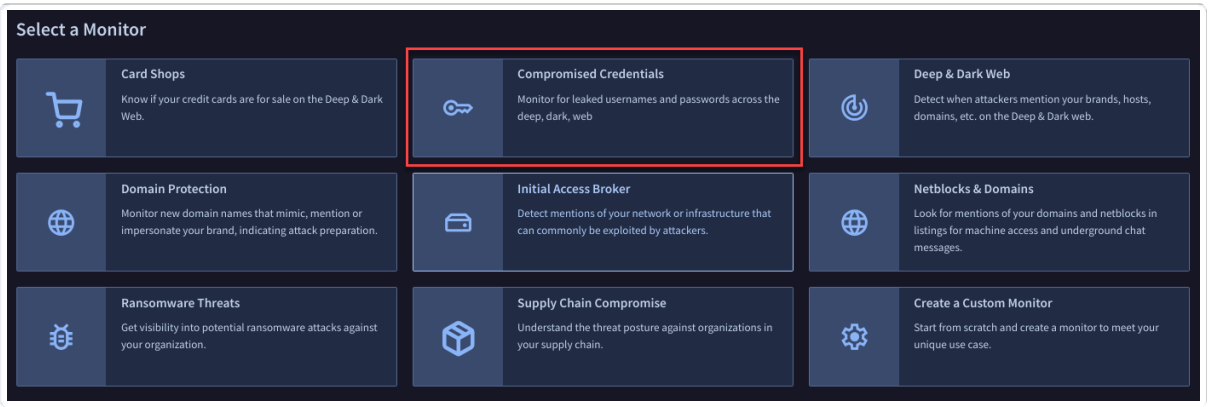
MONITOR COMPROMISED CREDENTIALS

Digital Threat Monitoring (DTM) automatically alerts you if any accounts linked to designated domains have appeared in compromised credential data collected from the deep, dark web.

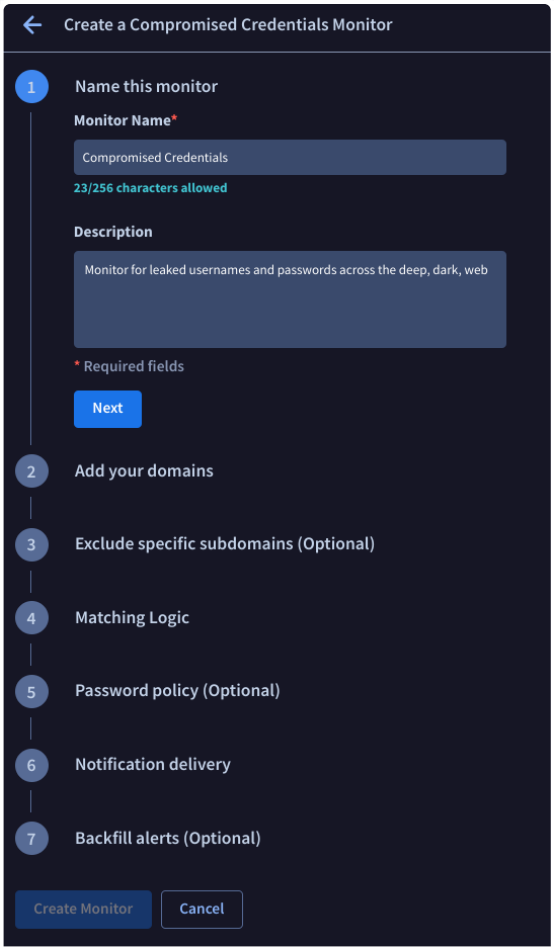
> Compromised Credentials monitoring automatically includes any associated subdomains.

Create a Compromised Credentials Monitor

1. In DTM, select the **Monitors** tab.
2. Select the **Compromised Credentials** Monitor template.



You are presented with a wizard to walk you through the monitor setup steps.



Compromised Credentials Monitor setup wizard

3. Name the Monitor.
    a. Enter a name for the Monitor.
    b. Optional: Provide a description.
    c. Click **Next**.

4. Add your domains.
    a. Enter domains to be monitored.
    b. Click **Next**.

    - Domains must be entered one per line.
    - You only need to add the most top-level domain; all sub-domains alerts are included.
    - You are required to prove that you own these domains in order to receive alerts containing unmasked login credential details.
    - Monitoring compromised credentials for free or public email domains is not supported.

5. Optional: Exclude specific subdomains if you want to reduce monitor noise and false positives.
    a. Enter domains to be excluded.
    b. Click **Next**.

6. Define Matching Logic. Select either or both of the following options:
    - **Match email domains in the login field**.
        - These are high-confidence employee credential matches.
        - When available, these matches deliver additional context around the breach including compromised machine's IP, hostname and other metadata.
        - Clear text passwords are provided for these credentials if the domain has been verified.
        - When there are matches to both of the email domain and web service domain, the matches are shown.
    - **Match the web service domain**.
        - Match your domains to the web service the compromised credential logs into.
        - These matches expand coverage for when there are not email domains in the login field.
        - Clear text passwords are provided for these credentials if the domain has been verified and the login domain field is empty.
7. Optional: Configure password policy to know if passwords in compromised credentials alerts meet your organization's password policy.
    a. Set a minimum and maximum password length.
    b. Configure Complexity Rules, such as at least one non-alphanumeric character or at least one uppercase character.
    c. Click **Next**.
8. Optional: Configure notification delivery.
    a. Select the checkbox to **Enable email alert notifications**.
    b. Select the checkbox to **Deliver email notifications from this monitor immediately**.
    c. Click **Next**.
9. Optional: Configure backfill alerts if you want to create historical alerts for the period you select.
    - Choose an option:
        - **No, do not backfill alerts**
        - **Yes, backfill alerts for the last**
            - Choose a time period from the drop-down. For example, **7 Days**.
10. Click **Create Monitor**.
11. Optional: Verify domain ownership with a TXT record.

    - Verifying ownership of a domain lets us enrich associated alerts with additional details such as PII that otherwise would not be displayed. This improved context typically results in more actionable alerts.
    - For more information on verifying domains with a TXT record, including step-by-step instructions, see **Verify your domain with a TXT record (https://support.google.com/a/answer/183895?hl=en)**.

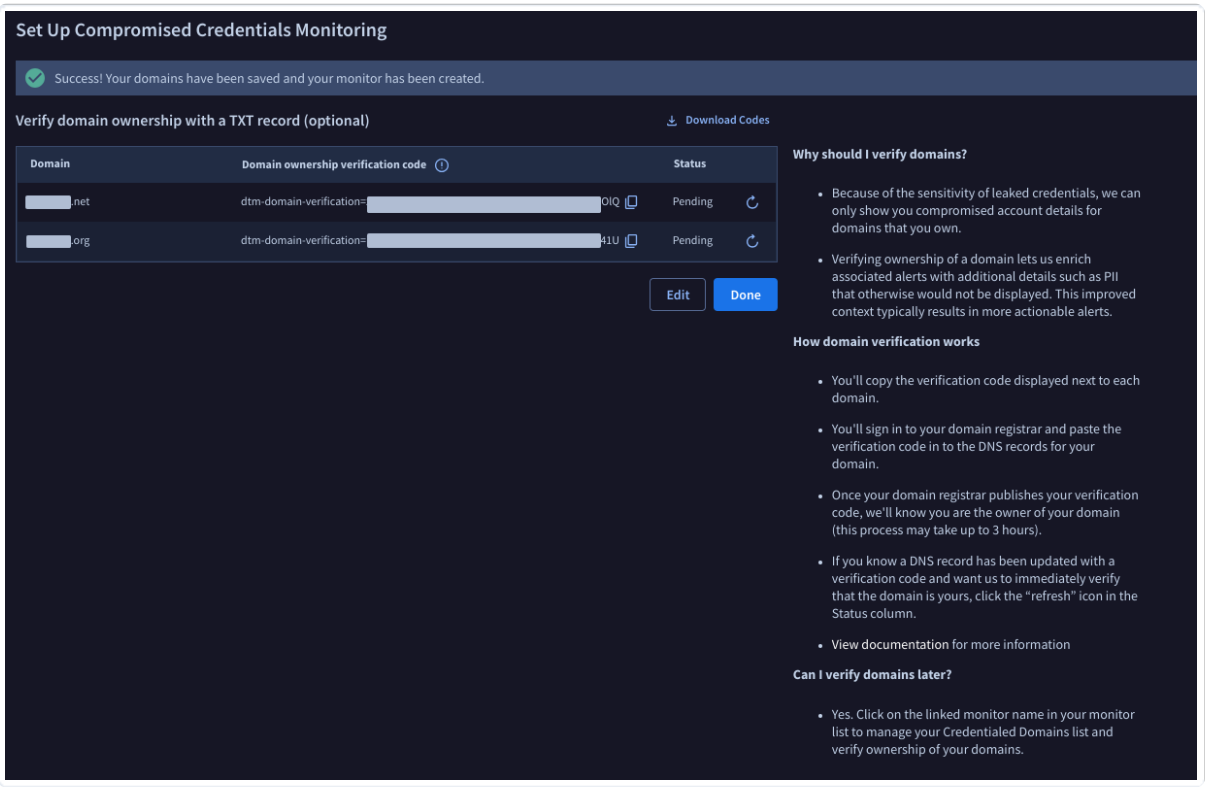
    a. Select **Click to Copy** to copy the verification code for the TXT record.
    b. Paste the verification code in to the DNS records for your domain. Once your domain registrar publishes your verification code, we'll know you're the owner of your domain.

    This process may take up to three hours.

    c. Optional: If you know that your DNS records have been updated, click **Refresh** to initiate an ad-hoc query to verify your domain.

d. Optional: Click **Download Codes** to download all TXT record verification codes in a CSV file.

12. Click **Edit** to modify your domain list or **Done** to save the Monitor for the listed domains.

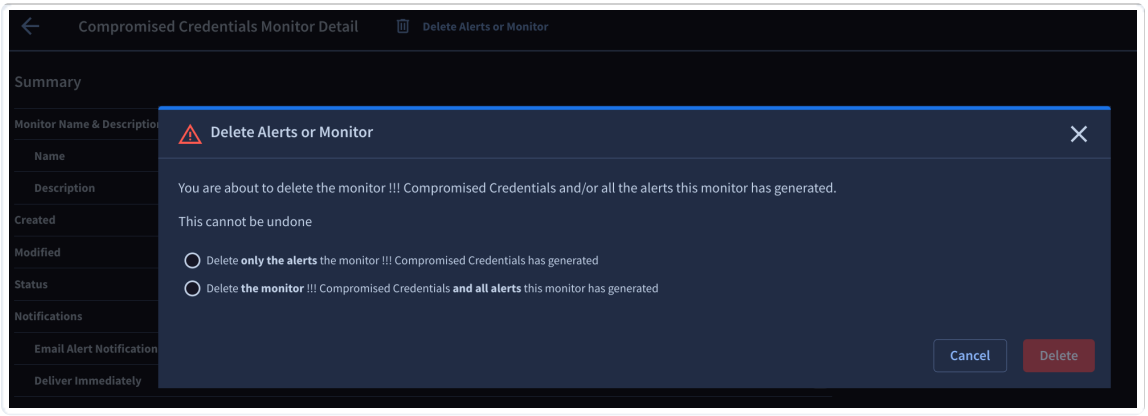


View, edit, or delete existing Compromised Credentials Monitors

Once created, monitors appear in Your Monitors list. Use the following workflow to edit or delete Monitors from this list.

1. From DTM, select the **Monitors** tab.
2. Select an existing monitor from the list of **Your Monitors**.
   - To delete, click **Delete Alerts or Monitor** and make a selection to delete the Alerts for this Monitor or the Monitor itself.

> This process cannot be undone. Deleted Alerts and Monitors can be recreated but they can't be restored with historical data intact.



   - Alternatively, to edit any field associated with the Monitor, click

Edit or the toggle associated with the field to make the necessary adjustments.

Explore Compromised Credentials Alerts

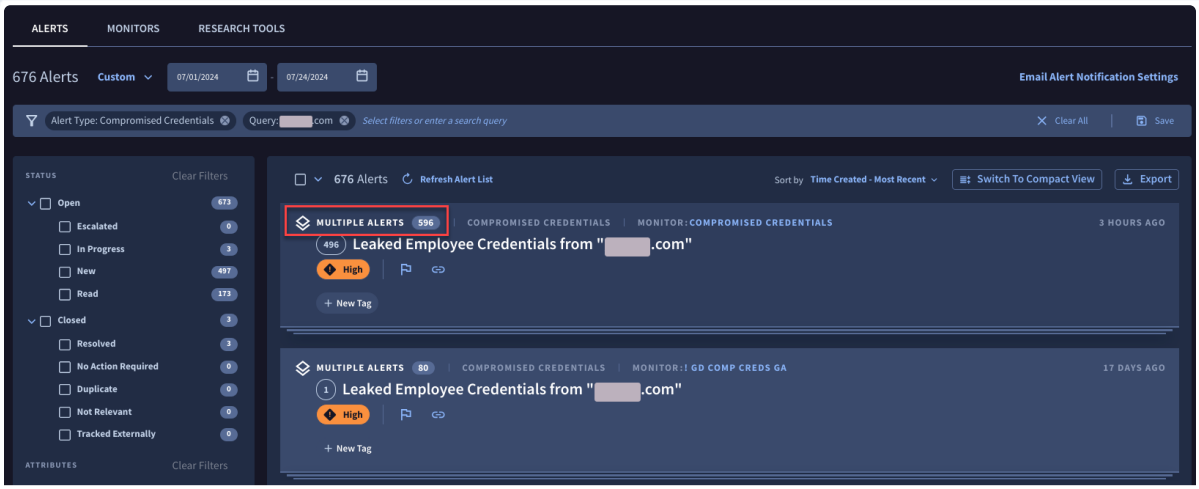
In DTM, the **Alerts** tab displays all Alerts generated from DTM Monitors.

> See **Working with Alerts** (https://docs.mandiant.com/home/dtm-alerts) for more information about DTM Alerts in general.

All Alerts associated with a single **Compromised Credentials** Monitor are automatically aggregated into a bucket Alert with a **Multiple Alerts** label. The label includes the number of related Alerts.

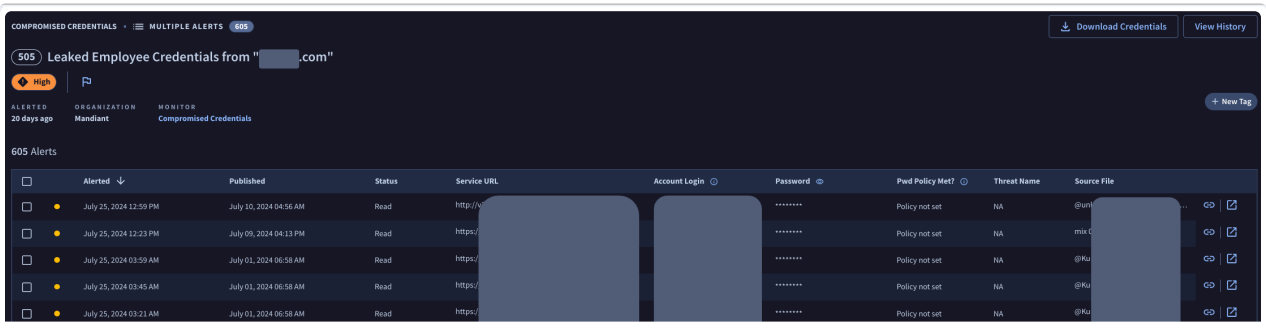
Filtering the Alerts list affects how aggregated Alerts are displayed:

- If any child ticket in an aggregated bucket matches the filtering criteria, the bucket is displayed in the Alerts list.
- When using a **Date Range** filter in the **Alert List** view, the date range determines which child Alerts are displayed when you select the bucket.



A filtered list of Alerts showing two buckets of multiple Alerts.

Click an aggregated bucket Alert to view a table containing all the associated Alerts. New Alerts are tagged with a yellow dot that becomes gray once the Alert has been opened.



A table of Compromised Credentials Alerts in DTM

The Alerts table includes the following:

- **Alerted**: Date and time the Alert was generated.

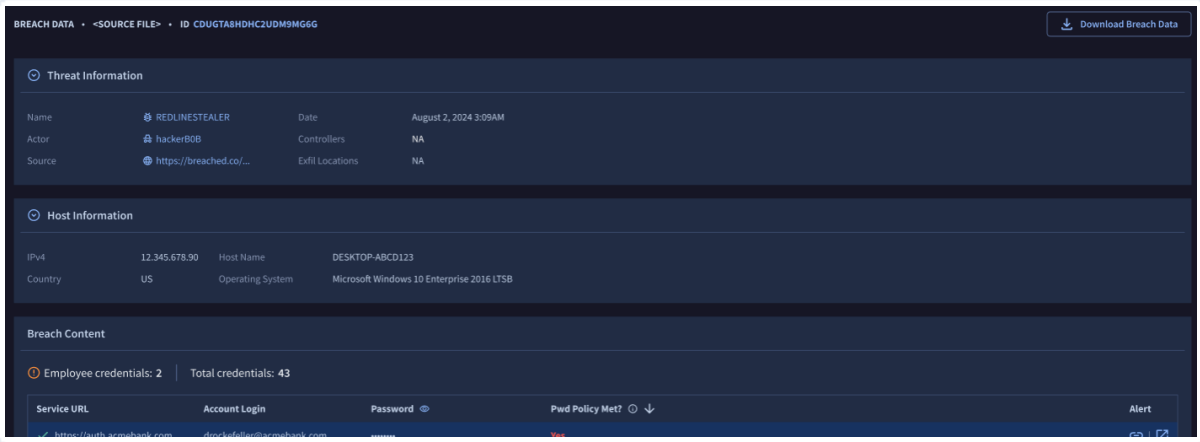
- **Published**: Date and time at which the credentials were exposed.
- **Status**: New, Read, or Closed.
- **Service URL**: The specific source URL used for sign in, such as `myownpersonaldomain.com`.
- **Account Login**: The username that was found in the compromised credentials data.
- **Password**: The password that was found in the compromised credentials data.

  - Password hashes and clear text passwords are displayed, if available, for domains that have been verified.
  - Passwords are only displayed if the Account Login contains the verified domain, or if the Service URL domain has been verified and the Account Login domain is empty.

- **Pwd Policy Met?**: A password policy can be established when the monitor is created.
- **Threat Name**: The associated threat, such as malware or threat actor, that was found in the compromised credentials data.

  Click the hyperlink for the threat to pivot directly to its profile in the Mandiant Advantage Threat Intelligence (MATI) platform.

- **Source File**: If the domain has been verified, you can use this link to navigate to the Breach Data view. This view contains information about the threat, the compromised host, and credentials related to your domain.



- **Copy link**: Copy the individual Alert URL to your clipboard.
- **View alert details**: Open the individual Alert URL in DTM.

Download Credentials and View History

DTM admins only: Click **Download Credentials** to export a CSV file that includes detailed information about each Alert such as:

- Date and time **Alerted**, **Collected**, **Published**
- **Service URL**
- **Account Login**
- **Password**

  The Password field is only shown for verified domains.

- **Threat Name**
- **Alert URL**

- **Alert Status**

Click **View History** for an audit trail of the following activities with timestamps and the name of the user that performed the activity:

- Opened, reopened, or closed an Alert
- Created or deleted a Monitor
- Downloaded the CSV file of Alert credentials data

Assign Alert Status

Alert status can be changed individually or in bulk. Select one or more Alerts and click **Mark Selected As**. Select a status to apply to the selected Alerts.

Add Tags

Click **+ New Tag** to select tags from the **Popular Tags** list, or enter your own tag and press enter to save.

Tags apply to all Alerts in the table. Alerts cannot be tagged individually.