Bundles Best Practices Guide

Published: 2021-08-27

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 Active Directory Bundle is designed to monitor Active Directory activity.

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, detection formats, 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.
- Applications - make note of all device group and alert dependencies and make sure all description fields are informative.
- Dashboards - make note of all trigger dependencies and make sure all description fields are informative.
- Detection Formats - make note of all trigger dependencies.
- Dynamic Device Groups - remove all criteria that might not be relevant in other environments from dynamic device groups 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 these settings, see Alerts.

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 applications in bundles

Applications contain multiple references to other components. Bundles that include an application must also include any custom dynamic device group or alert configuration that is referenced by the application.

If you add an application to a bundle, make sure the application and all of the device groups and alerts it references do not contain any sensitive information, such as internal IP addresses or subnets. Check the following application settings before including an application in a bundle. For more information about modifying these settings, see Create an application.

Settings	Notes
Display name	Type an application name that is descriptive and does not contain sensitive information.
Application ID	Type a unique, permanent ID that is appropriate for a general audience and does not contain sensitive information. After the application is saved, the ID cannot be modified or deleted.
Site	If you are creating an application on a Command appliance or Reveal(x) 360, the selected site is not included when you add the application to a bundle. Site IDs are specific to your environment and are automatically removed when an application is exported in a bundle.
Sources	Your bundle must include any dynamic device groups that are referenced by your application. Do not include applications that reference individual devices.
Alerts	If an application has alerts assigned to it, your bundle must also include the assigned alert.

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 these settings, see Dashboards.

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 specified on another ExtraHop system. If a dashboard from a bundle includes a permalink that is already specified 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 detection formats in bundles

Detection formats enhance custom detections by specifying friendly display names and adding MITRE techniques to the detection.

Bundles that include a detection format must also include the trigger that defines the custom detection associated with the detection format. If you add a detection format to a bundle, make sure the detection type ID it references matches the detection type ID in the commitDetection function of the associated trigger.

Check the following detection format settings before including an application in a bundle. For more information about modifying these settings, see Create a custom detection and Create a detection format.

Settings	Notes
Display Name	Type a display name for the custom detection that is descriptive and does not contain sensitive information.
Detection Type ID	Type the detection type ID value that is referenced in the commitDetection function of the custom detection trigger.
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.
MITRE Technique	Select one or more MITRE techniques that you want to link to the detection.

Including device groups in bundles

Bundles can include dynamic device groups, but not static device groups. Static device groups rely on static IP addresses and are unlikely to be relevant across multiple environments. If you include a dynamic device group 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 these settings, see Create a dynamic device group.

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	Remove any environment-specific configurations. For example, remove references to internal IP addresses or subnets.

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 Record Queries.

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 Create a custom record format.

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 these settings, see Triggers.

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 debug log	Deselect the Enable Debugging checkbox. 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.
Advanced Options	Deselect the **Assign to all devices** 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.