PAMtutorials 8: User Account security

Basic Security Salvos

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* 8

PAMtutorials 8 provides a look into application user accounts covering the following items:

Aged Application accounts

Alert when application accounts have never been accessed or have not been used in the past 120 days (aging days). We have also introduced an account grace feature to exclude newly created accounts not used for a period of 30 days. Both grace period and aging days are configurable

Unsuccessful logins

Alert if there has been more than 3 (default) unsuccessful login attempts on any application account during the day

Monitor selected application accounts

PAM provides the ability to monitor selected application accounts for:

- Accounts that should never be end dated but have been given an end date
- A monitored account that has been end dated and that end date has passed

Accounts due to expire

Alert when an end dated account is due to expire within the next calendar month. Whilst not directly a security issue, it is an important business process and can prevent waited time and effort

This tutorial is just a first look into basic application security; we have built a user account audit module which will be released later, as the ***PAM*** tutorial / learning regime dictates we want to tidy up first then look at the detail.

2 Aged application user accounts UA-001

All too often accounts are created but rarely closed (end dated) when a person leaves.

An application account cannot be removed, only end dated.

One option is to treat management of your application user account in a similar manner to aged debtors. That is, to identify any accounts that are either not being used or have not been used in the past 120 days.

2.1 How this works (technical)

All the information you need is in the table applsys.fnd_user in the column last_logon_date. Whenever an account is accessed the last_logon_date is updated.

Note: In some very earlier versions of 11i self service connections did not update this field.

If the last_logon_date value is null then the account has never been used or if the last_logon_date value is older than 120 days the account is a candidate for investigation

2.2 *PAM* aged user account e-mail alert

Once per month ***PAM*** will check and raise an alert for application user accounts that have either never been accessed (after the new account grace period) or has not been accessed in the past 120 days.

Example *PAM* UA-001 – *PAM* Aged accounts e-mail alert message

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

Company = Company name
Site = Site name
Alert Level = **Informational**
Detected = 23-Feb-11 (Wed) 05:00:00
Alert Frequency = 1 Month

---

56 aged application user accounts have been detected

Alert Information:

UA-001 Aged Application Accounts

ONE OR MORE AGED APPLICATION ACCOUNTS HAVE BEEN DETECTED.

An aged application account is any account that has either never been used or has not been used in the threshold number of days

If you want to obtain a list of aged application accounts you can use ***PAMreports*** - Actions **PAMAUA001 Aged Application Accounts**

Note 1: Application accounts can be excluded from the aged account check by adding the accounts **user_id** to the **piper_rx_pam_account_ex** table

Note 2: If you want to obtain a list of excluded accounts you can use ***PAMreports*** - Config **PAMC011 PAM Aged Users Exclusions**. Any account information shown in red in this report indicates the account has been accessed

Note 3: A new account grace period has been included so as not to identify new application accounts as never connected until the grace period has passed [Default 30 days]

Note 4: An aged account is any account that has not been accessed in the past **X** days [Default 120 days]

Note 5: Both the grace period and aging days are ***PAM*** settings. If you want change these values refer to FAQs for more information

2.3 What to do with this information

You can use ***PAMreports*** -Actions PAMAUA001 Aged Application Accounts to list aged user accounts:

Example **PAMAUA001 Aged Application Accounts** report

PAMAUA001-20

PAM - PIPER-RX - APPLICATION MONITOR
Aged Application User Accounts
Account grace days - 30 : Account aging days - 120
as at 25-Feb-11 09:08
for APPS 12i

PIPER - Rx

user ID	User Name	User Description	Account Start Date	Last Connect Date	Age (days)
1325	APERKINS	Alan Perkins	05-May-97	Never Connected	
1874	COMPSERV	Customer, Computer Service & Rentals	17-Jul-98	Never Connected	
1876	KWALLUK		17-Jul-98	Never Connected	
1877	LDOUGLAS		17-Jul-98	Never Connected	
1	AUTOINSTALL	This application user name represents conversion o...	01-Jan-51	10-Aug-95 16:58	5,678
1076	ALAW		01-Mar-97	05-Mar-97 08:56	5,105
1404	RESTRICTED	Restricted access to HRMS applications	03-Jul-97	05-Aug-98 18:29	4,251
1068	MFG	MANUFACTURING SUPER USER	01-Jan-96	06-Aug-98 09:43	4,250
1322	LEDGER	ALL GL responsibilities for all sets of	22-Apr-97	06-Aug-98 12:09	4,250
1050	CBLACK	Chris Black	19-Feb-97	06-Aug-98 13:51	4,250
1384	HRMS	HRMS Superuser responsibility	01-Jan-90	06-Aug-98 14:09	4,250
1649	DHOF	JE Workflow Approval user	13-Dec-97	07-Aug-98 10:22	4,249
1278	FLOW	Terry Green	11-Apr-97	04-Sep-98 16:15	4,221
1318	OPERATIONS	Pat Stock	01-Apr-96	12-Aug-99 18:17	3,879

Accounts excluded from the Aged Application Account check: 2

This report will also show the number of accounts that have been excluded from the ***PAM*** aged accounts alerting process. This will be covered later in this section of the tutorial.

Note: This report will not display any new accounts that have not been accessed within the Account grace day's period.

You can send this report to HR or whoever manages user accounts for action.

2.4 Aged user grace days

When new accounts have been created, often they are not used for some time. So as to prevent these new accounts from appearing in the ***PAM*** aged accounts as accounts not used, ***PAM*** has included the aged user account grace days feature, that is the number of days a new account has to have been in place before that account is included in the aged account alert - default (30 days).

You can change the number of grace days using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_AGED_USER_SETTINGS_GRACE ( 30 );
```

Parameter: The number of grace days

2.5 Aged user days

An account must have had no activity for 120 days (default) for ***PAM*** to alert that the account has not been used. In some instance you may wish to increase or lower the number of days. The number of inactive days can be changed using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_AGED_USER_SETTINGS_AGE ( 120 );
```

Parameter 1: The number of days an account is inactive before ***PAM*** will alert on that account

2.6 Aged user account exclusion list

You can obtain a list of accounts excluded from the aged user check using ***PAMreports*** - Config PAMC011 PAM Aged Users Exclusions:

Example **PAMC011 PAM Aged Users Exclusions** report

PAMC011-20

PAM - PIPER-RX - APPLICATION MONITOR
Aged User Exclusion List
As at 25-Feb-11 09:13:37
For APPS 12i

PIPER - Rx

User ID	User Name	Description	Check Status	Account Activity		
				Full Service	CR	Self Service
0	SYSADMIN	System administrator	Enabled	-	24-Jan-11	03-Aug-08
6	GUEST	guest	Enabled	-	-	-

Accounts displayed in red colour indicates the account has been accessed and should be reviewed

PAM has included an additional audit check in this report by showing if the excluded account has been used. ***PAM*** will check both the full and self service audit objects fnd_logins and icx_sessions as well as fnd_concurrent_requests and shows the last activity date if any activity was found in any of these objects related to the excluded user account. Obviously this is dependant on the amount of available on-line history available at your site.

2.7 Excluding Application accounts from the aged user check

Application accounts can be excluded from this check by adding the application accounts internal user_id to the ***PAM*** application user accounts exceptions table piper_rx_pam_account_ex.

We specifically use the Application accounts user id as it is unique and not changeable where as the user name is changeable (Refer to the section ***"Did you know you can change a user account name"***).
However, for ease of use when adding accounts to the ***PAM*** account exceptions using the ***PAM*** API we enter the account by account name, the API will determine the application account id

An account can be added to the ***PAM*** account exceptions table using the following ***PAM*** API:

```
BEGIN

   PIPER_RX_PAM_API.PAM_ACCOUNT_EXCEPTION_ADD
       ( 'GPIPER', -- Application account
         'Y',      -- Account check status
         'Y',      -- Exclude from aged accounts
         'N',      -- Include in account end date check
         'N' );    -- Include in expired account check

END;
```

Parameter 1:
The application account name, this Will be converted to user_id by the API
Parameter 2:
Overall check status, setting this value to 'N' is similar to temporarily removing the account from the exceptions table
Parameter 3:
Exclude this account from the aged accounts check (AU-001)
Parameter 4:
Exclude this account from the account end date check – covered later in this tutorial
Parameter 5:
Exclude this account from the expired account check – covered later in this tutorial

2.8 Removing an account from *PAM* account exceptions

An application account can be removed from the account exception list using the following ***PAM*** API:

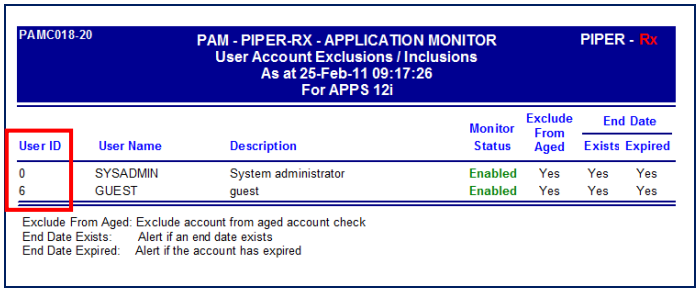
```
exec PIPER_RX_PAM_API.PAM_ACCOUNT_EXCEPTION_DEL  ( 1914 );
```

Parameter: This is the application user account ID

2.8.1 How to find the account ID for the account you want to remove.

You can use ***PAMreports*** - Config **PAMC018 PAM Account Exclusions Inclusions** to list the current ***PAM*** user account exceptions:

Example **PAMC018 PAM Account Exclusions Inclusions** report



PAMC018-20

PAM - PIPER-RX - APPLICATION MONITOR
User Account Exclusions / Inclusions
As at 25-Feb-11 09:17:26
For APPS 12i

PIPER - Rx

User ID	User Name	Description	Monitor Status	Exclude From Aged	End Date Exists	End Date Expired
0	SYSADMIN	System administrator	Enabled	Yes	Yes	Yes
6	GUEST	guest	Enabled	Yes	Yes	Yes

Exclude From Aged: Exclude account from aged account check
End Date Exists: Alert if an end date exists
End Date Expired: Alert if the account has expired

This report provides the account User ID which can then be used in the ***PAM*** API.

2.9 How do I turn the *PAM* aged user account alert off and on again?

The ***PAM*** aged user account alert can be turned off using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'UA-001', 'N');
```

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

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'UA-001', 'Y');
```

2.10 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.

2.11 Did you know you can change a user account name?

Whilst the account name has to be unique, the internal key is based on the account ID not the name.

So why would you change an account name?

- You want to implement a user naming standard

- The user name was entered incorrectly
- A new employee has the same name as an ex employee
- A user changed their name

Example:

> Once a user is no longer with the company, end date the account and change the account name by adding an X_ to the beginning of the account name i.e. The account DSMITH becomes X_DSMITH.
>
> Firstly it now becomes very clear that the account name is no longer used and secondly the account name DSMITH can be used by the new employee.

Of course you will need to get this approach signed off by internal audit first. Usually, as long as there is consistent documented evidence of the change audit are generally ok.

This is all done via the standard Oracle application screens (Users > Define) just select the user, change the users name and commit.

Note: If you change the name of an active account, i.e. a user's name has changed, you will need to reset that user's password and let them know the password you have set and that they will be required to change their password on first connecting with the new name.

3 UA-003 Unsuccessful logins

An unsuccessful login is when the login fails in most cases due to an incorrect password. I have seen instances where there have been over 50 failed attempts on a users account in one day – they were persistent if nothing else. I have also witnessed multiple failed after hours attempts on a high level account.

It is also understood that you don't want to be notified on every failed attempt so ***PAM*** has implemented a threshold value where by the number of failed attempts must be greater than the threshold value before an alert is raised. Once this threshold has been exceeded for any account, any additional failed attempts during the day will raise a ***PAM*** alert. The number of failed attempts is reset to zero each midnight (database server time).

Note: ***PAM*** will identify the account that is being accessed it does not provide any additional tracking information.

3.1 PAM unsuccessful login e-mail alert

When the number of unsuccessful login attempts for any exceeds the ***PAM*** threshold value a ***PAM*** alert e-mail is raised:

Example *PAM* UA-003 – *PAM* unsuccessful login e-mail alert message

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

Company = Company name
Site = Site name
Alert Level = **Warning**
Detected = 25-Feb-11 (Fri) 07:00:00
Alert Frequency = 1 Hour

There have been 4 failed login attempts on account GPIPER

Alert Information:

UA-003 - Unsuccessful logins

THE NUMBER OF UNSUCCESSFUL LOGINS HAS EXCEEDED THE THRESHOLD VALUE

If you want to obtain a list of unsuccessful login attempts for each account that day where there have been more than the threshold value of unsuccessful attempts you can use ***PAMreports*** -Actions **PAMAUA003 Unsuccessful Logins (day)** entering the alert date

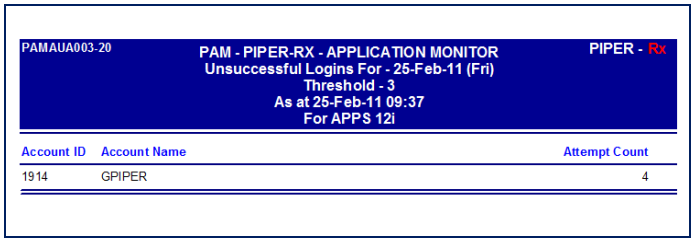
Note 1: An additional alert will be raised for each additional unsuccessful login attempt on this account during the current day

Note 2: If you want to change the alert threshold value refer to the FAQs for more information

3.2 What to do with this information

You can use ***PAMreports*** - Actions PAMAUA003 Unsuccessful Logins (day) to view the unsuccessful login attempts for any given day:

Example **PAMAUA003 Unsuccessful Logins (day)** report



PAMAUA003-20

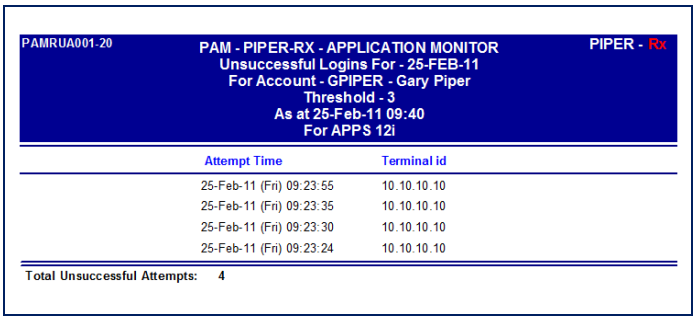
PAM - PIPER-RX - APPLICATION MONITOR
Unsuccessful Logins For - 25-Feb-11 (Fri)
Threshold - 3
As at 25-Feb-11 09:37
For APPS 12i

PIPER - Rx

Account ID	Account Name	Attempt Count
1914	GPIPER	4

For more detailed information you can use ***PAMreports*** - General PAMRUA001 Unsuccessful Logins Detail (day) to list failed attempt details for a selected user id and date:

Example **PAMRUA001 Unsuccessful Logins Detail (day)** report



PAMRUA001-20

PAM - PIPER-RX - APPLICATION MONITOR
Unsuccessful Logins For - 25-FEB-11
For Account - GPIPER - Gary Piper
Threshold - 3
As at 25-Feb-11 09:40
For APPS 12i

PIPER - Rx

Attempt Time	Terminal id
25-Feb-11 (Fri) 09:23:55	10.10.10.10
25-Feb-11 (Fri) 09:23:35	10.10.10.10
25-Feb-11 (Fri) 09:23:30	10.10.10.10
25-Feb-11 (Fri) 09:23:24	10.10.10.10

Total Unsuccessful Attempts: 4

Time of day shown in this report could indicate inappropriate activity.

The next step is to contact the user and ask them if they are experiencing an issue logging into the application and can you help in any way, if its not them having a problem then you have an issue.

Note: Unsuccessful login attempts data is purged as part of the OEBS applications sign-on audit purge process.

In more recent times the profile option signon_password_failure_limit is often set, in which case that account is locked when the number of failed attempts is reached. Where this is the case you may wish to set the ***PAM*** failed attempts threshold to the profile option value in which case you will be notified when a user account becomes locked.

3.3 Setting the unsuccessful login attempt threshold

The ***PAM*** unsuccessful login attempt threshold can be set using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_UNSUCCESSFUL_LOGIN_SET ( 3 );
```

Parameter: The number of failed login attempts in any given day after which an alert will be raised.

3.4 How do I turn the *PAM* Unsuccessful login alert off and on again?

The ***PAM*** unsuccessful login alert can be turned off using the following ***PAM*** API:

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

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

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

3.5 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.

3.6 How to manual force a password reset

It is possible to force a user's password to expire requiring them to reset their password when they next connect.

THIS PROCESS IS INFORMATIONAL ONLY AND IS ABSOLUTELY NOT A RECOMMENDED PROCESS – YOU MUST NEVER DIRECTLY CHANGE A BASE TABLE USING SQL

You simply set the users password_date in applsys.fnd_user table to null, don't forget the table audit columns…. The next time the user connects they will be forced to reset their password.

```
UPDATE FND_USER
   SET password_date = null,
       last_update_date = sysdate,
       last_updated_by = 0, -- 0 is SYSADMIN
       last_update_login = 0 -- 0 is SYSADMIN
 WHERE user_id = USER_ID;
```

WHERE [USER_ID] is the user ID of the application account who's password you want to reset.

Why would you do this?

A good example is for a possible security breach and you want to force a reset of a large number of passwords - Under audit supervision of course

A more fun example; although not recommended, is to regularly reset an annoying user's password ☺

4 Monitored Application Accounts

PAM will monitor application accounts for:

- Accounts that should never be end dated but has been given an end date
- A monitored account who's end date has passed
- Accounts that are due to expire within the next months

4.1 UA-008 Account end dated

There are a number of OEBS application accounts that should never be end dated such as sysadmin, Guest etc… ***PAM*** provides the ability to monitor selected user accounts and to alert if any of the monitored accounts are ever end dated.

4.1.1 *PAM* monitored account - end dated e-mail alert

A ***PAM*** alert e-mail is raised when ***PAM*** detects that a monitored account has been given an end date:

Example *PAM* UA-008 – *PAM* monitored account end dated alert message

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

Company = Company name
Site = Site name
Alert Level = **Warning**
Detected = 25-Feb-11 (Fri) 05:00:00
Alert Frequency = 4 Hours

Monitored account GPIPER has been end dated

Alert Information:

UA-008 - A Monitored Account has been End Dated

A MONITORED ACCOUNT HAS BEEN END DATED

This has the potential to cause issues with the normal running of the application. E.g. If the GUEST account is end dated there are several application functions that require that account to be active that will cease to function

If you want to view the current list of monitored accounts you can use ***PAMreports*** - Config **PAMC018 PAM Account Exclusions Inclusions**

Note 1: If you want to add, change or modify a monitored user account refer to the FAQs for more information

Note: Once a ***PAM*** alert has been raised for any given account, ***PAM*** will not raise additional alerts until the next day if the account is still end dated.

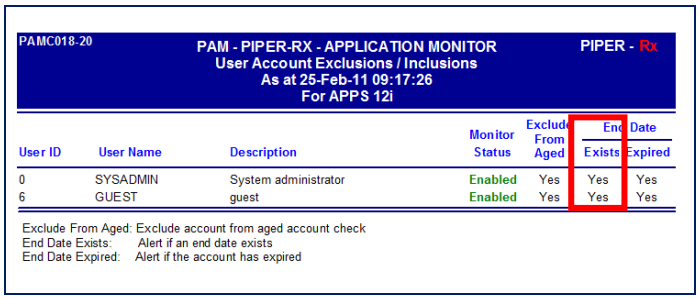
You may want to monitor your own account, that way you can identify if your services are no longer required ☺

4.1.2 What to do with this information

Depending on the account, immediate action may be required in removing the end date.

You can use ***PAMreports*** - Config PAMC018 PAM Account Exclusions Inclusions to list the current ***PAM*** user account exceptions:

Example **PAMC018 PAM Account Exclusions Inclusions** report



PAMC018-20

PAM - PIPER-RX - APPLICATION MONITOR
User Account Exclusions / Inclusions
As at 25-Feb-11 09:17:26
For APPS 12i

PIPER - Rx

User ID	User Name	Description	Monitor Status	Exclude From Aged	End Date Exists	End Date Expired
0	SYSADMIN	System administrator	Enabled	Yes	Yes	Yes
6	GUEST	guest	Enabled	Yes	Yes	Yes

Exclude From Aged: Exclude account from aged account check
End Date Exists: Alert if an end date exists
End Date Expired: Alert if the account has expired

4.1.3 How do I turn the *PAM* monitored accounts end dated alert off and on again?

The ***PAM*** monitored accounts end dated alert can be turned off using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'UA-008', 'N');
```

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

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'UA-008', 'Y');
```

4.1.4 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.

4.2 UA-009 Monitored accounts closed

PAM alerts when a monitored account has been end dated and that accounts end date has passed (Account closed). Generally you would use this check for high value accounts only that should not be closed.

4.2.1 *PAM* monitored account closed e-mail alert

A ***PAM*** alert e-mail is raised when ***PAM*** detects that a monitored accounts end date has passed and that account is now closed:

Example *PAM* UA-009 – *PAM* monitored account closed alert message

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

Company = Company name
Site = Site name
Alert Level = **Warning**
Detected = 25-Feb-11 (Fri) 05:00:00
Alert Frequency = 15 Minutes

Monitored account GPIPER has expired

Alert Information:

UA-009 - A Monitored Account has been closed

A MONITORED ACCOUNT HAS BEEN CLOSED (The end date time has

passed)

This has the potential to cause issues with the normal running of the application. E.g. If the GUEST account is end dated there are several application functions that require that account to be active that will cease to function

If you want to view the current list of monitored accounts you can use ***PAMreports*** - Config **PAMC018 PAM Account Exclusions Inclusions**

Note 1: If you want to add, change or modify a monitored user account refer to the FAQs for more information

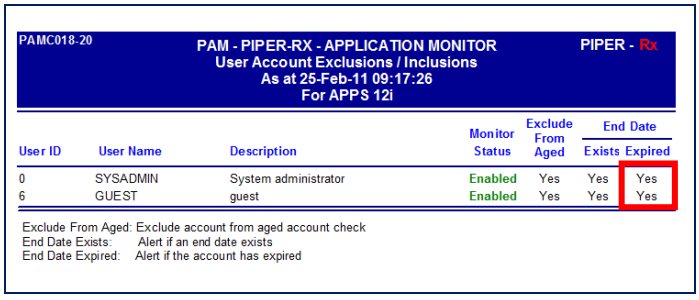
This alert will continue to alert every check cycle (default 15 minutes) until the account end date is changed or the account is removed from the ***PAM*** exceptions list

4.2.2 What to do with this information

Depending on the account, immediate action may be required in removing or extending the accounts end date.

You can use ***PAMreports*** - Config PAMC018-10 PAM Account Exclusions Inclusions to list the current ***PAM*** user account exceptions:

Example **PAMC018-10 PAM Account Exclusions Inclusions** report



PAMC018-20

PAM - PIPER-RX - APPLICATION MONITOR
User Account Exclusions / Inclusions
As at 25-Feb-11 09:17:26
For APPS 12i

PIPER - Rx

User ID	User Name	Description	Monitor Status	Exclude From Aged	End Date Exists	End Date Expired
0	SYSADMIN	System administrator	Enabled	Yes	Yes	Yes
6	GUEST	guest	Enabled	Yes	Yes	Yes

Exclude From Aged: Exclude account from aged account check
End Date Exists: Alert if an end date exists
End Date Expired: Alert if the account has expired

4.2.3 How do I turn the *PAM* monitored accounts closed alert off and on again?

The ***PAM*** monitored accounts closed alert can be turned off using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'UA-009', 'N');
```

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

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'UA-009', 'Y');
```

4.3 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.

5 UA-010 Account due to expire

PAM will send an alert when any end dated accounts is due to expire within the next calendar month, being pre notified of accounts that are due to expired. The rationale is to identify those accounts where the user's time with the company has been extended but the account end date has not been extended. What we are endeavoring to prevent is the user to turning up one morning to find that their accounts has expired and then having to spend half a day trying to get the account extended.

Example:

> User X is a contractor whose contract expires 10th November. The temporary OEBS account created for the contractor has been set to expire on the 11th November. Prior to the end of the contractors term the contractors contract was extended for an additional 3 months, but the end date for the contractors account has not been changed. On the 11th the contractor spends most of the day dealing with support trying to prove their contract had been extended to get the account reopened – one lost day…

This ***PAM*** check will not include any accounts that are currently being monitored by ***PAM*** for:

End date check:
Alert is a monitored account has been given an end date (UA-008)

Expired account:
Alert when a monitored account has been end dated and that end date has passed (UA-009)

PAM only alerts once per account unless the end date is changed.

5.1.1 *PAM* account/s due to expire e-mail alert

A ***PAM*** alert e-mail is raised when ***PAM*** detects that a monitored accounts end date has passed and that account is now closed:

Example *PAM* UA-010 – *PAM* accounts/s due to expire alert message

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

Site = Site name
Alert Level = **Informational**
Detected = 25-Feb-11 (Fri) 05:00:00
Alert Frequency = 1 Day

User account GPIPER will expire within 30 days on the 22-May-10. The account was last accessed 19-Apr-10 (2 day/s ago)

Alert Information:

UA-010 - Account/s due to expire

ONE OR MORE END DATED USER ACCOUNTS WILL EXPIRE WITHIN THE NEXT CALENDAR MONTH

This proactive notification is provided to alert when one or more user accounts has been end dated and that account will expire within the next calendar month

The rationale is to identify those accounts where the users time with the company has been extended but the account end date has not been extended. What we are endeavoring to prevent is the user to turning up one morning to find that their accounts has expired and then having to spend half a day trying to get the account extended.

You may want to on forward this notification to the appropriate internal group responsible for user accounts to check if the end dating of the account is still valid.

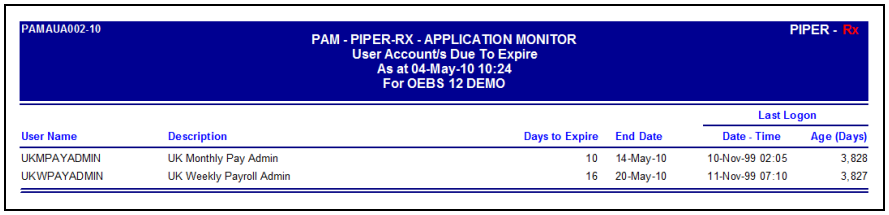
If you want to view the current list of accounts due to expire you can use ***PAMreports*** -Actions **PAMAUA008 Accounts Due To Expire**

Note: This alert will report only once per account, if the end date has been extended this alert will report again on that account

5.1.2 What to do with this information

You can use ***PAMreports*** - Actions PAMAUA008 PAM Accounts Due To Expire to list the current ***PAM*** user account that are due to expire within the next calendar month:

Example **PAMAUA008 PAM Accounts Due To Expire** report



PAMAUA002-10 PIPER - Rx

PAM - PIPER-RX - APPLICATION MONITOR
User Account/s Due To Expire
As at 04-May-10 10:24
For OEBS 12 DEMO

User Name	Description	Days to Expire	End Date	Last Logon Date - Time	Last Logon Age (Days)
UKMPAYADMIN	UK Monthly Pay Admin	10	14-May-10	10-Nov-99 02:05	3,828
UKWPAYADMIN	UK Weekly Payroll Admin	16	20-May-10	11-Nov-99 07:10	3,827

Send this report to HR or the group responsible for maintaining application user accounts so as they can extend the end dates as required.

5.1.3 How do I turn the *PAM* monitored accounts due to close on or off?

The ***PAM*** accounts due to closed alert can be turned off using the following ***PAM*** API:

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'UA-010 'N');
```

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

```
exec PIPER_RX_PAM_API.PAM_ALERT_ENABLE ( 'UA-010 'Y');
```

5.2 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.

5.3 User account exceptions

Application accounts can be excluded from the above ***PAM*** checks by adding the accounts internal User Id to the ***PAM*** application user accounts exceptions table piper_rx_pam_account_ex.

We specifically user the Application accounts user id as it is unique and not changeable. However, when adding, accounts using the ***PAM*** API we enter the account by account name, the API will determine the application account id.

An account can be added to the ***PAM*** account exceptions table using the following ***PAM*** API:

```
BEGIN
```

```
   PIPER_RX_PAM_API.PAM_ACCOUNT_EXCEPTION_ADD
       ( 'GPIPER', -- Application account
         'Y',      -- Account check status
         'Y',      -- Exclude from aged accounts
         'Y',      -- Include in account end date check
         'Y' );    -- Include in expired account check

END;
```

Parameter 1:
The application account name, this will be converted to the user_id by the API
Parameter 2:
Overall check status, setting this value to 'N' is similar to temporarily removing the account from the exceptions table
Parameter 3:
Exclude this account from the aged accounts check (AU-001)
Parameter 4:
Exclude this account from the account end date check – covered later in this tutorial
Parameter 5:
Exclude this account from the expired account check – covered later in this tutorial

5.4 Removing an account from *PAM* account exceptions

An application account can be removed from the account exception list using the following ***PAM*** API:

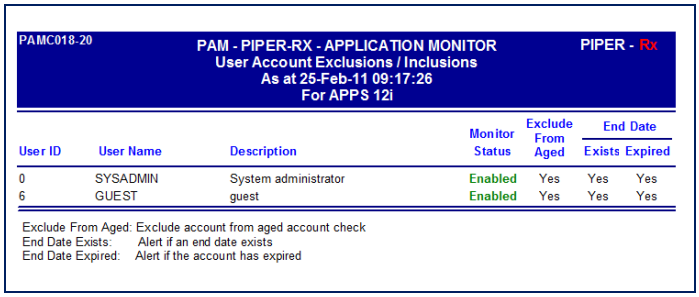
```
exec PIPER_RX_PAM_API.PAM_ACCOUNT_EXCEPTION_DEL  ( 1914 );
```

Parameter: This is the application user account ID

5.4.1 How to find the account ID for the account you want to remove

You can use ***PAMreports*** -Config PAMC018 PAM Account Exclusions Inclusions to list the current ***PAM*** user account exceptions:

Example **PAMC018 PAM Account Exclusions Inclusions** report



PAMC018-20

PAM - PIPER-RX - APPLICATION MONITOR
User Account Exclusions / Inclusions
As at 25-Feb-11 09:17:26
For APPS 12i

PIPER - Rx

User ID	User Name	Description	Monitor Status	Exclude From Aged	End Date Exists	End Date Expired
0	SYSADMIN	System administrator	Enabled	Yes	Yes	Yes
6	GUEST	guest	Enabled	Yes	Yes	Yes

Exclude From Aged: Exclude account from aged account check
End Date Exists: Alert if an end date exists
End Date Expired: Alert if the account has expired

This report provides the account User ID which can then be used in the ***PAM*** API.

6 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.