **LDAP-Einstellungen** Seite.
- Ein Administrator aktualisiert eine Gruppe, indem er auf **Alle Benutzergruppen aktualisieren** oder **Benutzer in der Gruppe aktualisieren**, oder programmgesteuert über die REST-API. Sie können eine Gruppe aktualisieren über Benutzergruppe Seite oder aus dem Liste der Mitglieder Seite.
- Ein Remote-Benutzer meldet sich zum ersten Mal beim ExtraHop-System an.
- Ein Benutzer versucht, ein geteiltes Dashboard zu laden, auf das er keinen Zugriff hat.

**Benutzerrechte**
Administratoren bestimmen die Modulzugriffsebene für Benutzer im ExtraHop-System.

Informationen zu Benutzerberechtigungen für die REST-API finden Sie in der REST-API-Leitfaden.

Informationen zu Remote-Benutzerrechten finden Sie in den Konfigurationsanleitungen für LDAP, RADIUS, SAML, und TACACS+.

**Privilegienstufen**
Legen Sie die Berechtigungsstufe fest, auf die Ihr Benutzer zugreifen kann, um zu bestimmen, auf welche Bereiche des ExtraHop-Systems er zugreifen kann.

**Zugriffsrechte für Module**

Diese Rechte bestimmen die Funktionen, auf die Benutzer im ExtraHop-System zugreifen können. Administratoren können Benutzern rollenbasierten Zugriff auf eines oder alle der Module Network Detection and Response (NDR), Network Performance and Monitoring (NPM) und Packet Forensics gewähren. Für den Zugriff auf Modulfunktionen ist eine Modullizenz erforderlich.

**Zugriff auf das NDR-Modul**

Ermöglicht dem Benutzer den Zugriff auf Sicherheitsfunktionen wie Angriffserkennungen, Untersuchungen und Bedrohungsinformationen.

**Zugriff auf das NPM-Modul**

Ermöglicht dem Benutzer den Zugriff auf Leistungsfunktionen wie Betriebserkennungen und die Möglichkeit, benutzerdefinierte Dashboards zu erstellen.

**Zugriff auf Pakete und Sitzungsschlüssel**

Ermöglicht dem Benutzer das Anzeigen und Herunterladen von Paketen und Sitzungsschlüsseln, nur Paketen oder nur Paketsegmenten.

**Systemzugriffsrechte**

Diese Rechte bestimmen den Funktionsumfang, über den Benutzer in den Modulen verfügen, für die ihnen Zugriff gewährt wurde.

Für Reveal (x) Enterprise können Benutzer mit Systemzugriffs- und Administratorrechten auf alle Funktionen, Pakete und Sitzungsschlüssel für ihre lizenzierten Module zugreifen.

Für Reveal (x) 360 müssen Systemzugriffs- und Administratorrechte sowie der Zugriff auf lizenzierte Module, Pakete und Sitzungsschlüssel separat zugewiesen werden. Reveal (x) 360 bietet auch ein

zusätzliches Systemadministrationskonto, das alle Systemberechtigungen gewährt, mit Ausnahme der Möglichkeit, Benutzer und API-Zugriff zu verwalten.

Die folgende Tabelle enthält ExtraHop-Funktionen und die erforderlichen Rechte. Wenn keine Modulanforderung angegeben ist, ist die Funktion sowohl im NDR- als auch im NDM-Modul verfügbar.

| | **System- und Zugriffsverw** | **Systemadmi (nur Reveal (x) 360)** | **Vollständige Schreiben** | **Eingeschränk Schreiben** | **Persönliches Schreiben** | **Vollständig schreibgesch** | **Eingeschränkter Schreibschutz** |
|---|---|---|---|---|---|---|---|
| Karten der Aktivitäten | | | | | | | |
| Karten für gemeinsame Aktivitäten erstellen, anzeigen und laden | Y | Y | Y | Y | Y | Y | N |
| Aktivitätskarten speichern | Y | Y | Y | Y | Y | N | N |
| Aktivitätskarten teilen | Y | Y | Y | Y | N | N | N |
| Warnmeldungen | NDM-Modullizenz und Zugriff erforderlich. | | | | | | |
| Warnmeldungen anzeigen | Y | Y | Y | Y | Y | Y | Y |
| Benachrichtigungen erstellen und ändern | Y | Y | Y | N | N | N | N |
| Prioritäten der Analyse | | | | | | | |
| Seite „Analyseprioritäten“ anzeigen | Y | Y | Y | Y | Y | Y | N |
| Analyseebenen für Gruppen hinzufügen und ändern | Y | Y | Y | N | N | N | N |
| Geräte zu einer Beobachtungsliste hinzufügen | Y | Y | Y | N | N | N | N |
| Verwaltung der Transferprioritäten | Y | Y | Y | N | N | N | N |
| Bündel | | | | | | | |
| Ein Paket erstellen | Y | Y | Y | N | N | N | N |

| | System- und Zugriffsverw | Systemadmi (nur Reveal (x) 360) | Vollständige Schreiben | Eingeschränk Schreiben | Persönliches Schreiben | Vollständig schreibgesch | Eingeschränkter Schreibschutz |
|---|---|---|---|---|---|---|---|
| Laden Sie ein Paket hoch und wenden Sie es an | Y | Y | Y | N | N | N | N |
| Liste der Bundles anzeigen | Y | Y | Y | Y | Y | Y | N |
| Dashboards | Zum Erstellen und Ändern von Dashboards sind eine NPM-Modullizenz und -zugriff erforderlich. | | | | | | |
| Dashboards anzeigen und organisieren | Y | Y | Y | Y | Y | Y | Y |
| Dashboards erstellen und ändern | Y | Y | Y | Y | Y | N | N |
| Dashboards teilen | Y | Y | Y | Y | N | N | N |
| Erkennungen | NDR-Modullizenz und Zugriff sind erforderlich, um Sicherheitserkennungen anzuzeigen und zu optimieren und Untersuchungen durchzuführen.<br>Zum Anzeigen und Optimieren von Leistungserkennungen sind eine NPM-Modullizenz und -zugriff erforderlich. | | | | | | |
| Erkennungen anzeigen | Y | Y | Y | Y | Y | Y | Y |
| Erkennungen bestätigen | Y | Y | Y | Y | Y | N | N |
| Erkennungsstatus und Hinweise ändern | Y | Y | Y | Y | N | N | N |
| Untersuchungen erstellen und ändern | Y | Y | Y | Y | N | N | N |
| Tuning-Regeln erstellen und ändern | Y | Y | Y | N | N | N | N |
| Gerätegruppen | Administratoren können die konfigurieren Globale Richtlinie „Gerätegruppe bearbeiten“ um anzugeben , ob Benutzer mit eingeschränkten Schreibrechten Gerätegruppen erstellen und bearbeiten können. | | | | | | |
| Gerätegruppen erstellen und ändern | Y | Y | Y | Y (Wenn die globale | N | N | N |

| | System- und Zugriffsverw | Systemadmi (nur Reveal (x) 360) | Vollständige Schreiben | Eingeschränk Schreiben | Persönliches Schreiben | Vollständig schreibgesch | Eingeschränkter Schreibschutz |
|---|---|---|---|---|---|---|---|
| | | | | Rechterichtlinie aktiviert ist) | | | |
| Metriken | | | | | | | |
| Metriken anzeigen | Y | Y | Y | Y | Y | Y | N |
| Regeln für Benachrichtigungen | NDR-Modullizenz und Zugriff sind erforderlich, um Benachrichtigungen für Sicherheitserkennungen und Bedrohungsinformationen zu erstellen und zu ändern.<br>NPM-Modullizenz und Zugriff sind erforderlich, um Benachrichtigungen für Leistungserkennungen zu erstellen und zu ändern. | | | | | | |
| Regeln für Erkennungsbenachrichtigungen erstellen und ändern | Y | Y | Y | N | N | N | N |
| Benachrichtigungsregeln Bedrohungsübersicht erstellen und ändern | Y | Y | Y | N | N | N | N |
| Regeln für Systembenachrichtigungen erstellen und ändern ( nur Reveal (x)) | Y | Y | N | N | N | N | N |
| Rekorde | Recordstore erforderlich. | | | | | | |
| Datensatzabfragen anzeigen | Y | Y | Y | Y | Y | Y | N |
| Aufzeichnungsformate anzeigen | Y | Y | Y | Y | Y | Y | N |
| Datensatzabfragen erstellen, ändern und speichern | Y | Y | Y | N | N | N | N |
| Datensatzformate erstellen, ändern und speichern | Y | Y | Y | N | N | N | N |
| Geplante Berichte | Konsole erforderlich. | | | | | | |
| Geplante Berichte erstellen, anzeigen und verwalten | Y | Y | Y | Y | N | N | N |

| | System- und Zugriffsverw | Systemadmi (nur Reveal (x) 360) | Vollständige Schreiben | Eingeschränk Schreiben | Persönliches Schreiben | Vollständig schreibgesch | Eingeschränkter Schreibschutz |
|---|---|---|---|---|---|---|---|
| Bedrohungsinformationen | NDR-Modullizenz und Zugriff erforderlich. | | | | | | |
| Bedrohungssammlungen verwalten | Y | Y | N | N | N | N | N |
| TAXII-Feeds verwalten | Y | Y | N | N | N | N | N |
| Bedrohungsinformationen anzeigen | Y | Y | Y | Y | Y | Y | N |
| Trigger | | | | | | | |
| Trigger erstellen und ändern | Y | Y | Y | N | N | N | N |
| Administratorrechte | | | | | | | |
| Greifen Sie auf die ExtraHop-Administrationseinstellungen zu | Y | Y | N | N | N | N | N |
| Stellen Sie eine Verbindung zu anderen Geräten her | Y | Y | N | N | N | N | N |
| Andere Appliances verwalten (Konsole) | Y | Y | N | N | N | N | N |
| Benutzer und API-Zugriff verwalten | Y | N | N | N | N | N | N |

## Sessions

Das ExtraHop-System bietet Steuerelemente zum Anzeigen und Löschen von Benutzerverbindungen zur Weboberfläche. Die Sessions Die Liste ist nach dem Ablaufdatum sortiert, das dem Datum entspricht, an dem die Sitzungen eingerichtet wurden. Wenn eine Sitzung abläuft oder gelöscht wird, muss sich der Benutzer erneut anmelden, um auf die Weboberfläche zuzugreifen.

## Fernauthentifizierung

Das ExtraHop-System unterstützt die Fernauthentifizierung für den Benutzerzugriff. Mithilfe der Remoteauthentifizierung können Unternehmen, die über Authentifizierungssysteme wie LDAP (z. B.

OpenLDAP oder Active Directory) verfügen, allen oder einem Teil ihrer Benutzer die Möglichkeit geben, sich mit ihren vorhandenen Anmeldedaten am System anzumelden.

Die zentralisierte Authentifizierung bietet die folgenden Vorteile:

- Synchronisation von Benutzerkennwörtern.
- Automatische Erstellung von ExtraHop-Konten für Benutzer ohne Administratoreingriff.
- Verwaltung von ExtraHop-Privilegien auf der Grundlage von Benutzergruppen.
- Administratoren können allen bekannten Benutzern Zugriff gewähren oder den Zugriff einschränken, indem sie LDAP-Filter anwenden.

**Nächste Schritte**

- Konfigurieren Sie die Remote-Authentifizierung über LDAP
- Konfigurieren Sie die Remote-Authentifizierung über SAML
- Konfiguration der Fernauthentifizierung über TACACS+
- Konfigurieren Sie die Remoteauthentifizierung über RADIUS

## Konfigurieren Sie die Remote-Authentifizierung über LDAP

Das ExtraHop-System unterstützt das Lightweight Directory Access Protocol (LDAP) für Authentifizierung und Autorisierung. Anstatt Benutzeranmeldedaten lokal zu speichern, können Sie Ihr ExtraHop-System so konfigurieren, dass Benutzer remote mit einem vorhandenen LDAP-Server authentifiziert werden. Beachten Sie, dass die ExtraHop-LDAP-Authentifizierung nur Benutzerkonten abfragt. Sie fragt nicht nach anderen Entitäten ab, die sich möglicherweise im LDAP-Verzeichnis befinden.

**Bevor Sie beginnen**

- Dieses Verfahren erfordert Vertrautheit mit der Konfiguration von LDAP.
- Stellen Sie sicher, dass sich jeder Benutzer in einer berechtigungsspezifischen Gruppe auf dem LDAP-Server befindet, bevor Sie mit diesem Verfahren beginnen.
- Wenn Sie verschachtelte LDAP-Gruppen konfigurieren möchten, müssen Sie die Datei Running Configuration ändern. Kontakt ExtraHop-Unterstützung um Hilfe.

Wenn ein Benutzer versucht, sich bei einem ExtraHop-System anzumelden, versucht das ExtraHop-System, den Benutzer auf folgende Weise zu authentifizieren:

- Versucht, den Benutzer lokal zu authentifizieren.
- Versucht, den Benutzer über den LDAP-Server zu authentifizieren, wenn der Benutzer nicht lokal existiert und wenn das ExtraHop-System für die Fernauthentifizierung mit LDAP konfiguriert ist.
- Meldet den Benutzer beim ExtraHop-System an, wenn der Benutzer existiert und das Passwort entweder lokal oder über LDAP validiert wurde. Das LDAP-Passwort wird nicht lokal auf dem ExtraHop-System gespeichert. Beachten Sie, dass Sie den Benutzernamen und das Passwort in dem Format eingeben müssen, für das Ihr LDAP-Server konfiguriert ist. Das ExtraHop-System leitet die Informationen nur an den LDAP-Server weiter.
- Wenn der Benutzer nicht existiert oder ein falsches Passwort eingegeben wurde, erscheint eine Fehlermeldung auf der Anmeldeseite.

> **Wichtig:** Wenn Sie die LDAP-Authentifizierung zu einem späteren Zeitpunkt auf eine andere Remoteauthentifizierungsmethode ändern, werden die Benutzer, Benutzergruppen und zugehörigen Anpassungen, die durch die Remoteauthentifizierung erstellt wurden, entfernt. Lokale Benutzer sind davon nicht betroffen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Zugriffs-Einstellungen Abschnitt, klicken **Fernauthentifizierung**.
3. Aus dem Methode zur Fernauthentifizierung Drop-down-Liste, wählen **LDAP** und dann klicken **Weiter**.
4. Auf dem LDAP-Einstellungen Seite, füllen Sie die folgenden Felder mit Serverinformationen aus:

a) In der Hostname Feld, geben Sie den Hostnamen oder die IP-Adresse des LDAP-Servers ein. Wenn Sie einen Hostnamen konfigurieren, stellen Sie sicher, dass der DNS-Eintrag des ExtraHop-Systems richtig konfiguriert ist.
b) In der Hafen Feld, geben Sie die Portnummer ein, auf der der LDAP-Server lauscht.
c) Aus dem Typ des Servers Drop-down-Liste, wählen **Posix** oder **Active Directory**.
d) Optional: In der DN binden Feld, geben Sie den Bind-DN ein. Der Bind-DN sind die Benutzeranmeldedaten, mit denen Sie sich beim LDAP-Server authentifizieren können, um die Benutzersuche durchzuführen. Der Bind-DN muss Listenzugriff auf den Basis-DN und alle für die LDAP-Authentifizierung erforderlichen Organisationseinheiten, Gruppen oder Benutzerkonto haben. Wenn dieser Wert nicht gesetzt ist, wird eine anonyme Bindung durchgeführt. Beachten Sie, dass anonyme Bindungen nicht auf allen LDAP-Servern aktiviert sind.
e) Optional: In der Passwort binden Feld, geben Sie das Bind-Passwort ein. Das Bind-Passwort ist das Passwort, das für die Authentifizierung mit dem LDAP-Server als dem oben angegebenen Bind-DN erforderlich ist. Wenn Sie eine anonyme Bindung konfigurieren, lassen Sie dieses Feld leer. In einigen Fällen ist eine nicht authentifizierte Bindung möglich, bei der Sie einen Bind-DN-Wert, aber kein Bind-Passwort angeben. Erkundigen Sie sich bei Ihrem LDAP-Administrator nach den richtigen Einstellungen.
f) Aus dem Verschlüsselung Wählen Sie in der Dropdownliste eine der folgenden Verschlüsselungsoptionen aus.

   • **Keine:** Diese Option spezifiziert Klartext-TCP-Sockets. In diesem Modus werden alle Passwörter im Klartext über das Netzwerk gesendet.

   • **LAPPEN:** Diese Option spezifiziert LDAP, das in SSL eingeschlossen ist.

   • **Starten Sie TLS:** Diese Option spezifiziert TLS LDAP. (SSL wird ausgehandelt, bevor Passwörter gesendet werden.)
g) Wählen **SSL-Zertifikate validieren** um die Zertifikatsvalidierung zu aktivieren. Wenn Sie diese Option auswählen, wird das Zertifikat auf dem Remote-Endpunkt anhand der vom Trusted Certificates Manager angegebenen Stammzertifikate validiert. Sie müssen auf der Seite Vertrauenswürdige Zertifikate konfigurieren, welchen Zertifikaten Sie vertrauen möchten. Weitere Informationen finden Sie unter Fügen Sie Ihrem ExtraHop-System ein vertrauenswürdiges Zertifikat hinzu.
h) Geben Sie einen Zeitwert in das Aktualisierungsintervall Feld oder belassen Sie die Standardeinstellung von 1 Stunde. Das Aktualisierungsintervall stellt sicher, dass alle Änderungen, die am Benutzer- oder Gruppenzugriff auf dem LDAP-Server vorgenommen werden, auf dem ExtraHop-System aktualisiert werden.

5. Konfigurieren Sie die folgenden Benutzereinstellungen:
   a) Geben Sie den Basis-DN in das Basis-DN Feld. Der Basis-DN ist der Punkt, von dem aus ein Server nach Benutzern sucht. Der Basis-DN muss alle Benutzerkonten enthalten, die Zugriff auf das ExtraHop-System haben. Die Benutzer können direkte Mitglieder des Basis-DN sein oder innerhalb einer OU innerhalb des Basis-DN verschachtelt sein, wenn **Ganzer Teilbaum** Option ist ausgewählt für Umfang der Suche unten angegeben.
   b) Geben Sie einen Suchfilter in das Suchfilter Feld. Mithilfe von Suchfiltern können Sie Suchkriterien definieren, wenn Sie das LDAP-Verzeichnis nach Benutzerkonten durchsuchen.

      **Wichtig:** Das ExtraHop-System fügt automatisch Klammern hinzu, um den Filter einzuschließen, und analysiert diesen Parameter nicht korrekt, wenn Sie Klammern manuell hinzufügen. Fügen Sie Ihre Suchfilter in diesem Schritt und in Schritt 5b hinzu, ähnlich dem folgenden Beispiel:

      ```
      cn=atlas*
      |(cn=EH-*)(cn=IT-*)
      ```

      Wenn Ihre Gruppennamen das Sternchen (*) enthalten, muss das Sternchen außerdem maskiert werden als `\2a`. Zum Beispiel, wenn Ihre Gruppe eine CN namens hat `test*group`, typ `cn=test\2agroup` im Feld Suchfilter.

c) Aus dem Umfang der Suche Wählen Sie in der Dropdownliste eine der folgenden Optionen aus. Der Suchbereich gibt den Umfang der Verzeichnissuche bei der Suche nach Benutzerentitäten an.

• **Ganzer Teilbaum:** Diese Option sucht rekursiv unter dem Gruppen-DN nach passenden Benutzern.

• **Einstufig:** Diese Option sucht nur nach Benutzern, die im Basis-DN existieren, nicht nach Unterbäumen.

6. Optional: Benutzergruppen importieren. Wählen Sie den **Benutzergruppen vom LDAP-Server importieren** kreuzen Sie das Kästchen an und konfigurieren Sie die folgenden Einstellungen.

**Hinweis:** Durch den Import von LDAP-Benutzergruppen können Sie Dashboards mit diesen Gruppen teilen. Die importierten Gruppen werden auf der Seite Benutzergruppe in den Administrationseinstellungen angezeigt.

a) Geben Sie den Basis-DN in das Basis-DN Feld. Der Basis-DN ist der Punkt, von dem aus ein Server nach Benutzergruppen sucht. Der Basis-DN muss alle Benutzergruppen enthalten, die Zugriff auf das ExtraHop-System haben. Die Benutzergruppen können direkte Mitglieder des Basis-DN sein oder innerhalb einer OU innerhalb des Basis-DN verschachtelt sein, wenn **Ganzer Teilbaum** Option ist ausgewählt für  Umfang der Suche unten angegeben.

b) Geben Sie einen Suchfilter in das Suchfilter Feld. Mit Suchfiltern können Sie Suchkriterien definieren, wenn Sie das LDAP-Verzeichnis nach Benutzergruppen durchsuchen.

**Wichtig:** Bei Gruppensuchfiltern filtert das ExtraHop-System implizit nach objectclass=group, weshalb objectclass=group diesem Filter nicht hinzugefügt werden sollte.

c) Aus dem Umfang der Suche Wählen Sie in der Dropdownliste eine der folgenden Optionen aus. Der Suchbereich gibt den Umfang der Verzeichnissuche bei der Suche nach Benutzergruppenentitäten an.

• **Ganzer Teilbaum:** Diese Option sucht rekursiv unter dem Basis-DN nach passenden Benutzergruppen.

• **Einstufig:** Diese Option sucht nach Benutzergruppen, die im Basis-DN existieren, nicht nach Unterbäumen.

7. klicken **Einstellungen testen**. Wenn der Test erfolgreich ist, wird unten auf der Seite eine Statusmeldung angezeigt. Wenn der Test fehlschlägt, klicken Sie auf **Zeige Details** um eine Fehlerliste zu sehen. Sie müssen alle Fehler beheben, bevor Sie fortfahren können.
8. klicken **Speichern und fortfahren**.

**Nächste Schritte**
Benutzerrechte für die Remote-Authentifizierung konfigurieren

**Benutzerrechte für die Remote-Authentifizierung konfigurieren**
Sie können einzelnen Benutzern auf Ihrem ExtraHop-System Benutzerrechte zuweisen oder Rechte über Ihren LDAP-Server konfigurieren und verwalten.

Wenn Sie Benutzerrechte über LDAP zuweisen, müssen Sie mindestens eines der verfügbaren Benutzerberechtigungsfelder ausfüllen. Für diese Felder sind Gruppen (keine Organisationseinheiten) erforderlich , die auf Ihrem LDAP-Server vordefiniert sind. Ein Benutzerkonto mit Zugriff muss ein direktes Mitglied einer bestimmten Gruppe sein. Benutzerkonten, die nicht Mitglied einer oben angegebenen Gruppe sind, haben keinen Zugriff. Gruppen, die nicht vorhanden sind, werden auf dem ExtraHop-System nicht authentifiziert.

Das ExtraHop-System unterstützt sowohl Active Directory- als auch POSIX-Gruppenmitgliedschaften. Für Active Directory `memberOf` wird unterstützt. Für POSIX `memberuid`, `posixGroups`, `groupofNames`, und `groupofuniqueNames` werden unterstützt.

1. Wählen Sie eine der folgenden Optionen aus der  Optionen für die Zuweisung von Rechten Drop-down-Liste:

- **Berechtigungsstufe vom Remoteserver abrufen**

  Diese Option weist Berechtigungen über Ihren Remote-Authentifizierungsserver zu. Sie müssen mindestens eines der folgenden DN-Felder (Distinguished Name) ausfüllen.

  • **System- und Zugriffsverwaltung DN:** Erstellen und ändern Sie alle Objekte und Einstellungen auf dem ExtraHop-System, einschließlich der Administrationseinstellungen.

  • **Vollständiger Schreib-DN:** Objekte auf dem ExtraHop-System erstellen und ändern, ohne Administrationseinstellungen.

  • **Eingeschränkter Schreib-DN:** Erstellen, ändern und teilen Sie Dashboards.

  • **Persönlicher Schreib-DN:** Erstellen Sie persönliche Dashboards und ändern Sie Dashboards, die für den angemeldeten Benutzer freigegeben wurden.

  • **Vollständiger, nur lesbarer DN:** Objekte im ExtraHop-System anzeigen.

  • **Eingeschränkter Nur-Lese-DN:** Zeigen Sie Dashboards an, die mit dem angemeldeten Benutzer geteilt wurden.

  • **Packet Slices-Zugriffs-DN:** Sehen Sie sich die ersten 64 Byte der Pakete an, die über die ExtraHop Trace-Appliance erfasst wurden, und laden Sie sie herunter.

  • **Paketzugriffs-DN:** Mit der ExtraHop Trace-Appliance erfasste Pakete anzeigen und herunterladen.

  • **Zugriffs-DN für Paket- und Sitzungsschlüssel:** Pakete und alle zugehörigen SSL-Sitzungsschlüssel, die über die ExtraHop Trace-Appliance erfasst wurden, anzeigen und herunterladen.

  • **NDR-Modulzugriffs-DN:** Sicherheitserkennungen, die im ExtraHop-System angezeigt werden, anzeigen, bestätigen und verbergen.

  • **NPM-Modulzugriffs-DN:** Leistungserkennungen, die im ExtraHop-System angezeigt werden, anzeigen, bestätigen und verbergen.

- **Remote-Benutzer haben vollen Schreibzugriff**

  Diese Option gewährt entfernten Benutzern vollen Schreibzugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, SSL-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.
- **Remote-Benutzer haben vollen Lesezugriff**

  Diese Option gewährt Remote-Benutzern nur Lesezugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, SSL-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.

2. Optional: Konfigurieren Sie den Paket- und Sitzungsschlüsselzugriff. Wählen Sie eine der folgenden Optionen, um Remote-Benutzern das Herunterladen von Paketerfassungen und SSL-Sitzungsschlüsseln zu ermöglichen.
   - **Kein Zugriff**
   - **Nur Paketsegmente**
   - **Nur Pakete**
   - **Pakete und Sitzungsschlüssel**
3. Optional: Konfigurieren Sie den Zugriff auf NDR- und NPM-Module.
   - **Kein Zugriff**
   - **Voller Zugriff**
4. klicken **Speichern und beenden**.
5. klicken **Erledigt**.

## Konfigurieren Sie die Remoteauthentifizierung über RADIUS

Das ExtraHop-System unterstützt den Remote Authentifizierung Dial In User Service (RADIUS) nur für die Fernauthentifizierung und die lokale Autorisierung. Für die Fernauthentifizierung unterstützt das ExtraHop-System unverschlüsselte RADIUS- und Klartext-Formate.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Auf Einstellungen zugreifen Abschnitt, klicken **Fernauthentifizierung**.
3. Aus dem Methode zur Fernauthentifizierung Drop-down-Liste, wählen **RADIUS** und dann klicken **Weiter**.
4. Auf dem RADIUS-Server hinzufügen Seite, geben Sie die folgenden Informationen ein:

   Gastgeber

   Der Hostname oder die IP-Adresse des RADIUS-Servers. Stellen Sie sicher, dass der DNS des ExtraHop-Systems richtig konfiguriert ist, wenn Sie einen Hostnamen angeben.

   Geheim

   Das gemeinsame Geheimnis zwischen dem ExtraHop-System und dem RADIUS-Server. Wenden Sie sich an Ihren RADIUS-Administrator, um den gemeinsamen geheimen Schlüssel zu erhalten.

   Auszeit

   Die Zeit in Sekunden, die das ExtraHop-System auf eine Antwort vom RADIUS-Server wartet, bevor es erneut versucht, die Verbindung herzustellen .
5. klicken **Server hinzufügen**.
6. Optional: Fügen Sie nach Bedarf weitere Server hinzu.
7. klicken **Speichern und beenden**.
8. Aus dem Optionen für die Zuweisung von Rechten Wählen Sie in der Dropdownliste eine der folgenden Optionen aus:

   - **Remote-Benutzer haben vollen Schreibzugriff**

     Diese Option gewährt entfernten Benutzern vollen Schreibzugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, SSL-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.
   - **Remote-Benutzer haben vollen Lesezugriff**

     Diese Option gewährt Remote-Benutzern nur Lesezugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, SSL-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.
9. Optional: Konfigurieren Sie den Paket- und Sitzungsschlüsselzugriff. Wählen Sie eine der folgenden Optionen, um Remote-Benutzern das Herunterladen von Paketerfassungen und SSL-Sitzungsschlüsseln zu ermöglichen.

   - **Kein Zugriff**
   - **Nur Paketsegmente**
   - **Nur Pakete**
   - **Pakete und Sitzungsschlüssel**
10. Optional: Konfigurieren Sie den Zugriff auf NDR- und NPM-Module.

    - **Kein Zugriff**
    - **Voller Zugriff**
11. klicken **Speichern und beenden**.
12. klicken **Erledigt**.

## Konfiguration der Fernauthentifizierung über TACACS+

Das ExtraHop-System unterstützt Terminal Access Controller Access-Control System Plus (TACACS+) für die Fernauthentifizierung und Autorisierung.

Stellen Sie sicher, dass jeder Benutzer, der per Fernzugriff autorisiert werden soll, über die Auf dem TACACS+-Server konfigurierter ExtraHop-Dienst bevor Sie mit diesem Verfahren beginnen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Zugriffs-Einstellungen Abschnitt, klicken **Fernauthentifizierung**.
3. Aus dem Methode zur Fernauthentifizierung Drop-down-Liste, wählen **TACACS+**, und klicken Sie dann **Weiter**.
4. Auf dem TACACS+ Server hinzufügen Seite, geben Sie die folgenden Informationen ein:

   • Gastgeber **:** Der Hostname oder die IP-Adresse des TACACS+-Servers. Stellen Sie sicher, dass der DNS des ExtraHop-Systems richtig konfiguriert ist, wenn Sie einen Hostnamen eingeben.

   • Geheim **:** Das gemeinsame Geheimnis zwischen dem ExtraHop-System und dem TACACS+-Server . Wenden Sie sich an Ihren TACACS+-Administrator, um den gemeinsamen geheimen Schlüssel zu erhalten.

   **Hinweis** Das Geheimnis darf das Nummernzeichen (#) nicht enthalten.

   • Auszeit **:** Die Zeit in Sekunden, die das ExtraHop-System auf eine Antwort vom TACACS+-Server wartet, bevor es erneut versucht, eine Verbindung herzustellen.
5. klicken **Server hinzufügen**.
6. Optional: Fügen Sie nach Bedarf weitere Server hinzu.
7. klicken **Speichern und beenden**.
8. Aus dem Optionen für die Zuweisung von Berechtigungen Wählen Sie in der Dropdownliste eine der folgenden Optionen aus:

   - **Berechtigungsstufe vom Remoteserver abrufen**

     Diese Option ermöglicht es entfernten Benutzern, Rechtestufen vom Remoteserver zu erhalten. Sie müssen auch Berechtigungen auf dem TACACS+-Server konfigurieren.

   - **Remote-Benutzer haben vollen Schreibzugriff**

     Diese Option gewährt entfernten Benutzern vollen Schreibzugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, SSL-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.
   - **Remote-Benutzer haben vollen Lesezugriff**

     Diese Option gewährt Remote-Benutzern nur Lesezugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, SSL-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.
9. Optional: Konfigurieren Sie den Paket- und Sitzungsschlüsselzugriff. Wählen Sie eine der folgenden Optionen, um Remote-Benutzern das Herunterladen von Paketerfassungen und SSL-Sitzungsschlüsseln zu ermöglichen.

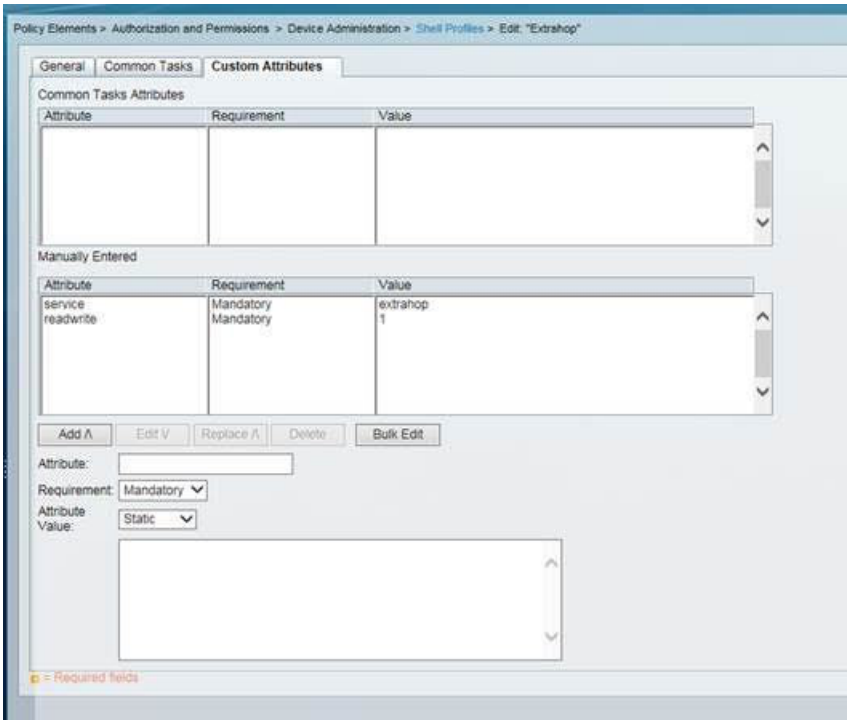
   - **Kein Zugriff**
   - **Nur Paketsegmente**
   - **Nur Pakete**
   - **Pakete und Sitzungsschlüssel**
10. Optional: Konfigurieren Sie den Zugriff auf NDR- und NPM-Module.

    - **Kein Zugriff**
    - **Voller Zugriff**

11. klicken **Speichern und beenden**.
12. klicken **Erledigt**.

**Den TACACS+-Server konfigurieren**
Zusätzlich zur Konfiguration der Remote-Authentifizierung auf Ihrem ExtraHop-System müssen Sie Ihren TACACS+-Server mit zwei Attributen konfigurieren, einem für den ExtraHop-Dienst und einem für die Berechtigungsstufe. Wenn Sie einen ExtraHop-Packetstore haben, können Sie optional ein drittes Attribut für die PCAP und Sitzungsschlüsselprotokollierung hinzufügen.

1. Melden Sie sich bei Ihrem TACACS+-Server an und navigieren Sie zum Shell-Profil für Ihre ExtraHop-Konfiguration.
2. Fügen Sie für das erste Attribut hinzu `Bedienung`.
3. Fügen Sie für den ersten Wert hinzu `zusätzlicher Hop`.
4. Fügen Sie für das zweite Attribut die Berechtigungsstufe hinzu, z. B. `lesen/schreiben`.
5. Für den zweiten Wert addieren Sie `1`.
   Die folgende Abbildung zeigt beispielsweise `extrahop` Attribut und eine Privilegienstufe von `readwrite`.




Hier ist eine Tabelle mit verfügbaren Berechtigungsattributen, Werten und Beschreibungen:

| Attribut | Wert | Beschreibung |
|---|---|---|
| `setup` | `1` | Erstellen und ändern Sie alle Objekte und Einstellungen auf dem ExtraHop-System und verwalten Sie den Benutzerzugriff |
| `readwrite` | `1` | Alle Objekte und Einstellungen auf dem ExtraHop-System erstellen und ändern, ohne Administrationseinstellungen |
| `limited` | `1` | Dashboards erstellen, ändern und teilen |

| Attribut | Wert | Beschreibung |
|---|---|---|
| `readonly` | `1` | Objekte im ExtraHop-System anzeigen |
| `personal` | `1` | Erstellen Sie persönliche Dashboards für sich selbst und ändern Sie alle Dashboards, die mit ihnen geteilt wurden |
| `limited_metrics` | `1` | Geteilte Dashboards anzeigen |
| `ndrfull` | `1` | Sicherheitserkennungen anzeigen, bestätigen und verbergen |
| `npmfull` | `1` | Leistungserkennungen anzeigen, bestätigen und verbergen |
| `packetsfull` | `1` | Pakete anzeigen und herunterladen, die in einem verbundenen Packetstore gespeichert sind. |
| `packetslicesonly` | `1` | Paketsegmente in einem verbundenen Packetstore anzeigen und herunterladen. |
| `packetsfullwithkeys` | `1` | Pakete und zugehörige Sitzungsschlüssel, die in einem verbundenen Packetstore gespeichert sind, anzeigen und herunterladen. |

6. Optional: Fügen Sie das folgende Attribut hinzu, damit Benutzer Sicherheitserkennungen anzeigen, bestätigen und verbergen können

| Attribut | Wert |
|---|---|
| `ndr voll` | `1` |

7. Optional: Fügen Sie das folgende Attribut hinzu, damit Benutzer Leistungserkennungen, die im ExtraHop-System angezeigt werden, anzeigen, bestätigen und verbergen können.

| Attribut | Wert |
|---|---|
| `npm voll` | `1` |

8. Optional: Wenn Sie einen ExtraHop-Packetstore haben, fügen Sie ein Attribut hinzu, das es Benutzern ermöglicht, Paketerfassungen oder Paketerfassungen mit zugehörigen Sitzungsschlüsseln herunterzuladen.

| Attribut | Wert | Beschreibung |
|---|---|---|
| `nur Scheiben verpacken` | `1` | Benutzer mit jeder Berechtigungsstufe können die ersten 64 Byte von Paketen anzeigen und herunterladen. |

| Attribut | Wert | Beschreibung |
|---|---|---|
| `volle Pakete` | `1` | Benutzer mit jeder Berechtigungsstufe können Pakete, die in einem verbundenen Packetstore gespeichert sind, anzeigen und herunterladen. |
| `packetslicesonly` | `1` | Paketsegmente in einem verbundenen Packetstore anzeigen und herunterladen. |
| `Pakete voll mit Schlüsseln` | `1` | Benutzer mit jeder Berechtigungsstufe können Pakete und zugehörige Sitzungsschlüssel, die in einem verbundenen Packetstore gespeichert sind, anzeigen und herunterladen. |

## API-Zugriff

Auf der Seite API-Zugriff können Sie den Zugriff auf die API-Schlüssel generieren, anzeigen und verwalten, die für die Ausführung von Vorgängen über die ExtraHop REST API erforderlich sind.

### API-Schlüsselzugriff verwalten

Benutzer mit System- und Zugriffsadministrationsrechten können konfigurieren, ob Benutzer API-Schlüssel für das ExtraHop-System generieren können. Sie können nur lokalen Benutzern erlauben, Schlüssel zu generieren, oder Sie können die API-Schlüsselgenerierung auch vollständig deaktivieren.

Benutzer müssen einen API-Schlüssel generieren, bevor sie Operationen über die ExtraHop REST API ausführen können. Schlüssel können nur von dem Benutzer, der den Schlüssel generiert hat, oder von Systemadministratoren mit unbegrenzten Rechten eingesehen werden. Nachdem ein Benutzer einen API-Schlüssel generiert hat, muss er den Schlüssel an seine Anforderungsheader anhängen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Auf Einstellungen zugreifen Abschnitt, klicken **API-Zugriff**.
3. In der API-Zugriff verwalten Abschnitt, wählen Sie eine der folgenden Optionen aus:
   - **Allen Benutzern erlauben, einen API-Schlüssel zu generieren**: Lokale und entfernte Benutzer können API-Schlüssel generieren.
   - **Nur lokale Benutzer können einen API-Schlüssel generieren**: Remote-Benutzer können keine API-Schlüssel generieren.
   - **Kein Benutzer kann einen API-Schlüssel generieren**: Es können keine API-Schlüssel von jedem Benutzer generiert werden.
4. klicken **Einstellungen speichern**.

### Cross-Origin Resource Sharing (CORS) konfigurieren

Quellübergreifende gemeinsame Nutzung von Ressourcen (CORS) ermöglicht Ihnen den Zugriff auf die ExtraHop REST-API über Domänengrenzen und von bestimmten Webseiten aus, ohne dass die Anfrage über einen Proxyserver übertragen werden muss.

Sie können eine oder mehrere zulässige Ursprünge konfigurieren oder den Zugriff auf die ExtraHop REST-API von jedem beliebigen Ursprung aus zulassen. Nur Benutzer mit System- und Zugriffsadministrationsrechten können CORS-Einstellungen anzeigen und bearbeiten.

1. In der **Auf Einstellungen zugreifen** Abschnitt, klicken **API-Zugriff**.
2. In der CORS-Einstellungen Abschnitt, geben Sie eine der folgenden Zugriffskonfigurationen an.
   - Um eine bestimmte URL hinzuzufügen, geben Sie eine Quell-URL in das Textfeld ein und klicken Sie dann auf das Pluszeichen (+) oder drücken Sie die EINGABETASTE.

     Die URL muss ein Schema enthalten, z. B. `HTTP` oder `HTTPS`, und der genaue Domänenname. Sie können keinen Pfad anhängen, Sie können jedoch eine Portnummer angeben.
   - Um den Zugriff von einer beliebigen URL aus zu ermöglichen, wählen Sie die Erlaube API-Anfragen von jedem Ursprung Ankreuzfeld.

     **Hinweis:** Das Zulassen des REST-API-Zugriffs von einem beliebigen Ursprung aus ist weniger sicher als das Bereitstellen einer Liste expliziter Ursprünge.
3. Klicken Sie **Einstellungen speichern** und klicken Sie dann **Erledigt**.

## Generieren Sie einen API-Schlüssel

Sie müssen einen API-Schlüssel generieren, bevor Sie Operationen über die ExtraHop REST API ausführen können. Schlüssel können nur von dem Benutzer eingesehen werden, der den Schlüssel generiert hat, oder von Benutzern mit System - und Zugriffsadministrationsrechten. Nachdem Sie einen API-Schlüssel generiert haben, fügen Sie den Schlüssel zu Ihren Anforderungsheadern oder dem ExtraHop REST API Explorer hinzu.

**Bevor Sie beginnen**
Stellen Sie sicher, dass das ExtraHop-System konfiguriert, um die Generierung von API-Schlüsseln zu ermöglichen.

1. In der Zugriffs-Einstellungen Abschnitt, klicken **API-Zugriff**.
2. In der Generieren Sie einen API-Schlüssel Abschnitt, geben Sie eine Beschreibung für den neuen Schlüssel ein, und klicken Sie dann auf **Generieren**.
3. Scrollen Sie nach unten zum Abschnitt API-Schlüssel und kopieren Sie den API-Schlüssel, der Ihrer Beschreibung entspricht.

Sie können den Schlüssel in den REST API Explorer einfügen oder den Schlüssel an einen Anforderungsheader anhängen.

## Privilegienstufen

Die Benutzerberechtigungsstufen bestimmen, welche ExtraHop-System- und Verwaltungsaufgaben der Benutzer über die ExtraHop-REST-API ausführen kann.

Sie können die Berechtigungsstufen für Benutzer über das `granted_roles` und `effective_roles` Eigenschaften. Das `granted_roles` Diese Eigenschaft zeigt Ihnen, welche Rechtestufen dem Benutzer explizit gewährt werden. Das `effective_roles` Diese Eigenschaft zeigt Ihnen alle Berechtigungsstufen für einen Benutzer an, einschließlich derer, die Sie außerhalb der erteilten Rolle erhalten haben, z. B. über eine Benutzergruppe.

Das `granted_roles` und `effective_roles` Eigenschaften werden durch die folgenden Operationen zurückgegeben:

- GET /users
- GET /users/ {username}

Das `granted_roles` und `effective_roles` Eigenschaften unterstützen die folgenden Berechtigungsstufen. Beachten Sie, dass die Art der Aufgaben für jedes ExtraHop-System je nach Verfügbarkeit variiert Ressourcen sind im REST API Explorer aufgeführt und hängen von den Modulen ab, die für die System- und Benutzermodulzugriffsrechte aktiviert sind.

| Privilegienstufe | Zulässige Aktionen |
|---|---|
| „system“: „voll“ | • Aktiviert oder deaktiviert die API-Schlüsselgenerierung für das ExtraHop-System.<br>• Generieren Sie einen API-Schlüssel.<br>• Sehen Sie sich die letzten vier Ziffern und die Beschreibung für jeden API-Schlüssel auf dem System an.<br>• Löschen Sie API-Schlüssel für jeden Benutzer.<br>• CORS anzeigen und bearbeiten.<br>• Führen Sie alle Verwaltungsaufgaben aus, die über die REST-API verfügbar sind.<br>• Führen Sie alle ExtraHop-Systemaufgaben aus, die über die REST-API verfügbar sind. |
| „write“: „voll“ | • Generieren Sie Ihren eigenen API-Schlüssel.<br>• Zeigen Sie Ihren eigenen API-Schlüssel an oder löschen Sie ihn.<br>• Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen.<br>• Führen Sie alle ExtraHop-Systemaufgaben aus, die über die REST-API verfügbar sind. |
| „write“: „begrenzt“ | • Generieren Sie einen API-Schlüssel.<br>• Zeigen Sie ihren eigenen API-Schlüssel an oder löschen Sie ihn.<br>• Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen.<br>• Führen Sie alle GET-Operationen über die REST-API aus.<br>• Führen Sie Metrik- und Datensatzabfragen durch. |
| „write“: „persönlich“ | • Generieren Sie einen API-Schlüssel.<br>• Zeigen Sie Ihren eigenen API-Schlüssel an oder löschen Sie ihn.<br>• Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen.<br>• Führen Sie alle GET-Operationen über die REST-API aus.<br>• Führen Sie Metrik- und Datensatzabfragen durch. |
| „Metriken“: „voll“ | • Generieren Sie einen API-Schlüssel.<br>• Zeigen Sie Ihren eigenen API-Schlüssel an oder löschen Sie ihn.<br>• Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen.<br>• Führen Sie Metrik- und Datensatzabfragen durch. |
| „metrics“: „eingeschränkt“ | • Generieren Sie einen API-Schlüssel.<br>• Zeigen Sie Ihren eigenen API-Schlüssel an oder löschen Sie ihn.<br>• Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen. |
| „ndr“: „voll“ | • Sicherheitserkennungen anzeigen<br>• Untersuchungen anzeigen und erstellen<br><br>Dies ist ein Modulzugriffsrecht, das einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann:<br><br>• „write“: „voll“ |

| Privilegienstufe | Zulässige Aktionen |
| --- | --- |
| | • „write“: „begrenzt“<br>• „write“: „persönlich“<br>• „schreiben“: null<br>• „Metriken“: „voll“<br>• „metrics“: „eingeschränkt“ |
| „ndr“: „keiner“ | • Kein Zugriff auf NDR-Modulinhalte<br>Dies ist ein Modulzugriffsrecht, das einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann:<br>• „write“: „voll“<br>• „write“: „begrenzt“<br>• „write“: „persönlich“<br>• „schreiben“: null<br>• „Metriken“: „voll“<br>• „metrics“: „eingeschränkt“ |
| „npm“: „voll“ | • Leistungserkennungen anzeigen<br>• Dashboards anzeigen und erstellen<br>• Benachrichtigungen anzeigen und erstellen<br>Dies ist ein Modulzugriffsrecht, das einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann:<br>• „write“: „voll“<br>• „write“: „begrenzt“<br>• „write“: „persönlich“<br>• „schreiben“: null<br>• „Metriken“: „voll“<br>• „metrics“: „eingeschränkt“ |
| „npm“: „keine“ | • Kein Zugriff auf NPM-Modulinhalte<br>Dies ist ein Modulzugriffsrecht, das einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann:<br>• „write“: „voll“<br>• „write“: „begrenzt“<br>• „write“: „persönlich“<br>• „schreiben“: null<br>• „Metriken“: „voll“<br>• „metrics“: „eingeschränkt“ |
| „Pakete“: „voll“ | • Pakete anzeigen und herunterladen über das `GET /packets/search` und `POST /packets/search` Operationen.<br>Dies ist eine Zusatzberechtigung, die einem Benutzer mit einer der folgenden Berechtigungsstufen gewährt werden kann:<br>• „write“: „voll“<br>• „write“: „begrenzt“ |

| Privilegienstufe | Zulässige Aktionen |
| --- | --- |
| | • „write“: „persönlich“<br>• „schreiben“: null<br>• „Metriken“: „voll“<br>• „metrics“: „eingeschränkt“ |
| „Pakete“: „voll_mit_Schlüsseln“ | • Pakete und Sitzungsschlüssel anzeigen und herunterladen über das `GET /packets/search` und `POST /packets/search` Operationen.<br><br>Dies ist eine Zusatzberechtigung, die einem Benutzer mit einer der folgenden Berechtigungsstufen gewährt werden kann:<br><br>• „write“: „voll“<br>• „write“: „begrenzt“<br>• „write“: „persönlich“<br>• „schreiben“: null<br>• „Metriken“: „voll“<br>• „metrics“: „eingeschränkt“ |
| „Pakete“: „slices_only“ | • Sehen Sie sich die ersten 64 Byte an Paketen an und laden Sie sie herunter über die `GET /packets/search` und `POST /packets/search` Operationen.<br><br>Dies ist eine Zusatzberechtigung, die einem Benutzer mit einer der folgenden Berechtigungsstufen gewährt werden kann:<br><br>• „write“: „voll“<br>• „write“: „begrenzt“<br>• „write“: „persönlich“<br>• „schreiben“: null<br>• „Metriken“: „voll“<br>• „metrics“: „eingeschränkt“ |

# Einstellungen der Appliance

Sie können die folgenden Komponenten der ExtraHop-Appliance in der Einstellungen der Appliance Abschnitt.

Alle Geräte haben die folgenden Komponenten:

**Konfiguration ausführen**
Laden Sie die laufende Konfigurationsdatei herunter und ändern Sie sie.

**Dienstleistungen**
Aktivieren oder deaktivieren Sie die Web Shell, die Management-GUI, den SNMP-Dienst, den SSH-Zugriff und den SSL-Sitzungsschlüsselempfänger. Die Option SSL Session Key Receiver wird nur auf der Discover-Appliance angezeigt.

**Firmware**
Aktualisieren Sie die ExtraHop-Systemfirmware.

**Systemzeit**
Konfigurieren Sie die Systemzeit.

**Herunterfahren oder Neustarten**
Halten Sie die Systemdienste an und starten Sie sie neu.

**Lizenz**
Aktualisieren Sie die Lizenz, um Zusatzmodule zu aktivieren.

**Festplatten**
Stellt Informationen zu den Festplatten in der Appliance bereit.

Die folgenden Komponenten kommen nur auf den angegebenen Appliances vor:

**Spitzname des Befehls**
Weisen Sie der Command-Appliance einen Spitznamen zu. Diese Einstellung ist nur auf der Command-Appliance verfügbar.

**Packetstore zurücksetzen**
Löschen Sie alle Pakete, die auf der ExtraHop Trace-Appliance gespeichert sind. Die Packetstore zurücksetzen Die Seite wird nur auf der Trace-Appliance angezeigt.

## Konfiguration ausführen

Die laufende Konfigurationsdatei gibt die Standardsystemkonfiguration an. Wenn Sie Systemeinstellungen ändern, müssen Sie die laufende Konfigurationsdatei speichern, um diese Änderungen nach einem Systemneustart beizubehalten.

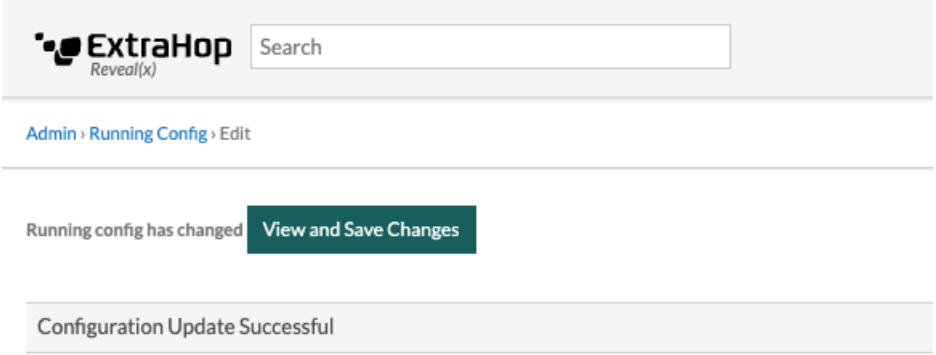
**Hinweis:** Es wird nicht empfohlen, Konfigurationsänderungen am Code von der Bearbeitungsseite aus vorzunehmen. Sie können die meisten Systemänderungen über andere Seiten in den Administrationseinstellungen vornehmen.

### Speichern Sie die Systemeinstellungen in der laufenden Konfigurationsdatei

Wenn Sie eine der Systemkonfigurationseinstellungen auf einem ExtraHop-System ändern, müssen Sie die Aktualisierungen bestätigen, indem Sie die laufende Konfigurationsdatei speichern. Wenn Sie die Einstellungen nicht speichern, gehen die Änderungen verloren, wenn Ihr ExtraHop-System neu gestartet wird.

Um Sie daran zu erinnern, dass sich die aktuelle Konfiguration geändert hat, erscheint (Ungespeicherte Änderungen) neben dem Link Running Config auf der Hauptseite mit den Administrationseinstellungen

sowie **Änderungen anzeigen und speichern** Schaltfläche auf allen Seiten mit Verwaltungseinstellungen, wie unten gezeigt.




1. klicken **Änderungen anzeigen und speichern**.
2. Überprüfen Sie den Vergleich zwischen der alten laufenden Konfiguration und der aktuellen (nicht gespeicherten) laufenden Konfiguration, und wählen Sie dann eine der folgenden Optionen aus:
   - Wenn die Änderungen korrekt sind, klicken Sie auf **Speichern**.
   - Wenn die Änderungen nicht korrekt sind, klicken Sie auf **Stornieren** und machen Sie dann die Änderungen rückgängig, indem Sie auf **Konfiguration zurücksetzen** .

## Bearbeiten Sie die laufende Konfiguration

Die ExtraHop-Administrationseinstellungen bieten eine Schnittstelle zum Anzeigen und Ändern des Codes , der die Standardsystemkonfiguration angibt. Zusätzlich zu den Änderungen an der laufenden Konfigurationsdatei über die Administrationseinstellungen können Änderungen auch an der Config wird ausgeführt Seite.

**Hinweis:** Es wird nicht empfohlen, auf der Seite „Bearbeiten“ Konfigurationsänderungen am Code vorzunehmen. Sie können die meisten Systemänderungen über andere Administrationseinstellungen vornehmen.

## Laden Sie die laufende Konfiguration als Textdatei herunter

Sie können die laufende Konfigurationsdatei auf Ihre Workstation herunterladen. Sie können diese Textdatei öffnen und lokal Änderungen daran vornehmen, bevor Sie diese Änderungen in das Config wird ausgeführt Fenster.

1. Klicken **Config wird ausgeführt**.
2. Klicken **Konfiguration als Datei herunterladen**.

Die aktuell ausgeführte Konfigurationsdatei wird als Textdatei in Ihr Standard-Download-Verzeichnis heruntergeladen.

## ICMPv6-Nachrichten vom Typ „Destination Unreachable“ deaktivieren

Sie können verhindern, dass das ExtraHop-System ICMPv6-Nachrichten vom Typ Destination Unreachable generiert. Möglicherweise möchten Sie ICMPv6-Nachrichten vom Typ Destination Unreachable aus Sicherheitsgründen gemäß RFC 4443 deaktivieren.

Um ICMPv6-Meldungen „Destination Unreachable“ zu deaktivieren, müssen Sie die Running Configuration bearbeiten. Wir empfehlen jedoch, die Running Configuration-Datei nicht manuell zu bearbeiten, ohne dass Sie vom ExtraHop-Support dazu angewiesen werden. Wenn Sie die laufende Konfigurationsdatei manuell falsch bearbeiten, kann dies dazu führen, dass das System nicht mehr verfügbar ist oder keine Daten mehr erfasst werden. Sie können kontaktieren ExtraHop-Unterstützung.

### Bestimmte ICMPv6-Echo-Antwortnachrichten deaktivieren

Sie können verhindern, dass das ExtraHop-System Echo-Antwortnachrichten als Antwort auf ICMPv6-Echoanforderungsnachrichten generiert, die an eine IPv6-Multicast- oder Anycast-Adresse gesendet werden. Möglicherweise möchten Sie diese Nachrichten deaktivieren, um unnötigen Netzwerkverkehr zu reduzieren.

Um bestimmte ICMPv6-Echo-Antwortnachrichten zu deaktivieren, müssen Sie die laufende Konfigurationsdatei bearbeiten. Wir empfehlen jedoch, die laufende Konfigurationsdatei nicht ohne Anweisung des ExtraHop-Supports manuell zu bearbeiten. Eine falsche manuelle Bearbeitung dieser Datei kann dazu führen, dass das System nicht mehr verfügbar ist oder keine Daten mehr erfasst werden. Sie können kontaktieren ExtraHop-Unterstützung.

## Dienstleistungen

Diese Dienste werden im Hintergrund ausgeführt und führen Funktionen aus, für die keine Benutzereingaben erforderlich sind. Diese Dienste können über die Administrationseinstellungen gestartet und gestoppt werden.

#### Aktivieren oder deaktivieren Sie die Management-GUI

Die Management-GUI bietet browserbasierten Zugriff auf das ExtraHop-System. Standardmäßig ist dieser Dienst aktiviert, sodass ExtraHop-Benutzer über einen Webbrowser auf das ExtraHop-System zugreifen können. Wenn dieser Dienst deaktiviert ist, wird die Apache Web Server-Sitzung beendet und der gesamte browserbasierte Zugriff wird deaktiviert.

**Warnung:** Deaktivieren Sie diesen Dienst nur, wenn Sie ein erfahrener ExtraHop-Administrator sind und mit der ExtraHop-CLI vertraut sind.

#### SNMP-Dienst aktivieren oder deaktivieren

Aktivieren Sie den SNMP-Dienst auf dem ExtraHop-System, wenn Ihre Netzwerkgeräteüberwachungssoftware Informationen über das ExtraHop-System sammeln soll. Dieser Dienst ist standardmäßig deaktiviert.

- Aktivieren Sie den SNMP-Dienst auf der Seite Dienste, indem Sie das Kontrollkästchen Deaktiviert aktivieren und dann auf **Speichern**. Nach der Aktualisierung der Seite wird das Kontrollkästchen Aktiviert angezeigt.
- Den SNMP-Dienst konfigurieren und laden Sie die ExtraHop MIB-Datei herunter

#### SSH-Zugriff aktivieren oder deaktivieren

Der SSH-Zugriff ist standardmäßig aktiviert, damit sich Benutzer sicher an der ExtraHop-Befehlszeilenschnittstelle (CLI) anmelden können.

**Hinweis:** Der SSH-Dienst und der Management GUI Service können nicht gleichzeitig deaktiviert werden. Mindestens einer dieser Dienste muss aktiviert sein, um Zugriff auf das System zu gewähren.

#### Den SSL-Sitzungsschlüsselempfänger aktivieren oder deaktivieren (nur Sensor)

Sie müssen den Sitzungsschlüsselempfängerdienst über die Verwaltungseinstellungen aktivieren, bevor das ExtraHop-System Sitzungsschlüssel vom Sitzungsschlüsselweiterleiter empfangen und entschlüsseln kann. Standardmäßig ist dieser Dienst deaktiviert.

**Hinweis:** Wenn Sie dieses Kontrollkästchen nicht sehen und die SSL Decryption-Lizenz erworben haben, wenden Sie sich an ExtraHop-Unterstützung um Ihre Lizenz zu aktualisieren.

### SNMP-Dienst

Konfigurieren Sie den SNMP-Dienst auf Ihrem ExtraHop-System, sodass Sie Ihre Netzwerkgeräteüberwachungssoftware so konfigurieren können, dass Informationen über Ihr ExtraHop-System über das Simple Network Management Protocol (SNMP) erfasst werden.

Beispielsweise können Sie Ihre Monitoring-Software so konfigurieren, dass sie bestimmt, wie viel freier Speicherplatz auf einem ExtraHop-System verfügbar ist, und eine Alarm senden, wenn das System zu über 95% voll ist. Importieren Sie die ExtraHop SNMP MIB-Datei in Ihre Monitoring-Software, um alle ExtraHop-spezifischen SNMP-Objekte zu überwachen. Sie können Einstellungen für SNMPv1/SNMPv2 und SNMPv3 konfigurieren

## Firmware

Die Administrationseinstellungen bieten eine Schnittstelle zum Hochladen und Löschen der Firmware auf ExtraHop-Geräten. Die Firmware-Datei muss von dem Computer aus zugänglich sein, auf dem Sie das Upgrade durchführen werden.

**Bevor Sie beginnen**
Lesen Sie unbedingt die Versionshinweise für die Firmware-Version, die Sie installieren möchten. Die Versionshinweise enthalten Anleitungen zum Upgrade sowie bekannte Probleme, die sich auf kritische Workflows in Ihrem Unternehmen auswirken können.

### Aktualisieren Sie die Firmware auf Ihrem ExtraHop-System

Das folgende Verfahren zeigt Ihnen, wie Sie Ihr ExtraHop-System auf die neueste Firmware-Version aktualisieren. Während der Firmware-Upgrade-Prozess für alle ExtraHop-Appliances ähnlich ist, müssen Sie bei einigen Appliances zusätzliche Überlegungen oder Schritte beachten, bevor Sie die Firmware in Ihrer Umgebung installieren. Wenn Sie Hilfe bei Ihrem Upgrade benötigen, wenden Sie sich an den ExtraHop Support.

**Video:** Sehen Sie sich die entsprechende Schulung an: Firmware aktualisieren

**Wichtig:** Wenn die Einstellungsmigration während des Firmware-Upgrades fehlschlägt, werden die zuvor installierte Firmware-Version und die ExtraHop-Systemeinstellungen wiederhergestellt.

**Checkliste vor dem Upgrade**
Im Folgenden finden Sie einige wichtige Überlegungen und Anforderungen zur Aktualisierung von ExtraHop-Appliances.

- Ein Systemhinweis erscheint auf Konsolen und Sensoren verbunden mit ExtraHop Cloud Services, wenn eine neue Firmware-Version verfügbar ist.
- Stellen Sie sicher, dass Ihr Reveal (x) 360-System auf Version 1 aktualisiert wurde 9.2 vor dem Upgrade Ihres selbstverwalteten Sensoren.
- Wenn Sie ein Upgrade von Firmware-Version 8.7 oder früher durchführen, wenden Sie sich an den ExtraHop-Support, um weitere Informationen zum Upgrade zu erhalten.
- Wenn Sie mehrere Typen von ExtraHop-Appliances haben, müssen Sie diese in der folgenden Reihenfolge aktualisieren:

  1. Konsole
  2. Sensoren (EDA und Ultra)
  3. Plattenläden
  4. Geschäfte für Pakete

**Hinweis:** Ihr Browser läuft möglicherweise nach 5 Minuten Inaktivität ab. Aktualisieren Sie die Browserseite, wenn das Update unvollständig erscheint.

Wenn bei der Browsersitzung ein Timeout auftritt, bevor das ExtraHop-System den Aktualisierungsvorgang abschließen kann, können Sie die folgenden Verbindungstests durchführen, um den Status des Upgrade-Vorgangs zu überprüfen:

- Pingen Sie die Appliance über die Kommandozeile einer anderen Appliance oder Client-Workstation an.

- Rufen Sie in den Administrationseinstellungen auf einer Konsole den Status der Appliance auf Verbundene Geräte verwalten Seite.
- Stellen Sie über die iDRAC-Schnittstelle eine Verbindung zur Appliance her.

### Konsolen-Upgrades

- Für umfangreiche Konsolenbereitstellungen (Verwaltung von 50.000 Geräten oder mehr) sollten Sie mindestens eine Stunde einplanen, um das Upgrade durchzuführen.
- Die Firmware-Version der Konsole muss größer oder gleich der Firmware-Version aller angeschlossenen Geräte sein. Um die Funktionskompatibilität sicherzustellen, sollte auf allen angeschlossenen Geräten die Firmware-Version 8.7 oder höher ausgeführt werden.

### Recordstore-Upgrades

- Aktualisieren Sie Recordstores nicht auf eine Firmware-Version, die neuer ist als die Version, die auf den angeschlossenen Konsolen und Sensoren installiert ist.
- Nach dem Upgrade der Konsole und Sensoren, deaktiviere die Datensatz von Datensätzen im Recordstore bevor Sie den Recordstore aktualisieren.
- Sie müssen alle Recordstore-Knoten in einem Recordstore-Cluster aktualisieren. Der Cluster funktioniert nicht richtig, wenn die Knoten unterschiedliche Firmware-Versionen verwenden.

  **Wichtig:** Die Botschaft `Could not determine ingest status on some nodes` und `Error` erscheinen auf der Seite Cluster-Datenmanagement in den Verwaltungseinstellungen der aktualisierten Knoten, bis alle Knoten im Cluster aktualisiert sind. Diese Fehler werden erwartet und können ignoriert werden.
- Sie müssen die Aufnahme von Datensätzen und die Neuzuweisung von Shards von der Cluster-Datenmanagement Seite, nachdem alle Knoten im Recordstore-Cluster aktualisiert wurden.

### Packetstore-Upgrades

- Aktualisieren Sie Packetstores nicht auf eine Firmware-Version, die neuer ist als die Version, die auf verbundenen Konsolen installiert ist, und Sensoren.

### Aktualisieren Sie die Firmware auf einer Konsole und einem Sensor

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Einstellungen der Appliance Abschnitt, klicken **Firmware**.
3. Aus dem **Verfügbare Firmware** Wählen Sie in der Dropdownliste die Firmware-Version aus, die Sie installieren möchten. Die empfohlene Version ist standardmäßig ausgewählt.

   **Hinweis:** Für Sensoren enthält die Liste nur Firmware-Versionen, die mit der Version kompatibel sind, die auf der angeschlossenen Konsole ausgeführt wird.
4. klicken **Downloaden und installieren**.

Nach der erfolgreichen Installation des Firmware-Upgrades wird die ExtraHop-Appliance neu gestartet.

### Aktualisieren Sie die Firmware in Plattenläden

1. Laden Sie die Firmware für die Appliance von der ExtraHop Kundenportal auf deinen Computer.
2. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
3. klicken **Cluster-Datenmanagement**.
4. klicken **Record Ingest deaktivieren**.
5. klicken **Admin** um zur Hauptverwaltungsseite zurückzukehren.
6. klicken **Firmware**.
7. klicken **Aufrüsten**.

8. Wählen Sie auf der Seite Firmware aktualisieren eine der folgenden Optionen aus:
   - Um Firmware aus einer Datei hochzuladen, klicken Sie auf **Wählen Sie Datei**, navigiere zum `.tar` Datei, die Sie hochladen möchten, und klicken Sie **Offen**.
   - Um Firmware von einer URL hochzuladen, klicken Sie auf **von URL abrufen** stattdessen und geben Sie dann die URL in das Firmware-URL Feld.
9. klicken **Aufrüsten**.
   Das ExtraHop-System initiiert das Firmware-Upgrade. Sie können den Fortschritt des Upgrades mit dem Aktualisierung Fortschrittsbalken. Die Appliance wird nach der Installation der Firmware neu gestartet.
10. Wiederholen Sie die Schritte 6-9 auf allen verbleibenden Recordstore-Clusterknoten.

**Nächste Schritte**
Nachdem alle Knoten im Recordstore-Cluster aktualisiert wurden, aktivieren Sie die Datensatzaufnahme und die Shard-Neuzuweisung auf dem Cluster erneut. Sie müssen diese Schritte nur auf einem Datensatzspeicherknoten ausführen.

1. Klicken Sie im Abschnitt Clustereinstellungen erkunden auf **Cluster-Datenmanagement**.
2. klicken **Record Ingest aktivieren**.
3. klicken **Shard-Neuzuweisung aktivieren**.

### Aktualisieren Sie die Firmware in Packetstores

1. Laden Sie die Firmware für die Appliance von der ExtraHop Kundenportal auf deinen Computer.
2. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
3. klicken **Aufrüsten**.
4. Wählen Sie auf der Seite Firmware aktualisieren eine der folgenden Optionen aus:
   - Um Firmware aus einer Datei hochzuladen, klicken Sie auf **Wählen Sie Datei**, navigiere zum `.tar` Datei, die Sie hochladen möchten, und klicken Sie **Offen**.
   - Um Firmware von einer URL hochzuladen, klicken Sie auf **von URL abrufen** stattdessen und geben Sie dann die URL in das Firmware-URL Feld.
5. Optional: Wenn Sie das Gerät nach der Installation der Firmware nicht automatisch neu starten möchten, löschen Sie das **Gerät nach der Installation automatisch neu starten** Checkbox.
6. klicken **Aufrüsten**.
   Das ExtraHop-System initiiert das Firmware-Upgrade. Sie können den Fortschritt des Upgrades mit dem Aktualisierung Fortschrittsbalken. Die Appliance wird nach der Installation der Firmware neu gestartet.
7. Wenn Sie sich nicht dafür entschieden haben, die Appliance automatisch neu zu starten, klicken Sie auf **Neustarten** um das System neu zu starten.

   Nachdem das Firmware-Update erfolgreich installiert wurde, zeigt die ExtraHop-Appliance die Versionsnummer der neuen Firmware in den Administrationseinstellungen an.

### Vernetzte Sensoren in Reveal (x) 360 aufrüsten
Administratoren können ein Upgrade durchführen Sensoren die mit Reveal (x) 360 verbunden sind.

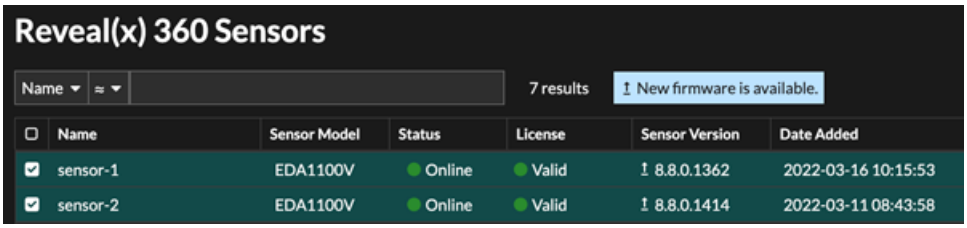
**Bevor Sie beginnen**

- Ihr Benutzerkonto muss über Rechte für Reveal (x) 360 für die System- und Zugriffsverwaltung oder die Systemadministration verfügen.

Hier sind einige Überlegungen zur Aufrüstung von Sensoren:

- Die Sensoren müssen mit den ExtraHop Cloud Services verbunden sein
- Benachrichtigungen werden angezeigt, wenn eine neue Firmware-Version verfügbar ist
- Sie können mehrere aktualisieren Sensoren zur gleichen Zeit

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann auf **Sensoren**.
   Sensoren, die für ein Upgrade in Frage kommen, zeigen einen Aufwärtspfeil in der Sensorversion Feld.




2. Markieren Sie das Kästchen neben jedem Sensor die Sie aktualisieren möchten.
3. In der Angaben zum Sensor Bereich, wählen Sie die Firmware-Version aus dem **Verfügbare Firmware** Dropdownliste.

   In der Dropdownliste werden nur Versionen angezeigt, die mit den ausgewählten Versionen kompatibel sind Sensoren.

   Nur die ausgewählten Sensoren für die ein Firmware-Upgrade verfügbar ist, finden Sie im Fühler Bereich „Details“.
4. Klicken Sie **Firmware installieren**.

   Wenn das Upgrade abgeschlossen ist, Sensorversion Das Feld wurde mit der neuen Firmware-Version aktualisiert.

## Systemzeit

Auf der Seite Systemzeit werden die aktuellen Zeiteinstellungen angezeigt, die für Ihr ExtraHop-System konfiguriert sind. Zeigen Sie die aktuellen Systemzeiteinstellungen, die Standardanzeigezeit für Benutzer und Details für konfigurierte NTP-Server an.

Systemzeit ist die Uhrzeit und das Datum, die von Diensten verfolgt werden, die auf dem ExtraHop-System ausgeführt werden, um genaue Zeitberechnungen zu gewährleisten. Standardmäßig ist die Systemzeit auf dem Sensor oder der Konsole lokal konfiguriert. Für eine bessere Genauigkeit empfehlen wir, die Systemzeit über einen NTP-Zeitserver zu konfigurieren.

Bei der Datenerfassung muss die Systemzeit mit der Uhrzeit der angeschlossenen Sensoren übereinstimmen, um sicherzustellen , dass die Zeitstempel in geplanten Berichten, exportierten Dashboards und Diagrammmetriken korrekt und vollständig sind. Wenn Probleme mit der Zeitsynchronisierung auftreten, überprüfen Sie, ob die konfigurierte Systemzeit, externe Zeitserver oder NTP-Server korrekt sind. Setzen Sie die Systemzeit zurück oder NTP-Server synchronisieren bei Bedarf

Die folgende Tabelle enthält Details zur aktuellen Systemzeitkonfiguration. Klicken Sie **Zeit konfigurieren** zu Systemzeiteinstellungen konfigurieren.

| Detail | Beschreibung |
|---|---|
| Zeitzone | Zeigt die aktuell gewählte Zeitzone an. |
| Systemzeit | Zeigt die aktuelle Systemzeit an. |
| Zeitserver | Zeigt eine kommagetrennte Liste der konfigurierten Zeitserver an. |

### Standardanzeigezeit für Benutzer

Im Abschnitt Standardanzeigezeit für Benutzer wird die Uhrzeit angezeigt, die allen Benutzern im ExtraHop-System angezeigt wird, es sei denn, ein Benutzer manuell ändert ihre angezeigte Zeitzone.

Um die Standardanzeigezeit zu ändern, wählen Sie eine der folgenden Optionen und klicken Sie dann auf **Änderungen speichern**:

- Uhrzeit des Browsers
- Systemzeit
- UTC

**NTP-Status**

Die NTP-Statustabelle zeigt die aktuelle Konfiguration und den Status aller NTP-Server an, die die Systemuhr synchron halten. Die folgende Tabelle enthält Details zu jedem konfigurierten NTP-Server. Klicken Sie **Jetzt synchronisieren** um die aktuelle Systemzeit mit einem Remote-Server zu synchronisieren.

| | |
|---|---|
| Fernbedienung | Der Hostname oder die IP-Adresse des Remote-NTP-Servers, mit dem Sie die Synchronisierung konfiguriert haben. |
| st | Die Stratum-Ebene, 0 bis 16. |
| t | Die Art der Verbindung. Dieser Wert kann `u` für Unicast oder Manycast, `b` für Broadcast oder Multicast, `l` für lokale Referenzuhr, `s` für symmetrischen Peer, `A` für einen Manycast-Server `B` für einen Broadcast-Server, oder `M` für einen Multicast-Server. |
| wenn | Das letzte Mal, als der Server für diese Uhrzeit abgefragt wurde. Der Standardwert ist Sekunden, oder `m` wird minutenlang angezeigt, `h` stundenlang und `d` tagelang. |
| Umfrage | Wie oft der Server nach der Uhrzeit abgefragt wird, mindestens 16 Sekunden bis maximal 36 Stunden. |
| erreichen | Wert, der die Erfolgs- und Ausfallrate der Kommunikation mit dem Remoteserver Server. Erfolg bedeutet, dass das Bit gesetzt ist, Misserfolg bedeutet, dass das Bit nicht gesetzt ist. `377` ist der höchste Wert. |
| Verzögerung | Die Roundtrip-Zeit (RTT) der ExtraHop-Appliance, die mit dem Remote-Server kommuniziert, in Millisekunden. |
| Offset | Gibt an, wie weit die Uhr der ExtraHop-Appliance von der vom Server gemeldeten Uhrzeit entfernt ist. Der Wert kann positiv oder negativ sein und wird in Millisekunden angezeigt. |
| Jitter | Gibt den Unterschied zwischen zwei Stichproben in Millisekunden an. |

## Systemzeit konfigurieren

Standardmäßig synchronisiert das ExtraHop-System die Systemzeit über die NTP-Server (Netzwerk Time Protokoll ) *.extrahop.pool.ntp.org. Wenn Ihre Netzwerkumgebung verhindert, dass das ExtraHop-System mit diesen Zeitservern kommuniziert, müssen Sie eine alternative Zeitserverquelle konfigurieren.

**Bevor Sie beginnen**

**Wichtig:** Konfigurieren Sie immer mehr als einen NTP-Server , um die Genauigkeit und Zuverlässigkeit der auf dem System gespeicherten Zeit zu erhöhen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der **Einstellungen der Appliance** Abschnitt, klicken **Systemzeit**.
3. klicken **Zeit konfigurieren**.
4. Wählen Sie Ihre Zeitzone aus der Drop-down-Liste aus und klicken Sie dann auf **Speichern und fortfahren**.
5. Auf dem Zeit-Setup Seite, wählen Sie eine der folgenden Optionen:
   - Zeit manuell einstellen

**Hinweis:** Sie können die Uhrzeit für Sensoren, die von einer Konsole oder Reveal (x) 360 verwaltet werden, nicht manuell einstellen.

- Zeit mit NTP-Server einstellen

6. Wählen **Zeit mit NTP-Server einstellen** und dann klicken **Wählen**.

   Die ExtraHop-Zeitserver, `0.extrahop.pool.ntp.org`, `1. extrahop.pool.ntp.org`, `2. extrahop.pool.ntp.org`, und `3. extrahop.pool.ntp.org` erscheinen in den ersten vier Zeitserver standardmäßig Felder.
7. Geben Sie die IP-Adresse oder den vollqualifizierten Domänenname (FQDN) für die Zeitserver in der Zeitserver Felder. Sie können bis zu neun Zeitserver haben.

   **Hinweis:** Nachdem Sie den fünften Zeitserver hinzugefügt haben, klicken Sie auf **Server hinzufügen** um bis zu vier zusätzliche Timer-Serverfelder anzuzeigen.
8. klicken **Erledigt**.

Die NTP-Status Die Tabelle zeigt eine Liste von NTP-Servern, die die Systemuhr synchron halten. Um die aktuelle Systemzeit eines Remoteservers zu synchronisieren, klicken Sie auf **Jetzt synchronisieren** knopf.

## Herunterfahren oder neu starten

Sie können die Trace-Appliance in den Administrationseinstellungen herunterfahren oder neu starten.

1. In der Einstellungen der Appliance Abschnitt, klicken **Herunterfahren oder Neustarten**.
2. Wählen Sie in der Spalte Aktionen eine der folgenden Optionen aus:
   - klicken **Neustarten** und klicken Sie dann auf der Bestätigungsseite auf **Neustarten** um die Appliance neu zu starten.
   - klicken **Herunterfahren**, und klicken Sie dann auf der Bestätigungsseite auf **Herunterfahren** um das System herunterzufahren und das Gerät auszuschalten.

## Lizenz

Die Administrationseinstellungen bieten eine Schnittstelle zum Hinzufügen und Aktualisieren von Lizenzen für Zusatzmodule und andere Funktionen, die im ExtraHop-System verfügbar sind. Die Seite Lizenzverwaltung enthält die folgenden Lizenzinformationen und Einstellungen:

**Lizenz verwalten**

Bietet eine Schnittstelle zum Hinzufügen und Aktualisieren des ExtraHop-Systems

**Informationen zum System**

Zeigt die Identifikations- und Ablaufinformationen zum ExtraHop-System an.

**Funktionen**

Zeigt die Liste der lizenzierten Funktionen an und ob die lizenzierten Funktionen aktiviert oder deaktiviert sind.

### Registrieren Sie Ihr ExtraHop-System

Dieses Handbuch enthält Anweisungen zum Anwenden eines neuen Produktschlüssels und zur Aktivierung aller von Ihnen gekauften Module. Sie müssen über Rechte auf dem ExtraHop-System verfügen, um auf die Administrationseinstellungen zugreifen zu können.

#### Registrieren Sie das Gerät

#### Bevor Sie beginnen

**Hinweis:** Wenn Sie einen Sensor oder eine Konsole registrieren, können Sie optional den Produktschlüssel eingeben, nachdem Sie die EULA akzeptiert und sich beim ExtraHop-System angemeldet haben ( `https://<extrahop_ip_address>/`).

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Lesen Sie die Lizenzvereinbarung, wählen Sie Ich stimme zu, und klicken Sie dann **Einreichen**.
3. Geben Sie auf dem Anmeldebildschirm Folgendes ein `Einrichten` für den Benutzernamen.
4. Wählen Sie für das Passwort eine der folgenden Optionen aus:
   - Geben Sie bei 1U- und 2U-Appliances die Seriennummer ein, die auf dem Etikett auf der Rückseite der Appliance aufgedruckt ist. Die Seriennummer finden Sie auch auf dem LCD-Display an der Vorderseite des Geräts in der `Info` Abschnitt.
   - Geben Sie für den EDA 1100 die Seriennummer ein, die im `Appliance info` Abschnitt des LCD-Menüs. Die Seriennummer ist auch auf der Unterseite des Geräts aufgedruckt.
   - Geben Sie für den EDA 1200 die Seriennummer ein, die auf der Rückseite des Geräts aufgedruckt ist.
   - Geben Sie für eine virtuelle Appliance in AWS die Instanz-ID ein. Dabei handelt es sich um die Zeichenfolge, die auf i- folgt (aber nicht auf i- selbst).
   - Geben Sie für eine virtuelle Appliance in GCP die Instanz-ID ein.
   - Geben Sie für alle anderen virtuellen Appliances Folgendes ein `Standard`.
5. klicken **Loggen Sie sich ein**.
6. In der Einstellungen der Appliance Abschnitt, klicken **Lizenz**.
7. klicken **Lizenz verwalten**.
8. Wenn Sie einen Produktschlüssel haben, klicken Sie auf **Registrieren** und geben Sie Ihren Produktschlüssel in das Feld ein.

   **Hinweis:** Wenn Sie eine Lizenzdatei vom ExtraHop Support erhalten haben, klicken Sie auf **Lizenz verwalten**, klicken **Aktualisiere**, fügen Sie dann den Inhalt der Datei in das Lizenz eingeben Feld. klicken **Aktualisiere**.
9. klicken **Registrieren**.

**Nächste Schritte**
Haben Sie weitere Fragen zu ExtraHop Licensing Works? Sehen Sie die Häufig gestellte Fragen zur Lizenz.

**Problembehandlung bei der Lizenzserverkonnektivität**

Bei ExtraHop-Systemen, die für die Verbindung mit ExtraHop Cloud Services lizenziert und konfiguriert sind, erfolgt die Registrierung und Überprüfung über eine HTTPS-Anfrage an ExtraHop Cloud Services.

Wenn Ihr ExtraHop-System nicht oder noch nicht für ExtraHop Cloud Services lizenziert ist, versucht das System, das System über eine DNS-TXT-Anfrage für zu registrieren `regions.hopcloud.extrahop.com` und eine HTTPS-Anfrage an alle ExtraHop Cloud Services-Regionen. Wenn diese Anfrage fehlschlägt, versucht das System, über DNS-Serverport 53 eine Verbindung zum ExtraHop-Lizenzserver herzustellen. Das folgende Verfahren ist nützlich, um zu überprüfen, ob das ExtraHop-System über DNS mit dem Lizenzserver kommunizieren kann.

Öffnen Sie eine Terminalanwendung auf Ihrem Windows-, Linux- oder macOS-Client, der sich im selben Netzwerk wie Ihr ExtraHop-System befindet, und führen Sie den folgenden Befehl aus:

```
nslookup -type=NS d.extrahop.com
```

Wenn die Namensauflösung erfolgreich ist, wird eine Ausgabe ähnlich der folgenden angezeigt:

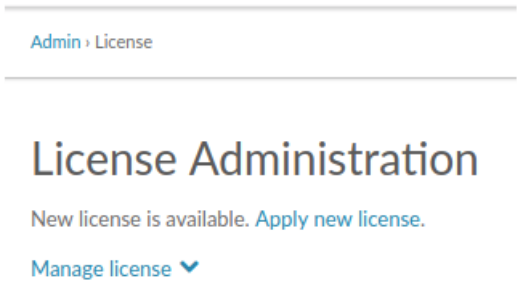
```
Non-authoritative answer:
d.extrahop.com  nameserver = ns0.use.d.extrahop.com.
d.extrahop.com  nameserver = ns0.usw.d.extrahop.com.
```

Wenn die Namensauflösung nicht erfolgreich ist, stellen Sie sicher, dass Ihr DNS-Server richtig konfiguriert ist, um nach `extrahop.com` domäne.

## Wenden Sie eine aktualisierte Lizenz an

Wenn Sie ein neues Protokollmodul, einen neuen Dienst oder eine neue Funktion erwerben, ist die aktualisierte Lizenz automatisch auf dem ExtraHop-System verfügbar. Sie müssen die aktualisierte Lizenz jedoch über die Administrationseinstellungen auf das System anwenden, damit die neuen Änderungen wirksam werden.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Appliance-Einstellungen auf **Lizenz**. Es wird eine Meldung über die Verfügbarkeit Ihrer neuen Lizenz angezeigt, wie in der folgenden Abbildung dargestellt.




3. klicken **Neue Lizenz beantragen**. Der Aufnahmevorgang wird neu gestartet, was einige Minuten dauern kann.

**Hinweis:** Wenn Ihre Lizenz nicht automatisch aktualisiert wird, Problembehandlung bei der Lizenzserverkonnektivität oder wenden Sie sich an den ExtraHop Support.

## Eine Lizenz aktualisieren

Wenn ExtraHop Support Ihnen eine Lizenzdatei zur Verfügung stellt, können Sie diese Datei auf Ihrem Gerät installieren, um die Lizenz zu aktualisieren.

**Hinweis:** Wenn Sie den Produktschlüssel für Ihr Gerät aktualisieren möchten, müssen Sie registrieren Sie Ihr ExtraHop-System.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Einstellungen der Appliance Abschnitt, klicken **Lizenz**.
3. klicken Lizenz verwalten.
4. klicken **Aktualisiere**.
5. In der Lizenz eingeben Textfeld, geben Sie die Lizenzinformationen für das Modul ein.

   Fügen Sie den Lizenztext ein, den Sie vom ExtraHop Support erhalten haben. Stellen Sie sicher, dass Sie den gesamten Text angeben, einschließlich des `BEGIN` und `END` Linien, wie im Beispiel unten gezeigt:

```
-----BEGIN EXTRAHOP LICENSE-----
serial=ABC123D;
dossier=1234567890abcdef1234567890abcdef;
mod_cifs=1;
mod_nfs=1;
mod_amf=0;
live_capture=1;
capture_upload=1;
...
ssl_decryption=0;
+++;
ABCabcDE/FGHIjklm12nopqrstuvwXYZAB12345678abcde901abCD;
12ABCDEFG1HIJklmnOP+1aA=;
```

```
=abcd;
-----END EXTRAHOP LICENSE-----
```

6. klicken **Aktualisiere**.

## Festplatten

Die Festplatten Diese Seite enthält Informationen zur Konfiguration und zum Status der Festplatten in Ihrer Trace-Appliance sowie der Festplatten in allen angeschlossenen Speichereinheiten.

**Hinweis:** Wir empfehlen Ihnen, die Einstellungen für den Empfang zu konfigurieren E-Mail-Benachrichtigungen über den Zustand Ihres Systems. Wenn auf einer Festplatte Probleme auftreten, werden Sie gewarnt.

Die folgenden Informationen werden auf der Seite angezeigt:

**Karte fahren**

Bietet eine visuelle Darstellung der Vorderseite der Trace-Appliance. Die Laufwerkszuordnung wird in den Administrationseinstellungen der virtuellen Trace-Appliance nicht angezeigt.

**Details zur RAID-Festplatte**

Bietet Zugriff auf detaillierte Informationen zu allen Festplatten im Knoten.

**Paketshop**

Zeigt Informationen über Festplatten an, die für die Paketspeicherung reserviert sind, und die Option, die Packetstore-Festplatte zu verschlüsseln. Weitere Informationen finden Sie in der Verschlüsseln Sie die Packetstore-Festplatte Abschnitt.

**Direkt verbundene Festplatten**

Zeigt Informationen zu den SD-Speicherkarten an. Die Speicherkarten haben die folgenden Rollen:

**Firmware**

Zeigt Informationen über Festplatten an, die für die Firmware reserviert sind.

**Nützlichkeit**

Zeigt Informationen über Festplatten an, die für Systemdateien reserviert sind.

**Erweiterte Speichereinheiten**

Zeigt Informationen zu ExtraHop Extended Storage Units an.

### Verschlüsseln Sie die Packetstore-Festplatte

Sie können die Festplatte verschlüsseln, einschließlich der angeschlossenen erweiterten Speichereinheiten, auf denen Paketerfassungen gespeichert werden, um die Sicherheit zu erhöhen. Die Packetstore-Festplatte ist mit einer 256-Bit-AES-Verschlüsselung gesichert.

**Warnung:** Sie können eine Packetstore-Festplatte nicht entschlüsseln, nachdem sie verschlüsselt wurde. Sie können eine verschlüsselte Festplatte neu formatieren. Alle auf der Festplatte gespeicherten Daten gehen jedoch verloren. Informationen zum sicheren Löschen (Secure Wipe) aller Systemdaten finden Sie in der Medienleitfaden für ExtraHop Rescue.

**Wichtig:** Der Packetstore ist gesperrt, wenn die ETA-Appliance neu gestartet wird. Bevor Pakete auf die Festplatte geschrieben werden können, müssen Sie die Festplatte von Packetstore-Verschlüsselungseinstellungen Seite.

1. In der Einstellungen der Appliance Abschnitt, klicken **Festplatten**.
2. Navigiere zum Packetstore-Verschlüsselungseinstellungen Seite.

| Option | Description |
| --- | --- |
| **Für virtuelle Appliances** | In der Direkt verbundene Festplatten Tabelle, klicken **Einstellungen**. |

| Option | Description |
| --- | --- |
| **Für physische Geräte** | In der Paketspeicher Abschnitt, neben Packetstore-Verschlüsselung, klicken **Einstellungen**. |

3. Klicken **Packetstore verschlüsseln**.
4. Geben Sie einen Festplattenverschlüsselungsschlüssel an, indem Sie eine der folgenden Optionen wählen.
   - Um die Festplatte mit einer Passphrase zu verschlüsseln, geben Sie eine Passphrase mit mindestens 8 Zeichen in das Passphrase und Bestätigen Felder. Die Passphrase muss eine Kombination aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.
   - Um die Festplatte mit einer Schlüsseldatei zu verschlüsseln, klicken Sie auf **Datei wählen**, und suchen Sie dann nach einer Verschlüsselungsschlüsseldatei.
5. Klicken **Verschlüsseln**.

## Ändern Sie den Verschlüsselungsschlüssel für die Paketerfassungsfestplatte

1. In der Status Abschnitt, klicken **Festplatten**.
2. In der Datenspeicher Abschnitt, klicken **Packetstore-Verschlüsselungseinstellungen**.
3. klicken **Packetstore-Verschlüsselungsschlüssel ändern**.
4. Geben Sie den vorhandenen Verschlüsselungsschlüssel an.

| Option | Description |
| --- | --- |
| **Wenn Sie eine Verschlüsselungspassphrase eingegeben haben** | Geben Sie eine Passphrase in das Passphrase Feld. |
| **Wenn Sie eine Verschlüsselungsschlüsseldatei ausgewählt haben** | klicken **Wählen Sie Datei**, und navigieren Sie dann zu einer Verschlüsselungsschlüsseldatei. |

5. Geben Sie einen neuen Festplattenverschlüsselungsschlüssel an.

| Option | Description |
| --- | --- |
| **Um eine Verschlüsselungspassphrase einzugeben** | Geben Sie eine Passphrase in das Passphrase und Bestätigen Felder. |
| **Um eine Verschlüsselungsschlüsseldatei auszuwählen** | klicken **Wählen Sie Datei**, und navigieren Sie dann zu einer Verschlüsselungsschlüsseldatei. |

6. klicken **Schlüssel ändern**.

## Erweitern Sie die ETA 6150 oder 8250 um Speicherkapazität

Wenn Sie Ihrem ExtraHop-Paketspeicher zusätzliche Speicherkapazität hinzufügen, können Sie mehr Pakete speichern und die Menge an Lookback erweitern, die bei der Ausführung von Paketabfragen verfügbar ist. Sie können ExtraHop Extended Storage Units problemlos zu einem Packetstore hinzufügen und alle Pakete behalten, die derzeit im Packetstore gespeichert sind.

### Kompatibilität

Die ExtraHop Extended Storage Unit (ESU) ist in zwei Modellen erhältlich, der 72-TB-ESU und der 96-TB-ESU.

| ExtraHop Paketshop | Erweiterte Speichereinheit |
| --- | --- |
| ETA 6150 | • 72 TB<br>• 96 TB ESU |

| ExtraHop Paketshop | Erweiterte Speichereinheit |
|---|---|
| | Sie können eine Mischung aus 72-TB- und 96-TB-ESU an die ETA 6150 anschließen. |
| ETA 8250 | • 96 TB ESU |
| Sie können bis zu vier ESUs an einen Packetstore anschließen. | |

**Voraussetzungen für die Installation**

Bevor Sie Ihre ESU anschließen, stellen Sie sicher, dass Sie die folgenden Artikel zur Verfügung haben:

- ExtraHop Packetstore mit Firmware 7.2 oder höher. Firmware 7.4 ist erforderlich, um die ESU zu verschlüsseln. Wenn Sie den Packetstore nicht bereitgestellt haben, folgen Sie den Anweisungen in der Stellen Sie den ETA 6150-Paketspeicher bereit und Stellen Sie den ETA 8250-Paketstore bereit Führungen.
- ExtraHop-Lizenz für die erweiterte Packetstore-Funktion
- ExtraHop erweiterte Speichereinheit
- 2 U Rackplatz und elektrische Anschlüsse für 2 x 600-W-Stromversorgungen.
- Stromkabel
- SAS-Kabel
- Schienen-Kit

**Richten Sie die erweiterte Speichereinheit ein**

1. Installieren Sie die erweiterte Speichereinheit mit dem mitgelieferten Rackmontage-Kit in Ihrem Rechenzentrum. Das Montageset unterstützt die meisten Racks mit vier Pfosten mit runden oder quadratischen Löchern.
2. Schließen Sie die Stromkabel an die Stromversorgungseinheiten (PSUs) an.

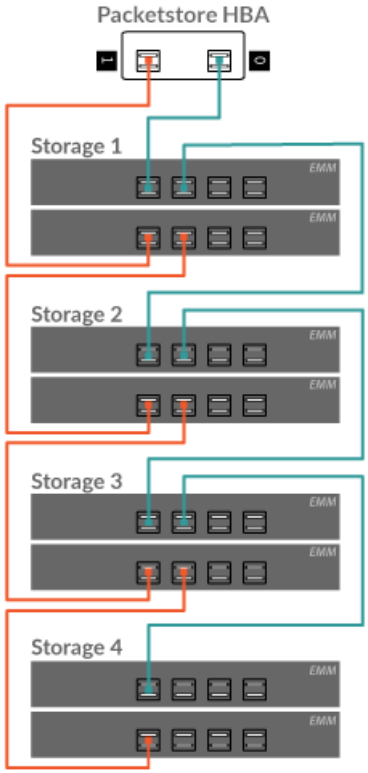
**Schließ den Packetstore**

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Einstellungen der Appliance Abschnitt, klicken **Herunterfahren oder Neustarten**.
3. In der Aktionen Spalte, klicken **Herunterfahren**.
4. Klicken Sie auf der Bestätigungsseite auf **Herunterfahren**.

**Schließen Sie die erweiterte Speichereinheit an**

Die erweiterte Speichereinheit ist über beide Gehäuseverwaltungsmodule (EMMs) mit dem Packetstore verbunden. Jedes EMM hat vier Anschlüsse für den Anschluss der SAS-Kabel.

In einer redundanten Konfiguration sind die Speichereinheiten in einer Reihe miteinander verbunden, wobei eine der erweiterten Speichereinheiten an beide Hostbusadapter (HBA) -Ports im Packetstore angeschlossen ist, wie in der folgenden Abbildung dargestellt.




1. Verbinden Sie die SAS-Kabel mit den EMM-SAS-Anschlüssen der Extended Storage Unit und mit den HBA-Ports am Packetstore. Schließen Sie das SAS-Kabel für die erste Speichereinheit wie folgt an:

   - HBA-Port 0 (rechts) zum oberen EMM-Port 1
   - HBA-Port 1 (links) zum unteren EMM-Port 1

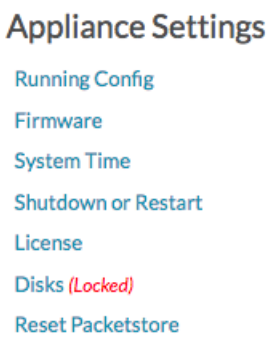
   Schieben Sie das Kabel in den Stecker, bis es einrastet. Grüne Verbindungsleuchten erscheinen neben den Anschlüssen, wenn die ESU und der Packetstore beide eingeschaltet sind.

   **Hinweis:**
   - Die Anschlüsse an beiden Enden des SAS-Kabels sind universell kodiert. Sie können jedes Ende des Kabels an das EMM oder den HBA im Packetstore anschließen.
   - Schließen Sie das SAS-Kabel mit der blauen Pull-Lasche an der Oberseite des Anschlusses an das EMM an.
   - Schließen Sie das SAS-Kabel so an den HBA im Packetstore an, dass sich die blaue Pull-Lasche an der Unterseite des Anschlusses befindet.
   - Um das SAS-Kabel zu entfernen, ziehen Sie an der Pull-Lasche, um das Kabel vom Anschluss am EMM und am Packetstore zu Freigabe.
2. Verkabeln Sie alle zusätzlichen Speichereinheiten wie oben dargestellt.
3. Vergewissern Sie sich, dass der Netzschalter an beiden Netzteilen ausgeschaltet ist, und schließen Sie dann die Netzteile an die Stromquelle an.
4. Schalten Sie die PSUs an jeder ESU ein und warten Sie dann 60 Sekunden, bevor Sie die Trace-Appliance einschalten.

**Befestigen Sie die erweiterte Speichereinheit**

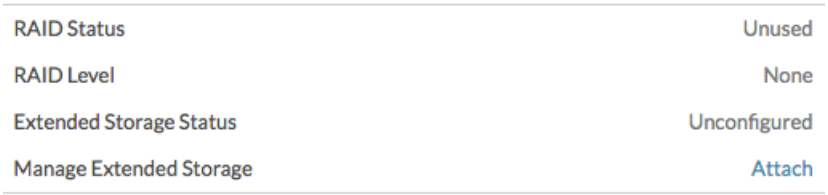
1. Mach den Packetstore an.
2. Loggen Sie sich in die Administrationseinstellungen ein.

   **Hinweis:** Wenn der Packetstore zuvor verschlüsselt war, wird er gesperrt, wenn er eingeschaltet wird. Ein verschlüsselter Packetstore muss gesperrt werden, bevor Sie die ESU anschließen können.

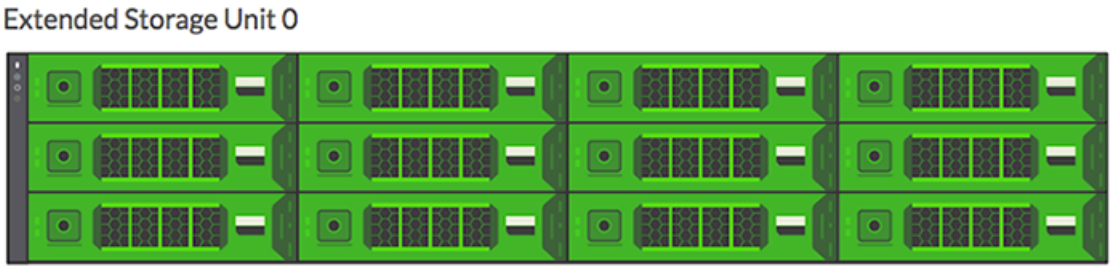



3. In der Einstellungen der Appliance Abschnitt, klicken **Festplatten**.
4. Vergewissern Sie sich, dass alle Laufwerke im Bereich Drive Map grün gefärbt sind, was darauf hinweist, dass sie fehlerfrei sind. Wenn eine Festplatte fehlerhaft ist, wenden Sie sich an ExtraHop-Unterstützung.

5. Am unteren Rand der Festplatten Seite, klick **Erweiterte Speichereinheiten**.
6. In der Unbenutzte Festplatten Abschnitt für die erweiterte Speichereinheit, klicken Sie **Anhängen**, und klicken Sie dann auf **OK**.




7. Stellen Sie nach Abschluss der Konfiguration sicher, dass alle Laufwerke in der erweiterten Speichereinheit grün gefärbt sind, was darauf hinweist, dass sie fehlerfrei sind. Wenn eine Festplatte fehlerhaft ist (gelb), wenden Sie sich an ExtraHop-Unterstützung.




8. Wiederholen Sie die Schritte 6 und 7 für alle weiteren erweiterten Speichereinheiten.
9. Optional: Wenn der Packetstore gesperrt ist, müssen Sie ihn von Packetstore-Verschlüsselungseinstellungen Seite, bevor die ESU verschlüsselt und neue Pakete gespeichert werden können.

## Verwaltung erweiterter Speichereinheiten mit einem ausländischen Packetstore-Status

Wenn eine erweiterte Speichereinheit mit einer vorhandenen RAID-Konfiguration an einen RAID-Controller auf der Trace-Appliance angeschlossen ist, wird die erweiterte Speichereinheit als „fremd“ bezeichnet. Dieser Status kann auftreten, wenn eine erweiterte Speichereinheit zuvor angeschlossen und dann vom RAID-Controller auf der Trace-Appliance getrennt wurde und wenn die erweiterte Speichereinheit auf einem anderen RAID-Controller als der Trace-Appliance konfiguriert wurde, mit der sie ursprünglich verbunden war.

**Für erweiterte Speichereinheiten, die getrennt und dann wieder mit derselben Trace-Appliance verbunden wurden**

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Einstellungen der Appliance Abschnitt, klicken **Festplatten**.
3. klicken **Erweiterte Speichereinheiten**.
4. klicken **Fremde Packetstore-Festplatten importieren**.
   Die erweiterte Speichereinheit wird automatisch konfiguriert und ist bereit, Pakete zu speichern.

**Für erweiterte Speichereinheiten, die auf einem anderen Gerät als der Trace-Appliance konfiguriert sind**

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Einstellungen der Appliance Abschnitt, klicken **Festplatten**.
3. klicken **Erweiterte Speichereinheiten**.
4. klicken **Fremde Packetstore-Festplatten importieren**, und klicken Sie dann auf **OK**.
5. In der RAID-Informationen Abschnitt, klicken **Konfiguration aufheben**, und klicken Sie dann auf **OK**.
6. Nachdem die Packetstore-Diskette gelöscht wurde, klicken Sie auf **Anhängen** und dann klicken **OK**.
   Die erweiterte Speichereinheit wird automatisch konfiguriert und ist bereit, Pakete zu speichern.

## Packetstore zurücksetzen

Unter bestimmten Umständen möchten Sie den Packetstore möglicherweise zurücksetzen. Wenn Sie beispielsweise versehentlich Pakete mit vertraulichen Daten oder aus dem falschen Datenfeed gesammelt haben, können Sie den Datenspeicher zurücksetzen, sodass die Pakete nicht in Paketabfragen erscheinen.

⚠ **Warnung:** Wenn Sie den Packetstore, können Paketabfragen nicht auf alle vorhandenen Pakete zugreifen.

1. In der Geräte-Einstellungen Abschnitt, klicken **Packetstore zurücksetzen**.
2. Typ `JA` im Bestätigungsfeld und dann auf **Packetstore zurücksetzen**.

Normalerweise dauert es weniger als eine Minute, den Packetstore zurückzusetzen.

# Cluster-Einstellungen verfolgen

Das Cluster-Einstellungen verfolgen Abschnitt umfasst die folgenden Abschnitte:

**Mit Reveal (x) 360 verbinden**

Diese Option wird nur angezeigt, wenn der Packetstore für Reveal (x) 360 lizenziert ist.

**Geschäftsführer**

Aktiviere eine Konsole um Support-Skripte aus der Ferne auszuführen und die Firmware im Packetstore zu aktualisieren.
Sehen Sie sich den Hostnamen des Konsole das so konfiguriert ist, dass es den Packetstore sowie eine Liste aller Sensoren verwaltet und Konsolen mit dem Packetstore verbunden.

**Status der Paketabfrage**

Eine Liste aller Paketabfragen anzeigen, die von einer verbundenen Konsole und angeschlossene Sensoren.

## Geschäftsführer

Das Geschäftsführer Seite enthält die folgenden Informationen und Steuerelemente:

**Geschäftsführer**

Zeigt den Hostnamen des Konsole das für die Verwaltung des Packetstore konfiguriert ist. Um eine zu verbinden Konsole klicken Sie über eine getunnelte Verbindung auf **Mit einer Command Appliance verwalten**. Eine getunnelte Verbindung ist möglicherweise erforderlich, wenn keine direkte Verbindung über die Command-Appliance hergestellt werden kann.

Klicken Sie **Manager entfernen** um das zu entfernen Konsole als der Manager.

**Hinweis:** Der Packetstore kann nur von einem verwaltet werden Konsole.

**Verbundene Geräte**

Zeigt eine Tabelle mit allen Sensoren und Konsolen mit dem Packetstore verbunden. Die Tabelle enthält den Hostnamen, den Produktschlüssel und die IP-Adresse des angeschlossenen ExtraHop-Systems.

## Status der Paketabfrage

Die Status der Paketabfrage Diese Seite bietet eine Sammlung von Metriken über den Packetstore.

Die Metriken auf dieser Seite können Ihnen helfen, Probleme zu beheben und festzustellen, warum der Packetstore nicht wie erwartet funktioniert.

**Status der Paketabfrage**

Zeigt Statistiken über Paketabfragen an, die auf der Seite Pakete ausgeführt werden.

Wenn die Anzahl der gleichzeitigen Paketabfragen den maximal zugewiesenen Systemspeicher überschreitet, können Fehler auftreten und Sie müssen laufende oder abgeschlossene Abfragen löschen, indem Sie auf **entfernen** oder **Alles entfernen** Schaltfläche, bevor Sie neue Abfragen erstellen können. Abfragen werden zwischengespeichert, bis Sie die Seite Pakete verlassen.

**Packetstore-Festplatten**

Zeigt Statistiken über Paketspeicherfestplatten an.

**Speicherung von SSL-Sitzungsschlüsseln**

Zeigt Statistiken über Sitzungsschlüssel an, die im Packetstore gespeichert sind. Hinweise zur Speicherung von Sitzungsschlüsseln finden Sie unter Speichern Sie SSL-Sitzungsschlüssel in verbundenen Paketspeichern.

## Paketabfragen entfernen

Sie können eine oder mehrere Paketabfragen entfernen, um den Abfragespeicher und den Festplattencache zu löschen.

1. In der Cluster-Einstellungen verfolgen Abschnitt, klicken **Status der Paketabfrage**.
2. Führen Sie einen der folgenden Schritte aus:
   - Um eine einzelne Abfrage zu entfernen, klicken Sie auf **entfernen** in der Aktionen Spalte der Abfrage, die Sie entfernen möchten.
   - Um alle aufgelisteten Abfragen zu entfernen, klicken Sie auf **Alles entfernen**.

## Mit einer Konsole verwalten

Verbinde den Packetstore mit einem Konsole um Support-Skripte remote auszuführen und die Firmware im Packetstore von der Konsole.

Der Packetstore verbindet sich mit dem Konsole durch eine Tunnelverbindung. Tunnelverbindungen sind in Netzwerkumgebungen erforderlich, in denen eine direkte Verbindung von Konsole ist aufgrund von Firewalls oder anderen Netzwerkeinschränkungen nicht möglich.

**Bevor Sie beginnen**

**Hinweis:** Mit diesem Verfahren können Sie Verwaltungsfunktionen nur von einer verbundenen Konsole oder von Reveal (x) 360 aus ausführen. Um Pakete aus dem ExtraHop-System zu suchen und herunterzuladen, folgen Sie den Anweisungen unter Sensoren und Konsole mit dem Packetstore verbinden.

1. In der Cluster-Einstellungen verfolgen Abschnitt, klicken **Manager**.
2. klicken **Mit Command Appliance verwalten**.
3. Konfigurieren Sie die folgenden Einstellungen:
   - Hostname der Befehls-Appliance : Geben Sie den Hostnamen oder die IP-Adresse der Konsole ein.
   - Setup-Passwort für Befehlsgerät : Geben Sie den `setup` Benutzerpasswort für die Konsole.
   - Spitzname der Trace-Appliance : Geben Sie einen benutzerfreundlichen Namen für den ExtraHop-Packetstore ein. Wenn kein Spitzname eingegeben wird, wird der Knoten durch den Hostnamen identifiziert.
4. Wählen Sie den Mit der Command-Appliance verwalten Checkbox und dann klicken **Managen**.