Microsoft Application Virtualization 4.5

ADM Template

White Paper Descriptor

This whitepaper was designed to provide administrators with the steps necessary to deploy configuration for the App-V client with Group Policies. The App-V Client ADM Template was created to provide administrators with the ability to centrally manage the most commonly configured App-V client settings. A working knowledge of Group Policies in Active Directory is required to implement the ADM Template to the appropriate clients, and is not described in this document.

Copyright © 2008 MICROSOFT CORPORATION

[Introduction 3](#_Toc206556060)

[Preference Settings 3](#_Toc206556061)

[Important Setup Consideration 4](#_Toc206556062)

[Installing the App-V Client ADM Template 5](#_Toc206556063)

[Download the ADM Template msi. 5](#_Toc206556064)

[Install the ADM Template 5](#_Toc206556065)

[Import the ADM Template into a Group Policy Object 5](#_Toc206556066)

[Configure the Group Policy Editor to Display the Settings 5](#_Toc206556067)

[Application Virtualization Client 4.5ADM Template Registry Settings 7](#_Toc206556068)

[Category: Communication 8](#_Toc206556069)

[Category: Permissions 12](#_Toc206556070)

[Category: Client Interface 15](#_Toc206556071)

[Conclusion 16](#_Toc206556072)

[More Information 16](#_Toc206556073)

# Introduction

The Administrative (ADM) Template exposes registry configurations on Application Virtualization client machines which were determined to be commonly changed settings. The App-V ADM Template allows administrators to use group policies to make changes and set default settings for the App-V client. The ADM Template for App-V was implemented using Group Policy preference settings.

NOTE: These are not the new Group Policy preferences that are built in to Windows Server 2008 and are available as an add-on for Windows 2003 and Windows XP.

For more information on the difference in the types of Group Policy settings, please read the Group Policy Team Blog on this subject.

<http://blogs.technet.com/grouppolicy/archive/2008/03/04/gp-policy-vs-preference-vs-gp-preferences.aspx>

## Preference Settings

**Preference settings are used for configuring client setting using the traditional registry settings for the client. The three preference settings behaviors are described below.**

* **Tattoo the registry**. When a GPO goes out of scope, the preference value will remain in the registry. If an administrator is responsible for removing the settings, he or she will need to make sure these values are set to disable, prior to the GPO going out of scope. Also, when removing the preference values, the removed values will not be replaced with the original application configuration value.
* **Overwrite an application's configuration setting.** Preference settings overwrite the original user-configured value for the application. No effort is made to retain the original value before overwriting the value with the preference setting. And, as was noted above, the values will not be removed when the GPO goes out of scope.
* **Not recognized by an application.** The application's settings can be changed either through the user interface or the registry editor if the user has permissions to complete this task. Most importantly, the Group Policy engine only recognizes when a GPO changes, not when the preference value has been changed on the client. This means the preference setting will be applied once and will not be reapplied if the user changes the value of a configuration item. Reapplication of the settings in the GPO will only occur if a change has been made to the GPO.

Understanding preference settings is important. The settings in the App-V ADM Template will replace the registry settings on the client, possibly overwriting preexisting settings. If a user changes a registry setting locally, either through the application or a registry editing tool, the Group Policy based setting will not be reapplied. The Group Policy would only be reapplied if a change was detected in the Group Policy itself. Finally, the administrator would have to disable any settings that had been applied via the ADM Template prior to removing the policy or the settings will remain.

### Important Setup Consideration

In many organizations the ADM Template for App-V will be imported into a Group Policy and then modified with preference settings configured for their environment. Once the ADM Template is applied, any client computers that already have the App-V client installed will have their settings updated with the new preference settings. However if the App-V client is installed after the ADM Template settings have already been applied to a computer, the installer will write all of its default settings over the top of the preference settings from the ADM Template. This would cause inconsistencies between clients.

In order to avoid this situation the best practice is to deploy the App-V ADM Template settings after installing the clients. This will not always be possible; therefore configuring App-V client setup to retain its current registry settings is required. An optional install switch for setup allows simple management of client preferences:

**KEEPCURRENTSETTINGS**

If present, setup will not overwrite registry settings placed by the ADM Template Preferences.

**Example:** The following two commands are different methods to do the same task, namely, retain the current settings on the client machine.

setup.exe /v” KEEPCURRENTSETTINGS=1”

msiexec.exe /i setup.msi KEEPCURRENTSETTINGS=1

NOTE: These commands are the minimum that would be required to install the client to retain the current settings. In the first command /v is used to pass additional parameters to MsiExec. In the second command /i is used to display status messages.

**For additional information on managing deployment setup settings, click the following link:** <http://go.microsoft.com/fwlink/?LinkId=122063>.

## Installing the App-V Client ADM Template

Deploying settings using the App-V Client ADM Template requires administrators to complete the following steps.

1. Download the ADM Template msi.
2. Install the ADM Template.
3. Import the ADM Template into a Group Policy Object.
4. Configure the Group Policy editor to display the settings.

### Download the ADM Template msi.

Download the App-V ADM Template from <http://go.microsoft.com/fwlink/?LinkId=121835>

### Install the ADM Template

1. Run the App-V ADM Template msi.
2. During setup choose a location to install the ADM Template.
3. Click on **Finish** to complete the process.

### Import the ADM Template into a Group Policy Object

1. Open Group Policy Object Editor.
2. Right click on **Administrative Templates**, click **Add/Remove Templates.**
3. Click **Add**, specify Application Virtualization Client (\*.ADM) file location.

### Configure the Group Policy Editor to Display the Settings

**Note:** This procedure is not required in Windows Server 2008 unless a filter has been applied to filter out preference settings.

1. Select **Administrative Templates.**
2. Select **View** on the Group Policy Object Editor menu bar, Click **Filtering**.
3. **Uncheck** the “Only show policies that can be fully managed” box, click **OK**.

* After importing the ADM Template and changing view configurations, the client preference settings are listed in the Group Policy Object Editor.

## Application Virtualization Client 4.5ADM Template Registry Settings

The App-V ADM Template allows administrators to configure thirty seven client registry settings. The following table is a categorized list of those settings with descriptions and default values, where available. The categories are used to group common settings in the ADM Template when looking at them in the Group Policy Editor. The tables below that list the registry settings that can be controlled using the App-V Client ADM template. Default values are based on a standard install of the Microsoft Application Virtualization Terminal Services Client (denoted by TS) or Application Virtualization Terminal Windows Desktop Client (denoted by WD).


### Category: Communication

Registry Path: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SoftGrid\4.5\Client\Configuration

| ADM Template Option | Registry Value Name | Type | Default Value(Decimal) | Description |
| --- | --- | --- | --- | --- |
| Allow Independent File Streaming | AllowIndependentFileStreaming | DWORD | 0 (WD/TS) | Indicates whether or not streaming from file will be allowed regardless of how the client has been configured (with the ASR). If it’s false, the transport will not allow streaming from files even if the OSD HREF or ASR contains a file path. 0 = False (default)1 = True |
| Application Source Root | ApplicationSourceRoot | String | N/A | A registry key that allows an override of the OSD CODEBASE for the HREF element (for example, the source location) for an application to enable an administrator or ESD system to ensure application loading is performed according to their topology management scheme.  Application Source Root supports URLs and UNC path formats.The correct format for the URL path is protocol://servername:[port][/path][/], where port and path are optional. If port is not specified, the default port for the protocol is used. Only the protocol://server:port portion of the OSD URL is replaced. Some example of acceptable formats for the ApplicationSourceRoot URLs include:rtsps://mainserver:322/prodapps<https://mainserver:443/prodapps>The correct format for the Universal Naming Convention (UNC) path is [\\computername\sharefolder\[folder][\](file:///%5C%5Ccomputername%5Csharefolder%5C%5Bfolder%5D%5B%5C)], where folder is optional. The computername can be a Fully Qualified Domain Name (FQDN) or an IP address, and sharefolder can be a drive letter. Only the [\\computername\sharedfolder](file:///%5C%5Ccomputername%5Csharedfolder) or drive letter portion of the OSD path is replaced. Some example of acceptable formats for the ApplicationSourceRoot UNC path include:[\\uncserver\share](file:///%5C%5Cuncserver%5Cshare)[\\uncserver\share\prodapps](file:///%5C%5Cuncserver%5Cshare%5Cprodapps) |
| OSD Source Root | OSDSourceRoot | String | N/A | Similar to Application Source Root, the OSD Source Root allows specification of a source location for OSD file retrieval for an application package during publication.  Acceptable formats for the OSDSourceRoot include UNC paths and URLs (http or https), as in the following example:[\\computername\sharefolder\resource](file:///%5C%5Ccomputername%5Csharefolder%5Cresource) or [\\computername\content](file:///%5C%5Ccomputername%5Ccontent)<http://computername/productivity/> or <https://computername/productivity/> |
| Icon Source Root | IconSourceRoot | String | N/A | Similar to Application Source Root, the OSD Source Root allows specification of a source location for OSD file retrieval for an application package during publication.  Acceptable formats for the OSDSourceRoot include UNC paths and URLs URLs (http or https), as in the following example:[\\computername\sharefolder\resource](file:///%5C%5Ccomputername%5Csharefolder%5Cresource) or [\\computername\content](file:///%5C%5Ccomputername%5Ccontent)<http://computername/productivity/> or <https://computername/productivity/> |
| Set Background Loading Triggers | AutoLoadTriggers | DWORD | 5 (WD/TS) | AutoLoad is a client runtime policy configuration parameter that enables the secondary feature block of a virtualized application to be streamed to the client automatically in the background. The AutoLoad Triggers are flags to indicate events that initiate AutoLoading of applications. AutoLoad implicitly uses background streaming to enable the app to be fully loaded into cache. Feature block 1 will be loaded first and the remaining feature blocks will be loaded in the background to allow for foreground operations (i.e. user interaction with applications) to take place and provide optimal perceived performance. Bit mask values::(0) Never: No bits are set (value is 0), no auto loading will be performed, as there are no triggers set(1) OnLaunch: Perform background loading when a user launches an application(2) OnRefresh: Perform background loading anytime a publishing refresh occurs.(4) OnLogin: Perform background loading for any application when a user logs in. Default: 0x5 (OnLaunch|OnLogin) |
| Specify What to Load in Background | AutoLoadTarget | DWORD | 1 (WD/TS) | This parameter indicates what will be autoloaded when any given AutoLoadTriggers occur. Bit mask values:(0) None - No autoloading, regardless of what triggers may be set.(1) PreviouslyUsed (default) - If any AutoLoad trigger is enabled, load only the packages where at least one app in the package has been previously used by a user (i.e. launched or precached,). This targets ‘important’ apps, meaning apps that have been used before are likely to be more important to a user than apps that have never been launched.(2) All - If any enabled AutoLoad trigger is enabled, all applications in the package (per package) or for all packages (set for client) will be automatically loaded, regardless of whether they have ever been launched. |

Registry Path: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SoftGrid\4.5\Client\Network

| ADM Template Option | Registry Value Name | Type | Default Value(Decimal) | Description |
| --- | --- | --- | --- | --- |
| Disconnected Operations: Online | Online | DWORD | 1 (WD/TS) | Enables or disables offline mode.If set to 0, then the client will not communicate with App-V Management Server servers or publishing servers. In Disconnected Operations the App-V client can launch loaded application even when it is not connected to an App-V Management Server. In offline mode, the App-V client does not attempt to connect to an App-V Management Server or Publishing Server. You must allow disconnected operations to be able to work offline. Default value is 1 enabled (online). 0 is disabled (offline). |
| Disconnected Operations: Allow | AllowDisconnectedOperation | DWORD | 1 (WD/TS) | Enables or disables disconnected operation.Default value is 1 enabled. 0 is disabled.In Disconnected Operations the App-V client can launch loaded application even when it is not connected to an App-V Management Server.  |
| Disconnected Operations: Fast Connect Timeout | FastConnectTimeout | DWORD | 1000 (WD/TS) | This value specifies the TCP connect timeout In milliseconds to determine when to go into disconnected operations mode. This value can be used to override the default ConnectTimeout of 20s (App-V connect timeout for network transactions) or the system’s TCP timeout of ~25s. This brings the client into disconnected operations mode quickly.  Applied on the next subsequent connect. |
| Disconnected Operations: Limit Disconnected Operations | LimitDisconnectedOperationDOTimeoutMinutes | DWORDDWORD | 1 (WD/TS)129600 (WD/TS) | Specifies whether disconnected operation mode can be used indefinitely or for only a specific period of time.  You must also enable Allow Disconnected Operations to be able to work offline. (0x0) False: Allows unlimited disconnected operation(0x1) True: Limits disconnected operation to a number of minutes specified by the DOTimeoutMinutes setting. Valid values are 1-999999 in days. The default value is 90 days. |

Registry Path: HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\SOFTGRID\4.5\Client\Reporting

| ADM Template Option | Registry Value Name | Type | Default Value(Decimal) | Description |
| --- | --- | --- | --- | --- |
| Reporting: Data Cache Limits | DataCacheLimit | DWORD | 20 (WD/TS) | This value specifies the maximum size in megabytes (MB) of the XML cache for storing reporting information.  The default value is 20 MB. The size applies to the cache in memory. When the limit is reached, the log file will “roll over.” When a new record is to be added (bottom of the list), one or more of the oldest records (top of the list) will be deleted to make room.  A warning will be logged to the client log and the event log the first time this occurs, and will not be logged again until after the cache has been successfully cleared on transmission and the log has filled up again. |
| Reporting: Data Block Size | DataBlockSize | DWORD | 65536 (WD/TS) | This value specifies the maximum size in bytes to transmit to the server at once on publishing refresh, to avoid permanent transmission failures when the log has reached a significant size.  The default value is 65536. When transmitting report data to the server, one block at a time of application records that is less than or equal to the block size in bytes of XML data will be removed from the cache and sent to the server.  Each block will have the general client data and global package list data prepended, and these will not factor into the block size calculations; the potential exists for an extremely large package list to result in transmission failures over low bandwidth or unreliable connections. |

### Category: Permissions

Registry Path: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SoftGrid\4.5\Client\Permissions

| ADM Template Option | Registry Value Name | Type | Default Value(Decimal) | Description |
| --- | --- | --- | --- | --- |
| Add Application | AddApp | DWORD | 0 (WD/TS) | Specifies whether users can add applications explicitly. This does not affect applications that are added through publishing refresh, nor does it prevent users from launching (and thereby implicitly adding) applications that have not already been added. Possible values are:(0) False (Default)(1) True |
| Change Cache Size | ChangeCacheSize | DWORD | 0 (WD/TS) | Specifies whether users can change the cache size. Possible values are:(0) False (Default)(1) True |
| Change File System Drive | ChangeFSDrive | DWORD | 0 (WD/TS) | Specifies whether users can choose a different drive letter to be used as the file system drive. Possible values are:(0) False (Default)(1) True |
| Change Log Settings | ChangeLogSettings | DWORD | 0 (WD/TS) | Specifies whether users are allowed to modify the log level, change the location of the log or reset it through the user interface. Possible values are:(0) False (Default)(1) True |
| Permission to Load Application | LoadApp | DWORD | 1 (WD0 (TS) | Specifies whether users are allowed to load applications into the file system cache.Possible values are:(0) False(1) True |
| Permission to Unload Applications | UnloadApp | DWORD | 0 (WD/TS) | Specifies whether users are allowed to unload applications from the file system cache.Possible values are:(0) False (Default)(1) True |
| Permission to Lock Applications | LockApp | DWORD | 1 (WD)0 (TS) | Specifies whether users are allowed to lock or unlock applications in the file system cache.Possible values are:(0) False(1) True |
| Permission to Manage File Type Associations | ManageTypes | DWORD | 1 WD)0 (TS) | Specifies whether the user can add, edit or remove personal file type associations but not global ones.Possible values are:(0) False(1) True |
| Permission to Trigger Publishing Refresh | RefreshServer | DWORD | 1 (WD)0 (TS) | Specifies whether a user is allowed to trigger a refresh from a MIME server. Possible values are:(0) False(1) True |
| Permission to Modify the OSD File | UpdateOSDFile | DWORD | 0 (WD/TS) | Specifies whether a user is allowed to use a modified OSD file. Possible values are:(0) False (Default)(1) True |
| Permission to Import Applications | ImportApp | DWORD | 0 (WD/TS) | Specifies whether users are allowed to import applications into the filesystem cache. Possible values are:(0) False (Default)(1) True |
| Permission to Change Publishing Refresh Settings | ChangeRefreshSettings | DWORD | 0 (WD/TS) | Specifies whether users are allowed to modify the refresh settings for servers (refresh on login and periodic refresh). Does not imply that the user can modify other server settings (path, host, etc.) Possible values are:(0) False (Default)(1) True |
| Permission to Manage Publishing Servers | ManageServers | DWORD | 0 (WD/TS) | Specifies whether users are allowed to add, edit or remove servers. Does not affect the users' ability to edit the refresh settings - this is controlled by the ChangeRefreshSettings permission. Possible values are:(0) False (Default)(1) True |
| Permission to Publish Shortcuts | PublishShortcut | DWORD | 0 (WD/TS) | Specifies whether users are allowed to publish shortcuts through the user interface. This does not affect shortcuts that are published during a publishing refresh. Possible values are:(0) False (Default)(1) True |
| Permission to View all Applications | ViewAllApplications  | DWORD | 0 (WD/TS) | Specifies whether users are allowed to view all applications through the user interface or only their own applications. Possible values are:(0) False (Default)(1) True |
| Permission to Repair Applications | RepairApp | DWORD | 1 (WD/TS) | Specifies whether users are allowed to use the Repair action on apps in SFTMime or the App-V Client Management Console. Possible values are:(0) False(1) True (Default) |
| Permission to Clear Applications | ClearApp | DWORD | 1 (WD/TS) | Specifies whether users are allowed to use the Clear action on apps in the App-V Client Management Console or the REMOVE verb without the /COMPLETE flag in SFTMime. Possible values are:(0) False(1) True (Default) |
| Permission to Delete Applications | DeleteApp | DWORD | 0 (WD/TS) | Specifies whether users are allowed to use the Delete action on apps in the App-V Client Management Console and the REMOVE verb with the /COMPLETE flag in SFTMime.. Possible values are:(0) False (Default)(1) True |
| Permission to Toggle into Offline Mode | ToggleOfflineMode | DWORD | 1 (WD)0 (TS) | Allows the users to select to run the client in Offline Mode. In Offline Mode the Application Virtualization client can launch loaded application even when it is not connected to an App-V Server. Possible values are:(0) False(1) True |

### Category: Client Interface

Registry Path: HKEY\_LOCAL\_MACHINE\Software\Microsoft\SoftGrid\4.5\Client\CustomSettings

| ADM Template Option | Registry Value Name | Type | Default Value(Decimal) | Description |
| --- | --- | --- | --- | --- |
| Tray: Always Run | TrayVisibility | DWORD | 0 (WD/TS) | Specifies whether the tray will run at startup and stay running after the last app shuts down (1) or only run when apps/options are in use (0). Applied the next time anything managed by the tray (message history dialog, options dialog, applications) closes |
| Tray: Success Display Delay | TraySuccessDelay | DWORD | 10 (WD/TS) | Specifies the time in seconds that the tray will display success messages like "Word launched" or "Excel shut down". If 0, those messages will be suppressed. Applied the next time an app launch or load starts. Set in seconds. The default is 10 seconds. Setting to 0 results in non error messages being suppressed.  |
| Tray: Show Refresh | TrayShowRefresh | DWORD | 1 (WD)0 (TS) | When present and set to 1 allows menu item “Refresh Applications” to be displayed on the Tray menu and accessible by the user. Applied on Tray Menu popup. |
| Tray: Show Load | TrayShowLoad | DWORD | 1 (WD)0 (TS) | When present and set to 1 allows menu item “Load Applications” to be displayed on the Tray menu and accessible by the user. Applied on Tray Menu Pop Up |

Registry Path: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SoftGrid\4.5\Client\Configuration

| ADM Template Option | Registry Value Name | Type | Default Value(Decimal) | Description |
| --- | --- | --- | --- | --- |
| Log Roll-over Count | LogRolloverCount | DWORD | 4 (WD/TS) | Defines the number of backup copies that are kept of the App-V log when it is reset.  The valid range is 0-9999.  The default is 4.  A value of 0 means no copies will be kept. |
| Log Max Size | LogMaxSize | DWORD | 256 (WD/TS) | Defines the size in Megabytes that the log file can reach before being reset.  The default size is 256 MB.  When this size is reached, a log reset will be forced on the next write attempt. |

# Conclusion

Using the ADM Template to manage App-V clients in the enterprise enables administrators to ensure that the settings on the clients are configured to the desired configurations. This will allow an organization to better support the App-V infrastructure. Careful consideration should be taken when planning an ongoing strategy for deploying the clients after the ADM Template settings have been deployed.

## More Information

To learn more about Group Policies, go to:
<http://technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx>