



Key benefits

- ▶ Maintains environment in optimal state
- ▶ Maintains service levels
- ▶ Reduces cost of support
- ▶ Users focused on primary activities
- ▶ Ensures adherence to security policy

User Environment Management

Proactive System Protection is part of AppSense User Environment Management. User Environment Management enables users to receive a consistent yet contextual environment that is protected from unauthorized activity and responsive to users' needs. You can find out more information about User Environment Management by visiting

www.appsense.com/solutions/uem.

AppSense Management Center

AppSense Management Center increases visibility into user environments through centralized monitoring and reporting of end user activity. Secure and scalable deployment capabilities ensure users benefit from the latest profile and configuration settings.



- ▶ Real-time environment management
- ▶ Enterprise Deployment and Auditing
- ▶ x64bit supported

Proactive System Protection

Prevent unauthorized application use and manage software licences.

User environments can be seriously degraded by the introduction of unauthorized, unknown and potentially malicious applications. Not only can these rogue applications create an unpredictable and unstable working environment, they can also drain system resources and distract users from more productive activities. In short, these applications cause an unnecessary risk to the user environment and to the system infrastructure as a whole.

AppSense Application Manager proactively prevents unknown and unauthorized applications from running within the user environment. Unauthorized applications need never be known to the administrator in order to be stopped.

Trusted Ownership

By more effectively managing access to production applications, AppSense Application Manager provides opportunities to deliver ROI and reduce administrative costs and management overheads. This is achieved using a method that does not need to know the nature and source of the unauthorized application.

Using secure Kernel level filter drivers and NTFS security policies, AppSense Application Manager intercepts all execution requests and, with applied rules, blocks any unwanted applications. Once a set of User, Group and Client rules is defined, AppSense Application Manager locates and applies the best matching set of rules for each user. If no specific rules are found, then a default level of protection is applied, which will only allow Administrator installed applications to run. This is called Trusted Ownership.

AppSense Application Manager also provides control over many other types of application content, including Installing of ActiveX controls, Screen Savers, VBScripts, Batch files, MSI packages and Registry configuration files. Self-extracting zip archives are safely extracted using the built-in Zip Extractor.

Licence Management

Another common area of concern for Administrators is licensing - controlling what users have access to which application. AppSense Application Manager can limit the number of users or groups of users who have permission to run applications. Limits can be placed on the number of application instances running, the timing of when users run a program and for how long.

Key features

- ▶ Trusted Ownership
- ▶ Kernel level filtering of execution attempts
- ▶ Rules-based configuration (user, group, client, script)
- ▶ White and black list configurations
- ▶ Digital signature support
- ▶ Time-based application restrictions
- ▶ Software license control
- ▶ Passive monitoring
- ▶ Integrated Auditing events
- ▶ Archiving of banned files



Protection in context

Not only do users require various levels of protection, but users in varying contexts must also have appropriate protection. For example, a user in an Internet Café should have different application access from a user within the secure confines of the company LAN.

AppSense Application manager is able to use information about the user's context in order to determine the level of protection necessary. Parameters such as location, security posture of accessing device and time of day can be used in combination to establish a necessary level of protection.

Trusted Ownership

By integrating closely with NTFS security, AppSense Application Manager automatically protects the system without the need for complex configurations and constant management. A pre-determined list of 'trusted owners' quickly determines which applications are unwanted. By default, only Administrators and system are trusted, which ensures only applications installed by an Administrator or the system are allowed to run. Complete configurability means you can extend your trusted owner list as required.

Passive Monitoring

Monitor unauthorized execution attempts without preventing users from running the applications. Passive monitoring can be enabled or disabled on a per user, group or per computer basis and provides an extremely useful tool to accurately track user behaviour prior to full implementation.

Application Limits & Time Restrictions

Application limits can be used to enforce corporate license policies; ensuring only authorized users can run business applications. A further level of control over application access can be achieved by applying time restrictions so users can only run programs during certain hours and for a certain length of time.

Zip Files & Windows Installer Packages

Safely open Self-Extracting Zip files using the built-in Zip Extractor. Restrict access to Windows Installer packages by specifying rules governing which packages are allowed to run.

Intuitive user interface

A graphically rich user interface provides centralized management of rules. Wizard driven actions negate the need for complex, time consuming and error-prone scripting, and because Application Manager uses the MMC standard, all our consoles are able to 'snap-in' to create one location for all the AppSense products.

Rules-based Configuration

Application execution policies can be added for individual users, group or clients by adding rules. Each rule contains a white list of accessible items and a black list of prohibited items. Extended configuration of execution policies can also be applied on a rule-by-rule basis.

Digital Signatures

Add digital signatures to your configuration for advanced security. SHA-1 digital signature checking gives the Administrator peace of mind knowing that the applications and files installed on a system remain unaltered, maintaining system integrity and lowering maintenance costs. Creating digital signature groups allows for simplified management of larger and more complex configurations.

White and Black List Configurations

Process large numbers of files and folders seamlessly with white and black list configurations. Define black lists to protect against known threats and problem applications, or create white lists to guarantee only known and trusted applications can execute on a system.

VBScripts and Batch Files

Prevent attacks from malicious code and viruses by ensuring users can only invoke scripts that have been authorized by the Administrator. Scripts such as Windows Script Host files and DOS Batch files are validated against rules to see if they are allowed to run. Added security can be achieved by applying Digital Signature checks to ensure that script content remains unaltered.

Rules Analyzer Console

The Rules Analyzer console allows administrators to troubleshoot any issues with an applied configuration. XML-based log files provide simplified access to information on why an application was or was not allowed to run.

Platforms Supported

- ▶ Windows Server 2003, Vista, XP (x32bit and x64bit)
- ▶ Windows 2000 Professional and Server
- ▶ Windows Terminal Server (2000 or greater)
- ▶ Citrix Presentation Server™, Citrix XenDesktop™, Citrix Access Gateway™
- ▶ Application Streaming and Virtual Desktops

AppSense Management Suite



AppSense Management Suite provides comprehensive profile management, protected system environments and consistently responsive applications.

For more details visit the AppSense Website
www.appsense.com/management suite

Web links

- ▶ **To learn more about AppSense visit**
<http://www.appsense.com>
- ▶ **Download your free evaluation**
<http://www.appsense.com/downloads>

