

# RE: Security groups being removed

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-10/msg01888.html>

---

- *From:* [v-mileli@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:v-mileli@xxxxxxxxxxxxxxxxxxxxxxxx) (Miles Li [MSFT])
  - *Date:* Mon, 20 Oct 2008 09:54:49 GMT
- 

Hello,

Thank you for posting here.

According to your description, I understand that:

You have 5 users that are removed from the BESAdmin group unexpectedly.

If I have misunderstood the problem, please don't hesitate to let me know.

From the description, I think that this issue is related to the it should be the expected behavior because of the AdminSDHolder thread on the DC that holds the primary domain controller (PDC) operations master role. It runs every hour to check the access control lists (ACLs) on the following groups and all of the member objects of these groups:

- Enterprise Admins
- Schema Admins
- Domain Admins
- Administrators
- Domain Controllers
- Cert Publishers
- Backup Operators
- Replicator Server Operators
- Account Operators
- Print Operators

This object is used to control the permissions of user accounts that are members of the built-in Administrators or Domain Administrators groups. If a user account is a member of one of these administrative groups because of its membership with a distribution group, the user account's ACL is checked when the thread is run and may be reset to match the ACL of the AdminSDHolder thread. This is by design and helps to protect these administrative accounts from being modified by unauthorized users if the accounts are moved to a container in which a user has been delegated

RE: Security groups being removed

administrative privilege for the modification of user accounts.

For this issue, you can choose a method according to your environment to correct the problem:

1. Remove these problematic 5 users from the domain admins group. In addition, please ensure that they are not included in other protected user groups listed above.
2. You can manually add BESAdmin permission on the AdminSDHolder object (DN: cn=adminsdholder,cn=system,dc=domain\_name,dc=com) to prevent the ACE of BESAdmin from being removed. However, the following operations just explain the way it works and is NOT recommended in productive environment for it will result in critical security issues.

1. In the command prompt, type "adsiedit.msc" and press Enter.
2. Connect to the domain name context of the Active Directory domain, open "cn=adminsdholder,cn=system,dc=domain\_name,dc=com"
3. Right click the "cn=adminsdholder" node--->Properties--->Security tab.
4. Add a custom ACE to test how it works.

Please note: This operation will add the that ACE on all administrative group listed above.

If the issue persists, please check whether you has configured Restricted Group group policy or any scripts to add user group automatically.

[Computer Configuration\Windows Settings\Security Settings\Restricted Groups]

For more detailed information please refer to:

AdminSDHolder Thread Affects Transitive Members of Distribution Groups  
<http://support.microsoft.com/?id=318180>

Description and Update of the Active Directory AdminSDHolder Object  
<http://support.microsoft.com/kb/232199/>

Hope it helps.

Best regards,  
Miles Li

Microsoft Online Partner Support  
Microsoft Global Technical Support Center

Get Secure! – [www.microsoft.com/security](http://www.microsoft.com/security)

=====

When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from your issue.

RE: Security groups being removed

RE: Security groups being removed

---

This posting is provided "AS IS" with no warranties, and confers no rights.