Reveal (x) 360 Installations- und Administrationshandbuch

Veröffentlicht: 2024-03-20

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 Reveal (x) 360-Systems.

Video: Sehen Sie sich die entsprechende Schulung an: Reveal (x) 360 — Überblick über die Administration

Aktiviere dein Administratorkonto

Die System- und Zugriffsadministrationsberechtigung wird der E-Mail-Adresse gewährt, die Sie bei der Registrierung angegeben haben.

1. Öffnen Sie Ihre Welcome to ExtraHop Reveal (x) 360-E-Mail.
2. Klicken Sie auf den URL-Link zu Ihrer Reveal (x) 360-Umgebung.
3. Geben Sie auf der Anmeldeseite Ihre E-Mail-Adresse und das in der E-Mail enthaltene temporäre Passwort ein.
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-Faktor-Authentifizierung den QR-Code oder geben Sie den angezeigten Code manuell in Ihre Authenticator-App 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 **Weiter**.

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.

Benutzer hinzufügen und verwalten

1. Klicken Sie auf der Reveal (x) 360-Übersichtsseite auf **Systemeinstellungen** und dann klicken **Gesamte Verwaltung**.
2. klicken **Benutzerzugriff**.
3. Klicken Sie im Bereich Benutzer auf **Benutzer ansehen**.
4. klicken **Erstellen**.
5. Geben Sie die E-Mail-Adresse, den Vornamen und den Nachnamen des neuen Benutzers ein.
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 Verwaltungsseiten, in Reveal (x) 360.
Verwaltung des Systems	Erstellen und ändern Sie Objekte und Einstellungen, ausgenommen Benutzerzugriff und API-Zugriff, auf der Administrationsseite.
Vollständiger Schreibvorgang	Erstellen und ändern Sie alle Objekte und Einstellungen, mit Ausnahme der Administrationsseiten.
Eingeschränktes Schreiben	Erstellen, ändern und teilen Sie Dashboards. Erstellen und ändern Sie Optimierungsregeln. Erstellen und ändern Sie Benachrichtigungsregeln für Erkennung- und Bedrohungsinformationen.
Persönliches Schreiben	Erstellen Sie persönliche Dashboards und ändern Sie Dashboards, die für den angemeldeten Benutzer freigegeben wurden.
Vollständig schreibgeschützt	Objekte im ExtraHop-System anzeigen.
Eingeschränkt schreibgeschützt	Dashboards anzeigen, 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.

Privileg	Beschreibung
Kein Zugriff	Kein Zugriff auf Leistungserkennungen.

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

Privileg	Beschreibung
Pakete und Sitzungsschlüssel	Suchen Sie nach Paketen und zugehörigen Sitzungsschlüsseln und laden Sie sie herunter.
Nur Pakete	Suchen Sie nach Paketen und laden Sie sie herunter.
Nur Paketsegmente	Suchen und laden Sie die ersten 64 Byte eines Paket herunter.
Kein Zugriff	Kein Zugriff auf Pakete.

10. klicken **Speichern**.
    Der Benutzer erhält eine E-Mail mit der URL der Reveal (x) 360-Umgebung und seinem temporären Passwort. Das temporäre Passwort läuft in 7 Tagen ab.
11. klicken **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**.

Multi-Faktor-Authentifizierung zurücksetzen

1. Klicken Sie im Abschnitt Benutzer auf den Namen des Benutzers, den Sie ändern möchten.
2. Lösche das **MFA-Konfiguration für diesen Benutzer zurücksetzen**.
   Der Benutzer muss die Multi-Faktor-Authentifizierung konfigurieren, wenn er sich das nächste Mal bei Reveal (x) 360 anmeldet.

Einen Benutzer löschen

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

2. Geben Sie im Abschnitt Globale Richtlinien eine oder mehrere der folgenden Optionen an.

Option	Description
Steuerung zur Bearbeitung 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 Editoren zu ihren Gerätegruppen hinzufügen.
Standard-Dashboard	Geben Sie das Dashboard an, das Benutzern angezeigt wird, 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 aus dem Befehlsmenü eines beliebigen Dashboard.

3. klicken **Änderungen speichern**.

Eine Zulassungsliste konfigurieren

Konfigurieren Sie eine Liste von IPv4-Adressen und CIDR-Blöcken, die auf Reveal (x) 360 zugreifen dürfen.

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

Systemzeit konfigurieren

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

Hier sind einige Überlegungen zu den Systemzeiteinstellungen in Reveal (x) 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 allen Benutzern im ExtraHop-System angezeigt wird, es sei denn, ein Benutzer ändert ihre angezeigte Zeitzone.

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und dann klicken **Systemzeit**.
2. Aus dem Standard-Systemzeit Drop-down-Liste, wählen Sie die gewünschte Zeitzone aus.
3. Aus dem Standardanzeigezeit für Benutzer Abschnitt, wählen Sie eine der folgenden Optionen aus:
   - Browserzeit
   - Systemzeit
   - UTC
4. klicken **Änderungen speichern**.

Vorrang des Gerätenamens

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

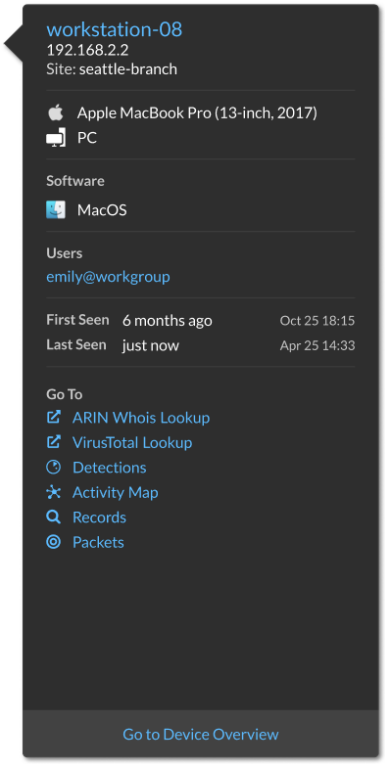
1. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Die gesamte Verwaltung**.
2. Klicken Sie im Abschnitt Konsoleneinstellungen auf **Rangfolge des Gerätenamens**.
3. Klicken und ziehen Sie Gerätenamen, um eine neue Rangfolge zu erstellen.
4. klicken **Speichern**.
   klicken **Auf Standard zurücksetzen** um Ihre Änderungen rückgängig zu machen.

Endpunkt-Lookup-Links 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. Melden Sie sich auf der Administrationsseite von Reveal (x) 360 an.
2. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und dann klicken **Die gesamte Verwaltung**.
3. Klicken Sie im Bereich Konsoleneinstellungen auf **Endpunktsuche**.
4. 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`

5. In der **Name anzeigen** Feld, geben Sie den Namen Link so ein, wie er angezeigt werden soll.
6. 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
7. klicken **Speichern**.

Sensoren anschließen

Hinzufügen Sensoren zu Reveal (x) 360, um Ihren Netzwerkverkehr zu überwachen.

Von ExtraHop verwaltete Enthüllung (x) Sensoren for AWS kann von der Reveal (x) 360-Konsole aus ausgewählt und bereitgestellt werden.

- Stellen Sie Reveal (x) 360-Sensoren für AWS bereit

Selbstverwaltet Sensoren und Packetstores können auch von der Reveal (x) 360-Konsole aus verbunden werden. Beachten Sie, dass Sie, wenn Sie über eine bestehende Konsole verfügen, die Konsole trennen müssen, bevor Sie eine Verbindung zu Ihrer selbstverwalteten Konsole herstellen Sensoren zu Reveal (x) 360.

- Stellen Sie über selbstverwaltete Sensoren eine Verbindung zu Reveal (x) 360 her

Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung (MFA) ist eine Sicherheitsverbesserung, bei der Sie zwei Arten von Anmeldedaten angeben müssen, wenn Sie sich bei Ihrem Konto anmelden. 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 bei Ihrem Reveal (x) 360-System anmelden.

Es stehen viele Authenticator-Apps zur Auswahl. Die folgenden Schritte sind eine allgemeine Richtlinie, Sie sollten jedoch 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 Reveal (x) 360-System an.
4. Folgen Sie den Anweisungen, um den Code zu scannen oder einzugeben, der auf dem Einrichtungsbildschirm für die Multi-Faktor-Authentifizierung von ExtraHop angezeigt wird, und geben Sie dann die von Ihrer Authenticator-App bereitgestellten Anmeldedaten ein.

Rüsten Sie angeschlossene Sensoren in Reveal (x) 360 auf

Administratoren können ein Upgrade durchführen Sensoren die mit Reveal (x) 360 verbunden sind.

Bevor Sie beginnen

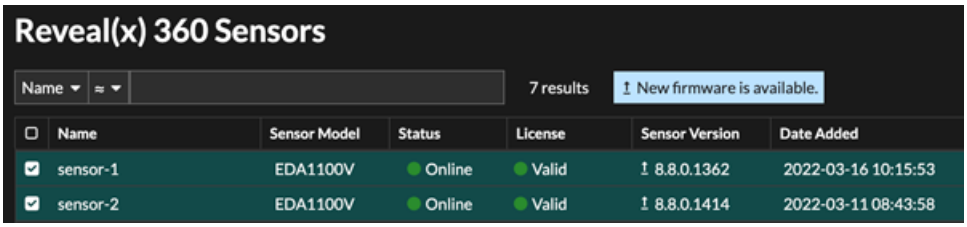
- Ihr Benutzerkonto muss über Rechte auf Reveal (x) 360 für System- und Zugriffsadministration oder Systemadministration verfügen.

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 aktualisieren Sensoren zur gleichen Zeit

1. Loggen Sie sich bei Reveal (x) 360 ein.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Sensorik**.

   Sensoren, die für ein Upgrade in Frage kommen, zeigen einen Aufwärtspfeil in der Sensorversion Feld.



3. Wählen Sie das Kontrollkästchen neben jedem Sensor die Sie aktualisieren möchten.
4. In der Einzelheiten zum Sensor Bereich, wählen Sie die Firmware-Version aus dem **Verfügbare Firmware** Drop-down-Liste.

   In der Dropdownliste werden nur Versionen angezeigt, die mit den ausgewählten Versionen kompatibel sind Sensoren.

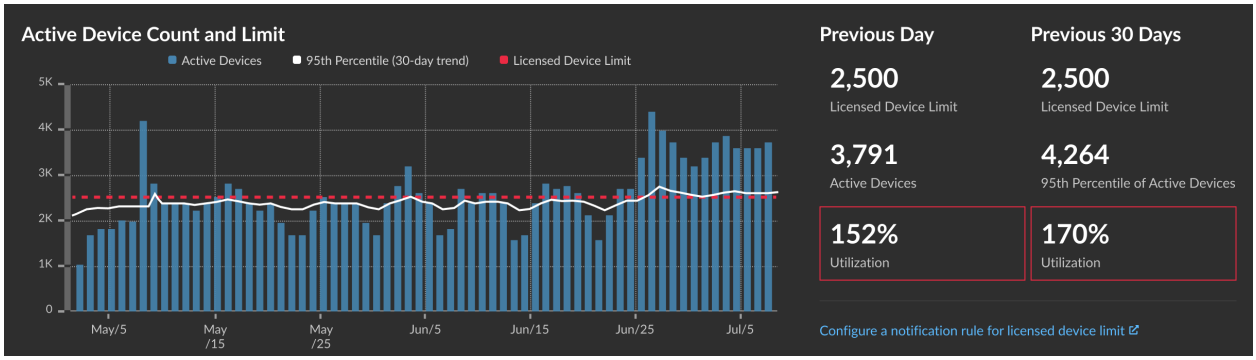
   Nur die ausgewählten Sensoren für die ein Firmware-Upgrade verfügbar ist, erscheinen im Fühler Bereich „Details“.
5. klicken **Firmware installieren**.

   Wenn das Upgrade abgeschlossen ist, Sensorversion Feld wurde mit der neuen Firmware-Version aktualisiert.

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.

Du kannst eine Regel für Systembenachrichtigungen erstellen um Sie zu warnen, wenn die Auslastung Ihrem lizenzierten Gerätelimit nahe (über 80%) oder über (über 100%) liegt. Die Prozentsätze für Grenzwerte können angepasst werden, wenn Sie eine Regel erstellen. Wenn Sie feststellen, dass Sie Ihr Lizenzlimit ständig erreichen oder überschreiten, empfehlen wir Ihnen, mit Ihrem Vertriebsteam zusammenzuarbeiten, um zum nächsten verfügbaren Kapazitätsband überzugehen.

Aufnahme und Kapazität aufzeichnen

Mit dem Diagramm Aufnahme und Kapazität von Datensatz auf der Hauptverwaltungsseite können Sie die Aufnahme und Kapazität von Datensätzen überwachen und sicherstellen, dass das Kapazitätslimit für Ihre Umgebung optimal ist.

Die gestrichelte rote Linie in der Tabelle steht für die Rekordkapazität Ihres Abonnements, und die blauen Balken stehen für die Menge der täglich aufgenommenen Daten bis zu den letzten 60 Tagen.

Du kannst eine Regel für Systembenachrichtigungen erstellen um Sie zu warnen, wenn die Recordstore-Aufnahmekapazität 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.