Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.24.1

November 10, 2023

This new release of the Qualys Cloud Platform (VM, PC) includes improvements to Vulnerability Management and Policy Compliance.

What's New

Qualys Vulnerability Management (VM)

Clear Report Cache

VMDR Dashboard Access for the Existing VM Users

Discontinued Scan Results Download in .MHT (Web Archive MHT) Format

Bugtraq Hyperlink no Longer Exists in Database

Qualys Policy Compliance (PC/SCAP/SCA)

Support for OS Authentication-Based Technology Teradata 16.x/17.x

Support for New Authentication Technologies

MITRE ATT&CK® Framework Support

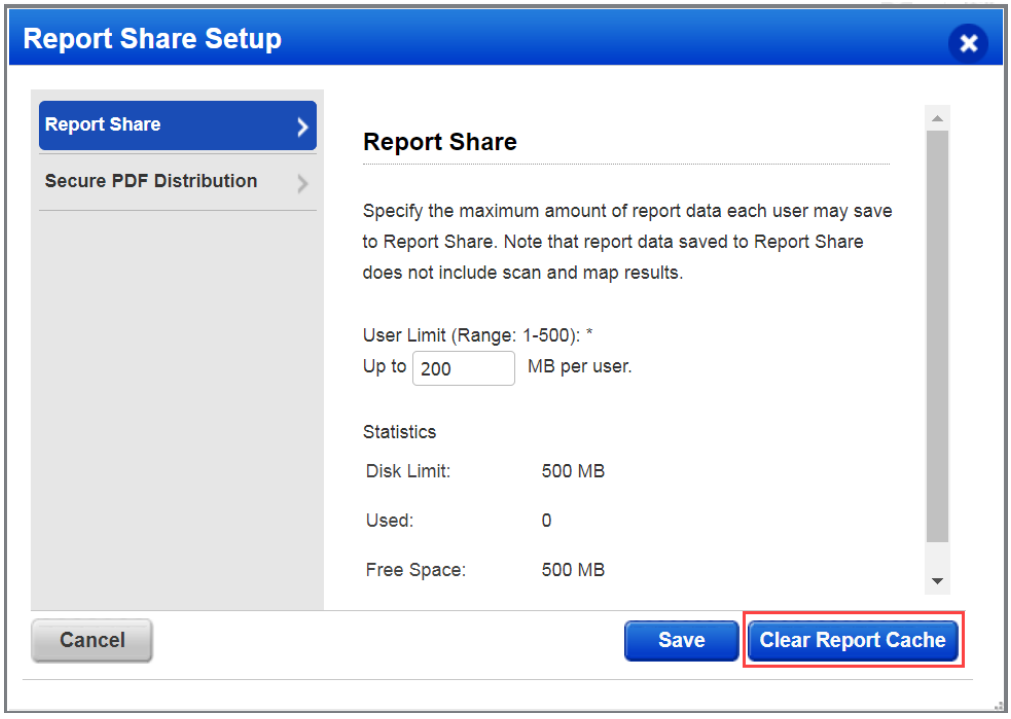
Qualys 10.24.1 brings you many more improvements and updates! Learn more

Clear Report Cache

The **Report Share** feature (**Reports**> **Setup**> **Report Share**) is enhanced to provide the ability to clear the report cache to avoid the report share disk space issue. A new button, Clear Report Cache, has been added to the Report Share Setup. With this feature, you can clear the report cache of the used report to free up the report share disk storage. Used reports are reports that are created or deleted by the users in your subscription but have not yet expired.

Notes:

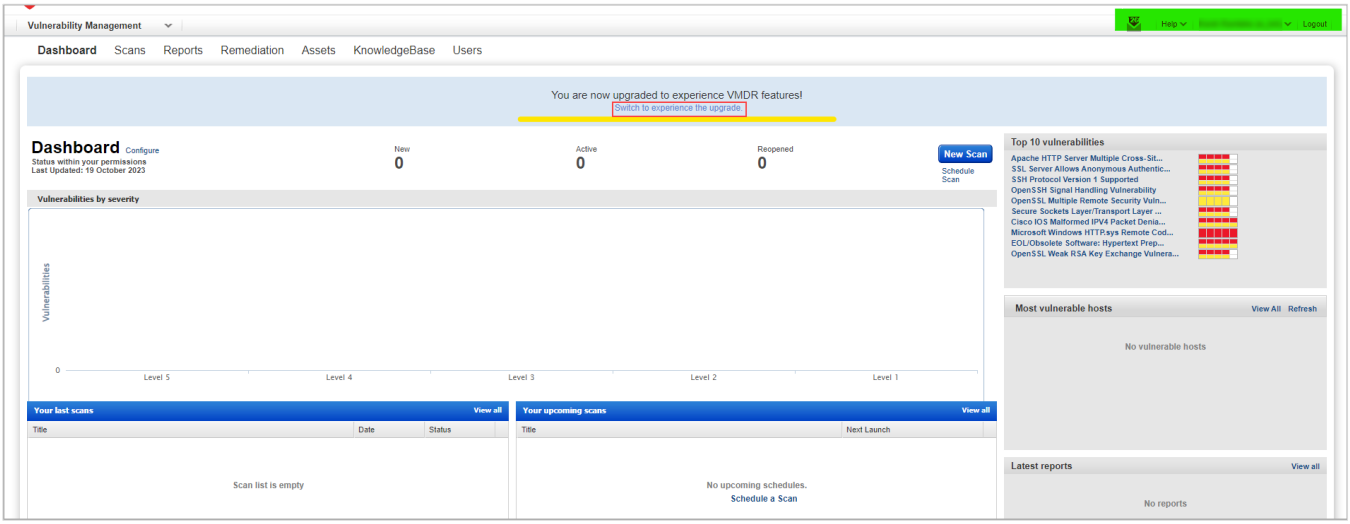
- To use this feature, the **Report Share** feature must be enabled for your subscription.
- The Qualys system already has an automated program which executes every 24 hours to clear the report cache of expired reports.
- The used report size displayed on the **Report Share Setup** comprises only the report share size for your subscription and reports deleted by the users in your subscription. It does not include expired reports.



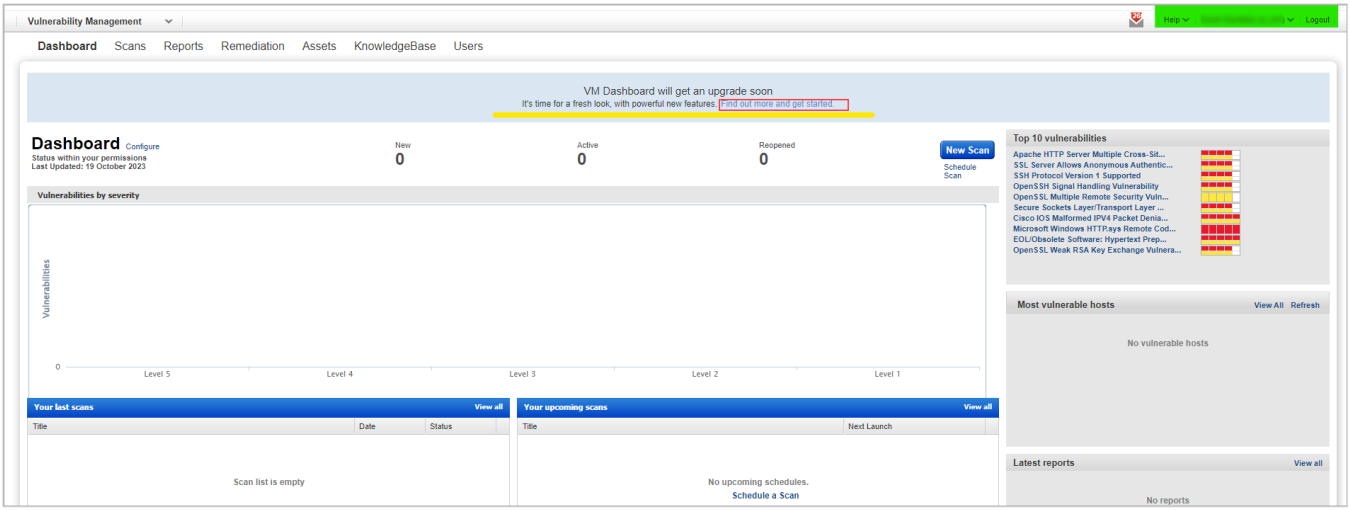
VMDR Dashboard Access for the Existing VM Users

A new option has been added to enable the following existing subscribers to access the VMDR dashboard. Click the link highlighted in the following screen captures to switch from the old VM dashboard to the new VMDR dashboard:

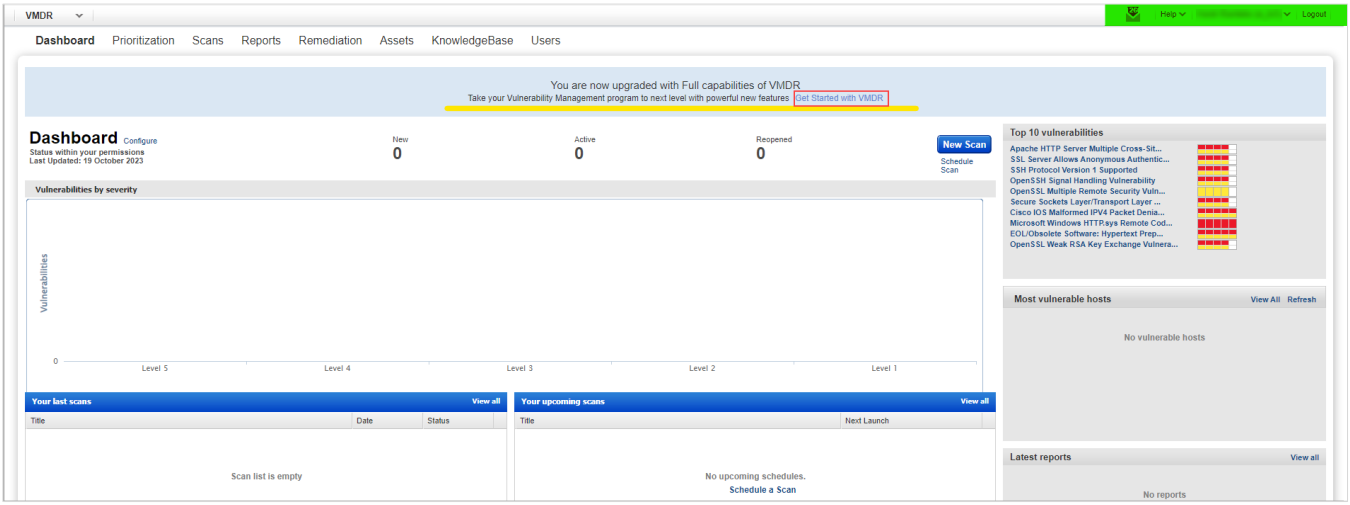
- VM Upgrade: Click the link, **Switch to experience the upgrade**.



- VM Account: Click the link, **Find out more and get started**.



- VMDR Account: Click the link, **Get started with VMDR**.



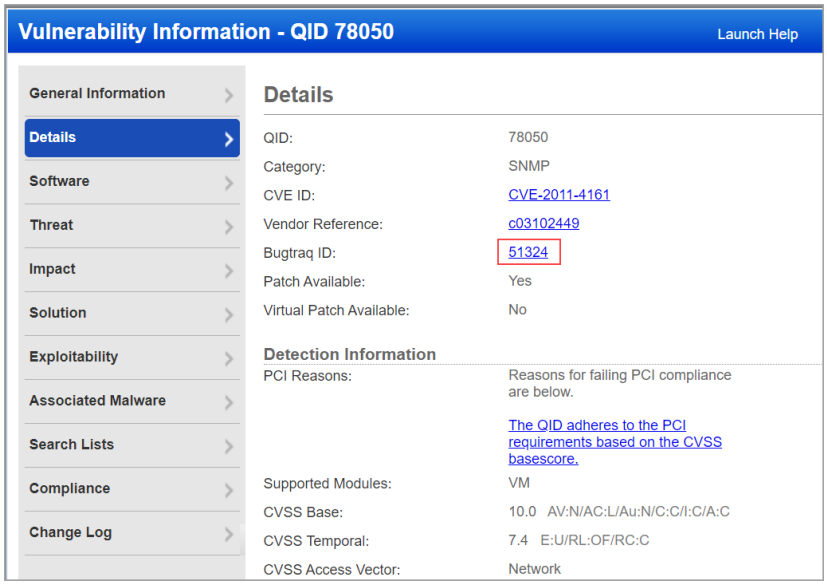
.

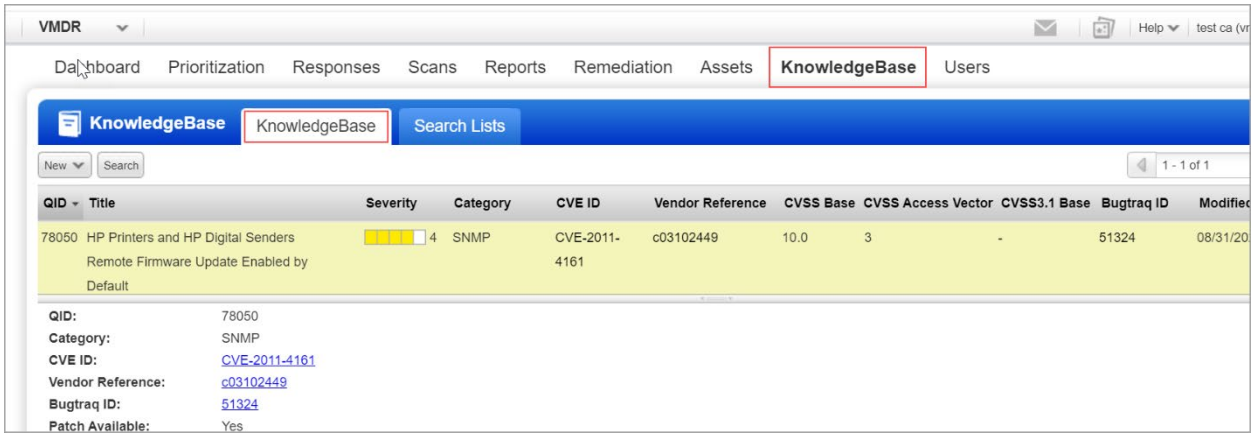
Discontinued Scan Results Download in .MHT (Web Archive MHT) Format

Downloading scan results in.MHT (Web Archive MHT) format has been deprecated and will be unavailable by the end of March 2024. This is only an Internet Explorer browser-supported format. Microsoft has already ended support for Internet Explorer, and Qualys will no longer support it in the future.

Bugtraq Hyperlink no Longer Exists in Database

With this release, Bugtraq hyperlinks are removed for the existing QIDs. However, Bugtraq ID is retained in the Knowledge Base.





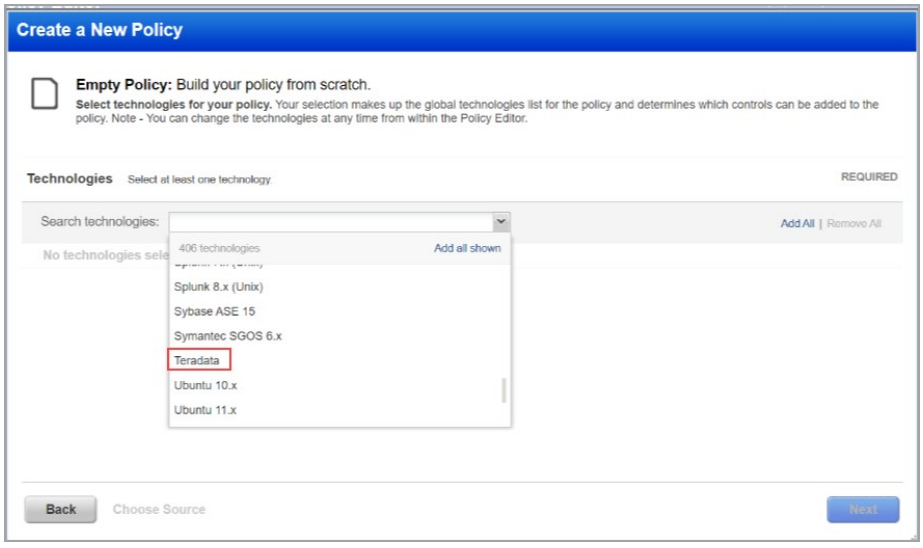
Support for OS Authentication-Based Technology Teradata 16.x/17.x

Teradata is an open and scalable database management system, that can enable businesses to improve their outcomes using data management tools. This system is used in various industries such as manufacturing, health care, and transport to optimize their processes.
We've extended our support of OS authentication-based technologies to include Teradata 16.x and Teradata 17.x.
You can now include the Teradata technology in your compliance policies and when searching controls. You'll also see Teradata host instance information in Policy Compliance authentication reports, scan results, and policy reports.

Note: Both the technologies Teradata 16.x and Teradata 17.x will be listed under Teradata for editing and generating authentication report.

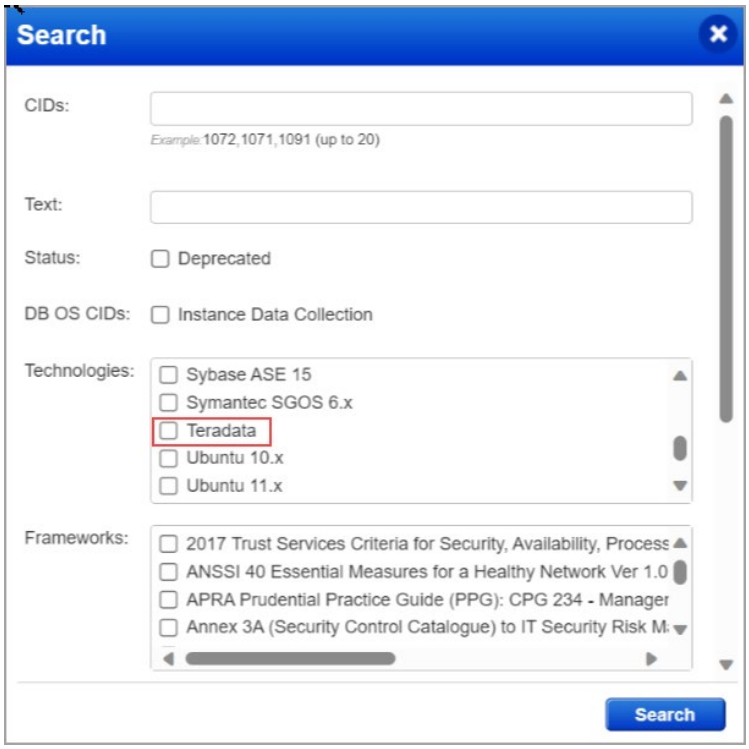
Policy Editor

When you create or edit a compliance policy, Teradata is now available in the list of supported technologies.



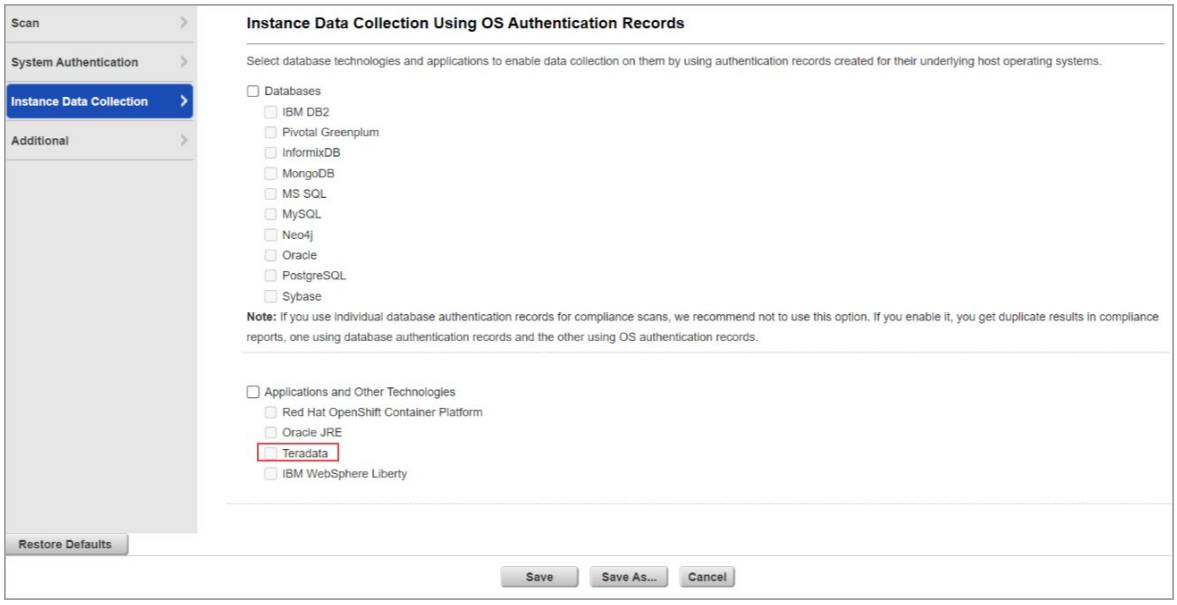
Search Controls

When you search controls, you see Teradata in the list of technologies.
Go to **Policies > Controls > Search** and select **Teradata** in the list.



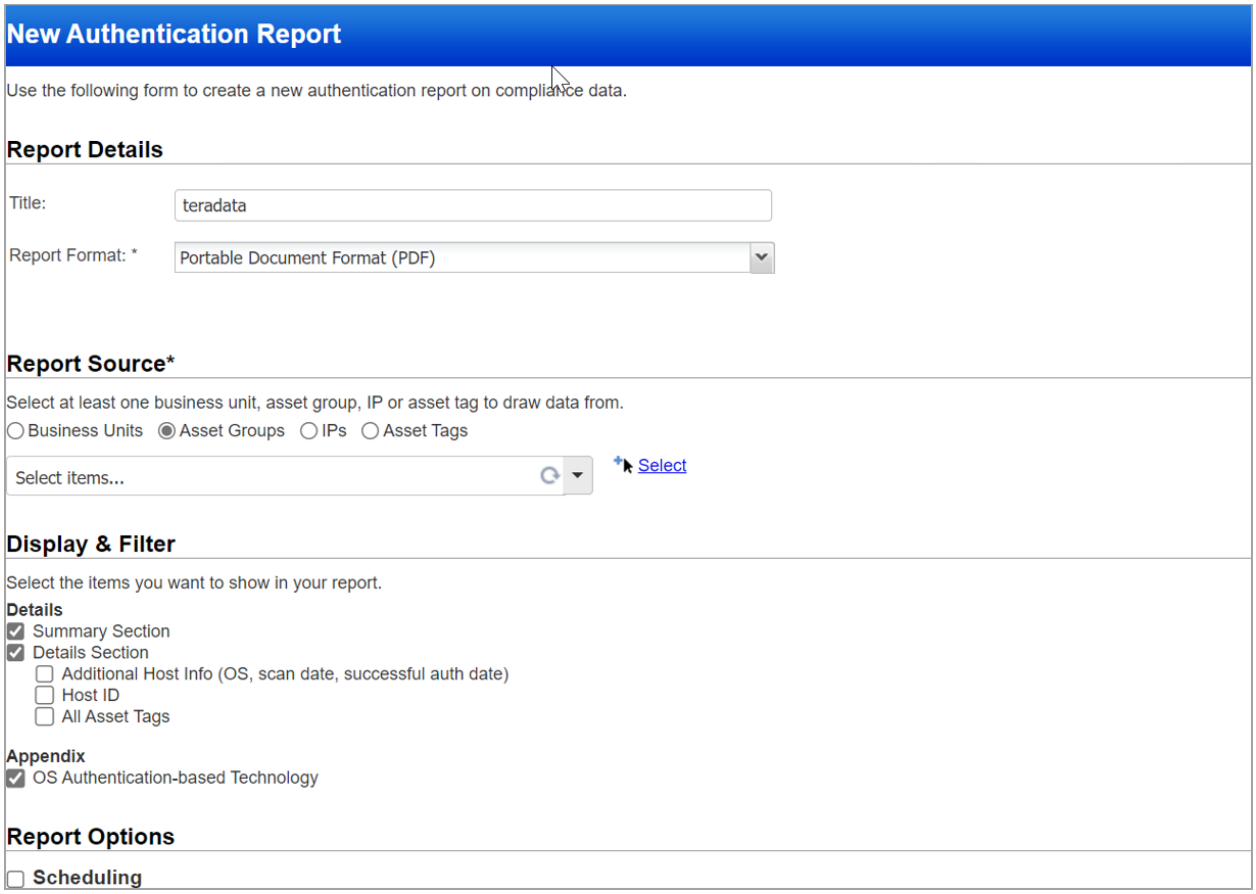
Option Profile

Select the option profile, go to **Instance Data Collection > Application and other Technologies > Teradata**, and enable the OS Authentication-based Technology option.

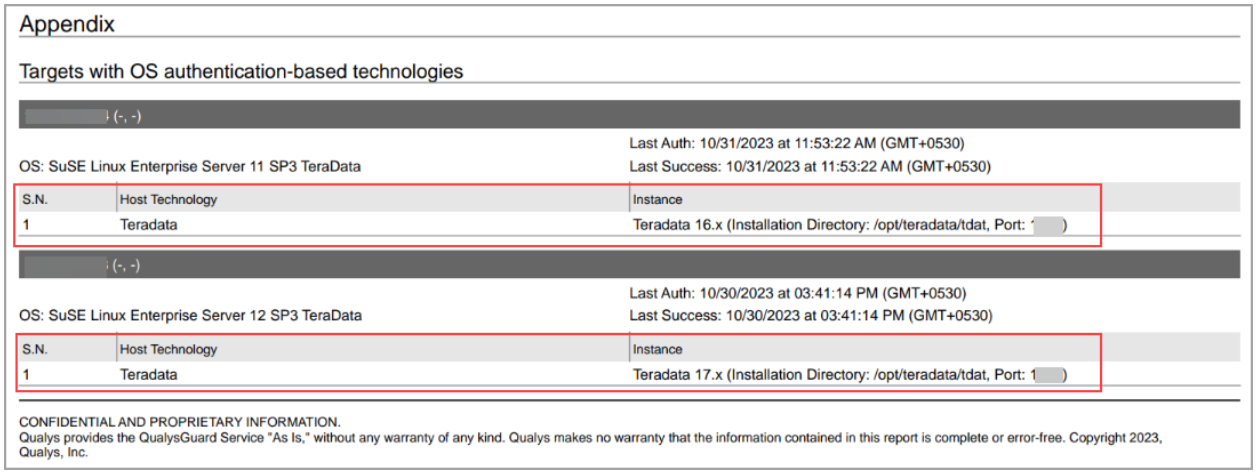


Authentication Reports

To display all OS auth-based instance technologies per host in your authentication report, go to **Reports > Compliance Report > Authentication Report**, and enable the OS Authentication-based Technology option under the Appendix.

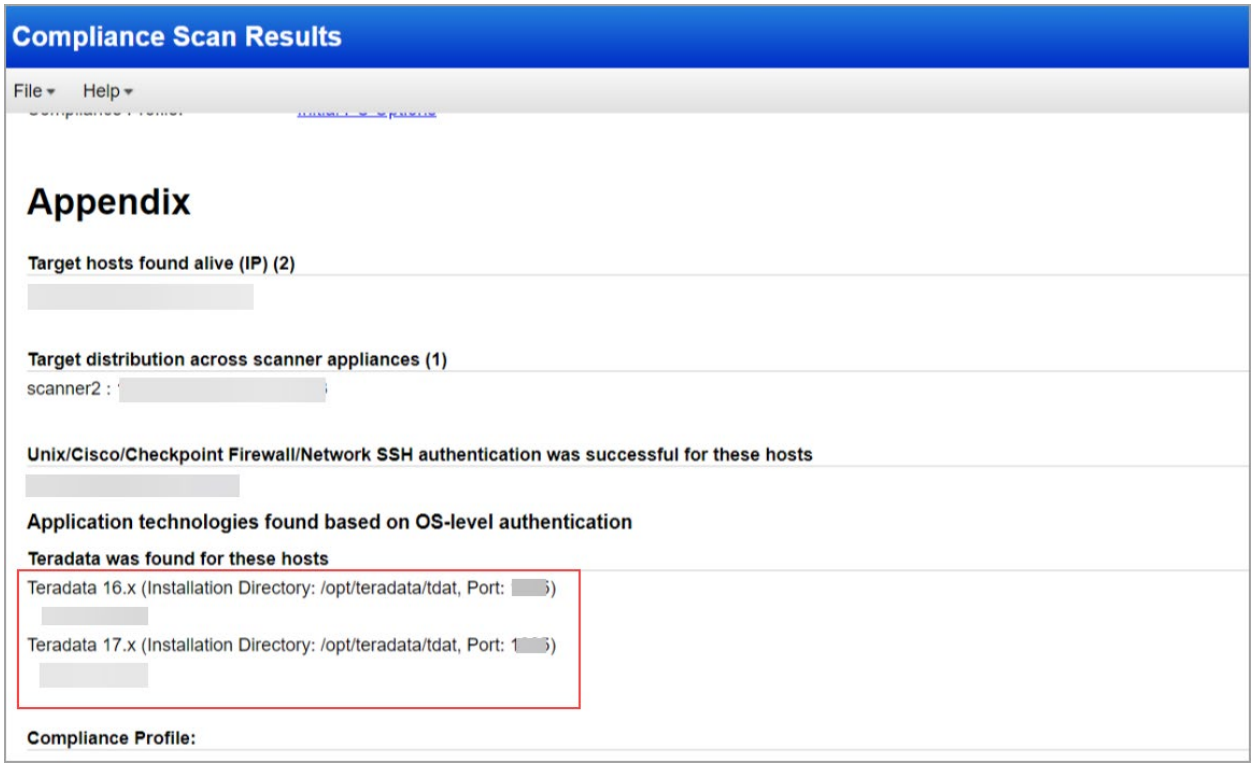


Scroll down to the **Appendix** section of your authentication report to see **Targets with OS authentication-based technologies**.



Scan Results

You see Teradata 16.x and Teradata 17.x listed under **Application technologies found based on OS-level authentication** in the **Appendix** section of a compliance scan result.



Support for New Authentication Technologies

With this release, the following technologies are now supported for Policy Compliance authenticated scans:

- Mongo DB 6.x is supported for PC
- PostgreSQL 15.x is supported for PC

For more information, see Authentication Technologies Matrix.

MITRE ATT&CK® Framework Support

The Policy Compliance application has been enhanced to leverage MITRE's ATT&CK® framework for cybersecurity. MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for developing specific threat models and methodologies in the private sector, government, and cybersecurity product and service community.

How does it work?

Controls are the primary building blocks for the Policy Compliance application. They provide first-hand insight into the configuration assessment of the organizational assets. We have implemented the mapping of these controls to this framework. We identify the controls and connect these controls to the MITRE ATT&CK® framework elements, Tactics and Techniques. This mapping allows you to quickly assess the state of your configuration assessments against these controls. This ultimately improves your security posture and fortifies your defenses against cyber threats, safeguarding your organization's assets and data.
This mapping offers you the following benefits:

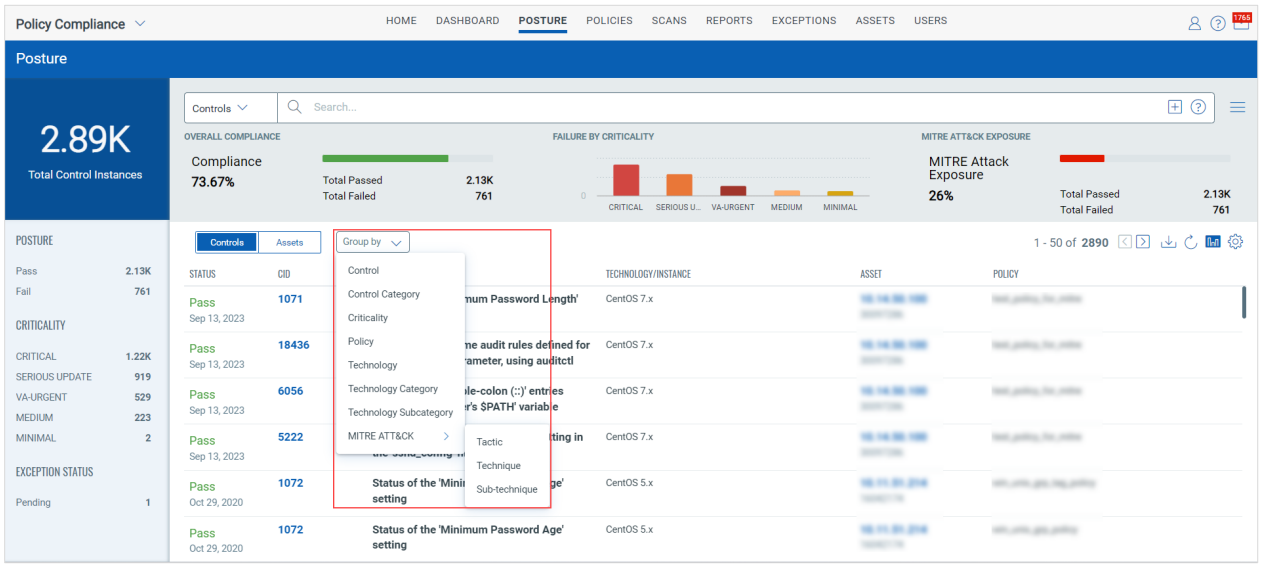
- **Comprehensive Coverage**: Mapping controls to the MITRE ATT&CK® framework ensures that your organization's security measures address a broad range of adversary tactics and techniques.
- **Alignment with Industry Standards**: Mapping controls to this framework demonstrates alignment with industry best cyber security practices as MITRE ATT&CK is widely recognized and used by both private and public sectors.
- **Incident Response and Detection**: Mapping control to this framework enhances your organization's ability to detect, respond to and recover from potential security incidents based on emerging threats.
- **Continuous Improvement and Threat Intelligence**: By mapping the controls to this framework, your organization can leverage this evolving knowledge base to stay ahead of the threat landscape. The MITRE ATT&CK Framework is constantly updated to reflect emerging threats and techniques employed by adversaries.

Key Highlights

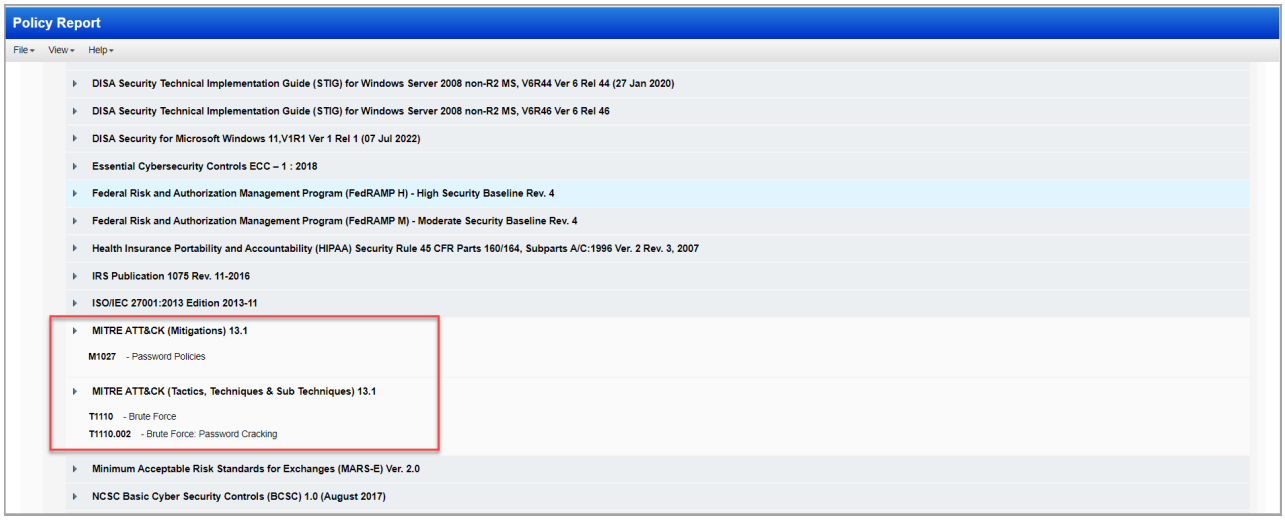
- Enhanced Posture tab to display MITRE ATT&CK® compliance information. You can now view MITRE ATT&CK® compliance score and compliance posture details. Use Group By options to filter out the posture records to understand MITRE compliance:

    - Group By MITRE ATT&CK Tactic: Displays compliance posture data based on MITRE Tactics.
    - Group By MITRE ATT&CK Technique: Displays compliance posture data based on MITRE Technique.
    - Group By MITRE ATT&CK Sub-Technique: Displays compliance posture data based on MITRE Sub-Technique.

For more details, refer to the online help topic, **Viewing Mitre Compliance**.



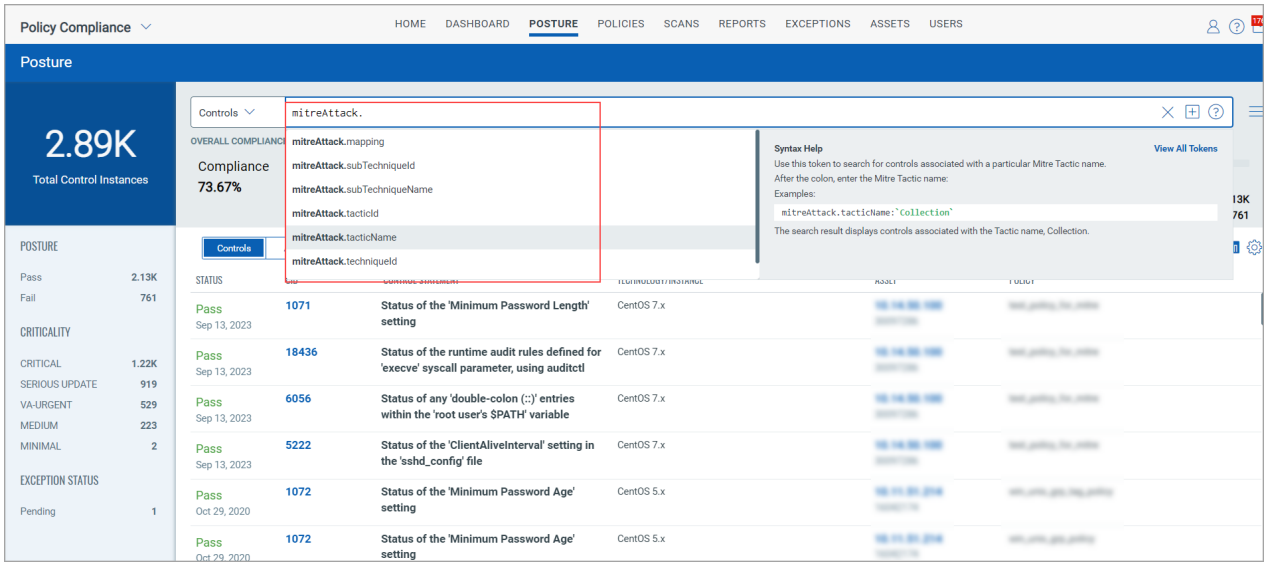
- Enhanced Policy Compliance report. You can now view MITRE compliance information. under the Control Glossary section of the report.



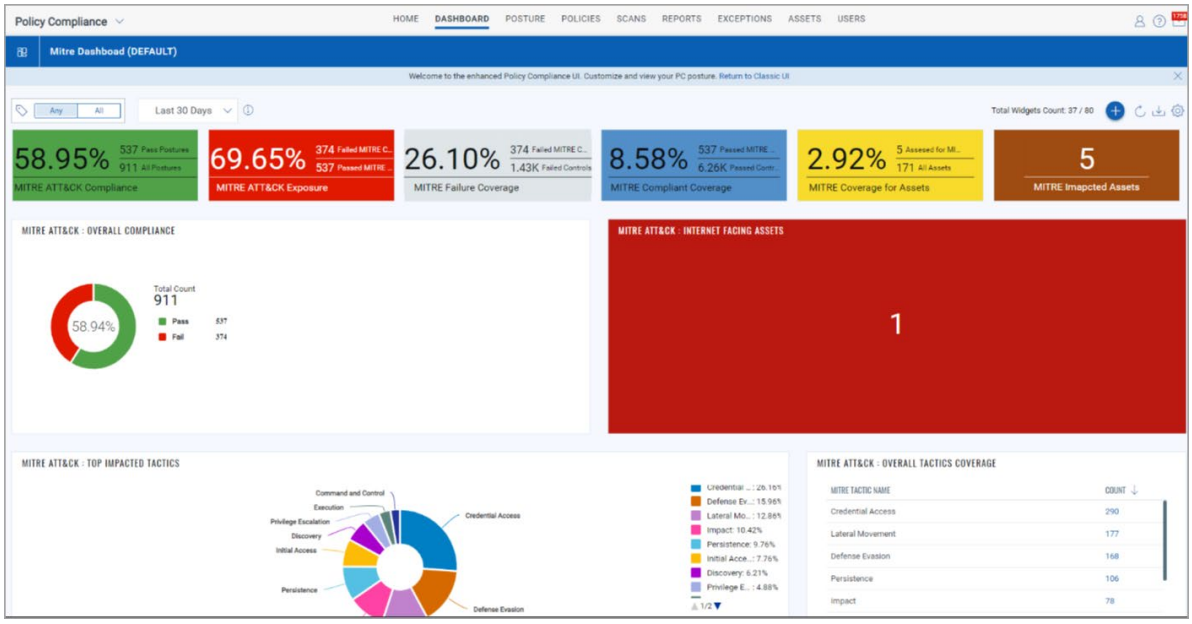
- New search tokens to search and filter MITRE compliance posture information. These search tokens are also available in the Query Settings for adding a PC Dashboard widget to visualize MITRE compliance data.

    - mitreAttack.tacticId
    - mitreAttack.tacticName
    - mitreAttack.techniqueId
    - mitreAttack.techniqueName
    - mitreAttack.subTechniqueId
    - mitreAttack.subTechniqueName
    - mitreAttack.mapping

For more information on search tokens, refer to **Search Tokens for PC Posture.**



- Default dashboard to visualize MITRE compliance. You can use this default dashboard or easily configure widgets and add them to your dashboard. For guidance on how to create widgets, dashboards, templates and more, refer to the **Unified Dashboard online help**.



Issues Addressed

The following issues are fixed with this release:

- The activity logs experienced search issues and displayed inaccurate user activity details. The activity logs displayed infra-API session calls for users without API access.

- Users were getting redirected to "status=timeout" page after trying to log in using SAML SSO. An extra log with the prefix “[Debug SAML Session]” has been added to resolve this issue.

- The scanner user was unable to edit the auth records on the Authentication (scan > Authentication) page using the Edit option from the Quick Actions menu. However, the user was able to edit the same authentication record using the Details menu on the Authentication (Scan> Authentication) page.

- The activity logs failed to generate an action log of the CSV report.

- The activity log was unable to log the user activities for the changes made in the following Password Security settings:
    - Allow users to change expired password at login.
    - Notify users in the UI to change password <number of days >before expiration.
    - Notify users by email to change password <number of days >before expiration.

- The Policy Summary tab encountered an error and did not show a dashboard view of the compliance status for the selected policy.

- Account Activity (Users->User Info->Account Activity) did not show updated data for any log-in attempts.

- Large slice value with a large number of active hosts was taking a long scan time. The maximum slice value was not reflected as per the maximum number of targets set in Option Profile settings and slices were not generated.

- Status in Security Technical Implementation Guide (STIG) based report was showing PASS* for failed control with approved exception.

- The subscriptions having only agent assets in their subscription encountered an incident signature error on the Remediation tab while creating a ticket policy for any manager user.

- Users with manager user access faced an issue for accepting the EULA with API request.

- In scan list API, if a deleted scan reference was provided, the message was displayed as (Given Scan Reference is deleted, please specify valid Scan Reference) in API Response.

- List asset groups API call with manager level access having more than 1000 asset groups in subscription with multiple combination of domains, IP's, NetBIOS, DNS names was failing with 'show attributes=All' as parameter.

- Inactive policy with an old last scan date got evaluated for the target asset and reflected the latest evaluation date.

- Password was not expired after 3 months, even after password expiry policy was set for 3 months.

- Password reset mail notification was triggered for an API user account with a never-password-expired setting on the account.

- User only had a system created authentication record for Oracle for that IP. However, when the user created authentication record option was selected in the Compliance profile, the system created authentication record was getting discarded and the instance was not getting authenticated.

- The scheduled report was configured to generate a report on the IPs that were removed from the subscription. However, it generated a report on the IPs that were available in the subscription instead of the IPs that were removed.

- The Qualys system failed to perform a compliance scan for certain IPs when SCA was enabled, and PC, and cloud agents were not enabled for the subscription.

- A scanner user encountered an error while creating a scan (host-based) template with the Asset Group "ALL" setting using the scan template API.

- The generation of Compliance-Policy reports in PDF format was interrupted due to an internal error when there was no host trends data to display for the host trend chart on the Compliance-Policy report.

- The user was unable to remove the asset present in the VM and Active OT scan from the Policy Compliance application with VM OT-enabled subscriptions.

- The ICS-enabled subscription user encountered an error while performing PC schedule scan on the asset group.

- Compliance Posture API Response returned incorrect content-type value in the API response header when output_format is set to CSV in posture API.