TPAM 2.5.921

Release Notes

July 2018

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 2.5.921 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 2.5.921.

Table 1: General enhancements

Enhancement	Issue ID
Can configure up to three syslog servers.	8851
Added TPAM version number to description column of the restore point listing.	9175
Using PSM Web Access can now download a file to DPAv4 and transfer it to local PC. For more details see the TPAM Client Setup Guide.	9675
Added One Identity Starling Two-Factor RADIUS Agent as external authentication option. The Starling Two-Factor RADIUS Agent allows customers to utilize their Starling SaaS subscriptions as a two-factor authenticator for any internal applications that allow RADIUS authentication.	9878
Added **Use Modify** field for LDAP/LDAPS system configuration. See the TPAM Administrator or Partition Administrator Guide for details.	9911
Alerts will contain the appliance name of the appliance that generated the alert.	9957
Improved the speed of the DPA patching process after a DPA is enrolled with TPAM.	10145
If a replica is in Maintenance mode now prevent failover to that replica.	10147
Increased the Restricted IP Address field for API/CLI user ID's to 200 characters.	10163
Now log user type when user ID's are added to TPAM.	10175
A TPAM cluster can be joined to a customer's Starling SaaS subscription. New alerts available for subscription related on Starling Monitor problems. New Starling Monitor log to monitor problems with Approval Anywhere and Starling Join. For more details see the TPAM System Administrator Guide.	10203
If a customer joins their TPAM cluster to Starling then TPAM users can be configured to use Approval Anywhere to receive push notifications to their mobile phone for TPAM requests that require approvals. For more details see the TPAM Administrator Guide or the TPAM Approvers Guide.	10204
OCSP (Online Certificate Status Protocol) check failures are logged in the Security log.	10226
Added logging to the proc log of CLR related errors encountered when generating passwords.	10228
Performance enhancements made to cache server initialization process.	10258
Added StarlingJoinInfo and Starling Monitor Log to support bundle.	10267

Resolved issues

The following is a list of issues addressed in this release.

Table 2: General resolved issues

Resolved Issue	Issue ID
PSM session using SYS account not working for Oracle platforms.	6541
Microsoft SQL Server connections using SSL not working through DPA.	8915
Error managing VMware ESXi 6.0 accounts when TLS set to 1.2.	9594
CheckPassword and ResetPassword Java API commands are not returning the entire output.	10107
When batch processing affinity assignments for collections, assignments for DPA v3's are not updating even though TLS is set to 1.0.	10161
For jumpbox platforms after requesting %newacctpwd%, the results are not being displayed in the output.	10164
When clicking the **Edit LDAP Mapping** or **Edit GN Mapping** buttons on the Systems Management page the filter on the associated Auto Discovery page is not parsing out Partition information.	10169
Data is missing when exporting reports as a result of a bug with the Max Rows to Display field.	10189
When changing an existing user password in the User Management or Sys-Admin User Management web pages a comma in the password would cause the rest of the password to be ignored. Does not affect initial password assignment, batch processing, or users changing their own passwords.	10190
Windows and Windows Active Directory accounts not being unlocked after password reset through a DPA.	10198
Receive error importing a web certificate.	10201
Unable to auto-discover systems on secondary Windows Active Directory domain that uses functional account from the primary domain.	10209
DPA v4 set to UTC time zone by default.	10213
Password change for PAN-OS accounts, with DSS key based functional account, reported as successful but results show error.	10240
A password change on PAN-OS firewall that is in HA mode but not synchronized fails.	10241

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
Session times out for a user logged in to TPAM using Internet Explorer® 8/9. The user tries to log back in and gets the message “Your session has timed out or been disconnected. Please close this browser and open a new one to reconnect”. Workaround: Close all open browsers before you can log back in to TPAM.	3391
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	10121

Known Issue	Issue ID
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/	

System requirements

Before installing TPAM 2.5.921, 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 9-11 (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	✓	
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	✓	

Platform	Privileged Password Manager	Privileged Session Manager
HP Tandem Nonstop	✓	✓
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	✓	

Platform	Privileged Password Manager	Privileged Session Manager
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 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 2.5.921 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 2.5.921

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. Reboot the primary and any replicas. **Once the appliance comes back up wait 5 minutes before proceeding to the next step.**
6. Select **Maint | Apply a Patch** from the menu.
7. Click the **Select File** button.
8. Click the **Browse** button. Select the patch file that you saved locally.
9. Click the **Upload** button.
10. Type the key provided on the download page in the in the **Key** box.
11. Type **/genkey** in the Options box.
12. Click the **Apply Patch** button.
13. While the patch is applying your TPAM session will end and you will have to log back in to the /admin interface.
14. Verify the patch has installed by viewing the patch log.

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

15. Set the appliance back to a run level of Operational.

    > NOTE: A cache server operating system resource setting has been modified in TPAM 2.5.921. After upgrading to 2.5.921 (cache server revision 2.4.5), the cache server appliance should be restarted to apply this setting change (note that this is a restart of the appliance, not just disable/enable of the cache server application). If desired, the restart can be delayed until a future maintenance window since the cache server application will continue running with the previous operating system resource setting until the restart is performed.

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 2.5.920 patch the following types of appliances will be patched to these versions:

DPA version 3.3.17

DPA version 4.0.18

Cache server v2.4.5

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.