The Privileged Appliance and Modules 2.5.920

ISA 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 ISA Guide
Updated - April 2018
Version - 2.5.920

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 Information Security Administrators (ISAs).

Your home page is based on the user type and permissions assigned to your user ID in the TPAM application. 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.

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.
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

Field name	Description
	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. 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.

Partitions

Introduction

Partitions are a logical separation of objects (systems, accounts, collections, users, groups, profiles) within a single TPAM deployment designated for delegated management. It is the responsibility of the TPAM Administrator to add partitions to TPAM. Partition Administrators can be defined who can perform equivalent functionality to the current administrator role, but only for objects within that partition. In order for partitions to be created in TPAM the System Administrator must enable the global settings related to partitions.

As an ISA you may belong to more than one partition which gives you the ability to add systems to those partitions.

4

Systems

Introduction

This chapter covers the steps to add and manage systems in TPAM.

NOTE: An ISA cannot add systems if the System Administrator has set the **Restrict ISA System Creation** global setting to **Yes**.

To add and manage systems, information is entered on the following tabs in the TPAM interface:

Table 2: Systems Management: TPAM interface tabs

Tab name	Description
Details/Information	Define main system information, such as name, IP address, contact.
Details/Custom Information	Enter data in custom fields, if they have been defined.
Details/Connection	Define functional account credentials.
Details/Management	Configure the settings for how TPAM will manage the passwords for the accounts on this system.
Details/Ticket System	Configure Ticket System Validation for requests on this system.
Details/LDAP Schema	For LDAP Directory systems, whose schema may require customizing.
Template	Used to save system settings as a template.
Account Discovery	Assign the account discovery profile to be used for this system.
Affinity	Define Distributed Processing Appliance (DPA) assignment for a system.

Tab name	Description
Collections	Assign a system to a collection/s.
Permissions	Assign users and groups permissions on this system.

Information tab

The table below explains all of the box options available on the details information tab.

Table 3: Systems Management: Details information tab options

Field	Description	Required?	Default
Partition	Partitions are a logical separation of objects within a single TPAM deployment. As an ISA you may belong to more than one partition which gives you the ability to add systems to those partitions. If partitions have been enabled and created this will be an available drop down. The system's partition can not be changed once the system is saved. Systems not assigned to a partition at the time they are first saved cannot be assigned to a partition at a later date.	Opt	No assign-ment
System Name	Descriptive name of the system. Typically, the host name (for UNIX systems) or the machine name (for Windows systems) is used. Within TPAM, the system name must be unique. The name can be 1-30 characters long, but cannot include empty space (i.e. spaces, carriage-returns, etc.).	Yes	
Network Address	The IP address (example: 192.168.0.15) or DNS name (example:server1.domain.bigco.com) of the system. It is imperative that this information is entered correctly, as the back-end automation procedures use this address to connect to the remote system.	Yes	

Field	Description	Required?	Default
	NOTE: MS SQL Server systems with dynamic ports can be entered as the **networkaddress\namedinstance** in this box. For more details see the Client Set Up Guide.		
ISA Policy	This option is listed after adding a system if your user ID is assigned an Access Policy that contains an ISA permission. From this list, select the ISA policy to be applied which allows you to access the system after it has been saved. If you have ISA access granted via a single Access Policy it is pre-selected. NOTE: If you select **Do not Assign an ISA Policy** you must assign the system to a collection to which you have access; otherwise once the system is saved you will no longer have access unless you are an administrator.		
Platform	This list shows the operating system platforms currently supported for proxied connections by TPAM. The platform of **Other** can be chosen for platforms not currently supported for TPAM auto management. Select the appropriate platform for the operating system running on the remote host. For PSM this box is primarily descriptive, since it is the proxy connection type that actually determines how the session is established. However, if the passwords for this system are managed by PPM, ensure the correct platform is selected, as PPM uses it to determine the most secure and reliable way to manage the passwords on the remote system.	Yes	AIX
Password Rule	The password rule to serve as the default for all accounts defined for the system. If the selection is not changed (or if no other rules have been defined in TPAM) the *Default Password Rule* is selected. The	Yes	Default Password Rule

Field	Description	Required?	Default
	password rule governs the construction requirements for new passwords generated by PPM. Password rules are managed by Sys-Admin users in the admin interface.		
Maximum Duration	This is the *maximum* duration for a password release on the account. If this is overridden by an Access Policy assignment, the *lower* of the two durations is used. The default duration that the requestor sees for any new password request is *2 hours*, or the maximum duration, whichever is less.	Yes	7 Days
Contact E-mail	Allows support personnel to receive email notifications from TPAM. Alerts are sent when there is a: • Password check or change failure based on password profile settings. • Scheduled password changes for a manually managed account • A PSM session expires • A non-managed account password release notification • Scheduled password changes for managed accounts with **Send notification only** selected on the password change profile. This box can be left blank, in which case errors are logged but notifications are not sent.	No	
Description	The description box may be used to provide additional information about the system, special notes, business owner, etc.	No	
Enable Automatic Password Management?	Tells TPAM whether to automatically manage remote system account passwords, based upon configuration parameters for each system. Auto-management includes automatic testing and changing of the passwords. Selected =	No	Enabled on appliances with Privileged Account Manager licenses.

Field	Description	Required?	Default
	enabled, cleared = disabled. This option is available at both the system and account levels, therefore it is possible to allow TPAM to auto-manage one account on a specific system, while another account on the same system is not auto-managed. However, if the option is not selected at the system configuration level, no accounts on the system can be auto-managed. NOTE: If the appliance has exceeded the number of PPM managed systems that were licensed this option cannot be selected for any new systems until you select the **Disable all PPM functions ...** check box on another managed system or increase your system license quantity. NOTE: This option will only appear if you have ISA permissions for passwords.		
Disable all PPM functions and delete any existing password history or secured files? (PSM Customers Only)	This check box sets the system to "PSM only", which means you cannot use any of the PPM features on this system such as password change history, release logs, password checking and changing, and releasing passwords. The reason for this is product licensing. You are not limited to the number of "PSM only" systems you can add, but the number of managed (PPM) systems you can add is limited to the number of system licenses you purchased. NOTE: This option will only appear if you have ISA permissions for passwords and sessions.	No	Off
Approver Escalation	You have the ability to send an escalation to a specific email address if no approvers have responded to a Password/File request within X minutes. You can enter multiple	No	

Field	Description	Required?	Default
	email addresses by separating them with a comma up to the box maximum of 255 characters.		
Delegation Prefix (specific platforms only)	This box can be used to preface the commands that PPM uses to manage passwords for this system. The delegation prefix can also be used to specify an absolute path to the command that PPM uses to manage passwords for the system.	No	
Computer Name (specific platforms only)	This box is designated for the system's computer name and is required for proper password management. If it is not populated, TPAM attempts to determine the system's computer name when the system is tested and update the box. The Computer Name box is also used with TPAM's Autologon feature. You have the option to have TPAM log the user into the remote system using the WORKSTATION\USERID format.This prevents any incorrect logon if the Default domain is saved as the DOMAIN name versus the Local Workstation. If a Domain user is selected from the Session Authentication window on PSM details, the user credentials are passed as DOMAIN\USERID. With both options the DOMAIN box is disabled at login.	Yes for specific platforms.	
Workstation ID (Specific platforms only)	For AS400 systems a specific workstation ID can be entered here that will be used when TPAM tries to connect to the system.	No	
Restricted URL (PSM Web Access platform only)	If a URL is entered the user is restricted to this address during the PSM web access session. If **ALLOWNAV;** is typed in before the restricted URL, the user can navigate away from the restricted URL.	No	
Initial Command (HP Non-Stop platform only)	Initial command sent to the system.	No	
Client ID (SAP platform only)	ALS Client ID. When the target is a cluster enter the **ClientID:R3Name:Group:Port** in this box. The network address entered	No	

Field	Description	Required?	Default
	for the system should be the network address of the message server.		
Password Release on Change (SPCW Pwd platform only)	This value specifies if the old password, new password, or both will be substituted for the %OLDPW% and %NEWPW% tags in the parameters for the command specified under **Execute a command if the password change succeeds** within SPCW.	No	
Extra DB Connection String (DB platforms only)	This value will be used in the database connection string when testing the system, checking or changing passwords, and, on supported platforms, auto discovery of accounts. The string must be semi-colon separated name=value pairs, such as encrypt=yes;database=master;... The connection string is checked for syntax, but the content can only be validated when used. The allowable name=value pairs vary across database platforms. For a full description consult the Client Setup Guide. NOTE: For MS SQL Server this connection string is ignored when using a domain or local computer functional account.	No	
TACACS+ Shared Secret	This value is the TACACS+ Shared Secret. This value must match the shared secret that is set when configuring TPAM as an AAA client.	No	

Custom information tab

There are six fields that can be customized to track information about each system. These custom fields are enabled and configured by the System Administrator in the /admin interface. If these fields have not been enabled then this sub-tab is not visible.

Connection tab

The connection tab is used to configure the functional account that TPAM will use to connect to the system. This tab is not enabled unless the **Enable Automatic Password Management?** check box is selected on the details information tab (except for the SPCW platforms). The boxes available on the connection tab are dependent on the platform type of the system being configured.

NOTE: As a PSM ISA you cannot access the Connection tab, except for SPCW platforms.

The table below describes the different box options on the Connection tab.

Table 4: Systems Management: Details Connection tab options

Field	Description	Required?	Default
Functional Account Name	The functional account defines the account that is used to manage the accounts on the managed system. This account must be defined and configured on the managed system as defined in the appropriate Client Setup Instructions. The credential defines whether SSH uses a predefined key (DSS) to authenticate or a standard password. DSS is the preferred and more secure way of managing accounts on systems that support SSH. You have the option to let PPM manage the functional account. The auto-change parameters for this password may then be configured via the account information tab, as with any other account. This helps to secure the managed system, by not maintaining a "static" password on a functional account.	Yes	funcacct

Field	Description	Required?	Default
	NOTE: After a system is saved for the first time, any changes in the system parameters are not automatically applied to the functional account, unless the **Push defaults out to All Accounts** switch on the management tab has been selected. The auto manage function never propagates to the functional account. It must be manually set.		
Alternate Port (platform specific)	Most non-Windows platforms allow alternate ports to be configured for communication of standard protocols, such as SSH, Telnet, or database ports.	No	
Domain Name (platform specific)	When the system platform being created represents a central authority such as Active Directory, BokS, or PowerPassword, the fully qualified domain name must be specified. DO not enter an alias, simple name or NetBIOS name. Max of varchar(255).	Yes	
Distinguished Name (platform specific)	LDAP/LDAPS and Novell systems require this field. Max is varcahr(2000).	Yes	
NetBIOS Domain Name (platform specific)	Windows domain systems (Active Directory or SPCW) also include the NetBIOS Domain Name box. Specify the name of the domain in NetBIOS format.	Yes	

Field	Description	Required?	Default
SID/ Service_Name (Oracle DB only)	Specifies either the security ID (SID) or the service name for Oracle databases, and should match the setting in SQLNET.ORA at the database server.	Yes	
Server O/S (BoKS only)	Select the O/S running on the server from the list.	Yes	AIX
Use Domain Account (platform specific)	If selected, uses the domain account to change accounts passwords on the central authority.	No	
Local Computer Account (MS SQL Server only)	If selected, uses Windows account on the host system, which also must be configured as a managed account in TPAM, to connect to the system. Format should be system\account. Named pipe connections must be enabled using SQL Server Configuration Manager on the target system.	No	
Connection Timeout	The connection timeout value determines the amount of time in seconds that a connection attempt to the managed system remains active before being aborted. In most cases, it is recommended to use the default value (*20* seconds). If there are problems with connection failures with the system, this value can be increased (for example, connections to Windows systems are often slower than SSH connections and may require a significantly higher timeout value). Max value 9999.	Yes	20

Field	Description	Required?	Default
PSM Functional Account (SPCW only)	The PSM functional account is used to provide secure communication during the session and file transfer during a session. If the PSM enabled account on the system is configured to use a proxy type of RDP through SSH, the PSM functional account is used during this connection.	Yes	psmfuncacct
Tunnel DB Connection Through SSH (platform specific)	Database tunneling through SSH provides the ability to securely connect to a remote database. Enter the account name used to connect to the remote system. If SSH is not listening on port 22, enter the correct port number to be used. For DBMS accounts, SSH tunneling only uses the public key for establishing the SSH connections. NOTE: Make sure that the default of AllowTCP Forwarding is set to Yes on the SSH Configuration file of the managed system.	No	Off
DSS Account Credentials	When using DSS key authentication, a function is available to permit specific configuration of the public/private keys used. • **Avail. System Std. Keys** – uses the single standard SSH keys (either Open SSH or the commer-	No	

Field	Description	Required?	Default
	cial key) stored centrally on TPAM. You have the ability to have up to three active keys simultaneously. These keys are configured in the admin interface. Use the list to select the key you want to retrieve. NOTE: When using the **Avail. System Std. Keys** you cannot specify the key that is used. One or all available keys may be downloaded to the remote system, but TPAM attempts to use *all* currently active keys when communicating with the remote system. • **Use System Specific Key** – allows the generation and download of a specific SSH key to be used with this system only. The key must first be generated using the **Get/Regen Key** button, and then downloaded in either Open SSH or Sec SSH (commercial) format.		
Password Account Credentials	If a password is entered it must match the password for the account on the managed system, otherwise password changes for accounts on this system will	No	

Field	Description	Required?	Default
	fail.		
Enable Password (platform specific)	Some systems may require the use of very specific accounts for access. Password to use for the "ENABLE" account (Cisco platforms only) or "EXPERT" account (for CheckPoint SP platforms only.		
Authentication Method (Cisco Router TEL only)	Username/password is used when a username is needed to connect to the system. Line definition is used when there is no username to be specified, it is simply a password on the terminal connection.	Yes	Username/ Password
Expert Password (CheckPoint SP only)	Setting up an Expert Password allows configuration access to the system.	Yes	
Custom Command (Mainframe only)	If there is a special command that needs to be entered prior to being prompted for authentication credentials, it is specified by placing the command in the custom command box.	No	
Use SSL? (platform specific)	Select this box if communications between TPAM and the device requires the SSL option.	No	Off
Non-Privileged Functional Account (Windows AD only)	If selected, any password changes for accounts on this system use the managed account's current password to log in and make the password change instead of using the functional account password.	No	Off
Allow Functional	If selected, requestors on	No	Off

Field	Description	Required?	Default
Account to be Requested for Password Release	this system can make a request to release the password for the functional account. If not selected, the functional account passwords are not available for release to a requestor and are only accessible to an ISA.		

Management tab

The management details tab is used to configure how TPAM manages the passwords for accounts on this system. This tab is not enabled unless the **Enable Automatic Password Management?** check box is selected on the details information tab. Once set, these parameters are inherited by accounts added to this system. These options can be overridden at the account level.

NOTE: As a PSM ISA you cannot access the management tab except for SPCW systems.

The table below explains the options on the Management Details tab.

Table 5: Systems Management: Details Management tab options

Field	Description	Required?	Default
Password Check Profile Name	Select a password check profile from the list to determine the rules for how the password is checked on the system against what is stored in TPAM. The partition selected determines the list of profiles available. The password check profiles are configured by the TPAM Administrators and the Partition Administrators.	Yes, if automatic password management has been selected.	Default from system template, or one marked as default.
Password Change Profile Name	Select a password change profile from the list to determine the rules for how the password is changed on the managed system. The partition selected determines the list of	Yes, if automatic password management has been selected.	Default from system template, or one marked as default.

Field	Description	Required?	Default
	profiles available. The password change profiles are configured by the TPAM Administrators and the Partition Administrators.		
Push Defaults out to All Accounts	Default change settings and management properties can be configured differently between systems and the defined accounts for those systems. If the desire is to ensure consistency throughout this parent-child relationship, it is possible to push the configuration of the default check and change settings from the system object to all child objects defined for the system. If selected, these settings will be pushed to the accounts when the **Save Changes** button is clicked. This is a one-time synchronization and may still be changed at the account level. NOTE: Synchronized password subscribers will not receive these updates.	No	Off
Enable auto management on All Accounts	To enable this check box the **Push Defaults out to All Accounts** must be selected first. If selected, auto management will be enabled on all accounts under this system when the **Save Changes** button is clicked. This is a one-time synchronization and may still be changed at the account level.	No	Off

Field	Description	Required?	Default
	NOTE: The functional account defined for the system does not receive the **Enable Auto Management on All Accounts** setting during a push. The auto-manage property must be manually enabled for the functional account. NOTE: Synchronized password subscribers will not receive these updates.		
Default duration for ISA releases of password	The duration for an ISA release may be specified up to a maximum of 21 days. This is the amount of time that transpires between the initial ISA retrieval and the automatic reset of the password (if enabled). If 0 is entered the ISA retrieval of a password will not trigger a post release reset of the password.	No	2 Hours
Allow ISA to enter Duration on Release	If selected, an ISA may enter a release duration other than the default when retrieving a password. The duration must be greater than zero and less than or equal to the maximum specified for either the ISA Duration or Max Release Duration (details information tab).The setting does not propagate to existing accounts, it will only get pushed to accounts added after it is selected. This check box is disabled when the Default duration for ISA releases of passwords is set to 0.	No	Off

Field	Description	Required?	Default
Profile Notification Certificate	This is required if this system is using a check or change profile that is using the **Allow system to notify TPAM it is available for check/change**. • No certificate - no thumbprint or certificate. Default • Thumbprint Only - The SHA1 thumbprint of the certificate used by the system to notify TPAM of availability for check-/change operations. • User-Supplied - user can upload their own certificate to TPAM. • Created by TPAM -TPAM will generate a certificate and record the thumbprint. This certificate must be installed on the system in order to call the TPAM notification service. There is an optional password on a TPAM generated certificate. This password will be required to install the certificate on the target system. The password is NOT stored and cannot be retrieved if forgotten.	Yes, depending on password profile options.	

How to call the notification service

For systems that are going to notify TPAM that they are online and available for check and changes, there is a new REST service endpoint is available on the TPAM appliance.

A system can make a call to the following address to notify TPAM that it is online and available for check/change: https://tpamAddress:9443/available

The call can be made using a language or scripting environment of the user's choice.It requires a certificate to be included with the http request. The thumbprint of that certificate

must be on file in TPAM for a managed system. When the call succeeds and TPAM finds the thumbprint all accounts on that system which have profiles allowing notification will be scheduled for checks/changes as required. The service returns a JSON dataset with the following information:

- CertificateThumbprint - 40-byte hexadecimal value of the certificate attached to the request. This does not indicate the request was accepted or not - it's just an echo of what the cert is. Debug purposes primarily. This value may or may not stay.
- ErrorID - number - 0 = good, non-zero = error occurred. Note that "success" does *not* necessarily mean anything was added flagged for processing.
- ResultMessage - text. Either "Success" or some error message. Right now it will return an error message informing you of an unrecognized thumbprint.
- If no certificate is attached the call will result in a 403 error (403 - Forbidden: Access is denied).

Ticket system tab

The ticket system tab is used to configure third party ticket system requirements when submitting password release, file release or session requests for this system. The ticket system tab is only enabled if the TPAM System Administrator has configured ticket system/s in the admin interface. The settings on this tab become the default settings for any accounts or files added to this system.

The following table explains the options on this tab.

Table 6: Systems Management: Details Ticket system tab options

Field	Description	Required?	Default
Ticket Required for	By selecting the check boxes you can require that ticket validation is enforced for Password/Files requests and/or Session requests.You also have the option to require ISAs to supply a ticket number prior to retrieving a password or file as well as requests made through the CLI or API. If a check box is not selected, users can still enter a ticket number on a request, but it is not required.	No	Off
Require Ticket Number from	If multiple ticket systems are enabled they are listed in the list for selection. You can specify the ticket system or allow entry of a ticket number from any system that is enabled.	No	Off
Send Email to	If any of the ISA, CLI or API required check	No	No

Field	Description	Required?	Default
	boxes are left clear you have the option of entering one or more email addresses (up to 255 characters) that will receive an email when an ISA, CLI or API user releases or retrieves a password or file without supplying a ticket.		
Push ticket defaults out to all accounts and files	If selected, when the **Save Changes** button is clicked, it will push these settings to all accounts and files under the system. New accounts and files will inherit these settings. NOTE: The propagation is a one time update each time this check box is selected and the **Save Changes** button is clicked. After that there is no forcing of the settings to remain in synch. The settings on the accounts and files can be overridden.	No	Off

LDAP schema tab

This tab is only enabled for LDAP, LDAPS and Novell NDS systems. It is used to customize the schema. The fields in this tab specify the value of core attributes as well as the name (s) of optional attributes. For example 'objectClass' is a core attribute with defined values that distinguish the specific directory object as group, user or computer. Similarly with attribute naming, a group object's member attribute may be called 'member' 'uniquemember' or 'memberUid', first name attribute may be called 'givenName', etc.

Template tab

The template tab is used to save all the settings for a system as a template. Templates may be used to quickly create new systems with a given set of default values via the web interface, CLI or API. Templates can only be created and edited by TPAM Administrators. Only TPAM Administrators and ISAs may use templates.

The table below explains all of the box options available on the Template tab.

Table 7: Systems Management: Template tab options

Field	Description	Required?	Default
Create a Template from this System	Selecting this flag saves this system as a System Template. NOTE: After a template has been created you cannot clear this flag.	No	Off
Use this as the Default Template	If selected, this template is used when adding new systems unless another template is chosen with the **Use Template** button. Only one template can be designated as the "Default" at a time. If a template is designated as the "Default" it is listed in purple italics on the Manage Systems listing.	No	Off
Retain Collection Membership in the template	If selected, TPAM creates the template with all the collection memberships currently defined on this system. Systems created from this template will have the same collection memberships. NOTE: If this system is a member of an AD Integration Collection, that membership is **not** transferred to the template and subsequent systems.	No	Off
Retain User/Group Permissions in the template	If selected, TPAM creates the template with all the User and Group permissions (Access Policy assignments) currently defined on the system. Systems created from this template will have the same permissions.	No	Off
Retain Existing Accounts in the template	When creating a template based on an existing system, this option allows you to retain up to 20 accounts from the existing system (including the functional account.) If this option is selected, use the table located below this option to select the accounts to be included in the template. The functional account cannot be cleared.	No	Off

Field	Description	Required?	Default
	NOTE: Accounts included in the template do **not** retain any passwords, password history, or dependent system information.		

Account discovery tab

Account discovery profiles allow TPAM to periodically check for accounts on a managed system and add or remove them from TPAM. Account discovery profiles can only be assigned to Windows, *nix and database systems. If account discovery is going to be used for a system, the account discovery profile to be used is assigned on this tab. The time displayed on the Log tab is the user's time zone.

The table below describes the options available on the Account Discovery tab

Table 8: Systems Management: Account discovery tab options

Field	Description	Required?	Default
Discovery Profile	Select the profile to be used for account discovery. Profiles available will be based on the partition selected on the Details tab. Only available for Windows, *nix, and database platforms.	No	
Exclude List	Any accounts that you want to be excluded from the account discovery process can be listed here. Up to 1000 characters, case insensitive.	No	
Timeout (seconds)	The number of seconds the auto discovery process will run before it will time out. If the discovery process times out it will continue to discover the remaining accounts during the next scheduled run. If the box is left null the default value of 300 seconds is used.	No	300
Test Discovery Profile	Once the profile has been saved, click the **Test Discovery Profile** button to see what accounts and actions are found. No changes are made, it is only a test.	n/a	
Run Discovery Profile	Click this button to run account discovery for this system on demand, rather than waiting for the scheduled run. The number of accounts that can be discovered by clicking	n/a	

Field	Description	Required?	Default
	this button is limited to 5,000. More than 5,000 can be discovered during the automated runs.		

Affinity tab

The Affinity tab is used to assign the system to a distributed processing appliance (DPA) if DPA's are configured to work with the TPAM appliance. Assigning the system to a DPA can help optimize performance for session recording, session playback and password checking and changing. The affinity tab is not enabled until the system has been saved.

IMPORTANT: If you have DPA's with version 3 software on them, and the TLS Global Setting has been set by the System Administrator to 1 or 2, then the DPA v3 appliances will be not listed on the Affinity tab. DPA v3's require a TLS global setting of 0.

The table below describes the options available on the Affinity tab.

Table 9: System Management: Affinity tab options

Field	Description	Required?	Default
Allow PSM Sessions to be run on any defined DPA	If selected, TPAM will select the DPA that has the least number of sessions running on it to conduct the session. NOTE: Must have ISA permissions for sessions.	No	Yes
Selected DPA affinity and priority	Select this option to prioritize which DPA is used for sessions conducted on this system. The default DPA is LocalServer, which is the local TPAM appliance. Use the Priority column in the table below this option to enter a priority number next to each DPA. Leave the box blank (NULL) for any DPAs you do not want to use for session recordings. When determining which DPA to use, the appliance looks at them in order from lowest to highest and uses the first one that has an open slot. NOTE: Must have ISA permissions for sessions.	No	No

Field	Description	Required?	Default
Use local PPM appliance for password checks and changes	If selected, then all password checks and changes will be run on the TPAM appliance. NOTE: Must have ISA permissions for passwords.	No	Yes
Selected DPA Affinity	Select this option to prioritize which DPA is used for password checking and changing on this system. If this is selected and auto account discovery has been configured the DPA will be used to process auto discovery for systems that allow a connection port to be specified and database systems that are NOT using SSH tunneling. NOTE: DPA v3 requires that SMBv1 be enabled for password check and changes on Windows systems. NOTE: We do not support using named instances for SQL Server when using a DPA for password checks and changes. The workaround is to specify the port. Use the Priority column in the table below this option to enter a priority number next to each DPA. Leave the box blank (NULL) for any DPAs you do not want to use for password management. When determining which DPA to use, the appliance looks at them in order from lowest to highest and uses the first one that has an open slot. A value of 0 (zero) is simply "more important" than any other value. NOTE: Must have ISA permissions for passwords.	No	No

Collections tab

A collection is a group of systems, accounts and or files. The collections tab is used to assign the system to a collection/s. Systems can belong to more than one collection. The collections list shows all collections that have been defined to the TPAM appliance if the user modifying the system is an administrator. If the user modifying the system is an ISA, only the collections that the user holds the ISA role for are displayed. By assigning the

system to collections, the system automatically inherits user and group permissions that have been assigned at the collection level.

NOTE: A system cannot belong to a collection that already contains any of its accounts or files. Conversely, an account or file cannot be added to a collection that already contains that entity's parent system.

NOTE: If a collection is tied to either AD or Generic Integration the system's membership status in that collection cannot be changed.

NOTE: An ISA can only assign a system to a collection if they have Password and Session ISA permissions on the system and the collection.

Use the **Filter** tab to enter search criteria for the collections to assign/un-assign. Click the **Results** tab.

The table below explains the fields on the Results tab.

Table 10: Systems Management: Collections Results tab options

Field	Description	Required?	Default
Type	On this tab type will always say **Collection**.		
Name	The name of the collection. Clicking on the name will take you to the collection management listing tab.	No	
Membership Status	To modify collection membership, simply click the **Not Assigned** or **Assigned** buttons next to each collection name and click the **Save Changes** button. You can set all members to either Assigned or Not Assigned by holding down the Ctrl key when clicking on any button.	No	Not Assigned

Permissions tab

The permissions tab is used to assign users and/or groups an access policy for this system.

NOTE: To assign an access policy to a system you must have password and session ISA permissions assigned for that system. Without both ISA permissions you will only be able to view access policy assignment.

To assign Access Policies:

1. Use the table on the left of the page to select the name/s of the user/s and/or group/s to which the selected access policy is to be assigned.

2. Select an access policy from the **Access Policy** list in the access policy details pane, located in the right upper side of the results tab. When you select an access policy on the list the detailed permissions describing this access policy are displayed on the rows below.
3. Select one of the icons in the access policy details pane (right upper side of page) to make the assignment.

Table 11: Access policy details pane icons

Icon	Action
	Refreshes list of available Access Policies.
	Scrolls the currently selected User or Group into view.
	Applies the currently selected policy to the current row. Assigning a policy of "Not Assigned" removes the current assignment. This affects only the current row (row with the dotted border) even if multiple rows are selected.
	Applies the currently selected policy to all selected rows in the list. You are asked to confirm the assignment if more than 10 rows are affected.
	Removes the currently selected policy from all selected rows in the list. If a row is not currently set to the selected policy it will not be changed. You are asked to confirm the assignment if more than 10 rows are affected.
	Removes unsaved edits on the current row. This only affects the current row (row with the dotted border) even if multiple rows are selected.
	Removes unsaved edits on all currently selected rows.

This icon () next to any row on the list simply means that row has been edited since the last save changes occurred.

You can "Shift+Click" to select a range of rows. The first row you click will be surrounded by purple dashed lines. The next row that you "Shift-Click" on will cause all the rows in between the original row and current row to be highlighted.

4. When you are finished assigning/un-assigning Access Policies, click the **Save Changes** button.

TIP: You may re-filter and re-retrieve the results list without losing existing edits. As the **Results** tab is reloaded any Groups or Users that you have already edited reflect their edited policy assignment. When you click the **Save Changes** button all the Access Policy assignment changes for the system are saved. The appliance saves these in batches, informing you of the number of assignments added, removed, or changed for each batch.

NOTE: You must be both a PPM **and** PSM ISA over a system to be allowed to assign an access policy.

Using Ctrl-Click or Shift-Click on the hyperlink in the Name column will open the details page for this entity in a new tab or window.

Add a system

When adding a system in TPAM, information is entered on the following tabs to configure the system:

- Details
- Template
- Connection
- Management
- Affinity
- Ticket System
- Collections
- Permissions
- Account Discovery
- LDAP Schema

The following procedure describes the **required** steps to add a system.

NOTE: If a user only has ISA permissions at the account and file level, they will not be able to add a system.

To add a system:

1. Select **Systems & Accounts | Systems | Add System** from the menu.
2. Enter information on the **Details Information** tab. For more information on this tab see Information tab.
3. Click the **Custom Information** tab to add custom information about this system. (Optional) For more details see Custom information tab.
4. Click the **Connection** tab to configure the functional account that TPAM will use to connect to the system. For more details see Connection tab.
5. Click the **Management** tab and select preferences for managing account passwords. For more details see Management tab.
6. Click the **Ticket System** tab and set external ticket system requirements for submitting password release requests. For more details see Ticket system tab. (Optional)

7. Click the **LDAP Schema** tab to tweak LDAP mapping attributes. For more details see LDAP schema tab. (Optional)
8. To save this system as a template, click the **Template** tab and enter the requested information. For more details see Template tab. (Optional)
9. Click the **Account Discovery** tab to assign an account discovery profile. (Optional) For more details see Account discovery tab.
10. Click the **Affinity** tab and make DPA assignments. For more details see Affinity tab. (Optional)
11. Click the **Collections** tab and assign/remove membership. For more details see Collections tab. (Optional)
12. Click the **Permissions** tab and assign/remove permissions. For more details see Permissions tab. (Optional)
13. Click the **Save Changes** button.

Add a system using a template

To add a system using a template:

1. Select **Systems & Accounts | Systems | Add System** from the menu.
2. Click the **Use Template** button.
3. Select a template on the listing tab.
4. Click the **Details** tab.
5. Enter the system name.
6. Change the system IP address.
7. Make any other changes as desired.
8. Click the **Save Changes** button.

If the administrator has set a template as the default template, every time you add a system it will

automatically use this template.

Test a system

Once a system has been saved, to test TPAM's connectivity to the system, click the **Test System** button. The results of the test will be displayed on the Results tab.

NOTE: You must have ISA permissions for passwords in order to test a system.

Clear a stored system host entry

The **Clear Sys. Host Entry** button removes the host entry from TPAM's known hosts file. An example of the necessity for this would be a situation where the SSH package on a managed system has been reinstalled, or the OS itself may be reinstalled. A test of the system would indicate that the host key entry does not match, and is preventing password authentication because of a perceived "man in the middle" attack. This can be performed through the CLI by running the ClearKnownHosts command.

NOTE: You must have ISA permissions for passwords in order to clear a stored system host entry.

To clear the System Host entry:

1. Select **Systems & Accounts | Systems | Manage Systems** from the menu.
2. Enter your search criteria on the filter tab.
3. Click the **Listing** tab.
4. Select the system whose host entry is to be removed from TPAM's known hosts file.
5. Click the **Clear Sys. Host Entry** button.

Duplicate a system

To ease the burden of administration and help maintain consistency, systems can be duplicated. This allows the administrator to create new systems that are very similar to those that exist, while only having to modify a few details. The new system inherits collection membership, permissions, affinity and ticket system settings from the existing system.

To duplicate a system:

1. Select **Systems & Accounts | Systems | Manage Systems** from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the system to be duplicated.
5. Click the **Duplicate** button. A new system object is created and the System Details page displays. The name of the new system is automatically **DupofXXXXX.**
6. Make any changes to the system configuration on the various tabs.
7. Click the **Save Changes** button.

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.

NOTE: ISAs with only password permissions will not see any "PSM Only" systems or systems with a platform of PSM Web Access in the system listing.

To list the systems:

1. Select **Systems & Accounts | 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.

5

Accounts

Introduction

This chapter covers the steps to add and manage accounts in TPAM. To add and manage accounts, information is entered on the following tabs in the TPAM interface:

Table 12: Account Management: TPAM interface tabs

Tab name	Description
Details/Information	Define main account information, such as name, password rule, contact.
Details/Reviews	Set review requirements for password releases on this account.
Details/Custom Information	Enter data in custom fields, if they have been defined.
Details/Management	Configure the settings for how TPAM will manage the password for the account.
Details/Ticket System	Configure Ticket System Validation for requests on this system.
Dependents	Set systems that are dependent on the domain level account.
Logs	Can view test, change and release history for the account.
Passwords	Can view past passwords and retrieve current password with ISA PPM permissions.
Collections	Assign an account to a collection/s.
Permissions	Assign users and groups permissions on this account.
PSM Details/General	Enable PSM functionality for the account and set approval requirements.
PSM Details/Session	Set authentication method sessions using this account.

Tab name	Description
Authentication	
PSM Details/File Transfer	Enable/disable file transfer.
PSM Details/Review Requirements	Set review requirements for sessions.

Information tab

The table below explains all of the box options available on the details information tab.

Table 13: Account Management: Details information tab options

Field	Description	Required?	Default
Account Name	This is the descriptive name of the account. Within TPAM, all the account names on one system must be unique. The name can be 1-30 characters long, but cannot include empty spaces.	Yes	
Name on Domain	Name of the account on the domain in the form of domain\account. Allows 286 characters (domain name of 255 + \ + accountname of 30). For *nix platforms when system is managed by a domain account.	No	
Account is Locked	This check box gives Administrators and ISA's the ability to "lock" and "unlock" an account. When an account is locked passwords for that account cannot be retrieved, released, changed or checked. Password requests or session requests can be submitted but the password or session is not available until the account is unlocked.	No	Off
Password	Enter the active current password for the account. If no password is specified (left blank), PPM stores the value *default initial password* as the password for the account.	No	
Confirm	To confirm the password reenter it in this box.	No	
Password Rule	Select the password rule to serve as the default for the account. If the selection is not changed (or if no other rules have been defined in TPAM) the Default Password Rule is selected. The	Yes	Default Password Rule

Field	Description	Required?	Default
	password rule governs the construction requirements for new passwords generated by PPM.		
Distinguished Name	Only required for LDAP, LDAPS, and Novell platforms.	Yes	
Issue ndmcom for this account?	Only visible for HP NonStop Tandem platform. If selected the ndmcom command is issued after the password for the account is changed.	No	Off
Change password for Windows Services started by this Account?	Only visible for Windows platforms. If this is the Administrator account, or another functional account that runs system services, this option ensures that the password change is also applied to each service the account runs.	No	Off
Automatically restart such services?	Only visible for Windows platforms. If selected, after the password is changed the services will automatically be stopped and restarted.	No	Off
Change the password for Scheduled Tasks started by this account?	Only visible for Windows platforms. If selected, after a task has been completed it will change the password.	No	Off
Use this account's current password to change the password?	Only visible for Windows platforms. This may be necessary on Windows XP and Windows Server 2003 where Encrypting File System or other third-party security products are used, and rely on authentication certificates stored in that account's personal store. NOTE: If the system is configured with a "non-privileged functional account" then this setting defaults for all accounts added to this system. NOTE: If the password has expired, TPAM will not be able to change the password.	No	See Note
Description	This is a free text box where additional descriptive information may be entered.	No	
Password Management	By default, the property of the parent system is inherited at the account level as either **None** or	Yes	Defaults to what

Field	Description	Required?	Default
	Automatic. • **None** - The Management tab will be disabled, and TPAM will not automatically check, change or reset the password. Manually pressing the Check Password or Reset Password buttons WILL result in a check or reset for this account. • **Automatic** - TPAM manages the password for this account based on the settings configured on the Management tab. • **Manual** - TPAM sends an email to the primary contact at the system and account level when it is time to manually reset the password. The email is sent based on the change frequency settings on the Management tab. The contact/s will keep receiving this email at regular intervals based on how this is configured by the Sys-Admin in the Auto Management Agent settings, until the password has been confirmed to be reset in PPM. NOTE: The manual password email notification relies on the Man Pwd Change Agent. If it is not running no email notifications to reset the password will be sent.		is set at the system level.
Ignore System Access Policies	If selected, any access policies assigned to the system will not apply to this account.	No	Off
Enable account before release	Only visible for Windows platforms. If selected TPAM will enable the account when: - releasing the password for a request - ISA password release - starting a PSM session which uses password authentication If the account cannot be enabled the password will not be released and the session will not start. If the account cannot be disabled when the password is changed the change will be marked as successful but an alert will raised. The alert	No	Off

Field	Description	Required?	Default
	must be subscribed to in the admin interface. See the help bubble text in the TPAM interface for more details. If this check box is selected, this account cannot be added as a Synchronized Password subscriber. NOTE: If this flag is selected and the account has the incorrect password, this will be reported as a mismatch if password is checked through the DPA, and disabled if checked through the TPAM console.		
Approvals Required	The default value of 1, indicates that a single approval allows the requestor to view the password. A value greater than 1 requires multiple approvers to approve each release request. A value of 0 means any release requests will be auto-approved by TPAM. If this value is overridden by an access policy the greater of the two values is used.	Yes	1
Require Multi-Group Approval from	Can only be selected if Approvals Required is greater than 1. If selected, you can require that approvals for requests come from two or more groups. At least 1 approval must come from each group. Select the check box in the **Sel** column to select the groups. NOTE: Any user with approver permissions will be able to approve the request, but unless the user is a member of one of the selected groups, their approval will not count. NOTE: Any authorized approver can approve or deny the request at any time.	No	Off
Multi-Group Approver Order	The number entered in the **Ord** column determines the order that the request must be approved. Once the first group approves the request then the email notification to the second group to approve will go out and so on. The number entered in the **#** column represents how many approvers from that group must approve the request.	No	Off

Field	Description	Required?	Default
Maximum Duration	Maximum duration for a password release on the account. If this is overridden by an Access Policy assignment, the lower of the two durations is used. The default duration that the requestor sees for any new password request is *2 hours*, or the maximum duration, whichever is less.	Yes	7 days
Notification Email	The email address specified in this box receives notification of certain password releases. • Password releases by ISA users, CLI/API users under all circumstances, and requests when no approvals are required. • Scheduled password changes for manually managed accounts. • Scheduled password changes for managed accounts with **Send notification only** selected on the password change profile. Multiple email addresses can be specified by entering each email address separated by a comma, up to a maximum of 255 characters. Any time a change is made to the notification email address box, an email is automatically sent to the old email address with a notification that this change has occurred.	No	Null
Simultaneous Privileged Access Release	This option allows an Admin or a PPM ISA to grant more than one Privileged Access User (PAC) to request and retrieve a password/session during the same or overlapping time period. NOTE: If another Requestor already has the password checked out the Privileged Access users must wait for that release window to expire before they can gain access.	Yes	1
Override Individual Accountability	The System Administrator must have this global setting turned on in order for the TPAM Administrator or ISA to select this flag. If selected, more than one requestor can request the password at the same time or during an overlapping duration. Any changes made to the override individual accountability check box at the account level are logged in the Activity Log.		

Field	Description	Required?	Default
	If the System Administrator disables the Global Setting allowing account override, any accounts that had been selected to override individual accountability will have their check boxes cleared.		

Reviews tab

The table below explains all of the options available on the Reviews tab.

Table 14: Account Management: Review tab options

Field	Description	Required?	Default
Reviews Required	Number of reviews required after a password release has expired.	No	0
Any Authorized Reviewer (excluding Requestor)	If selected, any auditor, and any user or group member with an access policy of Review Password permission will be eligible to complete the review.	No	Off
Specific User	If selected, the specific user with review permission will be the only user allowed to review password releases for this account.	No	Off
Any Auditor	If selected, any user with a user type of auditor will be eligible to review password releases for this account.	No	Off
Member of a Group	If selected, any users that are members of the group that is chosen will be eligible to review password releases for this account. Only groups that have review permissions will be available in the list.	No	Off
If the review isn't complete ...	To have a user receive an email notification if the review is not complete within X hours, enter the hours threshold and the email address. The password release is not eligible for review until the release duration expires.	No	NullDetails

Custom Information tab

There are six fields that can be customized to track information about each account. These custom fields are enabled and configured by the System Administrator in the /admin interface. If these fields have not been enabled then this sub-tab is not visible.

Management tab (PPM ISAs only)

The Management tab is used to configure how TPAM manages the passwords for this account. This tab is not enabled unless **Automatic** or **Manual** is selected on the Details Information tab. The settings here will default from the system settings but can be overridden.

The table below explains the options on the Management Details tab.

Table 15: Acount Management: Details Management tab options

Field	Description	Required?	Default
Password Check Profile Name	Select a password check profile from the list to determine the rules for how the password is checked on the system against what is stored in TPAM. The password check profiles are configured by the TPAM Administrator.	Yes, if automatic password management has been selected.	Whatever profile is assigned for the system.
Password Change Profile Name	Select a password change profile from the list to determine the rules for how the password is changed on the managed system. The password change profiles are configured by the TPAM Administrator.	Yes, if automatic password management has been selected.	Whatever profile is assigned for the system.
Pull Defaults from System	If selected, upon saving, the Management settings of the system are populated at the account level. This is a one time action and does not prevent any of these settings from being modified again at the account level.	No	Off
Default duration for ISA releases of password	The duration for an ISA release may be specified up to a maximum of 21 days. This is the amount of time that transpires between the initial ISA retrieval and the automatic reset of the password (if enabled). If 0 is entered the ISA retrieval of a password will not trigger a post release reset of the password.	No	From System

Field	Description	Required?	Default
Allow ISA to enter Duration on Release	If selected, an ISA may enter a release duration other then the default when retrieving a password. The duration must be greater than zero and less than or equal to the maximum specified for either the ISA Duration (Mgt Details tab) or Max Release Duration (Details tab). This check box is disabled when the Default duration for ISA releases of passwords is set to 0.	No	From System
Next Change Date	Schedule an account password to be changed at a specific date/time. Overrides password change profile schedule. Password mismatch, post release reset, and force resets will still be processed as they occur.	No	

Ticket System tab (PPM ISAs only)

The Ticket System tab is used to configure third party ticket system requirements when submitting password release requests for this account. The Ticket System tab is only enabled if the TPAM System Administrator has configured ticket system/s in the /admin interface.

The following table explains the options on this tab.

Table 16: Account Management: Details Ticket System tab options

Field	Description	Required?	Default
Ticket Required for	By selecting the check boxes you can require that ticket validation is enforced for Password/Files requests and/or Session requests.You also have the option to require ISAs to supply a ticket number prior to retrieving a password or file as well as requests made through the CLI or API. If a check box is not selected, users can still enter a ticket number on a request, but it is not required.	No	Off
Require Ticket Number from	If multiple ticket systems are enabled they are listed in the list for selection. You can specify the ticket system or allow entry of a ticket number from any system that is enabled.	No	Off
Send Email notification to	If any of the ISA, CLI or API required check boxes are left clear you have the option of entering one or more email addresses (up to 255 characters) that will receive an email when an ISA, CLI or API user	No	From System

Field	Description	Required?	Default
	releases or retrieves a password without supplying a ticket.		
Pull defaults from system	If selected, when the **Save Changes** button is clicked, it will pull these settings from the system The propagation is a one time update each time this check box is selected and the **Save Changes** button is clicked. After that there is no forcing of the settings to remain in synch. The settings on the accounts can be overridden.	No	Off

Dependents tab (Windows AD only)

If the account managed by PPM is a Windows domain account (the system is defined as Active Directory), services running on domain member systems using this account can also be managed in terms of password changes.

Logs tab (PPM ISAs only)

The Logs tab contains three sub-tabs that provide detailed password history for the account. The log data displays the user's time zone. The following table explains the sub-tabs.

Table 17: Account Management: Logs tab sub-tabs

Tab	Description
Filter	This filter tab can be used to specify your search criteria in any of the other log tabs.
Change Log	Provides details on password change history.
Test Log	Provides details on password test activity.
Release Log	Provides details on password release history.
Dependent Change Log	Only visible if account resides on Windows Domain Controller with dependent systems assigned. Provides details on changes of the domain account.
Change Agent Log	Provides details on change agent log records for the account that have occurred after a 2.3+ TPAM upgrade.

Past Password tab (PPM ISAs only)

This tab allows a PPM ISA to view past password for an account. This allows you to select a password that was valid for a specific period of time. This is especially important if the managed system has been restored from a backup and the password that was effective at the time of the backup is required.

NOTE: Depending on how the TPAM System Administrator has configured global settings, this tab may not be available, or a warning message may pop up every time this tab is accessed.

Current Password tab (PPM ISAs only)

The tab allows users with ISA password permissions to retrieve the current password.

Collections tab

A collection is a group of systems, accounts and or files. The Collections tab is used to assign the account to a collection/s. Accounts can belong to more than one collection. The collections list shows all collections that have been defined in the TPAM appliance if the user modifying the account is an administrator. If the user modifying the account is an ISA, only the collections that the user holds the ISA role for are displayed. By assigning the account to collections, the account automatically inherits user and group permissions that have been assigned at the collection level.

NOTE: An ISA can only assign an account to a collection if they have Password and Session ISA permissions on the account and the collection.

NOTE: An account cannot belong to the same collection as its parent system, or vice versa.

Use the **Filter** tab to enter search criteria for the collections to assign/un-assign. Click the **Results** tab.

The table below explains the fields on the Results tab.

Table 18: Account Management: Collection Results tab options

Field	Description	Required?	Default
Type	On this tab type will always say **Collection**.		
Name	The name of the collection. Clicking on the name will take you the collection management listing tab.	No	

Field	Description	Required?	Default
Membership Status	To modify collection membership, simply click the **Not Assigned** or **Assigned** buttons next to each collection name and click the **Save Changes** button. You can set all members to either Assigned or Not Assigned by holding down the Ctrl key when clicking on any button.	No	Not Assigned

Permissions tab

The Permissions tab is used to assign users and/or groups an Access Policy for this account.

NOTE: To assign an access policy to an account you must have password and session ISA permissions assigned for that account. Without both ISA permissions you will only be able to view access policy assignment.

To assign Access Policies:

1. Use the table on the left of the page to select the name/s of the user/s and/or group/s to which the selected access policy is to be assigned.
2. Select an Access Policy from the **Access Policy** list in the Access Policy Details pane, located in the right upper side of the Results tab. When you select an Access Policy on the list the detailed permissions describing this Access Policy are displayed on the rows below.
3. Select one of the icons in the Access Policy Details pane (right upper side of page) to make the assignment.

Table 19: Access Policy Details pane icons

Icon	Action
	Refreshes list of available Access Policies.
	Scrolls the currently selected User or Group into view.
	Applies the currently selected policy to the current row. Assigning a policy of "Not Assigned" removes the current assignment. This affects only the current row (row with the dotted border) even if multiple rows are selected.
	Applies the currently selected policy to all selected rows in the list. You are asked to confirm the assignment if more than 10 rows are affected.
	Removes the currently selected policy from all selected rows in the list. If a

Icon	Action
	row is not currently set to the selected policy it will not be changed. You are asked to confirm the assignment if more than 10 rows are affected.
	Removes unsaved edits on the current row. This only affects the current row (row with the dotted border) even if multiple rows are selected.
	Removes unsaved edits on all currently selected rows.

This icon () next to any row on the list simply means that row has been edited since the last save changes occurred.

You can "Shift+Click" to select a range of rows. The first row you click will be surrounded by purple dashed lines. The next row that you "Shift-Click" on will cause all the rows in between the original row and current row to be highlighted.

4. When you are finished assigning/un-assigning Access Policies, click the **Save Changes** button.

TIP: You may re-filter and re-retrieve the results list without losing existing edits. As the **Results** tab is reloaded any Groups or Users that you have already edited reflect their edited policy assignment. When you click the **Save Changes** button all the Access Policy assignment changes for the account are saved. The appliance saves these in batches, informing you of the number of assignments added, removed, or changed for each batch.

Using Ctrl-Click or Shift-Click on the hyperlink in the Name column will open the details page for this entity in a new tab or window.

PSM Details tab (PSM ISAs only)

The PSM Details tab is composed of four sub-tabs: General, Session Authentication, File Transfer, and Review Requirements, that allow users to configure the account for Privileged Session Manager (PSM). PSM licences are required for this functionality to be enabled.

NOTE: PSM sessions to Windows machines using an RDP proxy connection type can be configured on the Windows machine to use SSL/TLS security for RDP connections. Note that the computer name set in TPAM for the system will be converted to uppercase for sessions.

General tab

The following table explains the options on the General tab.

Table 20: Account Management: PSM General tab options

Field	Description	Required?	Default
Enable PSM Sessions?	If selected, allows users to request access to this account through a recorded session. All subsequent options on the PSM tabs are contingent upon this being selected.	No	Off
Proxy Connection Type	Used to select the type of remote connection compatible with the configuration of the remote systems. Options are dependent on the system platform. NOTE: When choosing any of the proxy methods listed below that use Automatic Login, the password is not automatically reset after the session is completed because the password is never displayed to the user. Available choices are: • **DPA - ICA Access** - Using a DPA, establish a connection to the system using Citrix ICA web client. (For PSM ICA Access only) • **DPA - Web Browser** - Using a DPA, establish a connection to the system using a web browser. (For PSM Web Access only) • **RDP-Automatic Login Using Password** – Connect to the system using RDP (Terminal services protocol) client and automatically login using the password retrieved from the local or remote TPAM. This ensures that the password is never displayed or known to the user. • **RDP-Interactive Login** – Connect to the system using an RDP client that PSM does not provide automatic login for. If the password is managed by PPM, it is displayed on the window when the session is started, otherwise the user must know	Yes, if PSM Enabled	

Field	Description	Required?	Default
	the account password when the authentication dialog is presented. • **RDP Through SSH – Automatic Login Using Password** (for SPCW systems only) Connect to the system using RDP client via the SSH protocol and automatically login using the password retrieved from the local or remote TPAM. • **RDP Through SSH – Interactive Login** (for SPCW systems only) Connect to the system using RDP client via the SSH protocol and allow the user to manually type the password. If the password is managed by PPM, it is displayed on the window when the session is started, otherwise the user must know account password when the authentication prompt is presented. • **SQLPlus – Automatic Login Using Password** - Connect to the system using the SQLPlus client and automatically login using the password retrieved from the local or remote TPAM. • **SQLPlus –Interactive Login** - Establish a connection to the remote system using the SQLPlus client. The user must know the SQLPlus password for the system. If the password is managed by PPM, it is displayed on the window when the session is started, otherwise the user must know the account password when the authentication dialog is presented. • **SQL Window – Automatic Login Using Password** - Connect to the system using the Sql Window Client and automatically login using the password retrieved from the local or remote TPAM.		
Proxy Connection Type	• **SQL Window – Interactive Login** - Establish a connection to the remote system using the SQL Window client. The user must know the SQL Window password for the system. If the password is managed by PPM, it is displayed on the		

Field	Description	Required?	Default
	window when the session is started, otherwise the user must know the account password when the authentication dialog is presented. • **SSH-Automatic Login Using DSS Key** – Connect to the system using SSH and authenticate via DSS private key. The private key must be previously uploaded to TPAM for this purpose. • **SSH– Automatic Login Using Password** (for UNIX systems only) – Connect to the system using SSH and automatically login using the password retrieved from the local or remote TPAM. • **SSH - Interactive Login** – Establish an SSH session to the remote system and allow the user to manually type the password. If the password is managed by a PPM, it is displayed on the window when the session is started, otherwise the user must know account password when the authentication prompt is presented. • **Telnet-Automatic Login Using Password** – Connect to the system using the Telnet protocol and automatically login using the password retrieved from the local or a remote TPAM. This ensures that the password is never displayed or known to the user. • **Telnet-Interactive Login** – Connect to the system using the Telnet protocol, to which PSM does not provide automatic login. If the password is managed by a PPM, it is displayed on the window when the session is started, otherwise the user must know the account password when the authentication dialog is presented. • **VNC Enterprise - Interactive Login -** Establish a connection to the remote system using the VNC Enterprise client. The user must know the VNC password for the system. If the password is managed by a PPM, it is displayed on the window		

Field	Description	Required?	Default
	when the session is started, otherwise the user must know the account password when the authentication dialog is presented. IMPORTANT: To use VNC Enterprise as a proxy type a DPA is required. • **VNC-Interactive Login** – Establish a connection to the remote system using the VNC client. The user must know the VNC password for the system. If the password is managed by PPM, it is displayed on the window when the session is started, otherwise the user must know the account password when the authentication dialog is presented. • **x3270 - Automatic Login** - Establish a connection to the remote system using a 3270 emulator and automatically login using the password retrieved from the local or a remote TPAM.		
Proxy Connection Type	• **x3270 - Interactive Login Using Password** - Connect to the system using a 3270 emulator and allow the user to manually type the password. If the password is managed by a PPM, it is displayed on the window when the session is started, otherwise the user must know account password when the authentication prompt is presented. • **x5250 - Interactive Login** - Connect to the system using a 5250 emulator and allow the user to manually type the password. If the password is managed by a PPM, it is displayed on the window when the session is started, otherwise the user must know account password when the authentication prompt is presented.		
Custom Connection Profile	The connection profile can be used to override the default connection parameters. If any custom profiles have been created they will be available in this list. See Add a PSM connection profile for more on creating custom connection	No	Use Standard Settings

Field	Description	Required?	Default
	profiles.		
Post Session Profile	The post session file is used to add additional steps at the end of a session request. If any post session profiles have been created they will be available in this list. For more details on Post Session Profiles see Add a post session processing profile	No	Use Standard Settings
Color Depth	Only an option for some proxy types. Used to set the number of possible colors displayed in the recorded sessions for this account. The choices are proxy type dependent. Options are: • 8 - 256 colors • 16 - 65,000 colors • 0 - very low • 1 - low • 2 - medium • 3 - auto select/full color	No	8 or 0, depending on proxy type.
Required # of Approvals	The number of approvers required for each session request. A value greater than 1 requires multiple approvers to approve each session request. A value of 0 means any session requests will be auto-approved by TPAM. If this value is overridden by an access policy the greater of the two values is used. If the system/account is managed by PPM it is possible to have a different value for session and password request approvals. In the event of such a conflict, the value set on the password approvals required may override the value set here. This occurs only for connection types that use interactive login (where the password is displayed).	Yes	0
Require Multi-Group Approval from	Can only be selected if Approvals Required is greater than 1. If selected, you can require that approvals for requests come from two or more groups. At least 1 approval must come from each group. Select the check box in the **Sel** column to select the groups.	No	Off

Field	Description	Required?	Default
	NOTE: Any user with approver permissions will be able to approve the request, but unless the user is a member of one of the selected groups, their approval will not count. NOTE: Any authorized approver can approve or deny the request at any time.		
Multi-Group Approver Order	The number entered in the **Ord** column determines the order that the request must be approved. Once the first group approves the request then the email notification to the second group to approve will go out and so on. The number entered in the **#** column represents how many approvers from that group must approve the request.	No	Off
Maximum Simultaneous Sessions	Specifies the maximum number of simultaneous sessions that may be established for account. This option only exists for accounts configured to auto-authenticate the user. If the password is provided by TPAM for interactive logon then only one concurrent session is allowed to preserve individual accountability.		1
Default Session Duration	Session duration that is displayed by default when requesting a session. It can be changed within the limits set by the max password duration and the access policy session duration.	Yes	2 hours
Notify primary contact	Allows email notifications to be sent to the primary contact specified for the system if a session exceeds the maximum session time for the request. Configurable parameters are: frequency (in minutes) of notifications; and threshold time (in minutes) before initial notification is sent for a session. Both values must be non-zero for notifications to be sent.	No	0,0, null
Send PSM Start Notification	Email address that receives notification when a session on this account starts. The following special addresses may also be included: • :AllApprovers - all users who can approve the request • :Approvers - users that approved the	No	null

Field	Description	Required?	Default
	request • :Group=Group1,Group2... - comma separated list of one or more group names • :RelNotify - release notification email for the account • :System - primary email contact for the account		
Enable Clipboard?	If selected, during a session, the user can use the clipboard option for copy/paste.	No	On
Enable Console Connection?	If selected, during a session, the user can connect to the system console. This option is only available with RDP proxy types.	No	Off
Record All Sessions?	If selected, all sessions for this account will be recorded.	No	On
Enable File Uploads?	If selected, files can be uploaded from the remote system during the session.: NOTE: THe file name including the extension can not be longer than 60 characters. NOTE: This option cannot be selected until file transfer is enabled on the File Transfer tab.	No	Off
Enable File Downloads?	If selected, files can be downloaded to the remote system during the session. NOTE: This option cannot be selected until file transfer is enabled on the File Transfer tab.	No	Off
Capture Events?	If selected, events during the session are captured and listed in session logs with hyper links to that point in the session. This option is only available for specific platforms. Clicking the **Test Event Configuration** button will mimic event capture during a session for testing with the system. There is a scheduled report, Daily Session Activity Detailed, that will list captured events during a session. For capturing events on Windows systems see Configuration for Capturing Events on Windows Systems.	No	Off

Field	Description	Required?	Default
	NOTE: A DPA is required to capture events. Should you elect to configure event capture, TCP/UDP ports 443 on the TPAM console must be accessible from the DPA.		

Session Authentication tab (PSM ISAs only)

The following table explains the options on this tab. The option selected on the session authentication tab determines the authentication credential storage method.

Table 21: Account Management: PSM Details Session Authentication tab options

Field	Description	Required?	Default
Password Managed by Local TPAM	If selected, the local TPAM manages this account.	No	Yes
Use Remote TPAM CLI	Select this option if the account is managed by another TPAM appliance, and specify the CLI user ID to be used to retrieve the password. This TPAM appliance makes a CLI call to the remote TPAM and pulls the password for the system/account specified and formats the account name at login time using the specified Domain. If the **System** and **Account** box are left blank then the system and account name of the account being configured is used. Access to the public key for the CLI ID is required, and must be supplied to TPAM. When this method of password retrieval is used, the number of approvals specified on the remote TPAM is ignored and access to the password is not limited to a single release.	No	No
Use DSS Key	Select this option if an authentication key is used for the account instead of a password. You have the additional options of using a system standard DSS Key (TPAM allows you to configure up to 3 active keys) or having TPAM generate a pair of keys for you.	No	No
Not Stored - Specify	Select this option if the account's password is not stored or managed by any TPAM. When this option is used the password must be specified when the session	No	No

Field	Description	Required?	Default
password during session	is initiated.		
Use Windows Domain Account	Select this option if the account's password is not stored or managed by any TPAM. The named account is a placeholder for the domain account TPAM uses to authenticate to the system. Through this method you can connect to a system using a domain account instead of a local account. On the **Session Authentication** tab the user name used to log in to the remote session must be added as an account associated with a Windows Active Directory System.	No	No

File Transfer tab (PSM ISAs only)

The following table explains the options on the File Transfer tab.

CAUTION: It is strongly recommended not to edit file transfer settings while a live file transfer is in process for the account.

Table 22: Account Management: PSM Details File Transfer tab options

Field	Description	Required?	Default
File Transfer Method	Select the method used to transfer the files. The options available in this list are platform dependent. NOTE: If using Windows File copy make sure that port 139 or 445 is open on the target system.	No	File Transfer Disabled
File Transfer Share/Path	The share where the files will be uploaded/downloaded.	Yes, if file transfer enabled.	Null
Same as Session Authentication	If selected, the same credentials that are used for the session will be used to transfer the file.	No	Yes
Specify at file transfer time	If selected, the user is prompted to specify the account name and password at the time of file transfer.	No	No

Review Requirements (PSM ISAs only)

The following table explains the options on the Review Requirements tab.

Table 23: Account Management: PSM Details Review Reuquirements tab options

Field	Description	Required?	Default
Reviews Required	Number of reviews required after a session has expired.	No	0
Any Authorized Reviewer (excluding Requestor)	If selected, any auditor, and any user or group member with an access policy of Review Password permission will be eligible to complete the review.	No	Off
Specific User	If selected, the specific user with review permission will be the only user allowed to review sessions for this account. NOTE: If the only eligible reviewer is also the same user that made the request the reviewer settings for the account will be changed to **Any Authorized Reviewer**, and the change will be logged.	No	Off
Any Auditor	If selected, any user with a user type of auditor will be eligible to review sessions for this account.	No	Off
Member of a Group	If selected, any users that are members of the group that is chosen will be eligible to review sessions for this account. Only groups that have review permissions will be available in the list.	No	Off
If the review isn't complete ...	To have a user receive an email notification if the review is not complete within X hours, enter the hours threshold and the email address. The session is not eligible for review until the release duration expires.	No	Null

Add an account

When adding an account in TPAM, information is entered on the following tabs to configure the account:

- Details - Information, Reviews, Custom Information, Management, Ticket System
- Dependents

- Collections
- Permissions
- PSM Details - General, Session Authentication, File Transfer, Review Requirements

The following procedure describes the **required** steps to add an account.

To add a new account:

1. Select **Systems & Accounts | Accounts | Add Account** from the menu.
2. Enter filter criteria on the Filter tab to find the system to add the account to.
3. Click the **System** tab.
4. Select the system or system template.

   NOTE: A total of 20 accounts can be added to a system template (including the functional account). Any accounts added in this way are added to new systems created from the template. Existing systems based on the template will not have any new accounts added or existing accounts removed. ISA users cannot add, view, or edit accounts on template systems.

5. Click the **Details** tab. Enter information on the Details tab. For more information on this tab see Information tab.
6. Click the **Reviews** sub-tab to configure review requirements for password releases. For more information on this tab see the Review Requirements (PSM ISAs only). (Optional)
7. Click the **Custom Information** sub-tab to enter custom information for the account. For more information on this tab see Custom information tab. (Optional)
8. Click the **Management** sub-tab and select preferences for managing account passwords. For more details see Management tab (PPM ISAs only).
9. Click the **Ticket System** sub-tab and set external ticket system requirements for submitting password release requests. For more details see Ticket System tab (PPM ISAs only). (Optional)
10. Click the **PSM Details** tab to enable/disable PSM sessions. For more information see PSM Details tab (PSM ISAs only). (Optional)
11. Click the **Session Authentication** sub-tab to select session authentication method. For more information see Session Authentication tab (PSM ISAs only). (Optional)
12. Click the **File Transfer** sub-tab to enable file transfers during sessions. For more information see File Transfer tab (PSM ISAs only). (Optional)
13. Click the **Review Requirements** sub-tab to set review requirements for sessions. For more information see Review Requirements (PSM ISAs only). (Optional)
14. Click the **Save Changes** button.
15. Click the **Dependents** tab to assign/remove dependents to Windows Active Directory systems. For more details see Dependents tab (Windows AD only). (Optional)

16. Click the **Collections** tab and assign/remove membership. (Optional) For more information on this tab see Collections tab.
17. Click the **Permissions** tab and assign/remove permissions. For more details see Permissions tab. (Optional)
18. Click the **Save Changes** button.

Duplicate an account

To ease the burden of administration and help maintain consistency, accounts can be duplicated. This allows the administrator to create new accounts that are very similar to those that exist, while only having to modify a few details. The new account inherits password management, review, ticket system, and PSM details settings from the existing account. Collections and permissions assignments are not inherited.

NOTE: A PPM only ISA cannot duplicate an account which is PSM enabled.

To duplicate an account:

1. Select **Systems & Accounts | Accounts | Manage Accounts** from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the account to be duplicated.
5. Click the **Duplicate** button. A new account object is created and the Details tab displays.
6. Enter the Account Name.
7. Make any changes to the account configuration on the various tabs. Click the **Collections** tab and assign membership. (Optional)
8. Click the **Permissions** tab and assign access policies. (Optional)
9. Click the **Save Changes** button.

Delete an account

When you delete an account from the Manage Accounts listing it is "soft" deleted. This means that the account information is retained in TPAM for "X" days depending on how the System Administrator has set the **Days in Trash** global setting in the /admin interface.

IMPORTANT: The only way to delete a functional account is to delete the system.

NOTE: You cannot delete an account that has an active PSM session

PSM ISAs can only delete accounts on PSM only systems. PPM ISAs can only delete accounts that are not PSM

enabled.

To "soft" delete an account:

1. Select **Systems & Accounts | Accounts | Manage Accounts** from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the account to be deleted.
5. Click the **Delete** button.
6. Click the **OK** button on the confirmation window.

Retrieve a password

A user with PPM ISA permission over an account can retrieve a password.

To retrieve a password:

1. Select **Retrieve | Retrieve Password** from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the account.
5. Click the **Passwords** tab.
6. Complete the following fields:

Table 24: Password tab fields

Field name	Description
Release Reason	Used to provide a brief description of the reason for the password release. May be optional, required or not allowed, depending on configuration.
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.
Ticket System	May be required, based on configuration.
Ticket	May be required, based on configuration. If the ticket number fails

Field name	Description
Number	validation the ISA will not be able to retrieve the password.
Proxy Release For	If the ISA is retrieving the password on behalf of another user, enter the user's name here. This name will be displayed on the Password Release Activity report.

7. Click the **Password tab**. The password will be displayed for a preconfigured time, after which the ISA must click the password tab again to view the password.

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.

NOTE: You must be both a PPM ISA and PSM ISA to be able to click on the Permissions tab.

To list the accounts:

1. Select **Systems & Accounts | 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 (PSM ISAs only)

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 | 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.

Password current status (PPM ISAs only)

The current status of a password for an account will report last password release, open password requests, scheduled password resets, password checks and reset history.

To check the current status of a password:

1. Select **Systems & Accounts | Accounts | Manage Accounts** from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the account to check.
5. Click the **Current Status** button.

Manual password management (PPM ISAs only)

Accounts that are not auto-managed by PPM may still take advantage of the secure storage and release mechanisms, as well as the logging and reporting functions of TPAM. Password changes for such system accounts can be accomplished in two ways – PPM generated passwords and User generated passwords.

When a non-managed account's password has been released to a user, the defined system contact email address for the system receives a notice when the release duration expires. This provides the opportunity to have the password manually reset. If the request is expired early, the email notification is sent immediately.

To use passwords generated by PPM:

1. Select **Systems & Accounts | Accounts | Manage Accounts** from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the account from the listing.
5. Click the **Details** tab.
6. Select **Manual** for the password management setting. If this was already selected, skip to step 8.
7. Click the **Save Changes** button.
8. Click the **Reset Password** button.
9. Take the new password that PPM has generated, and set it to this on the remote system.
10. If the password update on the remote system was successful, click the **Update Successful** button. If the password was unable to be reset on the remote system, click the **Update Failed** button. PPM will discard the new password and rollback to the previously stored password.

To use password not generated by PPM:

1. Select **Systems & Accounts | Accounts | Manage Accounts** from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the account from the listing.
5. Click the **Details** tab.
6. Select **Manual** for the password management setting. If this was already selected, skip to step 8.
7. Click the **Save Changes** button.
8. Enter the new password in the **Password** and **Confirm** fields.
9. Click the **Save Changes** button.

Password management (PPM ISAs only)

Password Management allows TPAM Administrators and PPM ISA's to do a "mass" forced reset of account passwords that are auto-managed. If manually managed passwords are scheduled for reset, the automatic email notification will be generated to the system contact to manually reset the password.

NOTE: If the account is a synchronized password subscriber, it cannot be reset from this window.

This window also gives you a central location to view the current password status for all passwords.

To perform a mass password reset:

1. Select **Systems & Accounts | Password Management**from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. To select all passwords returned on the Listing tab for reset, select the **All** check box in the column header. To select more than one, but not all, select the check box in the **Select for Scheduling** column for the passwords to be reset.
5. Click the **Schedule Resets** button.

To select one password for reset:

1. Select **Systems & Accounts | Password Management**from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the individual row.
5. Click the **Reset Individual** button.
6. If the account is manually managed, after manually resetting the password on the system, click the **Update Successful** or **Update Failed** button, according to the results.

To view password history:

1. Select **Systems & Accounts | Password Management**from the main menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select an account.
5. Click the **Logs** tab.
6. Enter your search criteria on the Filter tab.
7. Click the **Change Log**, **Test Log**, **Release Log**, **Dependent Change Log**, or **Change Agent Log** to view the specific history.

Managing services in a Windows domain environment (PPM ISAs only)

If the account managed by PPM is a Windows domain account (the system is defined as Active Directory in TPAM), services running on domain member systems using this account can also be managed in terms of password changes.

The prerequisite for domain members systems to have these service account passwords changed is that each system must be configured in TPAM and the domain functional account must be properly privileged on that system (i.e. member of local Administrators group).

NOTE: Dependent systems will always have the passwords for Windows Services and Scheduled Tasks changed regardless if the check boxes are selected on the Account Details Information tab.

Add the domain controller as a managed system:

1. Select **Systems & Accounts | Systems| Add System.**
2. When adding the system on the Information tab make sure that **Enable Automatic Password Management** is selected.
3. On the Connection tab, specify the functional account credentials.
4. Click the **Save Changes** button.

In Active Directory use the Delegation Control wizard to assign the following minimum permissions:

- Object type: User Objects
- Reset Password
- Read and write account restrictions
- Read lockout time
- Write lockout time

Add the managed account on the domain controller system for the Active Directory user specified on the Windows services and tasks:

1. Select **Systems & Accounts | Accounts | Add Account** from the main menu.
2. Filter for the domain controller managed system added in the step above.
3. Click the **Listing** tab.
4. On the Information tab make sure that **Enable Automatic Password Management** is selected.
5. The following check boxes should NOT be selected UNLESS there are services and tasks that need to be managed locally on the domain controller itself:
    - Change password for Windows services started by the account?
    - Automatically restart such services?

- Use this account's current password to change the password?

6. Click the **Save Changes** button.
7. The options only apply to the local system to which the managed account belongs. If you wish to manage services and tasks on other systems, click the **Dependents** tab.
8. Enter your search criteria on the Filter tab.
9. Click the **Results** tab.
10. Select the **Dependent** button for systems for which you would like the Windows services and tasks to be updated.
11. Click the **Save Changes** button.

A managed system must exist in TPAM for each system where you have Windows services and/or Scheduled Tasks for which the credentials need to be updated. Ensure that Password Management is enabled on each of these systems in TPAM, so that Functional Account credentials can be specified on the Connection tab. This system must then be set as a Dependent on the AD Account as specified in the step above.

The Functional Account must have the following local permissions on system(s) running the Services and Tasks.

- Member of the local Administrators group OR
- Members of the local Backup Operators group and granted the "Log on as a batch job" local policy.

To verify the configuration:

1. Go to the managed account configured on the domain controller that was added above.
2. Perform a forced reset by clicking the **Reset Password** button.

If everything is configured properly and the correct permissions are assigned, the password will be reset and any Dependent systems will also be updated. If you receive any errors about password reset failures or access denied, you will need to verify the permissions assigned above.

Add generic account to TPAM for PSM sessions to a user specified Windows account (PSM ISAs only)

TPAM provides the ability to create a generic TPAM account that can be used to log in to any user-specified Windows account during a PSM session. The user is prompted to input the desired Windows account name and password when the PSM session is starting. This allows TPAM to provide the account name and password during RDP session initiation, thereby allowing the RDP session to succeed even when the RDP session security layer is set to SSL/TLS on the Windows machine.

To configure a generic TPAM account:

1. The target system must be added to TPAM. The platform for the system can be any of the Windows or SPCW platforms. For details on how to add a system see Add a system.
2. Select **Systems & Accounts | Accounts | Add Account** from the menu.
3. Enter filter criteria on the Filter tab to find the system to add the account to.
4. Click the **System** tab.
5. Select the system in the listing.
6. Click the **Details** tab.
7. Enter **:prompt:** for the account name.
8. Select **None** for the Password Management option.
9. Click the **PSM Details** tab.
10. Select the **Enable PSM Sessions** check box.
11. Select **RDP- Interactive Login** as the Proxy Connection Type.
12. Click the **Session Authentication** tab. Select **Not Stored - Specify password during session**.
13. Click the **Permissions** tab. Assign permissions to this account. For details see Permissions tab. Assign Requestor permissions to the appropriate TPAM users.

How it works

A TPAM user requests a session using the :prompt: account on the target system. When the PSM session is initiated, the user is prompted to enter the Windows account name and password.

After the account name and password are entered, the RDP session is connected as desired.

NOTE: It is not possible to monitor events in this scenario.

NOTE:If performing file transfer, credentials must be specified at file transfer time.

Files (PPM ISAs only)

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.

To add and manage files, information is entered on the following tabs in the TPAM interface:

Table 25: Files Management: TPAM interface tabs

Tab name	Description
Details	Define main file information, such as name, approvals required, contact.
Ticket System	Configure Ticket System Validation for requests on this file.
Collections	Assign a file to a collection/s.
Permissions	Assign users and groups permissions on this file.

Details tab

The Details tab is where you upload the file to TPAM and set approval requirements.

The table below explains all of the options available on the File Details tab.

Table 26: Files Management: Details tab options

Field	Description	Required?	Default
File Display	The name users see when requesting access to stored files.	Yes	

Field	Description	Required?	Default
Name			
Filesize (in bytes)	Display only. The size of the file that is uploaded.		
Select Local Filename	Where the file is uploaded by clicking the browse button.	Yes	
Approvals Required	The default value of 1, indicates that a single approval allows the requestor to access the file. A value greater than 1 requires multiple approvers to approve each request. A value of 0 means any requests will be auto-approved by TPAM. If overridden by an access policy the greater of the two values will be used.	No	1
Maximum Duration	This is the *maximum* duration for a file release. If this is overridden by an Access Policy assignment, the *lower* of the two durations is used. The default duration that the requestor sees for any new file request is *2 hours*, or the maximum duration, whichever is less.	Yes	7 Days
Require Multi-Group Approval from	Can only be selected if Approvals Required is greater than 1. If selected, you can require that approvals for requests come from two or more groups. At least 1 approval must come from each group. Select the check box in the **Sel** column to select the groups. NOTE: Any user with approver permissions will be able to approve the request, but unless the user is a member of one of the selected groups, their approval will not count. NOTE: Any authorized approver can approve or deny the request at any time.	No	Off
Multi-Group Approver Order	The number entered in the **Ord** column determines the order that the request must be approved. Once the first group approves the request then the email notification to the second group to approve will go out and so on. The number entered in the **#** column represents how many approvers from that group must approve the request.	No	Off
Notification Email	The email address specified in this box receives notification of certain file releases. This would apply	No	Null

Field	Description	Required?	Default
	to releases by ISA users, CLI/API users under all circumstances, and requests when no approvals are required. Multiple email addresses can be specified by entering each email address separated by a comma, up to a maximum of 255 characters. Any time a change is made to the notification email address box, an email is automatically sent to the old email address with a notification that this change has occurred.		
Description	The description box may be used to provide additional information about the file, special notes, business owner, etc.	No	

Ticket System tab

The Ticket System tab is used to configure third party ticket system requirements when submitting file release requests for this file. The Ticket System tab is only enabled if the TPAM System Administrator has configured ticket system/s in the /admin interface.

The following table explains the options on this tab.

Table 27: Files Management: Ticket System tab options

Field	Description	Required?	Default
Require Ticket Number from	Select this check box to require ticket number validation every time a file request is submitted. If multiple Ticket Systems are enabled they are listed in the list for selection. You can specify the ticket system or allow entry of a ticket number from any system that is enabled. If this check box is not selected, users can still enter a Ticket Number on a request, but it is not required.	No	From System
Perform Ticket Validation for	If ticket validation is required, then all requestors are required to provide a ticket number. You also have the option to require ISAs to supply a ticket number prior to retrieving a file.	No	From System
Send Email notification to	If any of the ISA, CLI or API required check boxes are left clear you have the option of entering one or more email addresses (up to 255 characters) that will receive an email when an ISA, CLI or API user releases or retrieves a file without supplying a ticket.	No	From System

Field	Description	Required?	Default
Pull defaults from system	If selected, when the **Save Changes** button is clicked, it will pull these settings from the system. The propagation is a one time update each time this check box is selected and the **Save Changes** button is clicked. After that there is no forcing of the settings to remain in synch. The settings on the file can be overridden.	No	Off

Logs tab

The Logs tab for stored files shows the activity associated with accessing the file.

The following table explains the fields on this tab.

Table 28: Files Management: Logs tab options

Field	Description
Request ID	Request ID for the file request.
User Name	User ID of the requestor.
User Full Name	Full name of the requestor.
Release Date	Date and time that the file was retrieved.
Release Type	Indicates of the file was retrieved by a requestor or an ISA.

File History tab

This tab shows the history of all physical files that have been associated with the file display name as well as the dates the file was originally stored and replaced. The older files, though no longer associated with the display name, remain on the appliance and may be accessed by and administrator using the filename link. Older files may also be deleted from history.

The following table explains the fields on this tab.

Table 29: Files Management: File History tab options

Field	Description
Actual Filename	The name of the file that was stored on TPAM.

Field	Description
Stored Date	The date the file was uploaded to TPAM.
Replaced Date	The date the file was replaced with another file.
Filesize	Size of the file in bytes.

Current File tab

The Current File tab allows you to retrieve the file if you have ISA permission for the file.

The following table explains the options on this tab.

Table 30: Files Management: Current File tab options

Field	Description	Required?
Release Reason	The reason for the file release.	Depends on configuration by System Administrator
Reason Code	The reason for the file release.	Depends on configuration by System Administrator
Ticket System	Ticket system to validate the request against.	Depends on configuration by Administrator.
Ticket Number	Ticket number to validate the request against.	Depends on configuration by Administrator.

Collections tab

A collection is a group of systems, accounts and or files. The Collections tab is used to assign the file to a collection/s. Files can belong to more than one collection. The collections list shows all collections that have been defined in the TPAM appliance if the user modifying the file is an administrator. If the user modifying the file is an ISA, only the collections that the user holds the ISA role for are displayed. By assigning the file to collections, the file automatically inherits user and group permissions that have been assigned at the collection level.

NOTE: A file cannot belong to the same collection as its parent system, or vice versa.

Use the **Filter** tab to enter search criteria for the collections to assign/un-assign. Click the **Results** tab.

The table below explains the fields on the Results tab.

Table 31: Files Management: Collections Results tab options

Field	Description	Required?	Default
Type	On this tab type will always say **Collection**.		
Name	The name of the collection. Clicking on the name will take you the collection management listing tab.	No	
Membership Status	To modify collection membership, simply click the **Not Assigned** or **Assigned** buttons next to each collection name and click the **Save Changes** button. You can set all members to either Assigned or Not Assigned by holding down the Ctrl key when clicking on any button.	No	Not Assigned

Permissions tab

The Permissions tab is used to assign users and/or groups an Access Policy for this file.

To assign Access Policies:

1. Use the table on the left of the page to select the name/s of the user/s and/or group/s to which the selected access policy is to be assigned.
2. Select an Access Policy from the **Access Policy** list in the Access Policy Details pane, located in the right upper side of the Results tab. When you select an Access Policy on the list the detailed permissions describing this Access Policy are displayed on the rows below.
3. Select one of the icons in the Access Policy Details pane (right upper side of page) to make the assignment.

Table 32: Access Policy Details pane icons

Icon	Action
	Refreshes list of available Access Policies.
	Scrolls the currently selected User or Group into view.
	Applies the currently selected policy to the current row. Assigning a policy of "Not Assigned" removes the current assignment.This affects only the current row (row with the dotted border) even if multiple rows are selected.
	Applies the currently selected policy to all selected rows in the list. You are asked to confirm the assignment if more than 10 rows are affected.

Icon	Action
	Removes the currently selected policy from all selected rows in the list. If a row is not currently set to the selected policy it will not be changed. You are asked to confirm the assignment if more than 10 rows are affected.
	Removes unsaved edits on the current row. This only affects the current row (row with the dotted border) even if multiple rows are selected.
	Removes unsaved edits on all currently selected rows.

This icon () next to any row on the list simply means that row has been edited since the last save changes occurred.

You can "Shift+Click" to select a range of rows. The first row you click will be surrounded by purple dashed lines. The next row that you "Shift-Click" on will cause all the rows in between the original row and current row to be highlighted.

4. When you are finished assigning/un-assigning Access Policies, click the **Save Changes** button.

   TIP: You may re-filter and re-retrieve the results list without losing existing edits. As the **Results** tab is reloaded any Groups or Users that you have already edited reflect their edited policy assignment. When you click the **Save Changes** button all the Access Policy assignment changes for the file are saved. The appliance saves these in batches, informing you of the number of assignments added, removed, or changed for each batch.

   NOTE: You must be both a PPM **and** PSM ISA over an account to be allowed to assign an Access Policy.

Using Ctrl-Click or Shift-Click on the hyperlink in the Name column will open the details page for this entity in a new tab or window.

Add a file

When adding a file in TPAM, information is entered on the following tabs to configure the file:

- Details - File name, Approvals required
- Ticket System
- Collections
- Permissions

The following procedure describes the **required** steps to add a file.

NOTE: To add a file to a system the ISA must have ISA File permissions on that system.

To add a new file:

1. Select **Systems & Accounts | Files | Add File** from the menu.
2. Enter filter criteria on the Filter tab to find the system to add the file to.
3. Click the **System** tab.
4. Select the system.
5. Click the **Details** tab. Enter information on the Details tab. For more information on this tab see Details tab.
6. Click the **Ticket System** tab and set external ticket system requirements for submitting file release requests. For more details see Ticket System tab. (Optional)
7. Click the **Save Changes** button.
8. Click the **Collections** tab and assign/remove membership. (Optional) For more information on this tab see Collections tab.
9. Click the **Permissions** tab and assign/remove permissions. For more details see Permissions tab. (Optional)
10. Click the **Save Changes** button.

Duplicate a file

To ease the burden of administration and help maintain consistency, files can be duplicated. This allows the administrator to create new files that are very similar to those that exist, while only having to modify a few details. The new file inherits approval requirements, ticket system settings, collection and permission assignments from the existing file.

To duplicate a file:

1. Select **Systems & Accounts | Files | Manage Files** from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the file to be duplicated.
5. Click the **Duplicate** button. A new file object is created and the Details tab displays.
6. Enter the file name.
7. Upload the file.
8. Make any other additional changes on the Details and Ticket System tabs. (Optional)
9. Click the **Save Changes** button.
10. Click the **Collections** tab and assign membership. (Optional)
11. Click the **Permissions** tab and assign access policies. (Optional)
12. Click the **Save Changes** button.

Review file history

To view file history:

1. Select **Systems & Accounts | Files | Manage Files** from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the file.
5. Click the **File History** tab. For more information see File History tab.

Delete a file

To delete a file:

1. Select **Systems & Accounts | Files | Manage Files** from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the file to be deleted.
5. Click the **Delete** button.
6. Click the **OK** button on the confirmation window.

Retrieve a file

A user with ISA permission over a file can retrieve it.

To retrieve a file:

1. Select **Retrieve | Retrieve File** from the menu.
2. Select the file to retrieve from the Listing tab.
3. Click the **Current File** tab.

4. Complete the following fields:

Table 33: Current File tab fields

Field name	Description
Release Reason	Used to provide a brief description of the reason for the password release. May be optional, required or not allowed, depending on configuration.
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.
Ticket System	May be required, based on configuration.
Ticket Number	May be required, based on configuration. If the ticket number fails validation the ISA will not be able to retrieve the file.

5. Click the **Retrieve File** button.

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 | 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.

Rebuild assigned policies

If the "Always use cached permission data" global setting is set to **Yes** or **Not for Password/File Retrieval and Session Start**, then it is recommended that Administrators and ISAs use the rebuild assigned policy page to update the cached permissions to the latest changes they have made. These changes include:

- Editing any permission assignment
- Adding/deleting systems, accounts, files, users, groups, or collections
- Changing the Ignore System Policies check box on the account
- Changing the user type (Administrator, Basic, Auditor, User Admin)
- Changing collection membership
- Changing the Global Groups setting in Global Settings

The Rebuild Assigned Policies page shows how much data is in the cache, when it was last updated, and the current state of the background job. An Administrator or a user with both PPM and PPM ISA permissions may use the **Run Now** button to run the job immediately if there are pending changes. This job will automatically run in the background every 60 seconds as needed to update changes.

To rebuild the assigned policies:

1. Select **Management | Rebuild Assigned Policies** from the menu.
2. Click the **Run Now** button to update TPAM with the latest changes.

The **Refresh Data** button can be clicked to see if there are any new changes in the queue that need to be processed.

Rebuild Assigned Policies

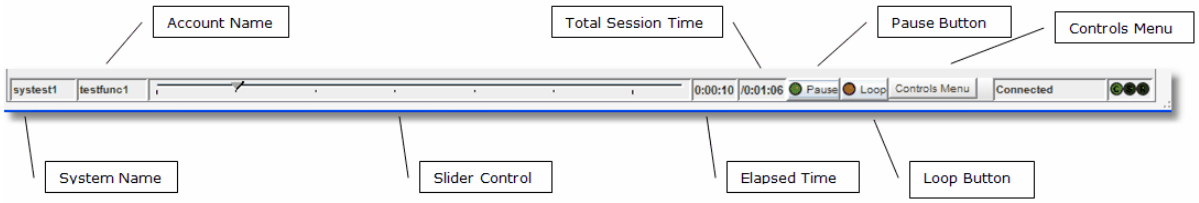
Session Management (PSM ISAs only)

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 34: 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

Option	Description
	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 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

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, 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 **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. 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.

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.

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 **Management | Session Mgmt | Manage Sessions** from the main menu.
2. Select the session to monitor. Live sessions will have a status of **Connected**.
3. Click the **Monitor Session** button. The PSM Session Monitor window will open with a view of the live session.

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.

   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 in TPAM.

Table 35: 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.
Requestor User Activity	Detailed records of all activities performed by users with Requestor permissions.
PSM Accounts	Accounts that are PSM enabled.

Report title	Description
Inventory (PSM Customers only)	
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.
Password Update Activity	Password modifications to systems managed by Privileged Password Manager.
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.

Report title	Description
	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 Releases	Password releases that did not require dual control approval.
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	Details on file releases, such as request reason, retrieval date and

Report title	Description
Activity	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.

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