# 25.2
# RevealX Enterprise Console Administrationshandbuch

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

Veröffentlicht: 2025-03-28

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

# Inhaltsübersicht


## Einführung in das RevealX Enterprise Console Administrationshandbuch 7
Unterstützte Browser 7

## Status und Diagnose 8
Gesundheit 8
Anzahl und Limit der aktiven Gerät 9
Anzahl der aktiven Gerät überprüfen 10
Audit-Protokoll 10
Audit-Log-Daten an einen Remote-Syslog-Server senden 10
Audit-Log-Ereignisse 12
Ausnahmedateien 17
Unterstützungsskripte 17
Führen Sie das Standard-Support-Skript aus 17
Führen Sie ein benutzerdefiniertes Support-Skript aus 17

## Netzwerk-Einstellungen 18
Stellen Sie eine Verbindung zu ExtraHop Cloud Services her 18
Konfigurieren Sie Ihre Firewallregeln 19
Stellen Sie über einen Proxy eine Verbindung zu ExtraHop Cloud Services her 20
Zertifikatsvalidierung umgehen 21
Trennen Sie die Verbindung zu den ExtraHop Cloud Services 21
Registrierung für ExtraHop Cloud Services verwalten 21
Konnektivität 22
Eine Schnittstelle konfigurieren 22
Stellen Sie eine statische Route ein 23
IPv6 für eine Schnittstelle aktivieren 23
Globaler Proxyserver 24
Einen globalen Proxy konfigurieren 24
ExtraHop Cloud-Proxy 24
Bond-Schnittstellen 24
Erstellen Sie eine Bond-Schnittstelle 25
Ändern Sie die Einstellungen für die Bond-Schnittstelle 25
Zerstöre eine Bond-Schnittstelle 26
Benachrichtigungen 26
E-Mail-Einstellungen für Benachrichtigungen konfigurieren 26
Konfigurieren Sie eine E-Mail-Benachrichtigungsgruppe 28
Konfigurieren Sie die Einstellungen, um Benachrichtigungen an einen SNMP-Manager zu senden 28
Laden Sie die ExtraHop SNMP MIB herunter 29
Extrahieren Sie die ExtraHop-Lieferantenobjekt-OID 29
Systembenachrichtigungen an einen Remote-Syslog-Server senden 30
TLS-Zertifikat 31
Laden Sie ein TLS-Zertifikat hoch 31
Generieren Sie ein selbstsigniertes Zertifikat 32
Erstellen Sie eine Anfrage zur Zertifikatsignierung von Ihrem ExtraHop-System 32
Vertrauenswürdige Zertifikate 33

Fügen Sie Ihrem ExtraHop-System ein vertrauenswürdiges Zertifikat hinzu 33

## Auf Einstellungen zugreifen 35

Globale Richtlinien 35
Passwörter 35
Ändern Sie das Standardkennwort für den Setup-Benutzer 36
Zugang zum Support 36
SSH-Schlüssel generieren 36
Den SSH-Schlüssel neu generieren oder widerrufen 36
Nutzer 37
Benutzer und Benutzergruppen 37
Lokale Benutzer 37
Fernauthentifizierung 37
Entfernte Benutzer 38
Benutzergruppen 38
Benutzerrechte 39
Lokales Benutzerkonto hinzufügen 44
Konto für einen Remote-Benutzer hinzufügen 45
Sessions 45
Fernauthentifizierung 45
Konfigurieren Sie die Fernauthentifizierung über LDAP 46
Benutzerrechte für die Fernauthentifizierung konfigurieren 48
Konfigurieren Sie die Fernauthentifizierung über SAML 50
SAML-Remoteauthentifizierung aktivieren 50
Zuordnung von Benutzerattributen 52
Attributaussagen gruppieren 52
Die nächsten Schritte 52
SAML-Single-Sign-On mit Okta konfigurieren 53
SAML auf dem ExtraHop-System aktivieren 53
SAML-Einstellungen in Okta konfigurieren 53
Weisen Sie das ExtraHop-System Okta-Gruppen zu 56
Fügen Sie Informationen zum Identitätsanbieter im ExtraHop-System hinzu 56
Loggen Sie sich in das ExtraHop-System ein 58
SAML-Single-Sign-On mit Google konfigurieren 58
SAML auf dem ExtraHop-System aktivieren 58
Benutzerdefinierte Benutzerattribute hinzufügen 58
Fügen Sie Identitätsanbieterinformationen von Google zum ExtraHop-System hinzu 59
Fügen Sie Informationen zum ExtraHop-Dienstanbieter zu Google hinzu 61
Benutzerrechte zuweisen 62
Loggen Sie sich in das ExtraHop-System ein 63
Konfigurieren Sie die Fernauthentifizierung über RADIUS 63
Konfigurieren Sie die Fernauthentifizierung über TACACS+ 64
Konfigurieren Sie den TACACS+-Server 65
API-Zugriff 68
API-Schlüsselzugriff verwalten 68
Cross-Origin Resource Sharing (CORS) konfigurieren 68
Generieren Sie einen API-Schlüssel 69
Privilegienstufen 69

## Konfiguration des Systems 73

Vorrang des Gerätenamens 73
Inaktive Quellen konfigurieren 74
Erkennungsverfolgung aktivieren 74

Ticket-Tracking von Drittanbietern für Erkennungen konfigurieren 75
Schreiben Sie einen Auslöser, um Tickets zu Erkennungen in Ihrem Ticketsystem zu erstellen und zu aktualisieren 76
Ticketinformationen über die REST-API an Erkennungen senden 77
Lookup-Links konfigurieren 79
Geomap-Datenquelle 81
Ändern Sie die GeoIP-Datenbank 81
Einen IP-Standort überschreiben 81
Einen Sensor oder eine Konsole sichern und wiederherstellen 82
Inhalt der täglichen Sicherungsdatei 82
Einen Sensor oder eine Konsole sichern 83
Stellen Sie einen Sensor oder eine Konsole aus einem System-Backup wieder her 84
Stellen Sie einen Sensor oder eine Konsole aus einer Sicherungsdatei wieder her 85
Einstellungen auf einen neuen Sensor oder eine neue Konsole übertragen 86
Schließen Sie die Sensoren wieder an die Konsole an 86

**Appliance-Einstellungen 88**

Konfiguration ausführen 88
Speichern Sie die Systemeinstellungen in der laufenden Konfigurationsdatei 88
Bearbeiten Sie die laufende Konfigurationsdatei 89
Laden Sie die aktuelle Konfiguration als Textdatei herunter 89
ICMPv6-Nachrichten vom Typ Destination Unreachable deaktivieren 89
Bestimmte ICMPv6-Echo-Antwortnachrichten deaktivieren 90
Dienstleistungen 90
SNMP-Dienst 91
Konfigurieren Sie den SNMPv1- und SNMPv2-Dienst 91
Konfigurieren Sie den SNMPv3-Dienst 91
Firmware 92
Aktualisieren Sie die Firmware auf Ihrem ExtraHop-System 92
Checkliste vor dem Upgrade 92
Aktualisieren Sie die Firmware auf einer Konsole und einem Sensor 93
Aktualisieren Sie die Firmware auf Recordstores 93
Aktualisieren Sie die Firmware auf Packetstores 94
Rüsten Sie die angeschlossenen Sensoren in RevealX 360 auf 94
Systemzeit 95
Konfigurieren Sie die Systemzeit 96
Herunterfahren oder Neustarten 97
Sensormigration 97
Migrieren Sie einen ExtraHop-Sensor 98
Bereite die Quelle- und Zielsensoren vor 99
Starten Sie die Migration 101
Konfigurieren Sie den Zielsensor 101
Lizenz 102
Registrieren Sie Ihr ExtraHop-System 102
Registrieren Sie das Gerät 102
Problembehandlung bei der Lizenzserverkonnektivität 103
Eine aktualisierte Lizenz anwenden 103
Eine Lizenz aktualisieren 104
Festplatten 104
Ersetzen Sie eine RAID 0-Festplatte 105
Installieren Sie eine neue Paketerfassungsdiskette 106
Spitzname der Konsole 107
Eine Meldung auf dem Anmeldebildschirm konfigurieren 108

## Plattenladen 109
Datensätze von ExtraHop an Google BigQuery senden 109
BigQuery als Recordstore aktivieren 109
Recordstore-Einstellungen übertragen 110
Datensätze von ExtraHop an Splunk senden 111
Splunk als Recordstore aktivieren 111
Recordstore-Einstellungen übertragen 112

## ExtraHop-Sensor-Einstellungen 113
Stellen Sie von einer RevealX Enterprise-Konsole aus eine Verbindung zu einem Sensor her 113
Generieren Sie ein Token auf dem Sensor 113
Verbinden Sie die Konsole und die Sensoren 113
Paketsensoren verwalten 114

## ExtraHop Recordstore-Einstellungen 115
Verbinden Sie den EXA 5200 mit dem ExtraHop-System 115
Trennen Sie den Recordstore 116
Verbinden Sie den EXA 5300 mit dem ExtraHop-System 117
Recordstore-Partitionen 117
Generieren Sie ein Token auf dem EXA 5300 117
Den EXA 5300 an eine Konsole oder einen Sensor anschließen 117
Datensatzaufnahme in einem Recordstore konfigurieren 118
Trennen Sie den Recordstore 118
Plattenläden verwalten 118
Flow-Aufzeichnungen sammeln 119
Status des ExtraHop Recordstore 120

## ExtraHop Packetstore-Einstellungen 121
Einen Packetstore mit RevealX Enterprise verbinden 121
Paketspeicher verwalten 122

## Anlage 124
Allgemeine Akronyme 124
Cisco NetFlow-Geräte konfigurieren 125
Konfigurieren Sie einen Exporter auf dem Cisco Nexus Switch 125
Konfiguration von Cisco Switches über Cisco IOS CLI 126

# Einführung in das RevealX Enterprise Console Administrationshandbuch

Das RevealX Enterprise Console-Administratorhandbuch enthält detaillierte Informationen zu den Verwaltungseinstellungen der RevealX Enterprise-Konsolen. Dieses Handbuch bietet einen Überblick über die globale Navigation und Informationen zu den Steuerelementen, Feldern und Optionen, die in der Admin-Benutzeroberfläche für Konsolen verfügbar sind.

Nachdem Sie Ihre bereitgestellt haben Konsole, siehe Checkliste für Sensor und Konsole nach der Bereitstellung.

Wir schätzen 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

Das Status und Diagnose Der Abschnitt enthält Kennzahlen zum allgemeinen Zustand Ihres ExtraHop-Systems.

## Gesundheit

Das Gesundheit Diese Seite bietet eine Sammlung von Metriken, die Ihnen helfen, den Betrieb Ihres ExtraHop-Systems zu überwachen, und ermöglicht es dem ExtraHop-Support, bei Bedarf Systemfehler zu beheben.

**System**

Meldet die folgenden Informationen zur CPU-Auslastung und zur Festplatte des Systems.

**CPU-Benutzer**

Der Prozentsatz der CPU-Auslastung, der dem ExtraHop-Systembenutzer zugeordnet ist.

**CPU-System**

Der Prozentsatz der CPU-Auslastung im Zusammenhang mit dem ExtraHop-System.

**CPU im Leerlauf**

Der Prozentsatz der CPU-Leerlaufzeit, der dem ExtraHop-System zugeordnet ist.

**CPU-IO**

Der Prozentsatz der CPU-Auslastung, der mit den I/O-Funktionen des ExtraHop-Systems verbunden ist.

**Status des Dienstes**

Meldet den Status der ExtraHop-Systemdienste.

**Exalarme**

Die Zeit, in der der ExtraHop-Systemwarnungsdienst ausgeführt wurde.

**ausdehnen**

Die Zeit, in der der ExtraHop-Systemtrend-Service ausgeführt wurde.

**exconfig**

Die Zeit, in der der ExtraHop-Systemkonfigurationsdienst ausgeführt wurde.

**exportale**

Die Zeit, in der der Webportaldienst des ExtraHop-Systems ausgeführt wurde.

**Exshell**

Die Zeitdauer, in der der ExtraHop-System-Shell-Service ausgeführt wurde.

**Schnittstellen**

Meldet den Status der ExtraHop-Systemschnittstellen.

**RX-Pakete**

Die Anzahl der Pakete, die von der angegebenen Schnittstelle empfangen wurden das ExtraHop-System.

**RX-Fehler**

Die Anzahl der empfangenen Paketfehler auf dem angegebenen Schnittstelle.

**RX Drops**

Die Anzahl der empfangenen Pakete, die durch den angegebenen Wert gelöscht wurden Schnittstelle.

**TX-Pakete**

Die Anzahl der Pakete, die von der angegebenen Schnittstelle übertragen werden auf dem ExtraHop-System.

**TX-Fehler**

Die Anzahl der übertragenen Paketfehler auf dem angegebenen Schnittstelle.

**TX Drops**

Die Anzahl der übertragenen Pakete, die durch den angegebenen Wert gelöscht wurden Schnittstelle.

**RX-Bytes**

Die Anzahl der Byte, die von der angegebenen Schnittstelle auf dem ExtraHop-System.

**TX-Bytes**

Die Anzahl der Byte, die von der angegebenen Schnittstelle übertragen werden das ExtraHop-System.

**Partitionen**

Meldet den Speicher, der Systemkomponenten für das ExtraHop-System zugewiesen wurde.

**Name**

Die Systemkomponenten, die eine Speicherpartition im NVRAM haben.

**Optionen**

Die Lese- und Schreiboptionen für die Systemkomponenten.

**Größe**

Die Partitionsgröße in Gigabyte, die der Systemkomponente zugewiesen ist.

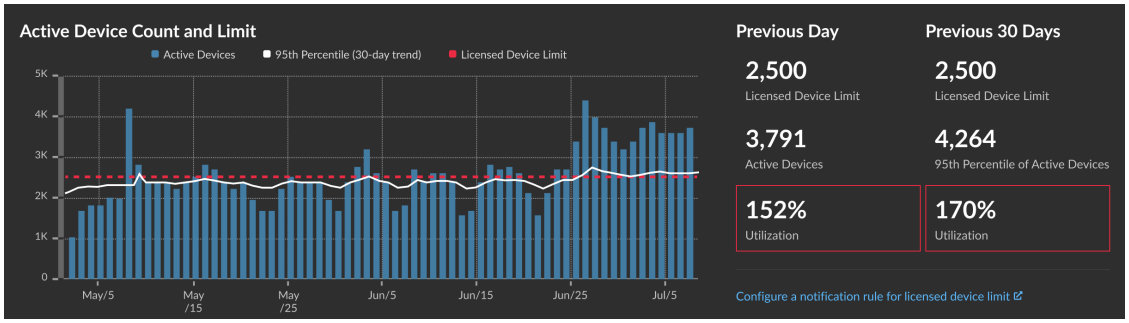
**Auslastung**

Die Menge an Arbeitsspeicher, die derzeit von den Systemkomponenten verbraucht wird, als Menge und als Prozentsatz der gesamten Partition.

## Anzahl und Limit der aktiven Gerät

Anhand des Diagramms Anzahl und Limit der aktiven Gerät können Sie überwachen, ob die Anzahl Ihrer aktiven Geräte das lizenzierte Limit überschritten hat. Beispielsweise sind für ein ExtraHop-System mit einem Frequenzband von 20.000 bis 50.000 Geräten bis zu 50.000 Geräte zulässig.

Klicken Sie **Systemeinstellungen** und klicken Sie dann **Die gesamte Verwaltung**. Aus dem Status und Diagnose Abschnitt, klicken Sie **Anzahl und Limit der aktiven Geräte** um das Diagramm anzusehen.




Das Diagramm „Anzahl und Limit aktiver Geräte“ zeigt die folgenden Metriken an:

- Die gestrichelte rote Linie steht für Limit für lizenzierte Gerät.
- Die durchgezogene schwarze Linie steht für das 95. Perzentil der aktiven Geräte, die in den letzten 30 Tagen täglich beobachtet wurden.
- Die blauen Balken stellen die maximale Anzahl aktiver Geräte dar, die in den letzten 30 Tagen täglich beobachtet wurden.

Auf dieser Seite werden auch die folgenden Metriken angezeigt:

- Das lizenzierte Gerätelimit für den Vortag und die letzten 30 Tage.
- Die Anzahl der am Vortag beobachteten aktiven Geräte.
- Das 95. Perzentil der in den letzten 30 Tagen beobachteten aktiven Geräte.
- Der Nutzungsprozentsatz des lizenzierten Gerätelimits für den Vortag und die letzten 30 Tage. Die Nutzung ist die Anzahl der aktiven Gerät geteilt durch das lizenzierte Limit.

Sie können eine Systembenachrichtigungsregel erstellen, die Sie warnt, wenn die Auslastung einen bestimmten Prozentsatz oder 100 % Ihres lizenzierten Gerätelimits überschreitet. Die prozentualen Grenzwerte können bei der Erstellung einer Regel angepasst werden. Wenn Sie feststellen, dass Sie sich ständig dem lizenzierten Limit nähern oder es überschreiten, empfehlen wir Ihnen, mit Ihrem Vertriebsteam zusammenzuarbeiten, um in den nächsten verfügbaren Kapazitätsbereich zu wechseln.

### Anzahl der aktiven Gerät überprüfen

Sie können das Diagramm „Anzahl aktiver Gerät und Limit“ anzeigen, um zu überwachen, ob die Anzahl Ihrer aktiven Geräte das lizenzierte Limit überschritten hat.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Aus dem Status und Diagnose Abschnitt, klicken **Anzahl und Limit der aktiven Geräte** um das Diagramm anzusehen.

## 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.

### Audit-Log-Daten an einen Remote-Syslog-Server senden

Das Audit-Log sammelt Daten über den Betrieb des ExtraHop-Systems, aufgeschlüsselt nach Komponenten. Das auf dem System gespeicherte Protokoll hat eine Kapazität von 10.000 Einträgen, und Einträge, die älter als 90 Tage sind, werden automatisch entfernt. Sie können diese Einträge in den Verwaltungseinstellungen einsehen oder die Audit-Log-Ereignisse zur Langzeitspeicherung, Überwachung und erweiterten Analyse an einen Syslog-Server senden. Alle protokollierten Ereignisse sind in der folgenden Tabelle aufgeführt.

Die folgenden Schritte zeigen Ihnen, wie Sie das ExtraHop-System so konfigurieren, dass Audit-Log-Daten an einen Remote-Syslog-Server gesendet werden.

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 Sie **Audit-Protokoll**.
3. Klicken Sie **Syslog-Einstellungen konfigurieren**.
4. In der Reiseziel Feld, geben Sie die IP-Adresse des Remote-Syslog-Servers ein.
5. Aus dem **Protokoll** Wählen Sie im Drop-down-Menü eine der folgenden Optionen aus:

   - **TCP**
   - **TLS**
   - **UDP**

   Diese Option gibt das Protokoll an, über das die Informationen an Ihren Remote-Syslog-Server gesendet werden.

**Hinweis:** Wenn Sie TLS auswählen, muss das ExtraHop-System die Syslog-Serveridentität überprüfen, indem es das TLS-Zertifikat des Server validiert. Du kannst konfigurieren Sie das ExtraHop-System so, dass es der Zertifizierungsstelle (CA) vertraut, die das Zertifikat des Syslog-Servers signiert hat in den Administrationseinstellungen.

6. In der Hafen In diesem Feld geben Sie die Portnummer für Ihren Remote-Syslog-Server ein.

   Der Standardwert ist 514.

7. Klicken Sie **Einstellungen testen** um zu überprüfen, ob Ihre Syslog-Einstellungen korrekt sind.

   Wenn die Einstellungen korrekt sind, sollte in der Syslog-Datei auf dem Syslog-Server ein Eintrag ähnlich dem folgenden angezeigt werden:

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```

8. Klicken Sie **Speichern**.
9. Optional: Ändern Sie das Format der Syslog-Meldungen:

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

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

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

      ```
      "auditlog_rsyslog": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "rfc_compliant_format": "rfc5424"
      }
      ```

   e) Klicken Sie **Aktualisieren**.
   f) Klicken Sie **Erledigt**.

10. 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 Konfiguration ändern.

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

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

       ```
       "auditlog_rsyslog": {
           "syslog_destination": "192.168.0.0",
           "syslog_ipproto": "udp",
           "syslog_port": 514,
           "syslog_use_localtime": true
       }
       ```

    e) Klicken Sie **Aktualisieren**.
    f) Klicken Sie **Erledigt**.

**Nächste Schritte**

Nachdem Sie bestätigt haben, dass Ihre neuen Einstellungen wie erwartet funktionieren, behalten Sie Ihre Konfigurationsänderungen bei, indem Sie die laufende Konfigurationsdatei speichern.

**Audit-Log-Ereignisse**
Die folgenden Ereignisse auf einem ExtraHop-System generieren einen Eintrag im Audit-Log.

| Kategorie | Ereignis |
|---|---|
| Abmachungen | • Eine EULA- oder POC-Vereinbarung wird vereinbart |
| API | • Ein API-Schlüssel wird erstellt<br>• Ein API-Schlüssel wird gelöscht<br>• Ein Benutzer wird erstellt.<br>• Ein Benutzer wird geändert. |
| Sensormigration | • Eine Sensormigration wird gestartet<br>• Eine Sensormigration war erfolgreich<br>• Eine Sensormigration ist fehlgeschlagen |
| Browsersitzungen | • Eine bestimmte Browsersitzung wird gelöscht<br>• Alle Browsersitzungen werden gelöscht |
| Cloud-Dienste | • Das System stellt eine Verbindung zu Cloud-Diensten her<br>• Das System trennt sich von den Cloud-Diensten<br>• Status eines angeschlossenen Sensor wird abgerufen |
| Konsole | • Ein Sensor wird mit einer Konsole verbunden<br>• Ein Sensor wird von einer Konsole getrennt<br>• Ein ExtraHop-Recordstore oder Packetstore stellt eine getunnelte Verbindung zu einer Konsole her<br>• Die Konsoleninformationen sind festgelegt<br>• Ein Konsolen-Spitzname ist festgelegt<br>• Einen Sensor aktivieren oder deaktivieren<br>• Der Sensor wird aus der Ferne betrachtet<br>• Eine Lizenz für einen Sensor wird von einer Konsole überprüft<br>• Eine Lizenz für einen Sensor wird von einer Konsole festgelegt |
| Armaturenbretter | • Ein Dashboard wird erstellt<br>• Ein Dashboard wird umbenannt<br>• Ein Dashboard wird gelöscht<br>• Ein Dashboard-Permalink, auch Kurzcode genannt, wird geändert<br>• Die Optionen zum Teilen von Dashboards wurden geändert |

| Kategorie | Ereignis |
| --- | --- |
| Datenspeicher | • Die erweiterte Datenspeicherkonfiguration wurde geändert<br>• Der Datenspeicher ist zurückgesetzt<br>• Ein Datenspeicher-Reset wurde abgeschlossen<br>• Anpassungen werden gespeichert<br>• Anpassungen werden wiederhergestellt<br>• Anpassungen werden gelöscht |
| Erkennungen | • Ein Erkennungsstatus wird aktualisiert<br>• Ein für die Erkennung beauftragter Empfänger wird aktualisiert<br>• Erkennungshinweise werden aktualisiert<br>• Ein externes Ticket wird aktualisiert<br>• Eine Tuning-Regel wird erstellt<br>• Eine Tuning-Regel wird gelöscht<br>• Eine Tuning-Regel wird geändert<br>• Eine Beschreibung der Tuning-Regel wird aktualisiert<br>• Eine Tuning-Regel ist aktiviert<br>• Eine Tuning-Regel ist deaktiviert<br>• Eine Tuning-Regel wird erweitert |
| Ausnahmedateien | • Eine Ausnahmedatei wird gelöscht |
| ExtraHop Recordstore Records | • Alle ExtraHop Recordstore-Datensätze werden gelöscht<br>• Ein Datensatztyp ist aktiviert<br>• Ein Datensatztyp ist deaktiviert |
| ExtraHop-Recordstore-Cluster | • Ein neuer ExtraHop-Recordstore-Knoten wird initialisiert<br>• Ein Knoten wird zu einem ExtraHop-Recordstore-Cluster hinzugefügt<br>• Ein Knoten wird aus einem ExtraHop-Recordstore-Cluster entfernt<br>• Ein Knoten tritt einem ExtraHop-Recordstore-Cluster bei<br>• Ein Knoten verlässt einen ExtraHop-Recordstore-Cluster<br>• Ein Sensor oder eine Konsole ist mit einem ExtraHop-Recordstore verbunden<br>• Ein Sensor oder eine Konsole ist von einem ExtraHop-Recordstore getrennt<br>• Ein ExtraHop-Recordstore-Knoten wurde entfernt oder fehlt, aber nicht über eine unterstützte Schnittstelle |
| ExtraHop Aktualisierungsservice | • Eine Entdeckungskategorie wird aktualisiert<br>• Eine Erkennungsdefinition wird aktualisiert<br>• Ein Erkennungsauslöser wird aktualisiert |

| Kategorie | Ereignis |
| --- | --- |
| | • Eine Ransomware-Definition wird aktualisiert<br>• Erkennungsmetadaten werden aktualisiert<br>• Erweiterter Erkennungsinhalt wird aktualisiert |
| Firmware | • Die Firmware wurde aktualisiert |
| Globale Richtlinien | • Die globale Richtlinie für die Bearbeitungssteuerung von Gerätegruppe wurde aktualisiert |
| Integrationen | • Eine Integration wird aktualisiert |
| Lizenz | • Eine neue statische Lizenz wird angewendet<br>• Die Lizenzserverkonnektivität wird getestet<br>• Ein Produktschlüssel ist auf dem Lizenzserver registriert<br>• Eine neue Lizenz wird beantragt |
| Loggen Sie sich in das ExtraHop-System ein | • Eine Anmeldung ist erfolgreich<br>• Eine Anmeldung schlägt fehl<br>• Ein Konto wird nach zu vielen fehlgeschlagenen Anmeldeversuchen gesperrt<br>• Ein Administrator entsperrt ein Konto |
| Loggen Sie sich über SSH oder REST API ein | • Eine Anmeldung ist erfolgreich<br>• Eine Anmeldung schlägt fehl<br>• Ein Konto wird nach zu vielen fehlgeschlagenen Anmeldeversuchen gesperrt<br>• Ein Administrator entsperrt ein Konto |
| Module | • Die Zugriffskontrolle für das NDR-Modul ist aktiviert<br>• Die Zugriffskontrolle für das NPM-Modul ist aktiviert |
| Netzwerk | • Eine Netzwerkschnittstellenkonfiguration wird bearbeitet<br>• Der Hostname oder DNS Einstellung wurde geändert<br>• Eine Netzwerkschnittstellenroute wird geändert |
| Regeln für Benachrichtigungen | • Eine Benachrichtigungsregel wird erstellt<br>• Eine Benachrichtigungsregel wird gelöscht<br>• Eine Benachrichtigungsregel wird geändert |
| Offline-Erfassung | • Eine Offline-Capture-Datei wird geladen |
| PCAP | • Eine Paketerfassungsdatei (PCAP) wird heruntergeladen |

| Kategorie | Ereignis |
|---|---|
| Fernzugriff | • Der Fernzugriff für das ExtraHop Support Team ist aktiviert<br>• Der Fernzugriff für das ExtraHop Support Team ist deaktiviert<br>• Fernzugriff für ExtraHop Support ist aktiviert<br>• Der Fernzugriff für ExtraHop Support ist deaktiviert |
| RPCAP | • Eine RPCAP-Konfiguration wird hinzugefügt<br>• Eine RPCAP-Konfiguration wird gelöscht |
| Konfiguration ausführen | • Die laufende Konfigurationsdatei ändert sich |
| SAML-Identitätsanbieter | • Ein Identitätsanbieter wird hinzugefügt<br>• Ein Identitätsanbieter wird geändert<br>• Ein Identitätsanbieter wird gelöscht |
| SAML-Anmeldung | • Eine Anmeldung ist erfolgreich<br>• Eine Anmeldung schlägt fehl |
| SAML-Privilegien | • Eine Privilegienstufe wird gewährt<br>• Eine Privilegienstufe wurde verweigert |
| Sensor-Tags | • Ein Sensor-Tag wird erstellt<br>• Ein Sensor-Tag wurde geändert<br>• Ein Sensor-Tag wird gelöscht<br>• Tags auf einem Sensor werden geändert |
| SSL-Entschlüsselung | • Ein TLS-Entschlüsselungsschlüssel wird gespeichert |
| SSL-Sitzungsschlüssel | • Ein PCAP-Sitzungsschlüssel wird heruntergeladen |
| Kundendienst-Konto | • Das Support-Konto ist deaktiviert<br>• Das Support-Konto ist aktiviert<br>• Der Support-SSH-Schlüssel wird neu generiert |
| Unterstützungsskript | • Ein Standard-Support-Skript wird ausgeführt<br>• Ein früheres Unterstützungsskript-Ergebnis wird gelöscht<br>• Ein Support-Skript wird hochgeladen |
| Syslog | • Remote-Syslog-Einstellungen werden aktualisiert |
| System- und Servicestatus | • Das System wird gestartet<br>• Das System wird heruntergefahren<br>• Das System wird neu gestartet<br>• Der Bridge-, Capture- oder Portal-Prozess wird neu gestartet |

| Kategorie | Ereignis |
| --- | --- |
| | • Ein Systemdienst ist aktiviert (z. B. SNMP, Webshell, Management, SSH)<br>• Ein Systemdienst ist deaktiviert (z. B. SNMP, Webshell, /management, SSH) |
| Systemzeit | • Die Systemzeit ist eingestellt<br>• Die Systemzeit wurde geändert<br>• Die Systemzeit ist rückwärts eingestellt<br>• NTP-Server sind eingerichtet<br>• Die Zeitzone ist eingestellt<br>• Eine manuelle NTP-Synchronisierung wird angefordert |
| Systembenutzer | • Ein Benutzer wird hinzugefügt<br>• Benutzermetadaten werden bearbeitet<br>• Ein Benutzer wird gelöscht<br>• Ein Benutzerkennwort ist gesetzt<br>• Ein anderer Benutzer als der `setup` Benutzer versucht, das Passwort eines anderen Benutzers zu ändern<br>• Ein Benutzerkennwort wird aktualisiert |
| TAXII-Feeds | • Ein TAXII-Feed wird hinzugefügt<br>• Ein TAXII-Feed wird geändert<br>• Ein TAXII-Feed wird gelöscht |
| Informationsgespräche über Bedrohungen | • Ein Bedrohungsübersicht wird archiviert<br>• Eine Bedrohungsübersicht wird wiederhergestellt |
| ExtraHop Packetstore | • Ein neuer ExtraHop-Paketstore wird initialisiert<br>• Ein Sensor oder eine Konsole ist mit einem ExtraHop-Packetstore verbunden<br>• Ein Sensor oder eine Konsole ist von einem ExtraHop-Packetstore getrennt<br>• Ein ExtraHop-Paketstore wird zurückgesetzt<br>• Eine Packetstore-Festplatte ist verschlüsselt<br>• Eine Packetstore-Festplatte ist entschlüsselt |
| Tendenzen | • Ein Trend wird zurückgesetzt |
| Trigger | • Ein Auslöser wird hinzugefügt<br>• Ein Auslöser wird bearbeitet<br>• Ein Auslöser wird gelöscht |
| Benutzergruppen | • Eine lokale Benutzergruppe wird erstellt<br>• Eine lokale Benutzergruppe wird gelöscht<br>• Eine lokale Benutzergruppe ist aktiviert<br>• Eine lokale Benutzergruppe ist deaktiviert |

## 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.

## 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-Support-Skript sammelt Informationen über den Zustand 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. In der Status und Diagnose Abschnitt, klicken **Unterstützungsskripte**.
3. klicken **Standard-Support-Skript ausführen**.
4. klicken **Lauf**.
   Wenn das Skript abgeschlossen ist, Ergebnisse des Support-Skripts Seite wird angezeigt.
5. Klicken Sie auf den Namen des Diagnose-Support-Pakets, das Sie herunterladen möchten.

   Die Datei wird am Standardspeicherort für Downloads auf Ihrem Computer gespeichert.

   Senden Sie diese Datei, normalerweise mit dem Namen `diag-results-complete.expk`, an den ExtraHop Support.

   Das `.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.

# Netzwerk-Einstellungen

Die Netzwerk-Einstellungen Dieser Abschnitt enthält Konfigurationseinstellungen für Ihr ExtraHop-System. Mit diesen Einstellungen können Sie einen Hostnamen festlegen, Benachrichtigungen konfigurieren und Verbindungen zu Ihrem System verwalten.

## 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.

Ihre Systemlizenz bestimmt, welche Dienste für Ihre ExtraHop-Konsole oder Ihren ExtraHop-Sensor verfügbar sind. Eine einzelne Lizenz kann jeweils nur auf eine einzelne Appliance oder virtuelle Maschine (VM) angewendet werden. Wenn Sie eine Lizenz von einer Appliance oder VM auf eine andere übertragen möchten, können Sie Systemregistrierung verwalten von der ExtraHop Cloud Services-Seite.

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**

- RevealX 360-Systeme werden automatisch mit 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. In der Netzwerkeinstellungen Abschnitt, klicken **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: In der Service für maschinelles Lernen Abschnitt, wählen Sie 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 Firewallregeln

Wenn Ihr ExtraHop-System in einer Umgebung mit einer Firewall bereitgestellt wird, müssen Sie den Zugriff auf ExtraHop Cloud Services öffnen und gRPC und HTTP/2 aktivieren. Stellen Sie sicher, dass der HTTP/2-Verkehr nicht von Zwischengeräten auf HTTP/1.1 herabgestuft wird. Für RevealX 360-Systeme, die verbunden sind mit Sensoren, müssen Sie auch den Zugriff auf den Cloud-basierten Recordstore öffnen, der in RevealX Standard Investigation enthalten ist.

#### Offener Zugang zu Cloud-Diensten

Für den Zugriff auf ExtraHop Cloud Services ist Ihr Sensoren muss in der Lage sein, DNS-Abfragen für*.extrahop.com aufzulösen und Zugriff auf TCP 443 (HTTPS) von einer der folgenden IP-Adressen aus haben, die Ihrer Sensor Lizenz. Wir empfehlen, den Zugriff auf beide IP-Adressen zu öffnen, um Betriebsunterbrechungen zu vermeiden.

| Region | IP-Adressen |
|---|---|
| Nord-, Mittel- und Südamerika (AMER) | 35,161,154,247<br>54,191,189,22 |
| Asien, Pazifik (APAC) | 54,66,242,25<br>13,239,224,80 |
| Europa, Naher Osten, Afrika (EMEA) | 52,59,110,168<br>18,198,13,99 |
| Bundesstaat der Vereinigten Staaten (US-FED) | 3,135,6,11<br>3,139,1111,240 |

#### Offener Zugang zu RevealX 360 Premium Investigation

Für den Zugriff auf RevealX 360 Premium Investigation ist Ihr Sensoren muss die folgenden Anforderungen erfüllen:

- Auf den Sensoren muss die ExtraHop-Firmware-Version 9.9 oder höher ausgeführt werden.
- Sensoren müssen in der Lage sein, über ausgehendes TCP 443 (HTTPS) auf bestimmte vollqualifizierte Domainnamen zuzugreifen.

- In den Vereinigten Staaten befindliche Sensoren müssen auf diese Domainnamen zugreifen können:
  - `eh.oem-2-1.logscale.us-2.crowdstrike.com`
  - `eh.oem-2-2.logscale.us-2.crowdstrike.com`
- Sensoren, die sich in der Europäischen Union befinden, müssen auf diesen Domänenname zugreifen können:
  - `eh.oem-2-3.logscale.eu-1.crowdstrike.com`

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

**Offener Zugang zu RevealX 360 Standard Investigation**

Für den Zugriff auf RevealX 360 Standard Investigation ist Ihr Sensoren muss in der Lage sein, auf ausgehendes TCP 443 (HTTPS) auf diese vollständig qualifizierten 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 können 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. Das ExtraHop-System kommuniziert auch mit dem ExtraHop-Lizenzserver über die Proxyverbindung.

**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. Wir empfehlen, eine Sicherheitsausnahme zu erstellen und die MITM-Inspektion für diesen Verkehr zu deaktivieren.

> **Wichtig:** Wenn Sie MITM auf Ihrem Proxy nicht deaktivieren können, müssen Sie die Zertifikatsvalidierung in der Konfigurationsdatei des ExtraHop-Systems deaktivieren. 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 Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. Klicken Sie **ExtraHop Cloud Proxy aktivieren**.
4. In der Hostname Feld, geben Sie den Hostnamen für Ihren Proxyserver ein, z. B. `Proxyhost`.
5. In der Hafen Feld, geben Sie den Port für Ihren Proxyserver ein, z. B. `8080`.
6. Optional: Falls erforderlich, in der Nutzername und Passwort Felder, geben Sie einen Benutzernamen und ein Passwort für Ihren Proxyserver ein.
7. Klicken Sie **Speichern**.

## Zertifikatsvalidierung umgehen

Einige Umgebungen sind so konfiguriert, dass verschlüsselter Datenverkehr das Netzwerk nicht verlassen kann, ohne von einem Drittanbietergerät überprüft zu werden. Dieses Gerät kann als TLS-Endpunkt fungieren, der den Datenverkehr entschlüsselt und erneut verschlüsselt, bevor die Pakete an ExtraHop Cloud Services gesendet werden.

Wenn ein System 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 Sicherheit der ExtraHop-Systemauthentifizierung und -verschlüsselung stellt sicher, dass die Kommunikation zwischen Systemen und ExtraHop Cloud-Diensten nicht abgefangen werden kann.

**Hinweis:** Für das folgende Verfahren müssen Sie mit der Änderung der laufenden ExtraHop-Konfigurationsdatei vertraut sein.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken Sie **Konfiguration ausführen**.
3. Klicken Sie **Konfiguration bearbeiten**.
4. Fügen Sie am Ende der laufenden Konfigurationsdatei die folgende Zeile hinzu:

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

5. Klicken Sie **Aktualisieren**.
6. Klicken Sie **Änderungen anzeigen und speichern**.
7. Überprüfe die Änderungen.
8. Klicken Sie **Speichern**.
9. Klicken Sie **Erledigt**.

## Trennen Sie die Verbindung zu den ExtraHop Cloud Services

Sie können ein ExtraHop-System von den ExtraHop Cloud Services trennen.

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 **ExtraHop Cloud-Dienste**.
3. In der Verbindung zu Cloud-Diensten Abschnitt, klicken Sie **Trennen**.

## Registrierung für ExtraHop Cloud Services verwalten

**Bevor Sie beginnen**
Ihre Systemlizenz bestimmt, welche Dienste für Ihre ExtraHop-Konsole oder Ihren ExtraHop-Sensor verfügbar sind. Eine einzelne Lizenz kann jeweils nur auf eine einzelne Appliance oder virtuelle Maschine (VM) angewendet werden. Wenn Sie eine Lizenz von einer Appliance oder VM auf eine andere übertragen möchten, können Sie die Systemregistrierung auf der Seite ExtraHop Cloud Services verwalten.
Durch die Aufhebung der Registrierung eines Systems werden alle Daten und historischen Analysen für den Machine Learning Service aus dem System gelöscht und sind nicht mehr verfügbar.

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 **ExtraHop Cloud-Dienste**.
3. In der Verbindung zu Cloud-Diensten Abschnitt, klicken **Abmelden**.

# Konnektivität

Das Konnektivität Die Seite 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 **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-Konsole oder anderen Geräten außerhalb des lokalen Netzwerk 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 mit dem EFC 1290v
- Paketweiterleitung mit RPCAP

**Einstellungen für die Paketaufnahme**

- Konfigurieren Sie die Quelle der von diesem Sensor aufgenommenen Pakete. Sie können den Sensor so einrichten, dass er Pakete aus einem direkten Feed oder Pakete, die von einem Drittanbieter weitergeleitet wurden, aufnimmt.

## Eine Schnittstelle konfigurieren

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 **Konnektivität**.
3. In der Schnittstellen Abschnitt, klicken Sie auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
4. Auf dem Netzwerkeinstellungen für die Schnittstelle *<interface number>* Seite, von der **Schnittstellen-Modus** Wählen Sie im Drop-down-Menü eine der folgenden Optionen aus:

   **Deaktiviert**

   Die Schnittstelle ist deaktiviert.

   **Verwaltung**

   Verwaltet die Konsole.
5. Konfigurieren Sie DCHP.

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.

6. Optional: Aktiviere IPv6.

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

### Stellen Sie eine statische Route ein

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

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 **Konnektivität**.
3. In der Schnittstellen Abschnitt, klicken Sie auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
4. Auf dem Netzwerkeinstellungen für die Schnittstelle *<interface number>* Seite, stellen Sie sicher, dass die **IPv4-Adresse** und **Netzmaske** Die Felder sind vollständig und gespeichert und klicken Sie auf **Routen bearbeiten**.
5. In der Route hinzufügen Abschnitt, geben Sie einen Netzwerkadressbereich in CIDR-Notation in das **Netzwerk** Feld und IPv4-Adresse im **Über IP** Feld und dann klicken **Hinzufügen**.
6. Wiederholen Sie den vorherigen Schritt für jede Route, die Sie hinzufügen möchten.
7. Klicken Sie **Speichern**.

### IPv6 für eine Schnittstelle aktivieren

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 **Konnektivität**.
3. In der Schnittstellen Abschnitt, klicken Sie auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
4. Auf dem Netzwerkeinstellungen für die Schnittstelle *<interface number>* Seite, auswählen **IPv6 aktivieren**.
   IPv6-Konfigurationsoptionen werden unten angezeigt **IPv6 aktivieren**.
5. 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 durch die automatische Konfiguration zustandsloser Adressen automatisch zuzuweisen, verwenden Sie das **Automatische Konfiguration zustandsloser Adressen** Wählen Sie im Dropdownmenü eine der folgenden Optionen aus:

     **MAC-Adresse verwenden**

     Konfiguriert die Appliance so, dass IPv6-Adressen automatisch auf der Grundlage der MAC-Adresse der Appliance zugewiesen werden.

     **Verwenden Sie eine stabile private Adresse**

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

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

6. Damit die Appliance Informationen zum rekursiven DNS-Server (RDNSS) und zur DNS-Suchliste (DNSSL) gemäß den Router-Ankündigungen konfigurieren kann, wählen Sie **RDNSS/DNSSL**.
7. Klicken Sie **Speichern**.

## Globaler Proxyserver

Wenn Ihre Netzwerktopologie einen Proxyserver erfordert, damit Ihr ExtraHop-System entweder mit einer Konsole oder mit anderen Geräten außerhalb des lokalen Netzwerk kommunizieren kann, 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. Stellen Sie sicher, dass der HTTP/2-Verkehr nicht von Zwischengeräten auf HTTP/1.1 herabgestuft wird.

**Einen globalen Proxy konfigurieren**

**Wichtig:** Sie können nur einen globalen Proxyserver pro ExtraHop-System konfigurieren.

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 **Konnektivität**.
3. In der Proxy-Einstellungen Abschnitt, klicken Sie **Globalen Proxy aktivieren**.
4. In der Hostname Feld, geben Sie den Hostnamen oder die IP-Adresse für Ihren globalen Proxyserver ein
5. In der Hafen In diesem Feld geben Sie die Portnummer für Ihren Proxyserver ein.
6. In der Nutzername Geben Sie in dieses Feld den Namen eines Benutzers ein, der privilegierten Zugriff auf Ihren globalen Proxyserver hat.
7. In der Passwort Feld, geben Sie das Passwort für den oben angegebenen Benutzer ein.

## 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 Schnittstellenelement und bis zu der Anzahl von Elementen erstellen, die für das Bonding verfügbar sind.

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 **Konnektivität**.
3. In der Einstellungen für die Bond-Schnittstelle Abschnitt, klicken Sie **Bond-Schnittstelle erstellen**.
4. Markieren 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.
5. Aus dem **Einstellungen übernehmen von** Wählen Sie im Dropdownmenü die Schnittstelle aus, die die Einstellungen enthält, die Sie auf die Bond-Schnittstelle anwenden möchten.

   Die Einstellungen für alle nicht ausgewählten Schnittstellen gehen verloren.
6. Für **Art der Anleihe**, wählen Sie eine der folgenden Optionen:
   - **Statisch**, wodurch eine statische Bindung entsteht.
   - **802.3ad (LACP)**, das durch IEEE 802.3ad Link Aggregation (LACP) eine dynamische Verbindung herstellt.
7. Aus dem **Hash-Richtlinie** Wählen Sie im Dropdownmenü eine der folgenden Optionen aus:
   - **Schicht 3+4** Richtlinie, die die Verteilung des Datenverkehrs auf die Schnittstellen gleichmäßiger verteilt. Diese Richtlinie entspricht jedoch nicht vollständig den 802.3ad-Standards.
   - **Ebene 2+3** Richtlinie, die den Datenverkehr weniger gleichmäßig verteilt und den 802.3ad-Standards entspricht.
8. Klicken Sie **Erstellen**.

Aktualisieren Sie die Seite, um die anzuzeigen Bond-Schnittstellen Abschnitt. Jedes Mitglied der Bond-Schnittstelle, dessen Einstellungen nicht in der ausgewählt wurden **Einstellungen übernehmen von** Dropdownmenüs werden angezeigt als **Deaktiviert ( Bond-Mitglied)** in der Schnittstellen Abschnitt.

**Ändern Sie die Einstellungen für die Bond-Schnittstelle**
Nachdem eine Bond-Schnittstelle erstellt wurde, können Sie die meisten Einstellungen so ändern, als ob die Bond-Schnittstelle eine einzelne Schnittstelle wäre.

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 **Konnektivität**.
3. In der Bond-Schnittstellen Abschnitt, klicken Sie auf die Bond-Schnittstelle, die Sie ändern möchten.
4. Auf dem Netzwerkeinstellungen für Bond Interface <*Schnittstellennummer*> Seite, 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 Bindung oder eine dynamische Bindung über IEEE 802.3ad Link Aggregation (LACP) erstellt werden soll.
- **Schnittstellen-Modus :** Die Art der Anleihemitgliedschaft. Eine Bond-Schnittstelle kann **Verwaltung** oder **Management+RPCAP/ERSPAN-Ziel** nur.
- **DHCPv4 aktivieren :** Wenn DHCP aktiviert ist, wird automatisch eine IP-Adresse für das Bond-Interface abgerufen.
- **Hash-Richtlinie:** Geben Sie die Hash-Richtlinie an. Das **Schicht 3+4** Die Richtlinie gleicht die Verteilung des Datenverkehrs auf die Schnittstellen gleichmäßiger aus, entspricht jedoch nicht vollständig den 802.3ad-Standards. Das **Ebene 2+3** Die Richtlinie verteilt den Verkehr 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.

5. Klicken Sie **Speichern**.

**Zerstöre eine Bond-Schnittstelle**

Wenn eine Bond-Schnittstelle zerstört wird, kehren die einzelnen Schnittstellenelemente 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 Mitgliedsoberfläche ausgewählt wird, um die Einstellungen beizubehalten, gehen die Einstellungen verloren und alle Mitgliedsoberflächen werden deaktiviert.

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 **Konnektivität**.
3. In der Abschnitt „Bond-Interfaces“, klicken Sie auf das rote **X** neben der Schnittstelle, die Sie zerstören möchten.
4. Auf dem Zerstöre die Bond-Schnittstelle < *Schnittstellennummer*> Wählen Sie auf dieser Seite die Mitgliedsoberfläche aus, auf die Sie die Einstellungen für die Bond-Schnittstelle verschieben möchten.

   Nur die Mitglieds-Schnittstelle, die ausgewählt wurde, um die Bond-Schnittstelleneinstellungen beizubehalten, bleibt aktiv, und alle anderen Mitglieds-Schnittstellen sind deaktiviert.
5. Klicken Sie **Zerstören**.

## Benachrichtigungen

Das ExtraHop-System kann Benachrichtigungen über konfigurierte Warnmeldungen per E-Mail, SNMP-Traps und Syslog-Exporten an Remoteserver 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, Benachrichtigungen über den Systemstatus 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 Sie **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 ist der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse eines Postausgangsservers, 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 Feld, geben Sie die Portnummer für die SMTP-Kommunikation ein.

   Port 25 ist der Standardwert für SMTP, und Port 465 ist der Standardwert für TLS-verschlüsseltes SMTP.
6. Aus dem Verschlüsselung Wählen Sie im Dropdownmenü eine der folgenden Verschlüsselungsmethoden aus:

   **Keine**

   Die SMTP-Kommunikation ist nicht verschlüsselt.

   **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 in dem vom SMTP-Server vorgelegten Zertifikat angegebene Hostname 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 ExtraHop-Konsole oder RevealX 360 aus gesendet werden.
10. Wählen Sie die **SMTP-Authentifizierung aktivieren** Ankreuzfeld.
11. In der Nutzername und Passwort Felder, geben Sie die Anmeldeinformationen für das SMTP-Server-Setup ein.
12. Optional: Klicken Sie **Einstellungen testen**, geben Sie Ihre E-Mail-Adresse ein (maximal 50 Zeichen), und klicken Sie dann auf **Senden**.

    Sie sollten eine E-Mail-Nachricht mit dem Betreff erhalten `ExtraHop Test Email`.
13. Klicken Sie **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 laufende Konfigurationsdatei speichern.

## Konfigurieren Sie eine E-Mail-Benachrichtigungsgruppe

Fügen Sie einer Gruppe eine Liste mit E-Mail-Adressen hinzu und wählen Sie dann die Gruppe aus, wenn Sie die E-Mail-Einstellungen so konfigurieren, dass Systemintegritätsbenachrichtigungen, eine Alarm oder ein geplanter Bericht gesendet werden. Sie können zwar einzelne E-Mail-Adressen angeben, E-Mail-Gruppen sind jedoch eine effektive Methode, um Ihre Empfängerliste zu verwalten.

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 **Benachrichtigungen**.
3. klicken **E-Mail-Benachrichtigungsgruppen**.
4. klicken **Gruppe hinzufügen**.
5. In der Informationen zur Gruppe Abschnitt, konfigurieren Sie die folgenden Informationen:

   • **Name:** Geben Sie einen Namen für die E-Mail-Gruppe ein.

   • **Benachrichtigungen zum Systemstatus:** Wählen Sie dieses Kontrollkästchen, wenn die E-Mail-Gruppe Systemwarnungen erhalten soll, die unter folgenden Bedingungen generiert werden:

   - Ein virtuelles Laufwerk befindet sich in einem heruntergekommenen Zustand.
   - Eine physische Festplatte befindet sich in einem heruntergefahrenen Zustand oder weist eine steigende Fehleranzahl auf.
   - Eine erforderliche Festplattenpartition für Firmware-, Datenspeicher- oder Paketerfassungsdaten fehlt.
   - Ein Gerät konnte sich nicht wieder mit ExtraHop Cloud Services verbinden.
   - Eine Lizenz ist abgelaufen oder läuft bald ab.
   - Ein Backup für Anpassungen und Ressourcen ist fehlgeschlagen.
6. In der E-Mail-Adressen Textfeld, geben Sie die Empfänger-E-Mail-Adressen ein, die die an diese Gruppe gesendeten E-Mails erhalten sollen. E-Mail-Adressen können eine pro Zeile eingegeben oder durch ein Komma, Semikolon oder Leerzeichen getrennt werden. E-Mail-Adressen werden nur überprüft für [*Name*] @ [*firma*] . [*Domäne*] Formatüberprüfung. Dieses Textfeld muss mindestens eine E-Mail-Adresse enthalten, damit die Gruppe gültig ist.
7. Klicken Sie **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 **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.

**Extrahieren Sie die ExtraHop-Lieferantenobjekt-OID**
Bevor Sie ein Gerät mit SNMP überwachen können, benötigen Sie `Sysobject-ID`, das eine OID enthält, bei der es sich um die vom Hersteller gemeldete Identität des Gerät handelt.

Die SNMP Vendor Object ID (OID) für das ExtraHop-System lautet iso.3.6.1.4.1.32015. Sie können diesen Wert auch extrahieren mit `snmpwalk`.

1. Melden Sie sich an der Befehlszeilenschnittstelle auf Ihrer Management-Workstation an.
2. Extrahieren Sie die OID, wobei *ip-adresse* ist die IP-Adresse für Ihr ExtraHop-System:
   In diesem Beispiel fragen Sie mit `Sysobject-ID`:

   `snmpwalk -v 2c -c öffentlich < ip-adresse> SNMPv2-MIB: :SysobjectID`

   Eine ähnliche Antwort wie in diesem Beispiel wird angezeigt:

   ```
   SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.32015.1.2
   ```

   In diesem Beispiel fragen Sie mit der OID ab:

   `snmpwalk -v 2c -c öffentlich < ip-adresse> 1.3.6.1.2.1.1.2`

   Eine ähnliche Antwort wie in diesem Beispiel wird angezeigt:

   ```
   SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.32015.1.2
   ```

**Tabelle 1: OID-Antwortgerätetypcode**

| Art des Geräts | Gerätetypcode |
|---|---|
| EDA | 1.1 |
| ECA | 1.2 |
| EXA | 1.3 |
| ETA | 1.4 |

## Systembenachrichtigungen an einen Remote-Syslog-Server senden

Mit der Syslog-Exportoption können Sie Warnmeldungen oder Audit-Logs 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.

Sie können die folgenden Arten von Benachrichtigungen an das Syslog senden:

- Benachrichtigungen über Speicherwarnungen
- ExtraHop Warnmeldungen

**Hinweis:** Informationen zum Senden von Auditprotokollen finden Sie unter Audit-Log-Daten an einen Remote-Syslog-Server senden

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**, klicken Sie dann auf **Syslog**.
3. In der Reiseziel Feld, geben Sie die IP-Adresse des Remote-Syslog-Servers ein.
4. Aus dem **Protokoll** Drop-down-Menü, wählen **TCP** oder **UDP**.

   Diese Option gibt das Protokoll an, über das die Informationen an Ihren Remote-Syslog-Server gesendet werden.
5. In der Hafen In diesem Feld geben Sie die Portnummer für Ihren Remote-Syslog-Server ein.

   Der Standardwert ist 514.
6. Klicken Sie **Einstellungen testen** um zu überprüfen, ob Ihre Syslog-Einstellungen korrekt sind.

   Wenn die Einstellungen korrekt sind, sollte in der Syslog-Datei auf dem Syslog-Server ein Eintrag ähnlich dem folgenden angezeigt werden:

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

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

   a) Klicken Sie **Admin**.
   b) Klicken Sie **Config ausführen (ungespeicherte Änderungen)**.
   c) Klicken Sie **Konfiguration bearbeiten**.
   d) Fügen Sie 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 Sie **Aktualisieren**.
f) Klicken Sie **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 Sie **Admin**.
   b) Klicken Sie **Config ausführen (ungespeicherte Änderungen)**.
   c) Klicken Sie **Konfiguration bearbeiten**.
   d) Fügen Sie 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 Sie **Aktualisieren**.
   f) Klicken Sie **Erledigt**.

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

## TLS-Zertifikat

TLS-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 TLS-Zertifikats wird der Webserverdienst neu gestartet. Die getunnelten Verbindungen von ExtraHop-Sensoren zu den ExtraHop-Konsolen gehen verloren, werden dann aber automatisch wiederhergestellt.

### Laden Sie ein TLS-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 automatisiere diese Aufgabe über die REST-API.

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 **TLS-Zertifikat**.
3. Klicken Sie **Zertifikate verwalten** um den Abschnitt zu erweitern.
4. Klicken Sie **Wählen Sie Datei** und navigieren Sie zu dem Zertifikat, das Sie hochladen möchten.
5. Klicken Sie **Offen**.
6. Klicken Sie **Upload**.
7. Speichern Sie die laufende Konfigurationsdatei

## Generieren Sie ein selbstsigniertes Zertifikat

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 **TLS-Zertifikat**.
3. Klicken Sie **Zertifikate verwalten** um den Abschnitt zu erweitern.
4. Klicken Sie **Erstellen Sie ein selbstsigniertes SSL-Zertifikat basierend auf dem Hostnamen** .
5. Auf dem Zertifikat generieren Seite, klicken **OK** um das selbstsignierte TLS-Zertifikat zu generieren.

   **Hinweis:** Der Standard-Hostname ist `extrahop`.
6. Speichern Sie die laufende Konfigurationsdatei

## Erstellen Sie eine Anfrage zur Zertifikatsignierung von Ihrem ExtraHop-System

Eine Certificate Signing Request (CSR) ist ein verschlüsselter Textblock, der Ihrer Zertifizierungsstelle (CA) zur Verfügung gestellt wird, wenn Sie ein TLS-Zertifikat beantragen. Die CSR wird auf dem ExtraHop-System generiert, auf dem das TLS-Zertifikat installiert wird, und enthält Informationen , die in das Zertifikat aufgenommen werden, wie 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. In der Netzwerkeinstellungen Abschnitt, klicken **TLS-Zertifikat**.
3. Klicken Sie **Zertifikate verwalten** und klicken Sie dann **Eine Zertifikatsignieranforderung (CSR) exportieren**.
4. In der Betreff Alternative Namen Abschnitt, geben Sie den DNS-Namen des ExtraHop-Systems ein.

   Sie können mehrere DNS-Namen und IP-Adressen hinzufügen, die durch ein einziges TLS-Zertifikat geschützt werden sollen.
5. In der Betreff Abschnitt, füllen Sie die folgenden Felder aus.

   Nur die **Allgemeiner Name** Feld ist erforderlich.

| Feld | Beschreibung | Beispiele |
|---|---|---|
| Allgemeiner Name | Der vollqualifizierte Domänenname (FQDN) des ExtraHop-Systems . Der FQDN muss mit einem der alternativen Betreffnamen übereinstimmen. | *.example.com<br>discover.example.com |
| E-mail-Adresse | Die E-Mail-Adresse des Hauptansprechpartners für Ihre Organisation. | webmaster@example.com |

| Feld | Beschreibung | Beispiele |
|---|---|---|
| Organisatorische Einheit | Die Abteilung Ihrer Organisation, die das Zertifikat bearbeitet. | IT-Abteilung |
| Organisation | Der offizielle Name Ihrer Organisation. Dieser Eintrag darf nicht abgekürzt werden und sollte 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 der sich Ihre Organisation befindet. Dieser Eintrag sollte nicht abgekürzt werden. | Washington |
| Landeskennzahl | Der zweibuchstabige ISO-Code für das Land, in dem sich Ihre Organisation befindet. | UNS |

6. Klicken Sie **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 TLS-Zertifikat von der CA erhalten haben, kehren Sie zur TLS-Zertifikat Seite in den Administrationseinstellungen und laden Sie das Zertifikat in das ExtraHop-System hoch.

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

## 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 von 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 mithilfe dieser Zertifikate validiert werden.

**Bevor Sie beginnen**
Sie müssen sich als Benutzer mit Setup- oder Systemberechtigungen anmelden und auf Administratorrechte zugreifen , 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 existieren, 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 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 Netzwerkeinstellungen Abschnitt, klicken Sie **Vertrauenswürdige Zertifikate**.
3. Optional: Wenn Sie den im ExtraHop-System enthaltenen integrierten Zertifikaten vertrauen möchten, wählen Sie **Vertrauenssystem-Zertifikate**, klicken **Speichern**, und dann speichern Sie die laufende Konfigurationsdatei.
4. Um Ihr eigenes Zertifikat hinzuzufügen, klicken Sie auf **Zertifikat hinzufügen** und dann in der Zertifikat Feld, fügen Sie den Inhalt der PEM-kodierten Zertifikatskette ein.
5. In der Name Feld, geben Sie einen Namen ein.
6. Klicken Sie **Hinzufügen**.

# Auf Einstellungen zugreifen

In der Auf Einstellungen zugreifen In diesem Abschnitt können Sie Benutzerkennwörter ändern, das Support-Konto aktivieren, lokale Benutzer und Benutzergruppen verwalten, die Fernauthentifizierung konfigurieren und den API-Zugriff verwalten.

## Globale Richtlinien

Administratoren können globale Richtlinien konfigurieren, die für alle Benutzer gelten, die auf das System zugreifen.

**Passwort-Richtlinie**

- Wählen Sie zwischen zwei Passwortrichtlinien: der standardmäßigen Passwortrichtlinie mit 5 oder mehr Zeichen oder einer strengeren Passwortrichtlinie mit den folgenden Einschränkungen:
  - 8 oder mehr Zeichen
  - Groß- und Kleinbuchstaben
  - Mindestens eine Zahl
  - Mindestens ein Symbol

  **Hinweis:** Wenn Sie die strikte Passwortrichtlinie mit 8 oder mehr Zeichen wählen, laufen Passwörter alle 60 Tage ab.

**Steuerung zum Bearbeiten von Gerätegruppen**

- Steuern Sie, ob Benutzer mit eingeschränkte Schreibrechte kann Gerätegruppen erstellen und bearbeiten. Wenn diese Richtlinie ausgewählt ist, können alle Benutzer mit eingeschränktem Schreibzugriff Gerätegruppen erstellen und andere Benutzer mit eingeschränktem Schreibzugriff als Redakteure zu ihren Gerätegruppen hinzufügen.

**Standard-Dashboard**

- Geben Sie das Dashboard an, das Benutzer sehen, wenn sie sich am System anmelden. Nur Dashboards, die mit allen Benutzern geteilt werden, können als globaler Standard festgelegt werden. Benutzer können diese Standardeinstellung überschreiben. über das Befehlsmenü eines beliebigen Dashboard.

**Passwort für Dateiextraktion**

- (Nur NDR-Modul) Geben Sie ein erforderliches Passwort an, das Sie mit zugelassenen Benutzern zum Entpacken teilen können Dateien, die aus einer Paketabfrage extrahiert und heruntergeladen wurden.

## 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, gibt es ein blaues **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 Administrationseinstellungen, klicken Sie auf das blaue **Standardpasswort ändern** knopf. Die Passwortseite wird ohne das Dropdownmenü für Konten angezeigt. Das Passwort ändert sich nur für den Setup-Benutzer.
2. In der Altes Passwort Feld, geben Sie das Standardkennwort ein.
3. In der Neues Passwort Feld, geben Sie das neue Passwort ein.
4. In der Bestätigen Sie das Passwort Feld, geben Sie das neue Passwort erneut ein.
5. Klicken Sie **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 ExtraHop Support eine Verbindung zu Ihrem ExtraHop-System herstellen kann, wenn Fernzugriff wird konfiguriert durch ExtraHop Cloud-Dienste .

1. In der Auf Einstellungen zugreifen Abschnitt, klicken **Zugriff auf den Support**.
2. klicken **SSH-Schlüssel generieren**.
3. Kopieren Sie den verschlüsselten Schlüssel aus dem Textfeld und senden Sie den Schlüssel per E-Mail an Ihren ExtraHop-Vertreter.
4. Klicken Sie **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.

## 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. Für RevealX 360 können Sie Benutzergruppen über die API hinzufügen

**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 erfahren, wie man Remote-Konten konfiguriert.

Die folgenden Konten sind standardmäßig auf ExtraHop-Systemen konfiguriert, erscheinen aber 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 vollständige System-Lese- und Schreibrechte für die browserbasierte Benutzeroberfläche und die ExtraHop-Befehlszeilenschnittstelle (CLI). Die standardmäßigen Anmelde- und Kennwortinformationen finden Sie unter Häufig gestellte Fragen zu Standardbenutzerkonten.

**Schale**

Das `shell` account hat standardmäßig Zugriff auf Shell-Befehle ohne Administratorrechte 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 beide Konten bei der Bereitstellung in Amazon Web Services (AWS) und Google Cloud Platform (GCP) ist die Instanz-ID der virtuellen Maschine.

### Nächste Schritte

- Fügen Sie einer Konsole oder einem Sensor ein lokales Benutzerkonto hinzu
- Fügen Sie einem Recordstore oder Packetstore ein lokales Benutzerkonto hinzu

### Fernauthentifizierung

Das ExtraHop-System unterstützt die Fernauthentifizierung für den Benutzerzugriff. Mithilfe der Fernauthentifizierung können Organisationen, die über Authentifizierungssysteme wie LDAP (z. B. OpenLDAP oder Active Directory) verfügen, allen oder einer Teilmenge ihrer Benutzer ermöglichen, sich mit ihren vorhandenen Anmeldedaten am System anzumelden.

**Wichtig:** Die Menüauswahl variiert je nachdem, welchen Appliance-Typ Sie konfigurieren. SAML ist beispielsweise nur für Sensoren und Konsolen verfügbar.

Die zentralisierte Authentifizierung bietet die folgenden Vorteile:

- Synchronisation des Benutzerkennworts.
- Automatische Erstellung von ExtraHop-Konten für Benutzer ohne Administratoreingriff.
- Verwaltung der ExtraHop-Rechte 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 Fernauthentifizierung über LDAP
- Konfigurieren Sie die Fernauthentifizierung über SAML (Nur Sensoren und Konsolen)
- Konfigurieren Sie die Fernauthentifizierung über TACACS+
- Konfigurieren Sie die Fernauthentifizierung 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 geteilte Inhalte nach Gruppen statt nach einzelnen Benutzern zu verwalten. Benutzerdefinierte Objekte wie Aktivitätskarten können mit einer Benutzergruppe geteilt werden, und jeder Benutzer, der der Gruppe hinzugefügt wird, hat automatisch Zugriff darauf. Sie können eine lokale Benutzergruppe erstellen, die entfernte 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 Sie **Benutzergruppe erstellen** um eine lokale Gruppe zu erstellen. Die Benutzergruppe wird in der Liste angezeigt. Markieren Sie dann das Kontrollkästchen neben dem Namen der Benutzergruppe und wählen Sie Benutzer aus dem **Benutzer filtern...** Drop-down-Menü. Klicken Sie **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 Sie **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 Sie **Benutzergruppe aktivieren** oder **Benutzergruppe deaktivieren** um zu steuern, ob ein Gruppenmitglied auf geteilte Inhalte für die ausgewählte Benutzergruppe zugreifen kann.
- Klicken Sie **Benutzergruppe löschen** um die gewählte 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 Benutzergruppentyp an.

  **Mitglieder**

  Zeigt die Anzahl der Benutzer in der Gruppe an.

  **Geteilte Inhalte**

  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 von der aus aktualisieren Benutzergruppe Seite oder aus dem Liste der Mitglieder Seite.
- Ein Remote-Benutzer meldet sich zum ersten Mal am 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 die rollenbasierte Zugriffskontrolle (RBAC) aktivieren, indem sie Benutzern 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, Pakete und Sitzungsschlüssel, nur Pakete, nur Paket-Header oder nur Paket-Slices anzuzeigen und herunterzuladen. Ermöglicht dem Benutzer auch das Extrahieren von Dateien, die Paketen zugeordnet sind.

### Systemzugriffsrechte

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

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

Für RevealX 360 müssen Systemzugriffs- und Administratorrechte sowie der Zugriff auf lizenzierte Module, Pakete und Sitzungsschlüssel separat zugewiesen werden. RevealX 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 RevealX 360)** | **Vollständige Schreiben** | **Eingeschränk Schreiben** | **Persönliches Schreiben** | **Vollständig schreibgesch** | **Eingeschränkter Schreibschutz** |
|---|---|---|---|---|---|---|---|
| Karten der Aktivitäten | | | | | | | |
| Karten für geteilte 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 |
| Analyse-Prioritäten | | | | | | | |
| 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 | | | | | | | |

| | System- und Zugriffsverw | Systemadmi (nur RevealX 360) | Vollständige Schreiben | Eingeschränk Schreiben | Persönliches Schreiben | Vollständig schreibgesch | Eingeschränkter Schreibschutz |
|---|---|---|---|---|---|---|---|
| Ein Paket erstellen | Y | Y | Y | N | N | N | N |
| Laden Sie ein Paket hoch und wenden Sie es an | Y | Y | Y | N | N | N | N |
| Laden Sie ein Paket herunter | Y | Y | Y | Y | Y | N | N |
| Liste der Bundles anzeigen | Y | Y | Y | Y | Y | Y | N |
| Armaturenbretter | | | | | | | |
| 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 |

| | System- und Zugriffsverw | Systemadmi (nur RevealX 360) | Vollständige Schreiben | Eingeschränk Schreiben | Persönliches Schreiben | Vollständig schreibgesch | Eingeschränkter Schreibschutz |
|---|---|---|---|---|---|---|---|
| Gerätegruppen | Administratoren können das 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 Rechterichtlinie aktiviert ist) | N | N | N |
| Integrationen | Nur RevealX 360 | | | | | | |
| Integrationen konfigurieren und ändern | Y | Y | N | N | N | N | N |
| Datei-Analyse | | | | | | | |
| Einstellungen und Regeln für die Dateianalyse konfigurieren | Y | Y | N | N | N | N | N |
| Metriken | | | | | | | |
| Metriken anzeigen | Y | Y | Y | Y | Y | Y | N |
| Regeln für Benachrichtigungen | NDR-Modullizenz und Zugriff sind erforderlich , um Benachrichtigungen für Sicherheitserkennungen, Sicherheitserkennungskataloge und Bedrohungsinformationen zu erstellen und zu ändern.<br>NPM-Modullizenz und Zugriff sind erforderlich, um Benachrichtigungen für Leistungserkennungen und den Leistungserkennungskatalog zu erstellen und zu ändern. | | | | | | |
| Regeln für Erkennungsbenachrichtigungen erstellen und ändern | Y | Y | Y | N | N | N | N |
| Regeln für Erkennungsbenachrichtigungen für SIEM-Integrationen erstellen und ändern (nur RevealX 360) | Y | Y | N | N | N | N | N |
| Benachrichtigungsregeln für den Erkennungskatalog erstellen und ändern | Y | Y | Y | N | N | N | N |

| | System- und Zugriffsverw | Systemadmi (nur RevealX 360) | Vollständige Schreiben | Eingeschränk Schreiben | Persönliches Schreiben | Vollständig schreibgesch | Eingeschränkter Schreibschutz |
|---|---|---|---|---|---|---|---|
| Benachrichtigungsregeln Bedrohungsübersicht erstellen und ändern | Y | Y | Y | N | N | N | N |
| Regeln für Systembenachrichtigungen erstellen und ändern | 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 |
| Bedrohungsinformationen | NDR-Modul | Lizenz 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 | | | | | | | |

| | System- und Zugriffsverw | Systemadmi (nur RevealX 360) | Vollständige Schreiben | Eingeschränk Schreiben | Persönliches Schreiben | Vollständig schreibgesch | Eingeschränkter Schreibschutz |
|---|---|---|---|---|---|---|---|
| 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 |

## Lokales Benutzerkonto hinzufügen

Indem Sie ein lokales Benutzerkonto hinzufügen, 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 Auf Einstellungen zugreifen Abschnitt, klicken **Nutzer**.
3. klicken **Benutzer hinzufügen**.
4. In der Personenbezogene Daten Abschnitt, geben Sie in das Feld Anmelde-ID den Benutzernamen ein, mit dem sich Benutzer am Sensor anmelden, der keine Leerzeichen enthalten darf.

   Zum Beispiel `Adalovelace`.
5. Geben Sie im Feld Vollständiger Name einen Anzeigenamen für den Benutzer ein.

   Der Name kann Leerzeichen enthalten. Zum Beispiel `Ada Lovelace`.
6. Geben Sie im Feld Passwort das Passwort für dieses Konto ein.

   **Hinweis:** Auf Sensoren und Konsolen muss das Passwort die vom globale Passwortrichtlinie. In ExtraHop-Recordstores und Packetstores müssen Passwörter mindestens 5 Zeichen lang sein.
7. Geben Sie im Feld „Passwort bestätigen“ erneut das Passwort aus dem Passwort Feld.
8. In der Authentifizierungstyp Abschnitt, auswählen **Lokal**.
9. In der Benutzertyp Abschnitt, wählen Sie die Art der Rechte für den Benutzer aus.
   - System- und Zugriffsadministrationsrechte ermöglichen den vollen Lese- und Schreibzugriff auf das ExtraHop-System, einschließlich der Administrationseinstellungen.
   - Eingeschränkte Rechte ermöglichen es Ihnen, aus einer Teilmenge von Rechten und Optionen auszuwählen.

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

10. Klicken Sie **Speichern**.

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

### Konto für einen Remote-Benutzer hinzufügen

Fügen Sie ein Benutzerkonto für LDAP- oder SAML-Benutzer hinzu, wenn Sie den Remote-Benutzer bereitstellen möchten, bevor sich dieser Benutzer beim ExtraHop-System anmeldet. Nachdem der Benutzer zum System hinzugefügt wurde, können Sie ihn zu lokalen Gruppen hinzufügen oder Elemente direkt mit ihm teilen, bevor er sich über den LDAP- oder SAML-Anbieter anmeldet.

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

   • **Anmelde-ID:** Die E-Mail-Adresse, mit der sich der Benutzer bei seinem LDAP- oder SAML-SSO-Identitätsanbieter anmeldet.

   **Hinweis:** Für Remotebenutzer werden nur E-Mail-Adressen in Kleinbuchstaben unterstützt.

   • **Vollständiger Name:** Der Vor- und Nachname des Benutzers.
5. In der Authentifizierungstyp Abschnitt, wählen **Ferngesteuert**.
6. Klicken Sie **Speichern**.

## 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 Fernauthentifizierung können Organisationen, die über Authentifizierungssysteme wie LDAP (z. B. OpenLDAP oder Active Directory) verfügen, allen oder einer Teilmenge ihrer Benutzer ermöglichen, sich mit ihren vorhandenen Anmeldedaten am System anzumelden.

**Wichtig:** Die Menüauswahl variiert je nachdem, welchen Appliance-Typ Sie konfigurieren. SAML ist beispielsweise nur für Sensoren und Konsolen verfügbar.

Die zentralisierte Authentifizierung bietet die folgenden Vorteile:

- Synchronisation des Benutzerkennworts.
- Automatische Erstellung von ExtraHop-Konten für Benutzer ohne Administratoreingriff.
- Verwaltung der ExtraHop-Rechte 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 Fernauthentifizierung über LDAP
- Konfigurieren Sie die Fernauthentifizierung über SAML (Nur Sensoren und Konsolen)
- Konfigurieren Sie die Fernauthentifizierung über TACACS+
- Konfigurieren Sie die Fernauthentifizierung über RADIUS

## Konfigurieren Sie die Fernauthentifizierung über LDAP

Das ExtraHop-System unterstützt das Lightweight Directory Access Protocol (LDAP) zur 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 keine anderen Entitäten ab, die sich möglicherweise im LDAP-Verzeichnis befinden.

**Bevor Sie beginnen**

- Für dieses Verfahren müssen Sie mit der Konfiguration von LDAP vertraut sein.
- 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 für 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 im 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 Methode der Fernauthentifizierung umstellen, werden die Benutzer, Benutzergruppen und zugehörigen Anpassungen, die über die Remote-Authentifizierung erstellt wurden, entfernt. Lokale Benutzer sind nicht betroffen.

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 der Fernauthentifizierung Drop-down-Menü, wählen **LDAP** und klicken Sie dann **Fortfahren**.
4. 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.
5. In der Hafen In diesem Feld geben Sie die Portnummer ein, auf der der LDAP-Server lauscht.
6. Aus dem **Servertyp** Drop-down-Menü, wählen **Posix** oder **Active Directory**.
7. Optional: In der Binden Sie DN Feld, geben Sie den Bindungs-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 Organisationseinheiten, Gruppen oder Benutzerkonto haben, die für die LDAP-Authentifizierung erforderlich sind. Wenn dieser Wert nicht gesetzt ist, wird eine anonyme Bindung durchgeführt. Beachten Sie, dass anonyme Bindungen nicht auf allen LDAP-Servern aktiviert sind.

8. Optional: In der Passwort binden Feld, geben Sie das Bindungskennwort ein. Das Bind-Passwort ist das Passwort, das für die Authentifizierung beim LDAP-Server als den 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. Fragen Sie Ihren LDAP-Administrator nach den richtigen Einstellungen.
9. Aus dem **Verschlüsselung** Wählen Sie im Dropdownmenü eine der folgenden Verschlüsselungsoptionen aus.

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

   • **SCHÜSSE:** Diese Option gibt LDAP an, das in TLS eingeschlossen ist.

   • **TLS starten:** Diese Option spezifiziert TLS LDAP. (TLS wird ausgehandelt, bevor Passwörter gesendet werden.)
10. Wählen **SSL-Zertifikate validieren** um die Zertifikatsvalidierung zu aktivieren. Wenn Sie diese Option auswählen, wird das Zertifikat auf dem Remote-Endpunkt anhand der Stammzertifikate überprüft, die vom Trusted Certificates Manager angegeben wurden. Auf der Seite Vertrauenswürdige Zertifikate müssen Sie konfigurieren, welchen Zertifikaten Sie vertrauen möchten. Weitere Informationen finden Sie unter Fügen Sie Ihrem ExtraHop-System ein vertrauenswürdiges Zertifikat hinzu.
11. In der Aktualisierungsintervall Feld, geben Sie einen Zeitwert ein 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.
12. In der Basis DN Feld, geben Sie den eindeutigen Basisnamen (DN) ein.

    Der Basis-DN ist der Punkt, von dem aus ein Server nach Benutzern sucht. Nur Benutzergruppen innerhalb des Basis-DN können auf das ExtraHop-System zugreifen. Die Benutzer können direkte Mitglieder des Basis-DN sein oder innerhalb einer OU innerhalb des Basis-DN verschachtelt sein, wenn **Gesamter Teilbaum** Option ist ausgewählt für Umfang der Suche unten angegeben.

    **Wichtig:** Für Recordstores und Packetstores erhalten alle Benutzer, die auf den Recordstore oder Packetstore zugreifen können, Administratorrechte. Mit dem Feld Vollzugriff-DN können Sie den Zugriff weiter einschränken.
13. In der Suchfilter Feld, geben Sie einen Suchfilter ein.

    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 zu umschließen, und analysiert diesen Parameter nicht korrekt, wenn Sie Klammern manuell hinzufügen. Fügen Sie in diesem Schritt und in Schritt 5b Ihre Suchfilter hinzu, ähnlich dem folgenden Beispiel:

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

    Wenn Ihre Gruppennamen außerdem das Sternchen (*) enthalten, muss das Sternchen als maskiert werden `\2a`. Zum Beispiel, wenn Ihre Gruppe eine CN mit dem Namen hat `test*group`, typ `cn=test\2agroup` im Feld Suchfilter.
14. Aus dem **Umfang der Suche** Wählen Sie im Dropdownmenü eine der folgenden Optionen aus.

    Der Suchbereich gibt den Umfang der Verzeichnissuche bei der Suche nach Benutzerentitäten an.

    • **Ganzer Unterbaum:** 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.
15. Für Plattenläden und Paketläden, in der **Vollzugriff DN** Feld, geben Sie einen DN innerhalb des Basis-DN ein.

Diese Option schränkt den Recordstore- oder Packetstore-Zugriff weiter nur auf den angegebenen DN ein.

**Wichtig:** Allen Benutzern, die auf den Recordstore oder Packetstore zugreifen können, werden Administratorrechte gewährt.

16. Optional: Wählen Sie für Sensoren und Konsolen die **Benutzergruppen vom LDAP-Server importieren** Markieren Sie das Kontrollkästchen und konfigurieren Sie die folgenden Einstellungen, um Benutzergruppen zu importieren.

    **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) In der Basis DN Feld, geben Sie den Basis-DN ein.

    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 werden. Die Benutzergruppen können direkte Mitglieder des Basis-DN sein oder innerhalb einer Organisationseinheit innerhalb des Basis-DN verschachtelt sein, wenn **Gesamter Teilbaum** Option ist ausgewählt für Umfang der Suche unten angegeben.

    b) In der Suchfilter Feldtyp einen Suchfilter.

    Mithilfe von 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 im Dropdownmenü eine der folgenden Optionen aus.

    Der Suchbereich gibt den Umfang der Verzeichnissuche bei der Suche nach Benutzergruppenentitäten an.

    • **Ganzer Unterbaum:** 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.

17. 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 Liste der Fehler zu sehen. Sie müssen alle Fehler beheben, bevor Sie fortfahren.

18. Klicken Sie **Speichern und fortfahren**.

**Nächste Schritte**
Benutzerrechte für die Fernauthentifizierung konfigurieren

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

**Wichtig:** Dieser Abschnitt bezieht sich nur auf Sensoren und Konsolen. Für Recordstores und Packetstores erhalten alle Benutzer, die auf den Recordstore oder Packetstore zugreifen können, Administratorrechte.

Wenn Sie Benutzerberechtigungen 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 anwesend sind, werden im 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 dem  Optionen für die Zuweisung von Rechten Drop-down-Menü:

   - **Berechtigungsstufe vom Remoteserver abrufen**

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

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

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

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

     • **Persönliches Schreiben DN:** Erstellen Sie persönliche Dashboards und ändern Sie Dashboards, die mit dem angemeldeten Benutzer geteilt werden.

     • **Vollständiger schreibgeschützter DN:** Objekte im ExtraHop-System anzeigen.

     • **Eingeschränkter schreibgeschützter DN:** Sehen Sie sich Dashboards an, die mit dem angemeldeten Benutzer geteilt wurden.

     • **Packet Slices Access DN:** Zeigen Sie die ersten 64 Byte von Paketen an, die über einen Packetstore erfasst wurden, und laden Sie sie herunter.

     • **Paket-Header Access DN:** Sucht und lädt nur die Paket-Header von Paketen herunter, die über einen Packetstore erfasst wurden.

     • **Paketzugriffs-DN:** Pakete anzeigen und herunterladen, die über einen Packetstore erfasst wurden.

     • **Paket- und Sitzungsschlüssel Access DN:** Pakete und alle zugehörigen TLS-Sitzungsschlüssel, die über einen Packetstore erfasst wurden, anzeigen und herunterladen.

     • **NDR-Modulzugriff DN:** Sicherheitserkennungen, die im ExtraHop-System erscheinen, anzeigen, bestätigen und ausblenden.

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

   - **Remote-Benutzer haben vollen Schreibzugriff**

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

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

   - **Kein Zugriff**
   - **Nur Paketsegmente**
   - **Nur Paket-Header**
   - **Nur Pakete**
   - **Pakete und Sitzungsschlüssel**

3. Optional: Konfigurieren Sie den NDR- und NPM-Modulzugriff (nur auf Sensoren und Konsolen).
   - **Kein Zugriff**
   - **Voller Zugriff**
4. Klicken Sie **Speichern und fertig**.
5. Klicken Sie **Erledigt**.

## Konfigurieren Sie die Fernauthentifizierung über SAML

Sie können die sichere SSO-Authentifizierung (Single Sign-On) für das ExtraHop-System über einen oder mehrere SAML-Identitätsanbieter (Security Assertion Markup Language) konfigurieren.

**Video:** Sehen Sie sich die entsprechende Schulung an: SSO-Authentifizierung

**Wichtig:** Dieses Handbuch ist nur für RevealX Enterprise. Informationen zu RevealX 360 finden Sie unter Ermöglichen Sie die Sensorzugriffskontrolle über Ihren eigenen Identitätsanbieter.

Wenn sich ein Benutzer bei einem ExtraHop-System anmeldet, das als Service Provider (SP) für die SAML-SSO-Authentifizierung konfiguriert ist, fordert das ExtraHop-System die Autorisierung vom entsprechenden Identity Provider ( IdP) an. Der Identitätsanbieter authentifiziert die Anmeldedaten des Benutzers und gibt dann die Autorisierung für den Benutzer an das ExtraHop-System zurück. Der Benutzer kann dann auf das ExtraHop-System zugreifen.

Konfigurationsleitfäden für bestimmte Identitätsanbieter sind unten verlinkt. Wenn Ihr Anbieter nicht aufgeführt ist, wenden Sie die vom ExtraHop-System erforderlichen Einstellungen auf Ihren Identitätsanbieter an.

Identitätsanbieter müssen die folgenden Kriterien erfüllen:

- SAML 2.0
- Unterstützt SP-initiierte Anmeldeabläufe. IDP-initiierte Anmeldeabläufe werden nicht unterstützt.
- Unterstützt signierte SAML-Antworten
- Unterstützt HTTP-Redirect-Binding

Die Beispielkonfiguration in diesem Verfahren ermöglicht den Zugriff auf das ExtraHop-System über Gruppenattribute.

Wenn Ihr Identitätsanbieter keine Gruppenattributanweisungen unterstützt, konfigurieren Sie Benutzerattribute mit den entsprechenden Rechten für Modulzugriff, Systemzugriff und Paketforensik.

### SAML-Remoteauthentifizierung aktivieren

**Bevor Sie beginnen**

**Warnung:** Wenn Ihr System bereits mit einer Fernauthentifizierungsmethode konfiguriert ist, werden durch das Ändern dieser Einstellungen alle Benutzer und zugehörigen Anpassungen entfernt, die mit dieser Methode erstellt wurden, und Remotebenutzer können nicht auf das System zugreifen. Lokale Benutzer sind nicht betroffen.

Sie können die Fernauthentifizierung mit SAML auf diesem ExtraHop-System aktivieren.

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 der Fernauthentifizierung** Drop-down-Menü, wählen **SAML**.
4. Klicken Sie **Weiter**.
5. klicken **SP-Metadaten anzeigen** um die Assertion Consumer Service (ACS) -URL und die Entitäts-ID des ExtraHop-Systems anzuzeigen.

Diese Zeichenfolgen werden von Ihrem Identitätsanbieter benötigt, um die SSO-Authentifizierung zu konfigurieren. Sie können auch nach unten scrollen, um die Metadaten als XML-Datei herunterzuladen , die Sie in Ihre Identitätsanbieter-Konfiguration importieren können.

**Hinweis:** Die ACS-URL enthält den in den Netzwerkeinstellungen konfigurierten Hostnamen. Wenn die ACS-URL einen nicht erreichbaren Hostnamen enthält, z. B. den Standardsystemhostnamen `extrahop`, müssen Sie die URL bearbeiten, wenn Sie die ACS-URL zu Ihrem Identitätsanbieter hinzufügen, und den vollqualifizierten Domänenname (FQDN) des ExtraHop-Systems angeben.

6. klicken **Identitätsanbieter hinzufügen**.
7. In der Name des Anbieters Feld, geben Sie einen Namen ein, um Ihren spezifischen Identitätsanbieter zu identifizieren.

   Dieser Name erscheint auf der Anmeldeseite des ExtraHop-Systems nach dem Text Anmelden mit Text.
8. In der Entitäts-ID Feld, fügen Sie die von Ihrem Identitätsanbieter bereitgestellte Entitäts-ID ein.
9. In der SSO-URL Fügen Sie in dieses Feld die von Ihrem Identitätsanbieter bereitgestellte Single Sign-On-URL ein.
10. In der Öffentliches Zertifikat Fügen Sie in dieses Feld das X.509-Zertifikat ein, das von Ihrem Identitätsanbieter bereitgestellt wurde.
11. Wählen Sie die **Automatische Bereitstellung von Benutzern** Kontrollkästchen, um anzugeben , dass ExtraHop-Benutzerkonten automatisch erstellt werden, wenn sich der Benutzer über den Identitätsanbieter anmeldet.

    Um manuell zu steuern, welche Benutzer sich anmelden können, deaktivieren Sie dieses Kontrollkästchen und konfigurieren Sie neue Remote-Benutzer manuell über die ExtraHop-Administrationseinstellungen oder die REST-API. Jeder manuell erstellte Remote-Benutzername sollte mit dem auf dem Identitätsanbieter konfigurierten Benutzernamen übereinstimmen.
12. Wählen Sie die **Diesen Identitätsanbieter aktivieren** Kontrollkästchen, um Benutzern die Anmeldung am ExtraHop-System zu ermöglichen.

    Dies ist standardmäßig aktiviert. Um zu verhindern, dass sich Benutzer über diesen Identitätsanbieter anmelden, deaktivieren Sie das Kontrollkästchen.
13. In der Attribute von Benutzerrechten Abschnitt, Konfiguration von Benutzerberechtigungsattributen.

    Dies muss abgeschlossen sein, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Bei Werten wird nicht zwischen Groß- und Kleinschreibung unterschieden und sie können Leerzeichen enthalten. Die Namen und Werte der Benutzerberechtigungsattribute müssen mit den Namen und Werten übereinstimmen, die Ihr Identitätsanbieter in SAML-Antworten einbezieht, die konfiguriert werden, wenn Sie die ExtraHop-Anwendung zu einem Anbieter hinzufügen. In Microsoft Entra ID konfigurieren Sie beispielsweise Anspruchsnamen und Anspruchsbedingungswerte, die mit den Namen und Werten der Benutzerberechtigungsattribute im ExtraHop-System übereinstimmen müssen.

    **Hinweis:** Wenn ein Benutzer mehreren Attributwerten entspricht, wird dem Benutzer das Zugriffsrecht mit den meisten Berechtigungen gewährt. Wenn ein Benutzer beispielsweise den Werten Eingeschränktes Schreiben und Vollständiges Schreiben entspricht, erhält der Benutzer volle Schreibberechtigungen. Weitere Hinweise zu Berechtigungsstufen finden Sie unter Benutzer und Benutzergruppen.

    Ausführlichere Beispiele finden Sie in den folgenden Themen:

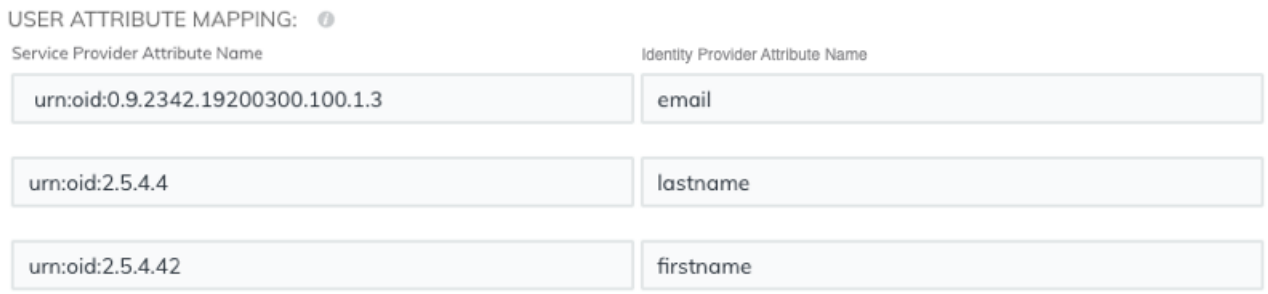
    - SAML-Single-Sign-On mit JumpCloud konfigurieren
    - SAML-Single-Sign-On mit Google konfigurieren
    - SAML-Single-Sign-On mit Okta konfigurieren
    - SAML-Single-Sign-On mit Microsoft Entra ID konfigurieren
14. In der Zugriff auf das NDR-Modul Abschnitt, Konfiguration von Attributen, um Benutzern den Zugriff auf NDR-Funktionen zu ermöglichen.

15. In der Zugriff auf das NPM-Modul Abschnitt, Konfigurieren Sie Attribute, um Benutzern den Zugriff auf NPM-Funktionen zu ermöglichen.
16. In der Zugriff auf Pakete und Sitzungsschlüssel Abschnitt, konfigurieren Sie Attribute, um Benutzern den Zugriff auf Pakete und Sitzungsschlüssel zu ermöglichen.

    Die Konfiguration von Paketen und Sitzungsschlüsselattributen ist optional und nur erforderlich , wenn Sie einen angeschlossenen ExtraHop-Paketstore haben.
17. Klicken Sie **Speichern**.

**Zuordnung von Benutzerattributen**
Sie müssen den folgenden Satz von Benutzerattributen im Abschnitt zur Zuordnung von Anwendungsattributen auf Ihrem Identitätsanbieter konfigurieren. Diese Attribute identifizieren den Benutzer im gesamten ExtraHop-System. Die richtigen Eigenschaftsnamen beim Zuordnen von Attributen finden Sie in der Dokumentation Ihres Identitätsanbieters.

| ExtraHop-Attributname | Freundlicher Name | Kategorie | Attributname des Identitätsanbieters |
|---|---|---|---|
| `urn:oid:0.9.2342.19200300.100.1.3` | mail | Standardattribut | Primäre E-Mail-Adresse |
| `urn:oid:2.5.4.4` | sn | Standardattribut | Nachname |
| `urn:oid:2.5.4.42` | Vorgegebener Name | Standardattribut | Vorname |




**Attributaussagen gruppieren**
Das ExtraHop-System unterstützt Anweisungen zu Gruppenattributen, um Benutzerberechtigungen einfach allen Mitgliedern einer bestimmten Gruppe zuzuordnen. Wenn Sie die ExtraHop-Anwendung auf Ihrem Identitätsanbieter konfigurieren, geben Sie einen Gruppenattributnamen an. Dieser Name wird dann in das Name des Attributs Feld, wenn Sie den Identity Provider auf dem ExtraHop-System konfigurieren.


Wenn Ihr Identitätsanbieter keine Gruppenattributanweisungen unterstützt, konfigurieren Sie Benutzerattribute mit den entsprechenden Rechten für Modulzugriff, Systemzugriff und Paketforensik.

**Die nächsten Schritte**

Nachdem Sie die Remote-Authentifizierung über SAML konfiguriert haben, überprüfen Sie diese Aufgaben.

- SAML-Single-Sign-On mit JumpCloud konfigurieren
- SAML-Single-Sign-On mit Google konfigurieren
- SAML-Single-Sign-On mit Okta konfigurieren

## SAML-Single-Sign-On mit Okta konfigurieren

Sie können Ihr ExtraHop-System so konfigurieren, dass sich Benutzer über den Okta Identity Management Service beim System anmelden können.

**Bevor Sie beginnen**

- Sie sollten mit der Verabreichung von Okta vertraut sein. Diese Verfahren basieren auf der Okta Classic-Benutzeroberfläche. Wenn Sie Okta über die Developer Console konfigurieren, ist das Verfahren möglicherweise etwas anders.
- Sie sollten mit der Verwaltung von ExtraHop-Systemen vertraut sein.

Bei diesen Verfahren müssen Sie Informationen zwischen dem ExtraHop-System und der Okta Classic-Benutzeroberfläche kopieren und einfügen. Daher ist es hilfreich, jedes System nebeneinander zu öffnen .

**SAML auf dem ExtraHop-System aktivieren**

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 der Fernauthentifizierung** Drop-down-Menü, wählen **SAML**.
4. Klicken Sie **Weiter**.
5. Klicken Sie **SP-Metadaten anzeigen**.

   Sie müssen die ACS-URL und die Entitäts-ID kopieren, um sie im nächsten Verfahren in die Okta-Konfiguration einzufügen.

**SAML-Einstellungen in Okta konfigurieren**
Bei diesem Verfahren müssen Sie Informationen zwischen den ExtraHop-Administrationseinstellungen und der Okta Classic-Benutzeroberfläche kopieren und einfügen. Daher ist es hilfreich, wenn alle Benutzeroberflächen nebeneinander geöffnet sind.

1. Loggen Sie sich bei Okta ein.
2. Ändern Sie in der oberen rechten Ecke der Seite die Ansicht von **Entwicklerkonsole** zu **Klassische Benutzeroberfläche**.


3. Klicken Sie im oberen Menü auf **Anwendungen**.
4. Klicken Sie **Anwendung hinzufügen**.
5. Klicken Sie **Neue App erstellen**.
6. Aus dem Plattform Drop-down-Menü, wählen **Netz**.
7. Für die Anmeldemethode, wählen **SAML 2.0** .
8. Klicken Sie **Erstellen**.
9. In der Allgemeine Einstellungen Abschnitt, in der App Namensfeld, geben Sie einen eindeutigen Namen ein, um das ExtraHop-System zu identifizieren.
10. Optional: Konfiguriere die Logo der App und Sichtbarkeit der App Felder, die für Ihre Umgebung erforderlich sind.
11. Klicken Sie **Weiter**.
12. In der SAML-Einstellungen Fügen Sie in den Abschnitten die URL des Assertion Consumer Service (ACS) aus dem ExtraHop-System in das Feld Single Sign On URL in Okta ein.

**Hinweis:** Möglicherweise müssen Sie die ACS-URL manuell bearbeiten, wenn die URL einen nicht erreichbaren Hostnamen enthält, z. B. den Standardsystemhostnamen `extrahop`. Wir

empfehlen Ihnen, den vollqualifizierten Domänenname für das ExtraHop-System in der URL anzugeben.

13. Fügen Sie die SP Entity ID aus dem ExtraHop-System in das Zielgruppen-URI (SP-Entitäts-ID) Feld in Okta.
14. Aus dem **Namens-ID-Format** Drop-down-Menü, wählen **Hartnäckig**.
15. Aus dem **Nutzername der Anwendung** Wählen Sie im Drop-down-Menü ein Benutzernamenformat aus.
16. In der Attributaussagen Abschnitt, fügen Sie die folgenden Attribute hinzu.

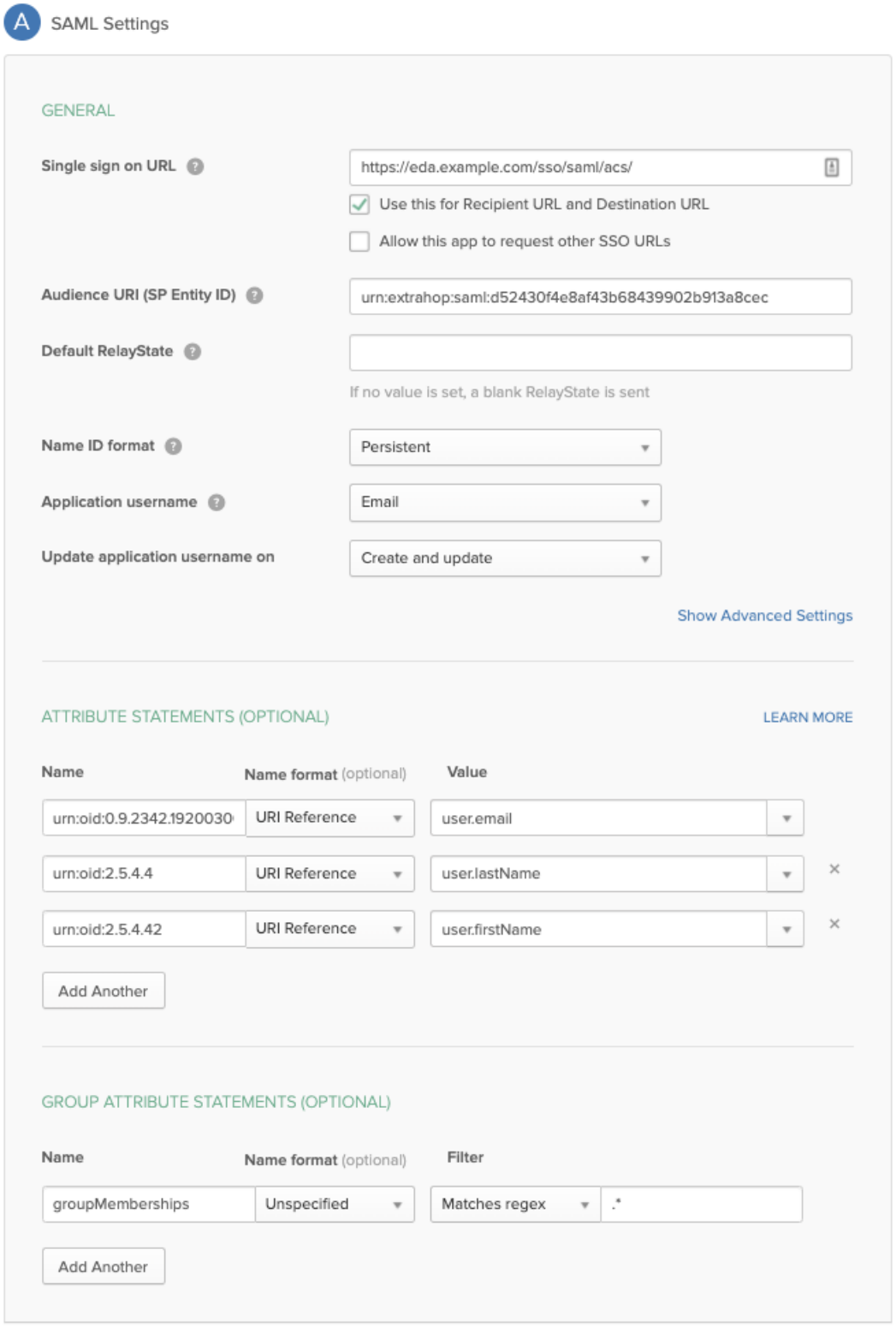
    Diese Attribute identifizieren den Benutzer im gesamten ExtraHop-System.

| Name | Format des Namens | Wert |
|---|---|---|
| `urn:oid:0.9.2342.19200300.100.1.3` | URI-Referenz | Benutzer.E-Mail |
| `urn:oid:2.5.4.4` | URI-Referenz | Benutzer.Nachname |
| `urn:oid:2.5.4.42` | URI-Referenz | Benutzer.Vorname |

17. In der Anweisung zu Gruppenattributen Abschnitt, in der Name Feld, geben Sie eine Zeichenfolge ein und konfigurieren Sie einen Filter.

    Sie geben den Namen des Gruppenattributs an, wenn Sie Benutzerberechtigungsattribute im ExtraHop-System konfigurieren.

    Die folgende Abbildung zeigt eine Beispielkonfiguration.




18. Klicken Sie **Weiter** und klicken Sie dann **Fertig**.
    Sie kehren zurück zum Einstellungen für die Anmeldung Seite.
19. In der Einstellungen Abschnitt, klicken Sie **Anweisungen zur Einrichtung anzeigen**.
    Ein neues Browserfenster wird geöffnet und zeigt Informationen an, die für die Konfiguration des ExtraHop-Systems erforderlich sind.

### Weisen Sie das ExtraHop-System Okta-Gruppen zu

Wir gehen davon aus, dass Sie bereits Benutzer und Gruppen in Okta konfiguriert haben. Falls nicht, schlagen Sie in der Okta-Dokumentation nach, um neue Benutzer und Gruppen hinzuzufügen.

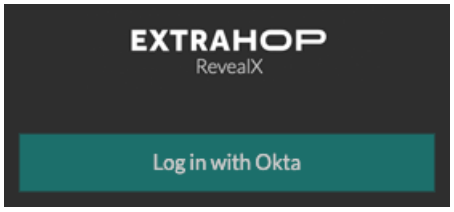
1. Wählen Sie im Menü Verzeichnis **Gruppen**.
2. Klicken Sie auf den Gruppennamen.
3. klicken **Apps verwalten**.
4. Suchen Sie den Namen der Anwendung, die Sie für das ExtraHop-System konfiguriert haben, und klicken Sie auf **Zuweisen**.
5. klicken **Erledigt**.

### Fügen Sie Informationen zum Identitätsanbieter im ExtraHop-System hinzu

1. Kehren Sie zu den Administrationseinstellungen auf dem ExtraHop-System zurück.

   Schließen Sie das Service Provider-Metadatenfenster, falls es noch geöffnet ist, und klicken Sie dann auf **Identitätsanbieter hinzufügen**.
2. In der Name des Anbieters Feld, geben Sie einen eindeutigen Namen ein.

   Dieser Name erscheint auf der Anmeldeseite des ExtraHop-Systems.




3. Kopieren Sie aus Okta das URL für einmaliges Anmelden des Identitätsanbieters und fügen Sie es in das SSO-URL-Feld auf dem ExtraHop-System ein.
4. Kopieren Sie aus Okta das URL des Ausstellers des Identitätsanbieters und füge es in das Entitäts-ID Feld auf dem ExtraHop-System.
5. Kopieren Sie das X.509-Zertifikat von Okta und fügen Sie es in das Öffentliches Zertifikat Feld auf dem ExtraHop-System.
6. Wählen Sie aus einer der folgenden Optionen aus, wie Sie Benutzer bereitstellen möchten.
   - Wählen Sie Benutzer automatisch bereitstellen, um ein neues Remote-SAML-Benutzerkonto auf dem ExtraHop-System zu erstellen, wenn sich der Benutzer zum ersten Mal anmeldet.
   - Deaktivieren Sie das Kontrollkästchen Benutzer automatisch bereitstellen und konfigurieren Sie neue Remote-Benutzer manuell über die ExtraHop-Administrationseinstellungen oder die REST-API. Zugriffs- und Berechtigungsstufen werden durch die Benutzerkonfiguration in Okta bestimmt.
7. Das **Diesen Identitätsanbieter aktivieren** Die Option ist standardmäßig ausgewählt und ermöglicht es Benutzern, sich beim ExtraHop-System anzumelden.

   Um zu verhindern, dass sich Benutzer anmelden, deaktivieren Sie das Kontrollkästchen.
8. Konfigurieren Sie Benutzerberechtigungsattribute.

   Sie müssen die folgenden Benutzerattribute konfigurieren, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Werte sind benutzerdefinierbar; sie müssen jedoch mit den Attributnamen übereinstimmen, die in der SAML-Antwort Ihres Identitätsanbieters enthalten sind. Bei Werten wird nicht zwischen Groß - und Kleinschreibung unterschieden und sie können Leerzeichen enthalten. Weitere Hinweise zu Berechtigungsstufen finden Sie unter Benutzer und Benutzergruppen.

   **Wichtig:** Sie müssen den Attributnamen angeben und mindestens einen anderen Attributwert konfigurieren als **Kein Zugriff** um Benutzern die Anmeldung zu ermöglichen.

In den folgenden Beispielen ist der Name des Attributs Feld ist das Gruppenattribut, das bei der Erstellung der ExtraHop-Anwendung auf dem Identity Provider konfiguriert wurde, und die anderen Attributfelder sind die Namen Ihrer Benutzergruppen. Wenn ein Benutzer Mitglied von mehr als einer Gruppe ist, wird ihm das Zugriffsrecht mit den meisten Berechtigungen gewährt.

| Feldname | Beispiel für einen Attributwert |
|---|---|
| Name des Attributs | `Gruppenmitgliedschaften` |
| System- und Zugriffsverwaltung | `Systemadministratoren` |
| Volle Schreibrechte | `Leitende Analysten` |
| Eingeschränkte Schreibrechte | `Analysten` |
| Persönliche Schreibrechte | `Nachwuchsanalysten` |
| Volle Nur-Lese-Rechte | `Web-Manager` |
| Eingeschränkte Leserechte | `Auftragnehmer` |
| Kein Zugriff | `Praktikanten` |

9. Konfigurieren Sie den NDR-Modulzugriff.

| Feldname | Beispiel für einen Attributwert |
|---|---|
| Name des Attributs | `Gruppenmitgliedschaften` |
| Voller Zugriff | `Sicherheitsoperationen` |
| Kein Zugriff | `Praktikanten` |

10. Konfigurieren Sie den NPM-Modulzugriff.

| Feldname | Beispiel für einen Attributwert |
|---|---|
| Name des Attributs | `Gruppenmitgliedschaften` |
| Voller Zugriff | `Leistungsoperationen` |
| Kein Zugriff | `Praktikanten` |

11. Optional: Konfigurieren Sie den Zugriff auf Pakete und Sitzungsschlüssel.

    Dieser Schritt ist optional und nur erforderlich, wenn Sie einen verbundenen Packetstore und das Packet Forensics Modul haben.

| Feldname | Beispiel für einen Attributwert |
|---|---|
| Name des Attributs | `Gruppenmitgliedschaften` |
| Pakete und Sitzungsschlüssel | `Systemadministratoren` |
| Nur Pakete | `Leitende Analysten` |
| Nur Paketsegmente | `Analysten` |
| Nur Paket-Header | `Nachwuchsanalysten` |
| Kein Zugriff | `Praktikanten` |

12. Klicken Sie **Speichern**.
13. Speichern Sie die laufende Konfigurationsdatei.

**Loggen Sie sich in das ExtraHop-System ein**

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Loggen Sie sich ein mit** <*provider name*>.
3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Anbieter an. Sie werden automatisch zur ExtraHop-Übersichtsseite weitergeleitet.

## SAML-Single-Sign-On mit Google konfigurieren

Sie können Ihr ExtraHop-System so konfigurieren, dass sich Nutzer über den Google-Identitätsverwaltungsdienst beim System anmelden können.

**Bevor Sie beginnen**

- Sie sollten mit der Verwaltung von Google Admin vertraut sein.
- Sie sollten mit der Verwaltung von ExtraHop-Systemen vertraut sein.

Bei diesen Verfahren müssen Sie Informationen zwischen dem ExtraHop-System und der Google Admin-Konsole kopieren und einfügen. Daher ist es hilfreich, jedes System nebeneinander zu öffnen.

**SAML auf dem ExtraHop-System aktivieren**

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 der Fernauthentifizierung** Drop-down-Menü, wählen **SAML**.
4. Klicken Sie **Weiter**.
5. Klicken Sie **SP-Metadaten anzeigen**.
6. Kopieren Sie das ACS-URL und Entitäts-ID in eine Textdatei.
   Sie werden diese Informationen in einem späteren Verfahren in die Google-Konfiguration einfügen.

**Benutzerdefinierte Benutzerattribute hinzufügen**

1. Loggen Sie sich in die Google Admin-Konsole ein.
2. Klicken Sie **Nutzer**.
3. Klicken Sie auf das Symbol Benutzerdefinierte Attribute verwalten  .
4. Klicken Sie **Benutzerdefiniertes Attribut hinzufügen**.
5. In der Kategorie Feld, Typ `ExtraHop`.
6. Optional: In der Beschreibung Feld, geben Sie eine Beschreibung ein.
7. In der Benutzerdefinierte Felder Abschnitt, geben Sie die folgenden Informationen ein:
   a) In der Name Feld, Typ `Level schreiben`.
   b) Aus dem **Art der Information** Drop-down-Menü, wählen **Text**.
   c) Aus dem **Sichtbarkeit** Drop-down-Menü, wählen **Sichtbar für Domain**.
   d) Aus dem **Anzahl der Werte** Drop-down-Menü, wählen **Einzelner Wert**.
8. Aktivieren Sie den Zugriff auf das NDR-Modul:
   a) In der Name Feld, Typ `ndr-Niveau`.
   b) Aus dem **Art der Information** Drop-down-Menü, wählen **Text**.
   c) Aus dem **Sichtbarkeit** Drop-down-Menü, wählen **Sichtbar für Domain**.
   d) Aus dem **Anzahl der Werte** Drop-down-Menü, wählen **Einzelner Wert**.
9. Aktivieren Sie den NPM-Modulzugriff:
   a) In der Name Feld, Typ `npm-Ebene`.
   b) Aus dem **Art der Information** Drop-down-Menü, wählen **Text**.
   c) Aus dem **Sichtbarkeit** Drop-down-Menü, wählen **Sichtbar für Domain**.

d) Aus dem **Anzahl der Werte** Drop-down-Menü, wählen **Einzelner Wert**.

10. Optional: Wenn Sie Paketspeicher verbunden haben, aktivieren Sie den Paketzugriff, indem Sie ein benutzerdefiniertes Feld konfigurieren:
    a) In der Name Feld, Typ `Paketebene`.
    b) Aus dem **Art der Information** Drop-down-Menü, wählen **Text**.
    c) Aus dem **Sichtbarkeit** Drop-down-Menü, wählen **Sichtbar für Domain**.
    d) Aus dem **Anzahl der Werte** Drop-down-Menü, wählen **Einzelner Wert**.
11. Klicken Sie **Hinzufügen**.

**Fügen Sie Identitätsanbieterinformationen von Google zum ExtraHop-System hinzu**

1. Klicken Sie in der Google Admin-Konsole auf das Hauptmenüsymbol und wähle **Apps** > **SAML-Apps**.
2. Klicken Sie auf SSO für eine SAML-Anwendung aktivieren Symbol .
3. Klicken Sie **RICHTE MEINE EIGENE BENUTZERDEFINIERTE APP EIN**.
4. Auf dem Google IdP-Informationen Bildschirm, klicken Sie auf **Herunterladen** Schaltfläche zum Herunterladen des Zertifikats (`GoogleIDPCertificate.pem`).
5. Kehren Sie zu den Administrationseinstellungen auf dem ExtraHop-System zurück.
6. Klicken Sie **Identitätsanbieter hinzufügen**.
7. In der Name des Anbieters Feld, geben Sie einen eindeutigen Namen ein.

   Dieser Name erscheint auf der Anmeldeseite des ExtraHop-Systems.
8. Aus dem Google IdP-Informationen Bildschirm, kopiere die SSO-URL und füge sie in das SSO-URL Feld auf der ExtraHop-Appliance.
9. Aus dem Google IdP-Informationen Bildschirm, kopieren Sie die Entitäts-ID und fügen Sie sie in das Feld Entitäts-ID auf dem ExtraHop-System ein.
10. Öffne das `GoogleIDPCertificate` Kopieren Sie den Inhalt in einem Texteditor und fügen Sie ihn in den Öffentliches Zertifikat Feld auf dem ExtraHop-System.
11. Wählen Sie aus einer der folgenden Optionen aus, wie Sie Benutzer bereitstellen möchten.
    - Wählen **Automatisches Provisioning von Benutzern** um ein neues Remote-SAML-Benutzerkonto auf dem ExtraHop-System zu erstellen, wenn sich der Benutzer zum ersten Mal anmeldet .
    - Löschen Sie das **Automatisches Provisioning von Benutzern** Markieren Sie das Kontrollkästchen und konfigurieren Sie neue Remote-Benutzer manuell über die ExtraHop-Administrationseinstellungen oder die REST-API. Zugriffs- und Berechtigungsstufen werden durch die Benutzerkonfiguration in Google bestimmt.
12. Das **Diesen Identitätsanbieter aktivieren** Die Option ist standardmäßig ausgewählt und ermöglicht es Benutzern, sich beim ExtraHop-System anzumelden. Um zu verhindern, dass sich Benutzer anmelden, deaktivieren Sie das Kontrollkästchen.
13. Konfigurieren Sie Benutzerberechtigungsattribute.

    Sie müssen die folgenden Benutzerattribute konfigurieren, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Werte sind benutzerdefinierbar; sie müssen jedoch mit den Attributnamen übereinstimmen, die in der SAML-Antwort Ihres Identitätsanbieters enthalten sind. Bei Werten wird nicht zwischen Groß - und Kleinschreibung unterschieden und sie können Leerzeichen enthalten. Weitere Hinweise zu Berechtigungsstufen finden Sie unter Benutzer und Benutzergruppen..

    **Wichtig:** Sie müssen den Attributnamen angeben und mindestens einen anderen Attributwert konfigurieren als **Kein Zugriff** um Benutzern die Anmeldung zu ermöglichen.

Im Beispiel unten ist der Name des Attributs Feld ist das Anwendungsattribut und Attributwert ist der Name des Benutzerfeldes, der bei der Erstellung der ExtraHop-Anwendung auf dem Identity Provider konfiguriert wurde.

| Feldname | Beispiel für einen Attributwert |
|---|---|
| Name des Attributs | `urn:extrahop:saml:2.0: Ebene schreiben` |
| System- und Zugriffsverwaltung | `illimitiert` |
| Volle Schreibrechte | `voll_schreiben` |
| Eingeschränkte Schreibrechte | `begrenztes_schreiben` |
| Persönliche Schreibrechte | `persönliches_schreiben` |
| Volle Nur-Lese-Rechte | `voll_schreibgeschützt` |
| Eingeschränkte Nur-Lese-Rechte | `restricted_readonly` |
| Kein Zugriff | `keine` |

14. Konfigurieren Sie den NDR-Modulzugriff.

| Feldname | Beispiel für einen Attributwert |
|---|---|
| Name des Attributs | `urn:extrahop:saml:2.0: ndrlevel` |
| Voller Zugriff | `voll` |
| Kein Zugriff | `keine` |

15. Konfigurieren Sie den NPM-Modulzugriff.

| Name des Feldes | Beispiel für einen Attributwert |
|---|---|
| Name des Attributs | `urn:extrahop:saml:2.0: npmlevel` |
| Voller Zugriff | `voll` |
| Kein Zugriff | `keine` |

16. Optional: Konfigurieren Sie den Zugriff auf Pakete und Sitzungsschlüssel.

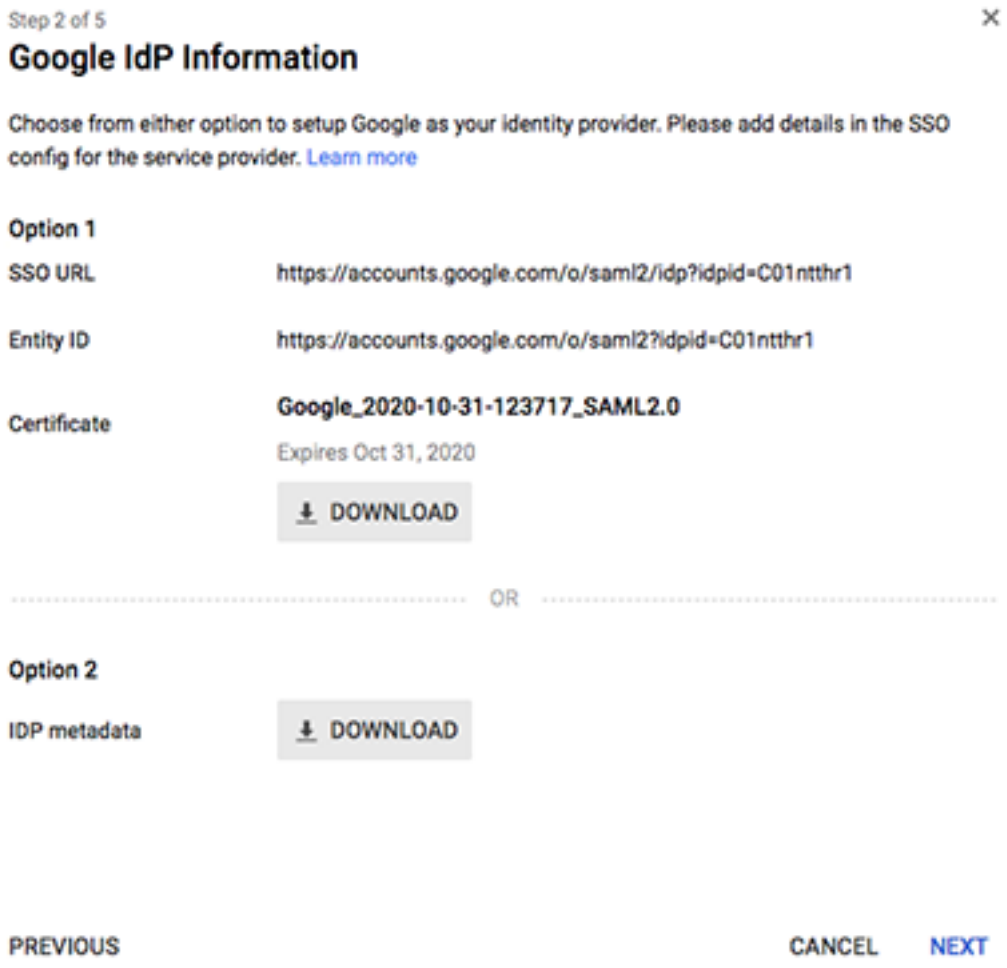
    Die Konfiguration von Paketen und Sitzungsschlüsselattributen ist optional und nur erforderlich , wenn Sie einen verbundenen Packetstore haben.

| Name des Feldes | Beispiel für einen Attributwert |
|---|---|
| Name des Attributs | `urn:extrahop:saml:2.0: Paketebene` |
| Pakete und Sitzungsschlüssel | `voll_mit_Schlüsseln` |
| Nur Pakete | `voll` |
| Pakete nur in Segmenten | `Scheiben` |
| Nur Paket-Header | `Kopfzeilen` |
| Kein Zugriff | `keine` |

17. Klicken Sie **Speichern**.
18. Speichern Sie die laufende Konfiguration.

**Fügen Sie Informationen zum ExtraHop-Dienstanbieter zu Google hinzu**

1. Kehren Sie zur Google Admin-Konsole zurück und klicken Sie auf **Weiter** auf dem Google Idp-Informationen Seite, um mit Schritt 3 von 5 fortzufahren.




2. In der Name der Anwendung Feld, geben Sie einen eindeutigen Namen ein, um das ExtraHop-System zu identifizieren.

   Jedes ExtraHop-System, für das Sie eine SAML-Anwendung erstellen, benötigt einen eindeutigen Namen.
3. Optional: Geben Sie eine Beschreibung für diese Anwendung ein oder laden Sie ein benutzerdefiniertes Logo hoch.
4. Klicken Sie **Weiter**.
5. Kopieren Sie das URL des Assertion Consumer Service (ACS) aus dem ExtraHop-System und füge es ein in das ACS-URL Feld in Google Admin.

   **Hinweis:** Möglicherweise müssen Sie die ACS-URL manuell bearbeiten, wenn die URL einen nicht erreichbaren Hostnamen enthält, z. B. den Standardsystemhostnamen `extrahop`. Wir empfehlen Ihnen, den vollqualifizierten Domänenname für das ExtraHop-System in der URL anzugeben.
6. Kopieren Sie das SP-Entitäts-ID aus dem ExtraHop-System und füge es ein in das Entitäts-ID Feld in Google Admin.
7. Wählen Sie die **Signierte Antwort** Ankreuzfeld.

8. In der Name ID Abschnitt, belassen Sie die Standardeinstellung **Grundlegende Informationen** und **Primäre E-Mail** Einstellungen unverändert.
9. Aus dem **Namens-ID-Format** Drop-down-Menü, wählen **HARTNÄCKIG**.
10. Klicken Sie **Weiter**.
11. Auf dem Zuordnung von Attributen Bildschirm, klicken **NEUES MAPPING HINZUFÜGEN**.
12. Fügen Sie die folgenden Attribute genau wie gezeigt hinzu.

    Die ersten vier Attribute sind erforderlich. Das `packetslevel` Das Attribut ist optional und nur erforderlich, wenn Sie einen verbundenen Packetstore haben. Wenn Sie einen Packetstore haben und den nicht konfigurieren `packetslevel` Attribut, Benutzer können Paketerfassungen im ExtraHop-System nicht anzeigen oder herunterladen.

| Anwendungsattribut | Kategorie | Benutzerfeld |
|---|---|---|
| `urn:oid:0.9.2342.19200300.100.1.3` | Grundlegende Informationen | Primäre E-Mail |
| `urn:oid:2.5.4.4` | Grundlegende Informationen | Nachname |
| `urn:oid:2.5.4.42` | Grundlegende Informationen | Vorname |
| `urn:extrahop:saml:2.0:Ebene schreiben` | ExtraHop | Level schreiben |
| `urn:extrahop:saml:2.0:ndrlevel` | ExtraHop | ndr-Niveau |
| `urn:extrahop:saml:2.0:npmlevel` | ExtraHop | npm-Ebene |
| `urn:extrahop:saml:2.0:Paketebene` | ExtraHop | Paketebene |

13. Klicken Sie **Fertig** und klicken Sie dann **OK**.
14. Klicken Sie **Dienst bearbeiten**.
15. Wählen **An für alle**.
16. Klicken Sie **Speichern**.

### Benutzerrechte zuweisen

1. Klicken Sie **Nutzer** um zur Tabelle aller Benutzer in Ihren Organisationseinheiten zurückzukehren.
2. Klicken Sie auf den Namen des Benutzers, dem Sie die Anmeldung am ExtraHop-System ermöglichen möchten.
3. In der Informationen zum Nutzer Abschnitt, klicken **Angaben zum Nutzer**.
4. In der ExtraHop Abschnitt, klicken **Level schreiben** und geben Sie eine der folgenden Berechtigungsstufen ein.

   - `illimitiert`
   - `voll_schreiben`
   - `begrenztes_schreiben`
   - `persönliches_schreiben`
   - `voll_schreibgeschützt`
   - `restricted_readonly`
   - `keine`

   Hinweise zu Benutzerrechten finden Sie unter Benutzer und Benutzergruppen.
5. Optional: Wenn du das hinzugefügt hast `packetslevel` Attribut oben, klicken **Paketebene** und geben Sie eines der folgenden Rechte ein.

- `voll`
- `voll_mit_schreiben`
- `keine`


6. Optional: Wenn du das hinzugefügt hast `detectionslevel` Attribut oben, klicken **Erkennungsstufe** und geben Sie eines der folgenden Rechte ein.
   - `voll`
   - `keine`
7. Klicken Sie **Speichern**.

**Loggen Sie sich in das ExtraHop-System ein**

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Loggen Sie sich ein mit** *<provider name>*.
3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Anbieter an. Sie werden automatisch zur ExtraHop-Übersichtsseite weitergeleitet.

## Konfigurieren Sie die Fernauthentifizierung über RADIUS

Das ExtraHop-System unterstützt den Remote Authentifizierung Dial In User Service (RADIUS) nur für Fernauthentifizierung und 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 der Fernauthentifizierung Drop-down-Menü, wählen **RADIUS** und klicken Sie dann **Fortfahren**.
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 das 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 das gemeinsame Geheimnis zu erhalten.

   Auszeit

   Die Zeit in Sekunden, die das ExtraHop-System auf eine Antwort vom RADIUS-Server wartet, bevor es erneut versucht, eine Verbindung herzustellen .

5. klicken **Server hinzufügen**.
6. Optional: Fügen Sie nach Bedarf weitere Server hinzu.
7. Klicken Sie **Speichern und fertig**.
8. Aus dem Optionen für die Zuweisung von Rechten Wählen Sie im Drop-down-Menü eine der folgenden Optionen aus:

   - **Remote-Benutzer haben vollen Schreibzugriff**

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

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

   - **Kein Zugriff**
   - **Nur Paketsegmente**
   - **Nur Paket-Header**
   - **Nur Pakete**
   - **Pakete und Sitzungsschlüssel**
10. Optional: Konfigurieren Sie den NDR- und NPM-Modulzugriff (nur auf Sensoren und Konsolen).

    - **Kein Zugriff**
    - **Voller Zugriff**
11. Klicken Sie **Speichern und fertig**.
12. Klicken Sie **Erledigt**.

## Konfigurieren Sie die Fernauthentifizierung über TACACS+

Das ExtraHop-System unterstützt das 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 ExtraHop-Dienst, der auf dem TACACS+-Server konfiguriert ist bevor Sie mit diesem Verfahren beginnen.

**Wichtig:** Bei Recordstores und Packetstores gewährt die Aktivierung des Fernzugriffs allen Benutzern im TACACS+-Authentifizierungssystem Administratorrechte, unabhängig von den Rechten, die das Authentifizierungssystem für jeden Benutzer festlegt.

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 der Fernauthentifizierung Drop-down-Menü, wählen **TACACS+**, und klicken Sie dann auf **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 das 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 das gemeinsame Geheimnis 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 Sie **Server hinzufügen**.
6. Optional: Fügen Sie nach Bedarf weitere Server hinzu.
7. Klicken Sie **Speichern und fertig**.
8. Für Recordstores und Packetstores klicken Sie auf **Erledigt** und dann springe zu Konfiguration des TACACS+-Servers . Führen Sie für Sensoren und Konsolen die verbleibenden Schritte unten aus.
9. Aus dem Optionen für die Zuweisung von Berechtigungen Wählen Sie im Drop-down-Menü eine der folgenden Optionen aus:

   - **Berechtigungsstufe vom Remoteserver abrufen**

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

   - **Remote-Benutzer haben vollen Schreibzugriff**

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

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

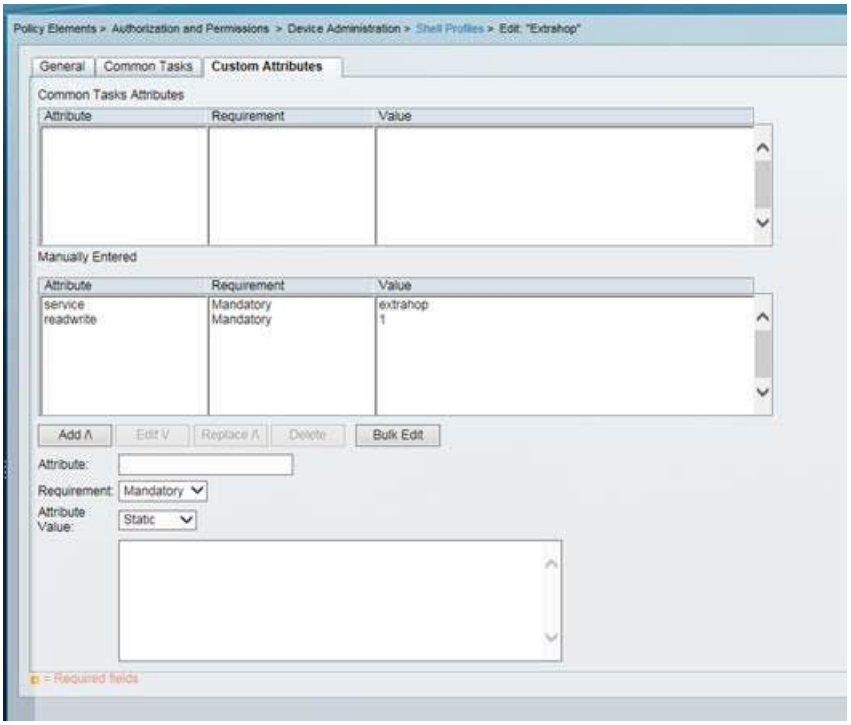
    - **Kein Zugriff**
    - **Nur Paketsegmente**
    - **Nur Paket-Header**
    - **Nur Pakete**
    - **Pakete und Sitzungsschlüssel**
11. Optional: Konfigurieren Sie den NDR- und NPM-Modulzugriff (nur auf Sensoren und Konsolen).

    - **Kein Zugriff**
    - **Voller Zugriff**
12. Klicken Sie **Speichern und fertig**.
13. Klicken Sie **Erledigt**.

**Konfigurieren Sie den TACACS+-Server**
Zusätzlich zur Konfiguration der Fernauthentifizierung auf Ihrem ExtraHop-System müssen Sie Ihren TACACS+-Server mit zwei Attributen konfigurieren, eines für den ExtraHop-Dienst und eines für die Berechtigungsstufe. Wenn Sie einen ExtraHop-Paketstore 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. Für den ersten Wert addieren `zusätzlicher Hopfen`.
4. Fügen Sie für das zweite Attribut die Berechtigungsstufe hinzu, z. B. `lesen/schreiben`.
5. Für den zweiten Wert addieren `1`.

Die folgende Abbildung zeigt zum Beispiel `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` | Erstellen und ändern Sie alle Objekte und Einstellungen auf dem ExtraHop-System, ohne die Administrationseinstellungen |
| `limited` | `1` | Dashboards erstellen, ändern und teilen |
| `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 ausblenden |
| `npmfull` | `1` | Leistungserkennungen anzeigen, bestätigen und ausblenden |

| Attribut | Wert | Beschreibung |
|---|---|---|
| packetsfull | 1 | Pakete anzeigen und herunterladen, die in einem verbundenen Packetstore gespeichert sind. |
| packetslicesonly | 1 | Paketsegmente in einem verbundenen Packetstore anzeigen und herunterladen. |
| packetheadersonly | 1 | Sucht und lädt nur Paket-Header in einem verbundenen Packetstore herunter. |
| packetsfullwithkeys | 1 | Pakete und zugehörige Sitzungsschlüssel anzeigen und herunterladen, die in einem verbundenen Packetstore gespeichert sind. |

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

| Attribut | Wert |
|---|---|
| ndrvoll | 1 |

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

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

8. Optional: Wenn Sie einen ExtraHop-Paketstore haben, fügen Sie ein Attribut hinzu, damit Benutzer Paketerfassungen oder Paketerfassungen mit zugehörigen Sitzungsschlüsseln herunterladen können.

| Attribut | Wert | Beschreibung |
|---|---|---|
| Pakete nur Scheiben | 1 | Benutzer mit jeder Berechtigungsstufe können die ersten 64 Byte an Paketen anzeigen und herunterladen. |
| Nur Paketheader | 1 | Benutzer mit jeder Berechtigungsstufe können Paket-Header in einem verbundenen Packetstore suchen und herunterladen. |
| Pakete voll | 1 | Benutzer mit jeder Berechtigungsstufe können Pakete, die in einem verbundenen Packetstore gespeichert sind, anzeigen und herunterladen. |

| Attribut | Wert | Beschreibung |
|---|---|---|
| `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. 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 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.

4. 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 Auf Einstellungen zugreifen Abschnitt, klicken Sie **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 API-Schlüssel Abschnitt 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. |

| Privilegienstufe | Zulässige Aktionen |
| --- | --- |
| | • 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>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“ |
| „ndr“: „keiner“ | • Kein Zugriff auf NDR-Modulinhalte |

| Privilegienstufe | Zulässige Aktionen |
| --- | --- |
| | 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“<br>• „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. |

| Privilegienstufe | Zulässige Aktionen |
| --- | --- |
| | Dies ist eine Zusatzberechtigung, die einem Benutzer mit einer der folgenden Berechtigungsstufen gewährt werden kann:<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>Dies ist eine Zusatzberechtigung, die einem Benutzer mit einer der folgenden Berechtigungsstufen gewährt werden kann:<br>• „write“: „voll“<br>• „write“: „begrenzt“<br>• „write“: „persönlich“<br>• „schreiben“: null<br>• „Metriken“: „voll“<br>• „metrics“: „eingeschränkt“ |

# Konfiguration des Systems

In der Konfiguration des Systems In diesem Abschnitt können Sie die folgenden Einstellungen ändern.

**Benennung von Geräten**

Konfigurieren Sie die Rangfolge, wenn mehrere Namen für ein Gerät gefunden werden.

**Inaktive Quellen**

Entfernen Sie Geräte und Anwendungen, die zwischen 1 und 90 Tagen inaktiv waren, aus den Suchergebnissen.

**Erkennungsverfolgung**

Wählen Sie aus, ob die Erkennungsuntersuchungen mit dem ExtraHop-System oder von einem externen Ticketsystem aus verfolgt werden sollen.

**Endpunktsuche**

Konfigurieren Sie Links zu einem externen IP-Adress-Suchtool für Endpunkte im ExtraHop-System.

**Geomap-Datenquelle**

Ändern Sie die Informationen in kartierten Geolokationen.

**Sichern und Wiederherstellen**

System-Backups erstellen, anzeigen oder wiederherstellen.

## Vorrang des Gerätenamens

Entdeckte Geräte werden automatisch anhand mehrerer Netzwerkdatenquellen wie Protokollen, MAC- oder IP-Adressen oder Geräterollen benannt. Wenn mehrere Namen für ein Gerät gefunden werden, gibt die Reihenfolge der Rangfolge der Gerätenamen an, welcher Name standardmäßig im ExtraHop-System angezeigt wird.

Das ExtraHop-System verwendet standardmäßig die folgende Rangfolge:

- Benutzerdefinierter Name
- Name der Cloud-Instanz
- CDP-Name
- DHCP-Name
- DNS-Name
- NetBIOS-Name
- Standardname

**Bevor Sie beginnen**

- Die Einstellungen für die Rangfolge von Gerätenamen gelten nur für die Konsole oder den Sensor, auf dem die Einstellungen konfiguriert sind.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Die gesamte Verwaltung**.
3. In der Konfiguration des Systems Abschnitt, klicken Sie **Rangfolge des Gerätenamens**.
4. Klicken und ziehen Sie die Gerätenamen, um eine neue Rangfolge zu erstellen.
5. Klicken Sie **Speichern**.
6. Optional: klicken **Zur Standardeinstellung zurückkehren** um Ihre Änderungen rückgängig zu machen.

## Inaktive Quellen konfigurieren

Geräte, die in den letzten 30 Minuten keine Daten gesendet oder empfangen haben, gelten als inaktiv und generieren keine Messwerte mehr. Inaktive Geräte können jedoch weiterhin in Funktionsbereichen wie Suchergebnissen, Aktivitätskarten, Dashboards und Erkennungen angezeigt werden.

Mit den folgenden Einstellungen können Sie inaktive Quellen sofort aus den Suchergebnissen entfernen und angeben, wann das System inaktive Geräte automatisch aus dem ExtraHop-System löschen kann.

Im Folgenden finden Sie einige Überlegungen zur Konfiguration inaktiver Quelleinstellungen:

- Sie müssen über System- und Zugriffsadministration verfügen Benutzerrechte.
- Einstellungen zum Löschen inaktiver Geräte müssen auf einem Sensor konfiguriert werden. Geräte, die vom Sensor gelöscht wurden, werden auch von der verbundenen Konsole gelöscht.
- Das ExtraHop-System sucht täglich nach inaktiven Geräten und löscht bei jeder Überprüfung bis zu 5.000 Geräte. Geräte, die am längsten inaktiv sind, werden zuerst gelöscht.
- Das Löschen von Geräten wirkt sich auf die Anzahl Ihrer Gerätekapazität aus.
- Gelöschte Geräte, die Funktionen wie Aktivitätskarten, Dashboards und Erkennungen zugeordnet sind, werden als unbekanntes Gerät angezeigt.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Systemkonfiguration auf **Inaktive Quellen**
3. Entfernen Sie im Abschnitt Suchergebnisse inaktive Quellen aus den Suchergebnissen, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die Anzahl der Tage (1 bis 90) an, an denen Geräte inaktiv waren.
   b) klicken **Jetzt entfernen**.
4. Konfigurieren Sie im Abschnitt ExtraHop-System, wann inaktive Geräte aus dem ExtraHop-System gelöscht werden sollen:
   a) Um Geräte zu löschen, die für eine bestimmte Anzahl von Tagen inaktiv waren, aktivieren Sie das entsprechende Kontrollkästchen und geben Sie dann einen Wert zwischen 10 und 1.000 an.
   b) Um inaktive Geräte zu löschen, nachdem eine bestimmte Anzahl von Geräten erkannt wurde, aktivieren Sie das entsprechende Kontrollkästchen und geben Sie dann einen Wert zwischen 50.000 und 10.000.000 an.
5. klicken **Speichern**.

## Erkennungsverfolgung aktivieren

Mit der Erkennungsverfolgung können Sie einem Benutzer eine Erkennung zuweisen, den Status festlegen und Notizen hinzufügen. Sie können Erkennungen direkt im ExtraHop-System, mit einem externen Ticketsystem eines Drittanbieters oder mit beiden Methoden verfolgen.

**Hinweis** Sie müssen die Ticketverfolgung auf allen angeschlossenen Sensoren aktivieren.

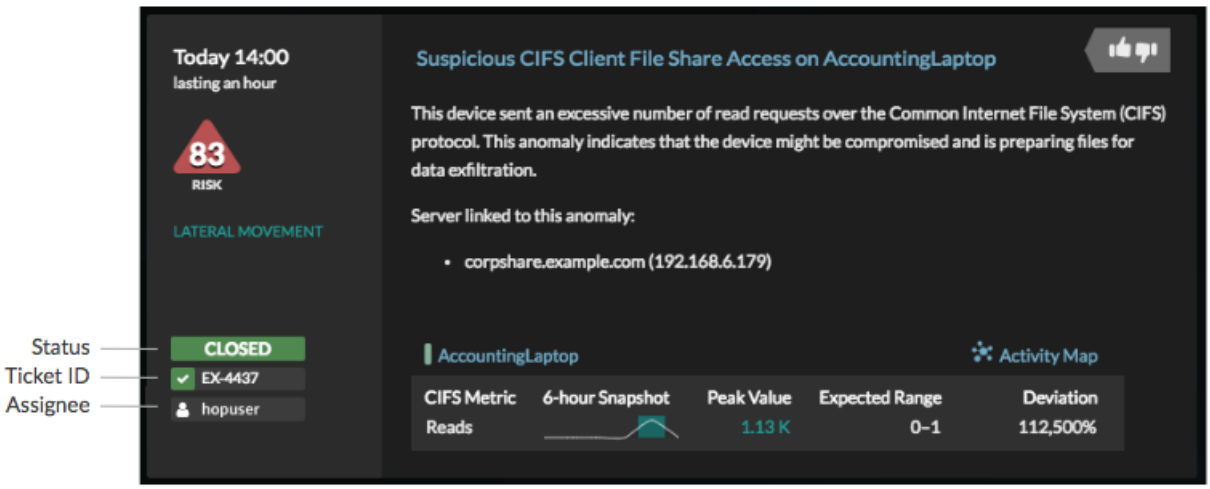
**Bevor Sie beginnen**

- Sie müssen Zugriff auf ein ExtraHop-System mit einem Benutzerkonto haben, das Administratorrechte.
- Nachdem Sie die externe Ticketverfolgung aktiviert haben, müssen Sie Ticket-Tracking von Drittanbietern konfigurieren indem Sie einen Auslöser schreiben, um Tickets in Ihrem Ticketsystem zu erstellen und zu aktualisieren, und dann Ticketaktualisierungen auf Ihrem ExtraHop-System über die REST-API aktivieren.
- Wenn Sie das externe Ticket-Tracking deaktivieren, werden zuvor gespeicherte Status- und Empfänger-Ticketinformationen in das ExtraHop-Erkennungs-Tracking umgewandelt. Wenn das Erkennungs-Tracking innerhalb des ExtraHop-Systems aktiviert ist, können Sie Tickets einsehen, die

bereits existierten, als Sie das externe Ticket-Tracking deaktiviert haben, aber Änderungen an diesem externen Ticket werden nicht im ExtraHop-System angezeigt.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erkennungsverfolgung**.
3. Wählen Sie eine oder beide der folgenden Methoden für die Nachverfolgung von Erkennungen aus:
   - Wählen **Ermöglichen Sie ExtraHop-Benutzern, Erkennungen aus dem ExtraHop-System heraus zu verfolgen**.
   - Wählen **Ermöglichen Sie externe Integrationen wie SOAR oder Ticket-Tracking-Systeme, um Erkennungen über die ExtraHop Rest API zu verfolgen** .
4. Optional: Nachdem Sie die Option zum Aktivieren externer Integrationen ausgewählt haben, geben Sie die URL-Vorlage für Ihr Ticketsystem an und fügen Sie die *$ Ticket_ID* variabel an der entsprechenden Stelle. Geben Sie beispielsweise eine vollständige URL ein, z. B. `https://jira.example.com/browse/$ticket_id`. Das *$ Ticket_ID* Die Variable wird durch die Ticket-ID ersetzt, die der Erkennung zugeordnet ist.

   Nachdem die URL-Vorlage konfiguriert ist, können Sie in einer Erkennung auf die Ticket-ID klicken, um das Ticket in einem neuen Browser-Tab zu öffnen.




**Nächste Schritte**

Wenn Sie externe Ticket-Tracking-Integrationen aktiviert haben, müssen Sie mit der folgenden Aufgabe fortfahren:

- Ticket-Tracking von Drittanbietern für Erkennungen konfigurieren

## Ticket-Tracking von Drittanbietern für Erkennungen konfigurieren

Mit der Ticketverfolgung können Sie Tickets, Alarme oder Fälle in Ihrem Work-Tracking-System mit ExtraHop-Erkennungen verknüpfen. Jedes Ticketsystem von Drittanbietern, das Open Data Stream (ODS) - Anfragen annehmen kann, wie Jira oder Salesforce, kann mit ExtraHop-Erkennungen verknüpft werden.

**Bevor Sie beginnen**

- Das musst du haben hat in den Verwaltungseinstellungen die Option zum Nachverfolgen der Erkennung durch Dritte ausgewählt.
- Sie müssen Zugriff auf ein ExtraHop-System mit einem Benutzerkonto haben, das System- und Zugriffsadministrationsrechte.
- Sie müssen mit dem Schreiben von ExtraHop-Triggern vertraut sein. siehe Trigger und die Verfahren in Einen Auslöser erstellen.

- Sie müssen ein ODS-Ziel für Ihren Ticket-Tracking-Server erstellen. Weitere Informationen zur Konfiguration von ODS-Zielen finden Sie in den folgenden Themen : HTTP, Kafka, MongoDB, Syslog, oder Rohdaten.
- Sie müssen mit dem Schreiben von REST-API-Skripten vertraut sein und über einen gültigen API-Schlüssel verfügen, um die folgenden Verfahren ausführen zu können. siehe Generieren Sie einen API-Schlüssel.

**Schreiben Sie einen Auslöser, um Tickets zu Erkennungen in Ihrem Ticketsystem zu erstellen und zu aktualisieren**
Dieses Beispiel zeigt Ihnen, wie Sie einen Auslöser erstellen, der die folgenden Aktionen ausführt:

- Erstellen Sie jedes Mal, wenn eine neue Erkennung im ExtraHop-System erscheint, ein neues Ticket im Ticketsystem.
- Weisen Sie einem Benutzer mit dem Namen neue Tickets zu `escalations_team` im Ticketsystem.
- Wird jedes Mal ausgeführt, wenn eine Erkennung auf dem ExtraHop-System aktualisiert wird.
- Senden Sie Erkennungsaktualisierungen über einen HTTP Open Data Stream (ODS) an das Ticketsystem.

Das vollständige Beispielskript ist am Ende dieses Themas verfügbar.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Auslöser**.
3. klicken **Neu**.
4. Geben Sie einen Namen und eine optionale Beschreibung für den Auslöser an.
5. Wählen Sie in der Liste Ereignisse **ERKENNUNGSUPDATE**.

   Das Ereignis DETECTION_UPDATE wird jedes Mal ausgeführt, wenn eine Erkennung im ExtraHop-System erstellt oder aktualisiert wird.
6. Geben Sie im rechten Bereich Folgendes an Erkennungsklasse Parameter in einem JavaScript-Objekt. Diese Parameter bestimmen die Informationen, die an Ihr Ticketsystem gesendet werden.

   Der folgende Beispielcode fügt die Erkennungs-ID, die Beschreibung, den Titel, die Kategorien, die MITRE-Techniken und -Taktiken sowie die Risikoscore zu einem JavaScript-Objekt mit dem Namen hinzu `payload`:

```
const summary = "ExtraHop Detection: " + Detection.id + ": " +
 Detection.title;
const description = "ExtraHop has detected the following event on your
 network: " + Detection.description
const payload = {
    "fields": {
        "summary": summary,
        "assignee": {
            "name": "escalations_team"
        },
        "reporter": {
            "name": "ExtraHop"
        },
        "priority": {
            "id": Detection.riskScore
        },
        "labels": Detection.categories,
        "mitreCategories": Detection.mitreCategories,
        "description": description
    }
};
```

7. Definieren Sie als Nächstes die HTTP-Anforderungsparameter in einem JavaScript-Objekt unter dem vorherigen JavaScript-Objekt.

Der folgende Beispielcode definiert eine HTTP-Anfrage für die im vorherigen Beispiel beschriebene Nutzlast: definiert eine Anfrage mit einer JSON-Payload:

```
const req = {
    'path': '/rest/api/issue',
    'headers': {
        'Content-Type': 'application/json'
    },
    'payload': JSON.stringify(payload)
};
```

Weitere Hinweise zu ODS-Anforderungsobjekten finden Sie unter Offene Datenstromklassen.

8. Geben Sie abschließend die HTTP-POST-Anfrage an, die die Informationen an das ODS-Ziel sendet. Der folgende Beispielcode sendet die im vorherigen Beispiel beschriebene HTTP-Anfrage an ein ODS-Ziel namens Ticket-Server:

```
Remote.HTTP('ticket-server').post(req);
```

Der vollständige Triggercode sollte dem folgenden Beispiel ähneln:

```
const summary = "ExtraHop Detection: " + Detection.id + ": " +
 Detection.title;
const description = "ExtraHop has detected the following event on your
 network: " + Detection.description
const payload = {
    "fields": {
        "summary": summary,
        "assignee": {
            "name": "escalations_team"
        },
        "reporter": {
            "name": "ExtraHop"
        },
        "priority": {
            "id": Detection.riskScore
        },
        "labels": Detection.categories,
        "mitreCategories": Detection.mitreCategories,
        "description": description
    }
};

const req = {
    'path': '/rest/api/issue',
    'headers': {
        'Content-Type': 'application/json'
    },
    'payload': JSON.stringify(payload)
};

Remote.HTTP('ticket-server').post(req);
```

**Ticketinformationen über die REST-API an Erkennungen senden**

Nachdem Sie einen Auslöser konfiguriert haben, um Tickets für Erkennungen in Ihrem Ticket-Tracking-System zu erstellen, können Sie die Ticketinformationen in Ihrem ExtraHop-System über die REST-API aktualisieren.

Ticketinformationen werden bei Erkennungen auf der Seite „Entdeckungen“ im ExtraHop-System angezeigt. Weitere Informationen finden Sie in der Erkennungen Thema.

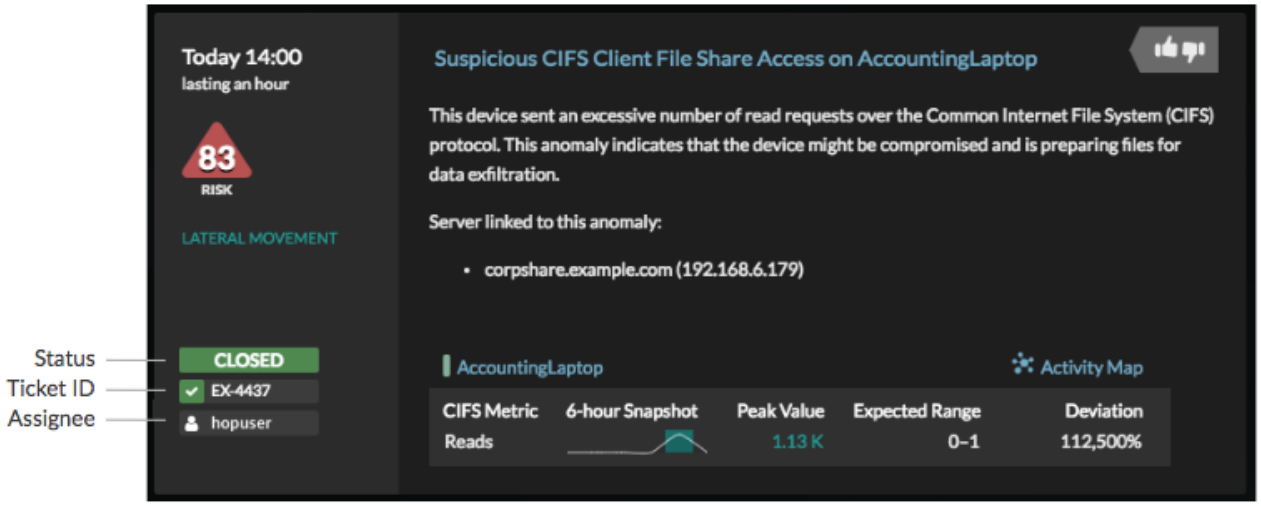
Das folgende Python-Beispielskript entnimmt Ticketinformationen aus einem Python-Array und aktualisiert die zugehörigen Erkennungen auf dem ExtraHop-System.

```
#!/usr/bin/python3

import json
import requests
import csv

API_KEY = '123456789abcdefghijklmnop'
HOST = 'https://extrahop.example.com/'

# Method that updates detections on an ExtraHop system
def updateDetection(detection):
    url = HOST + 'api/v1/detections/' + detection['detection_id']
    del detection['detection_id']
    data = json.dumps(detection)
    headers = {'Content-Type': 'application/json',
               'Accept': 'application/json',
               'Authorization': 'ExtraHop apikey=%s' % API_KEY}
    r = requests.patch(url, data=data, headers=headers)
    print(r.status_code)
    print(r.text)

# Array of detection information
detections = [
                {
                    "detection_id": "1",
                    "ticket_id": "TK-16982",
                    "status": "new",
                    "assignee": "sally",
                    "resolution": None,
                },
                {
                    "detection_id": "2",
                    "ticket_id": "TK-2078",
                    "status": None,
                    "assignee": "jim",
                    "resolution": None,
                },
                {
                    "detection_id": "3",
                    "ticket_id": "TK-3452",
                    "status": None,
                    "assignee": "alex",
                    "resolution": None,
                }
            ]

for detection in detections:
    updateDetection(detection)
```

**Hinweis:** Wenn das Skript eine Fehlermeldung zurückgibt, dass die TLS-Zertifikatsüberprüfung fehlgeschlagen ist, stellen Sie sicher, dass Ihrem Sensor oder Ihrer Konsole wurde ein vertrauenswürdiges Zertifikat hinzugefügt. Alternativ können Sie das hinzufügen `verify=False` Option zur Umgehung der Zertifikatsüberprüfung. Diese Methode ist jedoch nicht sicher und wird nicht empfohlen. Der folgende Code sendet eine HTTP GET-Anfrage ohne Zertifikatsüberprüfung:

```
requests.get(url, headers=headers, verify=False)
```

Nachdem die Ticketverfolgung konfiguriert wurde, werden Ticketdetails im linken Bereich der Erkennungsdetails angezeigt, ähnlich der folgenden Abbildung:




**Status**

Der Status des Tickets, das mit der Erkennung verknüpft ist. Das Ticket-Tracking unterstützt die folgenden Status:

- Neu
- Im Gange
- geschlossen
- Mit ergriffenen Maßnahmen geschlossen
- Geschlossen, ohne dass Maßnahmen ergriffen wurden

**Ticket-ID**

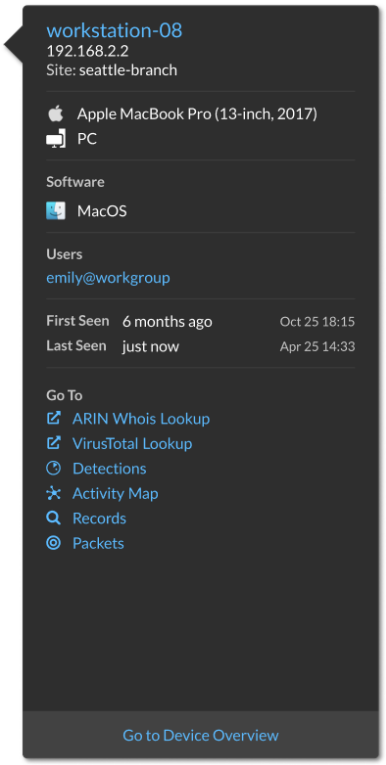
Die ID des Tickets in Ihrem Work-Tracking-System, das mit der Erkennung verknüpft ist. Wenn Sie eine Vorlagen-URL konfiguriert haben, können Sie auf die Ticket-ID klicken, um das Ticket in Ihrem Work-Tracking-System zu öffnen.

**Abtretungsempfänger**

Der Benutzername, der dem Ticket zugewiesen wurde, das mit der Erkennung verknüpft ist. Graue Benutzernamen weisen auf ein Konto hin, das kein ExtraHop-Konto ist.

## Lookup-Links konfigurieren

Sie können eine Liste externer Tools konfigurieren, die zum Abrufen von Informationen über IP-Adressen und SHA-256-Datei-Hashes innerhalb des ExtraHop-Systems verfügbar sind. Links zum Suchtool werden normalerweise angezeigt, wenn Sie auf den Seiten „Geräte“, „Dateien“, „Aufzeichnungen“ oder „Erkennungen“ auf eine IP-Adresse oder einen Datei-Hash klicken oder den Mauszeiger darüber bewegen. Klicken Sie auf den Link, um das Suchtool zu starten, das nach der zugehörigen IP-Adresse oder dem Datei-Hash sucht.




Im Folgenden finden Sie einige Überlegungen zur Konfiguration von Lookup-Links:

- Sie benötigen System- und Zugriffsadministration oder Systemadministration (nur RevealX 360) Benutzerrechte.
- Sie können bis zu 15 Suchlinks jedes Typs konfigurieren.
- Die folgenden Suchlinks sind standardmäßig konfiguriert und können geändert oder gelöscht werden:
  - ARIN Whois-Suche (nur IP-Adressen)
  - VirusTotal-Suche

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Konfigurieren Sie einen Link zum Nachschlagen einer IP-Adresse, indem Sie auf den **IP Adresse** klicken Sie auf die Registerkarte und führen Sie die folgenden Schritte aus:
   a) klicken **Such-Link hinzufügen**.
   b) In der **URL-Vorlage** Feld, geben Sie die URL des Suchwerkzeugs ein.

      Die URL muss Folgendes enthalten `$ip` Variable, die bei der Suche durch die IP-Adresse des Endpunkt ersetzt wird. Zum Beispiel `https://search.arin.net/rdap/?query=$ip`
   c) In der **Name anzeigen** Feld, geben Sie den Namen des Links so ein, wie er angezeigt werden soll.
   d) Wählen Sie eine der folgenden Optionen Optionen anzeigen:

   - Diesen Link auf allen Endpunkten anzeigen
   - Diesen Link auf externen Endpunkten anzeigen
   - Diesen Link auf internen Endpunkten anzeigen
   - Diesen Link nicht anzeigen
3. klicken **Speichern**.
4. Konfigurieren Sie einen Datei-Hash-Suchlink, indem Sie auf den **Datei-Hash** klicken Sie auf die Registerkarte und führen Sie die folgenden Schritte aus:
   a) klicken **Such-Link hinzufügen**.
   b) In der **URL-Vorlage** Feld, geben Sie die URL des Suchwerkzeugs ein.

Die URL muss Folgendes enthalten `$filehash` Variable, die bei der Suche durch den SHA-256-Hash der Datei ersetzt wird. Zum Beispiel: `https://www.virustotal.com/gui/search/$filehash`

c) In der **Name anzeigen** Feld, geben Sie den Namen des Links so ein, wie er angezeigt werden soll.

d) Wählen Sie eine der folgenden Optionen Optionen anzeigen:

- Diesen Link auf allen Dateien anzeigen
- Diesen Link nicht anzeigen

5. klicken **Speichern**.

## Geomap-Datenquelle

Im Produkt zugeordnete geografische Standorte und Trigger verweisen auf eine GeoIP-Datenbank, um den ungefähren Standort einer IP-Adresse zu ermitteln.

### Ändern Sie die GeoIP-Datenbank

Sie können Ihre eigene GeoIP-Datenbank in das ExtraHop-System hochladen, um sicherzustellen, dass Sie über die neueste Version der Datenbank verfügen oder ob Ihre Datenbank interne IP-Adressen enthält, deren Standort nur Sie oder Ihr Unternehmen kennen.

Sie können eine Datenbankdatei im MaxMind-DB-Format (.mmdb) hochladen, die Details auf Stadt- und Länderebene enthält .

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken Sie **Geomap-Datenquelle**.
3. Klicken Sie **GeoIP-Datenbank**.
4. In der Datenbank auf Stadtebene Abschnitt, auswählen **Neue Datenbank hochladen**.
5. Klicken Sie **Wählen Sie Datei** und navigieren Sie zur neuen Datenbankdatei auf Stadtebene auf Ihrem Computer.
6. Klicken Sie **Speichern**.

### Einen IP-Standort überschreiben

Sie können fehlende oder falsche IP-Adressen in der GeoIP-Datenbank überschreiben. Sie können eine durch Kommas getrennte Liste oder eine Liste mit Tabulatoren von Überschreibungen in das Textfeld eingeben.

Jede Überschreibung muss einen Eintrag in den folgenden sieben Spalten enthalten:

- IP-Adresse (eine einzelne IP-Adresse oder CIDR-Notation)
- Breitengrad
- Längengrad
- Stadt
- Bundesland oder Region
- Name des Landes
- ISO-Alpha-2-Ländercode

Sie können Elemente nach Bedarf bearbeiten und löschen, müssen jedoch sicherstellen, dass für jede der sieben Spalten Daten vorhanden sind. Weitere Informationen zu ISO-Ländercodes finden Sie unter https://www.iso.org/obp/ui/#search und klicken Sie **Ländercodes**.

1. Unter Konfiguration des Systems, klicken **Geomap-Datenquelle** .
2. klicken **IP-Standort überschreiben**.

3. Geben Sie in das Textfeld eine tabulatorgetrennte oder kommagetrennte Liste von Überschreibungen im folgenden Format ein oder fügen Sie sie ein:

```
IP address, latitude, longitude, city, state or region, country name, ISO
alpha-2 country code
```

Zum Beispiel:

```
10.10.113.0/24, 38.907231, -77.036464, Washington, DC, United States, US
10.10.225.25, 47.6204, -122.3491, Seattle, WA, United States, US
```

4. Klicken Sie **Speichern**.

## Einen Sensor oder eine Konsole sichern und wiederherstellen

Nachdem Sie Ihren ExtraHop konfiguriert haben Konsole und Sensor Bei Anpassungen wie Bundles, Triggern und Dashboards oder administrativen Änderungen wie dem Hinzufügen neuer Benutzer empfiehlt ExtraHop, dass Sie Ihre Einstellungen regelmäßig sichern, um die Wiederherstellung nach einem Systemausfall zu erleichtern.

Tägliche Backups werden automatisch im lokalen Datenspeicher gespeichert. Wir empfehlen jedoch, vor der Aktualisierung der Firmware oder vor größeren Änderungen an Ihrer Umgebung (z. B. Änderung des Datenfeeds zum Sensor) manuell ein System-Backup zu erstellen. Laden Sie dann die Sicherungsdatei herunter und speichern Sie sie an einem sicheren Ort.

### Inhalt der täglichen Sicherungsdatei

Die tägliche Sicherungsdatei enthält wichtige Informationen, die erforderlich sind, um eine EDA auf die letzte funktionierende Konfiguration zurückzusetzen.

**Im Backup enthalten**

- Anpassung JSON
- Konfigurationsdateien
  - Konfiguration JSON
  - Ausstehende Lizenzaktualisierung
  - Verschlüsselte Passwörter für Shell- und Systembenutzer
  - Gerätezertifikate
  - Für das Tunneling verwendete Client-Zertifikate
  - Verschlüsselte geheime Schlüssel
  - Zeitzone
- Variablendateien
  - Geografische Daten des Benutzers
  - Vertrauenswürdige Zertifikate, die vom Benutzer hochgeladen wurden
  - Status erfassen
  - Hopcloud-Zertifikate
  - Konfigurationsdateien für Knotentunnel
  - Persistente SSH-Daten

**Aus dem Backup ausgeschlossen**

- Konfigurationsdateien
  - Datenspeicher (Metriken und Datenspeicher-Anmeldeinformationen)
  - Erfassen Sie SSL-Entschlüsselungsschlüssel

  - Zwischengespeicherte Zertifikate
  - AWS-ID-Dateien (AMI, Instanz, Seriennummer)
  - SSH-Konfiguration und Schlüssel der Festplatte
- Variablendateien
  - Benutzername, SID
  - Reinitialisierung der Paketerfassung
  - Aktivierung der Paketerfassung
  - SID einrichten
  - Hosttabelle mit IP-Adresse
  - Anpassungen
  - OUI-Datenbank (Organizational Unique Identifier) und MD5-Dateien
  - Portaldateien
  - Unterstützt SSH-Login-Dateien
- Variable Bibliotheksdateien
  - DHCP-Leasing
  - Dateien abstürzen
  - Dateien sperren
  - Logdateien
  - Paketerfassungsdateien
  - Ergebnisse des Diagnosepakets
  - Bridge-Dateien, Disk-Images
  - Datenbank-Dateien

## Einen Sensor oder eine Konsole sichern

Erstellen Sie eine Systemsicherung und speichern Sie die Sicherungsdatei an einem sicheren Ort.

**Wichtig:** System-Backups enthalten vertrauliche Informationen, einschließlich TLS-Schlüssel. Wenn Sie eine Systemsicherung erstellen, stellen Sie sicher, dass Sie die Sicherungsdatei an einem sicheren Ort speichern.

Die folgenden Anpassungen und Ressourcen werden gespeichert, wenn Sie ein Backup erstellen.

- Benutzeranpassungen wie Bundles, Trigger und Dashboards.
- Konfigurationen, die aus Administrationseinstellungen vorgenommen wurden, z. B. lokal erstellte Benutzer und remote importierte Benutzergruppen, die Konfigurationsdateieinstellungen, TLS-Zertifikate und Verbindungen zu ExtraHop-Recordstores und Packetstores ausführen.

Die folgenden Anpassungen und Ressourcen werden nicht gespeichert, wenn Sie ein Backup erstellen oder zu einem neuen Ziel migrieren.

- Lizenzinformationen für das System. Wenn Sie Einstellungen für ein neues Ziel wiederherstellen, müssen Sie das neue Ziel manuell lizenzieren.
- Präzise Paketerfassung. Sie können gespeicherte Paketerfassungen manuell herunterladen, indem Sie die Schritte unter Paketerfassungen anzeigen und herunterladen.
- Bei der Wiederherstellung einer virtuellen Konsole, die über eine getunnelte Verbindung von einem Sensor, der Tunnel muss nach Abschluss der Wiederherstellung und aller Anpassungen an der Konsole dafür neu eingerichtet werden Sensor muss manuell neu erstellt werden.
- Vom Benutzer hochgeladene TLS-Schlüssel für die Entschlüsselung des Datenverkehrs.
- Sichere Keystore-Daten, die Passwörter enthalten. Wenn Sie eine Sicherungsdatei auf demselben Ziel wiederherstellen, das das Backup erstellt hat, und der Keystore intakt ist, müssen Sie die Anmeldedaten nicht erneut eingeben. Wenn Sie jedoch eine Sicherungsdatei auf einem neuen Ziel wiederherstellen oder zu einem neuen Ziel migrieren, müssen Sie die folgenden Anmeldedaten erneut eingeben:

- Alle SNMP-Community-Zeichenketten, die für die SNMP-Abfrage von Flow-Netzwerken bereitgestellt werden.
- Jedes Bindkennwort, das für die Verbindung mit LDAP für Fernauthentifizierungszwecke bereitgestellt wird.
- Jedes Passwort, das für die Verbindung zu einem SMTP-Server bereitgestellt wird, für den eine SMTP-Authentifizierung erforderlich ist.
- Jedes Passwort, das für die Verbindung zu einem externen Datenspeicher angegeben wurde.
- Jedes Passwort, das für den Zugriff auf externe Ressourcen über den konfigurierten globalen Proxy bereitgestellt wird.
- Jedes Passwort, das für den Zugriff auf ExtraHop Cloud Services über den konfigurierten ExtraHop-Cloud-Proxy angegeben wurde.
- Alle Authentifizierungsdaten oder Schlüssel, die zur Konfiguration von Open Data Stream-Zielen bereitgestellt werden.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Sichern und Wiederherstellen**.
3. Klicken Sie **System-Backup erstellen**, und klicken Sie dann auf **OK**.
   Eine Liste der vom Benutzer gespeicherten und automatischen Backups wird angezeigt.
4. Klicken Sie auf den Namen der neuen Sicherungsdatei. **Benutzer gespeichert <*Zeitstempel*> (neu)**.
   Die Backup-Datei mit einem `.exbk` Dateierweiterung, wird automatisch am Standard-Download-Speicherort für Ihren Browser gespeichert.

## Stellen Sie einen Sensor oder eine Konsole aus einem System-Backup wieder her

Sie können das ExtraHop-System anhand der vom Benutzer gespeicherten oder automatischen Backups wiederherstellen, die auf dem System oder an einem anderen Ort gespeichert sind. Sie können zwei Arten von Wiederherstellungsvorgängen ausführen: nur Anpassungen (z. B. Änderungen an Warnungen, Dashboards, Triggern, benutzerdefinierten Metriken) oder sowohl Anpassungen als auch Systemressourcen.

**Bevor Sie beginnen**
Auf dem Ziel muss dieselbe Firmware-Version ausgeführt werden, die den ersten und zweiten Ziffern der Firmware entspricht, die die Backup-Datei generiert hat. Wenn die Versionen nicht identisch sind, schlägt der Wiederherstellungsvorgang fehl.

Dieses Verfahren beschreibt die Schritte, die erforderlich sind, um eine Sicherungsdatei auf demselben Sensor oder derselben Konsole wiederherzustellen, die die Sicherungsdatei erstellt hat. Wenn Sie die Einstellungen auf einen neuen Sensor oder eine neue Konsole migrieren möchten, finden Sie unter Einstellungen auf einen neuen Sensor oder eine neue Konsole übertragen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Sichern und Wiederherstellen**.
3. klicken **System-Backups anzeigen oder wiederherstellen**.
4. klicken **Wiederherstellen** neben dem Benutzer-Backup oder dem automatischen Backup, das Sie wiederherstellen möchten.
5. Wählen Sie eine der folgenden Wiederherstellungsoptionen:

   **Systemanpassungen wiederherstellen**

   Wählen Sie diese Option, wenn beispielsweise ein Dashboard versehentlich gelöscht wurde oder eine andere Benutzereinstellung wiederhergestellt werden muss. Alle Anpassungen, die nach der Erstellung der Sicherungsdatei vorgenommen wurden, werden nicht überschrieben, wenn die Anpassungen wiederhergestellt werden.

**Systemanpassungen und Ressourcen wiederherstellen**

Wählen Sie diese Option, wenn Sie das System in den Zustand zurückversetzen möchten, in dem es sich bei der Erstellung des Backups befand.

⚠ **Warnung:** Alle Anpassungen, die nach der Erstellung der Sicherungsdatei vorgenommen wurden, werden überschrieben, wenn die Anpassungen und Ressourcen wiederhergestellt werden.

6. Klicken Sie **OK**.
7. Optional: Wenn du ausgewählt hast **Systemanpassungen wiederherstellen**, klicken **Import-Protokoll anzeigen** um zu sehen, welche Anpassungen wiederhergestellt wurden.
8. Starten Sie das System neu.
   a) Kehren Sie zu den Administrationseinstellungen zurück.
   b) In der Appliance-Einstellungen Abschnitt, klicken Sie **Herunterfahren oder Neustarten**.
   c) In der Aktionen Spalte, für die System Eintrag, klicken **Neustarten**.
   d) klicken **Neustarten** zur Bestätigung.

## Stellen Sie einen Sensor oder eine Konsole aus einer Sicherungsdatei wieder her

Dieses Verfahren beschreibt die Schritte, die erforderlich sind, um ein System aus einer Sicherungsdatei auf demselben Sensor oder derselben Konsole wiederherzustellen, die die Sicherungsdatei erstellt hat.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Sichern und Wiederherstellen**.
3. Klicken Sie **Laden Sie die Sicherungsdatei hoch, um das System wiederherzustellen**.
4. Wählen Sie eine der folgenden Wiederherstellungsoptionen:

   **Systemanpassungen wiederherstellen**

   Wählen Sie diese Option, wenn beispielsweise ein Dashboard versehentlich gelöscht wurde oder eine andere Benutzereinstellung wiederhergestellt werden muss. Alle Anpassungen, die nach der Erstellung der Sicherungsdatei vorgenommen wurden, werden nicht überschrieben, wenn die Anpassungen wiederhergestellt werden.

   **Systemanpassungen und Ressourcen wiederherstellen**

   Wählen Sie diese Option, wenn Sie das System in den Zustand zurückversetzen möchten, in dem es sich bei der Erstellung des Backups befand.

   ⚠ **Warnung:** Alle Anpassungen, die nach der Erstellung der Sicherungsdatei vorgenommen wurden, werden überschrieben, wenn die Anpassungen und Ressourcen wiederhergestellt werden.

5. Klicken Sie **Wählen Sie Datei** und navigieren Sie zu einer Sicherungsdatei, die Sie zuvor gespeichert haben.
6. Klicken Sie **Wiederherstellen**.
7. Optional: Wenn du ausgewählt hast **Systemanpassungen wiederherstellen**, klicken Sie **Importprotokoll anzeigen** um zu sehen, welche Anpassungen wiederhergestellt wurden.
8. Starten Sie das System neu.
   a) Kehren Sie zu den Administrationseinstellungen zurück.
   b) In der Appliance-Einstellungen Abschnitt, klicken **Herunterfahren oder Neustarten**.
   c) In der Aktionen Kolumne für die System Eintrag, klick **Neustart**.
   d) Klicken Sie **Neustart** zur Bestätigung.

## Einstellungen auf einen neuen Sensor oder eine neue Konsole übertragen

Dieses Verfahren beschreibt die Schritte, die erforderlich sind, um eine Sicherungsdatei auf eine neue wiederherzustellen Konsole oder Sensor. Nur Systemeinstellungen von Ihrer vorhandenen Konsole oder Sensor werden übertragen. Metriken im lokalen Datenspeicher werden nicht übertragen.

**Bevor Sie beginnen**

- Erstellen Sie eine Systemsicherung und speichern Sie die Sicherungsdatei an einem sicheren Ort.
- Schalten Sie die Quelle aus Sensor oder Konsole um es vor der Übertragung der Einstellungen aus dem Netzwerk zu entfernen. Ziel und Quelle können nicht gleichzeitig im Netzwerk aktiv sein.

  **Wichtig:** Trennen Sie keine Sensoren die bereits mit einer Konsole verbunden sind.
- Bereitstellen und Register der Zielsensor oder die Zielkonsole.
  - Stellen Sie sicher, dass es sich bei dem Ziel um den gleichen Typ handelt Sensor oder Konsole (physisch oder virtuell) als Quelle.
  - Stellen Sie sicher, dass das Ziel dieselbe Größe oder größer hat (maximaler Durchsatz auf dem Sensor; CPU, RAM und Festplattenkapazität auf der Konsole) wie die Quelle.
  - Stellen Sie sicher, dass das Ziel über eine Firmware-Version verfügt, die der Firmware-Version entspricht, die die Sicherungsdatei generiert hat. Wenn die ersten beiden Ziffern der Firmware-Versionen nicht identisch sind, schlägt der Wiederherstellungsvorgang fehl.
- Nach der Übertragung der Einstellungen auf ein Ziel Konsole, Sie müssen alle manuell erneut verbinden Sensoren.
- Bei der Übertragung von Einstellungen auf ein Ziel Konsole das für eine getunnelte Verbindung zum konfiguriert ist Sensoren, wir empfehlen Ihnen, das Ziel zu konfigurieren Konsole mit demselben Hostnamen und derselben IP-Adresse wie die Quellkonsole.

1. Melden Sie sich bei den Administrationseinstellungen auf dem Zielsystem an über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Sichern und Wiederherstellen**.
3. Klicken Sie **Laden Sie die Sicherungsdatei hoch, um das System wiederherzustellen**.
4. Wählen **Systemanpassungen und Ressourcen wiederherstellen**.
5. Klicken Sie **Wählen Sie Datei**, navigieren Sie zur gespeicherten Sicherungsdatei, und klicken Sie dann auf **Öffnen**.
6. Klicken Sie **Wiederherstellen**.

   **Warnung:** Wenn die Sicherungsdatei nicht mit dem lokalen Datenspeicher kompatibel ist, muss der Datenspeicher zurückgesetzt werden.

   Nach Abschluss der Wiederherstellung werden Sie vom System abgemeldet.
7. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin` und stellen Sie sicher, dass Ihre Anpassungen auf dem Zielsensor oder der Konsole korrekt wiederhergestellt wurden.

   **Hinweis:** Wenn der Quellsensor oder die Konsole mit ExtraHop Cloud Services verbunden war, müssen Sie das Ziel manuell mit ExtraHop Cloud Services verbinden.

**Schließen Sie die Sensoren wieder an die Konsole an**

Wenn Sie Einstellungen auf ein neues übertragen haben Konsole, Sie müssen alle zuvor verbundenen manuell erneut verbinden Sensoren.

**Bevor Sie beginnen**

**Wichtig:** Wenn Ihre Konsole und Ihre Sensoren für eine getunnelte Verbindung konfiguriert sind, empfehlen wir, die Quelle- und Zielkonsole mit derselben IP-Adresse und demselben Hostnamen zu konfigurieren. Wenn Sie nicht dieselbe IP-Adresse und denselben Hostnamen festlegen können, überspringen Sie dieses Verfahren und stellen Sie eine

neue Tunnelverbindung zu der neuen IP-Adresse oder dem neuen Hostnamen der Konsole her.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Verwaltung verbundener Appliances Abschnitt, unter ExtraHop-Sensor-Einstellungen, klicken **Sensoren verwalten**.
3. In der Spalte Aktionen für die erste Sensor, klicken **Erneut verbinden**.
4. Geben Sie das Passwort für den Setup-Benutzer von Sensor.
5. Klicken Sie **Verbinden**.
6. Wiederholen Sie die Schritte 3—5 für alle verbleibenden Verbindungsabbrüche Sensoren.
Alle getrennten Sensoren sind jetzt online.

# Appliance-Einstellungen

Sie können die folgenden Komponenten der ExtraHop-Appliance im Appliance-Einstellungen 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 Verwaltungs-GUI, den SNMP-Dienst, den SSH-Zugriff und den TLS-Sitzungsschlüsselempfänger. Die Option SSL Session Key Receiver wird nur auf Paketsensoren 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.

**Meldung auf dem Anmeldebildschirm**
Konfigurieren Sie eine benutzerdefinierte Meldung, die angezeigt wird, bevor sich Benutzer beim ExtraHop-System anmelden

Die folgenden Komponenten sind nur auf den angegebenen Appliances enthalten:

**Spitzname für die Konsole**
Weisen Sie einer ExtraHop-Konsole einen Spitznamen zu. Diese Einstellung ist nur auf der Konsole verfügbar.

**Packetstore zurücksetzen**
Löschen Sie alle Pakete, die in ExtraHop-Paketstores gespeichert sind. Das Packetstore zurücksetzen Seite erscheint nur in Packetstores.

## 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.

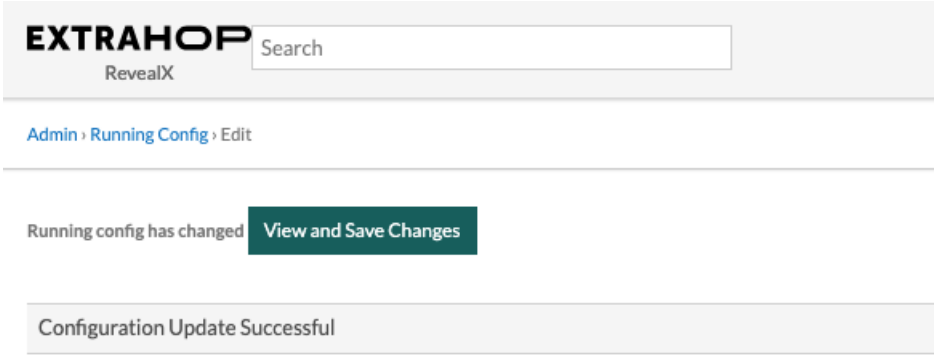
**Hinweis:** Es wird nicht empfohlen, Konfigurationsänderungen am Code von der Bearbeitungsseite aus vorzunehmen. Sie können die meisten Systemänderungen über andere Seiten in den Administrationseinstellungen vornehmen.

### 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 Verwaltungseinstellungen sowie eine **Änderungen anzeigen und speichern** Schaltfläche auf allen Seiten mit Administrationseinstellungen.

1. Klicken Sie **Änderungen anzeigen und speichern**.




2. Prüfen 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 Konfigurationsdatei

Die ExtraHop-Administrationseinstellungen bieten eine Schnittstelle zum Anzeigen und Ändern des Codes , der die Standardsystemkonfiguration spezifiziert. Zusätzlich zu den Änderungen an der laufenden Konfigurationsdatei über die Administrationseinstellungen können Sie auch Änderungen an der Konfiguration ausführen Seite.

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

## Laden Sie die aktuelle 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 die Konfiguration ausführen Fenster.

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

Die aktuell laufende Konfigurationsdatei wird als Textdatei an Ihren Standard-Download-Speicherort 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 vom Typ Destination Unreachable zu deaktivieren, müssen Sie die Running Configuration bearbeiten. Wir empfehlen jedoch, die Running Configurations-Datei nicht manuell ohne Anweisung des ExtraHop-Supports zu bearbeiten. Wenn Sie die laufende Konfigurationsdatei manuell

falsch bearbeiten, kann dies dazu führen, dass das System nicht mehr verfügbar ist oder die Erfassung von Daten beendet wird. Sie können Kontakt aufnehmen 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 Sie möchten, dass Ihre Netzwerkgeräteüberwachungssoftware Informationen über das ExtraHop-System sammelt. 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 dem Aktualisieren der Seite wird das Kontrollkästchen Aktiviert angezeigt.
- Konfigurieren Sie den SNMP-Dienst 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 TLS Session Key Receiver aktivieren oder deaktivieren (nur Sensor)

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

**Hinweis:** Wenn Sie dieses Kontrollkästchen nicht sehen und die TLS-Entschlüsselungslizenz gekauft 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.

**Konfigurieren Sie den SNMPv1- und SNMPv2-Dienst**
Mit der folgenden Konfiguration können Sie das System mit einem SNMP-Manager überwachen, der SNMPv1 und SNMPv2 unterstützt.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken Sie **Dienstleistungen**.
3. Für SNMP-Dienst, klicken **Konfiguriere**.
4. Wählen Sie die **Aktiviert** Kontrollkästchen, um den SNMP-Dienst zu aktivieren.
5. Wählen Sie die **SNMPv1 und SNMPv2 aktiviert** Kontrollkästchen, um den SNMPv1- und SNMPv2-Dienst zu aktivieren.
6. In der SNMP-Gemeinschaft Feld, geben Sie einen benutzerfreundlichen Namen für die SNMP-Community ein.
7. In der SNMP-Systemkontakt Geben Sie in dieses Feld einen gültigen Namen oder eine gültige E-Mail-Adresse für den SNMP-Systemkontakt ein.
8. In der Standort des SNMP-Systems Feld, geben Sie einen Speicherort für das SNMP-System ein.
9. Klicken Sie **Einstellungen speichern**.

**Nächste Schritte**
Laden Sie die ExtraHop SNMP MIB-Datei von der Seite SNMP Service Configuration herunter.

**Konfigurieren Sie den SNMPv3-Dienst**
Mit der folgenden Konfiguration können Sie das System mit einem SNMP-Manager überwachen, der SNMPv3 unterstützt. Das SNMPv3-Sicherheitsmodell bietet zusätzliche Unterstützung für Authentifizierung - und Datenschutzprotokolle.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken Sie **Dienstleistungen**.
3. Für SNMP-Dienst, klicken **Konfiguriere**.
4. Wählen Sie die **Aktiviert** Kontrollkästchen, um den SNMP-Dienst zu aktivieren.
5. Wählen Sie die **SNMPv3 aktiviert** Kontrollkästchen, um den SNMPv3-Dienst zu aktivieren.
6. In der SNMPv3-Benutzername Feld, geben Sie den Namen des Benutzers ein , der auf den SNMPv3-Dienst zugreifen kann.
7. Wählen Sie für das Drop-down-Menü Authentifizierung und Datenschutzmodus **Authentifizierung und Datenschutz** oder **Authentifizierung und kein Datenschutz**.

   Wenn du auswählst **Authentifizierung und Datenschutz**, müssen Sie auch das ausfüllen Datenschutz-Passwort Feld.

   **Wichtig:** ExtraHop-Systeme unterstützen die AES-128-Verschlüsselung für den Datenschutz von SNMPv3-Nachrichten.
8. In der Passwort für die Authentifizierung Geben Sie in dieses Feld ein Passwort ein, mit dem sich der Benutzer beim SNMPv3-Dienst authentifizieren kann.

9. Aus dem **Authentifizierungsalgorithmus** Drop-down-Menü, wählen **SHA-256** oder **SHA-1**.
10. Geben Sie im Feld Datenschutzkennwort das Passwort zum Entschlüsseln von SNMPv3-Traps ein. Dieses Feld ist erforderlich, wenn Sie **Authentifizierung und Datenschutz**.
11. Klicken Sie **Einstellungen speichern**.

**Nächste Schritte**
Laden Sie die ExtraHop SNMP MIB-Datei von der Konfiguration des SNMP-Dienstes Seite.

# 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 zum Upgrade von ExtraHop-Appliances.

- Ein Systemhinweis erscheint auf Konsolen und Sensoren mit ExtraHop Cloud Services verbunden , wenn eine neue Firmware-Version verfügbar ist.
- Stellen Sie sicher, dass Ihr RevealX 360-System auf Version aktualisiert wurde 25,2 bevor Sie Ihr Upgrade durchführen Sensoren.
- Wenn Sie ein Upgrade von der Firmware-Version 8.7 oder früher durchführen, wenden Sie sich an den ExtraHop-Support, um weitere Informationen zum Upgrade zu erhalten.
- Wenn Sie einen virtuellen ExtraHop-Sensor aktualisieren, der auf einem VMware ESXi/ESX, Microsoft Hyper-V, oder Linux-KVM Für Plattformen ab Firmware-Version 9.6 oder früher muss die VM Streaming SIMD Extensions 4.2 (SSE4.2) und POPCNT-Anweisungen unterstützen; andernfalls schlägt das Upgrade fehl.
- 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. Paketshops

**Hinweis:** Ihr Browser könnte nach 5 Minuten Inaktivität das Timeout beenden. Aktualisieren Sie die Browserseite, wenn das Update unvollständig erscheint.

Wenn die Browsersitzung abläuft, bevor das ExtraHop-System den Aktualisierungsvorgang abschließen kann, können Sie die folgenden Konnektivitätstests durchführen, um den Status während des Upgrade-Vorgangs zu bestätigen:

- Pingen Sie die Appliance von der Kommandozeile einer anderen Appliance oder Client-Workstation aus.
- Sehen Sie sich in den Administrationseinstellungen auf einer Konsole den Appliance-Status auf der Verbundene Geräte verwalten Seite.
- Stellen Sie über die iDRAC-Schnittstelle eine Verbindung zur Appliance her.

### Konsolen-Upgrades

- Bei großen Konsolenbereitstellungen (Verwaltung von 50.000 Geräten oder mehr) sollten Sie sich mindestens eine Stunde Zeit nehmen, 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-Aktualisierungen

- 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, Datensatzaufnahme im Recordstore deaktivieren 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 Nachrichten `Could not determine ingest status on some nodes` und `Error` werden auf der Seite Cluster-Datenverwaltung in den Verwaltungseinstellungen der aktualisierten Knoten angezeigt, bis alle Knoten im Cluster aktualisiert wurden. Diese Fehler werden erwartet und können ignoriert werden.
- Sie müssen die Aufnahme von Datensätzen und die Neuzuweisung von Shards aus aktivieren 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 auf den angeschlossenen Konsolen installierte Version 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 Appliance-Einstellungen Abschnitt, klicken **Firmware**.
3. Aus dem **Verfügbare Firmware** Wählen Sie im Drop-down-Menü die Version der Firmware 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 Sie **Downloaden und installieren**.

Nachdem das Firmware-Upgrade erfolgreich installiert wurde, wird die ExtraHop-Appliance neu gestartet.

### Aktualisieren Sie die Firmware auf Recordstores

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 Sie **Cluster-Datenmanagement**.
4. Klicken Sie **Record Ingest deaktivieren**.
5. Klicken Sie **Admin** um zur Haupt-Administrationsseite zurückzukehren.
6. Klicken Sie **Firmware**.
7. Klicken Sie **eine Datei aktualisieren oder eine URL angeben**.
8. Auf dem Firmware aktualisieren Seite, wählen Sie eine der folgenden Optionen:
   - Um Firmware aus einer Datei hochzuladen, klicken Sie auf **Wählen Sie Datei**, navigieren Sie zum `.tar` Datei, die Sie hochladen möchten, und klicken Sie auf **Öffnen**.
   - Um Firmware von einem HTTP (s) -Staging-Server in Ihrem Netzwerk hochzuladen, klicken Sie auf **stattdessen von der URL abrufen** und geben Sie dann die URL in das Firmware-URL Feld.
9. Klicken Sie **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 Recordstore-Knoten ausführen.

1. Klicken Sie im Abschnitt Recordstore Cluster Settings auf **Cluster-Datenmanagement**.
2. Klicken Sie **Datensatzaufnahme aktivieren**.
3. Klicken Sie **Shard-Neuzuweisung aktivieren**.

### Aktualisieren Sie die Firmware auf 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 **eine Datei hochladen oder eine URL angeben**.
4. Auf dem Firmware aktualisieren Seite, wählen Sie eine der folgenden Optionen:
   - Um Firmware aus einer Datei hochzuladen, klicken Sie auf **Wählen Sie Datei**, navigieren Sie zum `.tar` Datei, die Sie hochladen möchten, und klicken Sie auf **Öffnen**.
   - Um Firmware von einem HTTP (s) -Staging-Server in Ihrem Netzwerk hochzuladen, klicken Sie auf **stattdessen von der URL abrufen** und geben Sie dann die URL in das Firmware-URL Feld.
5. Optional: Wenn Sie die Appliance nach der Installation der Firmware nicht automatisch neu starten möchten, löschen Sie das **Gerät nach der Installation automatisch neu starten** Ankreuzfeld.
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.

### Rüsten Sie die angeschlossenen Sensoren in RevealX 360 auf
Administratoren können ein Upgrade durchführen Sensoren die mit RevealX 360 verbunden sind.

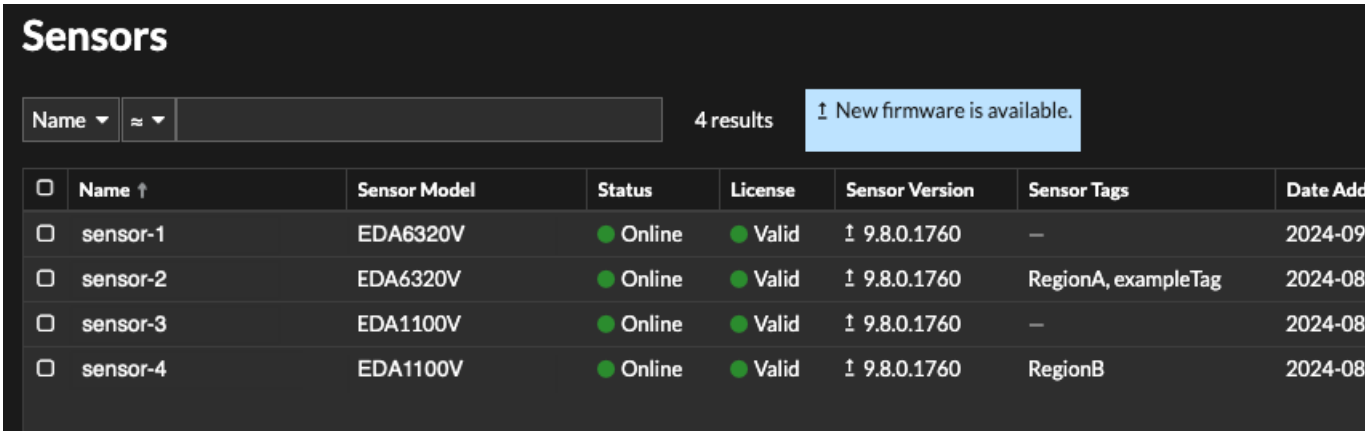
**Bevor Sie beginnen**

- Ihr Benutzerkonto muss über Rechte auf RevealX 360 für die System- und Zugriffsadministration 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 upgraden Sensoren zur gleichen Zeit

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann **Sensorik**.
   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** Drop-down-Menü.
   Das Dropdownmenü zeigt nur Versionen an, 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. |

## Konfigurieren Sie die Systemzeit

Standardmäßig synchronisiert das ExtraHop-System die Systemzeit über die NTP-Server (*.extrahop.pool.ntp.org Netzwerk Time Protokoll). 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 Appliance-Einstellungen Abschnitt, klicken **Systemzeit**.
3. Klicken Sie **Zeit konfigurieren**.
4. Aus dem **Wählen Sie eine Zeitzone** Drop-down-Menü, wählen Sie Ihre Zeitzone aus.
5. Klicken Sie **Speichern und fortfahren**.
6. Auf dem Uhrzeit einrichten Seite, wählen Sie eine der folgenden Optionen:
   - Zeit manuell einstellen

     **Hinweis:** Sie können die Zeit für Sensoren, die von einer Konsole oder RevealX 360 verwaltet werden, nicht manuell einstellen.
   - Stellen Sie die Zeit mit dem NTP-Server ein
7. Wählen Sie **Zeit mit NTP-Server einstellen** und klicken Sie dann **Wählen Sie**.

   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.
8. In der Zeitserver Felder, geben Sie die IP-Adresse oder den vollqualifizierten Domänenname (FQDN) für die Zeitserver ein.

   Sie können bis zu neun Zeitserver angeben.

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

Das NTP-Status In der Tabelle wird eine Liste von NTP-Servern angezeigt, die die Systemuhr synchron halten. Um die aktuelle Systemzeit auf einem Remoteserver zu synchronisieren, klicken Sie auf **Jetzt synchronisieren** knopf.

## Herunterfahren oder Neustarten

Die Administrationseinstellungen bieten eine Schnittstelle zum Anhalten, Herunterfahren und Neustarten des ExtraHop-Systems und seiner Systemkomponenten. Für jede ExtraHop-Systemkomponente enthält die Tabelle einen Zeitstempel zur Anzeige der Startzeit.

- Starten Sie das System neu oder fahren Sie es herunter, um das ExtraHop-System anzuhalten oder herunterzufahren und neu zu starten.
- Starten Sie Bridge Status (nur Sensor) neu, um die ExtraHop Bridge-Komponente neu zu starten.
- Starten Sie Capture neu (nur Sensor), um die ExtraHop-Capture-Komponente neu zu starten.
- Starten Sie Portal Status neu, um das ExtraHop-Webportal neu zu starten.
- Starten Sie Scheduled Reports (nur Konsole) neu, um die ExtraHop-Komponente für geplante Berichte neu zu starten.

## Sensormigration

Sie können Ihre gespeicherten Metriken, Anpassungen und Systemressourcen auf Ihren vorhandenen physischen ExtraHop migrieren Sensor zu einem neuen Sensor.

**Hilfe auf dieser Seite**

- Migrieren Sie einen ExtraHop-Sensor

## Migrieren Sie einen ExtraHop-Sensor

Wenn Sie bereit sind, Ihr bestehendes zu aktualisieren Sensor, können Sie problemlos auf neue Hardware migrieren, ohne geschäftskritische Kennzahlen und zeitaufwändige Systemkonfigurationen zu verlieren.

Die folgenden Anpassungen und Ressourcen werden nicht gespeichert, wenn Sie ein Backup erstellen oder zu einem neuen Ziel migrieren.

- Lizenzinformationen für das System. Wenn Sie Einstellungen für ein neues Ziel wiederherstellen, müssen Sie das neue Ziel manuell lizenzieren.
- Präzise Paketerfassung. Sie können gespeicherte Paketerfassungen manuell herunterladen, indem Sie die Schritte unter Paketerfassungen anzeigen und herunterladen.
- Bei der Wiederherstellung einer virtuellen Konsole, die über eine getunnelte Verbindung von einem Sensor, der Tunnel muss nach Abschluss der Wiederherstellung und aller Anpassungen an der Konsole dafür neu eingerichtet werden Sensor muss manuell neu erstellt werden.
- Vom Benutzer hochgeladene TLS-Schlüssel für die Entschlüsselung des Datenverkehrs.
- Sichere Keystore-Daten, die Passwörter enthalten. Wenn Sie eine Sicherungsdatei auf demselben Ziel wiederherstellen, das das Backup erstellt hat, und der Keystore intakt ist, müssen Sie die Anmeldedaten nicht erneut eingeben. Wenn Sie jedoch eine Sicherungsdatei auf einem neuen Ziel wiederherstellen oder zu einem neuen Ziel migrieren, müssen Sie die folgenden Anmeldedaten erneut eingeben:
  - Alle SNMP-Community-Zeichenketten, die für die SNMP-Abfrage von Flow-Netzwerken bereitgestellt werden.
  - Jedes Bindkennwort, das für die Verbindung mit LDAP für Fernauthentifizierungszwecke bereitgestellt wird.
  - Jedes Passwort, das für die Verbindung zu einem SMTP-Server bereitgestellt wird, für den eine SMTP-Authentifizierung erforderlich ist.
  - Jedes Passwort, das für die Verbindung zu einem externen Datenspeicher angegeben wurde.
  - Jedes Passwort, das für den Zugriff auf externe Ressourcen über den konfigurierten globalen Proxy bereitgestellt wird.
  - Jedes Passwort, das für den Zugriff auf ExtraHop Cloud Services über den konfigurierten ExtraHop-Cloud-Proxy angegeben wurde.
  - Alle Authentifizierungsdaten oder Schlüssel, die zur Konfiguration von Open Data Stream-Zielen bereitgestellt werden.

**Bevor du anfängst**

**Wichtig:** Wenn der Quellsensor über einen externen Datenspeicher verfügt und der Datenspeicher auf einem SMB-Server konfiguriert ist, für den eine Passwortauthentifizierung erforderlich ist, wenden Sie sich an den ExtraHop-Support, um Sie bei der Migration zu unterstützen.

- Quelle und Ziel Sensoren muss dieselbe Firmware-Version ausführen.
- Migrieren Sie nur auf den gleichen Typ von Sensoren, wie RevealX Enterprise bis RevealX Enterprise. Wenn Sie zwischen Sensortypen (wie RevealX Enterprise zu RevealX 360) migrieren müssen, wenden Sie sich an Ihr ExtraHop-Vertriebsteam, um Unterstützung zu erhalten.
- Die Migration wird nur zwischen physischen Geräten unterstützt Sensoren. Virtuell Sensor Migrationen werden nicht unterstützt.
- Die Migration von einer früheren Serie zu einer neueren Serie wird nur unterstützt (Sie können beispielsweise nur eine EDA 6200 auf eine EDA 6300, EDA 9300 oder ähnliches migrieren.) Außerdem können Sie nur von einem kleineren Sensor auf einen größeren Sensor migrieren.

### RevealX-Kompatibilitätsmatrix

Die unterstützten Migrationspfade sind in der folgenden Tabelle aufgeführt.

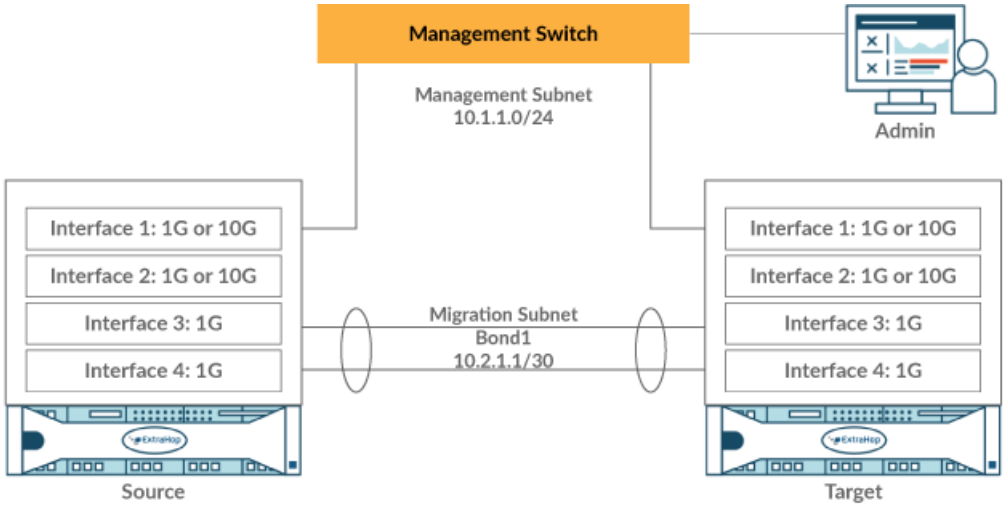
| Quelle | Ziel | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | SEIT 1200 | SEIT 6200 | AB 820 | SEIT 8320 | SEIT 9200 | SEIT 9300 | VON 10200 | VON 10300 |
| SEIT 1200 | JA | JA | JA | JA | JA | JA | JA | JA |
| SEIT 6200 | NEIN | JA* | JA | JA | JA | JA | JA | JA |
| AB 8200 | NEIN | NEIN | JA* | JA* | JA* | JA | JA | JA |
| SEIT 8320 | NEIN | NEIN | NEIN | JA | NEIN | JA | NEIN | JA |
| SEIT 9200 | NEIN | NEIN | NEIN | NEIN | JA* | JA | JA | JA |
| SEIT 9300 | NEIN | NEIN | NEIN | NEIN | NEIN | JA | NEIN | JA |
| VON 10200 | NEIN | NEIN | NEIN | NEIN | NEIN | NEIN | JA* | JA |
| VON 10300 | NEIN | NEIN | NEIN | NEIN | NEIN | NEIN | NEIN | JA |

*Die Migration wird nur unterstützt, wenn Quelle und Ziel Sensor wurden im Mai 2019 oder später hergestellt. Wenden Sie sich an den ExtraHop Support, um die Kompatibilität zu überprüfen.

Für Informationen über die frühere Performance Edition wenden Sie sich bitte an Ihren ExtraHop-Vertreter, um Hilfe zu erhalten.

### Bereite die Quelle- und Zielsensoren vor

1. Folgen Sie den Anweisungen in der Bereitstellungsanleitung für Ihr Sensormodell, um den Zielsensor einzusetzen.
2. Registrieren der Zielsensor.
3. Stellen Sie sicher, dass das Ziel und die Quelle Sensor verwenden exakt dieselbe Firmware-Version. Sie können die aktuelle und frühere Firmware von der herunterladen ExtraHop Kundenportal.
4. Wählen Sie eine der folgenden Netzwerkmethoden, um zum Ziel zu migrieren Sensor.
   - (Empfohlen) Um die Migration so schnell wie möglich abzuschließen, verbinden Sie die Sensoren direkt mit 10G-Managementschnittstellen.
   - Erstellen Sie eine Bond-Schnittstelle (optional) der verfügbaren 1G-Managementschnittstellen. Verbinden Sie mit den entsprechenden Netzwerkkabeln den oder die verfügbaren Anschlüsse des Quellsensors direkt mit ähnlichen Anschlüssen am Zielsensor. Die folgende Abbildung zeigt eine Beispielkonfiguration mit gebondeten 1G-Schnittstellen.




**Wichtig:** Stellen Sie sicher, dass Ihre IP-Adresse und die Subnetzkonfiguration auf beiden Sensoren den Verwaltungsdatenverkehr an Ihre Verwaltungs-Workstation und den Migrationsverkehr an den Direktlink weiterleiten.

- Migrieren Sie den Sensor über Ihr bestehendes Netzwerk. Die Quelle- und Zielsensoren müssen in der Lage sein, über Ihr Netzwerk miteinander zu kommunizieren. Beachten Sie , dass die Migration bei dieser Konfiguration erheblich länger dauern kann.

**Erstellen Sie eine Bond-Schnittstelle (optional)**
Folgen Sie den nachstehenden Anweisungen, um 1G-Schnittstellen zu verbinden. Durch das Erstellen einer Bond-Schnittstelle wird die Zeit reduziert, die benötigt wird, um die Migration über 1G-Schnittstellen abzuschließen.

Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.

1. In der Netzwerkeinstellungen Abschnitt über die Quelle Sensor, klicken **Konnektivität**.
2. In der Einstellungen für die Bond-Schnittstelle Abschnitt, klicken **Bond-Schnittstelle erstellen**.
3. In der Mitglieder Abschnitt, wählen Sie die Mitglieder der Bond-Schnittstelle aus, abhängig von Sensor Typ.

   Schließen Sie die aktuelle Verwaltungsschnittstelle, in der Regel Schnittstelle 1 oder Schnittstelle 3, nicht in die Bond-Schnittstelle ein.
4. Aus dem **Einstellungen übernehmen von** Wählen Sie im Drop-down-Menü eines der Mitglieder der neuen Bond-Schnittstelle aus.
5. Für Art der Anleihe, wählen **Statisch**.
6. Aus dem **Hash-Richtlinie** Wählen Sie im Drop-down-Menü eine der folgenden Optionen aus:
   - **Schicht 3+4** Richtlinie, die die Verteilung des Datenverkehrs auf die Schnittstellen gleichmäßiger verteilt. Diese Richtlinie entspricht jedoch nicht vollständig den 802.3ad-Standards.
   - **Ebene 2+3** Richtlinie, die den Datenverkehr weniger gleichmäßig verteilt und den 802.3ad-Standards entspricht.
7. Klicken Sie **Erstellen**.
8. Auf dem Konnektivität Seite, in der  Bond-Schnittstellen Abschnitt, klicken **Bond-Schnittstelle 1**.
9. Aus dem **Schnittstellen-Modus** Drop-down-Menü, wählen **Verwaltung**.
10. Geben Sie die IPv4-Adresse, die Netzwerkmaske und das Gateway für Ihr Migrationsnetzwerk Netzwerk.
11. Klicken Sie **Speichern**.
12. Wiederholen Sie diesen Vorgang am Ziel Sensor.

**Starten Sie die Migration**
Die Migration wird für Upgrades empfohlen, bei denen Sie die Daten und die Appliance-Konfiguration beibehalten möchten. Der Abschluss der Migration kann mehrere Stunden dauern. Während dieser Zeit weder die Quelle noch das Ziel Sensor kann Daten sammeln. Der Migrationsvorgang kann nicht unterbrochen oder abgebrochen werden.

1. Loggen Sie sich in die Administrationseinstellungen der Quelle ein Sensor.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. Notieren Sie sich die IP-Adresse der Verwaltungsschnittstelle, der DNS-Server und aller statischen Routen. Sie werden diese Einstellungen auf dem Ziel konfigurieren, nachdem die Migration abgeschlossen ist.
4. In der Appliance-Einstellungen Abschnitt, klicken **Appliance-Migration**.
5. In der Ziel-Appliance Geben Sie in dieses Feld die IP-Adresse der Schnittstelle ein, die Sie für die Migration auf dem Ziel konfiguriert haben.
6. In der Benutzerkennwort einrichten Feld, geben Sie das Passwort des Setup-Benutzers auf dem Ziel ein.

   Das Standardkennwort ist die Systemseriennummer des Zielsensors.
7. Klicken Sie **Weiter**.
8. Vergewissern Sie sich auf der Seite „Fingerabdruck bestätigen“, dass der auf dieser Seite angezeigte Fingerabdruck genau mit dem Fingerabdruck übereinstimmt, der auf der Seite „Fingerabdruck“ in den Verwaltungseinstellungen des Ziels angezeigt wird.

   Wenn die Fingerabdrücke nicht übereinstimmen, stellen Sie sicher, dass Sie den richtigen Hostnamen oder die richtige IP-Adresse des Ziels angegeben haben, das Sie in Schritt 5 eingegeben haben.
9. Klicken Sie **Migration starten**.
   Warten Sie, bis die Erfolgsmeldung der Migration angezeigt wird. Dies kann mehrere Stunden dauern. Während der Migration ist das ExtraHop-System auf dem Ziel nicht zugänglich. Wenn Sie versehentlich die Seite mit dem Migrationsstatus der Appliance auf der Quelle schließen, können Sie zu `https://<source hostname>/admin/appliance_migration_status/` um die Migration weiter zu überwachen.

   Wenn die Migration aus irgendeinem Grund fehlschlägt, starten Sie die Migration neu. Wenn die Migration weiterhin fehlschlägt, wenden Sie sich an den ExtraHop-Support, um Unterstützung zu erhalten.

   **Hinweis:** Das Ziel wird nach Abschluss der Migration automatisch neu gestartet.
10. Klicken Sie **Herunterfahren** um die Quelle auszuschalten.

    **Wichtig:** Um Sensor-ID-Konflikte zu vermeiden, schalten Sie den Quellsensor nicht ein, solange er mit demselben Netzwerk verbunden ist, in dem sich der Zielsensor befindet, es sei denn, Sie setzen ihn mit ExtraHop Rescue Media auf die Werkseinstellungen zurück.

**Konfigurieren Sie den Zielsensor**
Wenn Sensor Das Netzwerk wird nicht über DHCP konfiguriert. Stellen Sie sicher, dass die Konnektivitätseinstellungen aktualisiert werden, einschließlich aller zugewiesenen IP-Adressen, DNS-Server und statischen Routen. Verbindungen zu ExtraHop Konsolen, Recordstores und Packetstores in der Quelle Sensor werden automatisch auf dem Ziel eingerichtet Sensor wenn die Netzwerkeinstellungen konfiguriert sind.

1. Loggen Sie sich in die Administrationseinstellungen auf dem Ziel ein Sensor.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. In der Schnittstellen Abschnitt, klicken Sie auf die Verwaltungsschnittstelle (normalerweise Schnittstelle 1 oder Schnittstelle 3, abhängig von Sensor Modell).
4. Geben Sie im Feld IPv4-Adresse die IP-Adresse der Quelle ein Sensor.

5. Konfigurieren Sie alle statischen Routen, die auf der Quelle konfiguriert wurden Sensor:
   a) Klicken Sie **Routen bearbeiten**.
   b) Fügen Sie alle erforderlichen Routeninformationen hinzu.
   c) Klicken Sie **Speichern**.
6. Klicken Sie **Speichern**.

**Nächste Schritte**
Wenn Sie Schnittstelleneinstellungen ändern mussten, um die Migration mit gebündelten Schnittstellen durchzuführen, stellen Sie sicher, dass die Schnittstellenmodi erwartungsgemäß konfiguriert sind.

Stellen Sie alle zusätzlichen Einstellungen wieder her, die werden nicht automatisch wiederhergestellt.

# Lizenz

Auf der Seite Lizenzverwaltung können Sie Lizenzen für Ihr ExtraHop-System einsehen und verwalten. Sie benötigen eine aktive Lizenz, um auf das ExtraHop-System zugreifen zu können, und Ihr System muss in der Lage sein, eine Verbindung zum ExtraHop-Lizenzserver herzustellen, um regelmäßige Updates und Check-ins über Ihren Lizenzstatus zu erhalten.

Weitere Informationen zu ExtraHop-Lizenzen finden Sie in der Häufig gestellte Fragen zur Lizenz.

## Registrieren Sie Ihr ExtraHop-System

Diese Anleitung enthält Anweisungen zum Anwenden eines neuen Produktschlüssels und zur Aktivierung all Ihrer 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 und wählen Sie Ich stimme zu, und klicken Sie dann auf **Einreichen**.
3. Geben Sie auf dem Anmeldebildschirm Folgendes ein `Einrichten` für den Nutzernamen.
4. Wählen Sie für das Passwort eine der folgenden Optionen aus:
   - Geben Sie bei 1U- und 2U-Geräten die Seriennummer ein, die auf dem Etikett auf der Rückseite des Geräts 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 im Feld angezeigte Seriennummer ein `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 **Einloggen**.
6. In der Appliance-Einstellungen Abschnitt, klicken Sie **Lizenz**.
7. klicken **Lizenz verwalten**.

8. Wenn Sie einen Produktschlüssel haben, klicken Sie auf **Registriere dich** 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 **Aktualisieren**, fügen Sie dann den Inhalt der Datei in das Lizenz eingeben Feld. Klicken Sie **Aktualisieren**.

9. klicken **Registriere dich**.

**Nächste Schritte**
Haben Sie weitere Fragen zur Lizenzierung von Werken von ExtraHop? Sehen Sie die Häufig gestellte Fragen zur Lizenz.

#### Problembehandlung bei der Lizenzserverkonnektivität

Für ExtraHop-Systeme, 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 für ExtraHop Cloud Services lizenziert ist oder noch nicht 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. Schlägt diese Anfrage fehl, versucht das System, über den DNS-Serverport 53 eine Verbindung zum ExtraHop-Lizenzserver herzustellen. Das folgende Verfahren ist hilfreich, 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:

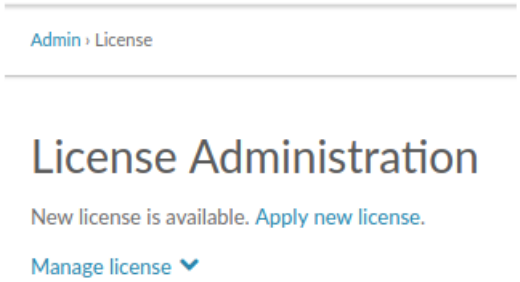
```
Non-authoritative answer:
d.extrahop.com  nameserver = ns0.use.d.extrahop.com.
d.extrahop.com  nameserver = ns0.usw.d.extrahop.com.
```

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

## Eine aktualisierte Lizenz anwenden

Wenn Sie ein neues Protokollmodul, einen neuen Dienst oder eine neue Funktion erwerben, ist die aktualisierte Lizenz automatisch im ExtraHop-System verfügbar. Sie müssen die aktualisierte Lizenz jedoch über die Verwaltungseinstellungen 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. In der Appliance-Einstellungen Abschnitt, klicken **Lizenz**.
   Es wird eine Meldung über die Verfügbarkeit Ihrer neuen Lizenz angezeigt.



3. Klicken Sie **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 Appliance-Einstellungen Abschnitt, klicken Sie **Lizenz**.
3. Klicken Sie Lizenz verwalten.
4. Klicken Sie **Aktualisieren**.
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 der `BEGIN` und `END` Zeilen, wie im folgenden Beispiel 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 Sie **Aktualisieren**.

## Festplatten

Die Seite Festplatten zeigt eine Übersicht der Laufwerke auf dem ExtraHop-System und listet deren Status auf. Anhand dieser Informationen können Sie feststellen, ob Laufwerke installiert oder ausgetauscht werden müssen. Automatische Systemzustandsprüfungen und E-Mail-Benachrichtigungen (falls aktiviert) können rechtzeitig über eine Festplatte informieren, die sich in einem heruntergefahrenen Zustand befindet. Bei Systemzustandsprüfungen werden Festplattenfehler oben auf der Seite „Einstellungen“ angezeigt.

#### Selbstverschlüsselnde Festplatten (SEDs)

Für Sensoren, die selbstverschlüsselnde Festplatten (SEDs) enthalten, ist der `Hardware Disk Encryption` Status kann gesetzt werden auf `Disabled` oder `Enabled`. Dieser Status wurde auf gesetzt `Unsupported` für Sensoren, die keine SEDs enthalten.

Diese Sensoren unterstützen SEDs:

- SEIT 9300
- VON 10300
- Intrusion Detection System 980

Hinweise zur Konfiguration von SEDs finden Sie unter Konfigurieren Sie selbstverschlüsselnde Festplatten (SEDs).

**ÜBERFALL**

Hilfe beim Austauschen einer RAID 0-Festplatte oder beim Installieren eines SSD-Laufwerks finden Sie in den folgenden Anweisungen. Die RAID 0-Anweisungen gelten für die folgenden Festplattentypen:

- Datenspeicher
- Paketerfassung
- Firmware

Versuchen Sie nicht, das Laufwerk in Steckplatz 0 zu installieren oder auszutauschen, es sei denn, Sie werden vom ExtraHop-Support dazu aufgefordert.

**Hinweis** Stellen Sie sicher, dass Ihr Gerät über einen RAID-Controller verfügt, bevor Sie das folgende Verfahren ausführen. Wenn Sie unsicher sind, wenden Sie sich an ExtraHop-Unterstützung. Eine dauerhaft beschädigte Festplatte kann mit diesem Verfahren möglicherweise nicht ausgetauscht werden.

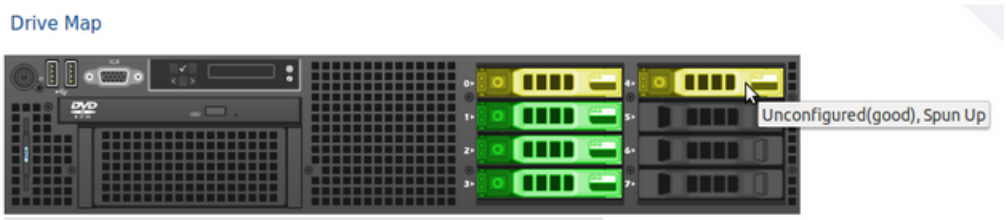
## Ersetzen Sie eine RAID 0-Festplatte

1. Notieren Sie in der E-Mail-Benachrichtigung zum Systemstatus, auf welchem Computer die problematische Festplatte installiert ist.
2. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
3. In der Appliance-Einstellungen Abschnitt, klicken Sie **Festplatten**.
4. Unter dem Abschnitt für den Festplattentyp (z. B. **Datenspeicher**), suchen Sie die problematische Festplatte und notieren Sie sich die Steckplatznummer.

   Klicken Sie **Details zur RAID-Festplatte** um mehr Details anzuzeigen.

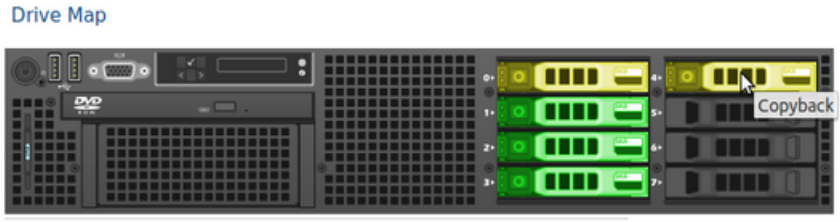
   **Wichtig:** Bewahren Sie die ausgefallene Festplatte auf, bis die Daten erfolgreich auf die neue Festplatte kopiert wurden.
5. Legen Sie eine identische Festplatte in einen verfügbaren Steckplatz ein.

   Das System erkennt die neue Festplatte und fügt eine neue Zeile (Disk Error Action) mit einem Link zum Ersetzen der defekten Festplatte hinzu.
6. Überprüfen Sie die neuen Festplatteninformationen:
   - Unter **Unbenutzte Festplatten** Stellen Sie auf der Seite Festplattendetails sicher, dass die neue Festplatte dieselbe Größe, Geschwindigkeit und denselben Typ hat wie die Festplatte, die ausgetauscht wird.
   - Fahren Sie mit der Maus über die alten und neuen Festplatten in der Drive Map. Die neue Festplatte zeigt die Meldung an"`Unconfigured(good), Spun Up`."



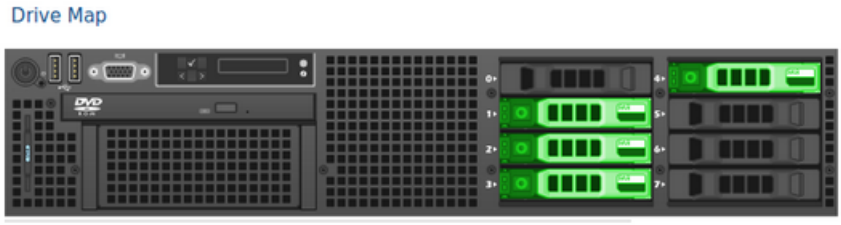
7. Klicken Sie unter dem Abschnitt für den Festplattentyp auf **Durch Diskette im Steckplatz #n ersetzen** in der Aktion „Festplattenfehler“ Reihe.

   Die Daten beginnen zu kopieren. In der Zeile Copy Status wird der Fortschritt angezeigt. Wenn Sie in der Drive Map mit der Maus über die Festplatte fahren, wird der Status angezeigt.




8. Stellen Sie nach Abschluss des Kopiervorgangs sicher, dass der Kopiervorgang erfolgreich war:
   - **Einstellungen** Auf der Schaltfläche und auf der Einstellungsseite werden keine Fehlermeldungen mehr angezeigt.
   - Auf der Festplattenseite wird die alte Festplatte im Abschnitt Unbenutzter Datenträger angezeigt
9. Entfernen Sie die alte Festplatte.

   Die Drive Map zeigt die neue Festplatte jetzt grün an.

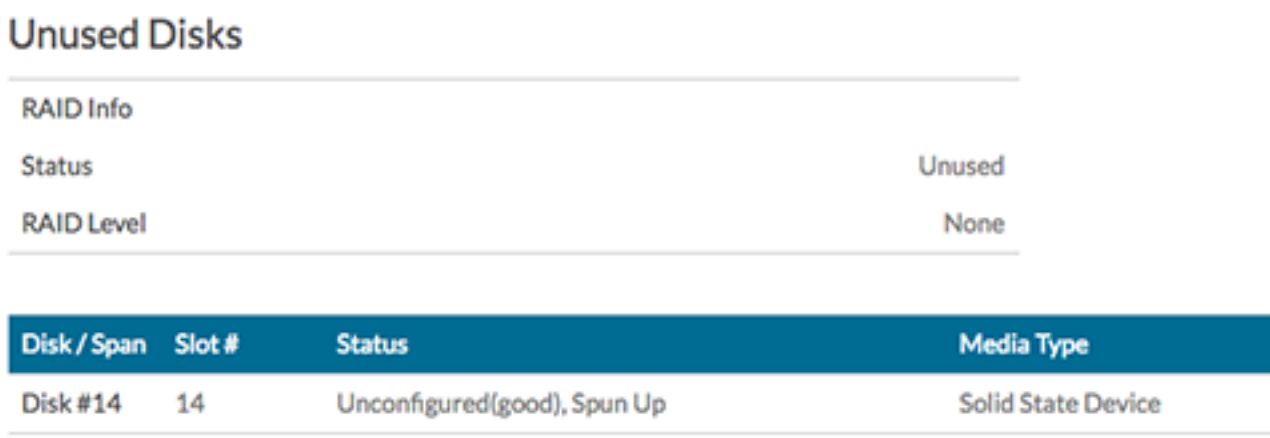



## Installieren Sie eine neue Paketerfassungsdiskette

1. In der Einstellungen der Appliance Abschnitt, klicken **Festplatten**.
   Wenn in der Laufwerksübersicht der Steckplatz, in dem die SSD installiert ist, rot angezeigt wird, müssen Sie die SSD austauschen.
2. Stecken Sie das SSD-Laufwerk in den Steckplatz, in dem die vorherige SSD installiert war, und warten Sie, bis die LED am Laufwerk grün leuchtet.
3. Aktualisieren Sie in den Administrationseinstellungen den Browser.

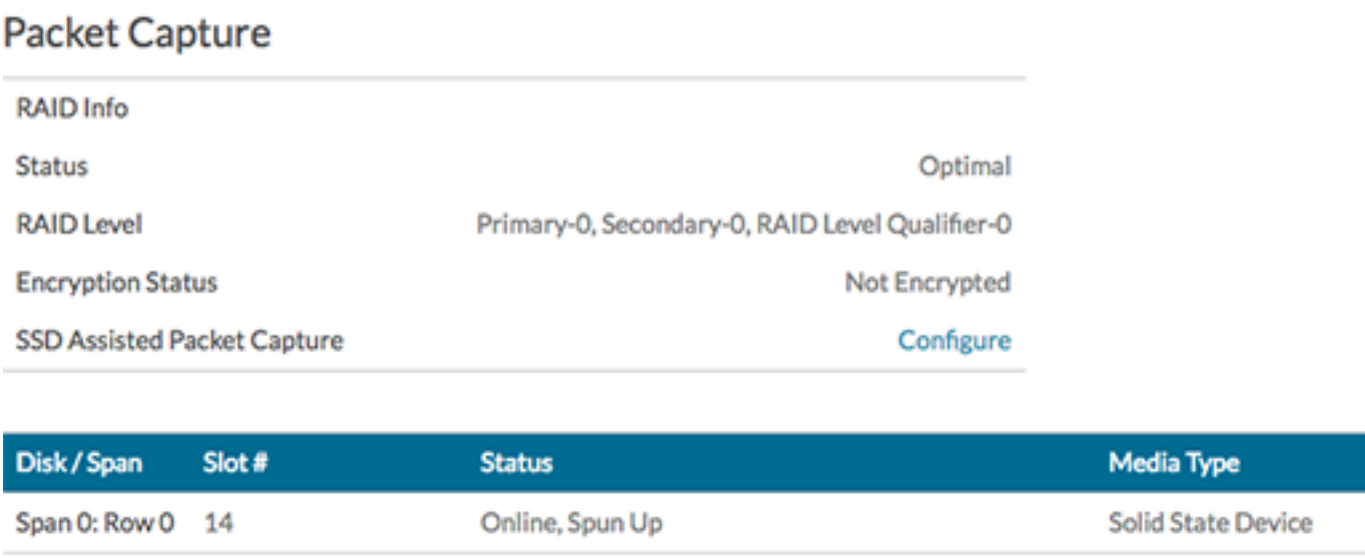
   In der Laufwerksübersicht wird der SSD-Steckplatz gelb angezeigt, da das Laufwerk nicht konfiguriert ist.

4. Neben SSD-gestützte Paketerfassung, klicken **Aktivieren**.




5. klicken **OK** um das Paketerfassungslaufwerk hinzuzufügen.

   Die Seite wird aktualisiert und die Drive Map zeigt die SSD grün an und der Status ändert sich zu `Online, Spun Up`.




**Hinweis:** Wenn das SSD-Laufwerk entfernt und wieder eingesetzt wird, können Sie es erneut aktivieren. Dieser Vorgang erfordert eine Neuformatierung der Festplatte, wodurch alle Daten gelöscht werden.

## Spitzname der Konsole

Standardmäßig ist Ihr ExtraHop Konsole wird auf angeschlossenen Sensoren anhand seines Hostnamens identifiziert. Sie können jedoch optional einen benutzerdefinierten Namen konfigurieren, um Ihre Konsole.

Wählen Sie aus den folgenden Optionen, um den Anzeigenamen zu konfigurieren:

- Wählen **Benutzerdefinierten Spitznamen anzeigen** und geben Sie den Namen in das Feld ein, das Sie für diese Konsole anzeigen möchten.
- Wählen **Hostnamen anzeigen** um den für diese Konsole konfigurierten Hostnamen anzuzeigen.

## Eine Meldung auf dem Anmeldebildschirm konfigurieren

Sie können dem Anmeldebildschirm eine benutzerdefinierte Nachricht hinzufügen, um Grafiken und Logos anzuzeigen und Benutzern Informationen wie Kennwortanforderungen, Richtlinienerklärungen, Support-Links oder Wartungsankündigungen zu übermitteln.

Im Folgenden finden Sie einige Überlegungen zur Anzeige einer benutzerdefinierten Meldung auf dem Anmeldebildschirm:

- Sie müssen über System- und Zugriffsadministration verfügen Benutzerrechte.
- Die Meldung auf dem Anmeldebildschirm gilt nur für die Konsole oder den Sensor, auf dem die Meldung konfiguriert ist.
- Die Meldung auf dem Anmeldebildschirm unterstützt Text und Grafiken in Markdown-Syntax, eine Auszeichnungssprache, die einfachen Text in HTML umwandelt.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann auf **Die gesamte Verwaltung**.
3. Aus dem Appliance-Einstellungen Abschnitt, klicken Sie **Meldung auf dem Anmeldebildschirm**.
4. Klicken Sie **Eine benutzerdefinierte Anmeldenachricht anzeigen**.
5. In der **Herausgeber** Bereich, formatieren Sie die gewünschte Nachricht und Grafiken und überprüfen Sie die Anzeigeausgabe im **Vorschau** Scheibe.
6. Klicken Sie **Änderungen speichern**.

# Plattenladen

Sie können vom ExtraHop-System geschriebene Datensätze auf Transaktionsebene an einen unterstützten Recordstore senden und diese Datensätze dann von der Datensatzseite oder der REST-API auf Ihrer Konsole abfragen und Sensoren.

**Erfahre mehr über ExtraHop Records**

- Konzepte aufzeichnen

## Datensätze von ExtraHop an Google BigQuery senden

Sie können Ihr ExtraHop-System so konfigurieren, dass Datensätze auf Transaktionsebene zur Langzeitspeicherung an einen Google BigQuery-Server gesendet werden, und diese Datensätze dann vom ExtraHop-System und der ExtraHop-REST-API abfragen. Datensätze in BigQuery-Datensatzspeichern laufen nach 90 Tagen ab.

**Bevor Sie beginnen**

- Auf jeder Konsole und allen angeschlossenen Sensoren muss dieselbe ExtraHop-Firmware-Version ausgeführt werden.
- Sie benötigen die BigQuery-Projekt-ID
- Sie benötigen die Anmeldeinformationsdatei (JSON) von Ihrem BigQuery-Dienstkonto. Für das Dienstkonto sind die Rollen BigQuery Data Editor, BigQuery Data Viewer und BigQuery User erforderlich.
- Für den Zugriff auf den cloudbasierten Recordstore, der in RevealX Standard Investigation enthalten ist, benötigen Sie Sensoren muss in der Lage sein, auf ausgehendes TCP 443 (HTTPS) auf diese vollständig qualifizierten 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.
- Wenn Sie die BigQuery-Recordstore-Einstellungen mit der Google Cloud-Workload-Identitätsverbundauthentifizierung konfigurieren möchten, benötigen Sie die Konfigurationsdatei aus Ihrem Workload-Identitätspool.

  **Hinweis:** Der Workload-Identitätsanbieter muss so eingerichtet sein, dass er als Antwort auf eine Anfrage mit Client-Anmeldeinformationen ein vollständig gültiges OIDC-ID-Token bereitstellt. Weitere Informationen zum Workload-Identitätsverbund finden Sie unter https://cloud.google.com/iam/docs/workload-identity-federation.

### BigQuery als Recordstore aktivieren

Führen Sie diesen Vorgang an allen angeschlossenen ExtraHop-Sensoren und der Konsole durch.

**Hinweis:** Alle Trigger, die für das Senden von Datensätzen konfiguriert sind `commitRecord` zu einem ExtraHop-Recordstore werden automatisch zu BigQuery umgeleitet. Es ist keine weitere Konfiguration erforderlich.

**Wichtig:** Wenn Ihr ExtraHop-System eine Konsole enthält, konfigurieren Sie alle Appliances mit denselben Recordstore-Einstellungen oder übertragen Sie die Verwaltung, um die Einstellungen von der Konsole aus zu verwalten.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken Sie **Plattenladen**.
3. Wählen **BigQuery als Recordstore aktivieren**.

   **Wichtig:** Wenn Sie von einem verbundenen ExtraHop-Recordstore zu BigQuery migrieren, können Sie nicht mehr auf die im Recordstore gespeicherten Datensätze zugreifen.
4. In der Projekt-ID Feld, geben Sie die ID für Ihr BigQuery-Projekt ein.

   Sie finden die Projekt-ID in der BigQuery API-Konsole.
5. In der JSON-Anmeldeinformationsdatei Feld, klicken **Wählen Sie Datei** und wählen Sie eine der folgenden Dateien aus:

   - Die Anmeldeinformationsdatei, die von Ihrem gespeichert wurde BigQuery-Dienstkonto.

     Informationen zum Erstellen eines Dienstkontos und zum Generieren eines Dienstkontoschlüssels finden Sie in der Google Cloud-Dokumentation.

     **Wichtig:** Erstellen Sie Ihr Dienstkonto mit den folgenden BigQuery-Rollen:

     - BigQuery-Dateneditor
     - BigQuery-Datenviewer
     - BigQuery-Benutzer
   - Die Konfigurationsdatei aus Ihrem Workload-Identitätspool.
6. Optional: Wenn Sie im vorherigen Schritt die Konfigurationsdatei aus Ihrem Workload-Identitätspool ausgewählt haben, wählen Sie **Authentifizieren Sie sich über den lokalen Identitätsanbieter für Workload Identity Federation** und geben Sie die Anmeldedaten Ihres Identitätsanbieters in die folgenden Felder ein:

   - **Token-URL**
   - **Kunden-ID**
   - **Geheimer Kunde**
7. Klicken Sie **Verbindung testen** um zu überprüfen, ob Ihr Sensor mit dem BigQuery-Server kommunizieren kann.
8. Klicken Sie **Speichern**.

Nachdem Ihre Konfiguration abgeschlossen ist, können Sie im ExtraHop-System nach gespeicherten Datensätzen abfragen, indem Sie auf **Rekorde**.

**Wichtig:** Ändern oder löschen Sie die Tabelle in BigQuery, in der die Datensätze gespeichert sind, nicht. Durch das Löschen der Tabelle werden alle gespeicherten Datensätze gelöscht.

## Recordstore-Einstellungen übertragen

Wenn du einen ExtraHop hast Konsole Wenn Sie an Ihre ExtraHop-Sensoren angeschlossen sind, können Sie die Recordstore-Einstellungen auf dem Sensor konfigurieren und verwalten oder die Verwaltung der Einstellungen an den Konsole. Durch die Übertragung und Verwaltung der Recordstore-Einstellungen auf der Konsole können Sie die Recordstore-Einstellungen für mehrere Sensoren auf dem neuesten Stand halten.

Die Recordstore-Einstellungen werden für verbundene Recordstores von Drittanbietern konfiguriert und gelten nicht für den ExtraHop-Recordstore.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.

2. In der Rekorde Abschnitt, klicken **Plattenladen**.
3. Aus dem **Recordstore-Einstellungen** Drop-down-Menü, wählen Sie die Konsole aus und klicken Sie dann auf **Inhaberschaft übertragen**.

   Wenn Sie sich später dazu entschließen, die Einstellungen auf der Sensor, wählen **dieser Sensor** aus dem Dropdownmenü Recordstore-Einstellungen und klicken Sie dann auf **Inhaberschaft übertragen**.

## Datensätze von ExtraHop an Splunk senden

Sie können das ExtraHop-System so konfigurieren, dass Datensätze auf Transaktionsebene zur Langzeitspeicherung an einen Splunk-Server gesendet werden, und diese Datensätze dann vom ExtraHop-System und der ExtraHop-REST-API abfragen.

Hier sind einige Überlegungen zum Senden von Datensätzen von ExtraHop an Splunk:

- Alle Trigger, die für das Senden von Datensätzen konfiguriert sind `commitRecord` zu einem Recordstore werden automatisch zum Splunk-Server umgeleitet. Es ist keine weitere Konfiguration erforderlich.
- Wenn Sie von einem verbundenen ExtraHop-Recordstore zu Splunk migrieren, können Sie nicht mehr auf die im Recordstore gespeicherten Datensätze zugreifen.
- Wenn Sie ExtraHop-Daten wie Metriken und Erkennungen in einer Splunk-Oberfläche anzeigen und analysieren möchten, konfigurieren Sie eine Splunk oder Splunk SOAR Integration.

### Splunk als Recordstore aktivieren

Führen Sie dieses Verfahren auf allen angeschlossenen ExtraHop-Systemen durch.

> **Wichtig:** Wenn Ihr ExtraHop-System eine Konsole oder RevealX 360 enthält, konfigurieren Sie alle Sensoren mit denselben Recordstore-Einstellungen oder Übertragungsmanagement, um die Einstellungen von der Konsole oder RevealX 360 aus zu verwalten.

**Bevor Sie beginnen**

- Auf jeder Konsole und allen angeschlossenen Sensoren muss dieselbe ExtraHop-Firmware-Version ausgeführt werden.
- Sie benötigen Version 7.0.3 oder höher von Splunk Enterprise und ein Benutzerkonto mit Administratorrechte.
- Sie müssen den Splunk HTTP Event Collector konfigurieren, bevor Ihr Splunk-Server ExtraHop-Datensätze empfangen kann. Sehen Sie die Splunk HTTP-Event-Collector Dokumentation für Anweisungen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken **Plattenladen**.
3. Wählen **Splunk als Recordstore aktivieren**.
4. In der Aufnahmeziel aufzeichnen Abschnitt, füllen Sie die folgenden Felder aus:

   • **Splunk Ingest Host:** Der Hostname oder die IP-Adresse Ihres Splunk-Servers.

   • **Port für HTTP-Event-Collector:** Der Port, über den der HTTP Event Collector Datensätze senden soll.

   • **HTTP-Event-Collector-Token:** Das Authentifizierungstoken, das Sie erstellt in Splunk für den HTTP Event Collector.
5. In der Ziel der Datensatzabfrage Abschnitt, füllen Sie die folgenden Felder aus:

   • **Splunk-Abfragehost:** Der Hostname oder die IP-Adresse Ihres Splunk-Servers.

   • **REST-API-Port:** Der Port, über den Datensatzabfragen gesendet werden sollen.

• **Methode der Authentifizierung:** Die Authentifizierungsmethode, die von Ihrer Splunk-Version abhängt.

Für Splunk-Versionen nach 7.3.0 wählen Sie **Authentifizieren Sie sich mit einem Token**, und fügen Sie dann Ihr Splunk-Authentifizierungstoken ein. Anweisungen zum Erstellen eines Authentifizierungstokens finden Sie in der Splunk-Dokumentation.

Für Splunk-Versionen vor 7.3.0 wählen Sie **Authentifizieren Sie sich mit Benutzername und Passwort**, und geben Sie dann Ihre Splunk-Anmeldeinformationen Anmeldedaten.

6. Löschen Sie das **Zertifikatsüberprüfung erforderlich** Kontrollkästchen, wenn für Ihre Verbindung kein gültiges TLS-Zertifikat erforderlich ist.

   **Hinweis:** Sichere Verbindungen zum Splunk-Server können verifiziert werden durch vertrauenswürdige Zertifikate die Sie in das ExtraHop-System hochladen.

7. In der Name des Indexes Feld, geben Sie den Namen des Splunk-Indexes ein , in dem Sie Datensätze speichern möchten.

   Der Standardindex auf Splunk heißt `main`Wir empfehlen jedoch, dass Sie einen separaten Index für Ihre ExtraHop-Datensätze erstellen und den Namen dieses Indexes eingeben. Anweisungen zum Erstellen eines Indexes finden Sie in der Splunk-Dokumentation.

8. (ExtraHop Sensor (nur) Klicken **Verbindung testen** um zu überprüfen , ob das ExtraHop-System Ihren Splunk-Server erreichen kann.

9. Klicken Sie **Speichern**.

Nachdem Ihre Konfiguration abgeschlossen ist, können Sie im ExtraHop-System nach gespeicherten Datensätzen abfragen, indem Sie auf **Rekorde** aus dem oberen Menü.

## Recordstore-Einstellungen übertragen

Wenn du einen ExtraHop hast Konsole Wenn Sie an Ihre ExtraHop-Sensoren angeschlossen sind, können Sie die Recordstore-Einstellungen auf dem Sensor konfigurieren und verwalten oder die Verwaltung der Einstellungen an den Konsole. Durch die Übertragung und Verwaltung der Recordstore-Einstellungen auf der Konsole können Sie die Recordstore-Einstellungen für mehrere Sensoren auf dem neuesten Stand halten.

Die Recordstore-Einstellungen werden für verbundene Recordstores von Drittanbietern konfiguriert und gelten nicht für den ExtraHop-Recordstore.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken **Plattenladen**.
3. Aus dem **Recordstore-Einstellungen** Drop-down-Menü, wählen Sie die Konsole aus und klicken Sie dann auf **Inhaberschaft übertragen**.

   Wenn Sie sich später dazu entschließen, die Einstellungen auf der Sensor, wählen **dieser Sensor** aus dem Dropdownmenü Recordstore-Einstellungen und klicken Sie dann auf **Inhaberschaft übertragen**.

# ExtraHop-Sensor-Einstellungen

Das ExtraHop-Sensor-Einstellungen Ein Abschnitt auf der ExtraHop-Konsole ermöglicht es Ihnen, eine Verbindung zu einem Paketsensor herzustellen und die angeschlossenen Sensoren zu verwalten.

Abhängig von Ihrer Netzwerkkonfiguration können Sie eine Verbindung vom Sensor (getunnelte Verbindung) oder von der Konsole (direkte Verbindung) herstellen.

- Wir empfehlen Ihnen, sich in den Administrationseinstellungen auf Ihrem Konsole und stellen Sie eine direkte Verbindung zum Sensor her. Direkte Verbindungen werden hergestellt von Konsole über HTTPS auf Port 443 und benötigen keinen speziellen Zugriff. Anweisungen dazu finden Sie unter Stellen Sie von einer RevealX Enterprise-Konsole aus eine Verbindung zu einem Sensor her.
- Wenn dein Sensor befindet sich hinter einer Firewall, daraus können Sie eine SSH-Tunnelverbindung herstellen Sensor zu deinem Konsole. Anweisungen dazu finden Sie unter Stellen Sie von einem Sensor aus eine Verbindung zu einer RevealX Enterprise-Konsole her.

## Stellen Sie von einer RevealX Enterprise-Konsole aus eine Verbindung zu einem Sensor her

Du kannst mehrere ExtraHop verwalten Sensoren von einem RevealX Enterprise Konsole. Nachdem Sie das angeschlossen haben Sensoren, können Sie das ansehen und bearbeiten Sensor Eigenschaften, weisen Sie einen Spitznamen zu, aktualisieren Sie die Firmware, überprüfen Sie den Lizenzstatus und erstellen Sie ein Diagnose-Support-Paket.

Das Konsole stellt über HTTPS auf Port 443 eine direkte Verbindung zum Sensor her. Wenn es aufgrund von Firewalleinschränkungen in Ihrer Netzwerkumgebung nicht möglich ist, eine direkte Verbindung herzustellen, können Sie eine Verbindung zum Konsole durch eine getunnelte Verbindung vom ExtraHop-Sensor.

**Video:** Sehen Sie sich die entsprechende Schulung an: Eine Appliance mit einer RevealX Enterprise Console (ECA) verbinden

**Bevor Sie beginnen**
Sie können nur eine Verbindung herstellen zu einem Sensor die für dieselbe Systemedition lizenziert ist wie die Konsole. Zum Beispiel ein Konsole auf RevealX Enterprise kann nur eine Verbindung herstellen zu Sensoren auf RevealX Enterprise.

**Wichtig:** Wir empfehlen dringend Konfiguration eines eindeutigen Hostnamens. Wenn sich die System-IP-Adresse ändert, kann die ExtraHop-Konsole die Verbindung zum System einfach über den Hostnamen wiederherstellen.

### Generieren Sie ein Token auf dem Sensor

Generieren Sie ein Token auf dem Sensor, bevor Sie mit dem Verbindungsvorgang auf der Konsole beginnen.

1. Loggen Sie sich in die Administrationseinstellungen des Sensor ein.
2. In der ExtraHop-Befehlseinstellungen Abschnitt, klicken **Token generieren**.
3. klicken **Token generieren**.
4. Kopieren Sie das Token und fahren Sie mit dem nächsten Verfahren fort.

### Verbinden Sie die Konsole und die Sensoren

1. Melden Sie sich bei den Administrationseinstellungen auf der Konsole an.
2. In der Verwaltung verbundener Appliances Abschnitt, klicken **Sensoren verwalten**.

3. klicken **ExtraHop-Sensor**.
4. klicken **Sensor anschließen**.
5. In der Gastgeber Feld, geben Sie den Hostnamen oder die IP-Adresse des Sensor.
6. Klicken Sie **Verbinde**.
7. In der Token von ExtraHop Sensor Feld, geben Sie das Token ein oder fügen Sie es ein, das Sie auf dem Sensor generiert haben.
8. Geben Sie im Feld Sensor-Nickname (empfohlen) einen benutzerfreundlichen Namen für das ExtraHop-System ein.

   Wenn kein Spitzname eingegeben wird, wird das System durch den Hostnamen identifiziert.
9. Optional: Wählen **Konfiguration zurücksetzen** um bestehende Systemanpassungen wie Gerätegruppen, Alarme und Trigger aus dem ExtraHop-System zu entfernen.

   Gesammelte Messwerte wie Aufnahmen und Geräte werden nicht entfernt.
10. Klicken Sie **Verbinde**.

## Paketsensoren verwalten

Von der ExtraHop-Konsole aus können Sie die angeschlossenen Sensoren anzeigen und einige Verwaltungsaufgaben verwalten.

Markieren Sie das Kontrollkästchen für einen oder mehrere angeschlossene Sensoren. Wählen Sie dann eine der folgenden Verwaltungsaufgaben aus.

- Klicken Sie **Lizenz überprüfen** um eine Verbindung zum ExtraHop-Lizenzierungsserver herzustellen und den neuesten Status für die ausgewählten Sensoren abzurufen. Wenn Ihre Command-Appliance nicht auf Daten von einem angeschlossenen Sensor zugreifen kann, ist die Lizenz möglicherweise ungültig.
- Klicken Sie **Unterstützungsskript ausführen** und wählen Sie dann aus den folgenden Optionen:
  - Klicken Sie **Standard-Support-Skript ausführen** um Informationen über die ausgewählten Sensoren zu sammeln. Sie können diese Diagnosedatei zur Analyse an den ExtraHop Support senden.
  - Klicken Sie **Benutzerdefiniertes Support-Skript ausführen** um eine Datei vom ExtraHop Support hochzuladen, die kleine Systemänderungen oder -verbesserungen enthält.
- Klicken Sie **Firmware aktualisieren** um den ausgewählten Sensor zu aktualisieren. Sie können eine URL zur Firmware auf dem Kundenportal Website oder laden Sie die Firmware-Datei von Ihrem Computer hoch. Bei beiden Optionen empfehlen wir dringend, die Firmware zu lesen Versionshinweise und die Anleitung zum Firmware-Upgrade.
- Klicken Sie **Deaktiviert** oder **Aktiviere** um die Verbindung zwischen Sensoren und Konsolen vorübergehend zu ändern. Wenn diese Verbindung deaktiviert ist, zeigt die Command-Appliance den Sensor nicht an und kann nicht auf die Sensordaten zugreifen.
- Klicken Sie **Gerät entfernen** um ausgewählte Sensoren dauerhaft abzuschalten.

# ExtraHop Recordstore-Einstellungen

Dieser Abschnitt enthält Konfigurationseinstellungen für den ExtraHop-Recordstore.

**Hinweis:** Dieser Abschnitt bezieht sich nur auf RevealX Enterprise. Sie müssen keine Sensoren mit dem cloudbasierten Recordstore verbinden, der in RevealX 360 enthalten ist.

## Verbinden Sie den EXA 5200 mit dem ExtraHop-System

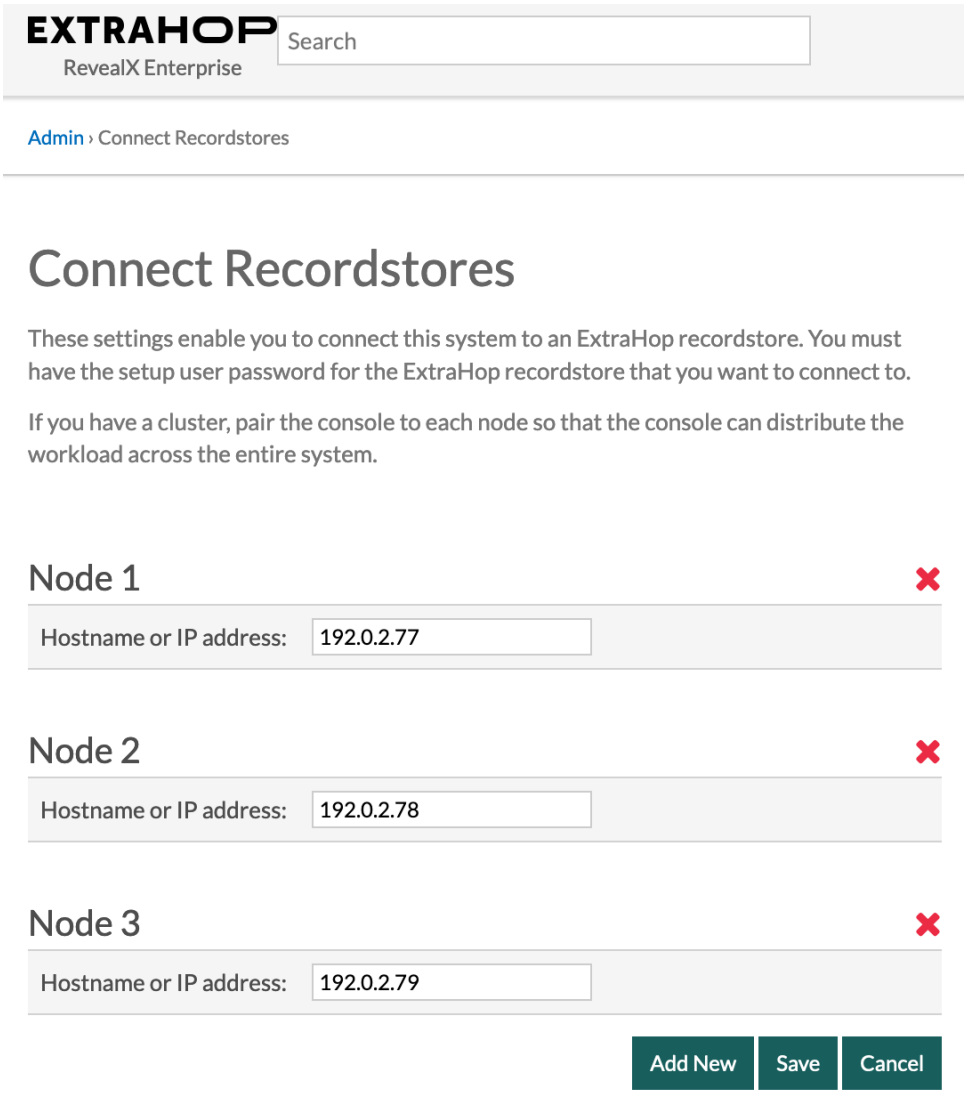
Nachdem Sie einen EXA 5200-Recordstore bereitgestellt haben, müssen Sie eine Verbindung von allen ExtraHop aus herstellen Sensoren und die Konsole zu den Recordstore-Knoten, bevor Sie nach gespeicherten Datensätzen abfragen können.

**Wichtig:** Wenn Ihr Recordstore-Cluster konfiguriert ist mit Knoten nur für Manager, Sie müssen nur die Sensoren und die Konsole mit den reinen Datenknoten im Recordstore-Cluster verbinden. Stellen Sie keine Verbindung zu den Knoten nur für Manager her, da Knoten nur für Manager keine Datensätze empfangen.

1. Loggen Sie sich in die Administrationseinstellungen auf der Konsole oder Sensor.

   **Hinweis:** Wenn die Recordstore-Verbindungen von einer Konsole aus verwaltet werden, müssen Sie dieses Verfahren von der Konsole aus und nicht von jedem Sensor aus ausführen.
2. In der ExtraHop Recordstore-Einstellungen Abschnitt, klicken **Synchronisiere Recordstores**.
3. Klicken Sie **Neues hinzufügen**.
4. In der Knoten 1 Feld, geben Sie den Hostnamen oder die IP-Adresse eines beliebigen Recordstore im Recordstore-Cluster ein.

   **Hinweis:** Wenn der Cluster auch Knoten nur für Manager enthält, fügen Sie nur die Knoten hinzu, die nur Daten enthalten.
5. Klicken Sie für jeden weiteren Recordstore-Knoten im Cluster auf **Neues hinzufügen** und geben Sie den individuellen Hostnamen oder die IP-Adresse in das entsprechende Feld ein Knoten Feld.




6. Klicken Sie **Speichern**.
7. Vergewissern Sie sich, dass der Fingerabdruck auf dieser Seite mit dem Fingerabdruck von Knoten 1 des Cluster übereinstimmt.
8. In der Recordstore-Setup-Passwort Feld, geben Sie das Passwort für Node 1 ein `setup` Benutzerkonto.
9. Klicken Sie **Verbinden**.
10. Wenn die Cluster-Einstellungen gespeichert sind, klicken Sie auf **Erledigt**.

**Nächste Schritte**
Wenn die Recordstore-Einstellungen von Sensoren und nicht von einer angeschlossenen Konsole verwaltet werden, wiederholen Sie diesen Vorgang auf der Konsole.

## Trennen Sie den Recordstore

Um die Aufnahme von Datensätzen in den Recordstore zu stoppen, trennen Sie alle Recordstore-Knoten vom ExtraHop Konsole und Sensoren.

**Hinweis:** Wenn Recordstore-Verbindungen von einer Konsole verwaltet werden, können Sie dieses Verfahren nur auf der Konsole ausführen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der ExtraHop Recordstore-Einstellungen Abschnitt, klicken **Synchronisiere Recordstores**.
3. Klicken Sie auf das rote **X** neben jedem Knoten im Recordstore-Cluster.


4. Klicken Sie **Speichern**.

## Verbinden Sie den EXA 5300 mit dem ExtraHop-System

Nachdem Sie einen EXA 5300-Recordstore bereitgestellt haben, müssen Sie eine Verbindung von allen ExtraHop aus herstellen Sensoren und die Konsole zu den Recordstore-Knoten, bevor Sie nach gespeicherten Datensätzen abfragen können.

Hier sind einige wichtige Überlegungen zu Recordstore-Verbindungen:

- Sie können Sensoren nicht an mehr als einen EXA 5300 anschließen, aber Sie können mehrere EXA 5300 an eine einzige Konsole anschließen.
- Wenn ein Sensor oder eine Konsole an einen EXA 5200 oder EXA 5100v angeschlossen ist, müssen Sie die Verbindung zum EXA 5200 oder EXA 5100v trennen , bevor Sie eine Verbindung zu einem EXA 5300 herstellen können.

### Recordstore-Partitionen

Der EXA 5300 organisiert Daten nach Tabellenpartitionen. Das Recordstore-Status  Seite enthält eine Zusammenfassung der Partition Abschnitt, der alle Partitionen auflistet, einschließlich der Daten für eine bestimmte Tabelle für ein ausgewähltes Datum.

Ältere Datensätze werden automatisch gelöscht, wenn die Festplatte voll ist. Sie können Partitionen jedoch bei Bedarf auch manuell aus dem System löschen. Auf dem Recordstore-Status Seite, wählen Sie eine oder mehrere Partitionen aus und klicken Sie auf **Ausgewähltes löschen**. Wenn Sie eine Partition löschen, werden bei der Suche nach Datensätzen keine Datensätze aus dieser Partition für dieses Datum zurückgegeben. Das Löschen von Partitionen wird im Audit-Log aufgezeichnet.

### Generieren Sie ein Token auf dem EXA 5300

Der EXA 5300 Recordstore stellt eine Verbindung zu einem ExtraHop her Konsole mit tokenbasierter Authentifizierung.

Generieren Sie ein Token im EXA 5300-Recordstore, bevor Sie den Verbindungsvorgang auf dem beginnen Konsole.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Verwaltung verbundener Appliances Abschnitt, unter Recordstore-Einstellungen, klicken Sie **Token generieren**.
3. Klicken Sie **Token generieren**.
4. Kopieren Sie das Token und fahren Sie mit dem nächsten Verfahren fort.

### Den EXA 5300 an eine Konsole oder einen Sensor anschließen

Verbinden Sie den EXA 5300 Recordstore mit einem ExtraHop Konsole oder Sensor.

**Wichtig:** EXA 5300 Recordstore-Verbindungen können nicht von einer Konsole aus verwaltet werden, daher müssen Sie dieses Verfahren sowohl von der Konsole als auch vom Sensor aus ausführen.

1. Loggen Sie sich in die Administrationseinstellungen auf der Konsole oder Sensor durch `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Recordstore-Einstellungen Abschnitt, klicken Sie **Synchronisiere Recordstores**.
3. Klicken Sie **Neues hinzufügen**.
4. In der Knoten 1 Feld, geben Sie den Hostnamen oder die IP-Adresse eines beliebigen Recordstore im Recordstore-Cluster ein.
5. Klicken Sie **Speichern**.
6. In der Token von ExtraHop Recordstore Geben Sie in dieses Feld das Token ein, das Sie auf dem EXA 5300 generiert haben, oder fügen Sie es ein.
7. Klicken Sie **Verbinden**.
8. Wenn die Recordstore-Einstellungen gespeichert sind, klicken Sie auf **Erledigt**.

### Datensatzaufnahme in einem Recordstore konfigurieren

Konfigurieren Sie die Einstellungen für die Aufnahme von Datensätzen in einem ExtraHop-Recordstore. Die Aufnahme von Datensätzen muss nur aktiviert werden, wenn Sie diese Einstellungen zuvor deaktiviert haben.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Die Einstellung für die Aufnahme von Datensätzen verwalten:
   - Für den EXA 5200, in der Recordstore-Einstellungen Abschnitt, klicken Sie **Cluster-Datenmanagement**.
   - Für den EXA 5300, in der Recordstore-Einstellungen Abschnitt, klicken Sie **Verwaltung der Daten**.
3. In der Aufnahme aufzeichnen Abschnitt, klicken Sie **Record Ingest aktivieren**.
4. Klicken Sie **Speichern**.

### Trennen Sie den Recordstore

Um die Aufnahme von Datensätzen in den Recordstore zu stoppen, trennen Sie alle Recordstore-Knoten vom ExtraHop Konsole und Sensoren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der ExtraHop Recordstore-Einstellungen Abschnitt, klicken **Synchronisiere Recordstores**.
3. Klicken Sie auf das rote **X** neben jedem Knoten im Recordstore-Cluster.


4. Klicken Sie **Speichern**.

## Plattenläden verwalten

Von der ExtraHop-Konsole aus können Sie verbundene Recordstores anzeigen und einige administrative Aufgaben verwalten.

Sehen Sie sich Informationen über verbundene Recordstores als einzelne Appliances oder als Teil eines Cluster an.

- Klicken Sie **Recordstore-Cluster** im Feld Name, um die Cluster-Eigenschaften zu öffnen. Sie können einen benutzerdefinierten Spitznamen für den Recordstore hinzufügen und die Cluster-ID anzeigen.
- Klicken Sie auf einen beliebigen Knotennamen, um die Knoteneigenschaften zu öffnen. Durch Anklicken **Admin-UI öffnen**, können Sie auf die Administrationseinstellungen für den jeweiligen Recordstore zugreifen.
- Zeigen Sie das Datum und die Uhrzeit an, zu denen die Appliance zu dieser Konsole hinzugefügt wurde.
- Sehen Sie sich den Lizenzstatus für Ihre Appliances an.
- Sehen Sie sich die Liste der Aktionen an, die Sie auf dieser Appliance ausführen können.
- In der Spalte Job können Sie den Status aller laufenden Support-Skripts einsehen.

Wählen Sie den Recordstore-Cluster oder einen einzelnen Knoten im Cluster aus, indem Sie auf einen leeren Bereich in der Tabelle klicken, und wählen Sie dann eine der folgenden Verwaltungsaufgaben aus.

- Klicken Sie **Unterstützungsskript ausführen** und wählen Sie dann aus den folgenden Optionen:
  - Wählen **Standard-Support-Skript ausführen** um Informationen über den ausgewählten Recordstore zu sammeln. Sie können diese Diagnosedatei zur Analyse an den ExtraHop Support senden.
  - Wählen **Benutzerdefiniertes Support-Skript ausführen** um eine Datei vom ExtraHop Support hochzuladen, die kleine Systemänderungen oder -verbesserungen enthält.
- Klicken Sie **Cluster entfernen** um den ausgewählten Recordstore dauerhaft zu trennen. Diese Option verhindert nur, dass Sie die Verwaltungsaufgaben auf dieser Seite von der Konsole aus ausführen. Der Recordstore bleibt mit Ihrem Paketsensor verbunden und sammelt weiterhin Datensätze.

## Flow-Aufzeichnungen sammeln

Sie können automatisch alle Datenflussdatensätze erfassen und speichern, bei denen es sich um Kommunikation auf Netzwerkebene zwischen zwei Geräten über ein IP-Protokoll handelt. Wenn Sie diese Einstellung aktivieren, aber keine IP-Adressen oder Portbereiche hinzufügen, werden alle erkannten Flussdatensätze erfasst. Die Konfiguration von Flow-Datensätzen für die automatische Erfassung ist ziemlich einfach und kann eine gute Möglichkeit sein, die Konnektivität zu Ihrem Recordstore zu testen.

**Bevor Sie beginnen**
Sie müssen Zugriff auf ein ExtraHop-System haben mit System- und Zugriffsadministrationsrechte.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken Sie **Automatische Flussaufzeichnungen**.
3. Wählen Sie die **Aktiviert** Ankreuzfeld.
4. In der Intervall veröffentlichen Feld, geben Sie eine Zahl zwischen 60 und 21600 ein.

   Dieser Wert bestimmt, wie oft Datensätze aus einem aktiven Fluss an den Recordstore gesendet werden. Der Standardwert ist 1800 Sekunden.
5. In der IP Adresse Feld, geben Sie eine einzelne IP-Adresse oder einen IP-Adressbereich im IPv4-, IPv6- oder CIDR-Format ein.
6. Klicken Sie auf das grüne Plus (**+**) Symbol.

   Sie können einen Eintrag entfernen, indem Sie auf das rote Löschen klicken (**X**) Symbol.
7. In der Portbereiche Feld, geben Sie einen einzelnen Port oder Portbereich ein, und klicken Sie dann auf das grüne Plus (**+**) Symbol.
8. Klicken Sie **Speichern**.

   Flow-Datensätze, die Ihre Kriterien erfüllen, werden jetzt automatisch an Ihren konfigurierten Recordstore gesendet. Warten Sie ein paar Minuten, bis die Aufzeichnungen gesammelt sind.

9. Klicken Sie im ExtraHop-System auf **Rekorde** aus dem Hauptmenü, und klicken Sie dann auf **Aufzeichnungen ansehen** um eine Abfrage zu starten.

   Wenn Sie keine Aufzeichnungen sehen, warten Sie ein paar Minuten und versuchen Sie es erneut. Wenn nach fünf Minuten keine Aufzeichnungen angezeigt werden, überprüfen Sie Ihre Konfiguration oder wenden Sie sich an ExtraHop-Unterstützung.

## Status des ExtraHop Recordstore

Wenn Sie einen ExtraHop-Plattenladen Recordstore Ihrem verbunden haben Sensor oder Konsole, können Sie auf Informationen über den Recordstore zugreifen.

Die Tabelle auf dieser Seite enthält die folgenden Informationen zu allen verbundenen Datensatzspeichern.

**Aktivität seit**

Zeigt die Zeitstempel als die Plattensammlung begann. Dieser Wert wird automatisch alle 24 Stunden zurückgesetzt.

**Datensatz gesendet**

Zeigt die Anzahl der Datensätze an, die von einem an den Recordstore gesendet wurden Sensor.

**I/O-Fehler**

Zeigt die Anzahl der generierten Fehler an.

**Warteschlange voll (Datensätze gelöscht)**

Zeigt die Anzahl der gelöschten Datensätze an, wenn Datensätze schneller erstellt werden, als sie an den Recordstore gesendet werden können.

# ExtraHop Packetstore-Einstellungen

ExtraHop Packetstores sammeln und speichern kontinuierlich Rohpaketdaten von Ihrem Sensoren.

## Einen Packetstore mit RevealX Enterprise verbinden

Bevor Sie Pakete auf RevealX Enterprise-Systemen abfragen können, müssen Sie einen bereitgestellten Packetstore haben und Sie müssen den Konsole und alle Sensoren zu deinem Packetstore.

**Hinweis:** Informationen zum Anschließen von Sensoren an die Konsole eines RevealX360-Systems finden Sie unter Einen Sensor an RevealX 360 anschließen

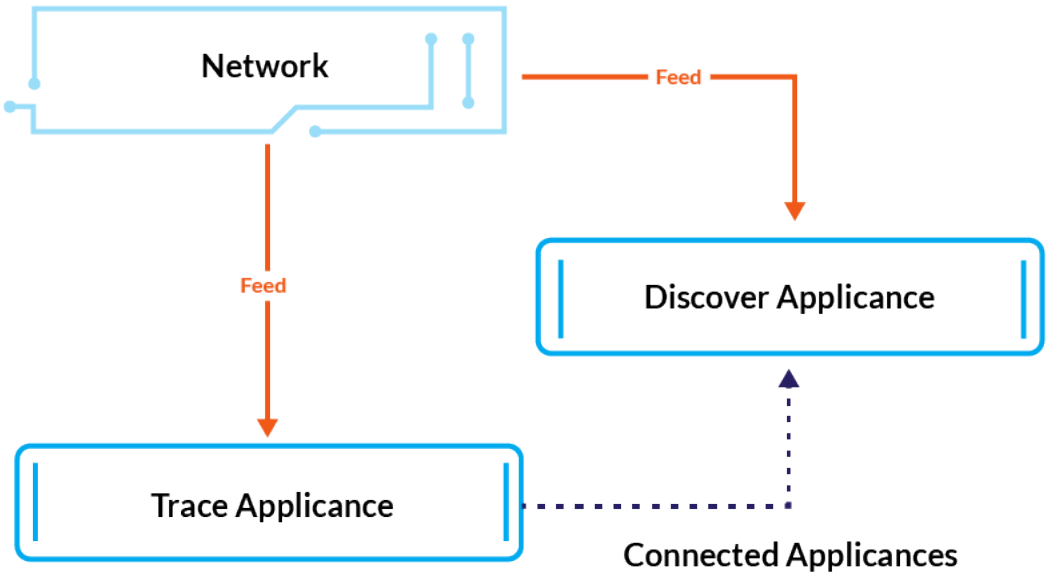



**Abbildung 1: An einen Sensor angeschlossen**

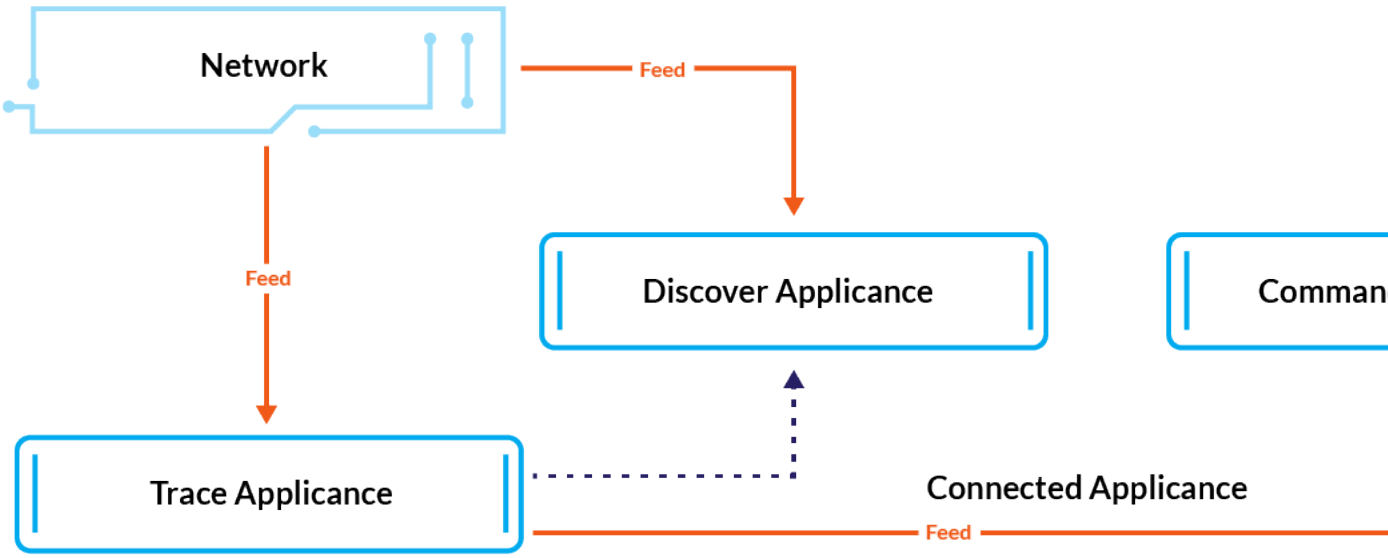



**Abbildung 2: Mit Sensor und Konsole verbunden**

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Packetstore-Einstellungen Abschnitt, klicken Sie **Synchronisiere Packetstores**.
3. In der Hostname des Paketspeichers Feld, geben Sie den Hostnamen oder die IP-Adresse des Packetstore ein.
4. Klicken Sie **Paar**.
5. Beachten Sie die Informationen in der Fingerabdruck Feld, und überprüfen Sie dann, ob der auf dieser Seite aufgeführte Fingerabdruck mit dem Packetstore-Fingerabdruck auf der Seite Fingerprint in den Administrationseinstellungen des Packetstore übereinstimmt.
6. In der Packetstore-Setup-Passwort Feld, geben Sie das Passwort des Packetstore ein `setup` Nutzer.
7. Klicken Sie **Verbinden**.
8. Um weitere Paketspeicher zu verbinden, wiederholen Sie die Schritte 2 bis 7.

   **Hinweis:** Sie können einen Sensor an zwanzig oder weniger Packetstores anschließen, und Sie können eine Konsole an fünfzig oder weniger Packetstores anschließen.
9. Wenn du eine hast Konsole, melden Sie sich in den Administrationseinstellungen auf der Konsole und wiederholen Sie die Schritte 3 bis 7 für alle Packetstores.

## Paketspeicher verwalten

Von der ExtraHop-Konsole aus können Sie verbundene Paketspeicher anzeigen und einige Verwaltungsaufgaben verwalten.

Zeigt Informationen über verbundene Packetstores an.

- Klicken Sie **Packetstore-Cluster** im Feld Name, um die Cluster-Eigenschaften zu öffnen. Sie können einen benutzerdefinierten Spitznamen für den Packetstore hinzufügen und die Cluster-ID anzeigen.
- Klicken Sie auf ein beliebiges Gerät, um die Eigenschaften anzuzeigen. Durch Anklicken **Admin-UI öffnen**, können Sie auf die Administrationseinstellungen für den jeweiligen Packetstore zugreifen.
- Zeigen Sie das Datum und die Uhrzeit an, zu denen die Appliance zu dieser Command-Appliance hinzugefügt wurde.
- Sehen Sie sich den Lizenzstatus für Ihre Appliances an.
- Sehen Sie sich die Liste der Aktionen an, die Sie auf dieser Appliance ausführen können.

- In der Spalte Job können Sie den Status aller laufenden Support-Skripts einsehen.

Wählen Sie einen Packetstore aus. Wählen Sie dann eine der folgenden Verwaltungsaufgaben aus.

- Klicken Sie **Unterstützungsskript ausführen** und wählen Sie dann aus den folgenden Optionen:
  - Klicken Sie **Standard-Support-Skript ausführen** um Informationen über den ausgewählten Packetstore zu sammeln. Sie können diese Diagnosedatei zur Analyse an den ExtraHop Support senden.
  - Klicken Sie **Benutzerdefiniertes Support-Skript ausführen** um eine Datei vom ExtraHop Support hochzuladen, die kleine Systemänderungen oder -verbesserungen enthält.
- Klicken Sie **Firmware aktualisieren** um den ausgewählten Packetstore zu aktualisieren. Sie können eine URL zur Firmware auf dem Kundenportal Website oder laden Sie die Firmware-Datei von Ihrem Computer hoch. Bei beiden Optionen empfehlen wir Ihnen dringend, die Firmware zu lesen Versionshinweise und die Anleitung zum Firmware-Upgrade.
- Klicken Sie **Gerät entfernen** um den ausgewählten Packetstore dauerhaft zu trennen. Diese Option verhindert nur, dass Sie die Verwaltungsaufgaben auf dieser Seite von der Konsole aus ausführen. Der Packetstore bleibt mit Ihrem Paketsensor verbunden und sammelt weiterhin Pakete.

# Anlage

## Allgemeine Akronyme

Die folgenden gängigen Akronyme für Computer- und Netzwerkprotokolle werden in diesem Handbuch verwendet.

| Akronym | Vollständiger Name |
|---|---|
| AAA | Authentifizierung, Autorisierung und Abrechnung |
| AMF | Format der Aktionsnachricht |
| CIFS | Gemeinsames Internet-Dateisystem |
| CLI | Befehlszeilenschnittstelle |
| CPU | Zentrale Verarbeitungseinheit |
| DB | Datenbank |
| DHCP | Dynamisches Host-Konfigurationsprotokoll |
| DNS | Domainnamensystem |
| ERSPAN | Gekapselter Remote-Switching-Port-Analysator |
| FIX | Austausch von Finanzinformationen |
| FTP | FTP |
| HTTP | Hypertext-Übertragungsprotokoll |
| IBMMQ | Nachrichtenorientierte IBM Middleware |
| ICA | Unabhängige Computerarchitektur |
| IP | Internet-Protokoll |
| iSCSI | Internetschnittstelle für kleine Computersysteme |
| L2 | Ebene 2 |
| L3 | Schicht 3 |
| L7 | Schicht 7 |
| LDAP | Leichtes Verzeichniszugriffsprotokoll |
| MAC | Medienzugriffskontrolle |
| MIB | Informationsbasis für das Management |
| NFS | NFS |
| NVRAM | Nichtflüchtiger Direktzugriffsspeicher |
| RADIUS | Benutzerdienst für Fernauthentifizierung mit Einwahl |
| RPC | Prozeduraufruf per Fernzugriff |
| RPCAP | Paketerfassung aus der Ferne |
| RSS | Größe des Resident-Sets |

| Akronym | Vollständiger Name |
|---|---|
| SMPP | Kurznachricht Peer-to-Peer-Protokoll |
| SMTP | Einfaches Nachrichtenübertragungsprotokoll |
| SNMP | Einfaches Netzwerkmanagement-Protokoll |
| SPAN | Analysator für geschaltete Anschlüsse |
| SSD | Solid-State-Laufwerk |
| SSH | Sichere Shell |
| SSL | Sichere Socket-Schicht |
| TACACS+ | Zutrittskontrollsystem für Terminalzugriffssteuerungen Plus |
| TCP | TCP |
| TLS | Sicherheit auf Transportebene |
| UI | Benutzerschnittstelle |
| VLAN | VLAN |
| VM | Virtuelle Maschine |

## Cisco NetFlow-Geräte konfigurieren

Im Folgenden finden Sie Beispiele für die grundlegende Cisco-Router-Konfiguration für NetFlow. NetFlow wird pro Schnittstelle konfiguriert. Wenn NetFlow auf der Schnittstelle konfiguriert ist, IP-Paket Fluss Informationen werden auf den ExtraHop-Sensor exportiert.

**Wichtig:** NetFlow nutzt den SNMP ifIndex-Wert, um Eingangs- und Ausgangsschnittstelleninformationen in Flow-Datensätzen darzustellen. Um die Konsistenz der Schnittstellenberichte zu gewährleisten, aktivieren Sie die SNMP ifIndex-Persistenz auf Geräten, die NetFlow an den Sensor senden. Weitere Informationen zur Aktivierung der SNMP ifIndex-Persistenz auf Ihren Netzwerkgeräten finden Sie in der Konfigurationsanleitung des Geräteherstellers.

Weitere Informationen zur Konfiguration von NetFlow auf Cisco Switches finden Sie in der Dokumentation zu Ihrem Cisco Router oder auf der Cisco-Website unter www.cisco.com.

### Konfigurieren Sie einen Exporter auf dem Cisco Nexus Switch

Definieren Sie einen Flow-Exporter, indem Sie das Exportformat angeben, Protokollund Ziel.

Melden Sie sich bei der Switch-Befehlszeilenschnittstelle an und führen Sie die folgenden Befehle aus:

a) Rufen Sie den globalen Konfigurationsmodus auf:

```
config t
```

b) Erstellen Sie einen Flow-Exporter und wechseln Sie in den Flow-Exporter-Konfigurationsmodus.

```
flow exporter <name>
```

Zum Beispiel:

```
flow exporter Netflow-Exporter-1
```

c) (Optional) Geben Sie eine Beschreibung ein:

```
description <string>
```

Zum Beispiel:

```
description Production-Netflow-Exporter
```

d) Legen Sie die IPv4- oder IPv6-Zieladresse für den Exporter fest.

```
destination <eda_mgmt_ip_address>
```

Zum Beispiel:

```
destination 192.168.11.2
```

e) Geben Sie die Schnittstelle an, die benötigt wird, um das zu erreichen NetFlow Collector am konfigurierten Ziel.

```
source <interface_type> <number>
```

Zum Beispiel:

```
source ethernet 2/2
```

f) Geben Sie die NetFlow-Exportversion an:

```
version 9
```

### Konfiguration von Cisco Switches über Cisco IOS CLI

1. Melden Sie sich bei der Cisco IOS-Befehlszeilenschnittstelle an und führen Sie die folgenden Befehle aus.
2. Rufen Sie den globalen Konfigurationsmodus auf:

```
config t
```

3. Geben Sie die Schnittstelle an und wechseln Sie in den Schnittstellenkonfigurationsmodus.
   - Cisco Router der Serie 7500:

```
interface <type> <slot>/<port-adapter>/<port>
```

Zum Beispiel:

```
interface fastethernet 0/1/0
```

   - Cisco Router der Serie 7200:

```
interface <type> <slot>/<port>
```

Zum Beispiel:

```
interface fastethernet 0/1
```

4. NetFlow aktivieren:

```
ip route-cache flow
```

5. NetFlow-Statistiken exportieren:

```
ip flow-export <ip-address> <udp-port> version 5
```

Wo *<ip-address>* ist die Management + Flow Target-Schnittstelle auf dem ExtraHop-System und *<udp-port>* ist die konfigurierte Collector-UDP-Portnummer.