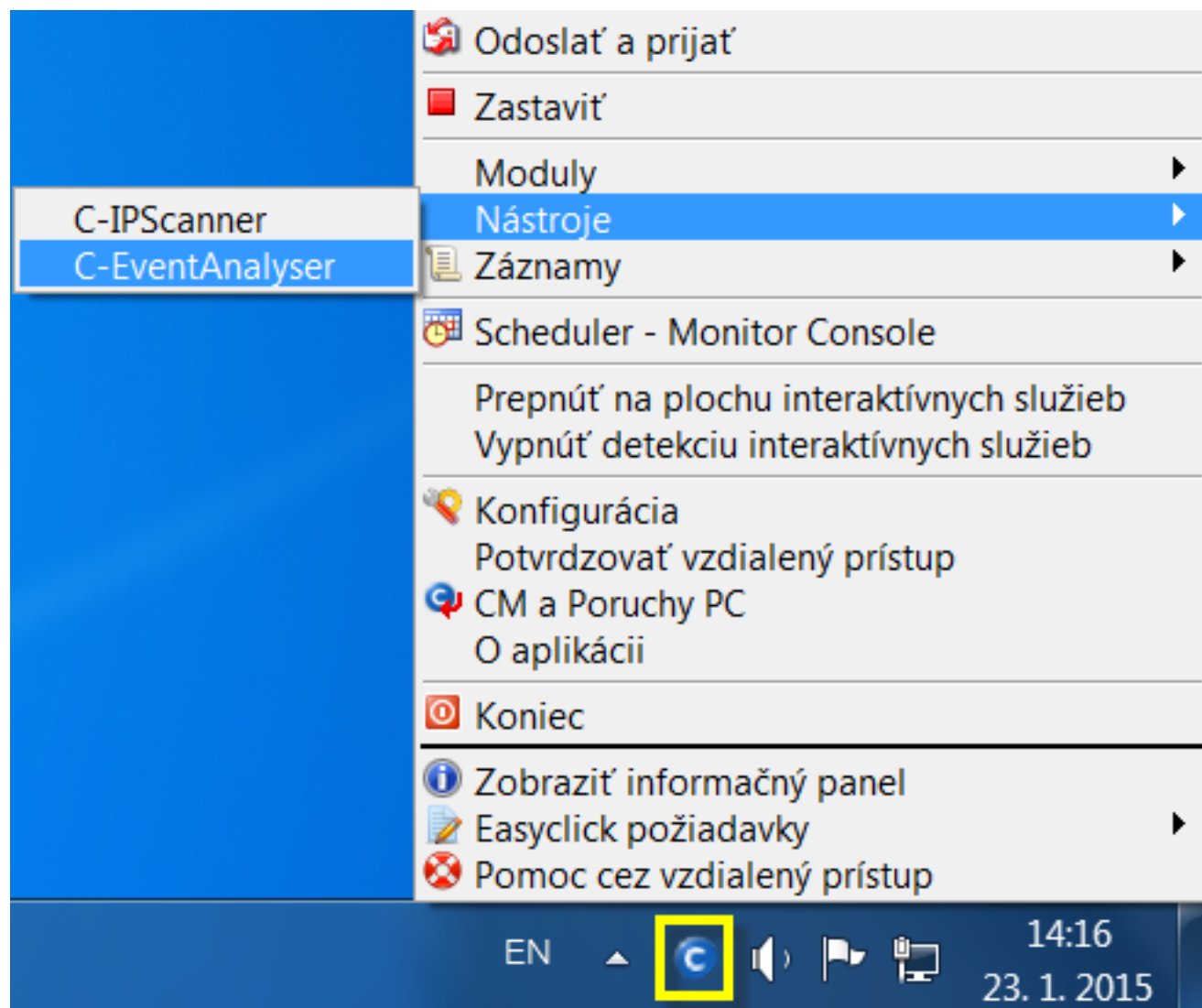


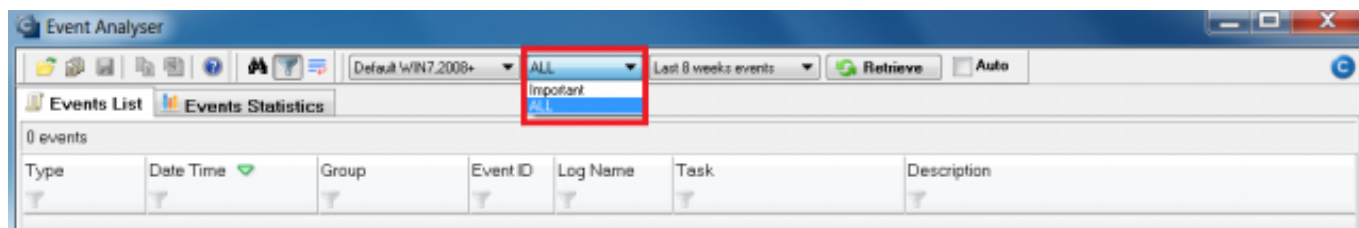
Spustíte EventAnalyser kliknutím pravého tlačidla myši na ikonu C-monitora v lište a zvolíte Nástroje
-> C-EventAnalyser.



Obrázok: Znáozornenie ikonky C-Monitora pre otvorenie EventAnalyseru.

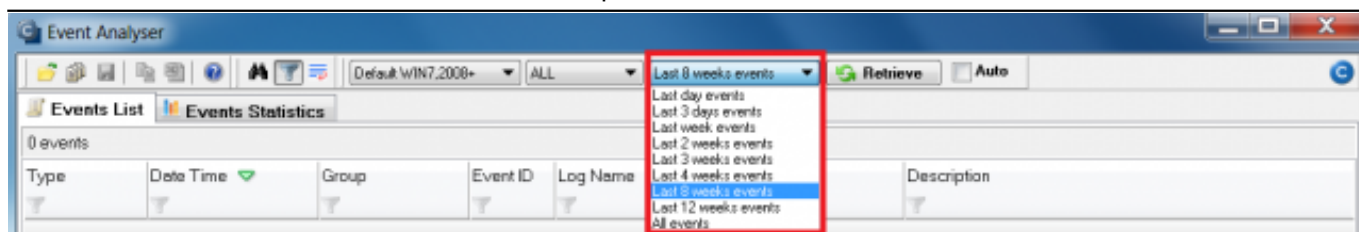
Nastavenie zobrazovania udalostí:

Vyberiete si, či chcete zobrazovať všetky typy udalostí, alebo iba tie, ktoré sú zaradené do kategórie dôležitých.



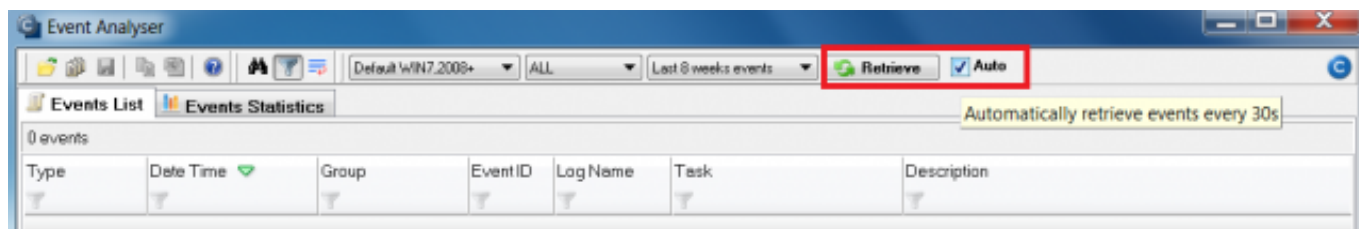
Obrázok: Nastavovanie zobrazovania udalostí v EventAnalyseri

Zvolíte obdobie, za ktoré sa vám zobrazia všetky zozbierané udalosti.



Obrázok: Nastavovanie zobrazovania udalostí v EventAnalyseri

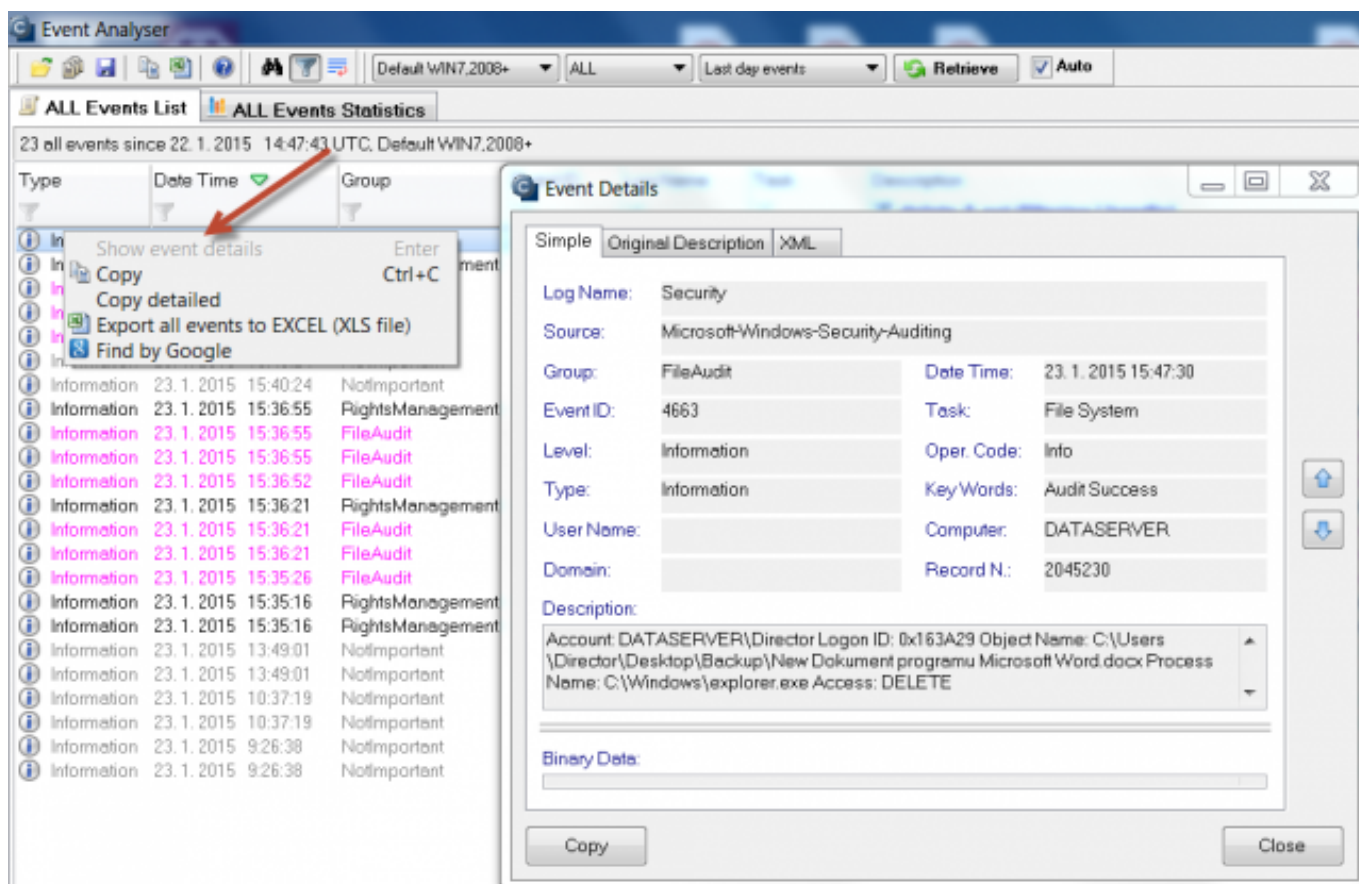
Udalosti na základe zvolených nastavení načítate tlačidlom **Retrieve**, a so získaným zoznamom viete ďalej pracovať. Pokiaľ chcete, aby EventAnalyser aktualizoval zoznam udalostí automaticky, zaškrtnite políčko **Auto**, a váš zoznam sa bude aktualizovať pravidelne každých 30 sekúnd.



Obrázok: Nastavovanie zobrazovania udalostí v EventAnalyseri

Zobrazenie podrobností konkrétnej udalosti:

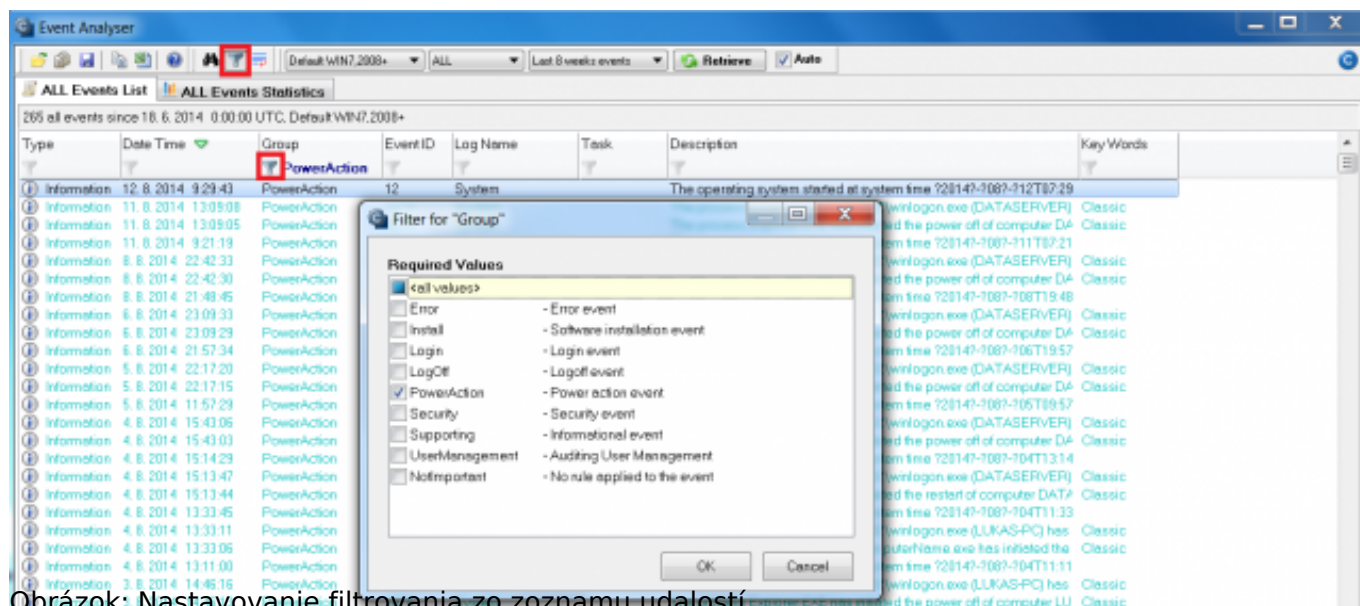
Pre zobrazenie podrobnejšieho výpisu kliknite pravým tlačidlom myši na riadok s danou udalosťou a zvolte možnosť Show event details prípadne použite dvojklik alebo stlačte Enter. V okne, ktoré sa vám zobrazí, si môžete prepínať medzi jednoduchým výpisom o udalosti, pôvodným výpisom tak, ako ho generuje Windows a XML zobrazením.



Obrázok: Otvorenie podrobného zobrazenia udalosti

Nastavenie filtrov

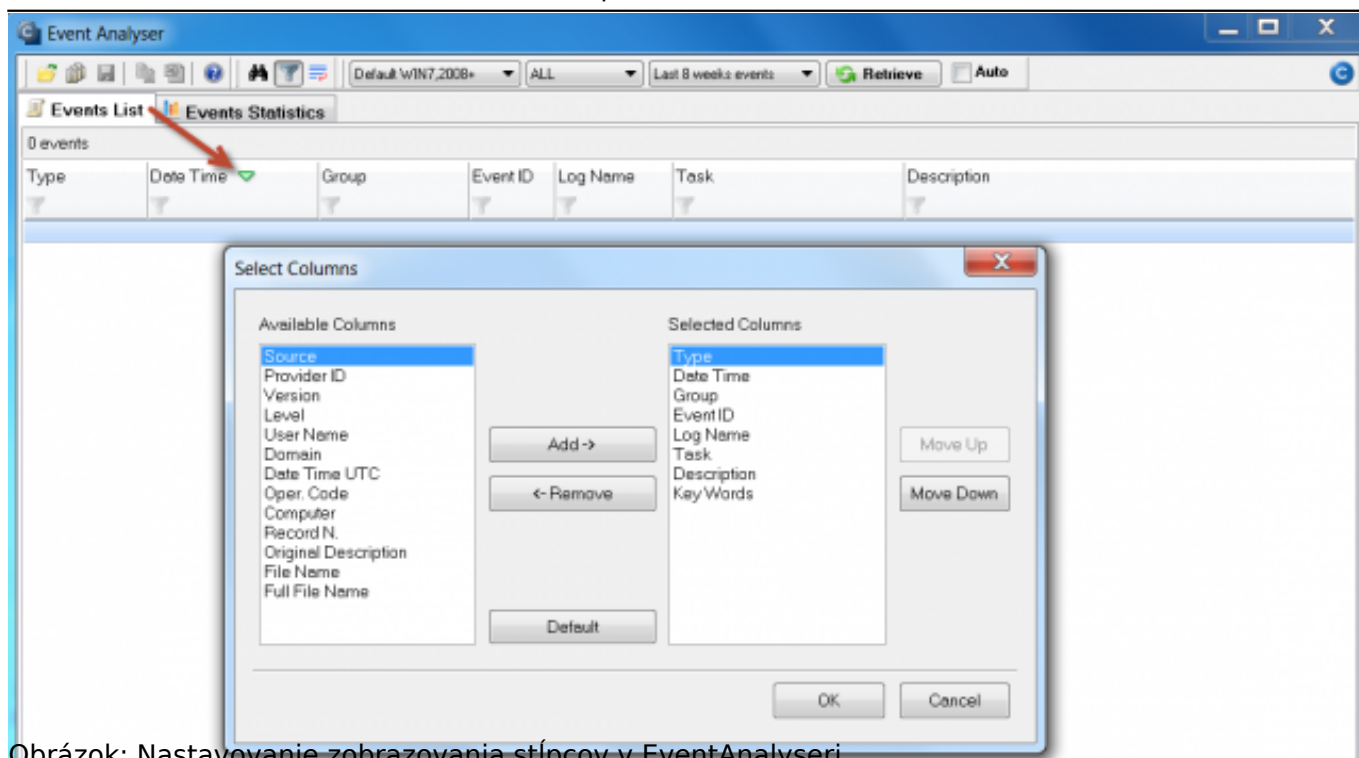
- Kliknutím na ikonu lievika v hornej lište zapnete filtrovací mód.
- Zvolíte si parameter(stĺpec) podľa ktorých chcete zo zoznamu udalostí filtrovať a kliknutím na ikonu lievika v danom stĺpci otvoríte okno pre nastavenie filtrovania.
- Nastavíte filtrovanie podľa potreby a kliknete OK. Zoznam udalostí, ktorý sa vám teraz zobrazuje obsahuje iba udalosti, ktoré vyhovujú nastaveným filtrom.
- Ak chcete filtrovať podľa viacerých parametrov súčasne, kliknite na ikonu lievika v ďalšom stĺpci a znovu zadajte nastavenie filtrovania. Po kliknutí OK bude zoznam udalostí obsahovať iba tie udalosti, ktoré vyhovujú všetkým zadaným filtrom.



Obrázok: Nastavovanie filtrovania zo zoznamu udalostí

Prispôsobenie zobrazovania udalostí v EventAnalyseri:

- Udalosti v zobrazenom zozname si môžete nechať zoradiť podľa ľubovoľného parametra kliknutím do príslušného políčka. Pri stĺpci, podľa ktorého je zoznam udalostí zoradený je zelená šípka(vid'. červená šípka na obrázku).
- Jednotlivé stĺpce parametrov udalostí môžete preusporiadať, pridať ďalšie alebo niektoré odstrániť. Kliknite do ľubovoľného stĺpca pravým tlačidlom myši a zvolte možnosť Select columns. V zobrazenej tabuľke máte vľavo celý zoznam stĺpcov, ktoré ešte môžete do vášho zobrazenia pridať, vpravo je zoznam aktuálne pridaných parametrov, môžete z nich niektoré odobrať, alebo ich preusporiadať.



Obrázok: Nastavovanie zobrazovania stĺpcov v EventAnalyseri

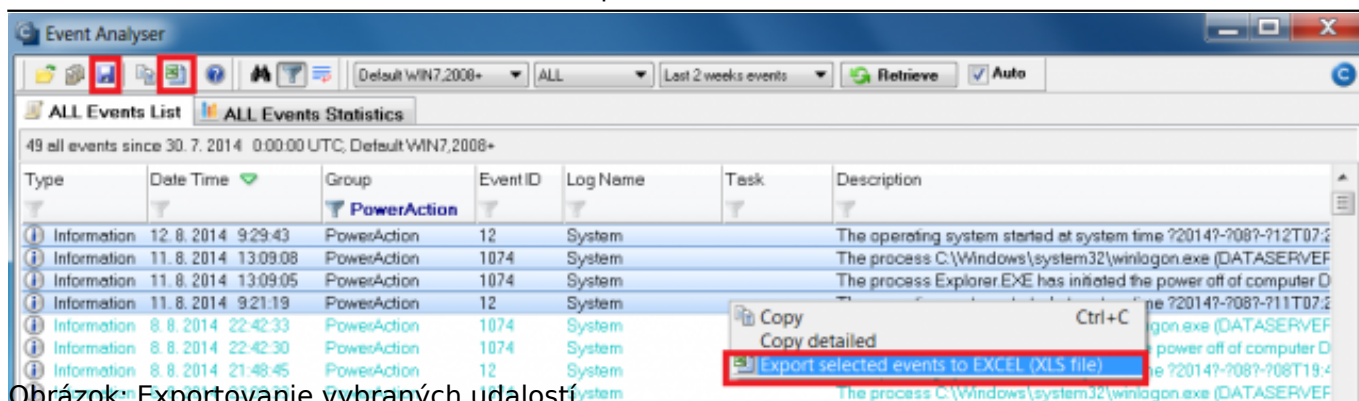
V EventAnalyseri si môžete pozrieť aj štatistiku výskytu udalostí za zvolené obdobie, zvolíte záložku **All Events Statistics** a uvidíte štatistické informácie o udalostiach: počet výskytov za zvolené obdobie, posledný výskyt a iné.

Type	Last Occurrence	Group	Event ID	Description	Last Occurrence UTC	Count
Information	23. 1. 2015 16:19:14	NotImportant	5152	The Windows Filtering	23. 1. 2015 15:19:14	1,311
Information	23. 1. 2015 16:18:59	NotImportant	4656	A handle to an object w	23. 1. 2015 15:18:59	1,229
Information	23. 1. 2015 15:38:01	NotImportant	5154	The Windows Filtering	23. 1. 2015 14:38:01	984
Information	23. 1. 2015 16:17:34	FileAudit	4663	Account Log	23. 1. 2015 15:17:34	528
Information	23. 1. 2015 16:18:59	NotImportant	7036	The service enter	23. 1. 2015 15:18:59	396
Information	23. 1. 2015 15:38:02	NotImportant	5157	The Windows Filtering	23. 1. 2015 14:38:02	203
Information	23. 1. 2015 15:42:29	NotImportant	4719	System audit policy wa	23. 1. 2015 14:42:29	135
Information	23. 1. 2015 15:44:34	NotImportant	4656	A handle to an object w	23. 1. 2015 14:44:34	120
Information	23. 1. 2015 15:37:49	NotImportant	4957	Windows Firewall did n	23. 1. 2015 14:37:49	63
Information	23. 1. 2015 15:39:23	NotImportant	2100	Received a Pnp or Po	23. 1. 2015 14:39:23	44

Obrázok: Príklad zobrazenia štatistiky udalostí

Exportovanie vybraných udalostí

- Zobrazené udalosti si môžete uložiť ako súbor programu C-EventAnalyser kliknutím na ikonu diskety v hornej lište, alebo ako Excelový súbor kliknutím na príslušnú ikonu vyznačenú na obrázku
- Pre uloženie len vybranej časti zoznamu, označte požadované udalosti a uložte ich



Obrázok: Exportovanie vybraných udalostí

Date:
9.6.2015