TPAM 2.5.919

Release Notes

September 2017

These release notes provide information about the The Privileged Appliance and Modules (TPAM) 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 2.5.919 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 2.5.919.

Table 1: General enhancements

Enhancement	Issue ID
In email notification configuration, message tags can be entered on the subject line.	BFER 2258
Added an export file that lists the alert MIB name, OID, severity level, and alert MIB description for all TPAM alerts. See the Alerts chapter in the TPAM System Administrator Guide for more details.	BFER 6166
Auto account discovery uses the system PPM affinity to process account discovery, DPAs will not be used for account discovery in cases where SSH Tunneling is used or a specific port is not allowed.	BFER 7284
Allow any non-alpha numeric character, except for double quote (“), to be typed in the Server Secret field for Radius and Defender external authentication.	BFER 7933
Uppercase letters are no longer required in the TPAM Computer Name field on the System Information tab.	BFER 8130
Added requestID and sessionlogID to the Session Logs tab for Archived Files on the Archive Server Management page.	BFER 8134
Added support for all **Alt Gr** keyboard mappings for Spanish keyboard.	BFER 8369
Ability to launch PSM session window as full screen.	BFER 8535
Manage Accounts and Manage Systems results pages now allow results up to 5,000 rows.	BFER 8597
TPAM backups can now be sent to more than one archive server.	BFER 8613
Can paste Georgian characters from the local desktop into a PSM session. Added Georgian as a language option on session connect options tab.	BFER 8618
Added functional account name to the Password Consecutive Check/Change Failures report.	BFER 8970
Added IBM DataPower as a supported platform for password management.	BFER 9060
The manage systems and manage accounts listing tabs now have adjustable column widths and the column width can be saved as default filter settings.	BFER 9061
Added new global setting that controls the behavior of the account Past Password tab for TPAM Administrators, Partition Administrators, and PPM ISAs. Depending on the setting, the tab may be disabled or a warning message presented every time it is accessed.	BFER 9135
Microsoft Edge browser is supported.	BFER 9153
Added data extract data set called CombinedEntitlements that reports on user PPM and PSM entitlements in one report.	BFER 9164

Enhancement	Issue ID
In email notification configuration added a new setting: **If email is generated from a failed over replica, send additional link to the replica network address.** If selected, the email will include a link from the failed over replica as well as the link from the original primary.	BFER 9170
In email notification configuration, a value of **DefaultNetworkAddress**, in the **Use the same URL for all Application Page links setting**, will always resolve to the IP address of the appliance sending the email.	BFER 9170
Added partitions to TPAM. Partitions are a logical separation of objects within a single TPAM deployment. TPAM System Administrators control the rules around the creation of partitions with new global settings. (See the Global Settings chapter of the System Administrator Guide) Partition Administrators can perform equivalent functionality to the current administrator role, but only for objects within that partition they are assigned. For more details see the TPAM Administrator Guide and Partition Administrator Guide.	BFER 9188
Added 3 global settings that control whether partitions are allowed in TPAM and the rules governing them. For more details see the Global Settings chapter in the TPAM System Administrator Guide.	BFER 9188
On the Batch Processing pages, changed the page layout. The Show Template button is now a Template tab.	BFER 9188
Added ability to configure MTU size on the Network Settings page in the /config interface.	BFER 9195
Cache user certificates now created with X.509 v3.	BFER 9225
Added LastChangeDt, LastAttemptedChangeDt, LastCheckDt, and LastSuccessfulCheckDt to the results for List Accounts, export to Excel or CSV.	BFER 9252
Added count of PSM enabled systems to the System Status page and Support Bundle.	BFER 9259
A change from release 2.5.916 for Windows Desktop platform has been reverted to the original behavior. Release 2.5.916 changed the platform to determine the target's computer name before attempting to change the target account's password. In this release, if the computer name is populated in TPAM, no attempt to determine the computer name is made.	BFER 9270
Performance improvements made for retrieving data on manage cache server permissions page.	BFER 9279
A PSM reviewer can now see the session log ID on the Session Logs listing page and in the title bar of the session replay if not in full screen mode.	BFER 9331
Added new flag on Password Change Profiles: **Send notification only. Require interactive forced reset**. If selected, scheduled password changes will **NOT** automatically be done by TPAM, instead an email notification will be sent to the system and account owners that it is time for a	BFER 9338

Enhancement	Issue ID
scheduled change. TPAM Administrators, Partition Administrators and PPM ISAs must change the password through a forced reset.	
Session logs from sessions that were not recorded will now be affected by the settings configured for session log archival and deletion.	BFER 9350
If a DPA performs the password check or change, the DPA Name is included in the password check and change logs and other password reports.	BFER 9368
Batch processing history results can be exported to Excel or CSV files. Batch history detail can be exported to Excel.	BFER 9380
Added a warning message on the profile management page for the check and change password profiles that are assigned to the factory default system template.	BFER 9462
Made changes to Solaris event capture, but 3des-cbc or blowfish-cbc cipher needs to be added to client sshd_config.	BFER 9475
DPA v4 can now handle file transfers for target servers that have SMBv1 disabled. SMB v2, 2.1 or 3 must be enabled on the target.	BFER 9541

Table 2: CLI/API enhancements

Enhancement	Issue ID
Added a parameter of --PartitionName to most of the CLI/API commands. See the API and CLI chapters of the TPAM Administrator Guide for details.	BFER 9188
Added global setting to log all CLI, API, and Sys-Admin CLI calls in the appropriate activity log. The default setting is off.	BFER 9226
Added LastChangeDt, LastAttemptedChangeDt, LastCheckDt, and LastSuccessfulCheckDt to the results for the ListAccounts command.	BFER 9252
Add new parameter, --NotifyOnlyFlag to AddProfile and UpdateProfile commands for PasswordChange profile types.	BFER 9338

Resolved issues

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

Table 3: General resolved issues

Resolved Issue	Issue ID
When failing back to a primary, the status page on the replica does not reflect the "failing back" status on the cluster status page.	BFER 7315

Resolved Issue	Issue ID
Werfault (Windows error reporting) processes visible in the process list file of a support bundle.	BFER 8542
For custom platforms the %acctdesc% (Account Description field) field is empty regardless of the data entered and saved in the field.	BFER 8645/9144
LDAP Auto Discovery fails with "search filter is invalid" error.	BFER 8883
Unexpected reboot of TPAM appliance.	BFER 8931
Using Internet Explorer, approvers do not see a scroll bar for the request reason field.	BFER 8957
Password checks fail on Linux systems if password contains * (asterisk) or \ (backslash).	BFER 9149
Some of the logs reports in the /admin interface are not handling the end date filter consistently. Some report data on the end date and some do not.	BFER 9155
TPAM hanging and requiring reboot related to a memory leak issue.	BFER 9185
When the load balancer hits the cache status page, the load balancer is unable to supply a client certificate.	BFER 9172
Password reset fails for NetApp Data ONTAP 8.24P4 7-mode systems.	BFER 9187
Some support bundles contain empty SQL graphs.	BFER 9202
With over 4500 password check and changes profiles the system and account management pages may have display problems.	BFER 9203
Test system fails for HP-UX system.	BFER 9207
An ISA with permissions on an account cannot duplicate the account.	BFER 9218
Cannot remove a DPA from a cluster.	BFER 9248
NetApp system only allowing one ssh connection at a time.	BFER 9267
Unable to approve password request when assigned ticket system name is greater than 30 characters.	BFER 9272
Discrepancy between the Passwords Currently In Use report and the Expired Passwords report.	BFER 9277
PSM session deadlocks and problems canceling sessions.	BFER 9278
If selected, the "Do not change password after Requests" check box on password change profiles is not working with manually managed accounts.	BFER 9281
Exporting the Password Consecutive Failures report to Excel or CSV limits the output to the first 5000 rows.	BFER 9291
If the Global Setting date format is set to DDMMYYYY, there are issues with	BFER 9283

Resolved Issue	Issue ID
start and end dates for Message of the Day.	
TPAM performance sluggish as a result of PSM archive delete failures.	BFER 9293
A PPM ISA cannot access the Password Management menu.	BFER 9294
MIB file does not contain SNMP v2 traps.	BFER 9296
When adding a synchronized password subscriber, receive error "Cannot insert duplicate key row in object 'dbo.SyncPassSubscribers' with unique index 'IX_SynchPassSubscribers'.	BFER 9302
When generating a new web certificate request, clicking the **Download Now** button results in an error.	BFER 9303
Generic Integration is truncating the network address field at 35 characters.	BFER 9314
PSM archive to FTP server not working.	BFER 9318
Auto Discovery for Windows Active Directory systems not working using a domain account.	BFER 9328
If logged in to TPAM with the same user name that was previously used for a deleted user, the first name and last name of the deleted user will intermittently display in the Activity log.	BFER 9329
During password checks and changes, no priority is given to the least recently checked/changed accounts.	BFER 9334
For Access Policies, the Assigned Count total on the Used By tab, is including soft deleted systems and accounts.	BFER 9347
When batch updating accounts, the Reviews Required field is getting updated incorrectly.	BFER 9352
When running the User Entitlement report, typing a space in the System Name or Collection Name report filter leads to erroneous results.	BFER 9356
When a soft deleted account is un-deleted, and the current password is released, there is no post release reset scheduled.	BFER 9336
When the "missing current password" error occurs, the change agent is not handling it as a password mismatch.	BFER 9339
Empty session logs are not aging as they should based on archive settings.	BFER 9343
Errant permissions granted for accounts on systems created from system templates.	BFER 9363
When retrieving session request details for a session request that is part of a multiple account request, all zero (0) characters are removed from the RequestID when it is selected for display.	BFER 9372

Resolved Issue	Issue ID
Batch update systems is not requiring that a Check and Change Password Profile is listed when updating a system to Yes for Auto Password Management. Batch update systems is not requiring that if a Release Duration is specified that Auto Password Management is set to Yes.	BFER 9385
A review cannot be completed because the specified reviewer was also the requestor.	BFER 9395
DPA cluster status is operational and failed after setting DPA to inactive and back to active again.	BFER 9398
Error running the Sys-Admin Activity log if there are user names longer than 20 characters.	BFER 9401
If a PAC user (privileged access user) requests a session using automatic login (no password released) and the PPM required approvals on the account are >0 then a Session Request Response Notification email is being sent in error.	BFER 9405
Manual password change notification emails are triggering password changes on dependent systems.	BFER 9414
File transfer through a DPA for Windows system using FQDN for system IP address does not work.	BFER 9419
PasswordReleaseActivity data extract has a blank column with no header.	BFER 9451
Dependent password change failures are not being retried.	BFER 9453
File transfer is failing using :myaccount: with file transfer credentials set to **Same as Session Authentication**.	BFER 9457
Performance problems removing large quantities of collection members through batch add/drop collection members.	BFER 9471
If the system date format is set to MM/DD/YYYY AM/PM and a request is submitted where the end date passes 12:00, then the estimated expiration date for the request is incorrect.	BFER 9489
When adding/removing a dependent system to an account, if any other account edits are made at the same time, the dependent system assignment is not saved.	BFER 9559
Issues editing and saving the **Send email X days before scheduled change to X** setting on the Password Change Profile editor page.	BFER 9581

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.	BFER 6638
A user, who only has ISA permissions on collections with no members, may get an error when trying to add a new system. Workaround: Grant the PPM or PSM ISA permissions on at least one other system to be able to add a new system.	BFER 7351
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.	BFER 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.	BFER 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.	BFER 8639
When starting a PSM session using SSH proxy type, session may fail to connect and result in a "broken pipe" error message. Workaround: Start another xterm within the PSM session. To help avoid the issue, the LoginGraceTime value in the sshd_config on the target system can be increased.	BFER 8652
TLS 1.2 is not supported for RDP on DPA v3.X.	BFER 8910

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.	BFER 3391
After updating Java™ 7 with update 45 you may see a Java™ error message when running a PSM session. Workaround: Go to Java™ in the Control Panel and clear the Java™ cache.	BFER 5827
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.	BFER 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.	BFER 8581

System requirements

Before installing TPAM 2.5.919, 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	v7 update 45+ 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	✓	✓

Platform	Privileged Password Manager	Privileged Session Manager
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	✓	✓
ForeScout CounterACT	✓	✓
Fortinet	✓	
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)	✓	✓

Platform	Privileged Password Manager	Privileged Session Manager
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	✓	
NetApp Filer 8.x	✓	
NetScreen	✓	✓
NIS+	✓	
Nokia IPSO	✓	✓
Novell NDS	✓	
OPENVMS	✓	✓
Oracle	✓	✓ DPA required
PAN-OS	✓	
PowerPassword	✓	
ProxySG	✓	
PSM ICA Access		✓ DPA required
PSM Web Access		✓ DPA required
SAP	✓	
SAP Adaptive Server Enterprise (use the Sybase platform)	✓	

Platform	Privileged Password Manager	Privileged Session Manager
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 2.5.919 is 2.5.904.

Installation instructions

To install TPAM 2.5.919

1. Take a backup and save it.
2. Generate a support bundle and save it. 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 reboot the primary appliance. If there are replicas in the cluster, check the Cluster Status tab to ensure the replicas have also been upgraded. Once the replicas have upgraded these should also be rebooted.
16. Set the appliance back to a run level of Operational.

IMPORTANT: If 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.

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.