Kaseya® Desktop Policy Management

Automated Desktop Policy Management with
the power of Intel vPro.

Overview

For many IT Administrators keeping users settings aligned with corporate policy can be a challenging task, often it can be difficult to even know what needs to be enforced. KDPM allows you to take stock of your environment and effectively manage desktop policy by enforcing; mapped drives, mapped printers, security settings, desktop look and feel, browser and productivity application settings.

KDPM allows Administrators to centrally control power settings on all Windows machines and so ensure all machines adhere to your corporate power policy. Powerful savings reporting allows you to calculate the savings to your business.

KDPM also brings powerful Out of Band management by teaming up with the market leading manufacturer, Intel®. This technology partnership brings last-mile remote management into the hands of all Kaseya customers.

Key Benefits

- Improved response times to OS failures by utilizing Out of Band technology in Intel® vPro™
- Desktop standardization increases efficiency of staff by providing a consistent capability across the business
- Power policies allow you to make energy savings and ensure your Green IT credentials
- Improved Security by centrally controlling important system settings and removing user interference with corporate governance
- Support overhead is lowered as a know environment is easier to support and quicker to put right through automation

Features

Policy Enforcement
KDPM Policy Enforcement gives control over all the critical settings you need for core Desktop Policy enforcement. You can create a corporate standard from a 'Golden Machine' and then enforce those primary system and application settings across all your Windows Desktops*. Specific Policy's that vary across the organization such as drive and printer mappings can be set by group.
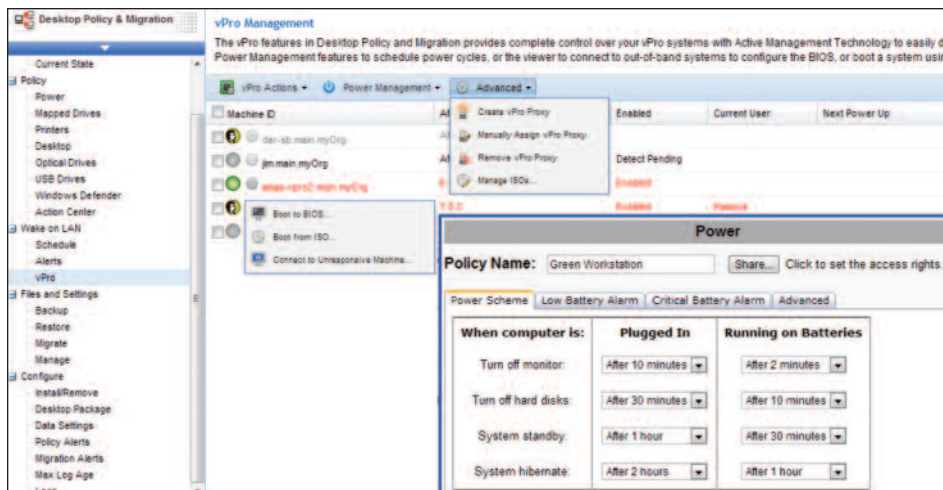
Using the Core Kaseya K2 functions, IT administrators can also layer the following capabilities onto their machines using the File, Network and Application protection functions:

- File Access Policies – Totally restrict access to a file or restrict to only being opened via allowed applications
- Network Access Policies - Permit or deny application access to the network per application, and track network usage by computer and/or application
- Application Access Policies - Select one or several applications and block access

Green IT
Join the many businesses today that are benefiting from KDPM's power policy management. KDPM's power policy enables you to create new power profiles based on corporate policies, such as monitor and hard drive standby times, suspension and hibernation settings – and to deploy them across your entire environment.

Kaseya provides dashboards to help you compare compliancy of the current environment to your company's policy and gives automated reports to gauge power savings across the organization based on information from your environment and energy prices.

Security related policy items allow enforcement of data protection standards by stopping files from being removed from machines via USB or Optical Drive.

- Desktop Standard – Automatically create a policy with accessibility, appearance, keyboard and sounds, as well as core productivity application settings such as Office and Internet Explorer.
- Add and Remove Mapped Drives – Keep access to data available to keep users productive
- Add and Delete Printers – As well as setting up Printers having a central record makes diagnosis and fixing printer mapping issues simple
- USB Drives – Allows you to switch off access to files via USB from drives and even USB devices such as an Android phone without effecting Human Interface devices such as keyboards or mice.
- Optical Drive Access – Keep corporate data on the network, not wandering off site on a DVD.
- Windows Defender – Whatever your corporate policy; on or off - enforcing it is simple.
- Action Center – Notifications from Action center can often lead users to raise unnecessary tickets or try changing settings themselves, now you can avoid these issues.
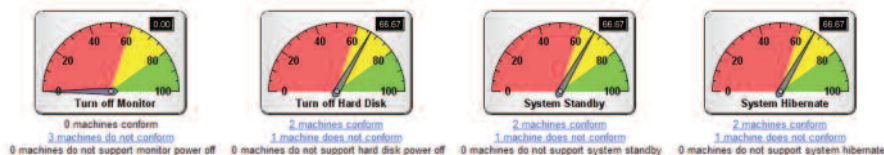
Enhance vPro Features

vPro Detection and Enablement

KDPM can directly scan and automatically detect the vPro capabilities on machines through the Kaseya Agent and once detected, machines can then be enabled remotely. This saves having to manually intervene on each machine to enable vPro through the BIOS.

- Detect which machines vPro is present on
- Enable and disable vPro through central console
- Centrally manage vPro passwords
- Set local Proxy for remote OOB connections (any machine)
- Enable certificates for Enterprise authentication

OOB Power Management

Using a combination of Intel vPro and Kaseya technology KDPM offers a broad array of power management options, including 'hard' power options, which will in effect pull the plug on a machine allowing you to reset even completely frozen machines, avoiding costly machine side visits.

- Power Up - Powers up the vPro machine immediately.
- Windows Shutdown - Shuts down the machine immediately.
- Force Power Down - Forces a power down immediately. Equivalent to pulling the plug on the machine.
- Schedule Power Up - Schedules a power up.
- Schedule Windows Shutdown - Schedules a Windows shutdown.

AMT Functions

Intel® AMT™ is part of the Intel Management Engine, which is built into PCs with Intel vPro technology. Like the other vPro functions these are all available Out of Band. In this release KDPM supports the following AMT management options:

- Boot to BIOS – Reboot the machine into BIOS mode and remotely edit the BIOS
- Boot from ISO – Reboot the machine and connect to an ISO image to boot the machine from
- Connect to unresponsive Machine – start a remote console session to a machine even if the OS has hung, allowing diagnosis and remediation

About Kaseya

Kaseya is the leading global provider of IT Systems Management software. Kaseya solutions empower virtually everyone — from individual consumers to large corporations and IT service providers — to proactively monitor, manage and control IT assets remotely, easily and efficiently from one integrated Web-based platform.

Go to www.kaseya.com/download for a FREE trial.

Visit: www.kaseya.com | Email: sales@kaseya.com | Like: Facebook.com/KaseyaFan | Follow: @KaseyaCorp

Experience increased productivity while pro-actively promoting energy efficiency.

"vPro and Kaseya maximize how much we can do remotely, which is crucial to lowering our costs and protecting our margins."

Mario Santiago
President and CEO
Sabio

Minimum System Requirements

System Requirements vary based on number of endpoints managed

Kaseya Desktop Policy Management Client Requirements

- *Microsoft Windows XP SP3 or later, Windows Vista and Windows 7
- vPro capabilities require Intel vPro chipset
- AMT Console connect (KVM) requires Intel AMT 6.1 or later

Kaseya Server Requirements

- Single processor (Intel Xeon 3 Ghz Dual Core, 1066 Mhz front side bus, 4MB cache)
- 8 GB RAM
- 3x73Gig 10k SAS (hardware RAID 5)
- Microsoft Windows Server 2003 or 2008 Standard Edition 64 Bit 2
- Microsoft SQL Server 2005 or 2008 32 Bit (with AWE enabled) or 64 Bit 3

www.kaseya.com