Národní úřad
pro kybernetickou
a informační bezpečnost

P. O. BOX 17
616 00 Brno 16
www.nukib.cz

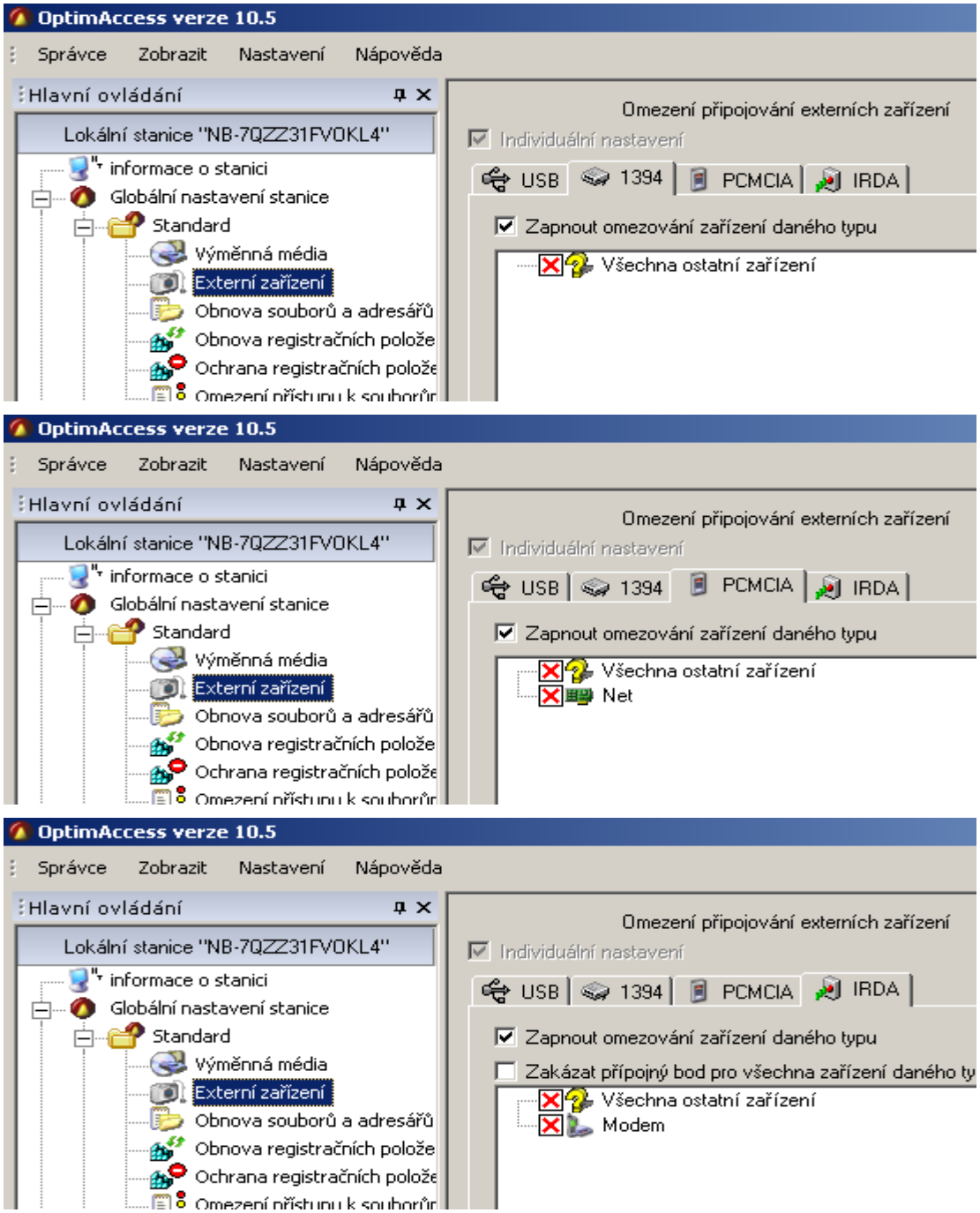
NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Minimální požadavky na konfiguraci produktu OptimAccess

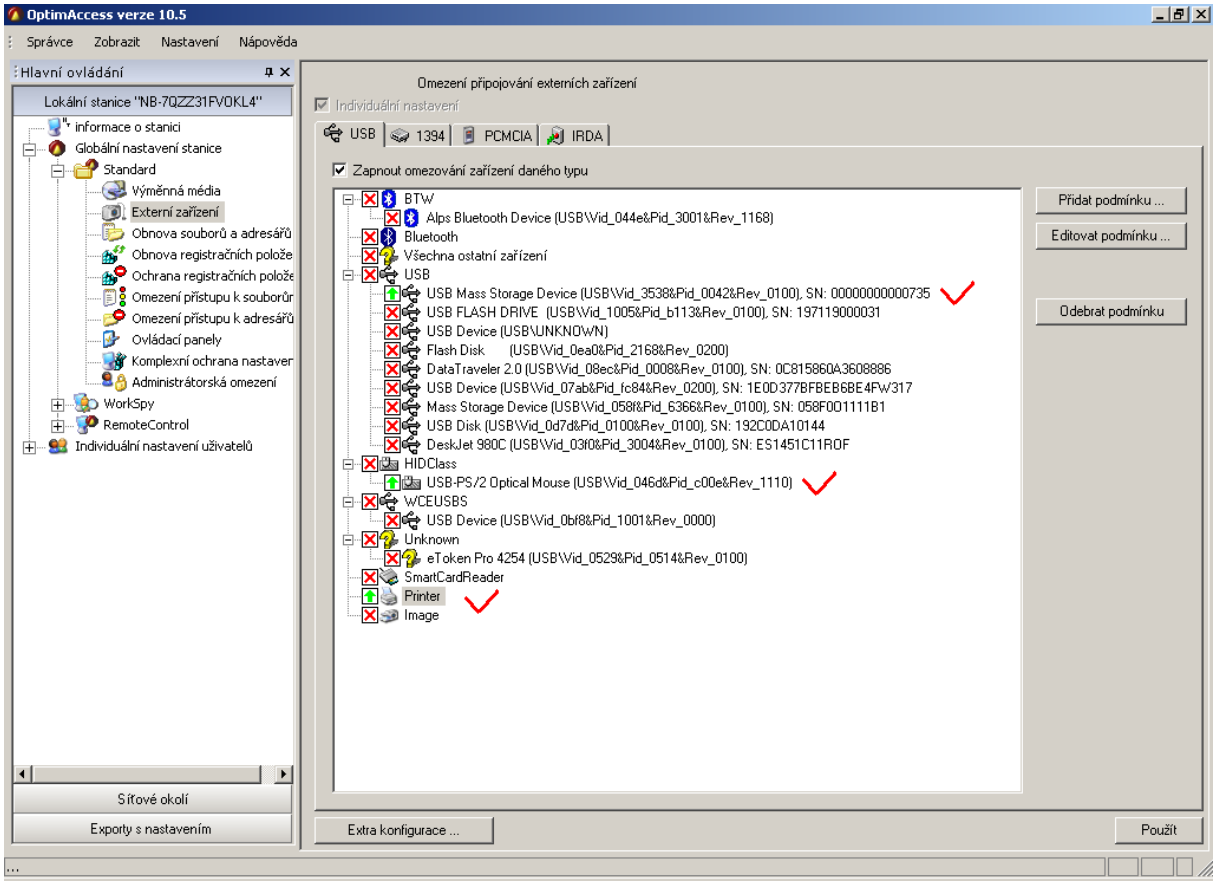
Pro prosazování politiky používání externích zařízení prostřednictvím produktu OptimAccess musí být dodrženy následující zásady při konfiguraci a provozu tohoto prostředku:

1. Všechny neschválené typy zařízení musí být v produktu zakázány, tak jak je uvedeno na následujícím obrázku:



Obrázek 1: Zákaz zařízení typu FireWire 1394, PCMCIA, IRDA

2. Povolení pouze schválených zařízení. Na následujícím obrázku je znázorněno povolení tiskárny, jedné USB paměti a USB optické myši.



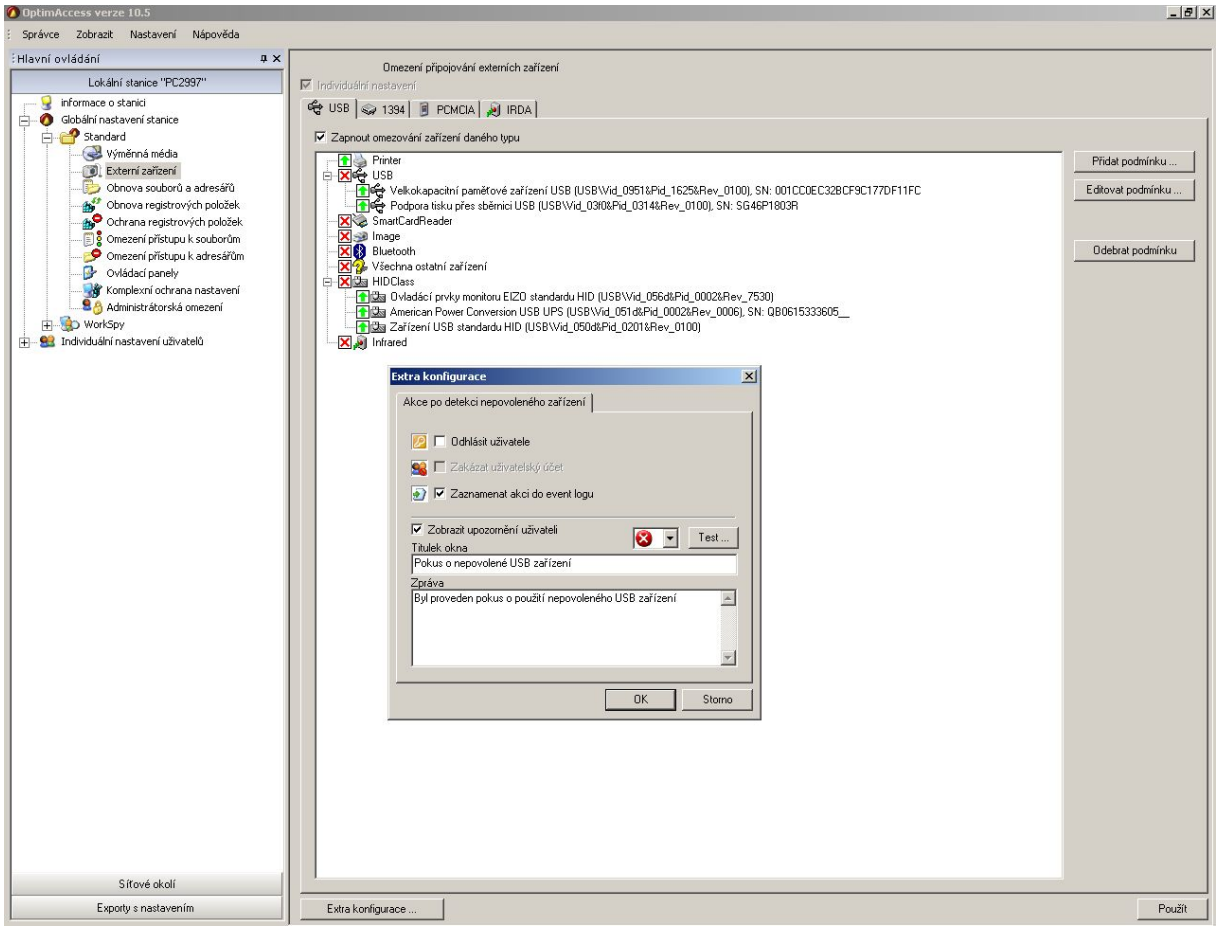
Obrázek2: Nastavení restrikcí USB externích zařízení

Primárně je nastavena nejvyšší úroveň zabezpečení (vše vypnuto - princip Whitelist), do seznamu bezpečnostních se přidávají opatření výjimky povolující vybraným uživatelům vybraný přístup.

Je povoleno pouze připojení takových zařízení, která umožňují jednoznačnou individuální identifikaci[1], tyto zařízení musí být náležitým způsobem označena a evidována.

[1] Standardní popis zařízení obsahuje položku **Serial Number (SN).** Norma nevyžaduje, aby tato položka byla vyplněna. Pokud vyplněna je, tak musí být dle normy unikátní. Unikátnost je plně na zodpovědnosti výrobce. Pokud je přítomno SN, pak identitu tvoří trojice VID (**Vendor ID**), PID (**Product ID**), SN. Často se setkáváme s zařízeními, kde SN chybí např.u některých levných masově vyráběných USB zařízení.

3. Pro detekci připojení nepovolených paměťových zařízení je nastaveno zaznamenávání pokusů o nepovolené připojení přímo do auditních záznamů operačního systému (volba Extra konfigurace Externí zařízení modulu STANDARD).



Obrázek 3: Nastavení zasílání auditních záznamů do systémového logu

Příklad auditních záznamů:

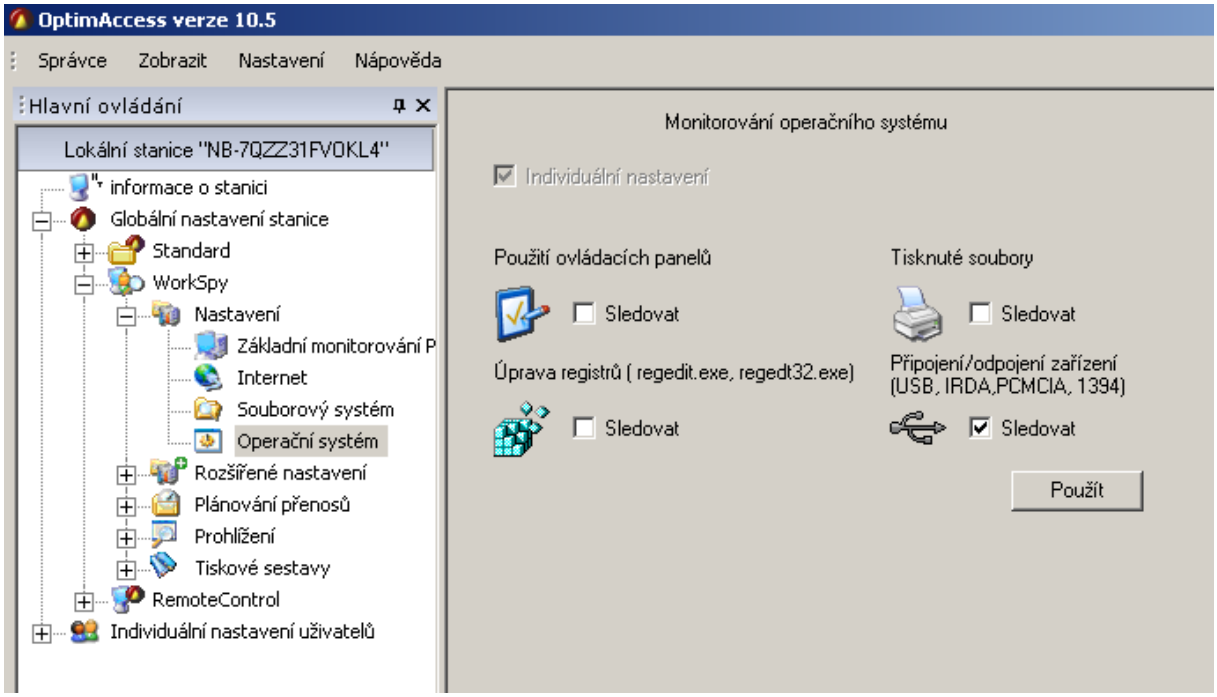
Aplikační auditní záznam:

Zdroj:	OptimAccess
Kategorie:	Removeable Device
Typ:	Upozornění (závisí na nastavení dialogového okna)
ID události:	1000
Popis:	OptimAccess – Restricted Device was detected HardwareID Location DeviceDescription SerialNumber

Systémový auditní záznam:

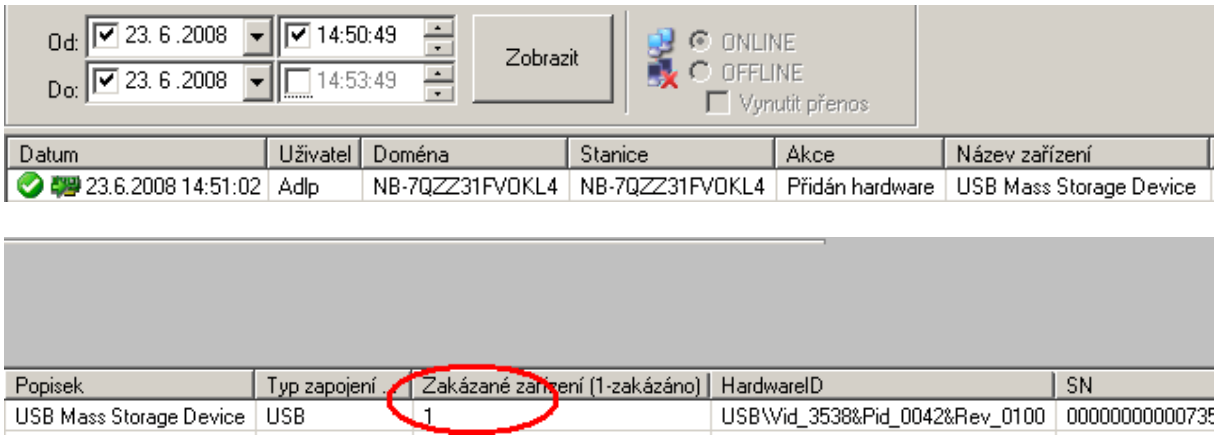
Zdroj:	Application Popup
Kategorie:	Není k dispozici
Typ:	Informace
ID události:	26
Popis:	Místní nabídka aplikace:Varování: Nedovolený přístup na USB zařízení (Text závisí na nastavení ialogového okna.)

4. V modulu WorkSpy musí být zapnuta funkce sledování Připojení/Odpojení zařízení (USB, IRDA, PCMCIA, 1394) tak, jako je znázorněno na následujícím obrázku.



Obrázek 4: Nastavení monitorování modulu WorkSpy

5. Auditní záznam vytvářený použitým nástrojem musí být pravidelně vyhodnocován v souladu s bezpečnostní politikou systému. Připojení nepovoleného zařízení je v auditu zaznamenáno následujícím způsobem:



Obrázek 5: Připojení zakázaného zařízení USB