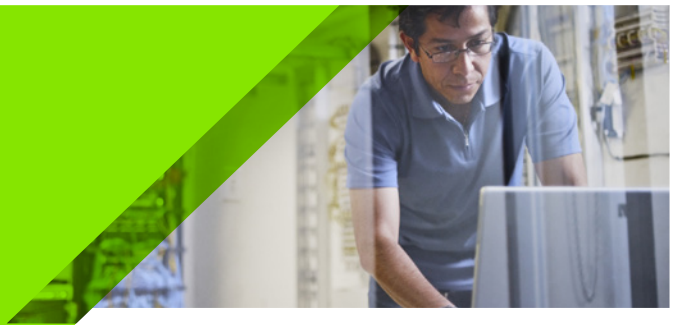
Product datasheet
AppSense Management Center

Centrally manage, deploy and report on user configurations across the enterprise



Key features:

- Multi-tier architecture
- Central management console
- Secure, enterprise-scalable deployment
- Role-based access control
- Configuration change control
- Automatic failover capabilities
- Events, alerts, reports and auditing system

Key benefits:

- Scale across thousands of users/servers/devices
- Scale across multiple delivery mechanisms
- Easy to use interface for rapid implementation
- Visibility into user environment and behavior
- Automated alerts and auto-fix reduces management overhead

Managing the user environment

Many organizations are using a mixture of server based computing, virtual desktops and local PCs to ensure desktop availability to an increasingly diverse workforce. Regardless of how a desktop is delivered to a user, it is essential the system is centrally managed and visibility into user and end point actions is available on-demand. Additionally, in enterprise environments where multiple sites exist, it is important that communication between management tools and end point devices remains continuously available and secure.

While using multiple delivery mechanisms provides the user with a flexible working environment, it often leaves IT spending additional time and resource trying to manage this disparate and changing infrastructure. The AppSense Management Center provides IT with the ability to control all aspects of the user environment from a central location, deploying tailored policy and user personalization settings to thousands of physical and virtual devices across many sites.

Although AppSense user virtualization products inter-operate with many other desktop management solutions, many of our customers choose the AppSense Management Center to manage the deployment of their AppSense configurations.

AppSense Management Center

The AppSense Management Center is a multi-tier system that enables scalability of policy and personalization data across multiple sites. This scalable architecture is also used to centrally manage and securely deploy user configuration information to thousands of endpoint devices and user environments.

Full back-end database management provides data replication for global data access.

Role-based access control is provided down to the object level, enabling roles to be assigned to groups of administrators.

As IT supports an ever increasing user base, full failover support is also fully integrated into the AppSense Management Center.

An intuitive solution

The management console has been designed to be easy to configure, manage and troubleshoot environment issues. The management console also provides visibility into personalization and policy data across the enterprise through a selection of reports, audits and graphical feedback capabilities. These reports are interactive, enabling granular drill-down on specific data and activities.

Early detection and correction

Should critical events occur, such as maximum resource usage, attempted unauthorized application access or corrupt personalization data, alerts are automatically raised to inform the business of potential disruption. In response to this, the system can also be configured to perform a series of automatic remedial actions to minimize IT intervention and user disruption. Such event monitoring and automated alerts provide instant visibility into the user environment along with the individual actions of each user, enhancing the ability for the business to plan ahead as opposed to reacting to situations as they occur.

About AppSense

AppSense is the global leader in user environment management (UEM) with over 3,500 enterprise customers worldwide that have deployed to over 8 million endpoints. AppSense DesktopNow and DataNow enable IT teams to deliver the ultimate user experience and productivity across physical and virtual desktops while optimizing security and reducing operational and infrastructure costs. The company is headquartered in Sunnyvale, CA with offices around the world.

Product datasheet
AppSense Management Center

AppSense Management Center features:

Active directory authentication

Tight integration with existing Microsoft Active Directory ensures all managed devices are authenticated before communications are established.

Client Communications Agent (CCA)

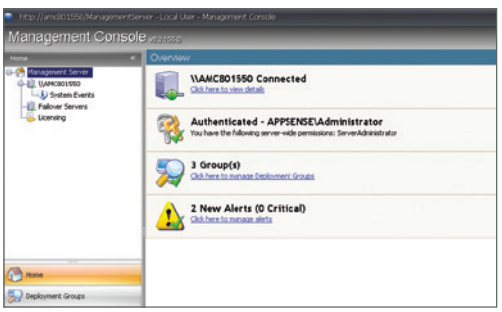
By utilizing Windows Management Instrumentation (WMI) the CCA can be installed on devices in any existing Management Center Directory Group or Computer Group. The CCA securely handles all communications between the device and the management server, adding the device to the correct deployment group, managing packaged installations and collecting and transferring audit data.

Automatic client registration

Any new device added to an environment automatically registers itself with the management server via the CCA. Based on membership rules, the properties of the device are used to automatically add it to the correct deployment group and automatically deploy the correct policy to the device.

Reporting

An interactive set of reports are used to monitor and audit user environment actions across the entire enterprise. Flexible options for grouping and filtering audit data means reports can be customized to show relative information to meet your business requirements, enabling forward planning and a move away from a reactive management approach.



Role-based access control

Provides granular control of access rights on all management server objects such as deployment groups, reports, packages and alerts. Based on a flexible role architecture, management server administrators can be granted read only or full access to each object on a per user basis.

Secure web-based communications

All data transfer and communications between the management server and target device are securely managed across HTTPS.

Watchdog agent

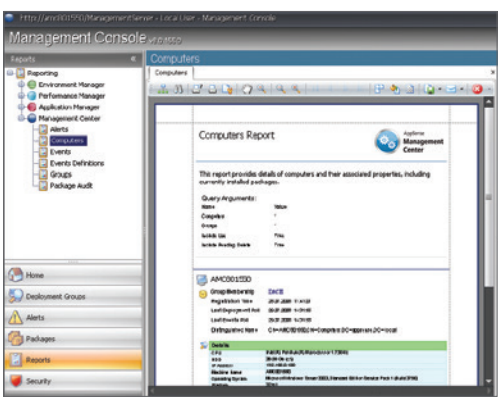
A Watchdog Agent resides on every managed device. Should any of the AppSense agents stop unexpectedly or become unstable, the Watchdog will automatically audit the detected error and if configured, raise an alert and take corrective actions to restart the agent.

Configuration check-out process

Single user configuration check-out supports multiple administrators simultaneously opening and editing configurations. Upon access to the management object (subject to Role-based Access Control), any objects already open by another user are available as read only. Metadata tags can be added as a description when saving back a new configuration version to the database.

Failover support

Multiple servers can be designated as an AppSense management server. Should the link to the current management server fail, the CCA will re-connect to a different server allowing for full failover support and continuous communication between the end point device and the management server.



Management Suite installer

The new Management Suite installer is used to install all or selected components of the AppSense Management Suite. During installation, the installer checks for all required prerequisites and offers to install if required.

Management of Server Configuration

The server configuration enables the administrator to easily configure parts of the Management Center framework such as the Microsoft Internet Information Server (IIS) and Microsoft SQL Server. The administrator is also presented with options to fine tune settings and if conflict arises, repairs are suggested. Support reports can also be generated and sent to AppSense Support.

Agent installation schedule

Options and controls of when AppSense agents are installed on endpoints enable enterprises to introduce or upgrade AppSense components without impacting the lite user desktop session. Options include:

- Immediately
- At next computer startup
- Any scheduled time

End-user postponement

Users can be empowered to postpone installations to a more convenient time if permitted to do so by IT, to a time frame given by IT.