Configuring Account Lockout

We can recommend an ideal configuration for most of the settings in our security guidance. For example, the “Debug programs” privilege should be granted to Administrators and to no one else. For account lockout, however, there is no “one size fits all” setting, but there’s a lot of heated discussion whenever anyone tries to pick one. Ultimately, each organization must determine what best meets their own needs. This blog post tries to help by discussing the issues and tradeoffs of enabling account lockout and how tightly to enforce it. We had to pick *something* for the baseline, so we discuss the settings we selected and why we changed them from what we had selected for other recent baselines. Again, though, this is one where you should take a close look at the threats and tradeoffs for your own environment before applying the settings we picked.

# The Basics of Account Lockout

The purpose of account lockout is to make it harder for password-guessing attacks to succeed. If account lockout is not configured, an attacker can automate an attempt to log on with different user accounts, trying common passwords as well as every possible combination of eight or fewer characters in a very short amount of time, until one finally works. When account lockout is configured, Windows locks the account after a certain number of failed logon attempts, and blocks further logon attempts even if the correct password is supplied.

Windows account lockout can be configured with these three settings:

* *Account lockout threshold*: the number of failed logon attempts that trigger account lockout. If set to 0, account lockout is disabled and accounts are never locked out.
* *Account lockout duration*: the number of minutes that an account remains locked out before it’s automatically unlocked. If set to 0, the account remains locked out until an administrator explicitly unlocks it.
* *Reset account lockout counter after*: the number of minutes after a failed logon attempt before the bad-logon counter is reset to 0. The counter is also reset after a successful logon.

# Account Lockout Tradeoffs

While account lockout can help prevent intrusion, it can also expose your organization to accidental lockouts as well as to denial of service attacks.

Not every bad logon attempt reflects an attempt to gain unauthorized access. Users sometimes forget their passwords. Also, applications, particularly those that use saved passwords, are often unaware of a password change and continue to use the old password, sometimes automatically retrying the same password many times in a short amount of time. This becomes increasingly true as users have more devices such as phones and tablets that log on to get email or other corpnet access. If the account lockout threshold is set too low, you are likely to see a lot of accidental lockouts. In addition to users not being able to perform their work, lockouts can lead to expensive helpdesk calls, especially when administrator intervention is required to unlock the account. Finding the root cause of accidental lockouts can be time-consuming as well. It’s therefore good to set a threshold that avoids accidental lockouts, while not setting the threshold so high that attackers are given too much opportunity to succeed. Setting the lockout duration to a “reasonable” non-zero value can also reduce helpdesk calls. The combination of threshold, lockout duration and reset settings determines how many guesses attackers get per day; ideally you slow them down to the point that it becomes impractical or at least not worthwhile for them to pursue this type of attack.

At the same time, whenever account lockout is configured at all it is easy for an attacker to conduct a denial of service attack and deliberately lock out accounts. It doesn’t matter whether you set the threshold to 5 or 50 – an automated attack can perform that many deliberately failed logon attempts on a large number of accounts very quickly and lock them out. If the lockout duration is short, an attacker can still maintain a sustained attack, locking out accounts as soon as they become unlocked. If the lockout duration is indefinite (0), then this can be a crippling attack.

# Reducing or Eliminating the Need for Account Lockout

If you employ other mitigations against password-guessing attacks, you can afford to set a higher lockout threshold or even disable account lockout altogether. Some of these mitigations are:

* Proactively monitor for failed logon events and have a robust response mechanism in place when password-guessing is detected.
* Configure “Smart card required for interactive logon” (SCRIL), and do not manually set a password for the account after doing so. When SCRIL is configured, the account’s password hash is replaced with a random value, making a password logon effectively impossible. When SCRIL is configured, therefore, account lockout should be disabled to prevent denial of service.
* Require long passwords. The entire set of eight-character passwords can be tested in a short amount of time. Windows policies allow you to set a minimum length of up to 14 characters, which is the setting we recommend. Passwords can be up to 256 characters, but Windows won’t let you *demand* more than 14 without a custom password filter.
* Require password complexity. Requiring multiple types of characters increases the likelihood that users will pick strong passwords. Note, however, that it does not guarantee strong passwords: for example, “Password!” meets the complexity requirement but is easily guessed.

# Baseline Selections

As we said at the outset, there is no single account lockout configuration that works for all organizations. Our recommendation regarding account lockout is to consider the tradeoffs and pick what’s right for your situation. However, our security guidance includes GPOs and security templates that you can apply directly, and it’s not possible to set the account lockout threshold in them to “do the right thing”. So we have to pick something.

The settings in our baselines are intended for large audiences. We recognize that many organizations will apply these settings without reading the fine print or considering the nuances and tradeoffs. We have to try to find the right balance between security and “break everything” that will work reasonably well for most organizations.

We have selected a threshold of 10 bad attempts, a 15 minute lockout duration, and counter reset after 15 minutes (10/15/15). That threshold value is a change from the Windows 8.1 / Windows Server 2012 R2 beta guidance as well as from past baselines.

The threshold we published with the Windows 7 / Windows Server 2008 R2 guidance was 50 bad attempts. With the 15 minute duration and 15 minute counter reset, that gave attackers up to 200 guesses per hour. For Windows 8 / Server 2012 we had changed it to 5, after much discussion with the external security community, including the Center for Internet Security (CIS), the US National Security Agency (NSA), the US Defense Information Systems Agency (DISA) and others. The thinking at that point was that a typical user is unlikely to mistype their password five times unless they really don’t remember it, in which case they’ll probably need to call the helpdesk anyway. We have increased that threshold to 10 because our support engineers have seen many accidental lockouts, particularly with the increase in devices per user. Increasing the threshold to 10 should reduce the number of accidental lockouts, while at the same time not giving attackers 200 guesses per hour again.

# Account Lockout Technical Errata

The public documentation may not be clear about these points, and they are worth knowing:

An attempted logon using either of an account’s two most recent previous passwords will not succeed, but will not increment the bad-logon counter either. In other words, repeated use of a saved password will trigger account lockout only after the third password change.

Failed attempts to unlock a workstation can cause account lockout even if the “Interactive logon: Require Domain Controller authentication to unlock workstation” security option is disabled. Windows doesn’t need to contact a DC for an unlock if you enter the same password that you logged on with, but if you enter a different password, Windows has to contact a DC in case you had changed your password from another machine. It’s actually easy to lock out an account on a locked workstation in seconds just by pressing Ctrl+Alt+Del and then holding down the Enter key.