Protecting Outlook Web App & Active Directory from Denial of Service and Brute Force Attacks

If you had to choose, which security attack would you allow: opening your network up to brute force attacks or tolerating denial of service attacks? The first answer that probably comes to mind is neither. Yet, when configuring the account lockout policies in the Group Policy Management Console, this is the all-important question that you must ask yourself, because, depending on how you configure the account lockout threshold, you will be forced to allow one or the other attack. If there is an alternative choice that protects against both attacks, it would be worth considering.
The account lockout threshold is one of three configurable account lockout policy settings in the Group Policy Object (GPO) that allows the system administrator to block a user’s access to the system when a user ID fails a predefined number of logon attempts sequentially. In a brute force attack, there are repeated failures as the brute force algorithm tries different password guesses over and over again. When the predefined threshold for logon failures is reached, the user ID is locked out and no one, including the legitimate user with a valid password, can access that account, effectively creating a denial of service. The locked account cannot be used again until an administrator unlocks it or the time specified by the account lockout duration setting has elapsed. The difficult choice comes in deciding how to deal with repeated logon failures, and whether to turn off the lockout threshold (a setting of 0, or set it to trigger when a maximum number of failed attempts occurs.

Logon failures can represent legitimate users forgetting or mistyping their passwords, or they can be malicious users trying to gain access to your systems. By leaving the threshold setting off, you are allowing an unlimited number of password guesses, which leaves the system vulnerable to brute force attacks, password guessing attacks, and other automated connections. (You can review your current account lockout settings by running the Powershell command in the reference section below to see if you are vulnerable to these attacks.

The advantage of turning the account lockout off is that you are not vulnerable to an account lockout Denial of Service (DoS. However, this means that you will be vulnerable to brute force attacks, but will have fewer support calls for account and password resets. This option is not ideal.

Let’s say that you choose to set a lockout threshold as you are more concerned with brute force and dictionary attacks than you are with user inconvenience and extra support desk workload. By setting an account lockout threshold, user accounts will be locked after a given number of failed password attempts. While this reduces the likelihood that an attacker will successfully carry out a password guessing attack, you are now vulnerable to account lockout DoS attacks where a malicious attacker could lock out a large number of your users from the system simply by logging on to multiple accounts with random passwords. Again, this is not an ideal option.

According to a Microsoft TechNet article (Account Lockout Policy describing account lockout settings, “because vulnerabilities can exist when this value is configured and when it is not, any organization should weigh their identified threats and risks that they are trying to mitigate.” The best practices laid out in the article for setting the account lockout threshold state “the threshold that you select is a balance between operational efficiency and security, and it depends on your organization’s risk level.” Not exactly the answer you were hoping for or a decision you want to make. Why should you have to compromise and be forced to choose to protect your organization from only one of the security issues?

Microsoft Exchange and Outlook Web

So, how does all of this impact Microsoft Exchange and Outlook Web? Well, Outlook Web (OWA) shares the same account lockout policy as the network account. This means that if a user gets locked out of either their OWA account or their network account, they are actually locked out of both!
Due to its very nature, OWA presents a convenient point of entry for would-be attackers as it is easily found on the internet and is accessible from anywhere in the world, making it a target for automated brute force password attacks or denial of service attacks.

OWA also provides the option to choose whether the OWA logon authentication honors the GPO account lockout policy settings or ignores them. If you honor the account lockout settings, then failed OWA logon attempts count towards the account lockout threshold that you have configured and you open yourself up to possible account lockout DoS attacks via OWA. If you do not honor the GPO account lockout settings, then automated password guessing scripts can be unknowingly run against your users’ accounts. The same catch-22 conundrum.

Protecting Outlook Web from Brute Force and DoS

Employing one or the other, account lockouts or unlimited password guesses, as your only security strategy for OWA is not recommended, but there are several products available to address these security concerns, including Messageware Exchange Protocol Guard, one time password (OTP) solutions, and 2-factor tokens.

Exchange Protocol Guard is the latest upgrade to our successful OWA Guard product, which has been protecting organizations for many years. EPG secures, monitors, records, analyses and alerts on incoming Exchange Server services like ActiveSync, Autodiscover, ECP, EWS, OWA, and OutlookAnywhere. EPG installs on your Exchange servers and maintains a lockout system independent of Active Directory, reducing lockouts of legitimate users and eliminating the need for constant password resets. EPG also enhances 2FA/MFA protection by securing the Exchange services and protocols that remain unprotected.

To learn more about the security options you have with Messageware Exchange Protocol Guard, visit [www.messageware.com/epg/](http://www.messageware.com/epg/)
References:

Microsoft TechNet: Group Policy Management Console
Microsoft TechNet: Account Lockout Policy

GPO - Computer Configuration \ Windows Settings \ Security Settings \ Account Policies \ Account Lockout Policy
  • Account lockout duration
  • Account lockout threshold
  • Reset account lockout counter after

Account Lockout Threshold:

The lockout threshold is turned off by default.

To review what your current account lockout settings are, run the following Powershell commandlet:
  • Ensure you can execute Active Directory Powershell commandlets
  • Launch Powershell as an Administrator and execute the command:
    • Get-ADDefaultDomainPasswordPolicy | Format-List lockout*

About Messageware

Messageware is the market leader in securing Microsoft Exchange Servers and enhancing Microsoft 365. Our security software provides login, attachment, protocol, and session security. Our productivity software provides Outlook Web and Windows desktop integrations, and Line of Business Office Add-ins. Combined, Messageware solutions give organizations a greater return on their messaging investments through increased security, increased employee productivity and reduced support and IT administration costs. Messageware products are used by over 2,500 enterprises and 5 million users worldwide in every industry.