

SecurityFocus Microsoft: RE: Group Policy: multiple password policies in the same domain?

RE: Group Policy: multiple password policies in the same domain?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-09/0010.html>

From: Derick Anderson (danderson_at_vikus.com)

Date: 09/01/05

Date: Thu, 1 Sep 2005 14:57:19 -0400

To: "Richard Whitworth" <Richard.Whitworth@hsbp.co.uk>, <focus-ms@securityfocus.com>

Responses inline.

> -----Original Message-----

> **From:** Richard Whitworth [<mailto:Richard.Whitworth@hsbp.co.uk>]

> **Sent:** Thursday, September 01, 2005 10:54 AM

> **To:** Derick Anderson; focus-ms@securityfocus.com

> **Subject:** RE: Group Policy: multiple password policies in the
> same domain?

>

> Good point Laura, I'd suspected that you might be able to use
> a different GPO at the same level but having never tested it
> I didn't want to committ it to writing! At least I know now :)

>

> Derick if you've filtered the security of the GPO's to just
> the service accounts then under what user account are you
> running RSoP? it will run under the context you are logged in
> as unless you are running it in planning mode to apply it to
> the account in question. Even then I am not sure that it will
> work properly if you've denied the user account you running
> it under access to the GPO.

I'm running it as Domain Admin. I've run modeling and planning modes with similar results. The consistent thing is that whenever there's a conflict with password policy that nothing gets set (red x or blank settings in the report). The conflict only happens when both policies can apply to the same computer. Doing a security filter with only users results in having the policy denied.

> Taking Laura's point into account, whilst the password policy
> is applied at the computer level, it still requires that the
> user accounts it affects be able to read it and have "apply
> group policy" permissions. Presumably then, if you were to
> set up an additional GPO at the top of the AD tree and deny
> all user accounts but the service accounts "apply group
> policy" permissions then the policy would only be applied to

RE: Group Policy: multiple password policies in the same domain?

SecurityFocus Microsoft: RE: Group Policy: multiple password policies in the same domain?

- > *the service accounts. Similarly you would need to ensure that*
- > *the rest of the user accounts in the domain have "apply group*
- > *policy" permissions denied on the GPO for the service*
- > *accounts, or that it is lower in the list.*

And that is what I tried first, to no avail. => I believe because the password policy is a computer-based setting it ignores filtering of users. Again, trying to apply two policies to one computer results in a clash that according to GPO modeling/planning/RSoP is resolved by not trying to do anything. I suppose this could be tested by applying one policy to the DCs only (using security filtering) and the other for Domain Computers (which is every computer but the DCs). I bet that local accounts on non-DCs would get the second policy while domain accounts would get the first, irrespective of where the user logged in.

- > *As to why the password policy is computer based or user based*
- > *– I think it makes no difference in the context of your*
- > *question – you can only apply a password policy at the top of*
- > *the AD tree and not in a GPO or object beneath it, so if it*
- > *was user based it would make no difference to what you are*
- > *trying to achieve.*
- >
- > *My thoughts as to why its computer based – well perhaps its*
- > *related to the fact that it is "the computer" that*
- > *authenticates the login? The account policies on a local*
- > *machine are found in the local security policy msc. on a*
- > *computer – which has no user related settings. A Group Policy*
- > *combines these settings with various other related policies,*
- > *it would make little sense then for password policy to be*
- > *found under the user node of a GPO since user objects have*
- > *nothing to do with authenticating logins.*
- >
- > *Richard*

I believe that you can apply password policies in other OUs but it will affect only the local computers in the OU for the very reason you state: the computer authenticates the login. For a domain account, the "local" computer is the domain controller, not the machine being logged into. I think that allowing multiple password policies tied to user groups is far more complicated than having it tied to a computer, and so that's why it's a computer setting.

Derick Anderson

- > -----Original Message-----
- > *From: Derick Anderson [mailto:danderson@vikus.com]*
- > *Sent: 31 August 2005 20:44*
- > *To: focus-ms@securityfocus.com*
- > *Subject: RE: Group Policy: multiple password policies in the*
- > *same domain?*
- >

RE: Group Policy: multiple password policies in the same domain?

SecurityFocus Microsoft: RE: Group Policy: multiple password policies in the same domain?

>
>
>
> > -----Original Message-----
> > From: Laura A. Robinson [mailto:laurarobinson@earthlink.net]
> > Sent: Wednesday, August 31, 2005 3:20 PM
> > To: Derick Anderson; focus-ms@securityfocus.com
> > Subject: RE: Group Policy: multiple password policies in the same
> > domain?
> >
> > *Inline replies to a couple of different people.*
> >
> > > *You can only set password policies affecting domain
> > > accounts using the
> > > "default domain policy" GPO – ie. the GPO at the top of
> > > the AD tree
> > > for a particular domain.*
> >
> > *Actually, that's not the case. You can only affect domain
> > accounts at
> > the domain level, but you do NOT have to use the "Default Domain
> > Policy" GPO.
> > You can create your own and it works. If you have multiple
> > domain-level policies that specify password settings, the
> > last applied
> > policy at the domain level will "win". My other post answering the
> > original question got bounced, but I clarified some of this in it.*
>
>
>
> *On my DC, running GPMC, if I do a GPO model with conflicting
> > policies, the report shows that the policies aren't set at
> > all. Are they actually set? Doing a RSoP gives me the red X
> > over all conflicting policies. I wasn't able to hunt down the
> > actual meaning of the red X in the couple minutes I could
> > spare to investigate, but I figure it's not good. I am just
> > wondering if the policy is actually set but the
> > reporting/RSoP features see it as a bad thing and that
> > explains their output.*
>
> > > *Does anyone know why the password policy is a computer and not a
> > > user-based setting?*
> >
> > *Why would it be a computer setting? That would make no
> > sense for all
> > of the users in the domain who are people rather than computers.
> > Again, you can only have a single password policy that affects
> > accounts stored in AD for a given domain.
> > Because both users and computers are stored in AD, the
> > password policy
> > applies to *any* account stored in AD.*

RE: Group Policy: multiple password policies in the same domain?

SecurityFocus Microsoft: RE: Group Policy: multiple password policies in the same domain?

> >

> > *Laura*

>

> *The password settings are in the computer section, not the user section.*

> *I couldn't fathom that idea, so I set up security filtering*

> *on the "Service Accounts" GPO to apply only to "Service*

> *Accounts" (a user group). Group Policy modeling reported back*

> *that the GPO was denied access due to security filtering.*

>

> *Here's my theory: It's easier to have the password policy*

> *computer-based instead of user-based. When a user*

> *authenticates/resets their password/is created, Windows*

> *checks the local computer password policies against the*

> *supplied password. Because it's a computer setting, there is*

> *only one thing to check: the local computer's policy (which*

> *is set by the domain policy on a domain). Since a domain user*

> *is like a local user on a domain controller (sort of), the*

> *domain controller policy is the only one that matters for*

> *that user in respect to passwords.*

>

> *Now let's imagine this was a user setting: I can now apply*

> *password policies to an individual user, group, whatever. I*

> *log on to a domain computer and the domain controller now has*

> *to figure out what group I'm in, what group policy applies to*

> *me, and therefore what my password requirements are. It must*

> *do this every time I attempt to authenticate (ignoring*

> *caching, etc.). And what if I'm a member of more than one*

> *group with differing password policies? Which group wins?*

>

> *I bet Microsoft thought about all that and said "nevermind."*

>

> *Derick Anderson*

>

> -----

> -----

> -----

> -----

>

>

> -----

> -----

> *Disclaimer: This email and any files transmitted with it are*

> *confidential and intended solely for the use of the*

> *individual or entity to whom they are addressed.*

>

> *If you have received this email in error please notify the*

> *originator of the message. This footer also confirms that*

> *this email message has been scanned for the presence of*

> *computer viruses and Henshaws Society for Blind People will*

> *not accept any responsibility for any loss of data or*

SecurityFocus Microsoft: RE: Group Policy: multiple password policies in the same domain?

- > *financial loss caused directly or indirectly by opening or*
- > *processing this email and any accompanying attachments.*
- >
- > *Any views expressed in this message are those of the*
- > *individual sender, except where the sender specifies and with*
- > *authority, states them to be the views of Henshaws Society*
- > *for Blind People.*
- >
- > *Please Note: Recipients of this message should be aware that*
- > *Henshaws Society for Blind People reserves the right to*
- > *monitor all email sent to and from the hsbp.co.uk domain or*
- > *any other domain that may be administered by the said organisation.*
- >
- > *Head office telephone number: 0161 872 1234 Head office fax*
- > *number: 0161 848 9889*
- > *website: <http://www.hsbp.co.uk>*
- >
- >
