

Stellen Sie eine Verbindung zu ExtraHop Cloud Services her

Veröffentlicht: 2024-04-10

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

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

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

▶ **Sehen Sie sich die entsprechende Schulung an: [Stellen Sie eine Verbindung zu ExtraHop Cloud Services her](#)**

Bevor Sie beginnen

- Reveal (x) 360-Systeme werden automatisch mit den ExtraHop Cloud Services verbunden. Möglicherweise müssen Sie jedoch [Zugriff über Netzwerkfirewalls zulassen](#).
 - Sie müssen die entsprechende Lizenz auf dem ExtraHop-System anwenden, bevor Sie eine Verbindung zu ExtraHop Cloud Services herstellen können. Sehen Sie die [Häufig gestellte Fragen zur Lizenz](#) für weitere Informationen.
 - Sie müssen eingerichtet haben oder [System- und Zugriffsadministrationsrechte](#) um auf die Administrationseinstellungen zuzugreifen.
1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
 2. Klicken Sie im Abschnitt Netzwerkeinstellungen auf **ExtraHop Cloud-Dienste**.
 3. Klicken Sie **Allgemeine Geschäftsbedingungen** um den Inhalt zu lesen.
 4. Lesen Sie die Allgemeinen Geschäftsbedingungen und aktivieren Sie dann das Kontrollkästchen.
 5. Klicken Sie **Stellen Sie eine Verbindung zu ExtraHop Cloud Services her**.
Nachdem Sie eine Verbindung hergestellt haben, wird die Seite aktualisiert und zeigt Status- und Verbindungsinformationen für jeden Dienst an.
 6. Optional: Wählen Sie im Abschnitt Machine Learning Service eine oder mehrere erweiterte Funktionen aus:

- Aktiviere den AI Search Assistant, indem du auswählst **Ich bin damit einverstanden, den KI-Suchassistenten zu aktivieren und Suchanfragen in natürlicher Sprache an ExtraHop Cloud Services zu senden.** (NDR-Modul erforderlich)
- Aktivieren Sie Expanded Threat Intelligence, indem Sie **Ich bin damit einverstanden, IP-Adressen, Domainnamen, Hostnamen, Datei-Hashes und URLs an ExtraHop Cloud Services zu senden.**
- Aktivieren Sie die kollektive Bedrohungsanalyse, indem Sie **Ich bin damit einverstanden, Domainnamen, Hostnamen, Datei-Hashes und externe IP-Adressen zu ExtraHop Cloud Services beizutragen.**

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

Konfigurieren Sie Ihre Firewall-Regeln

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

Offener Zugang zu Cloud-Diensten

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

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

Offener Zugang zu Cloud Recordstore

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

- bigquery.googleapis.com
- bigquerystorage.googleapis.com
- oauth2.googleapis.com
- www.googleapis.com
- www.mtls.googleapis.com
- iamcredentials.googleapis.com

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


Zusätzlich zur Konfiguration des Zugriffs auf diese Domänen müssen Sie auch die [globale Proxyserver-Einstellungen](#).

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

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

Bevor Sie beginnen

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

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

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

Zertifikatsvalidierung umgehen

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

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



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

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

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

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