Modul Migration

Veröffentlicht: 2023-09-13

Das ExtraHop-System bietet jetzt separate Module mit segmentierten und für Sicherheits- und Performance-Anwendungsfälle optimierten Funktionen.

Das Network Detection and Response (NDR) -Modul bietet Sicherheits- und Ermittlungsworkflows, und das Network Performance Management (NPM) -Modul bietet Betriebs- und Leistungsworkflows. Zusätzliche Module sind für Packet Forensics und Intrusion Detection Systems verfügbar. Erfahre mehr über Module.

Dieser Leitfaden enthält Informationen über globale Systemänderungen, administrative Aufgaben, und Richtlinien darüber, welche Eigenschaften sind für jedes Modul verfügbar.

Globale Systemänderungen

Das ExtraHop-System aktualisiert im Rahmen der Modulmigration automatisch bestimmte Funktionen.

Standard-Anmeldeseite

Für Benutzer mit NPM-Zugriff kann die Standard-Dashboard-Seite, die nach der Anmeldung angezeigt wird, von einem Administrator angegeben werden.

Für NPM-Benutzer die Standardeinstellung Dashboard Die Seite , die nach der Anmeldung angezeigt wird, kann angegeben werden weltweit von einem Administrator oder von einem Benutzer persönlich festgelegt werden. Wenn kein Dashboard angegeben ist, Active Directory Directory-Dashboard erscheint.

Benutzer können zu ihrem bevorzugten Standard-Dashboard navigieren, auf das Befehlsmenü in der oberen rechten Ecke der Seite klicken und Als Standard-Dashboard festlegen auswählen.

Tuning-Regeln

Das System entfernt die Option Alle Erkennungstypen aus den Erkennungstyp-Kriterien für Optimierungsregeln.

Tuning-Regeln werden basierend auf den Modulzugriffsoptionen angezeigt, die von angegeben sind Benutzerrechte.

Bestehende Optimierungsregeln, die die Kriterien „Alle Erkennungstypen“ enthalten, werden automatisch in zwei Regeln aufgeteilt, die entweder für Sicherheits- oder Leistungskategorien spezifisch sind. Die bestehende Regel wird geändert, um Alle Sicherheitserkennungstypen anzugeben, und eine neue Regel wird für Alle Leistungserkennungstypen erstellt. Während der Migration können versteckte Erkennungen mit einer neuen Optimierungsregel verknüpft werden, die den Erkennungskriterien entspricht.

Wenn Sie eine Optimierungsregel erstellen oder bearbeiten, können Sie abhängig von Ihren Modulzugriffsberechtigungen Kriterien für den Erkennungstyp angeben. Die Dropdownliste Erkennungstyp kann Optionen für Alle Sicherheitserkennungstypen oder Alle Leistungserkennungstypen enthalten.

Regeln für Benachrichtigungen

Regeln für Erkennungsbenachrichtigungen unterstützen keine Kriterien mehr, die sowohl für Sicherheits - als auch für Leistungserkennungen gelten. Benachrichtigungsregeln werden auf der Grundlage Ihrer Modulzugriffsrechte angezeigt.

Regeln für Erkennungsbenachrichtigungen die den Ereignistyp Erkennung angeben, werden automatisch in zwei Regeln aufgeteilt, die entweder für Sicherheits- oder Leistungskategorien spezifisch sind. Die bestehende Regel wird geändert, um den neuen Ereignistyp Sicherheitserkennung anzugeben, und enthält nur die Sicherheitskriterien der ursprünglichen Regel. Für den neuen Ereignistyp Leistungserkennung wird eine neue Regel erstellt, die nur die Leistungskriterien der ursprünglichen Regel enthält.

Wenn eine Benachrichtigungsregel während der Migration aufgeteilt wird, sind Erkennungstypen, die sowohl mit Sicherheit als auch mit Leistung verknüpft sind, nur in der Sicherheitsversion der Regel enthalten, um doppelte Benachrichtigungen zu vermeiden.

Deaktivierte Benachrichtigungsregeln, die sowohl Sicherheits- als auch Leistungskriterien enthalten, werden nicht aufgeteilt. Die Regel wird in eine reine Sicherheitsregel umgewandelt und bleibt deaktiviert.

Aktionen, die durch Benachrichtigungsregeln spezifiziert werden, wie E-Mail-Verteilerlisten und Webhooks, sind in der geänderten NDR-Regel und der neuen NPM-Regel enthalten. Überprüfen Sie diese Aktionen, um sicherzustellen, dass Sicherheits- und Leistungsbenachrichtigungen an die richtige Zielgruppe gesendet werden.

Wenn Sie eine Benachrichtigungsregel erstellen, können Sie entweder die Ereignistypen Sicherheitserkennung oder Leistungserkennung angeben, abhängig von den in Ihrem Benutzerrechte. Nachdem Sie einen Ereignistyp ausgewählt haben, können Sie nur Erkennungstyp und Kategoriekriterien hinzufügen, die dem ausgewählten Ereignistyp zugeordnet sind.

Administrative Aufgaben

Migrierte Systeme gewähren allen Benutzern Zugriff auf die Module Network Performance Monitoring (NPM) und Network Detection and Response (NDR).

Administratoren müssen allen Benutzern, die sich anmelden, rollenbasierten Zugriff gewähren Fernauthentifizierung (LDAP, RADIUS, SAML und TACACS+) sowie lokale Benutzer.

Es gibt zwei Sätze von Benutzerrechte das muss gewährt werden:

Zugriff auf das Modul

Diese Benutzerrechte bestimmen, auf welche Funktionen ein Benutzer zugreifen kann. Beispielsweise muss einem Benutzer Vollzugriff auf das NDR-Modul gewährt werden, um Angriffserkennungen sehen zu können. siehe spezifische Funktionen für jedes Modul.

Zugriff auf das System

Diese Benutzerberechtigungsstufen bestimmen den Funktionsumfang, den Benutzer mit Modulfunktionen haben. Benutzer mit vollem Schreibzugriff können beispielsweise alle Systemobjekte erstellen und bearbeiten.

Die folgenden Abschnitte enthalten Anweisungen zum Aktualisieren von Benutzerberechtigungen.

Aktualisierung der Einstellungen für die Remoteauthentifizierung

Administratoren müssen die Einstellungen für die Fernauthentifizierung für die NDR- und NPM-Module überprüfen und gegebenenfalls aktualisieren.

Zugriff auf das Network Detection and Response (NDR) -Modul

Die Einstellungen für die Fernauthentifizierung für den Zugriff auf das NDR-Modul müssen konfiguriert sein Enthülle (x) Enterprise Systeme, auf denen die inzwischen veraltete globale Rechterichtlinie Detections Access zuvor nicht aktiviert war.

Der Benutzerzugriff auf das NDR-Modul wird direkt von der globalen Rechterichtlinien-Einstellung Detections Access übernommen. Wenn beispielsweise vor der Migration nur bestimmten Benutzern Erkennungszugriff mit vollem Schreibzugriff auf das System gewährt wurde, haben dieselben Benutzer jetzt nach der Migration Zugriff auf das NDR-Modul mit vollen Schreibsystemrechten.

Zugriff auf das NPM-Modul (Network Performance and Monitoring)

Die Einstellungen für die Fernauthentifizierung für den NPM-Modulzugriff müssen auf beiden konfiguriert sein Enthüllen (x) 360 und Enthülle (x) Enterprise systeme.

Aktualisieren Sie die benutzerdefinierte IdP-Konfiguration in Reveal (x) 360

Aktualisieren Sie Ihre benutzerdefinierte Identity Provider (IdP) -Konfiguration in Reveal (x) 360, um Benutzerberechtigungen für den Zugriff auf NDR- und NPM-Module zu gewähren.

Fernauthentifizierung für den Zugriff auf das NDR-Modul
Der Zugriff auf das NDR-Modul wird automatisch mit den vorherigen Einstellungen für Detections Access Control konfiguriert.

Fernauthentifizierung für den NPM-Modulzugriff
Sie müssen Ihre benutzerdefinierte Identity Provider (IdP) -Konfiguration aktualisieren, um Benutzern Zugriff auf das NPM-Modul in Reveal (x) 360 zu gewähren.

Fügen Sie der ExtraHop-Anwendung in Ihrem Identity Provider NPM-Rechte hinzu
Wenn Ihr IdP kein Gruppenattribut für die ExtraHop-Anwendung enthält, müssen Sie ein Benutzerattribut und einen Namen hinzufügen, die dem entsprechen, was Sie in Reveal (x) 360 konfigurieren werden.

1. Loggen Sie sich bei Ihrem Identity Provider ein.
2. Fügen Sie einen Attributnamen und einen Wert hinzu.
3. Speichern Sie die Konfiguration.

Nächste Schritte
Erfahren Sie mehr über die Konfiguration Okta, Google, Azure AD, oder Jumpcloud.
Fügen Sie NPM-Rechte zu Ihren Identitätsanbieter-Einstellungen in Reveal (x) 360 hinzu

1. Melden Sie sich beim Reveal (x) 360-System mit einem Konto an, das über System- und Zugriffsadministrationsrechte verfügt.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Zugriff für Benutzer**.
   Ein Bereich „Aktion erforderlich“ führt Sie durch die verbleibenden Konfigurationsschritte. Wenn der Bereich Aktion erforderlich nicht angezeigt wird, müssen Sie Ihre IdP-Einstellungen nicht aktualisieren.
3. Geben Sie einen Namen in das Feld Attributname ein.
4. Geben Sie einen Namen in das Feld Attributwert ein.

   Hinweis: Der Name und der Wert des Attributs müssen mit den Einstellungen übereinstimmen, die auf Ihrem IdP konfiguriert sind.
5. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie bereit sind, mit dem Update zu beginnen.

   Wichtig: Alle Benutzer werden vom System abgemeldet, nachdem Sie geklickt haben **Jetzt aktualisieren** im nächsten Schritt.
6. klicken **Jetzt aktualisieren**.

Aktualisieren Sie die benutzerdefinierte IdP-Konfiguration in Reveal (x) Enterprise

Aktualisieren Sie Ihre benutzerdefinierte Identity Provider (IdP) -Konfiguration in Reveal (x) Enterprise, um Benutzerberechtigungen für den Zugriff auf NDR- und NPM-Module zu gewähren.

Fernauthentifizierung für den NPM-Modulzugriff
Sie müssen Ihre benutzerdefinierte Identity Provider (IdP) -Konfiguration aktualisieren, um Benutzern Zugriff auf das NPM-Modul in Reveal (x) Enterprise zu gewähren.

1. Melden Sie sich bei der Reveal (x) Enterprise-Konsole mit einem Konto an, das über System- und Zugriffsadministrationsrechte verfügt.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Die gesamte Verwaltung**.
3. Klicken Sie im Abschnitt Zugriffseinstellungen auf **Weltweite Richtlinien**.
   Im Bereich Aktion erforderlich wird ein Link angezeigt, über den Sie Ihre Einstellungen für die Fernauthentifizierung einsehen können. Wenn der Bereich Aktion erforderlich nicht angezeigt wird, müssen Sie Ihre IdP-Einstellungen nicht aktualisieren.
4. klicken **Fernauthentifizierung anzeigen**.
5. Wählen Sie Ihre Authentifizierungsmethode aus der **Methode zur Fernauthentifizierung** Dropdown.

6. Führen Sie die folgenden Schritte für die von Ihnen gewählte Remoteauthentifizierungsmethode aus:

Option	Description

LDAP	Konfigurieren Sie den NPM-Modulzugriff basierend auf Ihrer Option zur Rechtezuweisung.
	1. Rufen Sie die Berechtigungsstufe vom Remoteserver ab:
	    1. Geben Sie einen eindeutigen Namen in das NPM-Modulzugriffs-DN Feld.
	2. Remote-Benutzer haben vollen Schreibzugriff
	    a. Wählen **Voller Zugriff**.
	3. Remote-Benutzer haben vollen Lesezugriff
	    a. Wählen **Voller Zugriff**.

RADIUS	Konfigurieren Sie den NPM-Modulzugriff basierend auf Ihrer Option zur Rechtezuweisung.
	1. Remote-Benutzer haben vollen Schreibzugriff
	    a. Wählen **Voller Zugriff**.
	2. Remote-Benutzer haben vollen Lesezugriff
	    a. Wählen **Voller Zugriff**.

SAML	Bearbeiten Sie die Einstellungen des Identitätsanbieters, um einen Attributnamen und einen Attributwert für den NPM-Modulzugriff hinzuzufügen. Der Name und die Werte des Attributs müssen mit den in Ihrem Identity Provider konfigurierten Werten übereinstimmen.

TACACS+	Konfigurieren Sie den NPM-Modulzugriff basierend auf Ihrer Option zur Rechtezuweisung.
	1. Rufen Sie die Berechtigungsstufe vom Remoteserver ab:
	    1. Fügen Sie auf Ihrem TACACS+-Server das folgende benutzerdefinierte Attribut hinzu:
	    Attribut: `npm voll`
	    Wert: 1
	2. Remote-Benutzer haben vollen Schreibzugriff
	    a. Wählen **Voller Zugriff**.
	3. Remote-Benutzer haben vollen Lesezugriff
	    a. Wählen **Voller Zugriff**.

7. Kehren Sie zurück zum Weltweite Richtlinien Seite.
8. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie bereit sind, das Update zu starten.

   Wichtig: Alle Benutzer mit Ausnahme des Setup-Benutzerkontos werden vom System abgemeldet.

9. klicken **Jetzt aktualisieren**.

Fernauthentifizierung für den Zugriff auf das NDR-Modul
Wenn auf Ihrem Reveal (x) Enterprise-System Detection Access Control vor der Migration als globale Richtlinie aktiviert war, wird der Zugriff auf das NDR-Modul automatisch mit den vorherigen Einstellungen für Detections Access Control konfiguriert.

Wenn Detection Access Control nicht aktiviert war, müssen Sie Ihre benutzerdefinierte Identity Provider (IdP) -Konfiguration aktualisieren, um Benutzern Zugriff auf das NDR-Modul in Reveal (x) Enterprise zu gewähren.

1. Melden Sie sich bei der Reveal (x) Enterprise-Konsole mit einem Konto an, das über System- und Zugriffsadministrationsrechte verfügt.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Die gesamte Verwaltung**.
3. Klicken Sie im Abschnitt Zugriffseinstellungen auf **Weltweite Richtlinien**.

   Im Bereich Aktion erforderlich wird ein Link angezeigt, über den Sie Ihre Einstellungen für die Fernauthentifizierung einsehen können. Wenn der Bereich Aktion erforderlich nicht angezeigt wird, müssen Sie Ihre IdP-Einstellungen nicht aktualisieren.
4. klicken **Fernauthentifizierung anzeigen**.
5. Wählen Sie Ihre Authentifizierungsmethode aus der **Methode zur Fernauthentifizierung** Dropdown.
6. Führen Sie die folgenden Schritte für die von Ihnen gewählte Remoteauthentifizierungsmethode aus:

Option	Description

LDAP	Konfigurieren Sie den Zugriff auf das NDR-Modul basierend auf Ihrer Rechtezuweisungsoption.
	1. Rufen Sie die Berechtigungsstufe vom Remoteserver ab:
	  1. Geben Sie einen eindeutigen Namen in das NDR-Modulzugriffs-DN Feld.
	2. Remote-Benutzer haben vollen Schreibzugriff
	  a. Wählen **Voller Zugriff**.
	3. Remote-Benutzer haben vollen Lesezugriff
	  a. Wählen **Voller Zugriff**.

RADIUS	Konfigurieren Sie den Zugriff auf das NDR-Modul basierend auf Ihrer Rechtezuweisungsoption.
	1. Remote-Benutzer haben vollen Schreibzugriff
	  a. Wählen **Voller Zugriff**.
	2. Remote-Benutzer haben vollen Lesezugriff
	  a. Wählen **Voller Zugriff**.

SAML	Bearbeiten Sie die Einstellungen des Identitätsanbieters, um einen Attributnamen und einen Attributwert für den Zugriff auf das NDR-Modul hinzuzufügen. Der Name und die Werte des Attributs müssen mit den in Ihrem Identity Provider konfigurierten Werten übereinstimmen.
TACACS+	Konfigurieren Sie den Zugriff auf das NDR-Modul basierend auf Ihrer Rechtezuweisungsoption. 1. Rufen Sie die Berechtigungsstufe vom Remoteserver ab:

Option	Description
	1. Fügen Sie auf Ihrem TACACS+-Server das folgende benutzerdefinierte Attribut hinzu: Attribut: `ndr voll` Wert: 1 2. Remote-Benutzer haben vollen Schreibzugriff a. Wählen **Voller Zugriff**. 3. Remote-Benutzer haben vollen Lesezugriff a. Wählen **Voller Zugriff**.

7. Kehren Sie zurück zum Weltweite Richtlinien Seite.
8. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie bereit sind, das Update zu starten.

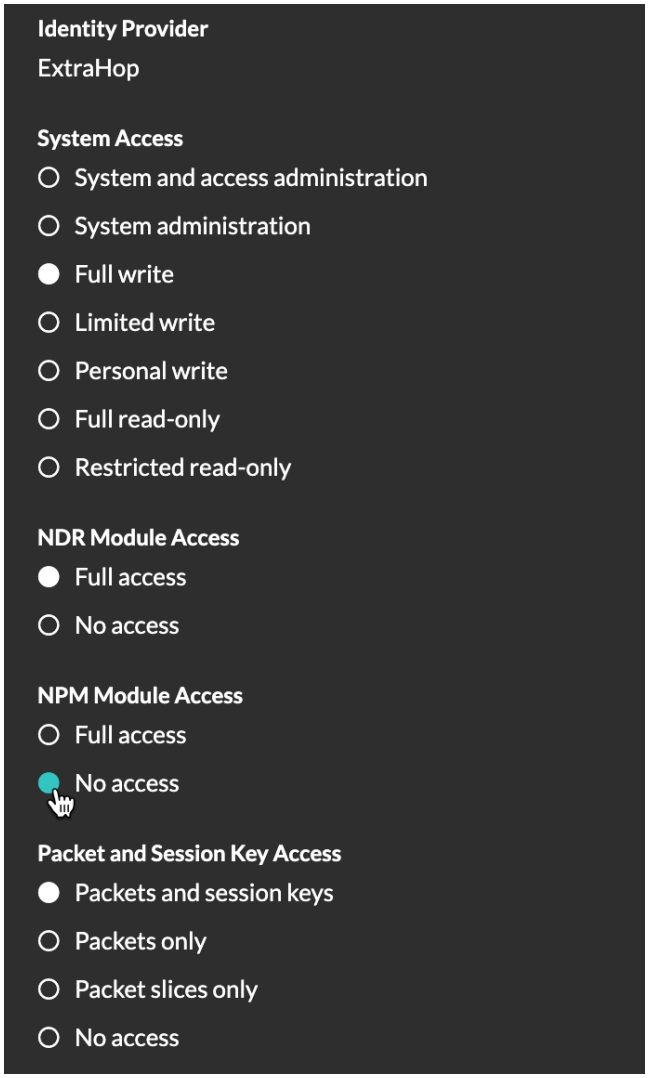
   Wichtig: Alle Benutzer mit Ausnahme des Setup-Benutzerkontos werden vom System abgemeldet.
9. klicken **Jetzt aktualisieren**.

Lokale Benutzereinstellungen aktualisieren

Administratoren müssen die lokalen Benutzerzugriffsrechte für die NDR- und NPM-Module überprüfen und gegebenenfalls aktualisieren.

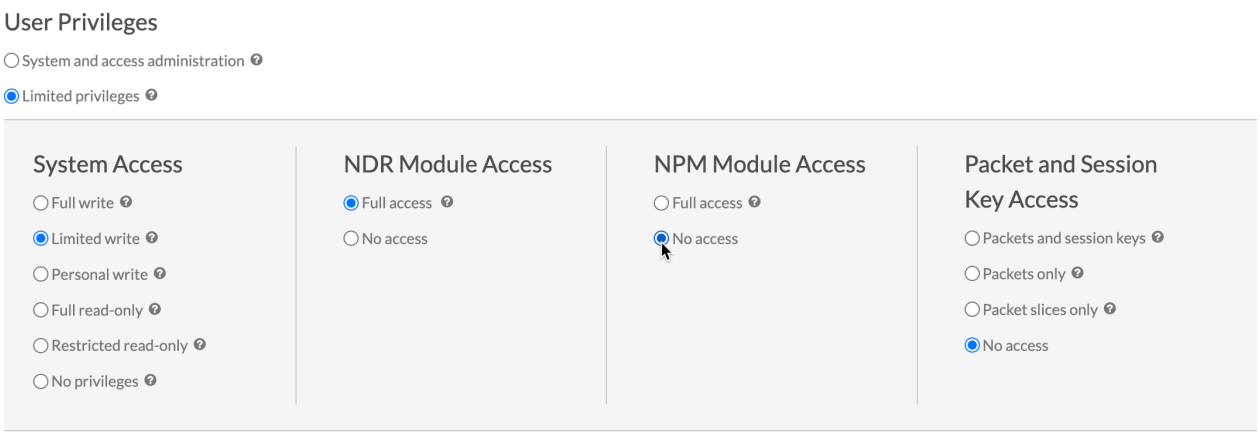
Lokale Benutzer in Reveal (x) 360 aktualisieren

1. Melden Sie sich bei Reveal (x) 360 an und klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann **Die gesamte Verwaltung**.
2. klicken **Benutzerzugriff**.
3. In der Nutzer Abschnitt, klicken **Benutzer ansehen**.
4. Klicken Sie auf einen Benutzer, um die Zugriffsrechte anzuzeigen und zu ändern.



Lokale Benutzer in Reveal (x) Enterprise aktualisieren

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Zugriffs-Einstellungen Abschnitt, klicken **Nutzer**.
3. Klicken Sie auf einen Benutzer, um die Zugriffsrechte anzuzeigen und zu ändern.



Verfügbare Funktionen pro Modul

Die folgende Tabelle zeigt die wichtigsten Funktionen, die nach Modulen verfügbar sind. Funktionen, die nicht aufgeführt sind, sind in beiden Modulen verfügbar.

Merkmal	NDR	NPM
Seite „Sicherheitsübersicht“	Y	N
Berichte der Geschäftsleitung	Y	N
Integrierte Sicherheits-Dashboards	Y	N
Sicherheitserkennungen	Y	N
MITRE karte	Y	N
Ermittlungen	Y	N
Optimierungsregeln für Sicherheitserkennungen	Y	N
Benachrichtigungsregeln für Sicherheitserkennungen und Bedrohungsinformationen	Y	N
Bedrohungsinformationen	Y	N
Bedrohungsinformationen	Y	N
Benutzerdefinierte Dashboards	N	Y
Integrierte Leistungs-Dashboards	N	Y
Leistungserkennungen	N	Y
Optimierungsregeln für Leistungserkennungen	N	Y
Benachrichtigungsregeln für Leistungserkennungen	N	Y
Alerts	N	Y