

microsoft.public.security: Re: password expiration policy for admin and system accounts ?

Re: password expiration policy for admin and system accounts ?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-10/0681.html>

From: Eddy – MCSE (*Eddy_at_noemail.postalias*)

Date: 10/25/05

Date: Tue, 25 Oct 2005 09:59:10 -0700

If you are worried about forced expirations, then I would implement a company policy that Admins manually reset these important account passwords every month (or whatever). You can still have the passwords set to never expire, but that does not mean that they should not be changed often. This may give you a little more control over when exactly is the best time to change passwords.

--

Eddy - MCSE

"Roger Abell [MVP]" wrote:

> Privileged accounts should be the most, not the least, well guarded.
> If your domain policy makes users change passwords each 60 days,
> your admins and domain admins accounts should get their passwords
> changed weekly (which means a human, not a machine enforced
> practice). Changing the passwords is not so much a limiter on the
> time available for cracking as it is a limiter on the length that a password
> that has travelled beyond appropriate hands can be usable there.
>
> You say changing service account passwords can cause critical services
> to stop working. That is not really the case, with planning and doing the
> right things at the right times. But, it can cause short-term
> interruptions.
> I feel most shops do not alter service account passwords on a regular
> basis, but I could be a good practice to implement. If you look you will
> notice that most services are not using custom accounts, which means
> that it is not all that many that are impacted by the auditor's request.
> For
> some of these the accounts are domain, but the scope of the others, the
> machine local service accounts (other than the built-in accounts local
> system, local service, network service) are limited to that one box.
> Perhaps you can arbitrate with the auditors on the frequency of change
> based on the scope of the exposure, the difficulty of gettings to the boxes
> to coordinate this, and, (this is the big one) your practice of using pass
> phrases for those accounts that have a minimum length that is some
> outrageously large size like 40 characters.
>
> --
> Roger Abell
> Microsoft MVP (Windows Server : Security)
> MCDBA, MCSE W2k3+W2k+Nt4
> "JJ" <johnny@tamtam.com> wrote in message
> news:pNz5f.9585\$oy3.4278@trnddc04...
> > Our auditors are objecting to our having Domain Administrator and domain

Re: password expiration policy for admin and system accounts ?

microsoft.public.security: Re: password expiration policy for admin and system accounts ?

> > system accounts with passwords that never expire.
> >
> > Yes, we change some of these passwords from time to time, but they're
> > normally set to never expire.
> >
> >
> > We are wondering about how other companies do it, since we've never heard
> > of
> > any IT Dept. that had such a policy, and we think the auditors are being
> > unreasonable -- forcing password expiration on such accounts could be a
> > logistical nightmare as it would cause critical services to stop running.
> >
> > We're not that big, but we do have about 30 servers and 200 users to
> > support. There's only 1 Win2K domain, with Exchange 2K, SQL and other
> > resource servers.
> >
> > Please post your experiences and opinions.
> >
> > Thanks.
> >
> >
>
>
>