

LANDesk Security Suite

Mit der LANDesk Security Suite können Sie eine verbindliche Sicherheitsrichtlinie in Ihrem Unternehmen planen und umsetzen, die Sie zentral über eine Konsole steuern und überwachen. Die LANDesk Security Suite bietet Ihnen darüber hinaus die Möglichkeit, die von Ihnen getroffenen Maßnahmen auf Ihre Konformität mit Sicherheitsstandards wie *Payment Card Industry Data Security Standards (PCI DSS)*, *National Institute of Standards and Technology (NIST)*, *National Security Agency (NSA)*, *Federal Information Security Management Act (FISMA)* hin zu überprüfen und Abweichungen jederzeit zu reporten bzw. nicht konformen Geräten den Zugriff auf Ihre Infrastruktur zu verwehren.¹

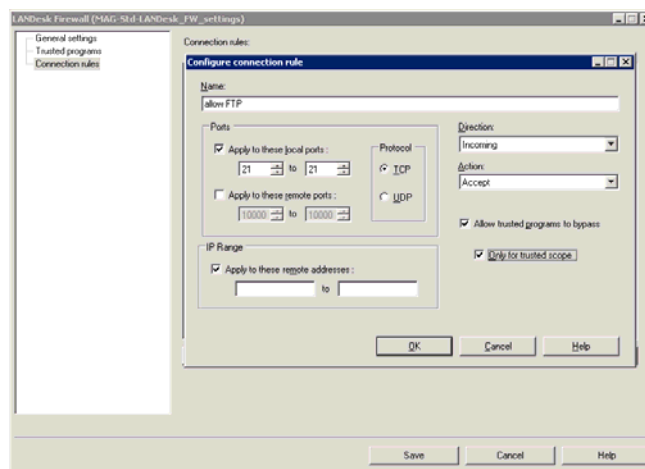
Sie schützen mit der LANDesk Security Suite unternehmenskritische Infrastruktur vor Zero-Day-Attacken, identifizieren potentielle Risiken und beseitigen diese automatisch. Mittels der Mechanismen der LANDesk Security Suite können Sie darüber hinaus den Zugriff auf unternehmenskritische Daten durch Unbefugte jeder Zeit protokollieren und unterbinden, auch wenn sich diese Daten auf externen Speichermedien befinden sollten.

Die LANDesk Security Suite ist mehrschichtig aufgebaut. Dies ermöglicht eine einfache Individualisierung der Sicherheitsmaßnahmen und eine nahtlose Integration der einzelnen Bausteine in bestehende Sicherungskonzepte. Neben der LANDesk Antivirus Lösung bietet Ihnen die LANDesk Security Suite die Möglichkeit die Antiviren-Lösungen anderer Hersteller und die Windows Firewall zu managen.

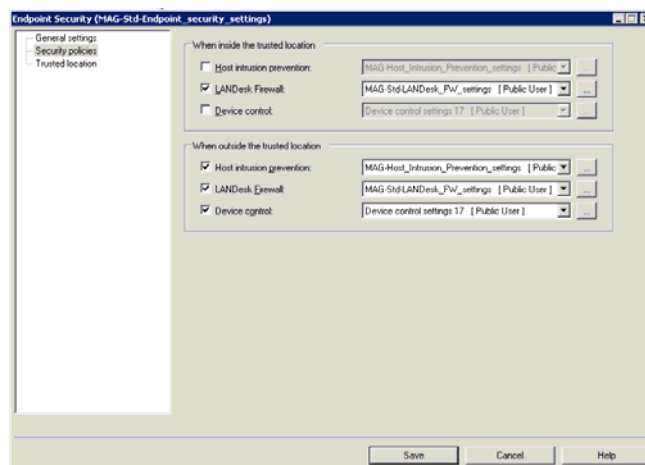
¹ optionales Modul *LANDesk Network Access Control*

LANDesk Personal Firewall

Die LANDesk Personal Firewall senkt die Wahrscheinlichkeit eines Angriffs auf Ihre Netzwerk-Clients, in dem sie den Zugriff eines Computers auf autorisierte Netzwerkdienste und IP Adressen begrenzt.

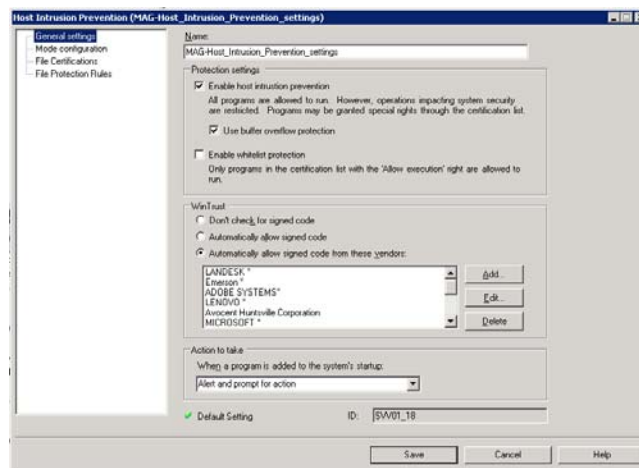


Dabei kann die LANDesk Personal Firewall abhängig von der Umgebung in der sich das Gerät befindet, Sicherheitsrichtlinien zu- oder –abschalten oder gegen andere austauschen (location-aware policies). Sie können somit für mobile Geräte jederzeit den optimalen Schutz sicherstellen.

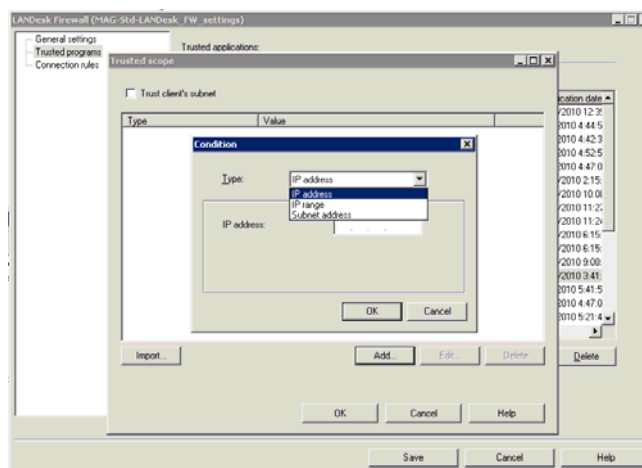


Host Intrusion Prevention

LANDesk Host Intrusion Prevention (HIPS) schützt Ihre Infrastruktur in der Zeit, die der Hersteller der Software für die Beseitigung eines Fehlers benötigt, der einen Missbrauch des Systems erlaubt. HIPS benötigt dafür kein Wissen über den eigentlichen Fehler. Vielmehr stellt HIPS das böswillige Verhalten der Software fest und blockiert deren Ausführung.



Mit White- und Blacklisting stehen dem Administrator darüber hinaus mächtige Mittel zur Definition einer autorisierten Softwarelandschaft zur Verfügung, die auch dann aufrecht erhalten wird, wenn der Computer gerade nicht mit dem Firmennetzwerk verbunden ist.





Magelan

Ihr Partner für optimales IT-Management

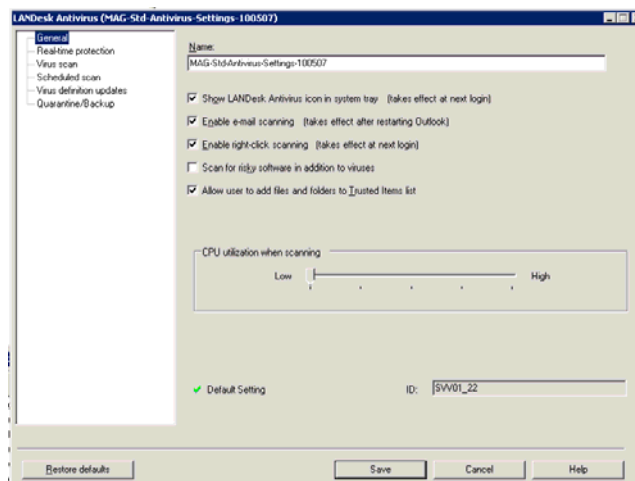
Die Erstellung der Listen kann innerhalb einer definierten Lernphase oder über eine Rechnergruppe von Pionieren erfolgen.

LANDesk Antivirus

Mit Antivirus bietet LANDesk einen in die LANDesk Security Suite integrierten Viren- und Root-Kit-Schutz, der auf Kaspersky Antivirus basiert. Die Antivirus Lösung kann sowohl so konfiguriert werden, dass sie ohne Zutun des Benutzers

- zu festgelegten Zeiten einen Voll-Scan des Clients
- eine Echtzeit-Überwachung definierter Dateitypen
- eine Überwachung des E-Mail-Postfachs

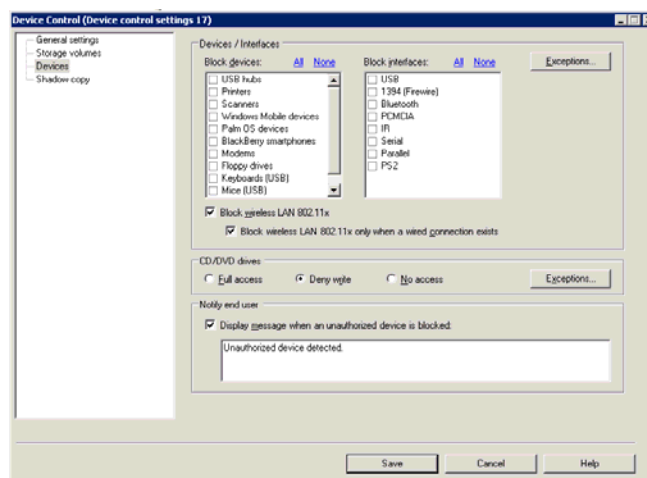
durchführt, als auch Dateien auf Anforderung des Benutzers auf Infektionen untersucht.



Dabei bietet LANDesk Antivirus die Möglichkeit, die Systemlast für den Scan-Vorgang so anzupassen, dass eine Beeinträchtigung des Benutzers möglichst gering ist.

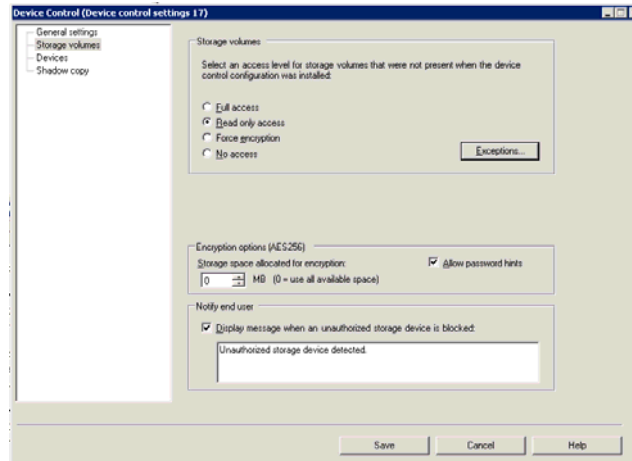
LANDesk Device Blocking

Der LANDesk Device Control Manager erlaubt es Ihnen, Zugriffe auf Geräte (z.B. USB Hubs, Scanner, RIM Blackberry) und Schnittstellen (z.B. USB, IEEE 1394 aka Firewire, Bluetooth, PCMCIA, Seriell, Parallel) zu protokollieren, einzuschränken oder auch zu unterbinden.

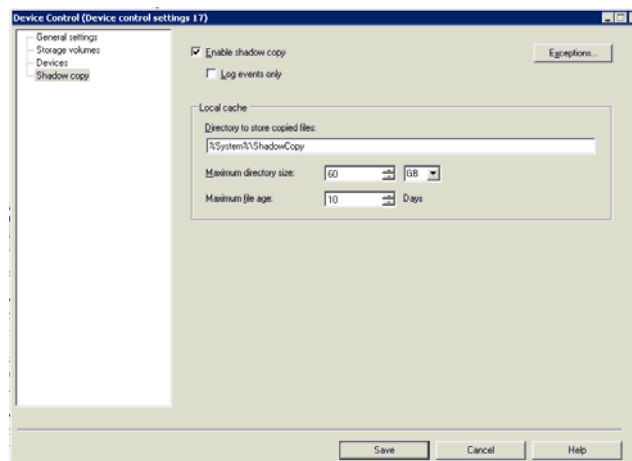


Sie können darüber hinaus den Zugriff auf externe Massenspeicher kontrollieren. So können Sie durch die Erlaubnis ausschließlich lesenden Zugriffes auf externe Massenspeicher Datenverlust und –diebstahl unterbinden.

Der LANDesk Device Control Manager kann so konfiguriert werden, dass Daten ausschließlich verschlüsselt auf externen Speichermedien abgelegt werden können. Sie können so durch den Einsatz starker Verschlüsselung (AES-256) die Preisgabe sensibler Informationen durch den Verlust eines externen Speichermediums verhindern.



Mittels der Funktion *Shadow Copy* können Sie den Weg der Daten von und auf den Client jederzeit an Hand eines Protokolls aller Aktivitäten oder an Hand tatsächlicher Schattenkopien nachvollziehen.



Security Activity

Über das Tool Security Activity werden die Sicherheitsstati der überwachten Geräte je LANDesk Security Modul in Echtzeit zusammengefasst. Darüber hinaus besteht die Möglichkeit eine Bereinigung der Protokolle zu planen.

The screenshot shows the 'Security activity' window. On the left is a tree view with categories like 'Infections by computer', 'Host intrusion prevention', 'LANDesk Firewall', and 'Device Control'. The main area displays a list of applications with columns for Application, File version, File size, File date, MD5 Hash, and Affected Computers. Below this is a section titled 'Computers reporting intrusions for the above application or action' containing a table with columns for Display Name, Description, Action Date, Action, Application, Mode, and File size.

Application	File version	File size	File date	MD5 Hash	Affected Comp...
FILEZILLA.EXE		7569920		8edb5d8e2166...	1
ITUNES.EXE		10358568		ee4c97a0769af...	1
MDCRASHREPORTTOOL.EXE		19744		58847353039b...	1
MDSRESPONDER.EXE	2.0.1.2	345376		ebad0f51d8d4d...	1
MSFEEDSSYNC.EXE		12288		cce78619f0826...	1
PCDRSCUIW32.EXE	6.0.5450.12	909296		0ab807856536...	1
PCDRREALTIME.PSX		104432		67e4ab72236b...	1
SPOOLSV.EXE		558080		89e8550c5862...	1
SUSERVICE.EXE		28672		dbbd685f75aff...	1

Display Name	Description	Action Date	Action	Application	Mode	File size
192.168.1.100	213.239.222.5 443	5/14/2010 7:07:28 PM	A disallowed network con...	%PROGRAM FILES% (X8...	Action was allowed (auto-1...	7569920