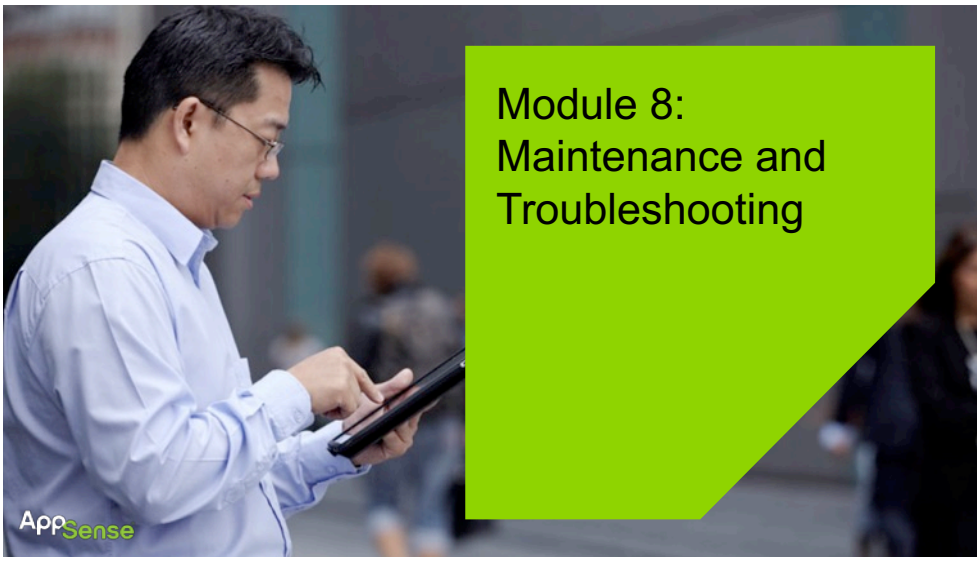


Module 8 : Maintenance and Troubleshooting

Exercise 1: Configuring and testing Diagnostics

Scenario

You have been asked to look at the different options available to troubleshoot endpoint behavior. Someone has mentioned Diagnostics to you previously as a way of helping identify issues. You have decided to test this feature on an endpoint.

Synopsis

During this lab you will enable and test Diagnostics on an end point.

Prerequisites

- FBN-DC01, FBN-SRV01 FBN-PC01.
- Ensure that **FBN-DC01** is started first
- Accounts used = FBN\administrator P/W= Pa55word

Objectives

At the end of this exercise, you will be able to:

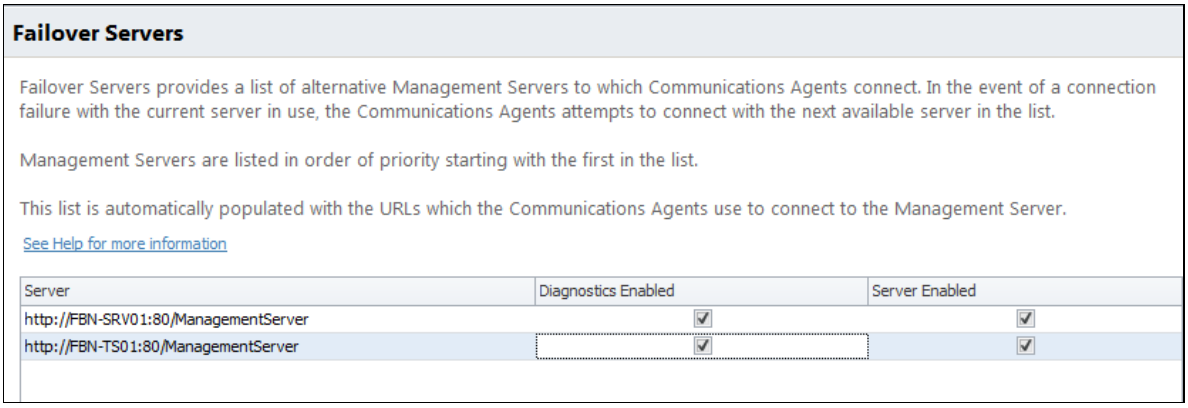
- Enable diagnostics from the Management Server and request diagnostics from an endpoint.
- Review the findings

Time Estimate

30 minutes

Enable Diagnostics on the Management Server

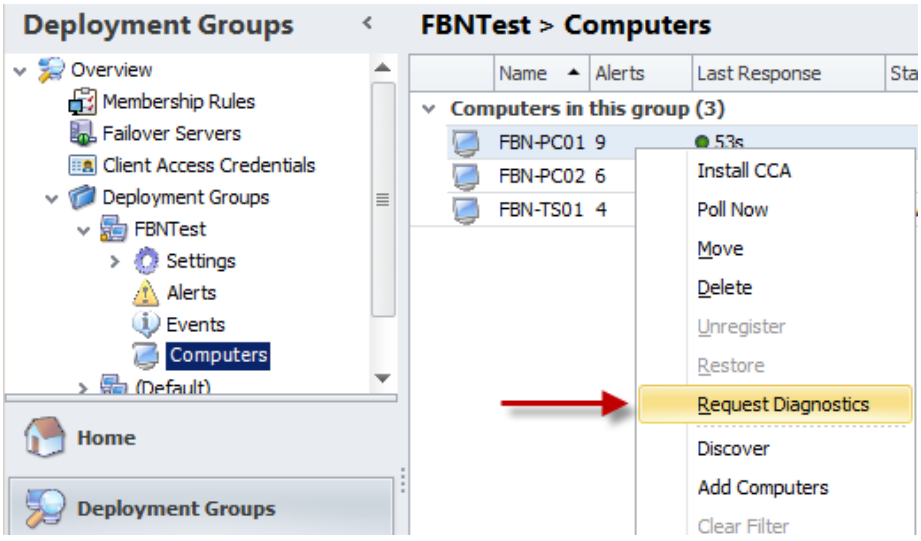
1. Log on to **FBN-SRV01** as **FBN\Administrator** and open the Management Centre console.
2. Select the **Deployment Groups** node from the left hand side.
3. Select **Overview >Failover Servers**. Ensure that the **Diagnostics Enabled** box is selected for both **FBN-SRV01** and **FBN-DC01**.



4. Remain logged on to **FBN-SRV01**

Running diagnostics on the Endpoints.

1. Logon to **FBN-PC01** as **FBN\Administrator**.
2. Browse to **C:\Postinstall\Lab\Module 8** and run **Break.exe.**
3. Change back to **FBN-SRV01**.
4. Select **Deployment Groups** on the Right hand side.
5. Expand **Overview >Deployment Groups >FBNTest >Computers**



6. In the Work Area Right click FBN-PC01 and select Request Diagnostics.

Wait for approximately 1 minute for the Diagnostics to complete.

Questions

What has passed the Diagnostics tests?

……

……

What has failed the Diagnostics tests?

……

……

Based on the of the failed Diagnostic Logging result, what services would need to be checked on the endpoint?

……

……

Repair FBN-PC01

Based on your assessment of the problem on FBN-PC01. Correct the issue and perform a successful Diagnostic test.

Note

You must complete this step in order to Continue with the Exercises.

End of Exercise

Exercise 2: Basic Troubleshooting- Application Manager

Scenario

Whilst undergoing POC testing for AM, one of the users in the HR department has reported the fact that they have been unable to run an instance of Word 2007 that they have found on a new public use machine located in the company's reception area. The machine should be part of the limited POC currently being undertaken and Word 2007 should be available on that endpoint. You have noted that there are no reasons why the user should not have been able to run the application, as there are no specific exclusion in the prohibited items listed for the users group, or rules prohibiting that application on that particular machine within the current AM configurations in use that you are aware of.

You need to start to determine why the application was not allowed to run?

Note

The role of the public endpoint will be taken by FBN-PC01 for the purpose of this lab.

Synopsis

In this exercise you will perform the 4 basic troubleshooting steps that should form part of any troubleshooting process involving AppSense's products.

The 4 steps are:

- Is the AppSense software installed?
- Are the AppSense Agents running?
- Is there a valid license installed?
- Is there a valid configuration installed?

Prerequisites

- FBN-DC01, FBN-SRV01, FBN-PC01.
- Ensure that **FBN-DC01** is started first
- Accounts used = FBN\administrator P/W= Pa55word

Objectives

At the end of this exercise, you will be able to:

- Perform a basic health check on the AMC and the endpoints.

Time Estimate

20 minutes

Is the AppSense software installed?

Based on the information not really required for the issue concerned, however not having the software installed on endpoints is a common error made and easy to check.

Log on to FBN\SRV01 as FBN\Administrator and check the version of the software installed?

Is this the same as the version installed on the endpoint FBN-PC01? Enter the version number below.

……..

Are the AppSense Agents running?

Although in this scenario it not likely, not having the agents running is a common cause of support calls. We have also stopped services in the previous exercise, so it is wise to check.

Log on to FBN\PC01 as FBN\Administrator.

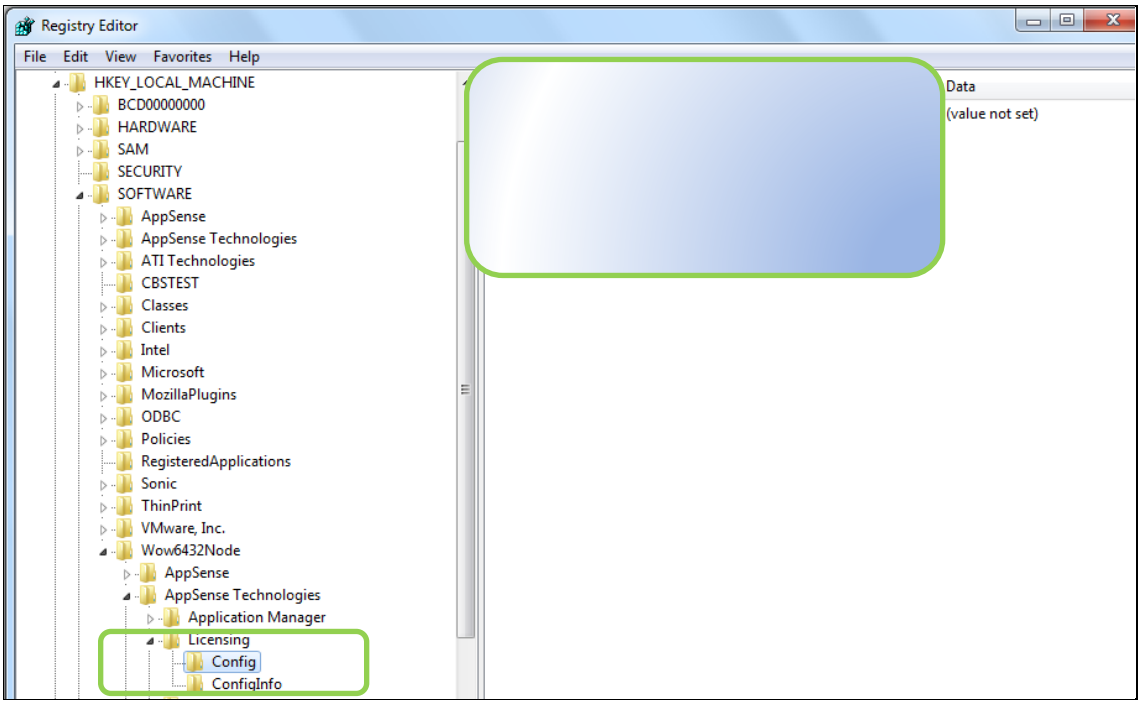
List the AppSense Services running on FBN\PC01.

What the relevant AM services and are they running?

Is there a valid license installed?

A valid licence is implied by the fact that AM has prevented an application running. However if for example a prohibited application had been allowed to execute on the endpoint then checking licenses would be a logical step to follow. Therefore, you will need to know how to check an endpoint for the presence of a license insuch and event.

7. Log on to FBN-PC01 as FBN\Administrator
8. Select Start and in the Search box and enter Regedt32.exe and press return.
9. In the tree items pane on the left hand side expand **HKEY_Local_MACHINE\SOFTWARE\Wow6432Node\AppSense Technologies\Licensing\Config** .



There should be a license or licenses listed (depending on environment).
You would probably check the AMC's licensing node to see if, a valid license was present first. However this only works if the AMC is being used.

10. Close **Regedt32**.

Enterprise Auditing could also be used to check the endpoint for the presence of a license.

What error code could you check for in relation to the problem faced, if you suspected it was licensing related?

……

……

Is there a Valid Configuration Installed?

This is probably the most common reason for an application not behaving the way intended. Configurations not being applied, configurations being applied to the wrong groups and configurations rules being incorrectly set, all account for a sizeable number of AppSense Support calls.

11. Log on to FBN-SRV01 as FBN\Administrator.

From within the **AMC** check the configuration that is applied to the Deployment Group that FBN-PC01 is a member of. Is the same configuration applied to the Endpoint FBN-PC01? Enter the configuration Number below.

……

……

12. Load the Current Am Configuration applied to FBN-PC01 into the AM Console on FBN-SRV01.

Check the rules, are there any rules specifically prohibiting the execution of Word to the HR group or to any group that the user could be a member of. (Check the Group membership via Active Directory Users and Computers if needed)?

……

……

You have just been through the 4 recommended basic troubleshooting steps. These were:

- **Is the Software installed?** The answer should be yes.
- **Are the Agents (services) running properly on the endpoints?** The answer should be yes.
- **Is there a valid License installed?** The answer should be yes.
- **Is there a valid configuration installed?** Again the answer should be yes.

So now we have ruled out all of the basics we can look at other possible issues.

End of Exercise

Exercise 3: Intermediate Troubleshooting- Rules Analyzer

Scenario

You've decided to use Rules Analyzer to see why the application was being blocked. You have a test HR account that you will use to check the behavior on the endpoint.

Synopsis

At the end of this exercise you will be able to use Rules Analyzer to determine why an application request has been allowed or denied.

Prerequisites

- **FBN-DC01**, **FBN-SRV01**, **FBN-PC01**.
- Ensure that **FBN-DC01** is started first
- Accounts used:
  - **FBN\administrator** - P/W= **Pa55word**
  - **FBN\HR1** - P\W= **Pa55word**

Objectives

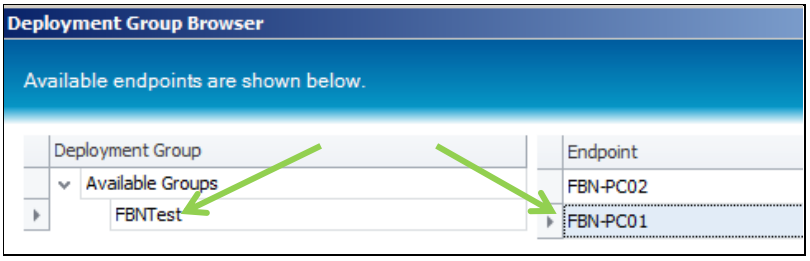
At the end of this exercise, you will be able to use the Rules Analyzer to check endpoint behavior.

Time Estimate

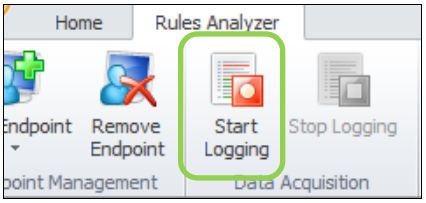
20 minutes

Enable Rules Analyzer and collate data for FBN-PC01

1. Log on to **FBN-SRV01** as **FBN\Administrator** and launch the AM Console.
2. Select the **Rules Analyzer** node on the left hand side of the console.
3. Select Add Endpoint >Browse Deployment Group and connect to the Management Server when prompted.
4. From within the Deployment Group Browser select the Deployment Group FBNTest and Endpoint FBN-PC01.

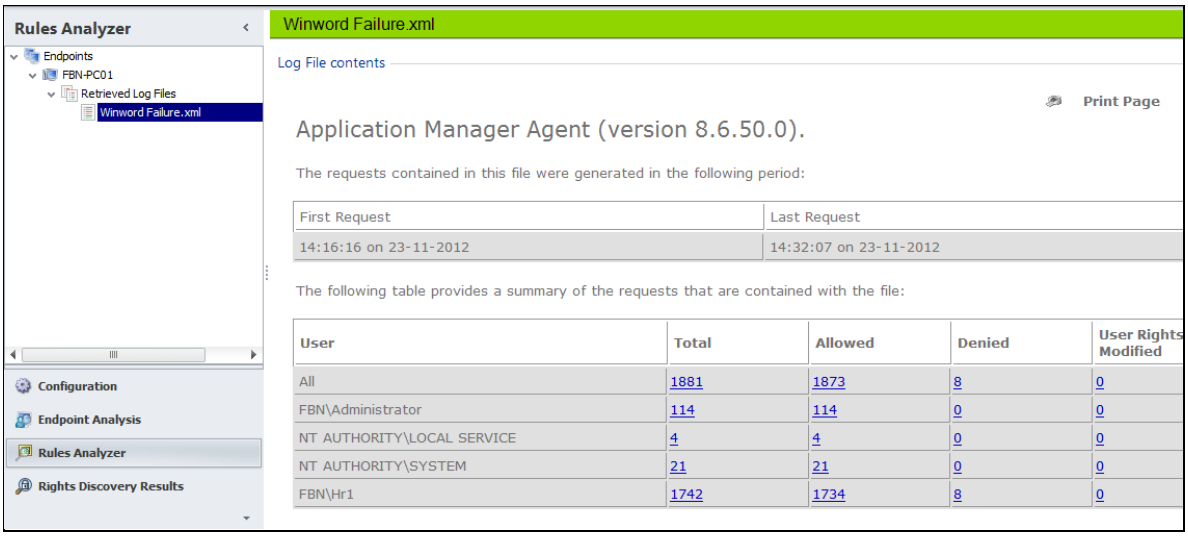


5. Click OK.
6. Click the Start Logging button from the Rules Analyzer menu bar

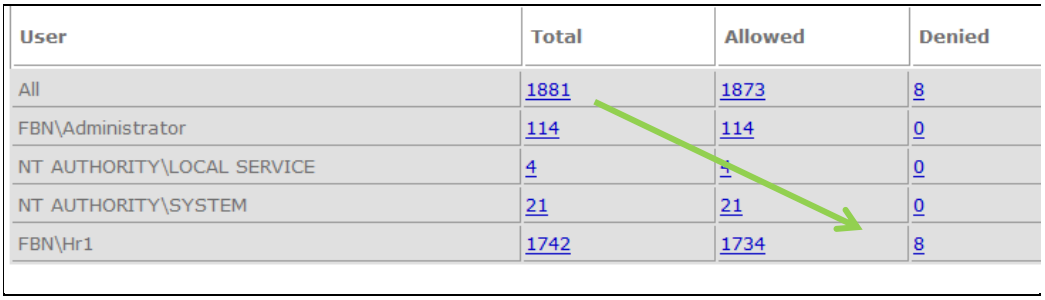


7. Whilst remaining logged on to **FBN-SRV01**, swap over to **FBN-PC01** and log on as **FBN\HR1**.
8. Navigate to **C:\Postinstall\Lab\Module 8** and run the **Winword** executable.
9. Log off **FBN-PC01** and switch back to **FBN-SRV01**.
10. From within the **Rules Analyzer node** select the **Stop Logging** button on the Menu bar.
11. When prompted to **Save Report** enter **Winword Failure** in the **Enter report name** box and click **Save**.

12. In the Rules Analyzer node on the left hand side select the Winword Failure.xml



13. From the Work Area Under the User Column Locate the entry for FBN\HR1 move to the Denied Column and click the blue number displayed.



14. From the Log File contents in the work area locate the entry for FBN\HR1 attempting to run C:\postinstall\lab\module 8\winword.exe and Double click the link.

What rule prevented winword.exe from running on FBN-PC01, and what reason was given?

……

……

Log into **FBN-PC01** as **FBN\Administrator** and browse to the **Module 8\ Lab** folder.

Who is listed as the owner of the winword.exe you have been trying to run?

……

Based on the answer above why can't the application run, and how would you enable the application to execute, assuming it was safe to do so?

……

……

Ask the instructor to explain the answer to any of the questions if needed!

End of Exercise

Exercise 4: Intermediate Troubleshooting- Archiving

Scenario

One of the first line support team have also logged onto the machine in reception using a non-administrative account and confirmed that Word is present on the endpoint and that it is being blocked by Application manager, they report that the message states that they are “not authorized to execute WINWORD.EXE”. However the Support engineer states that they could run Excel and Outlook without any problem at all. Having gone through a series of basic troubleshooting steps you have and excluded simple configuration errors and are now looking to carry out further in depth investigation.

You’ve decided to check that Enterprise auditing is enabled on deployment group concerned for Prohibited execution requests for AM.

Aware that you may be dealing with a security issue you have also decided to enable archiving on the endpoint so you can capture any unauthorized applications and then take them for examination in your Sandboxed environment.

Synopsis

At the end of this exercise you should be able to enable Enterprise auditing of Prohibited execution requests and enable Archiving of applications on Endpoints.

Prerequisites

- **FBN-DC01**, **FBN-SRV01**, **FBN-PC01**.
- Ensure that **FBN-DC01** is started first
- Accounts used:
  - **FBN\administrator** P/W= **Pa55word**
  - **FBN\HR1** P\W= **Pa55word**

Objectives

At the end of this exercise, you will be able to:

- Perform a basic health checking on the AMC and the endpoints.

Time Estimate

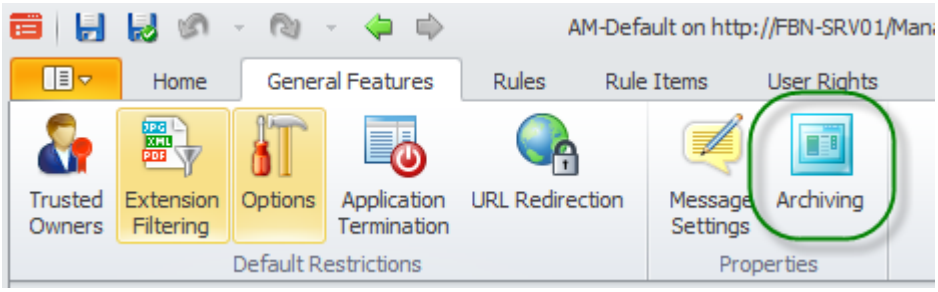
30 minutes

Enable enterprise auditing of Prohibited execution requests for Application Manager on an endpoint.

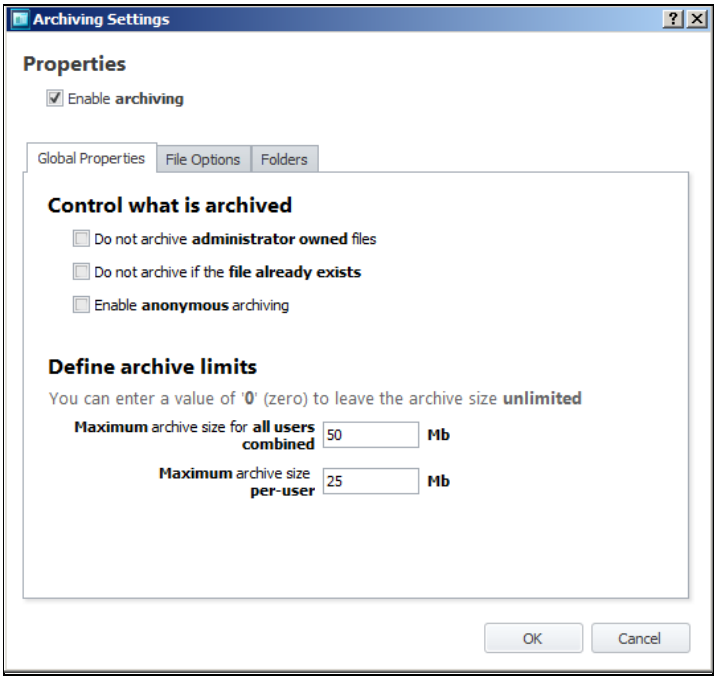
This should have already been done in the lab for **Module 4 Exercise 2**. If you are unsure refer to this lab and check that **9000 events** are being audited for the **FBNTest Deployment Group** !

Enable Archiving of applications on an endpoint.

1. Log on to **FBN-SRV01** as **FBN\Administrator** launch the Application Manager console and load the **AM-Default** config from the Management Centre.
2. Select the **General Features** tab and Click on the **Archiving** button.



3. Select **Enable archiving** and click **OK**.



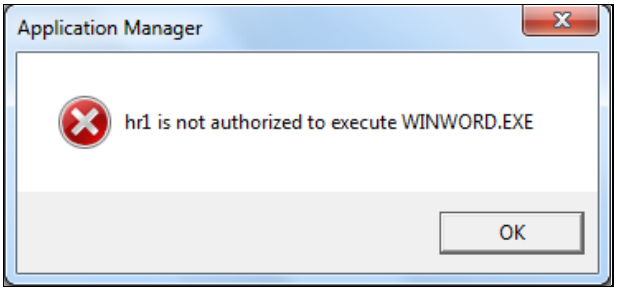
4. **Save and unlock** the updated **AM-Default** configuration to the **Management Server.** When prompted in the **Reason field** select **Other** and in the **Additional info** field enter **Module 8 Ex 3**. **Enabled Archiving**.
5. Select **OK**
6. Ensure the configuration has deployed to the endpoints.
7. Remain logged on as **FBN\Administrator**

Capturing the prohibited application on the endpoint.

You will now archive the application on the endpoint.

1. Log on to **FBN-PC01** as **FBN\HR1**.
2. Navigate to **C:\Postinstall\Lab\Module 8** and run the **Winword** executable.

   The application will fail with the following Application Manager dialog box

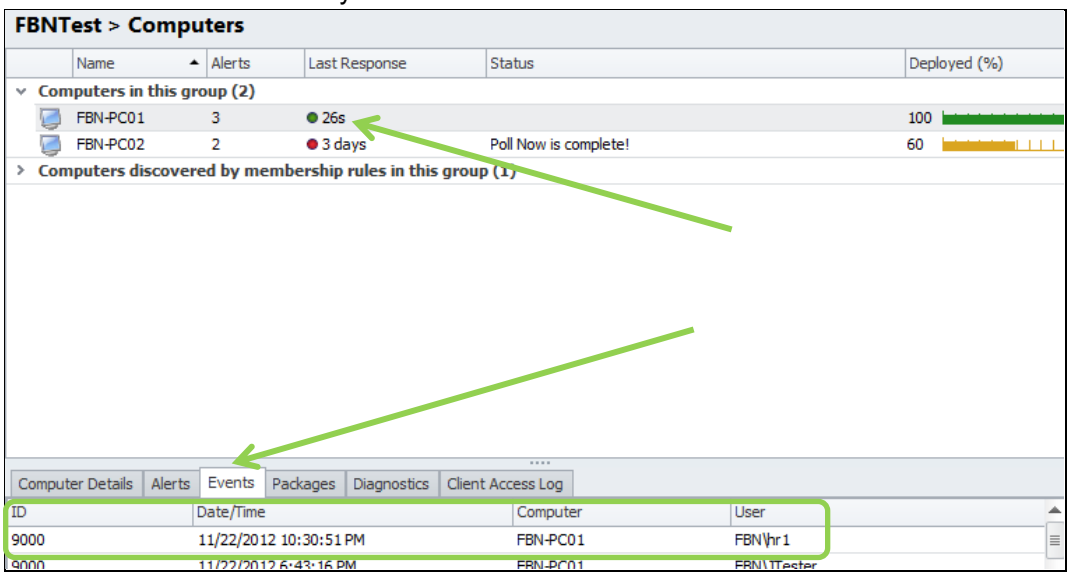


3. Log off **FBN-PC01**.

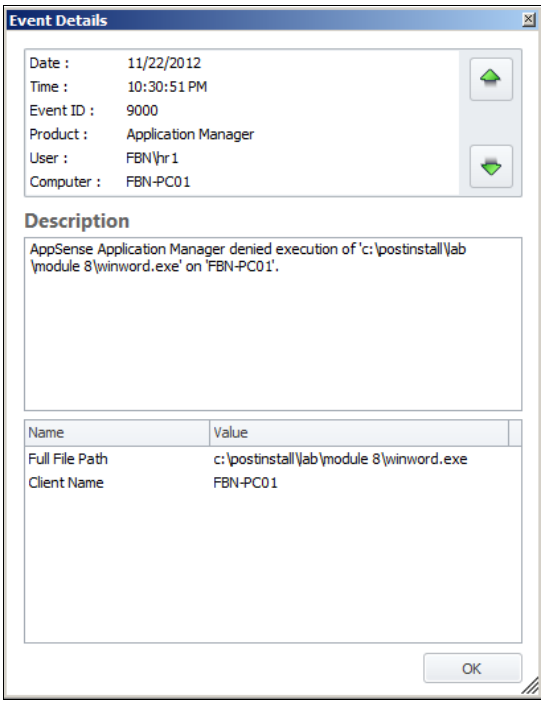
Checking the Events.

1. Switch back to FBN-SRV01 and log into the Management Centre (if it is not already open).
2. Select the **Deployment Groups** node on the left hand side and then navigate to **Deployment Groups >FBNTest >Computers**.
3. Select **FBN-PC01** from the top of the work area, then select the **Events tab** from the bottom half.

   There should be a 9000 entry for FBN-PC01 with a User of FBN\HR1



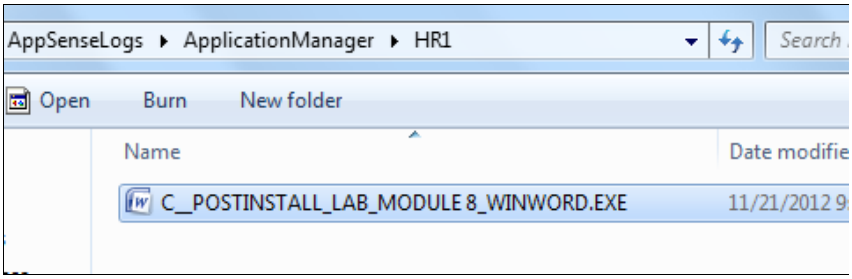
4. **Double click** the **9000** event listed for **FBN-PC01**
5. Review the **Event Details**



Retrieve the archived file from the Endpoint

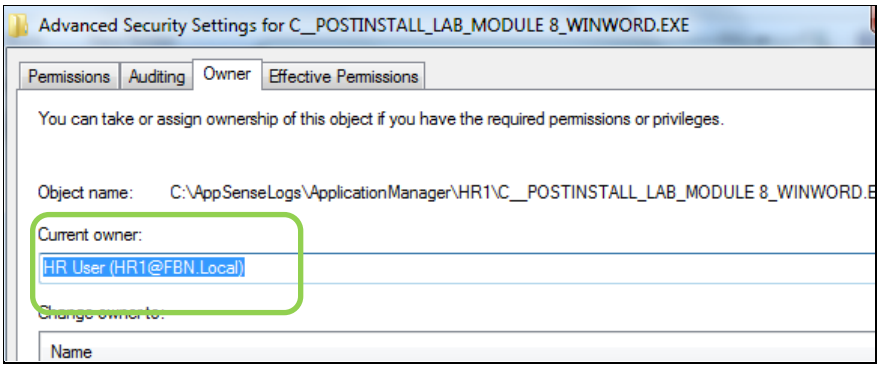
1. Switch back to **FBN-PC01** and log on as **FBN\Administrator**.
2. Browse to **C:\AppSenseLogs\ApplicationManager\HR1**.

   A copy of Winword.exe should have been saved as C__POSTINSTALL_LAB_MODULE 8_WINWORD.



   When an application is Archived in this way, it will be saved using the users context that attempted to run it.
3. **Right click** the application and select **Properties**.
4. Select the **Security tab** and click the **Advanced** button.
5. Select the **Owner** tab.

   The current owner should be listed as HR User 1



6. Select the **Details** tab.

Do the application properties look legitimate? Record the size of the file and version number below.

When you run the application, what happens? did the application run in a way that you expected?

……

……

Warning

At no point would you attempt to run this application whilst logged on as a member of the Builtin\ Administrators in a real life scenario as AM is disabled for this group and any previously blocked applications would be allowed to run.

The application would need to be placed in a sandboxed environment before progressing with further analysis. At the very least in this instance the Public PC should be removed from the network until a clarification is obtained as to the legitimacy of any application captured.

End of Exercise

Exercise 5: Intermediate Troubleshooting- Trusted Vendors

Scenario

The Word.exe located on the Public machine turned out to be a virus disguised as a legitimate Winword.exe.

You would like to ensure that in future software from legitimate sources will be allowed to be installed and run, however you do not want to enable trusted ownership for Domain admins or any other group to allow for this. You've decide to look at the Trusted Vendor option as a possible way to deal with the problem.

Synopsis

At the end of this lab you will be able to enable Trusted Vendors rules to allow software from legitimate 3rd party software vendors to be installed and run.

Prerequisites

FBN-DC01, **FBN-SRV01**, **FBN-PC01**.

Ensure that **FBN-DC01** is started first

Accounts used:

- **FBN\administrator** P/W= **Pa55word**
- **FBN\HR1** P\W= **Pa55word**

Objectives

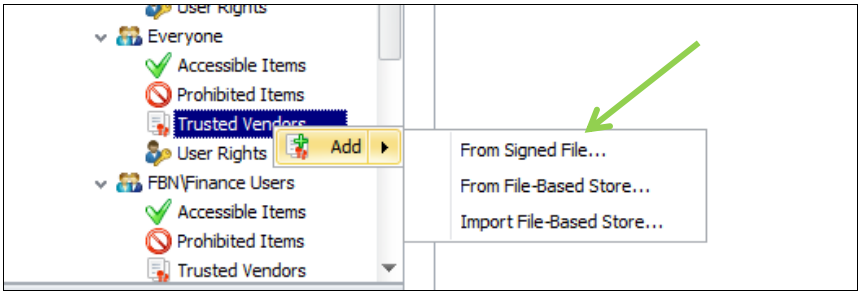
At the end of this exercise, you will be able to enable trusted vendors to allow signed software to execute in your environment.

Time Estimate

20 minutes

Create a trusted vendor rule.

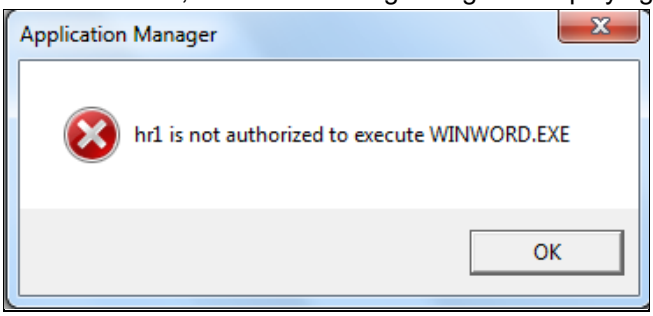
1. Log onto FBN-SRV01 as FBN\Administrator and load the AM-Default configuration from the Management Center into the Application Manager console.
2. From within the **Configuration Node** on the left hand side expand **Rules >Group > Everyone**.
3. Right Click the **Trusted Vendors** node and Select **Add > From a Signed File**



4. From within the **Select Signed File** dialog box browse to **C:\Postinstall\Lab\Module 8\Winword Actual** and select **Winword.exe**.
5. **Save and unlock** the configuration back to the **Management Centre**. When prompted in the **Reason** field select **Changed Group Rule** and in the **Additional Info** field enter **Module 8 Ex 5 Trusted Vendor**.
6. Check to ensure the configuration is deployed to the endpoints.
7. Swap over to **FBN-PC01** and Log on as **FBN\HR1**.
8. Browse to **C:\Postinstall\Lab\Module 8\Winword Actual** and double click **Winword.exe**.

   Word will launch, however it is missing all the files required to run properly.
9. Use **Task Manager** to end the hanging Word application.
10. Browse to **C:\Postinstall\Lab\Module 8** and run the fake instance of **Winword.exe**.

    This should fail, with the following dialog box displaying.



Check the ownership on both rules, who is listed as the Owner of both copies of Winword?

……

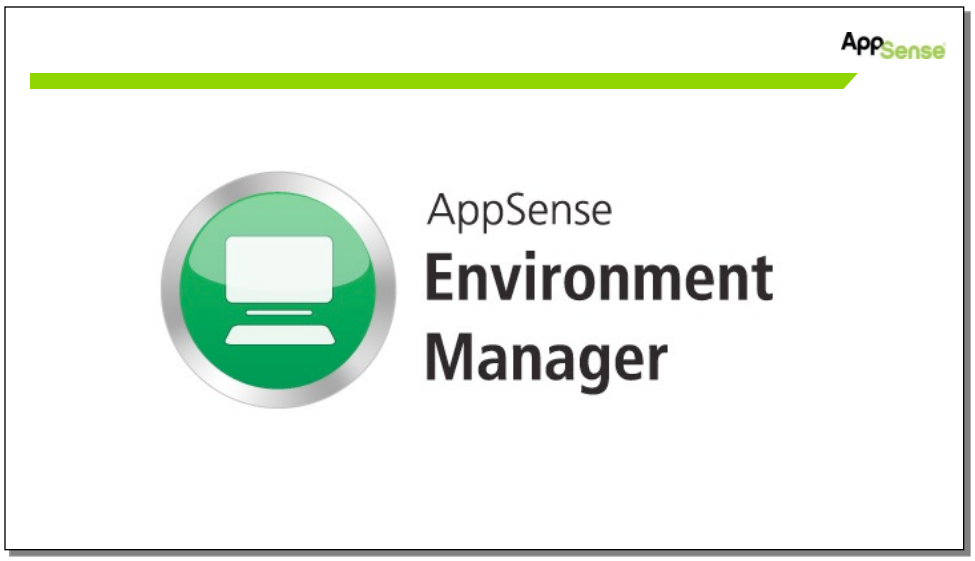
……

What advantages and disadvantages does use of Tusted Vendor certificates in this instance provide?

……

……

End of Exercise



Environment Manager – (M8)

Exercise 1: Personalization Analysis

Scenario

A user has filed a helpdesk ticket complaining that she cannot get the settings for one of her applications set the way she wants them to be. She is also complaining that the settings for another application have become corrupted. Using Personalization Analysis, you edit the registry values to set her desired settings in the first application and then use rollback to reset the second application's settings back to their last known good state.

Synopsis

In this exercise, you will use Personalization Analysis to view user's personalization usage, edit their settings and perform a restore.

Objectives

At the end of this exercise, you will be able to:

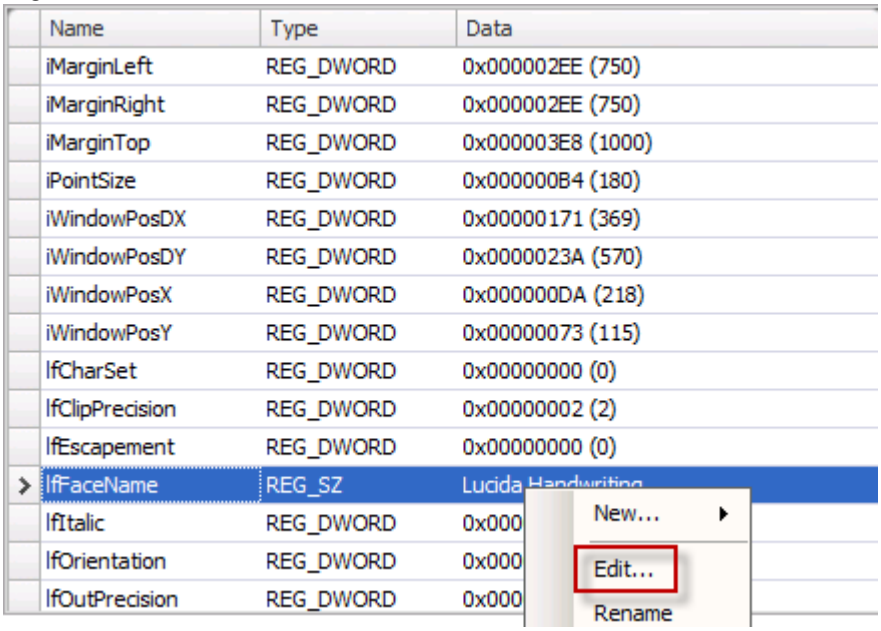
- Use Personalization Analysis to view a user's personalization usage
- Edit a user's settings for a specific application
- Rollback a user's settings

Time Estimate

30 minutes

Perform Personalization Analysis for HR1

1. Log into FBN-SRV01 as the domain administrator and launch the EM Console
2. Select Personalization from the left hand navigation and connect to the personalization server
3. Expand Personalization Groups and select HR
4. With HR selected, click on the Tools tab and select Personalization Analysis
5. Select Report By User and click Display
6. Select the yellow bar for FBN\HR1
7. You should now see the personalization usage split out by application.
8. Right-click the yellow bar for Notepad and select Edit application registry
9. Click OK
10. Select User > the SID > Software > Microsoft > Notepad.
11. Right-click ifFaceName and select Edit



12. Enter Arial as the Value data and click OK
13. Click OK to close the Edit Registry Settings Window
14. Close the Personalization Analysis window

Test the Registry Edit

Log into FBN-PC02 as HR1. Launch Notepad

Is the font set to Arial?

Create an Archive

1. You should already have the EM Console open and connected to the personalization server, but if not, launch the console, select Personalization and connect to the personalization server.
2. Expand Personalization Groups, select HR and select Personalization Analysis from the Tools tab
3. Select the "…" to specify the HR1 user
4. Type "HR" in the search field and click search
   Select FBN\HR1 and click OK
5. Select the Archives tab and click Display
6. Right-click Microsoft Excel and select Archive Microsoft Excel now
7. Click Yes
8. Click OK
9. You should now see an archive with the current date and time listed below Microsoft Excel
10. Leave this window open

Change the settings for Microsoft Excel

1. Log into FBN-PC02 as HR1
2. Launch Microsoft Excel
3. Take note of the color, size and position of the Excel window. Also take note of the Dictionary language setting
4. Change all of those settings
5. Close Excel, but stay logged in to FBN-PC02

Rollback the personalization settings for Microsoft Excel

1. Switch back to FBN-SRV01
2. Right-click the archive for Microsoft Excel created earlier and select Roll back to this archive
3. Click Yes
4. Click OK
5. Switch back to FBN-PC02. You should still be logged in as HR1.
6. Launch Microsoft Excel
7. Were all of the settings you changed restored?

End of Exercise

Exercise 2: EM Browser Interface and Self Service Portal

Scenario

You need your helpdesk personnel to be able to perform many of the tasks available in Personalization Analysis, but you do not want to give them access to the EM Console as that will also give them access to your personalization server settings. Instead, you install and configure the EM Browser Interface to allow your helpdesk task to perform their job without exposing them to your server.

You then enable the Self Service Portal to allow select end users perform their own maintenance tasks.

Synopsis

In this exercise, you will use Personalization Analysis to view user's personalization usage, edit their settings and perform a restore.

Objectives

At the end of this exercise, you will be able to:

- Use Personalization Analysis to view a user's personalization usage
- Edit a user's settings for a specific application
- Rollback a user's settings
- Enable the Self Service Portal for users

Time Estimate

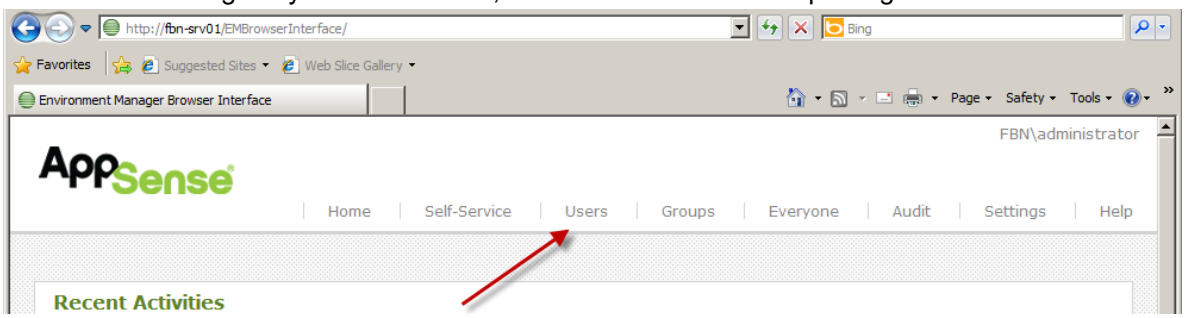
30 minutes

Install the EMBroswer Interface

1. Log into FBN-SRV01 as the administrator.
2. Navigate to C:\PostInstall\AppSense\Software\Products and double-click EMBrowserInterface64 to start the install
3. Follow the prompts through, accepting the defaults until the EM Browser Interface Configuration launches
4. Click Next
5. On the Prerequisites screen, click Next
6. On the Web Site screen, accept the default value of Default Website and click Next
7. On the Client Authentication screen, accept the default of Use Windows authentication and click Next
8. On the Configuration Credentials screen, enter the following:
    - Authentication Type - Impersonate Windows Authentication
    - User Name - FBN\sql-creator
    - Password - Pa55word
    - Server Name - FBN-SRV01
    - Database Name – PersonalizationServer
9. Click **Next**
10. On the Database Service Credentials screen, enter the following:
    - Authentication Type - Impersonate Windows Authentication
    - User Name - FBN\sql-acct
    - Password - Pa55word
11. Click **Next**
12. On the Summary screen, click Accept.
13. Click Finish when it completes
14. Click Finish on the installation GUI

Use the EMBrowser Interface to manage a user's personalization settings

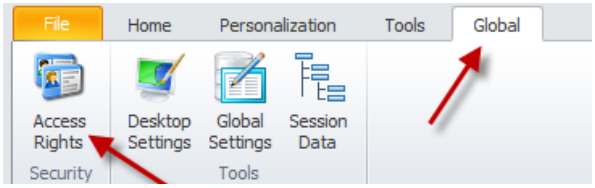
1. Launch Internet Explorer
2. Go to http://fbn-srv01/EMBrowserInterface
3. To view and manage any individual users, click on Users from the top navigation menu



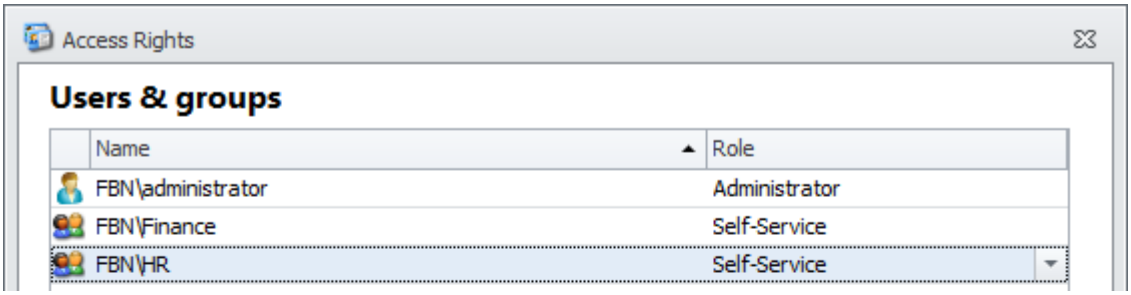
4. You should now see a list of users with personalization data on the server
5. Click on HR1
6. This will give you a list of their applications Desktop Settings, Session Data and Certificates
7. Click on _Notepad
8. This brings up the available archives for the application. From here, you may choose to rollback, delete or protect the archive. You may also manually take an archive and delete the current data.
9. Close the window
10. Click on Groups from the top navigation menu
11. This will give you the list of personalization groups
12. Click on HR
13. From the Whitelist Applications tab, click on _Notepad
14. Note that from here, you can perform a rollback for every user in the group. You may also take an archive, delete archives and delete current data for all users in the group.
15. Close the window
16. Click on Everyone from the top navigation menu
17. From here, you may perform rollbacks and manage archives and data for all users.

Enable access to the Self Service Portal for Finance and HR users

1. From FBN-SRV01, as the administrator, launch the EM Console
2. Connect to the Personalization Server
3. Click on the Global tab and select Access Rights



4. Click Add and add in the Finance group
5. Click Add and add in the HR group
6. Set the Role for both groups to Self-Service



7. Click Close
8. Log on to FBN-PC01 as Finance1
9. Launch Firefox
10. Go to http://fbn-srv01/EMBrowserInterface
11. When prompted for username and password, enter in Finance1 and Pa55word
12. On the Welcome screen, scroll down to the bottom and click Next
13. This brings you to the “My Applications” screen
14. You should see a list of your most used applications, application groups and usage counts. You may click the All tab to see all of your applications
15. Select the Microsoft Office 2010 Group and click Next (you may have to scroll down to see the Next button)
16. From here, you may restore to a backup, protect a backup, delete a backup, create a backup and reset (delete) all settings for the application group.
17. Click the Create Backup button
18. Select Create the backup when you next logoff or close Microsoft Office 2010 Group and click Create Backup
19. Click OK
20. Scroll to the bottom of the screen and click Summary
21. The summary screen will list the tasks you completed during the session.
22. Close Firefox

End of Exercise

Exercise 3: EM Debug Logging

Synopsis

In this exercise, you will use Personalization Analysis to view user's personalization usage, edit their settings and perform a restore.

Objectives

At the end of this exercise, you will be able to:

- Use Personalization Analysis to view a user's personalization usage
- Edit a user's settings for a specific application
- Rollback a user's settings
- Enable the Self Service Portal for users

Time Estimate

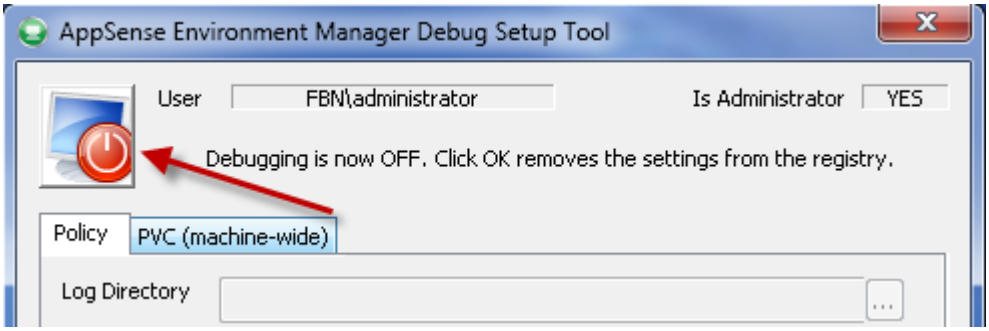
30 minutes

Install EMTools

1. Log into FBN-PC01 as the domain administrator
2. Go to \\FBN-SRV01\appsense\Software\Products
3. Double click EnvironmentManagerTools64
4. Follow the prompts to install the tools

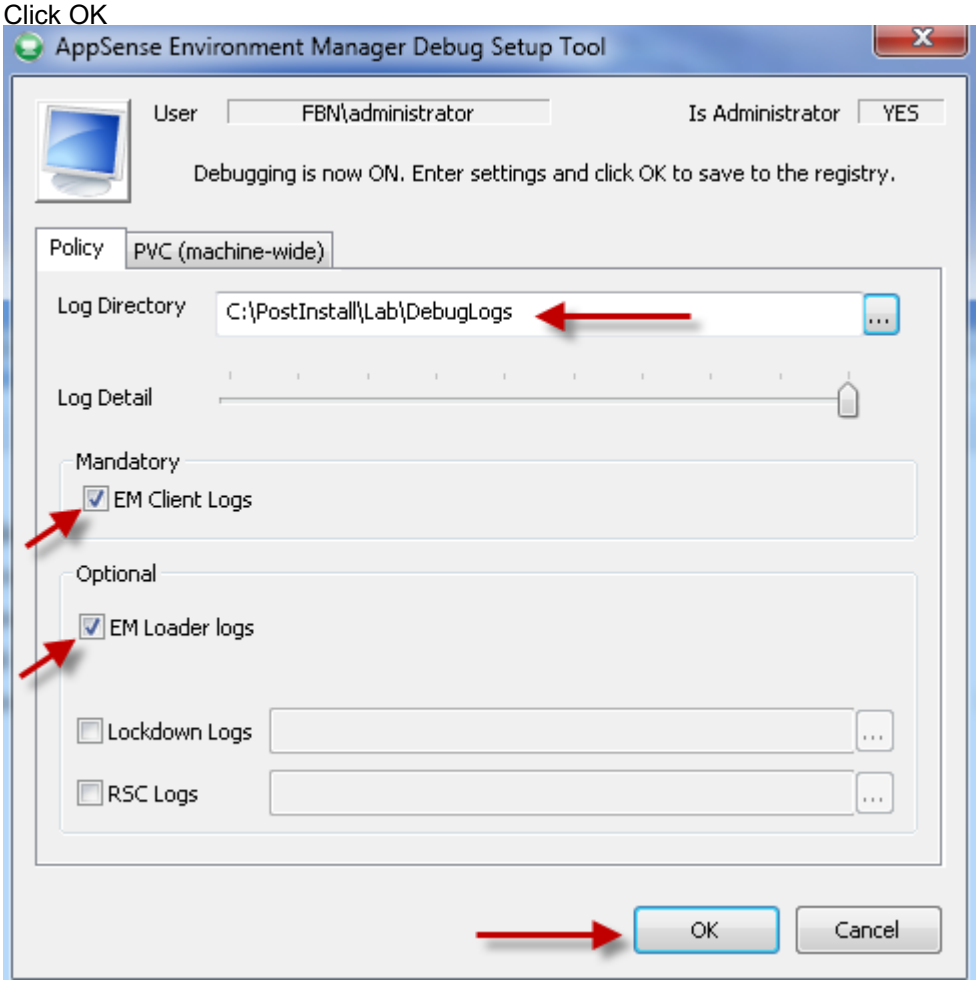
Enable debugging and gather some logs

1. Launch the EM Debug Setup Tool
   Start > All Programs > AppSense > Environment Manager > Tools > EM Client Debug Setup
2. Click the start/on button to enable debugging.

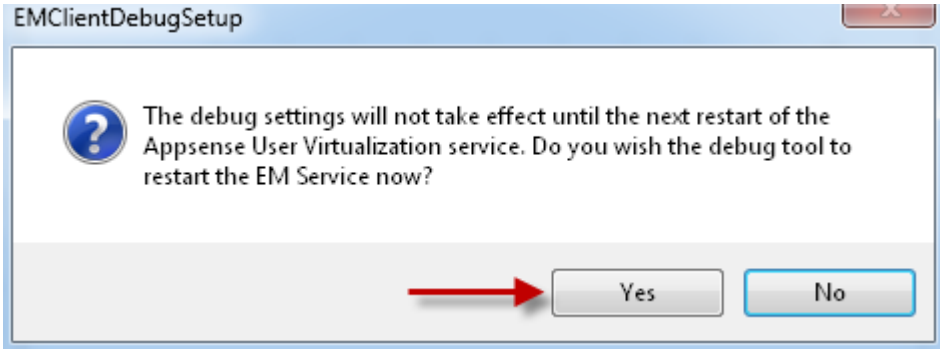


3. Set the following:
   - Log Directory - C:\PostInstall\Lab\DebugLogs
   - Mandatory - EM Client Logs selected
   - Optional - EM Loader Logs selected

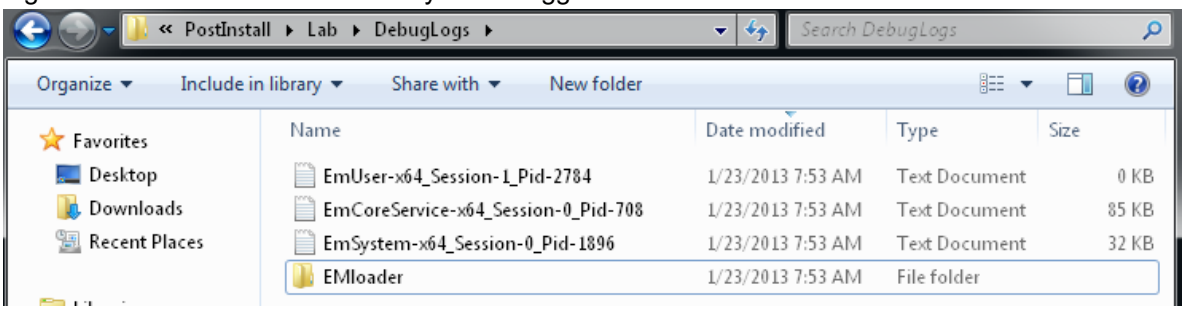
4. Click OK



5. Click Yes



6. Open C:\PostInstall\Lab\DebugLogs. Note that some files have already been created. These are log files for the current session that you are logged in as administrator.

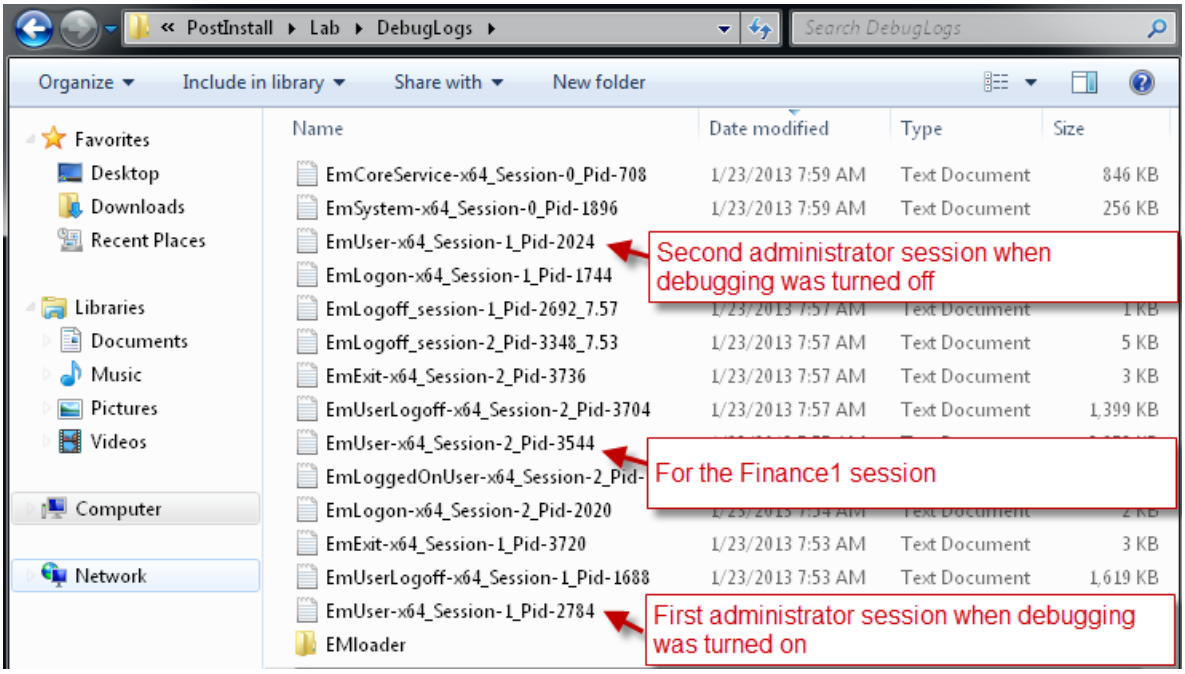


7. Log off of FBN-PC01 and log back on as FBN\Finance1
8. Once logged on, launch Notepad.
9. Wait about one minute and then close notepad.
10. Log off of FBN-PC01 and log back on as FBN\Administrator
11. Launch the EM Client Debut Setup tool and turn it off.

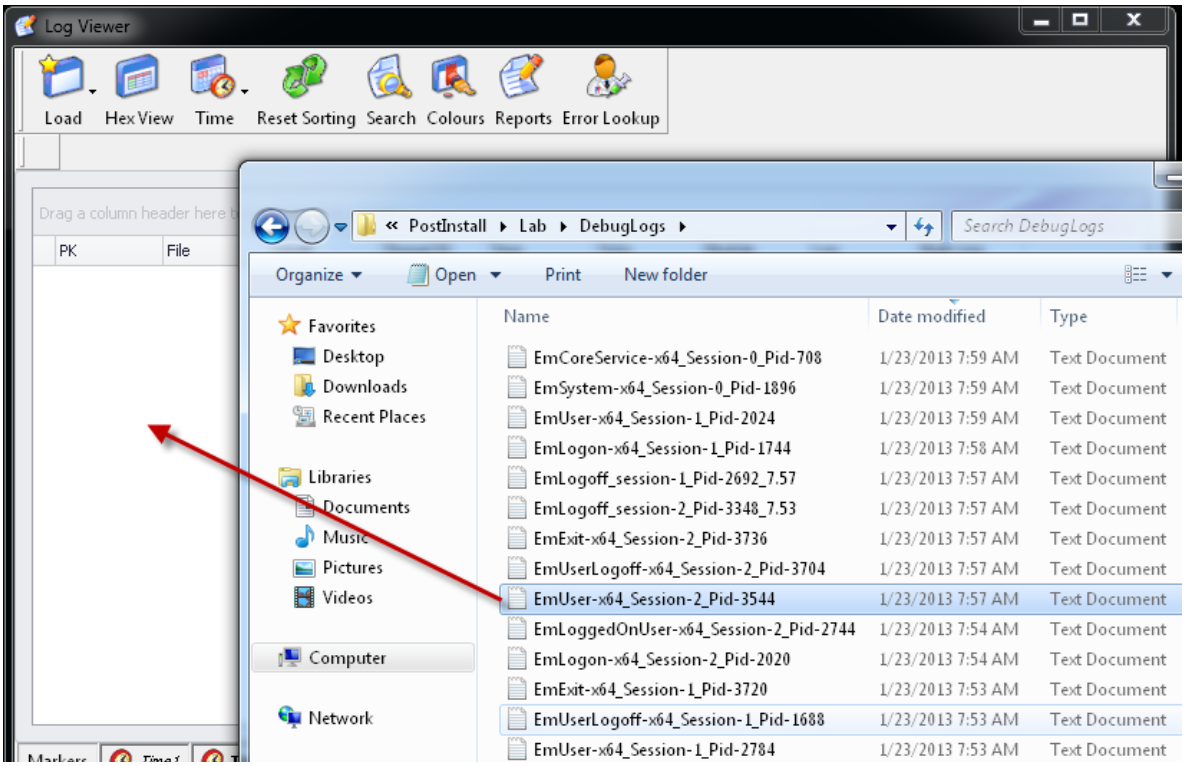
12. Click OK and then click Yes.
13. Click Yes one more time to restart the EM service.

View log files

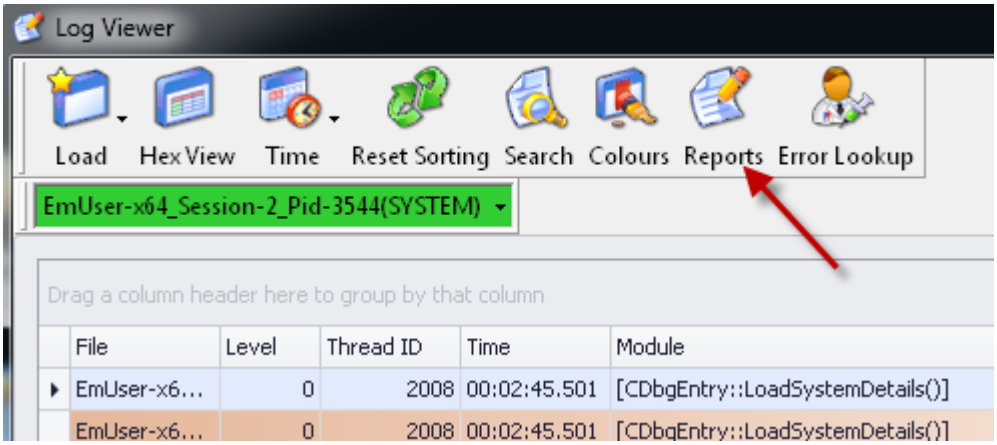
1. Click Start > All Programs > Environment Manager > Tools > EM Log Viewer
2. Open C:\PostInstall\Lab\DebugLogs and sort by Date Modified. Notice that more files have been added. Remember, the first EMUser-x64_Session was for the Administrator's session when you turned debug logging on. The second EMUser-x64_Session is for the session you logged in as Finance1. The third EMUser-x64 is for the current session when you logged in as the administrator and turned debugging off.



3. Drag the second EMUser-x64_Session (for Finance1) into the white workspace area of the log viewer

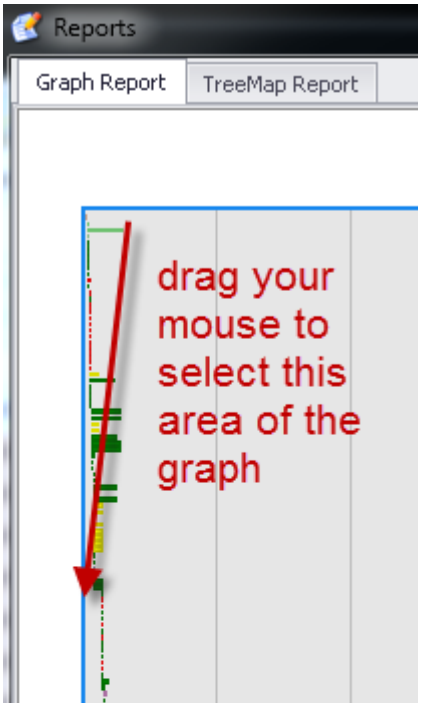


4. Once the log loads, click on Reports

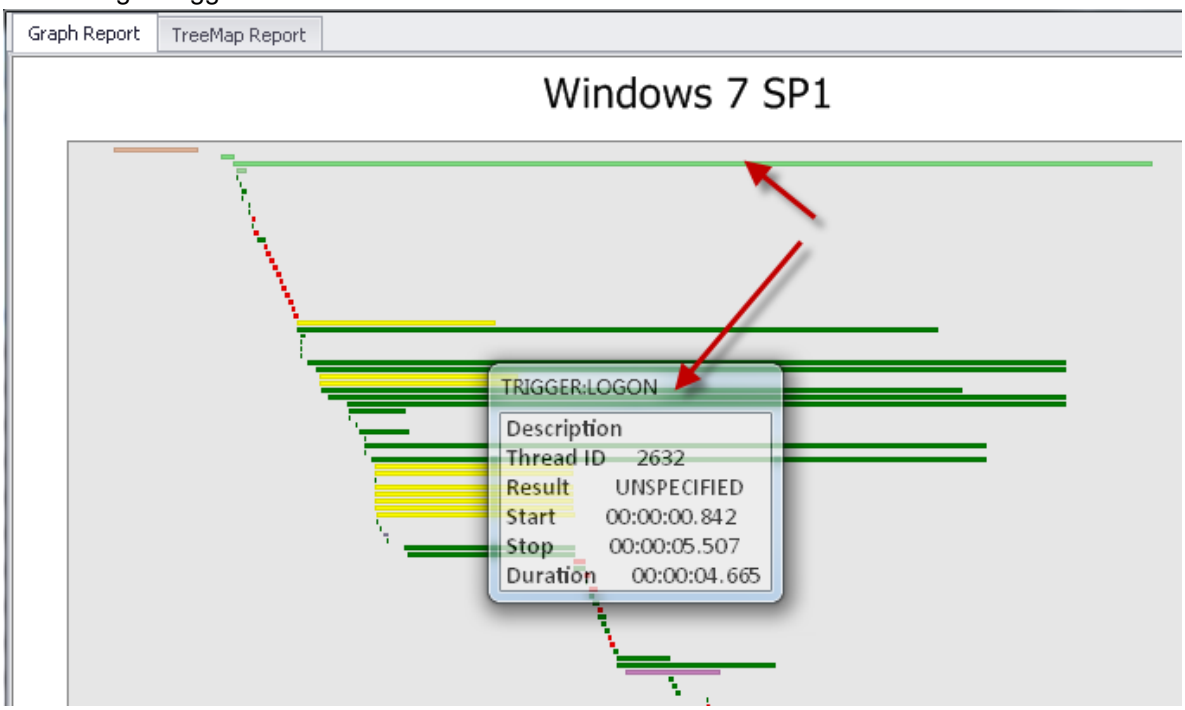


5. Click OK on the Orphans Found screen

6. This displays a graphic timeline of events. The grouping of items to the left of the graph is your logon. To zoom in on the top left area, click and drag your mouse from just right of the green bar at the top to the left edge of the graph and about half way down



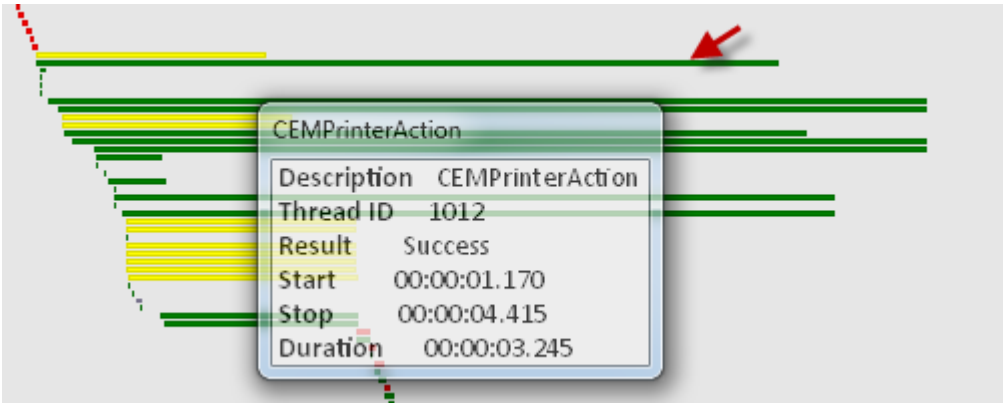
7. Hold your cursor over the top green bar to get information about it. This represents the time it took for the Logon trigger to run.



Note

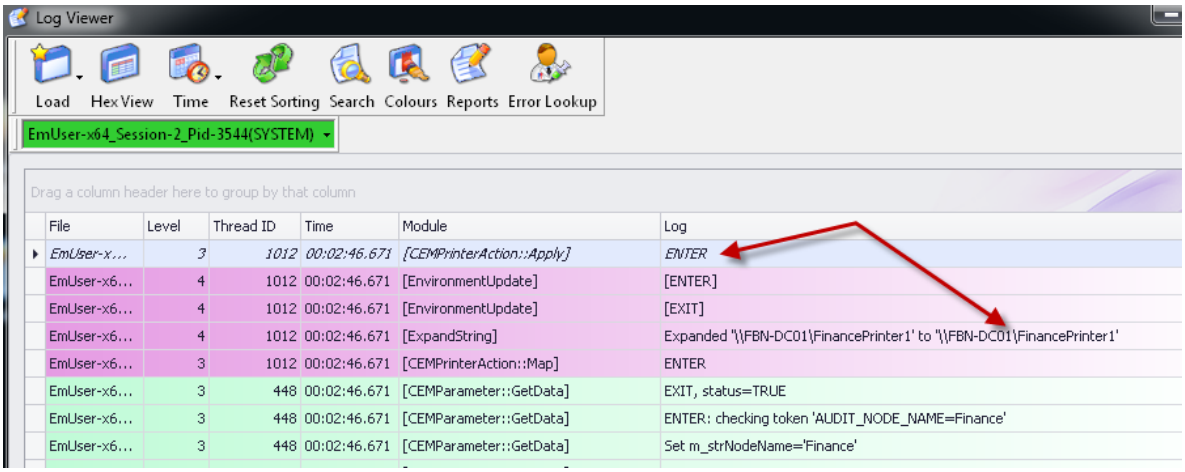
If the popup/information window appears in an annoying spot, you may drag it out of the way.

8. Highlight some of the other lines to see what they are.
9. Some of the information in the reports you see on your system will vary from what you see here in the book, so please just use these steps as a guideline when you explore around.
10. Move your cursor over one of the green bars. In this example, it represents a successful printer action with a thread ID of 1012.



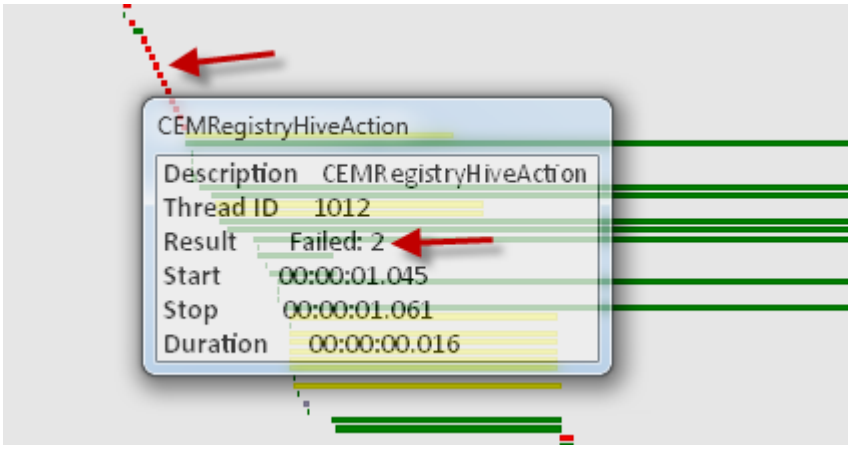
11. To actually see this in the log file, right-click the bar and select Zoom to Start

12. This will take you to the start of this action in the log file. In this example, it is for mapping FinancePrinter1.



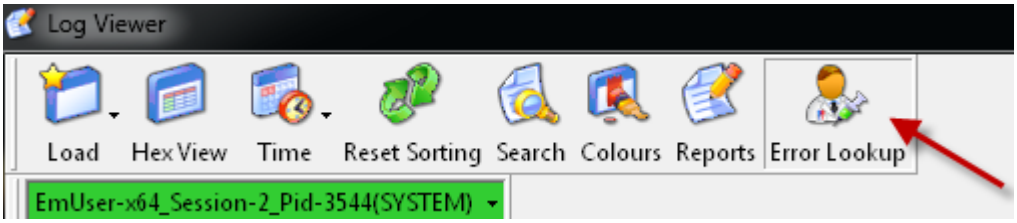
View an error

1. From the log viewer, click on Reports and then click OK on the Orphans found screen.
2. Zoom back in on your top left area
3. Hold your cursor over one of the red items. In this example, it is a registry hive action that has failed with an error code of 2.

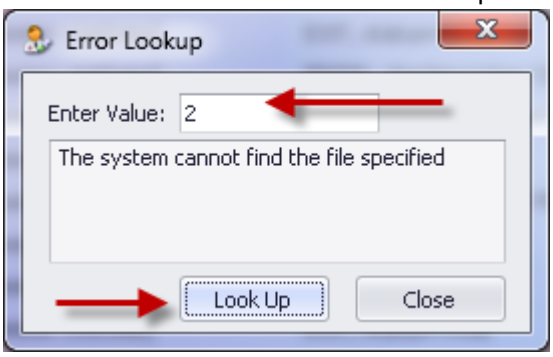


4. Right click the red item and select Zoom to Start
5. This takes you to the start of the action in the log file. In this example, if you were to scroll down you will see the specific file it was trying to copy and the error and exit code. Note here that the error and exit status code is 2. For reference, an exit status = 0 means success.

6. To find out what the error code means, select Error Lookup



7. Enter in the error value and click Look Up



8. In this example, you would have looked up error code 2 and found that it means the system cannot find the file specified.

   In this case, the reason the file could not be found is because it was never hived out. This is most likely because the setting was not applied on the registry, probably because the user never set that option in Windows, and therefore, it was never hived out. Sometimes, as in this instance, the errors can be benign.

End of Exercise