



Best Practice / Technical Update Intercept Sept 09

Simon Townsend

Head of Pre Sales / Systems Engineering

user environment management™

Agenda

- Recap and Demonstration of UEM
- Common Questions
- EM SP1 and SP2 Update
- Best Practice
 - EM Policy and EM Personalisation
- Troubleshooting
- Architecture, Scalability and Multi Site
- Streamed “Provisioned OS”
- Streamed Applications
- PM Update
 - Default Configuration
 - Statistics
- AM Update
 - Default Configuration
 - ANAC
- Other resources



Latest Versions

- AppSense Management Suite SP2a
 - Released 3rd August 2009
 - Suite Version 8.0.702.0
 - Available from www.myappsense.com



www.appsense.com

myAppSense

Home Notifications Licenses Account Leads **Download** Configuration Center Support Subscriptions

AppSense Software

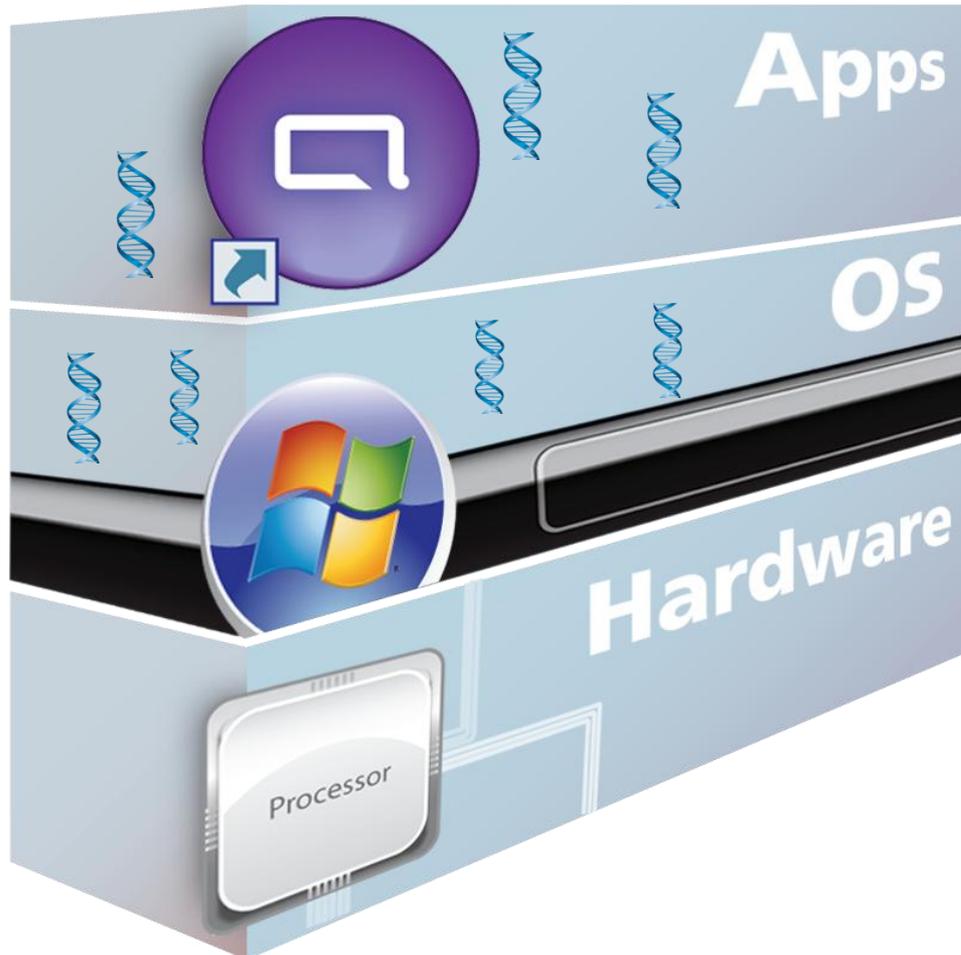
Here are the latest downloads for the AppSense Software Suite.

Downloading version 7.2? [Please read this message.](#)

Management Suite Environment Manager Application Manager Performance Manager Management Center Desktop Security

Product	Version	Description	Release Date	Size (mb)
AppSense Management Suite Service Pack 2a	8.0.702.0	The latest release of the world leading user environment management solution for the enterprise - A fully integrated solution comprising four components: Application Manager, Environment Manager, Performance Manager and the Management Center, providing complete Policy and Personalization Management, Application Entitlement and System Resource Entitlement across all desktop and application delivery mechanisms with reporting, auditing and failover capabilities. View release notes for list of updates.	03-Aug-2009	505

Virtualization in Client Computing



Virtualization in Client Computing



Virtualization in Client Computing



Virtualization in Client Computing

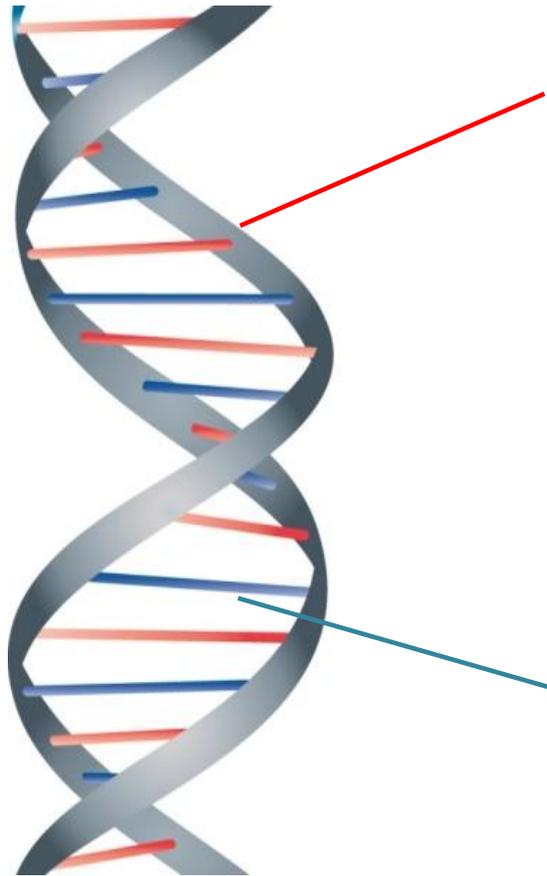


User Personality

The Third Layer - User Personality



The User Personality



Policy

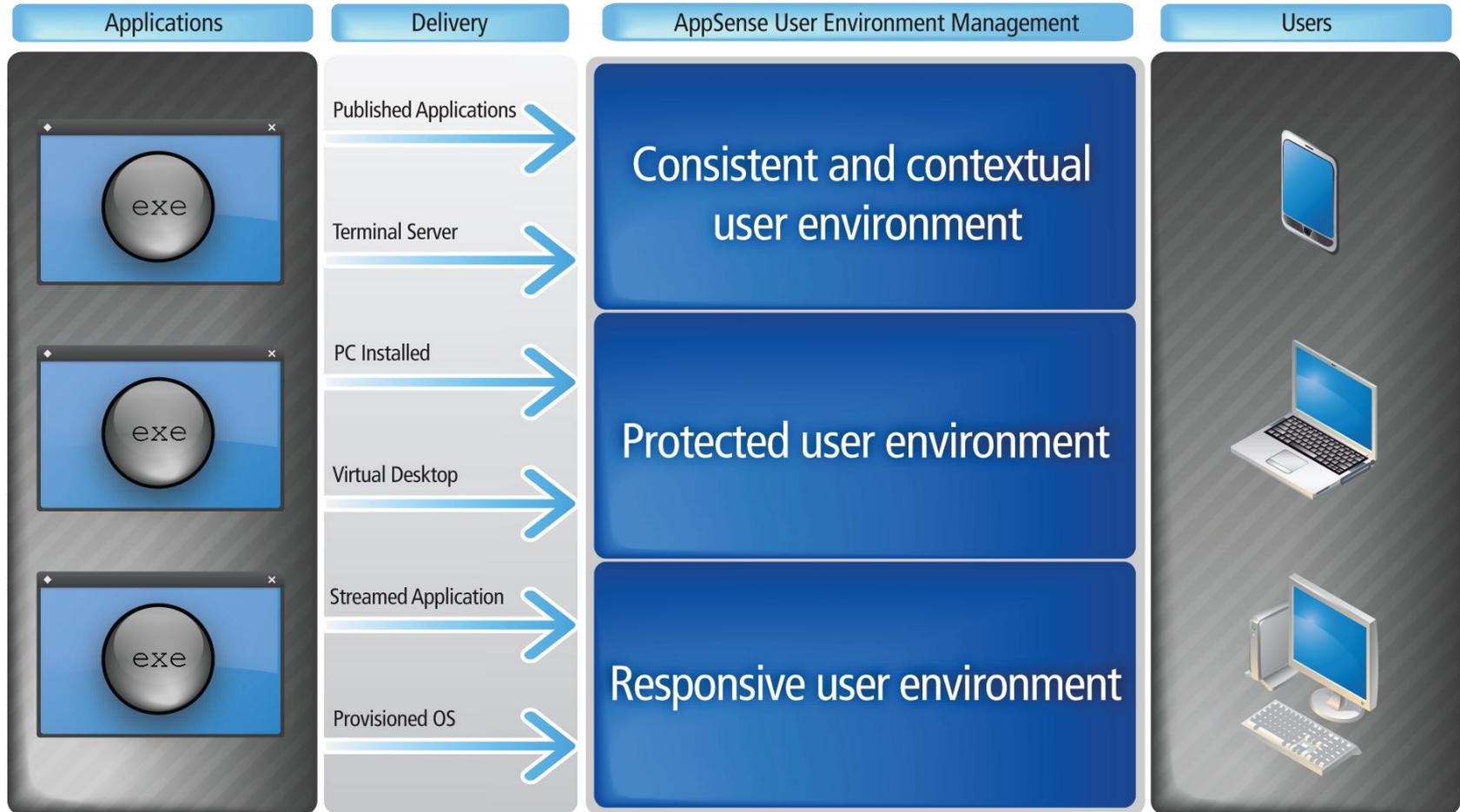
Set up and maintain a desktop



Personalization

Enable the user to make it their desktop

Introducing user environment management



user environment management Solution

AppSense user environment management

Consistent and contextual user environment

Protected user environment

Responsive user environment

AppSense Management Suite

Policy and Personalization Management

Application Entitlement

Resource Entitlement



AppSense Solution Set



- W2K3, W2K8, Windows XP and Vista
- All 32bit and 64bit
- Both consoles and Agents

A complete solution

- Personalization and Policy Management

- Faster user logon times
- Reduce profile corruption & support call remediation
- Replacement of complex logon scripts



- Application Entitlement

- Deny unauthorised executables
- Control authorised application usage
- Reduce Microsoft application licence requirements



- System Resource Management

- More users per server / server consolidation
- Improved quality of service / prevent server lockups
- Extend hardware lifecycle



AppSense®

Demo

user environment management™

AppSense®

Some Basics

user environment management™

Some Basics

- The AMC
 - W2K3, IIS, BITS, HTTP(s)
- The Agents
 - MSI
- The Config's
 - XML, Packaged as MSI, can be saved in A**P format (zip)
- Deployment Groups
 - Directory vs Computer

Manual Installation of CCA

- Deployment Options
 - SCCM, Altiris, GPO, AppSense Deployment Tool,
- `msiexec.exe /qn /i "<MSI file path>\CommunicationsAgent.msi"`
`WEB_SITE="https://<Management Server Name>"`
`GROUP_NAME="<DeploymentGroup>"`



AppSense Environment Manager Sp1 and Sp2 Update

user environment management™

AppSense Environment Manager 8.0 SP1

Policy Configuration

- Override Personalization option on Process Start nodes
- Automated Desktop Settings Refresh on Policy Configuration Triggers
- Microsoft App-V support Policy Configuration
- Reusable conditions in reusable nodes
- Performance enhancements

AppSense Environment Manager 8.0 SP1

User Personalization

- Microsoft App-V support for User Personalization
- Discover All Processes mode (passive monitoring)
- Personalization Analysis improvements
- Ability to disable Desktop Settings per Personalization Group
- Ability to move users between Personalization Groups
- Large performance enhancements

AppSense Environment Manager 8.0 SP2

Policy Configuration

- Stop condition for controlling action and node execution
- Run As User Action
- Highlight nodes that make use of reusable nodes
- Exclusions for Registry Hiving actions
- Process name condition to allows wildcards and parameters
- Run Once option
- Auditing action to record user logon duration

AppSense Environment Manager 8.0 SP2

User Personalisation

- Active Directory Site Condition for Personalization Settings
- Delete client side caches
- Global Properties Editor
- Manipulate files in User Personalization cache
- User Created Application White list

AppSense®

Demo

user environment management™



AppSense Environment Manager Policy - Best Practice

user environment management™

AppSense Environment Manager Policy - Goals

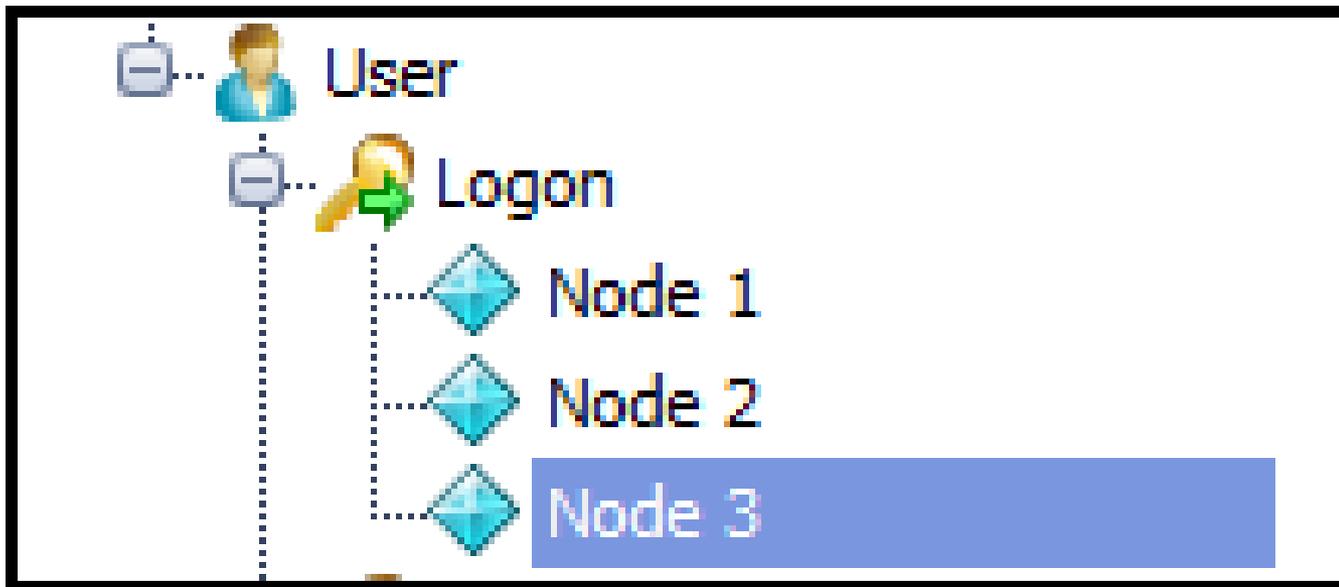
- Reduce user logon times
 - Configuration and Agent run locally on client.
 - XML configuration allow parallel processing
- Centralise management of scripts and group policies
 - Actions typically done in scripts are done via EM
 - GPO Administrative Templates managed in the same console.
 - Version control of policy allows controlled deployments and configuration.
- Provide increased granular control

AppSense Environment Manager Policy - Basics

- Configuration is made up of
 - Nodes - containers for conditions and actions
 - Actions - applied to the user to manipulate their environment.
 - Conditions - control which situations actions should be applied

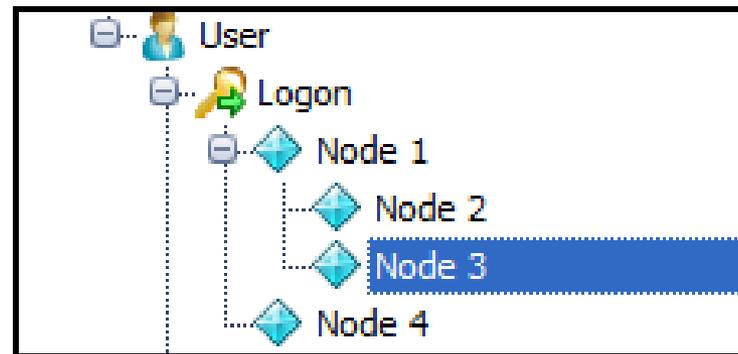
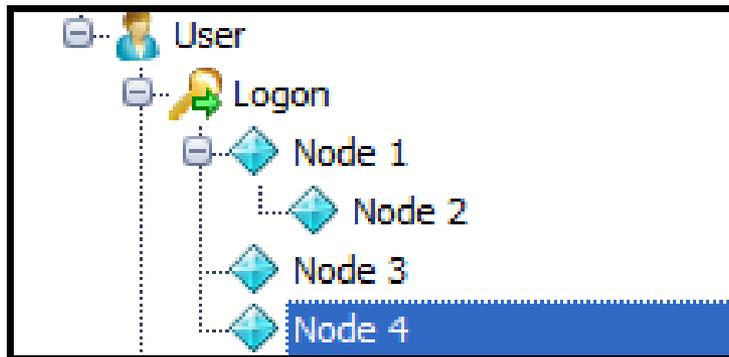
AppSense Environment Manager Policy - Nodes

- Sibling Nodes
 - Run Synchronously



AppSense Environment Manager Policy - Nodes

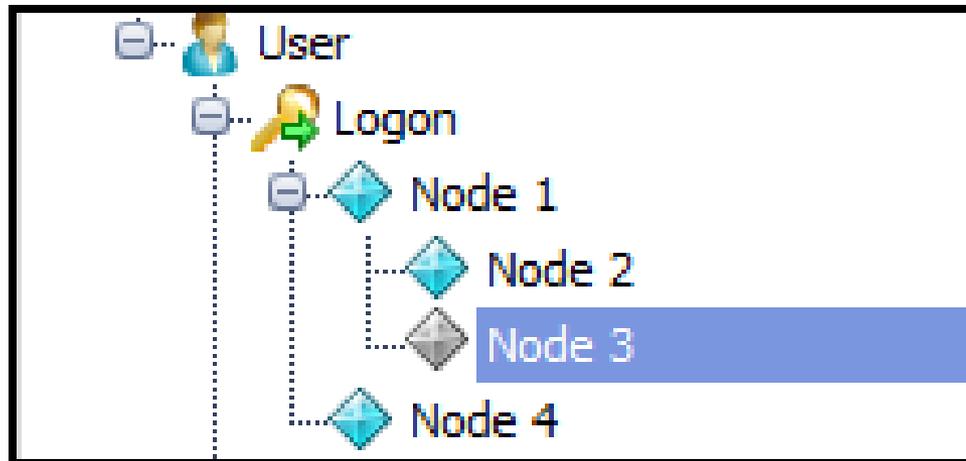
- Parent and Child Nodes
 - Child will not execute until it's parent has completed
 - Stop If Fails is the replacement for the dependency of functionality of v7.x



Actions		
Action	Enabled	Stop if fails

AppSense Environment Manager Policy - Nodes

- Disable Nodes
 - Achieved by “Toggle State” functionality



AppSense Environment Manager Policy - Actions

- Execution Order
 - Actions will be run synchronously

Node 1

Actions

Action	Enabled
Map Drive > M:\ to \\server\transfer	<input checked="" type="checkbox"/>
Create Folder > M:\TESTFOLDER	<input checked="" type="checkbox"/>
Create Key > \Software\Microsoft\Keyboard\Native Media Players\WMP	<input checked="" type="checkbox"/>

- Folder Action will execute after Drive Mapping has completed.
- Drive and Registry action will run synchronously

Node 1

Actions

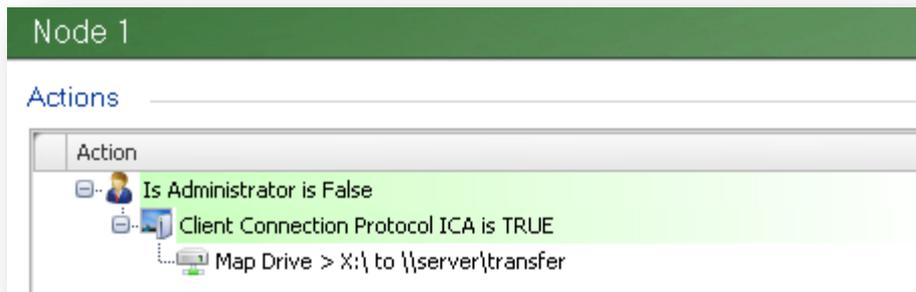
Action	Enabled
Map Drive > M:\ to \\server\transfer	<input checked="" type="checkbox"/>
Create Folder > M:\TESTFOLDER	<input checked="" type="checkbox"/>
Create Key > \Software\Microsoft\Keyboard\Native Media Players\WMP	<input checked="" type="checkbox"/>

AppSense Environment Manager Policy - Conditions

- Conditions are essentially IF statements.
- They be set as a single condition

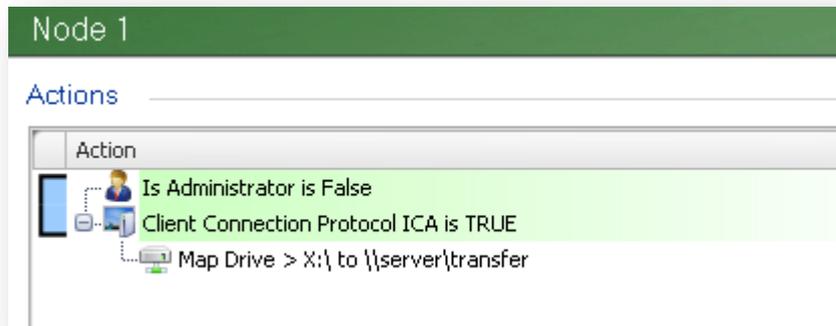


- They be set as an AND condition



AppSense Environment Manager Policy - Conditions

- They can be set as an OR condition



AppSense Environment Manager Policy - Actions + Conditions

- Actions are placed underneath Conditions
 - This makes the action execution dependant on the condition being true.

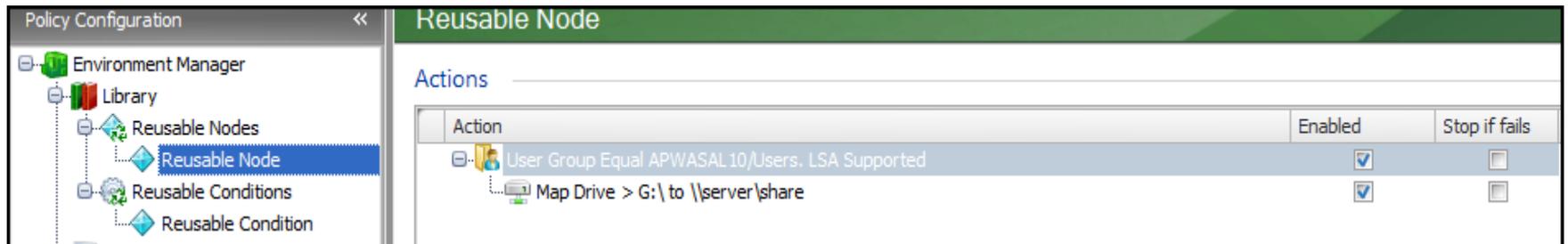
Node 1

Actions

Action	Enabled
 Is Administrator is False	<input checked="" type="checkbox"/>
 Map Drive > M:\ to \\server\transfer	<input checked="" type="checkbox"/>
 Create Folder > M:\TESTFOLDER	<input checked="" type="checkbox"/>
 Computer Name Is Equal To PC0001	<input checked="" type="checkbox"/>
 Create Key > {Software}\Microsoft\Keyboard\Native Media Players\WMP	<input checked="" type="checkbox"/>

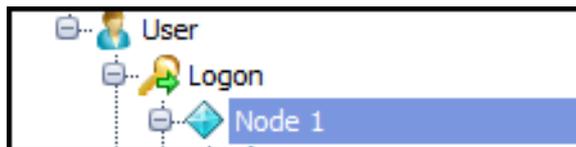
AppSense Environment Manager Policy - Reusable Nodes and Conditions

- Allows you to build up a library of Actions and Conditions within nodes that can be reused.
- Speeds up time to complete configurations.

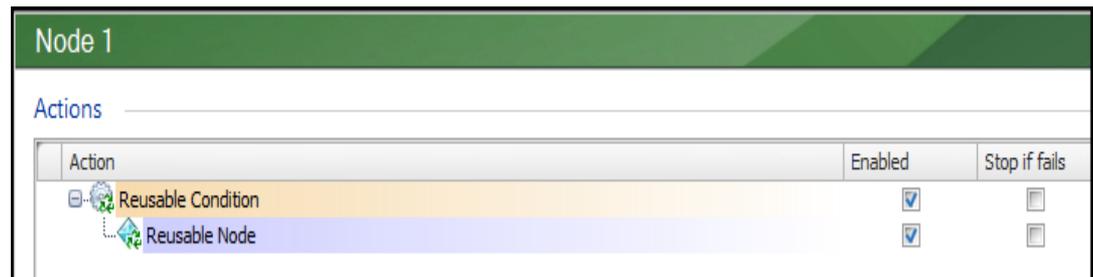


The screenshot shows the 'Policy Configuration' window with a tree view on the left and a 'Reusable Node' configuration pane on the right. The tree view includes 'Environment Manager', 'Library', 'Reusable Nodes', 'Reusable Conditions', and 'Reusable Condition'. The 'Reusable Node' is selected. The configuration pane shows a table of actions:

Action	Enabled	Stop if fails
User Group Equal APWASAL10/Users. LSA Supported	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Map Drive > G:\ to \\server\share	<input checked="" type="checkbox"/>	<input type="checkbox"/>



The screenshot shows a 'User' configuration pane with a tree view on the left. The tree view includes 'User', 'Logon', and 'Node 1'. 'Node 1' is selected.



The screenshot shows the 'Node 1' configuration pane with a table of actions:

Action	Enabled	Stop if fails
Reusable Condition	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reusable Node	<input checked="" type="checkbox"/>	<input type="checkbox"/>

AppSense Environment Manager Policy - Best Practices

- Group like actions together synchronously
 - The more that can be parallel processed the less time for Environment Manager to run.
- Use Environment Manager native actions where possible
 - Relying heavily on custom actions / conditions and execute actions can degrade Environment Manager performance.
- Run Actions only when required
 - Why map a drive for an application at logon when you can do it when the application is started.
 - Removes overhead on the logon process

AppSense Environment Manager Policy - Best Practices

- Where possible used Group Policy ADM's within Environment Manager
 - Reduces the negative effect GPO's can have on logon by being delivered by Active Directory
- Copy Shortcuts rather than creating them.
 - Reduces Environment Manager execution time.
- Make use of Environment Variables
 - Makes your configuration portable
- Make use Session reconnect within XenApp
 - Can evaluate your users when they move locations.

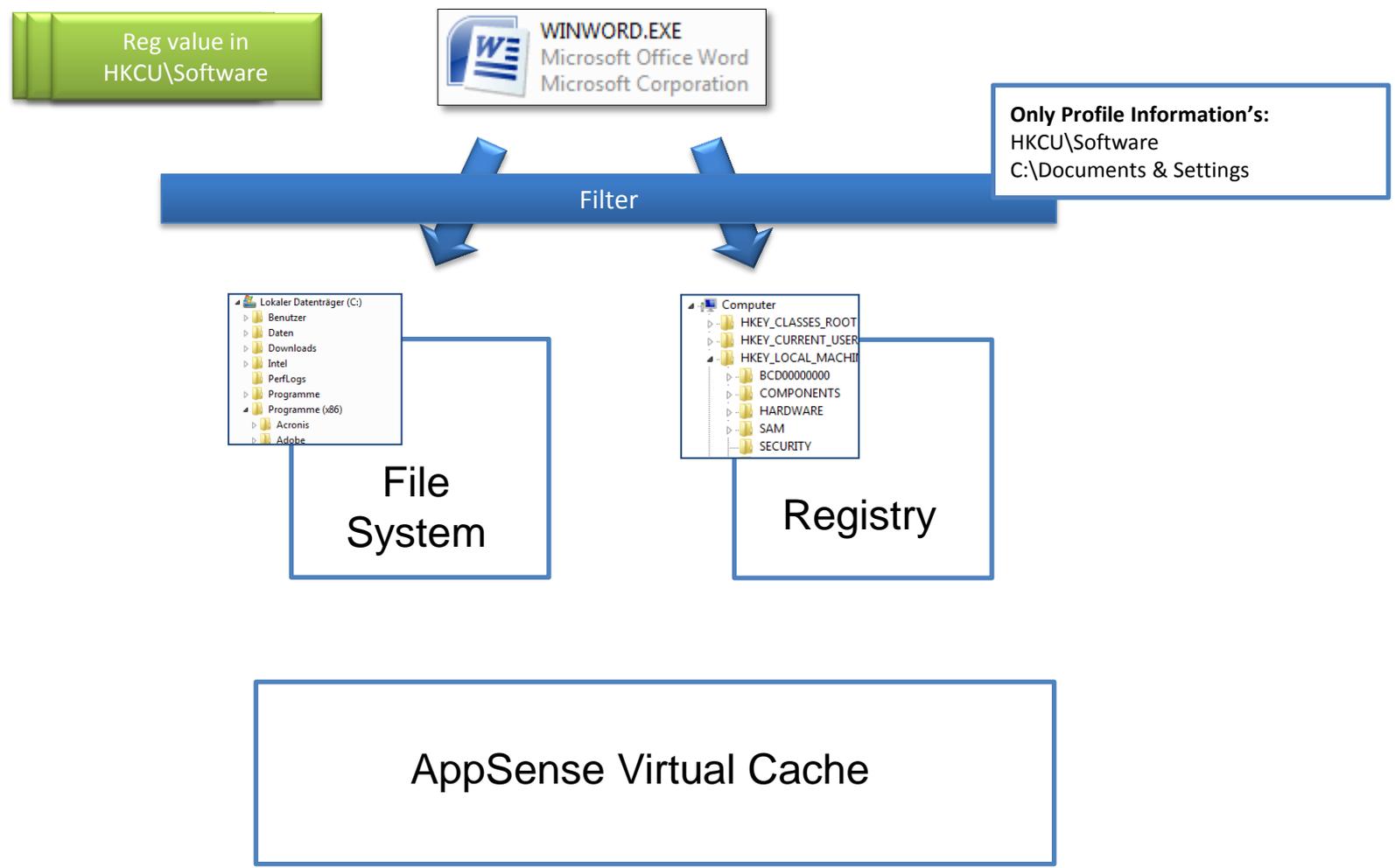
AppSense Environment Manager Policy - Best Practices

- Don't use custom conditions within Reusable Conditions.
 - Environment Manager will evaluate the condition twice in this configuration.

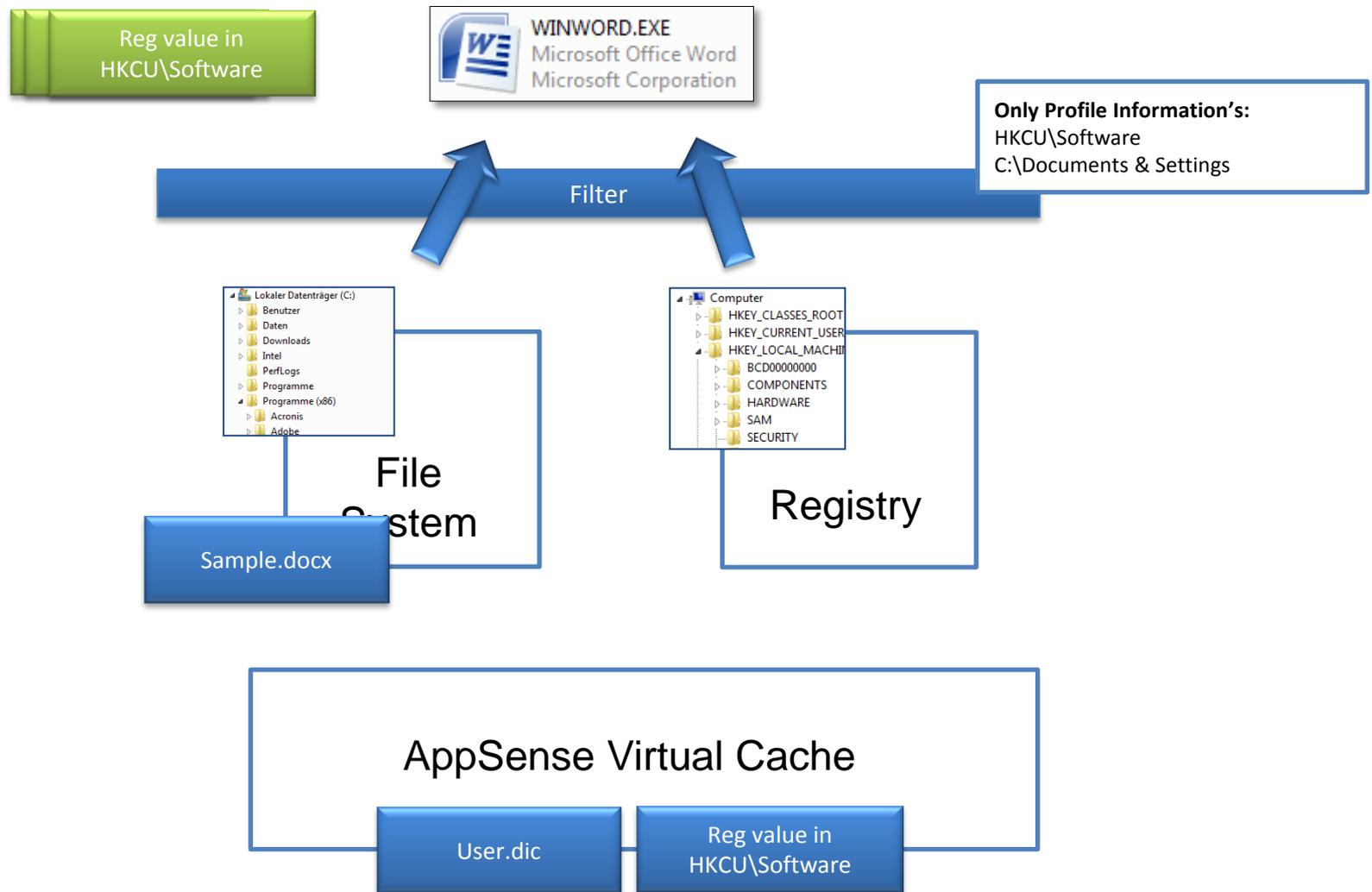
How works User Personalization

[New Pre Sales Doc\Tech Ref EMPS Transactions.docx](#)

How works User Personalization (write)

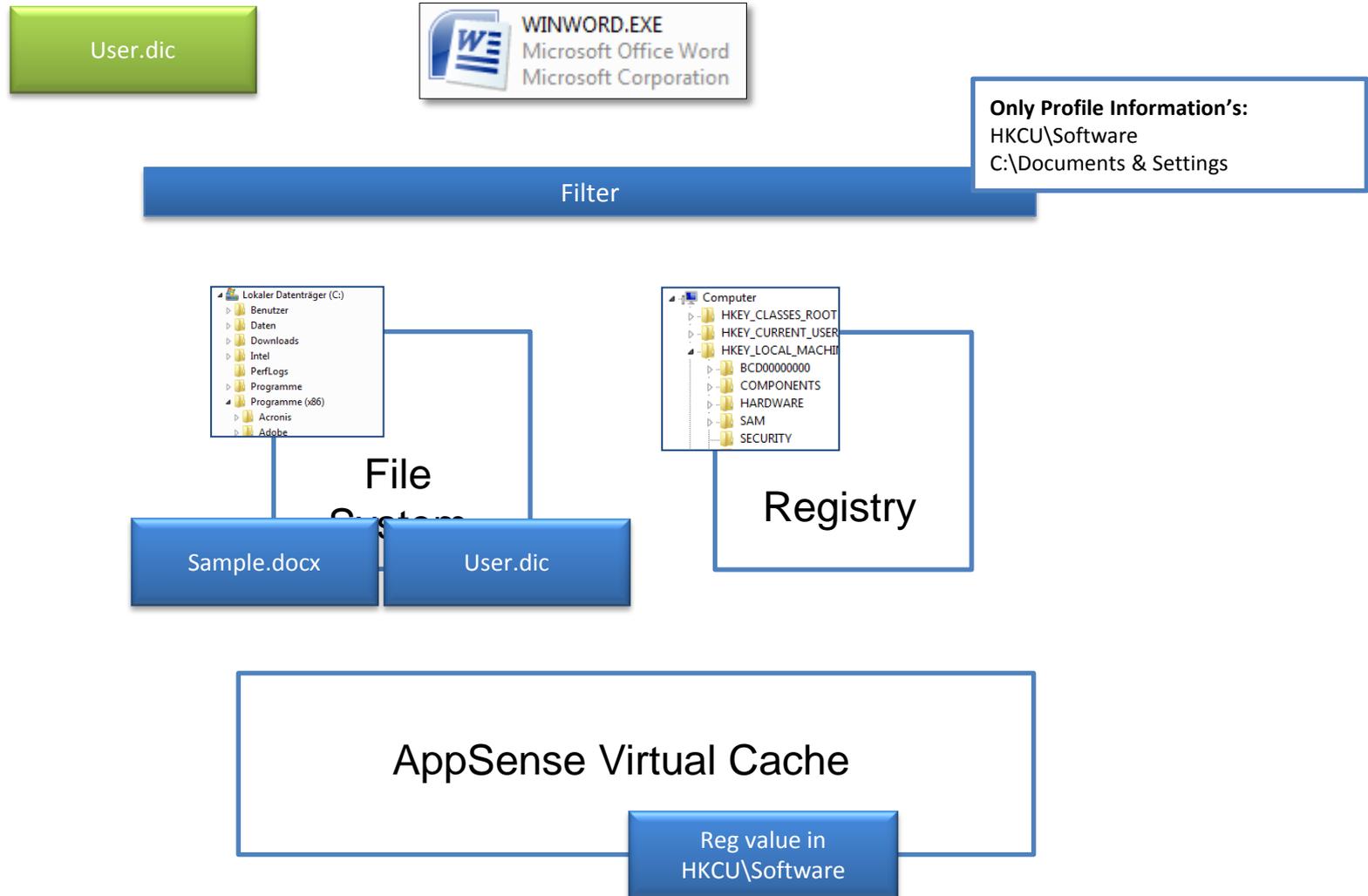


How works User Personalization (read)



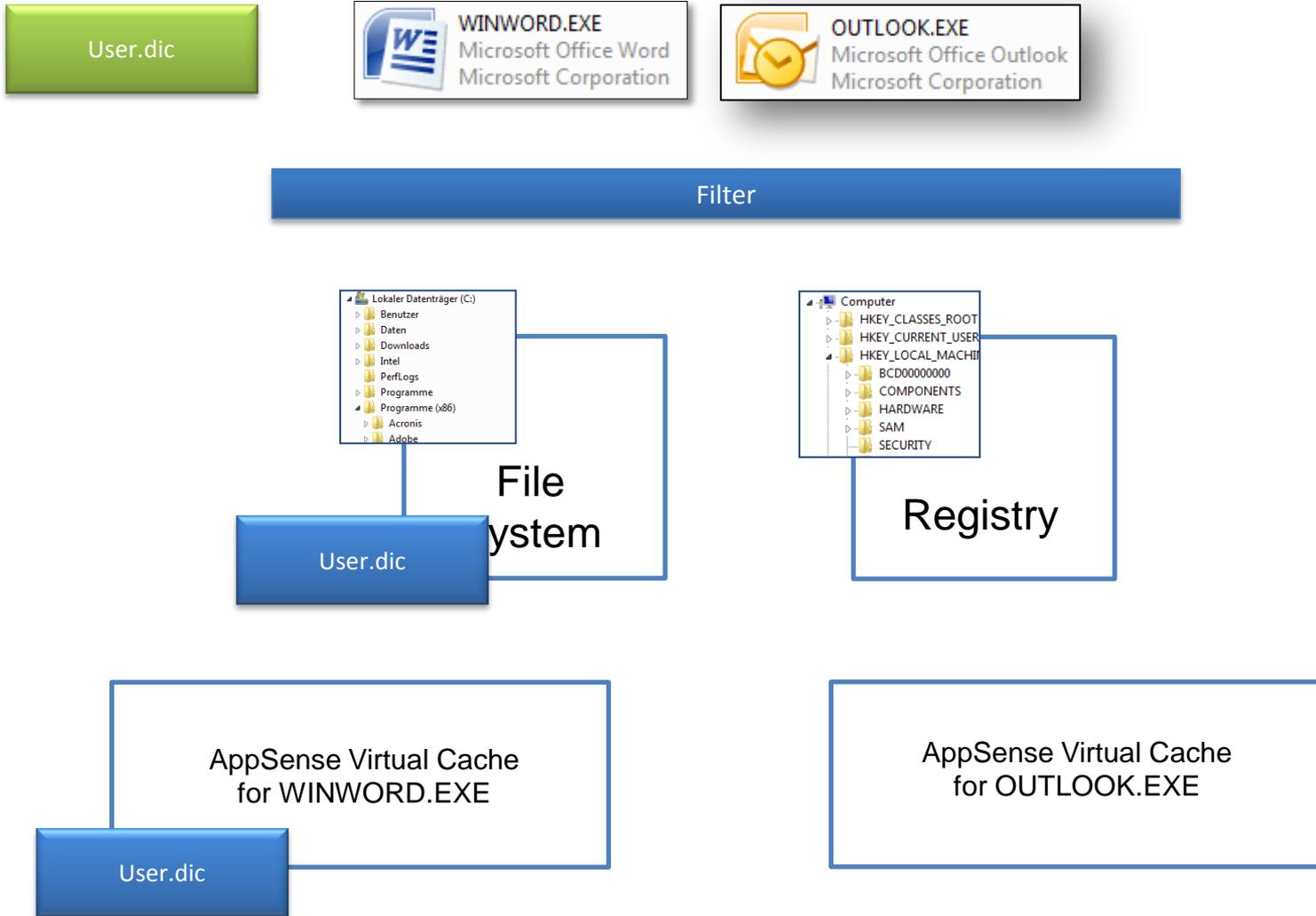
How works User Personalization (read)

Missing file in AppSense Virtual Cache



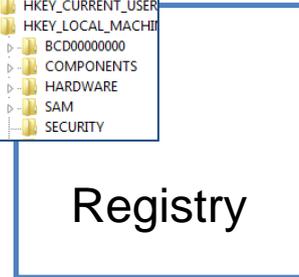
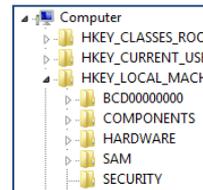
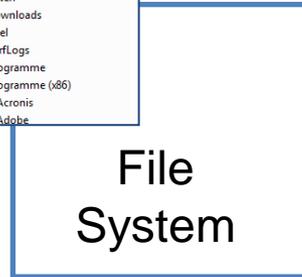
How works User Personalization (read)

Two Application & One User Setting File



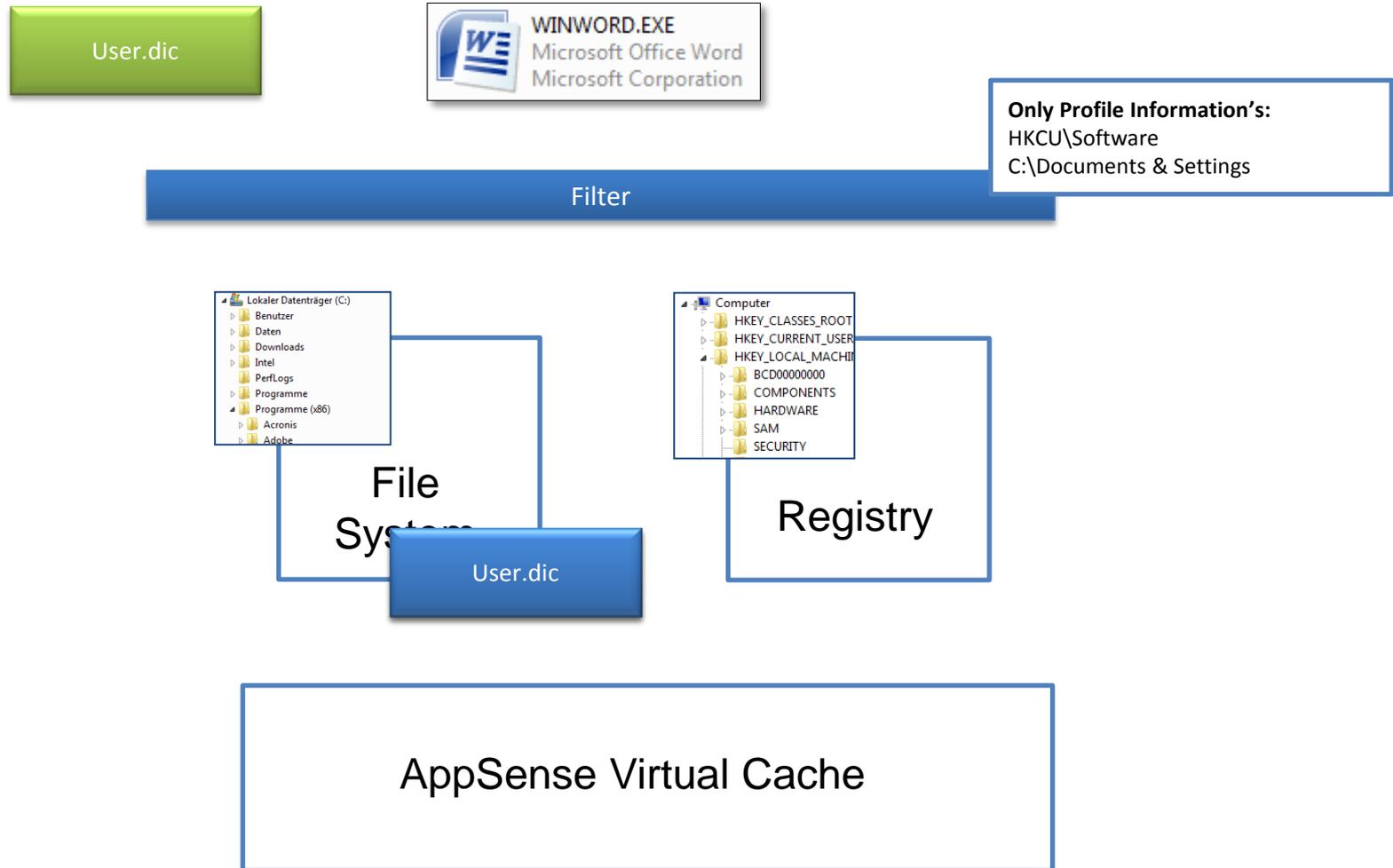
How works User Personalization (read)

Two Application & One User Setting File (Application Group)



How works User Personalization (Migration Mode)

During Read Process





AppSense Environment Manager Personalisation - Best Practice

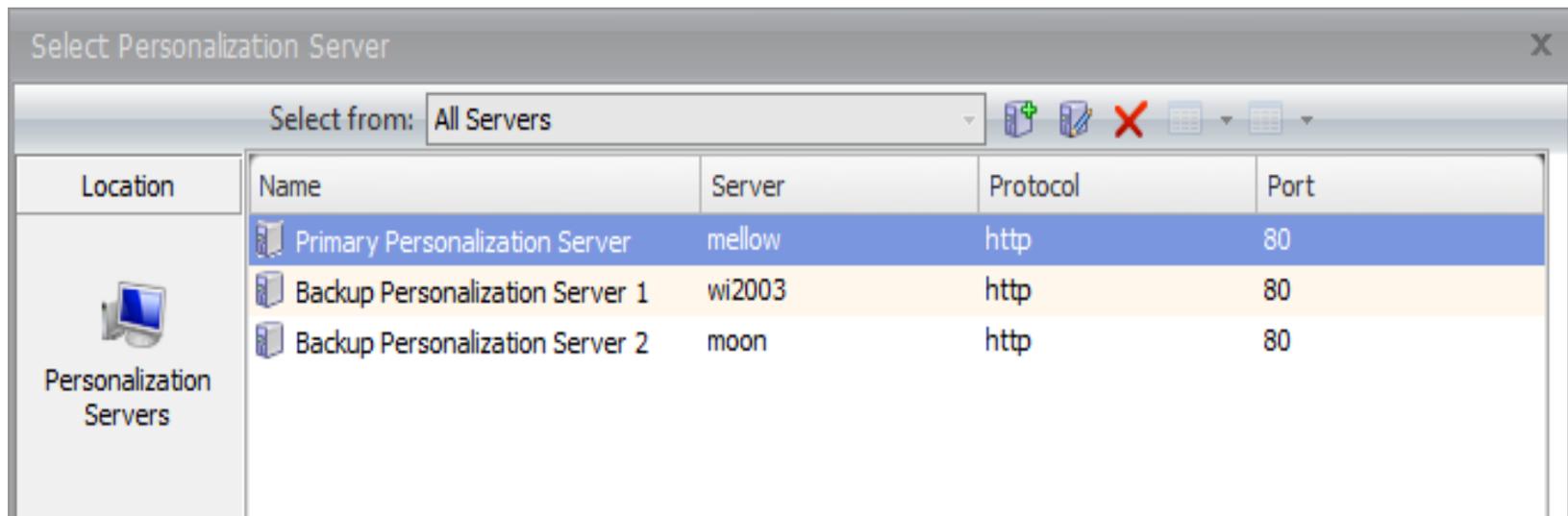
user environment management™

EM Personalisation Server - Best Practice

- Creating Personalization Groups
- Personalization Group Settings
- Manually creating Applications and Application Groups
- Discover and convert Applications to Whitelist
- White Listing Applications
- Desktop Settings
- Outlook Best Practice
 - Reg Keys, Desktop Settings and Application Grouping
- When to use offline mode

Enabling User Personalization

- Single or multiple Personalization Servers can be added
- It is recommended multiple Personalization Servers are added here (where applicable) for failover purposes:



Enabling User Personalization

- The list of Personalization Servers is queried from the top down
- If communication with the 1st Personalization Server in the list is successful, the *ProfileConfig.xml* file is downloaded via this Server
- If the 1st Personalization Server in the list is unavailable then the next Server in the list is contacted until successful communication is achieved
- If the list is exhausted then the *ProfileConfig.xml* file is not downloaded and no Personalization will take place
- It is recommended that the following auditing event be enabled to monitor this:

Event 9661 - Timeout Communicating with Personalization Server

Personalization Group Usage

- *Personalization Groups* allows different personalization settings to be applied to users based on membership rules
- A user may be a member of more than one Personalization Group
 - The user is assigned to the first Personalization Group in the list where the membership rule is valid
 - Personalization Groups can be ordered in the list by means of the *Move Up* and *Move Down* Personalization ribbon options

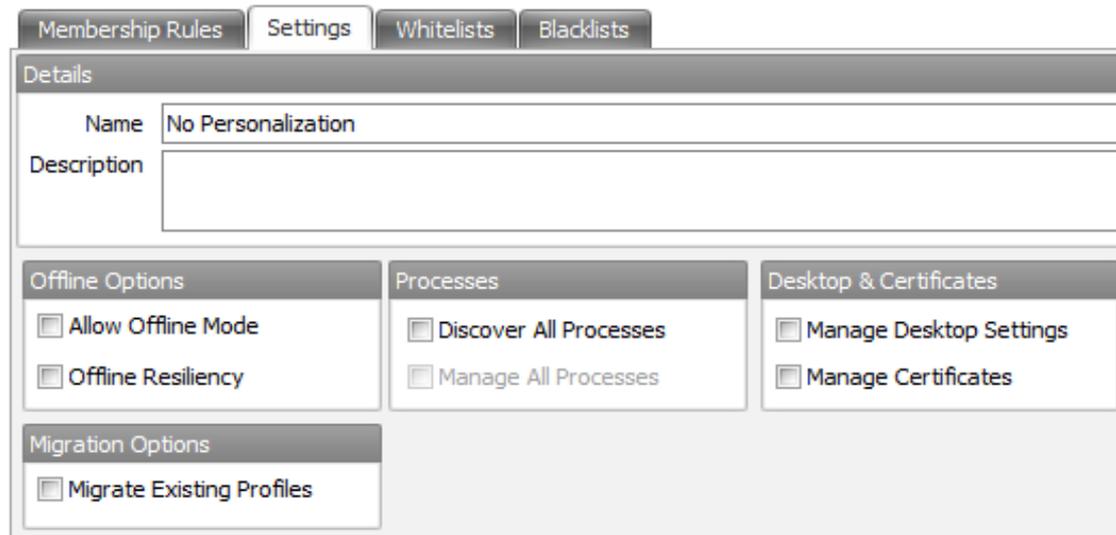


Personalization Group Usage

- It is recommended that Personalization Groups be ordered in terms of importance to ensure that your users are assigned to the more relevant Personalization Group
- The *Default Users* Personalization Group is used as the catch-all group should none of the membership rules be passed in any of the other Personalization Groups
- This is *always* located at the bottom of the Personalization Groups list and cannot be moved up or down

Excluding Users from User Personalization

- To exclude a user from User Personalization each option on the Settings tab of the chosen Personalization Group will need to be disabled:



The screenshot shows the 'Settings' tab of a Personalization Group configuration. The 'Name' field is set to 'No Personalization'. Below the 'Details' section, there are three columns of settings, all of which are currently disabled (checkboxes are unchecked):

Offline Options	Processes	Desktop & Certificates
<input type="checkbox"/> Allow Offline Mode	<input type="checkbox"/> Discover All Processes	<input type="checkbox"/> Manage Desktop Settings
<input type="checkbox"/> Offline Resiliency	<input type="checkbox"/> Manage All Processes	<input type="checkbox"/> Manage Certificates

Below these columns is a 'Migration Options' section with one setting:

Migration Options
<input type="checkbox"/> Migrate Existing Profiles

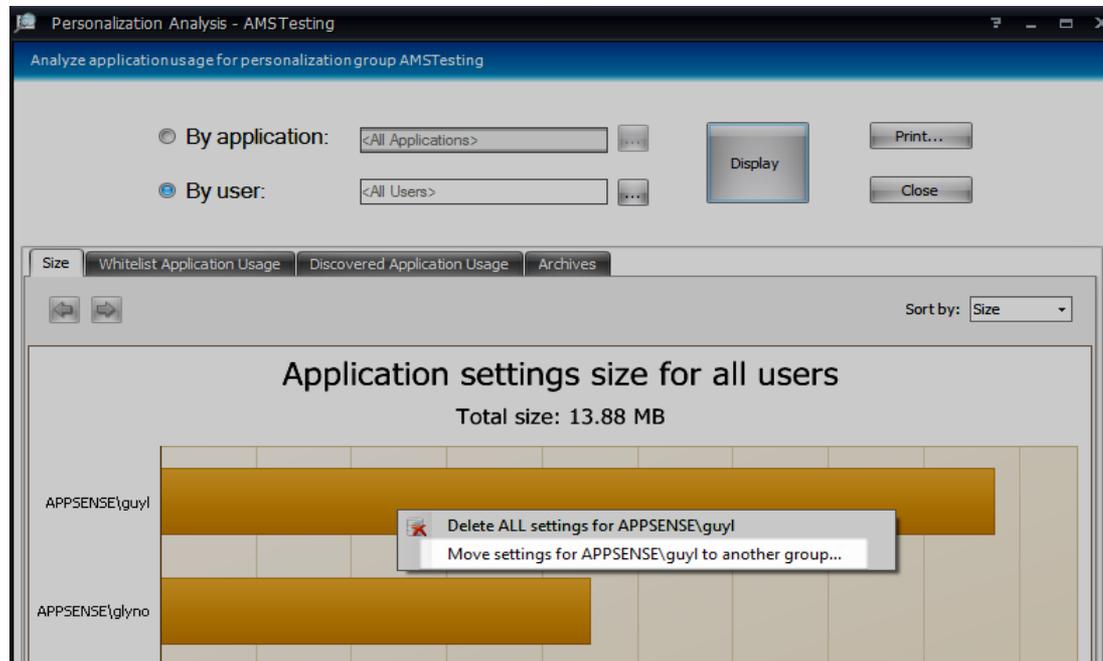
- You must then add the relevant membership rules to the Personalization Group to include the users or computers you wish to exclude

Moving Users Between Personalization Groups

- Personalization settings cannot *currently* be shared between Personalization Groups
- If you need to move a user's settings to another Personalization Group this can now be done via Personalization Analysis
- This is achieved by running up a Personalization Analysis report, By user, from either the *Size*, *Whitelist Application Usage* or *Discovered Application Usage* reports

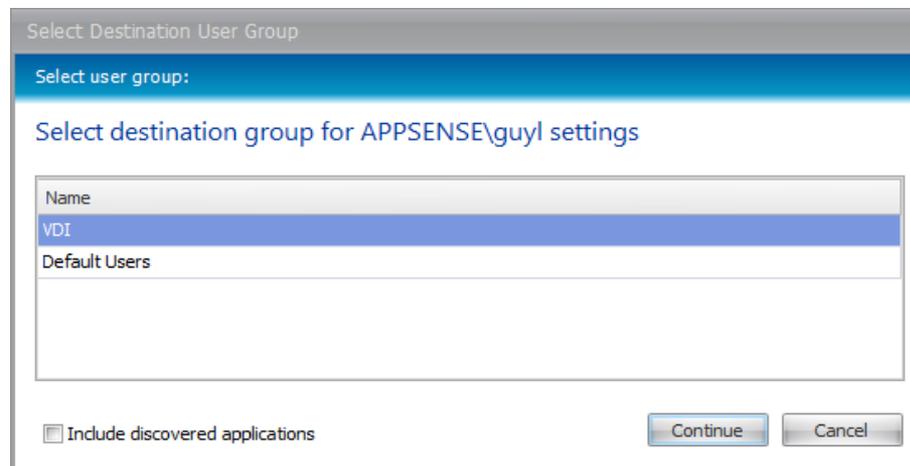
Moving Users Between Personalization Group

- Select the user you wish to move
- Right click and choose *'Move settings for <user> to another group...'*:



Moving Users Between Personalization Groups

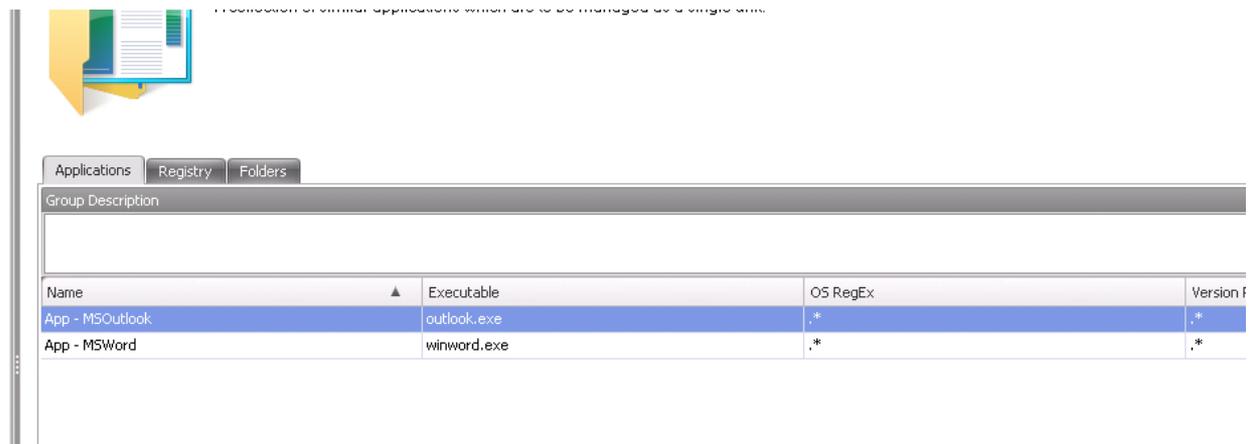
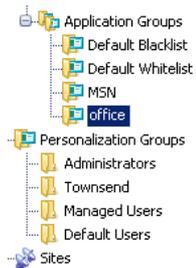
- This will prompt the administrator to choose another available group to move the chosen user's personalization settings to:



- *'Include discovered applications'* (off by default) moves discovered applications too
- It is recommended this also be checked

Personalization Server - Application Groups

- Placing applications into the same group means that applications can be managed and streamed as one.
- Very useful to Group Outlook and Winword together as they are closely linked
- When the user launches Outlook.exe, both Outlook and Word profile settings will be pulled down to the client
- Disadvantage means that these applications must be “rolled back“ together
- Examples of this are:
 - Internet Explorer and IEUser.exe
 - MSN Messenger and SimpLite



Personalization Server - Desktop Settings

- Desktop Settings

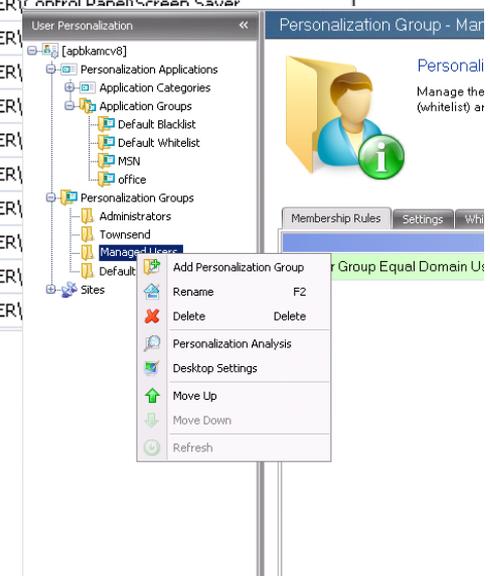
Keys are imported to the real registry at logon, and exported from the real registry at logoff.

They contain all the information regarding the desktop, wallpaper, mouse keys, keyboard settings, etc.

Keys listed must be present on the OS before these can be imported.

Desktop settings can be accessed and viewed through the Profile Analysis tool

Name ▲	Key
Accessibility	HKEY_CURRENT_USER\Control Panel\Accessibility
Appearance	HKEY_CURRENT_USER\Control Panel\Appearance
Colors	HKEY_CURRENT_USER\Control Panel\Colors
Current	HKEY_CURRENT_USER\Control Panel\Current
Cursors	HKEY_CURRENT_USER\Control Panel\Cursors
Custom Colors	HKEY_CURRENT_USER\Control Panel\Custom Colors
Desktop	HKEY_CURRENT_USER\Control Panel\Desktop
Keyboard	HKEY_CURRENT_USER\Control Panel\Keyboard
Language	HKEY_CURRENT_USER\Control Panel\Language
Mouse	HKEY_CURRENT_USER\Control Panel\Mouse
Plus!	HKEY_CURRENT_USER\Software\Microsoft\Plus!
Screen Saver	HKEY_CURRENT_USER\Control Panel\Screen Saver
Screen Saver.3DFlyin...	HKEY_CURRENT_USER\...
Screen Saver.3DPipes	HKEY_CURRENT_USER\...
Screen Saver.Bezier	HKEY_CURRENT_USER\...
Screen Saver.Marquee	HKEY_CURRENT_USER\...
Screen Saver.Mystify	HKEY_CURRENT_USER\...
Screen Saver.Stars	HKEY_CURRENT_USER\...
Screen Savers	HKEY_CURRENT_USER\...
Theme Manager	HKEY_CURRENT_USER\...
Themes	HKEY_CURRENT_USER\...



AppSense Personalization Server - Configuration

- Personalization Group - Settings

The screenshot shows the configuration interface for a Personalization Group. At the top, there are four tabs: "Membership Rules", "Settings", "Whitelists", and "Blacklists". The "Settings" tab is selected. Below the tabs is a "Details" section with a "Name" field containing "ProfileManagement" and a "Description" field. Below the details are three panels of settings:

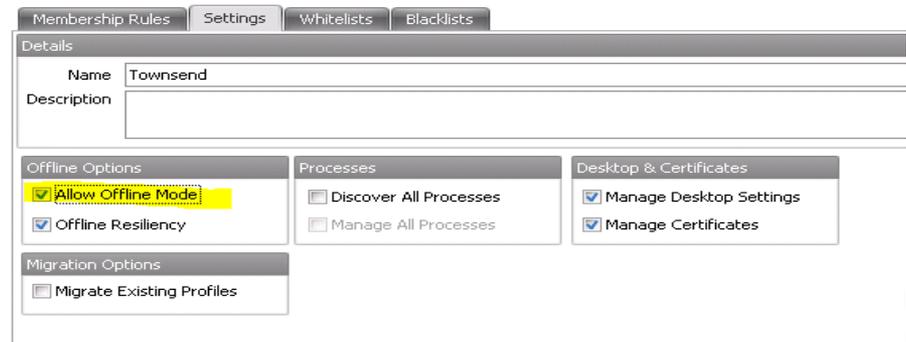
- Offline Options:**
 - Allow Offline Mode
 - Offline Resiliency
- Processes:**
 - Discover All Processes
 - Manage All Processes
- Desktop & Certificates:**
 - Manage Desktop Settings
 - Manage Certificates

Below these panels is a "Migration Options" section with one setting:

- Migrate Existing Profiles

Allow Offline Mode

- *Allow Offline Mode* is off by default
- This enables mobile users to still have access to their personalization settings whilst off the corporate network
- By enabling this option, a local copy of the virtual personalization cache is retained on the managed endpoint device when the user logs off
- It is recommended this option *only* be switched on for managed endpoints that are mobile, i.e. laptops, notebooks etc..



Offline Resiliency

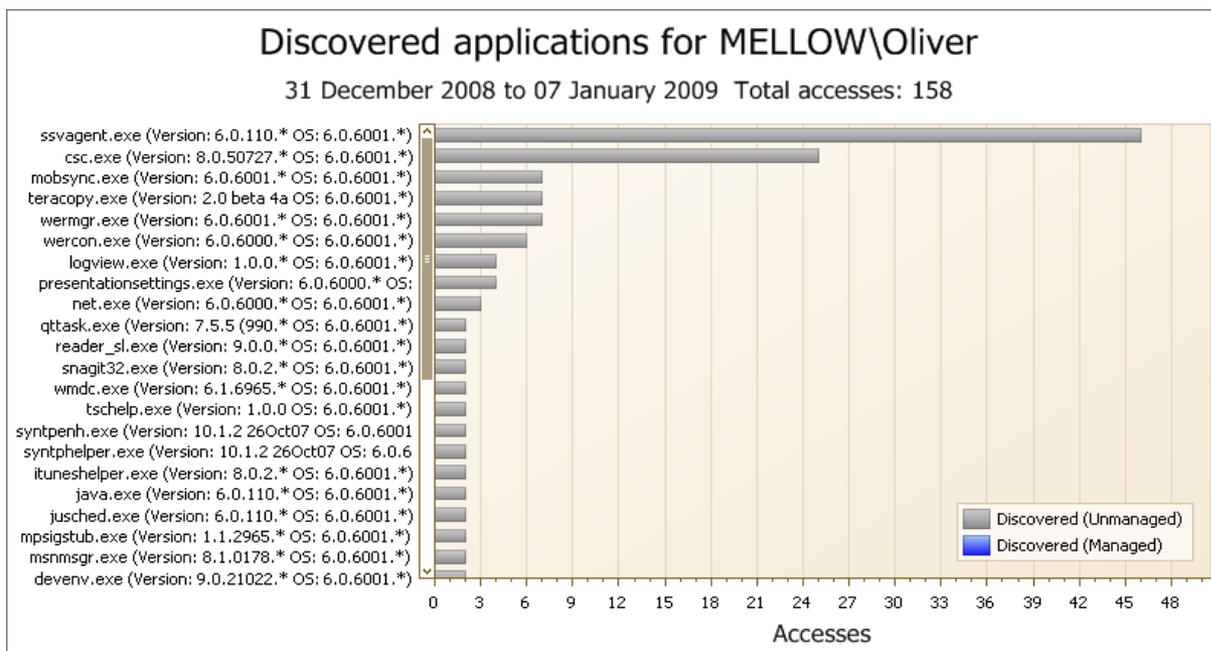
- *Offline Resiliency* is on by default
- It is recommended this setting remains enabled
- Ensures if communication between the managed endpoint and the database is lost, synchronization of personalization data is re-attempted until communication is re-established

Discover All Processes

- *Discover All Processes* is off by default
- A ‘passive monitoring’ mode which allows managed endpoints to be monitored for launched applications
- Each application a user launches is ‘discovered’ and recorded so that, at a later date, it can either be added to a whitelist, blacklist or deleted
- It is recommended that ‘Discover All Processes’ is switched on so that applications being used by users can be identified

Discover All Processes

- Personalization Analysis reports can be run that show applications discovered by the 'Discover All Processes' option:



- It is recommended that discovered applications are then converted to Whitelisted applications where required.

Manage All Processes

- *Manage All Processes* is **off** by default
- The '*Manage All Processes*' option is now a sub option of the '*Discover All Processes*' option and can *only* be enabled if '*Discover All Processes*' is also enabled
- It is **not** recommended that this option be used in a live environment for long periods of time
- It **is** recommended that this option be used in a pilot environment to identify applications and also prove that they can be personalized without issue

Whitelist and Blacklist

- It is recommended that a Whitelist be utilized along with ‘Discover All Processes’
- This allows only a specific set of user applications to be personalized
 - Add user configurable applications to the whitelist such as MS Office Applications, Web Browsers, instant messaging applications etc..
- Any applications added to a Blacklist will **not** be managed
 - Exclude ‘utility’ applications such as compression software, anti-virus and system tools from being personalized.

Personalization Server - Creating Applications

Using .* means that all OS types can be used EM will capture all instances of this app across multi platform

Application Registry Folders

Application

Name App - MSWord

Executable winword.exe

Operating System Regular Expression

Application Version Regular Expression

History

Created By APPSENSEBK\Administrator

Created Date 24/11/2008 15:25:24

Last Modified By APPSENSEBK\Administrator

Modified Date 05/03/2009 15:15:30

Using a .* will allow all versions of the application to be captured in the same profile.

If you want to manage different versions of an application separately, then use the boxes to edit the .*

Application Groups

- Application Groups are recommended when one application relies on another applications settings
- Examples of this are:
 - Internet Explorer and IEUser.exe
 - MSN Messenger and SimpLite

Manage Desktop Settings

- *Manage Desktop Settings* is on by default
- Globally configured from *Desktop Settings* on the Tools Ribbon
- Now enabled on a per Personalization Group basis
- Recommended *Manage Desktop Settings* only be enabled for Personalization Groups for which the desktop settings need to roam

Manage Certificates

- *Manage Certificates* is on by default
- Enabling this option instigates '*profile state emulation*' whereby the operating system is fooled into thinking the user is logged in with a roaming profile
- It is recommended that this option be disabled on Personalization Groups where the members of that group are not utilizing a mandatory profile

Migrate Existing Profiles

- *Migrate Existing Profiles* is off by default
- *Migrate Existing Profiles* utilizes a ‘Virtualize-on-Read’ technique
- Recommended when:
 - migrating users from local or roaming profiles
 - migrating from one OS to another
- This option should be disabled once all users have launched each application to be personalized
 - This can be ascertained from the Whitelist Application Report

Sites

- For organizations with concentrations of geographically dispersed users
- The primary site should be installed where the largest user base is located
 - This becomes the *Default Site* listed under the *Sites* list
- Branch sites can be added by installing Personalization Servers at other locations
- Users retrieve their *ProfileConfig.xml* from the first Personalization Server contactable as detailed in the configuration.aemp file
- Subsequent synchronizations will then occur via the designated *Site* based on the membership rules assigned to the *Sites*

Database Replication & Synchronization

- Where multiple databases are required (for failover support or to support geographically dispersed locations) replication can be configured
 - See the *AppSense Environment Manager Administration Guide*
- When configured this replication will occur once per day by default
- It is recommended that the ‘*Synchronize Site Databases*’ option be utilized if replication between databases is required immediately:



Best Practice Microsoft Outlook

- “Send To” and “Mail Configuration in Control Panel”

Make sure the following key is present in either the default.dat or the NTUser.MAN that the user is using when they logon

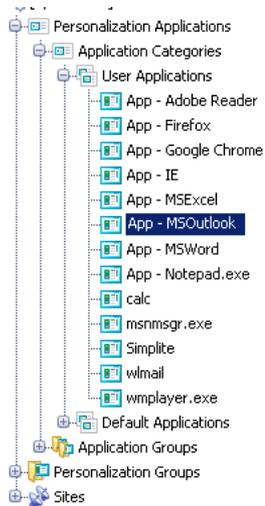
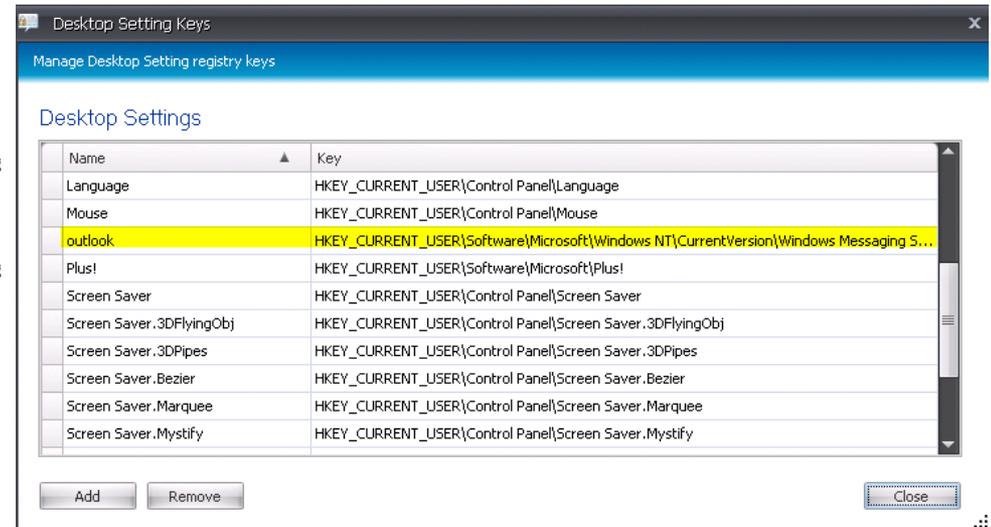
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem
- This would just be the KEY with NO DATA in it

- Tell AppSense not to vitalize the key required by both Outlook

- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem key should be added as an exclusion on the Outlook.exe process under the personalised Applications section.

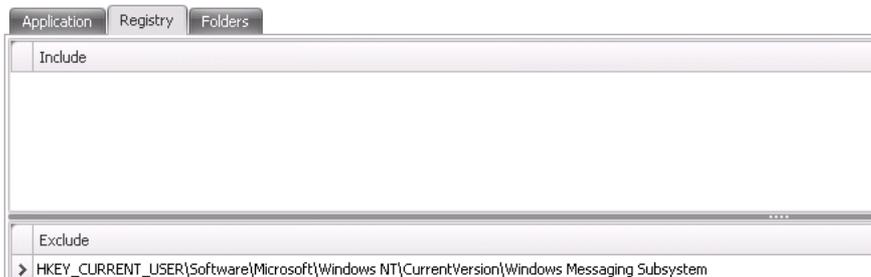
- Then tell AppSense to import and export the same key into the real registry and logon and logoff

- This is achieved by Adding HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem in the “desktop settings” section of the EM Personalisation server console. This key will in effect be delivered along with any other desktop settings such as certs, wallpaper etc



Application

Details of an application which can be managed at the client computer.

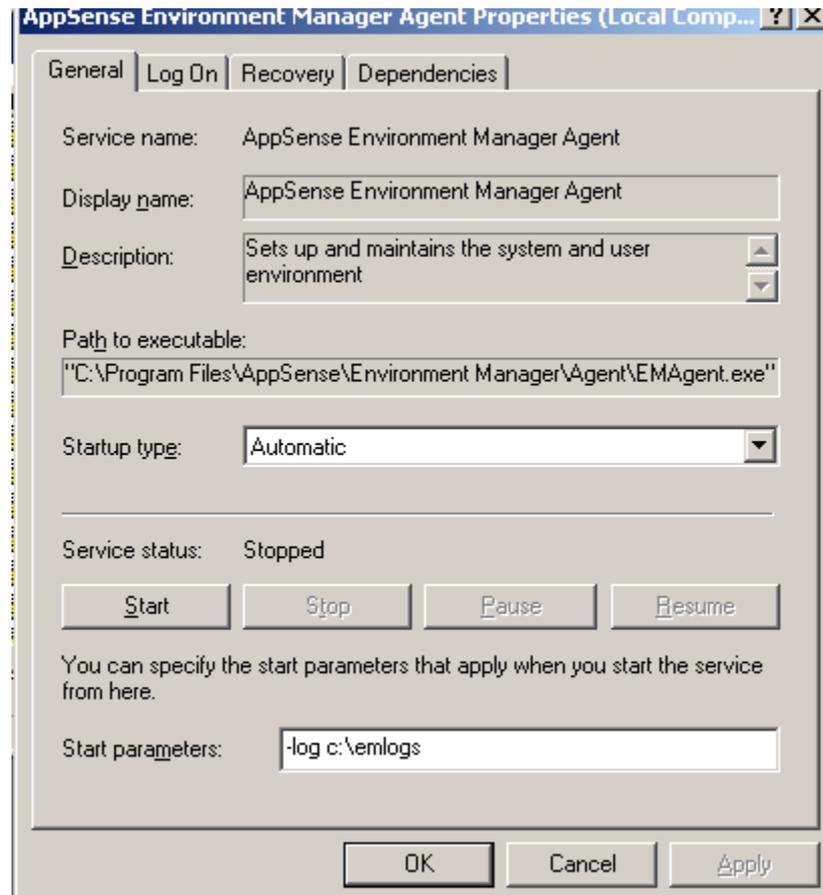


Troubleshooting EM policy

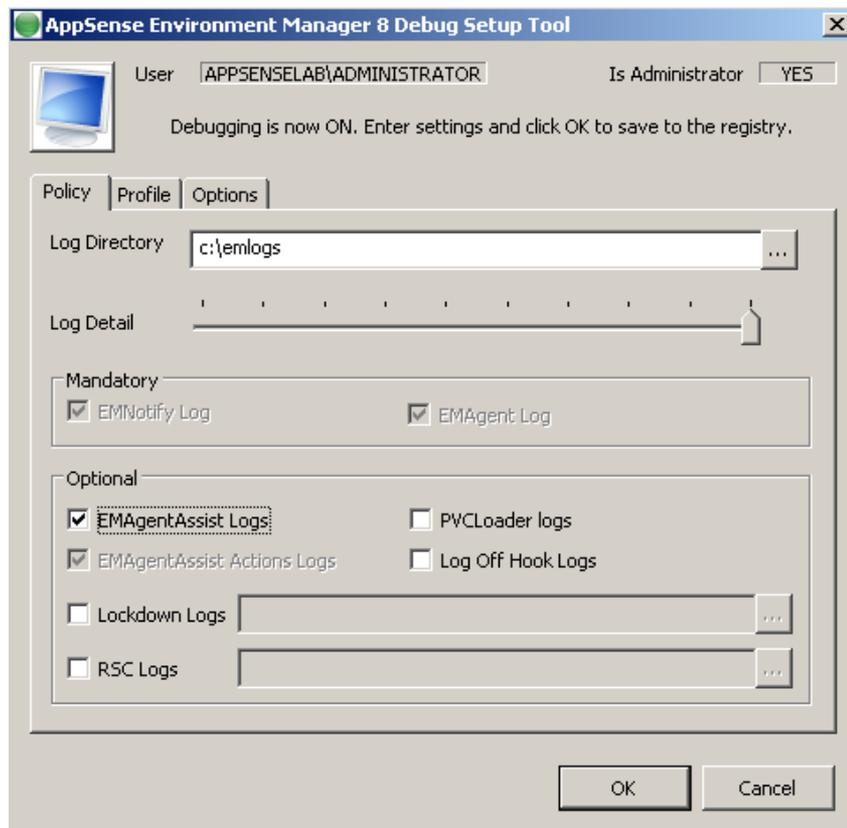
Troubleshooting

- Check licence!
- Confirm machine has been deployed to.
- Confirm correct packages
- Confirm “use latest is enabled”
- Check add remove programs on client machine
- Check Task Manager on client machine and confirm EMAgent is running
- Check the services tab and make sure that both AppSense Environment Manager Agent and EM Notify Services are enabled and started.
- Check Task Manager whilst logged on as the user - There should be at least 2 EMAgent Assist running - one for the system, one per session
- Place “test” - RUN CALC.exe in policy

Enable Logging

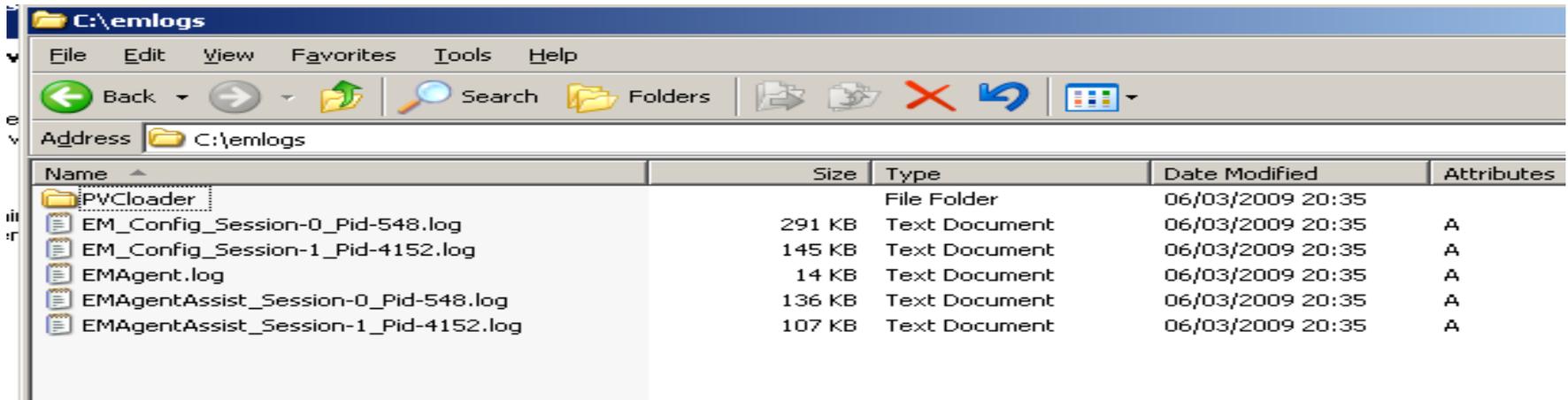


EM Logger tool



- Use the tool when troubleshooting Machine Start Up Actions as it sets registry keys which will not be forgotten post reboot
- Always enabled EMAgentAssist logs

Collect the logs

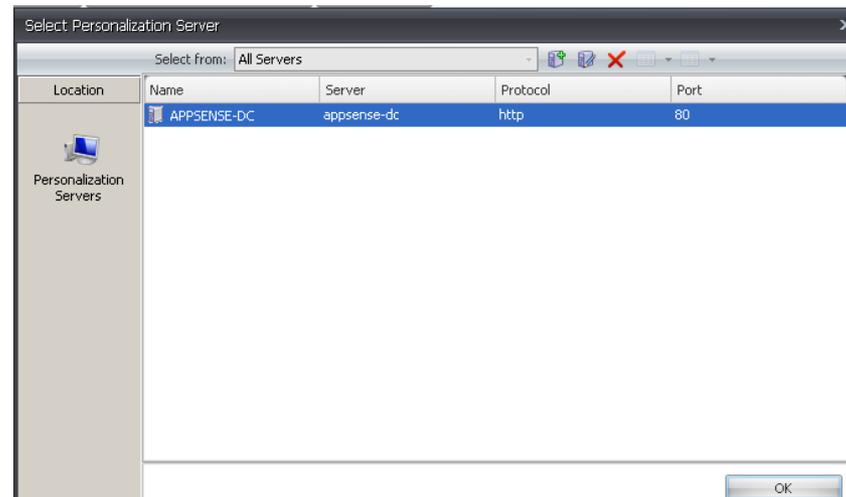


- Match the user to the session ID and look into the EM Agent Config logs
- Use the EM Log viewer to analyse errors
- Run reports to see what the timings of logon are.

Troubleshooting EM policy

Personalisation

- Confirm you have enabled the Personalization Server in the Policy side of the configuration



Confirm you have at least one site

The screenshot displays the AppSense Management Server interface. At the top, the browser address bar shows "EMDEMOCONFIG on http://appsense-dc/ManagementServer - Environment Mana". The interface has a navigation bar with "Home", "Personalization", and "Tools" tabs. Below this is a toolbar with various icons for actions like "Connect", "Disconnect", "Move Up", "Move Down", "Add Application Group", "Add Personalization Group", "Add Server", "Add Site", "Delete", "Rename", and "Refresh".

The main content area is titled "User Personalization" and features a tree view on the left. The tree view shows a hierarchy under "[APPSENSE-DC]":

- Personalization Applications
- Personalization Groups
 - EM Test Group
 - Administrators
 - Default Users
- Sites
 - Default Site
 - APPSENSE-DC

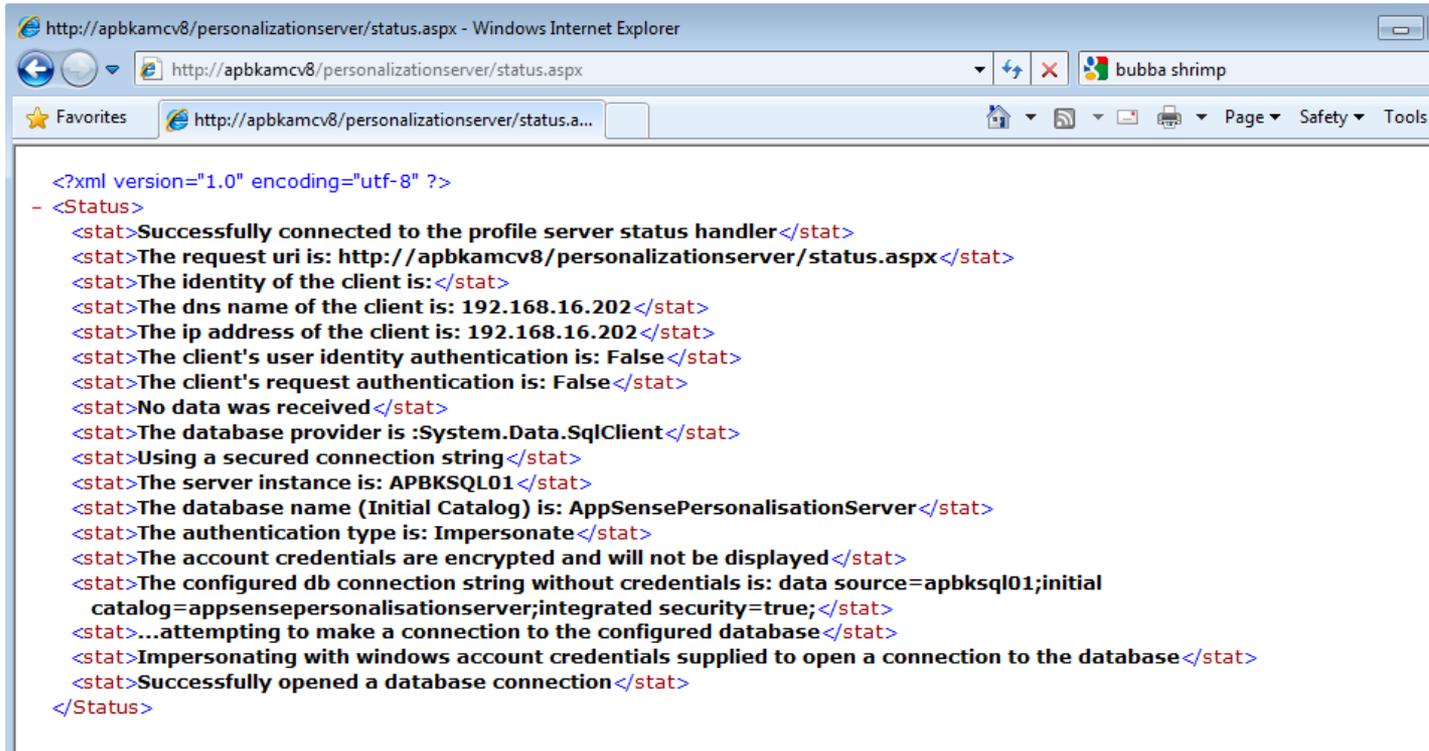
On the right side of the "User Personalization" section, there is a blue informational box with the following text:

User Personalization
User Personalization provides the ability to capture the changes that users make to the application and also desktop settings on a per session basis. These changes are then stored in a database associated with the user from wherever they log on, regardless of operating system or delivery mechanism.

[Connect to Personalization Server](#)
Get started by connecting to a Personalization Server

How to test the Personalisation Server Connection

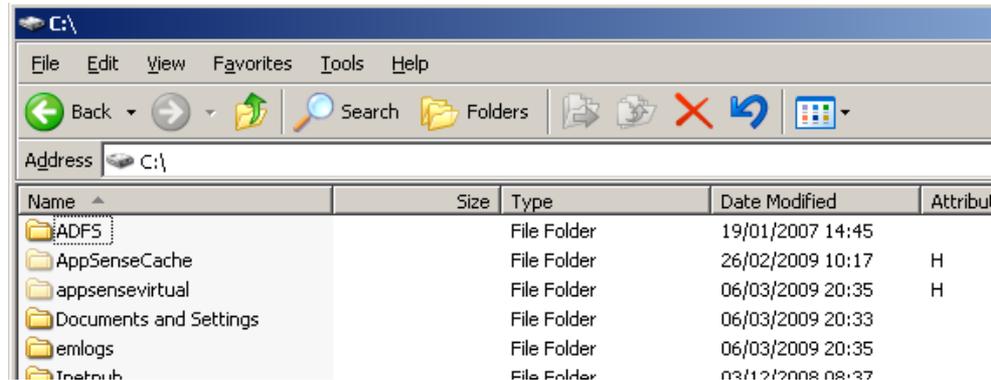
- <http://machinename/personalizationserver/status.aspx>



```
<?xml version="1.0" encoding="utf-8" ?>
- <Status>
  <stat>Successfully connected to the profile server status handler</stat>
  <stat>The request uri is: http://apbkamcv8/personalizationserver/status.aspx</stat>
  <stat>The identity of the client is:</stat>
  <stat>The dns name of the client is: 192.168.16.202</stat>
  <stat>The ip address of the client is: 192.168.16.202</stat>
  <stat>The client's user identity authentication is: False</stat>
  <stat>The client's request authentication is: False</stat>
  <stat>No data was received</stat>
  <stat>The database provider is :System.Data.SqlClient</stat>
  <stat>Using a secured connection string</stat>
  <stat>The server instance is: APBKSQL01</stat>
  <stat>The database name (Initial Catalog) is: AppSensePersonalisationServer</stat>
  <stat>The authentication type is: Impersonate</stat>
  <stat>The account credentials are encrypted and will not be displayed</stat>
  <stat>The configured db connection string without credentials is: data source=apbksql01;initial
  catalog=appsensepersonalisationserver;integrated security=true;</stat>
  <stat>...attempting to make a connection to the configured database</stat>
  <stat>Impersonating with windows account credentials supplied to open a connection to the database</stat>
  <stat>Successfully opened a database connection</stat>
</Status>
```

How to test the Personalisation Server Connection

- Check the client machine and look for the ProfileConfig.XML
 - C:\AppSenseCache\SID\ProfileConfig.XML



Check the PVC has loaded..

PVCload_s0-pid6108-t20995281.log - Notepad

File Edit Format View Help

```
T3940 20995281 Logging started
T3940 20995281 Acquiring config
T3940 20995281 Sending cfg req (85 bytes), "C:\WINDOWS\system32\notepad.exe"
T3940 20995437 Got cfg reply (0 bytes)
T3940 20995437 Process NOT managed by PMM
T3940 20995437 All done
T3940 20995437 PVCloader all done
```



Architecture and Scalability

user environment management™

AppSense Management Console

- AppSense Management Centre
 - Used to deploy agents and configs
 - Updates to configurations
 - Control different groups of machines
 - Configuration version control
 - Centralised Auditing

AMC Sizing

- AppSense Management Centre
 - Agent typically between 5 - 10MB
 - Configuration typically apx 500KB
 - Average DB size apx 5 - 10GB for 10,000 users / 500 servers
 - Single AMC can support apx 5000 connections (machines)~
 - N+1 should be used for fault tolerance
 - AMC supports Windows Network Load Balancing

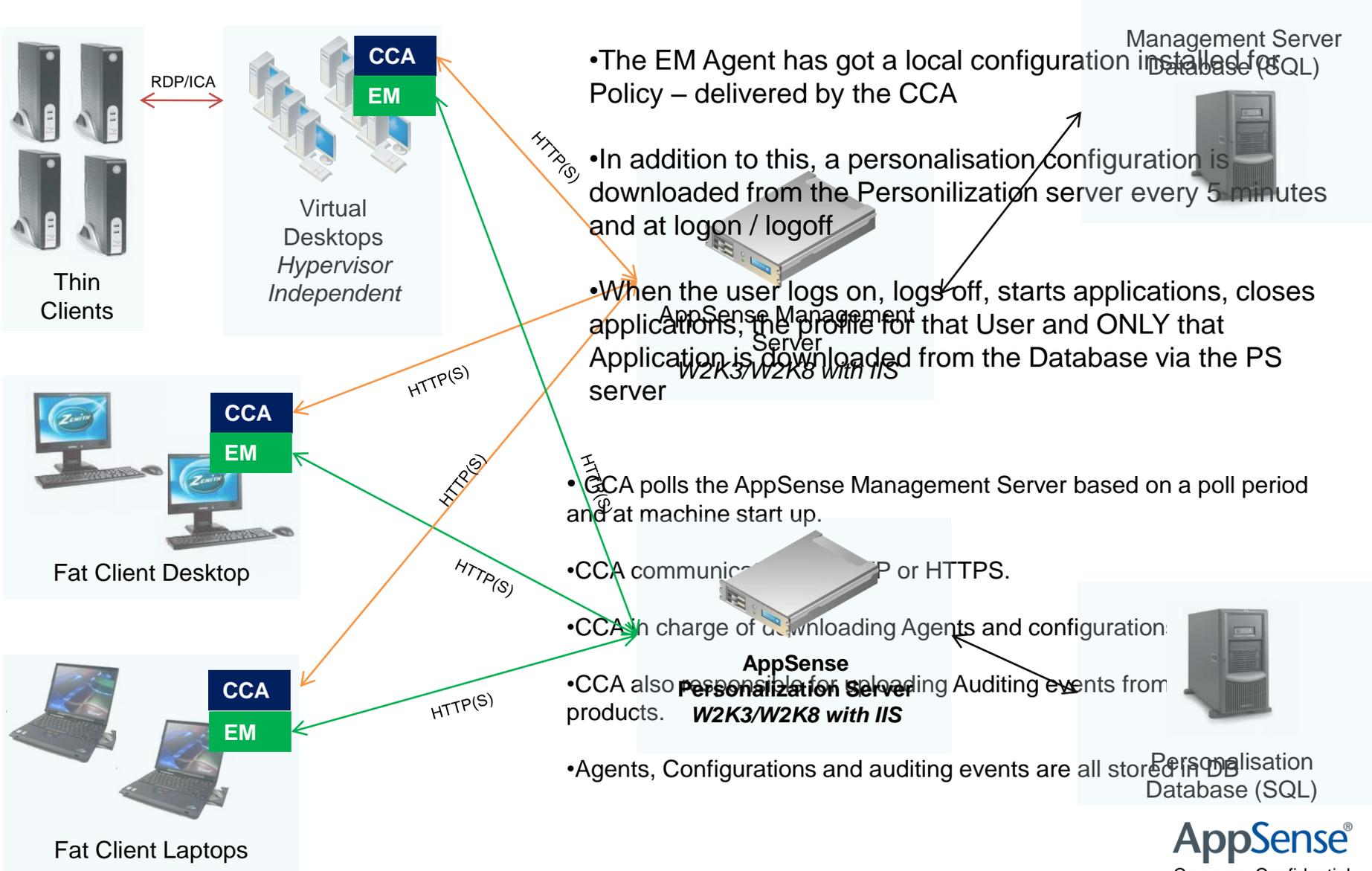
Personalisation Server

- Used to “stream” profile information down to client machine on application start
- Streams the files and registry settings needed by the application
- On application close, the settings are streamed back to the server and stored in the database
- PS Communication Diagram.....

Personalisation Server Sizing

- AppSense Environment Manager
 - Typical Profile Size 3 - 5MB per user
 - Default 5 profile snapshot per user
 - Data is compressed for the PS Server and DB
 - 2000 users
 - $2000 \times 5\text{MB} = 10\text{ GB}$
 - $10\text{GB} \times 5\text{ snapshots} = 50\text{GB}$
 - Single PS can support apx 7000 connections per CORE!
 - N+1 should be used for fault tolerance
 - PS supports Windows Network Load Balancing

V8 Architecture - Personalization & Communication



•The EM Agent has got a local configuration installed for Policy – delivered by the CCA

•In addition to this, a personalisation configuration is downloaded from the Personalization server every 5 minutes and at logon / logoff

•When the user logs on, logs off, starts applications, closes applications, the profile for that User and ONLY that Application is downloaded from the Database via the PS server

•CCA polls the AppSense Management Server based on a poll period and at machine start up.

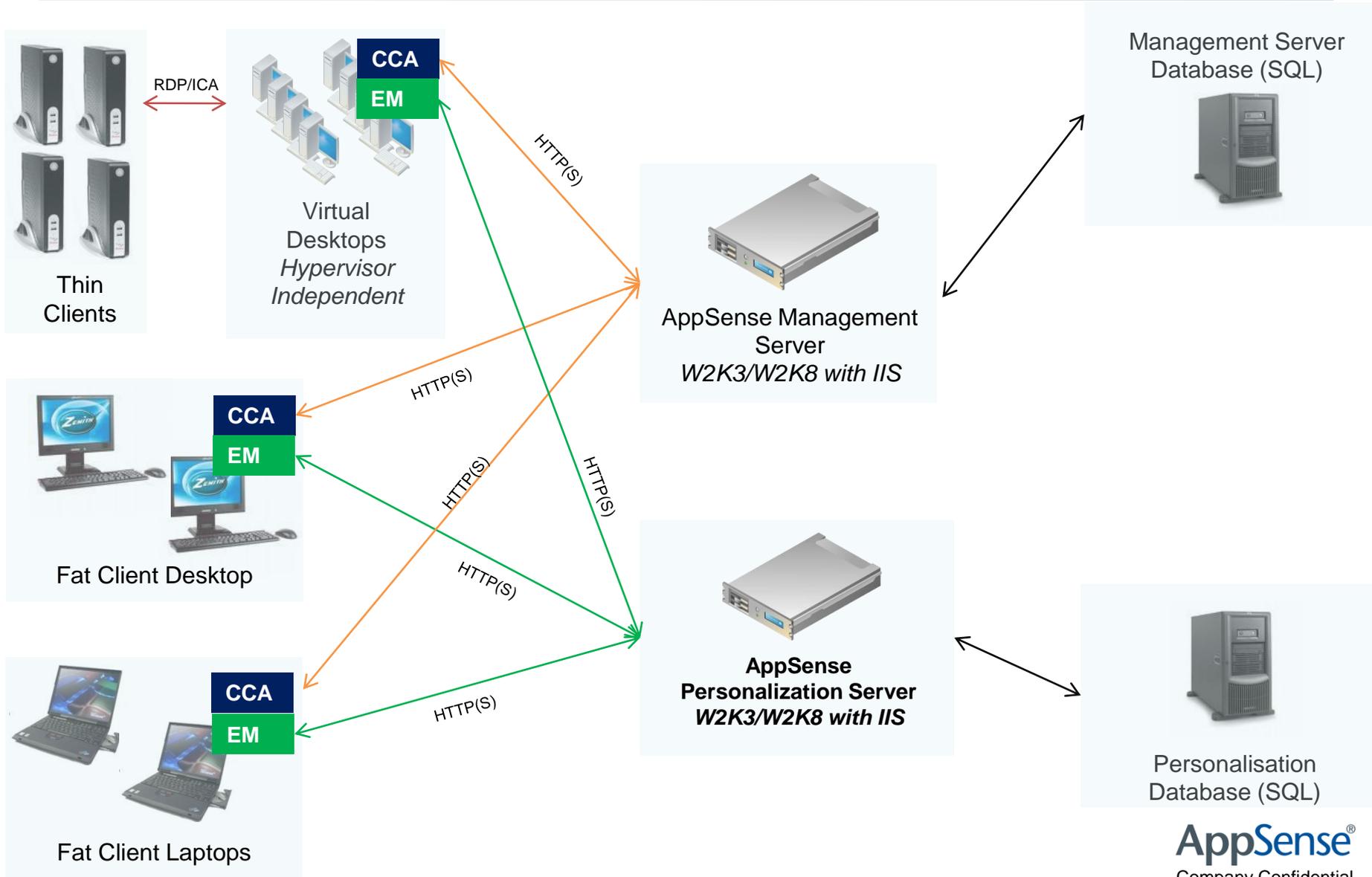
•CCA communicates with PS or HTTPS.

•CCA in charge of downloading Agents and configuration:

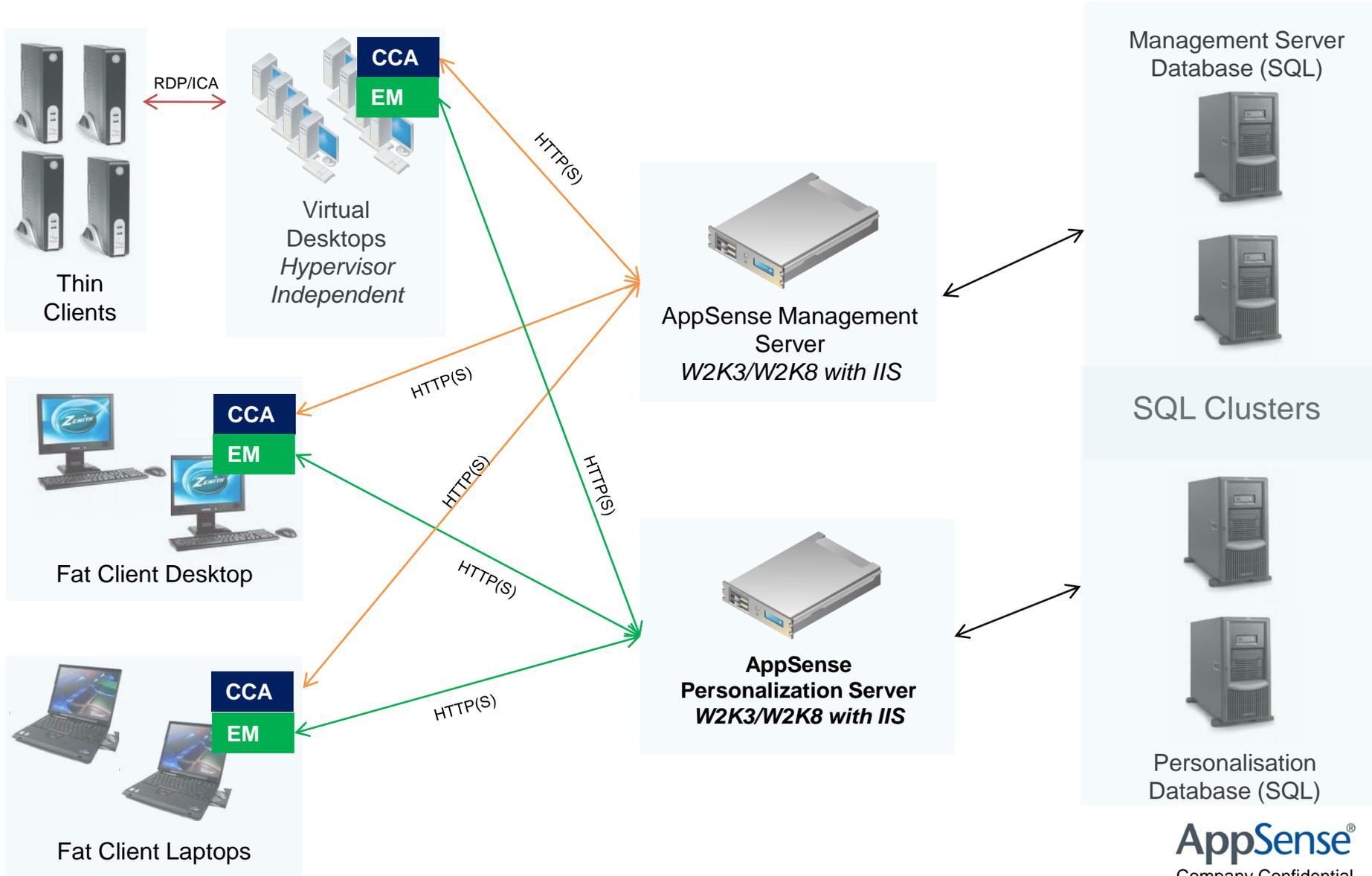
•CCA also responsible for uploading Auditing events from products.

•Agents, Configurations and auditing events are all stored in DB

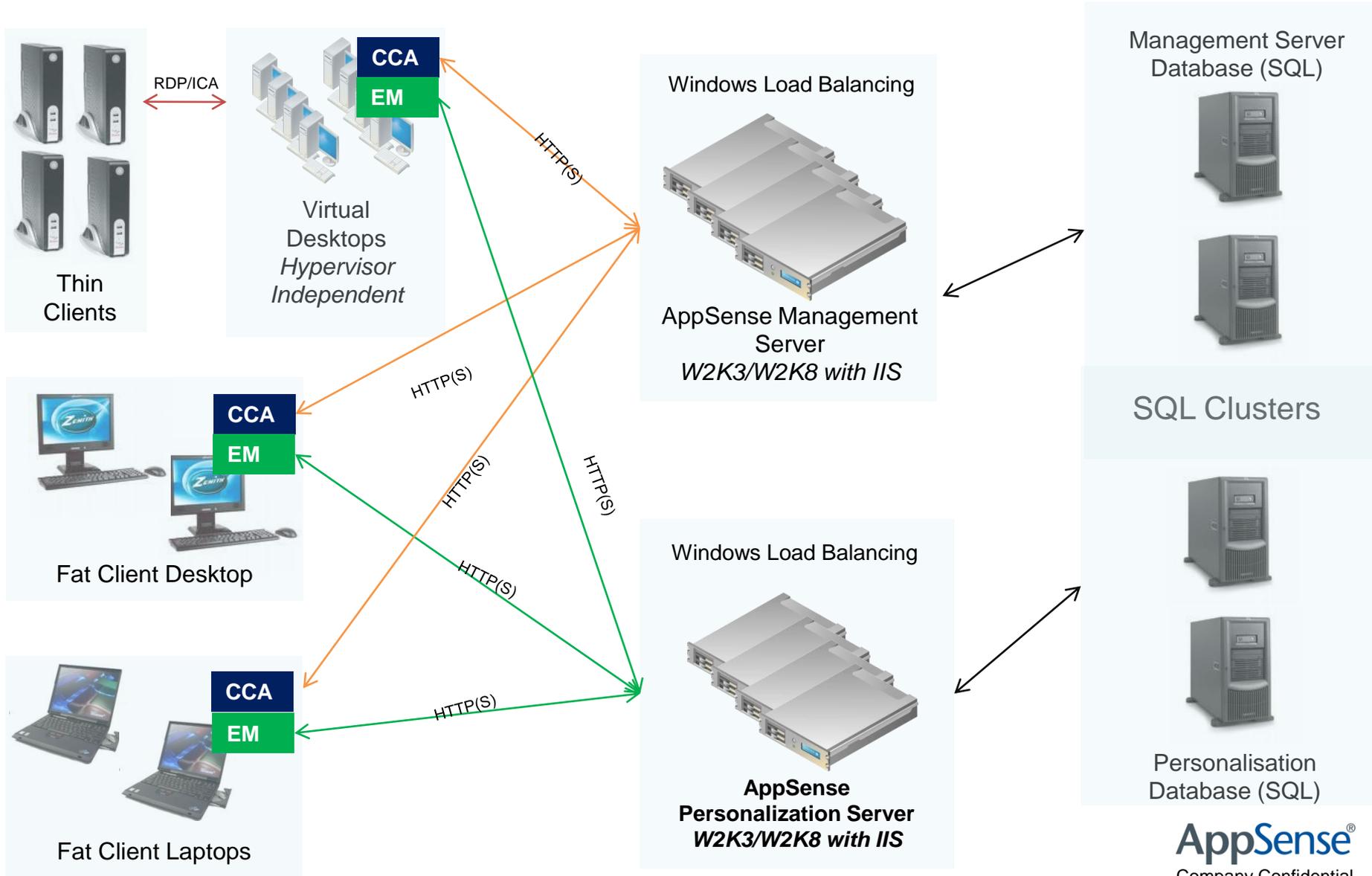
V8 Architecture - Summary



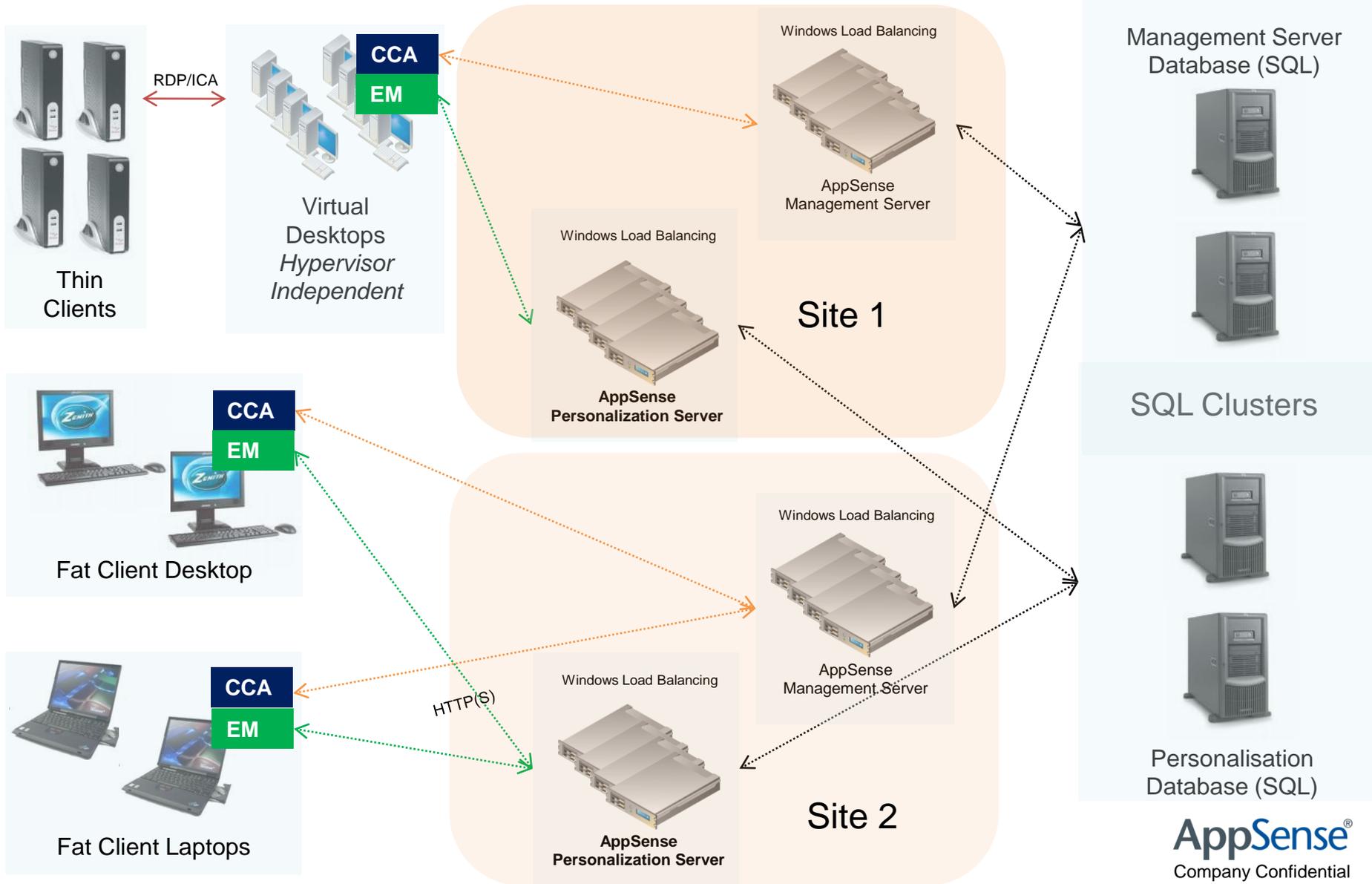
V8 Architecture - DB Scalability



V8 Architecture - AMC and PS Server Scalability

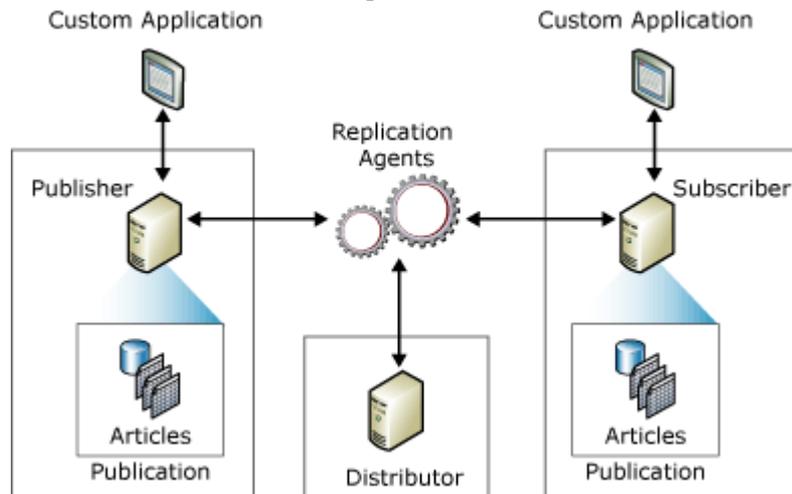


V8 Architecture - Failover / Proxy / MultiSite



PS Database Replication

- Used in multi site environments
- Allows users to roam
- Uses sequel “merge” replication
- One becomes the “publisher,”
- Others become subscribers
- In the event of conflict the publisher wins
- Snapshots are not replicated



PS Database Replication

- Two publications are made available by the master:
 - 1. Config- all the configuration data (ie. data set up by the console). The merge agent runs every 5 minutes
 - 2. Data: The actual personalization data (users and application settings). The merge agent runs daily at midnight.
- Subscriptions to these publications are set up for each slave.
- These are “updatable push merge”
- subscriptions.
- This means data from the publisher is merged with data on the subscriber, updates made on the subscriber are propagated back to the publisher, and the subscription agent runs on the publisher (hence “push”).
- Data transferred consists only of changes made, so slaves must be initialized from a snapshot stored on the publisher.
- A “Synchronize Site Databases” button is provided which runs the stored procedure “ForceReplicationNow”.



PS Database Replication

- Scripts found....
 - c:\Program Files\AppSense\Environment Manager\Personalization Server\Replication\
- SQL Replication Best Practice Doc



AppSense in Streamed OS

user environment management™

Citrix Provisioning Server

- Installation of most agents cause a reboot
 - No good in CPS environment
- Agents must be installed in “Private” mode
- Need to install all agents - not just the CCA
 - No Need to install the configs *
- Once the vDisk is in READ ONLY the machine will start with all agents installed and contact the AMC

Citrix Provisioning Server

- Must allow CCA to self register

http://uemdcr001/ManagementServer - Local User - Management Console

Management Console v3.0.705.0

Deployment Groups << Virtual Servers > Settings

Polling

Computer poll period
1 Minute

The Computer poll period controls how frequently the Client Communications Agent (CCA) on client computers checks for updates.

Upload poll period
1 Minute

The Upload poll period controls how frequently the CCA on client computers uploads event data to the Management Console.

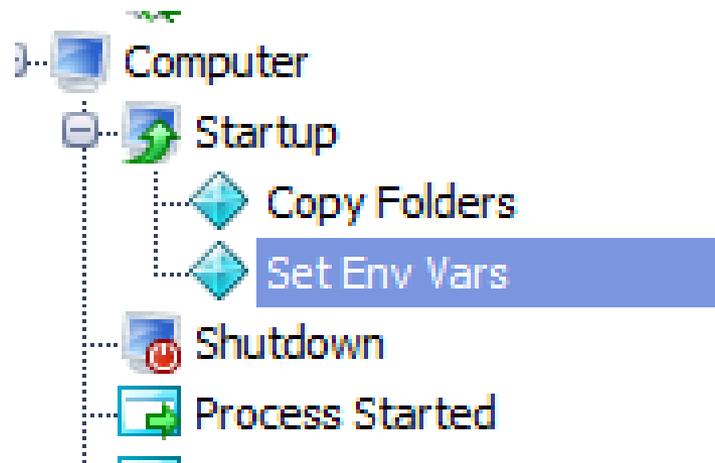
Registration

Allow CCAs to self-register with this group.

When selected, any user can choose during CCA installation for the computer to join this computer group.

Citrix Provisioning Server

- The agents will not download as they are already present
 - Check Add/Remove Programs
- All configs for the group will be downloaded
- * If EM Start Up Actions are being used then the EM config **MUST** be installed when the vdisk is in private mode!



Citrix Provisioning Server

- When using Computer groups machines will not self register
 - CCA only registers when installing
 - Machines can be pre listed or....
 - Use RE - ARM vb script.....(see best practice doc)
-
- net stop "AppSense Client Communications Agent"
 - REG DELETE "HKLM\SOFTWARE\AppSense Technologies\Communications Agent" /v "machine id" /f
 - REG DELETE "HKLM\SOFTWARE\AppSense Technologies\Communications Agent" /v "group id" /f
 - REG ADD "HKLM\SOFTWARE\AppSense Technologies\Communications Agent" /v "self register" /d "GroupName"



Using Personalisation with Streamed Applications

user environment management™

Streamed Apps

- Natively installed
- Symantec SVS
- Microsoft App V
- Citrix Streaming
- Coming Soon...
 - ThinApp *
 - Installfree

SVS

- In EM exclude C:\fsldr (the SVS file cache)
- In EM make sure you are matching firefox by filename only, not full path - in SVS it is executed from C:\fsldr\...
- In the SVS layer, exclude:
 - C:\appsensevirtual (and subdir's)
 - AppData (and subdir's)
 - LocalAppData (and subdir's)

App V

- Navigate to **Microsoft Application Virtualization Sequencer**.
- Open the required **Application Package**.
- Select **Tools > Options**.
- The **Options dialog box** displays.
 - Select the **Exclusion Items** tab.
 - Click **New**.
 - The **Exclusion Item dialog box** displays.
 - In the **Exclude Path** enter *C:\AppSenseVirtual*.
 - Select the **Mapping Type VFS**.
 - Click **OK**.
 - The main package screen is re-displayed, click **OK**.
- 10. Save the Package.
- 11. Repeat for each Application Package as required.

Citrix Streamed Apps

- **For relaxed security:** - All named pipes need to be added to the streaming profile.
- Right click the target i.e. Windows Server 2003 [All service packs], select properties
- Select “Rules” tab
- Add, select Ignore and Named Objects, Next
- Select All Named Objects, Next
- Rule Name should read “Ignore All named objects2
- Select Finish.
-
- **For enhanced security:** - All named pipes need to be added to the streaming profile and the AppSense virtual cache.
-
- Repeat the above steps to “Ignore All named objects”.
- Right click the target i.e. Windows Server 2003 [All service packs], select properties
- Select “Rules” tab
- Add, select Ignore and Files and Folders, Next
- Add, type c:\appsensevirtual, ok
- Next
- Rule Name should read “Ignore c:\appsensevirtual”
- Select Finish
- [StreamingPersonalization.avi](#)

AppSense®

AppSense Performance Manager

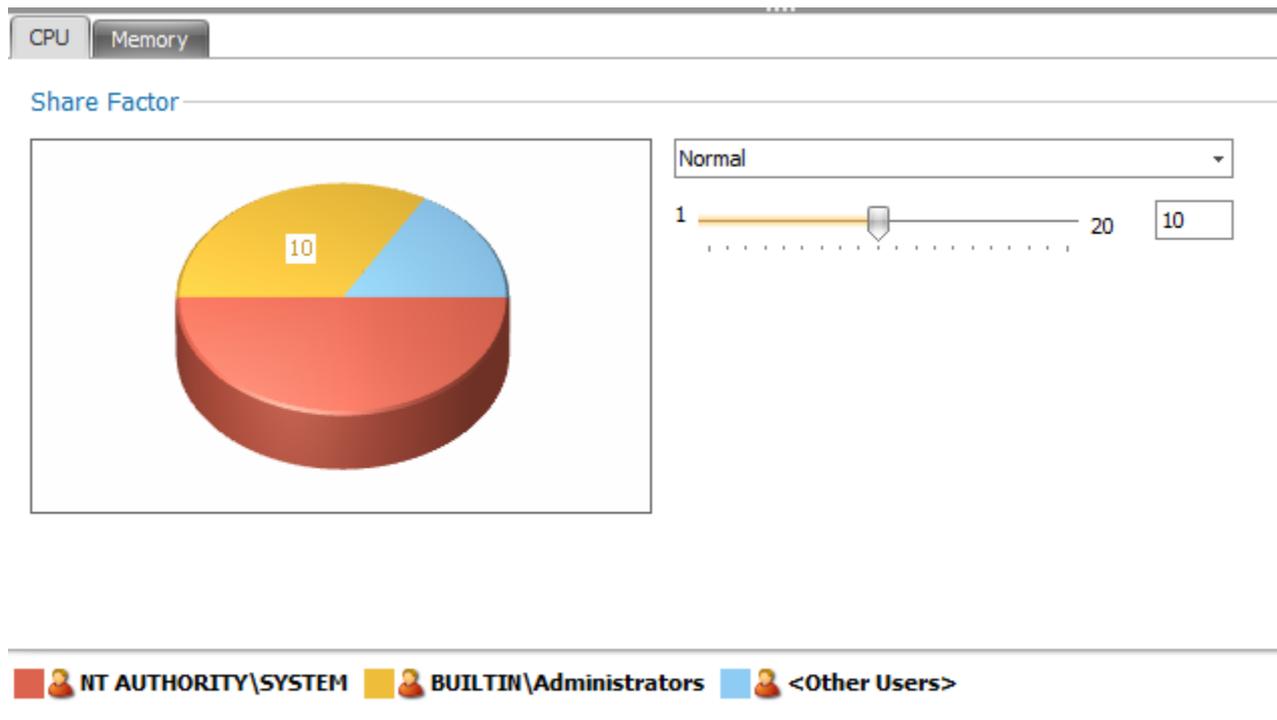
user environment management™

Performance Manager - Default Configuration

- From a new template
 - Smart Scheduling Enabled
 - Thread Throttling Enabled
 - Physical Memory Control Enabled
 - DLL Optimization Enabled
 - Statistics Disabled
 - CPU Hard and Soft limits disabled
 - Physical and Virtual Memory Limits disabled
 - Disk Control Disabled

Smart Scheduling

- In most cases these share factors do not need changing
- System Processes get 3 x Share
- Administrators 2 x Share
- Users 1 x Share



Smart Scheduling

- Users additionally get Share factors based on session state
 - Normal 2 x Share for application in foreground, connect etc
 - Desktop locked ½ share
 - Disconnected Session ½ share

CPU				Memory		Disk
Share	Reservation	Limit	Affinity	Application	Physical	Priority
Window is Foreground, Session is connected and Desktop is unlocked						
Normal (10)						
Desktop is locked						
Low (5)					Trim	
Session is disconnected						
Low (5)					Trim	

Thread Throttling

- Default TT enabled when CPU hits 100% for more than 2 seconds
- Make sure that Multi CPU is enabled

Thread Throttling



With Thread Throttling™ you can set system wide CPU thread throttling policies that will automatically trigger when the system is heavily loaded and apply gradual throttling to any runaway threads within each process.

Monitor

Enabled

Apply clamping when CPU reaches % for seconds

For multi-processor systems, damp when any one processor reaches the threshold

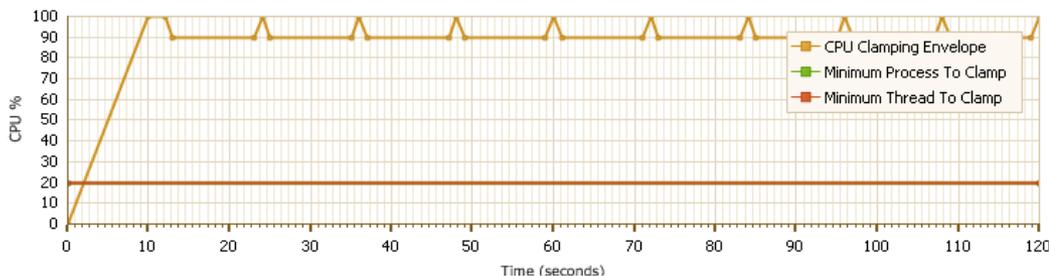
Action

Clamp CPU by % for seconds

Exceptions

Do not clamp processes below %

Do not clamp threads below %



- Always clamp by 10 or 20%

- Make TT more aggressive by changing the MIN PROC and MIN THREAD to clamp

- Good for test scripts

DLL Optimization - Analysis

Analysis Schedule Optimize Schedule Excluded Components Excluded Applications

When to perform Analysis

Don't Analyze Interval Basis Every Day Specify Day

Analysis Interval

Analyze every: Mins

Analysis Time

Analysis time of day: every

[Perform a Manual Analysis...](#)

- Default is 60 mins
- Set this to 120 mins once DLL has been found
- Less CPU activity during the day
- Still finds most DLL within 3 days

DLL Optimization - Optimization

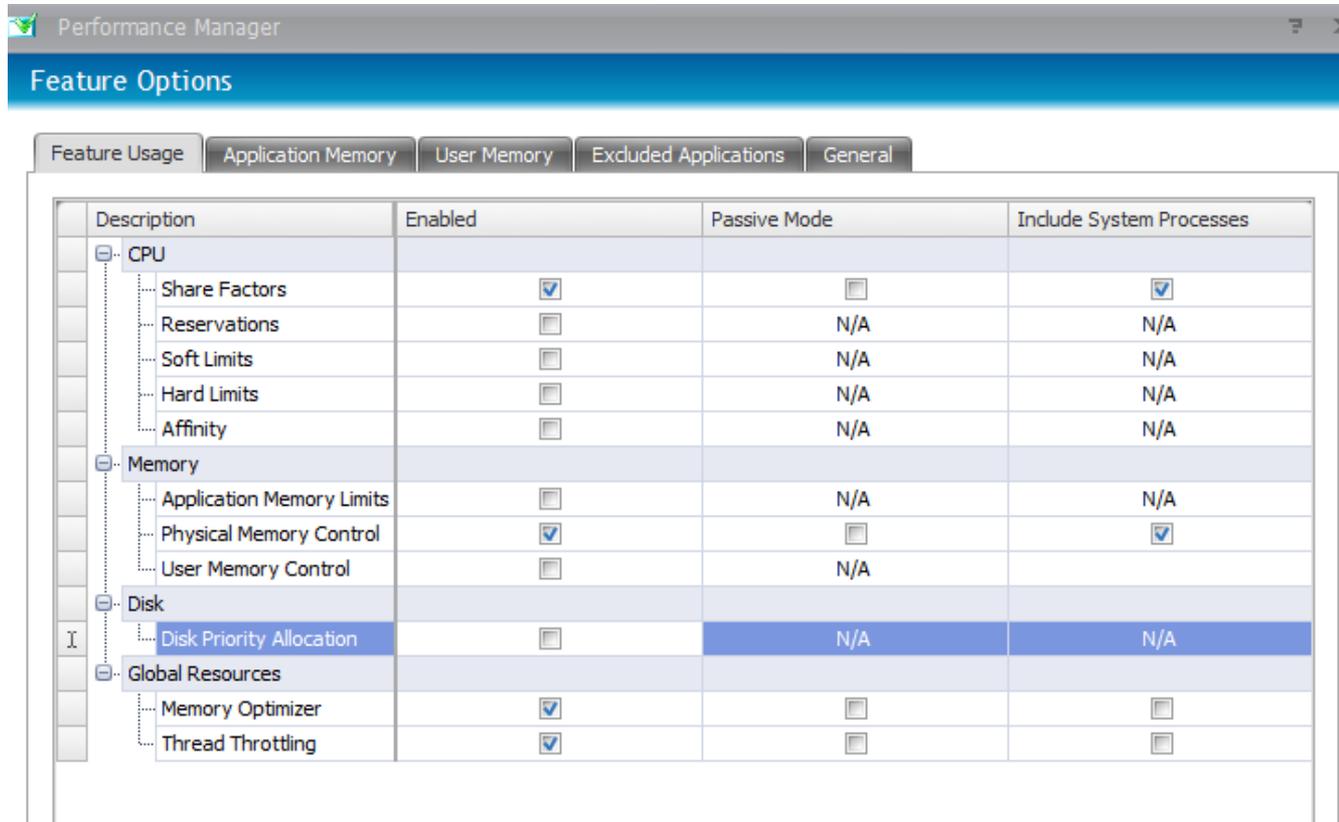
The screenshot shows the 'Optimize Schedule' tab of the AppSense configuration interface. It is divided into three sections:

- When to perform Optimisation:** Four radio buttons are present: 'Don't Optimize', 'After Analysis', 'Every Day' (which is selected), and 'Specify Day'.
- Optimize Time:** A field for 'Optimize time of day' is set to '23:00', followed by the frequency 'every' and a dropdown menu set to 'Sunday'.
- Optimizer Options:** Three checkboxes are shown: 'Include Signed Components' (checked), 'Include Network Components' (checked), and 'Include Windows File Protection list Components' (unchecked). To the right, there is a 'Local Cache Drive' dropdown menu set to '%SYSTEMDRIVE%'.

- Optimize copies the files to the APPSENSECACHE
 - Cache is same drive as Application
 - Network Cache is AppSenseCacheN
- Good practice to set this to “Out of Hours”
- Include Signed Components
- Include Network Components
- Not many Applications need excluding - .NET done already
- Don't forget to CLEAN DLL which may of been optimized by Citrix DLL Optimization

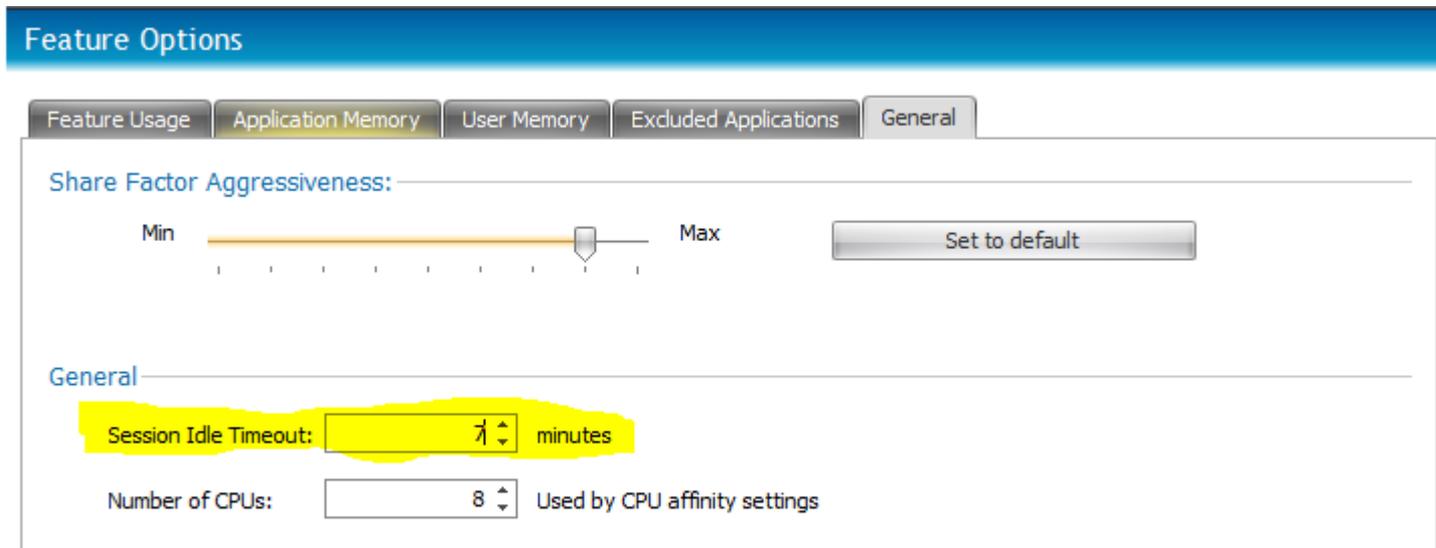
Feature Options

- Use Feature options to quickly disable parts of Performance Manager you don't need
- Disable Thread Throttling and DLL optimization for SYSTEM BASED processes



Session Idle Time Out

- Time Out useful when using CPU or Memory Control based on IDLE
- IDLE time IS NOT CITRIX or MS session idle timeout – its PM Idle time
- Setting to 7 mins (from 15) will make memory trimming and CPU SS more aggressive

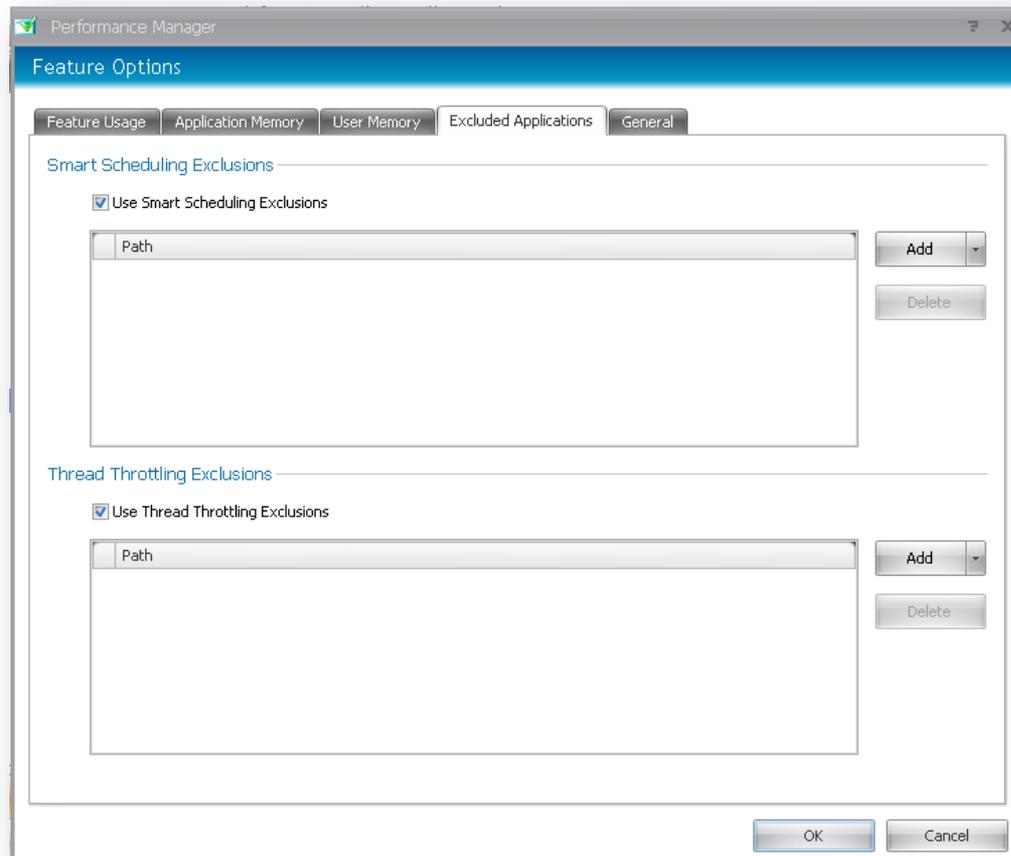


The screenshot shows the 'Feature Options' configuration window with the 'General' tab selected. The 'Share Factor Aggressiveness' slider is visible, ranging from 'Min' to 'Max', with a 'Set to default' button. Below this, the 'General' section contains the following settings:

- Session Idle Timeout: 7 minutes (highlighted in yellow)
- Number of CPUs: 8 (Used by CPU affinity settings)

AppSense Performance Manager 8.0 SP2

- New in SP2
- Excluded Processes from TT or SS
- Used on all customers using Symantec Anti Tamper – v9 +



Adding the LSS

The screenshot shows the AppSense Management Console interface. The browser address bar displays `http://aldabs01.livedemo.appsense.com/ManagementServer - Local User - Management Console`. The main title is "Management Console v8.0.705.0".

Deployment Groups: Overview, Unassigned Computers, Computers, Directory Groups, Computer Groups, Central Europe, Settings, Membership, Packages, Installation Schedule, Failover Servers, Enterprise Auditing, Alerts, Events, Computers, North America, Northern Europe.

Central Europe > Packages

The following packages will be installed:

Type	Name	Platf...
Management Center		
Agent	AppSense Client Communications Agent	32 Bit
Agent	AppSense Client Communications Agent (x64)	64 Bit
Performance Manager		
Agent	AppSense Performance Manager Agent	32 Bit
Agent	AppSense Performance Manager Agent (x64)	64 Bit
Agent	AppSense Performance Manager Local Statistics Service	32 Bit
Agent	AppSense Performance Manager Local Statistics Service (x64)	64 Bit
Configuration PM LIVE Demo		

The following packages are available:

Name	De...
AppSense Performance Manager Agent	Serve...
AppSense Performance Manager Agent	Serve...
AppSense Performance Manager Agent (x64)	Serve...
AppSense Performance Manager Agent (x64)	Serve...
AppSense Performance Manager Agent (x64)	Serve...
AppSense Performance Manager Agent (x64)	Serve...
AppSense Performance Manager Local Statistics Service	Serve...
AppSense Performance Manager Local Statistics Service	Serve...
AppSense Performance Manager Local Statistics Service	Serve...
AppSense Performance Manager Local Statistics Service (x64)	Serve...
AppSense Performance Manager Local Statistics Service (x64)	Serve...
AppSense Performance Manager Local Statistics Service (x64)	Serve...
AppSense Performance Manager Local Statistics Service (x64)	Serve...
fgfdfhdfhggrfh	Config...
fgfhgfhg	Config...

Actions: Assign, Unassign, Show All Versions, Show Latest Version, Use Latest Version, Refresh, Help.

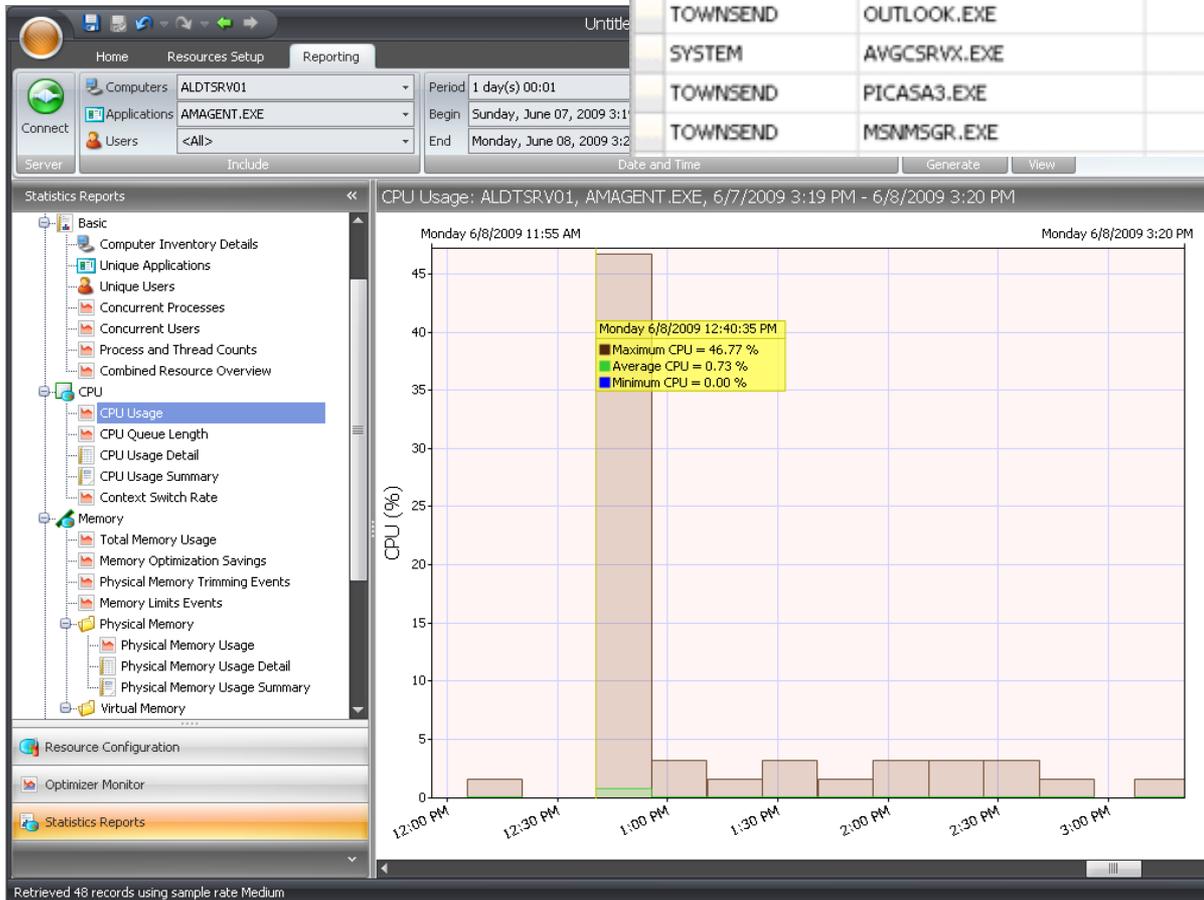
Submit

Statistics - Reporting

CPU Usage Detail Report: TOWNSXPS, 21/08/2009 16:12 - 21/08/2009 17:14

Print Group By

		CPU			
User	Application	% (avg)	% (min)	% (... ▼)	Priority Changes (avg)
TOWNSEND	OUTLOOK.EXE	0.65	0.00	50.78	0
SYSTEM	AVGCSRVX.EXE	25.50	0.00	50.39	19
TOWNSEND	PICASA3.EXE	27.27	2.34	43.75	23
TOWNSEND	MSNMSGR.EXE	0.31	0.00	40.63	0



Collecting Stats

User	Process	Collection Level = High
User01	Winword.exe	All 5 seconds a record for that unique process for that unique user in the LSS db.
	Excel.exe	All 5 seconds a record for that unique process for that unique user in the LSS db.
User02	Excel.exe	All 5 seconds a record for that unique process for that unique user in the LSS db.
	Access.exe	All 5 seconds a record for that unique process for that unique user in the LSS db.

Collection Consolidation Data Volume Estimates Options

Statistics Collection

Off
 Low
 Medium
 High

Statistics collected with this setting

Statistics collection will occur every 5 seconds. All detailed data is recorded locally at a high frequency. As a result this will only be consolidated once a day to a remote server for reporting purposes. This is to minimize the load on both the controlled machine and server. This collection rate can only be maintained for a maximum of 21 days.

Fallback collection type:

Use fallback collection type:

Stats Collection

- **Off (default)** - the Statistics Collection node in the navigation tree is grayed out when the Statistics Collection setting is off and the LSS service is stopped in this mode. For all other modes the LSS will be started by the Performance Manager Agent.
- **Low** - machine wide every 5 seconds and every 15 minutes an Application Group summary from a sample rate of 5 seconds.
- **Medium** - as Low, but every 15 minutes a per process, per user summary is generated from a sample rate of 5 seconds.
- **High** - as Medium, but every 5 seconds a per process, per user *actual* statistic values are recorded. This is the most accurate way of recording statistics, but the most expensive.

AppSense®

Questions ?

user environment management™

AppSense®

AppSense Application Manager

user environment management™

Default Configurations

- \\CD Image\Software\Products\Templates\EN
 - English and German AM “Passive mode”
 - English and German AM “active mode”
- Only allows executables from Local Drive
 - Network Apps blocked by default
- Only allow executables owned by Trusted Owners

What wins?



Trusted Owners in Windows Desktop vs Server.

- Default owner is the person who “introduced” (installed) the file(s)
 - Eg: Office installed by x is owned by x.....
- In Windows 2003/2008, by default, the owner is set to the group the installer belongs to.
 - Eg: SimonT is a member of the Administrators group.
 - NTFS ownership of files is set to Administrators
- In Windows XP and Vista, by default, the owner is the account actually logged on, not the group
 - SimonT is a member of the Domain Admins
 - SimonT is the owner of all files he installs
 - Users can not run files installed by SimonT as the default config doesnt have SimonT listed as a trusted owner

Trusted Owners

- In Desktop environment, either add SimonT to the Trusted Owners or
- Change GPO
 - Computer Configuration > Windows Settings > Local Policies > Security Options > System Objects > Default Owner for objects

Trusted Owners

Trusted Owner	Textual SID
> NT AUTHORITY\SYSTEM	S-1-5-18
BUILTIN\Administrators	S-1-5-32-544
%COMPUTERNAME%\Administrator	
NT SERVICE\TrustedInstaller	S-1-5-80-956008885-3418522649-1831038044-...
appsensebk\simont	

Add Trusted Owner

Delete

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled
System objects: Default owner for objects created by members of the Administrators group	Administrators group
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled

Best Practice

- Add Network Based Applications as Accessible items
 - Use folders for ease of use
 - Turn off NTFS checks on non NTFS shares
 - Use SHA #1 Signature checks on non NTFS drives
- Ignore restrictions during logon to allow logon scripts to run
- Use Passive mode for a week trail
- Use the AM Rules analyser to find out why executables are allowed / blocked.



Application Manager - ANAC
Application Network Access Control

user environment management™

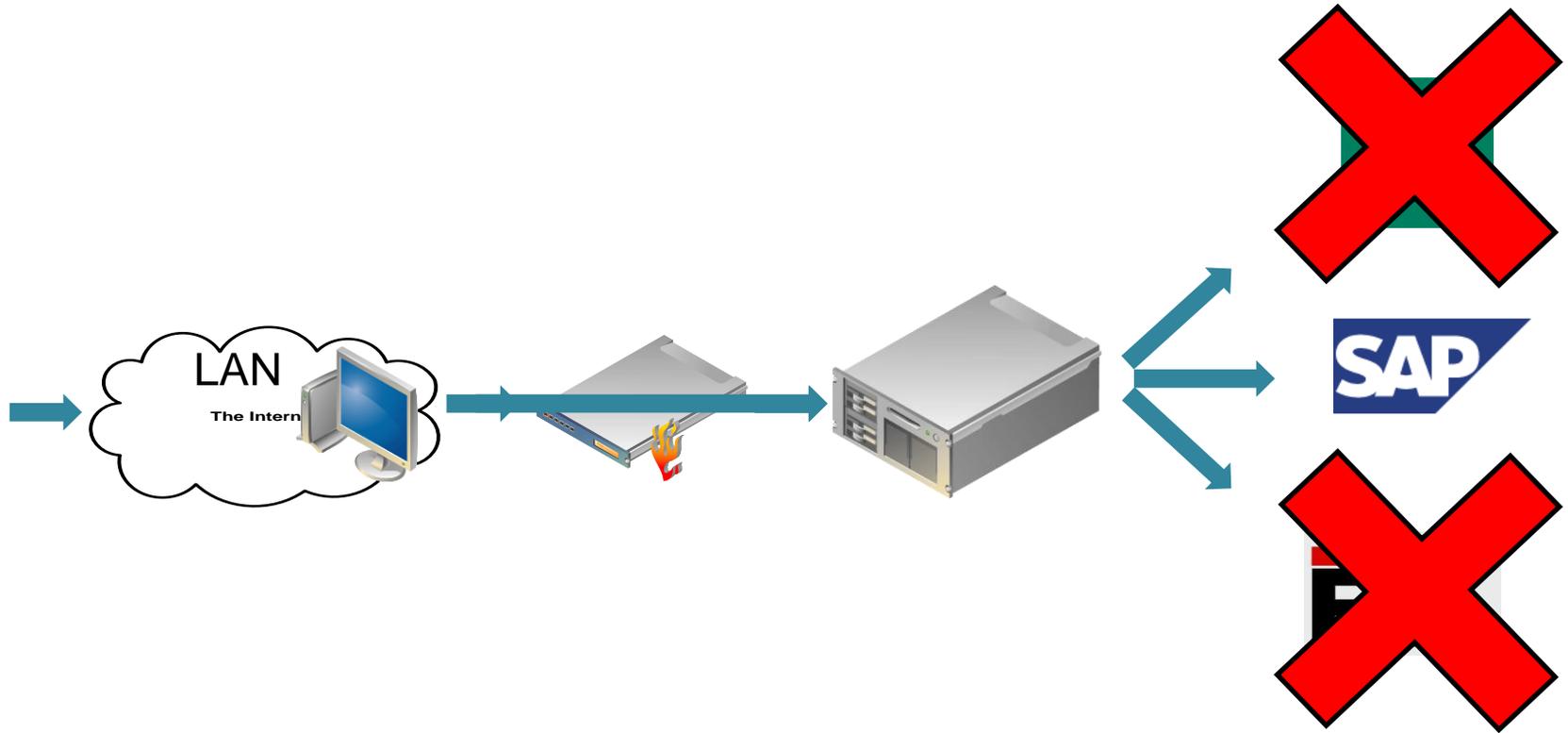
Application Network Access Control

- What is ANAC?
 - The ability to control the Network access of a User, Group, Device or on the outcome of a script.
- What can it control?
 - 99% of items that use the Winsock layer
 - Access to Servers by name or by their IP address
 - Access to ports
 - Access to urls (Designed for internal urls only)
 - Combinations of Host name/IP & port
- What can't it control?
 - Items that create their own packets (cmd.exe ping command)
 - Items that operate at a lower level than the winsock layer
 - Drivers that access Network traffic
 - SVC host and AM components are exempt from control among others
 - Outlook comms to exchange

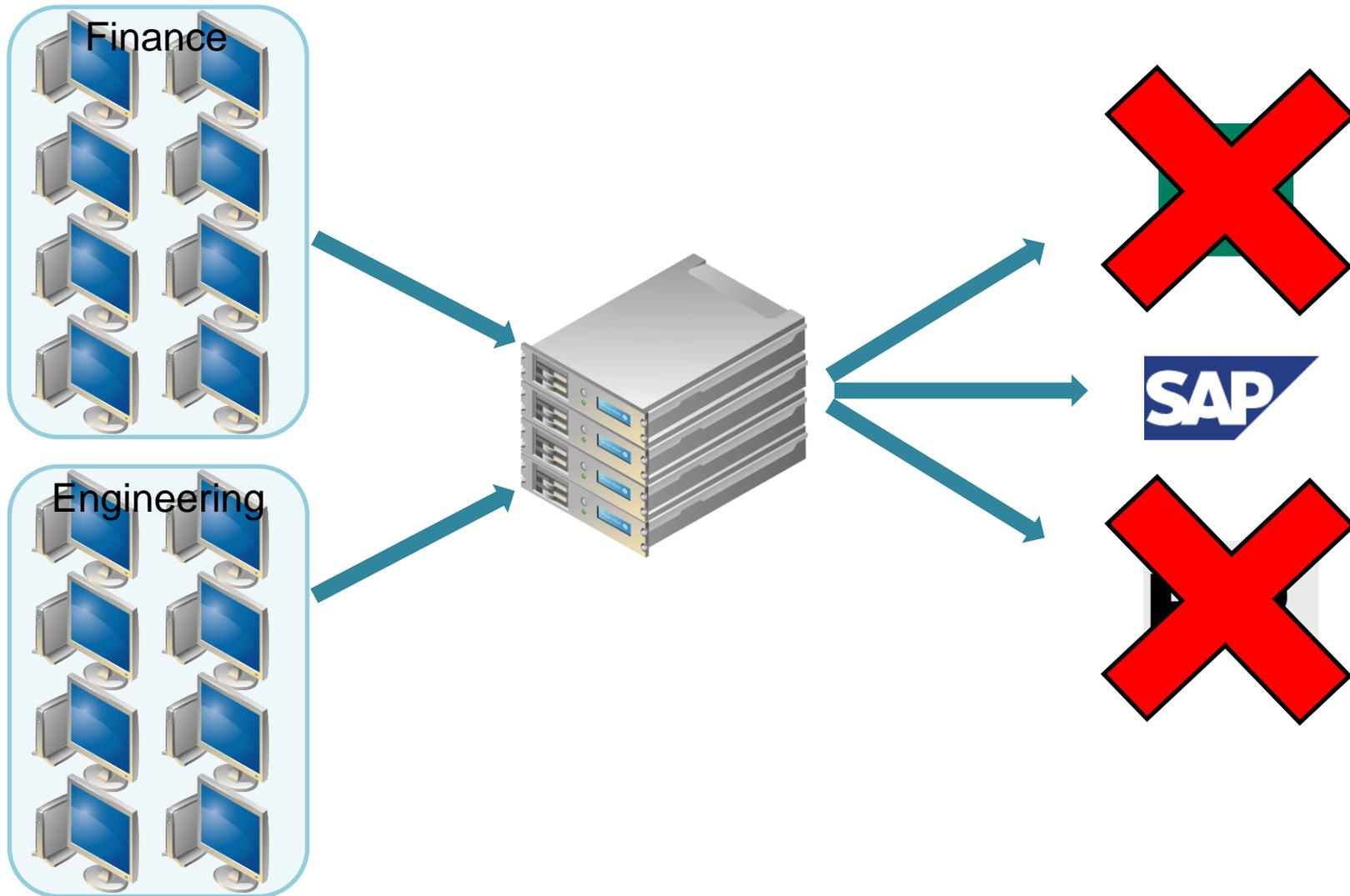
ANAC How it works

- **Components**
 - Hooking Mechanism
 - Redirection Engine
 - ANAC.dll
 - Mini filter driver
 - AM agent
- **What happens for URLs, IPs and host names**
 - Our hook, hooks in to applications when they start and injects our ANAC.dll
 - When the application tries to access the network we re-direct to our AM agent. To allow or deny access to the Network location

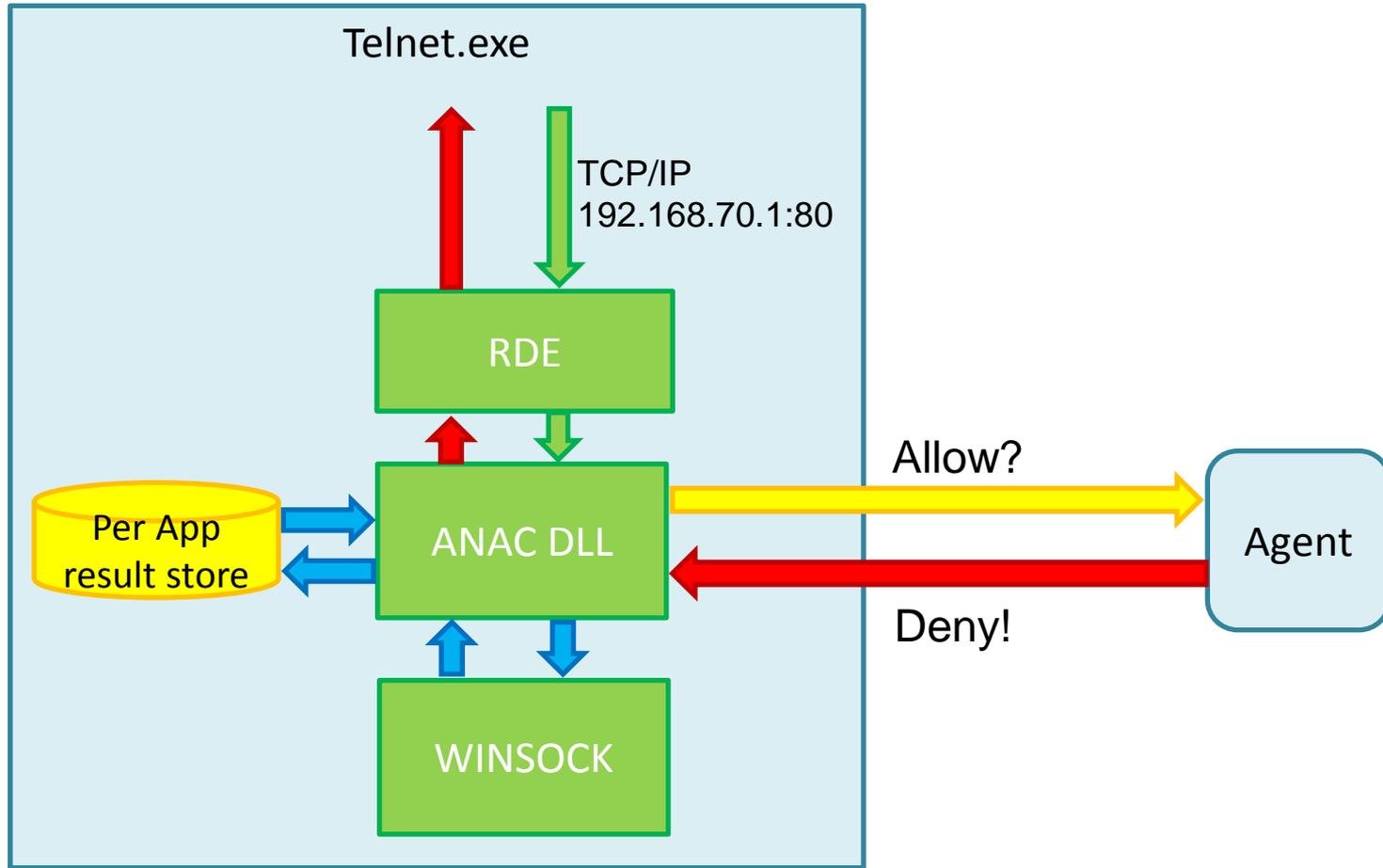
Why Control NAC? Where a user can go if external?



Role Based Network Access



ANAC How it works



ANAC how to use, Controlling IPs

Network Connection Details

Please enter the connection details

Connection Type

IP Address

Network Share

Host Name

Connection Options

Host 192.168.70.206

Port(s)

Common Ports...

Path

Text contains wildcard characters.

Include subdirectories.

Description

OK Cancel

IP Address Radio Button

The IP of the console machine by default currently

Ports left blank

This default will block complete access to this IP if added to a prohibited item

ANAC how to use, Controlling host names

Host Name Radio Button
The IP of the console machine by default
The server name needs to be added

Ports left blank

Network Connection Details

Please enter the connection details

Connection Type

- IP Address
- Network Share
- Host Name

Connection Options

Host:

Port(s):

Path:

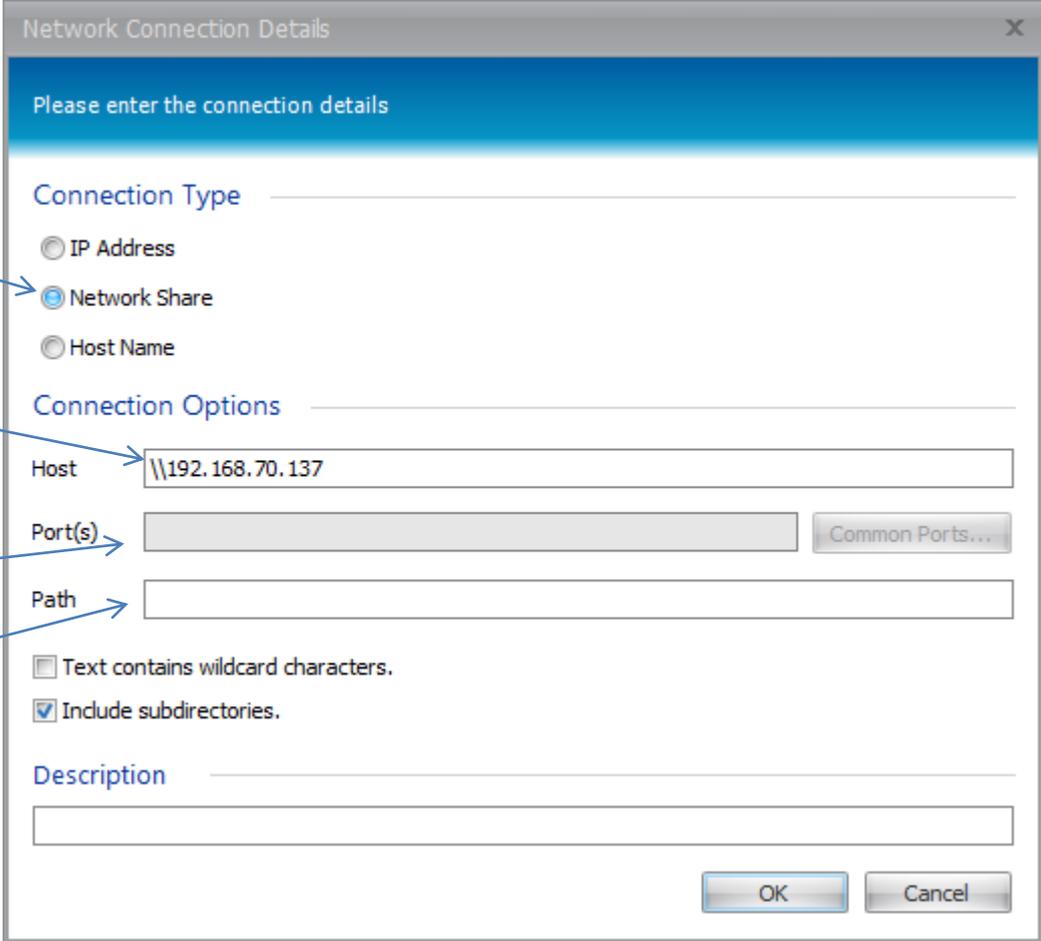
Text contains wildcard characters.

Include subdirectories.

Description

This default will block complete access to this host if added to a prohibited item

ANAC how to use, Controlling access to UNC's



The screenshot shows a dialog box titled "Network Connection Details" with a close button (X) in the top right corner. The dialog has a blue header bar with the text "Please enter the connection details". Below the header, there are three sections: "Connection Type", "Connection Options", and "Description".

- Connection Type:** Contains three radio buttons: "IP Address", "Network Share" (which is selected), and "Host Name".
- Connection Options:** Contains three text input fields: "Host" (with the value "\\192.168.70.137"), "Port(s)" (which is greyed out), and "Path". To the right of the "Port(s)" field is a button labeled "Common Ports...".
- Description:** Contains a text input field.

At the bottom of the dialog are "OK" and "Cancel" buttons.

Annotations on the left side of the image point to specific elements in the dialog:

- "Network share Radio Button" points to the "Network Share" radio button.
- "The IP of the console machine by default" points to the "Host" text field.
- "Ports greyed out" points to the "Port(s)" text field.
- "Enables the ability to add the path you want control" points to the "Path" text field.

This default will block complete access to this IP if added to a prohibited item

ANAC how to use, Controlling access to URLs

Host Name Radio Button

The IP of the console machine by default
However the host will need to be added

URL path can be entered in the host section
And will automatically be moved to this location

Network Connection Details

Please enter the connection details

Connection Type

IP Address

Network Share

Host Name

Connection Options

Host

Port(s)

Path

Text contains wildcard characters.

Include subdirectories.

Description

This will block access to the appsense phone list if placed in a prohibited rule

Things to be aware of

- Specifying *.*.*.* for an Blanket block for everyone
 - Will block all outbound network traffic and will force you to add everything that that needs network access to function we will be adding 0.0.0.0 as part of SP2
- Blocking applies to the user, not things that run as system
- Reverse DNS lookups are turned off by default
 - An engineering key exists to turn on if needed for local
- Controlling Internet traffic will have a negative impact on performance
- An accessible rule will override a denied rule of the same type
 - Think of host an IP addresses in the same way as files folder rules and paths as file rules

Best Practises

- Try to limit the use of wildcard *
- Limit use for controlling external web access
- Make sure that Turn off the reverse DNS look up for internal web sites/web applications
 - HKLM\software\AppSense Technologies\Application Manager\MessageConfig\Engineering
- Try not to mix different types of network connection
 - If you have blocked all urls in your blacklist then you should allow the same type in your white list

AppSense®

Questions ?

user environment management™

AppSense®

AOB

user environment management™

Other Resources...

- AppSense Blogs
 - <http://www.appsense.com/community/>
 - Updated daily by Marketing, pre sales, support, product managers
- Videos
 - www.appsense.com/media
- AppSense Consultant - Jon Wallace (MVP)
 - www.insidetheregistry.com
- AppSense Pre Sales / System Engineering
 - RoWPreSales@AppSense.com
- AppSense un official forums
 - <http://www.apug.info/>