Support Policies and Technical Bulletins

- Support Policies

This guide contains support policies, agreements, and information on how to interact with the support team, including how to upload logs and support packages.

- Customer Support User Account Registration Policy (KBA1028)
- Delphix Support Policies (KBA1504)
- HIPAA Compliance and the Delphix Masking Engine (KBA1340)
- How to Add a New User Account to the Delphix Support Portal (KBA1007)
- How to Obtain Support for Delphixpy (Delphix Python Module) (KBA1843)
- How to Obtain Support for Delphix Plugin for Jenkins (KBA1829)
- How to Obtain Support for DXAnalyze (KBA1844)
- How to Obtain Support for Dxm-Toolkit (KBA3995)
- How To Obtain Support for DxToolkit (KBA1842)
- How to Open a Follow-Up Case (KBA4641)
- PlatinumPlus Data Sheet (KBA1009)
- Product Lifecycle Policies (KBA1003)
- Requirements to Access Delphix Support (Firewall Rules, Outbound) (KBA5565)
- User Account Management (KBA1550)
Delphix Technical Bulletins concern different issues that may arise within the product and are meant to alert end users to these issues as well as their resolutions.

- TB018 CVE-2014-3566 Vulnerability Statement
- TB017 CVE-2014-6271 and CVE-2014-7169 "Shellshock" Vulnerability Statement
- TB019 CVE-2015-0235 "Ghost" Statement
- TB016 Delphix Engine Configuration May Be Damaged When Management Service Starts
- TB030 Delphix Engine GUI is Unavailable Using Latest Version of Chrome With HTTPS
- TB034 Delphix Engine May Fail to Restart Following Device Removal
- TB029 Delphix Engine May Hang During Heavy I/O Load
- TB049 Delphix Engine May Restart Unexpectedly After Application of ESXi Patches
- TB021 Delphix Engine Performance Issues on Large or Memory-constrained Virtual Guests
- TB010 Delphix May Create Incomplete SnapShots After Upgrade
- TB028 Delphix Virtualization Engine Admin Interfaces May Become Unresponsive
- TB033 Device Removal May Lead to Delphix Engine Crash
- TB044 Environment Discovery Fails if Process Name Contains Space or Hyphen
- KBA1070 OpenSSL HeartBleed Bug Statement
- TB036 Masking Feature Exposes Database Passwords to Non Administrative Users
- TB039 Mission Control VM May Be Vulnerable to CVE-2016-5195
- TB020 Non-RDBMS Activity May Result in Delphix Engine Restarts
- KBA1591 Operations on Oracle virtual databases Colocated With a Source Database may lead to data loss (ASM)
- TB032 Provisioning to Oracle Source Environments May Cause Data Loss
- TB022 Spurious faults can be generated after an upgrade
- TB001 Duplicate iSCSI Qualified Names may Lead to Failure of Delphix iSCSI Service
- TB011 Clock Drift May Lead to Server Hangs or Performance Issues
- TB024 Delphix Engine May Hang During File Removal
- TB040 CVE-2017-3623 "Ebbisland" Vulnerability
- TB042 CVE-2017-5753 and CVE-2017-5715 (Spectre) and CVE-2017-5754 (Meltdown)
- TB045 PDB Failover Process Results in Non-Provisionable Snapshots
- TB046 JMX Port Vulnerability for Delphix Masking
- TB047 Masking Engine Export Data Includes Database, FTP and SFTP Connector Passwords In Clear Text
- TB048 Segmented Mapping Masking Algorithm Data Escape Security Vulnerability
- TB051 Delphix Engine May Crash or Restart Unexpectedly Under Heavy I/O Load
- TB052 Vulnerability When Masking Excel and XML Files Via SFTP or FTP
- TB053 Administrative Username Change
- TB054 Performance of Masking Jobs May Degrade or Introduce Inconsistent Results
- TB055 Masking Job Monitoring Failures
- TB056 5.3.1.1 Release Performance Issues
- TB057 Java Attach API Enabled on AIX Systems Vulnerability
- TB058 Masked Provisioning with Advanced Connector Could Result in Data Masking Errors
- TB059 Slow Oracle JDBC Connections After Upgrade
- TB060 Improper Command Line Interface (CLI) Responses
- TB061 Azure Non-Unique iSCSI Qualified Name Target Assignments
- TB062 Device Removal May Lead To Delphix Engine Crashes or Data Loss
- TB063 Sensitive Information May Be Written to Masking Log Files
- TB064 Linux TCP SACK Impact on Network Performance
- TB065 Sensitive Information May Be Written to Log Files
- TB066 Deletion of User on Masking Engine Removes Associated Jobs
- TB067 Sensitive Information May Be Present in Phone-Home Data
- TB068 XSS Vulnerability on the Masking Audit Page
- TB069 XSS Vulnerability on the Masking Rule Set and Inventory Pages
- TB070 Pluggable Oracle Databases with Lower/Mixed Case Names Will Not Enable
- TB071 Windows-Based VDBs and Data Sources May Experience Reduced Performance
- TB072 Shuffle Algorithm Leaves Data Unmasked But Reports Success When Used With Extended Connectors
- TB073 XSS Vulnerability on the Masking Mainframe Inventory UI
- TB074 Pattern in File Ruleset is Vulnerable to XSS Attack
- TB075 Operations on Windows-Based Sources and Databases May Stop Responding
- TB076 I/O Operations on VDBs and Other Sources May Intermittently Become Non-Responsive
TB077 XSS Vulnerability on the Masking Engine
  • TB078 Passwordless Login Succeeds to Masking Engine Configured for LDAP
  • TB079 Delphix Engine May Become Non-Responsive After Device Expansion
  • TB080 Billion Laughs DoS Vulnerability in Masking and Virtualization Engines
  • TB081 Delphix Engine API and User Interface May Become Non-Responsive
  • TB082 Updating Masking Ruleset May Clear Configuration for Other Tables
  • TB083 Non-Privileged User May Be Able to Perform Certain Actions on the Masking Engine
  • TB084 Leaked Password When Using EBS Plugins, HANA Plugins, or ASE Hooks
  • TB085 libpam Can Cause Buffer Overflow (CVE-2020-27678)
  • TB086 XSS Vulnerability with Masking Environment Overview Page
  • TB087 An Authenticated Delphix User May Be Granted OS-Level Access on Engines Deployed in Azure
  • TB088 Delphix Engine May Become Permanently Unmanageable
  • TB089 Oracle Database Passwords May Be Exposed in Logs and Process Tools
  • TB090 Delphix Engines Using SDD May Become Unresponsive
  • TB091 Oracle Data Blocks May Be Corrupted with dNFS
  • TB092 jQuery Version Affected by CVE-2020-11023 (Cross-Site Scripting Vulnerability)
  • TB093 Oracle V2P Operations Can Remove Existing Database Files
  • TB094 Arbitrary Code Execution May Be Performed by Engine System Administrators
  • TB015 Unexpected Reboots On Intel® Xeon® E5-2600 v2 Systems
  • TB041 VDB Operations on Windows Environments May Fail With iSCSI Mount Errors
  • TB026 Virtual Database Provisioning Performance May Degrade for Oracle 12c Databases
  • TB031 Windows Targets May Fail to Reestablish iSCSI Connections with the Delphix Engine
  • TB038 Windows vFiles Provisioning May Delete Files in Mount Path

• EoL and EoS Articles
This guide provides the end-of-life (EoL) and end-of-support (EoS) announcements for Delphix products.

- TB050 End of Life for Supported Software in Dynamic Data Platform 5.2