RevealX 360 Installations- und Administrationshandbuch

Veröffentlicht: 2024-10-26

Nachdem Sie Ihre erste E-Mail von ExtraHop Networks erhalten haben, müssen Sie einige Verfahren ausführen, bevor Sie mit der Analyse Ihres Datenverkehrs beginnen können. Dieses Handbuch enthält Verfahren für die grundlegende Einrichtung und Verwaltung des RevealX 360-Systems.

Video: Sehen Sie sich die entsprechende Schulung an: Überblick über die RevealX 360-Administration

Aktiviere dein Administratorkonto

Das Recht zur System- und Zugriffsverwaltung wird der E-Mail-Adresse gewährt, die Sie bei der Registrierung angegeben haben.

1. Öffnen Sie Ihre Welcome to ExtraHop RevealX 360-E-Mail.
2. Klicken Sie auf den URL-Link zu Ihrer RevealX 360-Umgebung.
3. Geben Sie auf der Anmeldeseite Ihre E-Mail-Adresse und das temporäre Passwort ein, das in der E-Mail enthalten ist.
4. klicken **Einloggen**.
5. Geben Sie auf dem Bildschirm Passwort ändern ein neues Passwort in beide Passwortfelder ein und klicken Sie dann auf **Senden**.
6. Scannen Sie auf der Einrichtungsseite für die Multi-Factor Authentication den QR-Code oder geben Sie den Code, der in Ihrer Authenticator-App angezeigt wird, manuell ein.
7. Geben Sie den von Ihrer Authentifizierungs-App bereitgestellten Code in das **Kode** Feld und dann klicken **Einrichtung abschließen**.
8. Klicken Sie auf der Seite Erfolg auf **Fortfahren**.

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.

Benutzer hinzufügen und verwalten

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann auf **Benutzerzugriff**.
2. Klicken Sie im Abschnitt Benutzer auf **Benutzer anzeigen**.
3. Klicken Sie **Erstellen**.
4. Geben Sie die E-Mail-Adresse, den Vor- und Nachnamen des neuen Benutzers ein.
5. Wählen Sie im Abschnitt Sensorzugriff Sensor-Tags aus, um Sensoren Paketzugriff zu gewähren.

   Klicken Sie **Sensor-Tags verwalten** um Tags zu erstellen, zu bearbeiten oder zu löschen. Erfahre mehr über Sensor-Zugriffskontrolle.
6. Wählen Sie im Abschnitt Systemzugriff eine der folgenden Berechtigungen aus.

Privileg	Beschreibung
System- und Zugriffsverwaltung	Erstellen und ändern Sie alle Objekte und Einstellungen, einschließlich Administrationsseiten, in RevealX 360.
Verwaltung des Systems	Erstellen und ändern Sie Objekte und Einstellungen, ausgenommen Benutzerzugriff und API-Zugriff auf der Administrationsseite.
Vollständig schreiben	Erstellen und ändern Sie alle Objekte und Einstellungen, mit Ausnahme der Administrationsseiten.
Eingeschränktes Schreiben	Erstellen, ändern und teilen Sie Dashboards. Erstellen und ändern Sie Tuning-Regeln. Erstellen und ändern Sie Regeln für Erkennung-Bedrohungsübersicht Bedrohungsinformationen.

Privileg	Beschreibung
Persönliches Schreiben	Erstellen Sie persönliche Dashboards und ändern Sie Dashboards, die mit dem angemeldeten Benutzer geteilt werden.
Vollständig schreibgeschützt	Objekte im ExtraHop-System anzeigen.
Eingeschränkter Schreibschutz	Zeigt Dashboards an, die mit diesem Benutzer geteilt wurden.

7. Wählen Sie im Abschnitt NDR-Modulzugriff eine der folgenden Berechtigungen aus.

Privileg	Beschreibung
Voller Zugriff	Zugriff auf Netzwerkerkennungen.
Kein Zugriff	Kein Zugriff auf Netzwerkerkennungen.

8. Wählen Sie im Abschnitt NPM-Modulzugriff eine der folgenden Berechtigungen aus.

Privileg	Beschreibung
Voller Zugriff	Zugriff auf Leistungserkennungen.
Kein Zugriff	Kein Zugriff auf Leistungserkennungen.

9. In der **Zugriff auf Pakete und Sitzungsschlüssel** Abschnitt, wählen Sie eine der folgenden Berechtigungen aus:

Privileg	Beschreibung
Pakete und Sitzungsschlüssel	Suchen und laden Sie Pakete und zugehörige Sitzungsschlüssel herunter.
Nur Pakete	Pakete suchen und herunterladen.
Nur Paket-Header	Suchen Sie nach Paket-Headern und laden Sie sie herunter.
Nur Paketsegmente	Sucht und lädt eine festgelegte Anzahl von Bytes am Anfang eines Paket herunter. Standardmäßig beträgt die Anzahl der herunterladbaren Byte 64. Passen Sie die Anzahl der herunterladbaren Byte mit der Einstellung Packet Slice Download Control unter an Globale Richtlinien.
Kein Zugriff	Kein Zugriff auf Pakete.

10. Klicken Sie **Speichern**.
    Der Benutzer erhält eine E-Mail mit der URL der RevealX 360-Umgebung und seinem temporären Passwort. Das temporäre Passwort läuft in 7 Tagen ab.
11. Klicken Sie **Erledigt**.

Benutzereinstellungen ändern

Sie können die zugewiesenen Berechtigungsstufen ändern, die Konfiguration der Multi-Faktor-Authentifizierung zurücksetzen oder den Benutzer löschen.

Benutzerrechte ändern

1. Klicken Sie im Abschnitt Benutzer auf den Namen des Benutzers, den Sie ändern möchten.
2. Wählen Sie im linken Bereich die neue Berechtigungsstufe für den Benutzer aus und klicken Sie dann auf **Speichern**.

Setzen Sie die Multi-Faktor-Authentifizierung zurück

1. Klicken Sie im Abschnitt Benutzer auf den Namen des Benutzers, den Sie ändern möchten.

2. Löschen Sie das **MFA-Konfiguration für diesen Benutzer zurücksetzen**.
   Der Benutzer muss die Multi-Faktor-Authentifizierung konfigurieren, wenn er sich das nächste Mal bei RevealX 360 anmeldet.

Einen Benutzer löschen

1. Klicken Sie im Abschnitt Benutzer auf den Namen des Benutzers, den Sie ändern möchten.
2. Klicken Sie **Löschen**.
3. Wählen Sie eine der folgenden Optionen aus:
   - **Übertrage Dashboards, Sammlungen und Aktivitätskarten, die Eigentum von *<username>* an den folgenden Benutzer:** und wählen Sie dann einen neuen Benutzer aus der Dropdownliste aus.
   - **Lösche alle Dashboards, Sammlungen und Aktivitätskarten, die Eigentum von *<username>***
4. Klicken Sie **Löschen**.

Globale Richtlinien verwalten

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

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann **Benutzerzugriff**.
2. Geben Sie im Abschnitt Globale Richtlinien eine oder mehrere der folgenden Optionen an.

Option	Description
Steuerung zum Bearbeiten von Gerätegruppen	Wählen Sie diese Option, um zu steuern, ob alle Benutzer mit eingeschränkten Schreibrechten Gerätegruppen erstellen und bearbeiten können. Wenn diese Richtlinie ausgewählt ist, können alle Benutzer mit eingeschränktem Schreibzugriff Gerätegruppen erstellen und andere Benutzer mit eingeschränktem Schreibzugriff als Redakteure zu ihren Gerätegruppen hinzufügen.
Packet Slice-Downloadsteuerung	Geben Sie die Anzahl der Byte an, die Benutzer mit den Rechten nur für Paketsegmente herunterladen können. Bytes werden vom Anfang des Paket an gezählt. Der Standardwert dieser Einstellung ist 64 Byte, was in der Regel den Paket-Header bei Downloads beinhaltet.
Standard-Dashboard	Geben Sie das Dashboard an, das Benutzer sehen, wenn sie sich am System anmelden. Nur Dashboards, die mit allen Benutzern geteilt werden, können als globaler Standard festgelegt werden. Benutzer können diese Standardeinstellung überschreiben über das Befehlsmenü eines beliebigen Dashboard.
Passwort für die Dateiextraktion	(Nur NDR-Modul) Geben Sie ein erforderliches Passwort an, das Sie mit zugelassenen Benutzern zum Entpacken teilen können Dateien, die aus einer Paketabfrage extrahiert und heruntergeladen wurden.

3. Klicken Sie **Änderungen speichern**.

Eine Zulassungsliste konfigurieren

Konfigurieren Sie eine Liste von IPv4-Adressen und CIDR-Blöcken, die auf RevealX 360 zugreifen dürfen.

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann **Benutzerzugriff**.
2. Klicken Sie im Abschnitt Zulassungsliste auf **Zulassungsliste aktivieren**.
3. Geben Sie eine kommagetrennte Liste der IPv4-Adressen oder CIDR-Blöcke ein, die auf das System zugreifen dürfen. IPv6-Adressen werden nicht unterstützt.
4. Klicken Sie **Speichern**. Es kann mehrere Minuten dauern, bis die Zulassungsliste aktiv wird.

Konfigurieren Sie die Systemzeit

Auf der Seite Systemzeit werden die Standardsystemzeiteinstellungen und die für Ihr ExtraHop-System konfigurierte Standardanzeigezeit angezeigt.

Hier sind einige Überlegungen zu den Systemzeiteinstellungen in RevealX 360:

- Sie müssen über Systemadministratorrechte oder besser verfügen, um Änderungen vornehmen zu können.
- Die Standardsystemzeit ist eine globale Zeitzone, die auf Ihr ExtraHop-System angewendet wird.
- Die Standardanzeigezeit für Benutzer ist die Zeitzone, die alle Benutzer im ExtraHop-System sehen, sofern ein Benutzer nicht manuell ihre angezeigte Zeitzone.

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann **Die gesamte Verwaltung**.
2. Klicken Sie im Abschnitt Konsoleneinstellungen auf **Systemzeit**.
3. Aus dem Standard-Systemzeit Wählen Sie in der Dropdownliste die gewünschte Zeitzone aus.
4. Aus dem Standardanzeigezeit für Benutzer Abschnitt, wählen Sie eine der folgenden Optionen aus:
   - Uhrzeit des Browsers
   - Systemzeit
   - UTC
5. Klicken Sie **Änderungen speichern**.

Sensoren

Paketsensoren erfassen, speichern und analysieren Metrik Daten über Ihr Netzwerk.

Sie können Ihrem RevealX 360-System selbstverwaltete Sensoren hinzufügen, die Sensorfirmware aktualisieren und Sensor-Tags zu einzelnen oder Gruppen von Sensoren hinzufügen. Sie können Sensor Access Control auch aktivieren, um Benutzer daran zu hindern, Pakete auf bestimmte Sensoren herunterzuladen.

Sensoren anschließen

Hinzufügen Sensoren zu RevealX 360, um Ihren Netzwerkverkehr zu überwachen.

Selbstverwaltet Sensoren und Paketspeicher können auch von der RevealX 360-Konsole aus verbunden werden. Beachten Sie, dass Sie, wenn Sie eine bestehende Konsole haben, die Verbindung trennen müssen, bevor Sie Ihre selbstverwaltete Konsole verbinden Sensoren zu RevealX 360 .

- Stellen Sie über selbstverwaltete Sensoren eine Verbindung zu RevealX 360 her

Rüsten Sie die angeschlossenen Sensoren in RevealX 360 auf

Administratoren können ein Upgrade durchführen Sensoren die mit RevealX 360 verbunden sind.

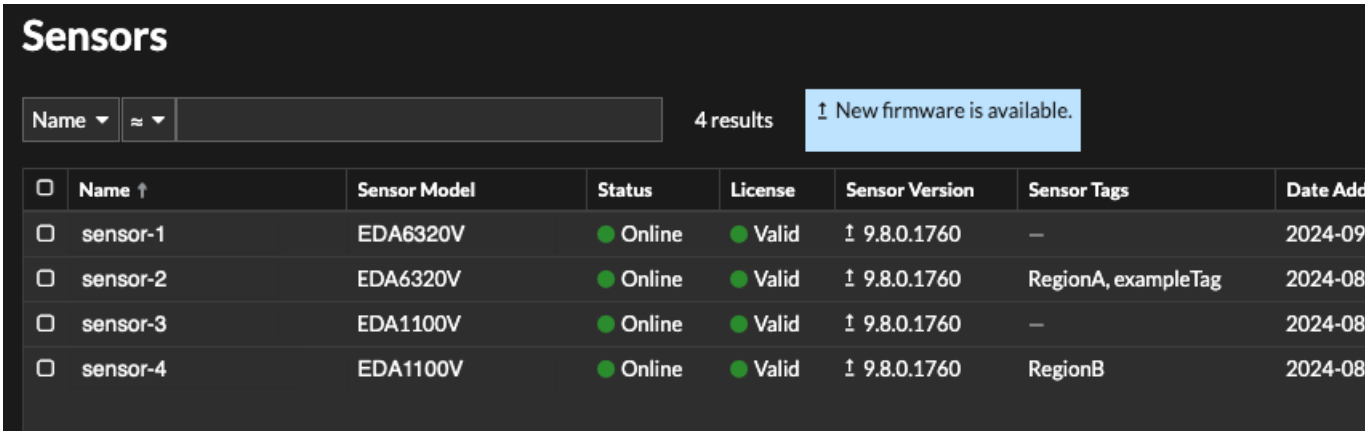
Bevor Sie beginnen

- Ihr Benutzerkonto muss über Rechte auf RevealX 360 für System- und Zugriffsadministration oder Systemadministration verfügen.

Hier sind einige Überlegungen zur Aufrüstung von Sensoren:

- Sensoren müssen mit 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 **Fühler**.
   Sensoren, die für ein Upgrade in Frage kommen, zeigen einen Aufwärtspfeil in der Sensorversion Feld.



2. Markieren Sie das Kästchen neben jedem Sensor die Sie aktualisieren möchten.
3. In der Angaben zum Sensor Bereich, wählen Sie die Firmware-Version aus dem **Verfügbare Firmware** Dropdownliste.
   In der Dropdownliste werden nur Versionen angezeigt, die mit den ausgewählten Versionen kompatibel sind Sensoren.

   Nur die ausgewählten Sensoren für die ein Firmware-Upgrade verfügbar ist , finden Sie im Fühler Bereich „Details“.
4. Klicken Sie **Firmware installieren**.
   Wenn das Upgrade abgeschlossen ist, wird Sensorversion Das Feld wurde mit der neuen Firmware-Version aktualisiert.

Erstellen Sie ein Sensor-Tag

Sensor-Tags ermöglichen Administratoren die einfache Identifizierung eines einzelnen Sensors oder einer Gruppe von Sensoren. Administratoren können Sensoren mit Sensor-Tags kennzeichnen und die Tags dann für andere Aufgaben verwenden, z. B. um einer Benutzergruppe Paketzugriff auf eine bestimmte Gruppe von Sensoren zu gewähren.

Bevor Sie beginnen

- Ihr Benutzerkonto muss Privilegien auf RevealX 360 für die Systemadministration.

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann **Fühler**.
2. Klicken Sie in der Sensortabelle auf einen Sensor.
3. Unter Sensor-Tags in der Angaben zum Sensor Panel, klicken **Sensor-Tags verwalten**.
4. In der Sensor-Tags verwalten Panel, klicken **Erstellen**.
5. Geben Sie einen Tag-Namen ein und klicken Sie auf **Speichern**.
6. Wählen Sie die Tags aus, die Sie dem Sensor hinzufügen möchten.
   Sensoren können mehrere Tags haben und ein Tag kann auf mehrere Sensoren aufgebracht werden.

Nächste Schritte
Nachdem Sie die Sensoren markiert haben, können Sie sie aktivieren Sensorzugriffskontrolle um den Zugriff auf Pakete nur auf diese Sensoren zu beschränken.

Sensor-Zugriffskontrolle

ExtraHop-Administratoren können den Benutzerzugriff auf Pakete auf bestimmten Sensoren einschränken. Nachdem die Sensorzugriffskontrolle aktiviert ist, können Benutzer nur Pakete für Sensoren anzeigen und herunterladen , die ihnen zugewiesen wurden.

Wenn Sie beispielsweise möchten, dass Analysten in Region A und Region B nur Zugriff auf Pakete von Sensoren in ihrer jeweiligen Region haben, können Sie Sensor-Tags erstellen genannt `regionA` und `regionB` und fügen Sie diese Tags zu Sensoren in ihrer jeweiligen Region hinzu. Nachdem die Sensor-Tags hinzugefügt wurden, können Sie allen markierten Sensoren Zugriff zuweisen `regionA` für Analysten in Region A, wobei deren Zugriff auf markierte Sensoren eingeschränkt ist `regionB`.

Der Sensorzugriff wird Benutzern direkt in der gewährt ExtraHop IdP oder indem Sie Sensor-Tags SAML-Benutzergruppen zuordnen in Ihr eigener Identitätsanbieter.

Hinweis Die primäre Ebene der Zugriffskontrolle für Pakete, Sitzungsschlüssel und Paket-Header sind Zugriffsrechte für Pakete und Sitzungsschlüssel. Selbst wenn ihnen Sensorzugriff gewährt wird, können Benutzer Pakete nur so weit herunterladen, wie ihnen die ihnen zugewiesenen Rechte zugewiesen wurden.

Administratoren können Benutzern, die über Rechte zum Herunterladen von Paket verfügen, aber keinen Sensorzugriff erhalten haben, eingeschränkten Zugriff gewähren.

Aktivieren Sie die Sensorzugriffskontrolle über den ExtraHop IdP
Administratoren können verwalten, welche Benutzergruppen auf Pakete auf Sensoren im ExtraHop-System zugreifen können, nachdem sie Benutzern über den ExtraHop-IdP Sensoren zugewiesen haben.

Bevor Sie beginnen

- Ihr Benutzerkonto muss Privilegien auf RevealX 360 für System- und Zugriffsadministration.
- Sensoren werden Benutzergruppen über Sensor-Tags zugewiesen. Du musst Erstellen Sie ein Sensor-Tag und fügen Sie ihn einem Sensor hinzu, bevor Sie diesen Sensor einer Benutzergruppe zuweisen können.

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann **Benutzerzugriff**.
2. Klicken Sie im Abschnitt Benutzer auf **Benutzer anzeigen**.
3. Klicken Sie auf einen Benutzer.
4. Wählen Sie im Bereich Benutzerdetails unter Sensorzugriff Sensor-Tags aus, um dem Benutzer Zugriff auf Sensoren zum Herunterladen von Paket zu gewähren, und klicken Sie dann auf **Speichern**.

   Du kannst klicken **Sensor-Tags verwalten** um Tags zu erstellen, zu bearbeiten oder zu löschen. Erfahre mehr über Sensor-Tags.
5. Klicken Sie im Bereich Benutzerdetails auf **Speichern**.
6. Klicken Sie auf **Benutzerzugriff** Breadcrumb oben auf der Seite , um zur Benutzerzugriffsseite zurückzukehren.
7. Klicken Sie im Abschnitt Sensor Access Control auf **Sensorzugriffskontrolle aktivieren**.
8. Markieren Sie im Bereich Sensorzugriffskontrolle bearbeiten das Kontrollkästchen, um Einschränkungen beim Herunterladen von Paket zu aktivieren.
9. Wählen Sie die Zugriffsebene aus, die Benutzern gewährt werden soll, denen gewährt wurde Zugriffsrechte für Pakete und Sitzungsschlüssel, sind aber nicht dem Sensor zugeordnet.

Option	Beschreibung
Eingeschränkter Zugriff	Auf nicht zugewiesenen Sensoren können Benutzer mit Paket-Download-Rechten nur Paket-Header herunterladen.

Option	Beschreibung
Kein Zugriff	Bei nicht zugewiesenen Sensoren haben Benutzer unabhängig von den Download-Rechten keinen Paketzugriff.

10. Klicken Sie **Speichern**.

Ermöglichen Sie die Sensorzugriffskontrolle über Ihren eigenen Identitätsanbieter
Administratoren können festlegen, welche Benutzergruppen auf den einzelnen Sensor im ExtraHop-System auf Pakete zugreifen können, indem sie einen SAML-Attributwert hinzufügen, der Sensor-Tags Benutzergruppen zuordnet.

Bevor Sie beginnen

- Ihr Benutzerkonto muss Privilegien auf RevealX 360 für System- und Zugriffsadministration.
- Das musst du haben hat einen SAML 2.0-Identitätsanbieter konfiguriert.
- Sensoren werden Benutzergruppen über Sensor-Tags zugewiesen. Du musst Erstellen Sie ein Sensor-Tag und fügen Sie ihn einem Sensor hinzu, bevor Sie diesen Sensor einer Benutzergruppe zuweisen können.

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann **Benutzerzugriff**.
2. Klicken Sie im Abschnitt Sensor Access Control auf **Sensorzugriffskontrolle aktivieren**.
3. Markieren Sie im Bereich Sensorzugriffskontrolle bearbeiten das Kontrollkästchen, um die Einschränkungen beim Herunterladen von Paket zu aktivieren.
4. Wählen Sie die Zugriffsebene aus, die Benutzern gewährt werden soll, denen gewährt wurde Zugriffsrechte für Pakete und Sitzungsschlüssel, sind aber nicht dem Sensor zugeordnet.

Option	Beschreibung
Eingeschränkter Zugriff	Auf nicht zugewiesenen Sensoren können Benutzer mit Paket-Download-Rechten nur Paket-Header herunterladen.
Kein Zugriff	Bei nicht zugewiesenen Sensoren haben Benutzer unabhängig von den Download-Rechten keinen Paketzugriff.

5. Geben Sie unter SAML-Konfiguration einen Attributnamen für die Sensorzugriffskontrolle ein.

   Hinweis: Attributnamen und -werte müssen mit den Namen und Werten übereinstimmen, die Ihr Identitätsanbieter in SAML-Antworten einbezieht, die konfiguriert werden, wenn Sie die ExtraHop-Anwendung zu einem Anbieter hinzufügen.
6. Die Attributwerte sind eine Liste der Sensor-Tags, die auf dem ExtraHop-System erstellt wurden. Geben Sie eine Benutzergruppe neben einem Sensor-Tag ein, um den Sensor dieser Gruppe zuzuweisen.

   Sie können einen Sensor nur einer Benutzergruppe zuweisen. Der Name der Benutzergruppe muss mit dem in Ihrem IdP definierten Benutzergruppennamen übereinstimmen.
7. Klicken Sie **Speichern**.

   Wichtig: Alle aktiven Benutzer werden nach dem Speichern der aktualisierten Konfiguration abgemeldet.

AI Search Assistant aktivieren

Mit dem KI-Suchassistenten können Sie mit Fragen oder Aufforderungen in natürlicher, alltäglicher Sprache nach Geräten suchen, um schnell komplexe Abfragen zu erstellen.

Der AI Search Assistant nutzt ein LLM eines Drittanbieters. Benutzeraufforderungen werden nicht für LLM-Schulungen bereitgestellt oder vom LLM gespeichert, können aber vom ExtraHop-System zur

Produktverbesserung gespeichert werden. Sehen Sie die Häufig gestellte Fragen zum AI-Suchassistenten für weitere Informationen.

Bevor Sie beginnen

- Ihr Benutzerkonto muss Privilegien auf RevealX 360 für System- und Zugriffsadministration.
- Ihr RevealX 360-System muss verbunden mit ExtraHop Cloud Services.
- AI Search Assistant kann derzeit nicht auf ExtraHop-Systemen aktiviert werden, die eine Verbindung zu ExtraHop Cloud Services aus den folgenden Regionen herstellen:
  - Asien-Pazifik (Singapur, Sydney, Tokio)
  - Europa (Frankfurt, Paris)

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** Symbol und klicken Sie dann **Die gesamte Verwaltung**.
2. Klicken Sie im Abschnitt Konsoleneinstellungen auf **KI-Suchassistent**.
3. Aktivieren Sie den AI-Suchassistenten, indem Sie **Ich bin damit einverstanden, den KI-Suchassistenten zu aktivieren und Suchanfragen in natürlicher Sprache an ExtraHop Cloud Services zu senden**.
4. klicken **Änderungen speichern**.

Nächste Schritte
Finden Sie Geräte mit AI Search Assistant

Rangfolge von Gerätenamen konfigurieren

Entdeckte Geräte werden automatisch anhand mehrerer Netzwerkdatenquellen benannt. Wenn mehrere Namen für ein Gerät gefunden werden, wird eine Standardprioritätsreihenfolge angewendet. Sie können die Rangfolge ändern.

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann **Die gesamte Verwaltung**.
2. Klicken Sie im Abschnitt Konsoleneinstellungen auf **Rangfolge des Gerätenamens**.
3. Klicken und ziehen Sie die Gerätenamen, um eine neue Rangfolge zu erstellen.
4. klicken **Speichern**.
   klicken **Zur Standardeinstellung zurückkehren** um Ihre Änderungen rückgängig zu machen.

Erkennungsverfolgung aktivieren

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

Hinweis Sie müssen die Ticketverfolgung auf allen angeschlossenen Sensoren aktivieren.

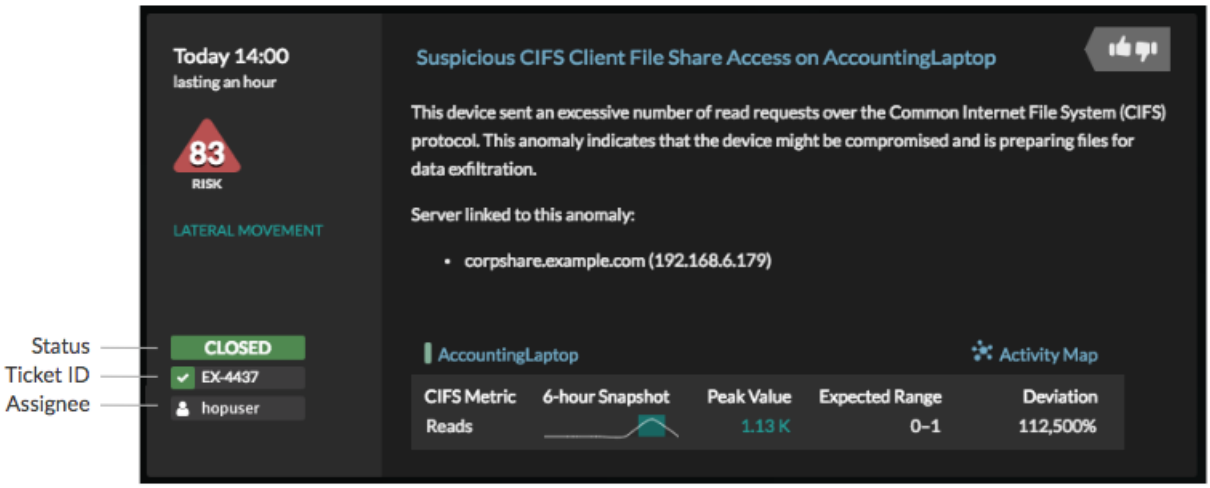
Bevor Sie beginnen

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

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

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann **Die gesamte Verwaltung**.
2. Aus dem Einstellungen der Konsole Abschnitt, klicken **Erkennungsverfolgung**.
3. Wählen Sie eine oder beide der folgenden Methoden für die Nachverfolgung von Erkennungen aus:
   - Wählen **Ermöglichen Sie ExtraHop-Benutzern, Erkennungen aus dem ExtraHop-System heraus zu verfolgen**.
   - Wählen **Ermöglichen Sie externe Integrationen wie SOAR oder Ticket-Tracking-Systeme, um Erkennungen über die ExtraHop Rest API zu verfolgen** .
4. Optional: Nachdem Sie die Option zum Aktivieren externer Integrationen ausgewählt haben, geben Sie die URL-Vorlage für Ihr Ticketsystem an und fügen Sie die *$ Ticket_ID* variabel an der entsprechenden Stelle. Geben Sie beispielsweise eine vollständige URL ein, z. B. `https://jira.example.com/browse/$ticket_id`. Das *$ Ticket_ID* Die Variable wird durch die Ticket-ID ersetzt, die der Erkennung zugeordnet ist.

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



Nächste Schritte

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

- Ticket-Tracking von Drittanbietern für Erkennungen konfigurieren

Ticket-Tracking von Drittanbietern für Erkennungen konfigurieren

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

Bevor Sie beginnen

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

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

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

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

Das vollständige Beispielskript ist am Ende dieses Themas verfügbar.

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

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

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

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

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

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

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

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

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

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

Der vollständige Triggercode sollte dem folgenden Beispiel ähneln:

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

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

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

Ticketinformationen über die REST-API an Erkennungen senden

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

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

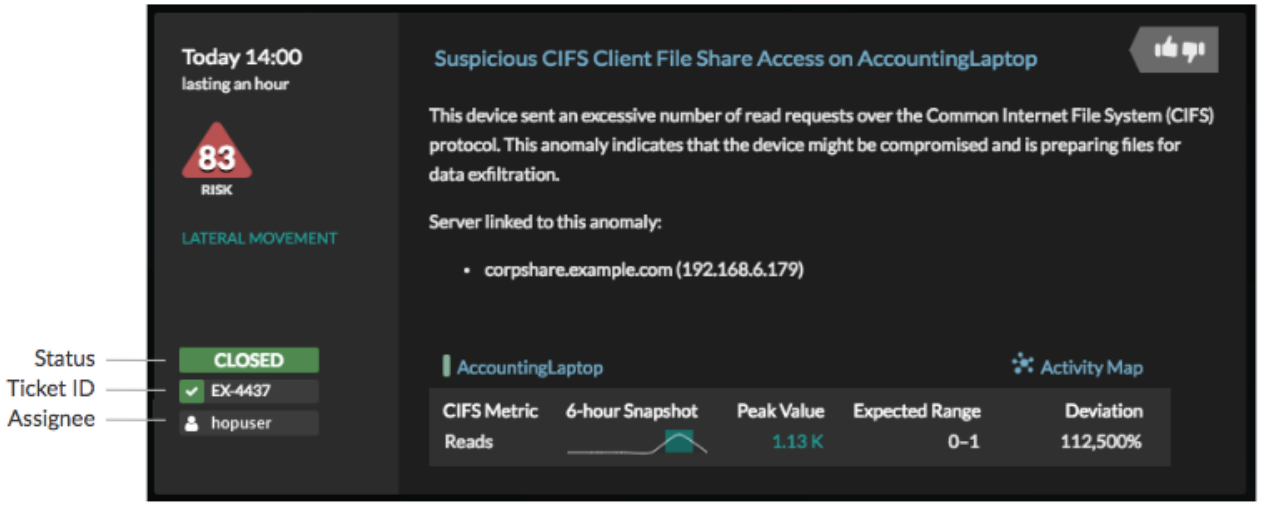
Das folgende Python-Beispielskript entnimmt Ticketinformationen aus einem Python-Array und aktualisiert die zugehörigen Erkennungen auf dem ExtraHop-System.

```
#!/usr/bin/python3

import json
import requests
import csv

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

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

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

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

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

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

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



Status

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

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

Ticket-ID

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

Abtretungsempfänger

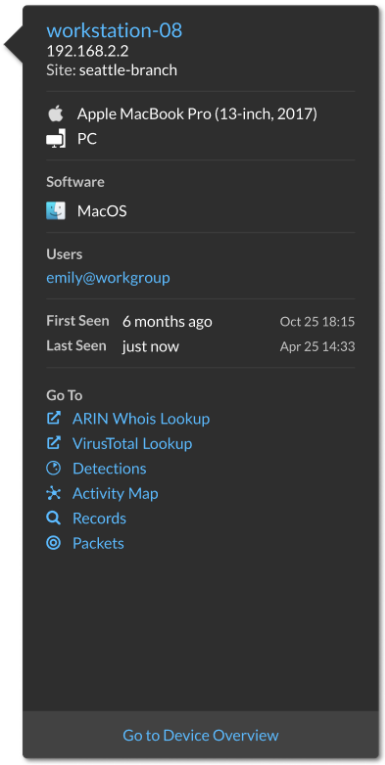
Der Benutzername, der dem Ticket zugewiesen wurde, das mit der Erkennung verknüpft ist. Graue Benutzernamen weisen auf ein Konto hin, das kein ExtraHop-Konto ist.

Endpunkt-Suchlinks konfigurieren

Mit der Endpunktsuche können Sie Tools für externe IP-Adressen angeben, die zum Abrufen von Informationen über Endpunkte innerhalb des ExtraHop-Systems verfügbar sind. Wenn Sie beispielsweise auf eine IP-Adresse klicken oder den Mauszeiger darüber bewegen, werden Links zum Suchtool angezeigt, sodass Sie leicht Informationen zu diesem Endpunkt finden können.

Die folgenden Suchlinks sind standardmäßig konfiguriert und können geändert oder gelöscht werden:

- ARIN Whois-Suche
- VirusTotal-Suche



1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann **Die gesamte Verwaltung**.
2. Klicken Sie im Abschnitt Konsoleneinstellungen auf **Endpunktsuche**.
3. In der **URL-Vorlage** Feld, geben Sie die URL des Suchtools ein.

   Die URL muss enthalten `$ip` Variable, die bei der Suche durch die IP-Adresse des Endpunkt ersetzt wird. Zum Beispiel `https://search.arin.net/rdap/?query=$ip`
4. In der **Name anzeigen** Feld, geben Sie den Namen Link so ein, wie er angezeigt werden soll.
5. Wählen Sie eine der folgenden Optionen Optionen anzeigen:
   - Diesen Link auf allen Endpunkten anzeigen
   - Diesen Link auf externen Endpunkten anzeigen
   - Diesen Link auf internen Endpunkten anzeigen
   - Diesen Link nicht anzeigen
6. Klicken Sie **Speichern**.

Integrationen

Auf der Seite Integrationen wird ein Katalog mit Produkten und Lösungen von Drittanbietern angezeigt, die mit dem ExtraHop-System funktionieren. Integrationen können Aufschluss darüber geben, wie Ihre Geräte in Ihrer Umgebung kommunizieren, oder Ihre Fähigkeit verbessern, Bedrohungen und Probleme zu untersuchen. Klicken Sie auf eine Kachel, um weitere Informationen zur Integration anzuzeigen.

Anforderungen und Konfigurationen variieren je nach Integration. Bei einigen Integrationen müssen Sie eine App oder ein Add-on installieren und konfigurieren, und bei den meisten Integrationen müssen Sie Anmeldedaten erstellen, um auf den ExtraHop REST-API.

Für Integrationen, die Daten übertragen, können Sie Ihren Sicherheitskontrollen statische Quell-IP-Adressen hinzufügen, um Anfragen von der RevealX 360-Konsole aus zuzulassen. Fügen Sie die für Ihre Region vorgesehenen IP-Adressen hinzu:

Vereinigte Staaten (US)

- 44,239,88,18
- 54,191,141,54

Europa, Naher Osten und Afrika (EMEA)

- 18,153,130
- 18,199,126,90

Asien-Pazifik (APAC)

- 52,64,254,4
- 54,66,82,248

Mehrstufige Authentifizierung

Die Multifaktor-Authentifizierung (MFA) ist eine Sicherheitsverbesserung, bei der Sie zwei Arten von Anmeldedaten angeben müssen, wenn Sie sich in Ihr Konto einloggen. Zusätzlich zu Ihren ExtraHop-Anmeldeinformationen müssen Sie Anmeldedaten aus einer Authentifikator-App eines Drittanbieters angeben.

Wählen Sie eine Authentifizierungsanwendung aus, laden Sie sie auf Ihr Gerät herunter und generieren Sie sichere, sechsstellige Codes, wenn Sie sich in Ihr RevealX 360-System einloggen.

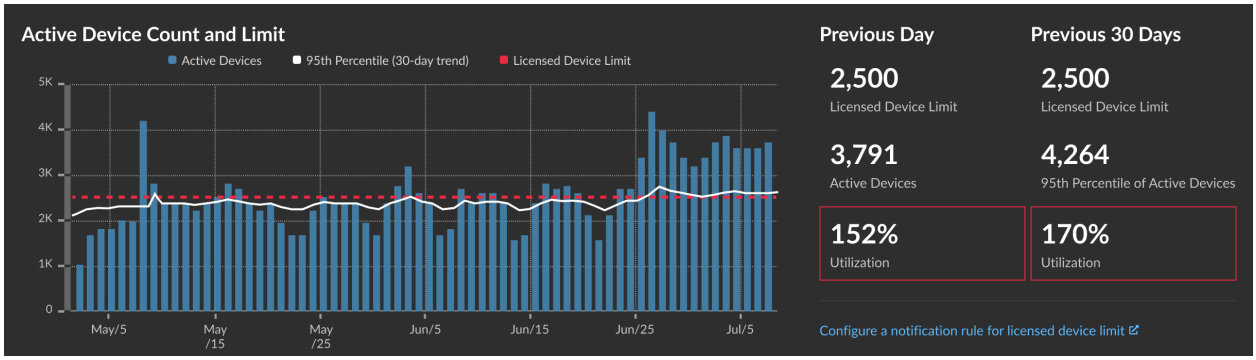
Es stehen viele Authenticator-Apps zur Auswahl. Die folgenden Schritte sind eine allgemeine Richtlinie, aber Sie sollten auch die Hilfedokumentation für die von Ihnen ausgewählte App lesen.

1. Wählen Sie ein Gerät, z. B. einen Computer oder ein mobiles Gerät (Telefon oder Tablet), auf dem Sie Apps installieren können.
2. Laden Sie eine Authentifizierungs-App herunter und installieren Sie sie auf dem Gerät. Hier sind einige beliebte Optionen:
   - Android und iOS: Google Authenticator, Authy
   - Windows und macOS: 1Password, OTP Manager
   - Chrome-Erweiterungen: Authenticator
3. Öffnen Sie einen neuen Browser und melden Sie sich bei Ihrem ExtraHop RevealX 360-System an.
4. Folgen Sie den Anweisungen, um den Code zu scannen oder einzugeben, der auf dem Einrichtungsbildschirm der ExtraHop Multi-Factor Authentication erscheint, und geben Sie dann die Anmeldedaten ein, die Sie von Ihrer Authenticator-App erhalten haben.

Anzahl und Limit der aktiven Gerät

Mithilfe der Tabelle zur Anzahl und zum Limit aktiver Geräteanzahl auf der Administrationshauptseite können Sie überwachen, ob die Anzahl Ihrer aktiven Geräte das lizenzierte Limit überschritten hat. Beispielsweise sind für ein ExtraHop-System mit einem Frequenzband von 20.000 bis 50.000 Geräten bis zu 50.000 Geräte zulässig.

klicken **Systemeinstellungen** und klicken Sie dann **Die gesamte Verwaltung** um das Diagramm anzusehen.



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

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

Auf dieser Seite werden auch die folgenden Metriken angezeigt:

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

Sie können eine Systembenachrichtigungsregel erstellen, die Sie warnt, wenn sich die Auslastung der lizenzierten Geräte dem Limit nähert (über 80%) or over (exceeds 100%). Die prozentualen Grenzwerte können bei der Erstellung einer Regel angepasst werden. Wenn Sie feststellen, dass Sie sich ständig dem lizenzierten Limit nähern oder es überschreiten, empfehlen wir Ihnen, mit Ihrem Vertriebsteam zusammenzuarbeiten, um in den nächsten verfügbaren Kapazitätsbereich zu wechseln.

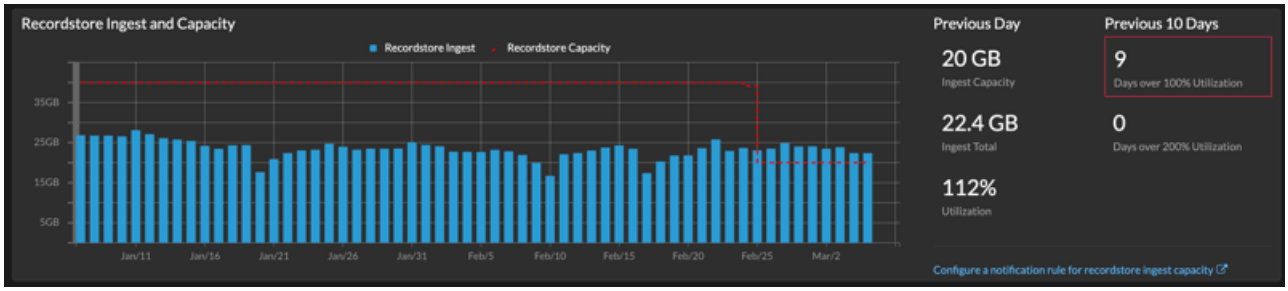
Aufnahme und Kapazität aufzeichnen

Mit dem Diagramm „Aufnahme und Kapazität von Datensatz“ auf der Hauptseite „Administration“ können Sie die Aufnahme- und Kapazitätsniveaus von Datensätzen überwachen und überprüfen, ob das Kapazitätslimit für Ihre Umgebung optimal ist.

Die gestrichelte rote Linie im Balkendiagramm steht für Ihre Rekordaufnahmekapazität, und die blauen Balken stellen die Menge der täglichen Aufnahme während des ausgewählten Intervalls dar. Sie können je nach Umfang des lizenzierten Datensatz-Lookbacks, das rechts neben dem Balkendiagramm angezeigt wird, ein Intervall von 30, 90 oder 180 Tagen auswählen.

Es werden Ingest- und Nutzungsdiagramme angezeigt, damit Sie die Aufzeichnung von Ingest nachverfolgen können. Du kannst eine Regel für Systembenachrichtigungen erstellen um Sie zu warnen, wenn die Aufnahme von Datensatz in der Nähe (über 80%) oder über (über 100%) Ihrer täglichen Aufnahmekapazität liegt.

Wenn Sie feststellen, dass Sie Ihre zugewiesene Kapazität ständig überschreiten, wenden Sie sich an Ihren ExtraHop-Vertriebsmitarbeiter.



Sensor-Zugriffskontrolle

ExtraHop-Administratoren können den Benutzerzugriff auf Pakete auf bestimmten Sensoren einschränken. Nachdem die Sensorzugriffskontrolle aktiviert ist, können Benutzer nur Pakete für Sensoren anzeigen und herunterladen , die ihnen zugewiesen wurden.

Wenn Sie beispielsweise möchten, dass Analysten in Region A und Region B nur Zugriff auf Pakete von Sensoren in ihrer jeweiligen Region haben, können Sie Sensor-Tags erstellen genannt `regionA` und `regionB` und fügen Sie diese Tags zu Sensoren in ihrer jeweiligen Region hinzu. Nachdem die Sensor-Tags hinzugefügt wurden, können Sie allen markierten Sensoren Zugriff zuweisen `regionA` für Analysten in Region A, wobei deren Zugriff auf markierte Sensoren eingeschränkt ist `regionB`.

Der Sensorzugriff wird Benutzern direkt in der gewährt ExtraHop IdP oder indem Sie Sensor-Tags SAML-Benutzergruppen zuordnen in Ihr eigener Identitätsanbieter.

Hinweis Die primäre Ebene der Zugriffskontrolle für Pakete, Sitzungsschlüssel und Paket-Header sind Zugriffsrechte für Pakete und Sitzungsschlüssel. Selbst wenn ihnen Sensorzugriff gewährt wird, können Benutzer Pakete nur so weit herunterladen, wie ihnen die ihnen zugewiesenen Rechte zugewiesen wurden.

Administratoren können Benutzern, die über Rechte zum Herunterladen von Paket verfügen, aber keinen Sensorzugriff erhalten haben, eingeschränkten Zugriff gewähren.

Audit-Protokoll

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

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

Audit-Log-Ereignisse

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

Kategorie	Ereignis
Vereinbarungen	• Eine EULA- oder POC-Vereinbarung wird vereinbart
API	• Ein API-Schlüssel wird erstellt • Ein API-Schlüssel wird gelöscht • Ein Benutzer wird erstellt. • Ein Benutzer wird geändert.

Kategorie	Ereignis
Sensormigration	• Eine Sensormigration wird gestartet • Eine Sensormigration war erfolgreich • Eine Sensormigration ist fehlgeschlagen
Browsersitzungen	• Eine bestimmte Browsersitzung wird gelöscht • Alle Browsersitzungen werden gelöscht
Cloud-Dienste	• Status eines angeschlossenen Sensor wird abgerufen
Konsole	• Ein Sensor wird mit einer Konsole verbunden • Ein Sensor wird von einer Konsole getrennt • Ein ExtraHop-Recordstore oder Packetstore stellt eine getunnelte Verbindung zu einer Konsole her • Die Konsoleninformationen sind festgelegt • Ein Konsolen-Spitzname ist festgelegt • Einen Sensor aktivieren oder deaktivieren • Der Sensor wird aus der Ferne betrachtet • Eine Lizenz für einen Sensor wird von einer Konsole überprüft • Eine Lizenz für einen Sensor wird von einer Konsole festgelegt
Armaturenbretter	• Ein Dashboard wird erstellt • Ein Dashboard wird umbenannt • Ein Dashboard wird gelöscht • Ein Dashboard-Permalink, auch Kurzcode genannt, wird geändert • Die Optionen zum Teilen von Dashboards wurden geändert
Datenspeicher	• Die erweiterte Datenspeicherkonfiguration wurde geändert • Der Datenspeicher ist zurückgesetzt • Ein Datenspeicher-Reset wurde abgeschlossen • Anpassungen werden gespeichert • Anpassungen werden wiederhergestellt • Anpassungen werden gelöscht
Erkennungen	• Ein Erkennungsstatus wird aktualisiert • Ein Erkennungsbeauftragter wird aktualisiert • Erkennungshinweise werden aktualisiert • Ein externes Ticket wird aktualisiert • Eine Tuning-Regel wird erstellt • Eine Tuning-Regel wird gelöscht • Eine Tuning-Regel wird geändert • Eine Beschreibung der Tuning-Regel wird aktualisiert • Eine Tuning-Regel ist aktiviert

Kategorie	Ereignis
	• Eine Tuning-Regel ist deaktiviert • Eine Tuning-Regel wird erweitert
Ausnahmedateien	• Eine Ausnahmedatei wird gelöscht
ExtraHop Recordstore Records	• Alle ExtraHop Recordstore-Datensätze werden gelöscht
ExtraHop-Recordstore-Cluster	• Ein neuer ExtraHop-Recordstore-Knoten wird initialisiert • Ein Knoten wird zu einem ExtraHop-Recordstore-Cluster hinzugefügt • Ein Knoten wird aus einem ExtraHop-Recordstore-Cluster entfernt • Ein Knoten tritt einem ExtraHop-Recordstore-Cluster bei • Ein Knoten verlässt einen ExtraHop-Recordstore-Cluster • Ein Sensor oder eine Konsole ist mit einem ExtraHop-Recordstore verbunden • Ein Sensor oder eine Konsole ist von einem ExtraHop-Recordstore getrennt • Ein ExtraHop-Recordstore-Knoten wurde entfernt oder fehlt, aber nicht über eine unterstützte Schnittstelle
ExtraHop Aktualisierungsservice	• Eine Entdeckungskategorie wird aktualisiert • Eine Erkennungsdefinition wird aktualisiert • Ein Erkennungsauslöser wird aktualisiert • Eine Ransomware-Definition wird aktualisiert • Erkennungsmetadaten werden aktualisiert • Erweiterter Erkennungsinhalt wird aktualisiert
Firmware	• Die Firmware wurde aktualisiert
Globale Richtlinien	• Die globale Richtlinie für die Bearbeitungssteuerung von Gerätegruppe wurde aktualisiert
Integrationen	• Eine Integration wird aktualisiert
Lizenz	• Eine neue statische Lizenz wird angewendet • Die Lizenzserverkonnektivität wird getestet • Ein Produktschlüssel ist auf dem Lizenzserver registriert • Eine neue Lizenz wird beantragt
Loggen Sie sich in das ExtraHop-System ein	• Eine Anmeldung ist erfolgreich • Eine Anmeldung schlägt fehl
Loggen Sie sich über SSH oder REST API ein	• Eine Anmeldung ist erfolgreich

Kategorie	Ereignis
	• Eine Anmeldung schlägt fehl
Module	• Die Zugriffskontrolle für das NDR-Modul ist aktiviert • Die Zugriffskontrolle für das NPM-Modul ist aktiviert
Netzwerk	• Eine Netzwerkschnittstellenkonfiguration wird bearbeitet • Der Hostname oder DNS Einstellung wurde geändert • Eine Netzwerkschnittstellenroute wird geändert
Offline-Erfassung	• Eine Offline-Capture-Datei wird geladen
PCAP	• Eine Paketerfassungsdatei (PCAP) wird heruntergeladen
Fernzugriff	• Der Fernzugriff für das ExtraHop Support Team ist aktiviert • Der Fernzugriff für das ExtraHop Support Team ist deaktiviert • Fernzugriff für ExtraHop Support ist aktiviert • Der Fernzugriff für ExtraHop Support ist deaktiviert
RPCAP	• Eine RPCAP-Konfiguration wird hinzugefügt • Eine RPCAP-Konfiguration wird gelöscht
Konfiguration ausführen	• Die laufende Konfigurationsdatei ändert sich
SAML-Identitätsanbieter	• Ein Identitätsanbieter wird hinzugefügt • Ein Identitätsanbieter wird geändert • Ein Identitätsanbieter wird gelöscht
SAML-Anmeldung	• Eine Anmeldung ist erfolgreich • Eine Anmeldung schlägt fehl
SAML-Rechte	• Eine Privilegienstufe wird gewährt • Eine Privilegienstufe wurde verweigert
Sensor-Tags	• Ein Sensor-Tag wird erstellt • Ein Sensor-Tag wurde geändert • Ein Sensor-Tag wird gelöscht • Tags auf einem Sensor werden geändert
SSL-Entschlüsselung	• Ein TLS-Entschlüsselungsschlüssel wird gespeichert

Kategorie	Ereignis
SSL-Sitzungsschlüssel	• Ein PCAP-Sitzungsschlüssel wird heruntergeladen
Kundendienst-Konto	• Das Support-Konto ist deaktiviert • Das Support-Konto ist aktiviert • Der Support-SSH-Schlüssel wird neu generiert
Unterstützungsskript	• Ein Standard-Support-Skript wird ausgeführt • Ein früheres Unterstützungsskript-Ergebnis wird gelöscht • Ein Support-Skript wird hochgeladen
Syslog	• Remote-Syslog-Einstellungen werden aktualisiert
System- und Servicestatus	• Das System startet • Das System wird heruntergefahren • Das System wird neu gestartet • Der Bridge-, Capture- oder Portal-Prozess wird neu gestartet • Ein Systemdienst ist aktiviert (z. B. SNMP, Webshell, Management, SSH) • Ein Systemdienst ist deaktiviert (z. B. SNMP, Webshell, /management, SSH)
Systemzeit	• Die Systemzeit ist eingestellt • Die Systemzeit wurde geändert • Die Systemzeit ist rückwärts eingestellt • NTP-Server sind eingerichtet • Die Zeitzone ist eingestellt • Eine manuelle NTP-Synchronisierung wird angefordert
Systembenutzer	• Ein Benutzer wird hinzugefügt • Benutzermetadaten werden bearbeitet • Ein Benutzer wird gelöscht • Ein Benutzerkennwort ist gesetzt • Ein anderer Benutzer als der `setup` Benutzer versucht, das Passwort eines anderen Benutzers zu ändern • Ein Benutzerkennwort wird aktualisiert
TAXII-Feeds	• Ein TAXII-Feed wird hinzugefügt • Ein TAXII-Feed wird geändert • Ein TAXII-Feed wird gelöscht
Informationsgespräche über Bedrohungen	• Ein Bedrohungsübersicht wird archiviert • Eine Bedrohungsübersicht wird wiederhergestellt

Kategorie	Ereignis
ExtraHop Packetstore	• Ein neuer ExtraHop-Paketstore wird initialisiert • Ein Sensor oder eine Konsole ist mit einem ExtraHop-Packetstore verbunden • Ein Sensor oder eine Konsole ist von einem ExtraHop-Packetstore getrennt • Ein ExtraHop-Paketstore wird zurückgesetzt
Tendenzen	• Ein Trend wird zurückgesetzt
Trigger	• Ein Auslöser wird hinzugefügt • Ein Auslöser wird bearbeitet • Ein Auslöser wird gelöscht
Benutzergruppen	• Eine lokale Benutzergruppe wird erstellt • Eine lokale Benutzergruppe wird gelöscht • Eine lokale Benutzergruppe ist aktiviert • Eine lokale Benutzergruppe ist deaktiviert