

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/2005-09/0009.html>

From: Derick Anderson (*danderson_at_vikus.com*)

Date: 09/01/05

Date: Thu, 1 Sep 2005 14:32:27 -0400

To: <focus-ms@securityfocus.com>

Why two policies?

I have single domain that contains both end users and mission-critical service accounts, and our company must be SAS70 type-II certified. So the auditors come and say, "You must have secure password policies." This amounts to (in our case) at least 8 character passwords, a maximum age of 90 days, complexity requirements, a lockout policy of 5 attempts with infinite lockout, and a 1 day period between failed attempt count resets. When I first came the minimum length was 7 characters. The day I upped it to 8 you should have heard all the crying.

I consider 8 characters the bare minimum for a secure account password. Unfortunately our users cannot fathom security and while I personally use passphrases that exceed 20 characters I doubt very much that I could ever get the whole company past 10 and then I'd spend all my mornings unlocking accounts or resetting forgotten passwords.

The second issue is the lockout policy and password age – if you are only going to require 8 characters you'd better have some sort of lockout policy, in my opinion. However, when a mission-critical system runs as a domain service account, and a developer tries to use that same account for "debugging" (.NET machine config for the uninitiated) and uses the wrong password, it locks out the service account and DoSes the system. Clearly a security risk from an availability standpoint.

So the dilemma is that I need shorter passwords with tighter lockout policies for users, and longer passwords with no lockout policies for service accounts, and I have to be able to demonstrate that the password policy is in effect to the auditors. I can make the service account passwords as long as I want, but unless it can be proven that this is the case, we don't pass the audit next time around.

Derick Anderson

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

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

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

> *From: Brady McClenon [mailto:BMcClenon@uamail.albany.edu]*
> *Sent: Thursday, September 01, 2005 10:53 AM*
> *To: Derick Anderson; focus-ms@securityfocus.com*
> *Subject: RE: Group Policy: multiple password policies in the*
> *same domain?*

>
> *Why would you ever want different password policies for*
> *different accounts? I don't see the point of only having a*
> *portion of your accounts with strong passwords. If you are*
> *going to be serious about password security, be serious about*
> *it. What account is it not necessary to have a strong*
> *password if the others are? I'm just curious...*

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

> *From: Derick Anderson [mailto:danderson@vikus.com]*
> *Sent: Wednesday, August 31, 2005 3:44 PM*
> *To: focus-ms@securityfocus.com*
> *Subject: 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*

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

- > *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.*
- >>
- >> *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?*
- >

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

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

>

> *Derick Anderson*

>

> -----

> -----

> ----

> -----

> -----

> ----

>

>
