New-Scale Security Operations Platform Administration Guide

October 29, 2026

Have feedback on this guide? We'd love to hear from you!
Email us at docs@exabeam.com.

Disclaimer: Ensure you are viewing the most up-to-date version of this guide by visiting the Exabeam Documentation Portal.

Exabeam
1051 E. Hillsdale Blvd, 4th Floor
Foster City, CA 94404
650.209.8599

Copyright

All content in this document, including text, graphics, logos, icons, images, and video clips, is the exclusive property of Exabeam or its content suppliers and is protected by U.S. and international copyright laws. The compilation (meaning the collection, arrangement, and assembly) of all content in this document is the exclusive property of Exabeam and is also protected by U.S. and international copyright laws. The content in this document may be used as a resource. Any other use, including the reproduction, modification, distribution, transmission, republication, display, or performance, of the content in this document is strictly prohibited.

Copyright ©2026 Exabeam, Inc. All Rights Reserved.

Trademarks

Exabeam and the Exabeam logo are trademarks or registered trademarks of Exabeam. All third-party trademarks mentioned in this document are the property of their respective owners. The trademarks and logos displayed in this document may not be used without the prior written consent of Exabeam or their respective owners.

Products

Exabeam owns and retains all right, title and interest in and to the Exabeam's products and services and portions, features and/or functionality of Exabeam's products may be protected under Exabeam's patents, as well as patents pending.

Other Policies

For information regarding Exabeam's treatment of personally identifiable information, please review Exabeam's current privacy policy at www.exabeam.com/privacy.

Table of Contents

Welcome to the New-Scale Security Operations Platform 5
New-Scale Security Operations Platform Architecture 5
Navigation Center 8
Application Organization 8
Global Search 8
Navigation Sidebar 10
Session Timeout 10
Supported Browsers 11
Licenses 12
New-Scale Security Operations Portfolio Licenses 12
New-Scale Security Operations Portfolio License Types 12
Features by New-Scale Security Operations Portfolio License Type 12
Exabeam Security Operations Portfolio Licenses 14
Exabeam Security Operations Portfolio License Types 14
Features by Exabeam Security Operations Portfolio License Type 15
Fusion Licenses 17
Fusion License Types 17
Features by Fusion License Type 18
Supported Regions for Data Residency 20
Get Started with the New-Scale Security Operations Platform 21
(Optional) Allow Exabeam IP Addresses for your Region 21
(Optional) Configure Detection Rule Display Preferences 22
Define a Unique Site Name 23
Enable Multi-factor Authentication 25
Setting up TOTP Authenticator 25
Resetting a token 26
Configuring Tenant Session Timeout 27
Important Considerations 27
How to Configure Session Timeout 28
Connect to Exabeam MCP Server 28
Connection Types 28
Connect Using User-Delegated Authentication (Recommended) 28
Connect Using API Key 29
Currently Supported Functionality 31
Example Queries 31
Webhooks 32
Add a Webhook 32
View Details/Edit a Webhook 34
Delete a Webhook 35
Notifications 36
Manage Notification Preferences 37
Manage Global Notifications Preferences 38
View New Notifications 45
View Inbox 46
Universal Role-Based Access 48

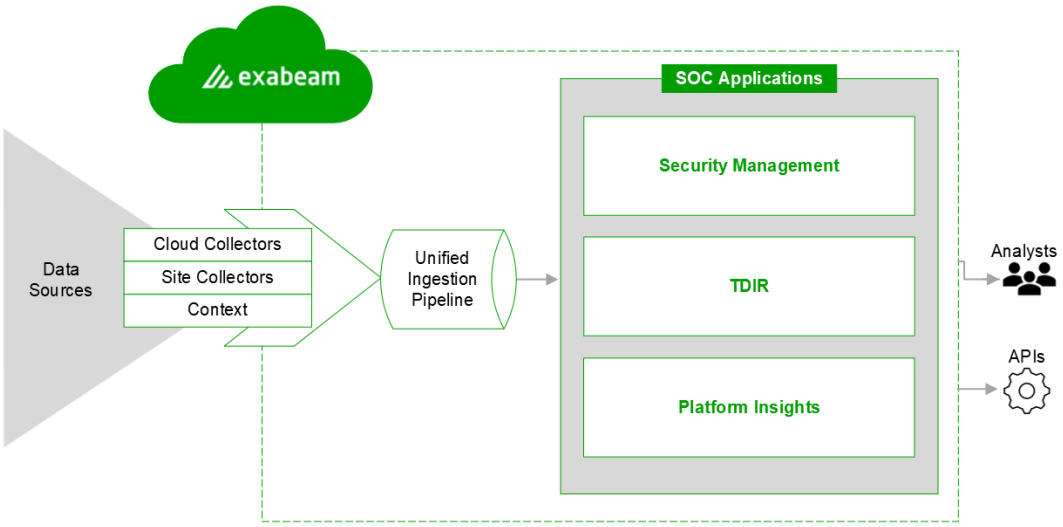
Considerations for Adopting Universal Role-Based Access 48
User Roles 49
User Permissions 49
View Permissions in a User Role 69
Create a Custom User Role 71
Duplicate, Edit, or Delete User Roles 72
Secured Resources 74
Local Users 78
Add New Local Users 78
Edit Account Details for Local Users 79
Activate or Deactivate a Local User Account 80
Reset the Password for a Local User Account 80
Third-Party Identity Providers 81
Add a Third-Party Identity Provider 82
Set up Okta as your Identity Provider 88
Set up Okta as your Identity Provider using Okta Integration Network 95
Set up Microsoft Entra ID (formerly Azure) as your Identity Provider 107
Manage Third-Party IdPs 112
Access Control APIs 112
Manage Access by IP Addresses 113
Accessing the IP-Based Access Settings 114
Add an IP or IP Range to the Allowed List 115
Edit Access for an IP or IP Range in the Allowed List 115
Delete an IP or IP Range from the Allowed List 116
Exabeam Nova 117
Getting Started 117
Example Supported Workflows 119
Exabeam Nova AI-Driven Features 119
AI Development 120
Personal Data Processing 121
Model Training 121
False Positives and Negatives 121
Policies and Support 121
Monitoring 122
Service Health and Consumption 122
Audit Logs 123
Types of Audit Logs 124
Audit Log Visibility 126
Export Your Exabeam Data 128

Welcome to the New-Scale Security Operations Platform

The New-Scale Security Operations Platform is a cloud-delivered, comprehensive solution for collecting and analyzing log data to detect security threats and automate incident responses. The New-Scale Security Operations Platform expedites the provisioning and consumption of new security management applications, tools, and content. It also provides single sign-on access to Exabeam products and centralized identity management.

As an alternative to the cloud-delivered New-Scale Security Operations Platform, Exabeam also offers the on-premises Exabeam Security Management Platform.

New-Scale Security Operations Platform Architecture



The New-Scale Security Operations Platform ingests logs using Exabeam Cloud Connectors, Site Collectors, and Context Management.

- **Cloud Collectors** – Previously known as cloud connectors, both services provide prebuilt, turnkey connectors for over 30 cloud applications and services. In addition, the services facilitate log ingestion into Exabeam Data Lake, Exabeam Advanced Analytics, or any other SIEM. To minimize blind spots within your organization, cloud connectors also provide additional custom connectors for services not natively supported. For more information, see the Cloud Collectors Guide.
- **Site Collectors** – Securely and efficiently upload event data from on-premises services such as external servers, systems, data centers, or Exabeam collectors (including Windows, File, and GZip) to Exabeam cloud-delivered services in the New-Scale Security Operations Platform. For more information, see the Site Collector Guide.

Depending on your License, Exabeam can also provide additional capabilities for security management, threat detection investigation and response (TDIR), and platform insights. These services can include:

- Security Management:
  - **Action Editor** – Create your own Incident Responder service and actions using Action Editor. This application is included on the New-Scale Security Operations Platform to all Incident Responder users. It guides you through the process to customize a prebuilt service and actions or create your own custom service and actions from scratch. For more information, see the Action Editor documentation.
  - **Attack Surface Insights** – A directory for organizational resources in your environment, also known as entities. Attack Surface Insights identifies entities in incoming parsed logs, connects related attributes and contextual data to build comprehensive profiles on those entities, and links related entities. For more information, see the Attack Surface Insights documentation.
  - **Auto Parser Generator** – Similar to Log Stream, you can use Auto Parser Generator to set up custom parsers to ingest logs and events within the original content information model. For the latest Exabeam products developed on the Common Information Model, use Log Stream. For more information, see the Auto Parser Generator documentation.
  - **Correlation Rules** – Develop fact-based rules that correlate to events matching specific criteria. Create automated outcomes to supplement behavioral analytics. Using the Correlation Rules app, you can easily build rules based on search queries. You can refine those rules with additional conditions and determine what outcomes should occur when the rule is triggered. For more information, see the Correlation Rules documentation.
  - **Log Stream** – Enables you to visualize, create, deploy, and monitor parsers within a unified ingestion pipeline for all Exabeam products and features. For more information, see the Log Stream documentation.
  - **Context Management** – Provides a single point of access for managing context data, such as data from threat intelligence services or identity providers. Supports the processing of context data from multiple sources and normalizes the data into a standardized schema for use by downstream applications. For more information, see the Context Management Guide.
  - **Threat Detection Management** – Create, test, and tune detections across all engines. Easily adjust and refine detection criteria, implement exclusion rules, and tune any detection rule. For more information, see the Threat Detection Management documentation.
- Threat Detection and Incident Response (TDIR):
  - **Advanced Analytics** – Advanced behavioral analytics platform that automatically links and analyzes user and entity activity to better inform security analysts about threats and remediation options. Advanced Analytics provides a powerful analytics layer on top of existing SIEM and log management technologies, to detect new attacks, prioritize incidents, and guide you to provide a more effective response. For more information, see the Advanced Analytics Administration Guide and the Advanced Analytics User Guide.
  - **Threat Center** – A triage and ticketing solution that centralizes all alerts and cases so you address potential threats with a streamlined workflow. Threat Center collects alerts from Threat Detection Management in one place and provides case creation capabilities so you move seamlessly from triage to response. For more information, see the Threat Center documentation.

- **Alert Triage** – A cloud-delivered application that categorizes, aggregates and enriches security alerts that enables you to dismiss or escalate security alerts confidently and efficiently. Alert Triage provides visibility into all of the alerts that security tools trigger through a centralized view, reducing the likelihood of missing a security alert. For more information, see the Alert Triage documentation.
- **Automation Management** – A security orchestration, automation, and response (SOAR) solution you use to create and manage your automation tools, like playbooks and services. It integrates third-party products and vendors with Exabeam applications and automates complex or repetitive operational tasks so you quickly triage, investigate, and remediate threats. For more information, see the Automation Management documentation.
- **Case Manager** – Organize, track, and streamline your investigation with Case Manager. Case Manager is a customizable case management solution with ticketing, messaging, and Key Performance Indicator (KPI) dashboards. It organizes and tracks investigations so you are more efficient and productive. For more information, see the Case Manager documentation.
- **Data Lake** – A log management system that provides collection, indexing, search, and visualization across your logs. The goal of Data Lake is to present log data to the user in a clear and consumable manner. For more information, see the Data Lake Administration Guide and the Data Lake User Guide.
- **Dashboards** – Provides a centralized location for a high-level view of data across your Exabeam products. Through a wide range of chart types offering different perspectives, Dashboards breathes life into raw data and paints a meaningful picture of network activities, helping to reveal the critical information that you need to guide your security decision-making. For more information, see the Dashboards documentation.
- **Incident Responder** – Provides automated, repeatable investigation and response capabilities. To reduce human error and manual investigation effort, Incident Responder also provides semi and fully-automated incident investigation and response actions with repeatable pre-built playbooks for common incidents. For more information, see the Incident Responder documentation.
- **Search** – Provides a single interface to enable you to quickly perform advanced search queries across multiple years-worth of events, IoCs, and Exabeam-generated anomalies. For more information, see the Search documentation.

- Platform Insights:
  - **Outcomes Navigator** – A cloud-delivered application that provides visibility into the efficacy of your environment's configuration to protect against Exabeam use cases. Outcomes Navigator analyzes your environment and suggests configuration changes to align your environment with your goals and improve security posture. For more information, see the Outcomes Navigator documentation.
  - **Service Health and Consumption** – Visualize the key metrics for monitoring data ingestion, system health, license consumption, and security budget needs. For more information, see the Service Health and Consumption documentation.

Navigation Center

The Navigation Center is the Exabeam Security Operations Platform homepage. The following is an introductory video on the Navigation Center:

https://player.vimeo.com/video/836698716

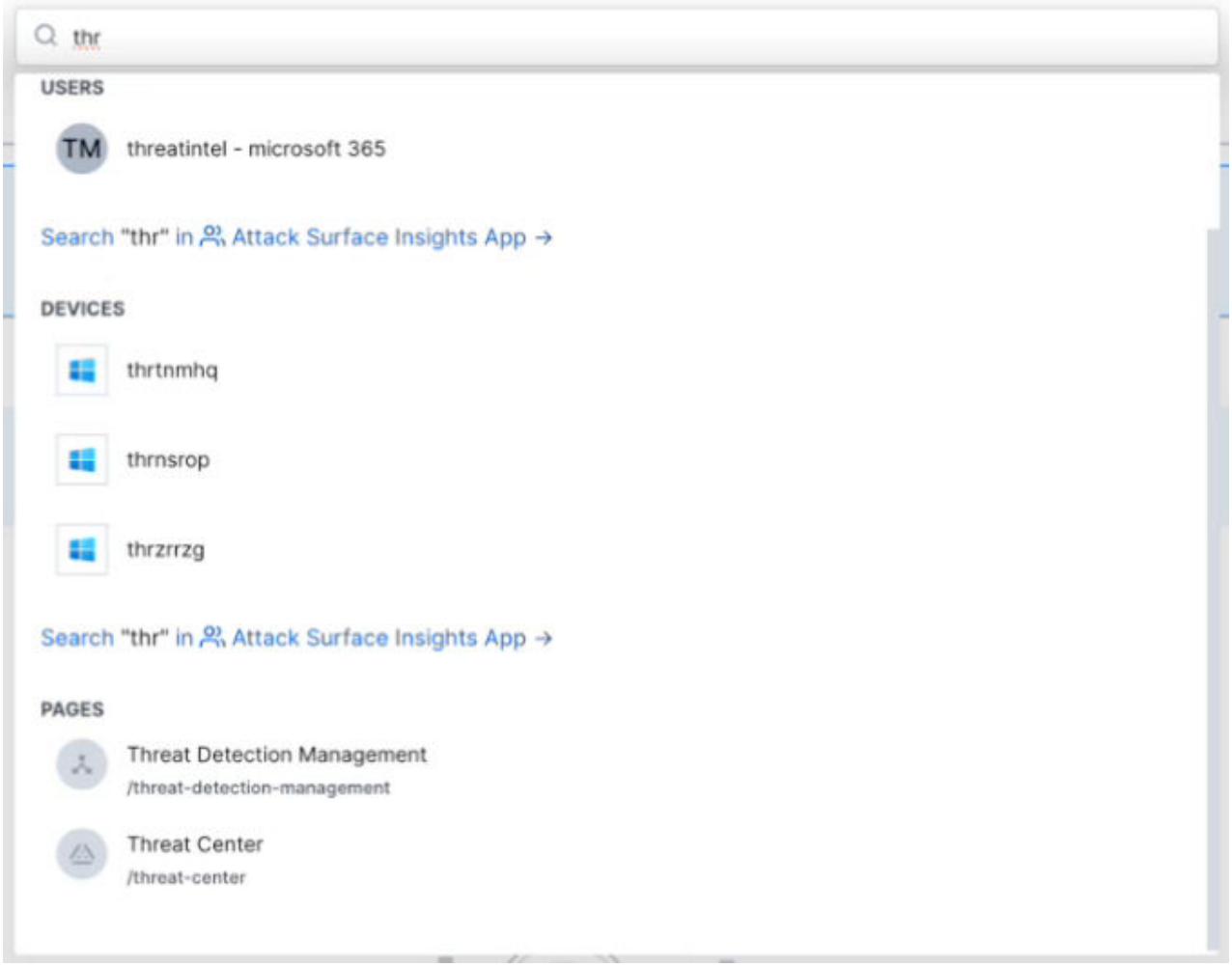
Application Organization

Applications in the Navigation Center are organized into the following four categories to align with common workflows and roles:

- **Collectors**: Apps for ingesting log and context data to glean visibility into attacks. This category is geared towards security administrators and engineers.
- **Security Management**: Apps for configuring and tuning your Exabeam data pipeline, threat detection, investigation, and response. This category is geared towards security administrators and engineers.
- **TDIR**: Apps for finding threats and taking action on alerts, events, and threats within your organization. This category is geared towards security analysts.
- **Platform Insights**: Apps for gaining insights into your organization's data and health. This category is geared towards security administrators and engineers.

Global Search

Located from any application, you can use the integrated global search bar to quickly locate users and devices from across the platform. This search bar may or may not be visible based on your license type and app permissions (such as Attack Surface Insights).



Search results are based on a prefix search of at least 3 characters across the fields *user_name*, *email_address*, *full_name*, *ip_address*, and *host_name* and include :

- Ability to navigate into the Search app for logs/events matching search criteria
- Attack Surface Insights user and device entities
- Pages and apps

The default search returns all types (up to 5 entities per category) or you can filter by specific options such as users or devices. Click to navigate into and search within a specific app for more results.

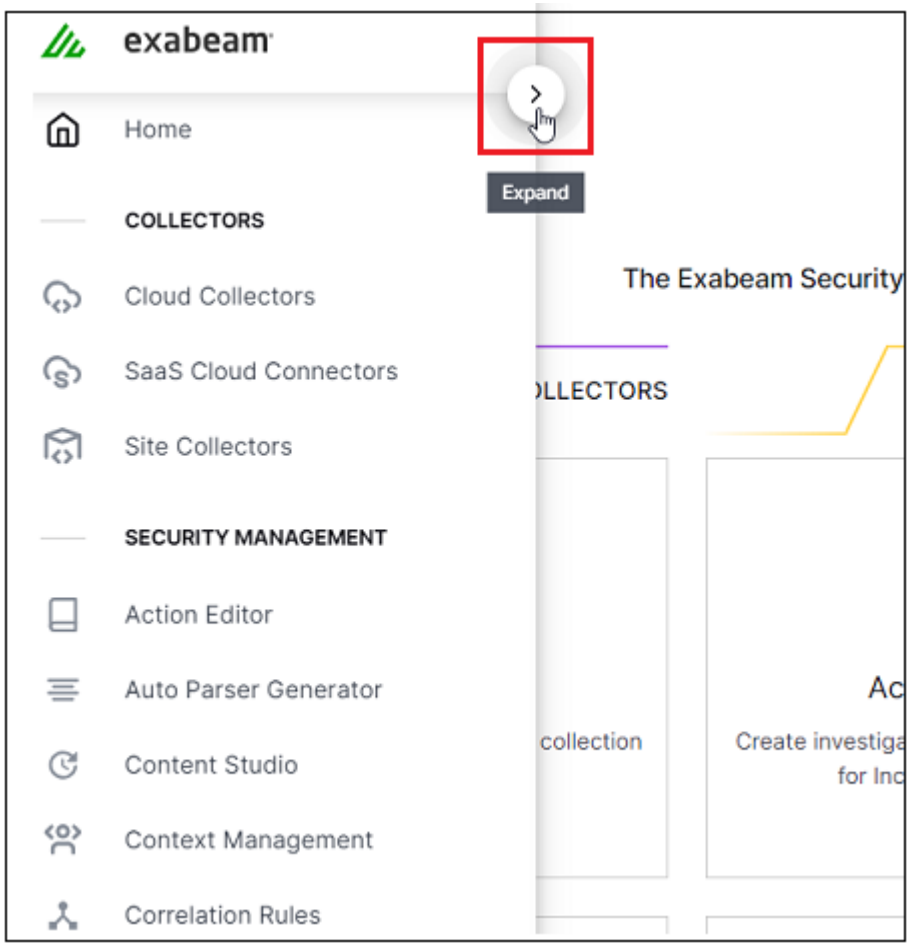
Hover over an entity in the results list and click it to open a details panel, which includes additional information such a Maximum Risk Score (over the last day), User Risk Trend graph, and User/Device tag information.

You can also click the icons for search results to **View timeline in Search**, **View Associated Alerts**, or **View Associated Cases**.

Navigation Sidebar

The navigation sidebar has the same organizational logic as the homepage, and enables you to quickly pivot between apps and settings without needing to return to the homepage. The sidebar can be expanded and pinned open so that the app and setting labels remain visible.

- To expand the sidebar, hover your pointer over it.
- To pin the expanded sidebar, click the › icon at the top; to collapse the sidebar, click the ‹ icon.



NOTE
The applications that appear in your Navigation Center depend on your licensing.

Session Timeout

When a session in the New-Scale Security Operations Platform has been inactive for four hours, it will timeout. A five-minute warning is displayed before the session reaches the four-hour timeout. The warning message includes options to continue the session or log out. If you opt to continue, the session automatically refreshes in the background for an additional four hours.

Supported Browsers

We support only the **latest** version of each of these browsers:

- Edge
- Chrome
- Firefox
- Safari

> **NOTE**
> Mobile browsers are not supported.

Minimum Screen Width: 1280px (responsive as possible for smaller widths, but not always possible)

Maximum Screen Width: 1920px (app is centered in larger screens)

Licenses

- New-Scale Security Operations Portfolio Licenses
- Exabeam Security Operations Portfolio Licenses
- Fusion Licenses

New-Scale Security Operations Portfolio Licenses

- New-Scale Security Operations Portfolio License Types
- Features by New-Scale Security Operations Portfolio License Type

New-Scale Security Operations Portfolio License Types

The following product licenses are available with the New-Scale Security Operations Platform:

New-Scale SIEM
New-Scale SIEM is a cloud-native solution designed to efficiently aggregate and normalize log data from cloud, on-premises, and third-party sources for enhanced threat detection, investigation, and response (TDIR). With AI-driven analytics and scalable architecture, it provides real-time visibility across environments, helping security teams manage and respond to growing volumes of data and threats with precision and speed.

New-Scale Analytics
New-Scale Analytics builds upon Exabeam Security Analytics with advanced multi-layer risk scoring and business factor adjustments. It enhances existing SIEM deployments by using machine learning and behavioral analytics to detect sophisticated, hard to spot threats. By automating event correlation and threat detection, it improves security operations, prioritizes risks, and accelerates response to complex attacks like insider and credential-based threats.

New-Scale Fusion
New-Scale Fusion is a comprehensive offering that marries the SIEM and the Analytics capabilities with advanced threat detection. It combines AI, automation, and scalable log management to enhance threat detection, investigation, and response (TDIR). It integrates advanced UEBA and machine learning to identify risks, automates workflows, and provides powerful, actionable insights. The platform supports seamless third-party integrations and offers flexible deployment options to optimize your security investments

Features by New-Scale Security Operations Portfolio License Type

The New-Scale Security Operations Portfolio is a cloud-delivered solution that is licensed as term subscriptions with three different product licenses.

The following table displays the features supported by each license type. A dash (—) indicates a feature is not supported. Where a feature is supported, additional limitations may apply. For terms, see Exabeam Product Entitlement.

- Collectors
- Security Management
- TDIR
- Platform Insights
- Add Ons

Feature	New-Scale SIEM	New-Scale Fusion	New-Scale Analytics
Collectors			
Collectors (cloud, site, context collectors; legacy cloud connectors are also available on-demand)	✔	✔	✔
Security Management			
Log Stream	✔	✔	✔
Context Management	✔	✔	✔
Attack Surface Insights	—	✔	✔
Threat Detection Management – Analytics rules	—	✔	✔
Threat Detection Management – Correlation rules	✔	✔	✔
TDIR			
Automation Management	✔	✔	✔
Dashboards	✔	✔	✔ (Pre-built dashboards only; No customization)
Pre-Built Dashboards			
• Threat Center Dashboards	✔	—	—
• Anomaly and Risk Dashboards	—	✔	✔
• Case Manager Dashboards	—	✔	✔
• Compliance and Event Store Dashboards	✔	✔	—
• Correlation Rules Dashboards	✔	✔	✔
Search	✔	✔	✔ (Unlimited anomalies; limited third-party events per search)
Threat Center	✔	✔	✔
Platform Insights			
Outcomes Navigator	✔	✔	✔
Service Health and Consumption	✔	✔	✔
Add Ons			
Exabeam Fusion Extension Extension of product capabilities beyond default retention: search, report, dashboard, correlation rules	—	✔	—

Feature	New-Scale SIEM	New-Scale Fusion	New-Scale Analytics
Long-term Search Capacity Long-term, easily accessible log storage with search and export capabilities	✔	✔	—
Long-term Storage Capacity Long-term, easily accessible log storage with limited search capabilities	✔	✔	—
Exabeam Ingester for CrowdStrike Collects filtered CrowdStrike Falcon Data Replicator (FDR) content	✔	✔	✔
Advanced Automation Includes custom services, advanced playbook designer, and dedicated automation visibility for alerts and cases in Threat Center	✔	✔	✔

The entitlements for Exabeam products, SaaS, and Technical Support offerings are limited to those described in Exabeam Product Entitlement. In the event of a conflict between the documentation, including this page, and the Product Entitlement Document, the Product Entitlement Document shall prevail.

Exabeam Security Operations Portfolio Licenses

- Exabeam Security Operations Portfolio License Types
- Features by Exabeam Security Operations Portfolio License Type

Exabeam Security Operations Portfolio License Types

The following product licenses are available with the New-Scale Security Operations Platform:

Exabeam Security Log Management
Exabeam Security Log Management is the industry's most advanced cloud-native solution for log ingestion, parsing, storage, and search. Built to support security use cases, Exabeam Security Log Management is the entry point for your organization, providing a lightning fast, modern search and dashboard experience across multi-year data.

Exabeam SIEM
Exabeam SIEM extends the cloud-scale capabilities of Exabeam Security Log Management with advanced features for threat detection, investigation and response (TDIR). In addition to its massively scalable ingestion, storage and intelligent search capabilities across petabytes of hot, warm, or cold data in seconds, Exabeam SIEM includes Threat Center and 100s of pre-packaged correlations. If more storage, longer storage time, or additional processing power is needed, Exabeam SIEM easily scales to meet your needs.

Exabeam Fusion
Exabeam Fusion is a comprehensive offering that marries SIEM and security investigation capabilities with advanced threat detection. With Exabeam Fusion, user and entity behavior analytics feed into your automated incident triage, investigation, and response workflows.

Exabeam Security Investigation
Similar to Exabeam Security Analytics, Exabeam Security Investigation augments a SIEM or data lake solution with the industry's most powerful UEBA and automation and adds additional investigation capabilities. Exabeam Security Investigation provides over 1,900 UEBA rules and behavioral models to automatically baseline normal behavior of users and devices with histograms to detect, prioritize and respond to anomalies based on risk as well as prioritizes third party alerts using machine learning.

Exabeam Security Analytics
Exabeam Security Analytics enables organizations to quickly perform threat detection and analysis on existing data streams and data lake/repositories with built-in log ingestion and parsing. Threat detection is powered by user and behavioral entity analytics, correlation rules, and threat intelligence, and augmented by alerting and case/incident management.

Features by Exabeam Security Operations Portfolio License Type

The Exabeam Security Operations Portfolio is a cloud-delivered solution that is licensed as term subscriptions with five different product licenses.

The following table displays the features supported by each license type. A dash (—) indicates a feature is not supported. Where a feature is supported, additional limitations may apply. For terms, see Exabeam Product Entitlement.

- Collectors
- Security Management
- TDIR
- Platform Insights
- Add Ons

Feature	Exabeam Security Log Management	Exabeam SIEM	Exabeam Fusion	Exabeam Security Investigation	Exabeam Security Analytics
Collectors					
Collectors (cloud, site, context collectors; legacy cloud connectors are also available on-demand)	✔	✔	✔	✔	✔
Security Management					
Action Editor	—	—	✔	✔	—
Correlation Rules	✔	✔	✔	✔ (Limited search)	✔ (Limited search)
Pre-built Correlation Rules	—	✔	✔	✔	✔
Log Stream	✔	✔	✔	✔	✔
Context Management	✔	✔	✔	✔	✔
TDIR					

Feature	Exabeam Security Log Management	Exabeam SIEM	Exabeam Fusion	Exabeam Security Investigation	Exabeam Security Analytics
Advanced Analytics (SaaS)	—	—	✔	✔	✔
Advanced Analytics retention of logs, events, sessions	—	—	(Measured in days. See Exabeam Product Entitlement for details.)		
Alert Triage	—	—	—	—	✔
Automation Management	—	✔	✔	✔	—
Case Manager (SaaS)	—	—	—	—	✔
Dashboards	✔	✔	✔	✔ (Pre-built dashboards only; No customization)	✔ (Pre-built dashboards only; No customization)
Pre-Built Dashboards					
• Threat Center Dashboards	—	✔	—	—	—
• Anomaly and Risk Dashboards	—	—	✔	✔	✔
• Case Manager Dashboards	—	—	✔	✔	✔
• Compliance and Event Store Dashboards	✔	✔	✔	—	—
• Correlation Rules Dashboards	✔	✔	✔	✔	✔
Incident Responder (includes Action Editor, Case Manager, and Alert Triage)			See Add Ons.		
Search	✔	✔	✔	✔ (Unlimited anomalies; limited third-party events per search)	(Unlimited anomalies; limited third-party events per search)
Threat Center	—	✔	✔	✔	—
Platform Insights					
Outcomes Navigator	✔	✔	✔	✔	✔
Service Health and Consumption	✔	✔	✔	✔	✔
Add Ons					
Exabeam Security Log Management Extension Extension of product capabilities beyond default retention: search, report, dashboard, correlation rules	✔	—	—	—	—

Feature	Exabeam Security Log Management	Exabeam SIEM	Exabeam Fusion	Exabeam Security Investigation	Exabeam Security Analytics
Exabeam SIEM Extension Extension of product capabilities beyond default retention: search, report, dashboard, correlation rules	—	✔	—	—	—
Exabeam Fusion Extension Extension of product capabilities beyond default retention: search, report, dashboard, correlation rules	—	—	✔	—	—
Long-term Search Long-term, easily accessible log storage with search and export capabilities	✔	✔	✔	—	—
Long-term Storage Long-term, easily accessible log storage with limited search capabilities	✔	✔	✔	—	—
Exabeam Ingester for CrowdStrike Collects filtered CrowdStrike Falcon Data Replicator (FDR) content	✔	✔	✔	✔	✔
Dynamic Alert Prioritization	—	—	✔	✔	—
Incident Responder	—	—	✔	✔	—
Action Editor	—	—	✔	✔	—

The entitlements for Exabeam products, SaaS, and Technical Support offerings are limited to those described in Exabeam Product Entitlement. In the event of a conflict between the documentation, including this page, and the Product Entitlement Document, the Product Entitlement Document shall prevail.

Fusion Licenses

- Fusion License Types
- Features by Fusion License Type

Fusion License Types

There are two types of fusion licenses:

Fusion XDR
Exabeam Fusion XDR is a cloud-delivered product that enables effective Threat Detection Investigation and Response (TDIR) and allows you to leverage and enhance the existing tools in your security stack, without forcing you to rip-and-replace them to centralize on a single vendor.

Fusion SIEM
Exabeam Fusion SIEM includes all Fusion XDR capabilities plus Data Lake for log management, log searches, and compliance reports.

Features by Fusion License Type

Fusion is a cloud-delivered solution that is licensed as term subscriptions with two different Fusion License Types.

Each of these two Fusion XDR and Fusion SIEM packages comes with two plan editions: Core and Enterprise.

	Fusion XDR		Fusion SIEM	
Feature	**Core**	**Enterprise**	**Core**	**Enterprise**
Collectors				
Cloud Connectors	✔	✔	✔	✔
Site Collector	✔	✔	✔	✔
Security Management				
Action Editor	✔	✔	✔	✔
TDIR				
Advanced Analytics	✔	✔	✔	✔
Alert Triage	✔	✔	✔	✔
Case Manager	✔	✔	✔	✔
Entity Analytics	✔	✔	✔	✔
Data Lake	—	—	✔	✔
Threat Center	✔	✔	✔	✔
Threat Hunter	✔	✔	✔	✔
Response				
Automation Management	✔	✔	✔	✔
Incident Responder turnkey playbooks	✔	✔	✔	✔
Incident Responder with custom playbooks, playbook editing, and third-party services (optional add-on)	✔	✔	✔	✔
Data Retention				
Data Lake retention (HOT)	—	—	1 month	1 month
Additional Data Lake retention (HOT) (optional add-on)	—	—	—	2 months
Advanced Analytics retention of logs, events, sessions	(Measured in days. See Exabeam Product Entitlement for details.)			
Cloud Archive (optional add-on)	—	—	✔	✔
Use Case Packages				

	Fusion XDR		Fusion SIEM	
Feature	**Core**	**Enterprise**	**Core**	**Enterprise**
Number of supported packages, a choice of: • External Threats Use Case Package • Compromised Insiders Use Case Package • Malicious Insiders Use Case Package	2	3	2	3
Customization of rules, models, and objects[a.]	—	✔	—	✔

[a.]During the term of the subscription: (1) CUSTOMER shall maintain complete and accurate records of its Product use solely for EXABEAM confirming compliance with the usage allowed under the Uses Cases Package and customization in the Order(s); and (2) EXABEAM shall have the right, no more than once per year, upon at least thirty (30) days prior written notice, to require CUSTOMER to self-certify that it complied with the usage metrics and limitations in the applicable Order(s). Any usage in excess of the allowed usage listed in the Order (s), will be subject to an additional charge.

The following table displays the features supported by each license type. A dash (—) indicates a feature is not supported.

The entitlements for Exabeam products, SaaS, and Technical Support offerings are limited to those described in Exabeam Product Entitlement. In the event of a conflict between the documentation, including this page, and the Product Entitlement Document, the Product Entitlement Document shall prevail.

Supported Regions for Data Residency

Your log data is ingested, parsed, and stored in the region chosen by your organization. The following table displays the regions that are supported along with the relevant instance base URL for each region:

Region	Instance URL
US West	*.exabeam.cloud
US East	*.use1.exabeam.cloud
Singapore	*.sg.exabeam.cloud
Australia	*.au.exabeam.cloud
Canada	*.ca.exabeam.cloud
Japan	*.jp.exabeam.cloud
Europe	*.eu.exabeam.cloud
Switzerland	*.euw6.exabeam.cloud
UK	*.uk.exabeam.cloud
KSA	*.sa.exabeam.cloud

Get Started with the New-Scale Security Operations Platform

Review the following considerations before using the New-Scale Security Operations Platform.

- (Optional) Allow Exabeam IP Addresses for your Region
- Define a Unique Site Name

(Optional) Allow Exabeam IP Addresses for your Region

Depending on your network requirements, if you need to allow features in the New-Scale Security Operations Platform—such as Advanced Analytics and Cloud Collectors—to receive traffic from public endpoints, you must enable egress access to the IP addresses for your region. In addition, the Exabeam API also has dedicated IP addresses for the API gateways (see API Base URLs).

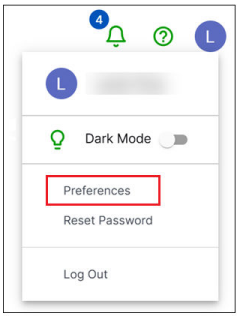
Region	IP Addresses
Australia	• 34.87.192.246 • 34.87.242.103 • 34.87.249.3 • 34.116.122.76 • 34.151.69.27 • 34.151.81.138 • 34.151.106.52 • 35.189.40.105 • 35.189.54.76 • 35.189.60.241 • 35.197.184.195 • 35.201.6.92 • 35.201.23.71 • 35.201.31.76 • 35.244.70.234 • 35.244.74.187 • 35.244.96.148 • 35.244.118.214
Canada	• 34.118.159.64/27
Europe	• 34.89.162.64/26
Japan	• 34.146.154.160/27
Saudi Arabia	• 34.166.95.192/26
Singapore	• 34.87.34.96/27
United Kingdom	• 34.39.39.64/27
US-East	• 34.138.78.128/26
US-West	• 34.168.226.64/26
Zurich, Switzerland	• 34.65.194.0/26

(Optional) Configure Detection Rule Display Preferences

The **Detection Rule Display** preference lets you control the amount of rule information displayed for detection events in the Search and Threat Center applications. You can opt to show just the rule name, just the rule reason, or both. The option you select is applied to rules that are displayed for detection events across the Search and Threat Center applications.

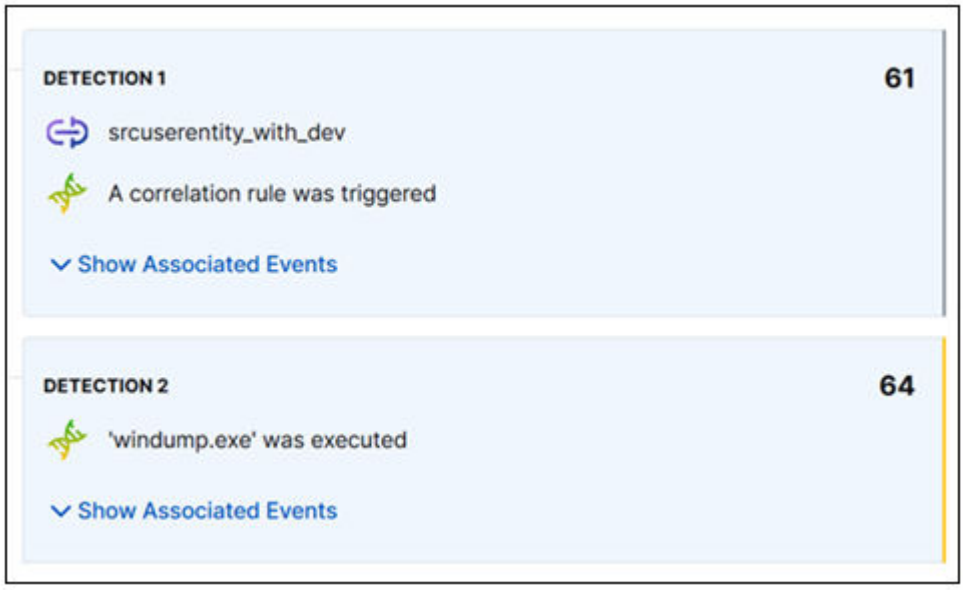
To configure your preference:

1. Click your account profile circle in the upper-right corner of the Exabeam application, and select **Preferences**.

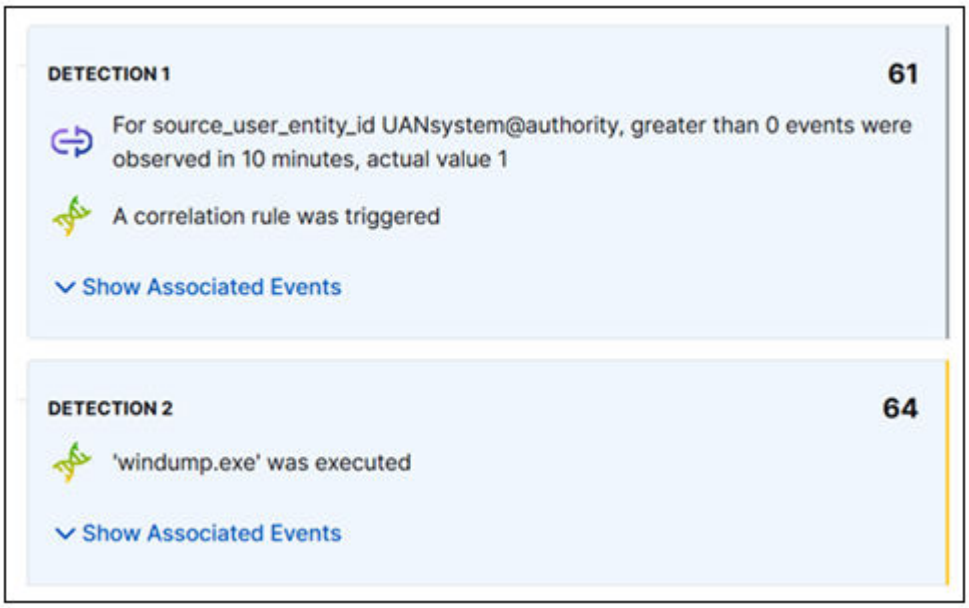


   The **Preferences** page opens.

2. At the top of the **Preferences** page, click the **General** tab. The **Detection Rule Display** options are displayed.
3. Select one of the following options:
   - **Show only rule name** `rules.rule` – This option will include only the rule name field when detections are displayed. See the sample image:



   - **Show only rule reason** `rules.rule_reason` – This option will include only the rule reason field when detections are displayed. This is the default option. See the sample image:



- **Show both rule name** `rules.rule` **and rule reason** `rules.rule_reason` – This option will show both the rule name and the rule reason fields when detections are displayed. The rule name will appear as a title, with the rule reason below it. See the sample image:



Define a Unique Site Name

Create unique site names within New-Scale Security Operations Platform to restrict access security data. You can manage multiple sites with distinct access.

Defining unique site names is a way to manage the access you provide to security data from specific sources. Once you create a unique site name, it becomes available to associate with a specific cloud or site collector instance. Event and alert data collected is then tagged with the site name and ID associated with that collector. Defining unique sites allows the following capabilities across your entire organization, including independent IT infrastructures or sites:

- Associate logs with the respective site or IT infrastructure by tagging all log sources with the site name during log collection.
- Use Search, Dashboard, and Correlation Rules within or across the entire organization, even when multiple sites have overlapping IP addresses.
- Use the metadata fields *m_sitename* and *m_siteid* to search, correlate, and visualize security data for any defined site.

To create a new site:

1. Log in to the New-Scale Security Operations Platform with your registered credentials as an administrator or security engineer.

   NOTE
   Ensure that you have the appropriate permissions to define the site. For more information, see site management permissions.

2. Navigate to **Settings** > **Site** > **Site Management**.

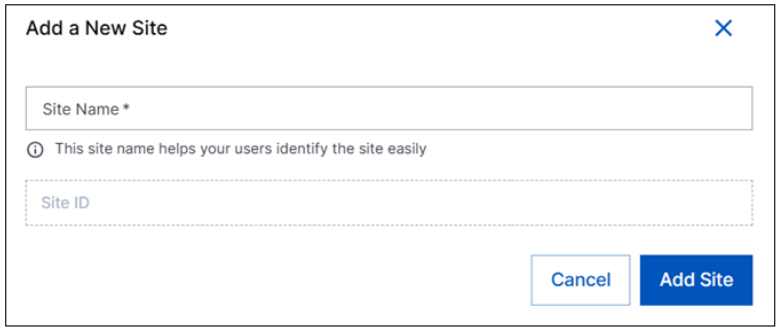
   

   The **Site Management** settings page opens.

3. At the top right of the page, click **Add a New Site**. The **Add a New Site** dialog box opens.

   NOTE
   You can create a new site while configuring a cloud collector and updating a site collector instance.

4. Enter a Site Name, and click **Add Site**.

   A site ID is generated automatically and the new site with a unique name and ID is created. The new site becomes available to associate collectors with so that data collected by either

cloud or site collectors is tagged appropriately. The `m_sitename` and `s_siteid` fields are added to all events ingested by the collector associated with a unique site. These fields are available in downstream applications such as Search to identify data from a specific source. The **Site ID** is automatically generated and cannot be changed. But you can edit the **Site Name** by clicking the options icon (⋮) in the row for a specific site.

> **NOTE**
> For all cloud collectors that use Webhooks, expect a delay of up to five minutes before logs reflect the updated site name tags.

Enable Multi-factor Authentication

To reduce downtime in the event of SSO interruption, you can require Multi-factor Authentication (MFA) for all local accounts. To enable it:

1. Log in to the New-Scale Security Operations Platform.

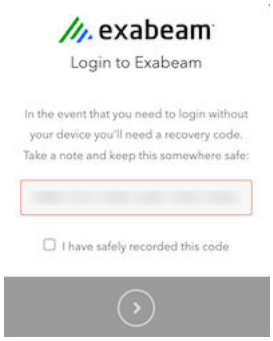
> **NOTE**
> If using a Multi-Org deployment, ensure you log in to the parent organization.

2. In Settings, select **Single Sign-On/MFA**.
3. Toggle the switch to enable MFA for local accounts. When enabled, local accounts will require registration of a MFA token on the next login.



Setting up TOTP Authenticator

1. Download a compatible Auth0 TOTP (Time-based One-Time Password) authenticator app. Exabeam currently supports Google Authenticator.
2. Log out and log back in to the New-Scale Security Operations Platform with a local account.
3. On your initial login after enabling MFA, scan the QR code that appears with your authenticator app and enter the 6-digit code.
4. On the next screen, note and save the recovery code in case you need to login without your device.

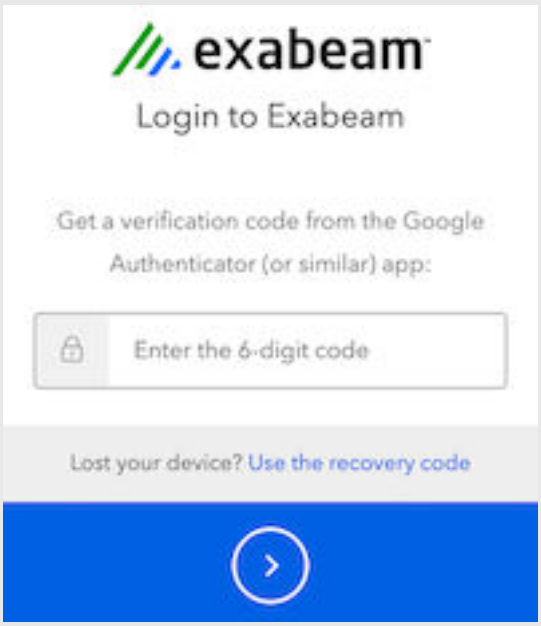


5. Click **Continue** on the success screen.



NOTE

On each subsequent login, local accounts will now need to use the TOTP authenticator to generate a 6-digit code to use when logging in.

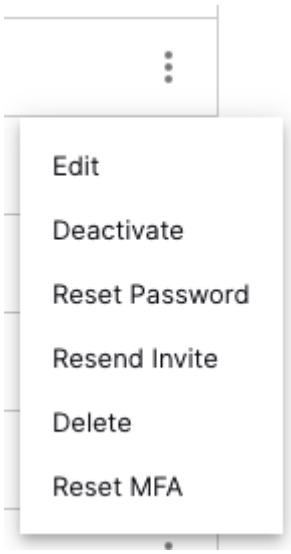


Resetting a token

You can reset a token anytime for a local account.

1. On the **Users** settings page, navigate to an account.

2. From the ⋮ menu, select **Reset MFA** to force new MFA on the account.



Configuring Tenant Session Timeout

Overview

To provide organizations with greater flexibility and control over their security posture, Administrators and Security Engineers can configure a custom session timeout duration for their specific tenant.

You can tailor your session lengths to meet your exact operational needs, whether that means shortening the timeout to meet heightened security and compliance controls, or extending it to support continuous visibility for Security Operations Center displays.

Important Considerations

Before modifying your session timeout settings, please review the following parameters:

- **Allowed Range:** The minimum allowed duration is **1 hour**, and the maximum is **24 hours**.
- **Scope of Enforcement:** Once applied, the configured session duration is enforced for all standard users within that tenant.
- **Roles:** Only Administrator and Security Engineer roles can configure session timeouts.
- **Default Value:** If no custom value is set, the session timeout defaults to **4 hours**.

> ⚠ **CAUTION**
> Extending the access-token lifetime beyond the 4-hour default increases the window in which a stolen or exposed token may be misused. Users who select a longer duration, up to 24 hours, are responsible for evaluating and accepting the associated security risk.

How to Configure Session Timeout

1. Log in to your tenant and navigate to **Settings**.
2. Under Team, select **Single Sign-On/MFA**.
3. Locate the **Session Timeout** configuration field.
4. Enter your desired timeout duration in hours or combination of hours and minutes. (must be between 1 and 24 hours).
5. **Save** your changes. The new session timeout will take effect for all users upon their next login.

Connect to Exabeam MCP Server

The Model Context Protocol (MCP) is an open standard for AI applications that acts as a bridge between an AI model and external data sources or tools. The main purpose of an MCP server is to make AI models more accurate and useful by providing access to internet-hosted tools and data. This offers real-time information and capabilities that were not part of their original training. Developers can build and host remote MCP servers that communicate with AI tools over the internet.

Exabeam offers a way to connect AI tools to an Exabeam MCP Server. With this connection, you can use your tool of choice to aid in discovering, retrieving, and acting on Exabeam data.

Connection Types

You can connect by either using user-delegated authentication or by application-level API keys. Using user-delegated authentication, you authenticate as yourself using your Exabeam credentials. This means All MCP tool calls, such as case queries and alert lookups, are recorded in the Exabeam Audit Log and attributed to your user account, not a shared application identity. Using API keys means all MCP tool calls are attributed to an application identity rather than the individual user making them.

Most users will want user-delegated due to enhanced compliance requirements and security investigations that require per-user audit trails.

Connect Using User-Delegated Authentication (Recommended)

When you connect an AI client — such as Claude, ChatGPT, or Microsoft Copilot — to Exabeam via the MCP you now authenticate as yourself using your Exabeam credentials. All actions taken through the AI client are performed under your identity, respect your existing role-based permissions, and are attributed to you in the Exabeam Audit Log.

When you connect a supported AI client to the Exabeam MCP server for the first time, you are redirected to an Exabeam login screen to complete a one-time authorization step. After you sign in, the AI client receives a token scoped to your identity. No API keys or client secrets are required.

Exabeam Region	Exabeam MCP Server URL	OAuth Client ID
US West	`https://api.us-west.exabeam.cloud/mcp`	`a45c8b47-56b1-4b20-82d2-bb16fd548746`
US East	`https://api.us-east.exabeam.cloud/mcp`	
Canada	`https://api.ca.exabeam.cloud/mcp`	
Europe	`https://api.eu.exabeam.cloud/mcp`	
Saudi Arabia	`https://api.sa.exabeam.cloud/mcp`	
Singapore	`https://api.sg.exabeam.cloud/mcp`	
Switzerland	`https://api.ch.exabeam.cloud/mcp`	
Japan	`https://api.jp.exabeam.cloud/mcp`	
Australia	`https://api.au.exabeam.cloud/mcp`	

Connection steps will vary depending on the tool. Some examples of connection steps include:

- Claude
- Microsoft Copilot (via Copilot Studio, not the end-user Copilot chat interface directly)
- ChatGPT (only supports custom connectors if your org has developer mode plus custom apps enabled)

An example of setup and connecting to Claude via a Custom Connector is below.

Example Setup: Claude

1. Go to https://claude.ai and sign in.
2. Open the left sidebar and select **Customize** > **Connectors**.
3. Click the plus icon and select **Add custom connector**.
4. Fill in the fields:
   - **Connector name** — any name you choose (e.g., Exabeam)
   - **Remote MCP Server URL** — the URL for your environment from the table above
   - **OAuth Client ID** — the client ID for your environment from the table above
   - **OAuth Secret** — leave this blank
5. Click **Add** to save.
6. Select the Exabeam connector you just created and click **Connect**.
7. When prompted, enter your Exabeam tenant domain (e.g., yourcompany.exabeam.cloud) and click **Continue**.
   You will be redirected to your organization's Exabeam login page.
8. Enter your credentials and complete authentication.
9. After a successful login, you will be redirected back to Claude.

You are now connected. Exabeam tools are available in your Claude conversations.

Connect Using API Key

To get started, you will need the following pieces of information:

- API Key
- API Key Secret
- Exabeam MCP Server URL (based on region)

Exabeam Region	Exabeam MCP Server URL	Authorization and Token URLs (if required)
US West	`https://api.us-west.exabeam.cloud/mcp`	**Auth URL**: `https://api.us-west.exabeam.cloud/oauth/authorize`
		Token URL: `https://api.us-west.exabeam.cloud/oauth/token`
US East	`https://api.us-east.exabeam.cloud/mcp`	**Auth URL**: `https://api.us-east.exabeam.cloud/oauth/authorize`
		Token URL: `https://api.us-east.exabeam.cloud/oauth/token`
Canada	`https://api.ca.exabeam.cloud/mcp`	**Auth URL**: `https://api.ca.exabeam.cloud/oauth/authorize`
		Token URL: `https://api.ca.exabeam.cloud/oauth/token`
Europe	`https://api.eu.exabeam.cloud/mcp`	**Auth URL**: `https://api.eu.exabeam.cloud/oauth/authorize`
		Token URL: `https://api.eu.exabeam.cloud/oauth/token`
Saudi Arabia	`https://api.sa.exabeam.cloud/mcp`	**Auth URL**: `https://api.sa.exabeam.cloud/oauth/authorize`
		Token URL: `https://api.sa.exabeam.cloud/oauth/token`
Singapore	`https://api.sg.exabeam.cloud/mcp`	**Auth URL**: `https://api.sg.exabeam.cloud/oauth/authorize`
		Token URL: `https://api.sg.exabeam.cloud/oauth/token`
Switzerland	`https://api.ch.exabeam.cloud/mcp`	**Auth URL**: `https://api.ch.exabeam.cloud/oauth/authorize`
		Token URL: `https://api.ch.exabeam.cloud/oauth/token`
Japan	`https://api.jp.exabeam.cloud/mcp`	**Auth URL**: `https://api.jp.exabeam.cloud/oauth/authorize`
		Token URL: `https://api.jp.exabeam.cloud/oauth/token`
Australia	`https://api.au.exabeam.cloud/mcp`	**Auth URL**: `https://api.au.exabeam.cloud/oauth/authorize`
		Token URL: `https://api.au.exabeam.cloud/oauth/token`

⚠ CAUTION

Before connecting, consider the data you wish to share with your AI tool. Exabeam is not responsible for data you expose to your tool.

If you wish to disable this functionality, open a support request or contact your account team.

1. Follow the Create An API Key instructions to generate an API Key and Secret in the New-Scale Security Operations Platform.
2. Copy and note the API Key and Secret strings.
3. In your AI tool's desktop or web UI, configure the connection to the Exabeam MCP server using the API Key, Secret, and MCP server url. Connection steps will vary depending on the tool.
4. After connecting, you can start interacting with Exabeam data in your AI tool.

Currently Supported Functionality

The list below details the currently supported functionality you can perform with the Exabeam MCP server. New functionality will be added as it becomes available.

Important Considerations

- **Number of calls:** You can perform up to 150,000 MCP calls per month
- **Number of records:** You can access up to 1,000 records across all applications

Application	Functionality
Threat Center	• Search cases • Get case details • Get threat timeline for a case • Get threat timeline for an alert • Create a case • Update a case • Create case notes • Update an alert • Get threat summary • Get related cases
Search	• Run searches • Get search results
Context Management	• Get context table records by ID • Get a list of all context tables
Threat Detection Management	• Get correlation rule details • Get a list of all correlation rules • Get a list of all analytics/detection management rules
Outcomes Navigator	• Get use case score • Get MITRE ATT&CK coverage score

Example Queries

Once connected, you can ask Claude to query Exabeam data in natural language. Claude uses your authenticated Exabeam identity to fulfill these requests. You can only access data that your Exabeam role permits so the same restrictions that apply in the Exabeam UI apply here.

- "Show me a list of critical severity cases from the last 7 days."
- "Tell me which users were involved in *xxxxx* case."
- "Run a search for IP address *x.x.x.x* and summarize the results."
- "What's the timelines for case *xxxxx*?"
- "Pull alerts from the last 7 days that include MITRE tags."
- "Create a case for this suspicious activity."
- "Close case *xxxxx* as a false positive."
- "What is our current use case score?"
- "Get a list of latest cases and send an email to *username@company.com*"
- "Are there any related cases for case *xxxxx*?"

> **NOTE**
> Exabeam also offers an MCP option for developers to interact directly with Exabeam's API documentation. For more information, see MCP Server for Developers on the Exabeam Developer portal.

Webhooks

Webhooks enable you to automatically send messages from Exabeam to third-party applications (such as Microsoft Teams or Slack) in real time whenever specified events are triggered. Webhooks are available for the following areas in Exabeam:

- Audit logs
- Notifications
- Correlation Rules
- Threat Center

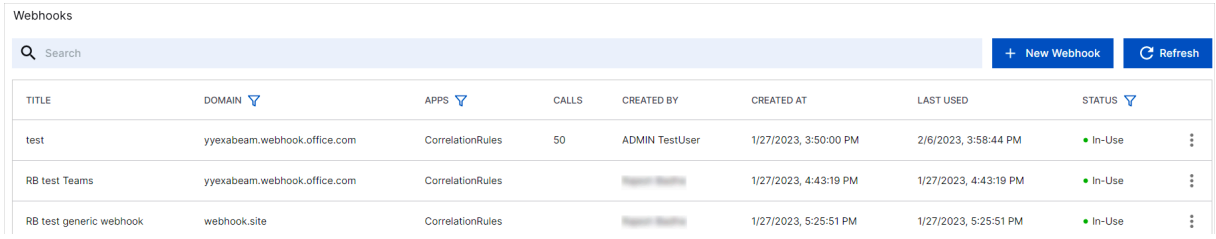
Add a Webhook

You must add webhooks to your environment before you can use them in your applications. They are added in the Exabeam Security Operations Platform settings.

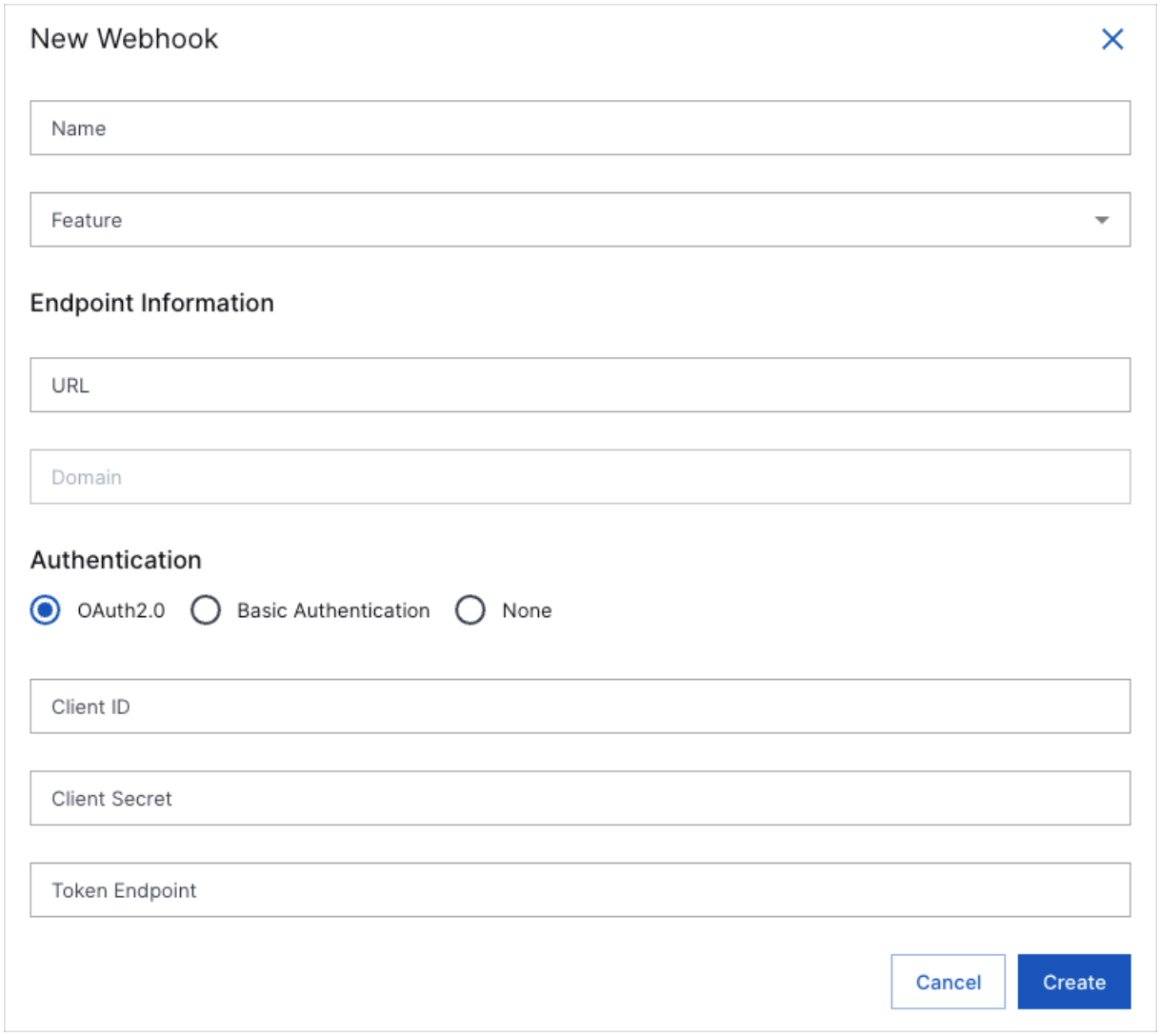
To add a webhook:

> **NOTE**
> If you selected **Add a new webhook in settings** from the **Define Rule Outcomes** page of Correlation Rules, skip to step 2.

1. Open the Exabeam Security Operations Platform and on the lower-left side of the page, click **Settings**, and then click **Webhooks**.
   A settings page displays with a list of the available webhooks.



2. Click **+ New Webhook**.
   The New Webhook dialog displays.



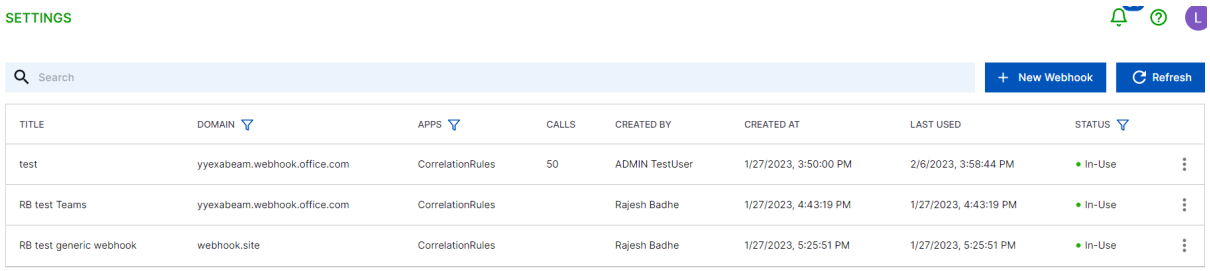
- **Name** your webhook.
- Select a **Feature** from the drop-down menu.
- Provide a **URL** for the webhook.
  The **Domain** field is auto-filled based on the URL you provide.

- Select an Authentication option, and then do the following if you selected **OAuth2.0** or **Basic Authentication**.
  - If you selected *OAuth2.0*:
    1. Enter a **Client ID**.
    2. Enter a **Client Secret**.
    3. Enter a **Token Endpoint**.
  - If you selected *Basic Authentication*:
    1. Enter a **Username**.
    2. Enter a **Password**.

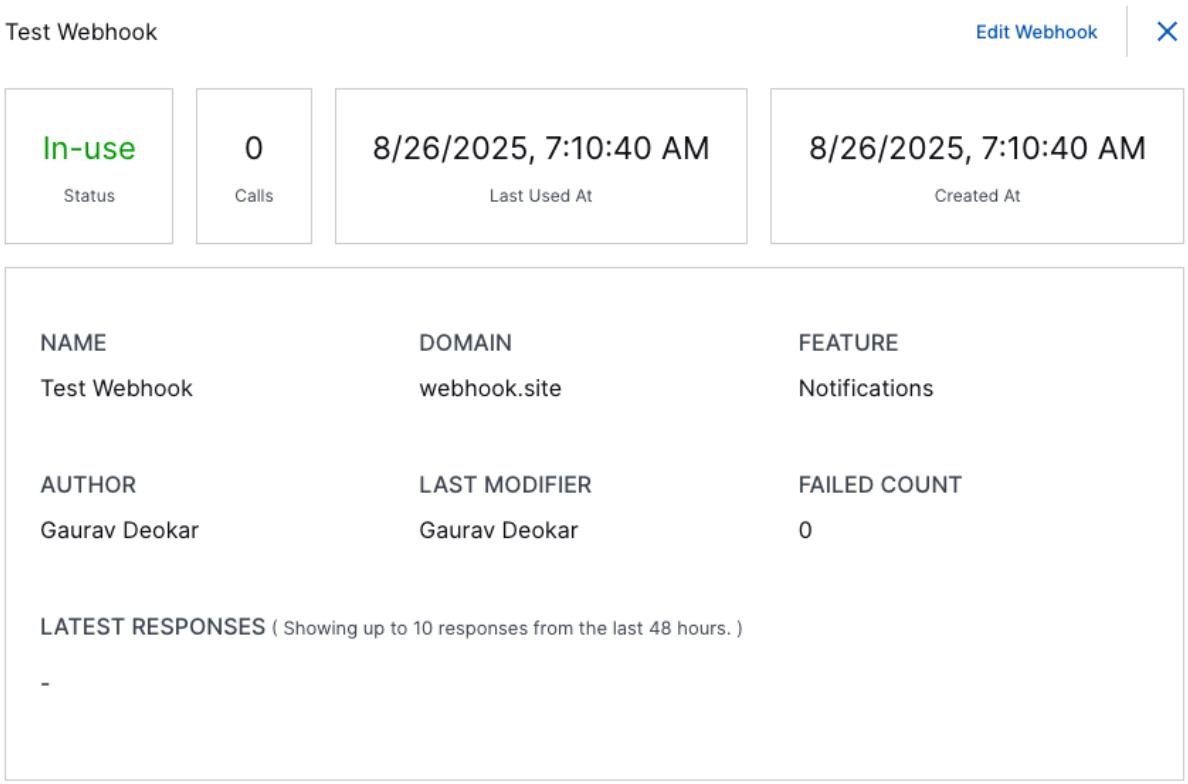
3. Click **Create**.

View Details/Edit a Webhook

1. Open the Exabeam Security Operations Platform and on the lower-left side of the page, click **Settings**, and then click **Webhooks**.
   A settings page displays with a list of the available webhooks.



2. Click the menu on the rule you wish to view/edit, and then select **View Details**.
   The View details webhook dialog displays.



NOTE
Only the 10 most recent responses over the past 48 hours will be displayed.

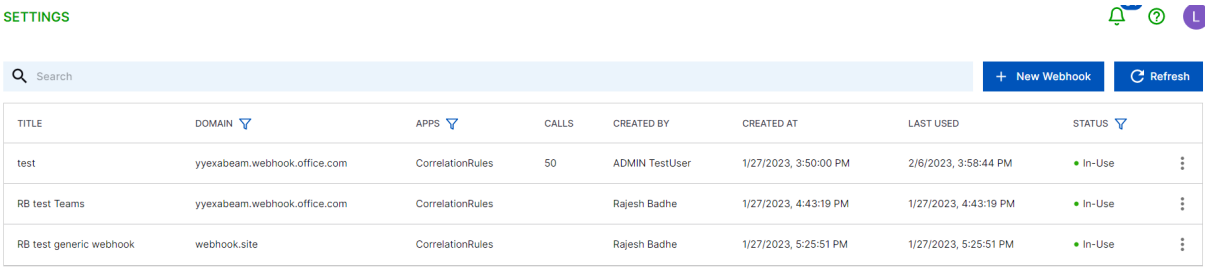
3. View additional details about the webhook. To edit the webhook properties, select **Edit Webhook** from the dialogue.

NOTE
You cannot change the URL of an existing webhook.

4. Make any edits and then click **Save Edits**.

Delete a Webhook

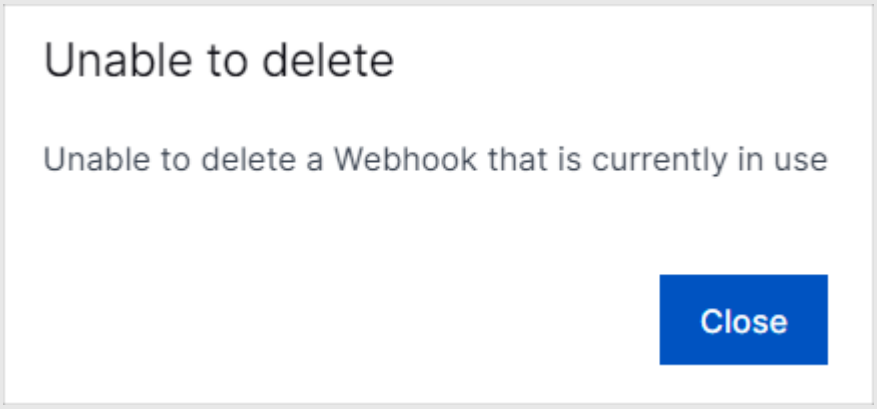
1. Open the Exabeam Security Operations Platform and on the lower-left side of the page, click **Settings**, and then click **Webhooks**.
A settings page displays with a list of the available webhooks.



2. Click the more menu icon ⋮ for the rule that you want to edit, and then select **Delete**.

NOTE

You cannot delete a webhook that is currently in use as an outcome for an existing rule. If you try to delete a webhook that is in use, a message displays to indicate that it cannot be deleted.

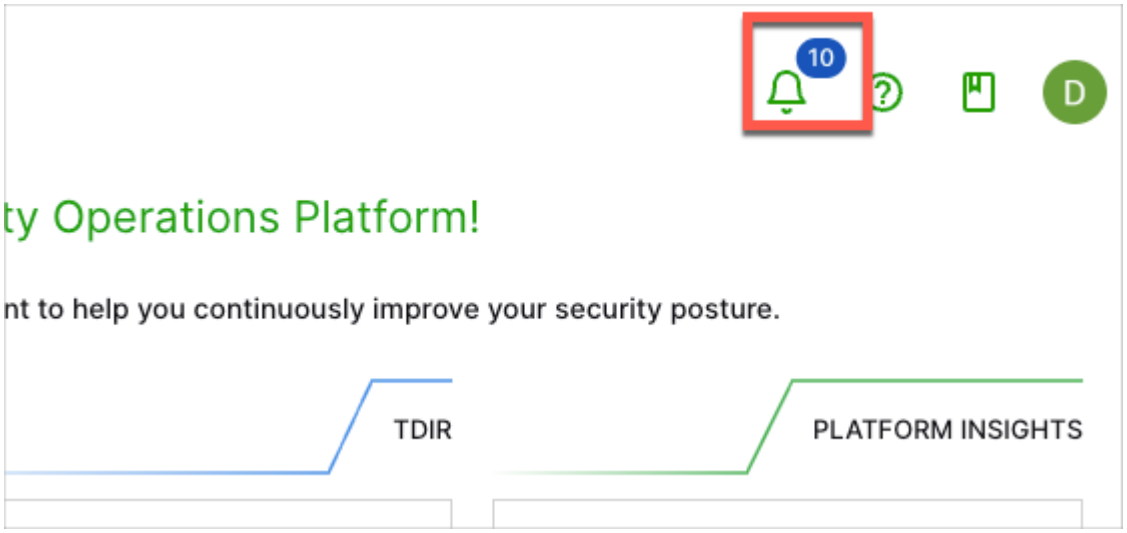


3. To confirm the deletion, click **Delete**.

Notifications

The Exabeam Security Operations Platform has a centralized notification system for receiving and managing notifications from the different Exabeam applications you're subscribed to. Notifications help you stay up to date with the health and performance of your applications, and are divided into three severities: Informational, Warning, and Critical. Notifications can be delivered in-app, via email, or via specific webhook channels. You have granular control over which notifications you receive and how you receive them.

You can access your notifications from any page on the Exabeam Security Operations Platform by clicking the notification icon on the upper-right side.



NOTE

The number next to the notifications icon indicates how many new notifications you have. If you do not currently have any new notifications, a number is not displayed.

For more information on viewing and managing notifications, see the following:

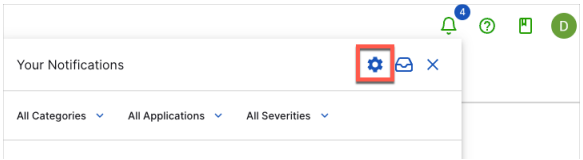
- Manage Notification Preferences
- Manage Global Notifications Preferences
- View New Notifications
- View Inbox

Manage Notification Preferences

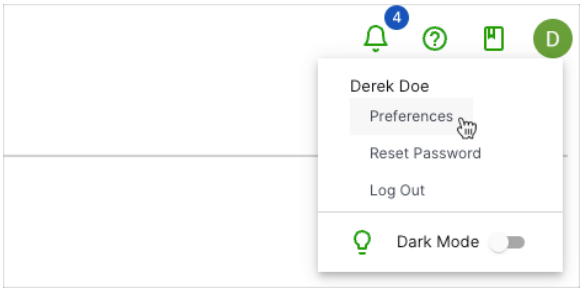
By default, you receive all notifications for the products that you're subscribed to. From the Preferences page, you can manage which notifications you receive and how you receive them.

To manage your notifications:

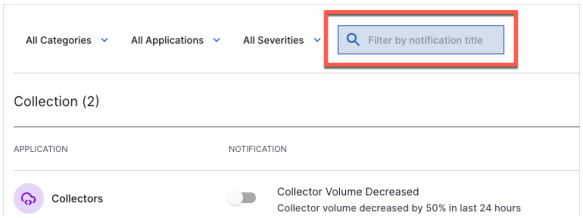
1. Do one of the following:
   - Click the notification icon to open the Your Notifications window, and then click the settings icon.

   - Click your account profile circle on the upper-right corner of the page, and then click **Preferences**.



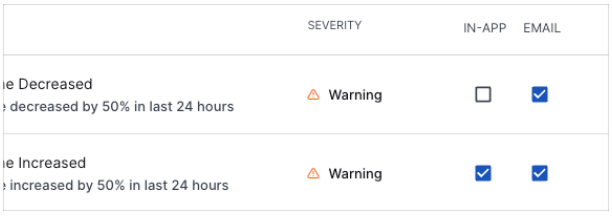
2. (Optional) Filter the notifications list to locate the notification(s) that you want to view.
   - To filter by **Categories**, **Applications**, and/or **Severities**, click their respective drop-down menus and select from the available values.
   - To **Filter by notification title**, click in the filter box and start typing a title or key words within a title.



3. (Optional) To turn notifications on or off, click their toggles.
   A blue toggle indicates a notification is on; a gray toggle indicates a notification is off.



4. (Optional) To modify the notification delivery methods for a notification, select or clear the **In-App** and **Email** checkboxes as needed.
   You can apply both delivery methods to a notification. A blue checkbox indicates the delivery method is enabled; an empty checkbox indicates the method is disabled.



Manage Global Notifications Preferences

Global notifications are created from webhooks, which enable you to automatically send messages from Exabeam to third-party applications (such as Microsoft Teams or Slack) in real time whenever specified events are triggered. The **Global Notifications** page is the interface for

administrators to turn these notifications on or off and select where to send them. From this page you can also edit existing webhooks and add new webhooks.

Managing global notifications requires creating a new webhook connection and configuring the notification options for different Exabeam applications and services. For details, follow the links below:

- Add a New Notification Channel
- Configure Global Notification Options

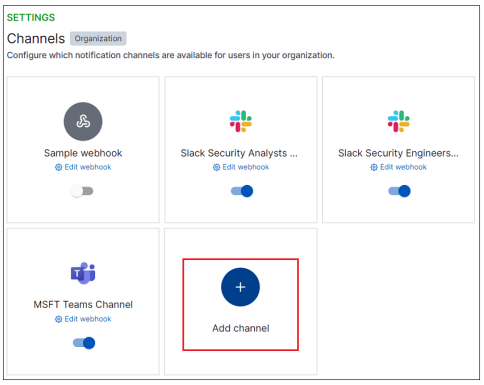
Add a New Notification Channel

Configure webhooks to add new notification channels. To create a new webhook connection:

1. In the New-Scale Security Operations Platform, click **Settings** (⚙) in the left navigation pane and select **Global Notifications**.
   The **Global Notifications** page opens. The **Channels** section at the top of the page displays your existing webhooks.

   > **NOTE**
   > This **Settings** page only shows webhook options for notification purposes. To configure options for other types of webhooks, navigate to **Settings** > **Developer** > **Webhooks**.

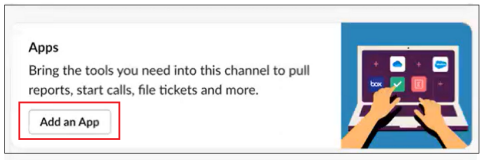
2. Click **Add channel**.



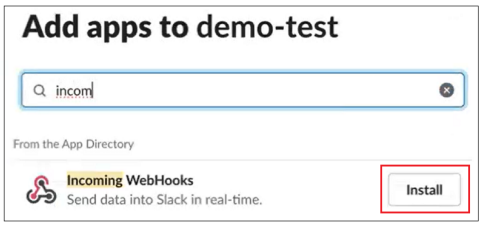
3. Select the type of notification channel you want to create. Current options include:
   - **Slack** – Create a webhook connected to a specific Slack channel. For the endpoint URL you'll need in the next step, follow the steps below in Find the Incoming Webhook Endpoint for Slack.
   - **Microsoft Teams** – Create a webhook connected to a specific Teams channel. For the endpoint URL you'll need in the next step, follow the steps below in Find the Incoming Webhook Endpoint for Microsoft Teams.
   - **Custom Webhook** – Create a custom webhook connected to a specific URL.
   - **Email** – Send notifications from system events to a specific user email or distribution list.

Find the Incoming Webhook Endpoint for Slack

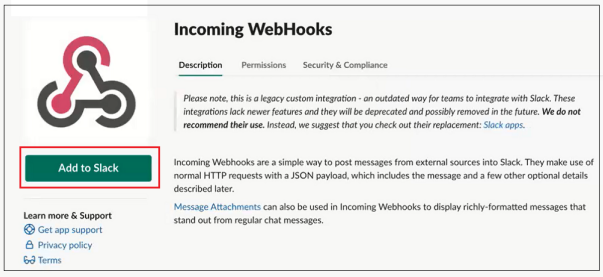
1. Log into Slack, either in the desktop application or online.
2. Create a new channel or locate an existing channel and click it to expand the options menu.
3. Select **View channel details**. A details dialog box opens.
4. Select the **Integrations** tab and click **Add an App**.



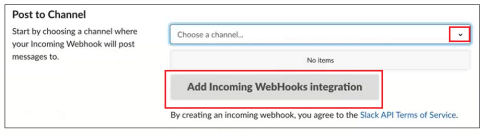
5. In the **Add apps** page, use the search bar to find **Incoming WebHooks**.
6. Click **Install**.



7. On the **Incoming WebHooks** page, click **Add to Slack**.



8. In the **Post to Channel** section, use the dropdown arrow to choose the channel you're creating a webhook for.



9. Click **Add Incoming WebHooks integration**. A WebHook URL is generated and displayed on the **Incoming WebHooks** page.
10. Copy the URL from the **Webhook URL** field.

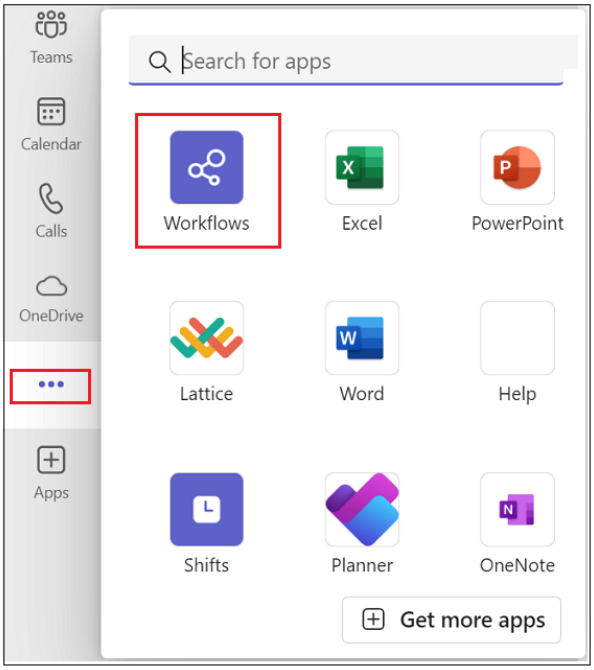


11. Paste this URL into the in the **Endpoint Information** section when configuring a new Slack webhook in the New-Scale Security Operations Platform.

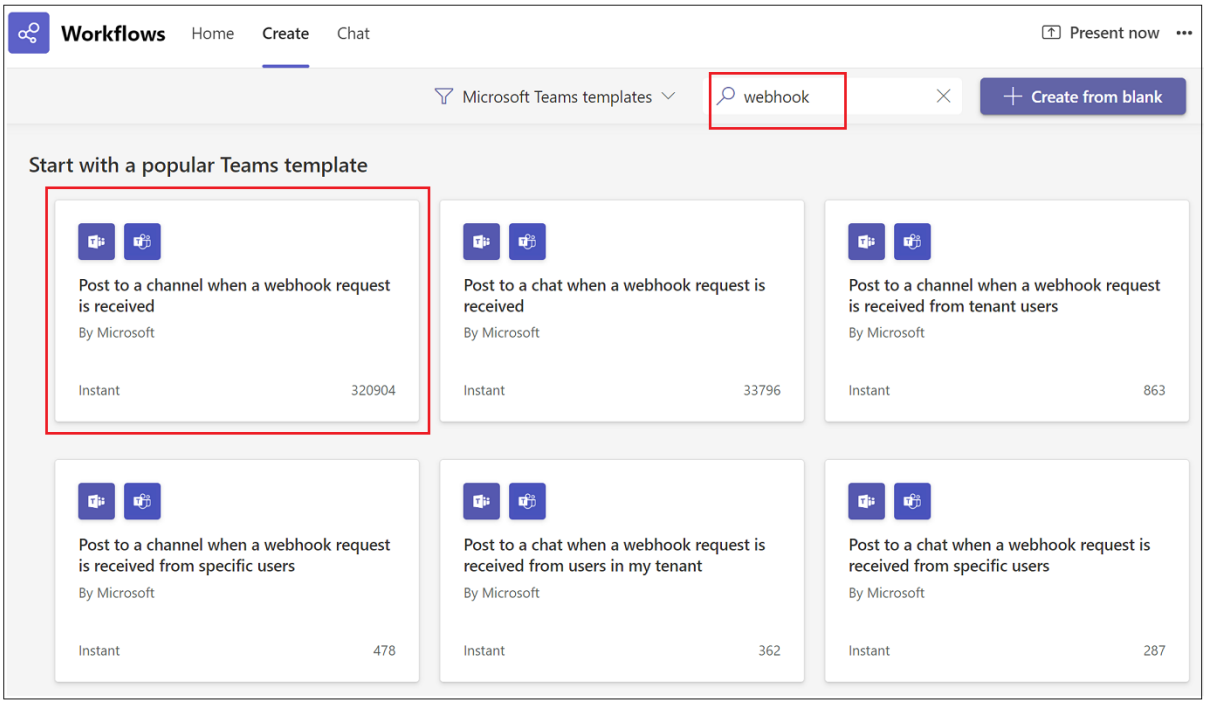
Find the Incoming Webhook Endpoint for Microsoft Teams

In Microsoft Teams, you will need to use the Workflows application to configure an endpoint for any Teams channel to which you want to send notifications.

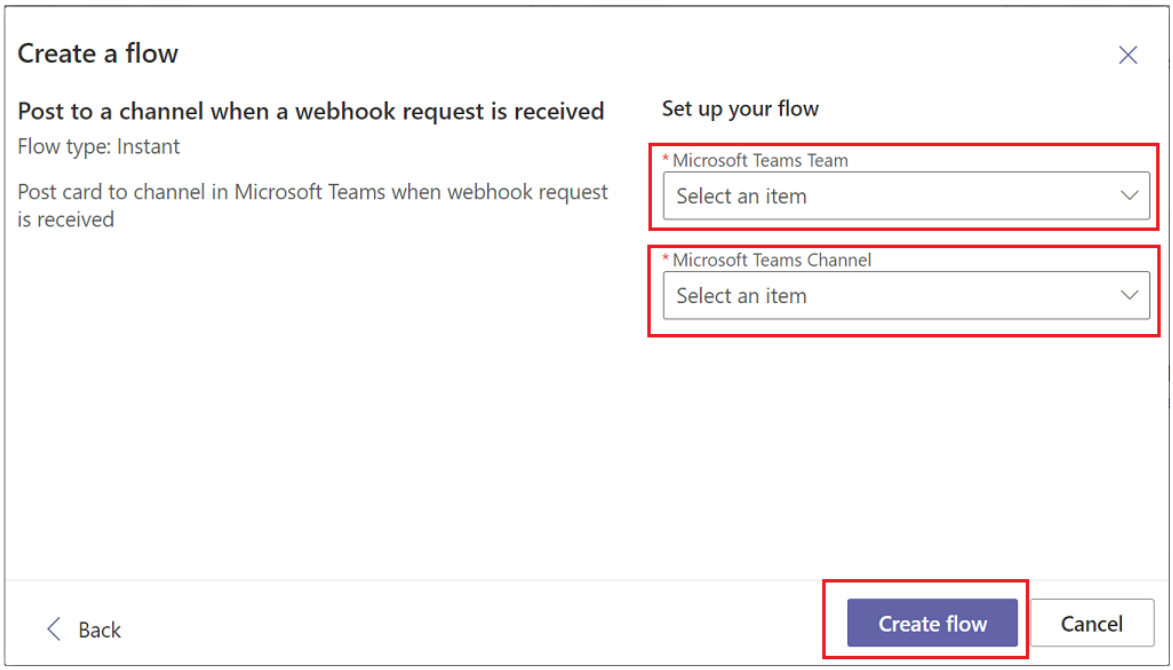
1. Log into Microsoft Teams.
2. In the left navigation panel, click the **View more apps** icon (•••) and select the Workflows application.
   If you have not used Workflows previously, you might need to search for it and click **Add** to add it to your available apps.



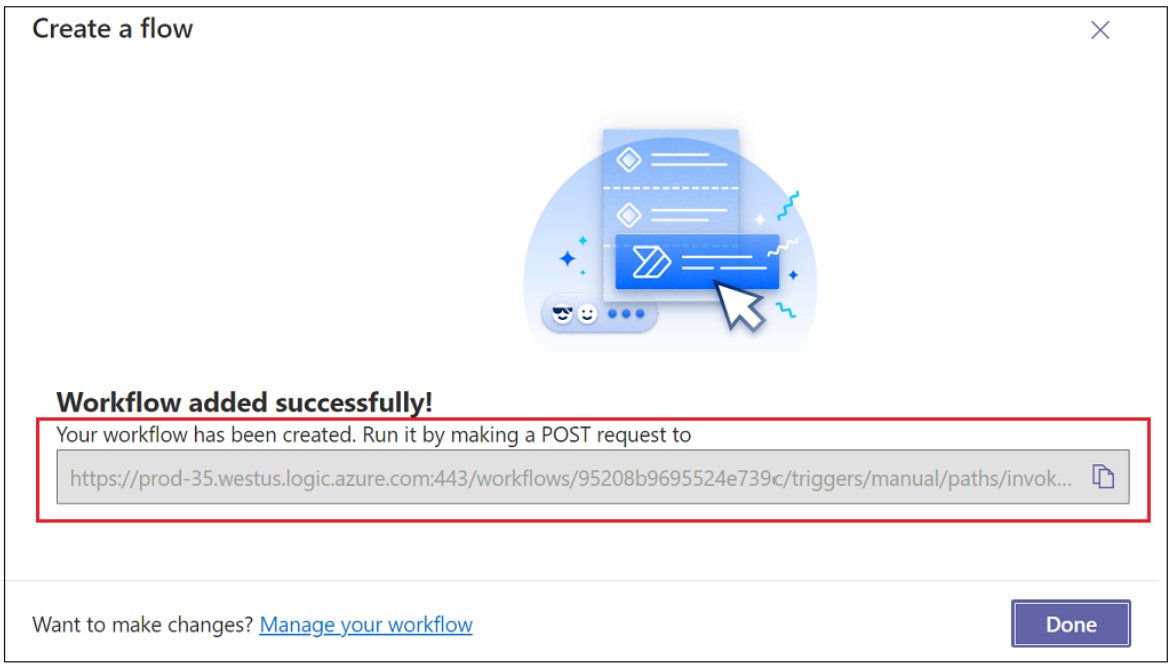
   The Workflows application opens in your Teams window.
3. At the top of the Workflows application window, click **Create**. A page of existing Microsoft Teams templates opens.
4. In the **Search templates...** field, enter `webhook` and press Enter on your keyboard to filter the templates.
5. Select the template in the top left corner called **Post to a channel when a webhook request is received**. A **Create a flow** dialog box opens.



6. Enter a name for the new flow in the **Flow name** field and click **Next**. The next flow configuration screen is displayed.
7. Enter information in the following fields:In the **Microsoft Teams Team** field, use the drop down arrow to find and select one of your existing teams.
   - **Microsoft Teams Team** – Use the drop down arrow to find and select one of your existing teams. Alternately, you can click **Add a custom item** and create a new team.
   - **Microsoft Teams Channel** – Use the drop down arrow to find and select an existing channel in the team you selected in the previous field. Alternately, you can click **Add a custom item** and create a new channel for the team



8. Click **Create flow**. If your new flow is added successfully, a URL link is generated and displayed in the dialog box.
9. Click the **Copy** icon ( ) to copy the URL to your clipboard.



10. Paste this URL into the **Endpoint Information** section when configuring a new Microsoft Teams webhook in the New-Scale Security Operations Platform.

> **TIP**
>
> When you create a workflow, you are the sole owner of that flow and only you can modify or manage it. It's a good idea to assign a co-owner to the flow so that it can be accessed even if you are unavailable. To add a co-owner:
>
> - Click **Home** at the top of the Workflows app screen.
> - Select a flow to open a details page.
> - From the **Connections** box on the top right, click **Edit**.
> - Enter a user or group to serve as a co-owner. The new co-owner is notified and is displayed in the **Co-owners** box below **Connections**.

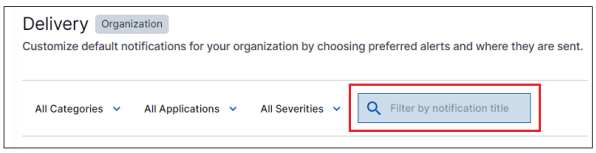
Custom Webhook

1. If using a custom webhook, enter a **Webhook name** and **Endpoint Information** in the **Add new custom webhook** dialog box.
2. Click **Add webhook**. A new webhook tile is displayed in the **Channels** section of the **Global Notifications** page.

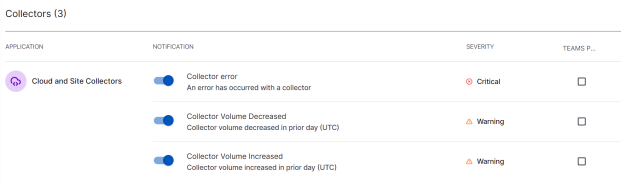
Configure Global Notification Options

The **Delivery** section of the **Global Notifications** page provides the following options for filtering and configuring the global notifications:

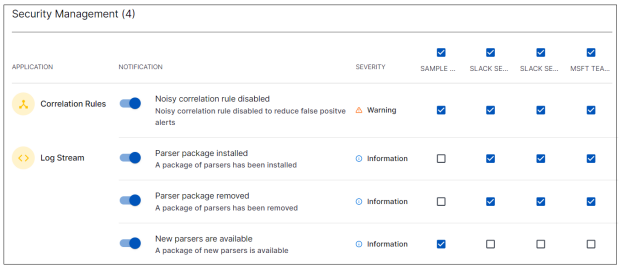
- You can filter the notifications lists to locate specific notifications you want to view:
  - To filter by **Categories**, **Applications**, or **Severities**, click their respective drop-down menus and select from the available values.
  - To **Filter by notification title**, click in the filter box and start typing a title or keywords within a title.



- To turn notifications from a specific application on or off for all channels, click their **Notification** toggles. A blue toggle indicates a notification is on; a gray toggle indicates a notification is off.



- To configure which channels should receive notifications from a specific application, select the appropriate check boxes for each application row.



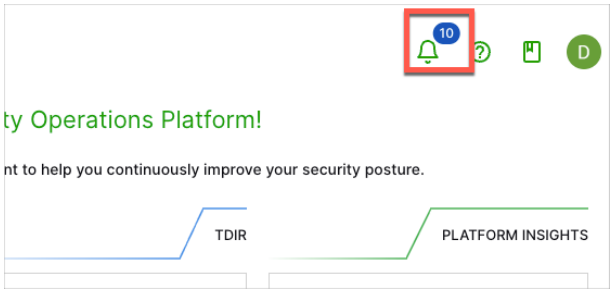
View New Notifications

You can quickly view your new notifications from any page of the Exabeam Security Operations Platform by opening the Your Notifications window. This window displays any new notifications that you have received within last seven days. You can filter the notifications to find the ones you want to view, and clear them from the window by marking them as read.

> **NOTE**
> Once you mark notifications as read, you can no longer view them in the Your Notifications window. However, you can still view them from the Inbox page. See View Inbox.

To view new notifications:

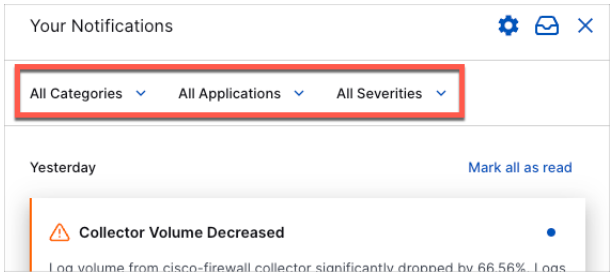
1. Click the notification icon .



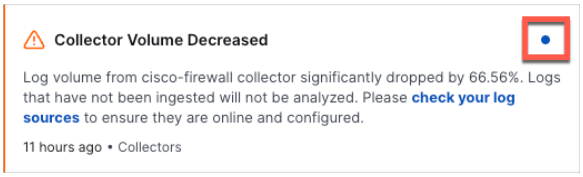
The Your Notifications window opens.

> **NOTE**
> Depending on the number of notifications, you may need to use the scroll bar on the right side of the window to view them all.

2. (Optional) To filter the notifications, click the **Category**, **Applications**, and/or **Severities** drop-down menus and select the options that you want to view.



3. (Optional) To mark notifications as read, do either of the following:
   - To mark an individual notification as read, click the icon on the notification card.

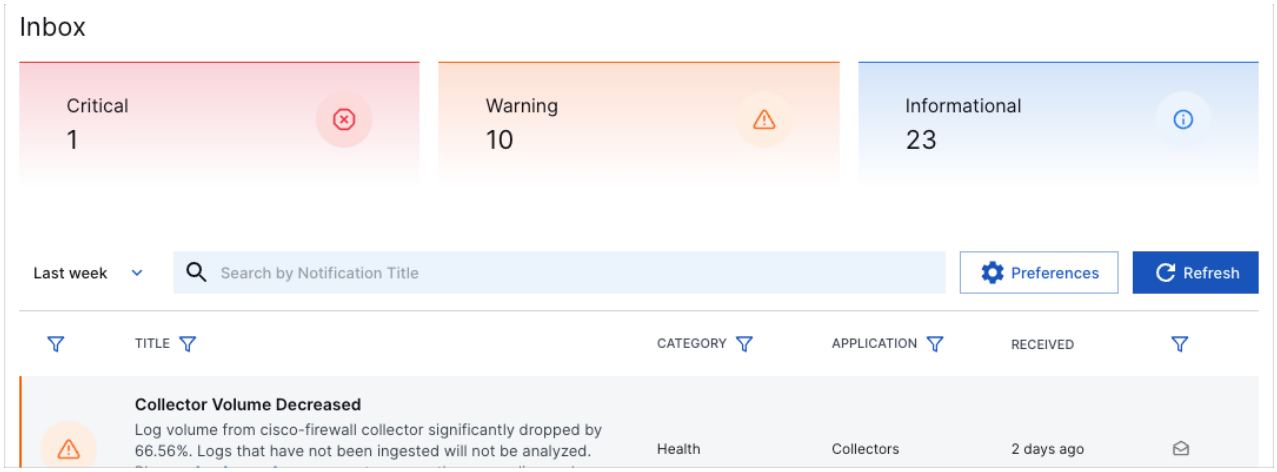


   - To mark all notifications as read, click **Mark all as read**.

View Inbox

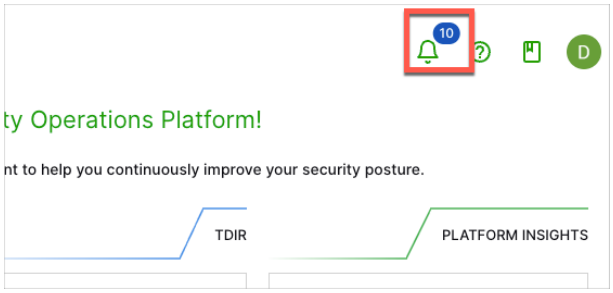
The Inbox page contains all the notifications that you've received over the last 90 days, including both new and read notifications. The Inbox includes a variety of filters for you to find the notifications that you want to view. You can mark new notifications as read, and you can change the status read notifications back into new (which enables you to view them in the Your Preferences window again).

The header of the Inbox page breaks down the number of Critical, Warning, and Informational notifications that you have received.



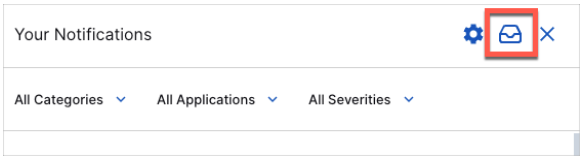
To view your inbox:

1. Click the notification icon .



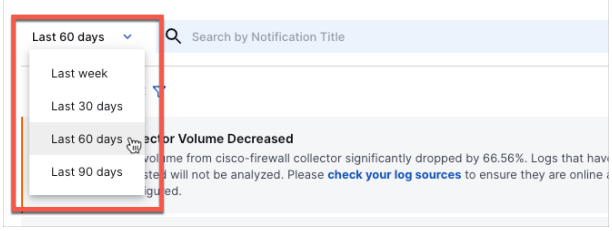
The Your Notifications window opens.

2. To open the Inbox page, do one of the following:
   - On the upper-right side of the window, click the inbox icon.



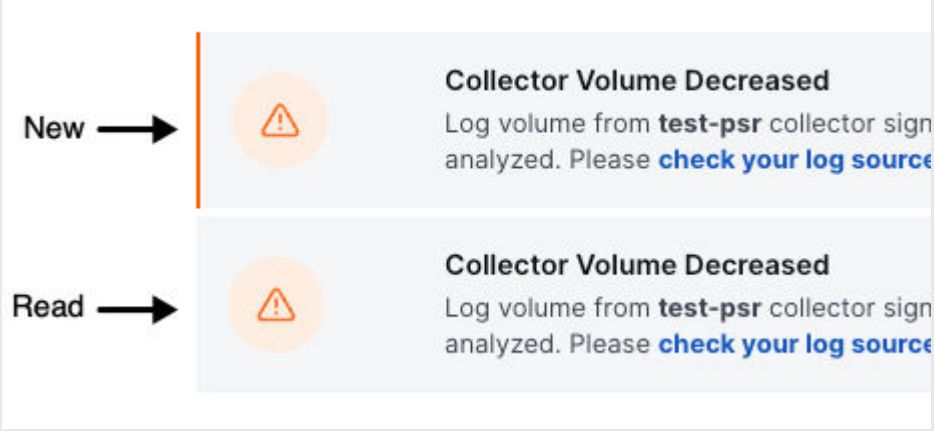
   - At the bottom of the window, click **View all notifications**.

3. (Optional) To change the notification timeframe filter, click the drop-down menu to the left of the search box, and then select a time value.



4. (Optional) To **Search by Notification Title**, click in the search box and start typing a title or key words within a title.
5. (Optional) To filter the notifications by severity, **Title**, **Category**, **Application**, and/or new or read status, click the respective drop-down icons from the column headings and select the items that you want to view.

NOTE
A red line on the left of the notification bar indicates that the notification is new.



6. (Optional) To change the new/read status of notifications, click the and icons to change from one status to the other.

Universal Role-Based Access

The universal role-based access centralizes user identity and access management for applications across the New-Scale Security Operations Platform. With universal role-based access, users can access all their Exabeam applications through a single login account. Likewise, administrators can manage user accounts and permissions for the entire New-Scale Security Operations Platform through a single interface. Universal role-based access streamlines the threat detection and incident response (TDIR) workflow by reducing access gaps and making it easier for users to navigate between products. It simplifies account administration and reduces opportunities for credential misuse.

Universal role-based access supports local user accounts created in Exabeam as well as account integration with SAML 2.0 compliant third-party identity providers.

IMPORTANT

Universal role-based access does not support IdP-initiated SAML authentication due to the security risk of man-in-the-middle-attacks.

Considerations for Adopting Universal Role-Based Access

You are encouraged to migrate to universal role-based access as soon as your organization is ready.

Before migrating to universal role-based access, note the following:

- Customers can continue to use legacy authentication until they are prepared to migrate.
- Migration to universal role-based access is permanent.
- Universal role-based access supports concurrent local authentication and SAML 2.0 compliant third-party IdP authentication.
- Universal role-based access does not support authentication from services such as LDAP, MS Active Directory, common access card (CAC), and personal identity verification (PIV).
- Advanced Analytics and Data Lake are migrated separately.
- User email addresses are required for migration. Each email address designates a single identity.
- Customers using third-party IdPs need to update their IdP configuration to complete the migration process.
- Legacy Advanced Analytics identities are still needed to authenticate into Cloud Connectors.

  NOTE

  When universal role-based access becomes available for Cloud Connectors, Cloud Connectors will automatically migrate to it.

- Universal role-based access is not available for on-premises applications.

User Roles

Exabeam uses role-based access control to manage user permissions and access to Secured Resources. A variety of preconfigured default roles are included in the New-Scale Security Operations Platform for its different features. The roles are designed for common user types such as analysts, administrators, and auditors. However, if the default roles do not meet all your needs, you can Create a Custom User Role with specific permission sets tailored to your security needs.

Each user is assigned one or more User Roles. Users who are assigned multiple roles receive the aggregate of all permissions across their assigned roles.

User Permissions

Each default and custom role defines the specific permissions entitled to users with that role assignment. Permissions are grouped by permission categories as described in the following topics:

- API Permissions
- Collectors Permissions
- Compliance Permissions
- Identity and Access Management Permissions
- Investigation and Response Permissions
- Log Stream Permissions
- Platform Insights Permissions
- Security Management Permissions
- Threat Detection Permissions

APIs Permissions

Application	Platform	Permission	Permission Description	Access	Roles
Application Programming Interfaces	New-Scale	Manage API keys	View and manage API keys.	• Read • Write • Delete	• Administrator • Security Engineer • Developer
Application Programming Interfaces	New-Scale	Manage webhooks	View and manage webhooks.	• Read • Write • Delete	• Administrator • Security Engineer • Developer

Collectors Permissions

Application	Platform	Permission	Permission Description	Access	Roles
Cloud Collectors	New-Scale	Cloud Collectors	View and manage Cloud Collectors.	Read	• Administrator • Security Engineer • Administrator (SaaS Cloud Connectors)
Cloud Collectors	New-Scale	Cloud Collectors	View and manage Cloud Collectors.	• Read • Write • Delete	• Administrator • Security Engineer • Administrator (SaaS Cloud Connectors)
SaaS Cloud Connectors	SaaS	SaaS Cloud Connectors	View and manage SaaS Cloud Connectors	Read	• Administrator • Security Engineer • Administrator (Advanced Analytics) • Administrator (Data Lake) • Administrator (SaaS Cloud Connectors)
SaaS Cloud Connectors	SaaS	SaaS Cloud Connectors	View and manage SaaS Cloud Connectors	• Read • Write • Delete	• Administrator • Security Engineer • Administrator (Advanced Analytics) • Administrator (Data Lake) • Administrator (SaaS Cloud Connectors)
SaaS Site Collectors	SaaS	SaaS Site Collectors manage collectors	Perform all collector operations, such as managing collectors, changing template assignments, and toggling operations in SaaS Site Collectors.	• Read • Write • Delete	Administrator (Data Lake)
Site Collectors	New-Scale	Site Collectors	View and manage Site Collectors' settings.	Read	• Administrator • Security Engineer
Site Collectors	New-Scale	Site Collectors	View and manage Site Collectors' settings.	• Read • Write • Delete	• Administrator • Security Engineer
Site Management	New-Scale	Site Management	View and manage sites.	Read	• Administrator • Security Engineer
Site Management	New-Scale	Site Management	View and manage sites	• Read • Write	• Administrator • Security Engineer

Compliance Permissions

Application	Platform	Permission	Permission Description	Access	Roles
Webhooks	New-Scale	Audit Events Export	Export audit events.	• Read • Write	• Administrator • Security Engineer • Compliance Manager • Administrator (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • Administrator (Data Lake) • Data Privacy Officer (Data Lake) • Administrator (SaaS Cloud Connectors)

Identity and Access Management Permissions

Application	Platform	Permission	Permission Description	Access	Roles
Settings	New-Scale	User, roles, and single sign-on	View and manage users, roles, and single sign-on settings	Read	• Administrator • Security Engineer
Settings	New-Scale	Identity and Access Management	View and manage users and associated roles	Read	• Administrator • Security Engineer
Settings	New-Scale	Identity and Access Management	View and manage users and associated roles	• Read • Write • Delete	• Administrator • Security Engineer
Settings	New-Scale	single sign-on configuration	View and manage single sign-on configurations.	Read	• Administrator • Security Engineer
Settings	New-Scale	single sign-on configuration	View and manage single sign-on configurations.	• Read • Write • Delete	• Administrator • Security Engineer

Investigation and Response Permissions

Application	Platform	Permission	Permission Description	Access	Roles
Advanced Analytics	SaaS	Advanced Analytics add comments	Add comments for entities in Advanced Analytics.	• Read • Write	• Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)

Application	Platform	Permission	Permission Description	Access	Roles
Advanced Analytics	SaaS	Advanced Analytics view unmasked data (PII)	View personally identifiable information (PII) when data masking is enabled in Advanced Analytics.	Read	Data Privacy Officer (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics approve lockouts	Accept account lockout activities for users in Advanced Analytics. Accepting lockouts indicates that the specific set of behaviors are deemed normal and allowed for that user.	• Read • Write	Tier 3 Analyst (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics send incidents to Incident Responder	Send incidents to Incident Responder from Advanced Analytics.	• Read • Write	• Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)
Alert Triage	New-Scale	Alert Rank	View and manage Alert Rank.	Read	• Administrator • Security Engineer • Tier 3 Analyst • Tier 2 Analyst • Tier 1 Analyst
Alert Triage	New-Scale	Alert Triage	View and manage Alert Triage	Read	• Administrator • Security Engineer • Tier 3 Analyst • Tier 2 Analyst • Tier 1 Analyst
Alert Triage	New-Scale	Alert Triage Public Saved Filters	View and manage public saved filters.	• Read • Write • Delete	• Administrator • Security Engineer • Tier 3 Analyst • Tier 1 Analyst

Application	Platform	Permission	Permission Description	Access	Roles
Automation Management	New-Scale	Automation Management playbooks	View and manage playbooks in Automation Management.	Read	• Administrator • Security Engineer • Tier 3 Analyst • Tier 2 Analyst • Tier 1 Analyst • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)
Automation Management	New-Scale	Automation Management playbooks	View and manage playbooks in Automation Management.	• Read • Write • Delete	• Administrator • Security Engineer • Administrator (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)
Case Manager	SaaS	Case Manager read, write, and delete incidents	Edit incidents in Case Manager	• Read • Write	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics)
Case Manager	SaaS	Case Manager bulk edit	Edit multiple incidents at the same time in Case Manager.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Case Manager	SaaS	Case Manager read, write, and delete incidents	View incidents in Case Manager.	Read	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)

Application	Platform	Permission	Permission Description	Access	Roles
Case Manager	SaaS	Case Manager add comments	Add comments in Case Manager.	• Read • Write	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics)
Case Manager	SaaS	Case Manager create incidents	Create incidents in Case Manager.	• Read • Write	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics)
Case Manager	SaaS	Case Manager read, write, and delete incidents	Delete incidents in Case Manager	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Case Manager	SaaS	Case Manager view comments	View case comments in Case Manager.	Read	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)
Case Manager	SaaS	Case Manager view restricted incidents	View incidents restricted to other users or groups in Case Manager.	Read	• Administrator (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)

Application	Platform	Permission	Permission Description	Access	Roles
Dashboards	New-Scale	Dashboards Case Management	View and manage Case Management Dashboards.	Read	• Administrator • Tier 3 Analyst • Tier 2 Analyst • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)
Dashboards	New-Scale	Dashboards Case Management	View and manage Case Management Dashboards.	• Read • Write • Delete	• Administrator • Tier 3 Analyst • Tier 2 Analyst • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)
Incident Responder	SaaS	Incident Responder run playbooks	Run playbooks from the workbench in Incident Responder.	• Read • Write	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics)
Incident Responder	SaaS	Incident Responder run actions	Launch individual actions from the user interface in Incident Responder.	• Read • Write	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics)

Application	Platform	Permission	Permission Description	Access	Roles
Threat Center	New-Scale	Threat Center alerts	View and manage alerts in Threat Center.	Read	• Administrator • Security Engineer • Tier 3 Analyst • Tier 2 Analyst • Tier 1 Analyst • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)
Threat Center	New-Scale	Threat Center alerts	View and manage alerts in Threat Center.	• Read • Write • Delete	• Administrator • Tier 3 Analyst • Tier 2 Analyst • Tier 1 Analyst • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)
Threat Center	New-Scale	Threat Center cases	View and manage cases in Threat Center.	Read	• Administrator • Security Engineer • Tier 3 Analyst • Tier 2 Analyst • Tier 1 Analyst • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)

Application	Platform	Permission	Permission Description	Access	Roles
Threat Center	New-Scale	Threat Center cases	View and manage cases in Threat Center.	• Read • Write • Delete	• Administrator • Security Engineer • Tier 3 Analyst • Tier 2 Analyst • Tier 1 Analyst • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)
Threat Center	New-Scale	Threat Center detection grouping rules	View and manage detection grouping rules in Threat Center.	Read	• Administrator • Security Engineer • Tier 3 Analyst • Tier 2 Analyst • Tier 1 Analyst • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)
Threat Center	New-Scale	Threat Center detection grouping rules	Manage detection grouping rules in Threat Center.	• Read • Write • Delete	• Administrator • Security Engineer • Administrator (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)

Log Stream Permissions

Application	Platform	Permission	Permission Description	Access	Roles
Log Stream	New-Scale	Log Stream	View or manage parsers, parser updates, enrichment, and event filtering and routing	• Read • Write • Detele	• Administrator • Security Engineer
Log Stream	New-Scale	Log Stream	View or manage parsers, parser updates, enrichment, and event filtering and routing	• Read	Tier 3 Analyst

Platform Insights Permissions

Application	Platform	Permission	Permission Description	Access	Roles
Advanced Analytics	SaaS	Advanced Analytics view health	Advanced Analytics view system health.	Read	Administrator (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics view trends	View overall trends with Advanced Analytics.	Read	• Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)
Notifications	New-Scale	Configure global notification channels	View and manage global notification channels for your organization.	• Read • Write • Delete	• Administrator • Security Engineer
Notifications	New-Scale	Manage security notifications	View and manage security notifications for your profile.	• Read • Write • Delete	• Administrator • Tier 3 Analyst • Tier 2 Analyst • Tier 1 Analyst • Compliance Manager
Notifications	New-Scale	Manage health notifications	View and manage health notifications for your profile.	• Read • Write • Delete	• Administrator • Security Engineer
Notifications	New-Scale	Manage consumption notifications	View and manage consumption notifications for your profile.	• Read • Write • Delete	• Administrator • Security Engineer
Notifications	New-Scale	Manage thirdparty-access	View and manage third-party access notifications for your profile.	• Read • Write • Delete	Administrator
Outcomes Navigator	New-Scale	Outcomes Navigator	View Outcomes Navigator.	Read	• Administrator • Security Engineer

Security Management Permissions

Application	Platform	Permission	Permission Description	Access	Roles
Action Editor	New-Scale	Actions Editor	View and manage custom actions.	Read	• Administrator • Security Engineer • Tier 3 Analyst

Application	Platform	Permission	Permission Description	Access	Roles
Advanced Analytics	SaaS	Advanced Analytics manage content packages	View and manage content packages for automatic installation in Advanced Analytics.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Administrator (Data Lake)
Advanced Analytics	SaaS	Advanced Analytics administrative operations	Perform all administrative operations in Advanced Analytics.	• Read • Write • Delete	Administrator (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics manage watchlists	Add and remove users from the watchlists in Advanced Analytics.	• Read • Write • Delete	• Tier 3 Analyst (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics view rules	View rules that determine how security events are handled in Advanced Analytics.	Read	• Security Engineer • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics manage data ingestion	Configure log sources, feeds, and email ingestion in Advanced Analytics.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Advanced Analytics	SaaS	Event Selection streams	View or modify streams in Advanced Analytics with Event Selection.	• Read • Write • Delete	• Administrator • Security Engineer
Advanced Analytics	SaaS	Event Selection streams	View or modify streams in Advanced Analytics with Event Selection.	Read	Administrator
Auto Parser Generator	New-Scale	Manage Auto Parser Generator	View and manage SaaS parsers in Auto Parser Generator.	Read	• Administrator • Security Engineer
Case Manager	SaaS	Case Manager manage queues	View and manage membership to queues in Case Manager.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Case Manager	SaaS	Case Manager manage incident rules	View and manage rules for how incidents are assigned, restricted, and prioritized on ingestion in Case Manager.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)

Application	Platform	Permission	Permission Description	Access	Roles
Case Manager	SaaS	Case Manager manage rules	View and manage rules that determine how security events are handled in Case Manager.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Case Manager	SaaS	Case Manager manage incident configuration	View and manage incident configurations including incident types, fields, layouts, case notifications, and checklists in Case Manager.	• Read • Write • Delete	Administrator (Advanced Analytics)
Case Manager	SaaS	Case Manager manage bi-directional Communication	Configure inbound and outbound settings for bidirectional communications in Case Manager.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Case Manager	SaaS	Case Manager delete entities and artifacts	Delete entities and artifacts in Case Manager.	• Read • Write • Delete	
Case Manager	SaaS	Case Manager manage checklist definitions	Configure checklist definitions in Case Manager.	• Read • Write • Delete	
Case Manager	SaaS	Case Manager manage incident definitions	View and manage incident definitions in Case Manager.	• Read • Write • Delete	
Context Management	New-Scale	Context Management	View and manage Context Management configuration.	• Read • Write • Delete	• Administrator • Security Engineer
Context Management	New-Scale	Context Management	View and manage Context Management configuration.	Read	• Administrator • Security Engineer

Application	Platform	Permission	Permission Description	Access	Roles
Correlation Rules	New-Scale	Correlation Rules	View and manage correlation rules.	Read	• Administrator • Security Engineer • Tier 3 Analyst • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics) • Administrator (Data Lake) • Tier 3 Analyst (Data Lake) • Tier 1 Analyst (Data Lake) • Auditor (Data Lake) • Data Privacy Officer (Data Lake) • CloudOpsMonitoring (Data Lake) • Administrator (SaaS Cloud Connectors)
Correlation Rules	New-Scale	Correlation Rules	View and manage correlation rules.	• Read • Write • Delete	• Administrator • Security Engineer • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Administrator (Data Lake) • Tier 3 Analyst (Data Lake)
Data Lake	SaaS	Data Lake manage indices	Re-parse and re-index the logs of indices in Data Lake	• Read • Write • Delete	Administrator (Data Lake)

Application	Platform	Permission	Permission Description	Access	Roles
Data Lake	SaaS	Data Lake manage correlation rules	View and manage correlation rules in Data Lake.	• Read • Write • Delete	Administrator (Data Lake)
Data Lake	SaaS	Data Lake manage data access	View and manage data access rules in Data Lake	• Read • Write • Delete	Administrator (Data Lake)
Data Lake	SaaS	Data Lake view saved objects	View saved searches, visualizations, dashboards, and reports in Data Lake.	Read	• Administrator (Data Lake) • Tier 3 Analyst (Data Lake) • Tier 1 Analyst (Data Lake) • Auditor (Data Lake) • Data Privacy Officer (Data Lake) • CloudOpsMonitoring (Data Lake)
Data Lake	SaaS	Data Lake manage saved objects	View and manage saved searches, visualizations, dashboards, and reports in Data Lake.	• Read • Write • Delete	• Administrator (Data Lake) • Tier 3 Analyst (Data Lake) • Tier 1 Analyst (Data Lake) • Auditor (Data Lake) • Data Privacy Officer (Data Lake) • CloudOpsMonitoring (Data Lake)
Data Lake	SaaS	Data Lake manage Kafka Connect	View and manage connectors in Kafka Connect in Data Lake.	• Read • Write • Delete	Administrator (Data Lake)
Data Lake	SaaS	Data Lake manage cross-cluster connection	Add and edit the connection to remote clusters in Data Lake.	• Read • Write • Delete	Administrator (Data Lake)
Entity Management	New-Scale	Attack Surface Insights	View and manage Attack Surface Insights.	Read	• Administrator • Security Engineer • Tier 3 Analyst • Administrator (SaaS Cloud Connectors)
Entity Management	New-Scale	Attack Surface Insights	View and manage Attack Surface Insights.	• Read • Write • Delete	Administrator

Application	Platform	Permission	Permission Description	Access	Roles
Incident Responder	SaaS	Incident Responder reset incident workbench	Reset incident workbench	• Read • Write	• Security Engineer • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Incident Responder	SaaS	Incident Responder manage playbooks	Manage playbooks in Incident Responder.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Incident Responder	SaaS	Incident Responder manage services	View and manage services (third-party integrations) in Incident Responder.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Incident Responder	SaaS	Incident Responder manage playbook templates.	View and manage playbook templates	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Incident Responder	SaaS	Incident Responder manage triggers	View and manage playbook triggers in Incident Responder.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Incident Responder	SaaS	Incident Responder manage custom services and packages	Manage custom services and related packages in Incident Responder.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)

Application	Platform	Permission	Permission Description	Access	Roles
Log Stream	New-Scale	Manage Log Stream Parsers	View and manage parsers, parser updates, view live parsed events, and re-parsing jobs in Log Stream. **NOTE** This permission will be deprecated in a future release (not yet scheduled) in favor of two new permissions in a dedicated Log Stream category. In the meantime, do not assign this permission to any new or updated user roles.	• Read • Write • Delete	• Administrator • Security Engineer
SaaS Context Collectors	SaaS	SaaS context tables manage users and context sources	View and manage users, roles, and context sources for decision support in SaaS.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Administrator (Data Lake)
SaaS context tables	SaaS	SaaS manage context tables	View and manage entities and other objects in SaaS context tables.	• Read • Write • Delete	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Administrator (Data Lake) • Tier 3 Analyst (Data Lake)
Search	New-Scale	Secured Resources	View and manage Secured Resources.	• Read • Write • Delete	• Administrator • Security Engineer
Search	New-Scale	Secured Resources	View and manage Secured Resources.	Read	• Administrator • Security Engineer

Application	Platform	Permission	Permission Description	Access	Roles
Search	New-Scale	Manage data retention settings	View and manage data retention.	• Read • Write • Delete	• Administrator • Security Engineer
Settings	New-Scale	Manage Administrative Settings	View and manage administrative settings.	Read	• Administrator • Security Engineer • Developer
Settings	New-Scale	Manage Administrative Settings	View and manage administrative settings.	• Read • Write • Delete	• Administrator • Security Engineer • Developer
Threat Detection Management	New-Scale	Analytics Rules	View or manage Analytics Rules.	Read	• Administrator • Security Engineer • Tier 3 Analyst
Threat Detection Management	New-Scale	Analytics Rules	View or manage Analytics Rules.	• Read • Write • Delete	• Administrator • Security Engineer
Threat Detection Management	New-Scale	Universal Prioritization	View or manage Universal Prioritization.	Read	• Administrator • Security Engineer • Tier 3 Analyst
Threat Detection Management	New-Scale	Universal Prioritization	View or manage Universal Prioritization.	• Read • Write • Delete	• Administrator • Security Engineer

Threat Detection Permissions

Application	Platform	Permission	Permission Description	Access	Roles
Advanced Analytics	SaaS	Advanced Analytics threat hunter search incidents	Perform basic threat hunter incident searches in Advanced Analytics. Basic threat hunter incident search allows one to search for an incident and associated details.	Read	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics manage threat hunter search library	View and manage threat hunter saved searches in Advanced Analytics.	• Read • Write • Delete	• Tier 3 Analyst (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)

Application	Platform	Permission	Permission Description	Access	Roles
Advanced Analytics	SaaS	Advanced Analytics view executive info	View the risk reasons and timeline of the executive users in the organization. You will be able to see the activities performed by executive users along with the associated anomalies.	Read	• Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics view global insights	View the organizational models and histograms showing normal behavior for users and assets in Advanced Analytics.	Read	• Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics threat hunting	Perform threat hunting in Advanced Analytics.	Read	• Tier 3 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics view data insights	View the normal behaviors for specific users and assets in Advanced Analytics.	Read	• Tier 2 Analyst • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)

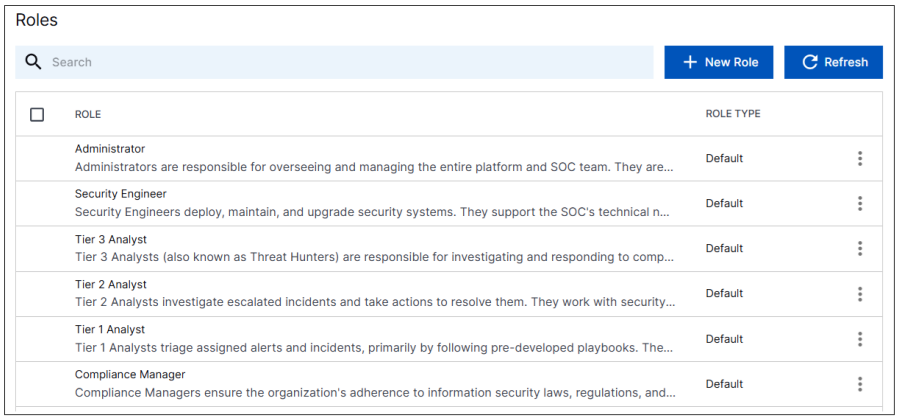
Application	Platform	Permission	Permission Description	Access	Roles
Advanced Analytics	SaaS	Advanced Analytics view threat hunter search library	View the Threat Hunter Search Library and the corresponding search results in Advanced Analytics.	Read	• Tier 2 Analyst • Tier 3 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics manage threat hunter public searches	View and manage saved threat hunter public searches.	• Read • Write • Delete	Tier 3 Analyst (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics view notable activities	View all notable users, assets, sessions, and related risk reasons in Advanced Analytics.	Read	• Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics view raw logs	View the raw logs that are used to build the events in the Advanced Analytics timeline.	Read	• Tier 2 Analyst • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics threat hunter search	Perform basic threat hunter searches in Advanced Analytics. Basic threat hunter incident search allows one to search for a specific user, asset, session, or a security alert.	Read	• Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)
Advanced Analytics	SaaS	Advanced Analytics accept sessions	Allow a user to accept an Advanced Analytics session.	• Read • Write	• Tier 3 Analyst (Advanced Analytics) • Data Privacy Officer (Advanced Analytics)

Application	Platform	Permission	Permission Description	Access	Roles
Dashboards	New-Scale	Dashboards	View and manage dashboards.	Read	• Administrator • Security Engineer • Tier 3 Analyst • Tier 2 Analyst • Tier 1 Analyst • Compliance Manager
Dashboards	New-Scale	Dashboards	View and manage dashboards.	• Read • Write • Delete	• Administrator • Security Engineer • Tier 3 Analyst • Tier 2 Analyst
Dashboards	New-Scale	Manage All Scheduled Reports	View, edit, and delete scheduled reports created by any user	• Read • Write • Delete	• Administrator • Administrator (Advanced Analytics) • Administrator (Data Lake) • Administrator (SaaS Cloud Collectors)
Dashboards	New-Scale	Dashboards Anomalies	View and manage Anomalies Dashboards.	Read	• Administrator • Tier 3 Analyst • Tier 2 Analyst • Tier 1 Analyst • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Tier 1 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)
Dashboards	New-Scale	Dashboards Anomalies	View and manage Anomalies Dashboards.	• Read • Write • Delete	• Administrator • Tier 3 Analyst • Administrator (Advanced Analytics) • Tier 3 Analyst (Advanced Analytics) • Auditor (Advanced Analytics) • Data Privacy Officer (Advanced Analytics) • CloudOpsMonitoring (Advanced Analytics)

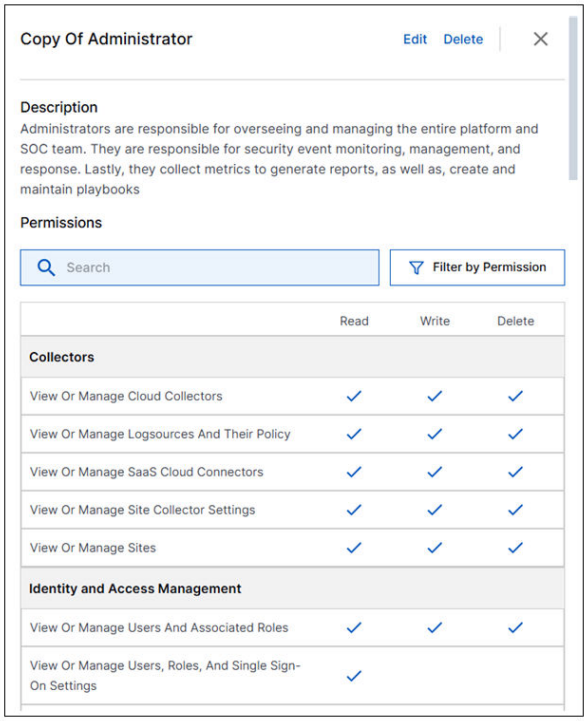
Application	Platform	Permission	Permission Description	Access	Roles
Dashboards	New-Scale	Dashboards Data Lake	View and manage Data Lake Dashboards.	Read	• Administrator • Tier 3 Analyst • Tier 2 Analyst • Administrator (Data Lake) • Tier 3 Analyst (Data Lake) • Tier 1 Analyst (Data Lake) • Auditor (Data Lake) • Data Privacy Officer (Data Lake) • CloudOpsMonitoring (Data Lake)
Dashboards	New-Scale	Dashboards Data Lake	View and manage Data Lake Dashboards.	• Read • Write • Delete	• Administrator • Tier 3 Analyst • Administrator (Data Lake) • Tier 3 Analyst (Data Lake) • Auditor (Data Lake) • Data Privacy Officer (Data Lake) • CloudOpsMonitoring (Data Lake)
Data Lake	SaaS	Data Lake run Elasticsearch Searches	Perform Elasticsearch search requests in Data Lake.	Read	Administrator (Data Lake)
Search	New-Scale	Search, Analyze and Export	Search, analyze, and export logs, alerts, and events.	Read	• Administrator • Tier 3 Analyst • Tier 2 Analyst • Compliance Manager

View Permissions in a User Role

1. Log in to the New-Scale Security Operations Platform.
2. At the bottom of the navigation panel on the left, click **Settings** (⚙), and then select **Roles**. The list of roles is displayed.



3. Scroll through the list of roles to locate the role whose permissions you want to view.
4. To the right of the role, click the **Options** menu (⋮) and select **View**. A panel opens on the right and displays the permissions granted to the selected role.



You can interact with the user role in the following ways:

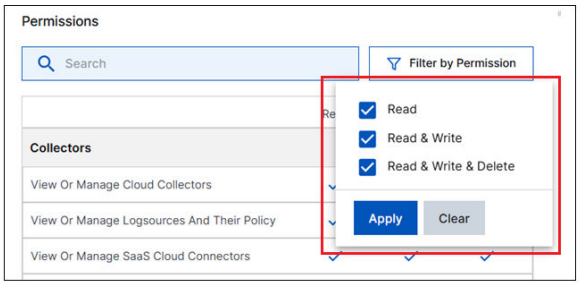
- **Edit** – Click to open the **Edit Role** dialog box where you can modify the permissions granted to the role.

> **NOTE**
> This option is only available for custom roles. Default roles cannot be edited. You can however duplicate a default role and then edit the copy.

- **Delete** – Click to open a **Delete Role** dialog box where you will be prompted to confirm the deletion.

> **NOTE**
> This option is only available for custom roles. Default roles cannot be deleted.

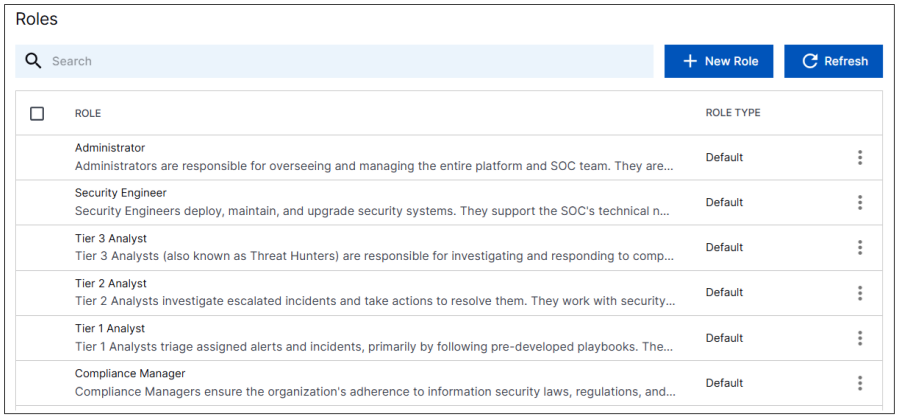
- **Search** – Enter a term to search for a specific permission in the list.
- **Filter by Permissions** – Click to select the type of permissions you want to view in the panel. Options include **Read**, **Read & Write**, or **Read & Write & Delete**. After you select the permission types, click **Apply**. The list in the panel will change according to your selections. Click **Clear** to remove the selections.



5. To close the permissions panel, click the close icon (×) in the upper right corner. The panel closes and the list of user roles is redisplayed.

Create a Custom User Role

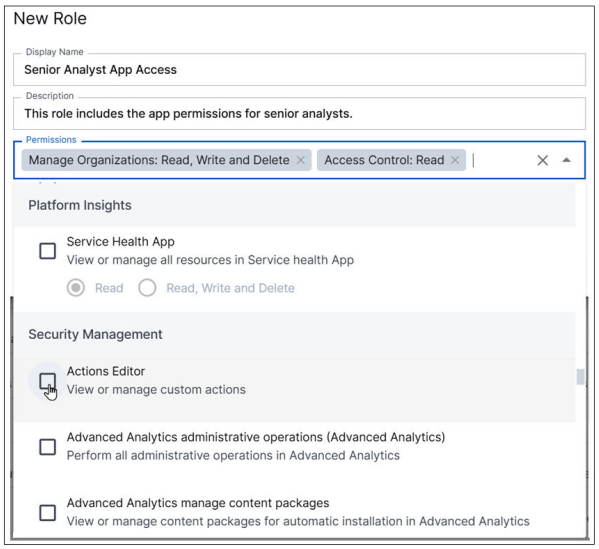
1. Log in to the New-Scale Security Operations Platform.
2. At the bottom of the navigation panel on the left, click **Settings** (⚙), and then select **Roles**. The list of roles is displayed.



3. On the upper-right side of the page, click **New Role**. The **New Role** dialog box opens.



4. In the **Display Name** field, enter a descriptive name for the role.
5. In the **Description** field, define the intended purpose or use of the role.
6. From the **Permissions** drop-down menu, select the permissions that you want to assign to the role.

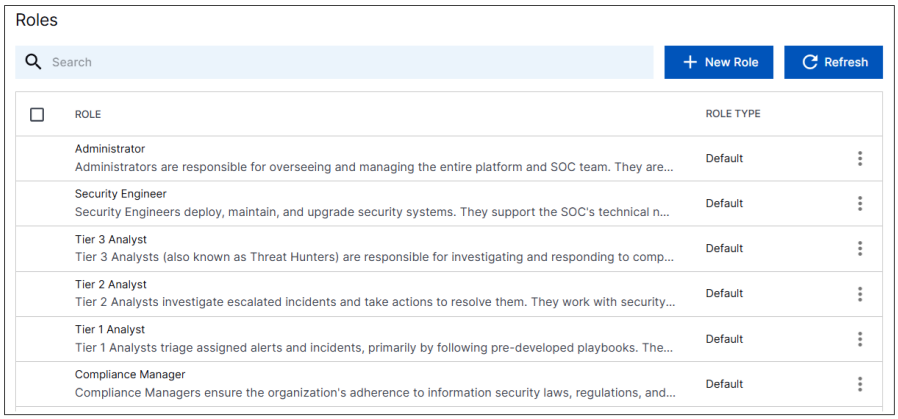


7. When you have selected all the permissions that you want to include, click outside the drop-down menu, and then click **Create**.
   The new role is added to the list on the **Roles** page.
8. Assign the role to to your users, as desired.

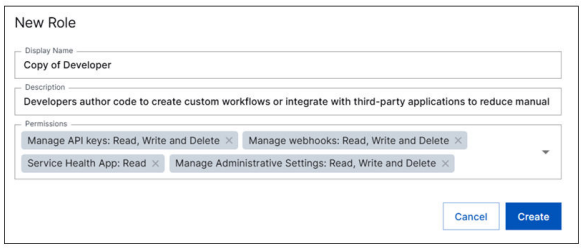
Duplicate, Edit, or Delete User Roles

NOTE
Default roles cannot be modified or deleted. You can however duplicate a default role and then modify it.

1. Log in to the New-Scale Security Operations Platform.
2. On the lower-left side of the user interface, click **Settings** (⚙), and then click **Roles**. The list of roles is displayed.

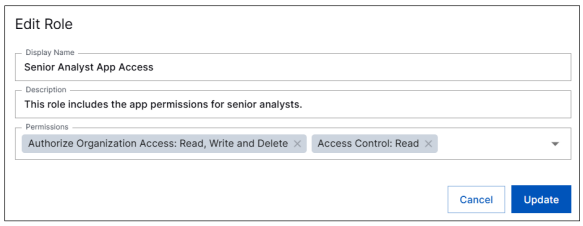


3. To the right of the role, click the **Options** menu (⋮) and select one of the following options:
   - **Duplicate** – A **New Role** dialog box opens with the permissions of the existing role listed. The **Display Name** is automatically appended with "Copy of" but you can modify the role name, description, and the list of permissions it includes. When you complete your modifications, click **Create** and the new role is added to the list on the **Roles** page.



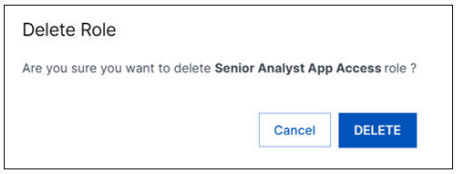
   - **Edit** – An **Edit Role** dialog box opens with the permissions of the selected role listed. You can edit the role name, description, and the list of permissions it includes. When you complete you modifications, click **Update** and the existing role is updated with your changes.

> **NOTE**
> This option is available only for custom user roles. You cannot edit a default role unless you duplicate it first.



   - **Delete** – A **Delete Role** dialog box opens and prompts you to confirm that you want to delete the existing role. Click **Delete** and the role is removed from the list on the **Roles** page.

> **NOTE**
> This option is available only for custom user roles. You cannot delete a default role.



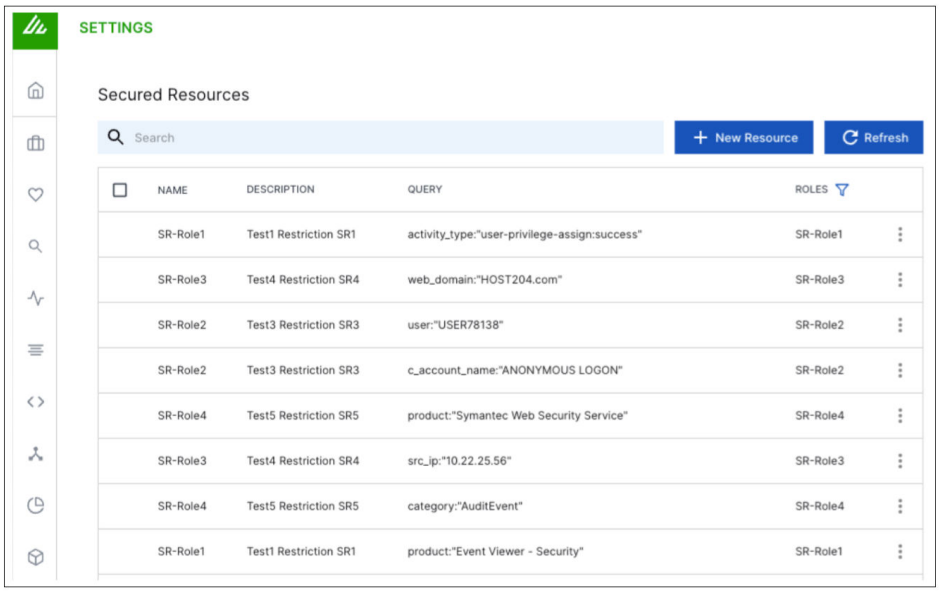
Secured Resources

The Secured Resources feature enables you to tailor data visibility to suit the needs of the different Exabeam user roles in your organization. In other words, you can enhance security and enforce data governance policies by allowing users to access only the data that they need to perform their jobs.

> **NOTE**
> Secured Resources works by limiting data access in user roles as opposed to allowing access. As such, user roles with no secured resources assigned to them will have unlimited data access.

When you add a secured resource, you create a query to filter the data that users see. For example, if you want to have a team that focuses only on Cisco and IBM events involving the `alert-trigger` activity type, you would define the resource as `vendor:("Cisco","IBM") AND activity_type:"alert-trigger"`.

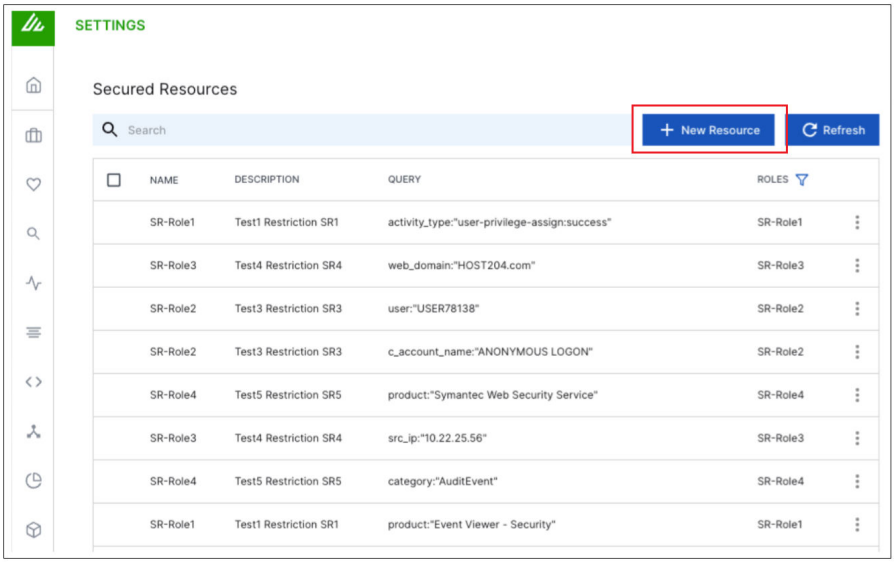
Secured Resources can be added to user roles that are attached to any of the following products: Search, Dashboards, and Threat Center.



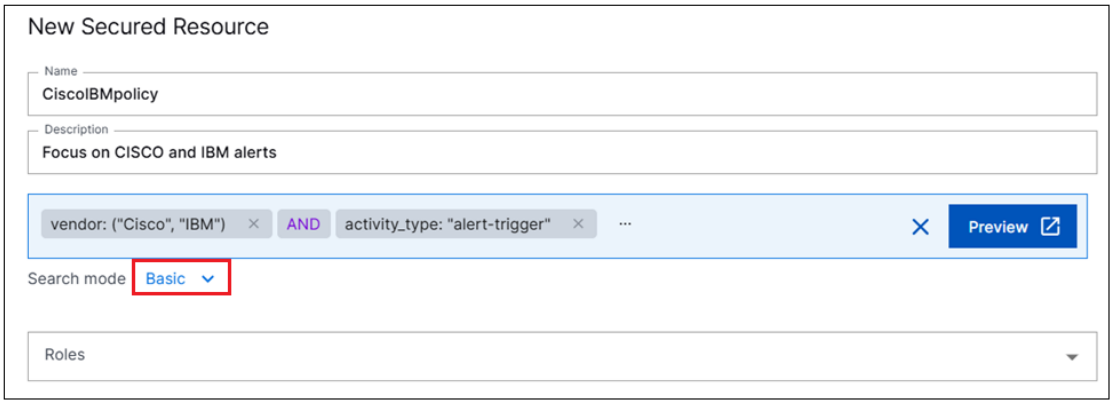
Add a Secured Resource

> **NOTE**
> To manage secure resources, you need to be an Administrator with full access to your organization's Exabeam subscription.

1. Log in to the New-Scale Security Operations Platform.
2. On the lower-left side of the page, click the settings icon, and then select **Secured Resources**.
   The **Secured Resources** page opens and displays a list of the existing secured resources in your environment.
3. Click the **New Resource** button.



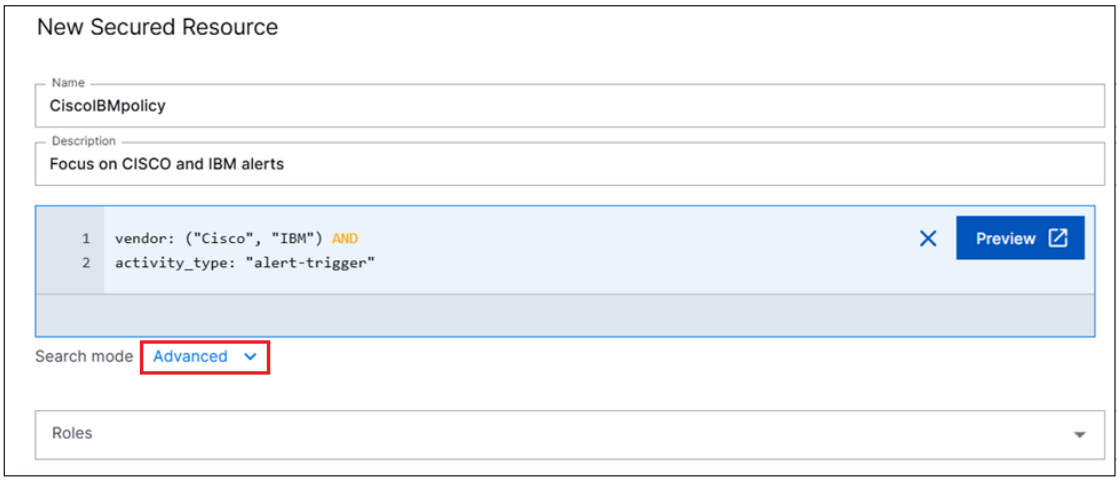
   The **New Secured Resource** page opens.
4. Enter a **Name** for the resource.
5. Enter a **Description** of the resource.
6. Build a query to define the the type of events users with this resource will be able to access. To build the query, select one of the following **Search mode** options:
   - **Basic** – In the Basic search mode, you can select search terms and fields from prebuilt lists to build a query. The pre-built lists include subjects, vendors, products, common fields that are part of the Exabeam common information model, and any metadata, anomaly, audit log, and custom fields that are used in your environment.
     For information about how to use the Basic search mode to build queries, see Basic Search in the *Search Guide*.



> **NOTE**
> Basic query building for secured resources does not support entity fields. However, you can enumerate the entity-related fields in a query to achieve the same affect. For example you can add both the username and email fields to the query.

- **Advanced** – In the Advanced search mode, you can construct your own queries using Exabeam Query Language (EQL) syntax and operators. The Advanced search mode includes several features to facilitate ease of use and readability when creating complex queries:
  - White space characters (such as spaces, tabs, and line breaks) can be used between query syntax terms.
  - Line numbering is displayed for queries that are formatted on multiple lines.
  - Color-coding is used to make syntax elements recognizable.
  - Warnings and syntax validation errors are displayed per line.

  For information about how to build queries using the Advanced search mode, and for detailed EQL syntax and operator information, see Advanced Search in the *Search Guide*.

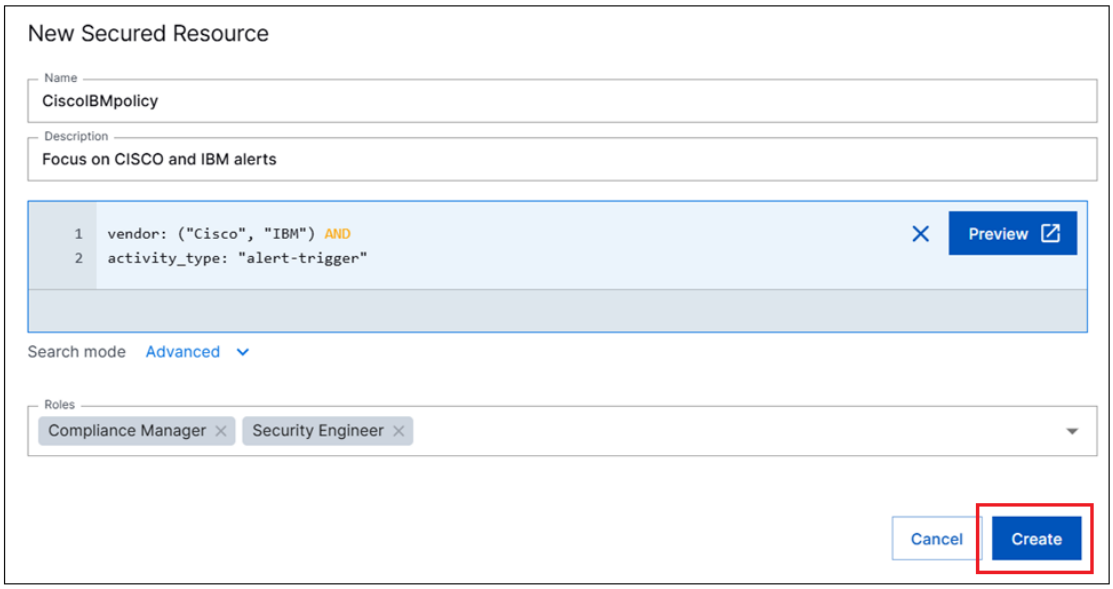


> **NOTE**
> Advanced mode query building for secured resources does not support the following specific EQL functionality:
>
> - SELECT, GROUP-BY, and LIMIT clauses
> - Pipe Operators
> - Entity fields – Instead, you can enumerate the entity-related fields in a query to achieve the same affect. For example you can add both the username and email fields to the query.

7. As an optional step, click the **Preview** button to verify that the query you constructed yields the intended results. You may need to expand the default time range for the query in Search.

Exabeam Search opens in a new browser tab and displays the query results. Run the query to ensure it returns the results you want.

8. From the **Roles** drop-down menu, select the user roles that you want assigned to this secured resource.
9. Click **Create** in the bottom right corner of the **New Secured Resource** page.



The new resource is added to the list on the **Secured Resources** page.

> **NOTE**
> For users who are logged into one of the affected products (Search, Dashboards, and Threat Center), the new data restrictions will not take effect until they clear their cookies or the cookies expire.

Edit or Delete a Secured Resource

> **NOTE**
> To manage secure resources, you need to be an Administrator with full access to your organization's Exabeam subscription.

1. Log in to the New-Scale Security Operations Platform.
2. On the lower-left side of the page, click the settings icon, and then select **Secured Resources**.
   The **Secured Resources** page opens and displays a list of the existing secured resources in your environment.
3. Find the secured resource you want to edit or delete and click the **Options** icon.
4. Do one of the following:

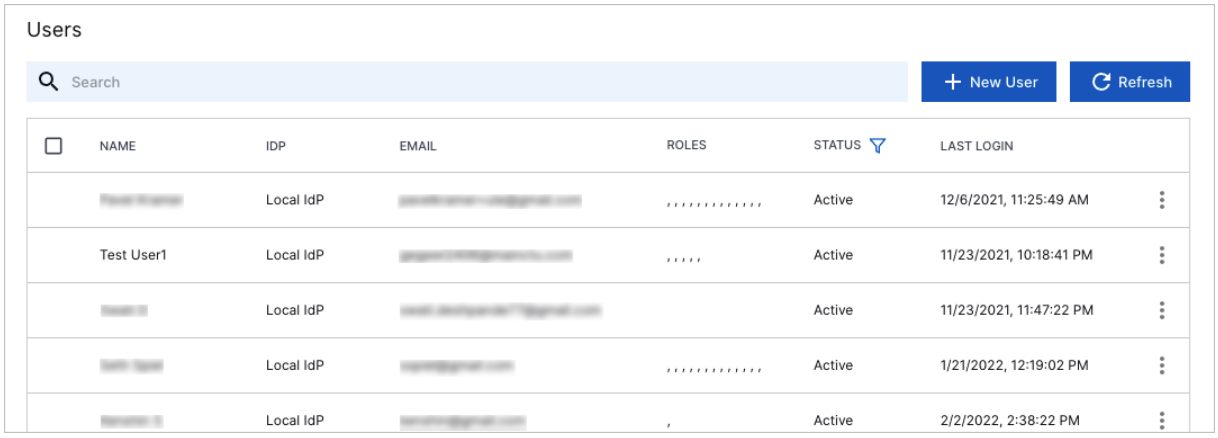
- To edit the resource, select **Edit**. The **Edit Secured Resource** page opens. Edit the resource definition as needed and click **Update**.
- To delete the resource, select **Delete**. When prompted, click **Delete** to confirm the action.

Local Users

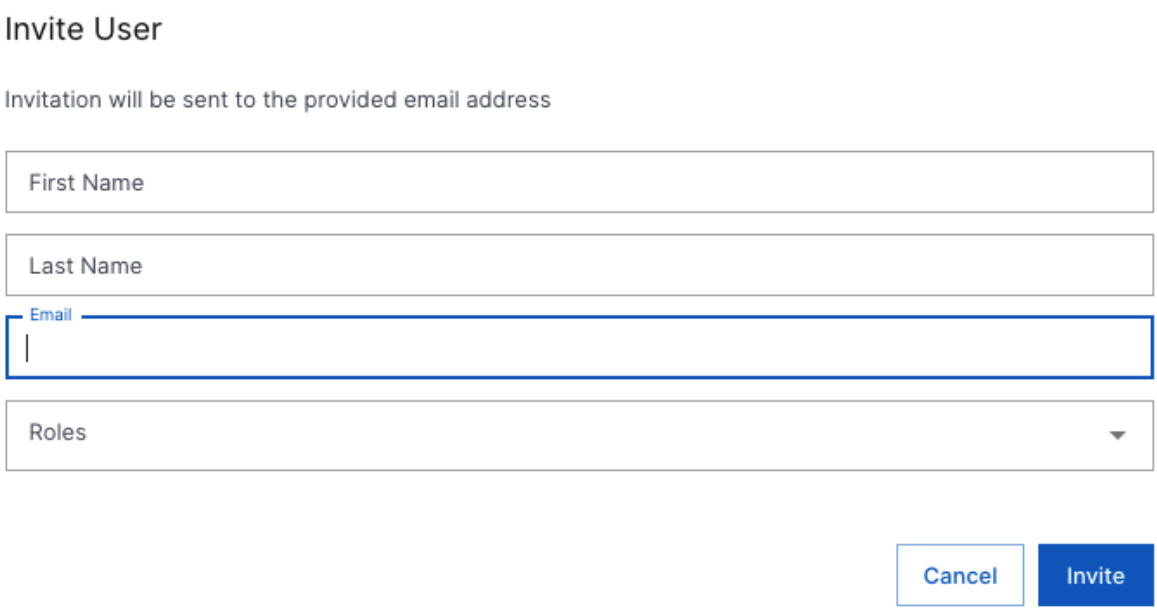
Local user accounts are created and managed within the New-Scale Security Operations Platform. To create a local account, you must have a unique user email address. When a new account is created, the user receives an email to activate the account and create a login password. As an alternative to local authentication, you can also set up single sign-on to use any preferred Third-Party Identity Providers.

Add New Local Users

1. On the lower-left side of the page, click **Settings** ⚙, and then click **Users**.



2. Click **+ New User**.

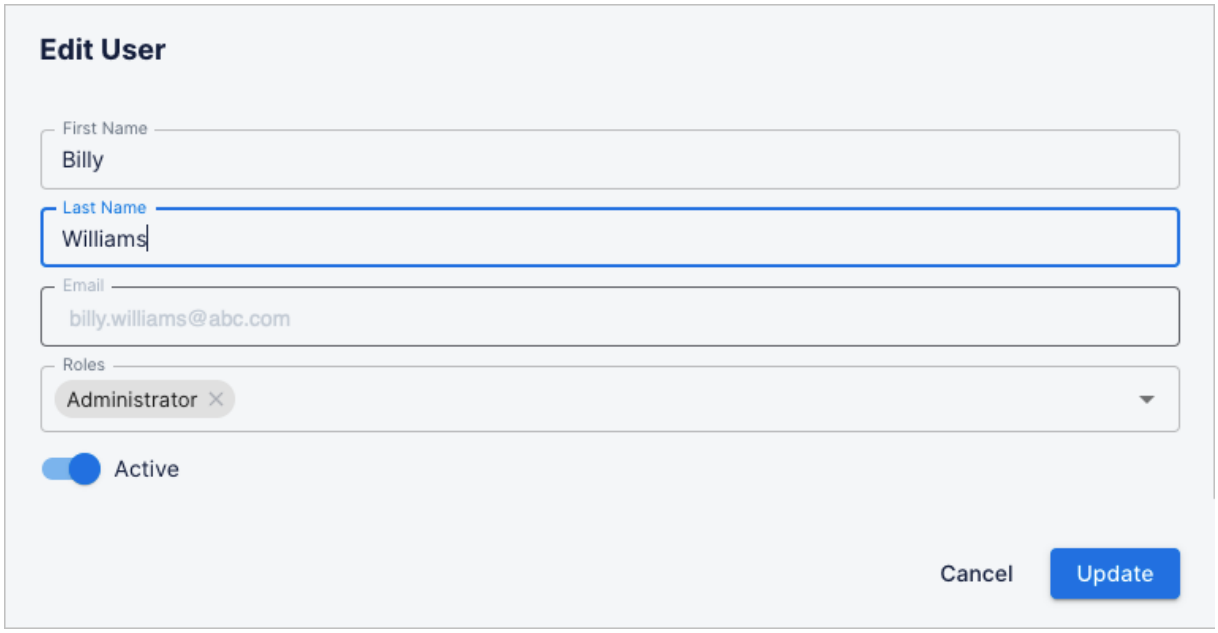


3. Enter the user's **First Name**, **Last Name**, and **Email** address, and then select one or more default or custom **Roles** for the user from the drop-down list.
4. Click **Invite**.
   An email is sent to the user with a link to confirm the account and create a login password. The account status is listed as *Pending* until the user confirms the account, at which time the status changes to *Active*.

Edit Account Details for Local Users

From the Users page in the New-Scale Security Operations Platform, you can edit account information for local users including names, email addresses, and roles.

1. Log in to the New-Scale Security Operations Platform.
2. On the lower-left side of the user interface, click **Settings**, and then click **Users**.
3. For the user that you want to edit, click the More Menu icon on the right, and then click **Edit**.



4. Edit the user's name, email address, and roles as needed.
5. Then click **Update**.

Activate or Deactivate a Local User Account

From the Users page in the New-Scale Security Operations Platform, you can activate and deactivate user accounts.

1. Log in to the New-Scale Security Operations Platform.
2. On the lower-left side of the user interface, click **Settings**, and then click **Users**.
3. For the user whose account you want to activate or deactivate, click the more actions icon on the right, and then click **Edit**.
   The Edit User dialog box appears.
4. Click the **Active** toggle to activate or deactivate the user's account.
   A blue toggle indicates an active account; a gray toggle indicates a deactivated account.



Reset the Password for a Local User Account

From the Users page in the New-Scale Security Operations Platform, you can reset the password for a local user account. When you reset the password it will send an email to the address associated with the account containing instructions to reset the password.

1. Log in to the New-Scale Security Operations Platform.
2. On the lower-left side of the user interface, click **Settings**, and then click **Users**.
3. For the user whose account you want to activate or deactivate, click the more actions icon on the right, and then click **Edit**.
   The Edit User dialog box appears.
4. For the user whose password you want to reset, click the more actions icon on the right, and then click **Reset Password**.
   The Reset Password confirmation box appears.



5. Click **Send**.
   An email containing a password reset link is sent to the user.

Third-Party Identity Providers

The New-Scale Security Operations Platform supports integration with SAML 2.0 compliant third-party identity providers (IdPs) for single sign-on (SSO), multi-factor authentication, and access control. You can integrate more than one IdP provided that the IdPs do not use the same email domains.

The following is a list of IdP providers that are known to support the SAML protocol. Exabeam may also support additional providers that are not included in the list.

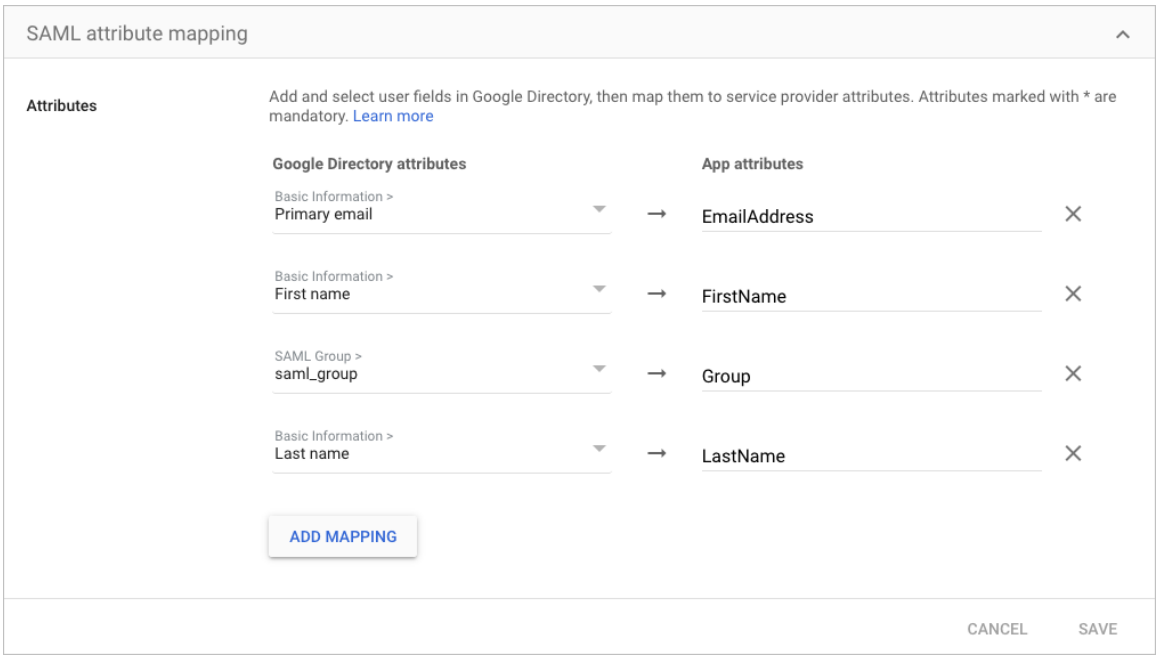
- CyberArk
- ForgeRock
- Google
- IBM
- Microsoft
- Okta
- OneLogin
- Oracle
- Ping Identity
- SecureAuth

Add a Third-Party Identity Provider

> **NOTE**
> To complete this procedure, you need administrative access to both Exabeam and your identity provider (IdP).

1. Log in to your IdP and perform the initial configuration steps for adding Exabeam:
   a. Begin the procedure to add a new application in your IdP for Exabeam (if needed, refer to your IdP's user guide for instructions).
   b. In the attribute mapping section, enter descriptive values for the IdP user attributes. You need to provide values for the following user attributes:
      - Email address
      - First name
      - Last name
      - Group
      - Username (this attribute is optional)

      For example, if **Primary email** is the user email attribute in your IdP, you could enter **`EmailAddress`** as the descriptive value. The following is an example of an attribute map in Google IdP:



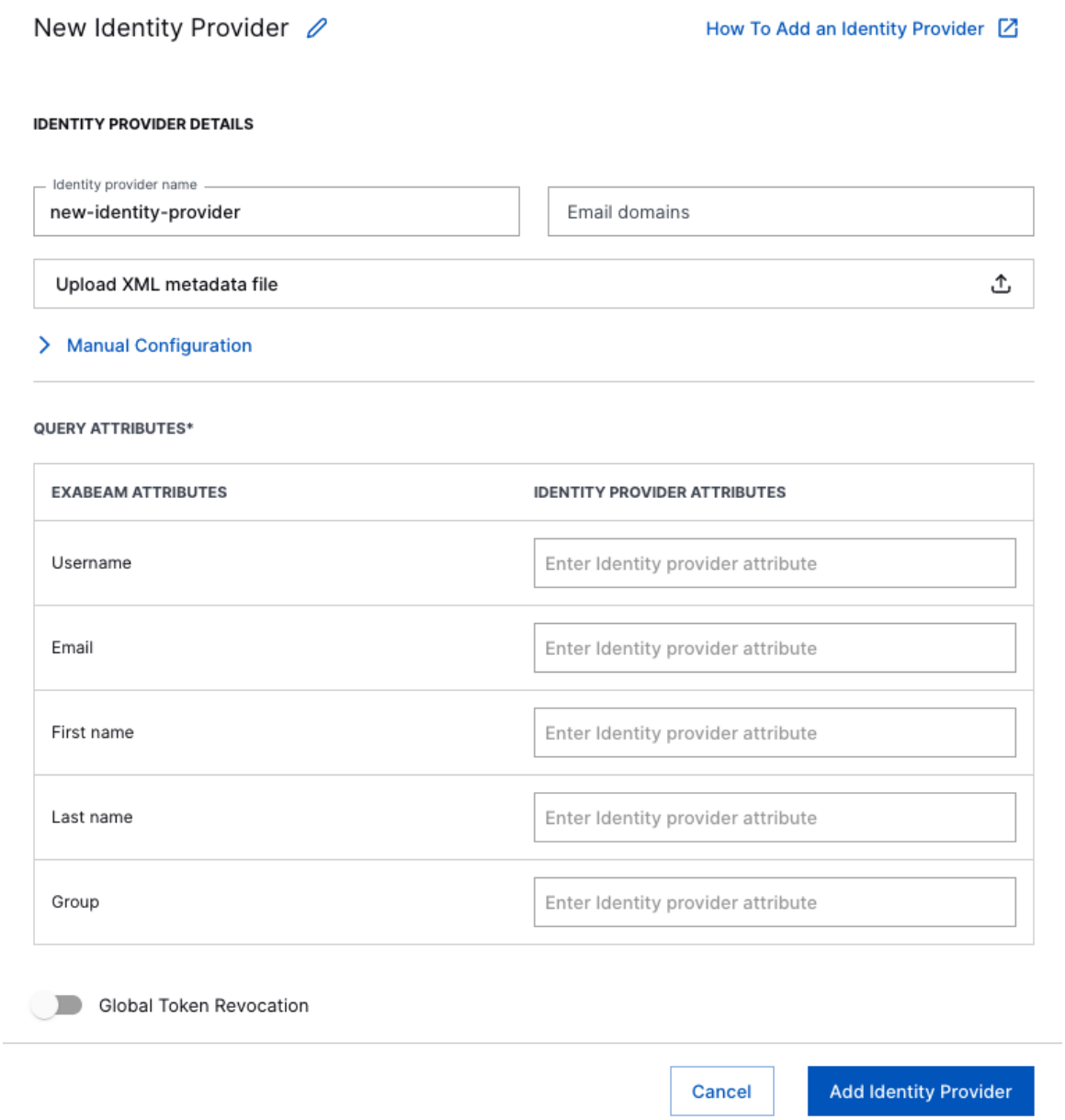
> **IMPORTANT**
> You will use the same descriptive values to map the Exabeam query attributes with corresponding IdP user attributes.

   c. Do one of the following:

- Download the IdP metadata file. (Preferred)
- Copy the *Entity ID* and *Login URL* (sometimes referred to as the "SSO URL"), and then download the *SAML certificate* (the exact names of these items may vary between IdPs).

> **NOTE**
> The information obtained in this step needs to be entered into Exabeam.

2. Log in to the New-Scale Security Operations Platform and do the following:
   a. On the lower-left side of the page, click **Settings**, and then click **Single sign-on**. The Single Sign-On (SSO) page opens.
   b. On the upper-right side of the page, click **Add new provider**.



c. In the **Identity provider name** box, enter a name for the IdP.

d. In the **Email domains** box, enter any user email domains in the IdP (example: *exabeam.com*).

> **IMPORTANT**
> The email domains must be unique. They cannot be the same as the domains used in another IdP or by local user accounts.

e. Do one of the following:

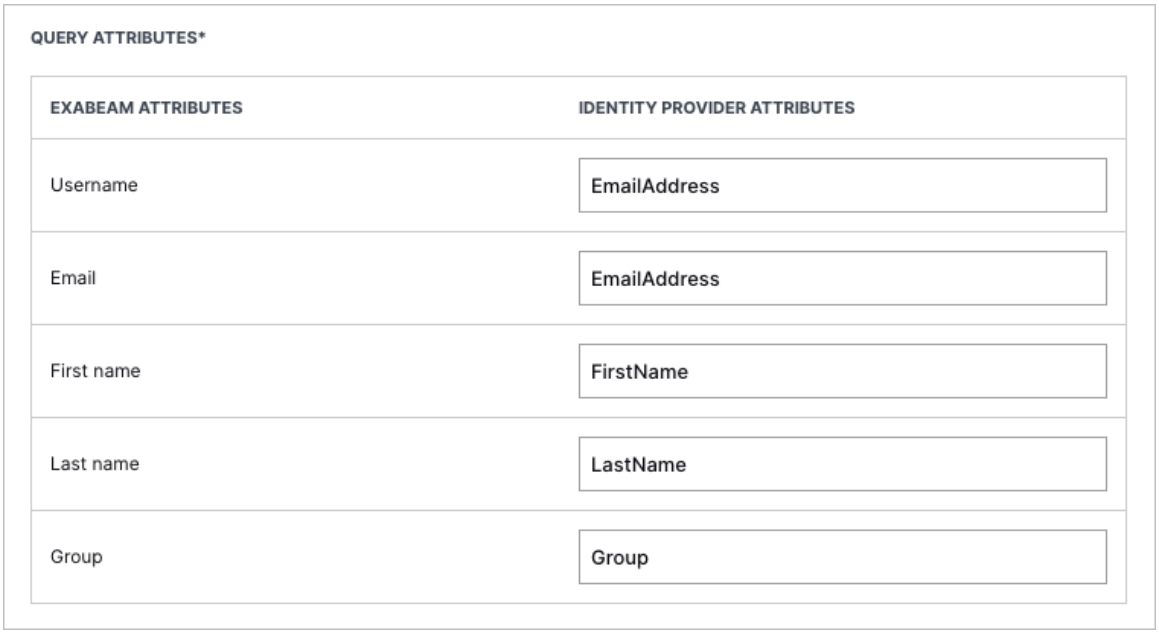
- Click **Upload XML metadata file**, navigate to the IdP metadata file that you downloaded in step 1b, and click to upload it.

The uploaded metadata file populates the required configuration fields.

- Click **Manual Configuration**, and then use the information that you obtained earlier to do the following:
  a. Enter values for the **SAML Entity ID** and **Login URL**.
  b. Click **Upload IdP Certificate**, navigate to the certificate and click to upload it.

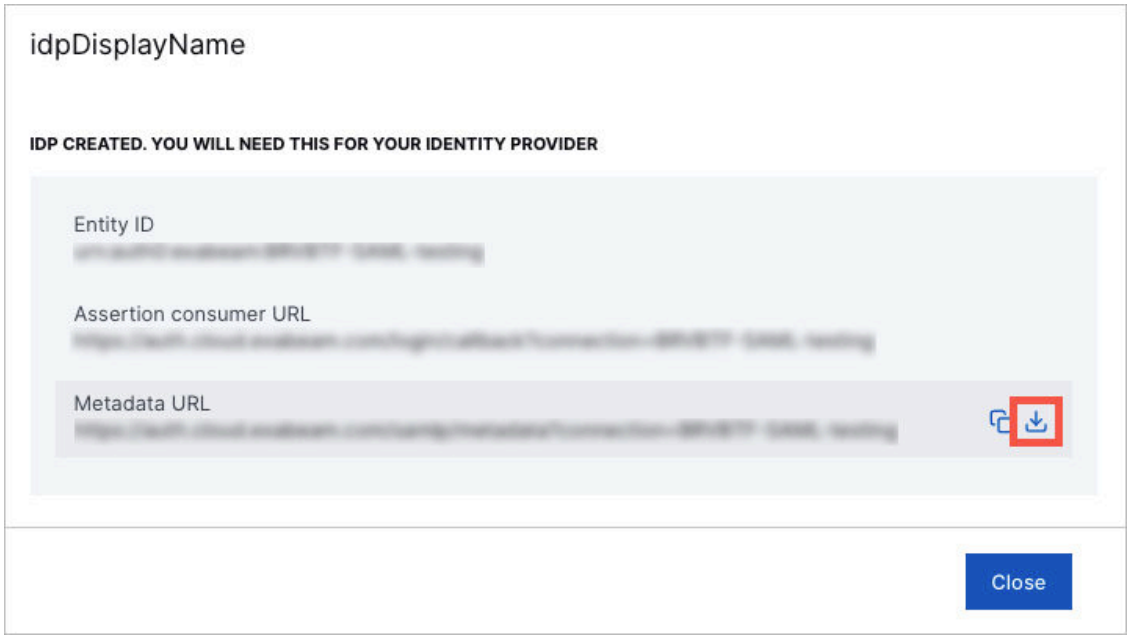
f. *(Optional)* Enter values for the **Logout URL** and **Logout redirect URL**.

g. In the **Query Attributes** table, map the Exabeam query attributes to the corresponding IdP user attributes by entering the same descriptive values that you did in step 1b, as demonstrated in the following example:



h. Click **Add Identity Provider**.
The idpDisplayName box appears.

i. Do one of the following:
- Download the **Metadata URL** file by moving your pointer over the URL and clicking the download icon on the right.

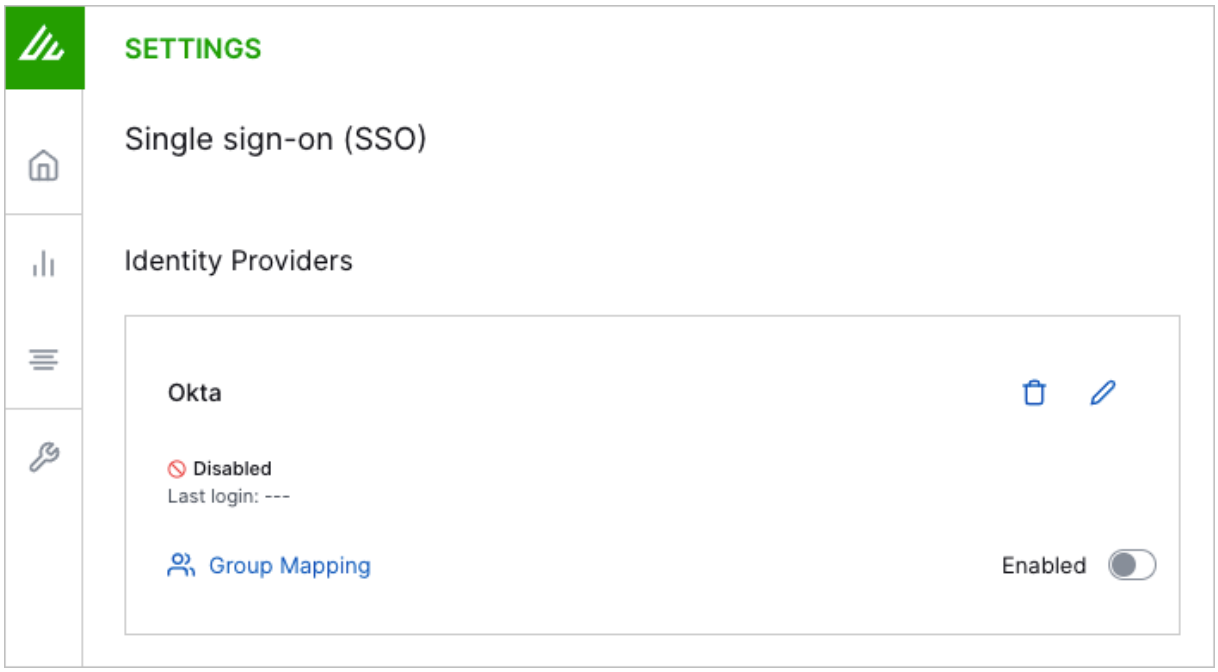


- Copy the **Entity ID** and **Assertion Consumer URL** values.

> **NOTE**
> The information obtained in this step needs to be added into your IdP.

3. Log in to your IdP to complete the Exabeam application configuration:
   a. From the information obtained in step 2i, enter the *Entity ID* and *Assertion Consumer (ACS) URL* values into their appropriate fields. You can also input these values by uploading the Metadata URL file if your IdP provides the option.
   b. Complete any additional steps in your IdP that are necessary to finish the configuration. Refer to your IdP user guide for details.

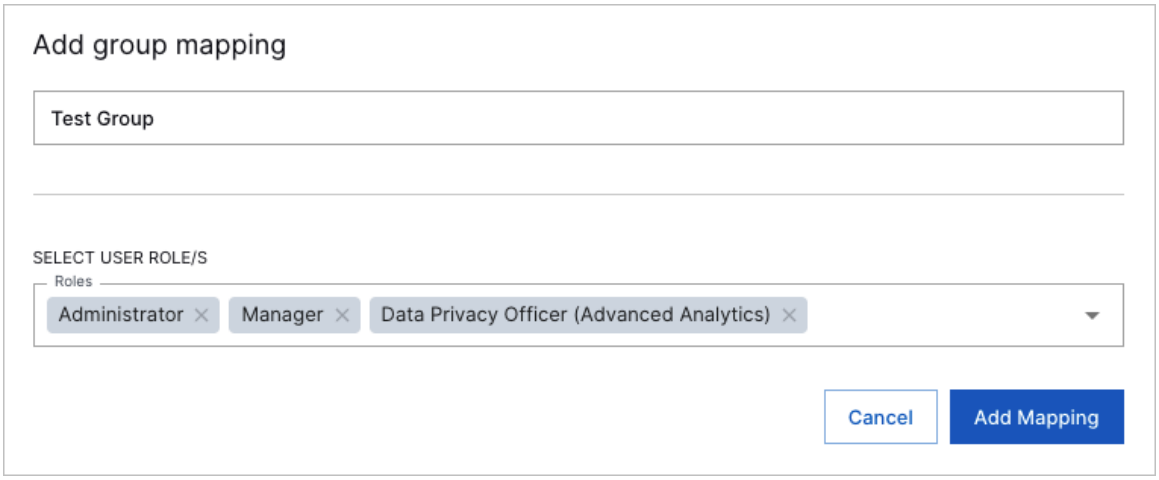
4. Log in to the New-Scale Security Operations Platform, click **Settings**, and then click **Single sign-on**.
   The IdP is listed on the Single Sign-On page.



5. Click **Group Mapping** and then do the following:

> **NOTE**
> The purpose of group mapping is to map the user groups in your IdP to the appropriate user roles in Exabeam. For example, if your IdP includes an `Advanced Analyst` user group that needs the permissions included in the `Tier 3 Analyst (Advanced Analytics)` role, you can map the group to that role. Each group can be mapped to one or more roles as needed.

   a. Click **Add new mapping**.
   The Add Group Mapping dialog box appears.
   b. In the **Group name** box, enter the name of an IdP group.
   c. Click the **Roles** drop-down list, and then select the Exabeam roles that you want to assign to the group.
   d. After you have selected all the roles that you want assigned to the group, click **Add Mapping**.



e. Repeat steps a–d as needed to map any other IdP groups.

Users from your third-party IdP and their assigned roles are displayed on the Users page.

6. To enable the IdP, click the **Enabled** toggle.
The Enabled toggle turns blue.

Set up Okta as your Identity Provider

If you use Okta as a third-party Single Sign-On (SSO) provider, you can integrate your Okta with Exabeam to ensure a secure login experience.

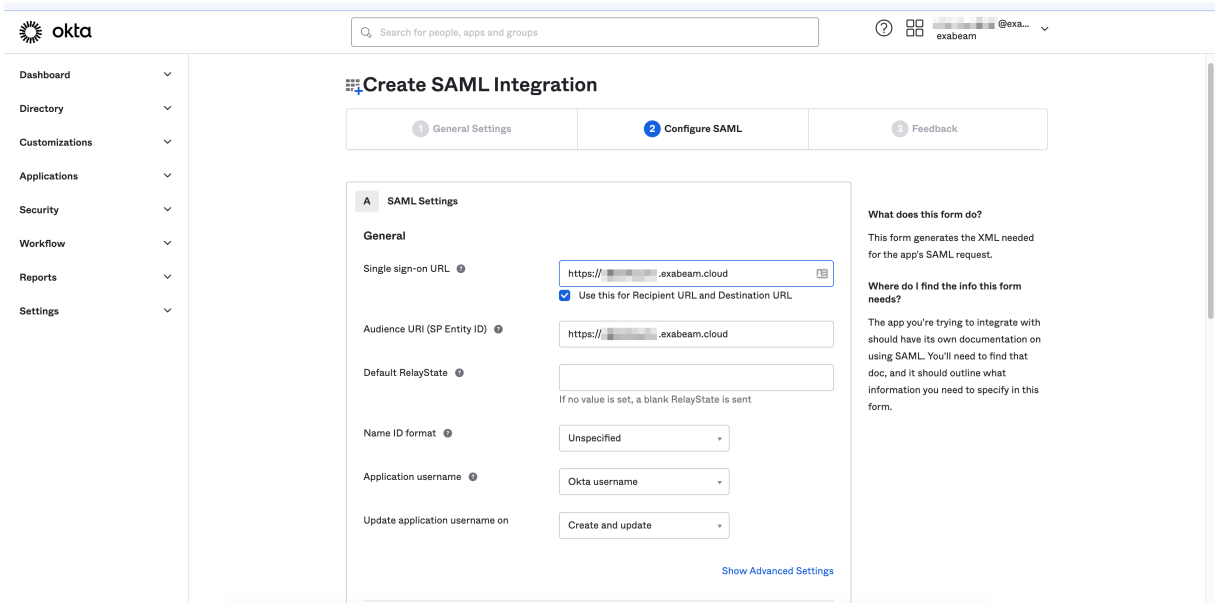
Before you set up the integration, ensure that you have your Okta Administrator available in case changes are needed on the Okta side.

- Add the Exabeam Application in Okta
- Add Okta as the IdP in Exabeam

Add the Exabeam Application in Okta

Before you set up the IdP settings in Exabeam, you must add an Exabeam Application in Okta. The attributes and SAML settings that you define will be needed for your Exabeam configuration.

1. Add a custom SAML 2.0 application for Exabeam in your Okta Admin Console (https://<your-okta-domain>/admin).
For full instructions, see the *Okta documentation* to Create SAML app integrations.



During the setup, you will:

a. Specify the URL for your New-Scale Security Operations Platform as both the **Single sign-on URL** and the **Audience URI**.
   This value acts as a placeholder while you complete the setup of your IdP configuration in the New-Scale Security Operations Platform. You will later return to and update this configuration with actual values.

b. Choose your preferred values for the **Name ID format**, **Application Username**, and **Update application username on**.

2. Specify which users and groups should be permitted to access the New-Scale Security Operations Platform using Okta.
   If you have not already done so, you will need to create a group for Exabeam access and assign users and rights to the group.

> **NOTE**
> Group names cannot contain spaces.

Take note of the group name as you will supply it in the next step.
For full instructions, see the *Okta documentation* about User Management.

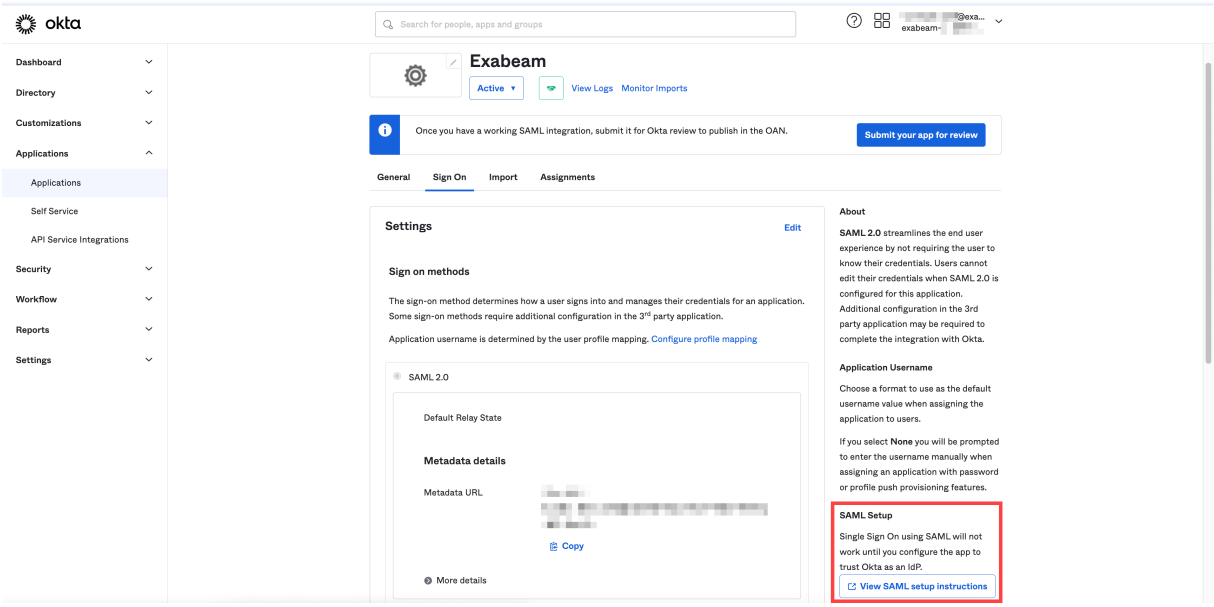
3. Define the attribute statements that Okta will share with Exabeam.
   For full instructions, see the *Okta documentation* to Define Attribute statements.

> **NOTE**
> Values are case sensitive. Later you will need to specify the exact values in the Query Attributes configuration of the Exabeam SSO Identity Provider.

In the Attribute Statements section of the Create SAML Integration page, define the following attributes for your Exabeam application:

Okta Name	Value
Attribute Statements	
FirstName	`user.FirstName`
LastName	`user.LastName`
Email	`user.email`
Username	`user.email` or `user.login`
Group Statements	
(Optional) Group	`<exabeamGroupName>` If you use multiple values for Exabeam (such as exabeam-users, exabeam-groups), you could, for example, define this field using the following filter: `Starts with exabeam`.

4. Configure the app to trust Okta as an IdP provider.

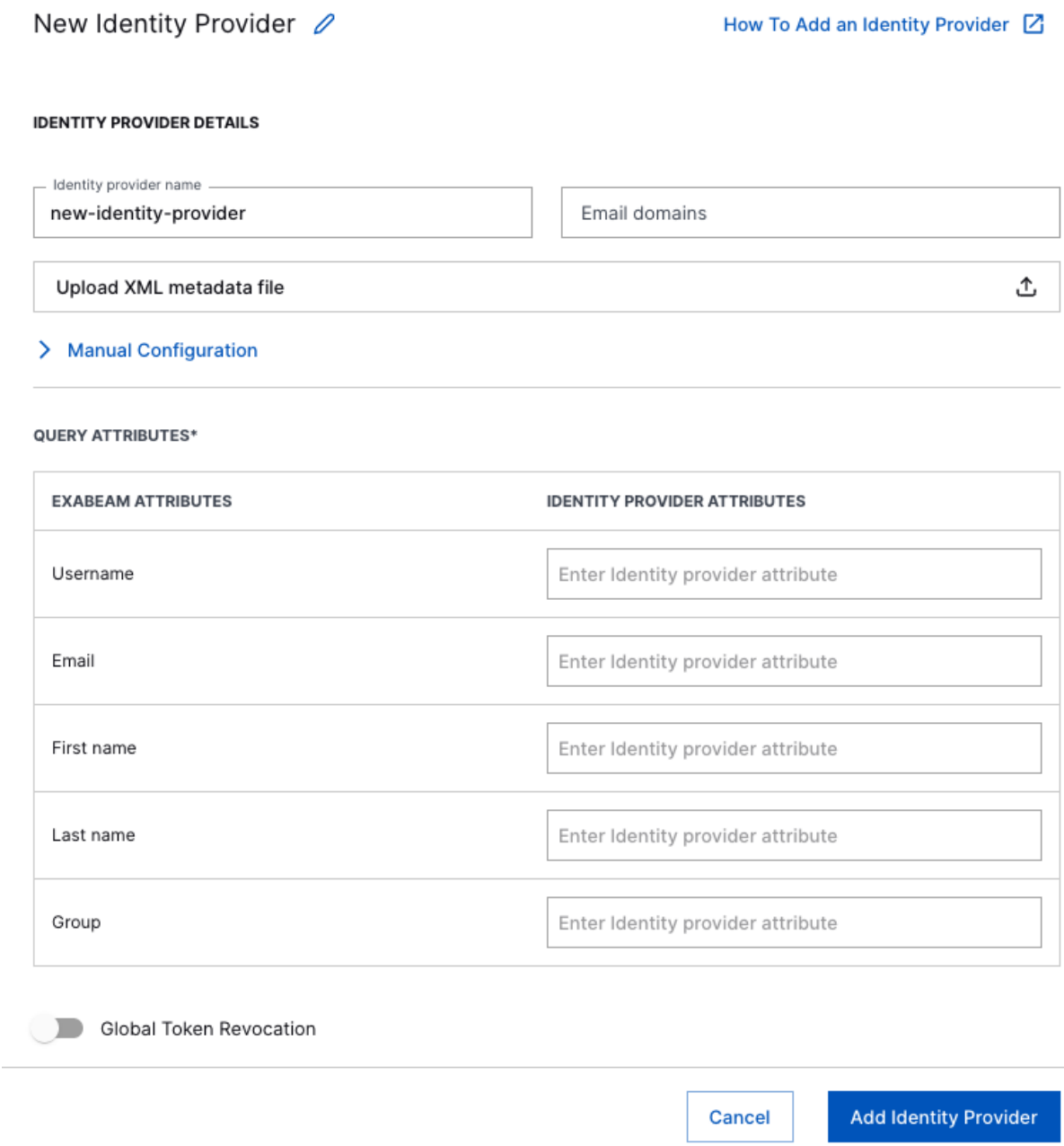


Follow any additional steps prompted by Okta to complete the setup. This may involve configuring attributes, mapping user profiles, and more.

5. Test the integration to ensure that users can successfully sign in to the application using Okta credentials.
6. If testing is successful, deploy the integration to make it active.

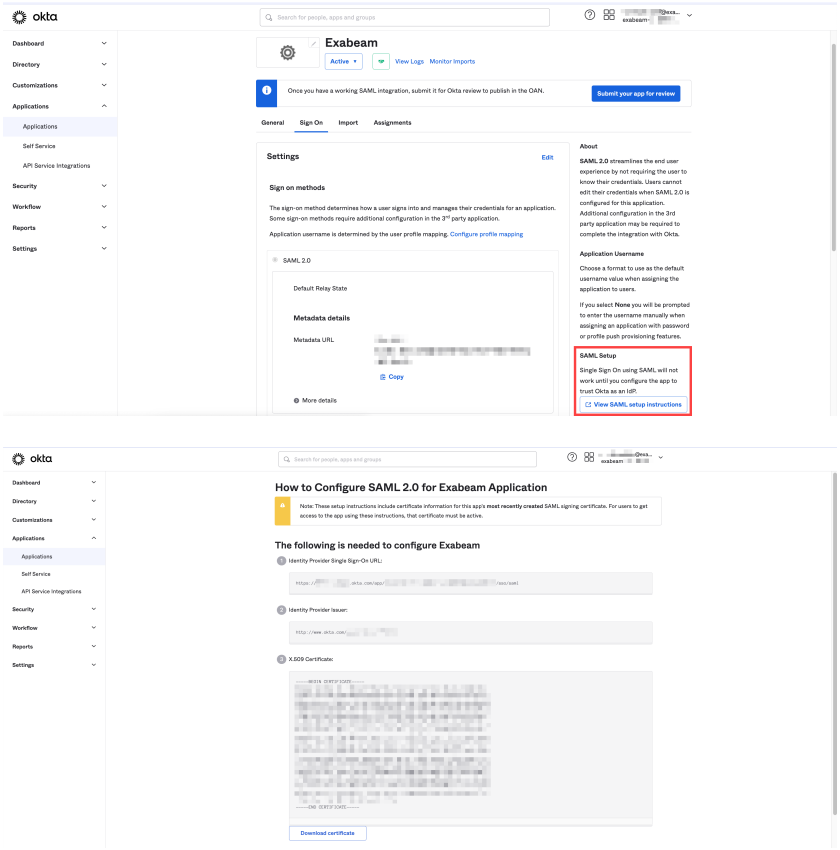
Add Okta as the IdP in Exabeam

1. Add a Third-Party Identity Provider for Okta.
   During this workflow, you will enter information about the Exabeam Application that you set up in Okta. It is recommended to have both the Exabeam IdP configuration and your Okta Admin Console open at the same time.



The following table identifies the fields that are relevant to configure Okta as the IdP:

Exabeam Field	Okta Inputs
Identity provider name	Okta

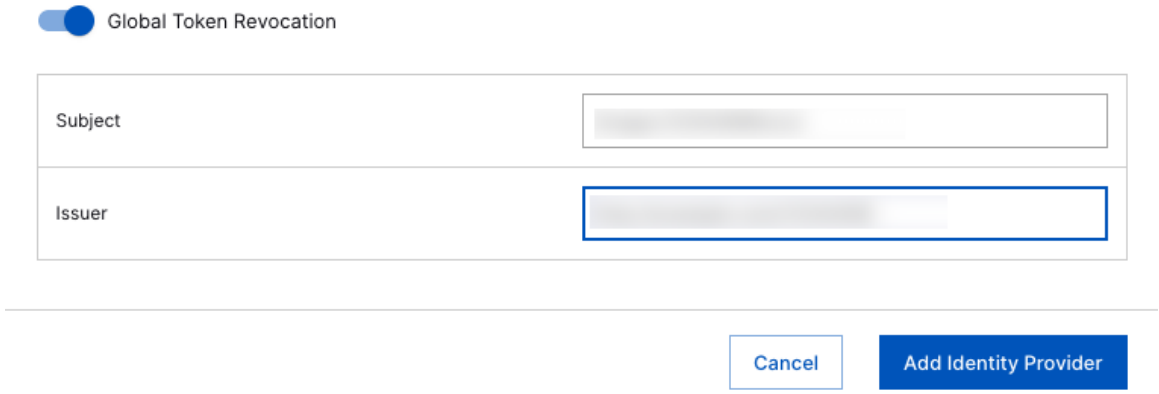
Exabeam Field	Okta Inputs
SAML Entity ID	Identity Provider Issuer. In Okta, see **Applications** > **Applications** > **Exabeam** > **Sign On** > **View SAML Setup Instructions**. 
Login URL	Identity Provider Single Sign-On URL. In Okta, see **View SAML Setup Instructions**.
Upload IdP Certificate	Copy or download the certificate. In Okta, see **View SAML Setup Instructions**.
Logout URL and **Logout Redirect URL**	These fields are optional in the New-Scale Security Operations Platform and will be automatically generated if left blank, however if you want redirect links, please input those.
Query Attributes	Match the attributes exactly to those you defined in Okta. See Step 3.

2. *(Optional step)* If setting up Global Token Revocation, follow this step. If not, continue to Step 3.

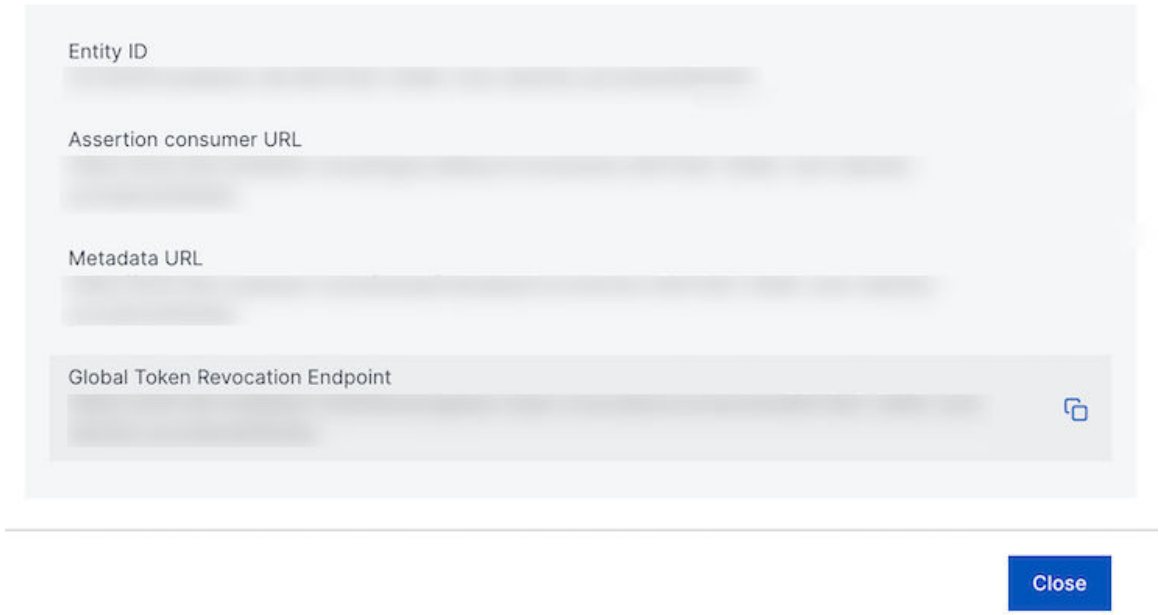
   You can enable Global Token Revocation/Universal Logout when using Auth0 with Okta Workforce Identity. With Universal Logout, if a user is logged out with the identity provider (IdP) —such as during an admin-initiated logout or a security event—they will also be logged out of all applications, including Exabeam. We currently use an Auth0 SAML connection for SSO. To enable Universal Logout end-to-end, a few configuration updates are required.

   a. In the New Identity Provider dialog box, toggle on **Global Token Revocation**.

   b. Enter the Subject and Issuer information (provided by your Okta admin) and select **Add**+**Identity**+**Provider**.

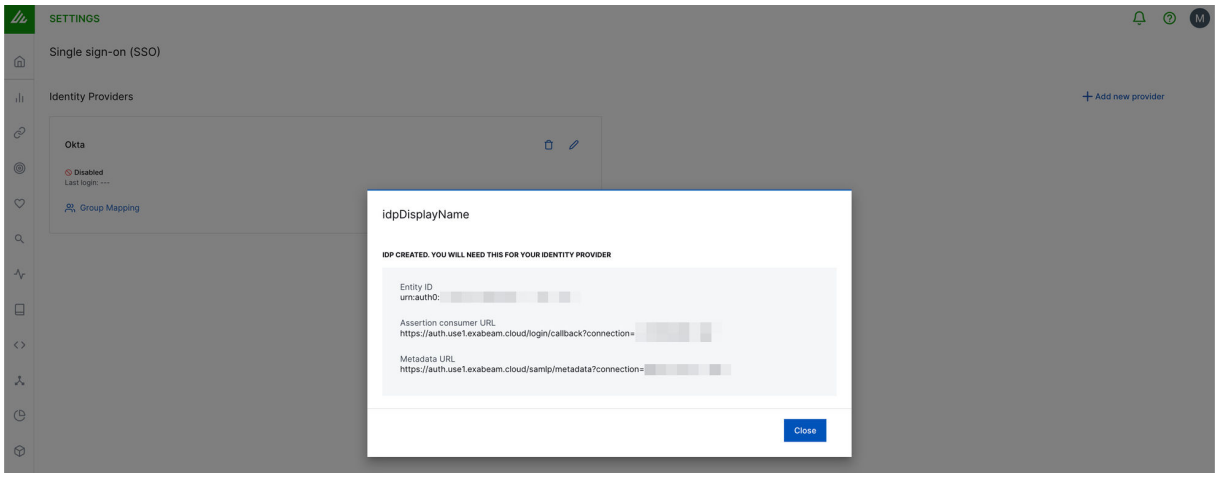


c. On the next screen, copy the Global Token Revocation Endpoint. You will need to configure this endpoint in Okta.



d. With the Global Token Revocation Endpoint you copied, follow the steps in Auth0/Okta docs in the Configure Universal Logout in Okta Workforce Identity section to add it to Okta in the Logout endpoint URL field.

3. Configure the Exabeam properties in Okta.
After you complete the setup, the New-Scale Security Operations Platform displays a summary of your IdP settings.

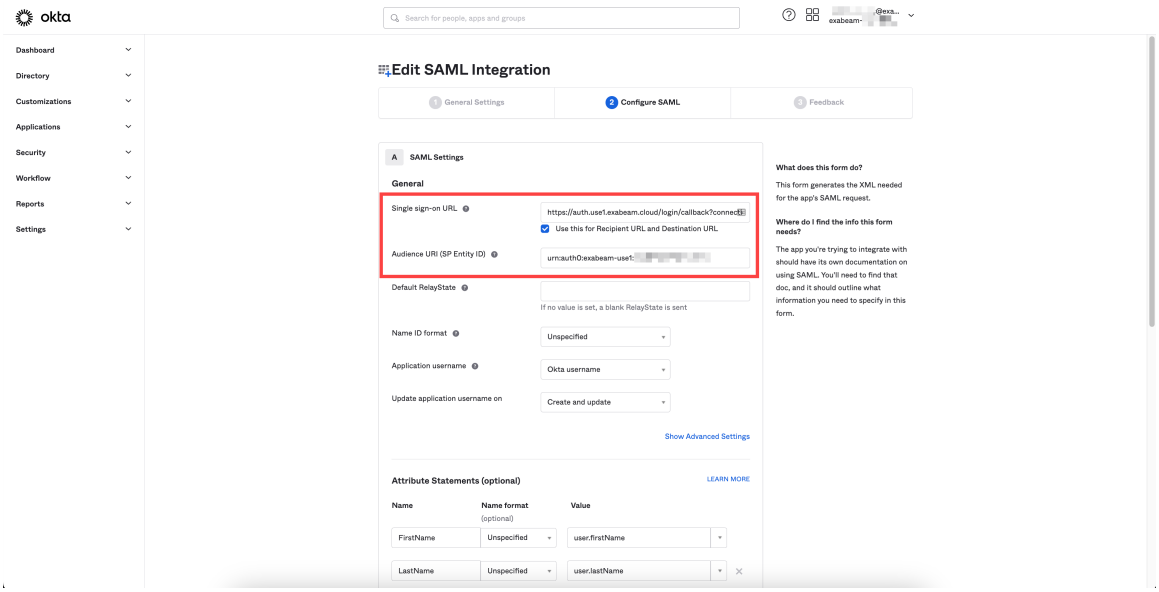


The Single sign-on URL will match Assertion consumer URL and Audience URI (SP Entity ID) will match Entity ID.

a. Note both values and return to the Okta Admin Console and edit your SAML integration.

b. Go to **Applications** > **Applications** > **Exabeam** > **Sign On**. In Settings click **Edit**.

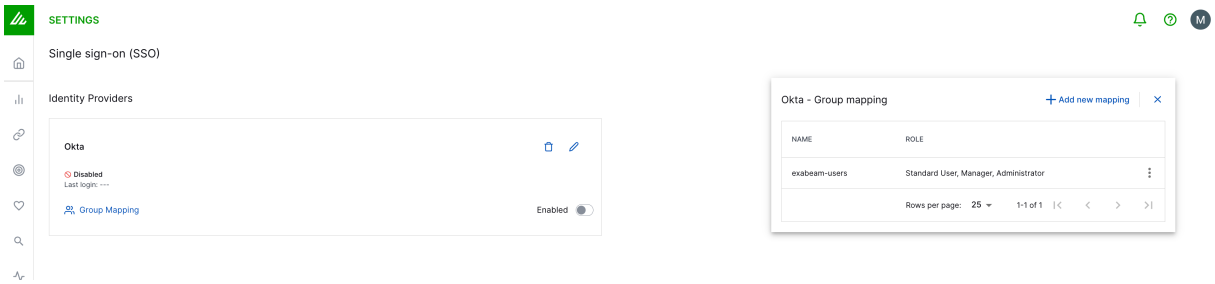
c. Enter the Assertion consumer URL value from the Exabeam configuration in the **Single sign-on URL** field.



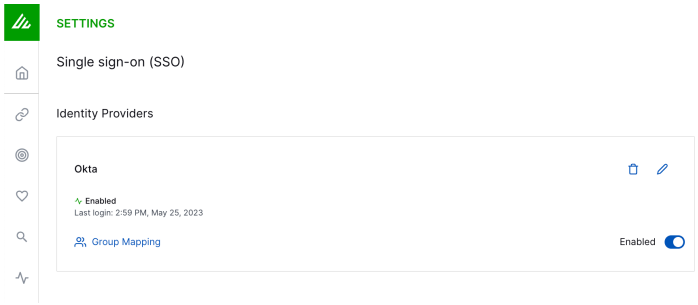
d. Enter the Audience URI from the Exabeam configuration in the **Entity ID** field.

e. Click **Next**.

4. Configure groups mapping in the New-Scale Security Operations Platform.



Ensure that group mapping matches the name of the group created in Okta.



For more information on this step, see Step 5.

5. Test your login in to the New-Scale Security Operations Platform to make sure your users can now access using their Okta credentials.

Set up Okta as your Identity Provider using Okta Integration Network

These instructions provide comprehensive instructions for configuring Okta as an Identity Provider (IdP) and implementing Universal Logout through the Okta Integration Network (OIN).

Single Sign-on Configuration

Prerequisites

To configure Single Sign-On (SS0), you must have a local user with administrative privileges for your Exabeam tenant. Alternatively, an Exabeam administrator must be available to assist with the configuration.

Supported Features

- Service Provider (SP) - initiated SSO
- Identity Provider (IdP) - initiated SSO
- Just-In-Time (JIT) provisioning

Configuration Steps

> **NOTE**
> Before initialing the integration, ensure that your Okta Administrator is available for necessary adjustments in Okta.

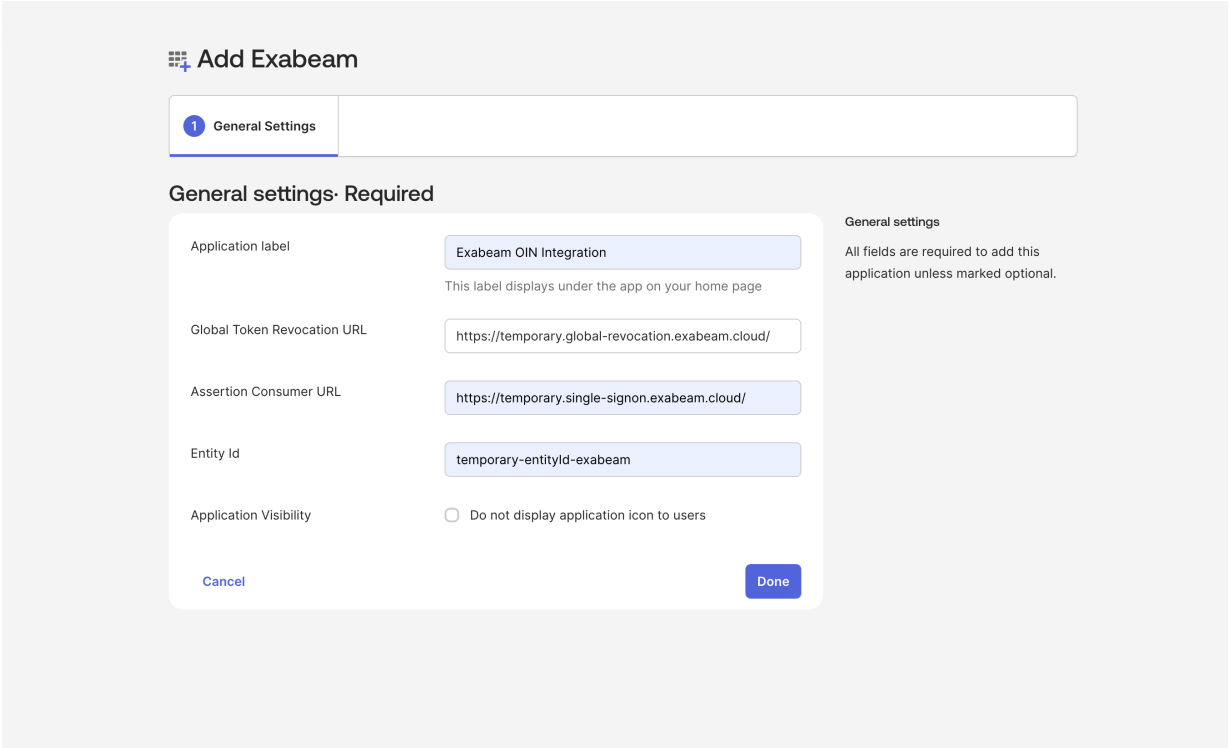
- Add the Exabeam application in Okta via OIN

- Add Okta as IdP in Exabeam
- Update the Entity ID and Assertion Consumer URL in the Okta Exabeam Application

Add the Exabeam Application in Okta via OIN

1. Sign in to your Okta instance as an administrator and navigate to **Applications > Applications > Browser App Catalog**.
2. On the Browse App Integration Catalog page, select the Exabeam application and click **Add Integration**.
3. On the General Settings page, specify the Application label, Global Token Revocation URL, Assertion Consumer URL, and Entity ID and click **Done:**
   - **Global Token Revocation URL**: https://temporary.global-revocation.exabeam.cloud/
   - **Single Sign-On URL**: https://temporary.single-signon.exabeam.cloud/
   - **Audience URI**: temporary-entityId-exabeam

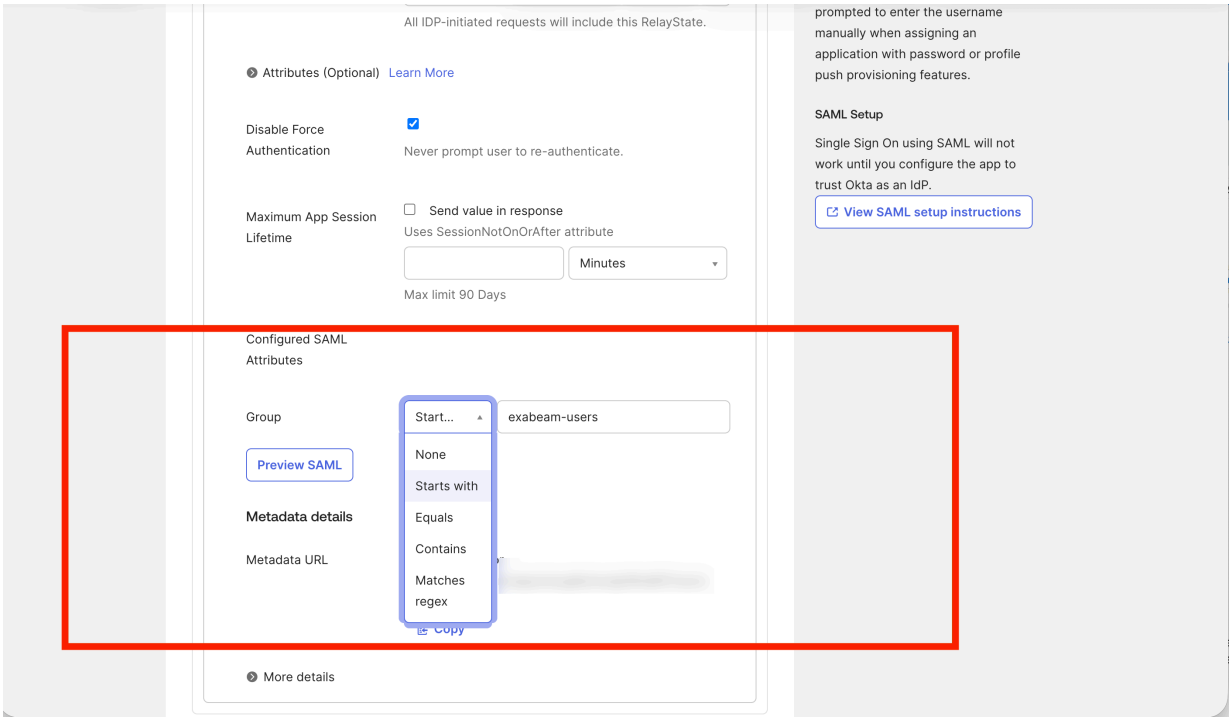
> ⚠ **CAUTION**
> These values serve as placeholders while you finalize the setup of the Okta IdP configuration in the Exabeam New-Scale Security Operations Platform. You will return later to update this configuration with actual values.



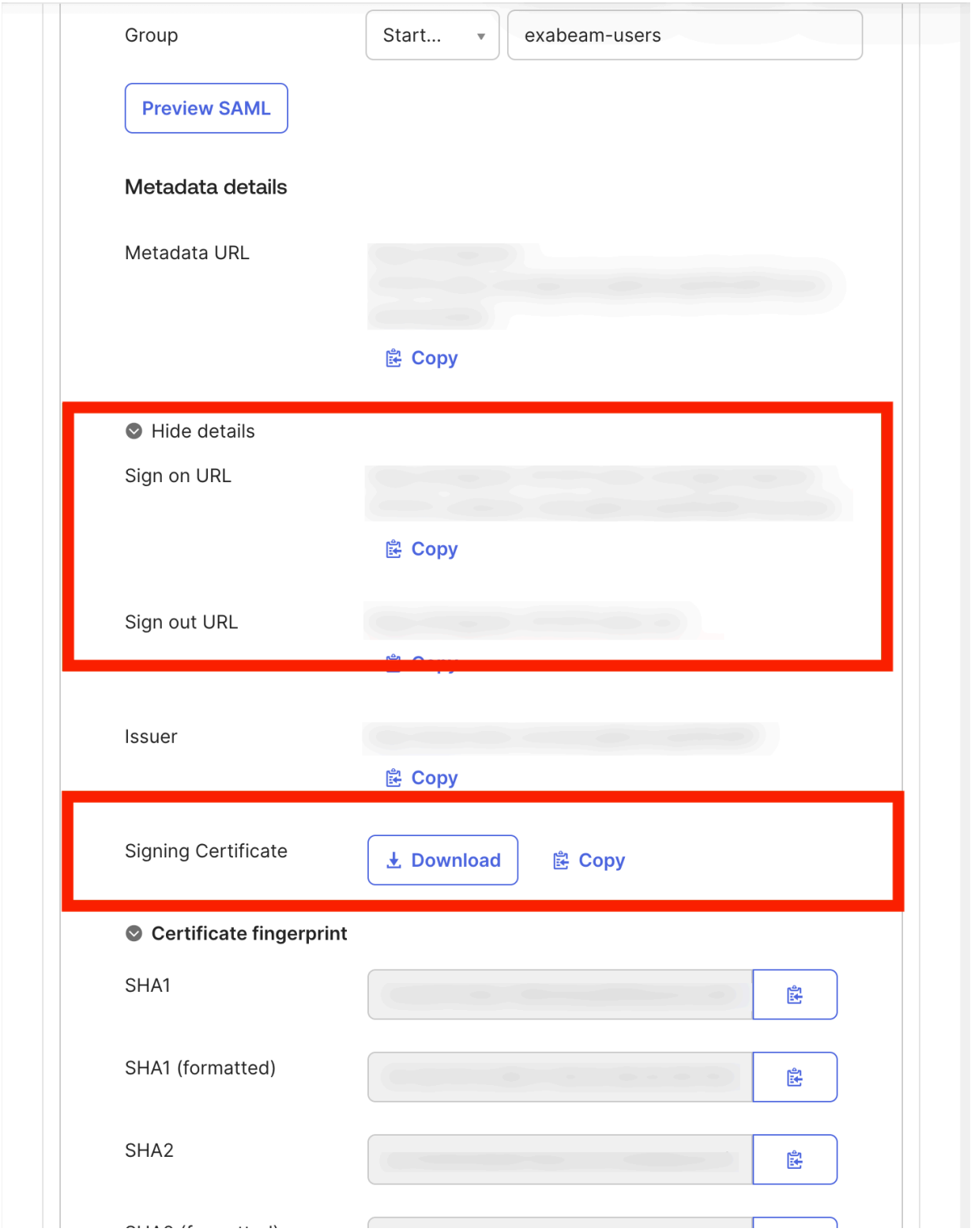
4. Navigate to the **Assignment** tab to specify which users and groups should be allowed to access the Exabeam New-Scale Security Operations Platform using Okta.

> **NOTE**
> If you haven't created a group for Exabeam access yet, you will need to do so and assign users and rights to this group.

5. Navigate to the **Single Sign-On** page, click **Edit**, and update the group.
   If you utilize multiple values for Exabeam (like exabeam-users, exabeam-groups), you can define this field using the filter:



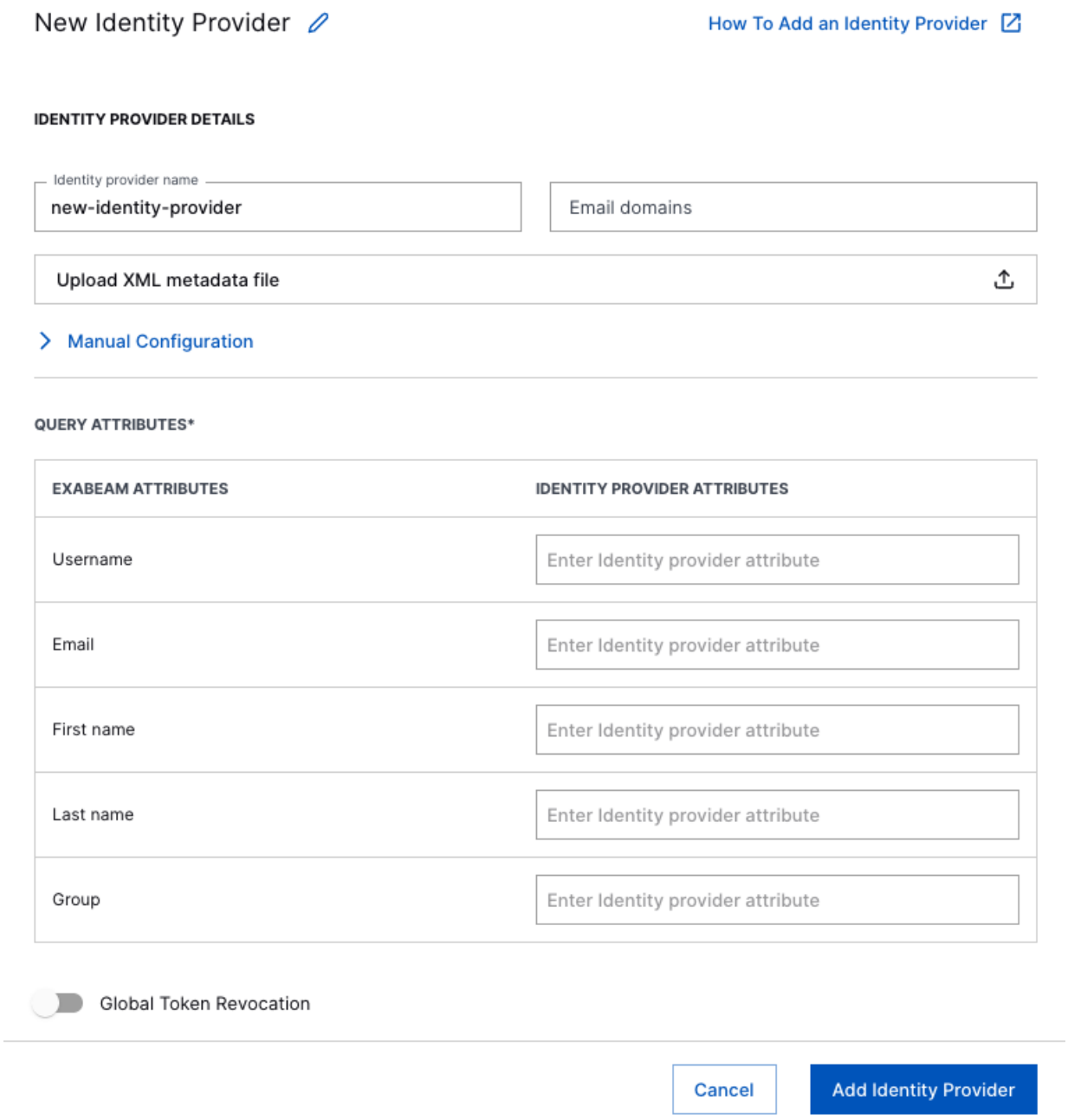
6. Navigate to the **Single Sign-On** tab. Note down the **Sign-On URL**, **Sign-Out URL**, and download the certificate. These values and the certificate will be required during IdP configuration in the Exabeam New-Scale Security Operations Platform.


Group
Start...
exabeam-users
Preview SAML
Metadata details
Metadata URL
Copy
Hide details
Sign on URL
Copy
Sign out URL
Issuer
Copy
Signing Certificate
Download
Copy
Certificate fingerprint
SHA1
SHA1 (formatted)
SHA2

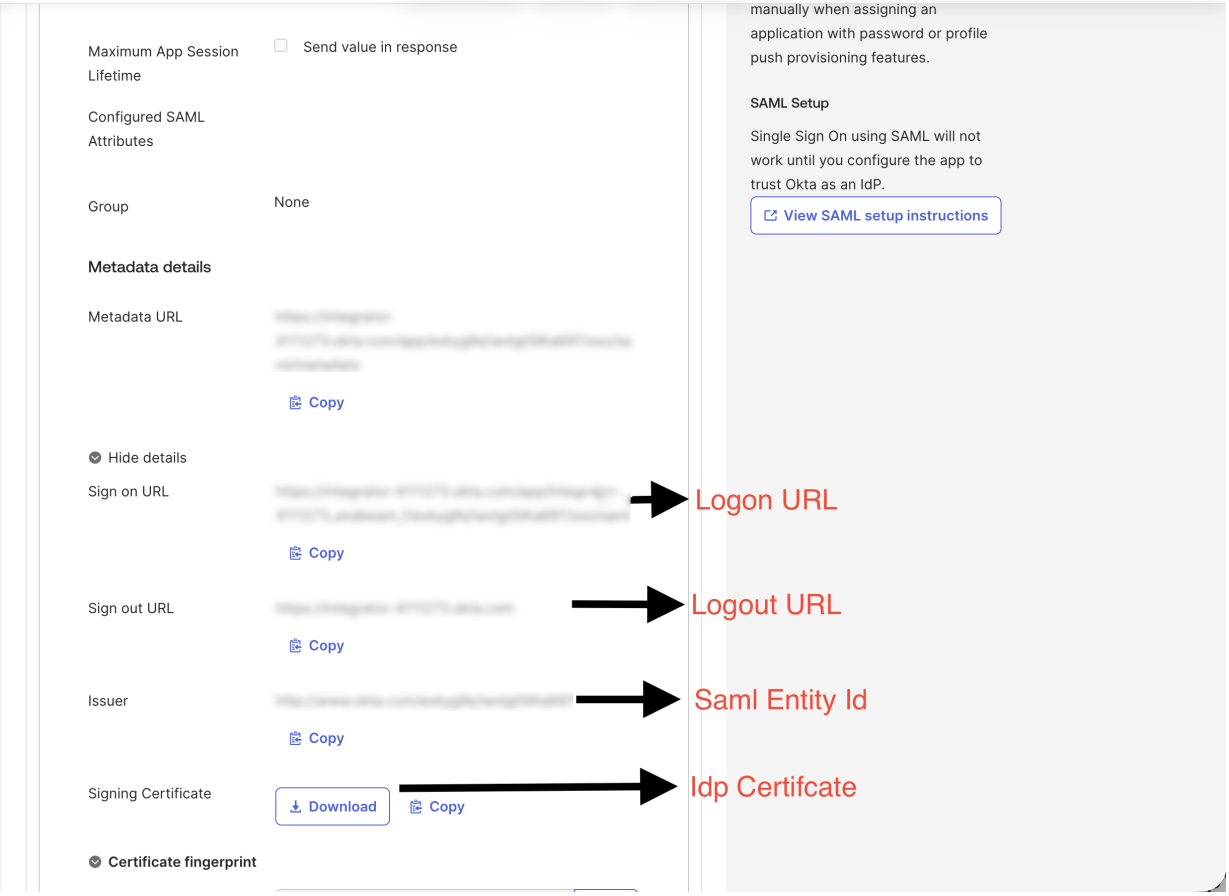
Add Okta as IdP in Exabam

In this section, you will enter information about the Exabeam Application that you configured in Okta using OIN. It is advisable to have both the Exabeam IdP configuration and your Okta Admin Console open at the same time.

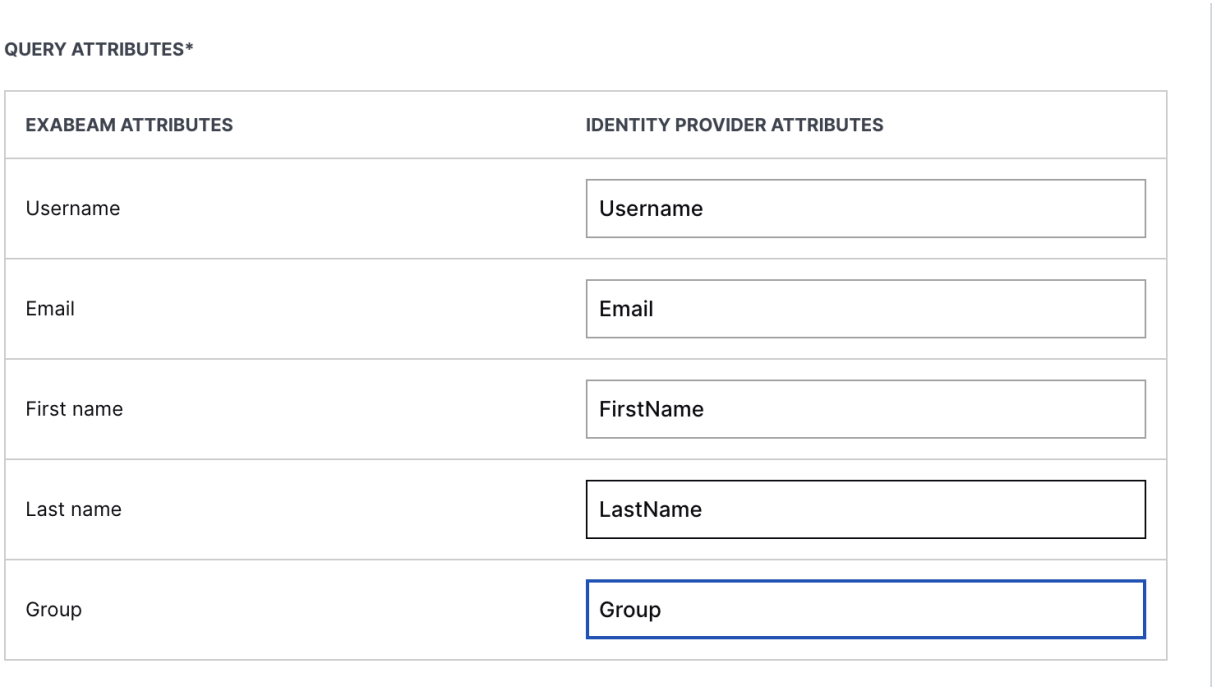
1. Log in to the Exabeam New-Scale Security Operations Platform, navigate to **Settings > Single Sign-On (SSO) MFA**, and click on **Add New Identity Provider**.
2. Enter the Identity Provider name and user email domain.



3. Under Manual Configuration, enter Enter the Issuer, Sign-On URL, and Sign-Out URL values from Okta into the Saml Entity ID, Logon URL, and Logout URL fields, respectively. Then upload the certificate from Okta.



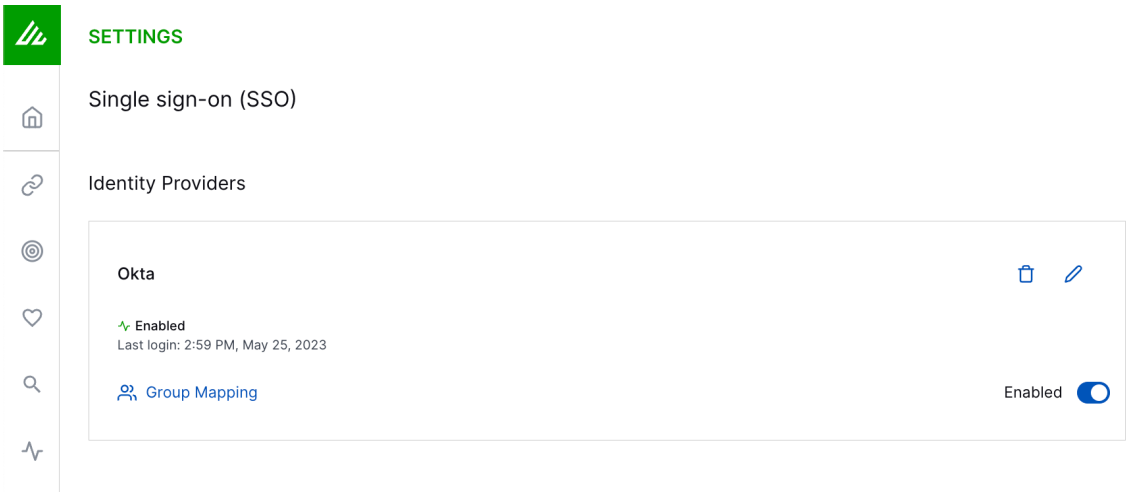
4. For Query Attributes, map the attributes in these fields to match those you defined in Okta as follows: *UserName*, *Email*, *FirstName*, *LastName*, *Group*.



5. Click **Add Identity Provider** to save the configuration.
6. Copy and note the **Entity ID** and **Assertion Consumer URL** values. These values need to be updated in the Okta Exabeam App in the next section.
7. Configure group mapping in the New-Scale Security Operations Platform. by clicking on **Group Mapping > Add new mapping**.
   a. In the Group name box, enter the name of the group from Okta.

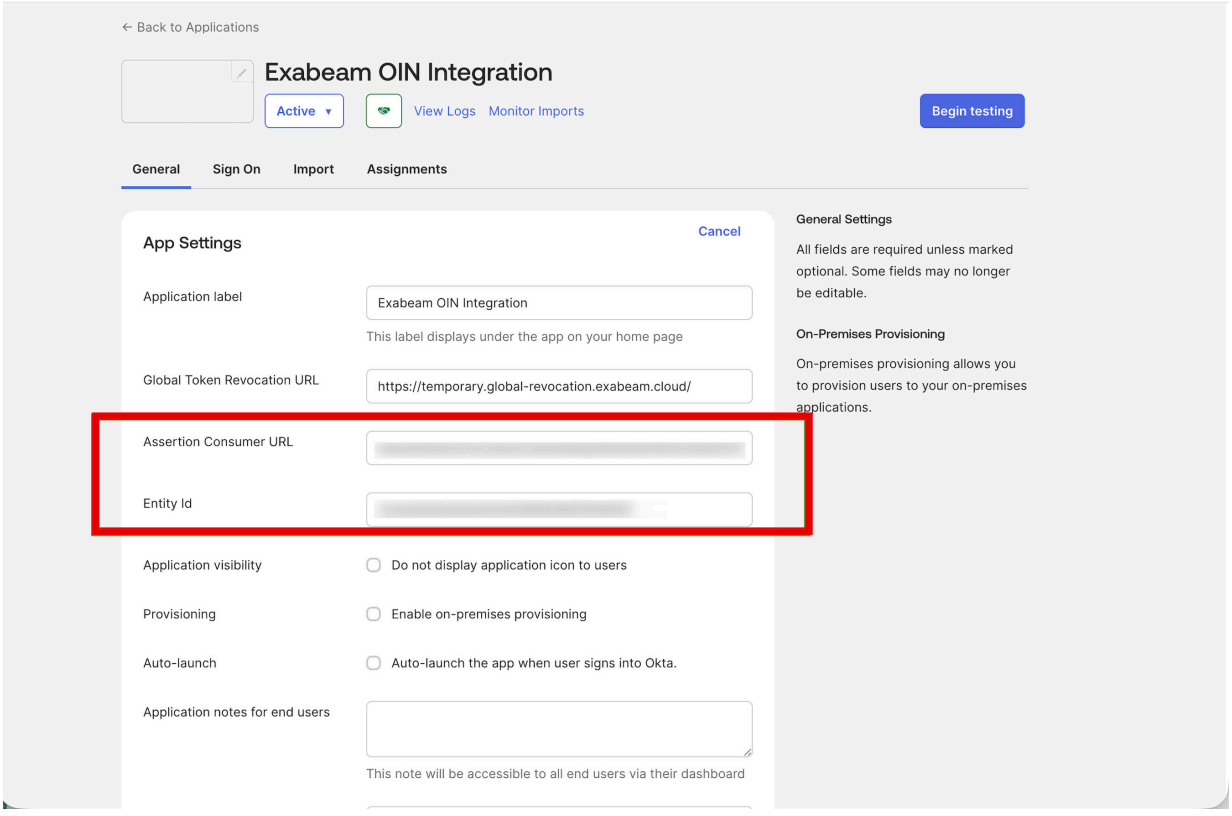
      NOTE
      Ensure that group mapping matches the name of the group created in Okta (See *Add the Exabeam Application in Okta via OIN* section above for more information).

   b. Click the Roles drop-down list, and then select the Exabeam roles that you want to assign to the group.
   c. After you have selected all the roles that you want assigned to the group, click **Add Mapping**.
   d. Toggle to enable the IdP.



Update the Entity ID and Assertion Consumer URL in the Okta Exabeam Application

1. Log in to the Okta admin console and navigate to the Exabeam application created using OIN.
2. Navigate to the **General** Tab. Update the **Entity ID** and **Assertion Consumer URL** from the last section , and save the configuration.



3. Test your login to the New-Scale Security Operations Platform to ensure users can now access it using their Okta credentials.
4. Test IdP-initiated login by accessing the Exabeam Application from Okta.

SP-initiated SSO

> **NOTE**
> This section is applicable only to SAML integrations that support app-initiated Single Sign-On (SSO), also known as Service Provider (SP) initiated SSO.

This sign-in flow begins at your Exabeam tenant. When you enter your username, you are redirected to Okta for authentication. After a successful Okta sign-in, you are returned to the Exabeam interface.

Sign-in Steps

1. Navigate to your Exabeam tenant sign-in page.
2. Enter your username to be redirected to the Okta sign-in page.
3. Enter your Okta credentials.

Configure Universal Logout/Global Token Revocation

> **NOTE**
> This is an optional step/configuration, but recommended for additional security protection.

Okta's Universal Logout feature allows you to terminate user sessions and tokens for supported applications when identity threat protection detects risk.

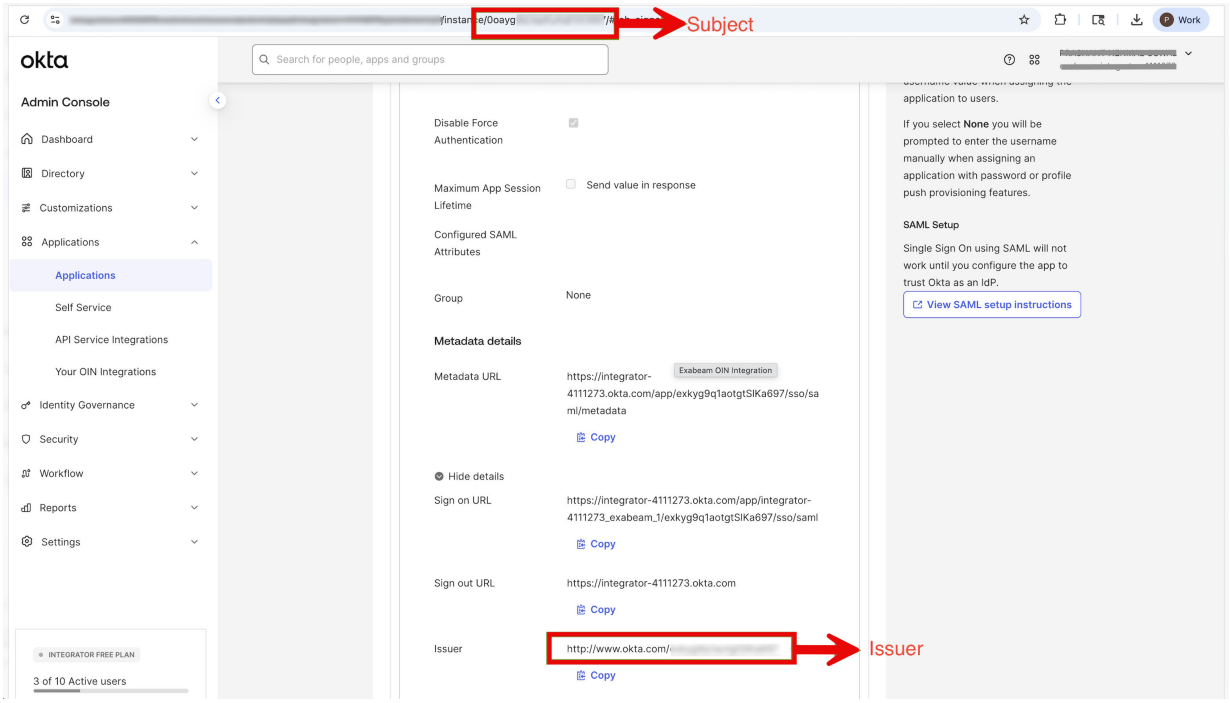
With Universal Logout, if a user is logged out with the identity provider (IdP) —such as during an admin-initiated logout or a security event—they will also be logged out of all applications, including Exabeam.

Configuration Steps

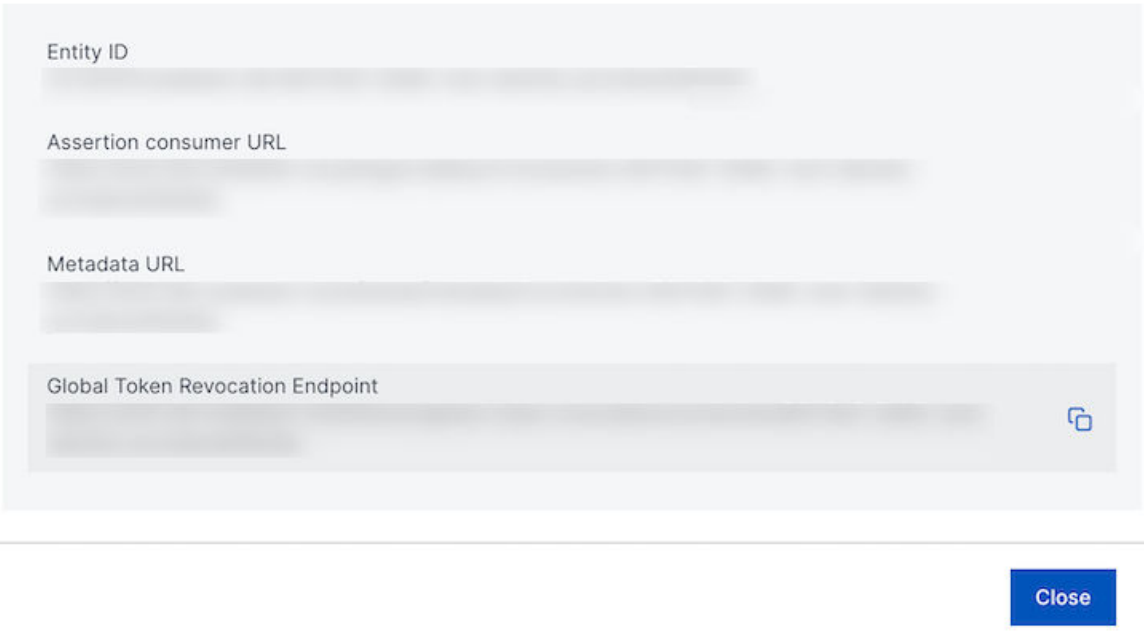
- Exabeam configuration
- Okta Exabeam Application configuration

Exabeam configuration

1. Log in to the Okta admin console and navigate to the Exabeam Application. Go to the **Sign On** tab and copy the **Issuer** and **Subject** from Okta. The Subject is an Application Id.

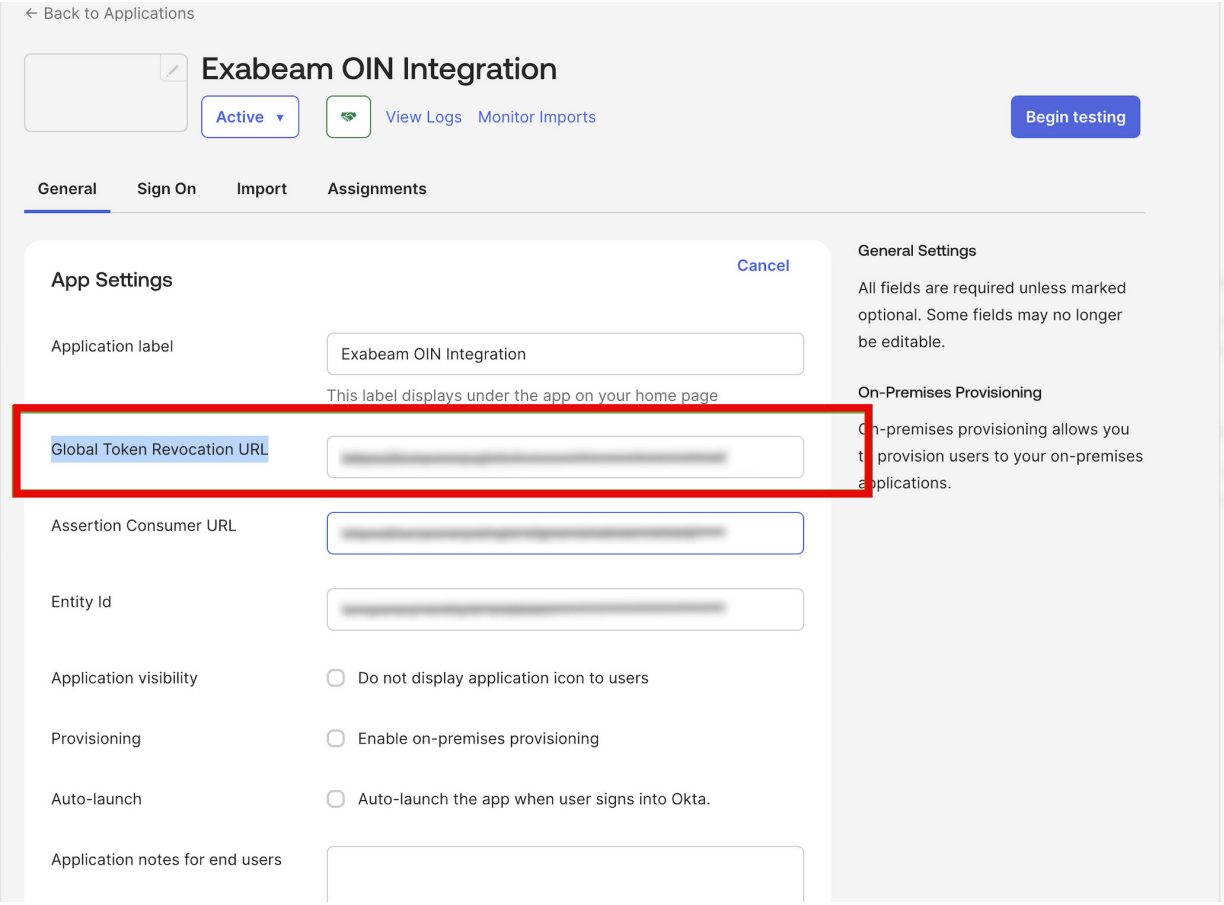


2. Log in to Exabeam New-Scale Secruity Operations Platform and navigate to Settings > Single Sign-On (SSO)/MFA, and edit the IdP configuration.
   a. Toggle on **Global Token Revocation**. Enter the **Subject** and **Issuer** information, and click **Update Identity Provider**.
   b. In the next box that appears, copy the **Global Token Revocation Endpoint**. This endpoint will need to be configured in Okta.

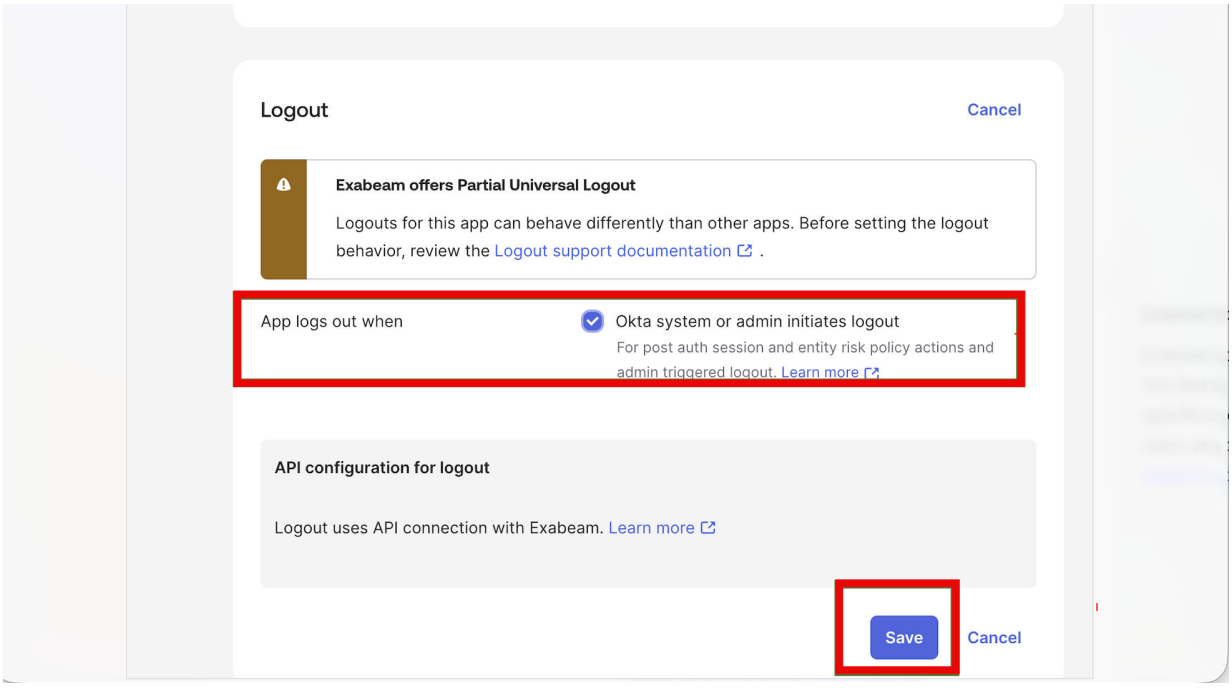


Okta Exabeam Application Configuration

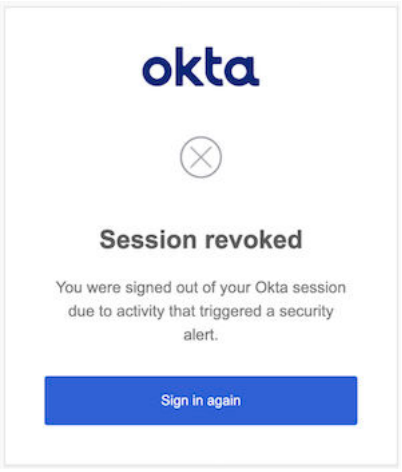
1. Log in to the Okta admin console and navigate to **Applications > Application** and select the Exabeam application created for SSO.
2. Navigate to the **General** tab and edit the app settings section to update the **Global Token Revocation URL**.



3. Navigate to the **Sign On** tab, edit the Logout section to enable Universal Logout, and save the configuration.



After enabling Universal Logout, users can be forcefully logged out by Okta due to security or administrative events. If this occurs, users will see a Session Revoked page on their next login attempt.



Users need to close the current browser tab and open a new tab to log in again.

NOTE

If you encounter any issues during the process, or receive a generic access denied message after authenticating through Okta, please open a case with the Exabeam support team at https://portal.exabeam.com/support/s/

Set up Microsoft Entra ID (formerly Azure) as your Identity Provider

If you use Microsoft Entra ID as a third-party Single Sign-On (SSO) provider, you can integrate your Microsoft Entra ID with Exabeam to ensure a secure login experience.

> **NOTE**
> Examples throughout these instructions may reflect the earlier name of Azure.

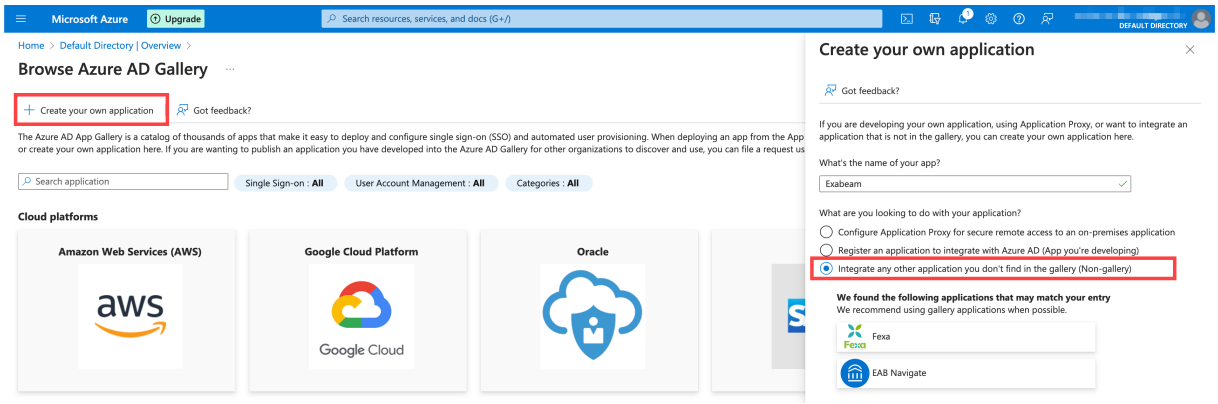
> **IMPORTANT**
> Ensure you select the appropriate account during SAML authentication after setting up. If you select an account under a different domain during the SAML authentication process, you may appear to be logged in with that alternate domain, even if it is not registered or intended for use with Exabeam SSO.

- Add the Exabeam Application in Microsoft Entra ID
- Add Microsoft Entra ID as the IdP in Exabeam

Add the Exabeam Application in Microsoft Entra ID

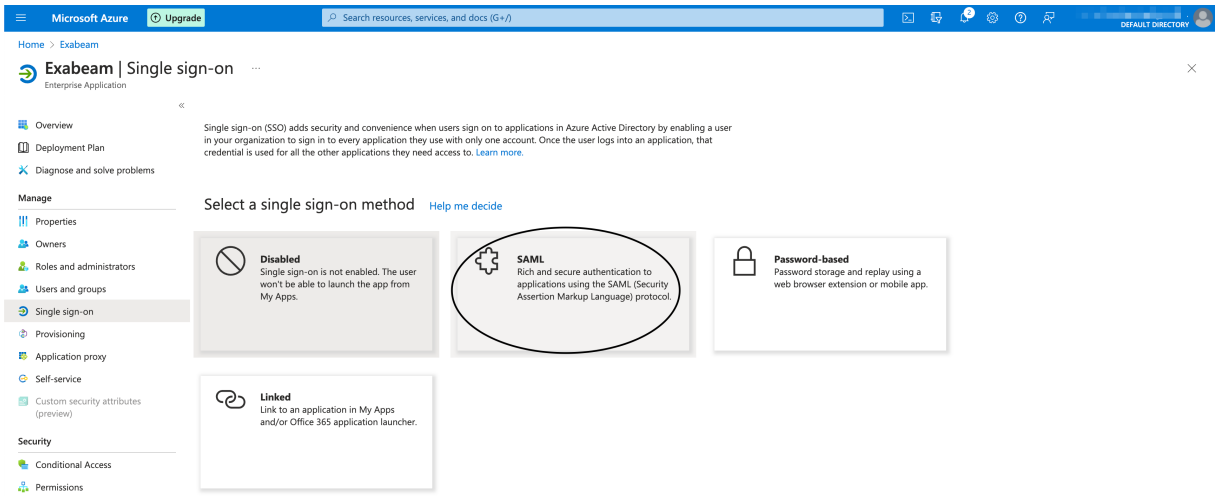
Before you set up the IdP settings in Exabeam, you must add an Exabeam Application in Microsoft Entra ID. The attributes and SAML settings that you define will be needed for your Exabeam configuration.

1. Create your own application for Exabeam as an Enterprise application in the Microsoft Entra admin center.



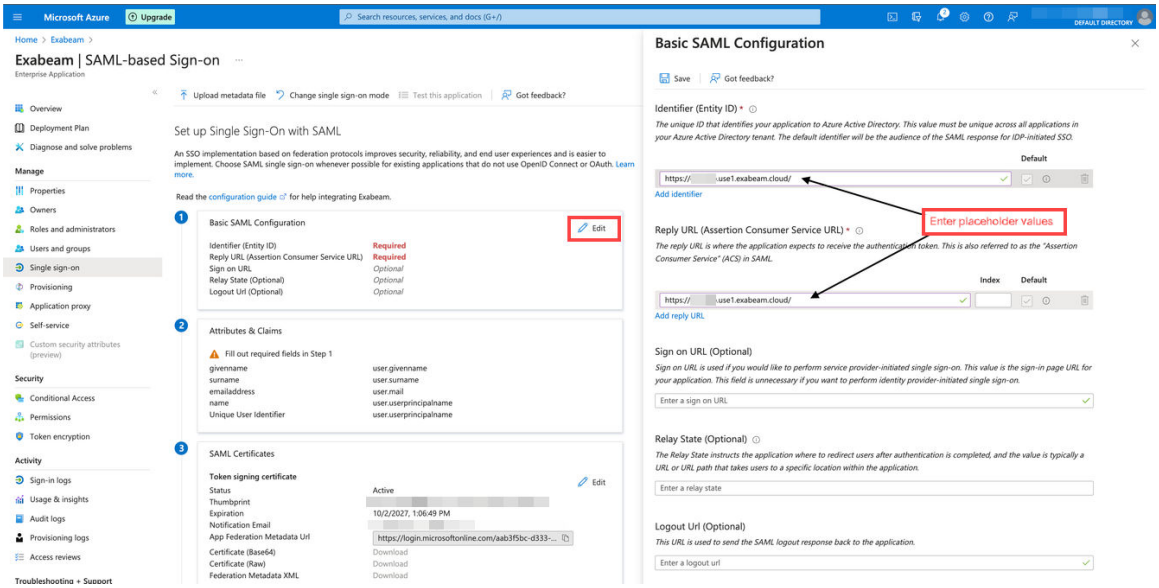
   For full instructions, see the Microsoft Entra ID Quickstart: Add an enterprise application.

2. Configure **Single Sign-On** as the authentication method for your Enterprise application.



During the setup, you will:

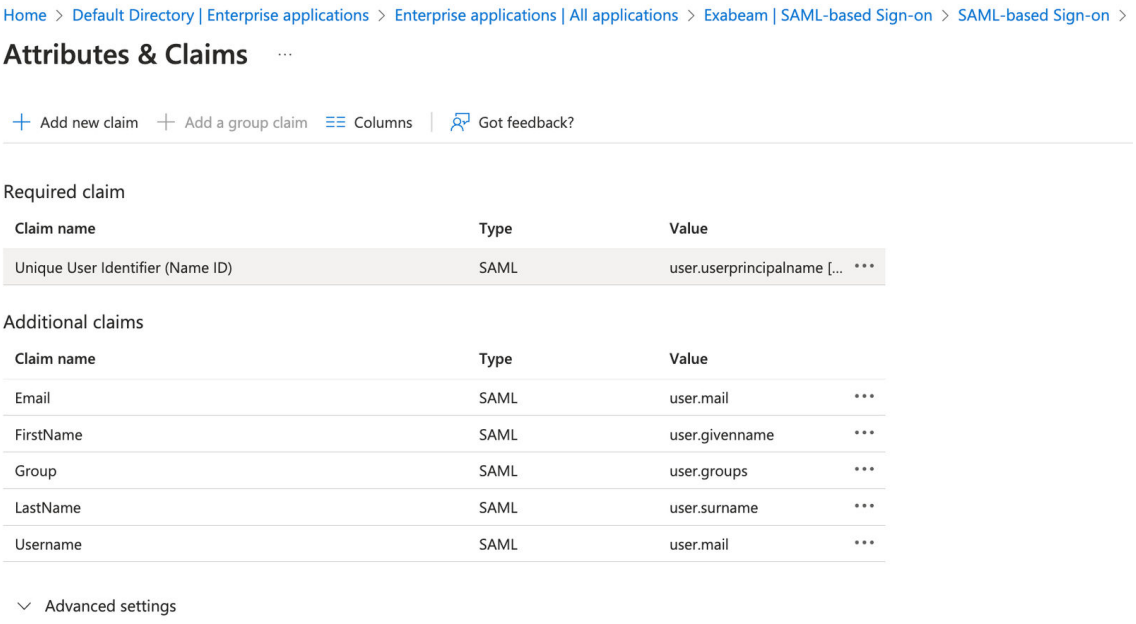
a. Supply placeholder links for the **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)**. You will later return to the configuration to replace the links after you complete the Exabeam-side configuration.



b. Edit or add the attribute statements that Microsoft Entra ID will share with Exabeam.

Microsoft Entra ID Name	Value
Unique User Identifier (Name ID)	**WARNING** Do not use this field. Instead, create a new Username field. If any field is missing, **Add new claim** and define it.
FirstName	`user.givenname`
LastName	`user.surname`
Email	`user.mail`
Username	`user.mail` or an alternate definition if you do not use email for your username.

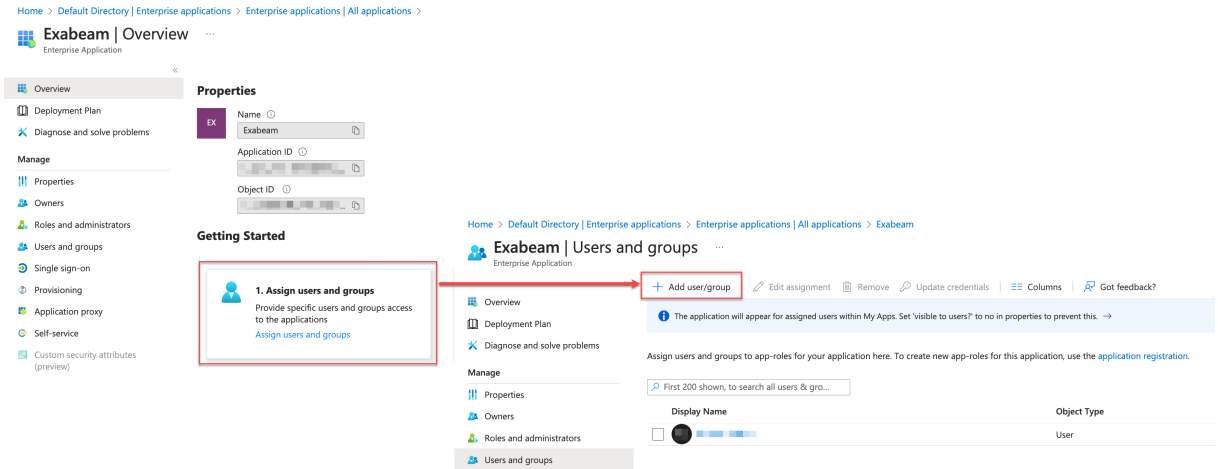
c. Configure a group claim to define the user's group membership information that you want to use in the application.



Set the Group Claims to an attribute assigned to the application (see Source attributes and then set that to an identifier for the group, such as Group ID).

> **IMPORTANT**
> Group ID is an immutable GUID. When using a different attribute, make sure to reflect any changes in both platforms for group mapping. Both strings need to match **exactly**, case-sensitive.

3. Configure group mapping for the new application.
Set up groups to limit access to the New-Scale Security Operations Platform to only the users who need it. For each group that you create, make sure to assign the Exabeam application to that group.

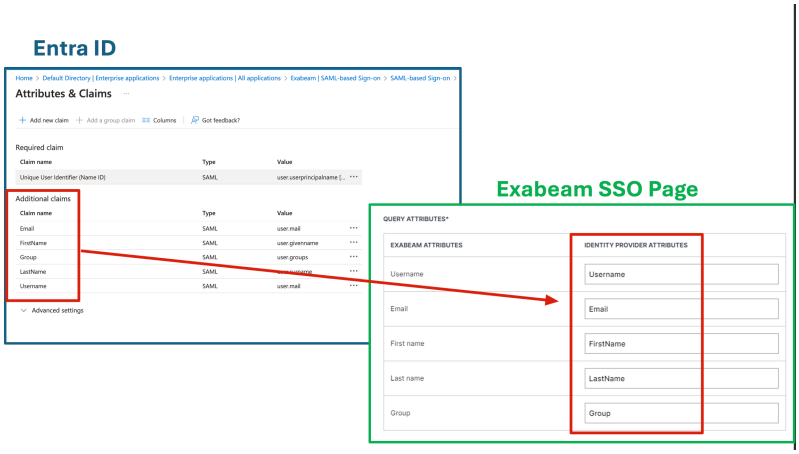


> **NOTE**
> Note the Object ID of the group. You will need the unique identifier when you configure group mapping in Exabeam.

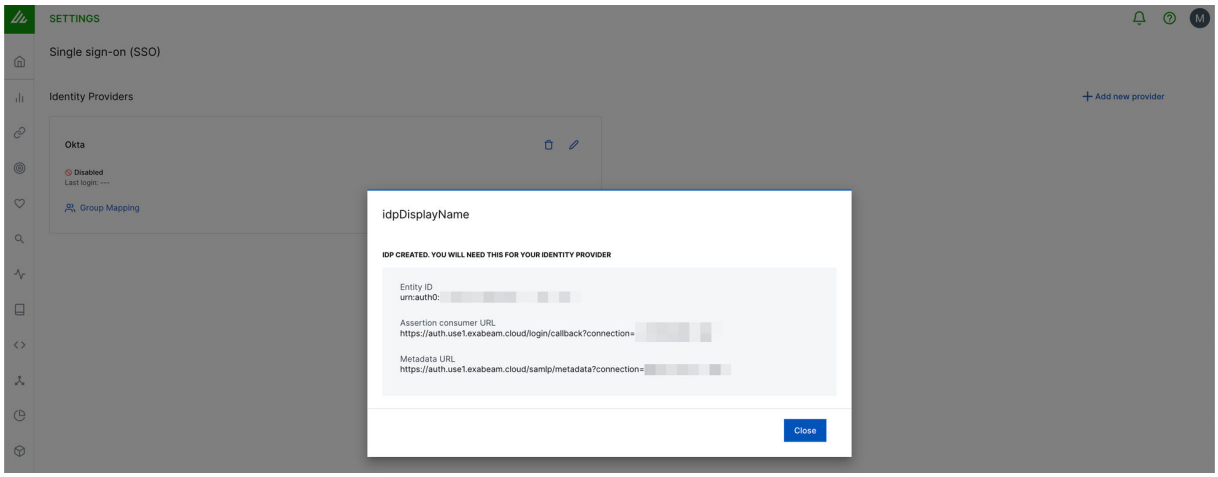
4. Test the integration to ensure that users can successfully sign in to the application using Microsoft Entra credentials.
5. If testing is successful, deploy the integration to make it active.

Add Microsoft Entra ID as the IdP in Exabeam

1. Add a Third-Party Identity Provider for Microsoft Entra ID.
   During this workflow, you will enter information about the Exabeam Application that you set up in Microsoft Entra ID. It is recommended to have both the Exabeam IdP configuration and the Microsoft Entra admin center open at the same time.
   The following table identifies the fields that are relevant to configure Microsoft Entra ID as the IdP:

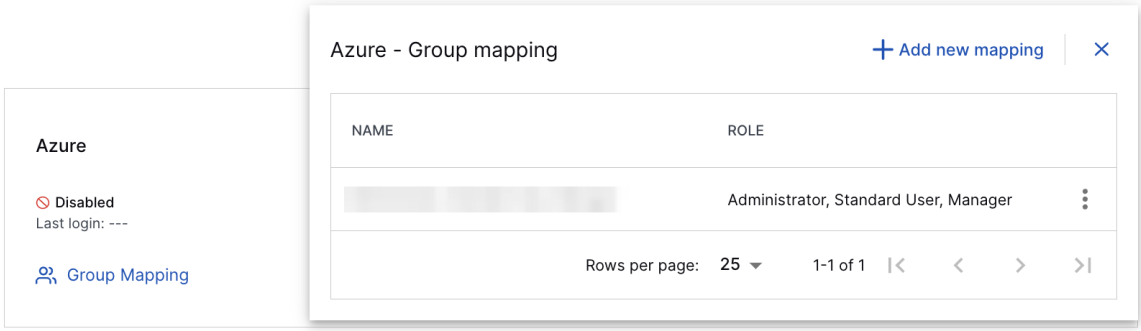
Exabeam Field	Microsoft Entra ID Inputs
Identity provider name	Microsoft Entra ID
SAML Entity ID	Identifier (Entity ID).
Login URL	Sign-On URL.
Upload IdP Certificate	Copy or download the certificate from the SAML certifications section of the app configuration in Microsoft Entra ID.
Logout URL and **Logout Redirect URL**	These fields are optional in the New-Scale Security Operations Platform and will be automatically generated if left blank, however if you want redirect links, input those.
Query Attributes	Match the attributes **exactly** to the Claim Name you specified in Microsoft Entra ID. 

2. Configure the Exabeam properties in Microsoft Entra ID.
   After you complete the setup, the New-Scale Security Operations Platform displays a summary of your IdP settings.

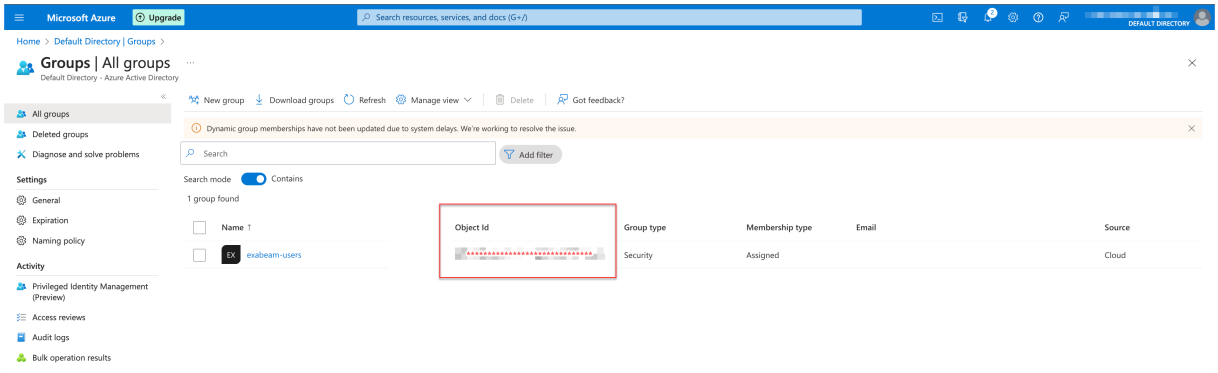


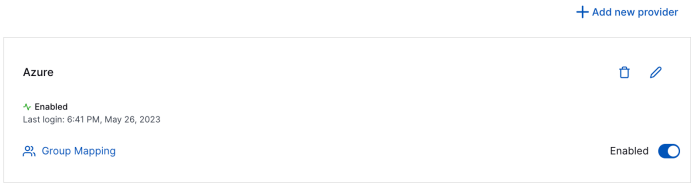
Update the app configuration Microsoft Entra ID to supply the Entity ID as the **Identifier (Entity ID)** and Assertion consumer URL as the **Reply URL (Assertion Consumer Service URL)**.

3. Configure and enable group mapping in the New-Scale Security Operations Platform.



Supply the Object ID you noted earlier from Microsoft Entra ID when you created the group.





For more information on this step, see Step 5 from Add a Third-Party Identity Provider.

4. Test your login in to the New-Scale Security Operations Platform to make sure your users can now access using their Microsoft Entra ID credentials.

Manage Third-Party IdPs

You can edit IdP group mappings, enable or disable IdPs, edit IdP details and attributes, and delete IdPs from the New-Scale Security Operations Platform.

1. Log in to the New-Scale Security Operations Platform.
2. On the lower-left side of the user interface, click **Settings**, and then click **Single Sign-On/ MFA**.
3. Do any of the following:
   - To edit group mappings:
     a. Click **Group Mapping** for the IdP that you modify.
     The Group Mapping dialog box appears.
     b. Do either of the following as needed:
        - To add a new group mapping, click **Add new mapping** to open the Add Group Mapping dialog box. In the **Group name** box, enter the group name, and then select the roles that you want to assign to it from the **Roles** drop-down list. When you are done, click **Add Mapping**.
        - To edit an existing mapping, click the corresponding More Menu icon and then edit the group name and/or user roles as needed. When you are done, click **Update Mapping**.
   - To enable or disable an IdP, click the corresponding **Enabled** toggle.
     When the toggle is blue, the IdP is enabled; when the toggle is gray, the IdP is disabled.
   - To edit an IdP's details and/or attributes, click the corresponding edit icon and then edit the information as needed. When you are done, click **Update Identity Provider**.
   - To delete an IdP from the SOC Platform, click the corresponding delete icon.

Access Control APIs

The Access Control APIs provide a way to programmatically view users, roles, and API keys that are configured in your environment. You can use the APIs to retrieve this type of information

without the need to log into the New-Scale Security Operations Platform and navigate the **Settings** options. The table below lists the current actions that can be managed via APIs.

To access these API endpoints, you must have an API key with **Access Control** permissions. For information about creating API keys, see Create an API Key in the *API Get Started Guide*.

The following table lists the Access Control APIs that are available. For specific information about API request and response parameters, see the Exabeam API Reference Guide and use the left navigation panel to find the **Access Control** endpoints.

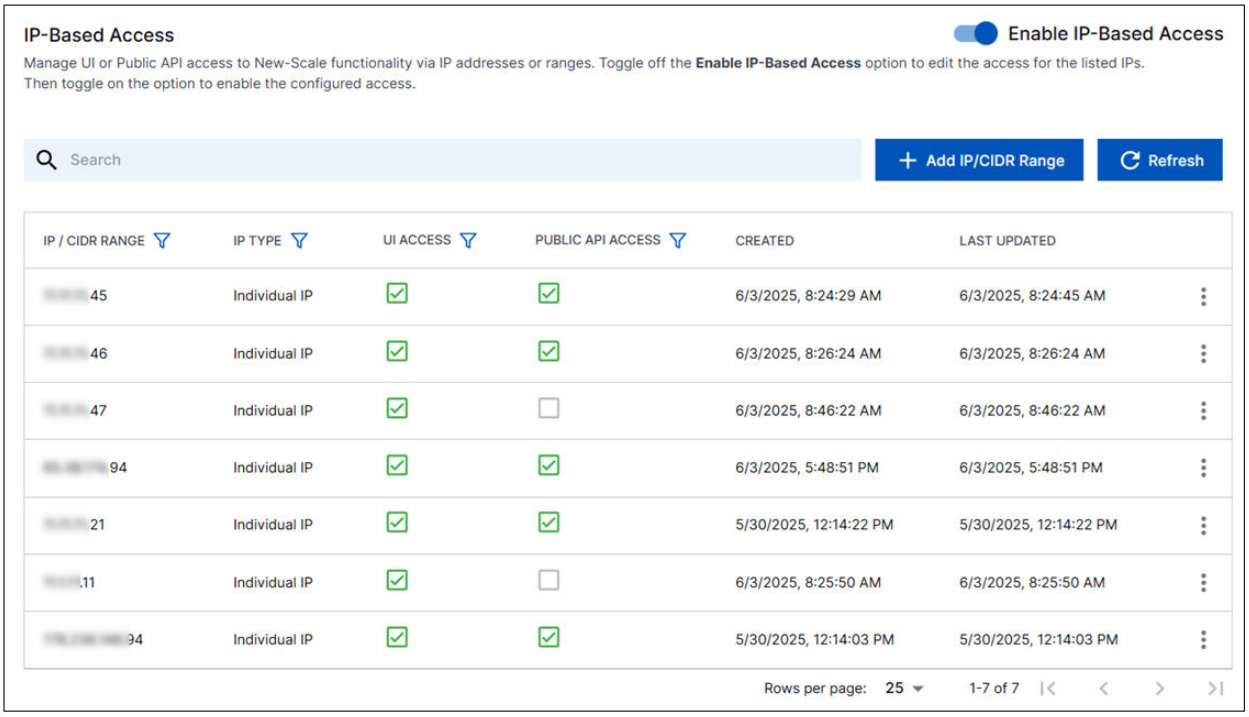
Endpoint	Summary	Description	Response
`GET access-control/v1/users`	View Users	Retrieve a list of configured users.	Returns a JSON array of information about each user, including Name, IdP, Email, Roles, Status, and Last Login.
`GET access-control/v1/roles`	View Roles	Retrieve a list of configured roles.	Returns a JSON array for each role, both default and custom, including the associated permissions for each role.
`GET access-control/v1/apikeys`	View API Keys	Retrieve a list of configure API keys.	Returns a JSON array of information about each API key, including the key Name, ID, and the last time it was used.

Manage Access by IP Addresses

The **IP-Based Access** page provides a way to configure UI and public API access to New-Scale functionality based on an allowed list of IP addresses. Each row in the list shows the UI and public API access granted to a single IP address or to a range of IP addresses. You can add IPs or IP ranges to the list and configure their access. You can also edit or delete IPs or IP ranges currently in the allowed list.

The page has a convenient on/off toggle at the top so you can avoid interrupting any ongoing processes while you configure an allowed list of access. With the toggle in the `off` position, you can configure all of the desired access and restrictions without implementing them. When you're ready, you can switch the toggle to the `on` position to implement the configured access for all of the listed IP addresses.

You can add up to a combined maximum of 250 IP addresses and ranges to the allowed list on the **IP-Based Access** page.



Keep in mind the following when managing access and restrictions in the allowed list:

- When the IP-based allowed list on the page is not enabled, the **Enable IP-Based Access** toggle in the top right is in the `off` position. If you click the toggle to the on position, you enable the allowed list and all of the access and restrictions it includes.
  If you toggle the **Enable IP-Based Access** option to the on position while your IP address is not included in the list, or does not allow both UI and public API access, your IP is automatically added to the list or updated to ensure both UI and API access.
- You cannot change or delete your own IP address from the allowed list.
- If a change in access is made while an IP address is in use, the change will not take affect until the user logs in again.
- When public API access is restricted, the private APIs necessary for UI functionality are not disabled.
- This feature supports the IPV4 protocol but not IPV6. If your system has IPV6 enabled, it must be turned off for IP management to function as expected.
- This feature is not applicable to modifying access for Multi-Org logins or for Multi-Org to Child-Org navigation. However, if Multi-Org users want to generate tokens to use the public APIs, they must have the appropriate public API access included in the **IP-Based Access** allowed list.

Accessing the IP-Based Access Settings

Only the Administrator or Security Engineer roles have configure or read access to the **IP-Based Access** page. To access the page:

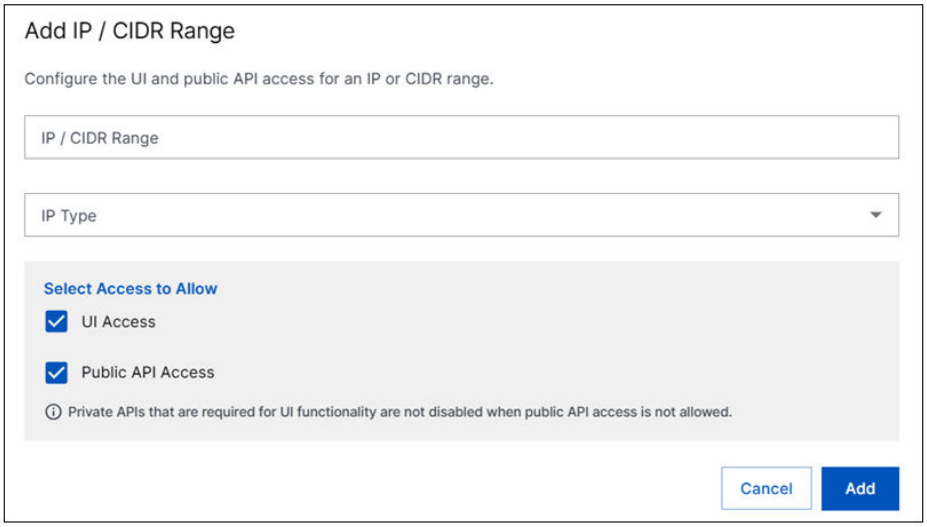
1. Log into the New-Scale Security Operations Platform with your registered credentials.
2. In the left navigation panel, click the **Settings** icon (⚙) at the bottom.
3. Scroll to the bottom of the **Settings** menu to find **Access Control** and select the **IP-Based Access** option. The **IP-Based Access** page opens.



Add an IP or IP Range to the Allowed List

To add a new IP or IP range:

1. On the **IP-Based Access** page, click **Add IP/CIDR Range**. A dialog box opens.

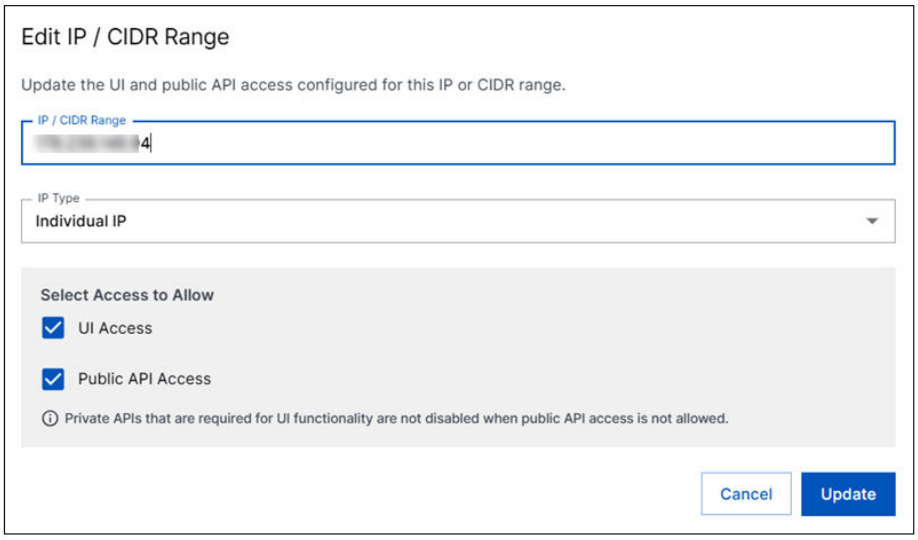


2. Provide information in the following fields:
   - **IP/CIDR Range** – Enter an individual IP address or an IP range using CIDR notation.
   - **IP Type** – Select an option depending on whether you entered an I**ndividual IP** or a **CIDR Range**.
3. Click the appropriate check box to select the access that you want to allow for the IP or IP range you are configuring. Options include **UI Access** and **Public API Access**.
4. Click **Add**. The new IP or IP range is added to the allowed list with the access you configured.

Edit Access for an IP or IP Range in the Allowed List

To edit access for an IP or IP range:

1. On the **IP-Based Access** page, locate the IP or IP range whose access you want to change.
2. On the far right side of the row, click the options menu (⋮) and select **Edit**. The **Edit IP/CIDR Range** dialog box opens.



3. Update the information in following fields as needed:
   - **IP/CIDR Range** – Enter an individual IP address or an IP range using CIDR notation.
   - **IP Type** – Select an option depending on whether you entered an I**ndividual IP** or a **CIDR Range**.
4. Click the appropriate check boxes to update the access that you want to allow for the IP or IP range you are editing. Options include **UI Access** and **Public API Access**.
5. Click **Update**. The updated access is displayed in the allowed list.

> **NOTE**
> Changed access for an IP currently in use may not take affect until the next time the user logs in.

Delete an IP or IP Range from the Allowed List

To delete an IP or IP range:

1. On the **IP-Based Access** page, locate the IP or IP range that you want to remove from the allowed list.
2. On the far right side of the row, click the options menu (⋮) and select **Delete**. The **Delete IP/CIDR Range** dialog box opens.
3. If you are certain you want to delete the IP or IP range, click **Delete**.

Exabeam Nova

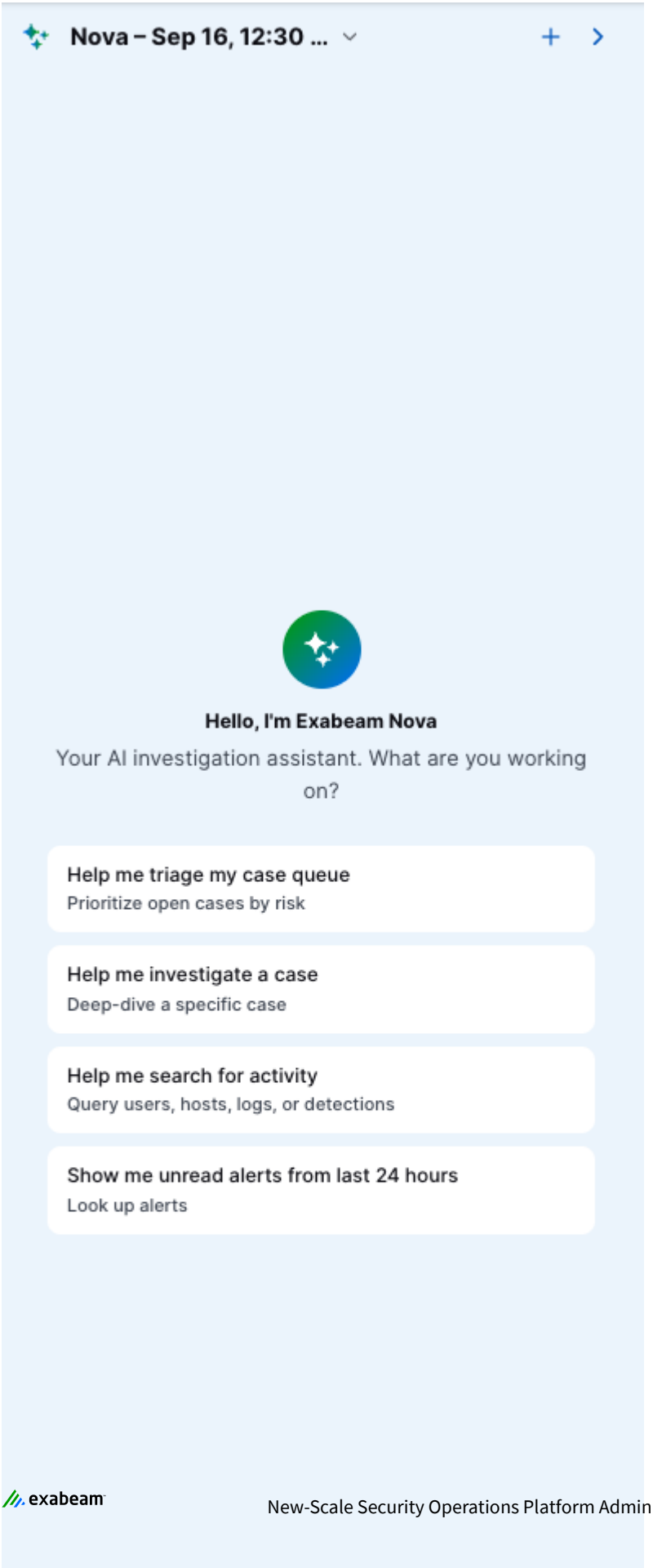
Exabeam Nova is an AI-powered investigation assistant built into the New-Scale Security Operations Platform UI. It enhances security team productivity and insights using natural language processing and generative AI capabilities. These tools elevate expertise in threat detection, investigation, and response (TDIR), making them faster and more precise.

Getting Started

Nova has expanded from a set of page-specific chat assistants into a single, persistent AI sidebar available everywhere in the New-Scale Security Operations Platform UI. Analysts no longer need to navigate to a specific page to access AI assistance.

To open it, click the Exabeam Nova icon in the upper-right corner of the UI. Nova remains available as you move between pages.

Your session context is preserved as you navigate. You can ask Nova follow-up questions, request deeper analysis on a specific entity or timeframe, or direct it to investigate a new angle — all within the same sidebar session. To dock the sidebar, click the **>** icon.


Nova – Sep 16, 12:30 ...
Hello, I'm Exabeam Nova
Your AI investigation assistant. What are you working on?
Help me triage my case queue
Prioritize open cases by risk
Help me investigate a case
Deep-dive a specific case
Help me search for activity
Query users, hosts, logs, or detections
Show me unread alerts from last 24 hours
Look up alerts

Important Considerations

- **Number of Sessions:** You can have up to 5 Nova sessions active at any given time.
- **Session Naming and Options:** Sessions are named by topic and after the first reply. You can rename, pin, and delete sessions by clicking on the session name at the top of Nova.
- **Session Length and Availability:** Sessions are automatically deleted after 30 days of inactivity. Sessions are saved per browser.
- **Docking the Sidebar:** To dock the sidebar and get back to full-screen view, click the **>** icon. To re-open it, click the Exabeam Nova icon again.
- **Scope of Information:** Exabeam Nova only provides responses and information included inside the New-Scale Security Platform.

While Exabeam Nova does not require a specific license, access to related features is dependent on the apps and services you have available through your license entitlement. For example, you can use Exabeam Nova features in Threat Center as long as you have a license that supports Threat Center.

Example Supported Workflows

Alert and Incident Investigation

Nova is designed for analysts actively triaging alerts and investigating incidents. Use Nova to:

- Investigate an alert end-to-end without leaving Threat Center
- Look up entities (users, hosts, IPs) and review associated activity timelines
- Carry investigation context across pages as you pivot between views

Example: "Help me investigate case *xxxxx*"

> **NOTE**
> Refer to the Exabeam MCP Server documentation for additional example queries.

Exabeam Nova AI-Driven Features

In addition to the sidebar, Exabeam Nova is also integrated into the New-Scale Security Operations Platform in the following areas:

Nova in Threat Center

- **Natural Language** – This feature extends the natural language technology available in Search to assist in finding alerts and cases within the Threat Center. For more information, see Use Natural Language to Search for Cases and Alerts in Threat Center.
- **Exabeam Nova Investigation Summary** – Receive an AI-generated summary of a threat described in a case or alert. View Full Summary to start a session in the sidebar panel. The

Exabeam Nova Investigation Summary uses information from the case or alert to provide an overview and recommend next steps. For more information, see Triage Alerts in Threat Center

- **Case Titles in Threat Center** – To ensure clarity and consistency during your threat investigations, Exabeam Nova in Threat Center automatically generates a title that best represents the nature of a case.

Nova in Search

- **Natural Language Prompts in Search** – Effortlessly create complex search queries, in almost any language, without the need for advanced knowledge about the Exabeam Query Language (EQL) syntax and operators. For more information, see Natural Language Search.

Nova in Dashboards

- **Natural Language in Dashboard Visualizations** – Use natural language prompts to describe the data you want to visualize and quickly create dashboard visualizations. Based on this plain language prompt, the measures, dimensions, filters, and chart type are configured automatically. For more information, see Auto-Create a Visualization from a Natural Language Prompt.

Nova in Outcomes Navigator

- **Coverage Summaries** – Quickly summarize your security coverage. The Exabeam Nova Use Case Coverage Summary and Exabeam Nova MITRE ATT&CK Coverage Summary uses security scoring data to provide an overview of trends in your security coverage and recommendations to improve your security coverage.
- **Exabeam Nova Advisor Agent** – Quickly obtain answers about your security posture using a security-trained AI assistant. Prompt the Exabeam Nova Analyst Assistant with a query, and it will generate a natural language response interpreting the MITRE ATT&CK Coverage Summary or Use Case Coverage Summary.

Nova in Threat Detection Management

- **Exabeam Nova Rule Creator** – Use natural language prompts to quickly create and edit correlation rules and analytics rules. Based on a natural language prompt, Exabeam Nova Rule Creator automatically drafts a correlation rule or analytics rule you can further tune with more prompting.

AI Development

Since 2013, Exabeam has leveraged Machine Learning (ML) and Behavioral Analytics as part of the broader AI efforts, establishing over a decade of expertise in these areas. In 2024, Exabeam released generative AI technology with Exabeam Copilot which was built on a foundation of proprietary patents and processes developed internally by our team of experts. Our internal research and development efforts have resulted in unique methodologies for ML event and statistical analytics, ensuring that our AI solutions remain cutting-edge and ahead of the curve.

More recently, Exabeam released agentic AI technology with Exabeam Nova which goes beyond traditional AI experiences. Exabeam Nova acts as a force multiplier, augmenting human analysts

with automation and intelligent insights. It is built directly into the New-Scale Security Operations Platform with no additional cost or complexity.

Personal Data Processing

We understand the importance of protecting personally identifiable information (PII). To ensure confidentiality, Exabeam models do not store PII. We use a third-party large language model (Google Gemini) to process your queries. The data used in these requests is ephemeral, stored only temporarily in memory during processing, and deleted immediately after the request is returned. This ensures your information remains private and secure. Our commitment to data privacy is unwavering, and we take all necessary measures to safeguard sensitive information.

Model Training

To maintain transparency and trust with our customers, Exabeam ensures that customer data is not used to train or fine-tune the large language model (Google Gemini). Our training processes rely exclusively on anonymized data and proprietary internal datasets. This approach preserves the integrity of our AI-driven security solutions while respecting your privacy.

False Positives and Negatives

Exabeam Nova is designed to condense security event data into easy-to-understand language, focusing on important security details. It can also answer follow-up questions and discuss security tech topics, but its accuracy might vary outside these areas.

In the context of threat detection and User and Entity Behavior Analytics (UEBA), false positives and false negatives are important considerations. While AI-driven security solutions are highly effective, these challenges can still arise. At Exabeam, we address them through human oversight, rigorous testing, and continuous improvement, ensuring that our solutions prioritize accuracy and precision. By focusing on these efforts, we build trust and deliver reliable results for our customers.

Always double-check responses for crucial decisions.

NOTE

Your queries and data will only be retained temporarily and won't be used for AI training.
Exabeam is actively improving Exabeam Nova and welcomes feedback.

Policies and Support

At Exabeam, we believe in transparency, accountability, and fairness when it comes to our AI practices. To support these values, we're committed to keeping customers informed about updates and improvements to our AI capabilities. Stay up-to-date with our latest news, releases, and best practices through our release notes and dedicated support channels.

Monitoring

The Exabeam Security Operations Platform provides valuable tools for monitoring your audit logs and system health.

To view the current and historical runtime status of all Exabeam services by region, visit the Exabeam Status page (https://exabeam.statuspage.io/).

For visualizations of the key metrics for monitoring data ingestion, system health, license consumption, and security budget needs, see Service Health and Consumption.

In the Search app, you can view audit logs for a specific time period and filter by log types. These features help you track activities and ensure compliance with regulations like GDPR. For more information, see Audit Logs.

Service Health and Consumption

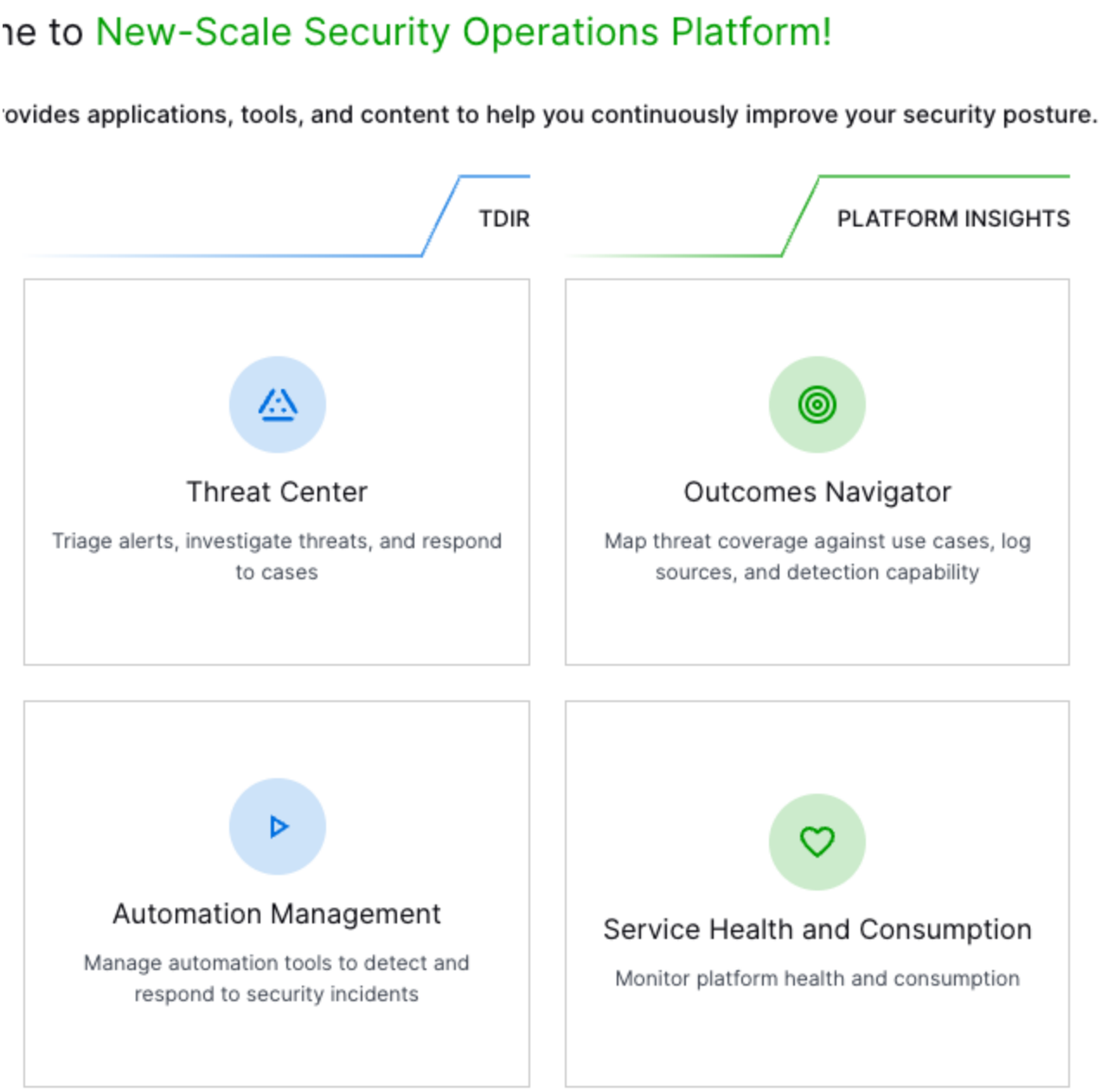
Service Health and Consumption dashboards display visualizations of the key metrics for monitoring data ingestion, system health, license consumption, and security budget needs. The dashboards are available to all Exabeam Security Operations Platform users.

Use Service Health and Consumption dashboards to:

- Monitor health trends and consumption impacts of new data sources.
- Receive health alerts.
- Make informed responses to license consumption warnings.
- Understand overage notifications.
- Monitor retention needs.
- Prioritize service needs.

> **NOTE**
> The data displayed in Service Health and Consumption dashboards is not in real-time. The dashboards are updated daily after midnight with data from the previous day.

To access Service Health and Consumption, click the tile on the Exabeam Security Operations Platform home page.



For more information, see the Service Health and Consumption Guide.

Audit Logs

Audit logs represent user, object, or setting events in your organization. Specific events related to all users identified in your New-Scale Security Operations Platform are logged, including activities within the user interface and configuration activities. This is especially useful for reviewing activities for audits (for example GDPR).

NOTE

Internal audit logs of activity performed by Exabeam employees supporting customer environments are not available for customer consumption.

Exabeam stores all audit logs and provides a query interface in Search that you can use to find and export audit logs.

NOTE

For information on setting retention limits for your audit logs, see Global Log Retention in the Exabeam Search Guide.

Types of Audit Logs

The following table displays the types of events captured in the audit log for the New-Scale Security Operations Platform by feature area. Each event also has an associated activity type—as defined in the common information model—that references additional, granular fields that you can use to search your audit logs. For each event, the activity type is displayed in parentheses.

Feature	Events
API Settings	• API key creation (key-create) • API key modified (key-write) • API key deleted (key-delete)
Authentication	• EULA signed (file-write) • Logged in (app-login)
Cloud Collectors	• Log source created (log_source-add) • Log source modified (log_source-modify) • Log source deleted (log_source-remove) • Log source enabled (log_source-enable) • Log source disabled (log_source-disable) • Log account created (log_account-create) • Log account modified (log_account-modify) • Log account deleted (log_account-delete)
Context Management	• Context table created (context_table-create) • Context table deleted (context_table-delete) • Context table modified (context_table-modify)
Correlation Rules	• Rule created (rule-create) • Rule modified (rule-modify) • Rule deleted (rule-delete) • Rule enabled (rule-enable) • Rule disabled (rule-disable)

Feature	Events
Dashboards	• Dashboard created (dashboard-create) • Dashboard deleted (dashboard-delete) • Dashboard downloaded (dashboard-download) • Dashboard duplicated (dashboard-create) • Dashboard exported (dashboard-export) • Dashboard imported (dashboard import) • Dashboard modified (dashboard-modify) • Dashboard published (dashboard-publish) • Dashboard schedule created (scheduled_task-create) • Dashboard schedule deleted (scheduled_task-delete) • Dashboard schedule modified (scheduled_task-modify) • Folder created (folder-create) • Folder deleted (folder-delete) • Folder modified (folder-modify)
Dashboard Visualizations	• Visualization created (visualization-create) • Visualization deleted (visualization-delete) • Visualization downloaded (visualization-download) • Visualization duplicated (visualization-create) • Visualization exported (visualization-export) • Visualization imported (visualization-import) • Visualization modified (visualization-modify) • Visualization published (visualization-publish) • Folder created (folder-create) • Folder deleted (folder-delete) • Folder modified (folder-modify)
Log Stream	• Event enricher created • Event enricher deleted • Event enricher disabled • Event enricher enabled • Event enricher force updated • Event enricher imported • Event enricher modified • Event enricher reordered • Parser created (parser-create) • Parser deleted (parser-delete) • Parser disabled (parser-disable) • Parser enabled (parser-enable) • Parser imported (parser-import) • Parser modified (parser-modify)

Feature	Events
Role Settings	• Custom role created (role-create) • Custom role modified (role-modify) • Custom role deleted (role-delete)
Search	• Log search (log-search) • Log download (log-download) • Log export (log-export)
SSO Settings	• Single sign-on deleted (configuration-delete) • Single sign-on created (configuration-create) • Single sign-on modified (configuration-modify)
Threat Center	• Alert created (alert-create) • Alert modified (alert-modify) • Alert read (alert-read) • Case created (case-create) • Case modified (case-modify) • Case read (case-read) • Detection grouping rule created (detection_group_rule-create) • Detection grouping rule deleted (detection_group_rule-delete) • Detection grouping rule disabled (detection_group_rule-disable) • Detection grouping rule enabled (detection_group_rule-enable) • Detection grouping rule modified (detection_group_rule-modify) • Case closed supporting reason setting modified (custom-config-modify)
User Settings	• User invited (user-invite) • User invitation canceled (user-invite-cancel) • User activated (user-enable) • User deactivated (user-disable) • User modified (user-modify) • User password reset (user-password-reset) • User deleted (user-delete)

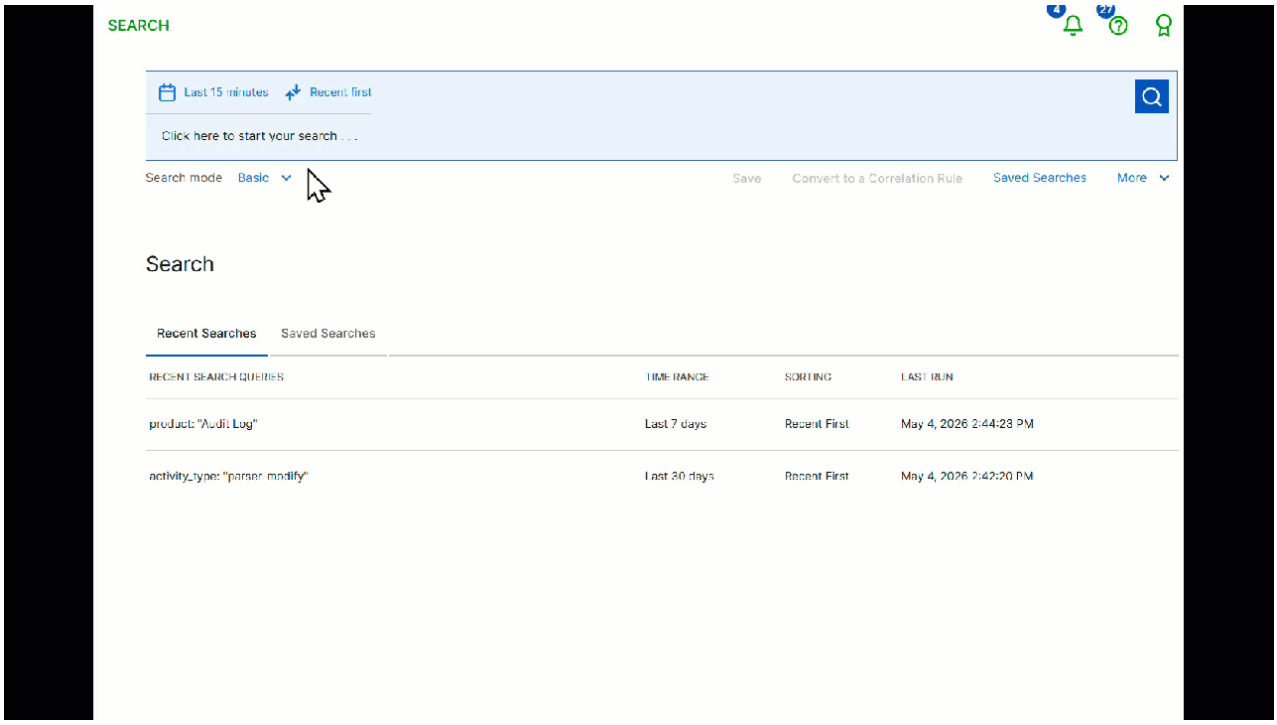
Audit Log Visibility

To access audit logs, use the Search app available from the New-Scale Security Operations Platform. From Search, you can view all audit logs over a specific time period and search for specific audit log types. For ease of use, an **Audit Logs** tab is accessible in the Search query builder. For information about using the **Audit Logs** tab, see Basic Search in the Search Feature Guide.

In the common information model, all audit logs are assigned to the Exabeam vendor and Audit Log product.

For example, to search for events related to case modification events in Threat Center, use the following parameters in your Search query:

- vendor: **`Exabeam`**
- product: **`Audit Log`**
- activity_type: **`case-modify`**



Export Your Exabeam Data

Easily and quickly deliver your Exabeam data to a Google Cloud Storage (GCS) bucket.

You may consider exporting your Exabeam data if you no longer want to store your data with Exabeam; for legal purposes; or if your Exabeam subscription is ending and you want to save your data before your environment is destroyed.

If you have a New-Scale Security Operations portfolio license, Exabeam Security Operations portfolio license, or Fusion license, Exabeam can help you export your Search logs to a Google Cloud Storage (GCS) bucket. Exabeam currently exports Search logs only. This service is available with an additional purchase. If your Exabeam subscription is ending, it's best that you purchase the service 30 days before your subscription ends to ensure a sufficient amount of time to transfer all your data.

1. To notify Exabeam that you would like to export your Exabeam data to a GCS bucket, create a support case in the Exabeam Community. In the case, specify a contiguous time frame of logs you'd like exported; for example, last 30 days or last 16 months.
   After you create the support case, you're asked to purchase the PS-DATA-EXPORT-1-TB SKU. If your Exabeam subscription is ending, it's best that you purchase the SKU 30 days before your subscription ends to ensure a sufficient amount of time to transfer all your data.
2. Create a GCS bucket. Keep in mind:
   - You can give the bucket any name that meets the requirements; for example, <your organization>-exa-logs.
   - The GCS bucket location must be the region where your Exabeam environment is deployed. You can infer the region from your Exabeam instance URL:

Exabeam Instance URL	GCS Bucket Location
<instance>.exabeam.cloud	us-west1
<instance>.eu.exabeam.cloud	europe-west3
<instance>.use1.exabeam.cloud	us-east1
<instance>.au.exabeam.cloud	australia-southeast1
<instance>.jp.exabeam.cloud	asia-northeast1
<instance>.ca.exabeam.cloud	northamerica-northeast1
<instance>sg.exabeam.cloud	asia-southeast1
<instance>.euw6.exabeam.cloud	europe-westt6
<instance>.sa.exabeam.cloud	me-central2
<instance>uk.exbeam.cloud	europe-west2

     For guidance on which location to select, contact your Exabeam technical support team through the support case you created.
3. Grant the Exabeam service account for Google Cloud Platform specific permissions to your GCS bucket:

- In **New principals**, enter *exabeam-util@ops-dist-mgmt.iam.gserviceaccount.com*, the identifier for the Exabeam service account.
- Under **Assign roles**, grant the Exabeam service account the following roles:
  - Storage Object User (`roles/storage.objectUser`)
  - Storage Object Creator (`roles/storage.objectCreator`)

4. In the support case, provide the name of the GCS bucket you created. After receiving the GCS bucket name, Exabeam begins exporting your data into the GCS bucket. Each week of data is separated into a folder. The folder is named event_<YYYY>_<DD>, where *YYYY* is the year and *DD* is the number of the week in that year.
   The amount of time the export process takes depends on the amount of data you're exporting. After the export is complete, you're notified in the support case.