

Schedule a dashboard report about Active Directory

Published: 2024-04-03

Active Directory is a critical application that can be time-consuming to monitor and troubleshoot. In the ExtraHop Bundle for Active Directory, we've compiled dashboards that provide a comprehensive top-level view of Active Directory data that makes it easy to watch for potential problems.

To help you easily monitor changes, you can schedule a report for your Active Directory dashboard. A dashboard report delivers a PDF file of dashboard data to any email recipient you specify.

In this walkthrough, we'll show you how to download and apply the bundle to your ExtraHop system, and how to schedule a bi-weekly dashboard report for your stakeholders about the health of your Active Directory environment.



Note: You can only schedule reports from a console.

Prerequisites

- You must have access to a console.
- You must have a user account with **limited or full write privileges** [↗](#) to create a dashboard

Retrieve the ExtraHop Active Directory Bundle

Before you can upload the Active Directory Bundle to your ExtraHop system, you must retrieve the bundle from the ExtraHop Solution Bundle Index.

1. Go to the [Active Directory bundle page](#) [↗](#).
2. If you have not already logged in to the ExtraHop website, click **Login** in the right pane and then specify a valid username and password.
3. In the How to Obtain this Bundle section, click the link to create a service request to retrieve the bundle.

Upload and apply the Active Directory bundle to your ExtraHop system

In the following steps, you will upload and install the bundle you downloaded from the ExtraHop website on your console.

1. Log in to the console through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon in the upper right corner.
3. Click **Bundles**.
4. On the Bundles page, click **Upload Bundle**.
5. Click **Choose File**, and then select the Active Directory .json file that you downloaded in the previous section.
6. In the Install Options section, select the following checkboxes:
 - a) Select the site where you want to install the bundle.
 - b) Select the **Apply 9 included assignments** checkbox.


This option assigns the bundle to the metric sources included with the bundle. In most cases, it is best to apply the default assignments.
 - c) Select the **Overwrite existing content** checkbox.

This option overwrites any objects that have the same name as objects in the bundle. If you have existing system objects with the same name that you want to preserve, you must rename those objects to avoid overwriting them with the objects in the bundle.

7. Click **Install**, and then click **Done**. Your bundle is installed and listed in the table!

Configure the Active Directory triggers

In the following steps, you will enable and configure a trigger to mirror the lockout and privileged account settings in your Active Directory environment.

1. Click the System Settings icon .
2. Click **Triggers**.
3. Enable each trigger in the Active Directory v4 bundle by completing the following steps.
 - a) In the table, click a trigger name beginning with **AD**.
 - b) Clear the **Disable Trigger** checkbox to enable the trigger.
 - c) Click **Save and Close**.
4. Modify specific fields in the Kerberos trigger to match your Active Directory accounts by completing the following steps.
 - a) In the table, click **AD: Kerberos** and then click the **Editor** tab.
 - b) Set the `failedLoginDisableInterval` constant to the match the value of the `Reset account lockout counter after policy` setting in your Active Directory environment.
 - c) Set the `accountLockoutDuration` constant to the value of the `Account lockout duration policy` setting in your Active Directory environment.
 - d) Add the complete names of any privileged accounts in your environment to the `priv_names` list and any partial matches to the `priv_regex` list. Examples of privileged accounts include:

```
var priv_names = {'admin', 'administrator', 'root', 'ss', 'sys',
                  'sysadmin', 'informix'}
```

- e) Click **Save and Close**.

Create, schedule, and save a dashboard report

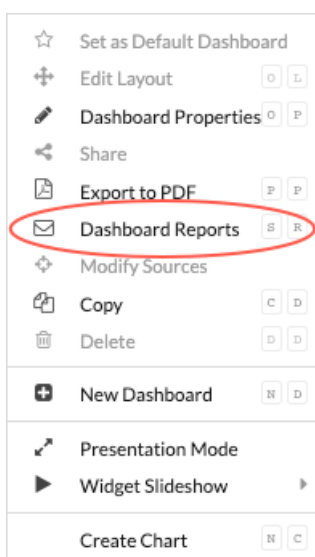
In the following steps, we'll show you how to schedule a weekly dashboard report that runs on Mondays and Thursdays at 7:00 am. We'll also show you how to send the dashboard report to a colleague, for example, someone who manages authentication services at your company.

1. Click **Dashboards** at the top of the page, and then click the **Active Directory Overview** dashboard in the left pane.



Note: Each report can only link to one dashboard. You can select any dashboard that you own or has been shared with you to create a report.

2. In the upper right corner of the dashboard page, click the command menu and then select **Dashboard Reports**.



A Dashboard Reports page appears that displays all the reports stored on the console. If this is your first report, this page will be empty.

3. In the upper right corner, click **Create**.
4. In the Report Name field, the name of the dashboard is displayed. Let's remove the host information of the connected site from the title, as shown in the following figure.

Create Dashboard Report

Properties

Report Name

Description

Owner

Report Contents

5. Let's jump down the page to set the dashboard report schedule. In the Time Interval section, select the time frame of dashboard data that you want to display in the report PDF file. For this walkthrough, let's report on the last 4 days of data. Click the **Last** field and then type 4.

Time Interval

 **Note:** For more information on how to configure each field, see [Create a scheduled report](#).

6. In the Report Frequency section, set the email delivery schedule. For this walkthrough, we'll send a weekly report on two different days at 7:00 am. Complete the following steps:
 - a) Click the **At** drop-down list and select **07:00**. This setting schedules the delivery of the report for 7:00 am.

The system time that is set for your console determines the time zone that is displayed when configuring your report. For more information about configuring the time zone for your ExtraHop system through the ExtraHop Administration settings, see [Configure the system time](#).

- b) Select the checkboxes next to M and Th to schedule the delivery of the report for Monday and Thursday.

Report Frequency

Hourly Daily Weekly

At ✕

On M T W Th F S Su

[Add Schedule](#)

7. To add your colleague's email address, scroll down to the Send To section. Click the Email Addresses field and type the email.


Send Email

Notification Groups

Select an item...

Recipients

sarah@example.com ✕

 **Note:** The ExtraHop system does not store email addresses for ExtraHop user accounts. However, if your ExtraHop Reveal(x) Enterprise system is [configured with an email group](#), you can select a notification group to email. Reveal(x) 360 does not support email notification groups.


8. Optional: Click **Send Now** to send a test email to the recipient.
9. Click **Done**. Your dashboard report now appears on the Dashboard Reports page, as shown in the following figure.


Dashboard Reports						
Report Name ▾ = ▾		7 results				
<input type="checkbox"/>	Report ID ↓	Report Name	Owner	Report Contents	Status	Description
<input type="checkbox"/>	22	Active Directory	Default	Active Directory	● Enabled	–
<input type="checkbox"/>	21	System Usage	Default	System Usage	● Enabled	–
<input type="checkbox"/>	20	New Devices	Default	New Devices	● Enabled	–

10. In the bottom right corner of the page, click **Done** again to return to your dashboard.

Your colleague will receive an similar email to the following example below with the attached PDF report file.

ExtraHop Report: Active Directory Inbox x 🖨️ 📧

 **ExtraHop** <no-reply@stage.notify.extrahop.com> 2:33 PM (0 minutes ago) ☆ ↶ ⋮
to me ▾

 **ExtraHop** Reveal(x) 360


Active Directory

June 25, 2023 17:32 (UTC-04:00) to June 29, 2023 17:32 (UTC-04:00)

Report Owner: Default


Contact the report owner to modify the content or frequency of this scheduled report. If you need further assistance or think you received this report in error, contact your ExtraHop administrator.

One attachment • Scanned by Gmail 🔄



PDF Active_Directory_...

↶ Reply
↷ Forward

 **Note:** In the top right corner of the PDF file, click the **View report on ExtraHop** link to access the dashboard that generated the report. For ExtraHop users, the link opens the console and sets the dashboard to the time interval listed in the report. You can now investigate metrics in more detail from the dashboard.

Add another email address to a saved report

If you want to make changes to a dashboard report, you can access it at any time. Let's add the email address for a new stakeholder to our Active Directory report.

1. From the dashboard page, click the command menu in the upper right corner, and then select **Scheduled Reports**.
2. In the **Report Name** field, click the title of your report.
3. Scroll down to the Send Email section.
4. Click the Email Addresses field.
5. Type a comma after the first email address and then type the new email address.

EMAIL ADDRESSES

sarah@example.com, alex@example.com

6. Click **Save**.
7. Click **Done** to return to your dashboard. The scheduled report for this walkthrough is now updated.

Next steps

Over time, you might want to pause the delivery of the report by [disabling a dashboard report](#). Or you might want to make changes to your dashboard to display different charts or data. For more information about changing a dashboard, check out these resources:

- [Edit a dashboard layout](#)
- [Using Dashboards to Organize and Present Data](#) (Online training)
- [Edit a dashboard chart with the Metric Explorer](#)
- [Edit a text box widget](#)

Here are additional walkthroughs about building dashboards from scratch to monitor protocol metrics:

- [Monitor website performance in a dashboard](#) (Walkthrough)
- [Monitor database health in a dashboard](#) (Walkthrough)
- [Monitor DNS errors in a dashboard](#) (Walkthrough)