

## Re: Membership in Admin groups resets Send As permissions – Blackberry's broken for administrators

---

*Source:*

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2006-06/msg00938.html>

---

- *From:* Andy David – MVP <[adavid@xx](mailto:adavid@xx)>
  - *Date:* Thu, 08 Jun 2006 20:48:00 –0400
- 

On Thu, 8 Jun 2006 15:28:58 –0700, "John D. Gwinner" <[JohnDOTgwinner@xxxxxxxxxxx](mailto:JohnDOTgwinner@xxxxxxxxxxx)> wrote:

Ok, this is an odd one.

Blackberry Enterprise Server (BES 4.0, SP4, HF 3, i.e. version 4.0.4.5)

Exchange 2003, SP2, 2003 native mode domain.

Using the script in <http://support.microsoft.com/kb/912918/en-us> (KB Article 912918) per the latest security patch, I attempted to set the 'send as' permission.

Everyone works but 4 people. I removed 2 of the people from administrative groups, and the script works.

What happens is that about 5–10 minutes after I grant the Blackberry service accounts permission to 'send as' ... they revert to not having 'send as' permission.

The other, non administrator, users work fine.

I called Blackberry support, and they said that Microsoft had 'hard coded' it so that Administrators CANNOT use Blackberry's. Apparently administrators will no longer be able to have another account have 'send as' authority.

Obviously, one possible 'best practice' is to remove my 'normal' account from admin groups and have a second account used only for administration, but NOTHING should remove a permission I have explicitly set without some kind of warning.

Also, this basically forces any admin to have 2 accounts, otherwise they won't get notifications about critical events, given that their blackberry's

Re: Membership in Admin groups resets Send As permissions – Blackberry's broken for administrators

are non operational with administrator accounts.

Now I'll be typing my password 100's of times a day.

It's extremely frustrating to me that this 'feature' is being jammed down our throats.

Thoughts?

== John ==

Doesnt the KB state exactly that?

"Special rules for adminSDHolder Protected Accounts

If you use the script to grant the Send As permission for a mailbox owner that is also a domain administrator, the Send As permission will not be effective. We strongly recommend that you do not mailbox-enable user accounts that have domain administrator rights or that are adminSDHolder protected.

The adminSDHolder object is a template for accounts that have broad Active Directory administrative rights. To prevent unintended elevation of privilege, any account that is protected by the adminSDHolder object must have access rights that match those that are listed on the adminSDHolder object itself.

If you change the rights or the permissions on the adminSDHolder object for a protected account, a background task will undo the change within several minutes. For example, if you grant the Send As permission on a domain administrator object for an application service account, the background task will automatically revoke the permission.

Therefore, you cannot grant the Send As permission to an application service account for an account that is protected by the adminSDHolder object unless you change the adminSDHolder object itself. If you do change the adminSDHolder object, this will change the access permissions for all protected accounts. You should only change the adminSDHolder object after a complete review of the security implications that may occur with the change.

To associate a mailbox with an account that is protected by the adminSDHolder object, follow these steps:1. Start the Active Directory Users and Computers management console.

2. On the View menu, make sure that the Advanced Features option is selected. If this option is not selected, the Security page will not be visible for User account objects.

3. Create an ordinary user account to act as the mailbox owner.

4. Assign the ordinary user account a mailbox on an Exchange server.

Re: Membership in Admin groups resets Send As permissions – Blackberry's broken for administrators

Re: Membership in Admin groups resets Send As permissions – Blackberry's broken for administrators

5. Open the properties of the new mailbox owner account.
  6. In the Exchange Advanced box, grant the Full Mailbox Access permission to the protected administrator account.
  7. In the Security page, grant the Send As permission to the protected administrator account.
  8. Click OK to exit the properties of the mailbox owner object.
  9. Right-click the mailbox owner account object, and then click Disable Account to disable the account for all logons.
- .

Re: Membership in Admin groups resets Send As permissions – Blackberry's broken for administrators