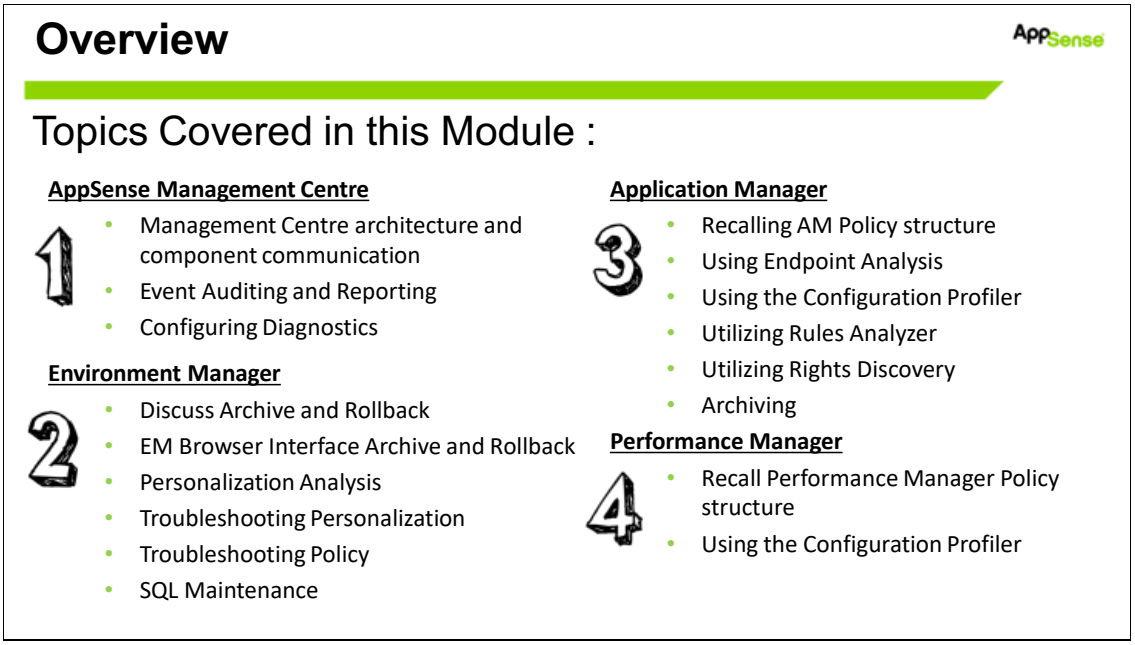
Module 8 Maintenance and Troubleshooting



Overview

In this module we will look at the tools we have available within the DesktopNow suite that can be utilized to help with monitoring and troubleshooting. Some of these will have been covered in part in previous modules and you will be expected to recall some of that information in order to aide you with the labs.

Objectives

At the end of this module you will be able to:

Management Centre

- Recall the Management Center architecture and component communication.
- Utilize alerts, event auditing and reporting for monitoring and troubleshooting.
- Utilize and configure Diagnostics.

Environment Manager

- Discuss and configure the functionality of Archiving and Rollback.
- Discuss and configure the EM Browser interface for Archive and Rollback.
- Configure Personalization Analysis.
- Utilize basic troubleshooting techniques for Personalization.
- Utilize basic troubleshooting techniques for Policy.

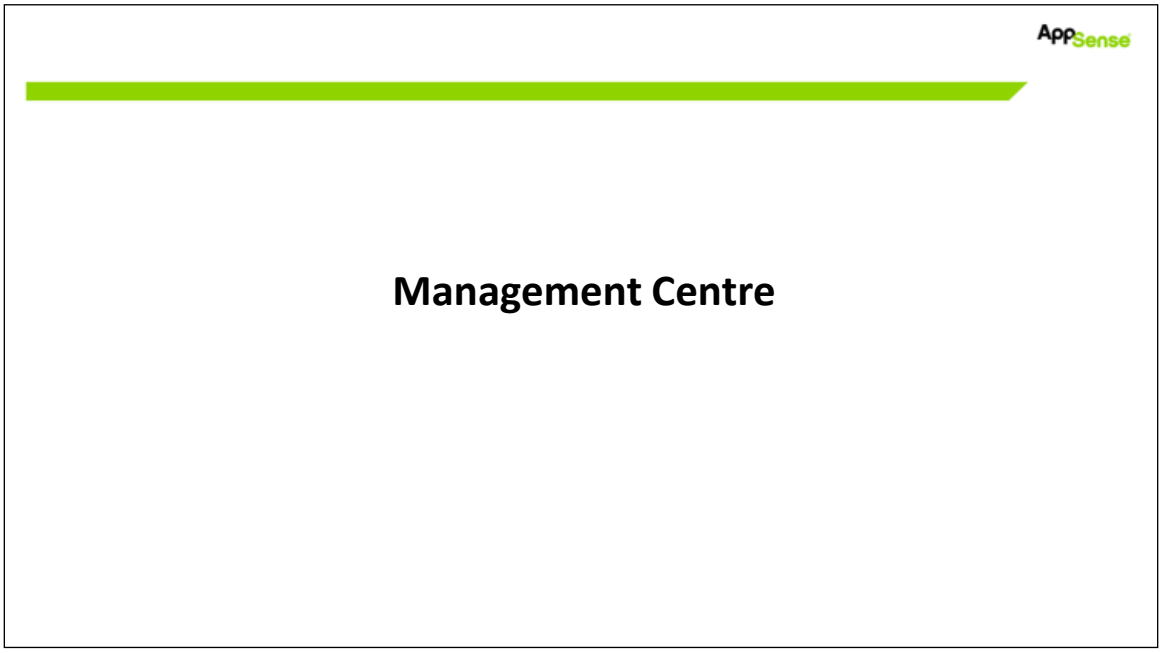
Application Manager

- Understand the basic troubleshooting techniques for AM
- Recall the structure of AM Policy.

- Utilize basic tools for troubleshooting

Performance Manager

- Understand basic troubleshooting techniques for PM.
- Recall the structure of PM Policy.
- Utilize the Configuration Profiler to validate a deployed configuration.



Notes:

CCA – Role

- Based on content covered earlier in the course describe the role and function of the CCA ?
- What are the default poll periods and where are they configured?

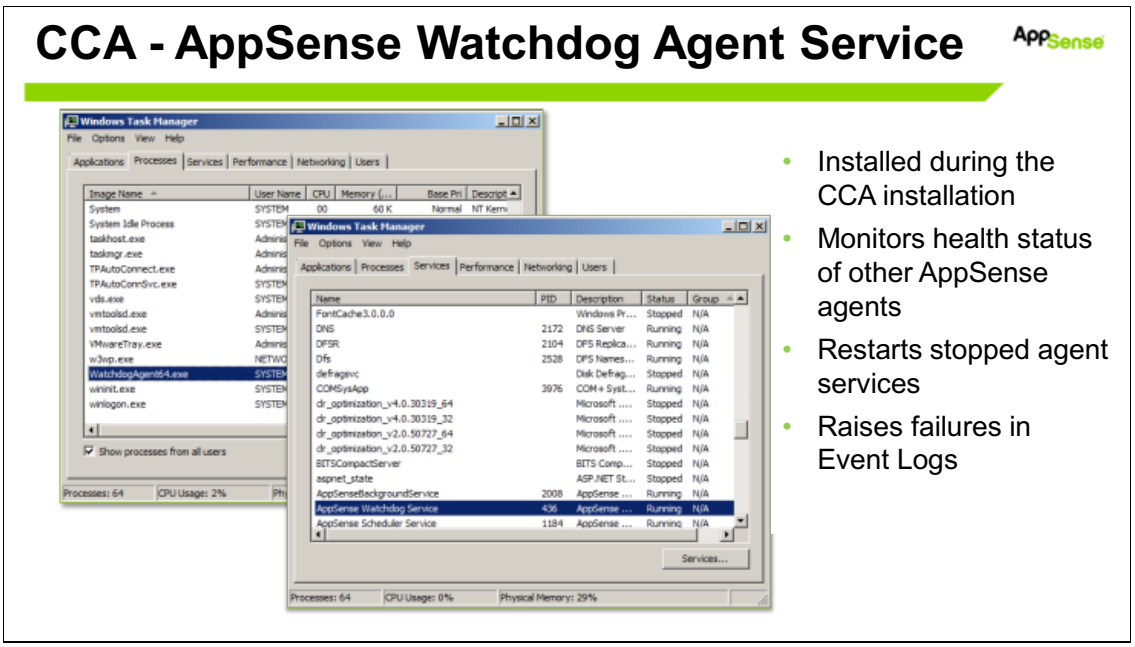
CCA – Role

Describe the role and function of the CCA?

A)

What are the default Poll periods and where are they configured

A)



CCA – AppSense Watchdog Agent Service

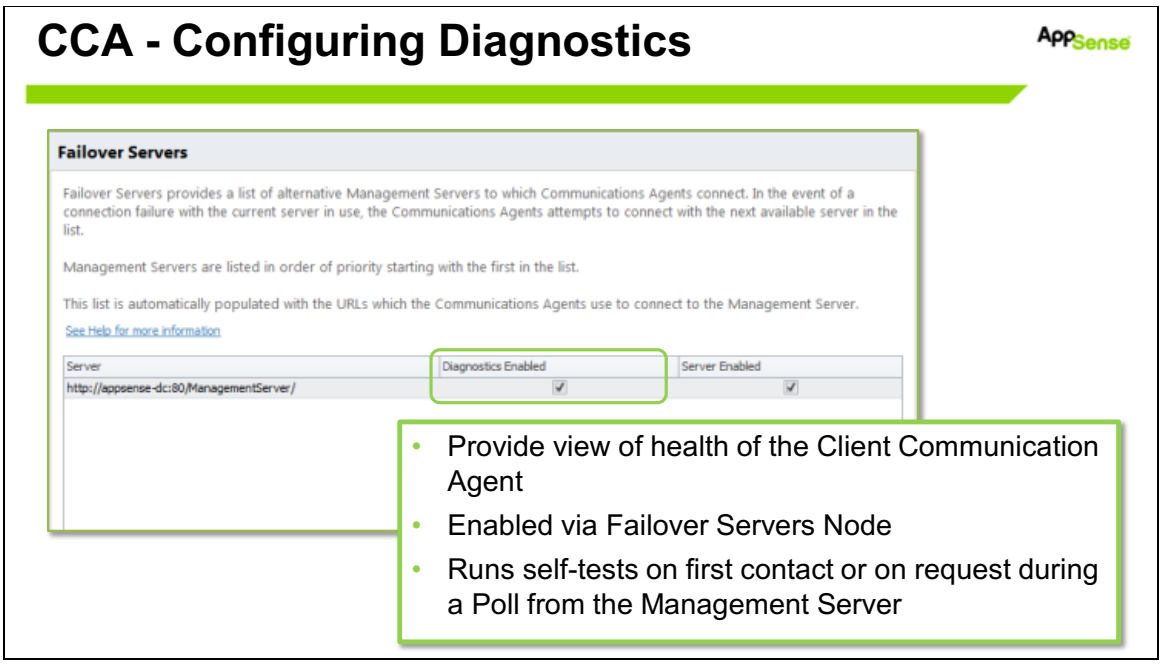
During the installation of the Client Communications Agent on the Client, an additional service is also installed – the AppSense Watchdog Agent Service. This service regularly checks the health status of any of the installed AppSense Agents on an Endpoint. Should the Watchdog Agent detect an Agent stopped via ungraceful means, then it will automatically restart the Agent and an event is raised to the Application Event logs in order to alert the Administrator that this service has been restarted. The Watchdog will not restart the agents if they have been closed correctly e.g. via services, MS, sc stop or net stop.

If the CCA has encountered any stability errors, an event raised from the Watchdog Agent is a good starting point for troubleshooting as these errors may point to something outside AppSense, for example an error itself with the Windows Installer service.

In the event that problems arise with the Watchdog service, it is possible to enable Diagnostic logging for the Watchdog service from within the agent itself. The steps for this are covered in TN-150787 available through:

https://www.myappsense.com/Knowledgebase/TN-150787.aspx

The Watchdog service would be required to be restarted in order for the changes to take effect. Please not that once the required information has been obtained the registry key configured in the above Tech-Note should be removed.



CCA Configuring Diagnostics

CCA Diagnostics allows an administrator to view the overall health of the Client Communication Agent in terms of its ability to communicate with the Management Server.

Diagnostics are enabled at a global level from within the Management Centre console via **Deployment Groups > Overview> Failover Servers**. This setting can be overridden on a deployment group by deployment group basis as needed via the deployment groups **Failover Servers** node. Diagnostics are disabled by default.

Enabling Diagnostics for the CCA on endpoints enables a series of automated self-tests to be carried out. These occur at:

- First contact with the Management server, typically on restart
- On request from the Management server during a poll

Additionally, a manual diagnostics test can be carried out by selecting the **Request Diagnostics** option from the **Actions** pane available from the **Computers** view of the specified deployment group.

Once a diagnostic request has been triggered, an event which indicates the test result, is raised in the Windows Event Log on the managed endpoint device and sent to the Management Server.

Each test provides a success or failure result and, where a test fails, a detailed error report is included in the event report.

In the event of a test failure the Management Console highlights, in **red**, the names of the computers where the failure occurred and also highlights the deployment groups in the navigation pane containing computers on which the tests failed

There are four specific tests that are run when diagnostics are requested:

- **Connectivity**: The connectivity test involves the CCA attempting to poll the Management Server. Any response, other than an HTTP 200 (Success) return value, indicates a failure and a detailed error message is returned. If this test fails, the results cannot be sent to the Management Server (as there is no connectivity) but can be viewed in the local Application Windows Event Log on the endpoint device.
- **Download of Packages**: This test downloads a sample file from the Management Server to the local hard disk of the endpoint device, using the Background Intelligent Transfer Service (BITS). Instead of downloading a full MSI package, the CCA downloads a small XML file which can be easily validated and has a minimal impact on network bandwidth. The XML file is downloaded from the same directory as standard MSI packages to ensure the same access rights affect both file types. Once the test is complete, the downloaded file is deleted.
- Since BITS downloads can be delayed if the local computer is under heavy load, the download occurs within a new high priority BITS job, ensuring the test completes in a shorter time. A single BITS job is used to download files from all enabled failover URLs. If any errors are reported during the download, the test fails. A description of the error is included in the test results.
- **High Priority Events**: The high priority events diagnostics test allows critical events to be sent to the Management Server database from the managed endpoint device. A typical high priority event is the reporting of a failure to install packages. The test attempts a call by the CCA from the managed endpoint to the Management Server with an empty list of events. Any error values returned by the call are added to the results.
- **Upload of Events**: The diagnostics test attempts to upload an events file using BITS from the local hard disk on the endpoint device to the Management Server. The events file is empty so as to help minimize impact on network bandwidth, and is uploaded to the same directory on the Management Server as standard event uploads.

  %\Program Files%\AppSense\Management Center\Server\Web Site\Deployment\Events

  Since BITS uploads can be delayed if the local computer is under heavy load, the upload occurs within a new high priority BITS job ensuring the test completes in a shorter time. If any errors are reported during the upload, the test fails. The description of the error is included in the test results.

This test only verifies that events can be sent from the CCA on the managed endpoint device to the Management Server. **No checks** are made to ensure that the events can be uploaded to the database. When this fails, an event is added to the Management Server event log and raises a Management Center event, where possible

The **Computers** view within a specific Deployment Group provides a **Diagnostic State** which indicates the current state of the diagnostics taking place on the endpoint device. There are four diagnostics states indicated:

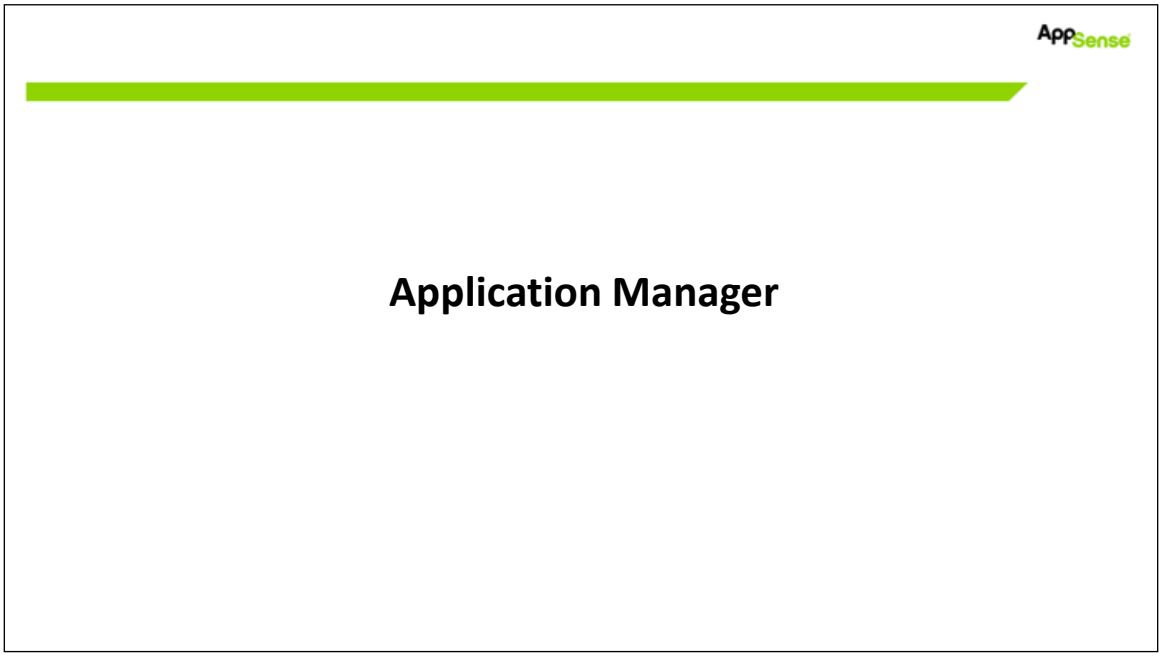
- Untested
- Pending
- Requested

- Completed

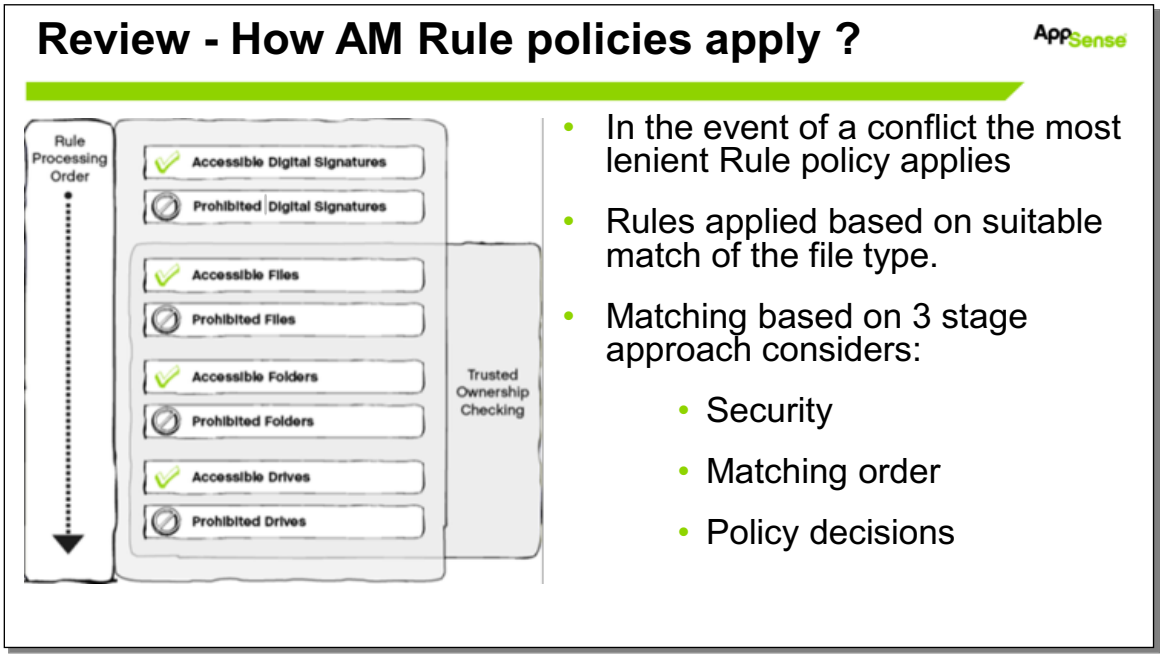
The diagnostics test results are reported to the Management Server and displayed in the Diagnostics tab in the Management Panel area of the Computers view within the relevant deployment group, including a breakdown of the test type and the result of each test.

Exercises

- Configure and test diagnostics



Notes:



Review – How AM Rule policies apply

If we use an example to high light the above:

A user is a member of two groups, Sales Managers and Sales. Sales have been prohibited from accessing the %SystemDrive%\postinstall folder on their computers. However the Sales Managers are required to run a single application from within the directory called Sales4.exe.

How could the above be achieved?

A)

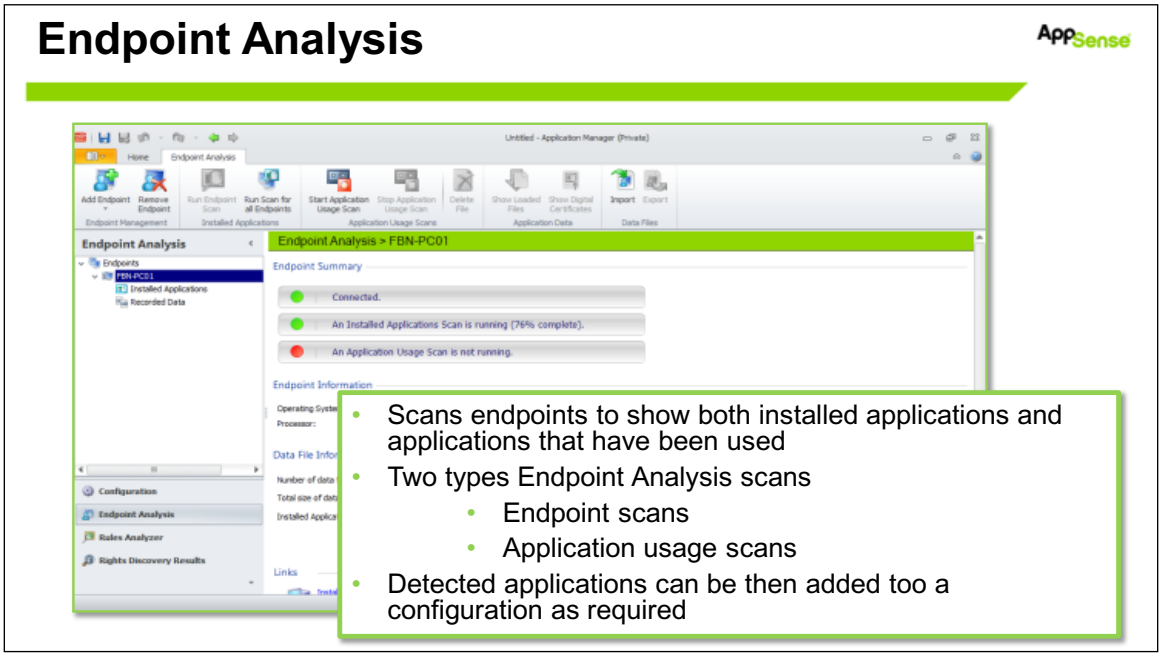
A Manager belong to the HR group. The HR group has access to %SystemDrive%\Apps\HR during office hours Monday to Friday. The manager requires access to the drive outside of office hours up until 9.00pm weekdays. List the different ways in which this could be achieved?

A)

Continuing on using the example from question 2. A new application has been purchased and located in the \Apps\HR folder. This application should only ever be used by the Manager and 3 other line managers from the HR department. How could this be achieved?

A)

Instructor:



Endpoint Analysis

Endpoint Analysis (EPA) allows you to scan single or multiple endpoints, to provide a list of applications that are present, or are present and that have run on a particular computer. You can use Endpoint Analysis helps to simplify the creation of an appropriate Application Manager Configuration. In order for endpoint analysis to function correctly certain prerequisites need to be met, these are:

- Application Manager agent installed on the endpoint.
- License installed on the endpoint.
- Application Manager configuration installed on the endpoint.
- Administrative share rights to the endpoint.
- Remote registry access to the endpoint.

On remote computers running Microsoft Vista and above, File Sharing and Remote Registry Service are disabled by default and must be enabled.

Turn on File Sharing in Start > Control Panel >Network and Sharing Center.

Start the Remote Registry Service in Start> Control Panel > Administrative Tools> Services

End Point Analysis Scans

There are two types of Endpoint Analysis scans. These are:

- Endpoint Scan
- Application Usage Scan

Endpoint Analysis files for a given endpoint are stored on the computer that has the Application Manager console installed under the following locations:

- For Windows XP and Server 2003, C:\Documents and Settings\All Users\Application Data\AppSense\Application Manager\Endpoint Analysis.
- For Vista and above, C:\ProgramData\AppSense\Application Manager\Endpoint Analysis.

Endpoint Scan

The Endpoint Scan searches the endpoint for any applications that are present. These can be any official or unofficially installed applications.

The scan reads the following locations:

- HKLM\SOFTWARE\Microsoft\Windows\Current\CurrentVersion\Installer\Folders
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
- Program Files

Endpoint Scans can take several minutes, due to Application Manger not only scanning the Program Files folder and the registry keys, but also each dependent file and digital signature. Application Manager records all this information.

During an Endpoint Scan, 100% of the CPU on the endpoint can be used. However, if user tasks need to be performed, the Application Manager agent utilizes built-in smart scheduling technology to allow tasks to take precedence over the scan itself, thus not affecting the end-user perception of performance.

Application Usage Scans

The Application Usage Scan is used to detect all applications in use on an endpoint.

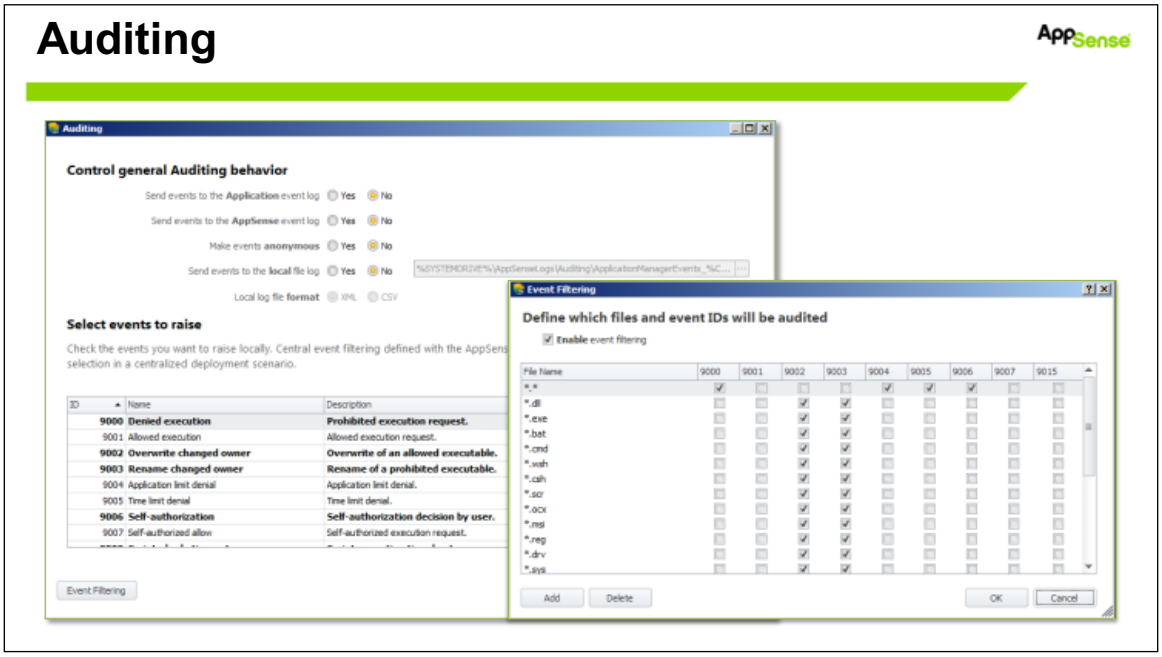
When an Application Usage Scan is in progress, all execute requests are passed through for Endpoint Analysis processing once the standard Application Manager rules checking has been performed on that request. The details of requests are held in memory. When the scan has stopped all the request data is saved to file.

If the endpoint is rebooted while a scan is in progress, for example, if a user takes their laptop from the workplace and switches it on at home, the Endpoint Analysis runtime detects that it should be recording application usage and restarts the recording. This is done on agent startup.

Order of Scans

Typically, the Endpoint Scan is run first to determine which applications are installed on the endpoint. This can be followed by the Application Usage Scan to track the applications that have been run on an endpoint over a period of time.

Through highlighting which applications are being used and which are not, unlicensed software can be identified and restricted and unlicensed software can be removed.

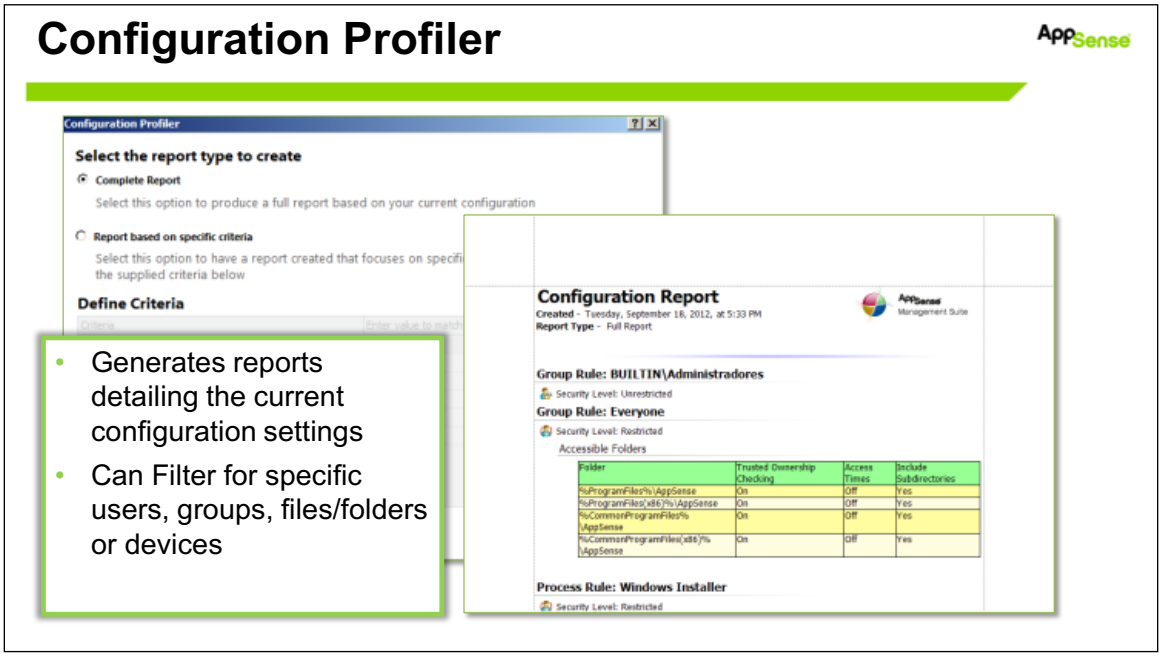


Auditing

As covered previously Application Manager has a comprehensive list of in built reporting and auditing features. These provide a significant aid in the troubleshooting process.

Application Manager auditing can be placed in an Audit Only mode to silently monitor security restrictions or can generate events when users attempt to access denied locations and are blocked. Auditing events are available from the Auditing dialog.

In Enterprise installations, events can be forwarded to the AppSense Management Center via the Client Communications Agent (CCA). When using this method for auditing, event data storage and filtering is configured through the Management Center console.

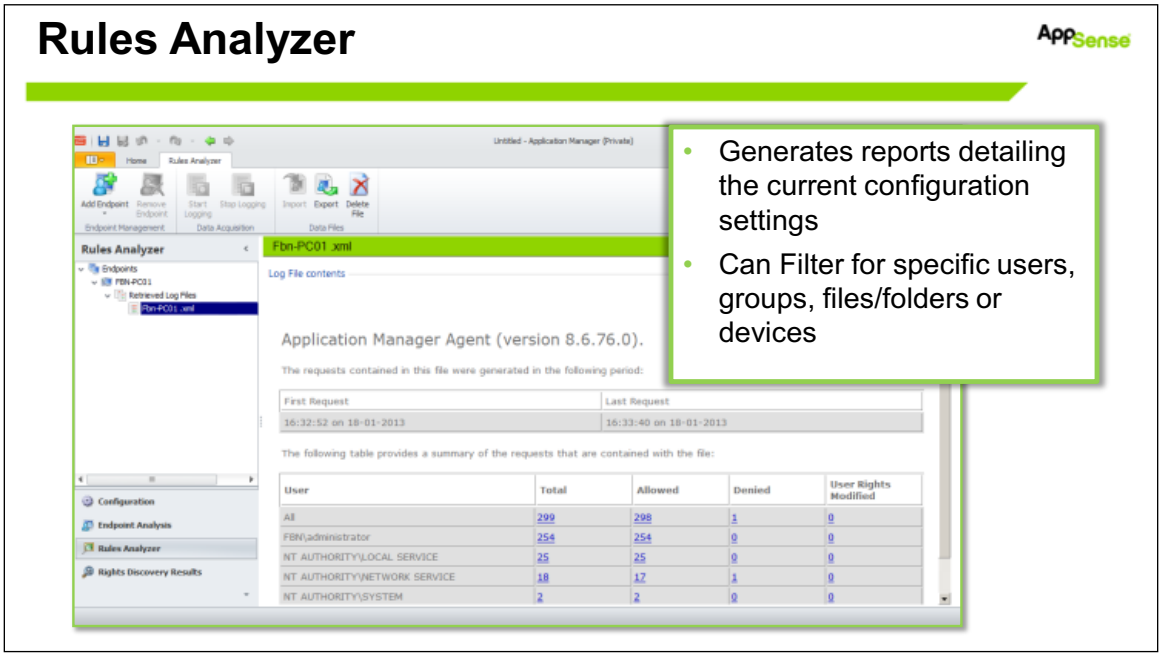


Configuration Profiler

A configuration profiler is available for Application Manager, Performance Manager and Environment Manager.

It allows us to run reports that can give a complete breakdown of the currently loaded configuration from within each of the respective consoles, alternatively it can be used to report on a selective section of the configuration, such as Rules that may have been applied to a specific group.

It can be used as part of an organization's change management procedures, in order to record configuration changes that may have been applied to currently active configurations. Alternatively it can also be used as a troubleshooting aid, allowing administrators to view a cross section or all of the configuration settings within a configuration as required.



Rules Analyzer

Standard AppSense auditing can be used to track unauthorized application usage or to track when users are overwriting \ renaming applications. It is a simple mechanism to use and can function without interaction. The standard auditing mechanism advises you when an application has not been allowed to execute however it does not indicate why this happened. Therefore an additional tool is required, one that allows analysis in real time and that indicates why an application is or is not allowed to execute.

Rules Analyzer provides a graphical interface that can be used to manually troubleshoot and fine tune Application Manager Configurations in real time. The only requirement is that a network link is available to the target endpoint, thus allowing Rules Analyzer to connect to the agent software and start the logging process.

When the logging is complete Rules Analyzer can be used to automatically retrieve the file back to the computer where the analysis is occurring for investigation. All logging information is held in XML format and each execution request that the Application Manager agent processed is listed along with the details of what occurred during processing, including if the process was allowed to execute or not and the reason for the outcome.

The Console

The **Rules Analyzer** is accessed from the navigation pane within the **Application Manager Console** and is used to create, retrieve and examine the log files. An Endpoint node allows you to control logging on to a specific managed endpoint to retrieve the log files. Below each **Endpoint node** is a node for each **Retrieved Log Files** node.

You can review a summary page, view all requests, or view the requests for a specific user. You can restrict the view to the denied or allowed requests. Within the analysis panel you can navigate to a specific request and view the full details of that request, including which rules were applied by Application Manager.

In order to use Rules Analyzer, you must be logged on with an account that allows read\ write access to the registry of any managed endpoint for which you wish to generate logs, you also require read\ write access to the local registry of the computer on which the console operates.

Pre-Requisites

The following list indicates the prerequisites that need to be met in order to run Rules Analyzer successfully:

- Application Manager Agent installed on the endpoint.
- License installed on the endpoint.
- Application Manager Configuration installed on the endpoint.
- Administrative share rights to the endpoint.
- Remote registry access to the endpoint.

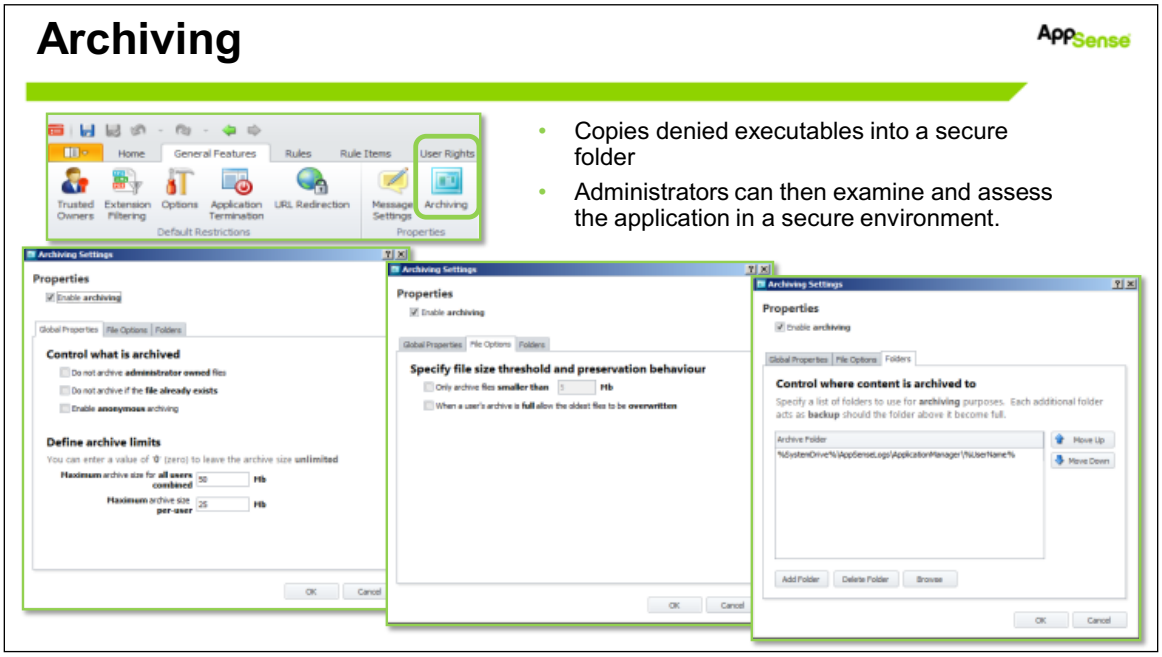
As with Endpoint Analysis on remote computers running Microsoft Vista and above, File Sharing and Remote Registry Service are disabled by default and must be enabled in order to allow access.

Turn on File Sharing in Start > Control Panel >Network and Sharing Center.

Start the Remote Registry Service in Start> Control Panel > Administrative Tools> Services

The Rules Analyzer console allows you to diagnose Application Manager problems by connecting directly to computers managed by Application Manager, and includes:

- **Creating Log Files** – You can create log files on managed endpoints.
- **Examining Log Files** – You can retrieve and examine log files to view the requests processed by Application Manager. In particular you can see which rules were applied to each request and whether the request was allowed or denied.



Archiving

Archiving allows you to copy any denied executables into a secure folder. When a user attempts to run an unauthorized executable, or an executable specified in the Prohibited Items list, Application Manager can take a copy of each application that attempted to execute and place them in a secured file system or archive. This information can be used by an administrator to inspect the kinds of executable content that Application Manager has blocked access to by taking a complete copy for the administrator.

It is often found that blocked applications are files with false names such as winword.exe. Unfortunately, the name alone does not tell the administrator a great deal as these are typically other executables that have been simply renamed in an attempt by the user to get the application to run on the computer. By having a specific copy of each executable, the administrator can accurately assess each application and what impact they would have on the enterprise had they been allowed to run.

Archiving is disabled by default it is enabled in the **Archiving** settings dialog available from the **General Features** ribbon.

When Archiving is selected there are 3 tabs available to configure these are:

Global Properties Tab

- **Do not archive administrator owned files**: When selected will not take an archive of applications owned (NTFS) by the administrator. An example of this is when a user tries to execute regedit.exe and is blocked by the Application Manager agent. It is unlikely you would require an archive of this file. However, it is useful to archive when the user attempts to execute their own copy of regedit.exe to determine what the application is and what effect it could have on the enterprise if it were to execute.

- **Do not archive if the file already exists**: Select to not take an archive of an unauthorized executable if a copy of the file already exist. The Application Manager agent does not try to copy it over again. This helps to save space, although it may result in inaccurate archiving as only one copy of an executable with the same name is ever retained.
- **Enable anonymous archiving**: Some locations have restriction laws in place, forbidding administrators to record which user attempted to execute unauthorized applications. Select this option to prevent the Application Manager agent from using any %username% file paths. The agent removes the percentage sign (%) leaving simply username. An example can be where an application is executed from a home directory that has the username as the folder name. Application Manager replaces the username with the text, username, so as to protect the user's identity in accordance with the local restriction laws.
- **Maximum archive size for all users combined**: The maximum size in Mb that Application Manager allows the archive to reach before it stops archiving for all users combined together.
- **Maximum archive size per-user**: The maximum size in Mb that a single user archive is allowed to reach before it stops archiving. For example, if an archive path is specified as C:\archive\%username% then every user on the computer would have a separate archive under the C:\archive directory. It is this user archive that is subject to the user limit.

File Options Tab

- **Only archive files smaller than**: This option allows you to specify the maximum file size to archive. By selecting this option and inserting a file size, you can ensure large executables are not copied to the archive. As an example, a user may well attempt to execute a service pack or other similarly large file which you typically would not want to copy over the network into an archive.
- **When a user's archive is full allow the oldest files to be overwritten**- Instead of simply stopping archiving when either the Total Limit or User Limit options are invoked, select this option to overwrite the oldest files. This is an easy way to ensure that the enterprise captures the most up to date information without utilizing huge data space for unauthorized applications.

Folders Tab:

The Folders tab is used to configure the location into which you want the archive files to go. The default location to place all archived files into is:

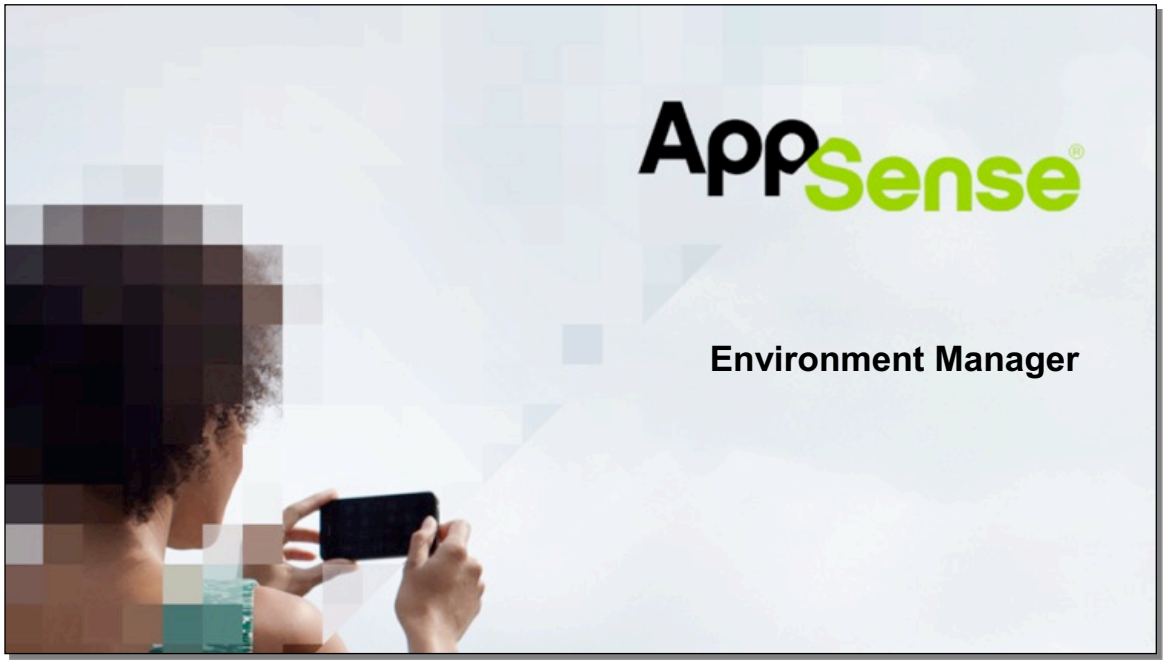
%SystemDrive%\AppSenseLogs\ApplicationManager\%UserName%

This has the effect of placing all archived files for a specific user in the same folder and the folder is named after the user making it easier to manage. Additional folders can be added to the list by using the **Add Folder** button. The location can be either typed in or browsed to on the local computer or local network by using the **Browse** button.

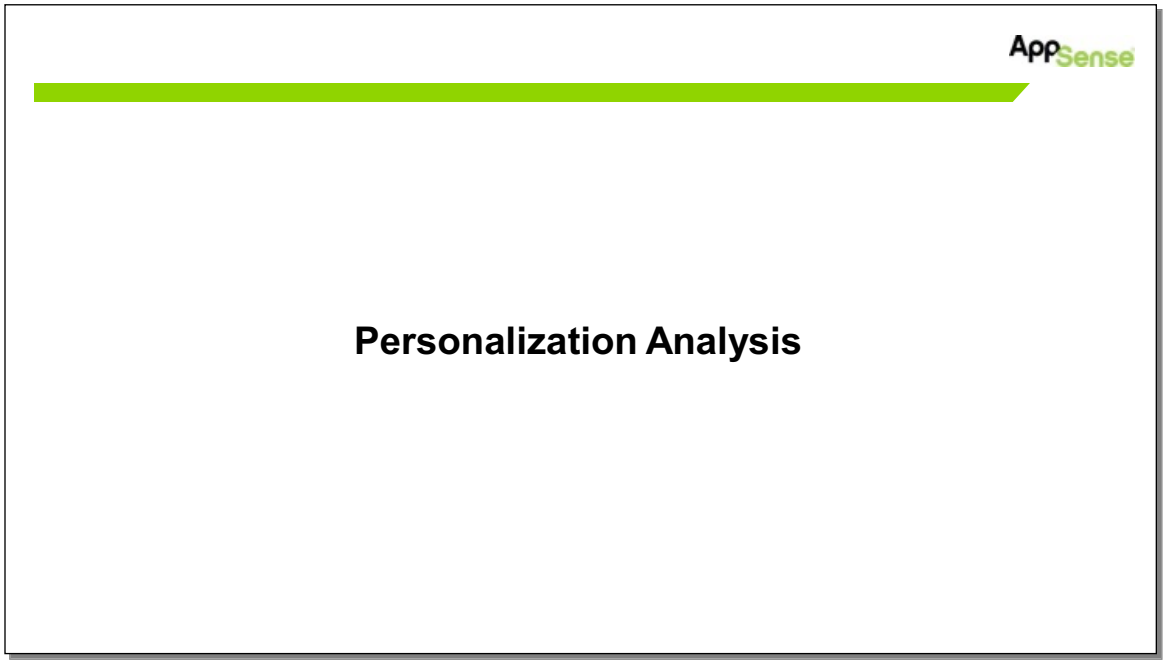
The order of the archive list is important as Application Manager attempts to copy the file to the first relevant archive in the list. If this copy fails then it attempts to copy the file to the second archive location, and so on. If the copy succeeds, Application Manager does not use any of the remaining archives. Use the Move Up and Move Down buttons to order any new folders ensuring you have the correct default folder at the top.

Exercises

- Basic troubleshooting – Application Manager
- Intermediate troubleshooting – Rules Analyzer
- Intermediate troubleshooting – Archiving
- Intermediate troubleshooting – Trusted Vendors



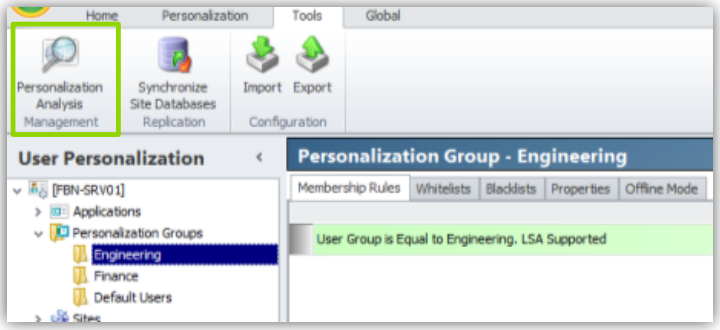
Environment Manager



Personalization Analysis

Personalization Analysis

- Graphical representation of the data collected on a per user and per application basis
- To enable:
  - Select the Personalization Group you wish to analyze
  - Select Personalization Analysis from the Tools menu

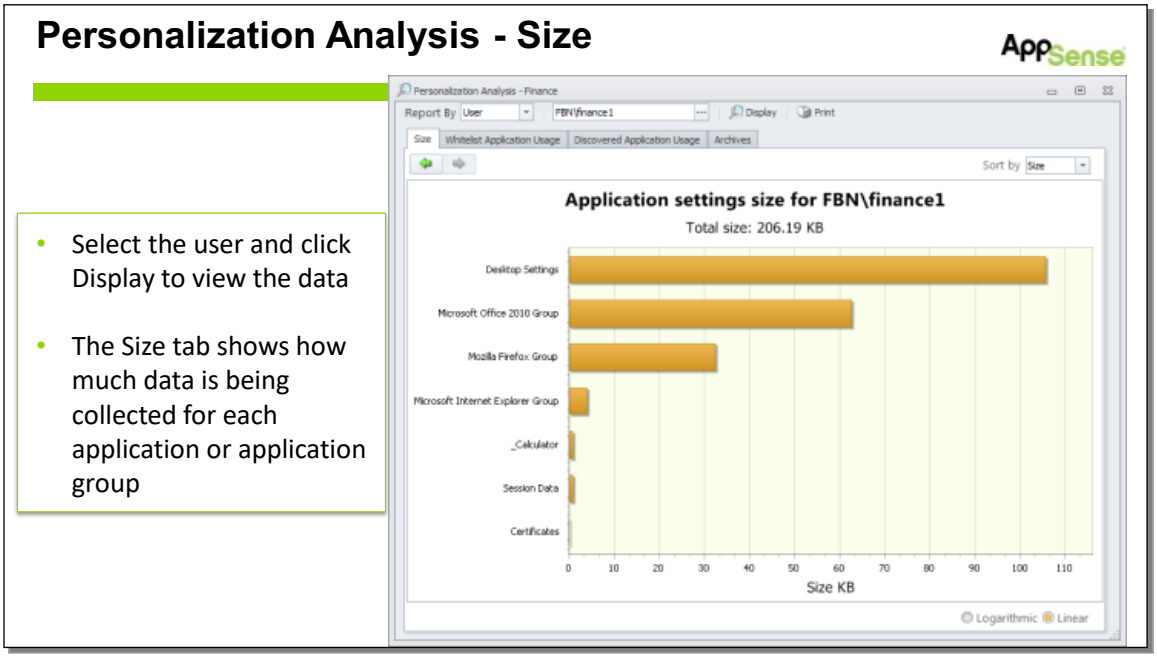


Personalization Analysis

Personalization Analysis displays reports showing data about current and historical personalization data for users, applications and application groups which is stored in the database. Graphical analysis can be produced for personalization data and the results sorted and displayed using various criteria such as date, application and user. This enables application usage and user activity to be monitored.

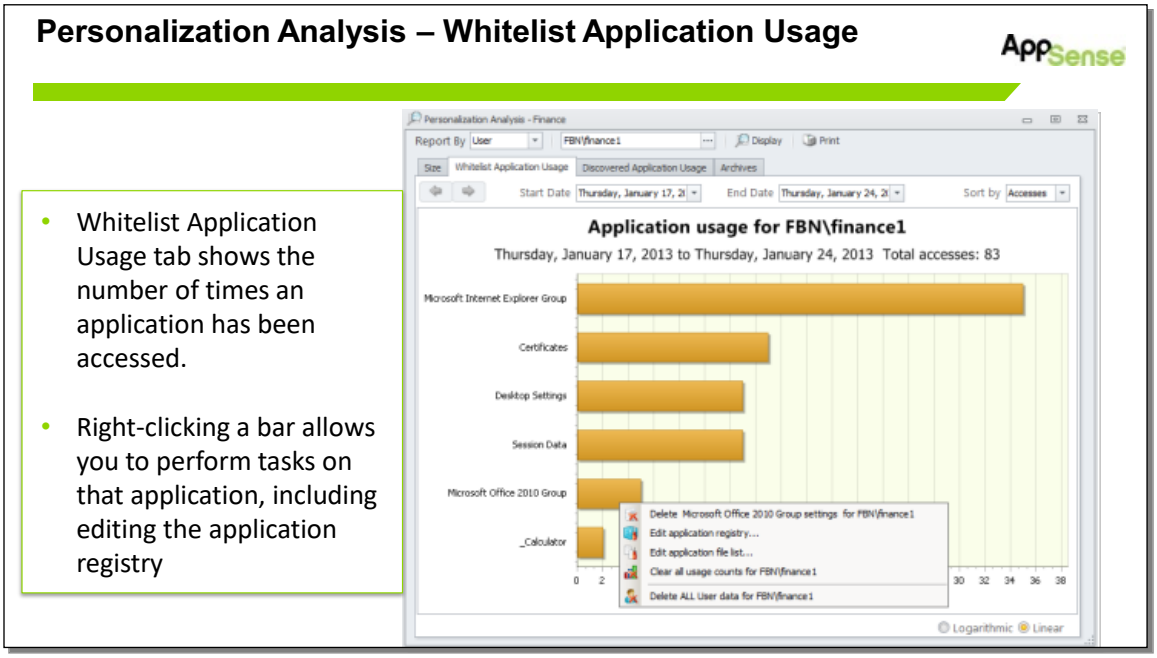
Personalization Analysis is run for a specific personalization group. Select the group you want to analyze and then click on Personalization Analysis from the Tools ribbon.

Multiple Personalization Analysis report windows can be opened at the same time allowing data to be easily compared between different users, applications and application groups.



Personalization Analysis – Size

The size tab displays the amount of data that has been captured for Desktop Settings, Session Data, Certificates, and white listed applications and application groups.



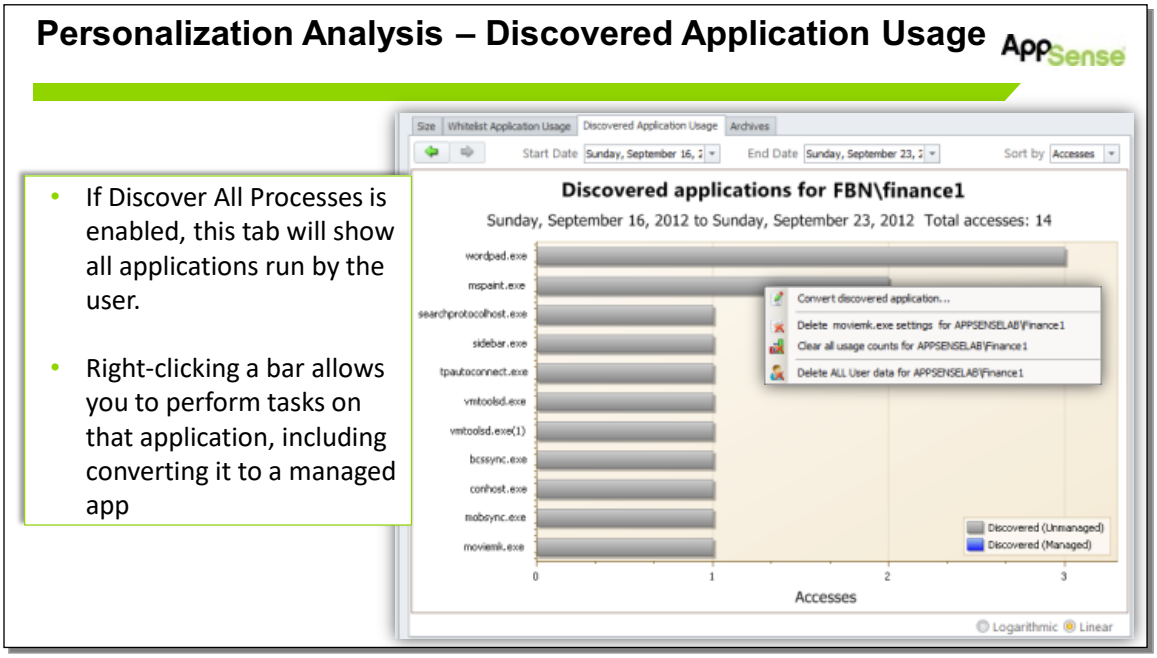
Personalization Analysis – Whitelist Application Usage

This tab displays how often a white listed application or application group has been accessed.

Personalization Analysis also enables the administrator to use the gathered information to directly manipulate data on the Personalization Server. Several options are available which have a real-time effect on application and user settings on the live database:

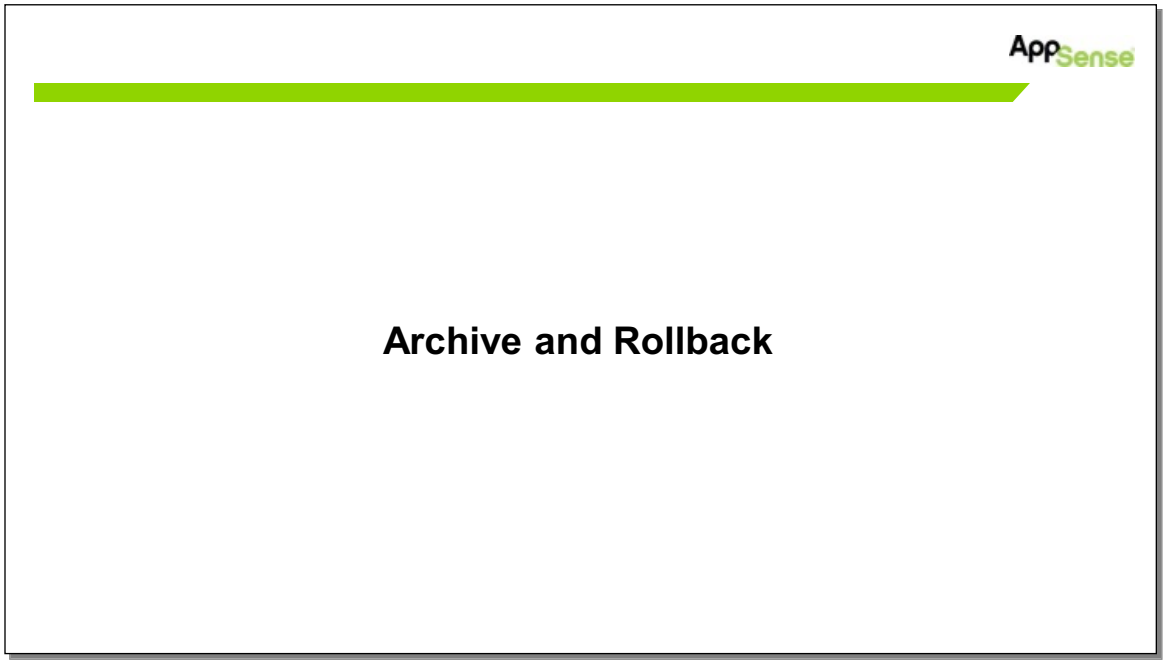
- Restore a user's application settings from a previous, archived state
- Manually create and delete archives for user's application settings
- Delete a user's application settings, reverting to the application's default settings
- View and edit an application's stored registry and file data
- Convert discovered applications to managed applications
- Move application settings between personalization groups

Right-clicking on a bar to access these options is available on both the Size and Whitelist Application Usage tabs.

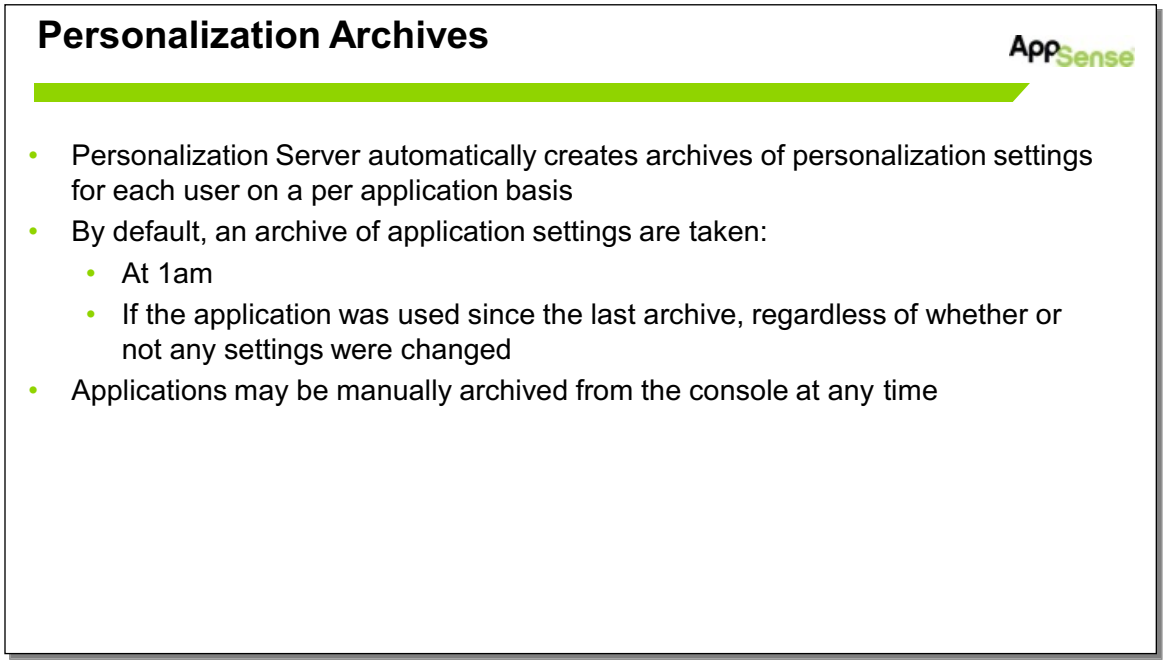


Personalization Analysis – Discovered Application Usage

If Discover All Processes is enabled for the personalization group, this tab will show all applications run by the user and how often they were accessed. Right-clicking a bar allows you to perform tasks, just as on the previous tabs, but note that one option is to convert the discovered application to a managed application.



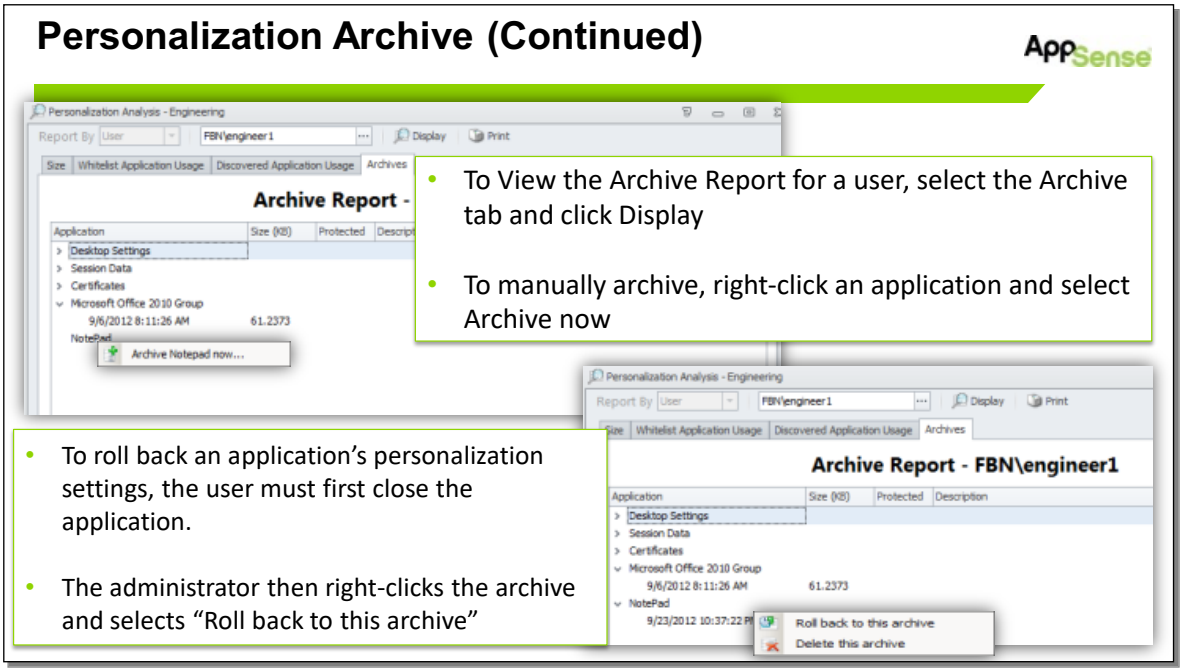
Archive and Rollback



Personalization Archives

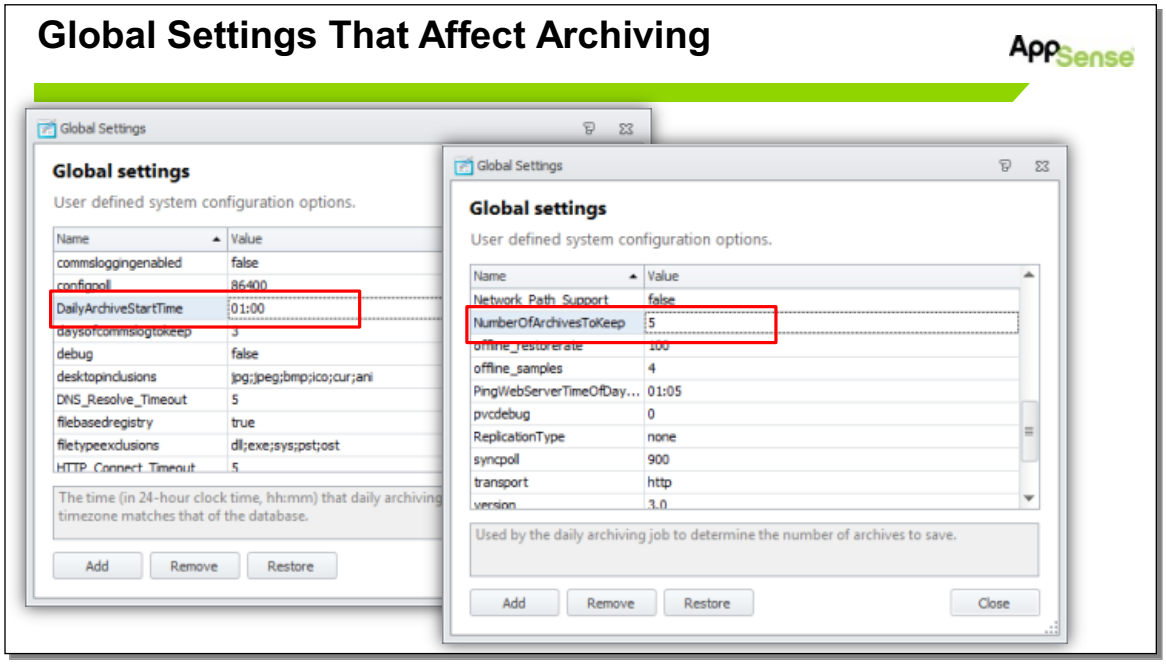
The personalization server automatically creates archives of personalization settings for each user on a per application basis. By default, an archive of application settings are taken at 1am local time. An archive of an application's settings is taken if the application was used since the last archive, regardless of whether or not any settings were changed.

Applications may also be manually archived from the console at any time.



Personalization Archive (Continued)

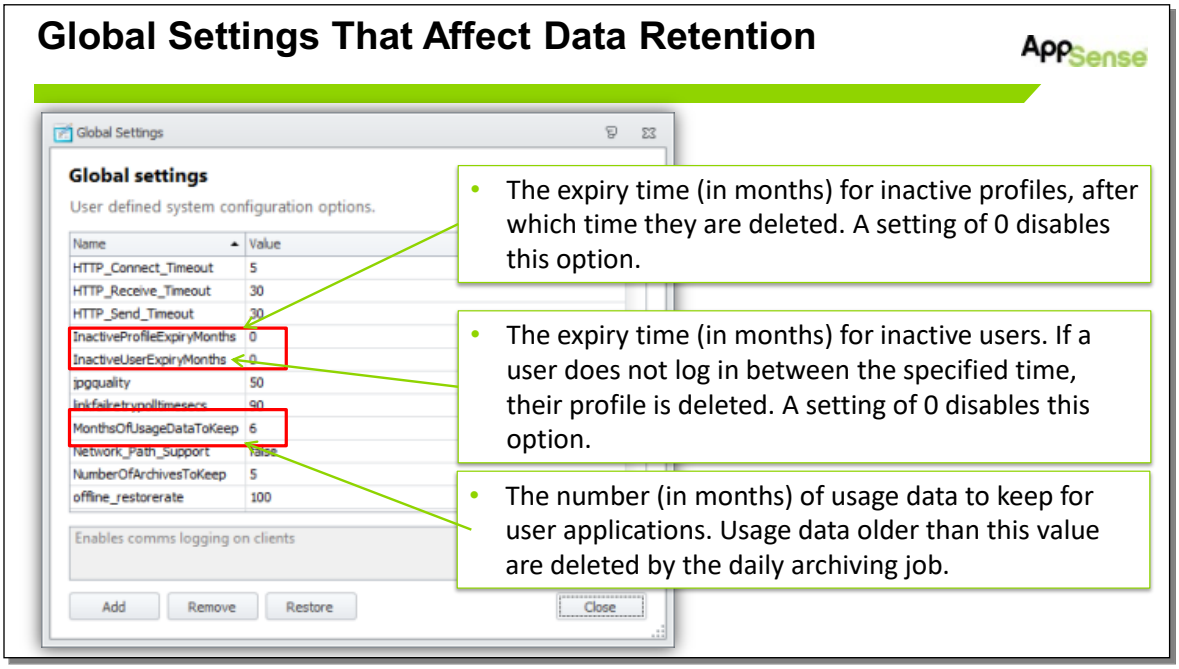
From Personalization Analysis, select the Archive tab to view the archive report for the user. Archives for each application and application group will be listed separately. To manually archive, right-click an application and select Archive now. To roll back an applications personalization settings, the user must first close the application. Then, the administrator right-clicks the archive and selects "Roll back to this archive." The next time the user launches the application, the restored (rolled back) settings will be downloaded to the endpoint.



Global Settings That Affect Archiving

To change the default archive settings, select Global Settings from the “Global” tab. To change the default archive time, change the value for “DailyArchiveStartTime” to the desired time using 24-hour clock time (17:00 = 5:00pm).

To change the default number of archives, change the value for “NumberOfArchivesToKeep.” Note that once the maximum number of daily archives is reached, the oldest archive is purged as the new one is taken. If you manually take archives, you can go past the number of archives specified in the Global Settings.

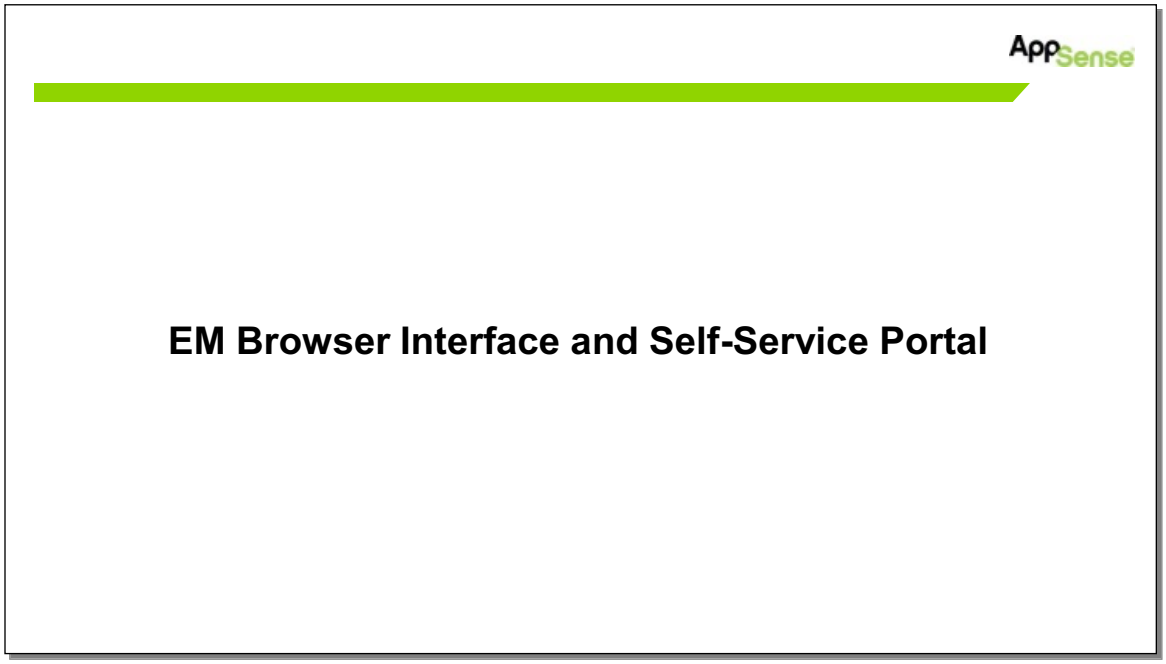


Global Settings That Affect Data Retention

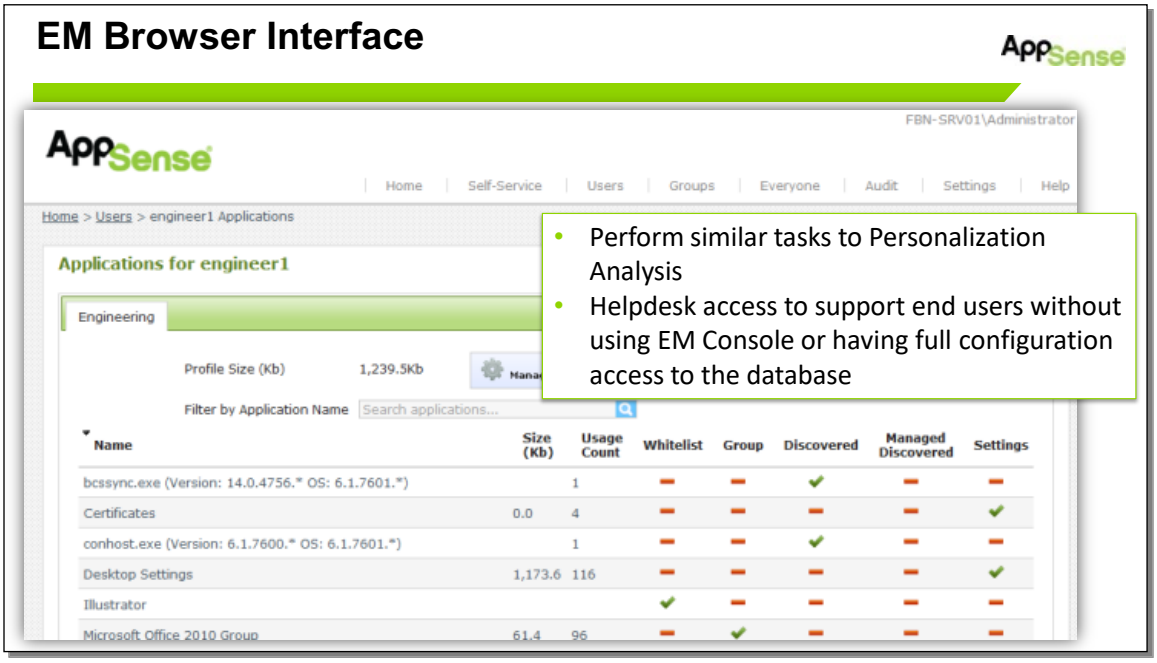
InactiveProfileExpiryMonths - The expiry time (in months) for inactive profiles, after which time they are deleted. A setting of 0 disables this option.

InactiveUserExpiryMonths - The expiry time (in months) for inactive users. If a user does not log in between the specified time, their profile is deleted. A setting of 0 disables this option.

MonthsOfUsageDataToKeep - The number (in months) of usage data to keep for user applications. Usage data older than this value is deleted by the daily archiving job.



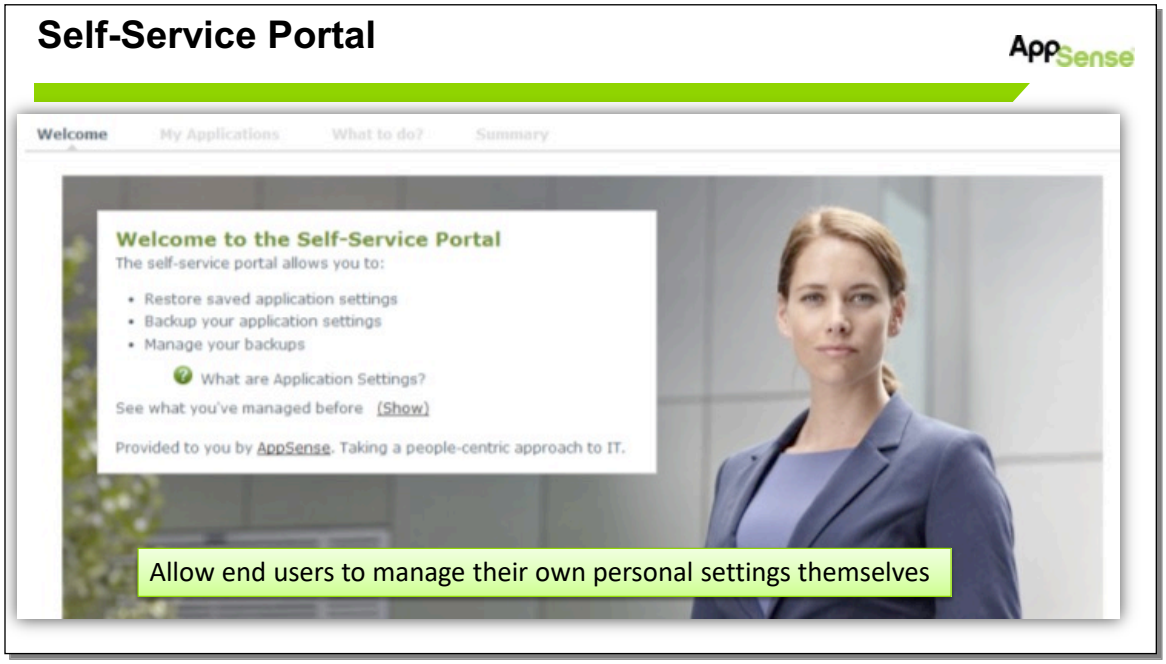
EM Browser Interface and Self-Service Portal



EM Browser Interface

The AppSense Environment Manager Browser Interface provides management of Personalization data, similar to the capabilities of Personalization Analysis, simply by navigating to a URL. This allows support teams to safely carry out routine maintenance for end users without using the Environment Manager console. This removes the need to have full configuration access to the database to perform these tasks.

The EM Browser Interface does require IIS and is configured through its own SCU.



Self-Service Portal

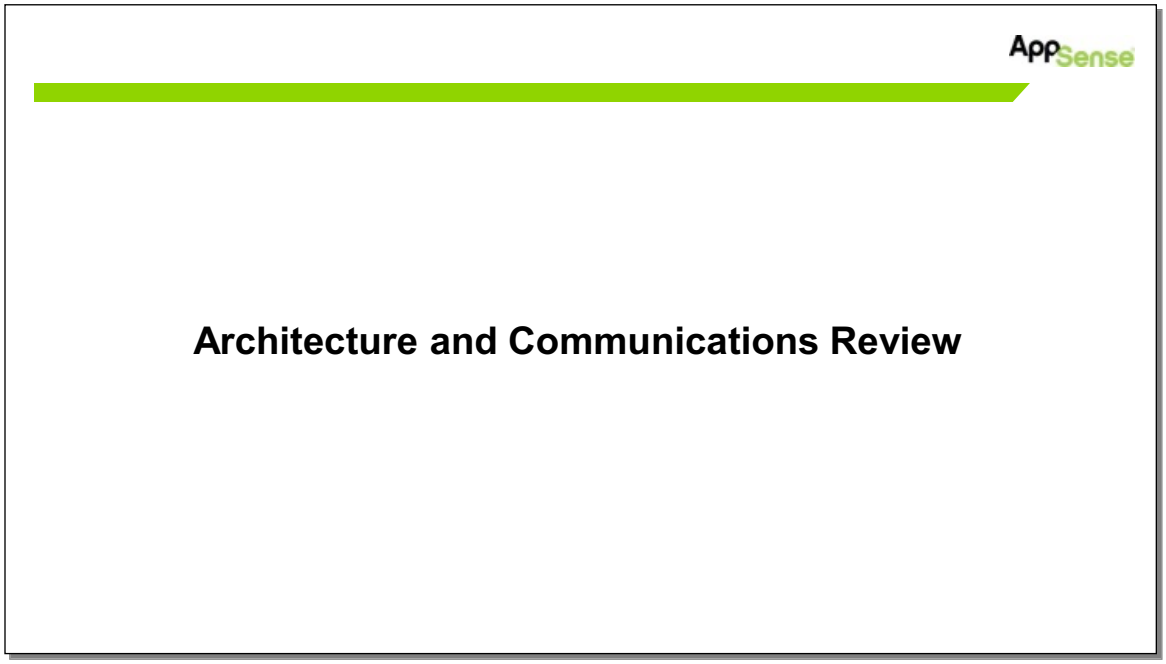
The Environment Manager Self-Service portal allows end users to manage their personal settings for the applications you use. It allows end users to:

- Create a backup of an application's settings
- Restore their backups - create, protect and delete backups
- Delete an application's settings and return them to their default

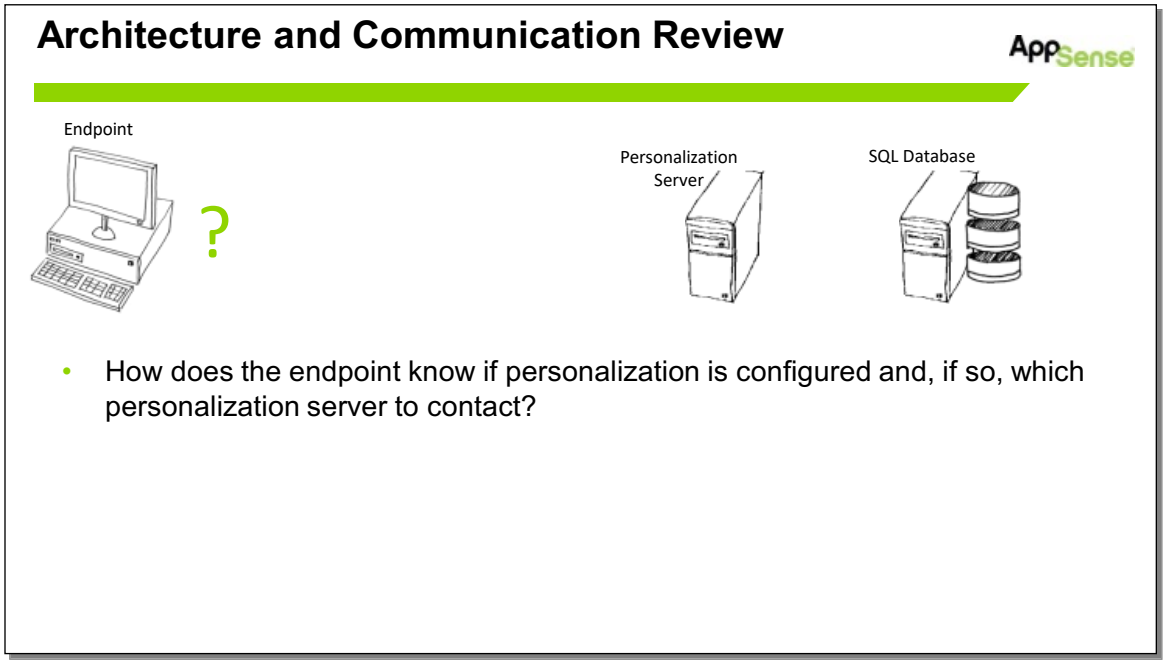
Exercises

- Using Personalization Analysis:
  - View the amount of personalization data is being used by an end user
  - Backup and restore an application's settings for a specific end user
  - Edit an application's registry settings for a specific end user
- Log into the EM Browser Interface as a regular user and perform the following:
  - Create a backup of an application's settings
  - Restore their backups – create, protect and delete backups
  - Delete an application's settings and return them to their default

Exercises

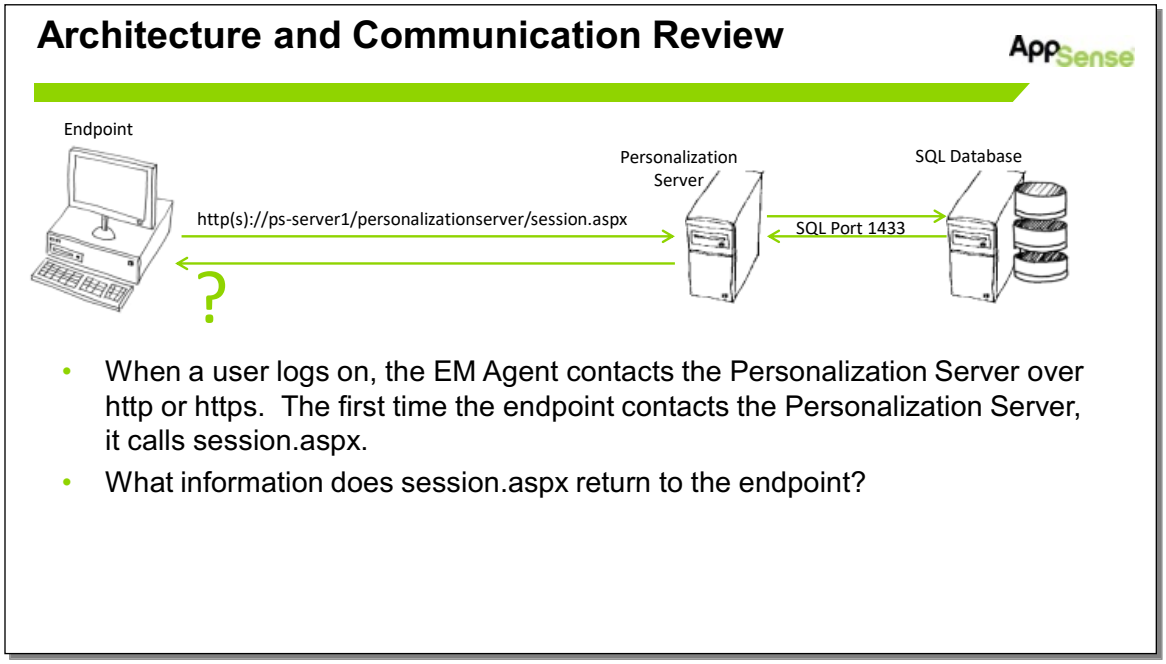


Architecture and Communication Review



Architecture and Communication Review

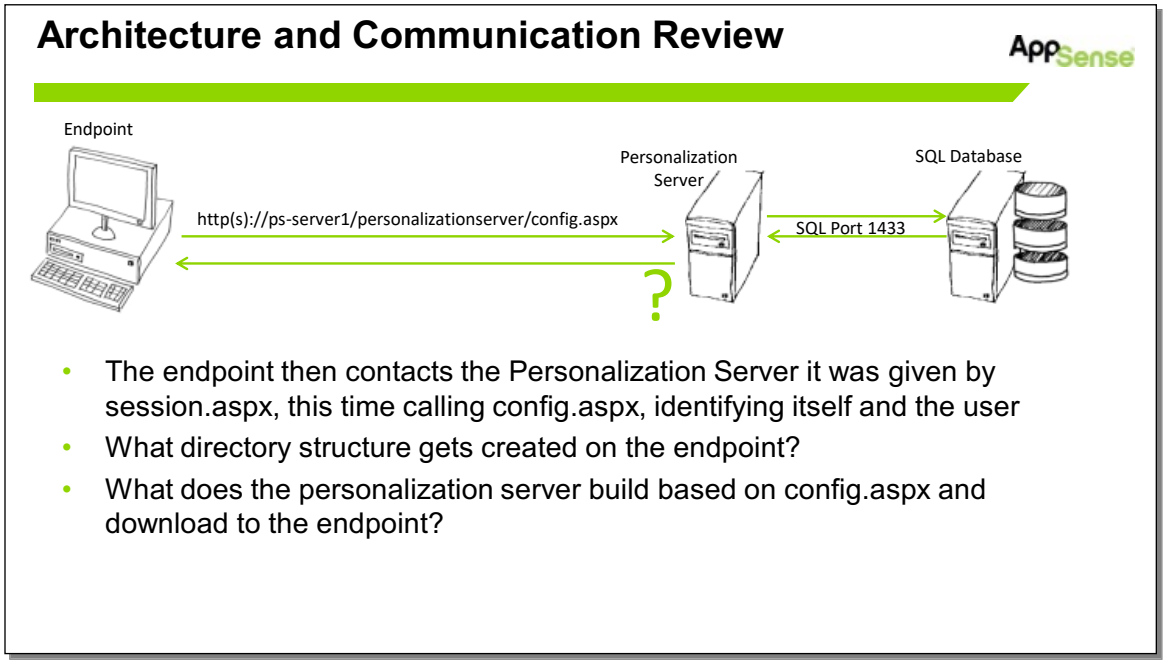
How does the endpoint know if personalization is configured and, if so, which personalization server to contact?



Architecture and Communication Review

When a user first logs on, the EM Agent contacts the Personalization Server(s) listed in the Configuration.aemp file, calling session.aspx. Remember, if you are not using policy, this can also be configured via GPO.

What information does session.aspx return to the endpoint?

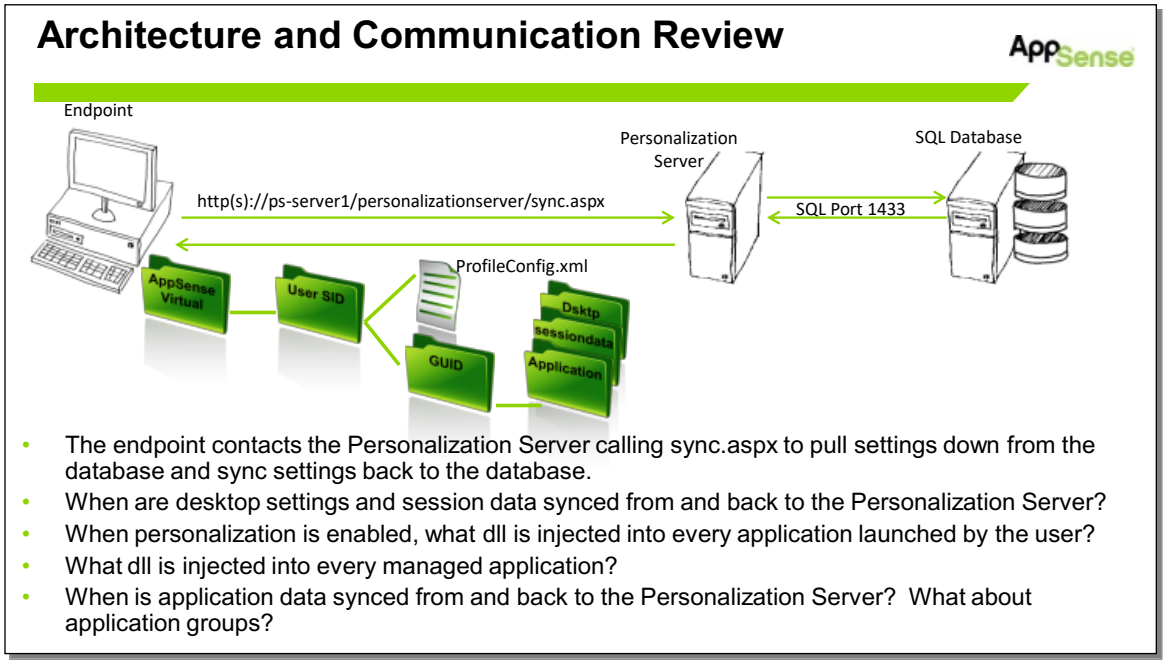


Architecture and Communication Review

The endpoint then contacts the personalization server it was given by session.aspx, this time calling config.aspx, identifying itself and the user.

What directory structure gets created on the endpoint?

What does the personalization server build based on config.aspx and download to the endpoint?



Architecture and Communication Review

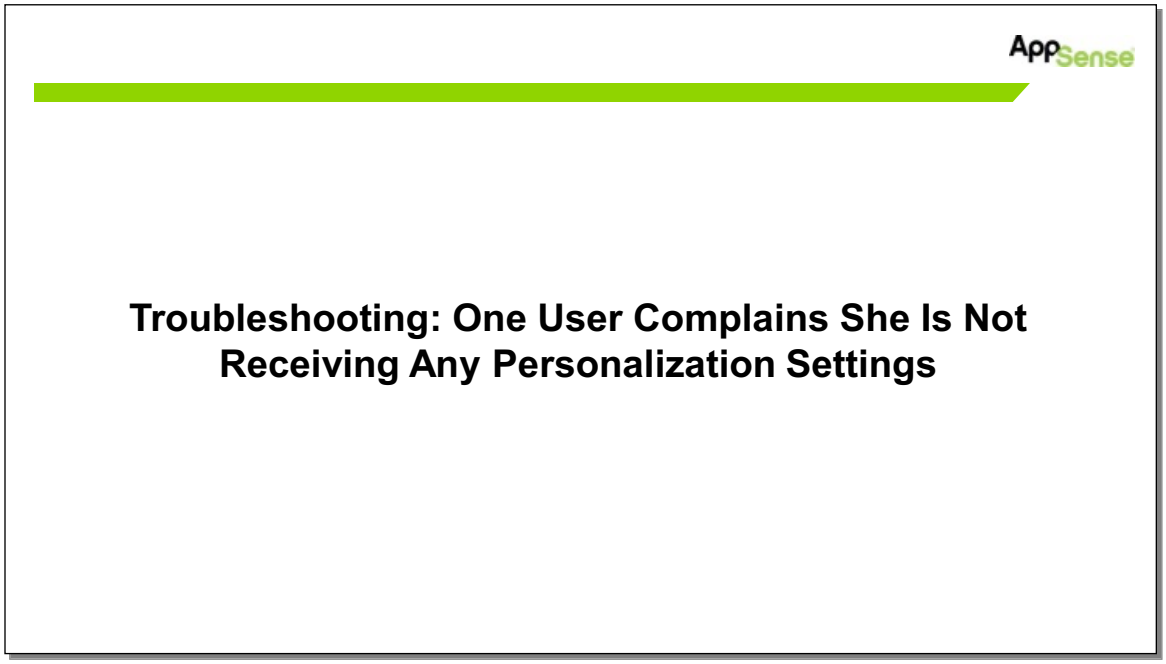
The endpoint contacts the personalization server calling sync.aspx to pull settings down from the database and sync settings back to the database.

When are desktop settings and session data synced from and back to the personalization server?

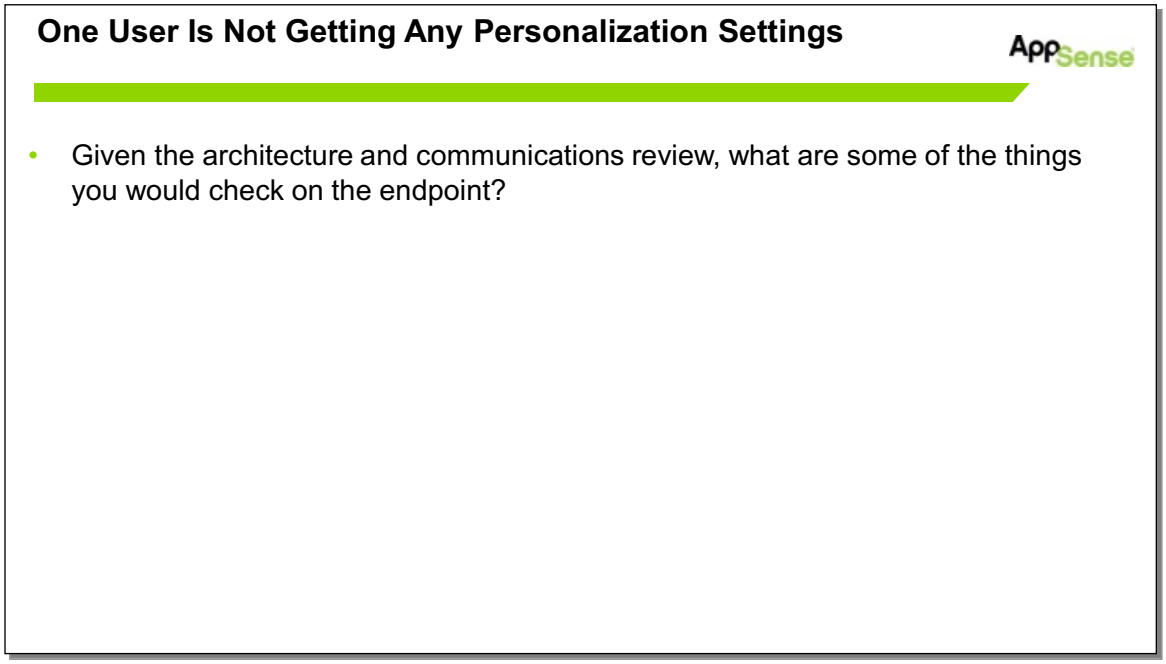
When personalization is enabled, what dll is injected into every application launched by the user?

What dll is injected into every managed application?

When is application data synced from and back to the personalization server? What about application groups?

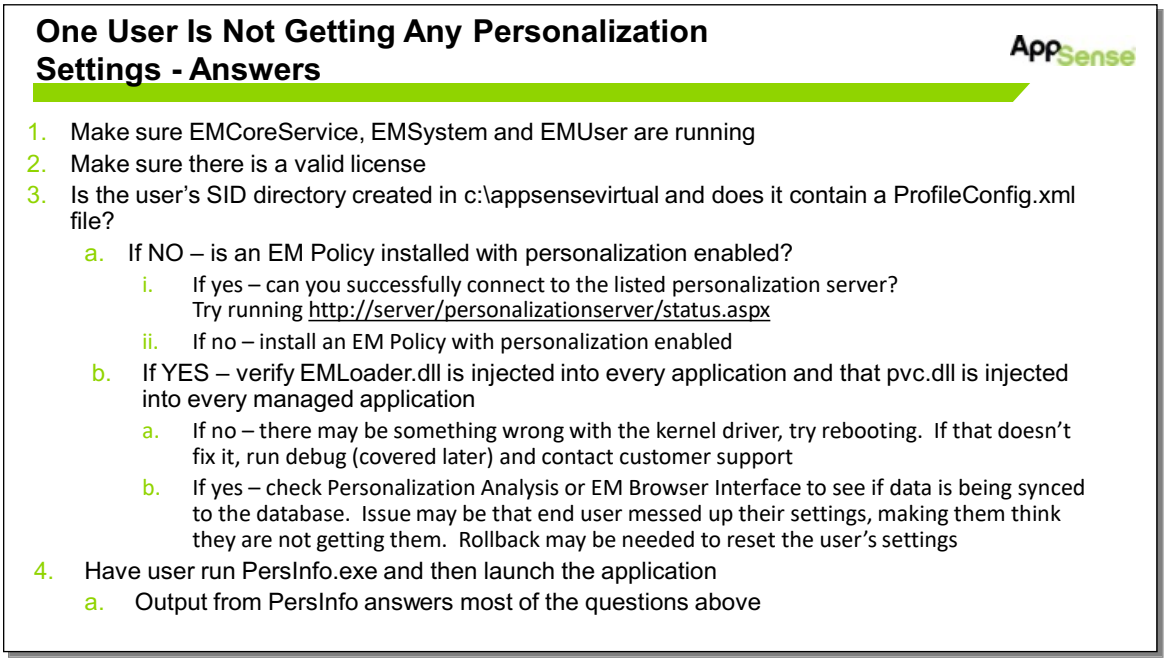


Troubleshooting: One User Complains She Is Not Receiving Any Personalization Settings



One User Is Not Getting Any Personalization Settings

Given the architecture and communications review, what are some of the things you would check on the endpoint?



One User Is Not Getting Any Personalization Settings

Make sure EMCoreService, EMSystem and EMUser are running. Make sure there is an EMUser running for the session where the user is having the issue.

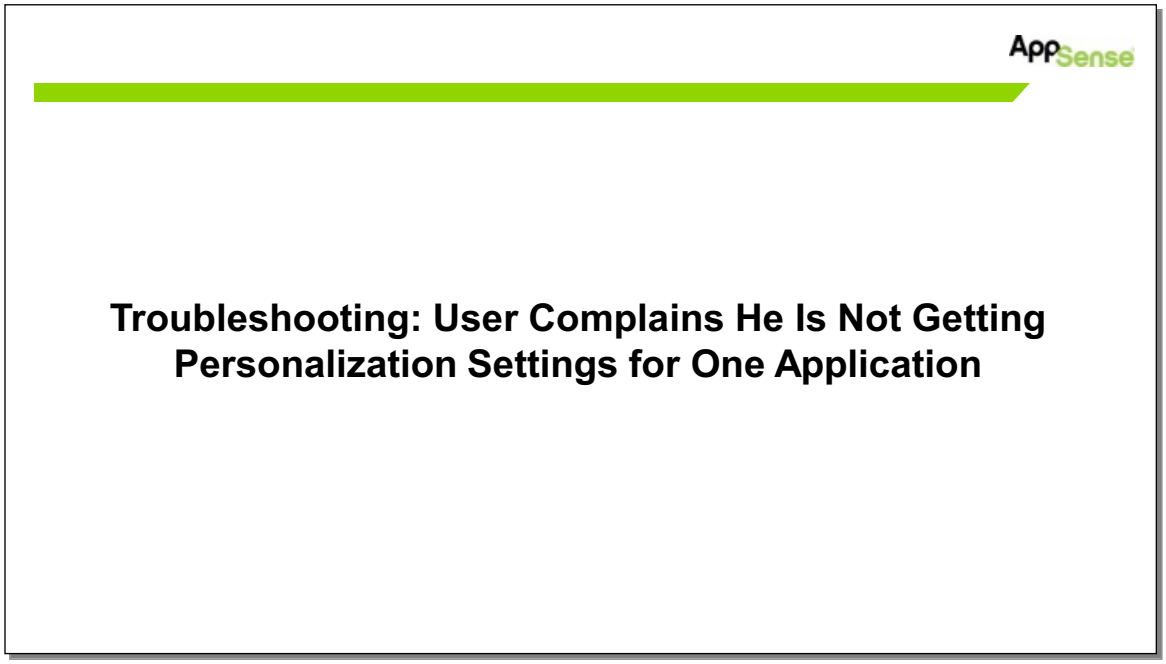
Make sure there is a valid license.

Is the user's SID directory created in c:\appsensevirtual and does it contain a ProfileConfig.xml file?

- If NO – is an EM Policy installed with personalization enabled, or has it been enabled via GPO?
    - If yes – can you successfully connect to the listed personalization server?
      Try running http://server/personalizationserver/status.aspx
    - If no – install an EM Policy with personalization enabled
- If YES – verify EMLoader.dll is injected into every application and that pvc.dll is injected into every managed application
    - If no – make sure that the asvfxldr driver is installed and running. Try rebooting. If that doesn't fix it, run debug (covered later) and contact customer support
    - If yes – check Personalization Analysis or EM Browser Interface to see if data is being synced to the database. Issue may be that end user messed up their settings, making them think they are not getting them. Rollback may be needed to reset the user's settings

Have user run PersInfo.exe and then launch the application.

- Output from PersInfo answers most of the questions above



Troubleshooting: User Complains He Is Not Getting Personalization Settings for One Application

User Is Not Getting Personalization Settings for One Application

- Given the architecture and communications review, what are some of the things you would check on the endpoint?

User Is Not Getting Personalization Settings for One Application

User Is Not Getting Personalization Settings for One Application – Answers

1. Make sure PVC.dll is being injected into the application in question
   a. If Yes, may be an issue with the PVC. Run debug and contact customer support.
   b. If no, open the user's ProfileConfig.xml file and verify the personalization group the user belongs to.
      i. If the user is in the wrong personalization group, adjust the personalization groups' membership rules or the user's AD group memberships accordingly
      ii. If the user is in the right personalization group, make sure the application in question is whitelisted
         i. If application is whitelisted, check Personalization Analysis or EM Browser Interface. Settings for the application may have become corrupt and require a restore/rollback
2. Have user run PersInfo.exe and then launch the application
   a. Output from PersInfo answers most of the questions above

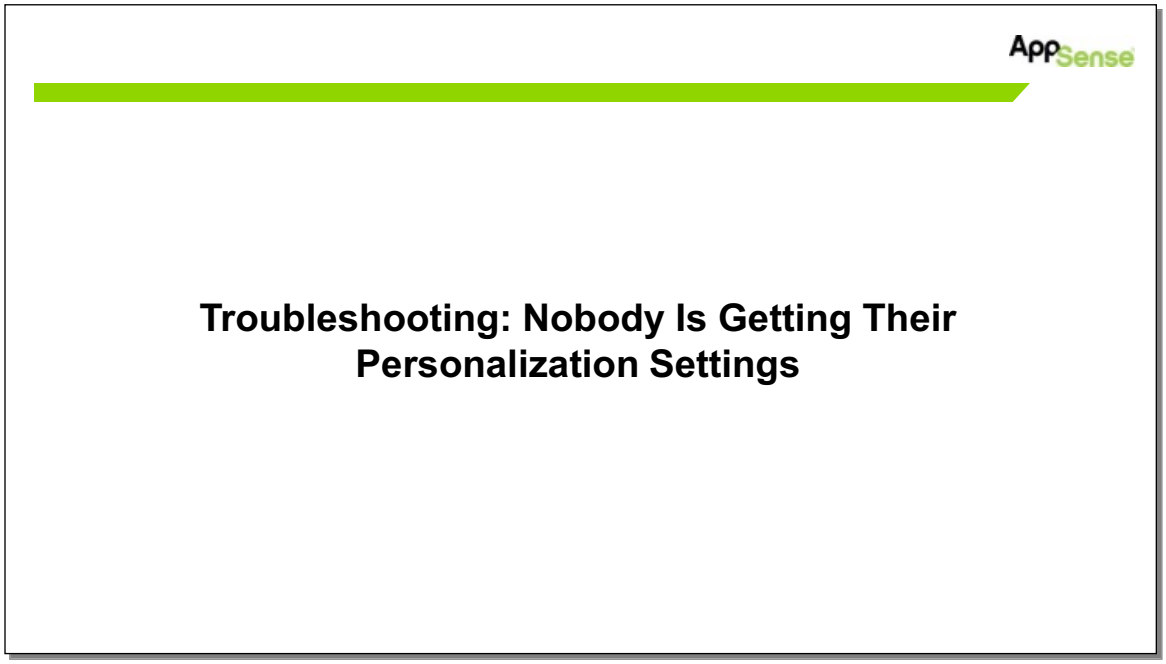
User Is Not Getting Personalization Settings for One Application

Make sure PVC.dll is being injected into the application in question

- If Yes, may be an issue with the PVC. Run debug and contact customer support.
- If no, open the user's ProfileConfig.xml file and verify the personalization group the user belongs to.
  - If the user is in the wrong personalization group, adjust the personalization groups' membership rules or the user's AD group memberships accordingly
  - If the user is in the right personalization group, make sure the application in question is whitelisted
    - If application is whitelisted, check Personalization Analysis or EM Browser Interface. Settings for the application may have become corrupt and require a restore/rollback

Have user run PersInfo.exe and then launch the application

- Output from PersInfo answers most of the questions above

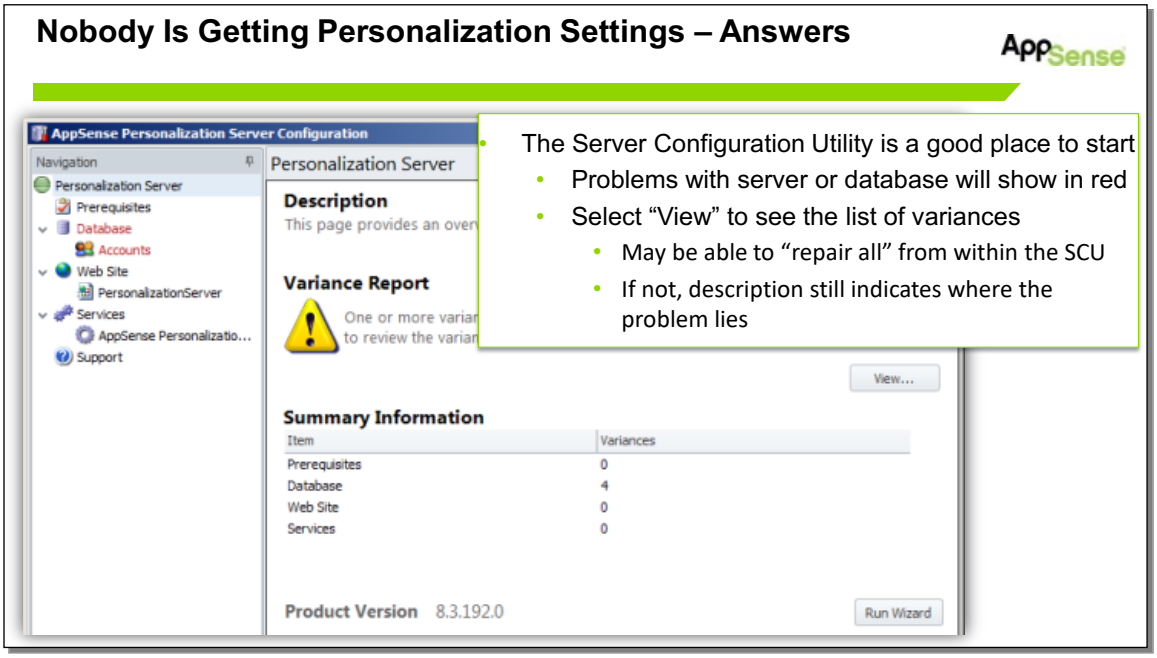


Troubleshooting: Nobody is Getting Their Personalization Settings

Nobody Is Getting Their Personalization Settings

- Given what you know about each of the components of the 3-tier architecture, what are some things you would check?

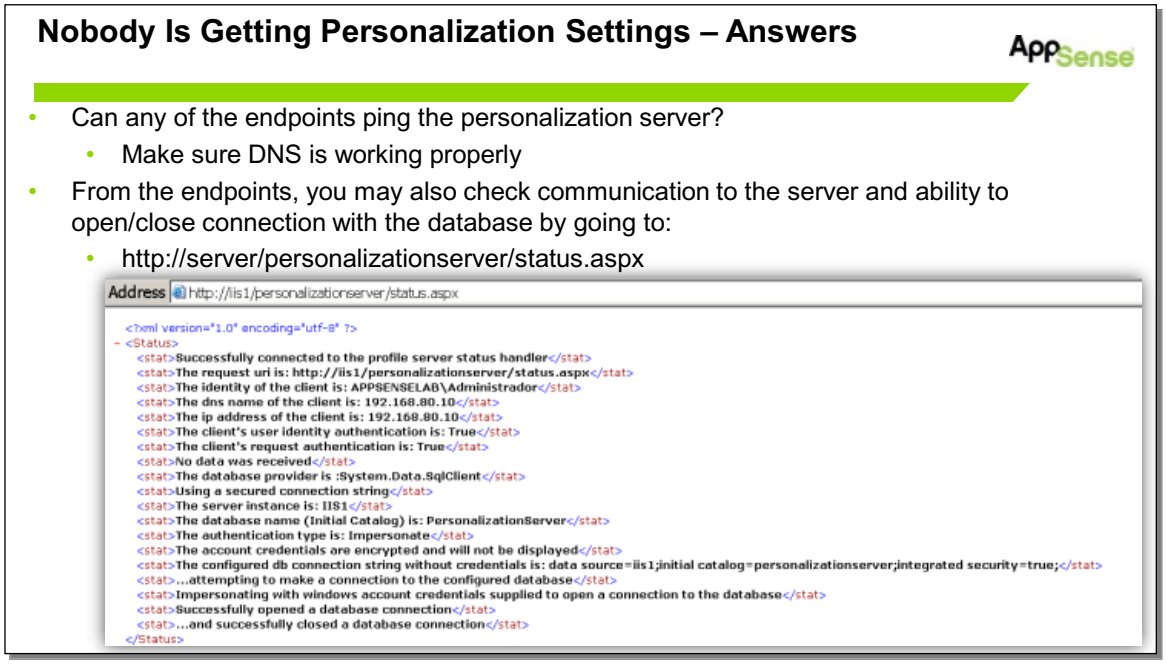
Nobody is Getting Personalization Settings



Nobody is Getting Personalization Settings

The Server Configuration Utility is a good place to start

- Problems with server or database will show in red
- Select “View” to see the list of variances
- May be able to “repair all” from within the SCU
- If not, description still indicates where the problem lies

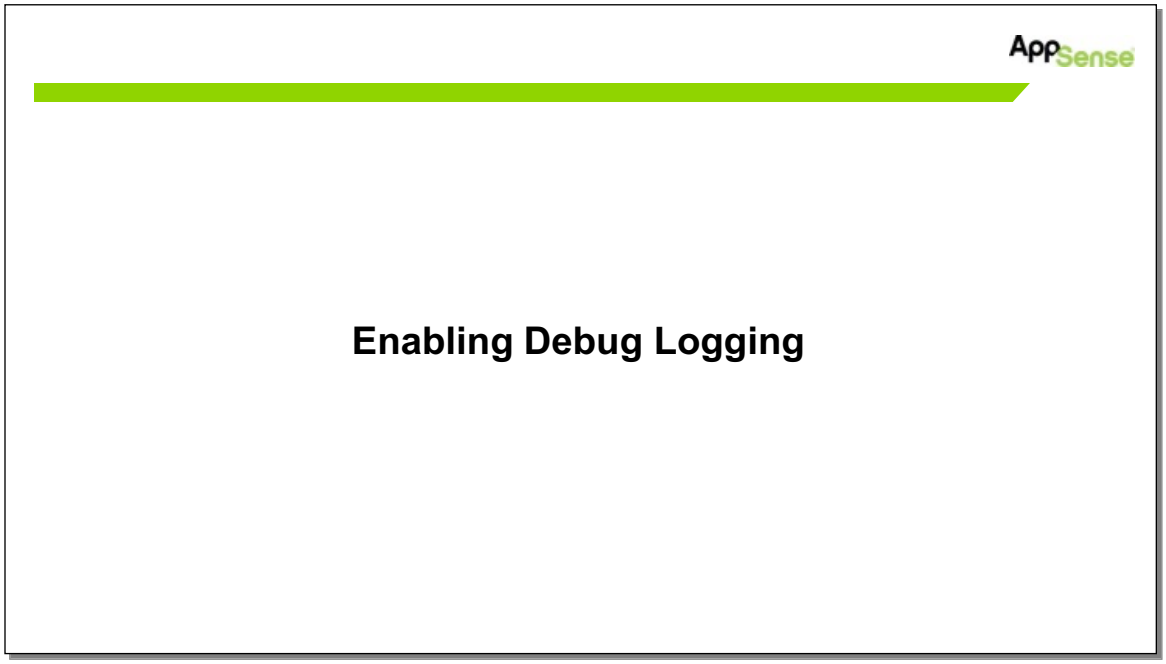


Nobody is Getting Personalization Settings

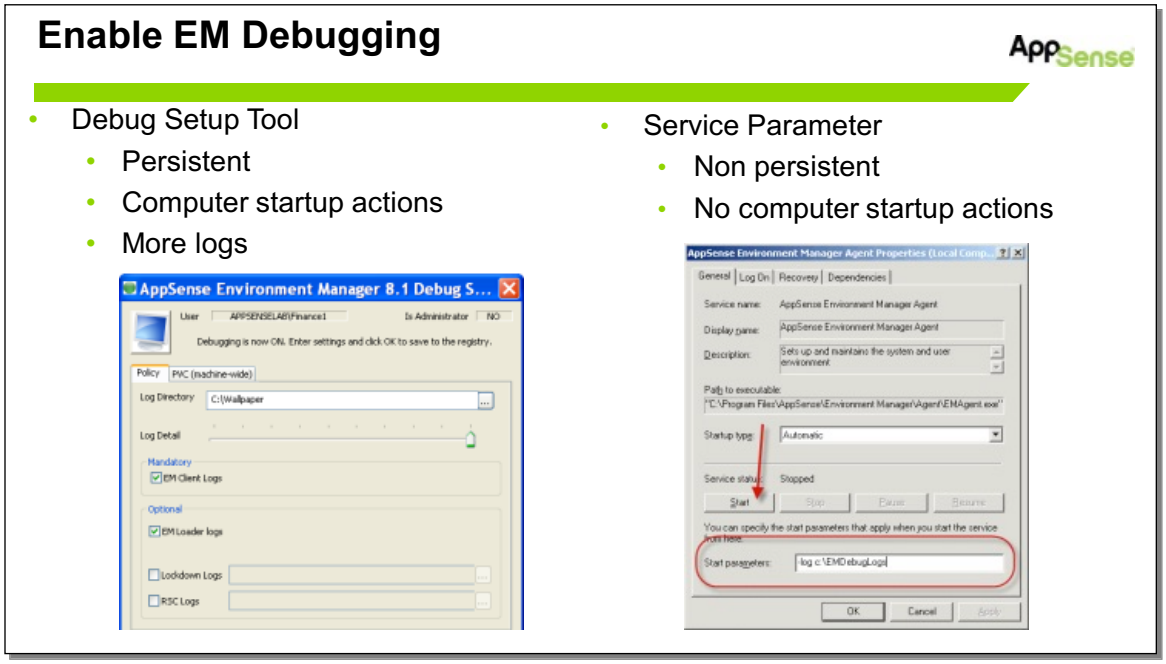
Verify that EM is installed and running. Make sure that it is correctly configured with a working personalization server and is licensed.

When checking communication from the endpoints, do not use ping as the firewall may block it. Instead, launch a browser and go to http(s)://servername/personalizationserver/status.aspx. This will test DNS, routing, firewalls, IIS, .NET, the personalization server and SQL all at once.

Also verify there is a functioning personalization server in the personalization site that the user and/or endpoint belongs to.



Enabling Debug Logging



Enable EM Debugging

The Debugging setup utility will enable :

- EM Client logs
- EM Loader logs
- PVC logs
- Lockdown logs

Administrator privileges are needed to use the Debug tool.

The screen is used to turn debugging on or off.

Don’t forget to turn debug off when you are done collecting data.

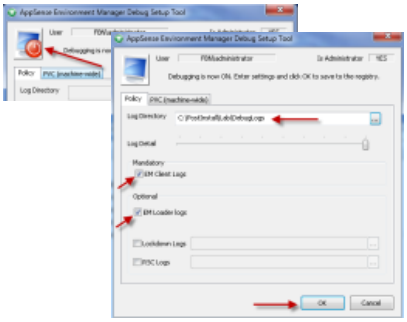
Service Parameter

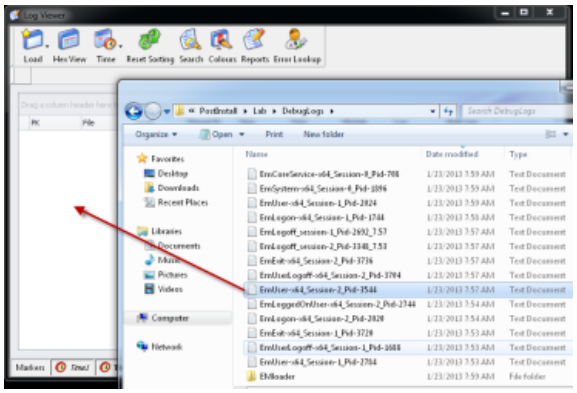
Enabling debug through the service parameter works in session, but it is not persistent across reboots. Because of this, you will not be able to collect all of the logs that support may need, such as:

- No emexit
- No emloggedonuser
- No emauthpackage
- No computer startup actions

Logging

- AppSense products all have the ability to enable debug logging
- These are turned off by default
- Use the AppSense Environment manager 8.4 Debug setup tool to turn on logging
- Use Log viewer to troubleshoot





Logging

To apply CCA debug mode to an endpoint, enable locally by editing the registry

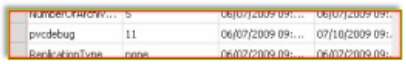
You can use logging to test that EMLoader has loaded PVC.dll into managed applications

TN-150428 - The EM Debug GUI displays this error: "The EM product registry does not exist"

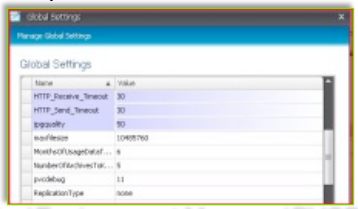
https://www.myappsense.com/Knowledgebase/TN-150428.aspx

PVC Debugging Logging

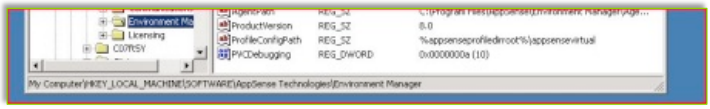
- This can be enabled in numerous places and can be defined as a value between 1 and 11. The first 2 methods set this globally for all client devices. The 3rd method enables on a per machine basis. Be aware PVC Debugging being enable can have a serious impact on performance
  - In the SQL Database in the dbo.GlobalProperties table



  - In the EM Console in Global Settings



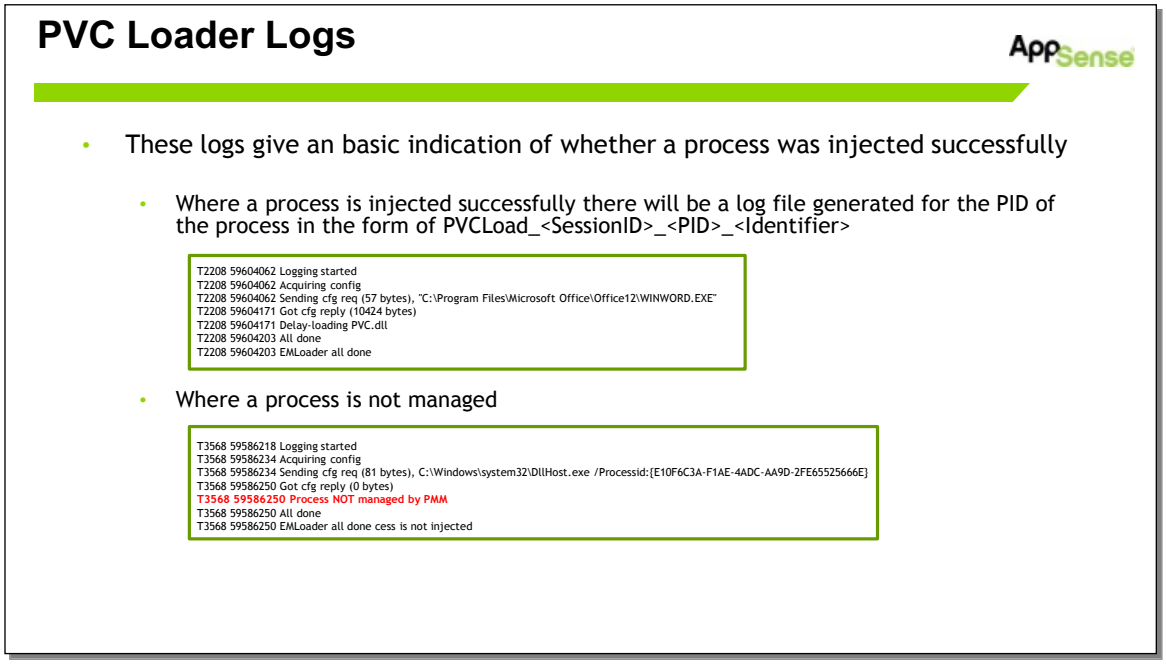
  - By setting the HKLM\Software\AppSense Technologies\Environment Manager\PVCDebugging key with a DWORD binary value of 11



PVC Debugging Logging

Turn on logging and check the corresponding log file that matches the process id.

If the application is personalized the log file will show that the EMLoader has loaded the PVC.dll.



PVC Loader Logs

These logs will indicate whether or not a process was successfully injected.

Event Codes of Interest

- 9390 ,9391, 9392 agent problems
- 9600,9601,9602 Personalization server database communications and accounts
- 9661 could indicate overloaded Personalization server or heavy traffic delaying http communications.

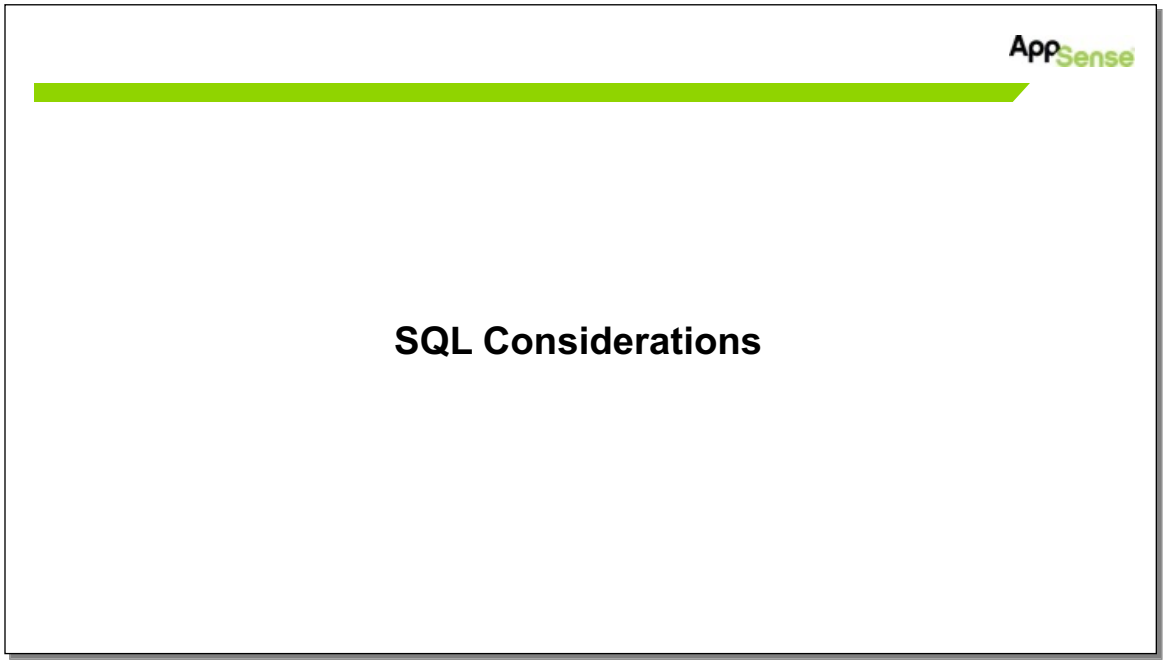
Event Codes of Interest

- 8399 No License
- 9495 Environment Manager not configured.
- 9499 The EMLoader hook required by Environment Manager User Personalization was missing and successfully restored. Please reboot system to re-enable User

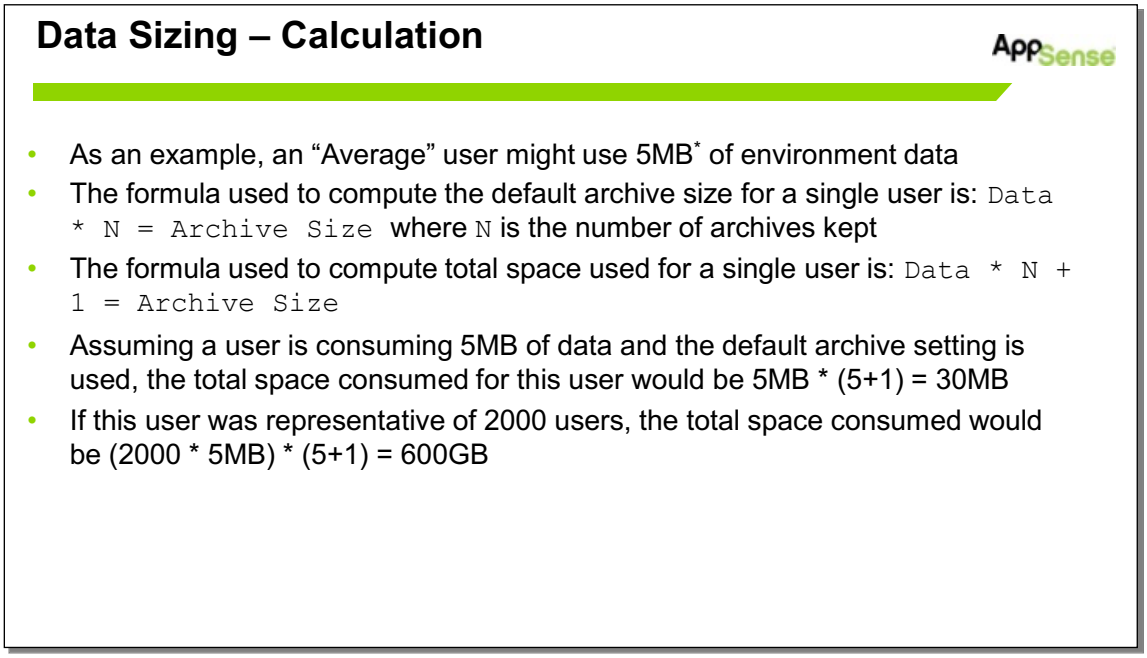
Personalization.

- 9596 Unsupported configuration detected.
- 9660 Personalization for a managed application failed.
- 9650 Managed application start
- 9651 Managed application stop
- 9652 Personalization load error
- 9653 Personalization save errorn
- 9654 Blacklisted process started
- 9655 Personalization not saved part of group
- 9656 Offline resiliency save started
- 9657 Offline resiliency save complete
- 9658 Personalization settings purged
- 9659 Personalization settings updated
- 9660 Personalization failed

- 9661 Timeout Communicating with Personalization Server



SQL Considerations



Data Sizing – Calculation

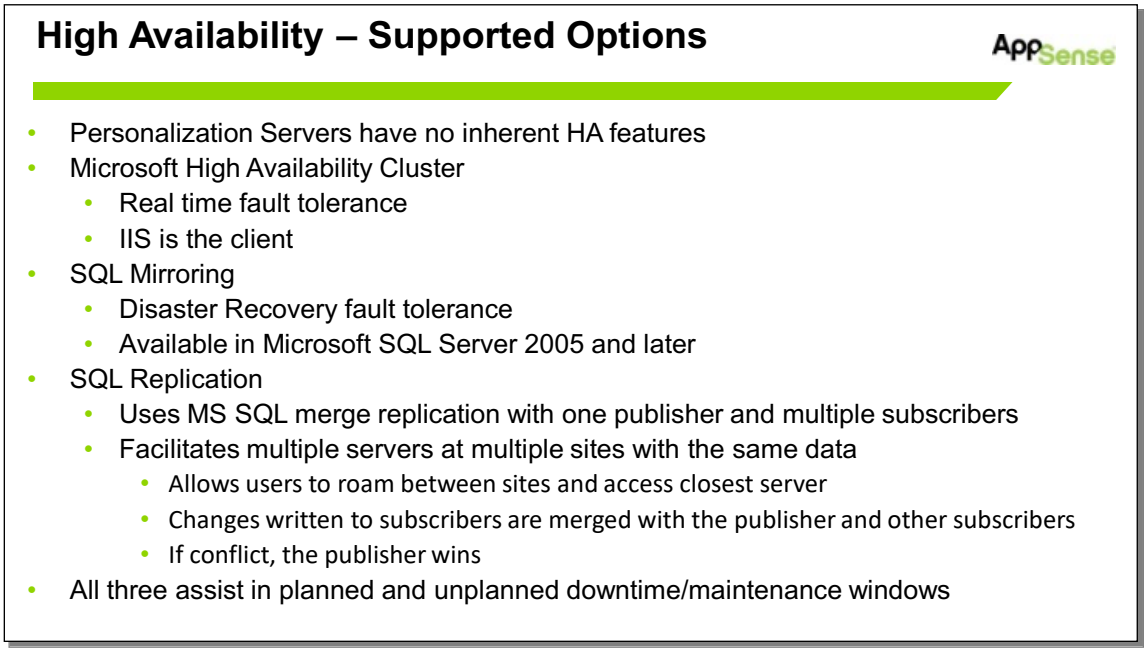
*This is just an average. Actual data consumed will vary considerably depending on specific implementation criteria. The best way to determine the actual data usage of a user is through the use of the Personalization Analysis tool. User profiles can be very small in tightly controlled environments, but may be up to 25 MB or more in others.

Sizing – Transaction Logs

- Default is Simple Recovery Model
  - Every transaction is logged but logs are truncated at checkpoint
  - Does not support Mirroring
  - Does not support arbitrary point in time recovery
- Full Recovery Model is the only model that can be used with mirroring
  - Can recover to an arbitrary point in time
  - Very resistant to data loss or damage
  - HIGHLY dependent on transaction logs
  - Logs are NOT truncated after full database backup
  - Logs are only truncated after log backups

Sizing – Transaction Logs

If using the Full Recovery Model, the transaction log size is a crucial consideration. The log size will vary from one environment to another, but you need to ensure that the log file can expand to include the throughput of all data between transaction log backups. For example, if daily backups are taken, the log needs to be able to store an entire day's worth of data.



High Availability – Supported Options

Microsoft High Availability Cluster

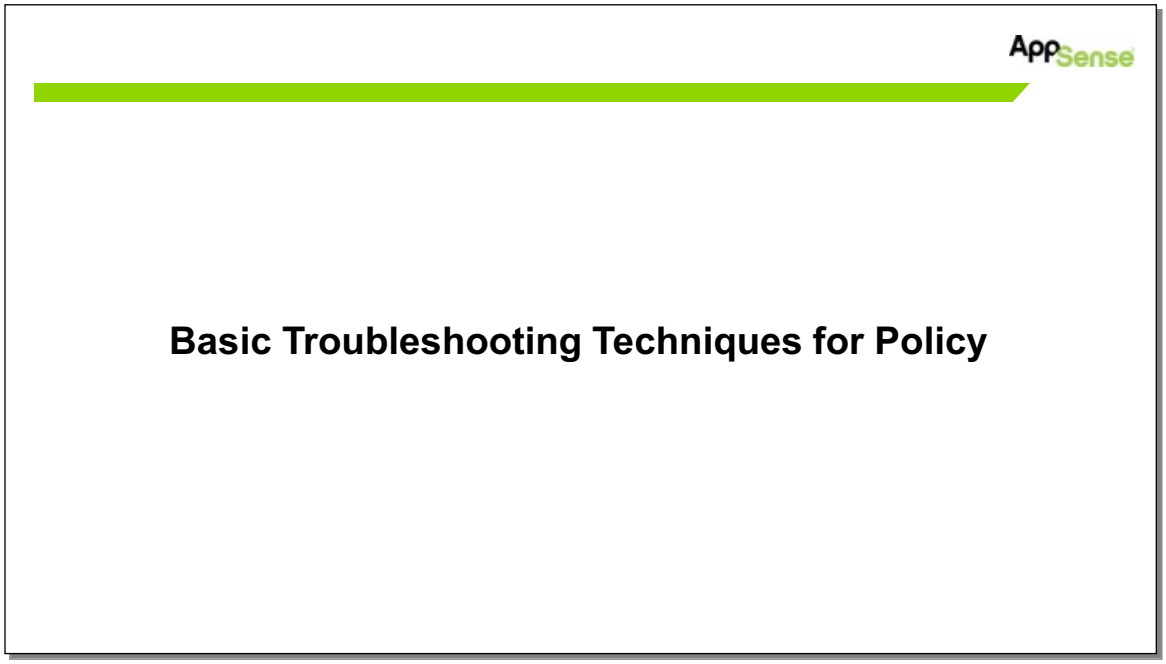
Where possible, install the Personalization Database with High Availability in mind. Typically for this, clustering of the Microsoft SQL Server is recommended.

SQL Mirroring

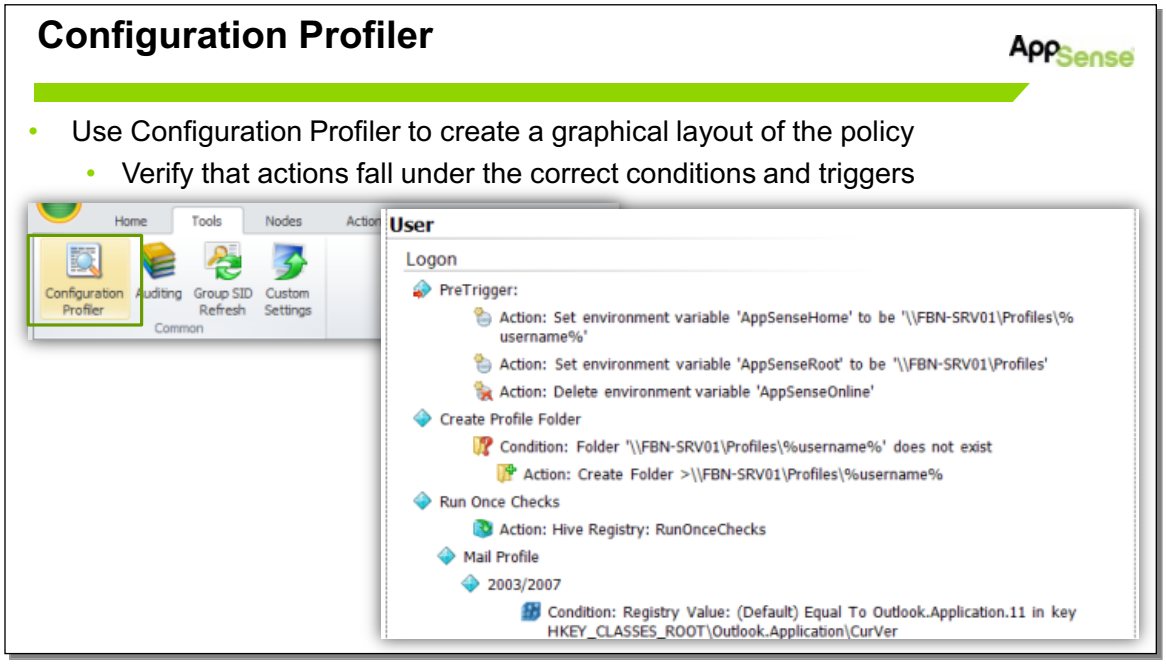
SQL Database Mirroring is a strategy which ensures data resiliency by maintaining a real-time copy of a database on a mirror SQL Instance. In the event of a failover, this Hot Standby Database can be employed to provide near immediate restoration of service. The originating server is known as the *principal* and the standby is known as the *mirror*. Data is automatically synchronized between the two so when required the mirror is up-to-date. If set up in accordance with Microsoft best practices, SQL Mirroring is supported by Environment Manager.

SQL Replication

- Replication uses an updatable push-merge subscription model
- Two publications are made available:
    - Config which contains the configuration
    - Data which contains personalization data
- Config merge runs every 5 minutes
- Data merge runs at Midnight
- Changes made on the Subscribers are reported back to the Publisher
- Recommended to use the Synchronize Site Databases to manually initiate a sync



Basic Troubleshooting Techniques for Policy

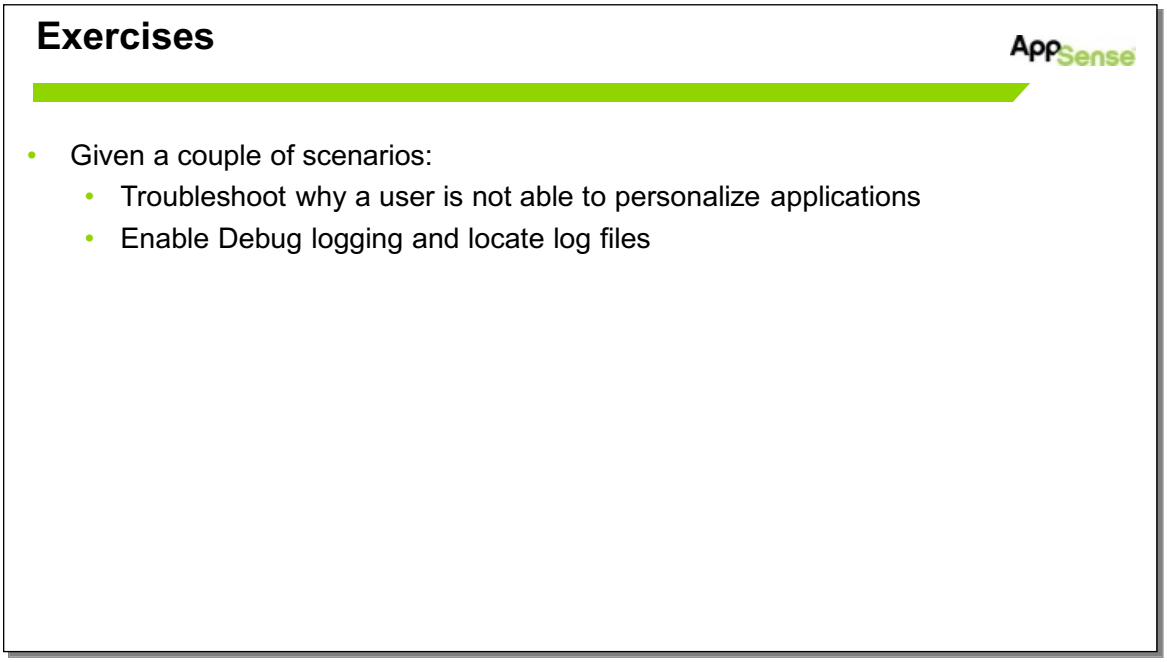


Configuration Profiler

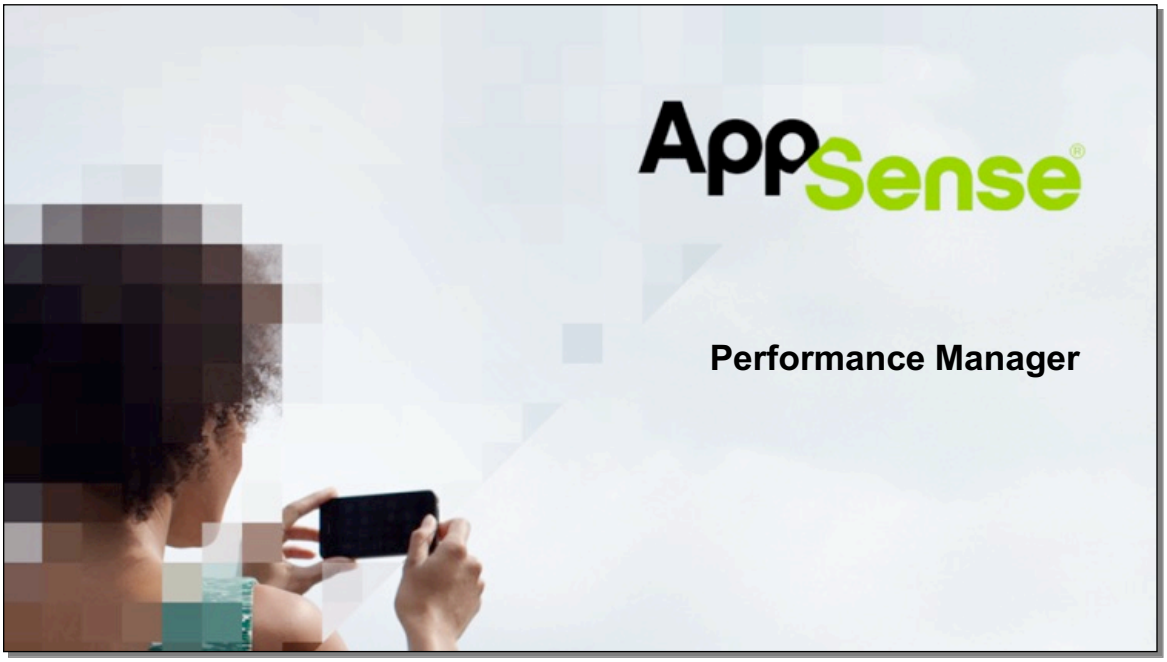
Configuration Profiler will generate a graphical representation of how your policy is configured. It lists each trigger. Under each trigger, it lists each node. It then lists every condition and action within the node as well as any child nodes and their conditions and actions. In short, you can easily see which action will run based on which parent conditions or actions and which trigger it resides under.

Configure Audit Events

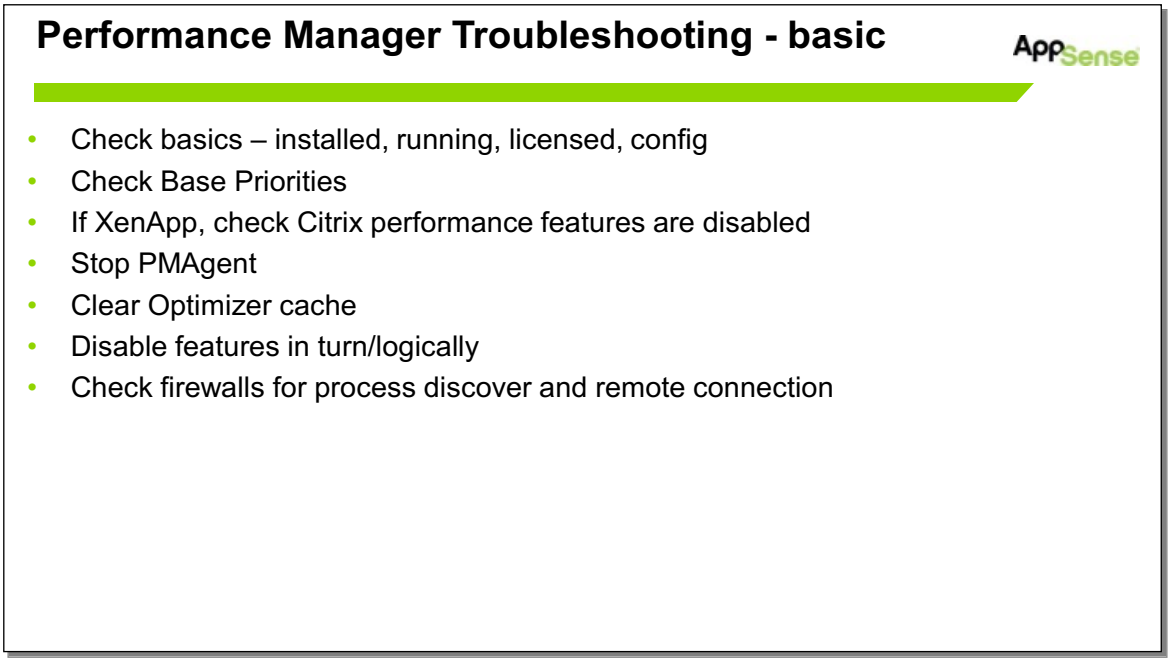
From within the policy, you can configure which events to audit and send those events to a local syslog file for monitoring and alerts.



Exercises



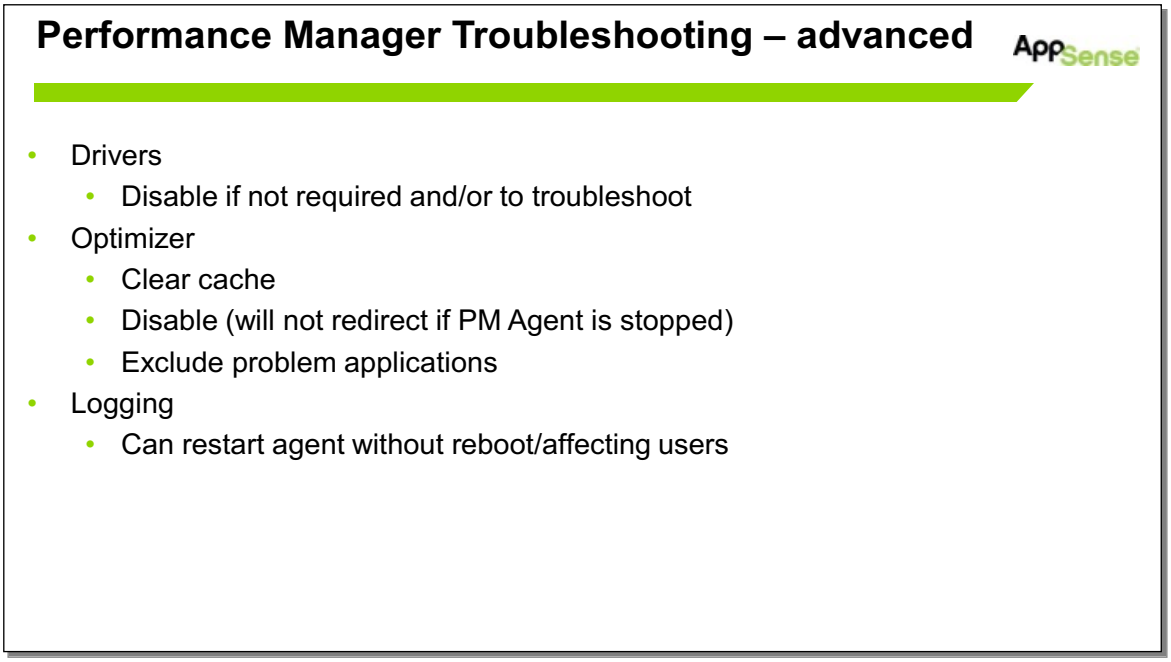
Performance Manager



Performance Manager Troubleshooting – basic

A quick way of basic health checking of PM is to add the Base Priorities column to task manager which should show the majority of processes at “Above Normal” if the PM agent is running, licensed and has a configuration. This is a byproduct of the Smart Scheduling feature. Note that if some components are excluded from Smart Scheduling or the whole feature is not enabled, which should be investigated/understood, then the Base Priorities will not be changed so will mostly appear as “Normal”.

Depending on the problem, does stopping the PMAgent stop the problem from occurring?



Performance Manager Troubleshooting – advanced

Performance Manager v8 uses two device drivers, namely:

- **pmusermem** – when user memory limit exceeded, stops further processes from launching
- **pmoptimizer** – redirects file access to dlls to optimized copies and implements disk control

By design, these drivers cannot be stopped so to disable them, you must set their start-up type to disabled and reboot. This is also why uninstalling or upgrading always requires a reboot.

Disabling can be done in two ways:

1) Change the “Start” value from 0 to 4 in “HKLM\CurrentControlSet\services\PmOptimizer” and “PMUsermem” keys
2) Use “sc config pmusermem start= disabled” and re-enable with “start= boot”

Performance Manager logging can be enabled by starting the service with a “-log <logfilename>” option. This is also the case for LSS. To log from boot, create “DebugFile” (REG_SZ) and “DebugLevel” (REG_DWORD) = 10 (decimal) in “HKLM\SOFTWARE\AppSense\Performance Manager” and restart. 43