TPAM 2.5.923

Release Notes

February 2020

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 2.5.923 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 2.5.923.

Table 1: Enhancements

Enhancement	Issue ID
Added ability to set minimum TLS version required for cache server communication from 1.0 through 1.2. New menu options have been added in the cache menu. Please see the TPAM Administrator Guide for details.	8896
Added more ciphers that can be enabled/disabled for use by the cache server. See the TPAM Administrator Guide for details.	8896
Introduced a restriction of ciphers used for TLS negotiation when only TLS 1.2 is enabled in TPAM. See the TPAM System Administrator Guide for a list of ciphers.	10457,10488
The following recommended Microsoft security updates have been included in this release to ensure TPAM is configured with the latest security updates: KB4520003,KB4525233,KB4530692,KB4534314.	10502

Resolved issues

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

Table 2: Resolved issues

Resolved issue	Issue ID
Address potential deadlock situation when creating password and session requests in high-load environments.	10483
Problems adding an account when using Internet Explorer v11	10484
Password generation could fail under heavy loads from multiple user sessions.	10485
Updated Linux platform to include additional error conditions when managing passwords.	10499
Archive server test fails when archive server name contains @ or backslash "\"	10508

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 at 9999 days as the default instead of 90 days. Workaround: Go to global settings and adjust the value.	6638
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 has this policy set to 'Allow' in order 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 2.5.923, 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 11 (32 and 64 bit)
Mozilla Firefox	v 68+
Google Chrome	v 79+
Microsoft Edge	v 44+

Java requirements

Table 6: Java requirements

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

Standard platforms supported

TPAM will only support versions of platforms that are supported by the vendor up to October 1, 2018. Versions of the platforms listed below released after that date may not work. In the event that a new version of a platform does not work or the platform is not listed below, then it is possible it may work through custom platforms. The TPAM Custom Platform guide includes instructions on setting up custom platforms. For assistance configuring custom platforms please contact Professional Services. Customers needing support for newer platforms should migrate to One Identity Safeguard. Please contract your sales representative for more information.

For TPAM releases under full and limited support we will not be adding any new platforms. For releases under full support we will look at fixing breaks that occur in the supported platforms. For releases under limited support our policy is that no new codes fixes will be generated except under extreme circumstances and at our discretion.

Table 7: Standard platforms supported

Platform	Privileged Password Manager	Privileged Session Manager
AIX	✓	✓
AIX LDAP	✓	✓
AS/400	✓	✓
BoKS	✓	
BoKS Linux	✓	
Check Point SP	✓	
Cisco ACS	✓	
Cisco CatOS	✓	✓
Cisco PIX	✓	✓
Cisco Router (SSH)	✓	✓
Cisco Router (TEL)	✓	✓
CyberGuard	✓	✓
Dell Remote Access	✓	✓
Dell Remote Access	✓	
ForeScout CounterACT	✓	✓
Fortinet	✓	
Fortinet v5	✓	
FreeBSD	✓	✓
H3C	✓	✓
HP iLO	✓	✓
HP iLO2	✓	✓
HP iLO3	✓	
HP ILO4	✓	
HP Tandem Nonstop	✓	✓

Platform	Privileged Password Manager	Privileged Session Manager
HP-UX	✓	✓
HP-UX Shadow	✓	✓
HP-UX Untrusted	✓	✓
IBM 4690 POS	✓	✓
IBM DataPower	✓	
IBM HMC	✓	✓
Juniper (JUNOS)	✓	✓
LDAP	✓	
LDAPS	✓	
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

Platform	Privileged Password Manager	Privileged Session Manager
PAN-OS	✓	
PostgreSQL	✓	
PowerPassword	✓	
ProxySG	✓	
PSM ICA Access		✓ DPA required
PSM Web Access		✓ DPA required
SAP	✓	
SAP Adaptive Server Enterprise (use the 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 2.5.923 TPAM is 2.5.920 AND OSPatch_4474419 MUST be installed on the primary and all replicas prior to installing 2.5.923. The 2.5.923

patch will fail if OSPatch_4474419 is not installed.

Installation instructions

IMPORTANT: OSPATCH_4474419 must be installed on the primary and all replicas prior to installing TPAM 2.5.923

NOTE: For customers with replicas start at Step 1. If patching a standalone TPAM proceed to Step 6.

To install TPAM 2.5.923

1. Log in to the TPAM /admin interface.
2. Set the **Replication Interval** global setting to a minimum value of **900**.
3. On the Cluster Management page select the Primary from the role list and click the **Restart Clustering** button.
4. On the Cluster Management page select each Replica from the role list and set the **Failover Timeout** to **3600**.
5. Set the **Database Backup Set Max Incr Usage MB** global setting to a value of **4096**.
6. On the Cluster Management page set the Run level to **Maintenance**.
7. Take a backup of the TPAM appliance.
8. Copy the supplied .zip file to your local computer.
9. 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.
10. Select **Maint | Apply a Patch** from the menu.
11. Click the **Select File** button.
12. Click the **Browse** button. Select the patch file that you saved locally.
13. Click the **Upload** button.
14. Type the key provided on the download page in the in the **Key** box.
15. Type **/genkey** in the Options box.
16. By default, if you are applying a patch to a primary member of a cluster, the replicas in the cluster will be listed and highlighted in the Target Replicas list. If any of the replicas are deselected, the patch will not be applied to it, unless it is directly applied by logging on to the replica or applying to the replica through the CLI/API.
17. Click the **Apply Patch** button.

18. While the patch is applying your TPAM session will end and you will have to log back in to the /admin interface.
19. Confirm that the patch has finished applying by checking the patch log on the primary and the Proc Log on the replicas, if applicable. **THE PATCH PROCESS CAN TAKE A LONG TIME SO PLEASE BE PATIENT.**

    IMPORTANT: The following errors in the patch log can be ignored: Cleaning up for Teradata 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
20. If your configuration includes a cache instance (physical or virtual) log on to the cache and select **Show Appliance Status** to confirm that the cache version is now 2.4.6.
21. **Reboot the primary and all the replicas once the patch has successfully completed on ALL appliances.**
22. Put the TPAM primary appliance back at a run level of **Operational**.

Any problems applying the patch should be reported to Technical Support.

After applying the TPAM 2.5.923 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 2.4.6

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.

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.