TPAM 2.5.922

Release Notes

July 2019

These release notes provide information about the The Privileged Appliance and Modules release.

About this release

TPAM automates, controls and secures the entire process of granting administrators the credentials necessary to perform their duties. Privileged Password Manager ensures that when administrators require elevated access, that access is granted according to established policy, with appropriate approvals, that all actions are fully audited and tracked and that the password is changed immediately upon its return. Privileged Session Manager provides session control, proxy, audit, recording and replay of high-risk users, including administrators, remote vendors and others. It provides a single point of control from which you can authorize connections, limit access to specific resources, view active connections, record all activity, alert if connections exceed pre-set time limits and terminate connections.

TPAM 2.5.922 is a patch release with enhanced features and functionality. See Enhancements and Resolved issues.

Enhancements

The following is a list of enhancements implemented in TPAM 2.5.922.

Table 1: Enhancements

Enhancement	Issue ID
Can regenerate a host key for a failed over replica without removing it from the cluster.	8515
Updates to Oracle chapters in the Client Setup Guide	9023
Added AllowStarling flag to Add/Update user API/CLI commands.	10245
Added a Test Notification button for Approval Anywhere users.	10251
Added request reason code and request/extension comments to Approval Anywhere notifications.	10318
Added additional logging of CLI calls to the Activity report.	10352
Added password rule information to Support Bundle and Password Rules Configuration Test Rule results page.	10356
Added more details to Client Set Up Guide iDRAC.	10363
Updated driver for Teradata platform to version 15.10	10389
Oracle platform upgraded to support SHA256 crypto.	10456
Changes made to address security vulnerabilities.	10459,10463,10465
Now support HTTP Strict Transport Security (HSTS).	10461
For external authentication methods using a "Secret", the "Secret" is no longer retrieved once initially saved, and not updated until a new value is entered.	10464

Resolved issues

The following is a list of issues resolved in this hotfix.

Table 2: Resolved issues

Resolved issue	Issue ID
When adding an account as an ISA, the settings from the parent system are not defaulting for the account.	10041
Cisco platforms using telnet have problems with automatic login for PSM sessions.	10255
Password checks are not occurring as scheduled for every account for customers that have a very large volume of accounts.	10280
Windows System Error, EventID:7031 in the Alert log.	10304

Resolved issue	Issue ID
Unable to approve a request extension if the TPAM appliance ID is 2 digits or greater.	10316
Daily Batch Reports not running.	10333
Addressed potential CSRF vulnerability.	10336
Errors managing Oracle 12 accounts.	10340
When many users are logged in to TPAM, when a user tries to view a current or past password occasionally an error message is received.	10350
Changes to address vulnerability CVE-2018-5394 (Fragment Smack)	10351
Dependent accounts for scheduled tasks on Windows 2016 systems are not being discovered.	10376
Replication alert: "Insufficient winsock resources available to complete socket connection initiation."	10382
Password check fails for IBM HMC systems.	10394
Batch update not logging any error messages when trying to add a domain functional account to a system in a different partition.	10407
After updating to Java version 8u202, TPAM is requiring Java cache to be cleared before each PSM session.	10420
The MIB file for tpamLoginFailure has a typo.	10427
Corrected typo in Administrator Guide in Managing PAR Admin ID section.	10431
Issue with certificate authentication process.	10440
LDAP authentication not validated properly when the Full Primary UserID is blank.	10441
Performance issues when deleting a large number of users at one time.	10472

Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

Table 3: General known issues

Known Issue	Issue ID
TPAM appliances are shipping out with the session log deletion global setting set	6638

Known Issue	Issue ID
at 9999 days as the default instead of 90 days. Workaround: Go to global settings and adjust the value.	
PSM file transfer using SCP can fail when a session is hosted by DPA v3 or console when older key exchange algorithms and ciphers are not allowed. SCP archive servers could have the same problem.	7346
TPAM does not support privileged password management through a DPA for Microsoft SQL Server systems using Windows authenticated functional accounts or if the network address is a named instance.	7552
A disabled Windows account with a password mismatch will be reported as a mismatch when checked through a DPA and disabled when checked through the TPAM console.	8522
For Windows accounts if a password is expired and “Use this account’s current password to change the password?” is selected, the password cannot be changed.	8639
TLS 1.2 is not supported for RDP on DPA v3.	8910

Table 4: Third-party known issues

Known Issue	Issue ID
Notifications are not occurring when restricted commands are run on Windows® 8.1 systems that have the latest Windows® updates applied. Microsoft is researching the problem, no current workaround.	7218
For Windows accounts, when the **Use this account’s password to change the password?** is selected for an account, the password change will fail if the password is longer than 63 characters.	8581
All fully patched Microsoft Windows platforms have a new Microsoft security policy setting called "**Network access: Restrict clients allowed to make remote calls to SAM**". TPAM requires that any managed account be defined to this security policy with the Allow permission for TPAM’s Check Password functionality to be successful. The managed account can be defined explicitly or as a member of a group. A Deny permission will take precedent over an Allow permission if multiple permissions exist. Further information can be found: https://support.oneidentity.com/kb/239045/	10121

System requirements

Before installing TPAM 2.5.922, ensure that your system meets the following minimum software requirements.

Browser requirements

Table 5: Browser requirements

Requirement	Details
Microsoft Internet Explorer NOTE: IE is not supported in compatibility mode.	v 10-11 (32 and 64 bit)
Mozilla Firefox	V 3.5+
Google Chrome	V 39+
Microsoft Edge	Third public release

Java requirements

Table 6: Java requirements

Requirement	Details
Java	v8 or higher required for PSM. 32 and 64 bit are supported

Standard platforms supported

In the event that a platform is not listed, it may be configured using custom platforms. The TPAM Custom Platform guide includes instructions on setting up custom platforms. For assistance configuring custom platforms please contact Professional Services.

Table 7: Standard platforms supported

Platform	Privileged Password Manager	Privileged Session Manager
AIX	✓	✓
AIX LDAP	✓	✓
AS/400	✓	✓
BoKS	✓	
BoKS Linux	✓	

Platform	Privileged Password Manager	Privileged Session Manager
Check Point SP	✓	
Cisco ACS	✓	
Cisco CatOS	✓	✓
Cisco PIX	✓	✓
Cisco Router (SSH)	✓	✓
Cisco Router (TEL)	✓	✓
CyberGuard	✓	✓
Dell Remote Access	✓	✓
Dell Remote Access 8, 9	✓	
ForeScout CounterACT	✓	✓
Fortinet	✓	
Fortinet v5	✓	
FreeBSD	✓	✓
H3C	✓	✓
HP iLO	✓	✓
HP iLO2	✓	✓
HP iLO3	✓	
HP ILO4	✓	
HP Tandem Nonstop	✓	✓
HP-UX	✓	✓
HP-UX Shadow	✓	✓
HP-UX Untrusted	✓	✓
IBM 4690 POS	✓	✓
IBM DataPower	✓	
IBM HMC	✓	✓
Juniper (JUNOS)	✓	✓
LDAP	✓	
LDAPS	✓	

Platform	Privileged Password Manager	Privileged Session Manager
Linux	✓	✓
Mac OS X	✓	✓
Mainframe	✓	✓
Mainframe ACF2	✓	✓
Mainframe LDAP ACF2	✓	
Mainframe LDAP RACF	✓	✓
Mainframe LDAP TS	✓	✓
Mainframe TS	✓	✓
MariaDB (Use MySQL platform)	✓	
Microsoft SQL Server	✓	✓ DPA required
MySQL	✓	
MySQL 5.6, 5.7	✓	
NetApp Filer 8.x	✓	
NetScreen	✓	✓
NIS+	✓	
Nokia IPSO	✓	✓
Novell NDS	✓	
OPENVMS	✓	✓
Oracle	✓	✓ DPA required
PAN-OS	✓	
PostgreSQL	✓	
PowerPassword	✓	
ProxySG	✓	
PSM ICA Access		✓ DPA required
PSM Web Access		✓ DPA required
SAP	✓	
SAP Adaptive Server Enterprise (use the	✓	

Platform	Privileged Password Manager	Privileged Session Manager
Sybase platform)		
SCO Openserver	✓	✓
Solaris	✓	✓
SonicWall (SonicOS)	✓	✓
Stratus VOS	✓	✓
Sybase	✓	✓ DPA required
Teradata	✓	
Tru64 Enhanced Security	✓	
Tru64 Untrusted	✓	
UnixWare	✓	✓
Unixware 7.X	✓	✓
VMWare vSphere 4,5,6	✓	
Windows	✓	✓
Windows 2012, 2016	✓	✓
Windows Active Directory	✓	✓
Windows Desktop	✓	✓

Upgrade and compatibility

The minimum requirement to upgrade to 2.5.922 is 2.5.920.

Installation instructions

IMPORTANT: During the time that a patch is applying, any scheduled activity, such as backups, and the daily maintenance job will NOT run.

To install TPAM 2.5.922

1. Take a backup and download it or send to an archive server.
2. Generate a support bundle and download it or send to an archive server. This can be

used by support if there are any problems after an upgrade.

3. Put the appliance in **Maintenance** mode.
4. Set the failover timeout for any replicas to 3600 seconds so that they will not failover during the patch process.
5. Select **Maint | Apply a Patch** from the menu.
6. Click the **Select File** button.
7. Click the **Browse** button. Select the patch file that you saved locally.
8. Click the **Upload** button.
9. Type the key provided on the download page in the in the **Key** box.
10. Type **/genkey** in the Options box.
11. Click the **Apply Patch** button.
12. While the patch is applying your TPAM session will end and you will have to log back in to the /admin interface.
13. Verify the patch has installed by viewing the patch log.

> **IMPORTANT:** The following errors in the patch log can be ignored: **Extracting Oracle driver updates, WARNING: error exec-command ignored, continuing** and **Extracting Teradata driver updates, WARNING: error from exec-command ignored, continuing.** If applying the patch through the CLI you will also see similar warning messages like these that can be ignored.

> NOTE: The patch process can take a long time so please be patient.

14. Once the patch has completed on the primary and replicas reboot them. **This is REQUIRED for this release.**
15. Set the appliance back to a run level of **Operational**.

Any problems applying the patch should be reported to Technical Support. Before applying the patch make sure that no active PSM sessions are running. Refer to TPAM System Administrator Guide for installation instructions.

After applying the TPAM 2.5.922 patch the following types of appliances will be patched to these versions:

DPA version 3.3.18

DPA version 4.0.19

Cache server version 2.4.5

Globalization

This release supports any single-byte character set. Double-byte or multi-byte character sets are not supported. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

This release has the following known capabilities or limitations: Although there are existing customers in all markets, the product supports US English only at this time. There is very limited support for non-US character sets and keyboards, and only in a small number of areas within the application.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.