



OPTION FÜR USB- und PORTSICHERHEIT

Kundenlisten, Entwürfe, Code-Namen, Kennwörter, Kontoinformationen – welche Informationen werden heute aus Ihrem Netzwerk kopiert? Heute ist es einfacher denn je, unberechtigt Daten zu kopieren: auf USB-Sticks, CD/DVD-R, FireWire, PDAs... und auf die gleiche Weise gelangen Viren, Spyware und illegale Inhalte in das Netzwerk. Die Option für USB- und Portsicherheit (UPS – USB and Port Security) bietet Ihnen Schutz.

Durch die unzähligen tragbaren Speichermedien ist es für Unternehmen unerlässlich geworden, die Verwendung bestimmter Geräte, die potentiell Gefahr für das Unternehmen darstellen, zu verbieten oder zumindest zu überwachen. Vertrauliche Daten können problemlos auf ein tragbares Gerät kopiert werden, Viren können auf das Netzwerk übertragen und unternehmensweit verbreitet werden, und illegale Software oder Inhalte können auf das Netzwerk eines Unternehmens kopiert werden. Die UPS-Option von Desktop Authority ermöglicht die zentralisierte Kontrolle über Benutzerzugriffe auf eine Vielzahl von Datengeräten und Speichermedien.

FLEXIBLE SICHERHEIT

Durch die hochpräzise Kontrolle über jede Art von Geräten können Unternehmen den Zugriff auf bestimmte Geräte auf einen schreibgeschützten Zugriff begrenzen. Benutzer können dann beispielsweise CDs oder DVDs lesen, jedoch nicht brennen. Darüberhinaus können mithilfe von Berechtigungsätzen für die einzelnen Geräte verschiedene Zugriffsbeschränkungen an verschiedene Benutzer oder Gruppen vergeben werden.

Auf Berichte zu Konfiguration und Benutzerportaktivität kann zentral zugegriffen werden.

VALIDATION LOGIC

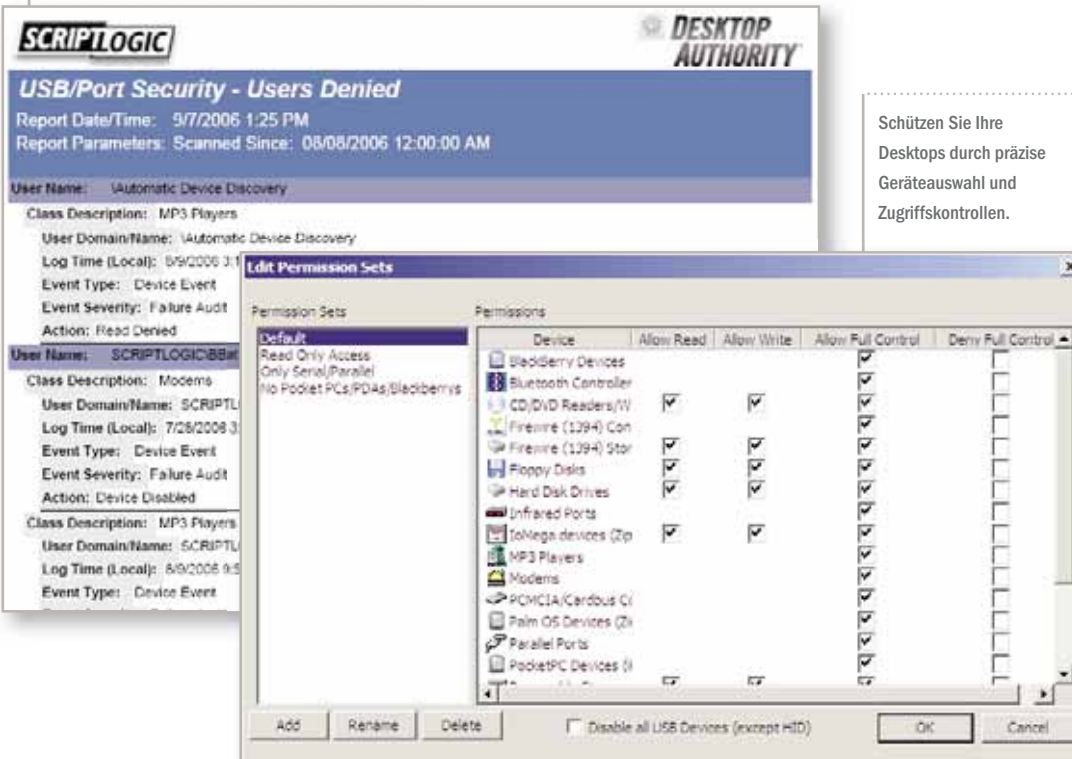
Mit der patentierten *Validation Logic*-Technologie von Desktop Authority kann der Administrator festlegen, für welche Desktops Gerätebeschränkungen eingesetzt werden. Als Kriterien können AD-Gruppen, AD-Standorte, IP-Subnets, Computerklassen und vieles mehr verwendet werden.

UMFASSENDE VERWALTUNG

Die UPS-Option von Desktop Authority schützt das Unternehmensnetzwerk vor unrechtmäßiger Verwendung von Geräten und Ports. Dazu gehören:

- Austauschbare Speichermedien – USB-Sticks, ThumbDrives, tragbare Medien
- USB
- Seriell/parallel/Infrarot
- NIC Adapter
- Festplatten
- CD-/DVD-R-Laufwerke
- MP3-Player
- Digitalkameras
- Firewire
- Bluetooth/WiFi
- Modems
- Diskettenlaufwerke
- PDAs
- Flashspeicher
- Zip-/Jaz-Laufwerke

Schützen Sie Ihre Desktops durch präzise Geräteauswahl und Zugriffskontrollen.



09-06

HAUPTVORTEILE

Schutz vor Datendiebstahl

Sie bestimmen, wie Daten in Ihr Unternehmen gelangen und wie sie es verlassen!

Angriffe und Prozesse verhindern

Verhindern Sie, dass Benutzer Spyware, Viren, illegale Inhalte und Software in das Netzwerk einbringen, und verhindern Sie, dass wichtige vertrauliche Informationen in falsche Hände geraten.

Legitime Aktivitäten zulassen

Beschränkungen können den schreibgeschützten Zugriff zulassen, beispielsweise wenn Benutzer Schulungsmaterial auf DVD-R lesen müssen. Mit Berechtigungssätzen können Administratoren austauschbare Speichermedien zur Problembeseitigung verwenden, ohne Benutzern die gleichen Berechtigungen zu erteilen.

Zentrale Verwaltung und Berichterstattung

Konfiguration und Berichterstattung werden ausschließlich in der Desktop Authority-Verwaltungskonsolle ausgeführt. Dies ermöglicht eine unternehmensweite Verwaltung von einem einzigen Ort aus.

HAUPTFUNKTIONEN

Präzise Konfiguration

Beschränkungen können für einen bestimmten Gerätetyp festgelegt werden, wie z. B. *BlackBerry* oder USB-Flashlaufwerk, oder für einen Porttyp wie *Bluetooth*. Der Zugriff kann für jedes Gerät festgelegt werden: Leszugriff, Schreib- und Lesezugriff, Uneingeschränkter Zugriff oder gar kein Zugriff.

Desktopwarnungen

Benutzer werden sofort darauf hingewiesen, wenn sie einen nicht autorisierten Vorgang ausführen möchten (z. B. Anschließen eines nicht autorisierten MP3-Players).

Zentrale Berichte

In den Berichten können Administratoren alle Zugriffsversuche auf beschränkte Aktivitäten einsehen, einschließlich wer auf eine Aktivität zugreifen wollte, wann, wo und auf welchen Aktivitätstyp.

SYSTEMANFORDERUNGEN

Verwaltung

Desktop Authority 7.5 oder höher.

Clientunterstützung

Windows 2000 SP4 & URP1, XP SP2.

LIZENZIERUNG

Desktop Authority wird **pro Arbeitsplatz** lizenziert. Die UPS-Option wird separat **pro Arbeitsplatz** lizenziert.

DR. MORAWIETZ
OFFICE SOFTWARE & SYSTEMHAUS
Schwanheimer Straße 144a
64625 Bensheim
Telefon: +49 (6251) 10 58-0
ScriptLogic@MORAWIETZ.de
www.morawietz.com

