Bundles Best Practices Guide

Published: 2018-02-06

If you have a bundle that you think might be useful to other ExtraHop users, we encourage you to upload the bundle to the ExtraHop Solution Bundles Gallery. Bundles in the gallery typically focus on monitoring a specific type of activity. For example, the Ransomware Bundle is designed to identify potential ransomware attacks.

If you upload a bundle to the ExtraHop Solution Bundles Gallery, it is important to inspect each object in your bundle to make sure those objects don't include any information that is sensitive to your organization. The names and descriptions of each object should be informative and well written. Finally, it is important to include all dependencies for each object. Dashboards, pages, alerts, and record queries often rely on custom metrics and applications, which are created through triggers.

Before uploading a bundle, we recommend that you review the settings for each of your bundle objects and apply the best practices guidelines provided in each of the following sections.

- Alerts - remove alert notifications, make note of any trigger dependencies, and make sure all description fields are informative.
- Device Groups - remove all machines that might not be relevant in other environments from device groups and make sure all description fields are informative.
- Dashboards - make note of all trigger dependencies and make sure all description fields are informative.
- Custom Pages - make note of all trigger dependencies and make sure all description fields are informative.
- Record Queries - make note of all record format dependencies and make sure all description fields are informative.
- Record Formats - make note of all trigger dependencies and make sure all description fields are informative.
- Triggers - make sure all trigger-dependent objects are defined and comments are informative.

Including alerts in bundles

Alerts are often configured with environment-specific settings. For example, an alert might be configured to send notifications to your company's email addresses. These configurations must be removed from alerts before including the alert in a bundle.

Check the following alert settings before including an alert in a bundle. For more information about modifying these settings, see the Configuring alerts section in the ExtraHop Web UI Guide.

Settings	Notes
Name	Type an alert name that is descriptive and does not contain sensitive information.
Author	Type an alert author that is appropriate for a general audience and does not contain sensitive information. For example, you might want to type your company name as the author, such as ExtraHop Systems.
Metric	If the alert references a custom application or metric, your bundle must also include the trigger that creates the custom application or metric.

Settings	Notes
Email notification groups	Remove all email groups from this field. Including notification groups in bundles can cause emails to be sent to the wrong recipients.
Additional email addresses	Remove all email addresses from this field. Including email addresses in bundles can cause emails to be sent to the wrong recipients.
Description	Type an alert description that provides useful information, such as the conditions that generate this alert, and does not contain sensitive information.
Assignments	Deselect the Assign to all checkbox. Bundles do not capture assignments to individual IP addresses. However, if an alert is assigned to a device group, the assignment will be captured in the bundle.

Including device groups in bundles

Although you can include both static and dynamic device groups, dynamic groups are more common components of bundles. Static groups rely on static IP addresses, which are unlikely to be relevant across multiple environments. If you include device groups in your bundle, make sure the device group does not contain any sensitive information, such as internal IP addresses or subnets.

Note: Assignments to device groups are captured in a bundle; however, the device group must also be included in the bundle.

Check the following device group settings before including a device group in a bundle. For more information about modifying these settings, see the Device Groups section in the ExtraHop Web UI Guide.

Settings	Notes
Name	Type a group name that is descriptive and does not contain sensitive information.
Author	Type an author that is appropriate for a general audience and does not contain sensitive information. For example, you might want to type your company name as the author, such as ExtraHop Systems.
Criteria	For dynamic device groups, remove any environment-specific configurations. For example, remove references to internal IP addresses or subnets.
Devices	For static device groups, remove any environment-specific configurations. For example, remove any internal IP addresses.

Including dashboards in bundles

Dashboards are the easiest way to display sets of metrics. However, if a dashboard in a bundle includes custom metrics and applications that were generated through a trigger, you must include that triggers in the bundle.

Dashboards can contain sensitive information in their metadata. It is important that you remove this sensitive information before including the dashboard in a bundle. It is also a good idea to review your dashboard to make sure that each component is labeled well.

Check the following dashboard settings before including them in a bundle. For more information about modifying these settings, see the Dashboards section in the ExtraHop Web UI Guide.

Settings	Notes
Dashboard Title	Type a dashboard title that is descriptive and does not contain sensitive information.
Dashboard Author	Type a dashboard author that is appropriate for a general audience and does not contain sensitive information. For example, you might want to type your company name as the author, such as ExtraHop Systems.
Dashboard Description	Type a dashboard description that provides useful information, such as the purpose of the dashboard, and does not contain sensitive information.
Dashboard Permalink	Include random characters in the permalink to ensure that the permalink is not already in use on another ExtraHop appliance. If a dashboard from a bundle includes a permalink that is already in use on the system, the dashboard from the bundle will be assigned a new permalink when the bundle is applied, which means that any links to that dashboard from another dashboard will not work.
Widget Title	Type widget titles that are descriptive and do not contain sensitive information.
Widget Sources and Metrics	If widget sources or metrics include custom applications or metrics, your bundle must also include the trigger that creates those custom applications or metrics.
Widget Details	Remove any environment-specific configurations and sensitive information from Widget Details. For example, a widget might be configured to display only results relating to a given hostname.
Text Box Widgets	Type descriptions in text box widgets that are well written and informative.

Including custom pages in bundles

Custom pages can contain sensitive information in their metadata. It is important that you remove this sensitive information before including the page in a bundle. It is also important to review the page to make sure everything is labeled well and is easy for other users to understand.

Check the following custom page settings before including a custom page in a bundle. For more information about modifying these settings, see the Custom Pages section in the ExtraHop Web UI Guide.

Settings	Notes
Page Title	Type a page title that is descriptive and does not contain sensitive information.
Page Author	Type a page author that is appropriate for a general audience and does not contain sensitive information. For example, you might want to type your company name as the author, such as ExtraHop Systems.
Page Description	Type a page description that provides useful information, such as the purpose of the page, and does not contain sensitive information.
Chart Title	Type chart titles that are descriptive and do not contain sensitive information.

Including record queries in bundles

Record queries are often configured to search on environment-specific resources, such as subnets or hostnames. Remove these internal references before uploading a record query in a bundle. Record queries can also reference record types that are defined in custom record formats; if a record query is dependent on a custom record format, the custom record format must be included in the bundle.

Check the following settings before including a record query in a bundle. For more information about modifying these settings, see the Record Queries section in the ExtraHop Web UI Guide.

Settings	Notes
Record Type	If the record type is defined in a custom record format, your bundle must also include that custom record format.
Filters	Remove any references to internal resources or sensitive information from filters.
Name	Type a name that is descriptive and does not contain sensitive information.
Description	Type a record query description that provides useful information, such as what information is captured in the query, and does not contain sensitive information.

Including record formats in bundles

Custom record formats define record types that can be referenced in queries. If you include a record query that is dependent on a custom record format, you must include the record format in the bundle.

If a custom record format references a custom record type, you must include the custom record format and the trigger that defines the custom record type in the bundle. Record formats can also contain sensitive information in their metadata.

Check the following properties of the Schema on Read settings of a record format before including the record format in a bundle. For more information about modifying these settings, see the Record formats section in the ExtraHop Web UI Guide.

Property	Notes
description	Type a record format description that provides useful information, such as what information the format displays, and does not contain sensitive information.
name	Type a name that is descriptive and does not contain sensitive information.
display_name	Type a display name that is descriptive and does not contain sensitive information.
meta_types	Set the meta_types field appropriately to avoid confusion. For example, a timestamp will not be formatted like a timestamp unless the meta_type is specified.

Including triggers in bundles

Triggers are often included in bundles to create custom metrics and applications, which are often required by other bundle objects like dashboards and alerts. After you have identified all dependencies from other bundle objects, you must make sure that you include the related triggers to support those objects.

Triggers can be configured to act on environment-specific traits or reveal sensitive information in the comments. Before including a trigger in a bundle, make sure that these configurations have been removed.

Check the following trigger settings before including a trigger in a bundle. For more information about modifying these settings, see the Triggers section in the ExtraHop Web UI Guide.

Settings	Notes
Name	Type a name that is descriptive and does not contain sensitive information.
Author	Type a trigger author that is appropriate for a general audience and does not contain sensitive information. For example, you might want to type your company name as the author, such as ExtraHop Systems.
Description	Type a trigger description that provides useful information, such as which metrics the trigger creates, and does not contain sensitive information.
Enable Debugging	Deselect the Enable Debugging checkbox.

Settings	Notes
	Make sure that a trigger has been debugged before sharing the trigger with others.
Trigger Script	• Define all dependencies from other bundle objects. • Remove any references to internal resources, such as hostnames or subnets, and remove sensitive information from the comments. • Explain the functionality of each section of the trigger in the comments.
Assignments	Deselect the Assign to all checkbox. Bundles do not capture assignments to individual IP addresses. However, if an trigger is assigned to a device group, the assignment will be captured in the bundle.