The Privileged Appliance and Modules 2.5.923

Auditor Guide

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

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

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

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.

Contents

Permission Based Home Page

Introduction

This document has been prepared to assist you in becoming familiar with The Privileged Appliance and Modules (TPAM). It is intended for TPAM auditors.

If the TPAM system has partitions created, as an auditor you will have visibility to date in all partitions.

Your home page is based on the user type and permissions assigned to your user ID in the TPAM application. You can return to the home page from anywhere in the TPAM application by clicking the **home icon** located on the far left side of the menu ribbon.

Message of the Day Tab

The first tab that displays is the default message of the day, which is configured through the admin interface.

Recent Activity Tab

The recent activity tab shows all your activity in TPAM for the last 7 days.

Pending reviews tab

As an auditor you will see all pending reviews, regardless if you have review permissions on the account. By clicking on the request id you are taken directly to the Password Release Review Details or Session Review Details tab. As an auditor you can always enter review comments. To use the auto-refresh option select the box and type the number of minutes you would like the window refreshed.

Manage Your TPAM User ID

Any user may change their password and update individual account details using the User menu option.

To reset your password:

1. From the User Menu select **Change Password**.
2. Enter the Old Password, the New Password, and Confirm New Password.
3. Click the **Save Changes** button.

ⓘ NOTE: User passwords are subject to the requirements of the Default Password Rule.

To edit your user details:

1. From the User menu select **User Details**.
2. Make changes in the following fields:

Table 1: Fields available on My User Details

Field name	Description
Phone Number	Phone number that is associated with your user id in TPAM.
Mobile Number	Mobile number that is associated with your user id in TPAM.
E-mail	The email address that TPAM will use for email notifications from TPAM.
My Timezone	The appropriate time zone must be chosen from the list. With this option most dates and times that the user sees in the application or on reports are converted to their local time. If a date or time still reflects server time it is noted on the window.
Description	The description box may be used to provide additional details about the user.
CLI Key Passphrase	Only applies to CLI users. This is an optional pass phrase to encrypt the user’s private key. The phrase is case sensitive, up to 128 characters, and does not allow double quotes (“). The phrase is not stored and cannot be retrieved after the key is generated.
Reset CLI Key	Click this button to create a new CLI key for the user ID.

Field name	Description
Get CLI Key	Click the button to retrieve the new CLI key.
Get API Key	Click this button to create a new API key for the user ID.
Get API Key	Click the button to retrieve the new API key.

NOTE: If the System-Administrator disables User Time zone changes in the /admin interface the User Time Zone Information block shown above is visible only for Administrator users.

3. Click the **Save Changes** button.

2

Systems

Introduction

This chapter covers the steps to list systems in TPAM.

List systems

The List Systems option allows you to export the system data from TPAM to Microsoft Excel or CSV format. This is a convenient way to provide an offline work sheet and also to provide data that may be imported into another TPAM – for example, to populate a lab appliance with data for testing, without making the lower level changes that restoring a backup would cause.

To list the systems:

1. Select **Systems, Accounts, & Collections | Systems | List Systems** from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Layout** tab to select the columns and sort order for the listing.
4. To view and store the data outside of the TPAM interface, click the **Export to Excel** button, or the **Export to CSV** button.
5. To view the data in the TPAM interface, click the **Listing** tab.
6. To view collection membership for a system, select the system and click the **Collections** tab.
7. To view the permissions assigned for the system, select the system and click the **Permissions** tab.

Local appliance systems

When looking at the system listing in TPAM, you will see two systems that are there by default, Local_Appliance_paradmin, and Local_Appliance_parmaster. These systems do not count against the total licensed systems in TPAM and are used for managing the paradmin and parmaster accounts if desired.

3

Accounts

Introduction

This chapter covers the steps to list accounts in TPAM.

List accounts

The List Accounts option allows you to export the account data from TPAM to Microsoft Excel or CSV format. This is a convenient way to provide an offline work sheet and also to provide data that may be imported into another TPAM – for example, to populate a lab appliance with data for testing, without making the lower level changes that restoring a backup would cause.

To list the accounts:

1. Select **Systems, Accounts, & Collections | Accounts | List Accounts** from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Layout** tab to select the columns and sort order for the listing.
4. To view and store the data outside of the TPAM interface, click the **Export to Excel** button, or the **Export to CSV** button.
5. To view the data in the TPAM interface, click the **Listing** tab.
6. To view collection membership for an account, select the account and click the **Collections** tab.
7. To view the permissions assigned to the account, select the account and click the **Permissions** tab.

List PSM accounts

The List PSM Accounts option allows you to export the account data from TPAM to Microsoft Excel or CSV format. This lists all accounts that are PSM enabled or have the option of being PSM enabled. This is a convenient way to provide an offline work sheet and also to provide data that may be imported into another TPAM – for example, to populate a lab appliance with data for testing, without making the lower level changes that restoring a backup would cause.

To list the accounts:

1. Select **Systems, Accounts, & Collections | Accounts | List PSM Accounts** from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Layout** tab to select the columns and sort order for the listing.
4. To view and store the data outside of the TPAM interface, click the **Export to Excel** button, or the **Export to CSV** button.
5. To view the data in the TPAM interface, click the **Listing** tab.

4

Files

Introduction

In addition to the secure storage and release capabilities for passwords, TPAM facilitates the same secure storage and retrieval controls for files. This functionality can be used for many file types, but its intent is to securely store and control access to public/private key files and certificates.

List files

The List Files option allows you to export the account data from TPAM to Microsoft Excel or CSV format. This is a convenient way to provide an offline work sheet.

To list files:

1. Select **Systems, Accounts, & Collections | Files | List Files** from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Layout** tab to select the columns and sort order for the listing.
4. To view and store the data outside of the TPAM interface, click the **Export to Excel** button, or the **Export to CSV** button.
5. To view the data in the TPAM interface, click the **Listing** tab.
6. To view collection membership for the file, select the file and click the **Collections** tab.
7. To view the permissions assigned to the file, select the file and click the **Permissions** tab.

5

Collections

Introduction

Collections are groups of systems, accounts and/or files. Collections can be used to simplify the process of assigning permissions.

List collections

The List Collections option allows you to export the collection data from TPAM to Microsoft Excel or CSV format. This is a convenient way to provide an offline work sheet and also to provide data that may be imported into another TPAM – for example, to populate a lab appliance with data for testing, without making the lower level changes that restoring a backup would cause.

ℹ TIP: Enter ! in the System, Account and File name filters to find empty collections.

To list the collections:

1. Select **Systems, Accounts, & Collections | Collections | List Collections** from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Layout** tab to select the columns and sort order for the listing.
4. To view and store the list of collection names outside of the TPAM interface, click the **Export to Excel** button, or the **Export to CSV** button. To view and store the list of collection members outside of the TPAM interface, click **Export Members to Excel** button, or the **Export Members to CSV** button.
5. To view the data in the TPAM interface, click the **Listing** tab.
6. To view membership of a collection, select the collection and click the **Members** tab.
7. To view the user and groups with permissions on the collection, select the collection and click the **Permissions** tab.

User ID's

Introduction

This chapter covers listing TPAM User ID's.

List user IDs

The List UserIDs option allows you to export the user data from TPAM to Microsoft Excel or CSV format. This is a convenient way to provide an offline work sheet and also to provide data that may be imported into another TPAM – for example, to populate a lab appliance with data for testing, without making the lower level changes that restoring a backup would cause.

The last access date/time on the report is in server time (UTC).

To list the user IDs:

1. Select **Users & Groups | UserIDs | List UserIDs** from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Layout** tab to select the columns and sort order for the listing.
4. To view and store the data outside of the TPAM interface, click the **Export to Excel** button, or the **Export to CSV** button.
5. To view the data in the TPAM interface, click the **Listing** tab.
6. To view group membership for a user, select the user ID and click the **Groups** tab.
7. To view the permissions assigned to the user, select the user and click the **Permissions** tab.

Groups

Introduction

Groups are defined sets of users. Groups can be used to simplify the process of assigning permissions.

List groups

The List Groups option allows you to export the group data from TPAM to Microsoft Excel or CSV format. This is a convenient way to provide an offline work sheet and also to provide data that may be imported into another TPAM – for example, to populate a lab appliance with data for testing, without making the lower level changes that restoring a backup would cause.

To list the groups:

1. Select **Users & Groups | Groups | List Groups** from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Layout** tab to select the columns and sort order for the listing.
4. To view and store the list of group names outside of the TPAM interface, click the **Export to Excel** button, or the **Export to CSV** button. To view and store the list of group members outside of the TPAM interface, click **Export Members to Excel** button, or the **Export Members to CSV** button.
5. To view the data in the TPAM interface, click the **Listing** tab.
6. To view membership of a group, select the group and click the **Members** tab.
7. To view the permissions granted to the group, select the group and click the **Permissions**tab.

Default global groups

Included with TPAM are several default global groups that can be used for assigning permissions. These are only visible in TPAM if the System Administrator has enabled these in the admin interface.

IMPORTANT: Any users assigned to a global group will gain the associated permissions on all systems unless overridden by other assignments.

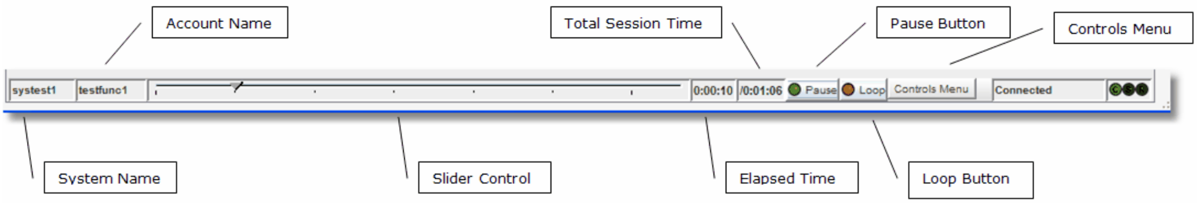
Session Management

Introduction

The session management menu provides access to session logs and the ability to playback sessions.

Session Playback Controls

To manipulate the playback of a session, the controls at the bottom of the session replay window lets the speed of the playback be changed, ranging from ½ normal speed to 16 times normal speed. Replay may be paused at any point.



The table below defines the functions and display information on the playback tool bar.

Table 2: Playback tool bar options

Option	Description
System Name	The name of the remote system where the session was established.
Account Name	The name of the remote account used to access the system during the session.
Slider Control	Displays the current position of playback, and after the session is paused lets a new position be selected. To reposition session replay, pause the session and position

Option	Description
	the slider control to the desired spot. Resume playback using the pause control. The session playback moves at maximum speed to the desired playback position. NOTE: The session time position is based on network packet timestamps. This means that the playback control slider may appear to move in an uneven fashion depending on the ‘data density’ of each packet, especially for very short recorded sessions. If for some period time there is a minimal amount of activity followed by a flurry of dialog openings and keystroke input, this would cause the uneven control slider movement. Longer session files tend to provide a smoother control slider movement.
Elapsed Time	Time elapsed in the session replay.
Total Session Time	Total length of time of the session.
Pause Button	When green the session is playing. When red the session is paused. To pause or resume playback simply click the control.
Loop Button	Selecting this button sets the session to replay over and over.
Controls Menu/Select Speed	Session play speed in relation to normal speed. For example .5x will play the session at half normal speed.
Controls Menu/Metadata/Open Dialog	If selected this opens a window to display the keystroke log, and tags for events and bookmarks. The keystroke slider at the top of the window can be adjusted so that they can see the keystrokes taking place in this window before or after they occur in the actual session replay window.
Controls Menu/Add Bookmark	If selected allows the user to add a bookmark at a specific point in the session.
Controls Menu/Always on Top	If selected, the meta data dialog window will be displayed in front of the session replay window.

Meta Data Window

While replaying the session the meta data window can be displayed in another window to view the keystroke/event log.

To open the meta data window during a session:

1. Click the **Replay Session** button.
2. Once the session has a status of connected in the replay window, select **Controls Menu | MetaData | Open Dialog**.

Keystrokes/events will be displayed in green as they occur during the session replay. Bookmarks are displayed in red. Slide the keystroke slider to the left to view the keystroke log in advance of the activity occurring in the session replay window. If the Clear on Loop check box is selected the keystroke log will be cleared before the session is replayed each time.

Replay a Session Log

ℹ NOTE:You cannot view the keystroke log when replaying a session unless the access policy that is granting you permission to replay the session has **Allow KSL View** selected.

To replay a session log:

1. Select **Session Mgmt | Session Logs** from the main menu.
2. Enter your search criteria on the filter tab.
3. Click the **Listing** tab.
4. Select the session log to replay.
5. Click the **Replay Session** button.
6. Click the **File Transfer** tab to view details on any files transferred during the session.
7. Click the **Captured Events / Bookmarks** tab to view details on events captured during the session.

ℹ NOTE: If the session log is stored on an archive server there may be a delay while TPAM retrieves the log from its remote storage location.

The remote access session is displayed and played back in real time. The playback session may be paused and resumed, moved ahead or back at increased speed, or continuously played at various speeds.

Add a Bookmark to a Session

Requestors, approvers, reviewers and auditors have the ability to add bookmarks to a session log. Adding a bookmark can point something out to another person replaying the session without them having to replay and watch the entire session.

To add a bookmark:

1. Select **Session Mgmt | Session Logs** from the main menu.
2. Enter your search criteria on the filter tab.
3. Click the **Listing** tab.
4. Select the session log to replay.
5. Click the **Replay Session** button.
6. When you get to the point in the session where you want to add a bookmark click the **Pause** button on the session playback controls at the bottom of the window.
7. Select **Controls Menu | Metadata | Add Bookmark**.
8. Enter text to label the bookmark and click the **OK** button.
9. After the bookmark is added the session will resume playback.

View Bookmarks/Captured Events

To view bookmarks and captured events from the session logs listing page:

1. Select **Session Mgmt | Session Logs** from the main menu.
2. Enter your search criteria on the filter tab.
3. Click the **Listing** tab.
4. Select the session log.
5. Click the **Captured Events, Bookmarks** tab. Events are only captured for sessions on an account if the **Capture Events?** check box is selected for the account on the PSM details tab.

Jump to a Bookmark

To jump to a bookmark while replaying a session:

1. Select **Session Mgmt | Session Logs** from the main menu.
2. Enter your search criteria on the filter tab.
3. Click the **Listing** tab.
4. Select the session log to replay.
5. Click the **Replay Session** button.
6. On the session playback menu select **Controls Menu | Metadata | Open Dialog**.

7. Click the **Select Bookmark** tab.
8. Select the bookmark you want to go to.
9. Click the **Jump to Bookmark** button.
10. The session replay will go to the bookmark but will continue replay, it will not be paused at the bookmark.

Jump to an Event

To jump to an event while replaying a session:

1. Select **Session Mgmt | Session Logs** from the main menu.
2. Enter your search criteria on the filter tab.
3. Click the **Listing** tab.
4. Select the session log to replay.
5. Click the **Replay Session** button.
6. On the session playback menu select **Controls Menu | Metadata | Open Dialog**.
7. Click the **Select Event** tab.
8. Select the event you want to go to.
9. Click the **Jump to Event** button.
10. The session replay will go to the event but will continue replay, it will not be paused at the event.

Monitor a Live Session

With the appropriate permissions a user can monitor another user’s session. The user running the session has no indication that their session is being watched.

ⓘ NOTE: You cannot view the Keystroke Log when monitoring a session.

To monitor a live session:

1. Select **Session Mgmt | Session Logs** from the main menu.
2. Enter search filter criteria.
3. Click the **Listing** tab.
4. Select the session to monitor. Live sessions will have a status of Connected.
5. Click the **Monitor Session**button. The PSM Session Monitor window will open with a view of the live session.

9

Logs

Introduction

The Logs menu lets the auditor to view many logs with critical information about the appliance. All logs can be exported to an excel or csv file.

Sys-Admin activity log

The Sys-Admin activity log reports the activity of all TPAM System Administrators. The sys admin activity log data can be displayed in server time (UTC) or the user's local time zone, whichever they select on the Report Filter tab.

To view the Sys-Admin Activity Log:

1. Select **Logs | Sys-Admin Activity Log** from the menu.
2. Enter your search criteria on the report filter tab.
3. Use one if the following methods to view the results:
    - Click the **Report** tab
    - Click the **Export to Excel** button
    - Click the **Export to CSV** button

Security log

The security log reports any events related to log on activity. Only failed events are displayed to conserve resources. The security log displays server time (UTC).

To view the Security Log:

1. Select **Logs | Security Log** from the menu.
2. Enter your search criteria on the report filter tab.
3. Use one if the following methods to view the results:
    - Click the **Report** tab
    - Click the **Export to Excel** button
    - Click the **Export to CSV** button

Firewall log

The firewall log displays events logged by the firewall component of TPAM. The firewall is configured to log all denied traffic. The firewall log displays server time (UTC).

To view the Firewall Log:

1. Select **Logs | Firewall Log** from the menu.
2. Enter your search criteria on the report filter tab.
3. Use one if the following methods to view the results:
    - Click the **Report** tab
    - Click the **Export to Excel** button
    - Click the **Export to CSV** button

Database log

The database log shows logged activity from the TPAM SQL Server database. The database log displays server time (UTC).

To view the Database Log:

1. Select **Logs | Database Log** from the menu.
2. Enter your search criteria on the report filter tab.
3. Use one if the following methods to view the results:
    - Click the **Report** tab
    - Click the **Export to Excel** button
    - Click the **Export to CSV** button

Alerts log

The Alerts log displays events related to any of the alerts that you can subscribe to. The alerts log displays server time (UTC).

To view the Alerts Log:

1. Select **Logs | Alerts Log** from the menu.
2. Enter your search criteria on the report filter tab.
3. Use one if the following methods to view the results:
4. Click the **Report** tab
5. Click the **Export to Excel** button
6. Click the **Export to CSV** button

10

On Demand Reports

Introduction

TPAM has a number of pre-defined reports to aid in system administration, track changes to objects, and provide a thorough audit trail for managed systems. All reports are accessed via the Reports menu. The reports can be filtered by criteria that are specific to each report type.

Report Time Zone Options

Time zone filter parameters are included on most of the reports allowing you to view the report data in your local or server time zone (UTC). These filter parameters only appear if you are configured with a local time zone. These parameters affect not only the data reported but also the filter dates used to retrieve the data.

NOTE: Access to different reports is based on the user’s permissions. Only TPAM Administrators and Auditors have access to all reports.

For example, the server is at UTC time and the user is in Athens, Greece (UTC +2). When the user enters a date range of 9/16/2009-9/17/2009 with the local time zone option, the report retrieves transactions that happened on the server between 9/15/2009 22:00 through 9/17/2009 21:59.

All reports that use the local time zone filter have an extra column indicating the UTC offset that was used to generate the report. This value is either the current UTC offset of the user. This column will also display in reports that are exported using Excel or CSV.

Run a Report

The following procedure describes the steps to run a report in TPAM.

To run a report:

1. From the Reports menu select the report.
2. On the Report Filter tab enter the filter criteria.
3. Click the **Report Layout** tab. (Optional)
4. Select the appropriate boxes in the Column Visible column to specify the columns to be displayed on the report.
5. Select the appropriate box in the Sort Column column to specify sort order.
6. Select the Sort Direction.
7. If viewing the report in the TPAM interface, select the Max Rows to display.

   > ℹ IMPORTANT: The Max Rows to Display limits the number of rows that are returned even if the number of rows that meet the filter criteria is greater than what is selected.

8. To view the report results in TPAM click the **Report** tab. To adjust the column size of any column on a report hover the mouse over the column edge while holding down the left mouse button and dragging the mouse to adjust the width.
9. To view the report results in an Excel or CSV file click the **Export to Excel** or **Export to CSV** button.

   > ℹ IMPORTANT: If you expect the report results to be over 64,000 rows you must use the CSV export option. The **Export to Excel** option only exports a maximum of 64,000 rows.

10. Open or Save the report file.

Report descriptions

The following table lists the on demand reports available in TPAM.

Table 3: TPAM report descriptions

Report title	Description
Activity Report	Detailed history of all changes made to TPAM.
ISA User Activity Report	Detailed records of all activities performed by users with ISA permissions.
Approver User Activity	Detailed records of all activities performed by users with Approver permissions.

Report title	Description
Requestor User Activity	Detailed records of all activities performed by users with Requestor permissions.
PSM Accounts Inventory (PSM Customers only)	Accounts that are PSM enabled.
Password Aging Inventory	Managed systems, and the managed accounts that reside on those systems.
File Aging Inventory	Secure stored files and the systems that manage them.
Release-Reset Reconcile	Audit evidence that released passwords have been reset appropriately.
User Entitlement	Data to review and audit users’ permissions for systems, accounts, files and commands on an enterprise scale. ⓘ NOTE: It is recommended that **Show Only Effective Permissions** is selected to reduce the size of the report. ⓘ NOTE: If any of the **Expand ...** options are selected, at least one of the text filters must be filled in with a non-wildcard value. For very large data sources the expansion of Collections, Groups, and/or Access Policies can very easily create a report beyond the retrieval and display capabilities of a web browser. For large data sets (10’s of thousands of accounts or thousands of large collections to expand) it is recommended to rely on the Data Extracts for unfiltered versions of the Entitlement Report.
Failed Logins	Failed login attempts to Privileged Account Manager. The data for the report is refreshed every 15 minutes.
Request Extensions	List details about request extensions that have been submitted.
DPA Affinity	Used to report on DPA assignments to systems and report on the DPA software version. ⓘ NOTE:This report is helpful for finding DPA v3 assigned to systems that may need to be removed if it is desired to set the TLS Global Setting to 2.
Password Update Activity	Password modifications to systems managed by Privileged Password Manager.

Report title	Description
Password Update Schedule	Scheduled password changes and the reason for the change.
Password Testing Activity	The results of automated testing of each managed accounts' password.
Password Test Queue	Accounts currently queued for password tests. NOTE: This is a useful report to view when troubleshooting performance related issues. A high number of queued password tests can impact system response time if the check agent is running. This report does not provide a mechanism for exporting data but does provide for deleting passwords from the test queue. So if there is some known reason why a large group of password tests are failing, such as a network outage, that group can be filtered out in the report and then deleted. An alternative would be to just stop the check agent.
Expired Passwords	Currently expired passwords, or passwords that will expire within a date range.
Passwords Currently in Use	Defines "in-use" passwords as: • Passwords that have been retrieved by the ISA/CLI/API that have not yet been reset. • Passwords that have been requested and retrieved, but have not yet been reset. • Password has been manually reset on the Account Details or Password Management pages, but has not yet been reset by PPM. • Password has been manually entered on the Account Details page, but has not yet been reset by PPM. • Account is created on the TPAM interface or as a result of Batch Import Accounts and is assigned a password by the user (as opposed to letting the system generate a random password).
Password Requests	Password requests and the details relating to the request. Selecting a row in the report, and clicking on the **Responses**, **Reviews** and **Releases** tab gives you additional details on the request.
Password Consecutive Failures	Password check and change failures for accounts.
Auto-Approved Password	Password releases that did not require dual control approval.

Report title	Description
Releases	
Auto-Approved File Releases	File releases that did not require dual control approval.
Password Release Activity	Details on password releases, such as request reason, retrieval date and ticket information.
File Release Activity	Details on file releases, such as request reason, retrieval date and ticket information.
Windows Domain Account Dependencies	Managed domain accounts that have dependencies on other systems.
Auto Approved Sessions (PSM customers only)	Sessions that were approved, as a result of no approval requirements for sessions on the account.
PSM Session Activity (PSM customers only)	Session details, such as start date, end date, and request reason.
PSM Session Requests (PSM customer only)	Session requests and the details relating to the request. Selecting a row in the report, and clicking on the **Responses**, **Reviews** and **Releases** tab gives you additional details on the request.

Scheduled Reports

Introduction

Scheduled reports (also known as Batch Reports) are standard reports available in TPAM. The TPAM Administrator configures these reports to automatically run on a daily, or weekly basis. The reports are run by the Daily Maintenance job which is configured in the /admin interface. The reports are stored on the appliance and can be emailed to designated subscribers or sent directly to an archive server. Only Administrators and Auditors can view these reports from the TPAM interface. Additional users can be configured to receive these reports via email.

Enable/disable scheduled reports

Administrators can enable or disable which scheduled reports can be subscribed to. On a new TPAM appliance all reports will be disabled by default.

> NOTE: The run time for these reports is controlled by the daily maintenance start time that is configured by the System Administrator in the admin interface.

To enable/disable scheduled reports:

1. Select **Reports | Scheduled Reports | Report Subscriptions** from the main menu.
2. Next to each report select one if the following from the far right hand column:
   - **Disabled** - the report will not run.
   - **HTML Only**- only the HTML version of the report will run.
   - **CSV Only** - only the CSV version of the report will run.
   - **HTML & CSV** - CSV and HTML versions will be run.
   - **XML Only** - the report will only be run in XML format.
3. Click the **Save Changes** button.

NOTE: If any option other than Disabled is selected the XML file is always generated (a zero byte file will be generated even if no data is reported).

IMPORTANT: The Entitlement reports are very resource intensive and can cause severe performance degradation for online users during the daily report cycle. If the reports will be used on a daily basis it is recommended that only the versions required are enabled. It is very common for these reports to be over 1 million rows and customers have found that the CSV files are more manageable.

Subscribe/unsubscribe to scheduled reports

Only Administrators and Auditors have permission to edit report subscriptions.

To subscribe/unsubscribe to Scheduled Reports:

1. Select **Reports | Scheduled Reports | Report Subscriptions** from the main menu.
2. In the Subscribed column select one or more of the output options (**HTML**, **CSV** or **XML**), for the reports you want to subscribe to.
3. Clear the **HTML**, **CSV** or **XML** check boxes in the Subscribe column for the reports you want to unsubscribe to.
4. Select the Zip check box to zip all subscribed formats of the report into one file to be emailed.
5. Click the **Save Changes** button.

   NOTE: When the select list does not include a format that is selected in the Subscribed column, the selection will be highlighted in red.

View scheduled reports

Scheduled Reports are generated daily by TPAM and stored internally. These reports are available for viewing by any administrator or auditor user. Stored reports are retained for a period of time specified by the System Administrator.

NOTE: The date and timestamp on the stored reports is server time.

To view scheduled reports that have run:

1. Select **Reports | Scheduled Reports | Browse Stored Reports** from the menu.
2. Select the date by clicking the hyperlink, formatted *yyyymmdd*.
3. The reports run on that date will be displayed. Click the hyperlink for the report you want to view.
4. Select **Open** to view the report immediately or **Save** to save the report.

Resubmit scheduled reports

The System Administrator has the ability to resubmit batch report runs for a prior date. Once the report run has been resubmitted, the reports can be viewed on the same page as the daily report runs. See the procedure above.

12

Data Extracts

Introduction

Data extracts are defined data sets that can be extracted from TPAM on a scheduled basis and automatically transferred to a pre-configured Archive server.

Extracted data is supplied as a *.CSV file and is easily viewed with MS Excel or any text editor. Information that may be extracted includes lists of systems, accounts, users, etc. and many logs of user activity and entitlement. The extracted files are compressed (ZIP file format) and named with a date and time stamp.

Data extracts are configured much in the same way as TPAM system backups. The extracts can be set to occur daily, weekly or monthly at a specific time. Only Administrators can enable and configure data extracts. Auditors can view the data extract logs.

Data extract logs

The data extract log tab displays the logged results of each scheduled extraction.

To view a data extract log:

1. Select **Reports | Scheduled Reports | Data Extract Schedules** from the main menu.
2. Select a schedule from the list.
3. Click the **Log** tab.
4. Enter filter criteria on the Filter tab.
5. Click the **Data Extract Log** tab.

To clear data extract log/s:

1. Select **Reports | Scheduled Reports | Data Extract Schedules** from the main menu.

2. To clear a specific log, select the schedule from the list and click the **Clear Log** button.
3. To clear all the logs, click the **Clear Log** button without selecting a specific schedule from the list.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product