

Stellen Sie eine Verbindung zu ExtraHop Cloud Services her

Veröffentlicht: 2024-10-26

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. AI Search Assistant kann derzeit nicht für die folgenden Regionen aktiviert werden:
 - Asien-Pazifik (Singapur, Sydney, Tokio)
 - Europa (Frankfurt, Paris)
 - 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

- 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 eingesetzt wird, müssen Sie den Zugriff auf ExtraHop Cloud Services öffnen. Für RevealX 360-Systeme, die mit selbstverwalteten Systemen verbunden sind 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 von der 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 RevealX 360 Premium Investigation

Für den Zugriff auf RevealX 360 Premium Investigation ist Ihr Sensoren muss in der Lage sein, auf 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 in der Europäischen Union 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 Proxy-Servereinstellungen](#) .

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 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. 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 **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 Nutzernamen 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

Wenn Sie eine bestehende Lizenz von einem ExtraHop-System auf ein anderes 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**.