PAMtutorials 14: Managing your OEBS customers

On Top of the Game

PIPER-Rx *A*pplication *M*onitor – *PAM*
VIRTUAL APPS ADMINISTRATOR

PAM Version 4.0

"Blurring the line between software product and training"

May 2012

Table of Contents

1 What you'll get out of *PAMtutorials* 14

In ***PAMtutorials*** 14 we will describe a couple of simple methods for easily discerning between your internal and external customers so you can manage the different groups properly and professionally.

In addition, we also provide two (2) alerts for self-service sessions that have been timing out as a result of two (2) profile options:

- UA-006 Alert when Self Service Sessions have timed out due to page limit exceeded
- UA-007 Alert when Self Service Sessions have timed out due to connect time limit exceeded

We will also give you a number of trigger points and ***PAM*** alerts to identify when your SLAs should be renegotiated (GA-003).

Finally, we will introduce the ***PAM*** auto threshold feature (IN-003), where a number of the ***PAM*** thresholds can be automatically set over time based on your application's actual activity levels.

2 Distinguishing internal from external user accounts

For a variety of reasons, when you have external users accessing your application it is important to be able to easily distinguish internal employee accounts from external customer accounts.

Example: When you have experienced a performance problem or an outage, you could list the user accounts that were connected either during the performance issue or, in the case of an outage, those connected just before the outage. In this way you have a list of users and more importantly the customers who were affected by the issue and you can provide good customer service by, for example, providing each group an individually tailored message about the performance problem. You could also have further follow up by passing on the list of external customers affected by the issue to your customer service reps so they can make sure your customers are happy and will not go elsewhere to purchase their goods and services.

I.e. From a credibility perspective, dealing with the effects of a performance issue can be as important as dealing with the issue itself.

Example SQL for reporting on internal and external users connected where there was an issue at approximately 9:35am 31-Dec-10

```
SELECT fl.user_id,
       fu.user_name,
       substr(fu.description, 1, 30) ||
           decode(sign(length(fu.description) - 30), 1, '...')
description,
       '('||decode(employee_id, null ,'-', 'E')||
                 decode(customer_id, null ,'-', 'C')||
                 decode(supplier_id, null ,'-', 'S')||')' user_type,
       to_char(fl.start_time, 'DD-Mon-YY HH24:MI:SS') start_time,
       nvl(to_char(fl.end_time, 'DD-Mon-YY HH24:MI:SS'), 'Active')
end_time
  FROM applsys.fnd_logins fl,
       applsys.fnd_user fu
 WHERE fl.user_id = fu.user_id
   and fl.start_time <= to_date('31-Dec-10 09:35', 'DD-Mon-YY
HH24:MI')
   and nvl(fl.end_time, sysdate) >= to_date('31-Dec-10 09:36', 'DD-
Mon-YY HH24:MI')
   and nvl(fl.terminal_id, 'X') != 'Concurrent';
```

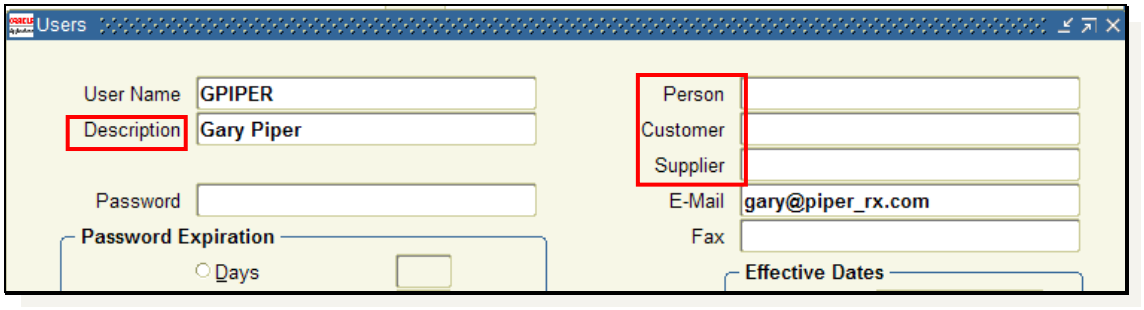
Example SQL output

USER_ID	USER_NAME	DESCRIPTION	USER_TYPE	START_TIME	END_TIME
1199	AHAMILTON	Anne Hamilton, Vision Services	(E--)	31-Dec-10 09:34:28	Active

This method of identifying user accounts is described in the examples below, however, there are any number of methods for distinguishing internal from external user accounts, here are just two (2):

2.1 Security > User > Define

Using the applications user definition screen, you can add the person id (Employee), Supplier and/or Customer IDs.



You can then add the following code to any user report to identify if the users account is a customer / supplier account.

```
'('||decode(employee_id, null ,'-', 'E')||
            decode(customer_id, null ,'-', 'C')||
            decode(supplier_id, null ,'-', 'S')||')' user_type
```

Example User accounts report

```
SELECT fu.user_id,
       fu.user_name,
       substr(fu.description, 1, 30) ||
           decode(sign(length(fu.description) - 30), 1, '...')
description,
       '('||decode(employee_id, null ,'-', 'E')||
                  decode(customer_id, null ,'-', 'C')||
                  decode(supplier_id, null ,'-', 'S')||')' user_type
  FROM applsys.fnd_user fu;
```

Example output

USER_ID	USER_NAME	DESCRIPTION	USER_TYPE
1854	ARAY	Amy Ray	(E--)
1874	COMPSERV	Customer, Computer Service & R...	(-C-)
1327	SUPPLIER	supplier, Office Supplies, Inc	(--S)
1326	CUSTOMER	customer, Business World	(-C-)
1491	CBAKER	Catherine Baker	(E--)

2.2 Labeling User Descriptions

A preferred option for labeling user accounts by type is to change the users account description, adding an identifier to clearly identify external customer accounts, something simple like adding a full stop to the end of the user's description.

Warning: The users description will be displayed in the self-service welcome screen, so be careful what description you use!

Also, remember in some implementations users can change their own description value which possibly makes using this method more difficult. It is possible to preclude users from being able to modify their description values and that should be done if needed.

3 Self-Service Session Timeouts

There are two (2) self-service timeout profile options that can become very annoying for the end user, especially if the end user is an external customer accessing your self-service applications. If the self-service session timeout values are set too low the user will have to reconnect whenever the session times out and this can cause much user frustration, particularly if it occurs regularly.

I once came across a site where the DBA was so exasperated at continually having to reconnect to the application that they set their own (user level) profile option values much higher. My question to the DBA was "if it is frustrating for you, what about your users, aren't they also getting frustrated?" The answer was "I had not thought about that".

PAM will monitor the two (2) service timeout values and alert if any user session has exceeded the timeout values and the user has been forced to

reconnect. In this way you will see if users are regularly forced to reconnect and you can take positive action.

3.1 Self-service timeout profile options

There are two (2) basic settings for self-service profile option user connection timeouts:

ICX_LIMIT_TIME

A user will be forced to reconnect to the application when the total connect time for their self-service session exceeds this profile option value. The profile option value is in hours. The user's current connect time can be calculated using the values (last_connect and first_connect) for their session in the icx_session table.

ICX_LIMIT_CONNECT

A user will be forced to reconnect to the application when the total number of page requests for their self-service session exceeds this profile option value. The profile option value is the number of page requests. The user's current page request count can be found in the counter attribute for their session in the icx_session table.

3.2 What are my current timeout values?

PAM provides two reports for finding your site's profile options and the settings:

Firstly, ***PAMreports*** - General PAMRGA011 Profile Options By Application report lists all profile options for a selected application including the number of changes at the application, responsibility and user levels:

Example **PAMRGA011 Profile Options By Application** report

PAMRGA011-10

PAM - PIPER-RX - APPLICATION MONITOR
PROFILE OPTIONS BY APPLICATION
(178) ICX - Oracle iProcurement
As at 05-Dec-10 13:45
For APPS 12i

PIPER - Rx

Option ID	Option Name Option Description Site Value	User Option Name	Status	Appn	Resp	User
1003402	ICX_ACCESSIBILITY_FEATURES *Enable addition Self Service accessibility features* N	Self Service Accessibility Features	Active	0	0	1
2516	ICX_ALLOW_OVERRIDE_FUNDS *User Level Profile that specifies if a user can override funds* N	ICX:Allow Funds Override	End Dated *11-Jul-06 00:00*	0	0	0
1000418	ICX_CLIENT_IANA_ENCODING *Client IANA Encoding used for setting up charset in HTTP response* UTF-8	ICX: Client IANA Encoding	Active	0	0	0
2325	ICX_DATE_FORMAT_MASK *User date format mask preference* DD-MON-RRRR	ICX: Date format mask	Active	0	0	252
3531	ICX_DATE_LANGUAGE *User date language preference* ** NOT SET **	ICX: Date language	Active	0	0	129
2645	ICX_DAYS_NEEDED_BY *Days Needed By to calculate the Need By Date* 2	ICX: Days Needed By	End Dated *11-Jul-06 00:00*	0	0	0
3813	ICX_DEFAULT_DISCO_WORKBO *Default Discoverer Workbook Owner* ** NOT SET **	ICX: Default Discoverer Workbook Owner	End Dated *01-Aug-06 00:00*	0	0	0
3568	ICX_DEFAULT_EUL *Discoverer Default End User Layer Schema Prefix*	ICX: Discoverer Default End User Layer Schema Prefix	Active	0	0	0

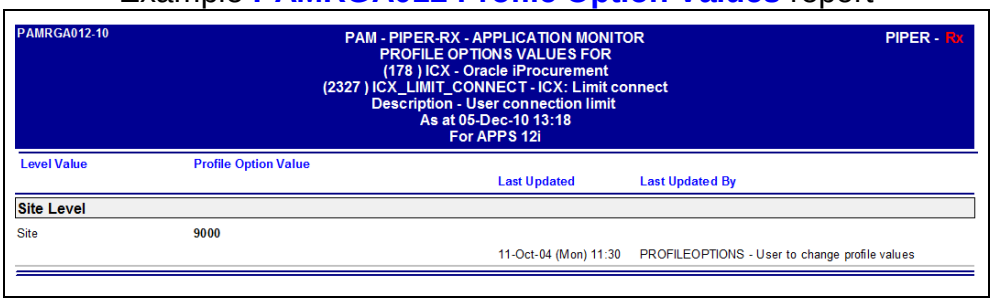
In the following example we can see that the site level values for both timeout profile options (ICX_LIMIT_CONNECT and ICX_LIMIT_TIME) are 9000 and 999 respectively and that there have been no profile option changes at the lower levels:

Example **PAMRGA011 Profile Options By Application** report

Option ID	Option Name Option Description Site Value	User Option Name	Status	Appn	Resp	User
3769	ICX_FORMS_LAUNCHER *** No Description Available *** http://earth.verdantservices.net:8001/forms/frmservlet	ICX: Forms Launcher	Active	0	0	4
2324	ICX_LANGUAGE *User language preference* AMERICAN	ICX: Language	Active	0	0	487
2327	ICX_LIMIT_CONNECT *User connection limit* 9000	ICX: Limit connect	Active	0	0	0
2326	ICX_LIMIT_TIME *User time limit* 999	ICX: Limit time	Active	0	0	0
1001489	ICX_MATCHCASE_LOV *Alter Match case functionality* Checked	ICX: Match case LOV	Active	0	0	0
1001491	ICX_MATCHCASE_VIEW *Alter Match case functionality* Unchecked	ICX: Match case View	Active	0	0	0

PAMreports - General PAMRGA012 Profile Option Values uses the profile option Application ID and the Profile Option ID from the first report to list all the profile option values for the selected profile option:

Example **PAMRGA012 Profile Option Values** report



PAMRGA012-10 PAM - PIPER-RX - APPLICATION MONITOR PIPER - Rx
PROFILE OPTIONS VALUES FOR
(178) ICX - Oracle iProcurement
(2327) ICX_LIMIT_CONNECT - ICX: Limit connect
Description - User connection limit
As at 05-Dec-10 13:18
For APPS 12i

Level Value	Profile Option Value	Last Updated	Last Updated By
Site Level			
Site	9000		
		11-Oct-04 (Mon) 11:30	PROFILEOPTIONS - User to change profile values

This report includes the last updated date and last updated by values to clearly show who made the last change and when.

3.3 How this all works

When a self-service session is created a record is added in the icx_sessions table. At that time the profile options are evaluated for that user and these values are set in the limit_time and limit_connects attributes of the self-service sessions record. On each update of the session's record the difference in hours between the values for (last_connect and first_connect) is evaluated. If it exceeds the value for limit_time a reconnect is required and if the sessions value for counter (page requests) exceeds the record value for limit_connects a reconnect is required.

PAM scans the icx_sessions table and will alert when sessions that have been started in the current day and have been found that have exceeded either of these values.

3.4 UA-006 Alert when Self Service Sessions have timed out due to page limit exceeded

Every hour (default) ***PAM*** checks the self-service sessions and will alert when sessions started in the current day have been found to have exceeded their page limit. ***PAM*** will alert again when addition timed out sessions have been found.

3.4.1 E-mail alert

When ***PAM*** detects self-service sessions that have been terminated due to the number of page requests exceeding the user's limit a ***PAM*** alert e-mail is raised:

Example: *PAM* UA-006 – *PAM* self-service page limit alert message

ALERT MESSAGE FROM *PAM* - PIPER-Rx Application Monitor - DO NOT REPLY

Company = Company name
Site = Site name
Alert Level = **Informational**
Detected = 28-Feb-11 (Mon) 16:00:20
Alert Frequency = 1 Hour

2 self-service sessions have timed out due to excessive page requests

Alert Information:

UA-006 - Self Service Session Timeout (Pages)

ONE OR MORE SELF SERVICE SESSIONS HAS TIMED OUT DUE TO THE SESSION EXCEEDING THE SESSIONS MAXIMUM NUMBER OF PAGE REQUESTS

If you want to obtain a list the sessions that have timed out for the selected day you can use ***PAMreports*** - Actions **PAMAUA006 Self Service Session Timeouts Pages (day)**

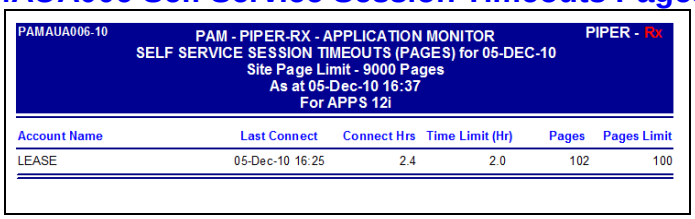
Note 1: Session page request limits are set via profile options. Session timeouts can cause a customer service issue and should be actioned accordingly

Note 2: This alert will continue to alert when more sessions have timed out during the day

3.4.2 What to do with this information

You can use the ***PAM*** action report PAMAUA006 Self Service Session Timeouts Pages (day) to list all self-service session that have timed out due to the number of page requests for the session exceeding the sessions limit value:

Example **PAMAUA006 Self Service Session Timeouts Pages (day)** report



PAMAUA006-10 — PAM - PIPER-RX - APPLICATION MONITOR — PIPER - Rx
SELF SERVICE SESSION TIMEOUTS (PAGES) for 05-DEC-10
Site Page Limit - 9000 Pages
As at 05-Dec-10 16:37
For APPS 12i

Account Name	Last Connect	Connect Hrs	Time Limit (Hr)	Pages	Pages Limit
LEASE	05-Dec-10 16:25	2.4	2.0	102	100

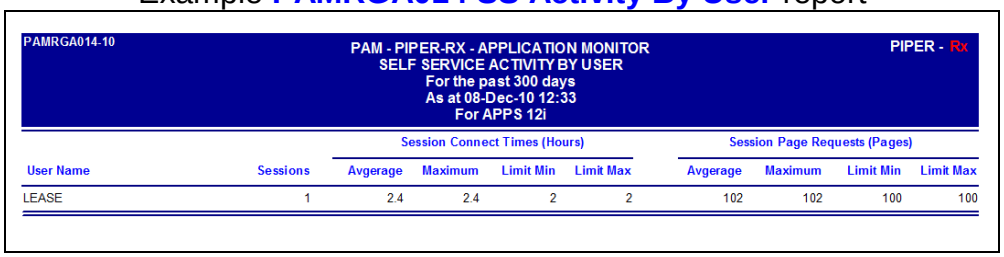
You should assess why the limit has been reached and if the limit should be extended for that user or all users performing the same role.

3.4.3 What should the page limits be set to?

Your site level values for ICX_LIMIT_CONNECT (page requests) should be set high enough to cover your site's normal activity; it is quite rare to set these values on a less than site level basis. Remember, a highly active user does not want to have to reconnect just because they are a heavy self-service user.

To help assess your site's self-service user activity ***PAM*** provides ***PAMreports*** - General PAMRGA014 SS Activity By User report which lists your site's activity for the past ***n*** days:

Example **PAMRGA014 SS Activity By User** report



PAMRGA014-10 — PAM - PIPER-RX - APPLICATION MONITOR — PIPER - Rx
SELF SERVICE ACTIVITY BY USER
For the past 300 days
As at 08-Dec-10 12:33
For APPS 12i

		Session Connect Times (Hours)				Session Page Requests (Pages)			
User Name	Sessions	Avgerage	Maximum	Limit Min	Limit Max	Avgerage	Maximum	Limit Min	Limit Max
LEASE	1	2.4	2.4	2	2	102	102	100	100

This report is also very usefull for self-service activity profiling

3.4.4 How do I turn the *PAM* Self-Service timeout pages alert off?

The ***PAM*** self-service timeout pages alert can be turned off using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'UA-006', 'N');
```

and can be re-enabled using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'UA-006', 'Y');
```

3.4.5 Changing alert check frequency and / or severity

Both the alert check frequency and alert severity can be changed. Please refer to the *PAM* FAQs for more information on how to change an alert frequency and alert severity.

3.5 UA-007 Alert when Self Service Sessions have timed out due to connect time limit exceeded

Every hour (default) *PAM* checks the self-service sessions and will alert when sessions started in the current day that have been found to have exceeded their time limit. *PAM* will alert again when addition timed out sessions have been found.

3.5.1 E-mail alert

When *PAM* detects self-service sessions that have been terminated due to their connect time exceeding the user's limit a *PAM* alert e-mail is raised:

Example *PAM* UA-007 – *PAM* self-service time limit alert message

ALERT MESSAGE FROM *PAM* - PIPER-Rx Application Monitor - DO NOT REPLY

Company = Company Name
Site = Site name
Alert Level = **Informational**
Detected = 28-Feb-11 (Mon) 16:00:22
Alert Frequency = 1 Hour

---

2 self-service sessions have timed out due to excessive connect time

---

Alert Information:

UA-007 - Self Service Session Timeout (Connect time)

ONE OR MORE SELF SERVICE SESSIONS HAS TIMED OUT DUE TO THE SESSION EXCEEDING THE SESSIONS CONNECT TIME LIMIT

If you want to obtain a list of the sessions that have timed out for the selected day you can use ***PAMreports*** - Actions **PAMAUA007 Self Service Session Timeouts Time (day)**

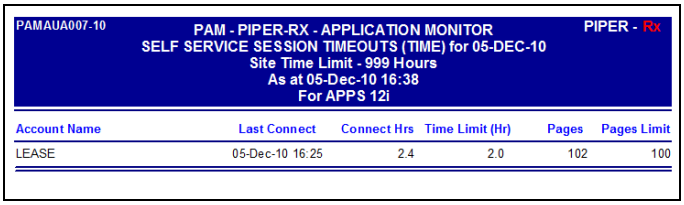
Note 1: Session connect time limits are set via profile options

Note 2: This alert will continue to alert when more sessions have timed out during the day

3.5.1 What to do with this information

You can use the ***PAMreports*** - Actions PAMAUA007 Self Service Session Timeouts Time (day) to list all self-service session that have timed out due to the session time exceeding the session's limit value:

Example **PAMAUA007 Self Service Session Timeouts Time (day)** report



PAMAUA007-10
PAM - PIPER-RX - APPLICATION MONITOR
SELF SERVICE SESSION TIMEOUTS (TIME) for 05-DEC-10
Site Time Limit - 999 Hours
As at 05-Dec-10 16:38
For APPS 12i
PIPER - Rx

Account Name	Last Connect	Connect Hrs	Time Limit (Hr)	Pages	Pages Limit
LEASE	05-Dec-10 16:25	2.4	2.0	102	100

You should asses why the limit has been reached and if the limit should be extended for that user or all users performing the same role.

3.5.2 What should the page limits be set to?

Your site level values for ICX_LIMIT_TIME (Session time in hours) should be set high enough to cover your sites normal activity.

Often this value is set as part of a security measure, that is, if a session has been idle for an amount of time, the next time the session is used a reconnect will be required. Unfortunately, the time limit is a hard value so if a session is in constant use once the time limit has been reached a reconnect will be required. Bit of a two edged sword this one…

To help assess your site's self-service user activity ***PAM*** provides ***PAMreports*** - General PAMRGA013 SS Activity By User report that lists your site's activity for the past ***n*** days:

Example **PAMRGA013 SS Activity By User** report

PAMRGA013-10

PAM - PIPER-RX - APPLICATION MONITOR
SELF SERVICE ACTIVITY BY USER
For the past 300 days
As at 08-Dec-10 11:16
For OEBS 12 DEMO

PIPER - Rx

		Session Connect Times (Hours)				Session Page Requests (Pages)			
User Name	Sessions	Avgerage	Maximum	Limit Min	Limit Max	Avgerage	Maximum	Limit Min	Limit Max
GUEST	356	0.0	0.2	4	4	2	2	1,000	1,000
IBEGUEST	14	0.0	0.0	4	4	1	1	1,000	1,000

This report is also very usefull for self-service activity profiling

3.5.3 How do I turn the *PAM* Self-Service timeout Time alert off?

The ***PAM*** self-service timeout time alert can be turned off using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'UA-007', 'N');
```

and can be re-enabled using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'UA-007', 'Y');
```

3.5.4 Changing alert check frequency and / or severity

Both the alert check frequency and alert severity can be changed. Please refer to the ***PAM*** FAQs for more information on how to change an alert frequency and alert severity.

4 Profile Option Cleanup

Whilst not a ***PAM*** alert, ***PAMreports*** - General PAMRGA012 Profile Option Values report could be used to aid in the cleanup of redundant profile options within your application.

In the following example the site level value for the selected profile option is set to 'Y'. All lower level values are set to 'N' except the responsibility level "CA Customer Discoverer" which is set to the same value as the site level, in affect possibly making this entry redundant and a candidate for removal.

Example **PAMRGA012 Profile Option Values** report

PAMRGA012-10

PAM - PIPER-RX - APPLICATION MONITOR
PROFILE OPTIONS VALUES FOR
(178) ICX - Oracle iProcurement
(1001406) ICX_DISCOVERER_USE_VIEWER - ICX: Discoverer use Viewer
Description - Use Discoverer Viewer instead of Web Discoverer
As at 05-Dec-10 13:19
For APPS 12i

PIPER - Rx

Level Value	Profile Option Value	Last Updated	Last Updated By
Site Level			
Site	Y	11-Oct-04 (Mon) 11:30	PROFILEOPTIONS - User to change profile values
Application Level			
Marketing	N	07-Sep-01 (Fri) 07:02	EBUSINESS - Mr. Phillip C. Taylor
Responsibility Level			
Audience Administrator	N	05-Dec-05 (Mon) 02:23	PROFILEOPTIONS - User to change profile values
Audience User	N	05-Dec-05 (Mon) 02:23	PROFILEOPTIONS - User to change profile values
CA Custom Discoverer	Y	15-May-02 (Wed) 06:27	CAHRMS - Access to all Canadian Responsibilities
Oracle Marketing Planning	N	07-Sep-01 (Fri) 07:02	EBUSINESS - Mr. Phillip C. Taylor
Oracle Marketing Super User	N	05-Dec-05 (Mon) 02:22	PROFILEOPTIONS - User to change profile values

Before you embark on clean up, you should be aware it is a big task for very little direct return.

4.1 Finding profile option duplicates

If you do decide you want to clean up redundant profile options you can use ***PAMreports*** - General PAMRGA013 Profile Option Duplicates report to list any profile options on an application by application basis that have the same values for Application, responsibility or user values as the overall site value:

Example **PAMRGA013 Profile Option Duplicates** report

PAMRGA013-10

PAM - PIPER-RX - APPLICATION MONITOR
PROFILE OPTION DUPLICATES
For appn (0) - FND - Application Object Library
As at 08-Dec-10 14:01
For APPS 12i

PIPER - Rx

Option ID	Option Name	Option Full Name	Site Level Value	Site Level Duplications		
				Appn	Resp	User
3101	ACCOUNT_GENERATOR:DEBUG_M...	Account Generator:Run in Debug Mode	N	0	1	0
3100	AFLOG_MODULE	FND: Debug Log Module	%	0	0	2
1000004	APPLET_PLUGIN_TYPE	Applet Plug-In Type	application/x-jinit-applet;version=1.1.7...	0	15	0
1000002	APPLET_PLUGIN_URL	Applet Plug-In URL	jinit.exe	0	15	0
1005142	APPLICATIONS_HOME_PAGE	Self Service Personal Home Page mode	FWK	0	2	0
1004441	APPS_SSO	Applications SSO Type	SSWA	0	0	1
1005146	APPS_SSO_LOCAL_LOGIN	Applications SSO Login Types	LOCAL	0	0	3
1803	ATCHMT_SET_INDICATOR	Indicate Attachments	Y	18	18	0
2355	ATTACHMENT_FILE_DIRECTORY	Attachment File Directory	/d07/app/applcsf/hm000a/attachme/	0	15	0
111	CONC_COPIES	Concurrent:Report Copies	0	0	0	1
1008341	CONC_PP_PROCESS_TIMEOUT	Concurrent:OPP Process Timeout	300	1	0	0
1008340	CONC_PP_RESPONSE_TIMEOUT	Concurrent:OPP Response Timeout	120	1	0	0
117	CONC_SAVE_OUTPUT	Concurrent:Save Output	Y	0	1	0
115	CONC_SINGLE_THREAD	Concurrent:Sequential Requests	N	0	6	0
1081	CURRENCY:POSITIVE_FORMAT	Currency:Positive Format	0	0	1	0
1082	CURRENCY:THOUSANDS_SEPARA...	Currency:Thousands Separator	Y	0	0	1
1804	DEFAULT_COUNTRY	Default Country	US	160	160	160
1781	EDITOR_PS	Viewer: PostScript	c:\msoffice\winword\winword.exe	0	0	1

In the above report you can see that for the profile option 1803 – ATCHMT_SET_INDICATOR there are 18 application and 18 responsibility profile options that are set to the same value as the site level.

You can then use ***PAMreports*** - General PAMRGA012 Profile Option Values report to view the individual changes at the profile option level:

Example **PAMRGA012 Profile Option Values** report

PAMRGA012-10

PAM - PIPER-RX - APPLICATION MONITOR
PROFILE OPTIONS VALUES FOR
(0) FND - Application Object Library
(1803) ATCHMT_SET_INDICATOR - Indicate Attachments
Description - Indicate whether attachments exist
As at 08-Dec-10 14:04
For APPS 12i

PIPER - Rx

Level Value	Profile Option Value	Last Updated	Last Updated By
Site Level			
Site	Y	28-Jun-96 (Fri) 10:16	Not Available
Application Level			
Depot Repair	Y	09-Feb-05 (Wed) 04:34	EBUSINESS - Mr. Phillip C. Taylor
Field Service	Y	09-Feb-05 (Wed) 04:43	SYUHOV - Yuhov, Sebastian
Service	Y	09-Feb-05 (Wed) 04:42	SYUHOV - Yuhov, Sebastian
Responsibility Level			
Depot Repair Manager, Vision	Y	27-Apr-05 (Wed) 02:11	SERVICE - Smith, Mr. Rick
Depot Repair Manager, Vision	Y	27-Apr-05 (Wed) 02:11	SERVICE - Smith, Mr. Rick
Field Service Dispatcher,	Y	27-Apr-05 (Wed) 02:10	SERVICE - Smith, Mr. Rick

You then need to evaluate if the profile options set at the lower levels can be removed… Good luck…

5 GA-003 - SLA Renegotiation Triggers

Firstly we need to make it very clear that PAM does not set out to either define or measure SLAs. What PAM does is identify some trigger points to prompt you considering renegotiation.

PAM detects when the level of daily application activity exceeds one or more ***PAM*** thresholds on **multiple** occasions. When this occurs ***PAM*** will raise an alert indicating it may be time to renegotiate your SLAs.

A **S**ervice **L**evel **A**greement (SLA) means many things to many people; to some it is the requirement to have a support call actioned within an agreed amount of time, to others is can be application response time "however that is measured" or indeed both…

Quite a few years ago I presented the following paper at the Irish User Group meeting in Dublin Feb 2005:

> A business approach to Oracle E-Business Suite response time, E-to-E and SLAs which can be found on my web site - http://www.piper-rx.com/pages/papers/e2e.html

Whilst some of the products shown in this paper are old or have been superseded the principles still hold true….

Defining the calculation of an SLA measure can be highly contentious; take for example "uptime". Technical people don't want to include backups and scheduled maintenance windows as this makes the overall uptime look bad, whereas the user generally thinks of uptime as being able to use the application whenever they need to. This is as good an example as any of a classic business / technical disconnect.

5.1 Renegotiating your SLAs

Often a company will add many new employees and expect you to maintain the current SLA levels, or the application workload will increase over time and you will be expected to maintain your current SLAs…

You cannot add an additional 15% of users and expect the same response time.

When SLAs are in place, whatever they are, often technical teams do not renegotiate the SLA level until forced to due to multiple breaches. When this occurs it is often an adversarial process as the business is frustrated and the technical teams often want breach levels that are set too high for business purposes…

PAM helps you get ahead of the game by providing some simple measures to prompt you when you should consider renegotiation of an SLA. It is better to renegotiate from a position of proactivity rather than off the back foot when you have a history of multiple breaches.

Also the type of wording you use in your SLA can help. E.g.:

> *Whist every effort will be undertaken to maintain the current SLA levels, it may not be feasible to continue to maintain these levels as the company grows over time. As such the current SLA levels will remain in force until one or more of the following triggers occur*:
>
> *The number of full service users exceeds **200** per day*
> *Or*
> *The number of self-service users exceeds **200** per day*
> *Or*
> *The number of full concurrent requests exceeds **5,000** per day*
> *Or*
> *The overall application response time as measured by the **PAM** application exceeds an average of **6** seconds per day*
>
> *When any one of these triggers points are exceeded this will trigger a renegotiation of the current SLAs.*

5.2 What *PAM* measures

PAM measures the activity level of four (4) key activities, Full service user activity, Self-service user activity, Concurrent request activity and Application response time, and any one of these measures could indicate your application and resource usage is increasing to a point where an SLA renegotiation is warranted.

The ***PAM*** SLA renegotiation triggers only use information held in the ***PAM*** daily activity repository piper_rx_pam_daily_activity

Trigger 1 – Full Service user activity

A ***PAM*** alert will be raised when the daily number of distinct active full service users exceeds the ***PAM*** threshold on more than ***n*** or more days in the past ***n*** days.

Trigger 2 – Self Service user activity

A ***PAM*** alert will be raised when the daily number of distinct active Self-service users exceeds the ***PAM*** threshold on more than ***n*** or more days in the past ***n*** days.

Trigger 3 – Concurrent request activity

A ***PAM*** alert will be raised when the daily number concurrent requests exceeds the ***PAM*** threshold on more than ***n*** or more days in the past ***n*** days.

Trigger 4 – Application response time

A ***PAM*** alert will be raised when the daily average response time (seconds) exceeds the ***PAM*** threshold on more than ***n*** or more days in the past ***n*** days.

The number of days history to evaluate (default 31) and the number of breaches (default 5) are set in the ***PAM*** settings.

From this description, you can see that a ***PAM*** alert is not raised every time a threshold is exceeded; the threshold must have been exceeded on **5** or more days in the past **31** days, that way any one off high activity days are excluded.

PAM only uses the information held in the ***PAM*** daily activity repository piper_rx_pam_daily_activity. As such the alerts are not dependent on the amount of information held within your application e.g. if self-service activity is purged weekly.

5.3 Setting the days history value

This setting is the number of consecutive day's history ***PAM*** will use when calculating SLA trigger points. The number of consecutive day's history to be used in the calculation can be set using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API_2.PAM_SLA_HISTORY_DAYS_SET ( 32 );
```

Parameter 1: The number of days history to be used

Note: ***PAM*** excludes weekend activity from the calculation

5.4 Setting the number of threshold breaches value

This setting is the number of occurrences where the ***PAM*** threshold value has been exceeded in the history period (days). This value can be set using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API_2.PAM_SLA_BREACHES_SET  ( 6 );
```

Parameter 1: The number of threshold exceptions before a ***PAM*** alert is raised.

5.5 Setting the SLA renegotiation values

5.5.1 Settings on install

PAM will set the renegotiation threshold levels as part of the ***PAM*** install process. The threshold levels set on install are based on actual activity found in the available on-line history plus 50% of that value. Example: If the average number of **distinct** full service user accounts that have accessed the application in the past 31 days (**excluding week ends**) is 100 then the ***PAM*** SLA renegotiation threshold level will be set to 150.

Minimum values set on ***PAM*** install:

- Full service distinct users 100 per day
- Self-service distinct users 100 per day
- Concurrent requests 5,000 per day
- Application response time 60 seconds

Note: These values can be changed after the installation

5.5.2 Setting SLA renegotiation reminder values automatically

The ***PAM*** SLA renegotiation reminder threshold levels can be set automatically using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_SETTINGS_SLA_LEVEL_AUTO ( 25 );
```

Parameter 1: The percentage uplift from the current application values

Note: The auto update will set minimum values as follows:
- Full service distinct users 100 per day
- Self-service distinct users 100 per day
- Concurrent requests 5,000 per day
- Application response time 60 seconds

Where you have more than 45 days current available history in the ***PAM*** daily activities repository piper_rx_pam_daily_activity ***PAM*** will use data from the repository; where there is less than 45 days history in the ***PAM*** daily activity repository ***PAM*** will use on-line application activity to calculate its thresholds.

Note: In both cases ***PAM*** excludes weekend activity from its calculations as weekend activity which is often inherently lower would skew the threshold values.

5.5.3 Setting values manually

The ***PAM*** SLA renegotiation threshold values can be set using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_SETTINGS_SLA_LEVEL_MANUAL ( 200, 200, 5000, 12 );
```

Parameter 1: The full service user value
Parameter 2: The self-service user value
Parameter 3: The number of concurrent requests
Parameter 4: The average application response time (sec)

Note: All 4 values must be set when using this API.

5.5.4 What are my current threshold values?

The current ***PAM*** SLA renegotiation thresholds can be found using the following SQL:

```
SELECT setting_description,
       setting_numeric_value
  FROM piper_rx_pam_settings
 WHERE setting_id in ('SLA_FS_USERS',
                      'SLA_SS_USERS',
                      'SLA_REQUESTS',
                      'SLA_RESPONSE_TIME');
```

Example output

The number of FS users connections to trigger SLA renegotiation	100
The number of concurrent requests to trigger SLA renegotiation	5000
The average response time (sec) to trigger SLA renegotiation	12
The number of SS users connections to trigger SLA renegotiation	200

5.6 E-mail alert

The ***PAM*** SLA renegotiation trigger check GA-003 will be run once per month; when ***PAM*** detects an SLA renegotiation trigger a ***PAM*** alert e-mail is raised:

Example *PAM* GA-003 – *PAM* SLA renegotiation trigger alert message

ALERT MESSAGE FROM *PAM* - PIPER-Rx Application Monitor - DO NOT REPLY

Company = Company name
Site = Site name
Alert Level = **Warning**
Detected = 28-Feb-11 (Mon) 20:01:05
Alert Frequency = 1 Month

In the past 35 days there has been 6 days where the number of FS sessions has exceeded the SLA renegotiation level of 200 sessions per day

---

Alert Information:

GA-003 - SLA Renegotiation Trigger

SELECTED *PAM* SLA LEVELS HAVE BEEN EXCEEDED.

This alert is designed as a trigger for you to consider whether a renegotiation of your current service level agreements is needed.

Based on the premise that you cannot maintain your current SLA levels when the business continues adding users and additional load to the application, this alert is generated if any of the following daily activities have exceeded their ***PAM*** SLA thresholds:

- The number of distinct Full Service users on any given day has exceeded the daily SLA threshold value
- The number of distinct Self Service users on any given day has exceeded the daily SLA threshold value
- The total number of concurrent requests on any given day has exceeded the daily SLA threshold value
- The average response time on any given day has exceeded the daily SLA threshold value

If you want to obtain more information on when ***PAM*** SLA levels have been exceeded, you can use one or more of the following ***PAMreports*** - General:

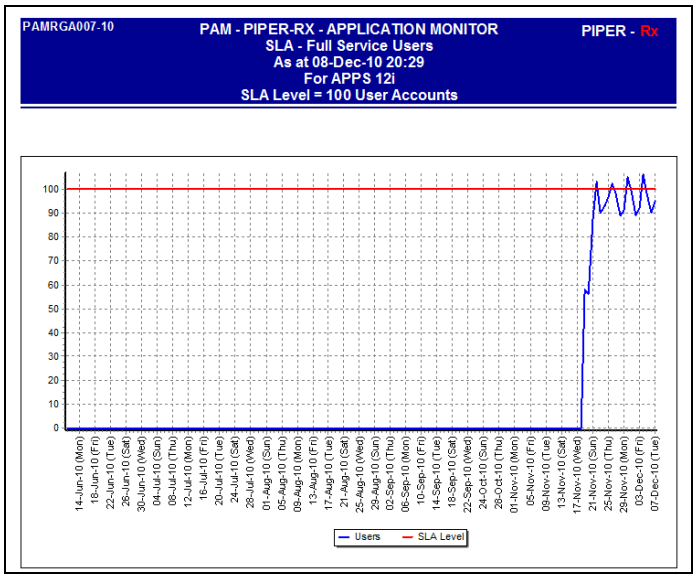
PAMRGA007 SLA Trigger FS Users
PAMRGA008 SLA Trigger SS Users
PAMRGA009 SLA Trigger Concurrent Requests
PAMRGA010 SLA Trigger Response Time

5.7 What to do with this information

Depending on the alert triggered you can use one of the following ***PAMreports*** - General to show when the breaches occurred:

- PAMRGA007 SLA Trigger FS Users
- PAMRGA008 SLA Trigger SS Users
- PAMRGA009 SLA Trigger Concurrent Requests
- PAMRGA010 SLA Trigger FS Response Time

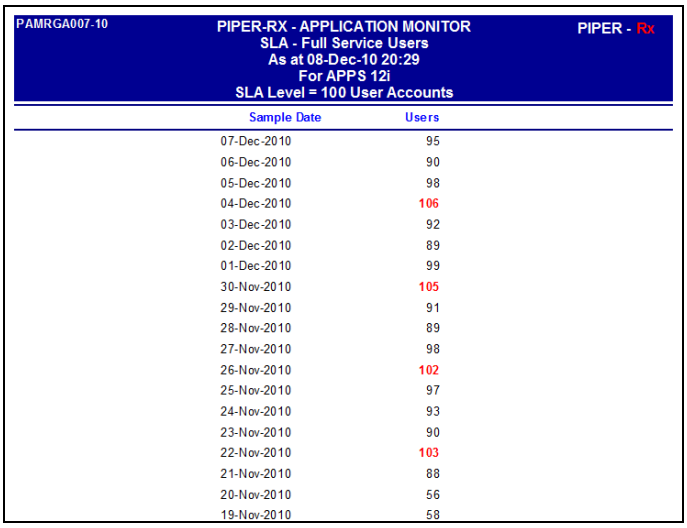
Example **PAMRGA007 SLA Trigger FS Users** report (Page 1)



The SLA level (shown in red) indicates the current ***PAM*** SLA threshold setting.

Note: In a “normal” environment over a period of time you will clearly see a steady increase in activity in a growing application, this report will aid in your explanation of growth and the renegotiation process.

Example **PAMRGA007 SLA Trigger FS Users** report (Page 2)



PAMRGA007-10
PIPER-RX - APPLICATION MONITOR
SLA - Full Service Users
As at 08-Dec-10 20:29
For APPS 12i
SLA Level = 100 User Accounts
PIPER - Rx

Sample Date	Users
07-Dec-2010	95
06-Dec-2010	90
05-Dec-2010	98
04-Dec-2010	106
03-Dec-2010	92
02-Dec-2010	89
01-Dec-2010	99
30-Nov-2010	105
29-Nov-2010	91
28-Nov-2010	89
27-Nov-2010	98
26-Nov-2010	102
25-Nov-2010	97
24-Nov-2010	93
23-Nov-2010	90
22-Nov-2010	103
21-Nov-2010	88
20-Nov-2010	56
19-Nov-2010	58

Page 2 of the report highlights in red where the ***PAM*** threshold has been exceeded.

5.8 How do I turn the *PAM* SLA renegotiation trigger alert off?

The ***PAM*** SLA renegotiation trigger alert can be turned off using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'GA-003', 'N');
```

and can be re-enabled using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'GA-003', 'Y');
```

5.9 Changing alert check frequency and / or severity

Both the alert check frequency and alert severity can be changed. Please refer to the ***PAM*** FAQs for more information on how to change an alert frequency and alert severity.

6 Auto Thresholds (IN-003 & AT-001)

As your application grows over time the ***PAM*** thresholds set in the past may be getting very close to your application's normal activity and as such you will be receiving more alerts. The normal ***PAM*** maintenance activity in this case is to review your application's current activity and reset the ***PAM*** thresholds based that activity level.

The ***PAM*** auto threshold feature provides the ability for some key threshold values to be automatically set based on your application's actual activity profiles. In this way ***PAM*** thresholds are set based on real application activity and will change with your applications processing profile.

Note: This feature is turned off on install and will need to be enabled.

6.1 How this all works

Once per week (default) ***PAM*** evaluates your application's activity from information held in the following ***PAM*** repositories:

- piper_rx_pam_daily_activity
- piper_rx_pam_idw_activity

PAM evaluates information for the past ***n*** days (excluding weekends as often general activity is lower than a normal working day and would skew the overall statistics) and calculates new thresholds based on the activity levels found.

PAM repositories are used as they are independent of your site's "normal" maintenance purging policy. (E.g. Purging concurrent requests every day holding 7 days on-line and running a special purge to remove workflow background process request information daily would not provide useful information for assessing a threshold level.)

6.2 What thresholds are calculated?

The ***PAM*** auto threshold feature calculates and sets thresholds for the following ***PAM*** checks:

- PF-001 - Application response time
- CR-002 – Requests completed error
- CR-003 - Total concurrent requests
- CR-004 – Requests completed warning
- UA-002 – Full service connections
- UA-004 – Self-service connections
- UA-005 – Self-service page requests
- UA-011 – Self-service page requests rate
- WF-111 – Total active workflows
- WF-112 – Total completed workflows
- WF-101 – Active workflow items
- WF-102 – Complete workflow items
- WF-103 – Deferred workflow items
- WF-104 – Error workflow items
- WF-105 – Notified workflow items
- WF-106 – Suspend workflow items
- WF-107 – Waiting workflow items
- WF-108 – Timeout workflow items
- WF-109 – Stuck workflow items
- WF-110 – Workflow mail items waiting to be sent

Note: Individual alerts can be excluded from the auto threshold calculation.

6.3 Auto threshold settings

There are number of ***PAM*** auto threshold settings that need to be set before the auto threshold should be enabled.

6.3.1 Available days on-line history

This value is the number of days of online history in the above mentioned ***PAM*** repositories that will be used when ***PAM*** calculates a new threshold value. Example: If the number of days is set to 35, ***PAM*** will use the past 35 day's history in its calculations.

Where there is less than 35 days history, ***PAM*** will not calculate a new threshold and will suspend the individual check until there is sufficient on-line information.

When calculating new threshold values weekends are excluded as often general activity is lower than a normal working day and would skew the results. In addition any day that has less than the minimum activity as defined by the ***PAM*** AT settings described below is also excluded.

6.3.2 Setting the minimum days value

The minimum number of days for the ***PAM*** auto threshold calculation can be set using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API_2.PAM_AT_HISTORY_DAYS_SET ( 35 );
```

Parameter 1:

The number of day's history to be used in the ***PAM*** auto threshold calculation.

Note: Minimum number of days allowable is 30 so as to ensure at least a full calendar month of activity is included.

6.3.3 Minimum activity levels

In order for a day's activity to be included in the ***PAM*** auto threshold calculation, there must be a minimum activity for that day. I.e. If for a period of time (maintenance, patching etc.) the application was shut down there would be lower than normal activity for that day. Including that day in the new threshold calculation would skew the resulting threshold value. Thus any working day that has less than the minimum activity will not be included in the new ***PAM*** threshold calculation.

6.3.1 Setting the minimum activity value

The minimum activity values for the ***PAM*** auto threshold calculation are outlined in the sub sections below.

6.3.1.1 Minimum concurrent requests

The minimum number of concurrent requests required for a day's activity to be included in the ***PAM*** auto threshold calculation can be set using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API_2.PAM_AT_MIN_REQUESTS_SET ( 200 );
```

Parameter 1:

The minimum number of concurrent request required before that day's data can be used in the ***PAM*** auto threshold calculation.

Note: Minimum number of requests allowable is 100

6.3.1.2 Minimum full service connections

The minimum number of full service connections required for a day's activity to be included in the ***PAM*** auto threshold calculation can be set using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API_2.PAM_AT_MIN_FS_CONNECTIONS_SET ( 50 );
```

Parameter 1: The minimum number of full service connections required before that day's data can be used in the ***PAM*** auto threshold calculation.

Note: Minimum number of requests allowable is 10

6.3.1.3 Minimum self-service connections

The minimum number of self-service connections required for a day's activity to be included in the ***PAM*** auto threshold calculation can be set using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API_2.PAM_AT_MIN_SS_CONNECTIONS_SET ( 200 );
```

Parameter 1: The minimum number of self-service connections required before that day's data can be used in the ***PAM*** auto threshold calculation.

Note: When assessing the minimum number of session, you should be aware that the Oracle OAM application or the Oracle enterprise manager applications will generate a self-service session every 10 minutes (default frequency) as part of its internal checking process.

6.4 What if I don't have sufficient on-line history?

Where there is insufficient online history in the ***PAM*** repositories for the ***PAM*** auto threshold process to access, ***PAM*** will disable the specific auto threshold

update affected by the lack of on-line information. The last threshold value will remain in place until there is sufficient online information.

6.5 E-mail alert

When there is insufficient information held in the ***PAM*** repository to calculate a threshold value for an alert, the auto threshold for that alert will be disabled and a ***PAM*** alert email will be sent:

Example *PAM* AT-001 – *PAM* auto threshold disabled alert message

ALERT MESSAGE FROM *PAM* - PIPER-Rx Application Monitor - DO NOT REPLY

Company = Company name
Site = Site name
Alert Level = **Informational**
Detected = 28-Feb-11 (Mon) 15:21:32
Alert Frequency = 1 Month

PAM Auto Threshold has disabled auto thresholds for CR-003

Note: No threshold changes will occur until there is sufficient information in the ***PAM*** repositories for the selected alert

If an auto threshold value had been disabled due to insufficient information being available and there is now sufficient information held in the ***PAM*** repositories for a threshold to be updated, ***PAM*** will re-enable that auto threshold and send an alert e-mail:

Example *PAM* AT-001 – *PAM* auto threshold enabled alert message

ALERT MESSAGE FROM *PAM* - PIPER-Rx Application Monitor - DO NOT REPLY

Company = Company name
Site = Site name
Alert Level = **Informational**
Detected = 28-Feb-11 (Mon) 15:03:11
Alert Frequency = 1 Month

PAM Auto Threshold has enabled auto thresholds for WF-101

6.6 Enabling the *PAM* auto threshold feature

The ***PAM*** auto threshold feature is disabled out of the box. The feature can be enabled using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'IN-003', 'Y');
```

and can be disabled using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'IN-003', 'N');
```

Note: IN-003 is the item that checks and sets the auto threshold values; AT-001 provides the ***PAM*** alert.

6.7 Turning off Auto threshold for individual checks

Auto threshold calculations can be disabled for individual ***PAM*** auto threshold checks using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API_2.PAM_AT_AUTO_CHECK_SET ( 'CR-002', 'N' );
```

Parameter 1: The ***PAM*** auto threshold check to be disabled
Parameter 2: 'Y' Enabled, 'N' Disabled

The ***PAM*** auto threshold can be re-enabled using the following ***PAM*** API:


```
exec PIPER_RX_PAM_API_2.PAM_AT_AUTO_CHECK_SET ( 'CR-002', 'Y' );
```

6.8 What are my current *PAM* AT settings?

The current ***PAM*** settings can be found using ***PAMreports*** - Config PAMC014 PAM Auto Threshold Settings:

Example **PAMC014 PAM Auto Threshold Settings** report

PAMC014-10 — PIPER-RX - APPLICATION MONITOR — PIPER - Rx
Auto Threshold Settings
As at 16-Dec-10 13:40:27
For APPS 12i

Alert ID	Description	AUTO	Status	STDDEVS
CR-002	Alert when the number of Completed Error Requests exceeds	Yes	Disabled	2.0
CR-003	Alert when the number of Total Completed Requests exceeds	Yes	Disabled	2.0
CR-004	Alert when the number of Completed Warning Requests	Yes	Disabled	2.0
PF-001	Alert when the overall application performance is degraded	Yes	Disabled	2.0
UA-002	Alert when the number of connected full service user accounts	Yes	Disabled	2.0
UA-004	Alert when the number of Self Service Sessions exceeds the	Yes	Disabled	2.0
UA-005	Alert when the total number of Self Service Page Requests (Day)	Yes	Disabled	2.0
WF-101	Alert when the number of Active Workflow Items exceeds the	Yes	Enabled	2.0
WF-102	Alert when the number of Completed Workflow Items exceeds	Yes	Enabled	2.0
WF-103	Alert when the number of Deferred Workflow Items exceeds the	Yes	Enabled	2.0
WF-104	Alert when the number of Error Workflow Items exceeds the	Yes	Enabled	2.0
WF-105	Alert when the number of Notified Workflow Items exceeds the	Yes	Enabled	2.0
WF-106	Alert when the number of Suspended Workflow Items exceeds	Yes	Enabled	2.0
WF-107	Alert when the number of Waiting Workflow Items exceeds the	Yes	Enabled	2.0
WF-108	Alert when the number of Timeout Workflow Items exceeds the	Yes	Enabled	2.0
WF-109	Alert when the number of Stuck Workflow Items exceeds the	Yes	Enabled	2.0
WF-110	Alert when the number of workflow Mail Items Waiting to be sent	Yes	Enabled	2.0
WF-111	Alert when the number of active workflows exceeds the	Yes	Enabled	2.0
WF-112	Alert when the number of completed workflows exceeds the	Yes	Enabled	2.0

AUTO = Allow auto threshold to be disabled if there is insufficient on-line history and re-enabled when there is sufficient on-line history

The **AUTO** attribute indicates the specific ***PAM*** alert that will be updated by the ***PAM*** auto threshold feature.

The **Status** attribute will display disabled if there is insufficient online history in the ***PAM*** repositories to calculate a suitable threshold value.

6.9 Setting the standard deviation values

The standard deviations are used as part of the ***PAM*** auto threshold calculation. The new threshold is calculated using the historical week day average plus a number of standard deviations.

In a normally distributed set of statistics (which this is not) two (2) standard deviations will cover 95.5% of all sample and three (3) standard deviation will cover 99.7% of all values, thus setting a value of three (3) standard deviations will in principle set a threshold high enough for ***PAM*** not to alert on “normal” high activity.

Note: Setting a value above 3 standard deviations is of no value as three (3) standard deviation covers 99.7% of samples, four (4) covers 99.993% and five (5) standard deviations covers 99.99994% of samples.

The standard deviations for all auto threshold alerts can be set using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_AT_STD_DEV_SET_ALL ( 2 ) ;
```

Parameter 1:

The number of standard deviations to set for all auto threshold alerts. Valid values are 1, 2 and 3.

The standard deviations for all individual auto threshold alerts can be set using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_AT_STD_DEV_SET ( 'CR-002', 3 ) ;
```

Parameter 1: The auto threshold alert that's standard deviation is to be set.
Parameter 2: The number of standard deviations. Valid values are 1, 2 and 3.

6.10 What are my current thresholds?

Current threshold values can be found using ***PAMreports*** - Config PAMC001b PAM Config (thresholds):

Example **PAMC001b PAM Config (thresholds)** report

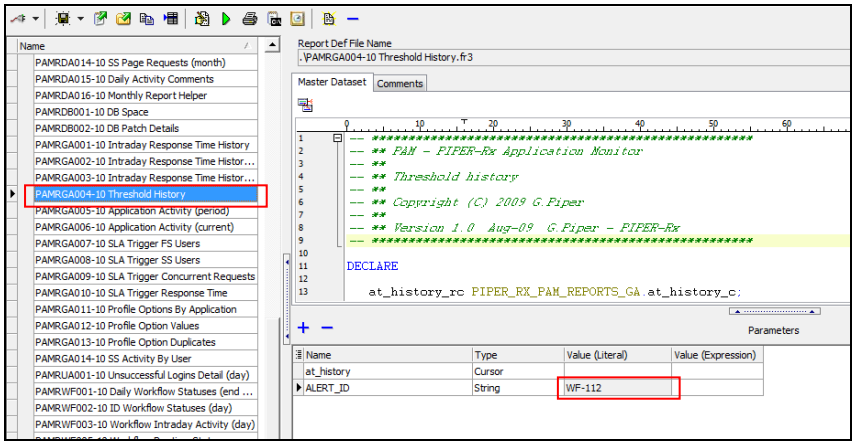
WF - Workflow Alerts					
WF-001	***Alert when there are excessive Workflow Background Processes running***		Active	1 Month	WF-001
	Number of workflow background processes runs per day	1000			
WF-002	***Alert when there are Long Running Workflows***		Active	1 Week	-
WF-003	***Alert when Old Active Workflows are detected***		Active	2 Months	-
	Workflow age in months	36			
WF-004	***Alert when possible Workflow spinners are detected***		Active	1 Week	WF-004
WF-101	***Alert when the number of Active Workflow Items exceeds the threshold value***		Active	1 Hour	WF-101
	Active workflow items threshold	47854			
WF-102	***Alert when the number of Completed Workflow Items exceeds the threshold value***		Active	1 Hour	WF-102
	Completed workflow items threshold	458339			
WF-103	***Alert when the number of Deferred Workflow Items exceeds the threshold value***		Active	15 Minutes	WF-103
	Deferred workflow items threshold	1772			
WF-104	***Alert when the number of Error Workflow Items exceeds the threshold value***		Active	30 Minutes	WF-104
	Error workflow items threshold	14107			

6.11 Auto threshold history

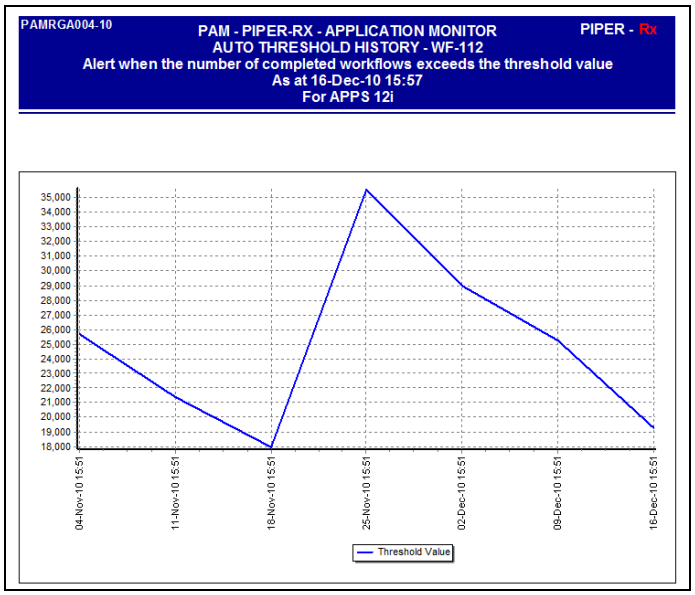
Whenever a ***PAM*** threshold is updated a record of that change is written to the ***PAM*** piper_rx_pam_at_history repository. The historical information can be viewed using ***PAMreports*** - General PAMRGA004 Threshold History. The report requires the alert_id of interest to be entered as a report variable

Valid auto threshold alert id's can be found using ***PAMreports*** - Config PAMC014 PAM Auto Threshold Settings:

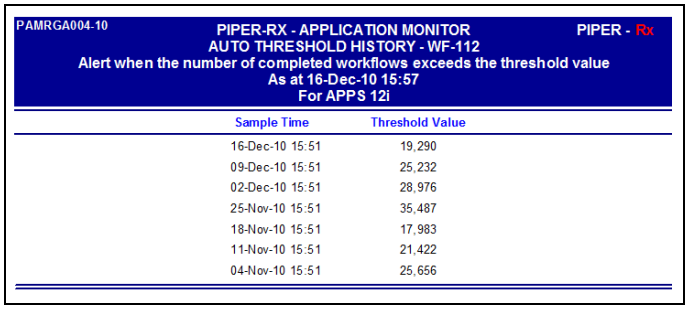
Example **PAMRGA004 Threshold History** variable entry page



Example **PAMRGA004 Threshold History** report (Page 1)



Example **PAMRGA004 Threshold History** report (Page 2)



Note: These values are the ***PAM*** threshold values, not actual values.

In the above example you can clearly see the purge date and the rate at which completed workflows are occuring.

These reports provide a good insight into the changing landscape of your business applications over time and are great KPI indicators as well as being immensely useful when renegotiating SLAs with the business.

6.11.1 Auto History purge

Whenever a ***PAM*** threshold is changed a record of that change is written to the ***PAM*** piper_rx_pam_at_history repository. There is an auto purge process that will purge all records older than the defined number of days (default 730 days). The number of days auto threshold history to be held on line can be set using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API_2.PAM_AT_PURGE_DAYS_SET    ( 730 ) ;
```

Parameter 1: The number of day's history to be held on-line.

7 Disclaimer

All material contained in this document is provided by the author "as is" and any express or implied warranties, including, but not limited to, any implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the author be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of any content or information, even if advised of the possibility of such damage. It is always recommended that you seek independent, professional advice before implementing any ideas or changes to ensure that they are appropriate.