

Technische Fragen.

Q. Ist DeviceLock Software oder Hardware?

A. DeviceLock ist Software.

Q. Was tut DeviceLock genau?

A. DeviceLock kontrolliert den Benutzerzugriff auf verschiedene Typen von Computergeräten (wie USB- und FireWire-Ports, Bluetooth- und Wi-Fi-Adapter, CD-ROM-Laufwerke usw.). DeviceLock erlaubt es Administratoren, den Zugriff auf Geräte für einen Benutzer zu sperren und gleichzeitig den Zugriff auf diese Geräte für einen anderen Benutzer zu erlauben.

NetworkLock, eine Erweiterung von DeviceLock, bietet Kontrolle über Netzwerkkommunikationen. Administratoren können Benutzerzugriff zuweisen für die Protokolle FTP, HTTP, SMTP, Telnet, Instant Messenger (ICQ/AOL Instant Messenger, Windows Live Messenger und Windows Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), Webmail- und Social-Networking-Anwendungen (Gmail, Hotmail, Yahoo! Mail, mail.ru, web.de, gmx.de; Facebook, Myspace, LinkedIn, LiveJournal, Odnoklassniki, Vkontakte, Twitter).

ContentLock, eine weitere Erweiterung von DeviceLock, extrahiert und filtert den Content von Daten, die auf entnehmbare Laufwerke und Plug-and-play-Speichergeräte kopiert oder über das Netzwerk übertragen werden. Administratoren können Regeln erstellen, die festlegen, welcher Content kopiert und übertragen werden darf.

Q. Ist DeviceLock Verschlüsselungssoftware, d.h. verschlüsselt es die Daten?

A. Nein. DeviceLock verschlüsselt keine Daten. Es kontrolliert nur den Benutzerzugriff auf Geräte.

Q. Wie schützt DeviceLock Daten?

A. Die Zugriffssteuerung für Geräte funktioniert auf folgende Weise: DeviceLock fängt jede Anfrage eines Benutzers an ein Gerät ab. Dann überprüft DeviceLock, ob dieser Benutzer berechtigt ist, dieses Gerät zu verwenden oder nicht. Wenn der Zugriff erlaubt ist, wird die Anfrage an das Gerät weitergegeben. Andernfalls erhält der Benutzer eine „Zugriff verweigert“-Nachricht und er kann nicht auf dieses Gerät zugreifen.

Die Zugriffssteuerung für Protokolle funktioniert auf folgende Weise: Jedes Mal, wenn ein Benutzer auf eine entfernte Netzwerkressource zugreifen möchte, fängt DeviceLock diese Verbindungsanfrage auf der Kernel-Ebene des OS ab und prüft die Benutzerrechte in der geeigneten Access Control List (ACL). Wenn der Benutzer keine Berechtigung hat, auf dieses Protokoll zuzugreifen, wird eine Fehlermeldung „Access denied“ zurückgegeben.

Q. Welche Geräte kann DeviceLock kontrollieren?

A. USB-Ports, FireWire (IEEE 1394)-Ports, serielle (COM) Ports (einschließlich interne Modems), parallele (LPT) Ports, Infrarotports (IrDA), Bluetooth-Adapter, Wi-Fi-Netzwerkadapter, CD- und DVD-Laufwerke (einschließlich beschreibbare Laufwerke), Diskettenlaufwerke, Bandgeräte, alle entnehmbaren Speichergeräte (einschließlich

Memorysticks, Flash-Geräte, externe Festplatten, ZIP-Laufwerke usw.), alle Arten von Drucker, einschließlich lokale, Netzwerk- und virtuelle Drucker, die Windows-Zwischenablage, Windows Mobile, BlackBerry, iPhone, iPod Touch, iPad und Palm OS-basierte PDAs und Smartphones.

Q. Welche Netzwerkprotokolle und Anwendungen können von DeviceLock kontrolliert werden?

A. Die Protokolle FTP, HTTP, SMTP, Telnet, Instant-Messenger (ICQ/AOL Instant Messenger, Windows Live Messenger und Windows Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), Webmail- und Soziale-Netzwerk-Anwendungen (Gmail, Hotmail, Yahoo! Mail, mail.ru, web.de, gmx.de; Facebook, Myspace, LinkedIn, LiveJournal, Odnoklassniki, Vkontakte, Twitter).

Q. Läuft DeviceLock unter UNIX (Linux, FreeBSD, usw.) oder Mac?

Q. Läuft DeviceLock unter Windows 95, Windows 98 oder Windows Me?

A. Nein. DeviceLock läuft nur unter Windows NT 4.0 SP 6, Windows 2000, Windows XP, Windows Vista, Windows 7 oder Windows Server 2003/2008.

Es gibt jedoch ein Produkt namens DeviceLock Me (ohne Support), das unter Windows 95/98/Me laufen kann. DeviceLock Me hat im Vergleich zu DeviceLock eingeschränkte Funktionalität – es kann keine USB-, FireWire-, Bluetooth-, Wi-Fi- und Infrarot-Geräte kontrollieren.

Q. Muss DeviceLock auf jedem Rechner im Netzwerk oder nur auf dem Server installiert sein?

A. DeviceLock muss auf jedem Rechner installiert sein, auf dem die Kontrolle des Benutzerzugriffs auf Geräte erforderlich ist. DeviceLock hat einen kleinen Agenten (DeviceLock Service), der für Benutzer unsichtbar ist und auf jedem Rechner läuft.

Q. Unterstützt DeviceLock entfernte Netzwerksteuerung?

A. Ja. DeviceLock hat eine zentralisierte Steuerungskonsole. Administratoren können DeviceLock-Agenten auf jedem Rechner in ihrem Netzwerk von dieser zentralen Konsole aus einsetzen.

Q. Kann DeviceLock entfernt auf den Netzwerkrechnern eingesetzt werden?

A. Ja. Administratoren können DeviceLock-Agenten auf jedem Rechner im Netzwerk von der zentralen Konsole aus einsetzen. DeviceLock-Agenten können auch in einer Active Directory-Domäne unter Verwendung des MSI-Installationspakets und Group Policy eingesetzt werden.

Q. Muss ich mich manuell mit jedem Rechner verbinden, um die Berechtigungen dort zu verändern?

A. Sie können es manuell tun, indem Sie sich mit jedem Rechner verbinden. Alternativ, können Sie, wenn Sie ein großes Netzwerk haben, mit Hilfe des Plugins Set Service Settings von DeviceLock Enterprise Manager gleichzeitig Berechtigungen auf jeder

beliebigen Anzahl von Computern einstellen. Darüber hinaus können Berechtigungen in DeviceLock in einer Active Directory-Domäne über die Group Policy verwaltet werden.

Q. Können Benutzer die Sicherheit durch DeviceLock auf ihrem lokalen Rechner umgehen, d.h. können sie DeviceLock deaktivieren?

A. Nein. Nur Benutzer mit Administratorrechten können DeviceLock steuern. Wenn Ihr Rechner richtig konfiguriert ist und normale Benutzer keine Administratorrechte haben, dann ist es für sie unmöglich, DeviceLock zu deaktivieren.

Q. Setzt DeviceLock Berechtigungen, wenn ein Benutzer sich am System anmeldet?

A. Nein. Die Berechtigungen gelten sofort, nachdem der Administrator sie in der Steuerungskonsole verändert hat.

Q. Was würde passieren, wenn zwei oder mehr Benutzer gleichzeitig an demselben Rechner angemeldet sind (im Falle von Terminal Server oder XP Fast User Switching)?

A. DeviceLock kontrolliert die Benutzeranfragen für Zugriff auf Geräte oder Protokolle in Echtzeit. Jeder Benutzer hat seinen eigenen Sicherheitskontext und DeviceLock weiß, welcher Benutzer versucht, auf ein Gerät oder Protokoll zuzugreifen. Daher ist es möglich, einem Benutzer den Zugriff auf ein Gerät oder Protokoll zu verweigern und gleichzeitig einem anderen Benutzer den Zugriff auf dieses Gerät oder Protokoll zu erlauben, auch wenn beide Benutzer versuchen, gleichzeitig auf das Gerät oder Protokoll zuzugreifen.

Q. Ist es möglich, Berechtigungen auf Geräte oder Protokolle für Benutzergruppen zu setzen?

A. Ja. Sie können die Berechtigungen sowohl für einzelne Benutzer als auch für Benutzergruppen setzen.

Q. Woher nimmt DeviceLock die Liste der Benutzer und Benutzergruppen?

A. DeviceLock übernimmt die Kontolisten aus dem Windows-Sicherheitssystem. Dies sind die Standardkonten, die überall in Windows benutzt werden (z.B. für Anmeldungen am System, Datei/Verzeichnis-Berechtigungen usw.).

Q. Arbeitet DeviceLock mit Active Directory?

A. Ja. Rechte und Einstellungen in DeviceLock können über die Group Policy geändert und in einer Active Directory-Domäne eingesetzt werden. DeviceLock ruft Konten auch vom Active Directory ebenso wie von den Domänencontrollern ab.

Q. Ist es möglich, den Zugriff auf Geräte mit einem Passwort zu schützen?

A. Nein. DeviceLock ist eine Zugriffssteuerung auf Benutzerebene. Es unterstützt keine schwachen Anpassungslösungen wie Passwortschutz.

Q. Ist es möglich, den Zugriff auf Geräte oder Protokolle für eine gewisse Zeitperiode zu schützen?

A. Ja. Sie können die Tageszeit und den Wochentag definieren, wann das Gerät oder Protokoll für einen Benutzer zugänglich sein soll.

Q. Ist es möglich, den USB-Port zu blockieren, aber USB-Maus und -Tastatur zu erlauben?

A. Ja. Sie können Ports völlig blockieren, aber gewisse Geräte zulassen, z.B. Maus, Tastatur, Drucker, Scanner, Modem und Bluetooth-Adapter.

Q. Ist es möglich, das Lesen von Dateien auf einem Gerät zuzulassen, aber das Schreiben darauf zu sperren?

A. Ja. Für diejenigen Geräte, die Lesen/Schreiben von Dateien unterstützen (wie Diskettenlaufwerk, CD-ROM, Flash-Laufwerk, Memory-Stick, ZIP-Laufwerk und andere Wechsellaufwerke), können Sie das Schreiben sperren, aber das Lesen zulassen.