VERITAS

VERITAS REDLab

January 2024

What's new?

Welcome to the recurring Veritas REDLab newsletter that provides you with the latest updates on the Veritas REDLab initiative.

The Veritas REDLab is a fully isolated security testing facility that is built in-house by Veritas to conduct thorough research and study ransomware and malware attacks first-hand and as they occur. The Veritas REDLab stress tests our solutions to ensure that our products are hardened against attacks, protecting both the backup data and administrative interfaces. This helps drive a deeper understanding of how we can best protect your primary data and provide meaningful signals to both security teams and data protection teams when an anomaly is detected. This ensures that the data is safe, protected, and that you can be confident in the cyber resilience that Veritas solutions offer.

Here are few of the ransomware families and their behavioral patterns that were studied in the REDLab:

Name	Ransomware family	Behavioral pattern
Faust	Phobos ransomware family	Phishing & Social engineering tactics
Mallox	Mallox ransomware family	Advanced URL Filtering, ProxyLogon, Lateral Movement, Credential Access

VERITAS

VERITAS

VERITAS REDLab

January 2024

REDLab findings:

- **Faust (attack on NetBackup client):**

  - **Family**: Phobos ransomware family | **Behavior pattern**: Phishing & Social engineering tactics
  - **Know Me:** This ransomware is part of the Phobos family and has built-in features to prevent recovery, such as disabling the startup recovery and deleting the shadow copies. It also creates an entry for itself to be started when Windows starts. A cybercriminal can also use it as a "RaaS" (ransomware as a service) to generate an encryptor. As such, it is almost impossible to attribute this attack to a specific or an established threat actor (TA). During the encryption process, it drops two files, info.hta and info.txt, containing the same ransom note. The ransom note contains an email address to contact to negotiate the terms as opposed to a link to an onion site, further reinforcing the belief that the TA behind this attack is not a organized group.
  - **Attack Pattern:** After the attack, this ransomware encrypted the user data and system files. A system anomaly (that detected unusual behaviour with respect to offline clients) was generated.

- **Mallox (attack on NetBackup client):**

  - **Family:** Mallox ransomware family| **Behavior pattern**: Advanced URL Filtering, ProxyLogon, Lateral Movement, Credential Access
  - **Know Me:** Mallox ransomware, like many other ransomware threat actors, follows the double extortion trend: stealing data before encrypting an organization's files, and then threatening to publish the stolen data on a leak site to convince victims to pay the ransom fee. Mallox group claims hundreds of victims, while the actual number of victims remains unknown. Their potential victims worldwide, includes professional and legal services, and manufacturing, wholesale, and retail businesses. According to the data that was collected from open threat intel sources, in 2023, there has been an increase of approximately 174% in Mallox attacks compared to the latter half of 2022.
  - **Attack Pattern:** After the attack, this ransomware encrypted the user data. A backup anomaly (that detected the change in deduplication ratio) was generated. Malware scan of the backup image detected the infection and tagged the image as 'Infected' and a critical notification of this status was generated.

VERITAS

VERITAS REDLab

January 2024

Impact of attacks on NetBackup by the given ransomware families

The following observations are noted when a targeted ransomware attack is carried out on a NetBackup client:

- Scenario 1: Data on NetBackup client is encrypted along with NetBackup configuration files or communication between NetBackup client and primary server is compromised that resulted in failures of backup jobs.

- Scenario 2: In certain attacks, NetBackup configuration files are not compromised, but the application data is encrypted. The backup of application data is successful, however, a reduction in data deduplication rate is observed.

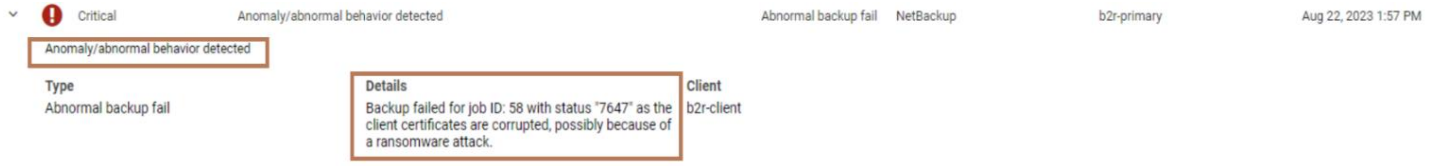
Recommended solutions:

Scenario 1: Data on NetBackup client is encrypted along with NetBackup configuration files.

Veritas Client Health system anomaly detects unusual network communication behaviour between NetBackup primary servers and clients. It checks the health of certificates that are deployed on the NetBackup client and starts the anomaly detection process.

When the anomaly is detected, the Client Health system anomaly creates a critical audit event that indicates failed communication with the NetBackup client. This audit event generates an alert and reports the affected client name to NetBackup IT Analytics or the SIEM/XDR platform.

The following screenshot shows the data from REDLab:

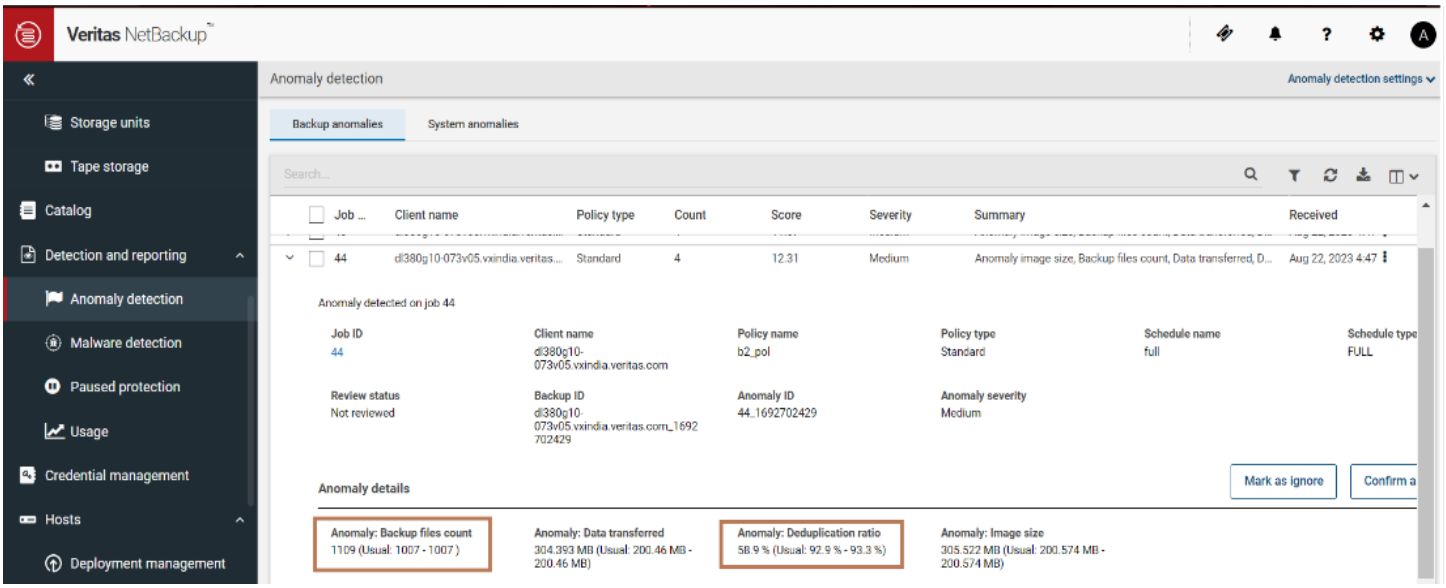


Anomaly extensions can be downloaded from the Veritas Download Center and deployed on NetBackup 10.2 or later versions of the NetBackup primary server. Review the NetBackup™ Anomaly Detection Extensions Guide for the steps to deploy and configure these anomaly extensions on the primary server.

Scenario 2: Data on NetBackup client is encrypted however NetBackup configuration files are intact and backup jobs are successful.

NetBackup uses machine learning (ML)-driven anomaly detection to detect anomalies using statistical data clustering analysis to calculate anomaly score. In this case, the change of data deduplication rate is detected by the ML algorithm and that generates an alert. It also starts an automatic malware scan of the backup image.

See the following screenshot from REDLab:



VERITAS

VERITAS REDLab

January 2024

New feature overview - NetBackup 10.3

Built-in multi-factor authentication

- Multi-factor authentication is a multiple-step account login process that requires you to enter a 6-digit one-time password along with your password. It is strongly recommended that you configure multi-factor authentication to protect the security of your account.

- Starting NetBackup 10.3, users can configure multi-factor authentication (MFA) for their NetBackup user accounts. Multi-factor authentication in NetBackup 10.3 implements recommendations from RFC-6238 “TOTP: Time-Based One-Time Password Algorithm”.

- Since this implementation is based on an open standard (RFC-6238); one may use any TOTP application confirming to such RFC mentioned earlier.

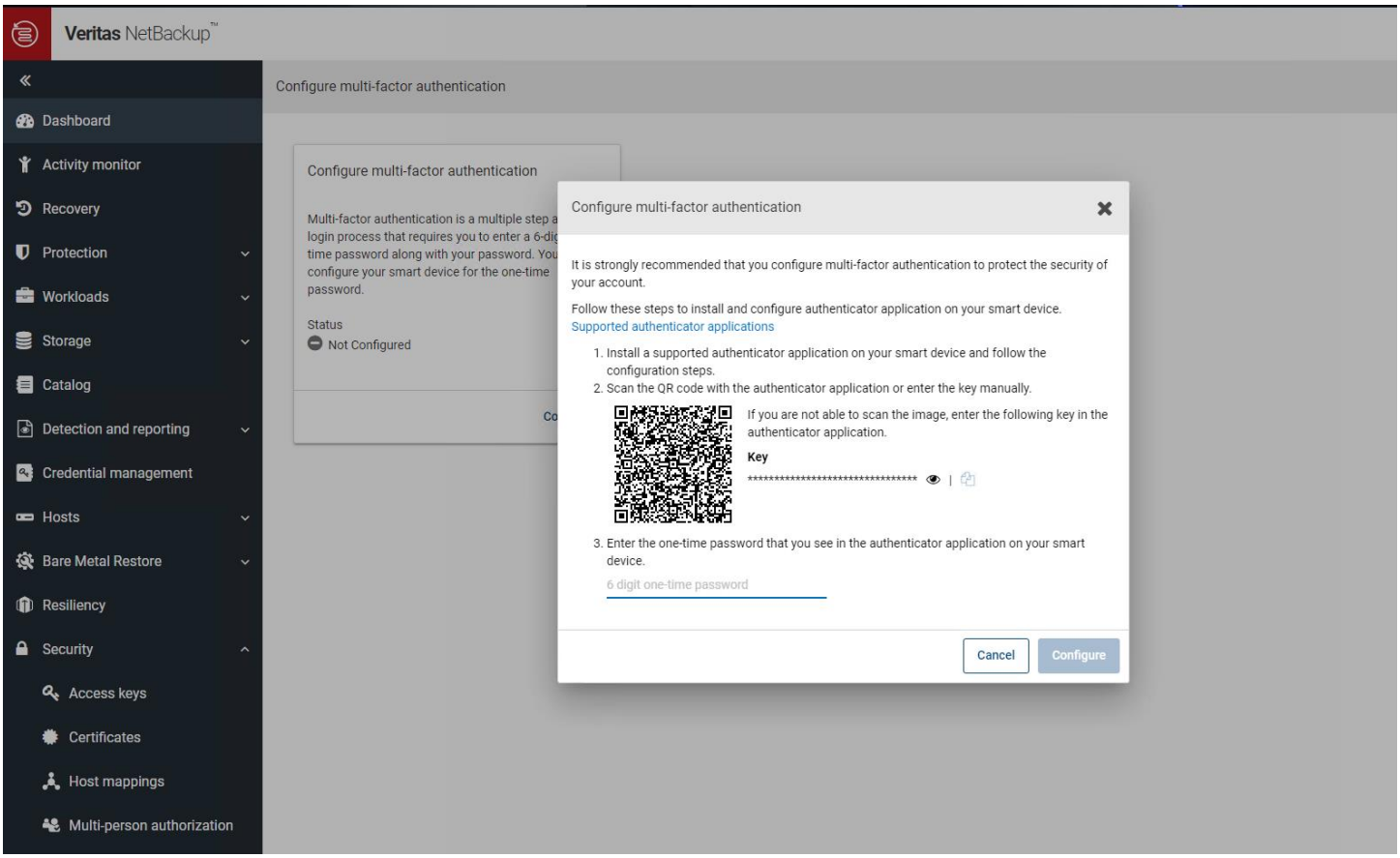
- The process of downloading and installing such an application is different based on the smart device platform (Android, iOS, Desktop).
  This newsletter focuses on the following widely used applications, such as:
  - Microsoft Authenticator
  - Google Authenticator
  - Okta Authenticator

- To configure multi-factor authentication for your user account:

  1. Sign into the NetBackup web UI.
  2. On the top right, click the profile icon and click **Configure multi-factor authentication**.
  3. On the **Configure multi-factor authentication** screen, click **Configure**.
  4. On the next screen, follow the given steps.

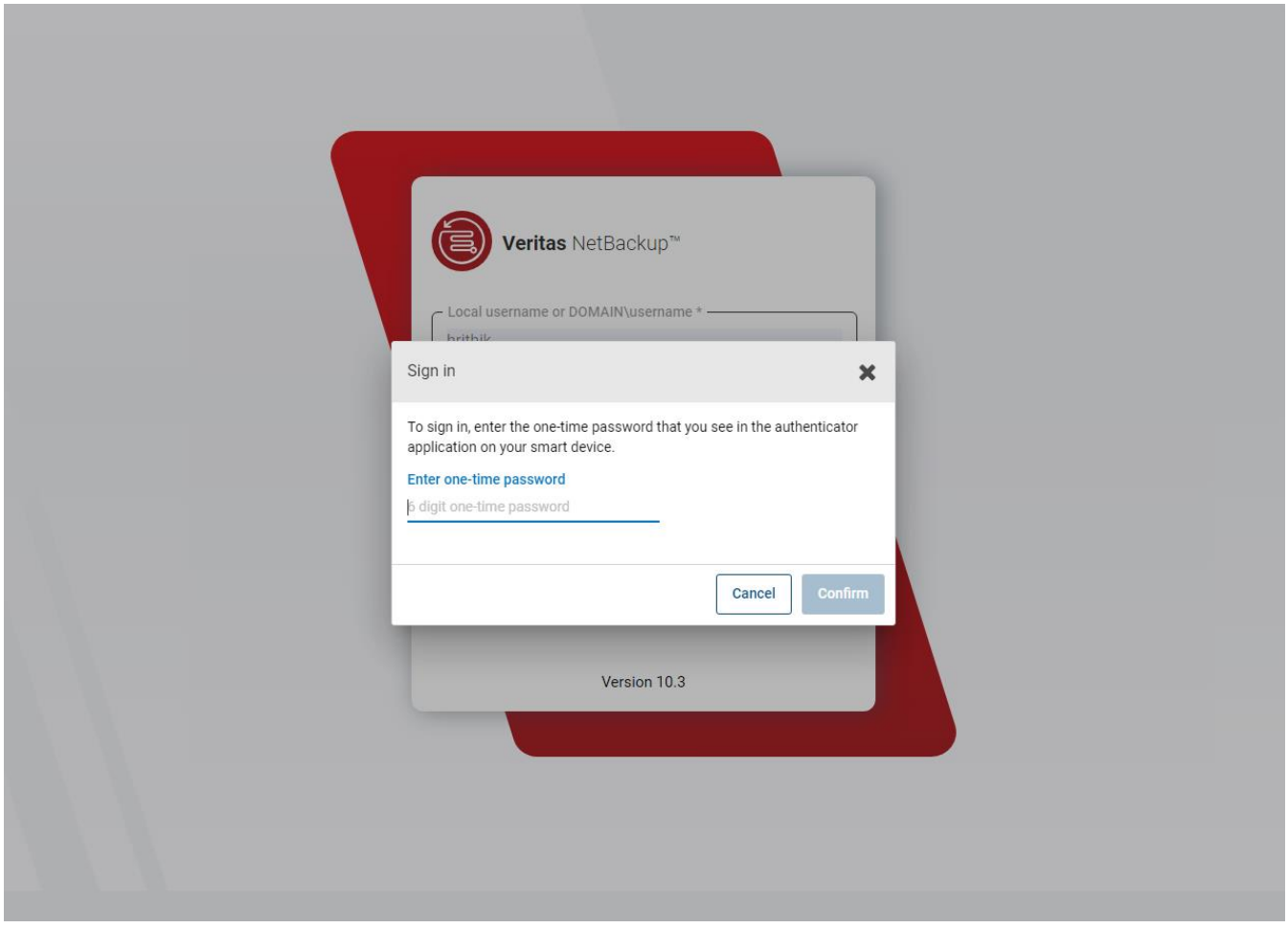
VERITAS

5. Install and configure authenticator application on your smart device. It generates one-time password and sends it on your smart device.



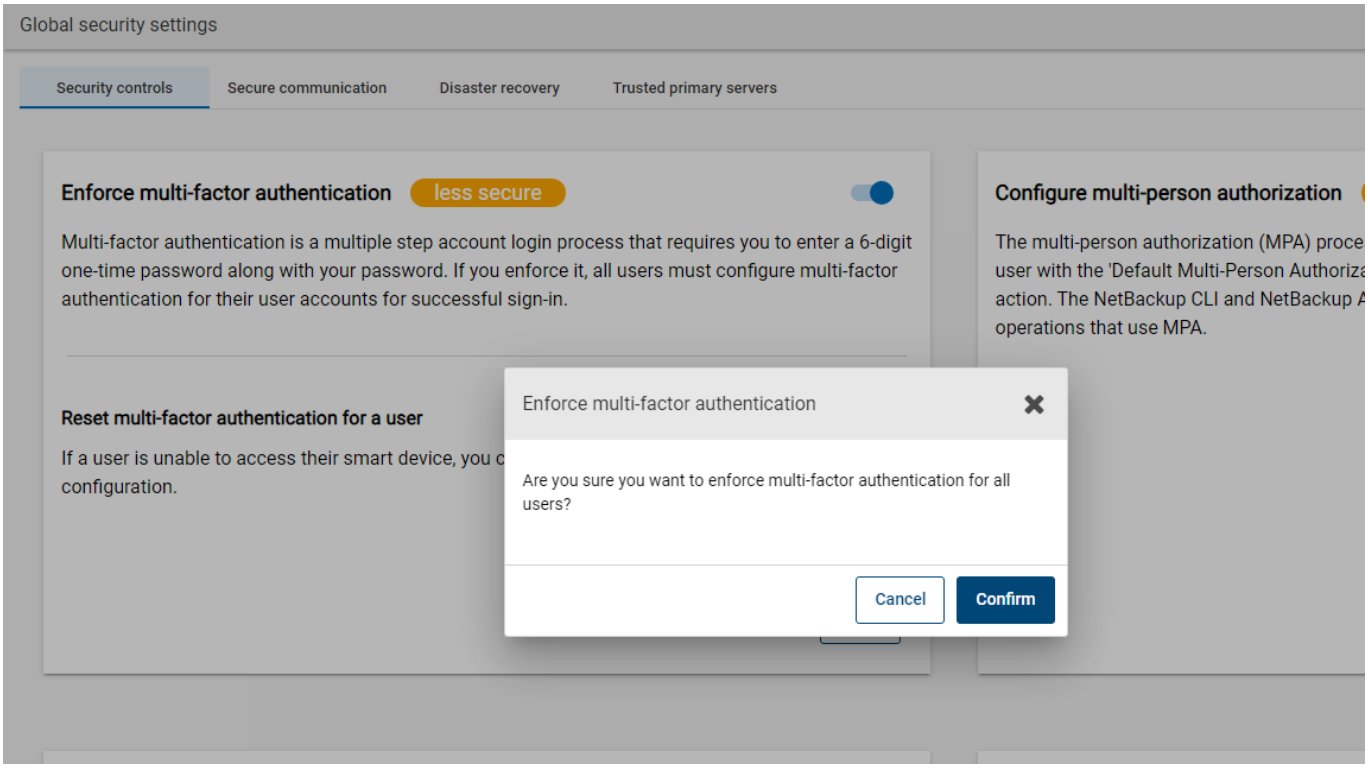
6. Scan the QR code with the authenticator application or enter the key manually.
7. Enter the one-time password that you see in the authenticator application on your smart device.
8. Click **Configure**.

9. At the time of next sign-in, you need to enter the one-time password along with the username and password.



- If multi-factor authentication is not enforced, you can disable MFA for your user account. However, it is strongly recommended that you configure multi-factor authentication to protect the security of your account.

- Apart from this, the NetBackup administrator can enforce multi-factor authentication for all NetBackup users. Before enforcing MFA for all users, ensure at least two users with either administrator or security administrators' role have provisioned MFA for their accounts within NetBackup.
    1. Sign into the NetBackup web UI.
    2. On the top right, click **Settings** > **Global security**.
    3. On the **Security controls** tab, turn on **Enforce multi-factor authentication**.



    4. Click Confirm to enforce multi-factor authentication for all NetBackup users.
    5. all users that they must configure multi-factor authentication for their user accounts to be able to successfully sign in.

More information about multi-person authentication can be found in the [NetBackup™ Security and Encryption Guide.]

VERITAS

VERITAS REDLab

January 2024

Research references:

- https://www.cisa.gov – Threat intelligence data and most pressing issues that CISA tracks, and notifications issued by government organizations.
- https://www.virustotal.com – Intelligence data, ransomware, or malware samples, discover threat commonalities and track new variants of surveilled malware families.
- https://www.hybrid-analysis.com – Malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.
- https://www.cyborgsecurity.com/ - Provides a library of expertly crafted, constantly updated threat hunting news and content.
- https://unit42.paloaltonetworks.com/ - Research blogs and Analysis of strains
- https://www.cert-in.org.in/ - Collection, forecast, and alerts of cyber security incidents.
- https://www.blackfog.com – Get monthly news around attacks and details of impacted organizations.
- https://www.bleepingcomputer.com – Daily news of recent activities carried out by ransomware gangs and methods used to infiltrate enterprises.
- https://www.truesec.com/ - Blogs and IOC’s
- https://www.sentinelone.com – Analytics data from various security vendors and insights around behavior pattens for each ransomware family
- https://decoded.avast.io/ - Latest threat research, ransomware analysis and IOC’s

VERITAS