Copyright 2020 One Identity LLC.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser’s personal use without the written permission of One Identity LLC.

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

If you have any questions regarding your potential use of this material, contact:
One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents
One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

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

Legend

⚠️ WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

⚠️ CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

ℹ️ IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.
## Contents

**Before You Begin** ........................................................................................................... 11
Introduction .................................................................................................................. 11
Information to gather ...................................................................................................... 11

**Initial Set Up** ............................................................................................................. 14
Introduction .................................................................................................................. 14
Recommended steps ...................................................................................................... 14

**Start Up** ..................................................................................................................... 16
Introduction .................................................................................................................. 16
Power on the TPAM appliance ....................................................................................... 16

**Network Settings** .................................................................................................... 18
Introduction .................................................................................................................. 18
Configure the network settings .................................................................................... 18
Configure DNS settings ............................................................................................... 18
View running values ..................................................................................................... 19
Flush DNS ..................................................................................................................... 19
DNS suffix search ......................................................................................................... 19
Host file mapping .......................................................................................................... 20

**Sys-Admin User ID’s** ................................................................................................ 21
Introduction .................................................................................................................. 21
Details tab ...................................................................................................................... 21
Web tab .......................................................................................................................... 22
Key based tab ............................................................................................................... 24
Time tab ........................................................................................................................ 25
Custom information tab ............................................................................................... 26
Add a web sys-admin user ID ....................................................................................... 26
Add a CLI sys-admin user ............................................................................................. 27
Regenerate keys for CLI users ...................................................................................... 28
Delete a sys-admin user ID .......................................................................................... 28
Disable/Enable a sys-admin user ID ............................................................................ 29
Unlock a sys-admin user ID ........................................................................................ 29
Reset sys-admin user ID password ................................................................. 29
Manage your TPAM sys-admin user ID .......................................................... 30
Promote a user ID ......................................................................................... 31
Demote a user ID ......................................................................................... 31
Manage the parmaster user ID ...................................................................... 32
Active logins .................................................................................................. 33

**Distributed Processing Appliances (DPAs)** .................................................. 34
Introduction ..................................................................................................... 34
Power on the DPA appliance ......................................................................... 35
Configure network settings ........................................................................... 35
Enable remote access .................................................................................... 36
Changing the setup password while logged into the DPA ......................... 37
Using TPAM to manage the DPA dpasetup account ..................................... 37
Define remote IP address restrictions ......................................................... 38
Prepare the DPA for enrollment .................................................................. 38
Logs menu ...................................................................................................... 38
Increase DPA license count .......................................................................... 38
Enroll DPA in cluster .................................................................................... 39
Manage DPA settings ................................................................................... 40
DPA log tab .................................................................................................... 41
Remove DPA from a cluster ......................................................................... 41
Re-enroll a DPA ............................................................................................. 41
Change DPA SSH port .................................................................................. 42
Manage host file entries ............................................................................... 43
DPA configuration using both network cards on a segmented network .......... 43
Net tools ......................................................................................................... 46
DPAs and failover ......................................................................................... 46
Test DPA ......................................................................................................... 47
DPA version number ..................................................................................... 47

**High Availability Cluster** ............................................................................ 48
Introduction ..................................................................................................... 48
Details tab ....................................................................................................... 48
Member status tab .......................................................................................... 50
Snapshots tab ................................................................................................. 51
Sybase trusted root certificates ......................................................... 130
MySQL trusted root certificates ....................................................... 130
Upload a certificate on a replica ....................................................... 131

**Automation Engine** ................................................................. 132
Introduction .................................................................................... 132
Agent status tab ............................................................................ 132
Start/Stop the auto management engine .......................................... 133
Disable/Enable an agent ................................................................. 133
Auto Management settings tab ...................................................... 134
Check password queue schedule .................................................. 134
Manually load the check password queue ....................................... 135
Agent logs ..................................................................................... 135

**Agents** ...................................................................................... 137
Introduction .................................................................................... 137
Daily Maintenance agent ............................................................... 137
Auto Discovery agent .................................................................. 137
Post-Session Processing agent ...................................................... 138
SSH daemon ................................................................................ 139

**Backups** .................................................................................. 140
Introduction .................................................................................... 140
Backup settings tab ...................................................................... 140
Configure the backup schedule ..................................................... 141
On demand backup ..................................................................... 141
View backup log .......................................................................... 142
View backup history ................................................................... 142
Download an online backup ......................................................... 142
Delete a backup .......................................................................... 143

**Alerts** ...................................................................................... 144
Introduction .................................................................................... 144
Add an alert receiver ................................................................... 144
Delete an alert receiver ................................................................ 145
Alert thresholds .......................................................................... 145
Alert details export ..................................................................... 145
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Authentication</td>
<td>147</td>
</tr>
<tr>
<td>Introduction</td>
<td>147</td>
</tr>
<tr>
<td>Certificate based authentication</td>
<td>147</td>
</tr>
<tr>
<td>SafeWord</td>
<td>147</td>
</tr>
<tr>
<td>RSA SecureID</td>
<td>148</td>
</tr>
<tr>
<td>LDAP</td>
<td>149</td>
</tr>
<tr>
<td>Windows Active Directory</td>
<td>150</td>
</tr>
<tr>
<td>RADIUS</td>
<td>150</td>
</tr>
<tr>
<td>Defender</td>
<td>151</td>
</tr>
<tr>
<td>Starling Two-Factor Radius Agent</td>
<td>151</td>
</tr>
<tr>
<td>Starling Join</td>
<td>153</td>
</tr>
<tr>
<td>Introduction</td>
<td>153</td>
</tr>
<tr>
<td>Configure Starling Join</td>
<td>153</td>
</tr>
<tr>
<td>Configure Starling monitor</td>
<td>154</td>
</tr>
<tr>
<td>Ticket Systems</td>
<td>156</td>
</tr>
<tr>
<td>Introduction</td>
<td>156</td>
</tr>
<tr>
<td>Details tab</td>
<td>157</td>
</tr>
<tr>
<td>Data tab</td>
<td>161</td>
</tr>
<tr>
<td>Special note regarding MySQL data sources</td>
<td>161</td>
</tr>
<tr>
<td>Web services</td>
<td>163</td>
</tr>
<tr>
<td>Rules listing tab</td>
<td>164</td>
</tr>
<tr>
<td>Rule details tab</td>
<td>164</td>
</tr>
<tr>
<td>Add a ticket system</td>
<td>164</td>
</tr>
<tr>
<td>Add a ticket system rule</td>
<td>166</td>
</tr>
<tr>
<td>Duplicate a ticket system rule</td>
<td>167</td>
</tr>
<tr>
<td>Delete a ticket system rule</td>
<td>167</td>
</tr>
<tr>
<td>Duplicate a ticket system</td>
<td>168</td>
</tr>
<tr>
<td>Delete a ticket system</td>
<td>168</td>
</tr>
<tr>
<td>Custom Logo</td>
<td>169</td>
</tr>
<tr>
<td>Introduction</td>
<td>169</td>
</tr>
<tr>
<td>File requirements</td>
<td>169</td>
</tr>
<tr>
<td>Upload custom logo</td>
<td>169</td>
</tr>
<tr>
<td>Remove custom logo</td>
<td>170</td>
</tr>
<tr>
<td>License Management</td>
<td>171</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Introduction</td>
<td>171</td>
</tr>
<tr>
<td>Adjust license limits</td>
<td>172</td>
</tr>
<tr>
<td>License management change log</td>
<td>172</td>
</tr>
<tr>
<td><strong>Login Banner and Message of the Day</strong></td>
<td>173</td>
</tr>
<tr>
<td>Introduction</td>
<td>173</td>
</tr>
<tr>
<td>Login banner</td>
<td>173</td>
</tr>
<tr>
<td>Message of the day</td>
<td>173</td>
</tr>
<tr>
<td><strong>Net Tools</strong></td>
<td>175</td>
</tr>
<tr>
<td>Introduction</td>
<td>175</td>
</tr>
<tr>
<td>The ping utility</td>
<td>175</td>
</tr>
<tr>
<td>Nslookup utility</td>
<td>175</td>
</tr>
<tr>
<td>TraceRoute utility</td>
<td>176</td>
</tr>
<tr>
<td>Telnet test utility</td>
<td>176</td>
</tr>
<tr>
<td>Route table management</td>
<td>176</td>
</tr>
<tr>
<td><strong>System, O/S Patch, and Job Status Pages</strong></td>
<td>178</td>
</tr>
<tr>
<td>Introduction</td>
<td>178</td>
</tr>
<tr>
<td>O/S patch status</td>
<td>178</td>
</tr>
<tr>
<td>System status page</td>
<td>178</td>
</tr>
<tr>
<td>System status graphs</td>
<td>179</td>
</tr>
<tr>
<td>How to create a support bundle</td>
<td>181</td>
</tr>
<tr>
<td>Job status page</td>
<td>181</td>
</tr>
<tr>
<td><strong>Software Updates</strong></td>
<td>182</td>
</tr>
<tr>
<td>Introduction</td>
<td>182</td>
</tr>
<tr>
<td>Types of software updates</td>
<td>182</td>
</tr>
<tr>
<td>Check TPAM current version</td>
<td>183</td>
</tr>
<tr>
<td>Download a software update from the customer portal</td>
<td>183</td>
</tr>
<tr>
<td>Apply a software update</td>
<td>183</td>
</tr>
<tr>
<td>View patch log</td>
<td>184</td>
</tr>
<tr>
<td>View patch history</td>
<td>185</td>
</tr>
<tr>
<td><strong>Shut Down/R Restart the Appliance</strong></td>
<td>186</td>
</tr>
<tr>
<td>Introduction</td>
<td>186</td>
</tr>
<tr>
<td>Shutdown appliance</td>
<td>186</td>
</tr>
<tr>
<td>Restart appliance</td>
<td>186</td>
</tr>
</tbody>
</table>
Before You Begin

Introduction

This document has been prepared to assist you in becoming familiar with Quest One Privileged Password Management. The System Administrator Guide explains the core functionality of the Privileged Password Management product regardless of modules and licenses purchased. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

Before beginning the initial configuration of TPAM, take a few minutes to copy and complete the worksheet on this page. The information below will be used in the process of setting up TPAM, and having it pre-organized here will ensure an easy setup.

NOTE: If you are configuring the High Availability, make an additional copy of this page and complete one for each device.

Information to gather

1. Have an available workstation or laptop that can be used to access the TPAM through direct crossover connection. Use the Ethernet cable provided with the appliance.
2. Write down the network configuration for the TPAM Primary:
   - IP address: ________________________________
   - Subnet Mask: ________________________________
   - Default Gateway: ________________________________
   - Primary DNS Server: ________________________________
   - Secondary DNS Server: ________________________________
3. Write down the network configuration for the TPAM Replicas:
   - IP address: ________________________________
   - Subnet Mask: ________________________________
4. If you have purchased DPAs, write down the network configuration for the DPAs.
   - IP address: ______________________________
   - Subnet Mask: ______________________________
   - Default Gateway: ______________________________
   - Primary DNS Server: ______________________________
   - Secondary DNS Server: ______________________________

5. If you have purchased a Cache server, write down the network configuration for the Cache.
   - IP address: ______________________________
   - Subnet Mask: ______________________________
   - Default Gateway: ______________________________
   - Primary DNS Server: ______________________________
   - Secondary DNS Server: ______________________________

6. Write down the information for the archive server you will use for backups.
   - Archive server name: ______________________________
   - IP Address: ______________________________
   - Account Name: ______________________________
   - Password/DSS Key: ______________________________

7. Write down the information for the archive server you will use for logs.
   - Archive server name: ______________________________
   - IP Address: ______________________________
   - Account Name: ______________________________
   - Password/DSS Key: ______________________________

8. For PSM Customers, write down the information for the archive server you will use for session logs.
   - Archive server name: ______________________________
   - IP Address: ______________________________
   - Account Name: ______________________________
   - Password/DSS Key: ______________________________

9. Obtain the password for the Parmaster account. This password is included in the Quick Start guide.
10. SMTP Mail Configuration (optional, but highly recommended)
   - IP address of the mail server: ____________________________
   - Email address to be used by TPAM: ________________________

11. NTP server address (optional): ____________________________

12. Allow remote access to /config? ________ Yes ________ No
This chapter covers the recommended steps for configuration steps in the /config and /admin interfaces. The order of the information presented in this manual reflects the recommended steps outlined below.

**Recommended steps**

**To configure the /config and /admin interface:**

1. Log on to the /admin interface with the **parmaster** user name. Put the appliance in Operational mode. Repeat this step for all appliances. See *Change the run level* for instructions on how to do this.

2. Log on to the /config interface with the **parmaster** username. Configure the network settings and DNS settings. Repeat this step for all appliances. See *Configure the network settings*.

3. Generate or import web certificates for all your TPAM devices. See *Generate web certificate request* on page 127 and *Import web certificate* on page 127.

4. Log onto the /admin interface with the **parmaster** user ID.

5. Add a Sys-Admin CLI user ID. Download and store the key outside of the appliance. See *Add CLI Sys Admin User* for details.

6. If applicable configure high availability cluster. See *Configure a cluster*.

7. Configure license usage. See *Adjust license limits* on page 172.


9. Configure archive server for logs. See *Archive log settings* on page 73.

10. Configure reason codes. (optional) See *Add a reason code* on page 75.

11. Configure global settings. See *Edit global settings*.

12. Configure password rules. See *Add a password rule*.
13. Configure email settings. See Configure mail agent and Configure email notification.
14. Configure the date and time settings. See Set date and time on page 123.
15. Configure the automation engine. See Auto Management settings tab on page 134.
16. Configure daily maintenance agent, auto discovery agent and post session processing agent (PSM customers only). See Daily Maintenance agent on page 137.
17. Configure backup schedule. See Configure the backup schedule.
18. Subscribe to alerts. See Add an alert receiver.
23. Configure a message of the day and/or login banner. (optional) See Login Banner and Message of the Day on page 173.
Start Up

Introduction

Take a few moments to gather the tools you will need to perform the initial setup of the TPAM appliance, and organize your environment. You will need the following items:

- A laptop or workstation computer with a web browser and ethernet interface that can be located near the appliance.
- A standard ethernet crossover cable.
- Document supplied by One Identity containing usernames and passwords (located on the CD).
- One IP address for each TPAM appliance on the network.

Power on the TPAM appliance

To power on the TPAM appliance:

Figure 1: Standard TPAM appliance
Figure 2: Enterprise TPAM appliance

1. Press the power button on the front panel of the appliance.
2. Connect a remote host computer (laptop, etc.) to the /config interface port using a crossover cable.
3. Set the IP address of the remote host to any address on the 192.168.1.XXX subnet, except for 192.168.1.105.
4. From the remote host, open a web browser session to: https://192.168.1.105/config. If prompted to accept the certificate, click Yes.
5. Enter parmasterr for the User Name. The password is supplied in the documentation accompanying the appliance.

TIP: If you have problems accessing the config interface check your browser Security Settings. Try using an alternate browser and/or make sure you have set up the URL as a trusted site.

Once logged on, you will see the /config home page.
Network Settings

Introduction

The /config interface provides the connection for the initial setup and configuration of the TPAM appliance, as well as an ongoing management interface for accessing logs and other forensic information.

The /config interface is used to set the following parameters for the appliance:

- IP Address
- Subnet Mask
- Default Gateway
- DNS server(s)

Configure the network settings

To configure the network settings:

1. Select **Network Settings | Modify Network Settings** from the menu.
2. Enter the IP Address, Subnet Mask, Default Gateway and MTU size. Click the **Save Settings** button.
   
   The default value used for MTU is 1500 if left blank. 1500 is also the maximum value allowed.

   **NOTE:** These settings take effect immediately, so if you change the IP address, upon clicking the save changes button your user session will end and you will have to log on to TPAM at the new IP address.
Configure DNS settings

Modifying the DNS settings allows a change in the configuration of just the DNS servers without making any changes to the built-in firewall or IP address of the appliance. This is a more desired method when no other network configuration changes are being made.

To configure the DNS settings:

1. Select Network Settings | Modify DNS Settings from the menu.
2. Enter the Preferred DNS Server and the Alternate DNS Servers. Click the Save Settings button.

View running values

If you select Network Settings | View Running Values from the main menu, the current values for the primary network interface for the appliance are displayed. This read only view lets the System Administrator confirm that the settings are correct.

Flush DNS

To immediately flush all cached DNS entries:

1. Select Network Settings | Flush DNS from the menu.
2. Click the FlushDNS button.

DNS suffix search

The DNS suffix search allows you to add domain suffix search order to the network settings. Adding these suffixes allows DNS to query for systems by appending these suffixes in order. For example: I enter a system in TPAM and give it a network address of questdevchad. If the suffix search order is blank, it will query the DNS for questdevchad without any other information and fail. Specifying a suffix search list allows the system to append the suffix to questdevchad to resolve an address. If the search order was: example.org,tpamexample.org, it would first try to resolve questdevchad.example.org first and then questdevchad.tpamexample.org if the first resolution fails.

To add DNS suffix search:

1. Select Network Settings | DNS Suffix Search from the menu.
2. Enter up to six DNS suffixes.
3. Click the **Save Settings** button.

**Host file mapping**

Host file mapping allows a static entry of a Host Name that is directly linked to an IP Address without the dependency of a DNS server.

**To map a host file:**

1. Select **Network Settings | Manage Hosts File** from the menu.
2. Enter the Host IP address and the Host Name. Click the + button.
3. To remove an entry click the X button.
4. Select **Replicate hosts file to other consoles and include in backup** to replicate the mappings to replicas in the cluster.
Sys-Admin User ID’s

Introduction

This chapter covers, adding and managing TPAM System Administrator user ID’s.
To add and manage Sys-Admin user ID’s, information is entered on the following tabs in the TPAM interface:

Table 1: Sys-Admin User Management: TPAM interface tabs

<table>
<thead>
<tr>
<th>Tab name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>Define main information, such as name, and contact information.</td>
</tr>
<tr>
<td>Details/Web</td>
<td>Configure access and authentication methods.</td>
</tr>
<tr>
<td>Details/Key Based</td>
<td>Define key based authentication method.</td>
</tr>
<tr>
<td>Details/Time</td>
<td>Define time zone and access times.</td>
</tr>
<tr>
<td>Details/Custom Information</td>
<td>Custom fields available for use.</td>
</tr>
</tbody>
</table>

Details tab

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

Table 2: Sys-Admin User Management: Details tab options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The user’s login id. Usernames may be a maximum of 30 characters long. The following special characters are allowed in the user name: <code>~#%&amp;(){}</code>.!</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
## Web tab

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

### Table 3: Sys-Admin User Management: Details Web tab options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow WEB Access?</td>
<td>If selected, the user can access TPAM via the web.</td>
<td>No</td>
<td>On</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password/Confirm Password</td>
<td>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.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Certificate Thumbprint</td>
<td>For users who authenticate using a client certificate with a thumbprint, the certificate’s SHA1 or SHA2 thumbprint should be entered here. This option will not appear unless certificate is selected as the primary user authentication type.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Principal Name</td>
<td>For users who authenticate using a certificate and the value of the subjectALTName:PrincipalName attribute contained in the certificate.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Primary User Authentication</td>
<td>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:</td>
<td>Yes</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td>• <strong>Certificate</strong> - 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Local</strong> - TPAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Windows Active Directory</strong> - WinAD is configured in the admin interface as an external source of authentication. The Windows AD primary user ID must always be in UPN( user principle name) format, allowing the use of multiple domains.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LDAP</strong> - LDAP is configured in the admin interface as an external source of authentication. You have the option of letting users type a shortened version of their LDAP user ID that expands to the full LDAP user ID for</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary User Authentication</td>
<td>If the user is using secondary authentication select the type, source and enter their user ID here. Choices of secondary authentication are:</td>
<td>No</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>- None</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Safeword</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SecureID</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- LDAP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Radius</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- WinAD</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Defender</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Starling Two-Factor Radius Agent</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Key based tab**

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

**Table 4: Sys-Admin User Management: Details Key Based tab options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI</td>
<td>If selected, the user can access TPAM via the CLI.</td>
<td>No</td>
<td>Off</td>
</tr>
<tr>
<td>CLI Key Passphrase</td>
<td>Only applies to CLI users. This is an optional passphrase to encrypt the user’s private key. The phrase is case sensitive, up to 128 characters, and does not allow double</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Field | Description | Required? | Default
---|---|---|---
| quotes ("). The phrase is not stored and cannot be retrieved after the key is generated. Remember to give the passphrase 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.

| Restricted IP Address | Only applies to CLI 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 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 you to set a System Administrator’s local time zone. This tab is not enabled for CLI users.

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

The table below explains all of the field options available on the UserID Time tab:
Table 5: Sys-Admin User Management: Details Time tab options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Timezone</td>
<td>Select a local time zone for the user.</td>
<td>Yes</td>
<td>Will default to the default user timezone global setting value.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> If the user is in a time zone that follows DST, TPAM will automatically adjust the time for them.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Based System Access</td>
<td>Choices are:</td>
<td>Yes</td>
<td>No Restrictions</td>
</tr>
<tr>
<td></td>
<td>- No Restriction - if selected, the user can access TPAM at any time/day.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Allow - To limit a user’s access to TPAM, select the <strong>Allow</strong> 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Prohibit - To restrict a user’s access to TPAM, select the <strong>Prohibit</strong> 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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Custom information tab**

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

**Add a web sys-admin user ID**

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

- Details
- Details/Web
The following procedure describes the steps to add a user ID.

**To add a new web user ID:**
1. Select **Sys-Admin UserIDs | Add Sys-Admin UserID** from the menu.
2. Enter information on the Details tab. For more information on this tab see **Details tab** on page 21.
3. Enter information on the Web tab. For more information on this tab see **Web tab**. (Optional)
4. To set time zone and access rules, click the **Time** tab and make changes. For more details see **Time tab** on page 25. (Optional)
5. To enter custom information, click the **Custom Information** tab. For more details see **Custom information tab** on page 26. (Optional)
6. Click the **Save Changes** button.

**Add a CLI sys-admin user**

A CLI Sys-Admin user ID is a special user account used to access TPAM remotely via the CLI (command line interface). It is 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. User IDs that have access to the system administrator CLI commands will have "CliA" listing in the interface column on the User Listing tab.

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

**To add a new Sys-Admin CLI user ID:**
1. Select **Sys-Admin UserIDs | Add Sys-Admin UserID** from the menu.
2. Enter information on the Details tab. For more information on this tab see **Details tab** on page 21.
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. Click the **Save Changes** button.
6. Click the **Details** tab.
7. Click the **Key Based** tab.
8. Click the **Download Key** button.
9. Save the key file that is generated.
10. Give this key file to the user. This key file must be placed on any computer that uses this user ID to access TPAM’s command line functions.

**NOTE:** The name of the key file can be renamed.

**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. The user must log on to TPAM to download and/or regenerate their own DSS key.

### Regenerate keys for CLI users

**To generate a new key:**

1. Select **Sys-Admin UserIDs | Manage Sys-Admin UserIDs** from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the **Listing** tab.
4. Select the user.
5. Click the **Details** tab.
6. Click the **Key Based** tab.
7. If you require a CLI Key Passphrase, enter one. If not proceed to step 8.
8. Click the **Regenerate Key** button.

### Delete a sys-admin user ID

**To delete a sys-admin user ID:**

1. Select **Sys-Admin UserIDs | Manage Sys-Admin 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 sys-admin user ID

To disable/enable a sys-admin user ID:
1. Select Sys-Admin UserIDs | Manage Sys-Admin 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.
7. Click the Save Changes button.

Unlock a sys-admin user ID

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

To unlock a sys-admin user:
1. Select Sys-Admin UserIDs | Manage Sys-Admin 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 sys-admin user ID password

To reset a sys-admin user’s password:
1. Select Sys-Admin UserIDs | Manage Sys-Admin 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 fields.
7. Click the Save Changes button.
8. Notify the user of their new password.
Manage your TPAM sys-admin 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 6: Fields available under User Details

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Number</td>
<td>Phone number that is associated with your user id in TPAM.</td>
</tr>
<tr>
<td>Mobile Number</td>
<td>Mobile number that is associated with your user id in TPAM.</td>
</tr>
<tr>
<td>E-mail</td>
<td>The email address that TPAM will use for email notifications from TPAM.</td>
</tr>
<tr>
<td>My Timezone</td>
<td>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.</td>
</tr>
<tr>
<td>CLI Key Passphrase</td>
<td>Only applies to CLI users. This is an optional passphrase to encrypt the user's private key. The phrase is case sensitive, up to 128 characters, and does not allow double quotes (&quot;). The phrase is not stored and cannot be retrieved after the key is generated.</td>
</tr>
<tr>
<td>Reset SysAdm CLI Key</td>
<td>Click this button to create a new CLI key for the user ID.</td>
</tr>
<tr>
<td>Get SysAdm CLI Key</td>
<td>Click the button to retrieve the new CLI key.</td>
</tr>
</tbody>
</table>
3. Click the **Save Changes** button.

### Promote a user ID

TPAM allows you to promote user IDs with Web or CLI access in the /tpam interface to sys-admin user IDs with access to the /admin and /config interface.

**NOTE:** You cannot promote the paradmin user ID.

**To promote a user ID:**

1. Select **Sys-Admin UserIDs | Manage Sys-Admin UserIDs** from the menu.
2. Click the **Promote User** button.
3. Enter filter criteria to find the user ID to promote.
4. Click the **Listing** tab and select the user ID.
5. Click the **Details** tab.

**NOTE:** If the user you are promoting has CLI access for the /tpam interface, they will not automatically have CLI access to the /admin interface when you promote them, you must select the **CLI** check box.

6. If the user is a CLI user, select the **CLI** check box on the Key Based tab.
7. Click the **Save Changes** button to grant the user system administrator privileges.

**TIP:** If a user ID that has web and CLI access is promoted, that user must log on to the /admin interface to generate their keys for CLI Sys Admin access.

### Demote a user ID

**To demote a user ID:**

1. Select **Sys-Admin UserIDs | Manage Sys-Admin UserIDs** from the menu.
2. Enter filter criteria to find the user ID to demote.
3. Click the **Listing** tab and select the user ID.
4. Click the **Demote User** button.
5. Click the **OK** button on the confirmation window.
NOTE: You cannot demote a user ID if they do not have a User Type assigned in the /tpam interface.

Manage the parmaster user ID

There is the option to have TPAM manage the parmaster user ID, so that any user wanting to log on as parmaster must go through the TPAM request and approval process to obtain the account password. When the parmaster account is managed through TPAM you cannot enter a new password for this account on the Sys-Admin Management User Details page. Additionally, when a user is logged on as parmaster they will not have access to the User menu Change Password option.

NOTE: The global approver and requestor groups will not automatically grant a user access the paradmin and parmaster accounts when they are managed. You must go to a user’s permissions tab to assign the permissions for these accounts.

To manage the parmaster user ID:

1. Create a sys-admin account. See Add a web sys-admin user ID on page 26.
2. Log on to the /admin interface using the new sys-admin account.
3. Select Sys-Admin UserIDs | Manage Sys-Admin UserIDs from the menu.
4. Filter for the parmaster account. Click the Listing tab.
5. Select the parmaster account.
6. Click the Details tab.
7. Select the Administer account password with local PPM? check box.
8. Click the Save Changes button.

After this is saved the parmaster account on the managed system Local_Appliance_parmaster will be set with the Automatic Password Management selected.

9. Logon to the /tpam interface.
10. Select Accounts | Manage Accounts from the menu.
11. Filter for the parmaster account. Click the Details tab.
12. Click the Management tab. Verify that the password check and changes profiles you want used to manage this account are assigned.

The password will be scheduled for an immediate reset. Depending on the number of password changes in the queue it may take some time to reset. Any users currently logged on as parmaster will be prompted to enter a new password once it has been reset.
To disable management of the parmster user ID:
1. Log on to the /admin interface using a sys-admin account other than parmster.
2. Select Sys-Admin UserIDs | Manage Sys-Admin UserIDs from the menu.
3. Filter for the parmster account. Click the Listing tab.
4. Select the parmster account.
5. Click the Details tab.
6. Clear the Administer account password with local PPM? check box.
7. Enter a new password in the password and confirm fields.
8. Click the Save Changes button.

Active logins

To view all user IDs currently logged on to TPAM select System Status/Settings | Active Logins from the menu. The session start time is displayed in server time (UTC). To view the user details select the User from the list and click the User Details tab. To terminate a user’s session in TPAM select the User from the list and click the Terminate button.
Distributed Processing Appliances (DPAs)

Introduction

You have the option to purchase Distributed Processing Appliances (DPAs) to increase the number of concurrent PSM sessions that can be run. Each additional DPA supports up to 150 additional concurrent sessions. PSM performs simplistic load balancing by sending the next session record or replay request to the active DPA with the most available sessions remaining.

With DPA v3.0+ you can now assign a DPA to a system to optimize password checking and changing. At the system level (on the Affinity tab) you can assign the DPA that should perform password checking and changing for all the accounts on that system.

To get the DPA up and running you must perform the following steps:

- Power on the DPA
- Configure the network settings
- Enable remote access (Optional)
- Define remote access IP restrictions (Optional)
- Prepare the DPA for enrollment
- Enroll the DPA in a cluster
- Manage DPA settings
- Assign systems to DPA
Power on the DPA appliance

To power on the DPA appliance:

1. Connect a keyboard and monitor to the DPA appliance.

2. Press the power button on the front panel of the appliance. After the power on self test, the appliance will boot to a log on prompt.

3. Type `dpasetup` for the user ID and `Setup4DPA` as the password. Both the user ID and password are case-sensitive, type them exactly as shown. This is the only user ID that can be used to log on to the console.

   The main menu will appear listing all of the commands available from the configuration console.

Configure network settings

To configure network settings:

1. Type 4 and press the ENTER key to configure the network settings.

2. If your DPA will be using only one NIC, type 3 and press the ENTER key to disable the eth1 network settings. A reason to configure both NICs would be in an enclave scenario. In this scenario, the TPAM appliance is not in the same network as the target systems. The DPA can act as a bridge to the target devices when TPAM can access the DPA via one of the NICs and the DPA can access the target systems with the other DPA NIC.

3. Type D and press the ENTER key to disable the eth1 interface or type the IP address if both eth1 and eth0 will be used.

4. Type Y and press the ENTER key to save your changes.

5. Press the ENTER key to return to the main menu.

6. Type 2 and press the ENTER key to modify the eth0 network settings.

7. Type the IP Address for eth0 as prompted and press the ENTER key

8. Type the Network Mask for eth0 as prompted and press the ENTER key.

9. Type the Default Gateway for eth0 as prompted and press the ENTER key.

10. Type the MTU Size if desired. If nothing is entered the default value is 1500.
11. Press the Y key and press the ENTER key to save your changes.
12. Press the ENTER key to return to the manage network settings menu.
13. If the DPA will use both NICs enter 3 and press the ENTER key to modify the eth1 settings.
14. Enter the IP Address for eth1 as prompted and press the ENTER key.
15. Type the Network Mask for eth1 as prompted and press the ENTER key.
16. Type the Default Gateway for eth1 as prompted and press the ENTER key.
17. Press the Y key and press the ENTER key to save your changes.
18. Press the ENTER key to return to the manage network settings menu.
19. Type 4 and press the ENTER key to modify the DNS settings.
20. Type the DNS IP and press the ENTER key.
21. Type the Alternate DNS IP and press the ENTER key. Up to four DNS can be configured.(Optional)
22. Type the DNS Domain and press the ENTER key. (Optional)
23. Type Y and press the ENTER key to save your changes.
24. Press the ENTER key to return to the manage network settings menu.
25. Type Q and press the ENTER key to return to the main menu.

Enable remote access

This step allows remote SSH access to the DPA. Allowing remote SSH access gives you the ability to copy and paste the enrollment string, rather than having to write it down and type it in manually. By default, remote access to the DPA is disabled.

To enable/disable remote access:

1. Type 5 and press the ENTER key to configure remote access.
2. Type 2 and press the ENTER key.
3. Type E and press the ENTER key to enable remote access to the DPA.
4. Type and confirm a password for the rdpsetup user.
5. Type Q and press the ENTER key to return to the main menu.
6. Type 8 and press the ENTER key to shutdown the appliance.

| NOTE: | The DPA will not shutdown or reboot if there are any active sessions running. |

7. Remove the monitor and keyboard from the appliance.
8. Place the DPA on your network.
9. Power the appliance on.
10. Using an SSH client, connect to the DPA with the user ID \texttt{rdpasetup} using the password you just set.

Changing the setup password while logged into the DPA

This step allows you to change the password associated with the \texttt{dpasetup} account.

\textit{To change the password for the dpasetup account:}

1. From the main menu type 5 and press the \texttt{ENTER} key.
2. Type 1 and press the \texttt{ENTER} key.
3. Type Y and press the \texttt{ENTER} key.
4. Type the current password and press the \texttt{ENTER} key.
5. Type the new password and press the \texttt{ENTER} key.

Using TPAM to manage the DPA dpasetup account

When a DPA server is added to a cluster in TPAM a system is automatically created for the DPA server and accounts created for the \texttt{dpasetup} and \texttt{rdpasetup} accounts. By default these accounts are not auto-managed. These can be set to auto-managed so that TPAM can manage the password for the DPA server. The password for the accounts will be set to \texttt{default initial password}. When a DPA server is removed from a cluster the DPA system and accounts will be automatically deleted from TPAM.

Password management operations on the \texttt{rdpasetup} account will not work unless remote access for this account has been enabled. PSM sessions are allowed to the \texttt{rdpasetup} account. Remote access for this account must be enabled, and the password for this account must be known by TPAM in order for PSM sessions to successfully authenticate.

\textbf{CAUTION:} If password management is enabled and the DPA server is going to be removed from a cluster, then it is critical to retrieve and save the passwords for the accounts prior to deletion. There is no mechanism to reset the account password(s) for a DPA server that is not a cluster member and to re-enroll the DPA the password will be needed.
Define remote IP address restrictions

You can configure IP address restrictions for the remote access to the DPA. If remote IP address restrictions are configured, the IP address of the remote machine is checked against all restrictions that are entered. If it meets all specified criteria, the login is allowed to proceed.

All restrictions must be entered at one time, comma separated. Wildcards and negation are allowed. A * matches zero or more characters. A ? matches exactly one character. A ! negates the criterion. In the example below, “192.168.30.*” says all IP addresses starting with “192.168.30.” are allowed. Then, the “!192.168.30.???” excludes 192.168.30.100 through 192.168.30.255. Also, 192.168.30.1 is explicitly excluded.

To configure restrictions:
1. From the main DPA menu, type 5 and press the ENTER key.
2. Type 3 and press the ENTER key.
3. Type the restriction rules and press the ENTER key.
4. Type Y and press the ENTER key.

Prepare the DPA for enrollment

The next step is to prepare the DPA for enrollment to your TPAM appliance. This step prepares temporary keys that are used to establish the secure connections between the DPA and your TPAM appliance(s). This step is best done remotely as the string necessary to enroll the DPA is rather long and remotely accessing the DPA allows you to copy the string more easily.

To prepare for enrollment:
1. From the main menu, type 3 and press the ENTER key.
2. When prompted, type the IP address of the TPAM primary device, and press the ENTER key.
3. Type E and press the ENTER key to enroll the DPA.
4. Type Y and press the ENTER key.
5. Copy the key that is presented. You will need to type this key in procedure below.
   See Increase DPA license count on page 39.

Logs menu

Through the logs menu you can access the following logs:
Table 7: Logs available on Logs menu

<table>
<thead>
<tr>
<th>Log name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Activity Log</td>
<td>Displays actions taken within the DPA setup menu such as login, enrollment, IP restrictions, etc from the current month.</td>
</tr>
<tr>
<td>Last Months Activity Log</td>
<td>Displays activity log from the previous month.</td>
</tr>
<tr>
<td>DPA Initialization Log</td>
<td>Displays information that can be used by technical support when troubleshooting an issue with a DPA.</td>
</tr>
<tr>
<td>Bad Login Attempts Log</td>
<td>Displays invalid log on attempts to the DPA console.</td>
</tr>
<tr>
<td>Current J2EE Server Log</td>
<td>Displays the</td>
</tr>
</tbody>
</table>

To view the DPA logs:

1. From the main menu, type 6 and press the ENTER key.
2. Type 1,2,3, 4 or 5, and press the ENTER key to view the different logs.

Increase DPA license count

Before the DPA can be enrolled in TPAM, you must increase the DPA license count in the admin interface.

To adjust license limits:

1. Select System Status/Settings | License Management from the menu.
2. Type a number in the MaxDPAs for the number of DPAs you will be adding to TPAM.
3. Click the Save Changes button.

Enroll DPA in cluster

To enroll a DPA in a cluster:

1. Log on to the /admin interface of the primary TPAM appliance.
2. Select System Status/Settings | Cluster Management from the menu.
3. Click the New Cluster Member button.
4. Type a name for the DPA.
5. Select **Distributed Processing Appliance** from the appliance type list.
6. Select one of the following from the appliance active list:
   - Active - DPA can be used for PSM sessions and password management
   - Inactive - DPA will not be used for PSM sessions or password management, regardless of affinity settings.
7. Type the network address for the DPA in the network address field.
8. Change the default SSH port if necessary.
9. Click the **Check Address** button.
10. Type or paste the enrollment string that was generated from the DPA console.
11. Click the **Save** button.
12. If the DPA is successfully enrolled, type Y back on the DPA console to complete the TPAM enrollment process on the console. This completes the DPA enrollment process.

**Manage DPA settings**

Once the DPA is enrolled, it is visible in the /tpam interface and its’ settings can be configured.

*To manage the DPA settings:*

1. Log on to the /tpam interface.
2. Select **Management** | **DPAs** from the menu.
3. Select the DPA from the servers list.
4. Click the **Details** tab.
5. Type a DNS name for the DPA. (Optional)
6. Type the maximum number of concurrent sessions that should run on this DPA. The maximum value is 150.
7. Type a description for the DPA. (Optional)
8. Select/Clear the **Allow PSM?** check box. If selected, the DPA can be used for session recording and playback. If cleared, the DPA cannot be used for session recording and playback. This will be selected by default if the DPA is saved as active when it is enrolled in the cluster.
9. Select/Clear the **PPM Only?** check box. If selected, the DPA can be used for password checks and changes, regardless of the Allow PSM? setting.
10. Select/Clear the **Auto-Archive Session Logs?** check box. If selected, as soon as a session is completed it is immediately pushed to the archive server. If selected, select an archive server to send the sessions to.
11. Select/Clear the **Use this DPA for replays of session logs archived here?** check box. This check box is only enabled if the **Auto-Archive Session Logs?** check box and the **Allow PSM?** check boxes are selected. If selected, this DPA will replay sessions that have been archived.

12. Change the Web Access Proxy Profile that will be used by the DPA if the default is not desired. This only applies to PSM Web Access systems. See the TPAM Client Setup Guide for more details.

13. Click the **Save Changes** button.

To view the systems assigned to the DPA and the DPA software version click on the **Affinity** tab.

## DPA log tab

The DPA log tab provides visibility to PSM related processes on the DPA that could be helpful when troubleshooting.

**To view a DPA log:**

1. Select **Management | DPAs** from the menu.
2. Select the DPA to view.
3. Click the **Log** tab.
4. Type your search criteria on the **Filter** tab.
5. Click the **Log** tab.

## Remove DPA from a cluster

When a DPA is removed from a cluster any systems that were assigned to the DPA revert to using the local appliance or other DPAs in the cluster based on the system’s affinity assignments.

**To remove a DPA from a cluster:**

1. Log on to the /admin interface of the primary appliance in the cluster.
2. Select **System Status/Setting | Cluster Management** from the menu.
3. Select the DPA to be removed from the cluster member list.
4. Click the **Remove Cluster Member** button.
5. Click the **OK** button on the confirmation window.
Re-enroll a DPA

If the need arises to replace a DPA with another physical DPA, you can re-enroll the new physical DPA under the same name and IP address as the old one and all the original System affinity settings will be preserved. Re-enrollment requires an enrollment string obtained from the DPA console. See Type Y and press the ENTER key. on page 38.

To re-enroll the DPA:

1. Log on to the /admin interface of the primary appliance in the cluster.
2. Select System Status/Setting | Cluster Management from the menu.
3. Select the DPA to re-enroll from the cluster member list.
4. Select the Enrollment String check box.
5. Type or paste in the enrollment string.
6. Click the Enroll/Re-enroll DPA button.

Change DPA SSH port

IMPORTANT: To change the port used by the DPA, it must be changed on the DPA console first, before it is changed on the Cluster Management page in the TPAM interface.

To change the port configuration for an existing DPA:

1. Log on to the DPA console.
2. Type 4 and press the ENTER key.
3. Type 5 and press the ENTER key.
4. Type the new port number and press the ENTER key.
5. Type Y and press the ENTER key.
6. Log off the DPA Console.
7. Log on to the admin interface of TPAM.
8. Select System Status/Settings | Cluster Management from the menu.
9. Click the Cluster Status tab.
10. Select the DPA you want to change in the Cluster Member list.
11. Select the Ssh Port check box.
12. Type the new port number.
13. Click the Save button.
Manage host file entries

Host file entries can be added, deleted and listed from the DPA Configuration interface. This allows a customer to add entries that will enable PSM Web Access sessions to work without DNS setup.

To add a host file entry:
1. Log on to the DPA console.
2. Type 4 and press the ENTER key.
3. Type 9 and press the ENTER key.
4. Type the host file entry in the format IP_address host_name(s). Press the ENTER key.
5. Type Y to continue.
6. Type N to return to the main menu if there are no more entries to add.

To delete a host file entry:
1. Log on to the DPA console.
2. Type 4 and press the ENTER key.
3. Type 10 and press the ENTER key.
4. Type the host file entry you want to delete. (0-...) Press then ENTER key.

To list host file entries:
1. Log on to the DPA console.
2. Type 4 and press the ENTER key.
3. Type 8 and press the ENTER key.

DPA configuration using both network cards on a segmented network

There are cases where TPAM is required to manage devices on networks not known to TPAM’s local segment. Using a DPA allows TPAM to manage these devices through use of a properly configured DPA. The example below requires TPAM to communicate with a device that is located behind a firewall on a network unknown by TPAM.

Figure A below shows the DPA’s network information when configured as follows:

DPA ETH0 : 192.168.7.247/24
DPA ETH0 GATEWAY: 192.168.7.1
DPA ETH1 : 10.9.6.247/22
The last gateway read during the network startup is the default gateway for the device. The network information is read in ascending order by device id. In this example, because eth1 is read last; the default gateway for the device is 10.9.4.1.

All traffic not originating from the DPA will attempt to leave the DPA via the default gateway. The exception to this is when either a static route is added, or the network is known locally. In this configuration, any device on 192.168.7.X network does not need a static route. However if there are other devices behind the 192.168.7.1 gateway, those devices/networks will need static routes. Static routes are not needed for anything behind the DPA’s default gateway.

In this configuration, remote access is available on 10.9.6.247 and 192.168.7.247. However, it is important to note that access via 192.168.7.247 will require that client to be connect to the 192.168.7.X network, or come from a network in which a static route has been placed. Accessing the device via 10.9.6.247 does not require any static routes. The client simply needs to be able to route to that network.

The network design is such that 192.168.7.X/24 and 10.9.4.X/22 network are physically and logically separate and have no routes in between. The DPA and TPAM both are members of the 10.9.4.X/22 network. When enrolling the DPA, the DPA must be enrolled
via the 10.9.4.X network. The DPA’s network address in the cluster management must be on 10.9.4.X/22 (or on the same segment as TPAM). When TPAM must manage devices on the 192.168.7.X/24 segment, affinity must be set for the corresponding DPA. Figures B, C, and D show examples of this configuration.

Figure B

![Figure B](image1)

Figure C

![Figure C](image2)

Figure D

![Figure D](image3)
Net tools

To assist the TPAM System Administrator with troubleshooting common network related problems, the DPA contains network tools that are accessible from the main menu.

To access the net tools menu from the main menu enter 9 and press the ENTER key.

The table below describes how each of the available tools:

<table>
<thead>
<tr>
<th>Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping Utility</td>
<td>The ping utility can be used to verify connectivity to remote hosts and determine latency. Many of the optional parameters for the ping command are available.</td>
</tr>
<tr>
<td>NsLookup Utility</td>
<td>Nslookup is a common TCP/IP tool used to test DNS settings and perform similar information gathering using DNS resolution. The DPA utility for nslookup will use the DNS server(s) configured to TPAM only. The option to specify a server is not provided. TPAM System Administrators can benefit from the ability to use nslookup to resolve hostnames to IP addresses and vice versa.</td>
</tr>
<tr>
<td>TraceRoute</td>
<td>The traceroute utility is available for examining network routing and connectivity from the DPA to a remote IP address or hostname. The use of traceroute is often disallowed by firewalls, routers, and other network security infrastructure – but if allowed, it can be a valuable diagnostic tool.</td>
</tr>
<tr>
<td>Telnet Test</td>
<td>The Telnet test utility lets a test be performed from the DPA to another system over a specific port. The tool will test the defined port using telnet functionality to verify the port, whether a connection can be made, and then immediately close the connection.</td>
</tr>
</tbody>
</table>

DPAs and failover

When a session terminates on a DPA, the DPA uses gossip protocol to determine where to complete the session. If the session is initiated by the primary and that primary is operational then the session is completed on the primary. If the originating primary is down but there are failed over replicas then the session will be completed on the first failed over replica ordered alphabetically. If there are no appliances available the DPA will hold the session log until a console becomes available. If the session originated from a failed over replica then it will complete with the failed over replica or the primary if the replica has failed back.
Test DPA

Testing a DPA checks the connectivity from the DPA to the primary and other replicas in the cluster. If using an archive server for PSM session logs, the connectivity between the DPA and archive server is tested. Details on sessions being recorded, replayed and monitored are also listed.

NOTE: TCP/UDP ports 9443 on the TPAM console must be accessible from the DPA. TCP/UDP ports 443 on the DPA must be accessible from the TPAM. These connections are tested during the Test DPA function. Should you elect to configure event capture TCP/UDP ports 443 on the TPAM console must be accessible from the DPA as well. Make sure there are no firewalls blocking access to these ports.

To test a DPA:

1. Select System Status/Setting | Cluster Management from the menu.
2. Select the DPA to test from the cluster member list.
3. Click the Test DPA button. The results of the test will appear on the Results tab.
   
   Init Pending: Y indicates that the initialization of the DPA is pending. The DPA would be found in this state just after enrollment or re-enrollment or after a restart of the DPA. The initialization includes pushing software updates from TPAM to the DPA. This may take a few minutes.

To test the DPA connectivity from the DPA console:

1. Log on to the DPA console.
2. Type 1 and press the ENTER key.

DPA version number

The DPA software version is occasionally updated when a patch is applied to TPAM.

To check the DPA software version number:

1. Select System Status/Settings | Cluster Management from the menu.
2. Click the Cluster Status tab.
3. Scroll down to see the DPAs and their latest version number.
High Availability Cluster

Introduction

High availability clustering is an option for customers to support TPAM with a minimum of down time and eliminate a single point of failure. Each appliance is configured with a cluster role. The cluster role choices are:

- **Primary** - Acts as the information source for the cluster. Only one primary allowed per cluster.
- **Replica** - redundant appliance that is kept in synch with the primary. Can be configured to automatically fail over if it loses contact with the primary.
- **Standalone** - this role only applies to DPAs enrolled in the cluster and cannot be changed.

For details on how to enroll DPAs in a cluster see Before the DPA can be enrolled in TPAM, you must increase the DPA license count in the admin interface. on page 39

Details tab

The table below explains all the of the options available on the cluster management details tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name to identify the appliance</td>
<td>Yes</td>
<td>TPAMCONSOLE</td>
</tr>
<tr>
<td>Appliance Type</td>
<td>Two appliance types:</td>
<td>Yes</td>
<td>Console Appliance</td>
</tr>
<tr>
<td></td>
<td>• <strong>Console</strong> - TPAM appliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>DPA</strong> - Distributed Processing Appliance.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Required?</td>
<td>Default</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Appliance Active</td>
<td>It is not possible to flag a primary appliance as inactive. The choices for replicas and DPAs are:</td>
<td>Yes</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>• Active - participating in cluster</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Not Active - For an appliance if marked as <strong>Not Active</strong> it is not participating in cluster replication. If a DPA is marked <strong>Not Active</strong> it will not be used for session recording or playback. A <strong>Not Active</strong> replica will not fail over. A <strong>Not Active</strong> replica will not be patched. If made active again it will not automatically be patched to the version of the primary. It will have to be failed over and patched separately.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Address</td>
<td>Network addresses must be unique within a cluster. After entering the network address you must click the <strong>Check Address</strong> button to be able to save the appliance in the cluster.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Ssh Port</td>
<td>Applies to DPAs. This is the port used to communicate with the DPA. The default is 22. If another port is required enter that port number here and in the DPA configuration screen.</td>
<td>Yes for DPAs</td>
<td>22</td>
</tr>
<tr>
<td>Enrollment String</td>
<td>The enrollment string generated when a DPA is configured must be entered here.</td>
<td>Yes, if you want to set DPA to Active and it was not previously enrolled</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>Choices of:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Primary</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Replica</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run Level</td>
<td>Choices of:</td>
<td>Yes</td>
<td>Operational</td>
</tr>
<tr>
<td></td>
<td>• Maintenance - In this mode users can only log on to the /admin and</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/config interfaces.</td>
<td><img src="image" alt="NOTE: DPAs and Cache servers are not patched while the primary is in maintenance mode. The DPAs and Cache servers are patched once the primary is put back into operational mode." /></td>
<td><img src="image" alt="NOTE: Operational - TPAM is fully functional" /></td>
<td><img src="image" alt="NOTE: A replica that is in maintenance mode will not automatically fail over." /></td>
</tr>
<tr>
<td>Failover Timeout</td>
<td>The number of seconds a replica will wait after losing contact with the primary before failing over. The minimum failover timeout is 60 seconds. A value of 0 (zero) means the replica will NOT failover.</td>
<td>Yes</td>
<td>300</td>
</tr>
<tr>
<td>Failback Timeout</td>
<td>The number of seconds a replica will wait after re-establishing contact with the primary before beginning failback processing. The minimum failback timeout is 60 seconds.</td>
<td>Yes</td>
<td>60</td>
</tr>
</tbody>
</table>

The **Restart Clustering** button should be used anytime the global settings for replication are changed.

### Member status tab

The member status tab displays many statistics about the appliance such as memory and disk space, software version and hot fixes installed, and serial number information. Here system administrators can see this information for all cluster members without having to log on individually to each cluster member. Much of this information is also visible of the System Status page for each appliance.
Snapshots tab

When a replica is enrolled in a cluster, during that process a snapshot is taken of the current state of the replica. This snapshot can be used as a restore point in case the enrollment process fails and it is necessary to get the replica back to its original state.

There are two CLI system administrator commands available to revert to the snapshot if needed, `ListRestorePoints` and `Revert`. For more details see Commands.

**IMPORTANT:** At this time do not “Revert to Snapshot” unless you are advised to do so by Technical Support.

Graphs tab

The graphs display data concerning the cluster member that is selected in the list. This data can be useful when working with technical support on replication issues. There are no graphs available for the primary appliance, only replicas and DPAs. A replica or DPA that has not yet been enrolled in the cluster will have empty graphs.

Below is a brief description of the available graphs:

**Table 10: Manage Cluster Settings and Members: Graphs tab options**

<table>
<thead>
<tr>
<th>Graph name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Transfers</td>
<td>Quantity of database data successfully published from a primary to a replica appliance. When viewed on the primary, gaps in this graph indicate that no database data was published to a replica.</td>
</tr>
<tr>
<td>Gossip Activity</td>
<td>Rate of gossip reports received from a peer appliance. Gaps or errors in this graph indicate that the peer appliance was down or unreachable.</td>
</tr>
<tr>
<td>Replication Bundles Published</td>
<td>Count of full and incremental replication bundles successfully published from a primary to a replica appliance. When viewed on the primary, gaps in this graph indicate that no data was published to a replica.</td>
</tr>
<tr>
<td>Replication File Transfers</td>
<td>Quantity of file-based data successfully published from a primary to a replica appliance. File-based data includes session logs, secure files and report output. When viewed on the primary, gaps in this graph indicate that no file data was published to a replica. This may be normal if no file updates were generated during this time.</td>
</tr>
</tbody>
</table>
Cluster status tab

The cluster status tab displays important information about the health and status of the cluster members, such as run level, replication status and software version level.

The possible values for replication status are:

- Failed Over - a replica has lost contact with the primary in the cluster and the failover time out has expired.
- Failing Back - a replica has re-established contact with the primary and the failback time out has expired.
- Replicating - normal status for a healthy primary.
- Standby - normal status for a healthy replica or a primary with no replicas defined.
- Unknown - when you have added a new cluster member but not uploaded the enrollment bundle or when a TPAM appliance is restarted but has not gossiped yet.
- Updating - Displayed when a replica is applying an update from the primary.

TIP: The Cluster Status tab reflects the status from the selected appliances’s point of view.

The possible values for cluster member state are:

- Failed - appears when a cluster member has not gossiped within the last minute, but has prior gossip activity in the past.
- Healthy - communicating with other cluster members.
- Unknown - when you have added a new cluster member but not but not uploaded the enrollment bundle or when a TPAM appliance is restarted but has not gossiped yet.

Appliance status

Any user can check the status of an appliance by going to https://tpamipaddress/status to get a quick view of the appliance status.

The appliance name, cluster role, run level, appliance status, replication status, and state are displayed.
Logs tab

The logs tab displays data pertinent to the high availability implementation on the appliance. Items such as replication status change, failover, etc are displayed in the logs. The Logs tab always displays logs from the primary appliance, regardless of the appliance selected in the cluster member list. The time displayed on the Logs tab is server time (UTC).

Configure a cluster

By definition, a cluster consists of one primary appliance, zero or more replica appliances, and zero or more DPAs. Each replica is individually configurable for failover and with its own delay values for failover and failback. When appliances are shipped to a customer all appliances will be pre-configured for the primary role and then can be changed during configuration.

**NOTE:** The TPAM appliances in a cluster communicate with one another using port 8000. TPAM appliances communicate with DPAs using port 22. Please ensure that your firewalls are configured to allow communication through these ports.

**TIP:** Before adding a replica to a cluster, it is recommended that a System Administrator CLI user ID is added to the replica and the keys are retrieved for this user ID, prior to enrolling the replica in the cluster. The System Administrator user ID can be used to execute the Revert command if the enrollment process fails.

**To configure a cluster:**

1. Turn on and configure the network settings for any appliances you want to use as replicas on your network. Make note of the IP addresses of each future replica.
2. Log on to the /admin interface for the appliance you want to label as the primary.
3. Select System Status/Settings | Cluster Management from the menu.
4. Select the Name check box. It is recommended to change the name of the appliance to include “primary” somewhere in the name. (optional)
5. Click the Save button.
6. Click the New Cluster Member button.
7. Enter the name for the replica.
8. Enter the network address of the replica.
9. Click the Check Address button.
10. Select Replica from the role list.
11. Enter the failover timeout.
12. Enter the failback timeout.
13. Click the **Save** button.
14. Click the **Make Enrollment Bundle** button. This generates the key file that will be used to communicate with the replica.
15. Click the **Continue with Change** button.

    **NOTE:** Make sure you have enabled pop-ups for your TPAM appliance.

16. You will be prompted to save the enrollment bundle file. Click the **OK** button and save the file locally.
17. Log on to the /admin interface of the replica appliance.
18. Select **System Status/Settings | Cluster Management** from the menu.
19. Select the **Run Level** check box.
20. Select **Maintenance** from the Run Level list.
21. Click the **Change Run Level** button.
22. Click the **Continue with Change** button.
23. Click the **Select File** button.
24. Click the **Browse** button. Select the file.
25. Click the **Upload** button.
26. Click the **Apply** button.
27. Click the **Continue with Change** button.
28. Log off the replica appliance or close the browser.

    **NOTE:** You may receive an error logging off depending on where the replica is in the enrollment process. This error can be ignored.

29. On the primary appliance select **System Status/Settings | Cluster Management** from the menu.
30. Select the replica in the cluster member list. Wait for the replica run level to change from Unknown to Maintenance, then proceed to the next step.

    **NOTE:** To refresh the page click the Details tab.

    **NOTE:** The replica may be visible in the cluster list but its status may be unknown for quite some time until it has fully enrolled with the primary. The time it takes to complete enrollment is dependent on the size of the backup being applied to the replica from the primary.

31. Select the **Run Level** check box.
32. Select **Operational** from the Run Level list.
33. Click the **Change Run Level** button.
34. Repeat steps 6 - 33 to add additional replicas to the cluster.

**Remove a cluster member**

*To remove a cluster member:*

1. Logon to the /admin interface of the primary appliance.
2. Select **System Status/Settings | Cluster Management** from the menu.
3. Select the appliance to remove from the cluster, either a console or DPA.
4. Click the **Remove Cluster Member** button.
5. Click the **OK** button on the confirmation window.
6. Click one of the following buttons:
   - **Remove and Reset Data** - Appliance is removed from the cluster. All customer data will be deleted, paradmin and parmaster accounts will have the password reset to the factory default. Network settings will remain.
   - **Remove and Retain Data** - Appliance is removed from the cluster, but all customer entered data persists. All other consoles, DPAs, and cache servers in that cluster are disassociated from the console being removed.
   - **Do Not Remove** - Cancel removing the appliance from the cluster.

The appliance will automatically be put in Maintenance mode with a role of primary when it is removed from the cluster.

**Reboot a replica**

You have the option to reboot the replicas in a cluster from the cluster management page of the primary.

*To reboot the replica:*

1. On the cluster management page of the primary appliance, select the replica from the cluster management list.
2. Click the **Reboot** button.
3. Click the **Continue with Change** button.
4. Click the **OK** button on the confirmation window.
Automatic failover

When a replica detects that the primary has failed it starts a failover timer if the failover timeout has a value other than 0 (zero). If the primary does not recover before the failover timer expires then an automatic failover to the replica/s occurs. The amount of time the replicas uses for its failover timer is entered in the failover timeout field.

**NOTE:** If a replica is in Maintenance mode, it will not be available for failover.

When an automatic failover occurs, TPAM users can log on to the failed over appliance and continue to create requests, approve requests, review requests, retrieve passwords and files, and start or replay sessions. Passwords can be reset manually, but will not automatically be reset after a password release or expired request. The automation engine cannot be started on a failed over replica. No data can be edited or added in the “failed over” mode.

Functionality on a failed over replica

When a replica is in "Failed Over" state the functionality available to users is limited. See the table below for details.

**Table 11: Functions available during failover**

<table>
<thead>
<tr>
<th>Function</th>
<th>Available during failover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add, edit or delete systems</td>
<td>No</td>
</tr>
<tr>
<td>Add system template</td>
<td>No</td>
</tr>
<tr>
<td>Hard delete a system</td>
<td>No</td>
</tr>
<tr>
<td>Manually test connection to a system</td>
<td>Yes</td>
</tr>
<tr>
<td>View system details</td>
<td>Yes</td>
</tr>
<tr>
<td>View soft deleted systems</td>
<td>Yes</td>
</tr>
<tr>
<td>List systems</td>
<td>Yes</td>
</tr>
<tr>
<td>Add, edit or delete accounts</td>
<td>No</td>
</tr>
<tr>
<td>Hard delete an account</td>
<td>No</td>
</tr>
<tr>
<td>View account details</td>
<td>Yes</td>
</tr>
<tr>
<td>Function</td>
<td>Available during failover</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>View soft deleted accounts</td>
<td>Yes</td>
</tr>
<tr>
<td>Retrieve account password</td>
<td>Yes</td>
</tr>
<tr>
<td>Manually reset an account password</td>
<td>Yes</td>
</tr>
<tr>
<td>Manually check an account password</td>
<td>Yes</td>
</tr>
<tr>
<td>View past passwords</td>
<td>Yes</td>
</tr>
<tr>
<td>List accounts and List PSM accounts</td>
<td>Yes</td>
</tr>
<tr>
<td>Add, edit or delete collections</td>
<td>No</td>
</tr>
<tr>
<td>View collection details</td>
<td>Yes</td>
</tr>
<tr>
<td>List collections</td>
<td>Yes</td>
</tr>
<tr>
<td>Add, edit or delete files</td>
<td>No</td>
</tr>
<tr>
<td>View file details</td>
<td>Yes</td>
</tr>
<tr>
<td>Retrieve file</td>
<td>Yes</td>
</tr>
<tr>
<td>List files</td>
<td>Yes</td>
</tr>
<tr>
<td>Add, edit, or delete a synchronized password</td>
<td>No</td>
</tr>
<tr>
<td>View synchronized password details</td>
<td>Yes</td>
</tr>
<tr>
<td>Reset the password for a synchronized password</td>
<td>No</td>
</tr>
<tr>
<td>Add, edit or delete a user ID</td>
<td>No</td>
</tr>
<tr>
<td>Disable a user ID</td>
<td>No</td>
</tr>
<tr>
<td>Reset the password for a user ID</td>
<td>Yes</td>
</tr>
<tr>
<td>View user ID details</td>
<td>Yes</td>
</tr>
<tr>
<td>List user IDs</td>
<td>Yes</td>
</tr>
<tr>
<td>Add user template</td>
<td>No</td>
</tr>
<tr>
<td>Add, edit or delete group</td>
<td>No</td>
</tr>
<tr>
<td>View group details</td>
<td>Yes</td>
</tr>
<tr>
<td>List groups</td>
<td>Yes</td>
</tr>
<tr>
<td>Add, edit, delete cache server</td>
<td>No</td>
</tr>
<tr>
<td>Batch imports and updates</td>
<td>No</td>
</tr>
<tr>
<td>Function</td>
<td>Available during failover</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Auto Discovery</td>
<td>No</td>
</tr>
<tr>
<td>Account Discovery</td>
<td>No</td>
</tr>
<tr>
<td>Add or Delete TPAM CLI ID</td>
<td>No</td>
</tr>
<tr>
<td>Test TPAM CLI ID</td>
<td>Yes</td>
</tr>
<tr>
<td>View and replay session logs</td>
<td>Yes</td>
</tr>
<tr>
<td>Monitor sessions</td>
<td>Yes</td>
</tr>
<tr>
<td>Add, edit or delete privileged commands</td>
<td>No</td>
</tr>
<tr>
<td>View privileged command details</td>
<td>Yes</td>
</tr>
<tr>
<td>View, add, edit or delete post session processing, PSM connection, restricted command or account discovery profiles</td>
<td>No</td>
</tr>
<tr>
<td>Add or edit DPAs</td>
<td>No</td>
</tr>
<tr>
<td>Test DPA connectivity</td>
<td>Yes</td>
</tr>
<tr>
<td>Add, edit or delete access policies</td>
<td>No</td>
</tr>
<tr>
<td>View access policies</td>
<td>Yes</td>
</tr>
<tr>
<td>Request a password</td>
<td>Yes</td>
</tr>
<tr>
<td>Approve a password</td>
<td>Yes</td>
</tr>
<tr>
<td>Request a session</td>
<td>Yes</td>
</tr>
<tr>
<td>Approve a session request</td>
<td>Yes</td>
</tr>
<tr>
<td>Review a session</td>
<td>Yes</td>
</tr>
<tr>
<td>Request a file</td>
<td>Yes</td>
</tr>
<tr>
<td>Approve a file request</td>
<td>Yes</td>
</tr>
<tr>
<td>Run on demand reports</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit batch report subscriptions</td>
<td>No</td>
</tr>
<tr>
<td>View batch report subscriptions</td>
<td>Yes</td>
</tr>
<tr>
<td>Browse old batch stored reports</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit data extract schedules and data sets</td>
<td>No</td>
</tr>
<tr>
<td>View data extract schedules and data sets</td>
<td>Yes</td>
</tr>
<tr>
<td>Auto Management Engine for checking and changing passwords.</td>
<td>No</td>
</tr>
<tr>
<td>Function</td>
<td>Available during failover</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Apply a patch</td>
<td>Yes</td>
</tr>
<tr>
<td>Generate Web Certificate Request</td>
<td>Yes</td>
</tr>
<tr>
<td>Upload TPAM Trusted CA certificate</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit Sybase and MySQL trusted root certificates</td>
<td>No</td>
</tr>
<tr>
<td>Edit Daily Maintenance Agent start time</td>
<td>No</td>
</tr>
<tr>
<td>Add, edit or delete an archive server</td>
<td>No</td>
</tr>
<tr>
<td>Add or remove a cluster member</td>
<td>No</td>
</tr>
<tr>
<td>Add, edit or delete external authentication settings</td>
<td>No</td>
</tr>
<tr>
<td>Edit Global Settings</td>
<td>No</td>
</tr>
<tr>
<td>Edit license counts</td>
<td>No</td>
</tr>
<tr>
<td>Edit Login Banner</td>
<td>Yes</td>
</tr>
<tr>
<td>Add, edit or delete message of the day</td>
<td>Yes</td>
</tr>
<tr>
<td>Add, edit or delete password rules</td>
<td>No</td>
</tr>
<tr>
<td>Add, edit or delete reason codes</td>
<td>No</td>
</tr>
<tr>
<td>Edit SysLog configuration settings</td>
<td>No</td>
</tr>
<tr>
<td>Create a support bundle</td>
<td>Yes</td>
</tr>
<tr>
<td>Add new ticket system</td>
<td>No</td>
</tr>
<tr>
<td>Edit existing ticket systems</td>
<td>Yes</td>
</tr>
<tr>
<td>Revert from a restore point</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The mail agent must be started to continue automatic email notifications.

**Automatic failback**

When a failed over replica re-establishes contact with the primary it starts the failback timer. If the replica continues to be communicating with the primary when the failback timer expires then automatic failback to the primary occurs. The amount of time the replica uses for its failback timer is entered in the failback timeout field.

During the automatic failback the replica that is failing back will experience a system outage while the failback process synchronizes the data between the appliances.
NOTE: The process to failback and synchronize the data on the replica with the primary takes several minutes. If you have trouble checking the status of the replica once the failback has started, wait a few minutes and check back again.

Change the run level

To change the run level of an appliance:

1. Select System Status/Settings | Cluster Management from the menu.
2. Select the Run Level check box.
3. Select Maintenance or Operational from the Run Level list.
4. Click the Change Run Level button.
5. Click the Continue with Change button.

When the appliance is in maintenance mode the following applies:

- Users cannot log on to the tpam interface.
- In the admin interface access to the mail settings, automation engine settings, agents, archive log settings, and re-submission of batch reports are disabled while in maintenance mode.

Force a failover

It is possible to force a failover to another cluster member. Forcing a failover can be useful during disaster recovery testing or if there is a scenario where the primary appliance has failed and none of the replicas are configured for automatic failover.

A failover can be forced by logging on to the /admin interface of the primary or by logging on to the /admin interface of the cluster member you want to force a failover to. When a failover is forced the following conditions exist in the cluster environment:

- The primary is STILL the authoritative primary.
- The appliance that has the forced failover mode is no longer receiving replication from the authoritative primary.
- With an appliance in forced failover mode TPAM users can log on to the authoritative primary OR the failed over appliance to create requests, retrieve passwords or start or replay sessions.
- The forced failover appliance will not automatically failback, according to the failback settings. The Un-force Failover button has to be clicked to reverse the failover. See Unforce a failover on page 61 for more details.
To force a failover from the primary appliance:

1. Logon to the /admin interface of the primary appliance.
2. Select System Status/Settings | Cluster Management from the menu.
3. Select the cluster member to force the failover to.
4. Click the Force Failover button.
5. Click the Continue with Change button on the confirmation window.
6. Click the Cluster Status tab to verify that the appliance has the mode of “FailedOver”. This may take a few minutes. Click the Cluster Status tab to refresh the page.

Unforce a failover

Once a failover is un-forced, any activity in TPAM that took place on the failed over appliance will be synchronized with the primary and then replicated to other cluster members as part of the failback processing job.

**IMPORTANT:** The process to un-force a failover and synchronize the data on the replica with the primary takes several minutes. If you have trouble checking the status of the replica once the failover has been unforced, wait a few minutes and check back again.

To un-force a failover:

1. Log on to the /admin interface of the primary appliance.
2. Select System Status/Settings | Cluster Management from the menu.
3. Select the cluster member that is currently failed over.
4. Click the Un-force Failover button.
5. Click the Continue with Change button. This kicks off the Failback timeout count down, so the failback will not start processing till the count down completes. Wait several minutes to allow the un-force failover processes to complete, eventually the replica will return to a replication status of standby.

Transfer authoritative primary

The transfer authoritative primary function is used when you want to switch the primary role from one cluster member to another. This should only be used when the original primary member is up and running.
To transfer the primary role to another console in the cluster:

1. Log on to the /admin interface of the primary.
2. Make sure the primary is selected in the cluster member list.
3. Select the Run Level check box.
4. Select Maintenance from the list.
5. Click the Change Run Level button.
6. Click the Continue with Change button.
7. Select the replica from the cluster member list that you want to transfer the primary role to.
8. Select the Run Level check box.
9. Select Maintenance from the list.
10. Click the Change Run Level button.
11. Click the Continue with Change button.
12. Click the Transfer Author. Primary button.
13. Click the Continue with Change button. The role of the replica will automatically change to “Primary” and the original primary will automatically have it’s role changed to “Replica”. Any other replicas in the cluster will automatically recognize the new primary.
14. Select the former primary from the cluster member list.
15. Select the Run Level check box.
16. Select Operational from the list.
17. Click the Change Run Level button.
18. Log on to the /admin interface of the new primary.
19. Select the Run Level check box.
20. Select Operational from the list.
21. Click the Change Run Level button.

Take over as authoritative primary

The take over authoritative primary function should be used when the primary has failed, is not going to be brought back up, and there are multiple replicas in the cluster.

To have a replica take over as authoritative primary:

1. Log on to the /admin interface of the replica that will become the new primary.
2. Select System Status/Settings | Cluster Management from the menu.
3. Make sure the replica is selected in the cluster member listing.
4. Select the Run Level check box.
5. Select Maintenance from the list.
6. Click the Change Run Level button.
7. Click the Take Over Author. Primary button.
8. Click the Continue with Change button.
9. Once the role of this appliance changes to Primary, select the Run Level check box.
10. Select Operational from the list.
11. Click the Change Run Level button.
12. Refresh the page. If the old primary is still appearing in the Cluster Members list, select it in the list and click the Remove Cluster Member button.
13. In the pop up box that appears select Remove and Retain data.
14. Next you must log on to the /admin interface of any other replica/s in the cluster to recognize the new primary. Select System Status/Settings | Cluster Management from the menu.
15. Select the replica you are logged on to from the cluster member list.
16. Select the Run Level check box.
17. Select Maintenance from the list.
18. Click the Change Run Level button.
19. Select the new primary from the cluster member list.
20. Click the Recognize New Author. Primary button.
21. Select the replica you are logged on to from the cluster member list.
22. Select the Run Level check box.
23. Select Operational from the list.
24. Click the Change Run Level button.

TIP: Give the replica a few minutes to save settings and then refresh the page. The old "original primary" should disappear from the cluster member list.

25. Repeat steps 14-23 for any additional replicas.

Any DPAs that were part of the original cluster should still be there and operating as normal with the "new" primary. No additional configuration is needed for the DPAs.

Any cache servers configured should also be operational without any additional configuration.

To add the replacement appliance into the cluster as a replica:

1. Turn on the replacement appliance.
2. Log on to it’s admin interface. Select System Status/Settings | Cluster Management from the menu.
3. Select the **Run Level** check box.
4. Select **Maintenance** from the list.
5. Click the **Change Run Level** button.
6. Log on to the admin interface of the new primary.
7. Select **System Status/Settings | Cluster Management** from the menu.
8. Click the **New Cluster Member** button.
9. Enter the name for the new replica.
10. Enter the network address of the old primary.
11. Click the **Check Address** button.
12. Select **Replica** from the role list.
13. Enter the failover timeout.
14. Enter the failback timeout.
15. Click the **Save** button. You will see a message that “Appliance at address x.x.x.x is not yet registered in the cluster.”
16. Click the **Make Enrollment Bundle** button. This generates the key file that will be used to communicate with the replica.
17. Click the **Continue with Change** button.
18. You will be prompted to save the enrollment bundle file. Click the **OK** button and save the file locally.
19. Log on to the /admin interface of the new replica appliance.
20. Select **System Status/Settings | Cluster Management** from the menu.
21. Click the **Select File** button.
22. Click the **Browse** button. Select the enrollment bundle file.
23. Click the **Upload** button.
24. Click the **Apply** button.
25. Click the **Continue with Change** button.
26. Log off the replica appliance or close the browser.

**NOTE:** You may receive an error logging off depending on where the replica is in the enrollment process. This error can be ignored.

27. On the primary appliance select **System Status/Settings | Cluster Management** from the menu.
28. Select the replica in the cluster member list. Wait for the replica run level to change from Unknown to Maintenance, then proceed to the next step.

**NOTE:** To refresh the page click the Details tab.
NOTE: The replica may be visible in the cluster list but its status may be unknown for quite some time until it has fully enrolled with the primary. The time it takes to complete enrollment is dependent on the size of the backup being applied to the replica from the primary.

29. Select the Run Level check box.
30. Select Operational from the Run Level list.
31. Click the Change Run Level button.

To make the replacement appliance the primary once it has been added to the cluster as a replica:

1. See the procedure for Transfer authoritative primary on page 61.

How to change the replication interval

To change the replication interval:

1. On the primary appliance select System Status/Settings | Global Settings from the menu.
2. Select Replication as the Category Filter.
3. Change the replication interval setting and click the Save Changes button.
4. Select System Status/Settings | Cluster Management from the menu.
5. Select the primary in the cluster member list.
6. Click the Restart Clustering button.
Archive Servers

Introduction

Archive servers provide an external storage location for logs and offline backup files from TPAM.

Configure archive servers

To configure an archive server:

1. Select System Status/Settings | Archive Servers from the menu.
2. Click the Add Server button.

The table below explains the options on the archive server management page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>The unique server name.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Network Address</td>
<td>The IP address or fully qualified domain name.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Archive Method</td>
<td>Select one of the following archive methods:</td>
<td>Yes</td>
<td>FTP</td>
</tr>
<tr>
<td></td>
<td>- FTP - lets the data be transmitted to any FTP server. Because the backup file is encrypted using AES256, there is not a security risk for the data, however authentication credentials may be exposed on the network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Required?</td>
<td>Default</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>sFTP using password</td>
<td>- let the data be transmitted to an sFTP server. In addition to the file encryption protection, the authentication credentials are also protected from network exposure.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCP using DSS Key</td>
<td>- the most secure transport method, data is transmitted through SCP (secure copy) with an encrypted SSH tunnel from TPAM to the archive server. The SCP method uses a public/private key pair for authentication. Supported keys are OpenSSH and SECSH keys. To complete the setup of the archive server for SCP communication, download the required public key using the Get Open SSH or Get Sec SSH button and store the key in the proper location on the archive server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Port number for TPAM to use.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>DSS Key Details</td>
<td>When using DSS key authentication, a function is available to permit specific configuration of the public/private keys used.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Avail. System Std. Keys</strong> – uses the single standard SSH keys (either Open SSH or the commercial key) stored centrally on TPAM. You have the ability to have up to three active keys simultaneously. These keys are configured in the paradmin interface. Use the list to select the key you want to retrieve.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** When using the **Avail.**
Field | Description | Required? | Default
---|---|---|---
**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 2084bit or 1024bit` buttons, and then downloaded in either Open SSH or Sec SSH (commercial) format.

The public key must be placed into the proper directory on the archive server. For most systems this is `[user’s home directory]/.ssh` (create the directory if it does not exist). The public key must also be specified as an authorized authentication method for the functional account. A new DSS key pair can be generated at any time (if for example it is felt that the existing keys have been compromised). Clicking the **Regen Key Pair** button generates a new public/private key pair.

The **Regen Key Pair** only regenerates the system specific key for the selected archive server, so only that archive server is affected.

Account Name | Used to authenticate to the archive server, and within whose home directory the logs are stored. | Yes | |
Path to Storage | Enter the full path as required for the storage location on the archive server. | Yes | |
Description | Descriptive text for the archive server. | No | |

3. Enter the settings and click the **Save Changes** button.
The connection and authentication between TPAm and the archive server can be tested by clicking the **Test** button.

To clear the existing host keys for the archive server from the TPAM appliance click the **Clear Host Entry** button.
Introduction

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

Sys-Admin activity log

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

To view the Sys-Admin Activity Log:

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

Security log

The security log reports any events related to log on activity. Only failed events are displayed to conserve resources. The security log displays server time (UTC).
To view the Security Log:
1. Select Logs | Security Log from the menu.
2. Enter your search criteria on the report filter tab.
3. Use one of the following methods to view the results:
   - Click the Report tab
   - Click the Export to Excel button
   - Click the Export to CSV button

Firewall log

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

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

Database log

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

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

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

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

Proc log

The Proc log displays information on cluster replication, software updates, batch report processing and system services. The proc log data can be displayed in server time (UTC) or the user’s local time zone, whichever they select on the Report Filter tab.

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

Starling Monitor log

The Starling Monitor log reports errors in the Starling Monitor jobs and can be used by technical support to troubleshoot problems with Approval Anywhere and Startling Join.

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

Archive log settings

Logs are maintained and stored on TPAM for the duration of the retention period configured in global settings. Log data is purged daily, based on these settings. To retain purged log data you have the option to send this data to an archive server prior to the purge.

To configure archive settings for logs:
1. Select System Status/Settings | Archive Log Settings from the menu.
2. Check the Enabled? box to enable the setting.
3. Select an archive server from the list. See Configure archive servers on page 66 for more details if needed.
4. Select All or Failed from the list and enter an email address for notifications. (Optional)
5. Click the Save Settings button.

SysLog configuration

TPAM allows the optional configuration of the sys-admin activity report and the user activity report to be transmitted to up to three syslog servers. This provides an alternate way to view activity reports as well as to monitor the TPAM appliance health and welfare.

To configure the reports to be sent to syslog servers:
1. Select System Status/Settings | SysLog Configuration from the menu.
2. Enter the IP address for the primary syslog server.
3. Enter the Port number.
4. Select Enable Syslog for Sys-Admin Activity Log to send this report to the syslog server.
5. Select Enable Syslog for User Activity Log to send this report to the syslog server.
6. Select Enable Syslog for Failed Logins to send this report to the syslog server.
7. Select Include **Source: ApplianceName in the syslog message?** to differentiate logs from different cluster members. The appliance name is pulled from the name on the cluster management page.

8. Select **Password Changes?** to send post-release resets to the syslog server.

9. Enter the IP address and port number for any additional syslog servers.

10. Click the **Save Settings** button.
Reason Codes

Introduction

Reason codes can be configured for requestors and ISAs to use when making a file, password or session request. To enable reason codes make sure that the reason code global settings have been set to Optional or Required. For more information on these global settings see Descriptions.

Add a reason code

To add a reason code:

1. Select System Status/Settings | Reason Codes from the menu.
2. Click the New Code button.
3. Enter a unique name for the reason code.
4. Enter a description for the reason code. (Optional)
5. Clear the Reason Code is active? check box if you do not want the reason code immediately available as a choice for requestors. (Optional)
6. Click the Save Changes button.

The reason code will now be available for requestors to select when making requests in the /tpam interface.

Delete a reason code

Reason codes can only be deleted if they have not been used on any requests. If the reason code was used but all those requests have aged out of TPAM based on the global setting retention period, then it may also be deleted.
To delete a reason code:
1. Select System Status/Settings | Reason Codes from the menu.
2. Select the reason code from the list to be deleted.
3. Click the Delete Code button.
4. Click the OK button on the confirmation window.

Enable/Disable a reason code

A reason code can be disabled so that it not available for requestors and ISA’s to use on requests, but not deleted, so it can be enabled in the future.

To enable/disable a reason code:
1. Select System Status/Settings | Reason Codes from the menu.
2. Select the reason code from the list.
3. Clear/Select the Reason Code is active? check box.
4. Click the Save Changes button.
Global Settings

Introduction

Global settings are used to maintain many key controls and parameters in TPAM. The number displayed in the Setting column represents the value set for the Option Name. You can narrow down the view of global settings on the page by using the Category Filter at the top of the page.

Edit global settings

To view and edit global settings:

1. From the /admin interface, select System Status/Settings | Global Settings from the menu.
2. To narrow the global settings displayed, select a choice from the Category Filter list.
3. Use the scroll bar to locate the global setting.
4. Enter the value in the Setting column, select the desired button in the setting column, or select the a value from the list. Repeat this step for each global setting to be edited.
5. Click the Save Changes button.

Descriptions

The table below provides a description of each global setting and the configurable parameters.
<table>
<thead>
<tr>
<th>Category</th>
<th>Option name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Login Control</td>
<td>Account Lockout Duration</td>
<td>The time (in minutes) that an account remains locked. Valid entries are 10 - 9999. A setting of 9999 requires an administrator to manually unlock the account. The minimum value of this setting is controlled by the current setting of the Lockout Window.</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> If you are going to require an administrator to manually unlock accounts, create a CLI Administrator ID and a CLI System Administrator ID, in the event that the parmaster and paradmin accounts get locked.</td>
<td></td>
</tr>
<tr>
<td>Account Login Control</td>
<td>Account Lockout Threshold</td>
<td>The number of consecutive failures within the lockout window required to lock a user account. Valid entries are 0 - 100. A value of 0 (zero) indicates the user’s account will never be locked due to failed logins. A value of 1 means that a single failed login attempt will lock an account.</td>
<td>5</td>
</tr>
<tr>
<td>Account Login Control</td>
<td>Account Lockout Window</td>
<td>The duration (in minutes) that failed logon attempts are counted. Valid entries are 0 - 15. The maximum value of this setting is controlled by the current setting of the lockout duration. A value of 0 (zero) means that there is no time limit to tracking failed logon attempts. All failed attempts will be counted until logon is successful or the account becomes locked.</td>
<td>10</td>
</tr>
<tr>
<td>Account Login Control</td>
<td>Allow 1024 bit key length for regenerated user key</td>
<td>User keys generated prior to 2.5.913 are 1024 bits. If Yes is selected they will continue to be generated as 1024. If No is selected they will continue to be generated as 1024.</td>
<td>No</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>selected keys generated will be 2048.</td>
<td></td>
</tr>
<tr>
<td>Account Login</td>
<td>Allow Multiple Sessions</td>
<td>If <strong>Yes</strong> is selected, users can have multiple browser sessions using the same user ID. If <strong>No</strong> is selected, each user ID may have only one authenticated session.</td>
<td>Yes</td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Login</td>
<td>Certificate User Identification</td>
<td>For user ID’s using a primary authentication type of <strong>Certificate</strong> this setting determines if the user is linked to the certificate through the thumbprint or the value of the subjectAltName:PrincipalName attribute in the certificate.</td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td><strong>NOTE:</strong> This setting affects ALL user ID’s using certificate authentication. <strong>Make sure you have at least one administrator and system administrator user ID setup without certificate authentication to make these updates.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Login</td>
<td>Disable after Inactive for n Days</td>
<td>Possible values are between 14 - 365 in days. If a user has not logged onto TPAM in this number of days, the user ID is disabled.</td>
<td>365</td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td><strong>NOTE:</strong> This setting only applies to local user IDs, not for externally primary authenticated users.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Login</td>
<td>Inform User of bad password</td>
<td>If <strong>Yes</strong> is selected, users will be told if they enter an invalid password when logging in. If <strong>No</strong> is selected, the user will be told that the username and/or password is invalid.</td>
<td>No</td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td>When both Inform User of bad password AND Inform User of bad password is <strong>Yes</strong>, users will be told that the password is invalid.</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>failed login attempts are both set to Yes, the user is informed that the password is invalid along with the number of failed logon attempts thus far.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> For security reasons we recommend leaving this set to <strong>No</strong>, unless you are troubleshooting login and authentication problems.</td>
<td></td>
</tr>
<tr>
<td>Account Login</td>
<td>Inform User of disabled account</td>
<td>If <strong>Yes</strong> is selected, users will be told if their account is disabled when they attempt to login. If <strong>No</strong> is selected, the user will be told that the username and/or password is invalid.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> For security reasons we recommend leaving this set to <strong>No</strong>, unless you are troubleshooting login and authentication problems.</td>
<td></td>
</tr>
<tr>
<td>Account Login</td>
<td>Inform User of failed login attempts</td>
<td>If <strong>Yes</strong> is selected, the system will display to the user the number of failed login attempts that have been made on their user ID since their last login.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> For security reasons we recommend leaving this set to <strong>No</strong>, unless you are troubleshooting login and authentication problems.</td>
<td></td>
</tr>
<tr>
<td>Account Login</td>
<td>Inform User of locked account</td>
<td>If <strong>Yes</strong> is selected, the user will be informed when attempting to login that their account is locked. If <strong>No</strong> is selected, the user will be told that the username and/or password is invalid.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> For security reasons we recommend leaving this set to <strong>No</strong>, unless you are troubleshooting login and authentication problems.</td>
<td></td>
</tr>
<tr>
<td>Account Login</td>
<td>Login token</td>
<td>The number of seconds a user can</td>
<td>300</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Control</td>
<td>lifespan</td>
<td>remain inactive on the login page before they are forced to refresh the page to login. Valid entries are 60-600.</td>
<td></td>
</tr>
<tr>
<td>Account Login Control</td>
<td>Maximum Password Age</td>
<td>Specifies the maximum time between password changes (in days). Valid entries are 0 – 180.</td>
<td>42</td>
</tr>
<tr>
<td>Account Login Control</td>
<td>Minimum Password Age</td>
<td>Specifies the minimum time between password changes (in days). Valid entries are 0 – 180.</td>
<td>0</td>
</tr>
<tr>
<td>Account Login Control</td>
<td>Password Grace Period</td>
<td>The number of days, prior to a user’s password expiring, that they will be reminded that their password will expire in X days. A setting of 0 means no warnings will be given. Valid entries are 0-30.</td>
<td>14</td>
</tr>
<tr>
<td>Account Login Control</td>
<td>Password History</td>
<td>Number of old passwords stored by TPAM for user accounts. Stored passwords may not be reused, and are replaced on a first-in first-out basis. Valid entries are 0 – 24.</td>
<td>5</td>
</tr>
<tr>
<td>Account Login Control</td>
<td>Session Inactivity Timeout</td>
<td>Time, in minutes, that a user’s session will time out after inactivity. Valid entries are 10-2880.</td>
<td>2880</td>
</tr>
<tr>
<td>Browser Window</td>
<td>Admin Interface default window size</td>
<td>Select a default screen resolution size from the list for the /admin interface.</td>
<td>1024x768</td>
</tr>
<tr>
<td>Browser Window</td>
<td>Admin Interface in new window</td>
<td>Select a default screen resolution size from the list for the /config interface.</td>
<td>No</td>
</tr>
<tr>
<td>Browser Window</td>
<td>Config Interface default window</td>
<td>Select a default screen resolution size from the list for the /config interface.</td>
<td>1024x768</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>size interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Browser Window</td>
<td>Config Interface in new window</td>
<td>If <strong>Yes</strong> is selected, a new browser window will be opened when a user logs on to the /config interface. Also the browser window will automatically close upon log out. If <strong>No</strong> is selected, the user can browse in the window they currently have open. The user must manually close the browser window when logging off.</td>
<td>No</td>
</tr>
<tr>
<td>Browser Window</td>
<td>Main Interface default window size</td>
<td>Select a default screen resolution size from the list for the /tpam interface.</td>
<td>1024x768</td>
</tr>
<tr>
<td>Browser Window</td>
<td>Main Interface in new window</td>
<td>If <strong>Yes</strong> is selected, a new browser window will be opened when a user logs on to the /tpam interface. Also the browser window will automatically close upon logging off. If <strong>No</strong> is selected, the user can browse in the window they currently have open. The user must manually close the browser window when logging off.</td>
<td>No</td>
</tr>
<tr>
<td>Custom Column Names</td>
<td>Managed Account Custom 1-6</td>
<td>Six custom boxes available to track account information. If configured these appear on the Account Custom Information tab and are listed as filter options on many filter tabs. Column names are limited to 32 characters, cannot be the same as any other Custom column name nor any existing column in the Accounts table. Must consist of only upper or lowercase letters, numbers, spaces, periods, hyphens, and underscores. A custom column name may be “undefined” by simply erasing the value.</td>
<td>Null</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Custom Column Names</td>
<td>Managed System</td>
<td>Six custom boxes available to track system information. If configured these appear on the System Custom Information tab and are listed as filter options on many filter tabs. Column names are limited to 32 characters, cannot be the same as any other Custom column name nor any existing column in the Systems table. Must consist of only upper or lowercase letters, numbers, spaces, periods, hyphens, and underscores. A custom column name may be “undefined” by simply erasing the value.</td>
<td>Null</td>
</tr>
<tr>
<td></td>
<td>Custom1-6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Column Names</td>
<td>User Custom</td>
<td>Six custom boxes available to track user information. If configured these appear on the User Custom Information tab and are listed as filter options on many filter tabs. Column names are limited to 32 characters, cannot be the same as any other Custom column name nor any existing column in the Users table. Must consist of only upper or lowercase letters, numbers, spaces, periods, hyphens, and underscores. A custom column name may be “undefined” by simply erasing the value.</td>
<td>Null</td>
</tr>
<tr>
<td></td>
<td>1-6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Any data entered while the custom column name is defined is inaccessible if the custom name is undefined.
<table>
<thead>
<tr>
<th>Category</th>
<th>Option name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Specified</td>
<td>Appliance Identity</td>
<td>Custom box available to name the appliance. This box is used on the Appliance Usage Batch Report.</td>
<td>Null</td>
</tr>
<tr>
<td>Customer Specified</td>
<td>Auto Discovery Reprocessing Delay</td>
<td>Number of hours TPAM will delay reprocessing auto discovery mapping errors.</td>
<td>24</td>
</tr>
<tr>
<td>Customer Specified</td>
<td>Hide Retrieved Passwords</td>
<td>In order to prevent over the shoulder exposure of retrieved passwords the displayed password can optionally be hidden so that is can be copied to a clipboard without revealing it to passerby. When the password is hidden the user can copy it to the clipboard by moving the mouse in the designated area and typing Ctrl-C. The options are as follows:</td>
<td>Never</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Never</strong> - the password is displayed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Hide, but allow password to be revealed</strong> - the password is hidden when retrieved but clicking the <strong>Reveal Password</strong> button will display it.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Always hide the retrieved password</strong> - the password is hidden and must be copied to the clipboard.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> Even if the password is hidden from view it is still considered “Released”.</td>
<td></td>
</tr>
<tr>
<td>Customer Specified</td>
<td>Log All CLI, API and CLIA calls</td>
<td>Adds additional logging to the Activity and Sys-Admin activity</td>
<td>None</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Logs</td>
<td></td>
<td>logs with information about all CLI, API, and CLIA calls made to the database. Logs include how the call was made (CLI or API), the CLI verb invoked, the user issuing the call, duration of the call, and the number of rows returned if the call is a list command.</td>
<td></td>
</tr>
<tr>
<td>Customer Specified</td>
<td>Max Attachment Size (MB)</td>
<td>The maximum total size (in megabytes) of batch report output files that can be sent to a user in a single email. When the user subscribes to more than one output file from a report this is the total size of all files to be attached. A message will be attached to the email body if one or more files cannot be attached due to this limit. Enter 0 (zero) for unlimited attachment size.</td>
<td>0</td>
</tr>
<tr>
<td>Customer Specified</td>
<td>System Date Format</td>
<td>System Date Global Setting that controls the default input and output date and time formats for the entire appliance. Choices are &quot;Month/Day/Year hh:mm AM/PM&quot; or &quot;Day/Month/Year hh:mm24&quot;.</td>
<td>Month/Day/Year</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> If this setting is changed all users must refresh their browsers or they may encounter a session time out error.</td>
<td></td>
</tr>
<tr>
<td>Global Groups</td>
<td>Allow Global Groups to be used for Permissioning</td>
<td>If <strong>No</strong> is selected, then Global Groups do not appear on the Group Listing and Group Membership assignment tab and are not used to determine permissions. For performance reasons, if Global Groups are not used, it is recommended that this setting be set at <strong>No</strong>.</td>
<td>No</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Individual Accountability</td>
<td>Allow Account specific override</td>
<td>If <strong>Yes</strong> is selected, individual accountability can be turned off at the account level, letting more than one requestor request this password at the same time or during an overlapping duration. Changing this value to <strong>No</strong> removes this from all accounts that were enabled in the TPAM interface.</td>
<td><strong>No</strong></td>
</tr>
<tr>
<td>Mobile Device</td>
<td>Allow Password Retrieval</td>
<td>This setting controls if mobile device users of TPAM are permitted to retrieve passwords on their mobile device.</td>
<td><strong>Yes</strong></td>
</tr>
<tr>
<td>Mobile Device</td>
<td>Quick Approve Text</td>
<td>Custom text you can enter that appears as the Password Approval Reason when approving a request from a mobile device. This message is used if the Approver uses the Quick Approve functionality or does not enter a message when approving a request.</td>
<td>Quick Approved from Mobile Device</td>
</tr>
<tr>
<td>Mobile Device</td>
<td>Quick Deny Text</td>
<td>Custom text you can enter that appears as the Password Denial Reason when denying a request from a mobile device. This message is used if the Approver uses the Quick Deny functionality or does not enter a message when denying a request.</td>
<td>Quick Denied from Mobile Device</td>
</tr>
<tr>
<td>Mobile Device</td>
<td>Quick Expire Text</td>
<td>Custom text you can enter that appears as the Password Cancellation/Expiration Reason when canceling/expiring a request from a mobile device. This message is used if the Requestor uses the Quick Expire functionality or does not enter a message when expiring a request.</td>
<td>Quick Cancel/Expire from Mobile Device</td>
</tr>
</tbody>
</table>

**IMPORTANT:** If **Yes** is selected, partitions cannot be enabled.
<table>
<thead>
<tr>
<th>Category</th>
<th>Option Name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Device</td>
<td>Quick Submit Text</td>
<td>Custom text you can enter that appears as the Password Request Reason when submitting a request from a mobile device. This message is used if the Requestor uses the Quick Submit functionality or does not enter a message when submitting a request.</td>
<td>Quick Submit from Mobile Device</td>
</tr>
<tr>
<td>Old Password Retention</td>
<td>Failed Password Days</td>
<td>Specifies the number of days that TPAM retains failed passwords. Valid entries are 1 – 90.</td>
<td>15</td>
</tr>
<tr>
<td>Old Password Retention</td>
<td>Minimum Retention Days</td>
<td>Specifies the least number of days that TPAM stores old passwords. Valid entries are 1 – 360.</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> If Past Passwords and Minimum Retention Days are configured differently, both conditions must be satisfied before a password is deleted from history.</td>
<td></td>
</tr>
<tr>
<td>Old Password Retention</td>
<td>Past Passwords</td>
<td>The number of previous passwords that TPAM stores for a managed system. Valid entries are 1 – 30.</td>
<td>5</td>
</tr>
<tr>
<td>Old Password Retention</td>
<td>Purge Password Batch Size</td>
<td>To minimize the performance impact for other interactive users this setting controls the number of passwords deleted in each transaction during the purge password portion of the Daily Maintenance process. Valid entries are 5-100.</td>
<td>10</td>
</tr>
<tr>
<td>Online Backups</td>
<td>Online Backups</td>
<td>The number of TPAM backups that are stored locally. Valid entries are 1 – 10.</td>
<td>5</td>
</tr>
<tr>
<td>PSM Session</td>
<td>Max Session Duration (Hours)</td>
<td>The allowed duration (in hours) for a PSM Session. A job runs every 10 minutes that terminates any sessions that are exceeding this threshold. A value of 0 lets sessions run with no time limit.</td>
<td>0</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Partitions</td>
<td>Max Partitions</td>
<td>The total number of partitions that can be created.</td>
<td>50</td>
</tr>
<tr>
<td>Partitions</td>
<td>Partition Admins</td>
<td>This setting controls whether partition administrators can add new users or only assign existing users to partitions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- create new partition users, but not partition administrators</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- create new partition users and partition administrators</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- only assign existing users</td>
<td></td>
</tr>
<tr>
<td>Partitions</td>
<td>Partition Method</td>
<td>Enterprise - partitions can be created by Administrators.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Administrators have access to all partitions. Basic users may be granted access to one or more partitions. Partition administrators may only manage a single partition.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No partitions allowed - partitions and partition administrators can not be created.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IMPORTANT: If Global Groups are enabled, then partitions cannot be created.</td>
<td></td>
</tr>
<tr>
<td>PSM Session</td>
<td>Maximum Recording Size</td>
<td>Maximum size in megabytes a session recording is allowed to reach. Warning messages will start when the session reaches 60% of the set limit. The session will be terminated when it reaches the size limit. Any sessions greater than 800 MB should be hosted through a DPA.</td>
<td>500</td>
</tr>
<tr>
<td>PSM Session</td>
<td>Replay all sessions before completing</td>
<td>Setting this value to Yes will require that the reviewer replay all the session logs before a review</td>
<td>No</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>review</td>
<td>can be completed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSM Session</td>
<td>Session Termination Wait Time</td>
<td>The maximum amount of time, in seconds, before TPAM will terminate a session as a result of a run level change on appliance, or during a failback to a primary appliance.</td>
<td>300</td>
</tr>
<tr>
<td>PSM Session</td>
<td>Session Termination Warning Interval</td>
<td>The number interval in seconds, that TPAM will warn users that a session is getting ready to terminate, up until the session is terminated.</td>
<td>60</td>
</tr>
<tr>
<td>Replication</td>
<td>Database Backup Set Max Incr Usage MB</td>
<td>The maximum amount of disk space (in megabytes) that TPAM will use for incremental database backups. Incremental database backups are only used for replication and not related to a TPAM backup.</td>
<td>1024</td>
</tr>
<tr>
<td>Replication</td>
<td>File Resynchronization Interval</td>
<td>The interval, in seconds, that a primary appliance will force a re-synchronization of replicated files, (session logs, report output, secure files, etc.) with each replica appliance.</td>
<td>3600</td>
</tr>
<tr>
<td>Replication</td>
<td>Replication Interval</td>
<td>The interval, in seconds, that the primary console will push</td>
<td>60</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>incremental updates to each replica appliance.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> Every time this value is changed you must go to the Cluster Management page, select the primary and click the <strong>Restart Clustering</strong> button.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requests</td>
<td>Allow unexpired requests to be extended</td>
<td>The number of times a password, file or session request can be extended. If Request Extensions are disabled, all other request extension related global settings are ignored. Options are:</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Request extensions are disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 1,2 or 3 extensions per request.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Unlimited extensions allowed per request.</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> Disabling request extensions will prevent future requests from being extended, but NOT affect existing requests with approved extensions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requests</td>
<td>Approvals required for request extensions</td>
<td>Requests which require approvals will follow the same approval rules for extensions, , including multi-group approval and password approval for PSM session that release the password. Requests which are auto-approved, will use existing permission data for approvals. Options are:</td>
<td>Only auto-approved requests can be extended..</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- only auto-approved requests can be extended, no approval required</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Requests</td>
<td>Detailed Reason Text for ISA Release</td>
<td>This setting controls if ISAs are required to enter a detailed reason when retrieving a password or file. Possible values are <strong>Required, Not Allowed</strong> and <strong>Optional</strong>.</td>
<td>Required</td>
</tr>
<tr>
<td><strong>NOTE:</strong> Setting this to <strong>Not Allowed</strong> or <strong>Optional</strong> and setting Reason Code for ISA Release to <strong>Not Allowed</strong> or <strong>Optional</strong> lets ISA’s retrieve passwords and files without entering a reason.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requests</td>
<td>Detailed Reason Text for Request</td>
<td>This setting controls whether a detailed request reason is required for any password, file or session request. Possible values are <strong>Required, Not Allowed</strong> and <strong>Optional</strong>.</td>
<td>Required</td>
</tr>
<tr>
<td><strong>NOTE:</strong> Setting this to <strong>Not Allowed</strong> or <strong>Optional</strong> and setting Reason Code for Release to <strong>Not Allowed</strong> or <strong>Optional</strong> lets requestors request passwords, files and sessions without entering a reason.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requests</td>
<td>Lockout period for approved extensions</td>
<td>When a request extension must be approved, this is the number of minutes prior to the current expiration date when a requestor may submit an extension for the</td>
<td>10</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Requests</td>
<td>Maximum time per extension</td>
<td>Maximum amount of time for allowed for extension request.</td>
<td>15 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> Requests cannot be extended if it will conflict with an approved request, and cannot be extended beyond the max duration set on the account and access policy.</td>
<td></td>
</tr>
<tr>
<td>Requests</td>
<td>Reason Code for ISA Release</td>
<td>This setting controls if ISAs are required to enter a reason code before they retrieve a password or file. Possible values are Required, Not Allowed and Optional.</td>
<td>Optional</td>
</tr>
<tr>
<td>Requests</td>
<td>Reason Code for Request</td>
<td>This setting controls if requestors are required to enter a reason code as they request a password, file or session. Possible values are Required, Not Allowed and Optional.</td>
<td>Optional</td>
</tr>
<tr>
<td>Requests</td>
<td>Require reason for extension</td>
<td>If Yes, the rules set in global settings for reasons will be followed. If No, the comments and reason code for extension will be optional, but not required.</td>
<td>Yes</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Account Discovery Agent Log</td>
<td>This setting controls the number of days that TPAM will store the Account Discovery Agent activity. Valid entries are 1-30.</td>
<td>30</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Activity Log</td>
<td>The number of days that TPAM stores log entries for TPAM activity events. Valid entries are 30 – 365.</td>
<td>90</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Alerts Log</td>
<td>The number of days that TPAM stores system generated alerts. Valid entries are 1-30.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Auto Discovery Agent Log</td>
<td>The number of days that TPAM stores the Auto Discovery Agent log entries. Valid entries are 1-30.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Backup Log</td>
<td>The number of days that TPAM stores backup activity logs. Valid entries are 10 – 365.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Batch Import-Update History (0 = Never Delete)</td>
<td>The number of days to retain Batch Import/Update history results, based on the date the batch was submitted, not completed, or canceled. A value of 0 means the results are never deleted. Valid entries are 0-999.</td>
<td>0</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Data Extract Log</td>
<td>The number of days that TPAM stores logs of data extract history. Valid entries are 1-90.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>DPA Server Activity Log</td>
<td>The number of days that TPAM stores DPA Server activity. Valid entries are 1-30.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>File Release Log</td>
<td>The number of days that TPAM stores file release activity logs. Valid entries are 30 – 365.</td>
<td>90</td>
</tr>
<tr>
<td>Retention Period</td>
<td>File Release Request</td>
<td>The number of days file release requests are retained before archival. Valid entries are 10-365.</td>
<td>90</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Firewall Log</td>
<td>The number of days that TPAM stores firewall activity logs. Valid entries are 1 – 90.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>ISA File Release Log</td>
<td>The number of days that TPAM stores ISA file activity release activity logs. Valid entries are 30-365.</td>
<td>90</td>
</tr>
<tr>
<td>Retention Period</td>
<td>ISA Release Log</td>
<td>The number of days that TPAM stores ISA file activity release activity logs. Valid entries are 30-365.</td>
<td>90</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Period</td>
<td></td>
<td>stores ISA password release activity logs. Valid entries are 30-365.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> Setting a lower retention period for the ISA Release Log affects how much data is available for the Password Release Log.</td>
<td></td>
</tr>
<tr>
<td>Retention Period</td>
<td>Mail Agent Log</td>
<td>The number of days that TPAM stores log entries for mail agent activity. Valid entries are 1 – 365.</td>
<td>10</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Online Batch Reports</td>
<td>The number of days that TPAM stores logs of scheduled batch job activity. Valid entries are 1 – 180.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Password Change Activity Detail</td>
<td>The number of days that TPAM stores detailed password change logs. Valid entries are 10 – 90.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Password Change Log</td>
<td>The number of days that TPAM stores password change activity logs. Valid entries are 30 – 365.</td>
<td>90</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Password Release Log</td>
<td>The number of days that TPAM stores password release activity logs. Valid entries are 30 – 365.</td>
<td>90</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Password Test Activity Detail</td>
<td>The number of days that TPAM stores detailed password test logs. Valid entries are 10 – 90.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Password Test Results</td>
<td>The number of days that success/failure results for automated password tests are retained. Valid entries are 10 – 90.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Post Session Processing Log (PSM customers only)</td>
<td>The number of days that TPAM stores post session processing logs. Valid entries are 1-365.</td>
<td>10</td>
</tr>
<tr>
<td>Retention Period</td>
<td>PSM Archive Log (PSM customers only)</td>
<td>The number of days that TPAM stores the PSM Archive Log, which reports on the success and failure of archiving sessions. Valid entries are 1-30.</td>
<td>5</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Pwd Change Agent Log</td>
<td>The number of days that TPAM stores password change agent activity logs. Valid entries are 10 – 90.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Pwd Test Agent Log</td>
<td>The number of days that TPAM stores password test activity logs. Valid entries are 10 – 90.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Release Request</td>
<td>The number of days password release requests are retained before archival. Valid entries are 10-999. A password release request will not be purged if it has uncompleted reviews, regardless of the age of the request.</td>
<td>90</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Security Log</td>
<td>The number of days that TPAM stores security event logs. Valid entries are 5 – 90.</td>
<td>10</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Sent Mail Log</td>
<td>The number of days that TPAM stores log entries for sent mail items. Valid entries are 1 – 365.</td>
<td>30</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Session Request (PSM customers only)</td>
<td>The number of days that session release requests are retained before archival. Valid entries are 10-2922. A session release request will not be purged if it has uncompleted session or password release reviews, regardless of the age of the request.</td>
<td>90</td>
</tr>
</tbody>
</table>

NOTE: Setting a lower retention period for the Release Request Log affects how much data is available for the Password Release Log.

NOTE: This setting limits the Max age in days for session log deletion in the PSM Archive Settings in the /tpam interface.
<table>
<thead>
<tr>
<th>Category</th>
<th>Option name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retention Period</td>
<td>Synchronized Password Change Log</td>
<td>The number of days that TPAM stores logs of synchronized password changes. Valid entries are 30-365.</td>
<td>90</td>
</tr>
<tr>
<td>Retention Period</td>
<td>Sys-Admin Log</td>
<td>The number of days that TPAM stores system administrator activity logs. Valid entries are 30 – 365.</td>
<td>90</td>
</tr>
<tr>
<td>Review Notification</td>
<td>Immediate Review Notification</td>
<td>If Yes is selected, a Review Requirement email is sent immediately, one email per review. If No is selected, emails are not sent for individual reviews, including the escalation emails configured at the account.</td>
<td>Yes</td>
</tr>
<tr>
<td>Review Notification</td>
<td>Periodic Review Notification Interval</td>
<td>Sends email notifications of uncompleted Session or Password Release reviews at the top of the hour, at the selected frequency. One email is sent per reviewer with as many uncompleted reviews that can fit in the body of the email. 1x/Day notifications are sent at midnight, server time. Reviewers are sent a single email notification when the review is required, and a single escalation email if so configured at the account. Setting both of the Review Notification settings to No and Disabled disables all Release Review emails.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Role Policy</td>
<td>Always use cached permission data</td>
<td>If No is selected, permissions are determined by querying the database to ensure the most up to date permissions are used, but this can slow down TPAM performance for customers with large data sets. If Yes is selected, the cached permissions data, that is updated every 60 seconds will be used to determine permissions. If Not for Password/File</td>
<td>No</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Retrieval and Session Start is selected, the most up to date data will be used to determine permissions for retrieving a password, file or starting a session, but the cached data will be used for all other permission calculations.</td>
<td>If Yes or Not for Password/File Retrieval and Session Start is selected it is recommended that Administrators and ISAs use the Rebuild Assigned Policies page in the /tpam interface after editing permissions to rebuild the cached permissions immediately.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Role Policy

#### Default new systems to no assigned ISA policy

If Yes is selected, when an administrator has one or more ISA access policies, and adds a new system the ISA policy will default to Do Not Assign an ISA policy.

**NOTE:** This global setting only affects systems added through the TPAM web interface. Not systems added through the API, CLI or batch import.

#### Ignore Policies includes collection membership

Changes the behavior of the Ignore System Access Policies check box when it is selected for an account.

If Yes is selected, the check box will ignore both system and collection level permission assignments which apply to the account’s parent system.

If No is selected, the check box will only ignore permissions assigned directly to the system. Permissions assigned to collections where the system is a member will still propagate to the account.

Default: No
<table>
<thead>
<tr>
<th>Category</th>
<th>Option name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
</table>
| Role policy | ISA and Admin access to past passwords           | Controls actions that occur when a TPAM Administrator, Partition Administrator or PPM ISA click on an account’s Past Password tab.  
  - No restrictions, log only when password is retrieved  
  - Warn before retrieving list of past passwords once per account retrieval  
  - Warn before retrieving list of past passwords every time  
  - No access to past passwords                                                                                                                             | No restrictions, log only when password is retrieved.                                       |
| Role Policy | Pause Rebuild Policies job during batch operations | The job which rebuilds the Assigned Policies data normally runs every 60 seconds and rebuilds the data whenever updates are detected. Some types of batch import or update jobs may trigger this rebuild process many times while they are running, as do Auto Discovery and Account Discovery. If the job starts while one of these processes it still modifying data it may slow down TPAM and put a strain on resources. This setting allows you to pause the rebuild job until the end of the batch process.  
The batch jobs and processes affected by this are: Import/Update Users, Systems, Accounts, Update Collection Membership, Update Permissions, LDAP and Generic Auto Discovery and Account Discovery.  
The settings are as follows:  
  - Never - the jobs will process updates as soon as they are detected.  
  - Only for updates triggered by the process itself - when one of the affected processes is | Never                                                                                       |
<table>
<thead>
<tr>
<th>Category</th>
<th>Option name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>running, all rebuilds triggered by updates from that process will be deferred until that process ends.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For all updates while a batch is running - while any of the affected batches are running ALL scheduled rebuilds will be deferred until the batch process has completed no matter what process performs the updates. An administrator or ISA can still force a rebuild by clicking the <strong>Run Now</strong> button in the tpam interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> If the <strong>Always use cached permission data</strong> global setting is set at <strong>Yes</strong> or <strong>Not for ....</strong>, we recommend leaving this setting at <strong>Never</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

<p>| Role Policy   | Require System and Account Name filters          | When administrators and ISAs have access to very large numbers of systems and accounts they may experience performance problems when doing unfiltered searches on the manage systems and manage accounts pages. If <strong>Yes</strong> is selected, they will be forced to enter a value for system and/or account name in order to retrieve a listing. | No      |
| Role Policy   | Restrict ISA System Creation                     | If <strong>Yes</strong> is selected, only Administrators can add systems.                                                                                                                                               | No      |
| Security Settings | Minimum TLS Version                          | This global setting applies to all inbound communication to the TPAM Web application, as well as the inter-appliance communication for all TPAM appliances in a cluster.                                       | 0       |</p>
<table>
<thead>
<tr>
<th>Category</th>
<th>Option name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0 - TLS 1.0-1.2</td>
<td>Outbound communication to managed targets will attempt to communicate using TLS 1.2 (where applicable), but can be permitted to negotiate down to lower levels if the target device does not support TLS 1.2. If ONLY TLS 1.2 is permitted then only these ciphers will be allowed:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 - TLS 1.1, 1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 - TLS 1.2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IMPORTANT:** Any time this setting is changed a reboot of the appliance is required for the setting to take effect for the primary AND replicas.
### IMPORTANT: DPA v3’s require a TLS setting of 0. TPAM will not allow you to set a TLS value of 1 or 2 if you have any DPA 3’s assigned to systems for PSM affinity. There is a DPA Affinity report in the /tpam interface to view DPA assignments.

<table>
<thead>
<tr>
<th>Category</th>
<th>Option name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trash Cleanup</td>
<td>Allow Manual Hard Deletes</td>
<td>If Yes is selected, hard deletes of systems and accounts are allowed regardless of how the Days in Trash global setting is set.</td>
<td>Yes</td>
</tr>
<tr>
<td>Trash Cleanup</td>
<td>Days in trash (0= never delete)</td>
<td>Specifies the number of days that TPAM retains deleted systems and deleted accounts. When set to zero they are not deleted. Valid entries are 0-999.</td>
<td>10</td>
</tr>
<tr>
<td>User Control</td>
<td>Allow User Self-Edit - Mapped Users</td>
<td>If Yes is selected, users brought into TPAM through auto discovery can edit their own contact information in TPAM. Users who are system administrators are not affected by this setting.</td>
<td>Yes</td>
</tr>
<tr>
<td>User Control</td>
<td>Allow User Self-Edit - Unmapped Users</td>
<td>If Yes is selected, users manually added or through batch update, can edit their own contact information in TPAM. Users who are system administrators are not affected by this setting.</td>
<td>Yes</td>
</tr>
<tr>
<td>User Control</td>
<td>Allow User Timezone Changes</td>
<td>If Yes is selected, the user can change their Time Zone in My Info/User Details. If No is selected, only an Administrator, Partition Administrator or User Admin can change a user’s Time Zone. This does not affect the Time Zone controls for System Administrators.</td>
<td>Yes</td>
</tr>
<tr>
<td>User Control</td>
<td>Default User Timezone</td>
<td>The default timezone for all new systems.</td>
<td>UTC</td>
</tr>
<tr>
<td>Category</td>
<td>Option name</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>102</td>
<td><strong>user ID’s in the /tpam and /admin interface. This value can be overwritten by a user template.</strong></td>
<td></td>
</tr>
</tbody>
</table>
Password Rules

Introduction

Password construction rules for managed systems are system and account specific. Two managed accounts on the same system can have different password rules assigned. If a system and account have different password rules the password rule assigned at the account level takes precedence. When creating a password rule make sure the password rules on the managed system match what is configured in TPAM.

Default password rule

Password rules govern the passwords that are generated by TPAM. TPAM is pre-configured with a default password rule that will appear in the listing. The default password rule can be modified to meet your needs but not deleted. The default password rule is also used for local user authentication so there are limitations on what values can be changed.

Add a password rule

To create a password rule:

1. Select System Status/Settings | Password Rules from the menu.
2. Click the New Rule button.
3. Enter a rule name.
4. Enter a description for the password rule. (Optional)
5. Enter values for the password rule definitions describes in the table below. If a password rule parameter turns orange then hover the mouse over the orange to read the recommended password rule warning.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Length</td>
<td>Specifies the shortest and longest password that can be generated. Valid entries are between 4-128.</td>
<td>6/10</td>
</tr>
<tr>
<td>Password Display Timeout</td>
<td>Specifies the number of seconds the password is displayed to requestor or ISA retrieving a password. Minimum is 5 seconds, maximum is 120 seconds.</td>
<td>20</td>
</tr>
</tbody>
</table>
| First Character Value | Specifies the properties for the first character of the password. Select from:  
  - Alpha characters only (not allowed if uppercase and lowercase not permitted)  
  - Any Character Permitted  
  - Alphanumeric Permitted | Any Character Permitted |
| Last Character Value  | Specifies the last character of the password. Select from:  
  - Alpha characters only (not allowed if uppercase and lowercase not permitted) | Any Character Permitted |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>permitted)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Any Character Permitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Alphanumeric Permitted</td>
<td></td>
</tr>
<tr>
<td>Uppercase Requirements</td>
<td>Specifies the use of uppercase characters within the password. Select from:</td>
<td>Require at least 1</td>
</tr>
<tr>
<td></td>
<td>- Not Permitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Permitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Require at least 1 - 5</td>
<td></td>
</tr>
<tr>
<td>Lowercase Requirements</td>
<td>Specifies the use of lowercase characters within the password. Select from:</td>
<td>Require at least 1</td>
</tr>
<tr>
<td></td>
<td>- Not Permitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Permitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Require at least 1 - 5</td>
<td></td>
</tr>
<tr>
<td>Numeric Requirements</td>
<td>Specifies the use of numeric characters in the password. Select from:</td>
<td>Require at least 1</td>
</tr>
<tr>
<td></td>
<td>- Not Permitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Permitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Require at least 1 - 5</td>
<td></td>
</tr>
<tr>
<td>Non-Alphanumeric Requirements</td>
<td>Specifies the use of non-alphanumeric characters in the password. Select</td>
<td>Not Permitted</td>
</tr>
<tr>
<td></td>
<td>from:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Not Permitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Permitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Require at least</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Valid Non-Alphanumeric</td>
<td>Specifies the non-alphanumeric characters in the password. This is only an option if Non-alphanumeric characters are Permitted. Choices are:</td>
<td>Null</td>
</tr>
<tr>
<td>Characters</td>
<td>• (blank space)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ~ (tilde)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ` (grave accent)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ! (exclamation mark)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• @ (at)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• # (pound)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• $ (dollar sign)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• % (percent)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ^ (carat)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• &amp; (ampersand)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• * (asterisk)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ( (open parenthesis)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ) (close parenthesis)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• _ (underscore)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• - (hyphen)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• + (plus sign)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• = (equals)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• { (open brace)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• } (close brace)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• [ (open bracket)</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td><img src="image_url" alt="Image" /></td>
<td><img src="image_url" alt="Image" /></td>
<td><img src="image_url" alt="Image" /></td>
</tr>
</tbody>
</table>

Invalid Characters

Designates alphanumeric characters that will not be allowed in the password. Examples would be uppercase I and lowercase L.

Password reuse (global)

Options are:

- Permitted - password generator can reuse a password
- Not Permitted - password generator will not reuse any account or synchronized account password for
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>as long as the passwords are retained. In order to enable this option the password minimum length must be at least 10, the max length at least 20, and must require at least 1 of each uppercase, lowercase, and numeric characters. Editing Min or Max Length may reset this to Permitted. This applies across all accounts and synchronized passwords that use this password rule. This applies only to passwords generated by TPAM. Passwords that have been manually typed in are used to prevent reuse, but a user will not be blocked from reusing an existing password. This only applies to generated passwords. It</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Password reuse per account</td>
<td>Options are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Permitted - password generator can reuse a password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Not Permitted - password generator will not reuse any account or synchronized account password for as long as the passwords are retained on a per-account basis. In order to enable this option the password minimum length must be at least 10, the max length at least 20, and must require at least 1 of each uppercase, lowercase, and numeric characters. Editing Min or Max Length may reset this to Permitted. This applies only to passwords generated by TPAM.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Permitted</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>passwords that have been manually typed in are used to prevent reuse, but a user will not be blocked from reusing an existing password. This only applies to generated passwords. It does not apply to user login passwords. This is per-account or synchronized password. It does not prevent the same password from being generated for multiple accounts or synchronized passwords.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consecutive Repeat Characters</td>
<td>Whether to allow a password with consecutive repeat characters. Case sensitive so aA is not considered repeating but AA would be.</td>
<td>Permitted</td>
</tr>
<tr>
<td></td>
<td>• Permitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Not Permitted</td>
<td></td>
</tr>
<tr>
<td>Nonconsecutive Repeat Characters</td>
<td>Whether to allow a password with any repeated characters anywhere in the password.</td>
<td>Permitted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td></td>
<td>password, consecutive or not. Case sensitive so e and E would not be</td>
<td></td>
</tr>
<tr>
<td></td>
<td>considered repeating.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Permitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Not Permitted - if selected, this will override Consecutive Repeat</td>
<td>Permitted, No limit</td>
</tr>
<tr>
<td></td>
<td>Characters setting.</td>
<td></td>
</tr>
<tr>
<td>Consecutive Uppercase</td>
<td>• Not allowed - a password will not contain any consecutive uppercase letters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Permitted, no limit - a password may contain any number of consecutive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>uppercase characters.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No more than $N$ - a password will not contain more than $N$ consecutive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>uppercase characters.</td>
<td></td>
</tr>
<tr>
<td>Consecutive Lowercase</td>
<td>• Not allowed - a password will not contain any consecutive lowercase letters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Permitted, no limit</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| limit - a password may contain any number of consecutive lowercase characters.  
  - No more than $N$ - a password will not contain more than $N$ consecutive lowercase characters. | | |
| Consecutive Alpha |  
  - Not allowed - a password will not contain any consecutive alphabetic characters (A-Z or a-z).  
  - Permitted, no limit - a password may contain any number of consecutive alphabetic characters.  
  - No more than $N$ - a password will not contain more than $N$ consecutive alphabetic characters. | Permitted, No limit |
| Consecutive Numeric |  
  - Not allowed - a password will not contain any consecutive numeric characters (0-9). | Permitted, No limit |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consecutive Alphanumeric</td>
<td>• Not allowed - a password will not contain any consecutive alphanumeric characters (A-Z, a-z,0-9).&lt;br&gt;• Permitted, no limit - a password may contain any number of consecutive alphanumeric characters.&lt;br&gt;• No more than $N$ - a password will not contain more than $N$ consecutive alphanumeric characters.</td>
<td>Permitted, No limit</td>
</tr>
<tr>
<td>Consecutive Non-alphanumeric</td>
<td>• Not allowed - a password will not contain any consecutive non-alpha-&lt;br&gt;• Not Permitted</td>
<td>Not Permitted</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>numeric characters. Nonconsecutive non-alphanumeric characters are still allowed.</td>
<td></td>
</tr>
<tr>
<td>Total # of characters available</td>
<td>The total number of unique characters available to create a password. When the <strong>Maximum Password</strong> length is longer than half this value the <strong>Nonconsecutive Repeat Characters</strong> option is set to <strong>Permitted</strong> and disabled.</td>
<td></td>
</tr>
</tbody>
</table>

6. Click the **Save Changes** button.

7. Click the **Test Password** rule button. Take note of the number of passwords requiring 10 or more attempts. A large number of these for a rule may create performance bottlenecks during the password change process. The test process limits the number of attempts to 30. If there are multiple “UNABLE TO CREATE PASSWORD” messages the rule is still allowed to be used, but should be restricted to low volume or infrequently changed accounts.

The password rule is now available in the /tpam interface for assignment to systems and accounts.
Delete a password rule

A password rule cannot be deleted if it is assigned to a system or account.

To delete a password rule:

1. Select System Status/Settings | Password Rules from the menu.
2. Select the password to be deleted.
3. Click the Delete Rule button.
4. Click the OK button on the confirmation window.
Email Configuration

Introduction

TPAM uses mail (SMTP) to provide notifications to approvers, requestors, reviewers, system contacts, account contacts, as well as providing error alerting for defined administrators.

Configure mail agent

The mail agent settings allow the System Administrator to define the local SMTP server so that TPAM can send email. The table below explains all of the options available on the Mail Agent Settings tab.

Table 15: Mail Agent Management: Settings tab options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use MX Lookup?</td>
<td>If selected, to send mail TPAM will query DNS for the SMTP server’s MX record.</td>
<td>No</td>
<td>Off</td>
</tr>
<tr>
<td>Domain Name</td>
<td>If Use MX Lookup is selected, enter the Domain Name here.</td>
<td>Yes, if using MX Lookup</td>
<td></td>
</tr>
<tr>
<td>PROSE Server Address</td>
<td>IP address for the SMTP server.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>SMTP Sender Email</td>
<td>This address will display as the sender email address for email that TPAM generates.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>SMTP Reply To Address</td>
<td>This is the address that will be used is a user replies to a TPAM generated email.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Send mail every ... minutes</td>
<td>The frequency, in minutes, that the mail agent will send email. Valid values are 1-20.</td>
<td>Yes</td>
<td>2</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Required?</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>Delete messages after ... failed attempts</td>
<td>The number of times the mail agent must try and send an email that fails to be delivered before it deletes the message.</td>
<td>Yes</td>
<td>5</td>
</tr>
<tr>
<td>Auto Start when system restarts</td>
<td>If selected, the mail agent will automatically restart when TPAM is restarted.</td>
<td>No</td>
<td>Off</td>
</tr>
<tr>
<td>Use blind carbon copy (bcc) when more than one recipient</td>
<td>If selected emails will be sent using &quot;Bcc&quot; instead of &quot;To&quot; and &quot;CC&quot; when there is more than one recipient.</td>
<td>No</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The Sent Mail Log will still show recipients as &quot;To&quot; or &quot;Cc&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use SMTP Sender or SMTP Reply To as the &quot;To&quot; recipient</td>
<td>When the &quot;Bcc&quot; option is selected, one of these must be selected. It will be used as the &quot;To&quot; recipient for all &quot;Bcc&quot; emails.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>IMPORTANT:</strong> If the selected email address resolves to a real mailbox then it will receive <strong>ALL</strong> emails that are sent &quot;Bcc&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test Email Address</td>
<td>Enter an email address to send a test email from TPAM. The Send Test Email button is not enabled until the mail agent has already been saved and has a status of Running. The email address entered here is not saved.</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**To configure the mail agent:**

1. Select **Mail Agent | Mail Agent** from the menu.
2. Enter the information on the Settings tab. For more information see **Configure mail agent**.
3. Click the **Save Changes** button.
4. Click the **Start** button.
5. Enter a Test Email Address.
6. Click the **Send Test Email** button.
7. Click the **OK** button on the confirmation window.

**NOTE:** The agent has to have a current status of Running before you will be able to send a test email.

8. Check to see if you received the test email.
To clear the mail agent log:

1. Select Mail Agent | Mail Agent from the menu.
2. Click the Clear Agent Log button.

Start/Stop the mail agent

The status of the mail agent is visible on the top right of Mail Agent Management pages. The Start and Stop buttons at the bottom of the page give the System Administrator the ability to stop and start the agent on demand.

**IMPORTANT:** Anytime a primary appliance is put in maintenance mode, the mail agent will be stopped. It will not restart automatically when the appliance is put back in operational mode unless the Auto Start when system restarts? check box is selected.

Sent mail report

The sent mail report provides a list of every email that has been queued for delivery by the mail agent. The sent mail report uses server time (UTC).

To view the sent mail report:

1. Select Mail Agent | Sent Mail Report from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the Results tab.

Clear the mail queue

TPAM provides a way to clear the mail queue. This could be helpful if the mail server has been down and you do not want to flood users with old emails that have been queuing up when the mail server is brought back up.

**TIP:** To avoid sending unwanted email, it is recommended to stop the mail agent before clearing the mail queue, and then restarting it.
To clear the mail queue:
1. Select Mail Agent | Sent Mail Report from the menu.
2. Enter the filter criteria for the messages that you want to remove from the queue.
3. Select Queued for Delivery as the Mail Status.
4. Click the Clear Mail Queue button.
5. Click the OK button on the confirmation window.
6. This will populate the Failed Date column on the Results page for these emails.

Mail agent log

The mail agent log provides a detailed report on SMTP activity. The mail agent log uses server time (UTC).

To view the mail agent log:
1. Select Mail Agent | Mail Agent Log from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the Results tab.

To clear the mail agent log:
1. Select Mail Agent | Mail Agent Log from the menu.
2. Enter your search criteria on the Filter tab.
3. Click the Results tab.

Configure email notification

The subject line and body text of the email messages sent by TPAM can be customized. The verbiage in the body of the email, embedded field information from TPAM (message tags) and hyperlinks can be customized for certain types of emails.

Email notifications that include a date/time reflect the user’s local time zone. For example on a session request the :SubmittedDate: reflects the server date, and :SubmittedUserDate:, reflects the date relative to the user making the request.

The table below describes the options on the Email Config page.
Table 16: Email Notification Configuration page options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the same URL for all Application Page links</td>
<td>If selected, all the different email notification types will use the URL entered here for application page links. A value of <code>DefaultNetworkAddress</code> will always resolve to the IP address of the appliance sending the mail. Any other IP address or FQDN will be substituted verbatim. It is important to consider whether this URL is accessible to all recipients of the email. For example, if TPAM has a RFC-1918 non-routable address, it is only accessible within that network (internally). If there is a NAT associated with an internal IP address for TPAM, that NAT address may be substituted. Application page links are not available for all email types. Typically they are included with approval and review notifications. This provides a convenient method for the approver to gain direct access to the request detail page for approval.</td>
<td>No</td>
<td><code>DefaultNetworkAddress</code></td>
</tr>
<tr>
<td>If email is</td>
<td>If selected, emails sent from a</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Requestors may receive copies of an email with approval links, but will not be able to gain access to the approval page by following the hyperlink because TPAM verifies each user’s authorization before displaying the page.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>generated from a failed over replica, send additional link to the replica network address</td>
<td>failed over replica will contain a link pointing to the failed over replica as well as a link from the original primary.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Type</td>
<td>A unique type of email notification. Email types preceded with an asterisk (*) have edits which have not been saved.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Subject Line</td>
<td>This is the subject line that the recipient will see. This can be edited.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Message Body</td>
<td>Each email type has a default message body that can be edited.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Message Body Tags</td>
<td>For each email type a list of Message Body tags is provided to copy and paste into the message body or subject line as desired.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Application Page Link</td>
<td>This address will be used for any links in the email which reference a URL in the appliance. This address can be edited for each email type if <strong>Use the Same URL for all Application Page Links</strong> check box is not selected.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Send To</td>
<td>For many of the Request notification email types you can select who the notification should be sent to: the Approvers, ISAs, Owner, and/or</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
### Field | Description | Required? | Default
--- | --- | --- | ---
Requestor. If none of the optional **Send To** check boxes are selected the email gets logged but not sent out. |  |  |  

**To configure email notification:**

1. Select **Mail Agent | Email Config** from the menu.
2. If all email types should use the same URL for application page links, select this check box and enter the URL to be used for the TPAM appliance.
3. Select an Email Type from the list and edit the subject line, message body, application page link, and send as desired.
4. Repeat this for each email type as needed.
5. Click the **Save Changes** button.

---

**Reset to factory defaults**

You can use the **Reset to Default** button for changing an individual email to the default. To change all altered email types back to the factory default click the **Reset All Emails to Factory Default** button.
Date and Time Configuration

Introduction

The server time of the appliance is based on coordinated universal time (UTC). The UTC time zone never undergoes transitions between Standard and Daylight Savings time.

Set date and time

To set the date and time of the appliance:

1. Select System Status/Settings | Date/Time Configuration | System Date from the menu.
2. Enter the date.
3. Enter the time.
4. Click the Save Settings button.

**NOTE:** If the TPAM appliance is configured to synchronize with an NTP server then the ability to manually set the system date and time is disabled.

Configure network time protocol

TPAM can use network time protocol (NTP) to keep the system clock in synchronization with a time server.

To configure NTP:

1. Select System Status/Settings | Date/Time Configuration | NTP Config from the menu.
2. Enter the network address of a primary and secondary (optional) NTP server.
3. Select the **Enable Time Synchronization** check box.
4. Click the **Save Settings** button.

To troubleshoot NTP synchronization click the **Diagnostics** tab.

Click one of the option buttons and click the **Perform Scheduled Diagnostic** button. The table below provides an overview of the options.

**Table 17: NTP synchronization: Diagnostics tab options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays Windows time service status.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Displays the configuration of run-time and where the setting comes from.</td>
</tr>
<tr>
<td>Restart W32Time Service</td>
<td>Stops and starts the Windows time service.</td>
</tr>
<tr>
<td>Resync with Current NTP Servers</td>
<td>Tells a computer that is should re-synchronize its clock as soon as possible, throwing out all accumulated error statistics.</td>
</tr>
<tr>
<td>Strip Chart</td>
<td>Displays a strip chart of the offset between this computer and another computer.</td>
</tr>
</tbody>
</table>
Keys and Certificates

Introduction

The options under the Keys menu allows the System Administrator to manage keys and certificates.

Manage host keys

The Manage Host Keys page is used to view and delete entries from the known_hosts file.

To delete an entry from the known_hosts file:

1. Select Keys | Manage Host Keys from the menu.
2. Type a search string to filter, click the Listing tab.
3. Select the network address to be deleted.
4. Click the Details tab for more information.
5. To delete the entry click the Clear Known Host button.

Manage SSH keys

The SSH Private Key is stored on TPAM, and is used to make secure connections to remote managed systems. The remote systems have the public key of the key pair. One Identity provides an initial key pair for these connections when TPAM is shipped. It is common (and recommended) that these keys eventually be replaced. This ensures that no one, not even One Identity, has the private key.

You have the ability to have up to three SSH Keys active simultaneously.
**To add an SSH key:**

1. Select **Keys** | **Manage SSH Keys** from the menu.
2. Click the **Add Key** button.
3. Enter the Key File Name.
4. Enter a Start Date and End Date. (Optional) If a start date is not entered, the key will not be active. If an end date is not entered, the assumed end date is 12/31/2037. If you enter an end date, a start date is required. TPAM will not allow you to save a key that will make more than 3 keys active at the same time. You will not be able to save the key until the dates are adjusted on the other keys so that only 3 will be active at one time.
5. Select a key source from the following choices:
   - **Gen 2048bit key** - TPAM will generate 2048 bit keys.
   - **Gen 1048bit key** - TPAM will generate 1048 bit keys.
   - **Enter private key** - Paste your private key in the field below.
   - **Upload private key file** - Click the **Select File** button. Click the Browse button and select the file. Click the **Upload** button.
6. Click the **Save Changes** button.

When the process is complete, the new public key is available for download to TPAM managed systems.

**To delete a key:**

1. Select **Keys** | **Manage SSH Keys** from the menu.
2. Select the key to be deleted on the Listing tab.
3. Click the **Delete Key** button.
4. Click the **OK** button on the confirmation window.

**NOTE:** If deleting a key will create a gap with no active keys, the key will not be deleted and you will get a warning message.

You have the ability to regenerate the TPAM appliances’ ssh host keys. Please use with caution. Changing the appliances’ ssh host key can affect CLI/API operations since the identification string for the appliance has been changed and will report an error to clients that have previously connected to the appliance. Also if you have DPAs enrolled and you regenerate the ssh host keys you must log onto the DPA console and delete TPAM from known_hosts. This is option is under the Network Settings menu, **Delete TPAM from known_hosts**.

**To regenerate a key:**

1. Select **Keys** | **Manage SSH Keys** from the menu.
2. Click the **Regen HostKey** button.
3. Click the **OK** button on the confirmation window.
NOTE: It is possible to regenerate the host key of a failed over replica without removing it from the cluster.

Generate web certificate request

Replacing the certificate is a process that includes generating a request, downloading and submitting the request file to a certificate authority (CA), obtaining and loading CA certificates as TPAM Trusted CA certificates and uploading the newly issued certificate to TPAM.

NOTE: Certificates must be generated or imported on all TPAM devices, the primary TPAM device will NOT replicate the certificate to replicas.

**To replace a certificate on TPAM:**
1. Select Keys | Web Certificate Request from the config menu.
2. Enter the information in the fields marked with asterisks.
3. Enter subject alternative names separated by semi-colons. (Optional)
4. Click the Generate button.
5. Click the Download File button to download the request file generated by TPAM. Use this request file with CA to obtain a new certificate.
6. Upload the issuing root CA’s certificate (and any other intermediate CA’s certificates) of the new web certificate into TPAM. See TPAM trusted CA certificates on page 128 for instructions.
7. Click the Select File button.
8. Click the Browse button to locate the new certificate. Select the file.
9. Click the Upload button.
10. Click the Install Web Certificate button to upload the new certificate provided by CA. If an invalid certificate is loaded TPAM will revert back to the last valid certificate.
11. Click the OK button on the confirmation window.
12. Refresh the page to view the new certificate.

Import web certificate

NOTE: Certificates must be generated or imported on all TPAM devices, the primary TPAM device will NOT replicate the certificate to replicas.
IMPORTANT: BEFORE importing a web certificate, intermediate certificates and root certificate authority certificates must be imported first.

To install your own web certificate on the TPAM appliance:

1. Select Keys | Web Certificate Request from the config menu.
2. Click the Import cert button.
3. Click the Select File button.
4. Click the Browse button. Select the file.
5. Click the Upload button.
6. Enter the import password.
7. Click the Import Web Certificate button.
8. Click the OK button on the confirmation window. If an invalid certificate is loaded TPAM will revert back to the last valid certificate.

TPAM trusted CA certificates

If you are adding a web certificate for your appliance, the certificate authority certificate(s) for the web certificate must be loaded into TPAM before the web certificate is installed or imported.

Also, if users will be authenticating with a client certificate (including smart card based authentication), the certificate authority for these client certificates must be loaded in TPAM, so TPAM recognizes it as a valid source.

First, obtain the CA certificate from the issuing certificate authority.

To load the trusted CA certificate:

1. Select Keys | TPAM Trusted CA Certs from the admin menu.
2. Click the Select File button.
3. Click the Browse button. Select the file.
4. Click the Upload button.
5. Select one of the Fail options:
   - None - only the Thumbprint is used for verification.
   - Failsafe - authentication is permitted if the OCSP response is “good”, or if the thumbprint matches.
   - Failsecure - authentication is denied if the OCSP responder gives any response other than “good”.
6. Click the Import Certificate button.
7. After the trusted CA certificates have been imported, reboot all DPAs so that the trusted CA certificates can be applied on the DPA, thereby allowing the DPA to
establish trust with the console after the new certificate is added. If you are using the TPAM profile notification service (https://address:9443/available), this appliance also needs to be rebooted to make sure the new certificate signing chain is fully recognized.

Web access trusted CA certificates

Trusted CA certificates can be installed into the browser used during PSM Web Access sessions to avoid warnings about invalid web site security certificates. These Trusted CA certificates can be imported into TPAM, and the certificates will be pushed to the DPA and installed into the browser when starting a PSM web access session.

**To load the trusted CA certificate:**

1. Select Keys | Web Access Trusted CA Certs from the admin menu.
2. Click the Select File button.
3. Click the Browse button. Select the file.
4. Click the Upload button.
5. Click the Import Certificate button.

Reset certificate to factory default

**To reset the web certificate to the factory default:**

1. Select Keys | Web Certificate Request from the config menu.
2. Click the Reset button.
3. Click the OK button on the confirmation window.

Certificate based web access for user IDs

User IDs can be configured to authenticate to the TPAM web interface using client certificates. As with web certificates, the certificate(s) of the CA’s that issued the client certificate must be loaded into TPAM. Sha1 certificate thumbprint for user IDs can be entered for users wanting to authenticate using a trusted authority.

When users log on to TPAM they will be prompted to confirm the certificate by clicking the OK button.
Sybase trusted root certificates

To use the secure communication channel from TPAM to ASE, there is additional configuration that must be performed on TPAM.

NOTE: If you decide to use a tunnel through SSL, these steps are not needed.

To configure Sybase trusted certificates:

1. Select Keys | Sybase Trusted Root Certs from the menu.
2. Paste the Base64 encoded certificate that was used to sign the certificate installed at the Sybase data server into the text box.

NOTE: If you use multiple Trusted Roots for signing certificates used at different Sybase instances in your organization (for example, having some issued from an internal Certificate Authority (CA) and others issued by a commercial CA), this text box should include All the root certificates used in your Sybase environment. This is accomplished by appending additional certificates (denoted by a -----BEGIN CERTIFICATE----- ... -----END CERTIFICATE----- ... ) You can also place comment information in between the certificates to make it easier to identify the information in there.

3. Click the Save Settings button.
4. After the certificate(s) has been loaded, set up the Sybase managed systems in TPAM to use this secure channel for communication. Update or add the Sybase managed system to specify the correct port for the secure channel (Sybase default is 5000) and select Use SSL.
5. Click the Save Changes button.
6. Click the Test System button to test the connection to the Sybase managed system.

MySQL trusted root certificates

To use the secure communication channel from TPAM to MySQL, there is additional configuration that must be performed in TPAM.

NOTE: If you decide to use a tunnel through SSH, these steps are not needed.

To configure MySQL trusted certificates:

1. Select Keys | MySQL Trusted Root Certs from the menu.
2. Paste in your MySQL certificate.
3. Click the **Save Settings** button.
4. After the certificate(s) has been saved, set up the MySQL managed systems in TPAM to use this secure channel for communication. Update or add the MySQL managed system to specify the correct port for the secure channel (MySQL default is 3306) and select **Use SSL**.
5. Click the **Save Changes** button.
6. Click the **Test System** button to test the connection to the MySQL managed system.

## Upload a certificate on a replica

**To generate and upload a certificate on a replica:**

1. Log on to the /admin interface of the primary.
2. Select **System Status/Settings | Cluster Management** from the menu.
3. Select the replica you want to generate/load a certificate on.
4. Click the **Force Failover** button.
5. Click the **Continue with Change** button on the confirmation window.
6. Log on to the /admin interface of the replica.
7. See **Generate web certificate request** on page 127, and **Import web certificate** on page 127. Once these steps are completed on the replica you will need to unforce the failover.
8. Log on to the /admin interface of the primary appliance.
9. Select **System Status/Settings | Cluster Management** from the menu.
10. Select the cluster member that is currently failed over.
11. Click the **Un-force Failover** button.
Automation Engine

Introduction

The automation engine is the heart of TPAM. This portion of the TPAM architecture is where password management on remote systems is configured and scheduled. Once the automation engine is running, several different agents can be enabled on the engine to perform privileged password management functions. Logs provide a record of agent activities and messages of success or failure.

Agent status tab

The current status of all the agents, either Enabled or Disabled, is displayed on the status tab, as well as events queued on the engine for processing. The table below describes the functions of the different agents.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Management</td>
<td>The auto management engine that runs all the various password management and discovery agents.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Check</td>
<td>If enabled, this agent periodically checks the passwords on remote managed system accounts and compares it to the password stored in the TPAM database. This provides an automated integrity checking mechanism that ensures that the password that is released for use by TPAM is valid on the remote system.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Change</td>
<td>If enabled, this agent looks for accounts that are scheduled for a password change and performs the change.</td>
<td>Enabled</td>
</tr>
<tr>
<td>DA Change</td>
<td>If enabled, the domain account agent looks for services that must have their password changed because they rely</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
### Start/Stop the auto management engine

**To start/stop the engine:**

1. Select Automation Engine | Auto Mgt Agent from the menu.
2. Click the **Start** or **Stop** button next to the Auto Management agent status.

Stopping the Automation Engine, stops all agents that are enabled on the engine.

**IMPORTANT:** Anytime a primary appliance is put in maintenance mode, the automation engine will be stopped. It will not restart automatically when the appliance is put into operational mode unless the Start Management Agent when system restarts? check box is selected.

**NOTE:** The automation engine cannot be started on a failed over replica.

### Disable/Enable an agent

**To disable/enable an agent:**

1. Select Automation Engine | Auto Mgt Agent from the menu.
2. Click the **Disable** or **Enable** button for the desired agent.

**NOTE:** If you disable an agent and the change process is currently busy processing changes, it may take some time for the service to stop.
Auto Management settings tab

The table below describes the fields on the auto management settings tab. The default settings for threads is dependent on whether you have a standard or enterprise TPAM appliance.

### Table 19: Auto Management Agent: Settings tab options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Worker Threads</td>
<td>TPAM uses a pool of worker threads to service a larger number of queries, which improves performance. Valid entries are 1-10.</td>
</tr>
<tr>
<td>Start Management Agent when system restarts?</td>
<td>If selected, the automation engine will automatically start when the TPAM appliance restarts.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This option is not available on a failed over replica.</td>
</tr>
<tr>
<td>Full Load Percentages</td>
<td>allocates the number of agent processes based on the number of max worker threads.</td>
</tr>
<tr>
<td>Maximum Threads</td>
<td>Sets upper limits that will override the percentage allocation of threads.</td>
</tr>
<tr>
<td>Retry Intervals</td>
<td>The amount of time in minutes, that an agent will wait before trying to change or check a failed attempt on an account. If the check process completes (even if it is unsuccessful) it will not retry. When checking an account on a system that is unreachable TPAM will retry the check using the retry interval, schedule and settings of the assigned password check profile.</td>
</tr>
</tbody>
</table>

Check password queue schedule

The check password schedule that was previously controlled by the settings on this page are now controlled by the Password Check Profile assigned to the account or synchronized password. For more details please see the TPAM Administrator Guide.

**IMPORTANT:** Passwords will not be checked if the Check agent is disabled. The Check agent must also be enabled to process the passwords in the queue.
Manually load the check password queue

Any accounts that are scheduled to be tested based on their password check profile settings will loaded into the queue when the Load Test Queue button is clicked.

To manually load the check password queue:

1. Select Automation Engine | Auto Mgt Agent from the menu.
2. Click the Load Test Queue button.

**NOTE:** Prior to TPAM v2.5.915 clicking this button loaded all managed accounts to be checked because password check profiles did not exist in prior versions of TPAM.

Agent logs

The table below describes the check and change logs available in TPAM. These logs use server time (UTC).

Table 20: TPAM Check and Change logs

<table>
<thead>
<tr>
<th>Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Agent Log</td>
<td>This log provides details on all password checks performed by the check agent.</td>
</tr>
<tr>
<td>Test Log</td>
<td>This logs provides details on password checks performed by the check agent and by users performing manual password checks.</td>
</tr>
<tr>
<td>Change Agent Log</td>
<td>This log provides details on all password changes performed by the change agent.</td>
</tr>
<tr>
<td>Change Log</td>
<td>This logs provides details on password changes performed by the change agent and by users performing manual password changes or by clicking the reset password button in the /tpam interface.</td>
</tr>
</tbody>
</table>

To view the logs:

1. Select Automation Engine | Auto Mgt Agent from the menu.
2. Click the Logs Filter tab.
3. Enter your filter criteria.
4. Click one of the Logs tabs to view the results.
**To clear a log:**

1. Select **Automation Engine | Auto Mgt Agent** from the menu.
2. Click the Log tab that you want to clear.
3. Click the **Clear Agent Log** button.
4. Click the **OK** button on the confirmation window. This will clear all the data in the log.
Agents

Introduction

The agents in TPAM execute scheduled tasks for different functions on a regular basis.

Daily Maintenance agent

The daily maintenance agent combines several back end jobs (batch report start time, purging of old data) into one. The daily maintenance agent and log uses server time (UTC).

To configure the start time for the daily maintenance agent:

1. Select System Status/Settings | Agents | Daily Maintenance from the menu.
2. Enter the start time using a 24-hour clock.
3. Click the Save Changes button.

To view the logs:

1. Select System Status/Settings | Agents | Daily Maintenance from the menu.
2. Click the Processing Log tab.
3. Enter your search criteria on the filter tab.
4. Click the Results tab.

Auto Discovery agent

The auto discovery agent controls LDAP and generic integration and the ability of TPAM to automatically create and update systems and users.
To start/stop the auto discovery agent:

1. Select System Status/Settings | Agents | Auto Discovery from the menu.
2. Click the Start or Stop button to start or stop the agent.

Select the Auto Start when system restarts? check box to have the auto discovery agent automatically restart whenever TPAM is restarted and click the Save Changes button.

IMPORTANT: Anytime a primary appliance is put in maintenance mode, the auto discovery agent will be stopped. It will not restart automatically when the appliance is put back in operational mode unless the Auto Start when system restarts? check box is selected.

The auto discovery agent log displays server time (UTC).

To view the log:

1. Select System Status/Settings | Agents | Auto Discovery from the menu.
2. Click the Agent Log tab.
3. Enter your search criteria on the filter tab.
4. Click the Results tab.

Post-Session Processing agent

For any post session profile activities to be triggered after a session expires, the post-session processing agent must be started. The agent will check and/or change passwords on accounts depending on how the post-session profile is configured.

Synchronized password subscribers are processed in priority order. If any of the subscribers fail to change, the agent stops and tries again based on the Synch Pass Change agent retry interval setting. If the prioritized subscribers succeed but some non-prioritized subscribers fail, then the failures will be processed by the regular change agent. Manual subscribers are scheduled with the regular manual change agent.

To start/stop the post-session processing agent:

1. Select System Status/Settings | Agents | Post-Session Processing from the menu.
2. Click the Start or Stop button to start or stop the agent.

To configure the agent interval select an agent frequency from the list and click the Save Changes button.

The post session processing agent log displays server time (UTC).
To view the logs:

1. Select System Status/Settings | Agents | Post-Session Processing from the menu.
2. Click the Agent Log tab.
3. Enter your search criteria on the filter tab.
4. Click the Results tab.

SSH daemon

The SSH daemon can be restarted without having to reboot the TPAM appliance.

⚠️ **CAUTION:** Stopping the SSH daemon when active PSM sessions are active could have an adverse affect.

To stop/start the SSH daemon:

1. Select System Status/Settings | Agents | SSHD Agent from the menu.
2. Click the Stop or Start button.
**Backups**

**Introduction**

Considering the value of the information stored in TPAM the backup engine is an integral part of TPAM. Backups can be configured to run on automatically and moved securely to offline storage. The backup is always encrypted, so the backup can be maintained without the risk of exposing sensitive data.

*IMPORTANT:* If PSM sessions are being recorded on the appliance and they are not sent to an archive server the TPAM backups can get extremely large. It is recommended to send session logs to an archive server to avoid this.

**Backup settings tab**

The table below describes all the options on the backup settings tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>If selected, the backup will occur based on the schedule selected.</td>
<td>On</td>
</tr>
<tr>
<td>Daily</td>
<td>If selected, the backup will occur daily at the time designated.</td>
<td>On</td>
</tr>
<tr>
<td>Weekly</td>
<td>If selected, the backup will occur on the day/s selected at the time designated.</td>
<td>Off</td>
</tr>
<tr>
<td>Monthly</td>
<td>If selected, the backup will occur on the day of the month specified at the time designated.</td>
<td>Off</td>
</tr>
<tr>
<td>Secondary Encryption</td>
<td>The backup will already be encrypted by default. To</td>
<td>No secondary</td>
</tr>
</tbody>
</table>
### Configure the backup schedule

**To configure the backup schedule:**

1. Select **Backup | Modify Backup Settings** from the menu.
2. Set the backup frequency and start time.
3. Enter password for secondary encryption. (Optional)
4. Select one or more archive servers from the list to store the backup on. To configure an archive server see **Configure archive servers** on page 66. By default the backup files will also be stored online.
   
   **TIP:** It is strongly advised that backups be sent to an archive server. In the event of disaster recovery, it may be necessary to have a recent backup stored safely offline.

5. Enter an email address to receive all or just failed notifications on the backup process.
6. Click the **Save Changes** button.

### On demand backup

**To run a backup on demand:**

1. Select **Backup | Modify Backup Settings** from the menu.
2. Click the **Backup Now** button. A message will be displayed on the bottom of the page that the backup has started.
**View backup log**

By default TPAM will store 30 days worth of backup logs. To change the retention period for the logs see Edit global settings. The backup log uses server time (UTC).

**To view backup logs:**

1. Select **Backup | Backup Log** from the menu.
2. Enter your search criteria on the filter tab.
3. Click the **Results** tab.

To clear the backup log click the **Clear Backup Log** button.

**View backup history**

The backup history report uses server time (UTC).

**To view backup history:**

1. Select **Backup | Backup History** from the menu.
2. Enter your search criteria on the filter tab.
3. Click the **Results** tab.

**Download an online backup**

The number of online backups that can be stored at one time is configured in Global Settings. See Edit global settings. The archive files are named TPAM_Date_Time.zip and listed in ascending order. The online backup completion time is displayed in server time (UTC).

**IMPORTANT:** Do not rename backup files, doing so will cause a restore to fail.

**To download an online backup:**

1. Select **Backup | Manage OnLine Backups** from the menu.
2. Select the backup to download.
3. Click the **Download** button.
4. Select **Save File** to save the backup offline.
5. Click the **OK** button.
Delete a backup

To delete an online backup:

1. Select Backup | Manage OnLine Backups from the menu.
2. Select the download to delete.
3. Click the Delete button.
4. Click the OK button on the confirmation window.
Alerts

Introduction

The alerts in TPAM allow you to receive notification via email or SNMP, for over eighty different errors or status notifications.

Add an alert receiver

To add an alert receiver:

1. Select System Status/Settings | Alerts | Receivers from the menu.
2. Click the Add Alert Receiver button.
3. Enter a receiver name.
4. Clear the Receiver Enabled? check box if you want to save the alert receiver without it being enabled. (Optional)
5. Enter a description for the alert receiver. (Optional)
6. Use one of the following methods to select the receiver type:
   - Select E-mail. Enter the email addresses that will receive these alerts.
   - Select SNMP. Enter the network address, community, port, and version.

   NOTE: If SNMP is selected, the MIB cannot be downloaded until after you select the alerts on the Alerts tab, click the Save Changes button and return to the Details tab.

7. Enter the number of times TPAM should attempt to re-send the alert if there is an unsuccessful attempt. An entry of 0 means indicates that no retries will be made.
8. Click the Save Changes button.
9. To send a test email click the Send Test Message button. (Optional)
10. Click the **Alerts** tab.

11. Select the subscribe check boxes for the alerts you want to subscribe to. Select the subscribe check box next to the component name to subscribe to all the alerts under that component. Clicking the **Select All** button will select all alerts. Clicking the **Select None** button will clear all the subscribe check boxes. Clicking the **Toggle** button selects any check box that was clear, and clears all the check boxes that were selected.

12. Click the **Save Changes** button.

Where you see %1%,%2% in the message, it represents a variable that will be populated on the alert notification when received. The alert severity will be displayed in the subject line of the message. The appliance that generated the alert will be included in the message.

**Delete an alert receiver**

*To delete an alert receiver:*

1. Select **System Status/Settings | Alerts | Receivers** from the menu.
2. Enter your search criteria on the filter tab.
3. Click the **Listing** tab.
4. Select the receiver to delete.
5. Click the **Delete Alert Receiver** button.
6. Click the **OK** button on the confirmation window.

**Alert thresholds**

Some of the alert receivers that you can subscribe to, such as CPU checks, have configurable thresholds. For example, the alert “The utilization of the appliance hard drive is %1%, exceeding the threshold of %2%.” The %2% that this alert references is configured here in the disk space threshold.

*To configure alert thresholds:*

1. Select **System Status/Settings | Alerts | Thresholds** from the menu
2. To change the default value enter the number and click the **Save Changes** button.

**Alert details export**
TPAM provides an export file where the component MIB name, alert OID, severity level, alert MIB name, and alert MIB description for each alert is listed.

To download the object identifiers (OID) for all the TPAM alerts:

1. Select System Status/Settings | Alerts | Receivers from the menu.
2. Click the Listing tab.
3. Select an alert receiver that has already been configured.
4. Click the Alerts tab.
5. For a listing of OIDs for all TPAM alerts click the Export All button. To only get the OIDs for subscribed alerts click the Export Selected button.
6. Save the file.
External Authentication

Introduction

TPAM supports several different methods of external authentication. These are described in detail below.

Certificate based authentication

TPAM supports PKI based external authentication through smart cards and web certificates. If users are authenticating with a client certificate, the certificate authority for these client certificates must be loaded in TPAM, so TPAM recognizes it as a valid source. For details on how to load the certificate see TPAM trusted CA certificates on page 128. When the user ID is added to TPAM the certificate sha1 thumbprint is entered as part of the user setup.

SafeWord

The table below explains the options when configuring SafeWord.

Table 22: Configure SafeWord: Settings tab options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>The IP address if the SafeWord server.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>Consult your SafeWord administrator</td>
<td>Yes</td>
<td>0</td>
</tr>
<tr>
<td>Conns</td>
<td>Consult your SafeWord administrator</td>
<td>Yes</td>
<td>0</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the TCP port that the SafeWord server will be listening on.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Required?</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>EASSP Version</td>
<td>Select one of the following as the SafeWord version:</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SafeWord 5.1.1 and older</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SafeWord 5.1.2 and newer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SafeWord Plus</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Premier Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Socket Timeout</td>
<td>The number of seconds before an unanswered request is dropped. This timeout only applies when this is being used a secondary authentication.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>System Name</td>
<td>Consult your SafeWord administrator.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Agent Name</td>
<td>Consult your SafeWord administrator.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Authentication Timeout</td>
<td>The maximum number of hours that an authenticated session can persist.</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

To configure select **System Status/Settings | External Authentication | SafeWord Config** from the menu. Enter the required information as described in the table above and click the **Save Changes** button.

Make sure that the port number entered in TPAM matches the port number for the SafeWord authentication engine server port.

To clear existing server verification data files click the **Clear Swec** button. The next successful log on attempt recreates this data file.

A TPAM user configured with SafeWord as external authentication method will be required to enter their token when logging on to TPAM.

### RSA SecureID

SecurID requires two files be imported into TPAM, sdconf.rec and sdopts.rec. These files contain specific information regarding the ACE server configurations and necessary parameters.

**To configure SecurID:**

1. Select System **Status/Settings | External Authentication | SecurID Config** from the menu.
2. Enter the max number of hours a session can persist in the Authentication Timeout field.
3. Select **SDOpts.rec** from the Import File Type list.
4. Click the **Select File** button.
5. Click the **Browse** button. Select the file.
6. Click the **Upload** button.
7. Click the **Import Options File** button.
8. Click the **OK** button on the confirmation window.
9. Select **SDConf.rec** from the Import File Type list.
10. Click the **Select File** button.
11. Click the **Browse** button. Select the file.
12. Click the **Upload** button.
13. Click the **Import Config File** button.
14. Click the **OK** button on the confirmation window.

The **Save** button is only related to the Authentication Timeout attribute of the SecurID external authentication. The upload of the SDConf.rec file is what is required to allow for SecurID external authentication. The SDOpts.rec file is optional. Once the SDConf.rec file has been imported to establish SecurID as an external authentication source, subsequent visits to the page will default the Import File Type to SDOpts.rec. The **Clear Settings** button will remove the files and clear SecurID as an external authentication source.

**NOTE:** The RSA Administrator must enter the host IP address of the TPAM appliance in the RSA server, making sure there are no existing node secrets, and the host is open to locally known users. The agent type for RSA versions 6 or earlier must be **netOS** or **Single Comm Trans**. The agent type for RSA versions 7 and higher must be **Web Agent** or **Standard Agent**.

### LDAP

TPAM supports Windows or Unix LDAP environments.

**To configure LDAP:**

1. Select **System Status/Settings | External Authentication | LDAP Config** from the menu.
2. Click the **New System** button.
3. Enter the LDAP server name.
4. Enter the IP address of FQDN of the authentication server.
5. Enter the number of maximum hours that an authenticated session can persist.
6. Select the **SSL** check box to enable SSL. (Optional)
7. Click the **Save Changes** button.
Windows Active Directory

To configure Windows Active Directory:

1. Select System Status/Settings | External Authentication | WinAD Config from the menu.
2. Click the New System button.
3. Enter the Windows Active Directory server name.
4. Enter the IP address of FQDN of the authentication server.
5. Enter the number of maximum hours that an authenticated session can persist.

**NOTE:** This timeout only applies when Win AD is being used as secondary authentication.

6. Click the Save Changes button.

RADIUS

TPAM can support challenge/response protocol for Radius when used as primary authentication.

To configure RADIUS:

1. Select System Status/Settings | External Authentication | RADIUS Config from the menu.
2. Click the New System button.
3. Enter the RADIUS server name.
4. Enter the IP address of FQDN of the authentication server.
5. Enter the number of maximum hours that an authenticated session can persist.

**NOTE:** This timeout only applies when Radius is being used as secondary authentication.

6. Change the Port if needed.
7. Enter the secret needed for authentication.
8. Click the Save Changes button.
Defender

TPAM can support challenge/response protocol for Defender when used as primary authentication.

To configure Defender:

1. Select System Status/Settings | External Authentication | Defender Config from the menu.
2. Click the New System button.
3. Enter the Defender server name.
4. Enter the IP address of FQDN of the authentication server.
5. Enter the number of maximum hours that an authenticated session can persist.

   NOTE: This timeout only applies with Defender is being used as secondary authentication.

6. Change the Port if needed.
7. Enter the secret needed for authentication.
8. Click the Save Changes button.

Starling Two-Factor Radius Agent

TPAM can support challenge/response protocol for the Starling Two-Factor Radius Agent when used as external authentication.

To configure Starling:

1. Select System Status/Settings | External Authentication | Starling Config from the menu.
2. Click the New System button.
3. Enter the Starling server name.
4. Enter the IP address of FQDN of the authentication server.
5. Enter the number of maximum hours that an authenticated session can persist.

   NOTE: This timeout only applies when Radius is being used as secondary authentication.

6. Change the Port if needed.
7. Enter the secret needed for authentication.
8. Click the **Save Changes** button.
Starling Join

Introduction

A TPAM cluster can be joined to a customer’s Starling SaaS subscription. Once joined to Starling, TPAM users can be configured to receive push notifications (Approval Anywhere) to their mobile phone for TPAM approvals. See the TPAM Administrator Guide for details on configuring Approval Anywhere.

Configure Starling Join

The table below describes the options on the Starling Join page.

Table 23: Starling Join Configuration page options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPAM Cluster ID</td>
<td>Generated automatically and will be unique for each cluster.</td>
</tr>
<tr>
<td>TPAM Cluster Name</td>
<td>Used along with the cluster ID when joining to Starling. Up to 100 characters, consisting of letters, numbers, underscore and hyphens (no spaces allowed). Once the cluster is joined this name cannot be edited.</td>
</tr>
<tr>
<td>click here</td>
<td>Clicking the hyperlink will open a new tab/window to the appropriate Starling instance with the appliance identification supplied. Supply your credentials to authenticate to Starling.</td>
</tr>
<tr>
<td>Credential String</td>
<td>Value provided by Starling</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Value provided by Starling</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client ID</td>
<td>Calculated value.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>Calculated value.</td>
</tr>
</tbody>
</table>

The Starling Join function can only be performed from the primary of a cluster.

**IMPORTANT:** All appliances in the TPAM cluster must be able to access network addresses outside of the company network in order for Starling Join and Approval Anywhere to work.

### To join a TPAM cluster to Starling:

1. Select **System Status/Settings | Starling** from the menu.
2. The TPAM Cluster ID is generated automatically and will be unique for each cluster.
3. Enter a TPAM Cluster Name.
4. Click the hyperlink to join the TPAM cluster to Starling.
5. A new tab will be opened to the Starling site. You will be prompted for your Starling credentials.
6. The credential string provided will consist of the ClientID:ClientSecret. Copy and paste these values into TPAM.
7. Copy and paste the Token Endpoint into the Endpoint field in TPAM.
8. Click the **Save Join Info** button.
9. Click the **Test Credentials** button. A connection will be attempted to the Starling subscription using the current credentials and success or failure reported.

### To unjoin from Starling:

1. Select **System Status/Settings | Starling** from the menu.
2. Click the **Unjoin** button.

Unjoining will drop the registration for this TPAM cluster. If successful the TPAM Cluster ID and TPAM Cluster name will be reset.

**NOTE:** Once unjoin is successful there is no way to regain the original cluster ID even when using the same cluster name. Removing an appliance from the cluster will also reset these values, but does not perform the unjoin function.

### Configure Starling monitor

Once the TPAM cluster has been joined to Starling you can configure the Starling monitor. Starling Monitor is responsible for sending Approval Anywhere notifications to Starling—
enabled users and recording Request Approve / Deny response from those users via their mobile devices. The table below describes the Starling Monitor settings. There are alerts that can be subscribed to in TPAM related to Starling Monitor problems. For more details see Alerts.

Table 24: Starling monitor settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Timeout</td>
<td>The timeout of an individual request to either add a notification or poll an existing notification. Range: 100-2000 milliseconds.</td>
<td>500</td>
</tr>
<tr>
<td>Thread Timeout</td>
<td>The timeout of an entire thread performing &quot;Requests per thread&quot; operations. Range: 10-60 seconds.</td>
<td>10</td>
</tr>
<tr>
<td>Max Thread Count</td>
<td>The maximum number of simultaneous threads performing notification operations. Range: 1-10</td>
<td>5</td>
</tr>
<tr>
<td>Requests per Thread</td>
<td>The maximum number of requests per thread. Range: 5-50</td>
<td>10</td>
</tr>
<tr>
<td>Run Starling Monitor on</td>
<td>The monitor will only run when an appliance is at Operational run level. Check the appropriate box to run the monitor on the Primary or on a Failed Over Replica.</td>
<td>Not selected</td>
</tr>
</tbody>
</table>

NOTE: If Failed Over Replica is not selected, the Starling Monitor process will not automatically run on any replicas that fail over. In this case for Approval Anywhere to continue to run, someone would need to log on to the failed over replica and select this value.

IMPORTANT: If Failed Over Replica is selected, and multiple replicas fail over, users may receive multiple Approval Anywhere notifications, one from each failed over replica.
Ticket Systems

Introduction

Ticket Systems are configured so that TPAM will validate ticket numbers and other information about the request that are entered at the time the password, file, or session request is submitted. If a password, file, or session is requested that requires a Ticket Number, the number is passed to the indicated ticket system for a “yes/no” answer. The validation may be as simple as “they entered a number and that’s all we need” or as involved as “not only must the ticket number exist in the ticket system but the data returned must match the user’s name, request, requested account, system, dates, and so on.” More than one ticket system can be configured.

If a password, file, or session request fails the validation rules that have been configured the request is immediately canceled and the requestor has the option to try again.

To set up ticket systems you must complete the following steps:

- Configure the ticket system in the /admin interface.
- Assign the ticket system to systems, accounts and files in the /tpam interface

To add a ticket system, information is entered on the following tabs in the /admin interface:

**Table 25: /admin interface tabs**

<table>
<thead>
<tr>
<th>Tab name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>Where name and connection information is configured.</td>
</tr>
<tr>
<td>Data</td>
<td>Where the commands are configured to retrieve the validation information.</td>
</tr>
<tr>
<td>Rules</td>
<td>Used to describe what to do with the data returned from the query.</td>
</tr>
</tbody>
</table>
# Details tab

The table below explains the fields available on the ticket system details tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket System Name</td>
<td>Descriptive name for the ticket system. Must be unique and no longer that 30 characters.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>The description box may be used to provide additional information about the ticket system.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Enable Validation for this Ticket System</td>
<td>If selected, TPAM will perform a validation against this ticket system.</td>
<td>No</td>
<td>Off</td>
</tr>
</tbody>
</table>
| Allow provisional validation when system is disabled | If selected, and the Enable Validation for this Ticket System is not selected, then any requests made against this ticket system still require a ticket number, but the ticket number will not be validated when the request is submitted. When the approver goes to approve/deny the request they will see the following note on the page: The ticket number listed above was provisionally validated because the Ticket System was disabled at the time of the request. Press the Revalidate button to attempt to revalidate the Ticket. The approver has the option to:  
  - Approve/Deny the request without revalidating the ticket.  
  - Clicking the **Revalidate Ticket** button before approving/deny the request. If the approver tries to revalidate the ticket and the ticket system is now enabled, and the ticket fails validation, the request is automatically denied. | No        | Off     |
| Ticket Select from                          | Select from:                                                                 | Yes       | Not     |

**NOTE:** This option is not available on Manual ticket system types.

---

TPAM 2.5.923 System Administrator Guide  
Ticket Systems  
157
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
</table>
| System Type                 | - Not Managed - A system not managed by TPAM. All connection information must be provided.  
- Managed - The system and account must be set up as managed in the /tpam interface.  
- Web Service - The service must reside on a system that is reachable from the TPAM appliance, using either HTTP POST or GET protocol and return a stream of XML with either data related to the ticket or an error condition.  
- Manual - There is no database integration for this type of ticket system. Validation of ticket numbers will be accomplished with an expression entered in the Connection Information. | Managed   | Managed |
| ODBC Driver (applies to Not Managed) | Select from:  
- MS SQL Server  
- Oracle  
- Sybase  
- MySQL                                                                                                                                                                                                                                                                           | Yes       |         |
<p>| Use SSL? (applies to Not Managed) | If selected, the validation query will use SSL to communicate with the target database unless a non-default value is entered.                                                                                                                                                                                                                       | No        | Off     |
| Network Address (applies to Not Managed) | An IP address or system name that is resolvable from the appliance.                                                                                                                                                                                                                                                                         | Yes       |         |
| Port Number (applies to Not Managed) | The port number will be automatically filled in after the ticket system is saved.                                                                                                                                                                                                                                                                  | Yes       |         |
| Timeout (applies to Not Managed) | The number of seconds the validation routines wait for a response before the database times out.                                                                                                                                                                                                                                              | No        |         |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Name (applies to Not Managed)</td>
<td>Applies to SQL Server, MySQL or Sybase databases. The name of the ticket system database on the indicated server.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>SID/Service Name (applies to Not Managed)</td>
<td>Applies to Oracle databases. The SID or service name to connect to on the Oracle server.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>User Name (applies to Not Managed)</td>
<td>The log on to get into the database. For SQL Server databases this must be a SQL server authentication ID. Windows authentication is not supported.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Password (applies to Not Managed)</td>
<td>The password is stored in TPAM using the same encryption method that is used for managed accounts. Blank passwords are supported, but not recommended. When editing a ticket system, leave the password field blank unless you want to change it.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>System (applies to Managed)</td>
<td>The system name of the managed system configured in the /tpam interface. The platform must be MS SQL Server, Oracle or Sybase.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Account (applies to Managed)</td>
<td>The managed account name for the managed system that has been set up in the /tpam interface.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>URI (applies to Web Service)</td>
<td>Enter the URI (uniform resource identifier) of the ticket system. Include extra query string information if the URI requires it, but do not include any query string data that passes the actual ticket number. That information is defined on the Data tab.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Type: (applies to Web Service)</td>
<td>Select a type of HTTP POST, HTTP GET, REST GET, and REST POST as the protocol. As opposed to HTTP GET/POST, REST calls incorporate substitution values into the Ticket System URI instead of a query string or form body. This means that the instead of adding name/value pairs in the Data tab’s Web Service Parameters, you put the desired :name:</td>
<td>Yes</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Required?</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>XML Path (applies to Web Service)</td>
<td>The optional path entered here uses the XPATH 1.0 standard to reference specific subsections of the XML. If no path is entered the system uses the top level element as the base element for the returned data. Only simple element values are processed as data, no complex sub-elements or attributes are processed.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>XML Error Path: (applies to Web Service)</td>
<td>An error may be returned by the web service in one of two ways. If no value is entered for the XML error path the error is expected to be returned through an HTTP response value. If a value is entered the system examines the XML and considers it to be an error if the error path object is present. Make sure that the value entered for the error path is only present when the web service returns an error. If both the XML path and the XML error path are found in the returned XML the call is considered to have failed.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>User Name / Password (applies to Web Service)</td>
<td>If the web service requires a fixed username and password to perform validation enter those values here. If the web service supports anonymous calls leave these values blank</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>System Name / Account (applies to Web Service)</td>
<td>A TPAM managed system and account can be used to supply a username and password for the web service request. The managed system does not have to be a specific platform type and may be a different platform than that used by the web service. The system uses the account name and current account password as the user name and password for the call.</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
| Validation Expressions (applies to Manual) | Select from one of the following validation expressions:  
  - Any number or character  
  - Only umbers  
  - Only uppercase letters | Yes      | Any number or character |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Ticket Number (applies to Manual)</td>
<td>Enter in a ticket number to test the regular expression. The test ticket number is not saved.</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

- Any letters
- Letters, numbers, underscores
- Letters, numbers, underscores, dashes

### Data tab

The data tab is where the actual commands being issued against the target system to retrieve ticket information are configured.

### Special note regarding MySQL data sources

If your MySQL data source contains any columns with string data types which have a collation other than Latin1, you must use the following syntax in your SQL command:

```
; CharSet=X; YourSQLCommand
```

The semi-colon before CharSet and after X are required, and there are no spaces before or after the semi-colon. Replace the X with the name of the character set for the collation being used. For example:

```
; CharSet=utf8; select * from userintegration.usersource
```

Note that all of the string type columns which are present in the data set must use the same collation. You cannot have one returned column as Latin1 and another as utf8. The CharSet indicator is not needed if your result set contains only numeric, date, or time column types.

The table below explains the fields available on the ticket system data tab for the SQL command option.
### Table 27: Ticket System Management: Data tab options for SQL command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
</table>
| SQL Command          | Enter a simple SELECT query or execute a stored procedure to return a single row result set. Substitution parameters may be entered in the command using :param: syntax. Oracle databases only support SELECT type syntax, no EXEC stored procedure for a result set. SQL Server supports SELECT and EXEC. Case sensitivity is controlled by the target database. The SELECT and EXEC statement must be written to produce a result set of exactly one row if successful. When validating ticket numbers for requests a results set of zero rows or more than one row is considered as a failed validation.  

![NOTE: This command is executed against the target database. Please ensure that the database login has proper safeguards to prevent accidental or intentional loss of data.](image)

| Substitution Values  | This list shows all the valid substitution values from a file, password, session request or ISA retrieval. Not all values apply to all types of requests. Any values which are entered in this list are only used when testing the SQL command by clicking the Generate List button. The values are saved, but are global to all ticket systems. The values are not used during regular ticket validation. |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|---------|
| Fields Returned      | This is the list of fields returned from the SQL command that will be used for ticket validation. Field Names, types, and length are from the database result set description. These field names will be usable when building the validation rules for this ticket system. You can edit the description of the result set by clicking on each field entry and editing field name, type, or length using the controls to the right. You may also use these to manually create a result set if you cannot successfully test your SQL command. |
Web services

The table below explains the fields available on the ticket system data tab for the web services option.

**Table 28: Ticket System Management: Data tab options for web services**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Service Parameters</td>
<td>Web service parameters consist of one or more sets of parameter name and value pairs. The parameter name must be unique and may only contain letters, numbers, hyphens (-), underscores (_) and periods. The parameter value may be any of the ticket system substitution values, blank or static text. If static text is selected from the Parameter Value list, then up to 255 characters of static text can be entered. When the validation call is made the text is passed as is. If you enter static text that includes one of the :substitution: values in the Parameter Value list, it will become that substitution value when it is validated.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Substitution Values</td>
<td>This list shows all the valid substitution values from a file, password, or session Request or ISA Retrieval. Not all values apply to all types of requests. When using a substitution value in the SQL command make sure to put colons on either side of the value name and quote the string appropriately, e.g., ':AccountName:', not 'AccountName'. The values in the list are only used when testing the web service call via the <strong>Generate List</strong> button. The test values are saved, but they are global to all ticket systems. The values are not used during regular ticket validation. You should enter a value for any substitution you reference in the Web Service Parameters before clicking the <strong>Generate List</strong> button.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fields Returned</td>
<td>This is the list of fields returned from the web service call that will be used for ticket validation. Field Names, types, and length are</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Rules listing tab

The rules and rules details tabs are used to describe what to do with the data returned from the query to determine if a valid ticket number has been entered.

The Listing tab shows a summary of all rules defined for the currently selected ticket system. If a ticket is entered that requires validation, all the enabled rules associated with the ticket system are executed in the order shown in this list. If all rules return a true value then the ticket number is accepted. The first rule that returns a false value makes the ticket number invalid and the password/session/release request is canceled.

After a ticket system is added the Ticket Exists rule appears as a default. This rule ensures that the SQL command from the Data tab must return one and only one row. If the SQL command returns 0 (zero) or more than one row of data this rule fails and no further rule checking is performed. This rule cannot be moved or disabled and is always executed first.

### Rule details tab

The Rule Details tab lets you create arbitrarily complex rules that can be used to validate the data returned from the SQL command or web services call in the context where the ticket number is being used.

The table below describes the fields on the Rule Details tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Enter the rule name. It does not need to be unique. A default rule name is created based on the ID of the ticket system and the position in the list of rules.</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

Table 29: Ticket System Management: Rules: Rules Details tab options
<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
<th><strong>Required?</strong></th>
<th><strong>Default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A brief description about the rule.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>After the rule has been validated, select this check box to enable the rule.</td>
<td>No</td>
<td>Off</td>
</tr>
<tr>
<td>Syntax Results</td>
<td>Displays a WHERE clause-like version of the entered syntax. After the rule syntax is created and validated this read only area shows the syntax and/or any errors that were detected. If all the syntax looks acceptable the indicator turns green. If any portion of the syntax is invalid (bad quoting, missing group start or end, missing conjunction, and so on) the error is included in the Syntax Results and the indicator to the left of it turns red.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Sequence</td>
<td>This is a read only value showing the execution order of this rule.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOT</td>
<td>The NOT indicator at the left of the line and the conjunction on the right can each be cycled through their allowed values by clicking on the block. NOT toggles to either show the word NOT or blank.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND/OR</td>
<td>The Conjunction block cycles between AND, OR, and blank.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Row Above/Below buttons</td>
<td>If clicked, these buttons add a new row of syntax above or below the current row (indicated by the symbol). The conjunction block defaults to either AND or blank and the conditional defaults to =.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete Current Row button</td>
<td>If clicked, this button deletes the current row of syntax. The last row of syntax cannot be removed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear button</td>
<td>If clicked, this button clears the syntax area and creates a single, default line.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start Group button</td>
<td>If clicked, this button inserts a left parenthesis above the current row.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>End Group button</td>
<td>If clicked, this button inserts a right parenthesis below the current row.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validate button</td>
<td>If clicked, this checks all entered syntax and converts it to WHERE clause format in the TPAM 2.5.923 System Administrator Guide Ticket Systems 165</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Field Description

**Syntax Results area of the page.**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required?</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nesting Level</td>
<td>This is a read only value that attempts to keep track of start/end groupings. If the user has more start groups than end groups the value is greater than zero. If the user has more end groups than start groups the value is negative. The value here does not reflect the nesting level of the current line, only the total nesting level of the entire syntax area.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** The :PwdCurrentlyReleased: substitution value can only be used on the Rules tab, it cannot be used as a substitution value when entering the SQL command on the Data tab.

:PwdCurrentlyReleased: can be used to control the retrieval of a password by an ISA if the ISA is using the **Proxy Release For** field to act as a proxy for another user. It evaluates to Y or N according to the following rules:

- An ISA release where the ISA does not enter a value for the Proxy Release For field :PwdCurrentlyReleased: evaluates to “N”.
- An ISA release where the ISA does enter a value for “Proxy Release For”:
  - If another ISA has retrieved the password as a proxy for somebody AND the password has not yet been reset :PwdCurrentlyReleased: evaluates to “Y”
  - If the ISA issuing the request has already retrieved the password for a different proxy AND the password has not yet been reset :PwdCurrentlyReleased: evaluates to “Y”
  - If the password has been released due to an approved request AND the password has not yet been reset :PwdCurrentlyReleased: evaluates to “Y”
- A requester enters a request where the request window (Requested Release Date + Duration) overlaps an ISA Release where the ISA has entered a proxy then :PwdCurrentlyReleased: evaluates to “Y”
- Under all other conditions :PwdCurrentlyReleased: evaluates to “N”

### Add a ticket system

**To add a ticket system:**

1. Select **System Status/Settings | Ticket Systems** from the menu.
2. Click the **Add Ticket System** button.
3. Enter the information on the Details tab. For more information on this tab see Details tab on page 157.

4. Click the Save Changes button.

5. Click the Test Connection, Test Account, or Test Expression button to make sure that TPAM can connect to the ticket system. (Optional)

6. For manual ticket systems types, the set up is complete. For Not Managed, Managed and Web Service ticket system types click the Data tab.

7. Enter information on the Data tab. For more information on this tab see Data tab on page 161. Click Generate List button. Click the Save Changes button.

8. Click the Rules tab. (Optional) Define additional ticket validation rules. For more information see Rule details tab on page 164 and Add a ticket system rule on page 167.

Add a ticket system rule

To add a ticket system rule:

1. Select System Status/Settings | Tickets Systems from the menu.
2. Select the ticket system from the Listing tab.
3. Click the Rules tab.
4. Click the Add Rule button.
5. Enter the data for the rule using the fields described in Rule details tab on page 164.
6. Click the Save Changes button.

To prioritize the order that the ticket system rules are executed, select a rule on the Listing tab and click the Move Up and Move Down buttons as needed.

Duplicate a ticket system rule

To duplicate a ticket system rule:

1. Select System Status/Settings | Tickets Systems from the menu.
2. Select the ticket system from the Listing tab.
3. Click the Rules tab.
4. Select the rule to duplicate.
5. Click the Duplicate Rule button.
6. The name, description, and syntax of the rule is copied, but is disabled by default.
Delete a ticket system rule

To delete a ticket system rule:
1. Select System Status/Settings | Tickets Systems from the menu.
2. Select the ticket system on the Listing tab.
3. Click the Rules tab.
4. Select the rule to be deleted.
5. Click the Delete Rule button.
6. Click the OK button on the confirmation window.

Duplicate a ticket system

To duplicate a ticket system:
1. Select System Status/Settings | Tickets Systems from the menu.
2. Select the ticket system to duplicate on the Listing tab.
3. Click the Duplicate button. The new ticket system will be saved with a default name of Copy of XXXXXXX and validation will be disabled by default.

Delete a ticket system

Any ticket system that is assigned to a system, account, or file will revert to Require a Ticket Number from Any Ticket System, if the assigned ticket system is deleted.

To delete a ticket system:
1. Select System Status/Settings | Tickets Systems from the menu.
2. Select the ticket system to be deleted on the Listing tab.
3. Click the Delete Ticket System button.
4. Click the OK button on the confirmation window.
Custom Logo

Introduction

Customers have the ability to upload a custom logo, that will be displayed in the header of the TPAM web interface.

File requirements

In order to be uploaded as a custom logo the file must meet the following requirements:

- JPEG, PNG, GIF or BMP file format
- GIF files must be static, no animation allowed
- Maximum size of 30KB
- Image dimensions must be between 10H x 10W and 47H x 120W pixels

Upload custom logo

To upload a custom logo:

1. From the /admin interface, select System Status/Settings | Custom Logo Image from the menu.
2. Click the Select File button.
3. Click the Browse button and locate your logo file.
4. Click the Upload button. Once the image is loaded you will see a preview of what the header will look like with your logo added.
5. Click the Apply Sample Logo button.
6. Click the **OK** button on the confirmation window.
7. Refresh the page to see new header.

## Remove custom logo

**To remove a custom logo from the header of the TPAM interface:**

1. From the `/admin` interface, select **System Status/Settings | Custom Logo Image** from the menu.
2. Click the **Remove Logo** button.
3. Click the **OK** button on the confirmation window.
4. Refresh the page.
License Management

Introduction

When initially configuring your TPAM appliance you need to update the license quantities that were purchased. This is also needed if additional licenses are purchased at a later date.

The table below describes the different license options for TPAM.

Table 30: License options for TPAM

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxSystems</td>
<td>Maximum number of systems that can be managed in the Privileged Password Manager module of TPAM. A system is defined as a device that has a unique IP address or unique IP address/port. Soft deleted systems, system templates, and PSM only systems, are not included in this count.</td>
</tr>
<tr>
<td>MaxUsers</td>
<td>Maximum number of users that can be created in TPAM. All user IDs are included in this count, with the exception of cache user types.</td>
</tr>
<tr>
<td>MaxCachedAccounts</td>
<td>The number of accounts that can be assigned to a cache server.</td>
</tr>
<tr>
<td>MaxCacheServers</td>
<td>The number of cache servers that can be configured in TPAM.</td>
</tr>
<tr>
<td>MaxDesktops</td>
<td>Maximum number of desktops that can be managed in the Privileged Password Manager module of TPAM. If you add and save more desktops in TPAM than the limit set here, available system licenses will be used until that limit is met.</td>
</tr>
<tr>
<td>MaxSessions</td>
<td>Maximum number of concurrent sessions, whether they are live sessions or replays.</td>
</tr>
<tr>
<td>MaxSPCWSystems</td>
<td>The number of managed systems that can be added under one of the SPCW platforms.</td>
</tr>
<tr>
<td>MaxDPAs</td>
<td>The number or DPAs that be configured in TPAM. Total includes virtual and physical DPAs.</td>
</tr>
</tbody>
</table>
Adjust license limits

System Administrators have the ability to adjust the license limits on the TPAM appliance.

**To adjust license limits:**
1. Select **System Status / Settings | License Management** from the menu.
2. Enter a number for the Current Limit for each license needed.
3. **IMPORTANT:** Changing license limits has financial implications. License usage will be reviewed with One Identity at the time of maintenance renewal.
4. Click the **Save Changes** button.

License management change log

A record of any changes to the license counts is recorded in a change log. The license management change log displays server time (UTC).

**To view the change log:**
1. Select **System Status / Settings | License Management** from the menu.
2. Click the **Change Log** tab.
3. Click the **Export to Excel** or **Export to CSV** buttons to save the data offline.
Login Banner and Message of the Day

Introduction

The login banner and message of the day are two ways that TPAM system administrators can post information for users that log on to TPAM. They can be customized to display any text, such as a company policy or legal warning message.

Login banner

To add/edit a login banner:

1. Select System Status/Settings | Login Banner from the menu.
2. Enter a message.
3. Click the Save Settings button.

Upon logging on to the /tpam, /admin, or/config interface the login banner will be presented to the user as shown below prior to landing on the home page.

Message of the day

Message of the day is a brief text message that will appear on the home page of the /tpam and /admin interfaces. The message of the day can also be added as an optional message body tag in the email notifications sent by TPAM. The tag for message of the day is :MOTD:. See Configure email notification for more details.
To configure the message of the day:

1. Select **System Status/Settings | Message of the Day** from the menu.
2. Click the **New Message** button.
3. Enter a start date/time for the message.
4. Enter an end date/time for the message.
5. Enter the message.
6. Click the **Save Changes** button.

The message of the day will be displayed on the TPAM home page.
Net Tools

Introduction

To assist the TPAM System Administrator with troubleshooting common network related problems, TPAM contains network tools that are accessible from the configuration interface. In addition, some specialized configurations can be made to add or manage static routes.

The ping utility

The ping utility can be used to verify connectivity to remote hosts and determine latency. Many of the optional parameters for the ping command are available. The available command options are listed along with the short description of each.

To use the ping utility:

1. Select Net Tools | Ping from the menu.
2. Enter the IP or Hostname.
3. Select the options desired.
4. Click the Ping button. The results will be displayed.

Nslookup utility

Nslookup is a common TCP/IP tool used to test DNS settings and perform similar information gathering using DNS resolution. The TPAM utility for nslookup will use the DNS server(s) configured to TPAM only. The option to specify a server is not provided. TPAM System Administrators can benefit from the ability to use nslookup to resolve hostnames to IP addresses and vice versa.
To use **Nslookup**:

1. Select **Net Tools | Nslookup** from the menu.
2. Enter the IP address or Hostname to look up.
3. Click the **Lookup** button.

**TraceRoute utility**

The traceroute utility is available for examining network routing and connectivity from TPAM to a remote IP address or hostname. The use of traceroute is often disallowed by firewalls, routers, and other network security infrastructure – but if allowed, it can be a valuable diagnostic tool.

To use **Traceroute**:

1. Select **Net Tools | TraceRoute** from the menu.
2. Enter the IP or Hostname to trace.
3. Select the `-d` check box. (Optional)
4. Change the default number of hops and timeout wait. (Optional)
5. Click the **Trace** button.

**Telnet test utility**

The Telnet test utility lets a test be performed from the appliance to another system over a specific port. The tool will test the defined port using telnet functionality to verify the port, whether a connection can be made, and then immediately close the connection.

To use the **Telnet test utility**:

1. Select **Net Tools | TelnetTest** from the menu.
2. Enter the network address, port and timeout period.
3. Click the **Trace** button.

**Route table management**

Several tools are available to manage the routing table on TPAM, if the need arises.

**IMPORTANT:** It is strongly recommended that the routing tools not be used unless
absolutely necessary and a network engineer is consulted for the proper routes required. Incorrectly defining a route can cause a communication outage.

To display current routes:

1. Select Net Tools | Show Routes from the menu.

To add a route:

1. Select Net Tools | Add Route from the menu.
2. Enter the IP address of the destination host or network, the proper subnet mask, and the default gateway for the new static route.
3. Select Check to make this route permanent, to retain the route after a reboot of the appliance.

To delete a route:

1. Select Net Tools | Delete Route from the menu.
2. Enter the IP address of the destination host.
3. Click the Delete Route button.
System, O/S Patch, and Job Status Pages

Introduction

The O/S patch status page and the system status page provide important information about the patch level of the TPAM appliance.

O/S patch status

Patches for the underlying operating system of TPAM are posted in the same manner as software updates and are applied using the same method. See Apply a software update for details. To view the history of patches applied to the operating system select System Status/Settings | O/S Patch Status from the menu. The install date and time displayed is server time (UTC).

System status page

The system status page displays valuable information about the TPAM appliance such as license levels, software version, build number, serial number, memory and CPU usage.

To view the system status page select System Status/Settings | System Status from the menu.

NOTE: The PPM systems defined does not include the 2 default local appliances.
System status graphs

The system status graphs provide a visual presentation of key statistics for system administrators and technical support. There are three categories of time series graphs:

- Appliance - appliance or OS information.
- Application - PSM or PPM statistics
- Cluster - High availability and replication statistics

There are three possible time frames for the graphs:

- Daily - displays the last day’s data, sometimes with prior day's average for comparison, updated every minute.
- Weekly - displays the last week’s data, sometimes with prior week's average for comparison, updated every 15 minutes.
- Yearly - displays the last year's data, updated every 60 minutes.

When a prior period average is graphed for comparison it is rendered as a dotted line.

To view the graphs select System Status/Settings | System Status from the menu. Click the Graphs tab. The time displayed on the graphs is server time (UTC).

Select the Auto-refresh check box to refresh the graphs every 60 seconds or click the Refresh Graphs button to refresh them on demand. You can choose to display Daily, Weekly or Yearly graphs by selecting the check boxes.

The following appliance graphs are available:

<table>
<thead>
<tr>
<th>Graph name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Logins</td>
<td>The number of active logins on each of the TPAM web sites (/admin, /config and /tpam).</td>
</tr>
<tr>
<td>Database Backup Set Usage</td>
<td>Amount of disk space used by full and incremental backups in the database backup set (varies due to daily backup job and replication activity). When the total size of the incremental backup size grows continually over time it indicates that regular full backups are not occurring. The size of the last full backup is also visible.</td>
</tr>
<tr>
<td>C: Disk Free</td>
<td>Percentage of the system disk that is free. If free disk space is trending down for long periods of time it may indicate that a problem is occurring.</td>
</tr>
<tr>
<td>C: Disk Time</td>
<td>Percentage busy of the system disk for read and write activity. If the disk is busy for long periods of time it may indicate that a problem is occurring.</td>
</tr>
<tr>
<td>C: Disk Transfer</td>
<td>Read/write throughput for the system disk.</td>
</tr>
<tr>
<td>OS CPU Time</td>
<td>Percent utilization of the appliance CPUs by user and system</td>
</tr>
<tr>
<td>Graph name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OS Paging Activity</td>
<td>Multiple measures of OS low-level virtual memory activity.</td>
</tr>
<tr>
<td>OS Memory Utilization</td>
<td>Total amount of memory allocated by the OS versus total amount of free memory. Note that the OS and database will tend to use large amounts of memory for buffer caches.</td>
</tr>
<tr>
<td>OS Scheduler Objects</td>
<td>Total number of processes and threads managed by the OS. Also shows the number of processes that are waiting in the run queue. If the number of processes or threads is trending up for long periods of time it may indicate that a problem is occurring. If a large number of processes are waiting in the run queue for long periods of time it indicates that the system is CPU-bound.</td>
</tr>
<tr>
<td>Primary/Config Interface Network Utilization</td>
<td>Total amount of traffic sent/received on network interfaces</td>
</tr>
<tr>
<td>SQL User Connections</td>
<td>Total number of database connections. If the number of database connections is trending up for long periods of time it may indicate that a problem is occurring.</td>
</tr>
<tr>
<td>SQL Query Activity</td>
<td>Multiple measures of database activity.</td>
</tr>
<tr>
<td>Other SQL Graphs</td>
<td>Multiple views of database server information. Used by TPAM developers and support.</td>
</tr>
</tbody>
</table>

The following application graphs are available:

**Table 32: System Status: Graphs tab Application Graphs**

<table>
<thead>
<tr>
<th>Graph name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured Accounts</td>
<td>Total number of accounts.</td>
</tr>
<tr>
<td>Configured Systems</td>
<td>Total number of systems.</td>
</tr>
<tr>
<td>Configured Users</td>
<td>Total number of TPAM users.</td>
</tr>
<tr>
<td>PSM Active Sessions</td>
<td>Active sessions, on both the local console appliance as well as all DPAs.</td>
</tr>
<tr>
<td>PSM Session Requests</td>
<td>Session request activity.</td>
</tr>
<tr>
<td>PPM Releases</td>
<td>Password release activity.</td>
</tr>
</tbody>
</table>
### How to create a support bundle

In order to troubleshoot issues with your TPAM appliance, Technical Support may ask you to generate a support bundle. The support bundle includes vital information about the TPAM appliance.

The support bundle is an un-encrypted file but does not contain any sensitive customer data such as passwords, only information about the appliance itself.

**To create a support bundle:**

1. Select **System Status/Settings | System Status** from the menu.
2. Click the **Support Bundle** tab.
3. Based on your conversation with technical support, select/clear the check boxes in the Optional Items section. Enter a Start and End Date to narrow the results.
4. Click the **Create Support Bundle** button. Once the bundle is complete it is displayed in the Bundle list.
5. Select the bundle name from the list that you want to download.
6. Click the **Download Bundle** button.
7. Click the **OK** button to save the file offline. Now the zip file can be emailed to Technical Support.

To delete all bundles click the **Delete All Bundles** button.

### Job status page

The job status page lists all TPAM quartz jobs and their current status. To view the system status page select **System Status/Settings | Job Status** from the menu. To run a job manually, select the job from the list and click the **Run Job Once** button. If a job seems stuck click the **Reset Job** button to reset the job schedule.
Software Updates

Introduction

This chapter covers the process to update your TPAM appliance with the latest software patches provided by One Identity.

Product patches are not always cumulative. This means that some product patches must be applied to the system in order and none can be skipped. The release notes for each product update list the prerequisite version of TPAM required before the update can be applied to the appliance.

To apply a patch to TPAM perform the following steps:

- Check the current version of TPAM
- Take a backup. See On demand backup
- Download the patch from the Customer Portal
- Stop any applicable agents
- Apply the Patch
- Check the Patch Log for errors
- Restart any applicable agents

Types of software updates

There are several different types of software updates that are released for the TPAM appliance.

- Hotfix - a hotfix is a single, cumulative package that includes one or more files that are used to address a problem in the product that cannot wait until the next scheduled upgrade. A hotfix does not increment the software version number.
- Feature Pack - a feature pack is new product functionality that is distributed outside the context of a product release and is typically included in the next scheduled upgrade. The software version number is changed after an upgrade.
- **Upgrade** - an upgrade is a software package that replaces an installed version of TPAM with a newer version of the product. The software version number is changed after an upgrade.

- **OS Patches** - patches for the specific purpose of upgrading the underlying TPAM OS. These patches bear the distinct naming convention beginning with TPAM_OS.

- **Documentation Patch** - these patches update the online documentation available under the Help menu in TPAM.

### Check TPAM current version

The current version of the TPAM appliance can be found by clicking on the user menu and selecting **About TPAM**.

### Download a software update from the customer portal

**To download a software update:**

2. Select **Software Downloads** from the menu on the left of the page.
3. Enter filter criteria to narrow the results of the downloads listed.
4. Click the on the download you want. For major releases you need to also need to download the key file.
5. Click the **Add to Downloads** button.
6. Click the **Download Now** button and save the file locally.

### Apply a software update

**TIP:** If the software update you are applying is a software upgrade, which will change the version number of the software you are running, it is strongly recommended that the appliance have a run level of "maintenance" before applying the update. By changing the run level users in a session running on the appliance will be given a warning before their session is terminated. For more details see **Change the run level**.
TIP: If the software update you are applying is a major upgrade that takes several minutes to apply, you may be advised in the release notes to increase the failover timeout on the replica appliances in your cluster. This will prevent the replicas from failing over during the patch process.

**To apply a software update:**

1. Log in to the /admin interface.
2. Select **Maint | Apply a Patch** from the menu.
3. Click the **Select File** button.
4. Click the **Browse** button. Select the patch file that you saved locally.
5. Click the **Upload** button.
6. Open the .key file that you downloaded and copy and paste this key in the in the **Key** box.
7. Type `/genkey` in the Options box.
8. By default, if you are applying a patch to a primary member of a cluster, the replicas in the cluster will be listed and highlighted in the Target Replicas list. If any of the replicas are deselected, the patch will not be applied to it. The replica can be patched at a later date by logging on directly to the /admin interface of the replica. If the software version numbers (excluding the build number) of the primary and the replica still match them the primary will still be able to send data to the replica. We recommend that you contact Technical Support before deciding to deselect any of the replicas on this list.

   **NOTE:** Any replicas that have a status of **Not Active** will not be patched.

9. Click the **Apply Patch** button.
10. To verify the status of the patch installation click the **Patch Log** tab.

   **TIP:** After a patch has installed on the primary and any replicas, a reboot of the primary and replicas is strongly recommended.

**View patch log**

It is recommended that Patch Log be reviewed after each upgrade to look for errors or other messages that may require action. The patch log displays time in server time (UTC).

**To view the patch log:**

1. Log in to the /admin interface.
2. Select **Maint | View Patch Log** from the menu.
3. Enter your search criteria on the Filter tab.
4. Click the Results tab.

**View patch history**

Patch history allows you to view a cumulative history of all updates that have been applied to the TPAM appliance. The patch history results display time in server time (UTC).

**To view patch history:**

1. Log in to the /admin interface.
2. Select **Maint | View Patch History** from the menu.
3. Enter your search criteria on the Filter tab.
4. Click the Results tab.
Shut Down/Restart the Appliance

Introduction

If the need arises to shutdown or restart your appliance this can be done from the /config or /admin interface.

Shutdown appliance

To shutdown the appliance:
1. Select Shutdown from the /config or /admin menu.
2. Clear the Restart? check box.
3. Click the Shutdown button.
4. Click the OK button on the confirmation window.

Restart appliance

To restart the appliance:
1. Select Shutdown from the /config or /admin menu.
2. Make sure the Restart? check box is selected.
3. Click the Shutdown button.
4. Click the OK button on the confirmation window.
Introduction

In the event of a catastrophic failure a System Administrator can restore the data using an offline backup to another appliance. Another use for restore is for test environments where customers may be testing an upgrade to a new version of TPAM.

- **IMPORTANT:** Applying a restore will stop the automation engine, mail agent, and auto discovery agents. These will not automatically restart when the restore is complete, even if the auto start check boxes were selected prior to the restore.

- **IMPORTANT:** Applying the restore will set any non-primary cluster members (replicas, DPAs) to inactive. Once the restore is complete these will have to manually be set to active on the cluster management page.

Restore from a backup

- **IMPORTANT:** Do not rename backup files. Doing so will cause the restore to fail.

- **IMPORTANT:** If applying a restore from one appliance to another, verify that the software version of the appliance you performing the restore on is the same version as the appliance the backup was taken from. The software version can be found under the User Menu | About TPAM.

*To restore the data from a backup:*

1. First the appliance must have a run level of “maintenance” and have a role of "Primary". From the /admin interface select System Status/Setting | Cluster.
2. Select appliance from the cluster member list.
3. Select the Run Level check box.
4. Select Maintenance from the Run level list.
5. Click the Change Run Level button.
6. Click the Continue with Change button. This puts the appliance in maintenance mode.
7. From the /config interface select Restore | Restore Appliance from the menu.
8. Use one of the following methods to select the backup file:
   - Select a file from the Online Backup list.
   - Select Upload Backup File. Click the Select File button. Click the Browse button and select the file. Click the Upload button.
   - Select Retrieve from Archive Server. Select an archive server from the list. Select a file from the archive server.

   NOTE: The archive server has to either be a *nix box and allow the "ls -l" command via the archive user OR if it's a windows box it needs to recognize the "ls -l" and treat it like a "dir" command (or have a cygwin or posix environment that understands ls).

9. If the backup file has secondary encryption, enter and confirm the password.
10. If any options have been provided by Technical Support enter them in the Options field, otherwise, leave it empty.
11. Click the Restore Now button.
12. Click the OK button on the confirmation window.
13. You will be disconnected from the /config interface. Log on to the /admin interface.
14. Select Restore | View Restore Log. The restore log displays results in server time (UTC).
15. Click the Results tab to monitor the progress of the restore. Once the restore is complete, log on to the /admin interface and select System Status/Setting | Cluster Management.
16. Select appliance from the cluster member list.
17. Select the Run Level check box.
18. Select Operational from the Run level list.
19. Click the Change Run Level button.
20. Click the Continue with Change button. This puts the appliance in operational mode.
Apply backup to a cluster

If your appliances are currently configured in a cluster, with a primary device and one or more replicas, the backup is applied to the primary device and the data will be replicated to the replicas. During the restore process any replicas and DPAs enrolled in the cluster will automatically be flagged as Not Active. After the restore on the primary is complete all these appliances must be flagged as active again so that replication can begin again.

To apply a backup to a cluster:

1. Follow steps 1 through 20 in the above procedure.
2. On the cluster management page select one of the replicas in the cluster.
3. Select the **Appliance Active** check box.
4. Select **Active** from the list.
5. Click the **Save** button.
6. Repeat steps 2-6 for all other appliances enrolled in the cluster, including DPAs.

**IMPORTANT:** When making the replicas active again after the restore you may initially see the message that the IP address is not yet registered in the cluster. This is a timing issue and should resolve itself within a few minutes.

Revert to factory default

Reverting the appliance to the factory default will erase all the data and configuration settings you have entered since you have received the box. Once the system revert is complete, a monitor and keyboard will have to be connected to the appliance to start configuration of the appliance from scratch.

**IMPORTANT:** Do not perform a revert to factory default without the assistance of Technical Support.

**NOTE:** The appliance must have a run level of Maintenance to allow a system revert.

To perform a system revert:

1. From the `/config` interface, select **Restore | System Revert** from the menu.
2. If the appliance is already in maintenance mode process to step 8. To change the appliance to maintenance mode log on to the `/admin` interface and select **System Status/Setting | Cluster Management**.
3. Select the appliance from the list.
4. Select the **Run Level** check box.
5. Select **Maintenance** from the list.
6. Click the **Change Run Level** box.
7. Click the **Continue with Change** button on the confirmation window.
8. Select the **Appliance Factory Defaults** restore point.
9. Click the **Revert** button.
10. Click the **OK** button on the confirmation window.

After the revert is complete a keyboard and monitor must be connected to the appliance and configuration must start from scratch. Refer to the TPAM Quick Start Guide for instructions.

**Revert to restore point**

A restore point is a snapshot taken of TPAM at a specific point in time. Restore points are created by TPAM automatically in two instances:

- Prior to applying specific patches, as indicated in the release notes. If there are issues with the patch after it is applied, reverting to the restore point allows you to roll back as if the patch was never applied.
- Prior to enrolling a replica in a cluster. If the enrollment process has errors the appliance can be reverted to that restore point.

A restore point can be applied to an appliance through the TPAM web interface or through the CLI.

**To revert to a restore point using the TPAM web interface:**

1. Log on to the admin interface of the appliance you want to restore.
2. select **System Status/Settting | Cluster Management**.
3. Select the appliance from the list.
4. Select the **Run Level** check box.
5. Select **Maintenance** from the list.
6. Click the **Change Run Level** box.
7. Click the **Continue with Change** button on the confirmation window.
8. Log on to the config interface of the appliance you want to restore.
9. Select **Restore | System Revert** from the menu.
10. Select the restore point to revert to.
11. Click the **Restore** button.
12. Click the **OK** button on the confirmation window.
IMPORTANT: Restoring an appliance can take some time. If you are unsure whether the restore is still running check with technical support.

To revert to a restore point using the CLI:

1. Log on to the appliance using the CLI system administrator user ID.
2. Run the ListRestorePoints command to see the snapshots available.
3. Run the Revert command with the sequence number of the selected snapshot.

NOTE: The appliance must be in maintenance mode before the Revert command can be run.
Remote Access

Introduction

Remote access to the /config interface is enabled by default. When enabled, TPAM will allow access to the /config interface through port 8443. To access the /config interface remotely enter https://[IP address]:8443/config.

Disable remote access

To disable remote access:

1. From the /config interface select Remote Access from the menu.
2. Select Disabled from the list.
3. Click the Save Changes button.
CLI Commands for the System Administrator

Introduction

The TPAM command line interface (CLI) provides a method for authorized system administrators or automated processes to retrieve information from the TPAM system. Commands must be passed to TPAM via SSH (secure shell) using an identity key file provided by TPAM. A specific CLI system administrator user ID is also required. See Add a CLI Sys Admin user for more details on creating the user ID. CLI user IDs are case sensitive when logging on.

SSH software must be installed on any system before it can be used for TPAM CLI access.

Commands accept parameters in the style of --OptionName option value (two dashes precede the option name) with the exception of the GetStatus command. Existing commands prior to TPAM v2.2.754 still also accept the comma-separated syntax, so existing scripts do not need to be modified unless you wish to take advantage of new parameters that have been added to the command in later versions of TPAM.

All commands recognize an option of --Help. This expanded help syntax will show all valid options for each command, whether the option is required or optional, and a description of the option and allowed values.

Command standards

- Options may be specified in any order in the command
- Option names are not case sensitive, --SystemName and --systemname are equivalent
- When the --Help option is used, no other processing takes place. The help text is printed and the command terminates.
- Options marked as “optional” are just that – optional. They do not need to be included in the command line to “save space” for commands that come afterwards.
Option names may be abbreviated “to uniqueness” for each command. For example if a command accepts options of --SystemName, --AccountName, and --Description the option names can be abbreviated to --S, --A, and --D, respectively. However if the options were --AccountName and --AccountDescription they can only be abbreviated to --AccountN and --AccountD.

Any option value that contains spaces, e.g., --Description or --RequestNotes, must surround the description with single or double quotes, depending on your command line shell. It’s also recommended that you surround the entire command invocation with quotes to prevent the shell from unintentionally stripping desired quotes from your command. Additionally your shell environment may require escaping extra quotes within your command. The following is an example using Windows cmd.exe

```bash
[...]"UpdateSystem[...]"Sytem1[...]"Description for System1"[...]
```

## Commands

### ApplyPatch --options

Installs a software update. Prerequisite is that the patch file must first be uploaded to TPAM vis SCP.

**Table 33: ApplyPatch options**

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--PatchName</td>
<td>Req</td>
<td>Patch file name. Include the .ZIP extension.</td>
</tr>
<tr>
<td>--Key</td>
<td>Req</td>
<td>The patch key generated for your appliance.</td>
</tr>
<tr>
<td>--Clear</td>
<td>Opt*</td>
<td>Clear the patch log. All other options are ignored if --Clear is used.</td>
</tr>
<tr>
<td>--Options</td>
<td>Opt</td>
<td>Supply these only if instructed by technical support.</td>
</tr>
<tr>
<td>--ExcludeList</td>
<td>Opt</td>
<td>List of cluster member appliance names to exclude. The default is to include all cluster member appliances when applied to the primary and local only when applied to a replica. Semicolon separated.</td>
</tr>
</tbody>
</table>

Legacy support:

ApplyPatch PatchName.zip key [/options]

### Backup

Schedules a backup to be taken immediately. No parameters.
ChangeAdminPassword--options
Forces a change to the password for the system administrator user listed.

Table 34: ChangeAdminPassword options

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--UserName</td>
<td>Reg</td>
<td>User ID that you want to change the password for. The user cannot be a CLI user.</td>
</tr>
<tr>
<td>--Password</td>
<td>Req</td>
<td>New password for the user ID. If password contains spaces or other non-alphanumeric characters it must be enclosed in double quotes.</td>
</tr>
</tbody>
</table>

Legacy support:
ChangeAdminPassword UserName Password

CreateSupportBundle
Creates a support bundle.

Table 35: CreateSupportBundle options

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
</table>
| --OptionalFiles | Opt     | Either "All" or a semi-colon list of optional files to include in the support bundle. If no files are specified "All" will be used. All may be used in combination with files to exclude by preceding each file with ",", i.e., All; ALERTLOG; PROCLOG would generate a support bundle with all optional files except ALERTLOG and PROCLOG. Valid optional file names are as follows:
ADMINACTIVITYLOG, ALERTLOG, AUTOAGENTSETTINGS, AUTOAGENTSTATUS, AUTODISCOVERYAGENTLOG, BACKUPHISTORY, BACKUPLOG, BACKUPSETTINGS, DAILYMAINTLOG, GLOBALSETTINGS, MAILAGENTLOG, MIGRATIONLOG, MIGRATIONPROCESS, PATCHHISTORY, PATCHLOG, PROCLOG, PROFILESCHEDULES, SCHEDULEDJOBSTATUS, SCHEDULEDJOBSTATUSLOCAL, SESSSERVERLOG, SQLLOG, TESTPWDSCHEDULE |
## Option name | Req/Opt | Description
---|---|---
--StartDate | Opt | An optional start date to be applied to all files that can be date filtered. If either --StartDate or --EndDate are supplied both values must be included. All dates and times must be specified in server time (UTC).

### --EndDate
Opt
An optional end date to be applied to all files that can be date filtered. If either --StartDate or --EndDate are supplied both values must be included. All dates and times must be specified in server time (UTC).

### FlushDNS
Attempts to flush the DNS settings on the appliance immediately. Take no parameters.

### ForceFailover
Allows you to force or unforce a failover from the primary to the replica or from the replica to itself.

#### Table 36: ForceFailover options

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--force</td>
<td>Opt</td>
<td>Used to force a failover to the replica.</td>
</tr>
<tr>
<td>--unforce</td>
<td>Opt</td>
<td>Used to unforce the failover to the replica.</td>
</tr>
</tbody>
</table>

### GetChangeQueue
Returns the current number of pending changes. Takes no parameters.

### GetStatus--options
Get information on specified statistics. You must select at least one option to display.

#### Table 37: GetStatus options

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>Opt</td>
<td>All information. Option to pass the appliance name of a primary or replica in the cluster. The local appliance is the default.</td>
</tr>
<tr>
<td>Option name</td>
<td>Req/Opt</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>-c</td>
<td>Opt</td>
<td>Cluster status. Option to pass the appliance name of a primary or replica in the cluster. The local appliance is the default.</td>
</tr>
<tr>
<td>-db</td>
<td>Opt</td>
<td>Database status/state.</td>
</tr>
<tr>
<td>-h</td>
<td>Opt</td>
<td>Usage information.</td>
</tr>
<tr>
<td>-i</td>
<td>Opt</td>
<td>Appliance information. Option to pass the appliance name of a primary or replica in the cluster. The local appliance is the default.</td>
</tr>
<tr>
<td>-p</td>
<td>Opt</td>
<td>OS patches applies to the system. Option to pass the appliance name of a primary or replica in the cluster. The local appliance is the default.</td>
</tr>
<tr>
<td>-q</td>
<td>Opt</td>
<td>Automation agent status and queue counts. Not available on a non-failed over replica.</td>
</tr>
<tr>
<td>-r</td>
<td>Opt</td>
<td>Process information on selected TPAM related processes, services, daemons, and other background tasks.</td>
</tr>
<tr>
<td>-s</td>
<td>Opt</td>
<td>System status information</td>
</tr>
<tr>
<td>-u</td>
<td>Opt</td>
<td>Appliance uptime. Option to pass the appliance name of a primary or replica in the cluster. The local appliance is the default.</td>
</tr>
<tr>
<td>-x</td>
<td>Opt</td>
<td>Resources used: CPU utilization, memory virtualization, last reset time of network adapter, disk space used/available. Option to pass the appliance name of a primary or replica in the cluster. The local appliance is the default.</td>
</tr>
</tbody>
</table>

**GetTestQueue**

Returns the current number of entries in the test queue. No parameters.

**ImportIntermediateCert**

As of TPAM v2.5.909 this command is now obsolete. This function can be done through the TPAM web interface.

**ListBackups--option**

Lists available online backup files.
ListBackups option

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ArchiveServer</td>
<td>Opt</td>
<td>The name of an archive server where backups are stored.</td>
</tr>
</tbody>
</table>

ListRestorePoints

Returns a list of all restore points currently available for revert on the appliance. Takes no parameters.

ListUsers--options

Lists all non-CLI system administrator users defined in TPAM.

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--UserName</td>
<td>Opt</td>
<td>User name to filter. Use * for wildcard.</td>
</tr>
<tr>
<td>--EmailAddress</td>
<td>Opt</td>
<td>Email address to filter. Use * for wildcard.</td>
</tr>
<tr>
<td>--Status</td>
<td>Opt</td>
<td>Filter for ENABLED, DISABLED, LOCKED, or ALL (default).</td>
</tr>
<tr>
<td>--ExternalAuthType</td>
<td>Opt</td>
<td>obsolete, replace by --SecondaryAuthType</td>
</tr>
<tr>
<td>--SecondaryAuthType</td>
<td>Opt</td>
<td>Filter for SAFEWORD, SECUREID, LDAP, WINAD, RADUIS, DEFENDER, NONE, or ALL (default).</td>
</tr>
<tr>
<td>UserCustom(1-6)</td>
<td>Opt</td>
<td>Filter based on contents of user custom level columns. Ignored if the appropriate custom column has not been defined in Global Settings.</td>
</tr>
<tr>
<td>--SortOrder</td>
<td>Opt</td>
<td>Sort results by UserName (default), FirstName, or LastName.</td>
</tr>
<tr>
<td>--MaxRows</td>
<td>Opt</td>
<td>Maximum number of rows to return. The default is 25.</td>
</tr>
</tbody>
</table>

Restore--options

Restore TPAM using the specified backup file.

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--BackupName</td>
<td>Req</td>
<td>Name of the backup to restore, including the .ZIP extension.</td>
</tr>
</tbody>
</table>
Option name | Req/Opt | Description
---|---|---
--Password | Req | Either the secondary encryption password or the phrase NOPASSWORD. The password is case sensitive. If the password contains spaces or other non-alphanumeric characters it must be surrounded by double-quotes.
--ArchiveServer | Opt | The name of an archive server where backups are stored. The archive server must be
--NoDB | Opt | Do not pass a value with this parameter, just use --NoDB. Normally the appliance must have a run level of maintenance to perform a restore. If the appliance cannot be put in maintenance mode the --NoDB parameter can be used to override this requirement and perform an emergency restore.

Legacy support:
restore TPAM_YYYYMMDD_HHMMSS.zip[<2 EncryptionPassword>:NOPASSWORD [/nodb]]

Revert--option
Revert the TPAM appliance to a specified restore point.

Table 41: Revert option
<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
</table>
| SequenceNumber | Req | Valid sequence number of a restore point.

RunLevel--options
Used to display the current run level for an appliance (operational or maintenance) or set the run level for an appliance.

Table 42: RunLevel option
<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--Action</td>
<td>Opt</td>
<td>Indicate whether to retrieve or set the current run level. If no action is specified GET is assumed. If action of SET is supplied then --RunLevel must be provided. GET/SET</td>
</tr>
<tr>
<td>--ApplianceName</td>
<td>Opt</td>
<td>If no appliance name is provided then the local appliance is assumed. If appliance name is provided it must be a TPAM appliance and not a DPA.</td>
</tr>
</tbody>
</table>
Option name | Req/Opt | Description
---|---|---
--RunLevel | | Required if --Action is SET. OPERATIONAL/MAINTENANCE

**Shutdown--options**

Shuts down or reboots the TPAM appliance.

**Table 43: Shutdown options**

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--Reboot</td>
<td>Req*</td>
<td>Shutdown the appliance and restart.</td>
</tr>
<tr>
<td>--NoReboot</td>
<td>Req*</td>
<td>Shutdown</td>
</tr>
</tbody>
</table>

Legacy support:

Shutdown /R (for reboot)
Shutdown /N (for shutdown)

**SSHKey--options**

Retrieves system standard keys.

**Table 44: SSHKey option**

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--KeyFormat</td>
<td>Opt</td>
<td>Format of the SSH key output - OpenSSH (default) or SecSSH.</td>
</tr>
<tr>
<td>--StandardKey</td>
<td>Req*</td>
<td>Name of the system standard key to export.</td>
</tr>
</tbody>
</table>

**UnlockAdminUser--option**

Unlocks system administrator user IDs. Cannot unlock CLI users.

**Table 45: UnlockAdminUser option**

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--UserName</td>
<td>Req</td>
<td>Name of user to unlock. Cannot unlock CLI users.</td>
</tr>
</tbody>
</table>

Legacy support:

UnlockAdminUser <username>
**UpdateAdminUser--options**

Modifies an existing system administrator user ID.

**Table 46: UpdateAdminUser option**

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--UserName</td>
<td>Opt</td>
<td>User Name. Maximum 30 characters.</td>
</tr>
<tr>
<td>--LastName</td>
<td>Opt</td>
<td>Maximum of 30 characters.</td>
</tr>
<tr>
<td>--FirstName</td>
<td>Req</td>
<td>Maximum of 30 characters.</td>
</tr>
<tr>
<td>--Email</td>
<td>Opt</td>
<td>Maximum of 255 characters. Use !NULL to clear.</td>
</tr>
<tr>
<td>--Phone</td>
<td>Opt</td>
<td>Maximum of 30 characters. Use !NULL to clear.</td>
</tr>
<tr>
<td>--Mobile</td>
<td>Opt</td>
<td>Maximum of 30 characters. Use !NULL to clear. Also recognizes the value --pager for legacy support.</td>
</tr>
<tr>
<td>--Disable</td>
<td>Opt</td>
<td>Whether the user’s ID is currently disabled. Y/N. Disabled users cannot log in to the appliance.</td>
</tr>
<tr>
<td>--SecondaryAuth</td>
<td>Opt</td>
<td>Secondary authentication system used for user login. Valid values are None (default), SecureID, Safeword, Radius, WinAD, Defender and LDAP.</td>
</tr>
<tr>
<td>--SecondaryAuthSystem</td>
<td>Opt</td>
<td>Name of the secondary authentication system of the type indicated in ExternalAuth. Values are defined by the appliance SysAdmin.</td>
</tr>
<tr>
<td>--SecondaryUserID</td>
<td>Opt*</td>
<td>User ID to use for secondary authentication. This is required when SecondaryAuth is other than None.</td>
</tr>
<tr>
<td>--PrimaryAuthExtra</td>
<td>Opt</td>
<td>The LDAP Primary Authentication Types support an “Extra” UserID. The User logs in using a shorthand value in the PrimaryAuthID, but the data in the PrimaryAuthExtra will be used to do the actual authentication against the external system. Use !NULL to clear.</td>
</tr>
<tr>
<td>--PrimaryAuthID</td>
<td>Opt*</td>
<td>The User ID to use for primary authentication when a non-local authentication system is used.</td>
</tr>
<tr>
<td>--PrimaryAuthType</td>
<td>Opt</td>
<td>The type of the primary authentication system for this user. Current values are Local, LDAP, WinAD, Radius or Defender. When Local is used the PrimaryAuthID, PrimaryAuthExtra and PrimaryAuthSystem values are ignored.</td>
</tr>
<tr>
<td>--PrimaryAuthSystem</td>
<td>Opt*</td>
<td>Name of the defined system to use when the PrimaryAuthType is not local. Systems are defined by the appliance System Administrator.</td>
</tr>
<tr>
<td>Option name</td>
<td>Req/Opt</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--CertThumbprint</td>
<td>Opt</td>
<td>The SHA1 or SHA256 thumbprint of the user’s certificate. SHA1 thumbprints must be 40 characters long. SHA256 must be 64 characters. Both should consist of only numbers and the letters A-F.</td>
</tr>
<tr>
<td>--Description</td>
<td>Opt</td>
<td>Maximum of 255 characters. Use NULL to clear.</td>
</tr>
<tr>
<td>--LogonHoursFlag</td>
<td>Opt</td>
<td>Indicates whether the LogonHours value represents allowed or prohibited hours. Valid values are A, P, or N (no restrictions).</td>
</tr>
<tr>
<td>--LogonHours</td>
<td>Opt</td>
<td>A listing of up to 4 hour ranges. Times must be expressed in 24-hour format in any of the following forms: 7, 07, 700, 0700, 07:00 (all indicating 07:00 AM). Separate multiple ranges with semi-colons, 07:00-12:00;18:00-23:59 (7AM-12AM and 6PM-11:59PM). If the LogonHoursFlag value is N this value is ignored.</td>
</tr>
<tr>
<td>--LogonDays</td>
<td>Opt</td>
<td>When Logon Hours are specified you may also specify the days of the week those hours are effective. Specify days with a string of 7 X's (to indicate an “on” day) or periods (for an “off” day) to represent the week from Sunday-Saturday. For example, .XXXXX. is Mon-Fri on, Sun and Sat off. If LogonHours are specified and LogonDays is left empty the default is all days “on”, e.g., XXXXXXX.</td>
</tr>
<tr>
<td>--LocalTimezone</td>
<td>Opt</td>
<td>The user's local time zone. You may enter any part of the time zone name as long as it is unique in the list, e.g., entering Guam will only find one time zone while entering 02:00 or US will find multiple entries. A value of “Server” indicates that the user is in the same time zone as the server and follows the same DST rules.</td>
</tr>
<tr>
<td>--DstFlag</td>
<td>Opt</td>
<td>Obsolete. Users will now automatically adjust DST per the local time zone which they are assigned.</td>
</tr>
<tr>
<td>--Custom1</td>
<td>Opt</td>
<td>Custom user columns, if defined. Use NULL to clear the value when updating.</td>
</tr>
<tr>
<td>--Custom2</td>
<td>Opt</td>
<td>see --Custom1</td>
</tr>
<tr>
<td>--Custom3</td>
<td>Opt</td>
<td>see --Custom1</td>
</tr>
<tr>
<td>--Custom4</td>
<td>Opt</td>
<td>see --Custom1</td>
</tr>
<tr>
<td>--Custom5</td>
<td>Opt</td>
<td>see --Custom1</td>
</tr>
<tr>
<td>--Custom6</td>
<td>Opt</td>
<td>see --Custom1</td>
</tr>
</tbody>
</table>
**UserSSHKey--options**

Regenerate or retrieve a key for yourself or others.

- **IMPORTANT:** If regenerating your own key make sure not to overwrite the old key file before the command has completed.

- **IMPORTANT:** Regenerating a user’s key will immediately make their old key invalid. The user will have to put this new key in place before being able to access TPAM again.

**Table 47: UserSSHKey option**

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--UserName</td>
<td>Opt</td>
<td>User name to retrieve. If no user name is supplied your own user name will be used. If retrieving or regenerating a key for a user other than yourself the user must be key based with no TPAM web access.</td>
</tr>
<tr>
<td>--KeyType</td>
<td>Opt</td>
<td>Must be CLIA.</td>
</tr>
<tr>
<td>--PassPhrase</td>
<td>Opt</td>
<td>Only allowed when generating a CLIA key. Passphrase must be at least 5 characters long and may be up to 128 characters and contain anything except double quote characters (&quot;).</td>
</tr>
<tr>
<td>--Regenerate</td>
<td>Opt</td>
<td>Regenerate the key before retrieving. Users without web access must retrieve and regenerate their own keys. Y/N. Default is N.</td>
</tr>
</tbody>
</table>

**ViewLog--options**

Can view the specified log. Only one log may be viewed at a time.

**Table 48: ViewLog options**

<table>
<thead>
<tr>
<th>Option name</th>
<th>Req/Opt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--restore</td>
<td>Opt</td>
<td>View the restore log.</td>
</tr>
<tr>
<td>--backup</td>
<td>Opt</td>
<td>View the backup log.</td>
</tr>
<tr>
<td>--patch</td>
<td>Opt</td>
<td>View the patch log.</td>
</tr>
</tbody>
</table>
Relocating/Readdressing an Appliance

Introduction

If it becomes necessary to relocate and readdress a TPAM primary or replica, follow the instructions below to ensure a smooth and trouble free move.

Change a primary’s IP address

To change the primary’s IP address:

1. Log on to the config interface of the primary.
2. Select Network Settings | Modify Network Settings from the menu.
3. Enter the new IP Address, Subnet Mask, and Default Gateway. Click the Save Settings button.

**NOTE:** These settings take effect immediately, so if you change the IP address, upon clicking the save changes button your user session will end and you will have to log on to TPAM at the new IP address.

Once the new settings are saved all the other cluster members (replicas and DPAs) will discover the IP address change through the normal replication updates.
Change a replica’s IP address

To change the primary’s IP address:

1. Log on to the config interface of the replica that is changing.
2. Select Network Settings | Modify Network Settings from the menu.
3. Enter the new IP Address, Subnet Mask, and Default Gateway. Click the Save Settings button.

   NOTE: These settings take effect immediately, so if you change the IP address, upon clicking the save changes button your user session will end and you will have to log on to TPAM at the new IP address.

4. Log on to the admin interface of the PRIMARY.
5. Select System Status/Settings | Cluster Management from the menu.
6. Select the replica that is changing in the cluster member list.
7. Select the Network Address check box.
8. Enter the new IP address.
9. Click the Check Address button.
10. If the address is found, click the Save button. This is how all the other cluster members are notified of the replica’s new address.

   NOTE: When you click Save, you will see a message that the device is not enrolled in the cluster, this is a timing issue. Please disregard and refresh the page after a few minutes.

Now all of the cluster members will be able to communicate with the replica at its new address.
Kiosk Access

Introduction

The kiosk should ONLY be accessed if recommended by Technical support. You will not be able to perform any of these functions without technical support providing you the keys needed.

The functions available on the kiosk are to be used as a last resort before having to return the appliance if an issue cannot be fixed over the phone with technical support.

How to access the kiosk

To access the TPAM Kiosk, connect a monitor and keyboard to the TPAM appliance that is already powered on and connected to your network.

Before contacting support please write down the software version, serial number, config MAC, and Windows product key displayed on the home page. You will need to give these to support but will not be able to go back to this screen until the entire process is complete.

Reset the parmaster password

The reset password option resets the parmaster password to factory default.

To reset the password:

1. Click on Reset.
2. Enter your email address and click the Next button.
3. Do not leave this screen until support gives you the keys. If you do you will have to start the entire process over again because a new Nonce identifier is generated every time you land on this page. Enter the keys provided to you by technical support and click the Next button.
4. Click the **Finish** button.

5. Log on to the /admin interface as parmaster with the factory default password. You will be prompted to change the password for the parmaster account.

## Restore from a backup

All of the online backups will be displayed and the user can select an online backup to restore from.

**To restore from a backup:**

1. Click on **Restore**.
2. Enter your email address and click the **Next** button.
3. Do not leave this screen until support gives you the keys. If you do you will have to start the entire process over again because a new Nonce identifier is generated every time you land on this page. Enter the keys provided to you by technical support and click the **Next** button.
4. Select the backup file you wish to for the restore. Click the **Next** button.
5. If you are sure you want to proceed, click the **Finish** button. The appliance will automatically reboot after a successful restore from the backup. Depending on the size of the database the restore process may take some time to complete, be patient.

## Revert to a snapshot

All of the snapshots will be displayed and the customer can select one to revert to.

**To revert to a snapshot:**

1. Click on **Revert**.
2. Enter your email address and click the **Next** button.
3. Do not leave this screen until support gives you the keys. If you do you will have to start the entire process over again because a new Nonce identifier is generated every time you land on this page. Enter the keys provided to you by technical support and click the **Next** button.
4. Select the snapshot and click the **Next** button.
5. If you are sure you want to proceed, click the **Finish** button. The appliance will automatically reboot after successfully reverting to the snapshot. Depending on the size of the database the revert process may take some time to complete, be patient.
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