TPAM 2.5.920

Release Notes

October 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 2.5.920 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 2.5.920.

Table 1: General enhancements

Enhancement	Issue ID
If a password is entered for a manually managed account that does not match the assigned password rule a warning message will appear.	6901
Updated PuTTY to support more key exchange algorithms and ciphers.	7346
Added Approvers in sequence. The order that groups must approve a password, session, or file request may now be specified. Changes made to Batch Import/Update Accounts and Batch Update PSM Details to accommodate the changes. For more details see the TPAM Administration Guide.	7465
Added ability for requestors to extend requested time for a password, session or file request. Global settings and automatic email notifications have been added for this functionality. New tabs added for requesting, approving, and reviewing extensions. Please see the Global Settings section of the TPAM System Administrator Guide and the Request and Approve chapters in the TPAM Administrator, Requestor and Approver Guides.	7472
Added a new audit report called "Request Extensions". Added new batch report called "Request Extension Activity (Daily)". Added Original Release Duration and Expires Date to the following on demand reports: Password Currently In-Use, Password Requests, Session Requests. Added Original Expiration Date and Duration to the following batch reports: Approver Activity (Daily), Reviewer Activity (Daily), Session Activity Detailed (Daily), Pending Password Release Reviews and Pending PSM Session Reviews.	7472
Added three new email notifications that can be turned on: Session Request End, Password Release Request End and File Request End. If enabled these will send email notification to the selected users when these requests are expired, whether expired early, or at the scheduled time.	7567
Added filter criteria of system and account description when adding or listing password, session or file requests.	7944
Added method to update dependent systems through batch processing.	8143
Added setting to Password Change Profiles to prevent a synchronized password change when one of the subscribers has an active password release.	8167
Added PostgreSQL as a supported platform for password management.	8319
Added a global setting to set the minimum acceptable TLS level (1.0 through 1.2). This global setting applies to all inbound communication to the TPAM Web application, as well as the inter-appliance communication for all TPAM appliances in a cluster. Outbound communication to managed targets will attempt to communicate using TLS 1.2 (where applicable), but can be permitted to negotiate down to lower levels if the target device does not support TLS 1.2. For more information see the TPAM System Administrator Guide.	8720 9390 9520 9664

Enhancement	Issue ID
IMPORTANT: DPA v3 used for PSM requires a TLS setting of 0 (TLS 1.0).	
Added more information to the Run Level help bubble on the Cluster Management page.	8747
Added a new blind carbon copy (bcc) option on the Mail Agent Setting page in the /admin interface. If selected, Bcc will be used for all recipients on the email when there is more than one recipient.	8954
Updated RSA DLLs to version 8.1.0.4.	8975
Added "pfiles" command as an option to retrieve network connection information from a target system when using event capture/restricted commands. This can be used with Solaris systems.	9004
X3270- Automatic Login proxy type for PSM sessions now available when creating custom platforms.	9019
When a password, session or file request expires it will be logged in the Activity log.	9021
Requestors can create a list of their most requested accounts, sessions and files and designate them as "Preferred Requests". See the TPAM Administrator and Requestor Guides for details.	9022
Added appliance status (active/not active) to the TPAM status page at *https://t-pamipaddress/status*	9245
Added a setting on Password Change Profiles that, if enabled, will prevent a requestor from obtaining a password *X* minutes after any password reset. ISA password retrieval is not affected by this setting.	9324
Automatic log on to the mainframe no longer requires user interaction.	9399
Changes made to TPAM's web interface password request screens to aid users of screen reader software.	9426
Can generate a support bundle from a replica appliance without it being in the "failed over" state.	9433
Added a yearly version of the PSM active sessions graph. Can be used to review concurrent session licenses.	9474
On password check and change profiles changed the minimum length of window to 15 minutes, and changed the minimum period between windows to 5 minutes.	9477
Improvements made to cache server for system/account/user/permission data handling. Increased number of database connections in the pool.	9483
Added ability to use some 256 bit ciphers on cache server. Added new menu option on the cache server to select the ciphers used by the application server.	9487

Enhancement	Issue ID
Performance improvements made when querying list of accounts for a PSM session request.	9558
Modified event capture/restricted command code to use updated SSH client during sessions to *nix systems. The updated SSH client provides additional and more secure ciphers than the prior SSH client code.	9564
Added a filter parameter for subscriber status on the Synchronized Password Management filter tab.	9596
Now passing the NetBIOS name for NetApp domain accounts.	9618
Updated the 3270 client for DPA 3's. After applying TPAM 2.5.920 DPA's will patch to version 3.3.17.	9681
Daily maintenance job will detect and remove any orphaned sessions.	9723
When using :myaccount: for PSM sessions, if the TPAM user is using external authentication, then the user's primary authentication ID will be passed instead of their TPAM user name.	9737
Now allow for TCP connection for MS SQL Server when using Windows functional account.	9750
Confirmed that Java 9 is compatible with TPAM for PSM.	9774
Added text on TPAM Trsuted CA Certificate page of a failed over replica as a reminder that any certificates loaded on the failed over replica will be removed after it fails back.	9844
Added Dell Remote Access versions 8 and 9 as supported platforms for password management.	9847 10056
Added Fortinet version 5 as a supported platform for password management.	9897 9929
Added detailed logging for all cache configuration updates, including permission assignments.	9903
Updated time zones with latest time zone update from Microsoft.	10012
Added a new report, "DPA Affinity", to view affinity assignments. Added "Affinity" tab to the DPA Management page to view affinity assignments.	10104

Table 2: CLI/API enhancements

Enhancement	Issue ID
For Approvers in sequence, added parameter of --MultiGroupApprovers to AddAcount, UpdateAccount, and UpdatePSMAccount commands. Added MultiGroupApprovers as output to ListAccounts and ListPSMAccounts	7465

Enhancement	Issue ID
commands.	
Added CLI/API commands for adding request extensions, approving/denying request extensions, and listing request extensions. For more details see the CLI chapter of the TPAM Administrator Guide.	7472
Added result columns of OriginalRequestDuration and OriginalExpiresDate to the GetPwdRequest and GetSessionRequest commands.	9812
Old legacy commands being retired: ListEGPAccounts, replaced by ListPSMAccounts and UpdateEGPAccount is replaced by UpdatePSMAccount. See the CLI chapter in the TPAM Administrator Guide for more details.	9837

Resolved issues

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

Table 3: General resolved issues

Resolved Issue	Issue ID
TPAM not able to check password for newer versions of MySQL.	8467
HP iLo 2 password not changing after upgrading to TPAM 2.5.916	9276
If a user's local time zone is set to UTC, the expiration date on the request page is not displayed in UTC.	9364
Problems with the User Entitlement report related to orphaned access policies.	9444
Alert emails not being sent even though the mail agent is running.	9476
PSM session using auto login to an AS400 system fails if the password contains a dollar sign ($).	9490
Cache server locking up. Added code to monitor shutting down of application server on cache server and force a shutdown if needed.	9595
Stuck shift key during PSM session causes a single mouse click to select multiple items.	9656
If a group name begins with a number or contains a dollar sign ($), erroneous data will show in the MultiGroupApproverNames column in the Accounts data extract.	9659
Slow performance as a result of many check and change processes running at the same time of heavy usage by interactive web based users.	9663
When performing password check/change on Cisco ACS getting "500 SSL	9668

Resolved Issue	Issue ID
negotiation failure."	
HP iLO 2 not working using DSS keys.	9672
CLI command AddPwdRequest with --ForUserName parameter is not using the time zone of the --ForUserName for the request times.	9673
CLI/API users can access a failed over replica while it is in the failing back process.	9690
Test system and check password failing for SAP ASE 16.0 using TPAM Sybase platform.	9697
Mainframe test system and check password reported as successful even though functional account userID is revoked.	9706
More than one gossip graph being displayed for a DPA when only one should appear.	9721
The date format in reports exported to CSV are not reflecting the date format selected in Global Settings.	9730
Missing expiration dates on the Expired Password report.	9734
Entering a backslash (\) in the account description field gets displayed as a double backslash in the description column on the Request Password and Request Session Listing page.	9761
An ISA user assigned to a partition can see password check and change profile names from other partitions in filter dropdowns.	9766
AltGR key not working with Italian keyboard during PSM session.	9771
After pasting in a user certificate thumbprint and clicking save changes, receive message "No Changes to Save".	9823
RSA Radius not working with TPAM because of hard coded NAS-IP-Address.	9828
Cannot run archive log using a single date as the filter. No results returned.	9868
Alert log reports "Failed processing message for cache server, Error: Document requires an element".	9924
Cache server rebooting and showing as disabled.	9937
If you are on TPAM 2.5.919 and configure transferring backups to an archive server for the first time, the auto archiving will fail.	9941
For PSM sessions using RDP proxy type, if NLA is not required on the Windows target system, you cannot enter return for username and password to get to the Windows GINA.	9943
Daily maintenance job is reporting failures when attempting to hard delete systems during the purge trash step.	9947

Resolved Issue	Issue ID
	10006
Fixed typo for Client ID for SAP systems in the documentation.	9958
Replica is still communicating with a DPA that is no longer a part of the cluster.	9968
Unable to edit DSS Key details for some custom platforms.	9973
If Radius secret contains certain characters, it will cause problems with the display of the Radius configuration page in TPAM.	9983
Failed login data is not removed from a TPAM appliance that is removed from a cluster when the Remove and Reset data option is selected.	9986
When using DPA to connect to Citrix, EULA acceptance message appears on every connection.	9988
Replica sending "Cannot connect to the cache server" alert emails.	9994
Login banner displays multiple times for users logging in using Radius or SecurID with a challenge required.	10008
File transfer not working with Authentication Services.	10009
Unable to reset a managed parmaster password through the kiosk.	10018
Receiving alert, "An error occurred that caused mail processing to abort. The step is unable to communicate to the SMTP server at XXXXXX. No mail will be sent."	10027
PAC (Privileged Access) users allowed to request and access password, even if the number of required approvers for the account are not assigned.	10053
Receive an error when trying to edit the MTU size on a replica.	10055
Batch update system error occurs when updating system requiring NetBiosName.	10067
When using PSM Web Access, TPAM is changing the restricted URL to all capital letters.	10069
Batch update of system domain functional account information not working.	10073
File transfer fails if file name contains a dollar sign ($).	10082
Users with only ISA or Reviewer permissions get no data returned when running the User Entitlement report.	10083
An attempt of uploading a file with a file name longer than 60 characters during file transfer results in a false positive.	10084
If ISA password retrievals are set to require a reason code, the CLI/API Retrieve command is not enforcing that rule.	10088

Resolved Issue	Issue ID
PSM session is not immediately terminated when approver denies a previously approved request.	10135

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 4: 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
Microsoft SQL Server connections using SSL will not work through a DPA.	8915

Table 5: 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®	7218

Known Issue	Issue ID
8.1 systems that have the latest Windows® updates applied. Microsoft is researching the problem, no current workaround.	
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 2.5.920, ensure that your system meets the following minimum software requirements.

Browser requirements

Table 6: 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 7: 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 8: 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	✓	

Platform	Privileged Password Manager	Privileged Session Manager
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	✓	
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	✓	

Platform	Privileged Password Manager	Privileged Session Manager
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 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	✓	

Platform	Privileged Password Manager	Privileged Session Manager
Windows	✓	✓
Windows 2012, 2016	✓	✓
Windows Active Directory	✓	✓
Windows Desktop	✓	✓

Upgrade and compatibility

The minimum requirement to upgrade to 2.5.920 is 2.5.913 AND OSPatch_3106991 MUST be installed on the primary and all replicas prior to installing 2.5.920. **The 2.5.920 patch will fail if OSPatch_3106991 is not installed.**

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 2.5.920

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.
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. Once the patch has completed on the primary and replicas reboot them. This is REQUIRED for this release.
16. After the appliances have been rebooted, log on to the primary admin interface and select **Backup | Modify Backup** from the menu. Click the **Backup Now** button.
17. Set the appliance back to a run level of Operational.

IMPORTANT: **If** you use RSA SecurID for external authentication **AND** you have **NOT** installed hotfix 7196 or 7196v2 then after installing 2.5.920 you should reimport sdconf.rec into TPAM and clear the node secret(s) on the SecurID server. A new node secret will be generated upon the next SecurID authentication request.

IMPORTANT: **If** you upgraded to TPAM 2.5.920 from TPAM **2.5.918 or lower**, **AND** you have cache servers, after the patch is installed, go to the Cache Server Management Details tab, clear the **Enabled** check box and click the **Save Changes** button. Wait one minute. Select the **Enabled** check box and click the **Save Changes** button. A large file will be copied from the TPAM console to the cache server. This file transfer must complete before the Java application server on the cache server appliance will be started. Repeat this process for all your cache servers.

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 4.0.17

Cache server v2.4.4

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.