The Privileged Appliance and Modules 2.5.923

User Administrator 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.

Contents

1

Permission Based Home Page

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.

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

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

2

User ID’s

Introduction

This chapter covers, adding and managing TPAM User ID’s.

To add and manage user ID’s, information is entered on the following tabs in the TPAM interface:

Table 2: Management: TPAM interface tabs

Tab name	Description
Details	Define main information, such as name, contact information, and user type.
Details/Web	Configure access and authentication methods.
Details/Key Based	Define key based authentication method.
Details/Time	Define time zone and access times.
Detail/PSM Connection Defaults	Default PSM connection options when recording a session.
Details/Custom Information	Custom boxes available for use.

Details tab

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

Table 3: User Management: Details tab options

Element	Description	Required?	Default
User Name	The user’s login id. User names may be a maximum of 30 characters long. The following	Yes	

Element	Description	Required?	Default
	special characters are allowed in the user name: `~#%&(){}.!'		
User Disabled?	If selected, the user cannot access TPAM.	No	Off
Last Name	Last name of the user.	Yes	
First Name	First name of the user.	Yes	
Phone Number	Phone number associated with the user ID in TPAM.	No	
Mobile Number	Mobile number associated with the user ID in TPAM. For mobile numbers outside North America the number ***must*** begin with the country calling code in the format of +##<space> ex. +44 1234 123456 for a phone number in the United Kingdom.	No	
Allow Approval Anywhere notifications	This will only display if TPAM has been joined to Starling. If selected, user will receive push notifications to their mobile phone for approvals in addition to the emails they already receive. User type must be Basic, Administrator, or Partition Administrator.	No	Off
Test Notification	Clicking this will send a test message to the approval anywhere user. (The user must be saved first) Results of the test are logged in the Activity report. If not already, the user will be provisioned in Starling.	N/A	
Email Address	The email address that TPAM will use for email notifications from TPAM. If multiple email addresses are to be associated with the user, this may be accomplished by using a semicolon and no spaces to separate them. An alias name can also be designated for the email (this name is displayed in the To: box). Example: John Doe<johndoe@work.com;johnd@home.net>,… To create an alias, type it as: *alias<email-address-1;email-address-2>* Double quotes may be required to include spaces in email addresses.	No	
Description	The description box may be used to provide additional details about the user.	No	

Element	Description	Required?	Default
User Type	Select the user type. Available choices are: • **Basic**: If selected, the user can be a requestor, approver, reviewer, privileged access, denied or ISA but does not have any administrator privileges.	Yes	Basic

Web tab

The table below explains all of the box options available on the Web tab:

Table 4: User Management: Details Web tab options

Field	Description	Required?	Default
Allow this user to access TPAM from a Mobile Device?	If selected, users can make requests, deny or approve requests, and review password releases and sessions by using their personal mobile device (Blackberry, iPhone). User administrators and cache user types may not access TPAM via a mobile device.	No	Off
Allow WEB Access?	If selected, the user can access TPAM via the web. NOTE: Allowing web access is permanent once saved. The only way to remove web access for the user id is to delete the user and add the user back.	No	On
Password/ Confirm Password	Enter/confirm a password for the user account.If left blank, a random password is generated by the TPAM system. The TPAM default password rule configured by the System Administrator is used for these passwords.	No	
Certificate Thumbprint	For users who authenticate using a client certificate with a thumbprint, the certificate's SHA1 or SHA2	No	

Field	Description	Required?	Default
	thumbprint should be entered here. This option will not appear unless certificate is selected as the primary user authentication type.		
Principal Name	For users who authenticate using a certificate and the value of the subjectALTName:PrincipalName attribute contained in the certificate.	No	
Primary User Authentication	If selected, user can use primary authentication to authenticate. The primary authentication user ID cannot be the same as any other user's TPAM user name or primary authentication ID. Available choices are: • **Certificate** - User's authenticate using a client certificate. Based on global settings the user will be linked to the certificate through the thumbprint or the value of the subjectAltName:PrincipalName attribute in the certificate. • **Local -** TPAM • **Windows Active Directory-** WinAD is configured in the admin interface as an external source of authentication. The Windows AD primary user ID must always be in (user principle name) format, allowing the use of multiple domains. The primary authentication ID cannot be the same as any other user's User Name or primary ID. • **LDAP** - LDAP is configured in the admin interface as an external source of authentication. Users can type a shortened version of their LDAP user ID that expands to the full LDAP user ID for	Yes	Local

Field	Description	Required?	Default
	authentication. • **Radius** - Radius is configured in the admin interface as an external source of authentication. • **Defender** - Defender is configured in the admin interface as an external source of authentication • **Starling Two-Factor Radius Agent** - Starling Radius Agent is configured in the admin interface as an external source of authentication.		
Secondary User Authentication	If the user is using secondary authentication select the type, source and enter their user ID here. Choices of secondary authentication are: • None • Safeword • SecurID • LDAP • Radius • WinAD • Defender • Starling Two-Factor Radius Agent	No	None

Key based tab

The table below explains all of the box options available on the Key Based tab:

Table 5: User Management: Details Key Based tab options

Field	Description	Required?	Default
CLI	If selected, the user can access TPAM via the command line interface (CLI).	No	Off

Field	Description	Required?	Default
API	If selected the user can access TPAM via the API.	No	Off
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. Remember to give the pass phrase to the CLI user along with their private key file. NOTE: If the CLI user ID and key are going to be used in any type of scripting or automation, be aware that any time a CLI key with a passphrase is used the passphrase **must** be typed by the user via the keyboard. Passphrase entry via any type of scripting is not allowed for DSS Keys.	No	
Restricted IP Address	Only applies to CLI/API users. If an address is specified, the user may only access TPAM from this address. More than one IP address may be specified by separating each with a comma – up to a limit of 200 characters for the entire string. The use of wildcards is also permitted to specify a complete network segment – i.e. 10.14.10.* Since a CLI/API user cannot be disabled with a check box, this box can be used to temporarily disable the user access by setting the value to an invalid IP address such as “disabled”.	No	

Time tab

The Time tab allows administrators and user administrators to set a user's local time zone. This tab is not enabled for Cache, CLI and API users.

NOTE: The TPAM server is always at UTC time and never uses daylight savings time.

The table below explains all of the box options available on the User ID Time tab:

Table 6: User Management: Details Time tab options

Field	Description	Required?	Default
User Timezone	Select a local time zone for the user. NOTE: If the user is in a time zone that follows DST, TPAM will automatically adjust the time for them.	Yes	Will default to the default user timezone global setting value.
Time Based System Access	Choices are: • No Restriction - if selected, the user can access TPAM at any time/day. • Allow - To limit a user's access to TPAM, select the **Allow** button, select days of the week and enter up to 4 time ranges. Multiple ranges must be separated by semi-colons. The ranges must be entered using 24-hour times with a hyphen between start and end times. • Prohibit - To restrict a user's access to TPAM, select the **Prohibit** button, select days of the week and enter up to 4 time ranges. The ranges must be entered using 24-hour times with a hyphen between start and end times.	Yes	No Restrictions

PSM connection defaults

Lists all possible PSM connection options and their values. Connection options and values are proxy specific. The selected values will be used as defaults the first time a user starts a PSM session to any given account. Once the user has started the session, the default values for that user are saved and will be the defaults the next time the user connects to that account. These user connection defaults are cleared any time the proxy type for the account is changed.

These defaults only apply to session recordings and not session playback or monitoring.

Custom information tab

There are six custom boxes that can be used to track information about each user. These custom boxes are enabled and configured by the System Administrator in the /admin interface. If these boxes have not been enabled the Custom Information tab will not be visible.

Add a web user ID

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

- Details
- Details/Web
- Details/Key Based
- Details/Time
- Details/PSM Connection Defaults
- Details/Custom

The following procedure describes the steps to add a user ID.

NOTE: User Administrators can only create non-partitioned users.

NOTE: User Administrators cannot assign Groups or Permissions to user IDs.

To add a new web user ID:

1. Select **UserIDs | Add UserID** from the menu.
2. Enter information on the **Details** tab. For more information on this tab see Details tab.
3. Enter information on the **Web** tab. For more information on this tab see Web tab.
4. To set time zone and access rules, click the **Time** tab and make changes. For more details see Time tab. (Optional)
5. To enter PSM connection defaults, click the **PSM Connection Defaults** tab.
6. To enter custom information, click the **Custom Information** tab.
7. Click the **Save Changes** button.

Add a user ID using a template

Users added using a template will automatically inherit the time information, group membership and permissions from the template used.As a User Administrator you will not be able to see the groups and

permissions associated with this template.

To add a user using a template:

1. Select **UserIDs | Add UserID** 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 user name, first name, last name, and other contact information.
6. Make any other changes as desired.
7. Click the **Save Changes** button.

NOTE: If the Administrator has set a default template, every time a user is added it will use this template.

Add a CLI user ID

A CLI user ID is a special user account used to access TPAM remotely via the CLI (command line interface). It possible for one user ID to be both a web and CLI user. When accessing TPAM through the CLI they can only execute specific commands supported by the TPAM CLI.

NOTE: The paradmin user ID cannot be given CLI access.

To add a new CLI user ID:

1. Select **UserIDs | Add UserID** from the menu.
2. Enter information on the **Details** tab. For more information on this tab see .
3. Enter information on the **Web** tab. For more information on this tab see Web tab.
4. Click the **Key Based** tab. Select the **CLI** check box. Enter information on the Key Based tab. For more information see Key based tab.
5. To enter custom information, click the **Custom Information** tab. For more details see Custom information tab. (Optional)
6. Click the **Save Changes** button.

IMPORTANT: If a user ID has both web and API or CLI access to TPAM you will not be able to download or generate keys for that user ID. They must log on to TPAM to download and/or regenerate their own DSS key.

Add an API user ID

An API user ID is required to use TPAM's Application Programming Interface (API). The TPAM API allows client applications, via an SSH (Secure Shell) connection to the TPAM appliance, to perform many of the operations provided in the TPAM User Interface.

To add an API user ID:

1. Select **UserIDs | Add UserID** from the menu.
2. Enter information on the **Details** tab. For more information on this tab see Details tab.
3. Enter information on the **Web** tab. For more information on this tab see Web tab.
4. Click the **Key Based** tab. Select the **API** check box. Enter information on the Key Based tab. For more information see Key based tab.
5. To enter custom information, click the **Custom Information** tab. For more details see Custom information tab. (Optional)
6. Click the **Save Changes** button.

TIP: If you are adding a user ID that has both Web access and CLI or API access, to generate keys they must first log in to TPAM and go to the User menu to generate and download their keys.

Delete a user ID

A user ID cannot be deleted if the user ID :

- has pending batch import or update processes running
- has an active PSM session
- is being used as a template for importing LDAP or Generic auto-discovery mappings
- is required to complete a review on a password release or PSM session.

Even if a user ID is deleted, any session logs, requests, reviews, etc. associated with that ID will remain in TPAM until the retention settings age the data out of TPAM.

To delete a user ID:

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

Disable/enable a user ID

To disable/enable a user ID:

1. Select **UserIDs | Manage UserIDs** from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the user ID to be changed.
5. Click the **Details** tab.
6. Select/Clear the **User Disabled?** box.
7. Click the **Save Changes** button.

Unlock a user ID

A user may need to be unlocked if they enter an incorrect password multiple times.

To unlock a user:

1. Select **UserIDs | Manage UserIDs** from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the user ID to be unlocked.
5. Click the **Unlock** button.

Reset user ID password

To reset a user's password:

1. Select **UserIDs | Manage UserIDs** from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the user ID to be reset.
5. Click the **Details** tab.
6. Enter the new password in the Password and Confirm boxes.
7. Click the **Save Changes** button.
8. Notify the user of their new password.

This creates a one time use password that the user will be forced to change upon logging on.

NOTE: You cannot change passwords for users with external primary authentication. If Primary Authentication has been minimilized then you cannot change the user's local password.

About us

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

Contacting us

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

Technical support resources

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

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

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