# The Privileged Appliance and Modules (TPAM) 2.5.919

## Requestor Guide

### 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.

TPAM Requestor Guide
Updated - August 2017
Version - 2.5.919

# 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 requestors of password, file and session requests.

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. To immediately make a session, file or password request click the links.

## Recent Activity Tab

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

## Current Requests tab

The Current Requests tab displays any request (Password, File or Session) that you have made. The requests stay visible on this tab until the release duration expires. By clicking on the Request ID link you are taken directly to the Session, Password or File Request Management tabs so you can see more details on this request.

# 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. |
| PSM Connection Defaults | Default PSM connection options when recording a session. |
| 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 |

| Field name | Description |
|---|---|
| | ID. |
| 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. |
| PSM Connection Defaults | Lists all possible PSM connection options and their values. Connection options and values are proxy specific. The selected values will be used as defaults the first time a user starts a PSM session to any given account. Once the user has started the session, the default values for that user are saved and will be the defaults the next time the user connects to that account. These user connection defaults are cleared any time the proxy type for the account is changed.<br>These defaults only apply to session recordings and not session playback or monitoring. |

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.

# Password Requests

## Introduction

System account passwords that are configured using Privileged Password Manager can be released by submitting a password request. The request will either require approval by one or more TPAM users, or be auto-approved, based on how the account is configured. This process ensures the security of the system account password, provides accountability, and provides dual control over the system accounts.

## Request a password

***To request a password:***

1. Select **Request | Password | Add Request** from the main menu.
2. To request a password on a specific system or a specific account type the criteria on the Filter tab.
3. Click the **Accounts** tab.
4. Select the check box next to each account to be included in the password request. When selecting multiple accounts in one request, the request time and release duration will be the same for all accounts requested.

   NOTE: If, through a Group or Collection assignment, the user has multiple Access Policies granting a REQ permission to the account, the account will be listed multiple times on the Accounts listing tab. Each row will show the Access Policy, Minimum Approvers, and Maximum Release Duration associated with it.

5. Click the **Details** tab.

6. Complete the following fields:

**Table 2: Password Request Management: Details tab fields**

| Field name | Description |
|---|---|
| Request Immediate | Select this check box to immediately request the password. |
| Date/Time Required | To have a password released on a future date and time, enter the date and time when the password is required. Enter the time in the user's local time. |
| Requested Duration | The requested duration is the period of time that the password(s) is available for release. The default requested duration will be pulled from the access policy or account setting. Once the request is saved this duration is added to the requested release date to determine the request expiration date. Valid parameters for release durations are from 15 minutes to 21 days, in 15 minute increments – however, the effective valid parameter for the maximum allowable release request duration is the value configured for maximum release duration at the account level. When requesting passwords for multiple accounts together, the Requested Duration defaults to the shortest "Default Duration" for all accounts listed on the request. |
| Reason Code | Reason codes will appear if they have been configured by the System Administrator. Reason codes streamline the request process, and may be optional, required, or not allowed depending on how they are configured. |
| Request Reason | Used to provide a brief description of the reason for the password release. May be optional, required or not allowed, depending on configuration. |
| Ticket System | May be required, based on configuration. Any boxes on the request highlighted in red, require a ticket system to be chosen from the list. |
| Ticket Number | May be required, based on configuration. If the ticket number fails validation when the request is submitted, then the request is automatically canceled. |

7. Click the **Save Changes** button.

NOTE: If a request is submitted that does not have enough approvers configured to meet the approval requirements, then the request is not submitted and a warning message is presented at the bottom of the page:

Once the request has been submitted it will reflect one of these statuses:

- Pending Approval - waiting for authorized approver/s to approve the request.
- Active/Approved - the request has been approved and is within the release duration window.
- Approved - the request has been approved but the request date/time is in the future.
- Denied - the request was denied by the approver/s.
- Canceled - the submitted request conflicts with a request that has already been approved for the same time period or the requestor decides to cancel the request prior to accessing the password. The request will also be cancelled if the ticket number entered on the request requires validation, and fails.
- Expired - the release window for the password has passed or the requestor is done accessing the password and expires the request early.
- If a request has a status of Pending Approval, additional accounts can be added up to 15 minutes from the original expiration date/time for the request.

***To add accounts to a request once it has already been submitted:***

1. Select **Request | Password | Manage Requests** from the main menu.
2. Enter filter criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the request to add accounts to.
5. Click the **Details** tab.
6. Click the **New Accounts** button.
7. Enter filter criteria to find the accounts you want to add.
8. Click the **Accounts** tab.
9. Select the check box on the Selected column for the accounts you want to add.
10. Click the **Details** tab.
11. Enter a Ticket System/Ticket Number if required.
12. Click the **Save Changes** button.

# Email notification

Once a password request is submitted, the requestor receives an email notification when the request is approved, denied, or automatically canceled as a result of a request conflict.

If a password request is submitted and does not require any approvals, the request is auto-approved and can be accessed immediately.

# View submitted password requests

***To view requests that have been submitted:***

1. Select **Request | Password | Manage Requests** from the main menu.
2. Enter filter criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the request.
5. Open the following tabs to view more detailed information about the request.
    - Details - Date and time stamps relevant to the life cycle of the request.
    - Responses - Request responses from approvers, or responses auto-generated by TPAM for auto-approved or canceled requests.
    - Approvers - All TPAM users with permissions to approve or deny the request.
    - Password - If enabled, displays the password for the account.

# Access the password

***Once a request is approved to view the account password:***

1. Select **Request | Password | Manage Requests** from the main menu.
2. Enter filter criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the request.
5. Click the **Password** tab. The password will be displayed. Depending on how your TPAM is configured the password will display in one of three ways:
    a. The password will be revealed on the screen. To copy and paste the password, click the mouse once over the password which will automatically select the password
    b. The **Reveal Password** button can be clicked to reveal the password or the password can be copied to the clipboard without displaying it on the screen.
    c. You must put your mouse in the designated area, and press the Ctrl-C keys to copy the password to a clipboard.

The password can be displayed by the requestor as often as necessary during the release duration period.

# Password reset during release window

While a requestor has an active release duration window, three possible circumstances could cause the password to be changed by TPAM during that time:

- The configured Default Change Setting for the account occurs during the release window. For example, if the password is to be changed every 30 days which happens to occur while a requestor has a password. This scenario can be prevented by selecting **Do not automatically change the password while a release is active** on the account details management tab.
- The ISA post-release reset interval has occurred. In this case, an ISA may have recently retrieved the password and it is being reset because the configured interval for that action has expired. This scenario can be prevented by selecting **Do not automatically change the password while a release is active** on the account details management tab.
- The ISA or the Administrator has forced a reset of the password.

The requestor should try and access the password at a later time.

# Access past passwords

A requestor can access past passwords if the access policy assigned to their user ID has this option selected for the account being requested.

***To access past passwords:***

1. Submit a password request following the normal procedure.
2. After the request is approved click on the **Passwords** tab.
3. On the left of the Password tab date ranges will be listed for passwords. Select a date range and the password for that date range will be displayed on the right side of the screen.

# Cancel/expire a password request

A password request can be canceled by the requestor if the status is Pending Approval. Once approved, a password request can be expired to immediately end the release duration. Expiring a request early makes the account available for request for other users and immediately queues the password for a reset (if so configured).

***To cancel/expire a password request:***

1. Select **Request | Password | Manage Requests** from the main menu.
2. Enter filter criteria on the Filter tab.

3. Click the **Listing** tab.
4. Select the request.
5. Click the **Details** tab.
6. Enter a reason in the Cancel/Expire Reason box.
7. If the request contains multiple accounts, select the **Apply Reason** check box next to the applicable accounts.
8. Click the **Save Changes** button.

# File Requests

## 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.

## Request a file

***To request a file:***

1. Select **Request | File | Add Request** from the main menu.
2. To request a file on a specific system enter the criteria on the Filter tab.
3. Click the **Files** tab.
4. Select the file to be included in the request.

   NOTE: If, through a Group or Collection assignment, the user has multiple Access Policies granting a REQ permission on the file, the file will be listed multiple times on the Files tab. Each row will show the Access Policy, Minimum Approvers, and Maximum Release Duration associated with it.
5. Click the **Details** tab.

6. Complete the following fields:

**Table 3: File Request Management: Details tab fields**

| Field name | Description |
|---|---|
| Request Immediate | Select this check box to immediately request the file. |
| Date/Time Required | To have a file released on a future date and time, enter the date and time when the file is required. Enter the time in the user's local time. |
| Requested Duration | The requested duration is the period of time that the file is available for release. The default requested duration will be pulled from the access policy or file setting. Once the request is saved this duration is added to the requested release date to determine the request expiration date. Valid parameters for release durations are from 15 minutes to 21 days, in 15 minute increments – however, the effective valid parameter for the maximum allowable release request duration is the value configured for maximum release duration at the access policy or file level. |
| Reason Code | Reason codes will appear if they have been configured by the System Administrator. Reason codes streamline the request process, and may be optional or required, depending on how they are configured. |
| Request Reason | Used to provide a brief description of the reason for the file release. May be optional, required or not required, depending on configuration. |
| Ticket System | May be required, based on configuration. |
| Ticket Number | May be required, based on configuration. If the ticket number fails validation when the request is submitted, then the request is automatically canceled. |

7. Click the **Save Changes** button.

NOTE: If a request is submitted that does not have enough approvers configured to meet the approval requirements, then the request is not submitted and the following message is presented at the bottom of the page: "There are not enough individuals authorized to approve this request."

Once the request has been submitted it will reflect one of these statuses:

- Pending Approval - waiting for authorized approver/s to approve the request.
- Active/Approved - the request has been approved and is within the release duration window.
- Approved - the request has been approved but the request date/time is in the future.
- Denied - the request was denied by the approver/s.

- Canceled - the submitted request conflicts with a request that has already been approved for the same time period or the requestor decides to cancel the request prior to accessing the password. The request will also be cancelled if the ticket number entered on the request requires validation, and fails.
- Expired - the release window for the file has passed or the requestor is done accessing the file and expires the request early.

# Email notification

Once a file request is submitted, the requestor receives an email notification when the request is approved, denied, or automatically cancelled as a result of a request conflict.

If a file request is submitted and does not require any approvals, the request is auto-approved by PPM and the Retrieve button will be enabled.

# View submitted file requests

***To view requests that have been submitted:***

1. Select **Request | File | Manage Requests** from the main menu.
2. Enter filter criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the request.
5. Open the following tabs to view more detailed information about the request.
    - Details - Date and time stamps relevant to the life cycle of the request.
    - Responses - Request responses from approvers, or responses auto-generated by TPAM for auto-approved or cancelled requests.
    - Approvers - All TPAM users with permissions to approve or deny the request.

# Access the file

***Once a request is approved to retrieve the file:***

1. Select **Request | File | Manage Requests** from the main menu.
2. Enter filter criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the request.

5. Click the **Retrieve** button.
6. Select to open or save the file.

# Cancel/expire a file request

A file request can be cancelled by the requestor if the status is Pending Approval. Once approved, a password request can be expired to immediately end the release duration. Expiring a request early makes the file available for other users to request.

***To cancel/expire a file request:***

1. Select **Request | File | Manage Requests** from the main menu.
2. Enter filter criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the request.
5. Click the **Details** tab.
6. Enter a reason in the Expiration Reason box.
7. Click the **Save Changes** button.

# Session Requests

## Introduction

Systems that are configured using Privileged Session Manager can be accessed remotely by submitting a session request. The request will either require approval by one or more TPAM users, or be auto-approved, based on how the account is configured. The activity during the session will be recorded and can be played back by authorized users.

## Request a session

***To request a session:***

1. Select **Request | Session | Add Request** from the main menu.
2. To request a session on a specific system or a specific account enter the criteria on the Filter tab.
3. Click the **Accounts** tab.
4. Select the check box next to each account to be included in the session request. When selecting multiple accounts in one request, the request time and release duration will be the same for all accounts requested.

   NOTE: If, through a Group or Collection assignment, the user has multiple Access Policies granting a REQ permission to the account, the account will be listed multiple times on the Accounts listing tab. Each row will show the Access Policy, Minimum Approvers, and Maximum Release Duration associated with it.

5. Click the **Details** tab.

6. Complete the following fields:

**Table 4: Session Request Management: Details tab options**

| Field name | Description |
|---|---|
| Request Immediate | Select this check box to immediately request the session. |
| Date/Time Required | To conduct a session on a future date and time, enter the date and time when the session is required. Enter the time in the user's local time. |
| Requested Duration | The requested duration is the period of time that access to the remote system/s is available. The default requested duration will be pulled from the access policy or account setting. Once the request is saved this duration is added to the requested release date to determine the request expiration date. This should be taken into consideration when selecting the request duration. If not approved quickly, the request duration available to the requestor could be considerably shorter than that specified. When expired, the session is no longer available to the requestor. The session is not terminated or interrupted, but after it has been closed the user can no longer restart it. When requesting sessions for multiple accounts together, the Requested Duration cannot exceed the shortest "default duration" for all accounts listed on the request. Also the "Maximum Duration" is never greater than the "Max Session Duration" configured by the System Administrator in Global Settings.<br>NOTE: If you will be conducting a file transfer during the session, the session duration must include the time that it takes for the fil e transfer to complete. |
| Reason Code | Reason codes will appear if they have been configured by the System Administrator. Reason codes streamline the request process, and may be optional or required, depending on how they are configured. |
| Request Reason | Used to provide a brief description of the reason for the session request. May be optional, required or not required, depending on configuration. |
| Ticket System | May be required, based on configuration. Any boxes on the request highlighted in red, require a ticket system to be chosen from the list. |
| Ticket Number | May be required, based on configuration. If the ticket number fails validation when the request is submitted, then the request is automatically canceled. |

7. Click the **Save Changes** button.

NOTE: If a request is submitted that does not have enough approvers configured to meet the approval requirements, then the request is not submitted and the following message is presented at the bottom of the page: "There are not enough individuals authorized to approve the request."

Once the request has been submitted it will reflect one of these statuses:

- Pending Approval - waiting for authorized approver/s to approve the request.
- Active/Approved - the request has been approved and is within the release duration window.
- Approved - the request has been approved but the request date/time is in the future.
- Denied - the request was denied by the approver/s.
- Canceled - the submitted request conflicts with a request that has already been approved for the same time period or the requestor decides to cancel the request prior to connecting to the remote system. The request will also be canceled if the ticket number entered on the request requires validation, and fails.
- Expired - the release window for the session has passed or the requestor is done conducting the session and expires the request early.

If a request has a status of Pending Approval, additional accounts can be added up to 15 minutes from the original expiration date/time for the request.

***To add accounts to a request once it has already been submitted:***

1. Select **Request | Session | Manage Requests** from the main menu.
2. Enter filter criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the request.
5. Click the **Details** tab.
6. Click the **New Accounts** button.
7. Enter filter criteria to find the accounts you want to add.
8. Click the **Accounts** tab.
9. Select the check box on the Selected column for the accounts you want to add.
10. Click the **Details** tab.
11. Enter a Ticket System/Ticket Number if required.
12. Click the **Save Changes** button.

# Email notification

Once a session request is submitted, the requestor receives an email notification when the request is approved, denied, or automatically canceled as a result of a request conflict.

If a session request is submitted and does not require any approvals, the request is auto-approved and the requestor can immediately start the session by clicking the **Connect** button.

# View submitted session requests

***To view requests that have been submitted:***

1. Select **Request | Session | Manage Requests** from the main menu.
2. Enter filter criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the request.
5. Open the following tabs to view more detailed information about the request.
    - Details - Date and time stamps relevant to the life cycle of the request.
    - Responses - Request responses from approvers, or responses auto-generated by TPAM for auto-approved or cancelled requests.
    - Approvers - All TPAM users with permissions to approve or deny the request.
    - Connect Options - If enabled can be used to change settings such as keyboard language mapping for the session.

# Cancel/expire a session request

A session request can be canceled by the requestor if the status is Pending Approval. Once approved, a session request can be expired to immediately end the release duration. Expiring a request early makes the account available for request for other users and immediately queues the password for a reset (if so configured).

***To cancel/expire a session request:***

1. Select **Request | Session | Manage Requests** from the main menu.
2. Enter filter criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the request.
5. Click the **Details** tab.
6. Enter a reason in the Cancel/Expire Reason box.
7. If the request contains multiple accounts, select the **Apply Reason** check box next to the applicable accounts.
8. Click the **Save Changes** button.

# Request a session using a linked account

If your user ID has been set up with linked accounts you can request a PSM session using :linkedaccount: which will grant you the ability to select many different accounts through the linked account.

***To request a session using a linked account:***

1. Select **Request | Session | Add Request** from the main menu.
2. To request a session on a specific system or a specific account enter the criteria on the Filter tab.
3. Click the **Accounts** tab.
4. Select the **:linkedaccount:.**
5. Click the **Details** tab.
6. Select the account desired for session request from the **Account Name** list.
7. Complete and save the request as normal.

# Start a Remote Session

## Introduction

Once a session is approved a user can use TPAM to connect to a remote system This chapter covers the steps for starting a session and files transfer options during a session.

## Client requirements

Java version 7 update 45 or higher is required to run the session applet.

IMPORTANT: If the recording session reaches the limit set in Max Recording Size global setting (set by the TPAM System Administrator), the session is automatically terminated. Warning messages will be sent when the session reaches 60% of the set limit.

## Start a session

***To start a session:***

1. Select **Request | Session | Manage Requests** from the main menu.
2. Enter filter criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the request.
5. Click the **Connect Options** tab. If you have pre-configured default PSM connection options at the user level, they will default here. Once a session is started, the user defaults are saved for the next time a connection is made. If **Use Default Connection options** is selected the options will be reset to the system connection

options and not the user defined defaults. Connection options are dependent on the platform, proxy type and if a DPA is assigned to the system. Clear the **Use Default Connection Options** check box to select different session connection options. The connection options selected by the user will persist for this user every time they connect with this account to a session, using the same proxy type. If the proxy type changes the user will have to save their preferred connection settings again, in order for them to persist. (optional)

**Table 5: Session Request Management: Connection Options**

| Connection option | Description |
|---|---|
| Cache Bitmaps | Turning this on may help responsiveness during session over a slow network connection. |
| Compression | Turn on to control compression of the RDP data stream. |
| Experience | Experience changes default bandwidth performance behavior. Choices are Default (theming is enabled) or 56Kbps (modem). |
| Keyboard | The keyboard type you want to emulate during the session. |
| Language | Sets the language (sometimes referred to as locale) on the target system for the session. On most operating systems this changes things like the language used for system menus, alerts, messages, and numeric formats for default date and time. |
| Mouse Motion | Option to send the mouse motion during the session or not. Not sending the mouse motion can save bandwidth, although some applications may rely on receiving mouse motion. |
| Putty:Background | Background color choices of black, green, blue or white. |
| Putty:Foreground | Foreground color choices of grey, black or white. |
| Putty:Geometry | Select a window size of 80 x 24 or 132 x 24. |
| Screen Updates | Screen updates can be sent as bitmaps or left at the default of higher level drawing operations. |
| XTerm:Backspace | If Ctrl-h is selected, then using the Backspace key during the session, will perform the same action as Ctrl-h. |
| XTerm:Del | If Ctrl-d is selected, then using the Delete key during the session, will perform the same action as Ctrl-d. |

6. Select the desktop display size for the session. (optional)

   NOTE: The window display size selection is not saved, and must be reselected before connecting each time.

7. Click the **Connect** button.The remote session is initiated in a new page. All activity

performed by the remote user is logged and recorded. When a session begins, depending on the browser being used, an JNLP pop up will appear. Click ok to proceed.

NOTE: If a Windows user tries to start a session and receives the error "ExitException: JNLP jar download failure", go to the Java Control Panel --> General --> Network Settings...and select **Direct Connection** instead of Use browser settings.

8. Depending upon the configuration for session authentication for the account one of these scenarios occurs:
    - The session uses auto-logon with a predefined account and its password.
    - The password is provided by TPAM but must typed in by the user.
    - The password is not stored in TPAM and must be typed in by the user.

NOTE: Sessions to remote systems are also subject to the configuration of the access method at the remote system. Example: if Windows RDP or Terminal Services is the connection method then the configuration for disconnected session time outs, maximum connections, and so on, govern certain session behavior. In addition, troubleshooting problems with connectivity to these systems should include examining the configuration of the remote system.

Clipboard transfer between the RDP session and the desktop is available if this option was selected at the account level on the PSM Details tab. The Clipboard transfer feature allows copy/cut and paste of text between the remote session and the desktop.

If the proxy type for the session is SSH, then the client is PuTTY. When connecting to the session a PuTTY security warning message will be presented to validate the client machine host keys. Clicking the **Accept** button will cache the host key so that this message will not be presented again during the session.

Pressing the Ctrl key and right clicking the mouse will bring up the Putty menu. This menu provides options to copy the scroll back buffer, change fonts, and reconfigure other settings.

On the bottom of the PSM session window you will see the system name, account name, keyboard mapping chosen, password (if display password is selected), the controls menu, session connection status and the size of any data pasted to the clipboard. The controls menu contains options for hot keys and file transfer.

# Controls Menu

The table below explains the options in the Controls menu.

**Table 6: Session Request Management: Control Menu**

| Control option | Description |
|---|---|
| Show Password | If selected, displays the password from the interactive logon. |
| Hotkeys/Send CTRL+ALt+DEL | Sends CTRL+ALT+DEL to the target. |
| Hotkeys/Send WIN Key | Sends the Windows Key to the target. |
| Hotkeys/Set Session Clipboard | When recording a session any time the user clicks anywhere on the session screen whatever is currently in the local clipboard buffer gets automatically sent to the remote session clipboard making it available for the user to paste in the session. This process is part of the VNC/RFB protocol -Client to Server messages -ClientCutText. The **Set Session Clipboard** control allows the user to force a re-send of the ClientCutText message based on what is currently available in the local clipboard buffer. |
| Hotkeys/Send F13 thru F24 | Sends F13 through F24 to the target instead of SHIFT + F1 through F12. |
| Hokeys/Convert to ASCII | Can be used to try and assist customers that are using a keyboards/languages not yet supported. |
| File Transfer | Click on **Open Dialog** to begin a file upload or download. |

# File transfer

Depending on how the account is configured there are options to upload files to the remote system and download files from the managed system during the session. The time out period for file transfers is 10 hours.

***To upload a file:***

1. Select **Controls Menu | File Transfer | Open Dialog** located on the bottom of the session window.
2. Click the **Select File** button to locate the file or directory to transfer. Repeat this step for each file or directory to upload. As files and/or directories are selected they are displayed in the Selected Files list.

   IMPORTANT: There is 20 GB size limit on any files transferred.
3. To remove a file that was selected by mistake use the **Remove Selected** or the **Remove All** buttons as needed. Additionally files and directories may be selected by simply dragging and dropping them on the Selected Files list.
4. If the Transfer Credentials fields appear on the screen, enter the **Account Name** and **Account Password** required to upload the file.

5. Click the **Upload** button to start the transfer process. After the transfer is complete the status will be reported as complete in the box at the bottom of the page.

IMPORTANT: The upload process overwrites any existing file(s) if the user has the file system rights to do so. If the user does not have sufficient rights to an existing file and they attempt to upload a file of the same name the upload fails.

***To download a file:***

**CAUTION: File downloads can put a big strain on the appliance. If other users start to see performance problems in TPAM the file download could be the cause.**

1. Select **Controls Menu | File Transfer | Open Dialog** on the bottom of the session window.
2. Enter the fully qualified name of the file in the Download File Name box.
3. If the Transfer Credentials fields appear on the screen, enter the **Account Name** and **Account Password** required to upload the file.
4. Click the **Download** button. After the download is complete the status will change to complete in the box at the bottom of the page.

# Terminate a session

A requestor user has the ability to terminate (kill) their active sessions. Unless the session request is also

expired or canceled the requestor has the ability to restart the session.

IMPORTANT: Be aware that terminating a session could leave unfinished work on the remote system and even do potential damage.

***To terminate a session:***

1. Select **Request | Session | Manage Sessions** from the main menu.
2. Enter filter criteria on the **Filter** tab.
3. Click the **Listing** tab.
4. Select the session to terminate.
5. Click the **Terminate** button.

# End a session

Once you have completed what you wanted to do on the remote system you can end the session. To end the session close the session window. A new session can be started until

the release duration on the request expires.

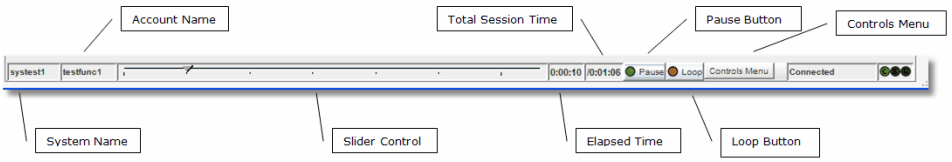
# Session Management

## 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 7: 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 the slider control to the desired spot. Resume playback using the pause control. The session playback moves at maximum speed to the desired |

| Option | Description |
| --- | --- |
| | playback position.<br>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

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 **Management | 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.

   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.

Prior to v2.5.915 a session logs could be "stranded" by closing the browser when a session was recording and clicking the **Terminate** button. To fix the problem so the session can be replayed, select the session from the Listing page and click the **Reset Stats** button.

# Add a bookmark to a session

Requestors, approvers, auditors and reviewers have the ability to add bookmarks to a session log. By adding a bookmark, the requestor, approver, auditor or reviewer can point something out to another approver or reviewer that they want them to look at 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 **Management | 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.

# On Demand Reports

## Introduction

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.

   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.

   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 for requestors in TPAM.

**Table 8: TPAM report descriptions**

| Report title | Description |
|---|---|
| Activity Report | Detailed history of all changes made to TPAM. |
| 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. |

# 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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product