Getting started with Aman Dark Web Monitoring

Aman - Dark Web Monitoring · https://www.aeserver.com/support/getting-started-with-aman-dark-web-monitoring/

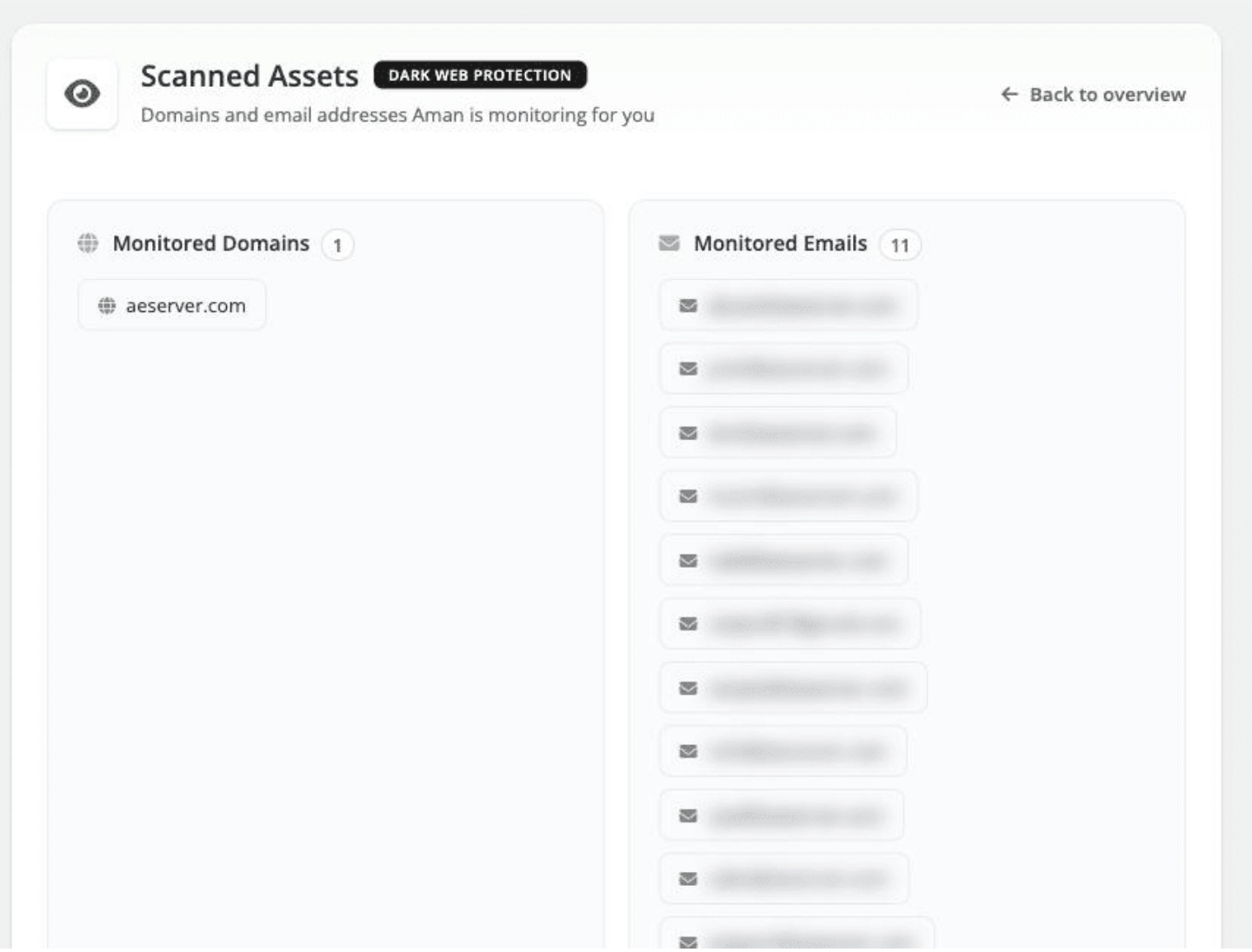
Getting started with Aman means telling it what to watch. This guide shows you how to review and update your monitored domains and email addresses, and what to expect from your first report.

Step 1. Open your Aman dashboard

Sign in to your AEserver account, open **My Products and Services**, and select your Aman service. You will land on the Aman dashboard, which shows your plan, renewal date, number of monitored assets and service status.

Step 2. Review what is being monitored

Select **Scanned Assets**. This page lists the domains and email addresses Aman is monitoring for you, grouped as **Monitored Domains** and **Monitored Emails**, each with a count.



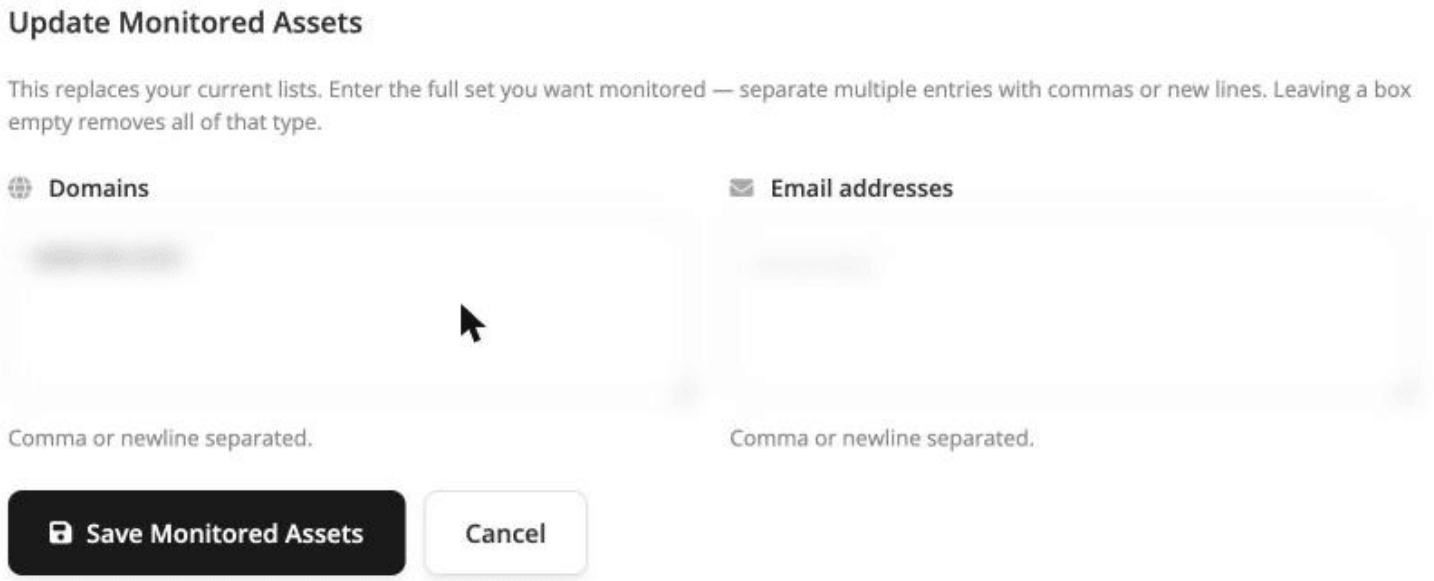
The Scanned Assets page: your monitored domains and email addresses.

Step 3. Update your monitored assets

Below the lists you will find **Update Monitored Assets**, with a box for domains and a box for email addresses. Enter your entries separated by commas or new lines, then select **Save Monitored Assets**.

This form replaces your lists Whatever you save becomes the complete list. It does not add to what is already there. Always enter the full set you want monitored, and be aware that leaving a box empty removes every asset of that type.

The safest way to add an address is to click into the box, go to the end of the existing text, add a comma, then type the new address. That way nothing already being monitored is lost.



The Update Monitored Assets form. Remember it replaces your lists rather than adding to them.

Step 4. Open your first report

Back on the dashboard, select **Login to Aman** or **Dark Web Breach Report**. The portal opens using your existing AEserver sign in, so there is no extra password to remember.

Your report is organised by month. Use the month filter to look back at earlier periods once you have been using Aman for a while.

What to expect from your first report

Historic breaches are already circulating on the dark web, so your first report shows everything Aman can find, not just recent events. It is normal to see findings going back several years, and to see more than you expected.

This is not a sign that something just went wrongA long first report reflects years of breaches at other companies, not a new problem with your systems. Work through the recommended actions in your own time, starting with any finding where passwords were exposed.
From then on, your attention only needs to go to new findings as they appear.

Choosing which addresses to add

You do not need to add every mailbox in the business on day one. A sensible starting point is:

- your main business domain
- shared mailboxes such as accounts, sales, support, info and admin
- anyone who can authorise payments or access customer records
- senior staff, who are the most common targets for impersonation

You can widen the list at any time as your team changes.

Get Aman Not set up yet? See pricing and get started.