Best Practices for Configuration

Best Practices for Configuration

This section outlines the key points for consideration when setting up your Environment Manager configuration, and includes:

Assign Generic Computer Settings

Configure generic Action settings on a computer that is used by multiple users to ensure that common settings are applied to the computer for all users.

For example, map common drives or printers by default for all users in the **Computer > Startup** node.

Use Group Rules

Simplify the configuration with actions that apply to groups of users rather than individual users, where appropriate. This reduces the complexity of the configuration and ensures the XML run-time engine can execute the configuration faster, improving user log on times.

Group Similar Action Types

Creating large configurations by grouping similar action types, such as actions which lockdown applications, under a single node or as few sub nodes as possible.

Grouping similar actions types under a single node creates configurations which are less complex to navigate and actions can be ordered in execution sequence, as required.

For more information, see Execute Actions in Sequence.

Execute Actions in Sequence

Multiple actions grouped together under a single node may need to execute in a certain order.

For example, a sub node under the **User > Logon** node creates a folder, copies some files into the folder and sets attributes for those files. The folder must exist before the files are copied into it and the files must be present in the folder before the attributes can be set.

Order the actions in the **Actions** panel by clicking **Move left**, **Move right**, **Move up** or **Move down** in the **Arrange** ribbon group or by dragging them up or down the list. Once actions are correctly ordered, the actions execute in order from the top down.

For more information, see Group Similar Action Types.

Avoid including **Execute** actions in nodes set to execute in sequence for files which require user interaction to complete, such as program files. Otherwise, the logon process is halted indefinitely as the logon script waits for the **Execute** script to complete. For example, if the **Execute** action launches notepad.exe, the logon script waits for the Notepad to end before proceeding with the logon process.

Execute Nodes in Sequence

When related actions are not grouped together in the same node, it may be necessary to ensure the actions in one node are executed before the actions in another can take place.

A node can be dependent on any other parent node.

Use Environment Variables

Configure complex environments which span multiple operating system versions using environment variables.

For example, you may wish to launch an application from the system root drive of a computer. Under Windows 2000, the system root drive is C:\WINNT but under Windows XP it is C:\WINDOWS.

By utilizing an environment variable, such as %systemroot%\app.exe, the application can execute independent of the operating system on which it is hosted as the variable is expanded at runtime by the Environment Manager Agent on the specific machine.

If using environment variables, you can replace % with %% to stop an environment variable from expanding.

Environment variables can also be used for configuring system drive letters, user-based rules and managing profiles.

Configure Warning Messages

Configure warning messages when locking down applications so that users are aware that they have been prevented from

accessing the relevant application component or device.

Failure to configure a message may cause increased numbers of help desk calls and reduce user satisfaction.

Use Self Healing for Smaller File Sizes

When configuring Self Healing actions, it is recommended that only small files are configured to be self healed.

Targeting only small files reduces the resource load on the Environment Manager Agent during run-time.

Otherwise, self healing large files can raise the following issues:

- Resource load is significantly increased as the Environment Manager Agent creates backup copies of the files.
- Resource load is significantly increased as the Environment Manager Agent heals a large file.
- Stability issues may arise if administrative installed patches and software are added to the system, as the Environment Manager agent automatically self heals these changes and removes them from the registry.

Use Selective Registry Self healing

When configuring Self Healing Registry actions, it is recommended that only relevant sections of the registry are configured to be self healed.

Targeting only specific portions of the registry reduces the resource load on the Environment Manager Agent during run-time.

Otherwise, self healing the whole registry can raise the following issues:

- Resource load is increased as the Environment Manager Agent continually checks the whole registry structure for changes.
- Stability issues may arise if administrative installed patches and software are added to the system, as the Environment Manager agent automatically self heals these changes and removes them from the registry.

Only Self Heal 32-bit or 64-bit Processes

Currently only 32-bit or 64-bit applications are fully supported by the self healing mechanism. It is not recommended to self heal DOS or 16-bit applications.

Attempting to self heal a DOS or 16-bit application, may present multiple instances of the same application in a short period of time.

Only Self Heal Critical Components

When configuring Self healing actions using Environment Manager, it is recommended that only critical application and operating system components are self healed.

Self healing should only be used for important processes, files, services and registry keys that are critical to the day-to-day running of the system.

Non-critical items, such as user introduced shortcuts, non-corporate software and low key services should not require self healing.

Only Lockdown 32-bit and 64-bit Applications

Currently only 32-bit and 64-bit applications are fully supported by the Lockdown mechanism. It is not recommended to lockdown DOS or 16-bit applications.

Audit Lockdown and Self Healing Actions

Environment Manager can record important security and management events in industry standard formats such as the system event log, e-mail and SNMP through the Management Center.

Although Environment Manager deters the majority of users, effective auditing pinpoints those users who continually attempt to bypass system security. In particular, any attempts by users to plant Trojans or worms, or terminate installed security software, need to be identified.

Use Reusable Conditions

To reduce configuration size and speed up processing.

Use Reusable Nodes

To reduce configuration size and speed up processing.

Toggle the state of nodes or actions

For troubleshooting purposes

Use Sites

To ensure optimized personalization usage across geographical sites.

Use Application Groups

To share personalization settings between related applications, for example, MS Word and MS Excel.

Use Personalization Rollback on a per application basis

To speed up the provisioning of personalization data.

Use Personalization Analysis

To identify personalization bottlenecks and assign discovered applications to the Applications list or the Users Personalization Group Whitelist or Blacklist.

Use AppSense Policy Templates

To aid in the construction of configurations over time make use of AppSense Policy Templates which allow you to save and restore specific areas of a configuration.

Use Quick Setup Wizard

To create well known actions, use the Quick Setup Wizard which contains a number of recommended industry standard actions.

Blacklist Application

Ensure that any processes which are *not* required to be managed and are not in the Default Blacklist are added to the Personalization Group Blacklist.

Whitelist Application

As an alternative to managing all processes a Whitelist of managed applications can be created, this can help to reduce storage space and improve performance.

Only use Offline Mode for Mobile Devices

It is possible to configure Offline mode on a per Personalization Group basis. Enabling this option ensures that at user logoff the local personalization cache is persisted on the endpoint. It is recommended that this option only be applied to mobile devices to ensure disk space on the endpoint device is not unnecessarily consumed.

Use Folder Redirection

To ensure user data is available between different or concurrent sessions redirect well known folders to a central location such as My Documents on the user's home drive.

Working With Streamed Applications

When using AppSense Environment Manager with streamed applications, for example, Citrix XenApp, ensure the relevant exclusions are setup. For details refer to the Streamed Applications appendix.