

msExchMailboxSecurityDescriptor and inherited rights

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.development/2007-02/msg00087.html>

- *From:* "Jared Cheney" <jcheney@xxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 23 Feb 2007 11:14:07 -0700
-

I have a question regarding the msExchMailboxSecurityDescriptor attribute. We have an application that is going to take care of enabling single-sign-on for an environment. To do this, the account used by the application needs the ability to grant the Full Mailbox Access and Associated External Account rights to a mailbox. Within Exchange System Manager, at the Administrative group level, I have granted this account (I'll call it the SSOAccount) a variety of permissions, one of which is the 'Change Permissions' right, and these rights are inherited throughout the Exchange organization.

To test that the necessary permissions are in place, I've been using the SSOAccount to run ADUC and go in and manually assign an account the Ext Assoc. Acct and Full Mbox rights. What I've noticed is that sometimes this works fine and sometimes instead I receive an 'Access is Denied' error message.

From within ADUC, When you look at an account's Mailbox Permissions, you can

see that the SSOAccount is inheriting the 'Change Permissions' right on the mailbox. However, when I use adfind.exe (from www.joeware.net) to export the actual msExchangeMailboxSecurityDescriptor then it doesn't reflect that SSOAccount has the Change Permissions right. If I *first* use my own account (i.e. Exchange Admin account) to go in and assign SSO rights to a mailbox – afterwards when I look at the msExchMailboxSecurityDescriptor it *then* reflects that SSOAccount has the Change Permissions right on the mailbox and I'm able to from then on perform SSO operations against that mailbox with the SSOaccount without problems. It's as though by touching the mailbox with an Admin account, I'm able to cause the propagation of the inherited rights to get written to the msExchMailboxSecurityDescriptor.

So it appears that though from an AD perspective the proper rights are inherited on the mailbox object, the rights aren't actually propagating down to a mailbox until an Exchange Admin account touches them. How can I force the rights to propagate to the Mailbox/Info.Store without having to touch every single mailbox with an ExchAdmin account?

msExchMailboxSecurityDescriptor and inherited rights