

User Application Entitlement

Whether a user environment is delivered through server based computing, virtual or physical desktops, or any combination of the above, it is essential users receive only the applications they require and are unable to introduce unknown executables into the environment.

The use of unauthorized software is a primary factor in destabilizing user environments and the costs associated with rectifying a corrupt desktop can be significant. In a shared user environment such as server based computing, those costs are exacerbated when the action of one user impacts many. Current methods for enforcing application usage are limited to complex scripts or high maintenance black and white lists.

Trusted Ownership™

Using secure kernel level filter drivers and Microsoft NTFS security policies, AppSense Application Manager intercepts all execution requests within a Windows desktop and blocks any unwanted applications. Application entitlement is based on the ownership of the application, with default ownership being Administrator. By using this method, current application access policy is immediately enforced 'out of the box' without the need for scripting or list management, this is called Trusted Ownership™. In addition to executable files, AppSense Application Manager also manages entitlement to application content such as ActiveX controls, VBScripts, batch files, MSI packages and registry configuration files.

Not just applications

In addition to locally installed applications, AppSense Application Manager ensures outbound connection requests to UNC paths and URLs are also managed by entitlement, providing one solution for all application and network entitlement rules.

Contextual Entitlement

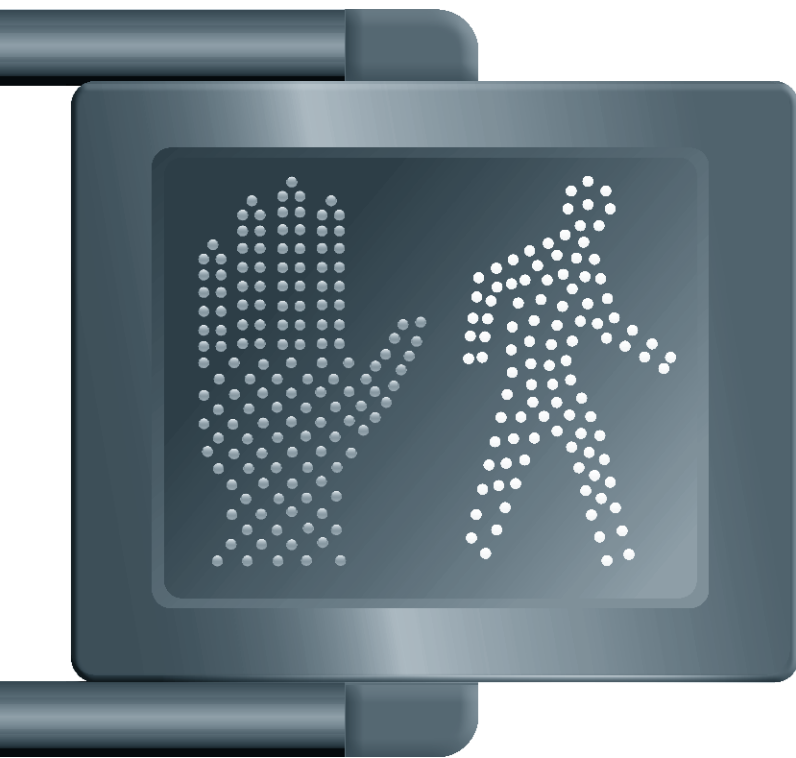
The extent to which an employee has access to corporate applications can depend on the context of the accessing device. For example, a user in an Internet Café will typically have a different level of application access from an employee within the secure confines of the corporate LAN. AppSense Application Manager is able to utilize information about the user's context in order to determine the level of entitlement necessary. Parameters such as location, firewall settings and even time of day can be used to establish a necessary level of entitlement.

Off-line Entitlement

With employees becoming increasingly mobile, it is imperative that entitlement rules are enforced when the user is not connected to the corporate network. AppSense Application Management ensures employees only access the applications and resources they have permission to when off-line by using entitlement rules on the endpoint device.

License Management

AppSense Application Manager is endorsed by Microsoft® for enforcing software license control in server based computing environments. Running the software in passive mode enables monitoring, auditing and reporting to detail the frequency of application access across the user and device base. By controlling which users or devices have permission to run named applications, limits can be placed on the number of application instances, which devices or users can run the application, the timing of when users run a program and for how long. License audits and access restriction based on number of licenses can now be enforced regardless of method of application delivery. Such license auditing can also be used in your virtual and physical desktop environments.



KEY FEATURES

- > Application Entitlement
- > End Point Analysis
- > Application Network Access Control
- > Software Licensing Control
- > Passive Mode Monitoring
- > Integrated Auditing Events

KEY BENEFITS

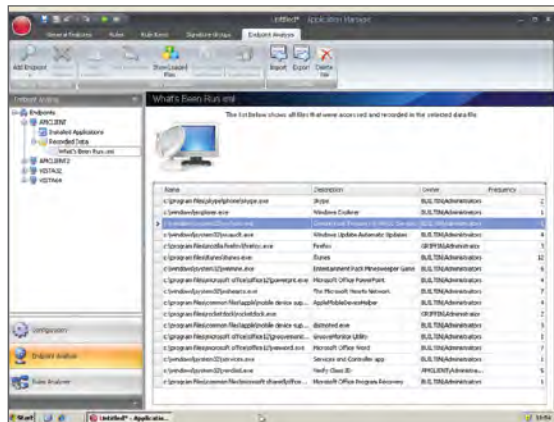
- > Maintain environment in desired state
- > Increased visibility into application landscape
- > Enforce licensing, ensure compliance
- > Reduces support calls
- > User acceptance

Trusted Ownership™

Protect the system without complex lists and constant management. Only code installed and owned by 'trusted owners' is allowed to execute. The trusted owners list can be extended to suit any environment or content directory infrastructure.

End Point Analysis

Identify all executable files on a target device and group the files into authorized and unauthorized to quickly create policy. Configurations can be deployed to a user, group of users, machine or group of machines. Within minutes, application entitlement will automatically control application usage.



Application Usage Scan

Scan a target device and identify how many times individual applications have been executed on a per user basis. By highlighting which applications are being used and which are not, unlicensed software can be identified and restricted and licensed software can be removed, reducing both the amount of applications on a device and the cost of licensing those applications.

Passive Monitoring

Monitor application usage without preventing users from running the applications. Passive monitoring can be enabled or disabled on a per user, device or group basis and provides an extremely useful tool to accurately track user behavior prior to full implementation or to understand application usage for software license management.

White & Black List Configurations

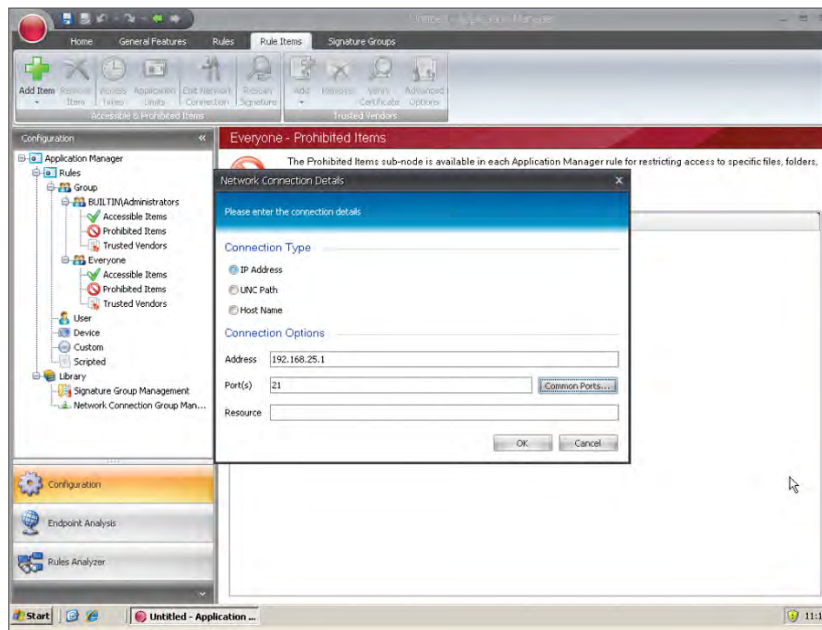
White & black List configurations can be used in conjunction with Trusted Ownership to control known applications which pass the NTFS owner check. Applications that users should not have access to such as administrator owned tools like cmd.exe or ftp.exe are automatically denied. Or, create white lists to guarantee only known and trusted applications can execute on a system.

Digital Signatures

Assign SHA-1 digital signatures to applications and files to ensure application integrity. Modified or spoofed applications are prevented from executing.

Application Network Access Control

Control network access without complex controls such as routers, switches and firewalls. Outbound connections from a target device are subject to entitlement rules. Connections include access to UNC paths (including all files & folders on that drive), servers, IP addresses, URL's, devices & FTP locations. Policy can be tailored to dynamically change based on user or device properties.



Self Authorizing Users

Allow nominated power users to execute applications they have introduced into the system. Applications can be added to a secure machine whilst outside the office without relying on IT support. A comprehensive audit details information such as application name, time and date of execution and device; furthermore, a copy of the application can be taken and stored centrally for examination.

Application Limits & Time Restrictions

Apply policy to control the number of application instances a user can run, along with at what times it can be run. Policy can be created to control or enforce licensing models by controlling application limits on a per device basis.

Extensive File Support

In addition to controlling applications such as .exe files, script, batch and registry files are also controlled. Digital signatures can also be applied to scripts to ensure content remains unaltered.

AppSense Configuration Templates

Take full advantage of pre-built corporate policy best practice by importing AppSense Configuration Templates. AppSense Application Manager is able to import an unlimited number of configuration files and use these configurations in combination. A selection of configuration templates such as 'common prohibited items' or 'End Point Analysis' is available from www.myappsense.com. This template library is maintained and updated frequently.



AppSense user virtualization solutions are used across all desktop and application delivery mechanisms to ensure users receive a consistent, predictable, compliant and responsive working environment while also reducing IT workload and desktop management costs.

AppSense ENVIRONMENT MANAGER
personalization and policy management

AppSense APPLICATION MANAGER
application entitlement

AppSense PERFORMANCE MANAGER
resource entitlement

To learn more about AppSense user virtualization solutions, please visit www.appsense.com

