# ExtraHop 25.2
# ExtraHop Explore Leitfaden für die Admin-Benutzeroberfläche

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 die ExtraHop Explore Admin UI

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

Darüber hinaus bietet dieses Handbuch einen Überblick über die globale Navigation und Informationen zu den Steuerelementen, Feldern und Optionen, die in den Administrationseinstellungen von Explore verfügbar sind.

Nachdem Sie Ihren ExtraHop Recordstore bereitgestellt haben, sehen Sie sich die Erkunden Sie die Checkliste nach der Bereitstellung .

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

## Unterstützte Browser

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

- Firefox
- Google Chrome
- Microsoft Edge
- Safari

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

# Status und Diagnose

Die Status und Diagnose Auf dieser Seite werden Metriken und Protokolldaten zum aktuellen Status der Explore-Appliance angezeigt und Systemadministratoren können den allgemeinen Systemzustand einsehen.

**Gesundheit**

Bietet Metriken zur Anzeige der Betriebseffizienz der Explore-Appliance.

**Audit-Protokoll**

Ermöglicht es Ihnen, Daten zur Ereignisprotokollierung anzuzeigen und die Syslog-Einstellungen zu ändern

**Fingerabdruck**

Bietet die einzigartige Hardware Fingerabdruck für die Explore-Appliance.

**Unterstützungsskripte**

Ermöglicht das Hochladen und Ausführen von Support-Skripten.

**Cluster-Status erkunden**

Stellt Statusinformationen über den Cluster bereit, einschließlich Indizes.

## Gesundheit

Die Seite Health bietet eine Sammlung von Metriken, mit denen Sie den Betrieb der Explore-Appliance überprüfen können.

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

**System**

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

**CPU-Benutzer**

Gibt den Prozentsatz der CPU-Auslastung an, der dem Benutzer der Explore-Appliance zugeordnet ist

**CPU-System**

Gibt den Prozentsatz der CPU-Auslastung an, der der Explore-Appliance zugeordnet ist.

**CPU im Leerlauf**

Identifiziert den Prozentsatz der CPU-Leerlaufzeit, der der Explore-Appliance zugeordnet ist.

**CPU-IO**

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

**Status des Dienstes**

Meldet den Status von Appliance entdecken Systemdienste

**Ex-Admin**

Gibt an, wie lange der Webportaldienst der Explore-Appliance ausgeführt wurde.

**exconfig**

Gibt an, wie lange der Explore-Appliance-Konfigurationsdienst ausgeführt wurde

**Ex-Receiver**

Gibt an, wie lange der Explore-Appliance-Empfängerdienst ausgeführt wurde.

**exsearch**

Gibt an, wie lange der Suchdienst der Explore-Appliance ausgeführt wurde.

**Schnittstellen**

Meldet den Status von Appliance entdecken Netzwerkschnittstellen.

**RX-Pakete**

Gibt die Anzahl der Pakete an, die von der Explore-Appliance auf der angegebenen Schnittstelle empfangen wurden.

**RX-Fehler**

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

**RX-Drops**

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

**TX-Pakete**

Gibt die Anzahl der Pakete an, die von der Explore-Appliance auf der angegebenen Schnittstelle übertragen werden.

**TX-Fehler**

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

**TX Drops**

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

**RX-Bytes**

Gibt die Anzahl der Byte an, die von der Explore-Appliance auf der angegebenen Schnittstelle empfangen wurden.

**TX-Bytes**

Gibt die Anzahl der Byte an, die von der Explore-Appliance auf der angegebenen Schnittstelle übertragen werden.

**Partitionen**

Meldet den Status und die Nutzung der Explore-Appliance-Komponenten. Die Konfigurationseinstellungen für diese Komponenten werden auf der Festplatte gespeichert und bleiben auch dann erhalten, wenn die Stromversorgung der Appliance ausgeschaltet wird.

**Name**

Gibt die Einstellungen der Explore-Appliance an, die auf der Festplatte gespeichert sind.

**Optionen**

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

**Größe**

Gibt die Größe der identifizierten Komponente in Gigabyte an.

**Nutzung**

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

**Quellen aufzeichnen**

Zeigt Metriken zu den Datensätzen an, die von der Discover-Appliance an den Explore-Cluster gesendet werden.

**Quelle EDA**

Zeigt den Namen der Discover-Appliance an, die Datensätze an den Explore-Cluster sendet.

**Letzte Aktualisierung**

Zeigt den Zeitstempel an, zu dem die Datensatzsammlung begann. Der Wert wird automatisch alle 24 Stunden oder bei jedem Neustart der Explore-Appliance zurückgesetzt.

**RX-Bytes**

Zeigt die Anzahl der komprimierten Datensatzbytes an, die von der Discover-Appliance empfangen wurden.

**Byte aufzeichnen**

Zeigt die Anzahl der von der Discover-Appliance empfangenen Bytes an.

**Gespeicherte Bytes aufzeichnen**

Zeigt die Anzahl der Byte an, die erfolgreich auf der Explore-Appliance gespeichert wurden.

**Gespeicherte Aufzeichnungen**

Zeigt die Anzahl der Datensätze an, die erfolgreich auf der Explore-Appliance gespeichert wurden.

**Fehler aufzeichnen**

Zeigt die Anzahl der einzelnen Datensatzübertragungen an, die zu einem Fehler geführt haben. Dieser Wert gibt die Anzahl der Datensätze an, die vom Ex-Receiver-Prozess nicht erfolgreich übertragen wurden.

**TXN-Fehler**

Zeigt die Anzahl der Sammeldatentransaktionen an, die zu einem Fehler geführt haben. Fehler in diesem Feld können auf fehlende Datensätze hinweisen.

**TXN-Tropfen**

Zeigt die Anzahl der Transaktionen mit Sammeldatensätzen an, die nicht erfolgreich abgeschlossen wurden. Alle Datensätze in der Transaktion fehlen.

## Audit-Protokoll

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

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

## Fingerabdruck

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

Wenn Sie einen ExtraHop-Recordstore oder Packetstore mit einem Paketsensor oder einer Konsole verbinden, stellen Sie sicher, dass der angezeigte Fingerabdruck genau dem Fingerabdruck entspricht, der auf der Join- oder Pairing-Seite angezeigt wird.

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

### Erweiterte Optionen

Auf Explore-Appliances können Sie ein extern signiertes Zertifikat konfigurieren. Mit signierten Zertifikaten können Sie die Compliance-Anforderungen Ihres Unternehmens erfüllen. Der Fingerabdruck wird automatisch neu generiert.

Standardmäßig wird der Fingerabdruck aus dem öffentlichen Schlüssel des internen TLS-Zertifikats abgeleitet. Dieses separate TLS-Zertifikat verschlüsselt nur die Kommunikation zwischen ExtraHop-Appliances und ist nicht für die Kommunikation zwischen ExtraHop-Appliances und externen HTTP-Clients erforderlich.

**Generieren Sie einen neuen Fingerabdruck**

**Hinweis:** Sie müssen keinen Fingerabdruck generieren, bevor Sie ein extern signiertes Zertifikat konfigurieren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie **Fingerabdruck**.
3. Klicken Sie **Erweiterte Optionen**.
4. Klicken Sie **Generieren Sie einen neuen Fingerabdruck**.
5. Klicken Sie **OK**.

**Extern signiertes TLS-Zertifikat konfigurieren**

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie **Fingerabdruck**.
3. Klicken Sie **Erweiterte Optionen**.
4. Klicken Sie **Extern signiertes SSL-Zertifikat konfigurieren**.
5. Kopieren Sie die Zertifikatsanforderung aus dem Textfeld und senden Sie sie an Ihre Zertifizierungsstelle (CA).
6. Nachdem Sie das signierte TLS-Zertifikat von Ihrer CA erhalten haben, kehren Sie in den Verwaltungseinstellungen zur Seite Extern signiertes SSL-Zertifikat konfigurieren zurück und fügen Sie den Inhalt der Zertifikatsdatei (.crt) in das zweite Textfeld ein.
7. Klicken Sie **Installieren**.
   Nach der Installation des Zertifikats wird ein neuer Fingerabdruck aus dem neu hinzugefügten öffentlichen Schlüssel generiert.
8. Wiederholen Sie diese Schritte für alle anderen Explore-Appliances im Cluster.

## 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.

## Erkunden Sie den Cluster-Status

Das Erkunden Sie den Cluster-Status Auf dieser Seite finden Sie Details zum Zustand der Explore-Appliance.

Die Metriken auf dieser Seite können Ihnen helfen, Probleme zu beheben und festzustellen, warum der Explore-Cluster nicht wie erwartet funktioniert. Darüber hinaus können Sie eine Reihe von Datensätzen löschen nach Datum von dieser Seite.

**Zusammenfassung des Indexes**

Zeigt Metriken an, die sich auf die Anzahl der auf der Appliance gespeicherten Indizes, Shards und Primärdatensätze beziehen.

**Zusammenfassung des Clusterknotens**

Zeigt die Anzahl der dedizierten Knoten nur für Manager, dedizierten Knoten nur für Daten und für Daten infrage kommenden Knoten nur für Manager im Explore-Cluster an.

**Einzelheiten zum Index**

**Datum (UTC)**

Zeigt das Datum an, an dem der Index erstellt wurde.

**ID**

Zeigt die ID des Indexes an. Eine andere ID als 0 bedeutet, dass ein Index mit demselben Datum, aber aus einer anderen Quelle, auf dem Cluster existiert.

**Quelle**

Zeigt den Hostnamen oder die IP-Adresse der Discover-Appliance an, von der die Datensatzdaten stammen.

**Aufzeichnungen**

Zeigt die Gesamtzahl der an die Explore-Appliance gesendeten Datensätze an.

**Größe**

Zeigt die Größe des Indexes an.

**Status**

Zeigt den Replikationsstatus der Daten auf dem Cluster an.

**Scherben**

Zeigt die Anzahl der Shards im Index an.

**Nicht zugewiesene Shards**

Zeigt die Anzahl der Shards an, die keinem Knoten zugewiesen wurden. Nicht zugewiesene Shards sind in der Regel Replikat-Shards, die auf einem anderen Knoten als dem Knoten mit dem entsprechenden primären Shard aufbewahrt werden müssen, aber es gibt nicht genügend Knoten im Cluster. Ein Cluster mit nur einem Mitglied hat beispielsweise keinen Platz zum Speichern der Replikat-Shards. Bei der Standardreplikationsstufe 1 hat der Index also immer nicht zugewiesene Shards und hat eine `yellow` Status.

**Scherben verschieben**

Zeigt die Anzahl der Shards an, die sich von einem Knoten zum anderen bewegen. Das Verschieben von Shards erfolgt in der Regel, wenn ein Explore-Knoten im Cluster ausfällt.

## Datensätze löschen

Unter bestimmten Umständen, z. B. beim Verschieben eines Explore-Clusters von einem Netzwerk in ein anderes, möchten Sie möglicherweise alle Datensätze aus einem Cluster löschen.

Sie können Datensätze nach Index löschen. Dabei handelt es sich um eine Sammlung von Datensätzen, die am selben Tag erstellt wurden. Indizes werden nach dem folgenden Muster benannt:

```
<node-id>-<date>-<index-id>
```

Zum Beispiel ein Index vom `2016-5-16` enthält Datensätze, die am 16. Mai 2016 erstellt wurden (Daten sind in UTC angegeben). Sie können alle Daten für einen bestimmten Tag oder eine bestimmte Zeitspanne löschen. Möglicherweise möchten Sie beispielsweise Datensatzinhalte löschen, von denen Sie wissen, dass sie vertrauliche Informationen enthalten.

1. In der Status und Diagnose Abschnitt, klicken **Erkunden Sie den Cluster-Status**.
2. In der Einzelheiten zum Index Wählen Sie im Abschnitt das Kontrollkästchen für jeden Index aus, den Sie löschen möchten.

   Die Quelle In der Spalte wird der Name des Sensor angezeigt, der die Daten gesammelt hat.
3. klicken **Ausgewählte löschen**.
4. klicken **OK**.

## Stellen Sie den Clusterstatus wieder her

In den seltensten Fällen kann der Explore-Cluster möglicherweise nicht von einem `Red` Status, wie in der Status Abschnitt über die Erkunden Sie den Cluster-Status Seite. Wenn dieser Zustand eintritt, ist es möglich, den Cluster auf einen `Green` Bundesstaat.

Wenn Sie den Clusterstatus wiederherstellen, wird der Explore-Cluster mit den neuesten gespeicherten Informationen über die Explore-Knoten im Cluster und alle anderen verbundenen Discover- und Command-Appliances aktualisiert.

**Wichtig:** Wenn Sie Ihren Explore-Cluster kürzlich neu gestartet haben, kann es eine Stunde dauern, bis der Cluster-Status erreicht ist `Green` wird angezeigt, und eine Wiederherstellung des Cluster ist möglicherweise nicht erforderlich. Wenn Sie sich nicht sicher sind, ob Sie den Clusterstatus wiederherstellen sollten, wenden Sie sich an ExtraHop-Unterstützung.

1. In der Erkunden Sie die Cluster-Einstellungen Abschnitt, klicken **Clusterstatus wiederherstellen**.
2. Auf dem Clusterstatus wiederherstellen Seite, klick **Clusterstatus wiederherstellen**.
3. klicken **Cluster wiederherstellen** zur Bestätigung.

# Netzwerk-Einstellungen

Der Abschnitt Netzwerkeinstellungen enthält die folgenden konfigurierbaren Netzwerkverbindungseinstellungen.

**Konnektivität**

Netzwerkverbindungen konfigurieren.

**SSL Zertifikat**

Generieren Sie ein selbstsigniertes Zertifikat und laden Sie es hoch.

**Benachrichtigungen**

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

Die Explore-Appliance verfügt über vier 10/100/1000BaseT-Netzwerkanschlüsse und zwei 10GbE SFP+-Netzwerkanschlüsse. Standardmäßig ist der Gb1-Port als Management-Port konfiguriert und erfordert eine IP-Adresse. Die Gb2-, Gb3- und Gb4-Ports sind deaktiviert und nicht konfigurierbar.

Sie können einen der 10-GbE-Netzwerkanschlüsse als Management-Port konfigurieren, aber Sie können jeweils nur einen Management-Port aktivieren.

Bevor Sie mit der Konfiguration der Netzwerkeinstellungen auf einer Explore-Appliance beginnen, stellen Sie sicher, dass ein Netzwerk-Patchkabel den Gb1-Port der Explore-Appliance mit dem Verwaltungsnetzwerk verbindet. Weitere Informationen zur Installation einer Explore-Appliance finden Sie in Stellen Sie den EXA 5200 Recordstore bereit Anleitung oder wenden Sie sich an den ExtraHop-Support, um Unterstützung zu erhalten.

Spezifikationen, Installationsanleitungen und weitere Informationen zu Ihrem Gerät finden Sie unter docs.extrahop.com.

## Stellen Sie eine Verbindung zu ExtraHop Cloud Services her

ExtraHop Cloud Services bietet Zugriff auf die Cloud-basierten Dienste von ExtraHop über eine verschlüsselte Verbindung.

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.

**Überwachung (nur Empfang)**

Überwacht den Netzwerkverkehr.

**Verwaltung**

Verwaltet den ExtraHop-Sensor.

**Verwaltung + RPCAP/ERSPAN/VXLAN/GENEVE Target**

Verwaltet den ExtraHop-Sensor und erfasst den von einem Paketweiterleiter weitergeleiteten Verkehr, ERSPAN*, VXLAN** oder GENEVE***.

Während die 10-GbE-Management+-Erfassungsschnittstellen auf diesem Sensor Verwaltungsfunktionen mit Geschwindigkeiten von 10 Gbit/s ausführen können, ist die Verarbeitung von Datenverkehr wie ERSPAN, VXLAN und GENEVE auf 1 Gbit/s begrenzt.

**Hinweis:** In Umgebungen mit asymmetrischem Routing neben den Hochleistungsschnittstellen gelangen Ping-Antworten möglicherweise nicht an den Absender zurück.

**Leistungsstarkes ERSPAN/VXLAN/GENEVE-Ziel**

Erfasst den von ERSPAN *, VXLAN** oder GENEVE*** weitergeleiteten Datenverkehr. Dieser Schnittstellenmodus ermöglicht es dem Port, mehr als 1 Gbit/s zu verarbeiten. Stellen Sie diesen Schnittstellenmodus ein, wenn der ExtraHop-Sensor über einen 10-GbE-Anschluss verfügt. Für diesen Schnittstellenmodus müssen Sie nur eine IPv4-Adresse konfigurieren.

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

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

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

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

**Hinweis:** Für Amazon Web Services (AWS) -Bereitstellungen mit einer Schnittstelle müssen Sie auswählen **Verwaltung + RPCAP/ERSPAN/VXLAN/GENEVE Target** für Interface 1. Wenn Sie zwei Schnittstellen konfigurieren, müssen Sie auswählen **Verwaltung + RPCAP/ERSPAN/VXLAN/GENEVE Target** für Interface 1 und **Verwaltung + RPCAP/ERSPAN/VXLAN/GENEVE Target** für Interface 2.

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

5. Optional: Wählen Sie eine Schnittstellengeschwindigkeit aus.

   **Automatisch aushandeln** ist standardmäßig ausgewählt; Sie sollten jedoch manuell eine Geschwindigkeit auswählen, wenn sie von Ihrem Sensor, Netzwerk-Transceiver und Netzwerk-Switch unterstützt wird.

   - **Automatisch aushandeln**
   - **10 Gbit/s**
   - **25 Gbit/s**
   - **40 Gbit/s**
   - **100 Gbit/s**

   **Wichtig:** Wenn Sie die Schnittstellengeschwindigkeit ändern auf **Automatisch aushandeln**, Sie müssen den Sensor möglicherweise neu starten, bevor die Änderung wirksam wird.

6. Optional: Wählen Sie einen FEC-Typ (Forward Error Correction).

   Wir empfehlen Auto-Negotiate, das für die meisten Umgebungen optimal ist.

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

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

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

   • **Deaktiviert:** Deaktiviert FEC.

7. 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.

8. Konfigurieren Sie den TCP-Health-Check-Port.

   Diese Einstellung ist nur für Hochleistungsschnittstellen konfigurierbar und wird benötigt, wenn GENEVE-Datenverkehr von einem AWS Gateway Load Balancer (GWLB) aufgenommen wird. Der Wert der Portnummer muss mit dem in AWS konfigurierten Wert übereinstimmen. Weitere Informationen finden Sie unter Weiterleiten von geneve-gekapseltem Datenverkehr von einem AWS Gateway Load Balancer.

9. Optional: Aktiviere IPv6.

   Weitere Hinweise zur Konfiguration von IPv6 finden Sie unter IPv6 für eine Schnittstelle aktivieren.

10. Optional: Fügen Sie manuell Routen hinzu.
11. Klicken Sie **Speichern**.

**Schnittstellendurchsatz**
ExtraHop Sensor Die Modelle EDA 6100, EDA 8100 und EDA 9100 sind für die Erfassung des Datenverkehrs ausschließlich an 10-GbE-Ports optimiert.

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

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

| ExtraHop-Sensor | Durchsatz | Einzelheiten |
|---|---|---|
| SEIT 1900 | Standarddurchsatz von 40 Gbit/s | Wenn die nicht verwaltbaren 1-GbE-Schnittstellen deaktiviert sind, können Sie bis zu vier der 10-GbE-Schnittstellen für einen kombinierten Durchsatz von bis zu 40 Gbit/s verwenden. |
| SEIT 1800 | Standarddurchsatz von 20 Gbit/s | Wenn die nicht verwaltbaren 1-GbE-Schnittstellen deaktiviert sind, können Sie entweder eine oder beide der 10-GbE-Schnittstellen für einen kombinierten Durchsatz von bis zu 20 Gbit/s verwenden. |
| AB 6100 | Standarddurchsatz von 10 Gbit/s | Wenn die nicht verwaltbaren 1-GbE-Schnittstellen deaktiviert sind, beträgt der maximale kombinierte Gesamtdurchsatz 10 Gbit/s. |
| SEIT 3100 | Standarddurchsatz von 3 Gbit/s | Keine 10GbE-Schnittstelle |
| SEIT 1100 | Standarddurchsatz von 1 Gbit/s | Keine 10GbE-Schnittstelle |

**Stellen Sie eine statische Route ein**

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

1. 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.

## 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 Alarme per E-Mail, SNMP-Traps und Syslog-Exporte an Remote-Server senden. Wenn eine E-Mail-Benachrichtigungsgruppe angegeben ist, werden E-Mails an die Gruppen gesendet, die der Alarm zugewiesen sind.

### E-Mail-Einstellungen für Benachrichtigungen konfigurieren

Sie müssen einen E-Mail-Server und einen Absender konfigurieren, bevor das ExtraHop-System Warnmeldungen, 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.

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

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

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

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

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

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

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

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

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

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

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

   Eine ähnliche Antwort wie in diesem Beispiel wird angezeigt:

```
Connection from UDP: [192.0.2.0]:42164->[ 192.0.2.255]:162
```

8. Klicken Sie **Speichern**.

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

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

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

## Systembenachrichtigungen an einen Remote-Syslog-Server senden

Mit der Syslog-Exportoption können Sie 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 |

| Feld | Beschreibung | Beispiele |
|---|---|---|
| E-mail-Adresse | Die E-Mail-Adresse des Hauptansprechpartners für Ihre Organisation. | webmaster@example.com |
| Organisatorische Einheit | Die Abteilung Ihrer Organisation, die das Zertifikat bearbeitet. | IT-Abteilung |
| Organisation | Der offizielle Name Ihrer Organisation. Dieser Eintrag 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.

## 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.

### Nutzer

Benutzer können auf drei Arten auf Recordstores und Packetstores 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

#### 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

### Lokales Benutzerkonto hinzufügen

Durch Hinzufügen eines lokalen Benutzerkonto können Sie Benutzern direkten Zugriff auf Ihren Recordstore oder Packetstore gewähren.

Weitere Informationen zu Standardsystembenutzerkonten finden Sie unter Lokale Benutzer.

**Hinweis:** Die Rechte können für lokale Benutzer in Recordstores und Packetstores nicht eingeschränkt werden. Allen neuen lokalen Benutzern werden volle Rechte zugewiesen.

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 Sie **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. 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.

### 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

## 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 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.

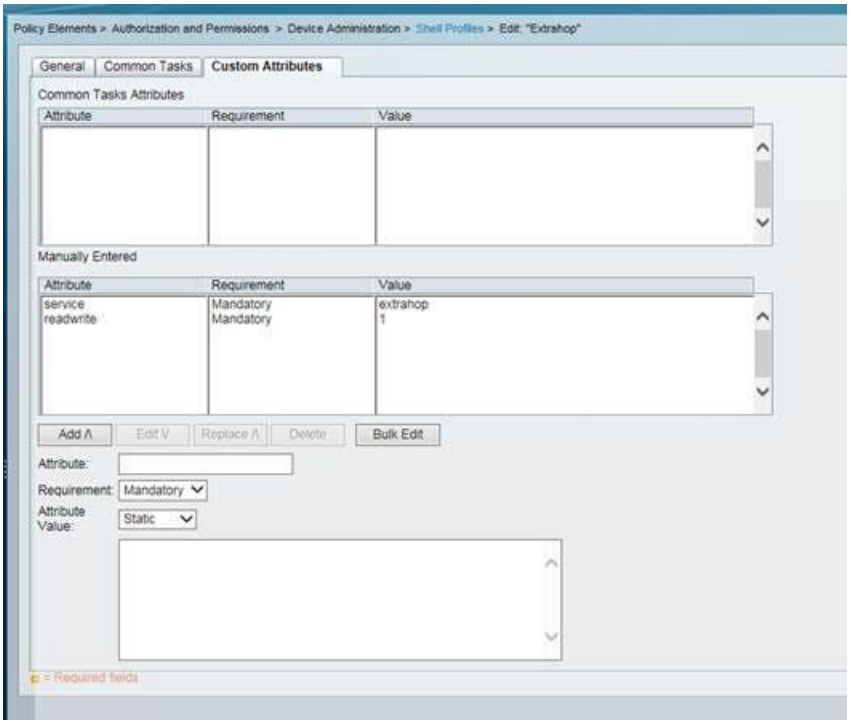
    - **Kein Zugriff**
    - **Nur Paketsegmente**
    - **Nur Paket-Header**
    - **Nur Pakete**
    - **Pakete und Sitzungsschlüssel**
11. Optional: Konfigurieren Sie den NDR- und NPM-Modulzugriff (nur auf Sensoren und Konsolen).

    - **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 |

| Attribut | Wert | Beschreibung |
|---|---|---|
| `readonly` | `1` | Objekte im ExtraHop-System anzeigen |
| `personal` | `1` | Erstellen Sie persönliche Dashboards für sich selbst und ändern Sie alle Dashboards, die mit ihnen geteilt wurden |
| `limited_metrics` | `1` | Geteilte Dashboards anzeigen |
| `ndrfull` | `1` | Sicherheitserkennungen anzeigen, bestätigen und ausblenden |
| `npmfull` | `1` | Leistungserkennungen anzeigen, bestätigen und ausblenden |
| `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 |

| Attribut | Wert | Beschreibung |
|---|---|---|
| | | 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. |
| `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.<br>• Führen Sie alle Verwaltungsaufgaben aus, die über die REST-API verfügbar sind.<br>• Führen Sie alle ExtraHop-Systemaufgaben aus, die über die REST-API verfügbar sind. |
| „write“: „voll“ | • Generieren Sie Ihren eigenen API-Schlüssel.<br>• Zeigen Sie Ihren eigenen API-Schlüssel an oder löschen Sie ihn.<br>• Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen.<br>• Führen Sie alle ExtraHop-Systemaufgaben aus, die über die REST-API verfügbar sind. |
| „write“: „begrenzt“ | • Generieren Sie einen API-Schlüssel.<br>• Zeigen Sie ihren eigenen API-Schlüssel an oder löschen Sie ihn.<br>• Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen.<br>• Führen Sie alle GET-Operationen über die REST-API aus.<br>• Führen Sie Metrik- und Datensatzabfragen durch. |
| „write“: „persönlich“ | • Generieren Sie einen API-Schlüssel.<br>• Zeigen Sie Ihren eigenen API-Schlüssel an oder löschen Sie ihn.<br>• Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen.<br>• Führen Sie alle GET-Operationen über die REST-API aus.<br>• Führen Sie Metrik- und Datensatzabfragen durch. |
| „Metriken“: „voll“ | • Generieren Sie einen API-Schlüssel.<br>• Zeigen Sie Ihren eigenen API-Schlüssel an oder löschen Sie ihn.<br>• Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen.<br>• Führen Sie Metrik- und Datensatzabfragen durch. |
| „metrics“: „eingeschränkt“ | • Generieren Sie einen API-Schlüssel.<br>• Zeigen Sie Ihren eigenen API-Schlüssel an oder löschen Sie ihn.<br>• Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen. |
| „ndr“: „voll“ | • Sicherheitserkennungen anzeigen |

| Privilegienstufe | Zulässige Aktionen |
| --- | --- |
| | • Untersuchungen anzeigen und erstellen<br><br>Dies ist ein Modulzugriffsrecht, das einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann:<br><br>• „write“: „voll“<br>• „write“: „begrenzt“<br>• „write“: „persönlich“<br>• „schreiben“: null<br>• „Metriken“: „voll“<br>• „metrics“: „eingeschränkt“ |
| „ndr“: „keiner“ | • Kein Zugriff auf NDR-Modulinhalte<br><br>Dies ist ein Modulzugriffsrecht, das einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann:<br><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><br>Dies ist ein Modulzugriffsrecht, das einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann:<br><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><br>Dies ist ein Modulzugriffsrecht, das einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann:<br><br>• „write“: „voll“<br>• „write“: „begrenzt“<br>• „write“: „persönlich“<br>• „schreiben“: null<br>• „Metriken“: „voll“<br>• „metrics“: „eingeschränkt“ |

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

# 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.

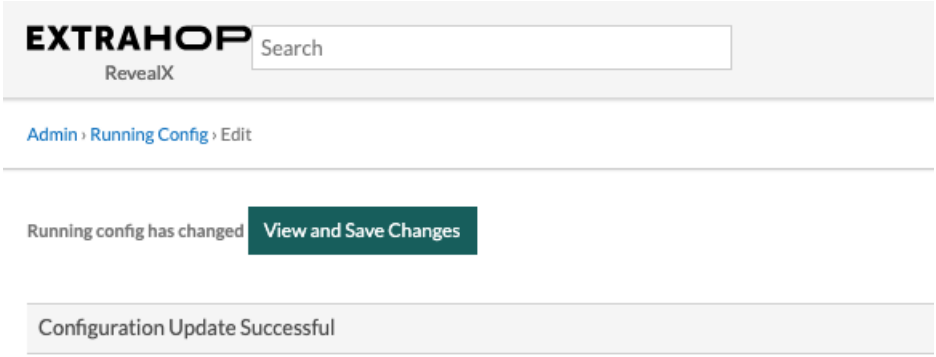
**Hinweis:** Es wird nicht empfohlen, Konfigurationsänderungen am Code von der Bearbeitungsseite aus vorzunehmen. Sie können die meisten Systemänderungen über andere Seiten in den Administrationseinstellungen vornehmen.

### 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.

## 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.

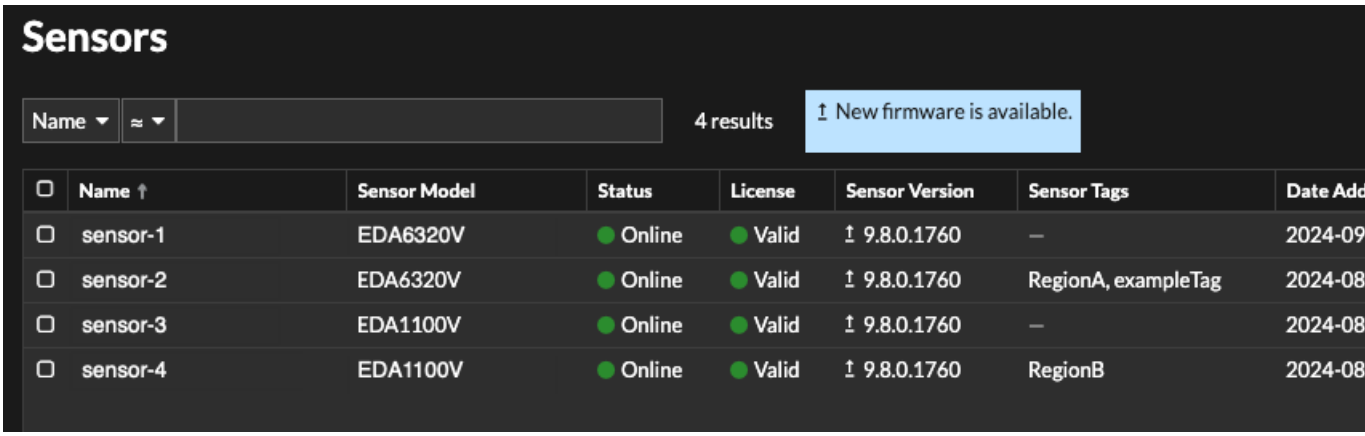
**Bevor Sie beginnen**

- 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 neu starten

Die Explore Admin-Benutzeroberfläche bietet eine Schnittstelle zum Anhalten, Herunterfahren und Neustarten der Explore-Appliance-Komponenten.

**System**

Starten Sie die Explore-Appliance neu oder fahren Sie sie herunter.

**Admin**

Starten Sie die Administratorkomponente der Explore-Appliance neu.

**Empfänger**

Starten Sie die Explore-Empfängerkomponente neu.

**Suche**

Starten Sie den Explore-Suchdienst neu.

Für jede Explore-Appliance-Komponente enthält die Tabelle einen Zeitstempel, der die Startzeit anzeigt.

### Starten Sie eine Explore-Appliance-Komponente neu

1. Auf dem Admin Seite in der Einstellungen der Appliance Abschnitt, klicken **Herunterfahren oder Neustarten**.
2. Wählen **Neustarten** für die Komponente, die Sie neu starten möchten:
   - System (kann auch komplett heruntergefahren werden)
   - Admin
   - Empfänger
   - Suche

## Lizenz

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

**Lizenz verwalten**

Bietet eine Schnittstelle zum Hinzufügen und Aktualisieren des ExtraHop-Systems

**Informationen zum System**

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

**Funktionen**

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

### Registrieren Sie Ihr ExtraHop-System

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.
```

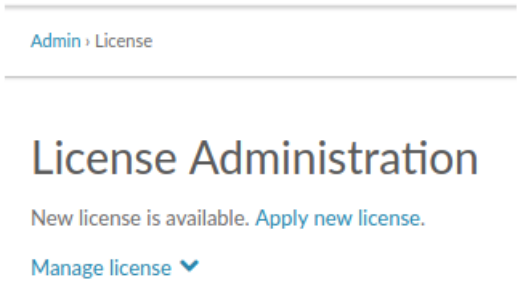
Wenn die Namensauflösung nicht erfolgreich ist, stellen Sie sicher, dass Ihr DNS-Server richtig konfiguriert ist, um nach dem `extrahop.com` Domäne.

## 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 Festplatten Diese Seite enthält Informationen zur Konfiguration und zum Status der Festplatten in Ihrer Explore-Appliance. Die auf dieser Seite angezeigten Informationen variieren je nachdem, ob Sie über eine physische oder virtuelle Appliance verfügen.

**Hinweis:** Wir empfehlen Ihnen, die Einstellungen für den Empfang zu konfigurieren E-Mail-Benachrichtigungen über Ihren Systemzustand. Wenn auf einer Festplatte Probleme auftreten, werden Sie gewarnt. Weitere Informationen finden Sie im Abschnitt Benachrichtigungen.

Die folgenden Informationen werden auf der Seite angezeigt:

**Karte fahren**

(Nur physisch) Bietet eine visuelle Darstellung der Vorderseite der Explore-Appliance.

**Details zur RAID-Festplatte**

Bietet Zugriff auf detaillierte Informationen zu allen Festplatten im Knoten.

**Firmware**

Zeigt Informationen über Festplatten an, die für die Firmware der Explore-Appliance reserviert sind.

**Nutzwert (Var)**

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

**Suche**

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

**Direkt verbundene Festplatten**

Zeigt Informationen zu virtuellen Laufwerken in Bereitstellungen virtueller Maschinen oder zu USB-Medien in physischen Geräten an.

# Erkunden Sie die Cluster-Einstellungen

Die Erkunden Sie die Cluster-Einstellungen Dieser Abschnitt bietet die folgenden konfigurierbaren Einstellungen:

**Cluster beitreten**

Verbinden Sie einen ExtraHop-Recordstore mit einem vorhandenen Cluster. Diese Einstellung wird nur für einzelne Knoten angezeigt, die noch nicht zu einem Cluster hinzugefügt wurden.

**Cluster-Mitglieder**

Zeigt alle Knoten an, die Mitglieder des Clusters sind.

**Cluster-Datenmanagement**

Zeigt Einstellungen an, um die Datenreplikationsebene zu konfigurieren, die Shard-Neuzuweisung zu aktivieren oder zu deaktivieren und die Aufnahme von Datensatz zu aktivieren oder zu deaktivieren. Diese Einstellungen werden auf alle Knoten im Cluster angewendet.

**Manager**

Zeigt den Hostnamen der Konsole an, die für die Verwaltung des ExtraHop-Recordstores konfiguriert ist, sowie eine Liste aller Sensoren und Konsolen, die mit dem Recordstore verbunden sind.

**Mit Command Appliance verwalten**

Konfigurieren Sie Einstellungen, damit eine Konsole per Fernzugriff Support-Skripte im ExtraHop-Recordstore ausführen kann.

**Clusterstatus wiederherstellen**

Stellen Sie den fehlerfreien Zustand des Clusters wieder her. Diese Einstellung wird nur angezeigt, wenn der Cluster den Status anzeigt `red` auf dem Cluster-Status Seite.

## Einen Recordstore-Cluster erstellen

Für die beste Leistung, Datenredundanz und Stabilität müssen Sie mindestens drei ExtraHop-Recordstores in einem Cluster konfigurieren.

Wenn Sie einen Recordstore-Cluster erstellen, stellen Sie sicher, dass Sie alle Knoten, einschließlich Manager-Knoten, am selben Standort oder Rechenzentrum bereitstellen. Weitere Informationen zu unterstützten Recordstore-Cluster-Konfigurationen finden Sie unter Richtlinien für Recordstore-Cluster.

**Wichtig:** Wenn Sie einen Recordstore-Cluster mit sechs bis neun Knoten erstellen, müssen Sie den Cluster mit mindestens drei Nur-Manager-Knoten konfigurieren. Weitere Informationen finden Sie unter Bereitstellung von Knoten nur für Manager.

Im folgenden Beispiel haben die Recordstores die folgenden IP-Adressen:

- Knoten 1:10.20.227.177
- Knoten 2:10.20.227.178
- Knoten 3:10.20.227.179

Sie verbinden die Knoten 2 und 3 mit Knoten 1, um den Recordstore-Cluster zu erstellen. Alle drei Knoten sind Datenknoten. Sie können keinen Datenknoten mit einem Manager-Knoten verbinden oder einen Manager-Knoten mit einem Datenknoten verbinden, um einen Cluster zu erstellen.

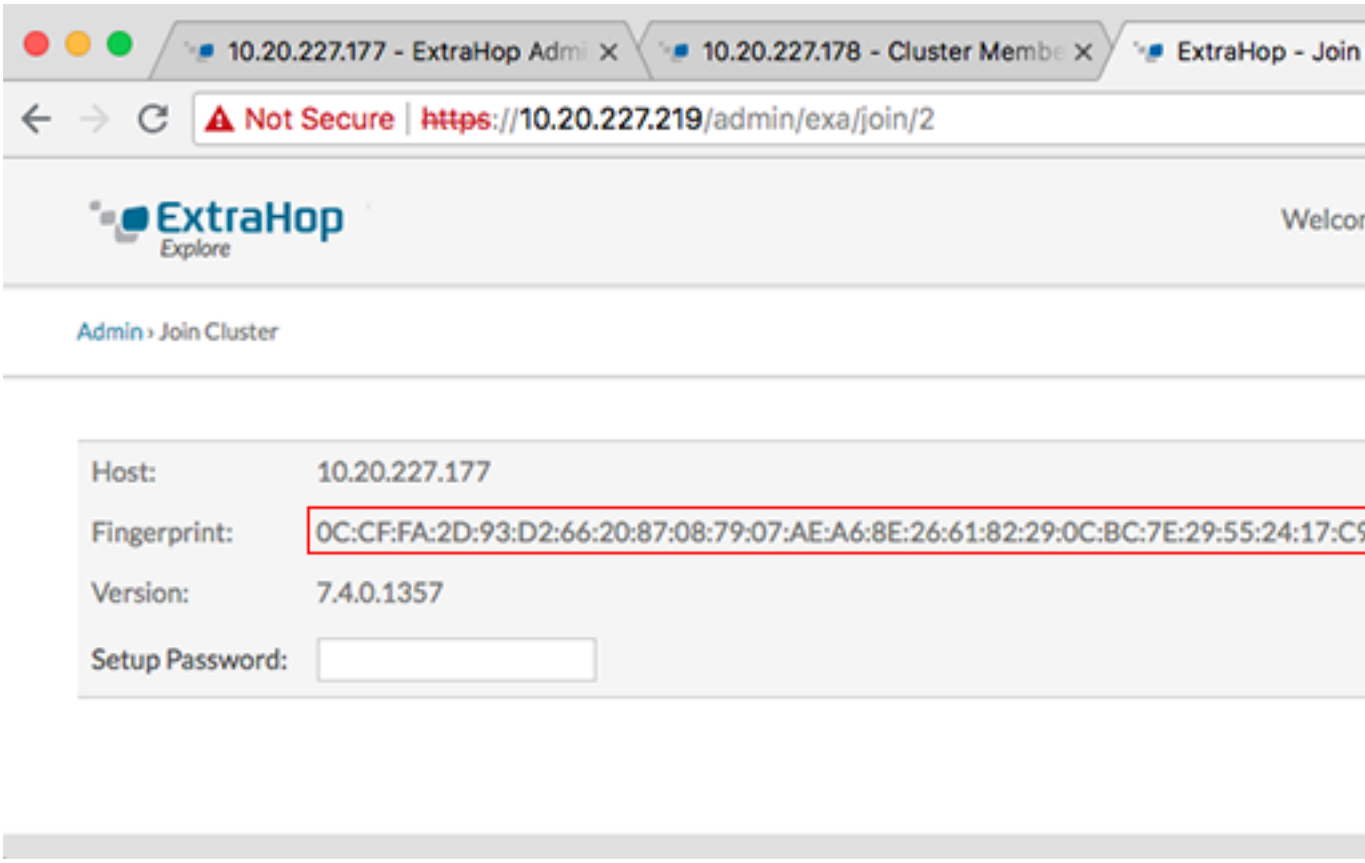
**Wichtig:** Jeder Knoten , dem Sie beitreten, muss dieselbe Konfiguration (physisch oder virtuell) und dieselbe ExtraHop-Firmware-Version haben.

**Bevor Sie beginnen**
Sie müssen die Recordstores bereits in Ihrer Umgebung installiert oder bereitgestellt haben, bevor Sie fortfahren können.

1. Loggen Sie sich in die Administrationseinstellungen aller drei Recordstores ein mit dem `setup` Benutzerkonto in drei separaten Browserfenstern oder Tabs.
2. Wählen Sie das Browserfenster von Knoten 1 aus.
3. In der Status und Diagnose Abschnitt, klicken Sie **Fingerabdruck** und notieren Sie sich den Fingerabdruckwert.

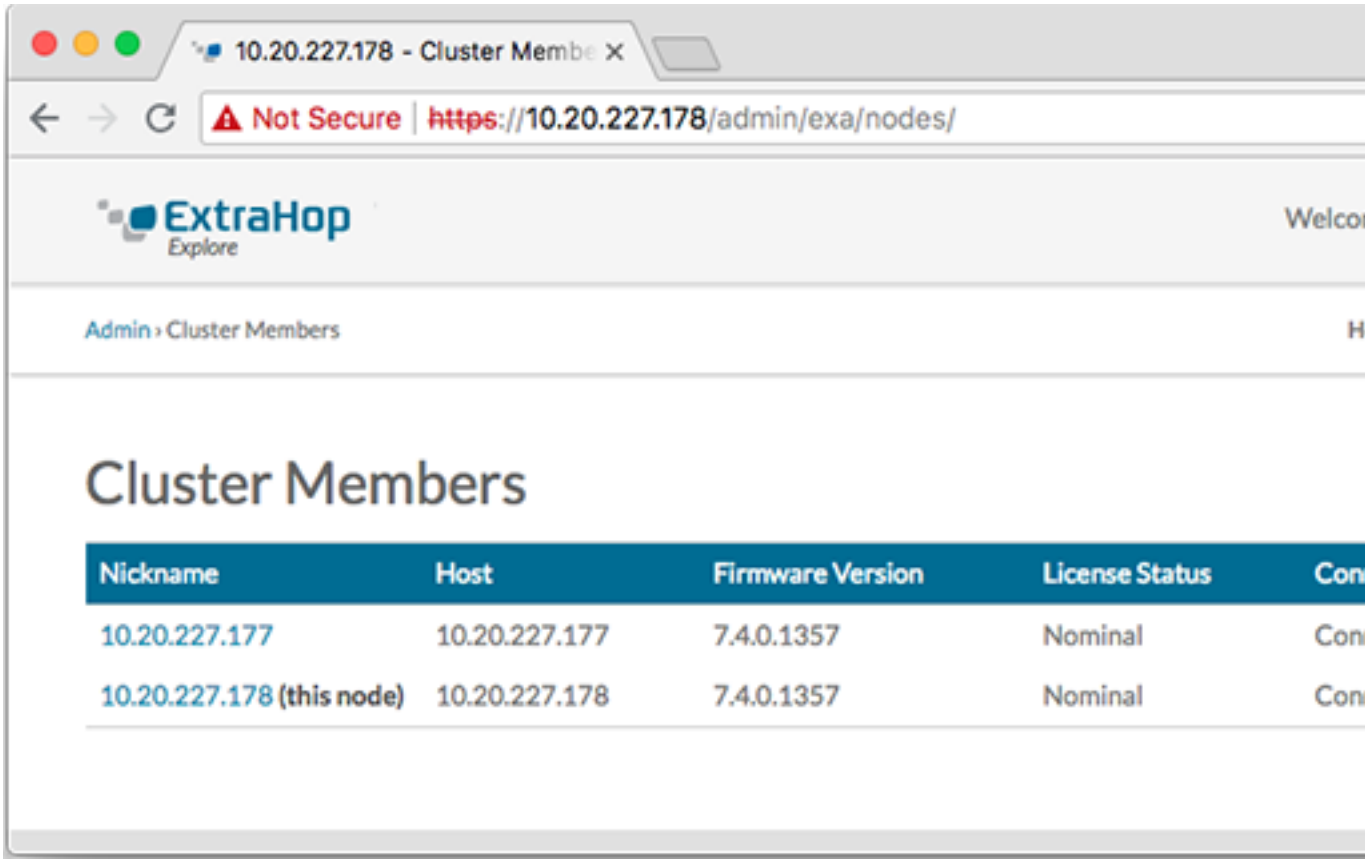
   Sie werden später bestätigen, dass der Fingerabdruck für Knoten 1 übereinstimmt, wenn Sie die verbleibenden zwei Knoten verbinden.
4. Wählen Sie das Browserfenster von Knoten 2 aus.
5. In der Recordstore-Cluster-Einstellungen Abschnitt, klicken Sie **Cluster beitreten**.
6. In der **Gastgeber** Feld, geben Sie den Hostnamen oder die IP-Adresse von Datenknoten 1 ein und klicken Sie dann auf **Fortfahren**.

   **Hinweis** Geben Sie bei cloudbasierten Bereitstellungen unbedingt die IP-Adresse ein, die in der Schnittstellentabelle auf der Seite Konnektivität aufgeführt ist.
7. Vergewissern Sie sich, dass der Fingerabdruck auf dieser Seite mit dem Fingerabdruck übereinstimmt, den Sie in Schritt 3 notiert haben.




8. In der **Passwort einrichten** Feld, geben Sie das Passwort für den Knoten 1 ein `setup` Benutzerkonto und klicken Sie dann auf **Beitreten**.
   Wenn der Join abgeschlossen ist, wird Erkunden Sie die Cluster-Einstellungen Abschnitt hat zwei neue Einträge: **Cluster-Mitglieder** und **Cluster-Datenmanagement**.
9. Klicken Sie **Cluster-Mitglieder**.

   Sie sollten Knoten 1 und Knoten 2 in der Liste sehen.

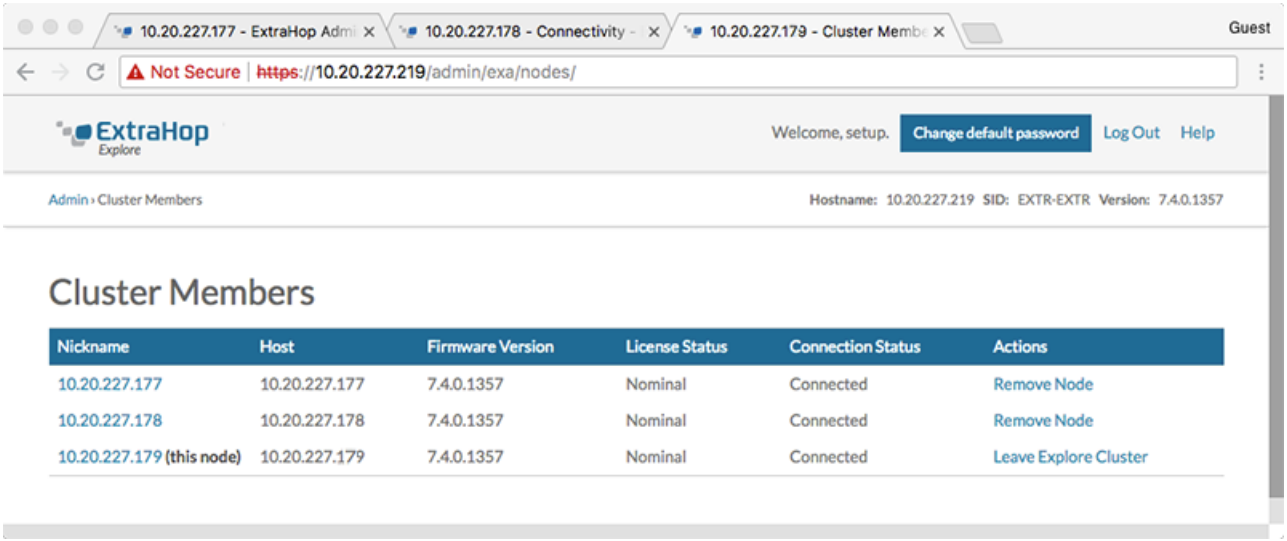



10. In der Status und Diagnose Abschnitt, klicken Sie **Erkunden Sie den Cluster-Status**.

    Warten Sie, bis das Statusfeld auf Grün wechselt, bevor Sie den nächsten Knoten hinzufügen.
11. Wiederholen Sie die Schritte 5 bis 10, um jeden weiteren Knoten mit dem neuen Cluster zu verbinden.

    **Hinweis:** Um zu vermeiden, dass mehrere Cluster erstellt werden, fügen Sie immer einen neuen Knoten einem vorhandenen Cluster und nicht einer anderen einzelnen Appliance hinzu.
12. Wenn Sie alle Ihre Recordstores zum Cluster hinzugefügt haben, klicken Sie auf **Cluster-Mitglieder** in der Erkunden Sie die Cluster-Einstellungen Abschnitt.

    Sie sollten alle verbundenen Knoten in der Liste sehen, ähnlich der folgenden Abbildung.




13. In der Erkunden Sie die Cluster-Einstellungen Abschnitt, klicken Sie **Cluster-Datenmanagement** und stellen Sie sicher, dass **Replikationsstufe** ist eingestellt auf **1** und **Neuzuweisung von Shards** ist **AUF**.

**Nächste Schritte**
Verbinden Sie den EXA 5200 mit dem ExtraHop-System.

### Richtlinien für Recordstore-Cluster

Die folgende Tabelle enthält empfohlene Richtlinien für die Recordstore-Cluster-Konfiguration.

| Anzahl der Datenknoten | Unterstützte Cluster-Zusammensetzung |
|---|---|
| 1 oder 2 | Wird nicht unterstützt |
| 3 | 3 gemischte Knoten (herkömmlicher Daten+Manager) |
| 4 | 4 gemischte Knoten (herkömmlicher Daten+Manager) |
| 5 | 5 gemischte Knoten (herkömmlicher Daten+Manager) |
| 6 | 6 dedizierte Datenknoten + 3 dedizierte Manager-Knoten |
| 7 | 7 dedizierte Datenknoten + 3 dedizierte Manager-Knoten |
| 8 | 8 dedizierte Datenknoten + 3 dedizierte Manager-Knoten |
| 9 | 9 dedizierte Datenknoten + 3 dedizierte Manager-Knoten |
| 10 oder mehr | Wird nicht unterstützt |

## Cluster-Mitglieder

Wenn Sie mehrere Knoten mit einem Explore-Cluster verbunden haben, können Sie Informationen zu jedem Knoten anzeigen.

Die Tabelle auf dieser Seite enthält die folgenden Informationen zu jedem Knoten im Cluster.

**Spitzname**

Zeigt die IP-Adresse oder den Spitznamen der Explore-Appliance an.
Um einem Cluster-Mitglied einen Spitznamen zuzuweisen oder den vorhandenen Spitznamen zu ändern, klicken Sie auf die IP-Adresse oder den Spitznamen in der Spitzname Spalte, geben Sie einen Namen in das Name Feld, und klicken Sie dann auf **Knoten umbenennen**.

**Gastgeber**

Zeigt die IP-Adresse der Explore-Appliance an.

**Firmware-Version**

Zeigt die Firmware-Version der Explore-Appliance an. Jeder Knoten im Cluster muss über dieselbe Firmware-Version verfügen, um unerwartetes Verhalten bei der Replikation von Daten auf allen Knoten zu verhindern.

**Status der Lizenz**

Zeigt den aktuellen Status der ExtraHop-Lizenz an. Das Status der Lizenz Das Feld zeigt einen der folgenden Zustände an:

**Nennwert**

Die Explore-Appliance verfügt über eine gültige Lizenz.

**Ungültig**

Die Explore-Appliance hat eine ungültige Lizenz. Neue Datensätze können nicht in diesen Knoten geschrieben werden und bestehende Datensätze können nicht abgefragt werden.

**Vorab abgelaufen**

Die Explore-Appliance hat eine Lizenz, die bald abläuft.

**Vorab getrennt**

Die Explore-Appliance kann keine Verbindung zum ExtraHop-Lizenzserver herstellen.

**Verbindung unterbrochen**

Die Explore-Appliance hat seit mehr als 7 Tagen keine Verbindung zum ExtraHop-Lizenzserver Server. Neue Datensätze können nicht in diesen Knoten geschrieben werden und bestehende Datensätze können nicht abgefragt werden.

**Status der Verbindung**

Zeigt an, ob die Appliance mit den anderen Mitgliedern im Cluster verbunden ist. Die möglichen Verbindungszustände sind `Connected` und `Unreachable`.

**Aktionen**

Entfernen Sie einen Explore-Knoten aus dem Cluster.

## Einen Knoten aus dem Cluster entfernen

1. In der Erkunden Sie die Cluster-Einstellungen Abschnitt, klicken **Cluster-Mitglieder**.
2. In der Aktionen Spalte, wählen Sie eine der folgenden Optionen:
   - klicken **Explore-Cluster verlassen** wenn Sie den Knoten entfernen möchten, bei dem Sie gerade angemeldet sind, und klicken Sie dann auf **OK** zur Bestätigung.
   - Klicken Sie **Knoten entfernen** neben dem Knoten, den Sie entfernen möchten, und klicken Sie dann auf **Knoten entfernen** zur Bestätigung.

## Manager und verbundene Geräte

Das Manager und verbundene Geräte Der Abschnitt enthält die folgenden Informationen und Steuerelemente.

**Geschäftsführer**

Zeigt den Hostnamen der Konsole an, die für die Verwaltung des ExtraHop-Recordstores konfiguriert ist. Um über eine getunnelte Verbindung eine Verbindung zu einer Command-Appliance herzustellen, klicken Sie auf **Stellen Sie eine Verbindung zu einer Command Appliance her**. Eine getunnelte Verbindung ist möglicherweise erforderlich, wenn keine direkte Verbindung über die Command-Appliance hergestellt werden kann.
klicken **Manager entfernen** um die Command-Appliance als Manager zu entfernen.

**Hinweis:** Die Explore-Appliance kann nur von einer Command-Appliance verwaltet werden.

**Kunden**

Zeigt eine Tabelle aller Discover-Appliances und Command-Appliances an, die mit der Explore-Appliance verbunden sind. Die Tabelle enthält den Hostnamen des verbundenen Client und den Client-Produktschlüssel.
klicken **Client entfernen** in der Aktionen Spalte, um einen verbundenen Client zu entfernen.

## Cluster-Datenmanagement

Auf der Seite Cluster-Datenmanagement können Sie Einstellungen für die Erfassung und Speicherung von Datensätzen in Ihrem Explore-Cluster anpassen. Du musst einen ExtraHop verbinden Sensor zum Recordstore-Cluster, bevor Sie die Einstellungen für die Replikationsstufe und die Shard-Neuzuweisung konfigurieren können.

Sie können verwalten, wie Datensatzdaten in Ihrem Recordstore-Cluster gespeichert werden.

- Ändern Sie die Replikationsstufe, um zu bestimmen, wie viele Kopien jedes Datensatz gespeichert werden. Eine höhere Anzahl von Kopien verbessert die Fehlertoleranz, wenn ein Knoten ausfällt, und verbessert auch die Geschwindigkeit der Abfrageergebnisse. Eine höhere Anzahl von Kopien nimmt jedoch mehr Speicherplatz in Anspruch und kann die Indizierung der Daten verlangsamen.

| Option | Beschreibung |
|---|---|
| **0** | Daten werden nicht auf andere Knoten im Cluster repliziert. Auf dieser Ebene können Sie mehr Daten im Cluster sammeln. Wenn es jedoch zu einem Knotenausfall kommt, verlieren Sie dauerhaft Daten. |
| **1** | Es gibt eine Kopie der Originaldaten, die auf dem Cluster gespeichert sind. Wenn ein Knoten ausfällt, verlieren Sie keine Daten dauerhaft. |
| **2** | Es gibt zwei Kopien der Originaldaten, die auf dem Cluster gespeichert sind. Diese Stufe benötigt den meisten Speicherplatz, bietet aber das höchste Maß an Datenschutz. Zwei Knoten im Cluster können ausfallen, ohne dass Daten dauerhaft verloren gehen. |

- Aktiviert oder deaktiviert die Shard-Neuzuweisung. Die Neuzuweisung von Shards ist standardmäßig aktiviert. Bevor Sie den Knoten für Wartungsarbeiten offline nehmen (z. B. um die Firmware zu aktualisieren, Festplatten auszutauschen, die Appliance einzuschalten oder die Netzwerkkonnektivität zwischen den Recordstore-Knoten zu entfernen), sollten Sie die Shard-Neuzuweisung deaktivieren. Nachdem die Wartung Knoten abgeschlossen ist, aktivieren Sie die Shard-Neuzuweisung.
- Aktiviert oder deaktiviert die Aufnahme von Datensätzen. Die Aufnahme von Datensätzen ist standardmäßig aktiviert und steuert, ob Datensätze in Ihren Recordstore-Cluster geschrieben werden können. Sie müssen die Aufnahme von Datensätzen deaktivieren, bevor Sie die Firmware aktualisieren.

## Stellen Sie eine Verbindung zu einer Command-Appliance her

Stellen Sie eine Verbindung zu einer Command-Appliance her, um Support-Skripts remote auszuführen und die Firmware auf der Explore-Appliance zu aktualisieren.

Dieses Verfahren verbindet die Explore-Appliance über eine Tunnelverbindung mit der Command-Appliance. Tunnelverbindungen sind in Netzwerkumgebungen erforderlich, in denen eine direkte Verbindung von der Command-Appliance aufgrund von Firewalls oder anderen Netzwerkeinschränkungen nicht möglich ist. Wenn möglich, sollten Sie Geräte immer direkt von der Command-Appliance aus anschließen.

1. In der Erkunden Sie die Cluster-Einstellungen Abschnitt, klicken **Stellen Sie eine Verbindung zu einer Command Appliance her**.
2. Konfigurieren Sie die folgenden Einstellungen:
   - Hostname der Befehls-Appliance **:** Der Hostname oder die IP-Adresse der Command-Appliance.
   - Setup-Passwort für Befehlsgerät **:** Die `setup` Benutzerpasswort für den Befehlsgerät.
   - Spitzname Knoten (optional) **:** Ein benutzerfreundlicher Name für den Explore-Knoten. Wenn kein Spitzname eingegeben wird, wird der Knoten durch den Hostnamen identifiziert.
3. Wählen Sie den Mit der Command-Appliance verwalten Checkbox und dann klicken **Verbinde**.

## Stellen Sie den Clusterstatus wieder her

In den seltensten Fällen kann der Explore-Cluster möglicherweise nicht von einem `Red` Status, wie in der Status Abschnitt über die Erkunden Sie den Cluster-Status Seite. Wenn dieser Zustand eintritt, ist es möglich, den Cluster auf einen `Green` Bundesstaat.

Wenn Sie den Clusterstatus wiederherstellen, wird der Explore-Cluster mit den neuesten gespeicherten Informationen über die Explore-Knoten im Cluster und alle anderen verbundenen Discover- und Command-Appliances aktualisiert.

**Wichtig:** Wenn Sie Ihren Explore-Cluster kürzlich neu gestartet haben, kann es eine Stunde dauern, bis der Cluster-Status erreicht ist `Green` wird angezeigt, und eine

Wiederherstellung des Cluster ist möglicherweise nicht erforderlich. Wenn Sie sich nicht sicher sind, ob Sie den Clusterstatus wiederherstellen sollten, wenden Sie sich an ExtraHop-Unterstützung.

1. In der Erkunden Sie die Cluster-Einstellungen Abschnitt, klicken **Clusterstatus wiederherstellen**.
2. Auf dem Clusterstatus wiederherstellen Seite, klick **Clusterstatus wiederherstellen**.
3. klicken **Cluster wiederherstellen** zur Bestätigung.