

Permission Explorer (C-PermExp)
skrácený návod pre vytvorenie grafického prehľadu
oprávnení (používateľských prístupov) v NTFS



SEAL IT Services, s.r.o.

Kontakt: **SEAL IT Services, s.r.o.**, Topoľová 4, 811 04 Bratislava 1, tel.: +421 2 5465 0242,
fax: 02/5478 9664 podpora: support@customermonitor.sk, web: www.customermonitor.sk

OBSAH :

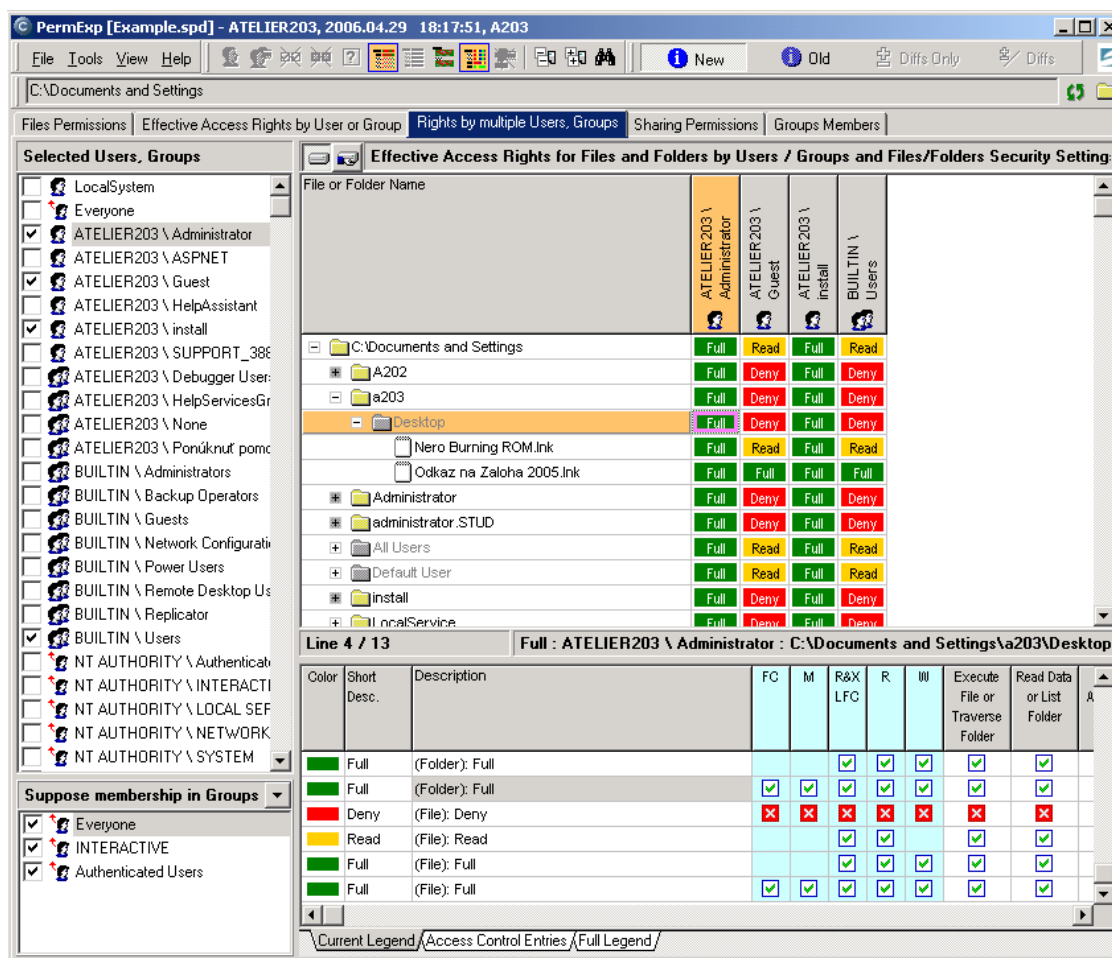
1	Program Permission Explorer (C-PermExp).....	3
1.1	Vlastnosti programu Permission Explorer:.....	3
1.2	Popis okien a ovládacích prvkov aplikácie :.....	3
1.2.1	Použitie jednotlivých záložiek :	4
1.2.2	Popis okien na obrazovke v záložke Effective Access Rights by User or Group.....	4
1.2.3	Popis okien na obrazovke v záložke Rights by multiple Users, Groups	4
1.2.4	Popis tlačítok na hlavnom nástrojovom paneli.....	5
1.2.5	Tlačítka ovplyvňujúce výpočet efektívnych práv podľa oprávnení a práv pri zdieľaní	5
1.3	Základy ovládania :	6
1.3.1	Načítanie údajov (informácií o prístupových právach)	6
1.3.2	Vytvorenie protokolu o prístupových právach	6
1.3.3	Úprava legendy	7
1.4	Použitie programu pre automatizovaný zber	7
1.5	Vysvetlenie pojmov :.....	7
1.6	Používané súbory :.....	8
1.6.1	Súbor *.spd.....	8
1.6.2	Súbor *.spl.....	8

1 Program Permission Explorer (C-PermExp)

1.1 Vlastnosti programu Permission Explorer:

- Graficky prehľadné sumárne zobrazenie prístupu do zložiek a k súborom pre vybraných používateľov (skupiny).
- Prehľadný zoznam zložiek a súborov v stromovej štruktúre, kam má používateľ (skupina) aký prístup, so zahrnutím členstva v skupinách.
- Prehľadný zoznam zložiek a súborov v stromovej štruktúre, kde je používateľ (skupina) uvedený v oprávneniach.
- Výpis zmien nastavení v prístupových právach medzi dvoma vzorkami
- Kompletný výpis oprávnení, ich uloženie do súboru (archivácia) a možnosť prehliadať kdekoľvek. Možnosť obnovenia oprávnení program neobsahuje.
- Prehľadný grafický výpis zaradenia používateľov do skupín
- Zohľadnenie práv pri pripojení na zdieľaný prostriedok; prihlásený lokálne; prihlásený cez vzdialenú plochu; prihlásený ako služba; práv vlastníka vždy meniť oprávnenia;...
- Sprehľadnenie výpisov skrytým zložiek, súborov, ktoré majú rovnaké oprávnenia, akoby boli zdedené; ktoré majú rovnaké efektívne práva ako zložka v ktorej sa nachádzajú;...
- Doplňujúce sprehľadňujúce filtre na zobrazenie len zložiek, súborov s neprístupnými nastaveniami oprávnení; ktorých je vybraný používateľ, skupina, vlastníkom; skrytie zložiek, súborov, kam je plný / nie je žiaden prístup;...
- Export do formátu XLS každého zobrazenia

1.2 Popis okien a ovládacích prvkov aplikácie :



Ilustračný obrázok

1.2.1 Použitie jednotlivých záložiek :

Files Permissions	Effective Access Rights by User or Group	Rights by multiple Users, Groups	Sharing Permissions	Groups Members
-------------------	--	----------------------------------	---------------------	----------------

- Files Permissions** – výpis nastavení oprávnění (ekvivalentné zobrazení „Permissions“ - prvej obrazovky záložky „Security“ vo Vlastnostiach zložky, súboru)
- Effective Access Rights by User or Group** – výpis práv v stromovej štruktúre pre vybraného používateľa, skupinu. Široké možnosti filtrácie predurčuje toto zobrazenie na odhaľovanie nesprávnych nastavení práv. (ekvivalentné zobrazení „Effective Permissions“ - poslednej obrazovky záložky „Security“ vo Vlastnostiach zložky, súboru)
- Rights by Multiple Users, Groups** – grafická prezentácia prístupov pre používateľov, skupiny, vhodné zobrazenie na vytváranie protokolov o nastavení prístupových práv čitateľný pre širší okruh používateľov.
- Sharing Permissions** – zoznam oprávnění pre zdieľané prostriedky. Záložka má len informačný charakter.
- Groups Members** – grafická prezentácia zaradenia používateľov, skupín do skupín

1.2.2 Popis okien na obrazovke v záložke Effective Access Rights by User or Group

- Found Users and Groups** – výpis nájdených používateľov a skupín. Služi na výber používateľa, skupiny, pre ktorého sa majú zobraziť práva.
- Okno pod Found Users and Group** – okno zobrazujúce členstvo používateľa, skupiny v iných skupinách.
- Suppose Member Ship in Groups** – určuje, v ktorých špeciálnych skupinách sa má pri výpočte práv predpokladať členstvo vybraného používateľa, skupiny. Členstvo v týchto skupinách je riadené operačným systémom, a závisí od spôsobu prihlásenia sa k počítaču. Napr. lokálne, cez vzdialenú plochu, ako služba...
Veľmi dôležité pre správny výpočet práv.
V tomto zozname sa nachádzajú iba tie špeciálne skupiny, ktoré sa vyskytujú v oprávneniach niektorého z načítaných súborov, zložiek, a iba členstvo v ktorých má teda zmysel predpokladať.
- Effective Access Rights For Files and Folders by User “...”** – (najväčšie) Okno obrazovky so stromovým výpisom zložiek a súborov s uvedením vypočítaných efektívnych prístupových práv pre zvoleného používateľa alebo skupinu z okna *Found Users and Groups*. Jednotlivé stĺpce sú označené skratkami a plný názov je možné získať nadínením kurzorom na danú skratku.
- Okno pod Effective Access Rights For Files and Folders by User “...”** – Okno pre výpis oprávnení vybranej zložky, súboru a práva zdieľaného prostriedku, cez ktorý je vybraná zložka, súbor nejakým spôsobom prístupný. Služi na informovanie administrátora, z čoho boli práva vypočítané a aby nemusel prechádzať do záložky *File Permissions*. Navyše sú farebne zvýraznené oprávnenia, ktoré boli pri výpočte práv použité.



















1.2.3 Popis okien na obrazovke v záložke Rights by multiple Users, Groups

- Selected Users and Groups** – Zvolený používateľ, skupina je zaradený do zobrazenia v okne *Effective Access Rights for Files nad Folders*
- Effective Access Rights For Files and Folders by Users / Groups** - – (najväčšie) Okno obrazovky so stromovým výpisom zložiek a súborov s grafickou prezentáciou vypočítaných efektívnych prístup. práv.
- Okno pod Effective Access Rights For Files and Folders by Users / Groups** – Okno má tri záložky :
 - Current Legend** - prehľad priradenia grafických symbolov (farieb a popisov) pre jednotlivé kombinácie efektívnych (vypočítaných) prístupových práv, zobrazené sú len kombinácie, ktoré sa nachádzajú v aktuálnom zobrazení stromovej štruktúry (vrátane zložiek, súborov, ktoré sú skryté niektorým filtrom, alebo sú manuálne zbalené). Služi pre kontrolu, aby si administrátor mohol overiť, čo ktorá farba, popis prezentuje, a aké všetky kombinácie sa v aktuálnom zobrazení vyskytujú. Legendu môže priamo v tomto okne upravovať. Viac v časti Úprava farebnej Legendy.
 - Access Control Entries** – rovnaké ako v záložke *Effective Access Rights by User or Group*
 - Full Legend** – zoznam všetkých kombinácií efektívnych prístupových práv, ktorým už bol nejakým spôsobom priradený grafický symbol (farba a popis).


1.2.4 Popis tlačítkov na hlavnom nástrojovom paneli

Upozornenie – tlačítka sú aktívne podľa zvolenej záložky





- a)  - Zobrazí len zložky, súbory, kde je vybraný používateľ, skupina uvedený v oprávneniach.
- b)  - Zobrazí len zložky, súbory, ktorých je používateľ, skupina vlastníkom.
- c)  - Skryje tie zložky, súbory, ktoré majú všetky príznaky efektívnych práv Povolené (Permitted).
- d)  - Skryje tie zložky, súbory, ktoré majú všetky príznaky efektívnych práv Zakázané (Denied).
- e)  - Zobrazí len zložky, súbory, ktoré majú neznáme (neprístupné) oprávnenia.
- f)  - Ak majú všetky súbory zložky rovnaké (alebo 100% ekvivalentné) oprávnenia, skryje ich a nahradí jediným fiktívnym súborom „*. * (All Files Same)“.
- g)  - Skryje tie zložky, súbory, ktoré majú rovnaké efektívne (vypočítané) prístupové práva, ako ich rodičovská zložka.
- h)  - Skryje tie zložky, súbory, ktoré majú rovnaké oprávnenia, ako keby vznikli iba dedením oprávnení z rodičovskej zložky. Pozor, to neznamená, že musia byť rovnaké, ako má rodičovská zložka – závisí to od toho, ktoré oprávnenia a ako sa dedia.
- i)  - Skryje tie zložky, súbory, ktoré majú rovnaký grafický symbol Legendy ako rodičovská zložka, a to pre všetkých vybraných používateľov, skupiny.
- j)  - Pri porovnávaní zmien oprávnení skryje súbory, zložky, ktoré boli oproti „starému stavu“ vytvorené alebo vymazané - v zobrazení ponechá teda len zložky, súbory, ktoré sa nachádzajú aj v „novom stave, aj v starom stave“.
- k)  - Rozvinie stromovú štruktúru. Ak je aktivovaný niektorý filter, zložky, ktorej všetky súbory, podzložky sú niektorým filtrom skryté, sú nerozvinuteľné, čo je indikované symbolom .
- l)  - Zbalí stromovú štruktúru.
- m)  - Hľadať. Poznámka: Hľadanie je možné aj z okna Legendy na vyhľadanie zvoleného stavu v stromovej štruktúre.
- n)  New - Aplikácia má dve pracovné plochy. Tlačítko na aktiváciu pracovnej plochy „New“, ktorá je používaná ako východzia
- o)  Old - Na aktiváciu pracovnej plochy „Old“. Používa sa pre uloženie údajov na vyhodnotenie rozdielov oproti údajom v ploche „New“.
- p)  Diffs Only - Zobrazí len rozdiely medzi údajmi v plochách „New“ a „Old“
- q)  Diffs - Zobrazí aj rozdielne položky aj rovnaké medzi plochami „New“ a „Old“

1.2.5 Tlačítka ovplyvňujúce výpočet efektívnych práv podľa oprávnení a práv pri zdieľaní

Tlačítka  sa nachádzajú v ľavom hornom rohu okna „**Effective Access Rights For Files and Folders**“ a „**Rights by multiple Users, Groups**“ a podľa ich aktiváciou je riadený výpočet efektívnych práv buď z pohľadu len oprávnení, alebo len práv pre zdieľanie alebo pri zohľadnení oboch typov nastavení, ktoré sú použité pri prístupe k zdieľanému prostriedku zo siete.





1.3 Základy ovládania :

1.3.1 Načítanie údajov (informácií o prístupových právach)

- a) Načítanie zložky, súboru, jednotky disku, sieťovej jednotky, do Permission Explrera cez File /
 Open alebo vpravo hore ikonou symbolu zložky . Zelená kruhová ikonka je pre opätovné načítanie. Poznámka: viac diskov alebo adresárových ciest naraz sa nedá do Permission Explrera načítať.
- b) Po načítaní sú údaje pripravené k prehliadaniu vo všetkých záložkách. Aktiváciou filtrov podľa 1.2.4 Popis tlačítok na hlavnom nástrojovom paneli získajte zobrazenie, ktoré potrebujete.
- c) Doporučenia a upozornenia:
 - i) **Aby údaje boli relevantné je nutné načítanie uskutočniť pod administrátorským účtom**
 - ii) Pri veľkom počte údajov (niekoľko stotisíc až miliónov Retrieved ACEs. Údaj je možné vidieť pri načítaní) sa obsadzuje väčšie množstvo pamäti a môže to ovplyvniť rýchlosť programu. Do porúčame pracovať s 500tisíc Retrieved ACEs na počítači s 1GB RAM, prípadne uskutočniť viac čiastkových spracovaní.
 - iii) Členmi skupín počítačov, ktoré sú členmi domény, sú doménoví používatelia, skupiny. Pre správne načítanie členov doménových skupín je nutné aby načítanie bolo realizované pod účtom doménového administrátora, resp. používateľa s dostatočnými oprávneniami. Ak je načítanie realizované pod lokálnym administrátorom, je možné nastaviť prihlasovanie údaje pre získanie prístupu k doméne cez menu „Tools / Change LogonParams for a domain connection“).

1.3.2 Vytvorenie protokolu o prístupových právach

Pre vytvorenie prehľadného protokolu je v programe zavedená prezentácia nastavení prístupových práv do farebne odlišených symbolov. Farebné odlíšenie sleduje zoskupenie rôznych nastavení do jednej kategórie napríklad Read, Write, Full Access.... V posledných operačných systémoch Microsoft majú prístupové práva množstvo parametrov, z ktorých niektoré kombinácie majú z pohľadu používateľa rovnakú funkciu a je možné ich zaradiť do jednej skupiny. Naopak niektoré parametre aj napriek zdanlivému zakázaniu prístupu, umožňujú nepovolaným používateľom pristupovať do takýchto zložiek a prípadne dokonca prevziať kontrolu nad zložkou. V rozvinutej adresárovej štruktúre a pri prístupe viacerým administrátorom je ťažké nájsť takéto chybné nastavenia. Pomocou Protokolu z Permission Explrera ich nájdete nasledovne :

- a) Po načítaní údajov v podľa bodu 1.3.1 Načítanie údajov (informácií o prístupových právach) sa prepnite do záložky Rights by Multiple Users, Groups.
- b) V okne **Suppose membership in Groups** (vľavo dole) vyberte / skontrolujte členstvo v ktorých špeciálnych skupinách sa má uvažovať – týmto sa určuje scenár prihlásenia používateľov. Tlačítkom  alebo kontextovým menu je možné vybrať niektorý z režimov prihlásenia.
- c) V okne **Selected Users and Groups** (vľavo) vyberte používateľov a skupiny, ktorých chcete mať v protokole
- d) Ak máte vlastnú legendu, načítajte ju cez Tools / Legend / Load from File.
- e) Aktivujte tlačítko , ktoré zakryje zložky, súbory s rovnakým symbolom legendy ako u rodičovskej zložky (pre všetkých vybraných používateľov, skupiny). Pokračovať môžete aj bez aktivácie tohto filtra, výstupné údaje však budú rozsiahle.
- f) Nastavte sa na prvý riadok a stlačte tlačítko  na rozbalenie stromovej štruktúry. Keďže máte aktivovaný filter nezobrazovania podzložiek a súborov s rovnakým symbolom Legendy ako rodičovská zložka, ukážu sa vám iba zložky, súbory s rôznymi nastaveniami a na malom priestore získate hodnotnú informáciu.
- g) Doporučujeme aktivovať tlačítko , ktoré v prípade že všetky súbory tej ktorej zložky majú rovnaké alebo 100% ekvivalentné oprávnenia, ich vo výpise nahradí jediným súborom „,*.* (All Files Same). Odstránite tak, zbytočne dlhý zoznam súborov s rovnakými nastaveniami práv.

- h) Pozrite si v spodnom okne **Current Legend**, a skontrolujte aké všelijaké kombinácie vypočítaných práv sa v načítaných údajoch vyskytujú. Legendu si podľa svojich potrieb môžete upraviť a definovať aj nové stavy - 1.3.3 Úprava legendy. Funkciou Hľadať môžete stav z legendy vyhľadať v stromovej štruktúre.
- i) Uložte si načítané údaje, aby ste ich mohli v budúcnosti v prípade potreby opätovne zobrazit'. Uloženie vykonajte cez *File / Save Compressed*, alebo v prípade vyššej bezpečnosti, aby údaje neotvorila neoprávnená osoba zvolte kryptovanie s údajmi z licencie technika alebo používateľa. Viac o licenciách sa dozviete v manuále k programu C-Monitor.
- j) Ak ste menili Legendu uložte podľa 1.3.3 Úprava legendy
- k) Exportujte výstup do Excelu prostredníctvom menu *Tools / Export to MS Excel*
- l) Pri čítaní výstupu si uvedomte, že každá nezobrazená zložka alebo súbor v protokole je zložka, ktorá má rovnakú legendu (farbu a popis) ako rodičovská zložka.

1.3.3 Úprava legendy

Vo vašom systéme sa môžu vyskytovať stavy, ktoré nie sú definované alebo si prajete zmeniť ich zaradenie. Legendu môžete upravovať priamo v záložke *Rights by Multiple Users, Groups* v spodnom okne v záložkách *Current Legend* alebo *Full Legend*. Stretnúť sa môžete s :

- i) už priradeným stavom, ktorý má priradenú farbu, nepovinne vypísaný *Short Description* a *Description*,
- ii) novým, dosiaľ neznámym stavom, ktorý nemá priradenú farbu a nemá žiaden *Description*,
- iii) s neúplnými údajmi.

Údaje môžete zmeniť klávesou F2 prípadne doubleclickom. Po jej zmene zvolte *Tools / Legend / Save To File*.

Pre výpočet Legendy sa používa šablóna (*Template*). Pomocou nej sú vypočítané stavy v Legendě podľa vybraných oprávnení a ostatné sa zanedbávajú. Tým pádom nie je nutné definovať práce každý stav pre položku v Legendě, ale určuje sa „pravidlo“ výpočtu. Ak budete potrebovať zmeniť už zadaný stav, pozrite do Šablóny a uskutočnite zmenu najprv tam, Prístupná je cez *Tools / Legend / Modify Template*. Po úprave si novú šablónu potom uložte. (Ukladá sa spolu s legendou)

Legenda sa pri spustení aplikácie automaticky načíta zo / pri jej skončení automaticky uloží do súboru *PermExp.spl* v zložke, kde sa nachádza spustený spustiteľný súbor aplikácie.

1.4 Použitie programu pre automatizovaný zber

Program má aj neinteraktívny (*command line*) mód a pomocou programu C-Monitor získané údaje odošle do servera Customer Monitor, kde sú archivované. Získa sa tak aktuálna záloha prístupových práv, ktorú je možné použiť pri oprave poškodeného servera (počítača) alebo pri analýze a tvorbe protokolov prístupov. Obnovu prístupových údajov je nutné vykonať manuálne nakoľko program nerieši problematiku meniacich sa SID. Nastavenie automatického zberu je uvedené v manuáli programu C-Scheduler.

1.5 Vysvetlenie pojmov :

Efektívne práva – výsledné prístupové práva, ktoré definujú možnosti prístupu používateľa, skupiny k súboru, zložke. Vypočítavajú sa z oprávnení, pričom sa berie do úvahy členstvo používateľa, skupiny v iných skupinách (aj v špeciálnych skupinách), vlastníka súboru, zložky, to, či sa dá k súboru, zložke prístupit' cez niektorý zdieľaný prostriedok, a toho, aké má prístupové práva.

1.6 Používané súbory :

1.6.1 Súbor *.spd

V tomto formáte sa ukladajú informácie o súboroch, zložkách, používateľoch, skupinách, oprávneniach. Súbor komprimovaný a šifrovaný.

1.6.2 Súbor *.spl

V tomto formáte sa ukladajú súbory legendy. V súbore legendy sa ukladá jednak samotná legenda, a jednak šablóna pre jej generovanie.

Legenda sa pri spustení automaticky načíta zo / pri skončení automaticky uloží do súboru PermExp.spl