

Schedule a report about Active Directory

Published: 2018-07-07

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 scheduled report delivers a PDF file of dashboard data to any email recipient you specify.

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



Note: You can only schedule reports from a Command appliance.

Prerequisites

- You must have access to an ExtraHop Command appliance
- You must have a user account with [limited or full write privileges](#) to create a dashboard

Download the ExtraHop Active Directory Bundle

Before you can upload the Active Directory Bundle to your appliance, you must download the bundle from the ExtraHop website.

1. Download the [Active Directory bundle](#).



Note: This walkthrough is based on the Active Directory v4 bundle.





Note: This walkthrough is based on the Active Directory v3 bundle.

2. If you have not already logged into the ExtraHop website, click **Login** in the right pane and then specify a valid username and password.
3. Click **Download Now**.
4. Save the .json file to a location on your local machine.

Upload and apply the Active Directory bundle to your Command appliance

In the following steps, you will upload and install the bundle you downloaded from the ExtraHop website on a Command appliance.


1. Log into the Web UI of a Command appliance.
2. Click the System Settings icon  in the upper right corner.
3. Click **Bundles**.
4. On the Bundles page, click **Upload**.
5. In the Load Bundle dialog box, click the **Choose File** button, and then select the Active Directory .json file that you downloaded in the previous section.
6. Click **Upload**.
7. In the lower right section, select the **Apply 9 included assignments** checkbox.
8. From the Existing objects drop-down menu, select **Overwrite**.

 **Warning:** Selecting this option will overwrite any objects, such as dashboards, on your system that have the same name as objects in the bundle. If you previously applied this bundle and modified its objects, any modifications will be overwritten.

9. Click **Apply** to launch the Bundle Node Selection dialog box.
10. In the Bundle Node Selection dialog box, select the Discover appliances that you want to add Active Directory dashboards for.
11. Click **OK**. The bundle is applied to the Command appliance. This step might take a minute. A success message displays when the bundle is applied.
12. Click **OK** to exit the Bundle Import Status dialog box.
13. Click **OK** to exit the View Bundle dialog box and return to the main Bundle page. 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.

The following example shows some common privileged accounts.



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

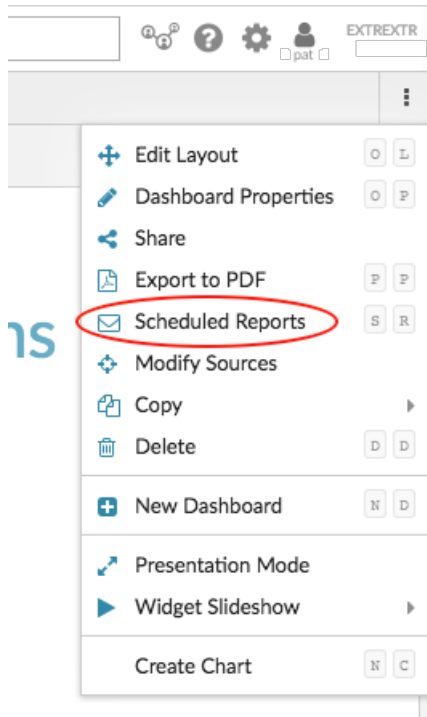
- e) Click **Save and Close**.

Create, schedule, and save a report

In the following steps, we'll show you how to schedule a weekly report that runs on Mondays and Thursdays at 7:00 am. We'll also show you how to send the 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 click **Scheduled Reports**.



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

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

Edit Report - Active Directory Overview

Report Enabled

REPORT NAME

Active Directory Overview

DESCRIPTION

Overview of Active Directory metrics for Kerberos authentication, Group Policy, LDAP, and DNS service resource records.

REPORT ON

Dashboard: Active Directory Overview (10.10.10.3)

5. Let's jump down the page to set the 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

LAST

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 Command appliance determines the time zone that is displayed when configuring your report. For more information about configuring the time zone for your appliance through the ExtraHop Admin UI, 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 another time](#)

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 To

NOTIFICATION GROUPS

EMAIL ADDRESSES

Note: If you want to receive a copy of the report, add your email address to this field, separated by a comma. The ExtraHop system does not store email addresses for ExtraHop user accounts.

8. Click **Done**. Your scheduled report now appears on the Scheduled Reports page, as shown in the following figure.

? ×

Scheduled Reports

Create Report

Any Column =
Copy Delete Enable Disable

☐	Report ID	Report Name	Contents	Status	Owner
☐	1	Active Directory Overview	Active Directory Overview (10.10.10.3)	■ ENABLED	pat

Displaying 1 - 1 of 1
⏪ 1 ⏩

Done

9. 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.

reports+my-eca@extrahop.com 10:30 AM (3)
to me

Active Directory Overview


ExtraHop Report Details

The report contains data from the following time range:
January 05, 2018 10:30:30 to January 09, 2018 10:30:30 UTC-08:00

The report is owned by the ExtraHop user: pat


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.




 **Tip:** ExtraHop users viewing the PDF can click the **View report on ExtraHop** link to open the Command appliance and investigate more metrics.

Add another email address to a saved report

You can make changes to your scheduled reports 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 click **Scheduled Reports**.



Note: Scheduled reports are only available from the command menu on a dashboard page. Legacy reports, which are deprecated, are available from the System Setting menu .

2. In the Report Name column, click the title of your report.
3. Scroll down to the Send To 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 scheduled 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)