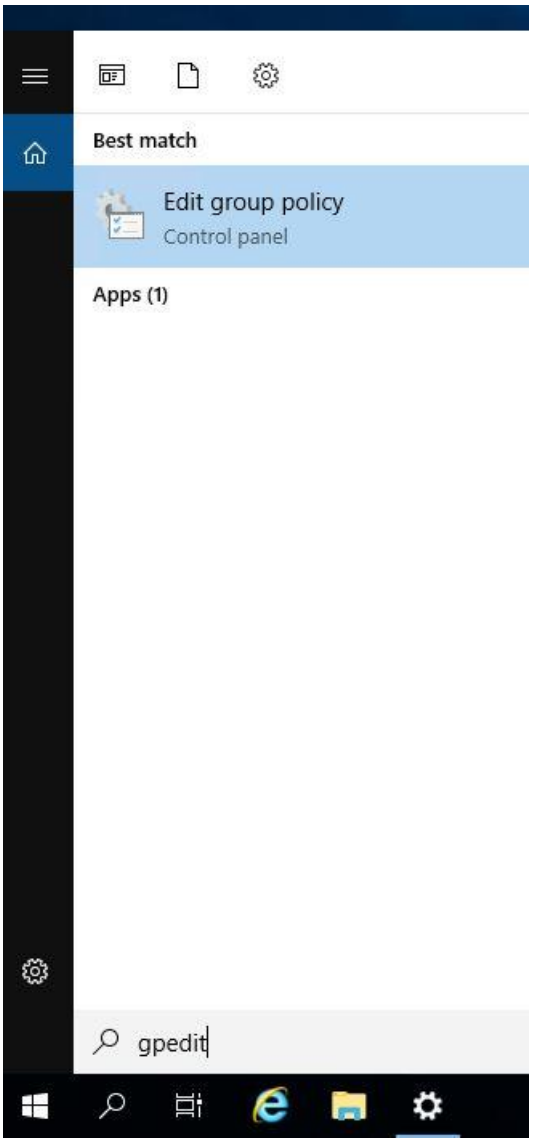
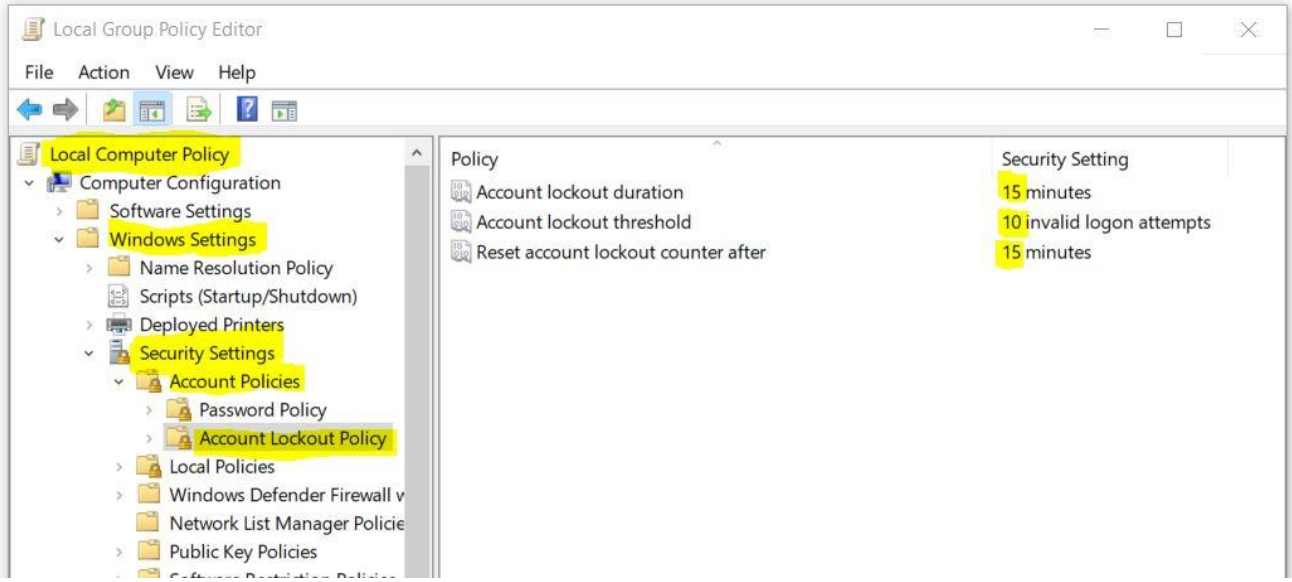
# Patstāvīga Microsoft Windows iekārta (nav pievienota domēnam) - lokālo lietotāju kontu bloķēšana pēc vairākiem neveiksmīgiem pieslēgšanās mēģinājumiem

1. **Windows darbstacijā/serverī, kas nav pievienota domēnam (piemēram, WORKGROUP), atveram "Local Group Policy Editor" un rediģējam "Local Computer Policy" .**




Spiežam uz Start/Windows logo un uzreiz rakstam jeb meklēšanas laukā (ikona ar lupu) ievadam `gpedit` (protams, var rakstīt arī pilno nosaukumu `edit group policy`) un izvēlamies "Edit Group Policy"

2. **Rediģējam esošo "Local Computer Policy" - kad lokālais lietotājs mēģina pieslēgties iekārtai (arī attālināti ar Remote Desktop), tiek skaitīti secīgi neveiksmīgas pieslēgšanās mēģinājumi (šeit piemērs ir ar 10 reizēm) un, kad definētais limits ir sasniegts, lietotāja konts tiek īslaicīgi bloķēts (šajā piemērā tas ir uz 15 minūtēm) vai arī līdz brīdim, kad sistēmas Administrators lietotāju atbloķē (skatīt 4. punktu).**



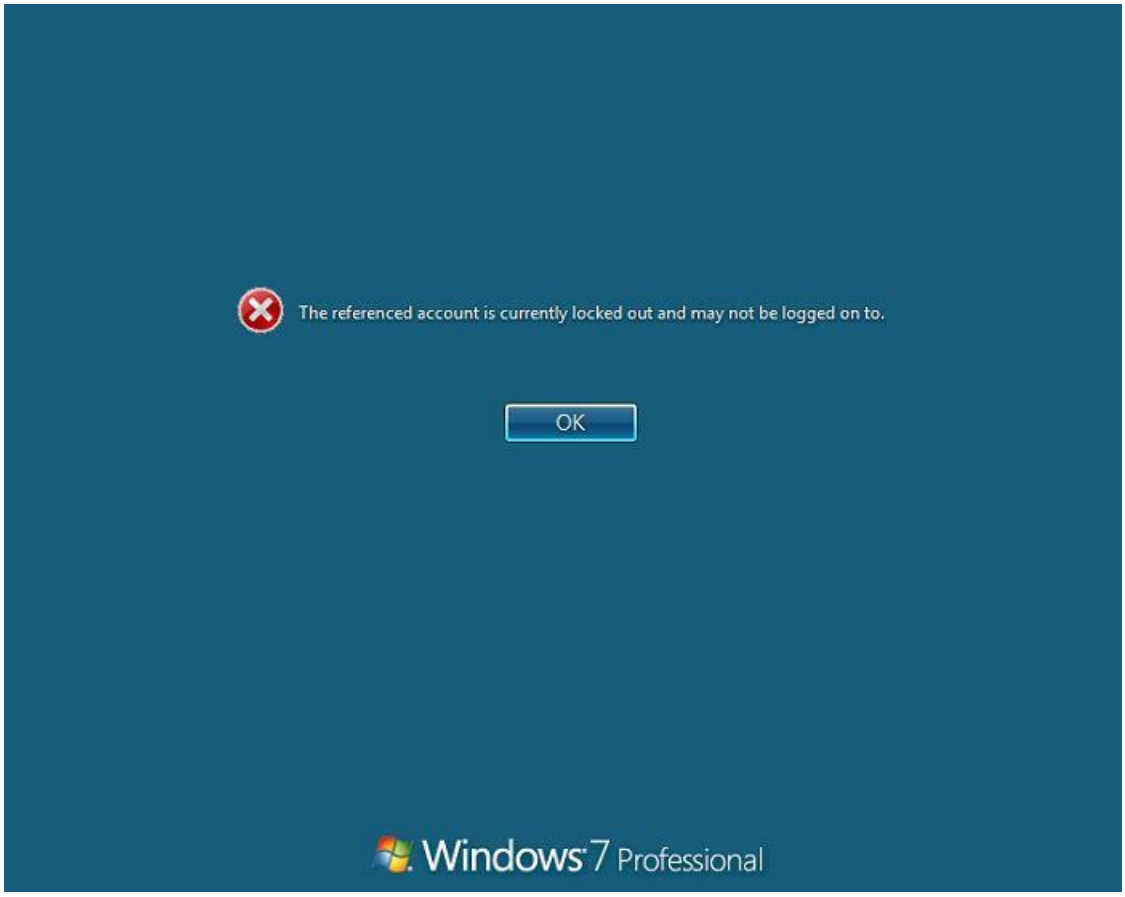

Atveram `Computer Configuration- > Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy`

Izvēlamies sekojošas vērtības (tās, protams, var pielāgot sava uzņēmuma/organizācijas vajadzībām):
Account lockout duration – **15**
Account lockout threshold **– 10**
Reset account lockout counter after – **15**

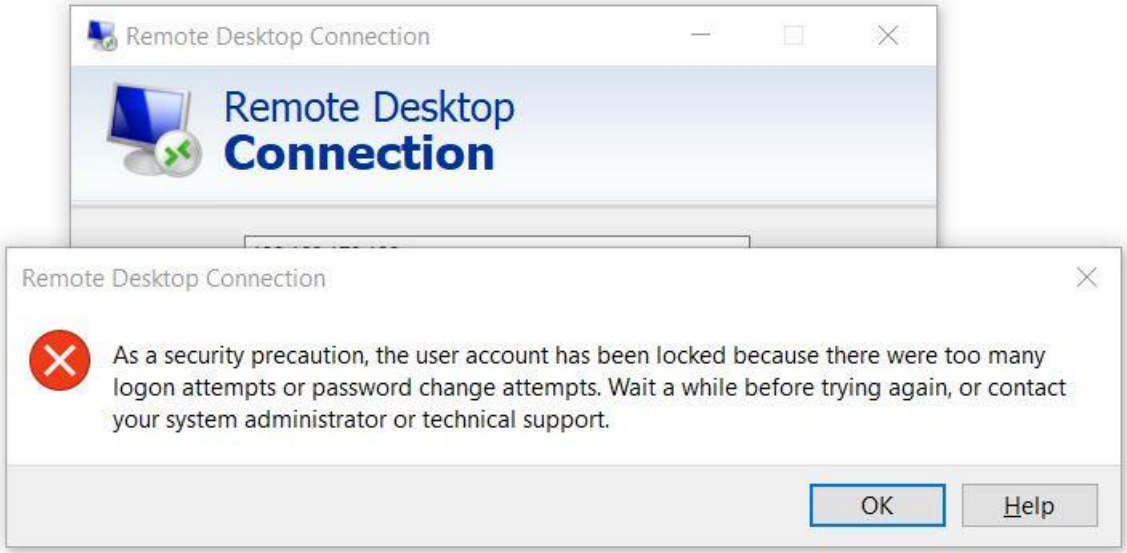
!!! Tieši šāds pieslēgšanās mēģinājumu skaits un bloķēšanas ilgums lietotāju kontiem tiek rekomendēts no Microsoft puses (*Windows security baselines*). Vairāk informācijas par šiem un arī citiem ar drošību saistītiem iestatījumiem, pieejama šeit: https://www.microsoft.com/en-us/download/details.aspx?id=55319

3. **Pēc "Local Computer Policy" politikas rediģēšanas, lietotāji, mēģinot pieslēgties Windows sistēmai ar vairāk nekā 10 secīgiem neveiksmīgiem mēģinājumiem, redzēs kādu no šiem vai citu līdzīgu paziņojumu (atkarīgs no OS versijas):**


Paziņojums par bloķētu lietotāja kontu Windows 10/Windows Server2016/ Windows Server2019 operētājsistēmā

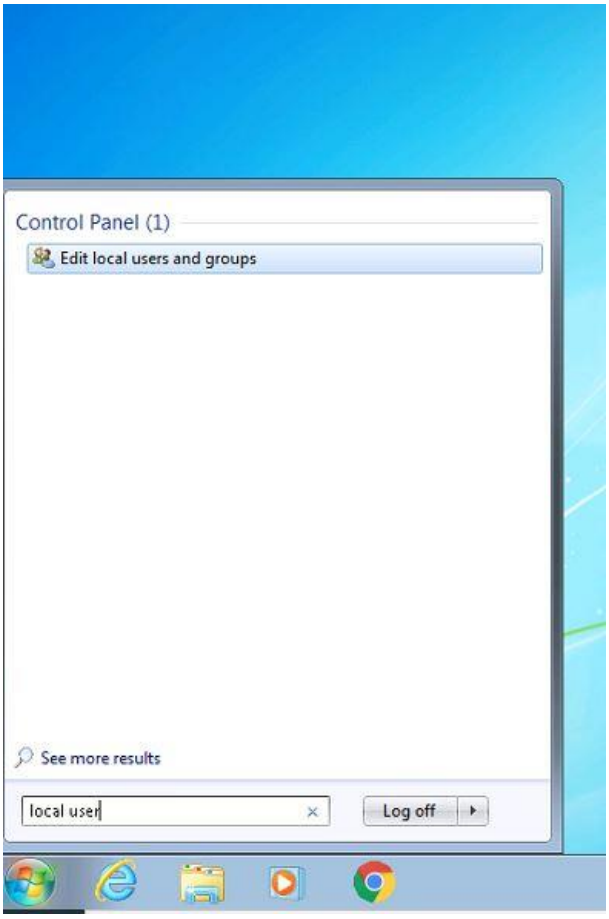



Paziņojums par bloķētu lietotāja kontu Windows 7 operētājsistēmā

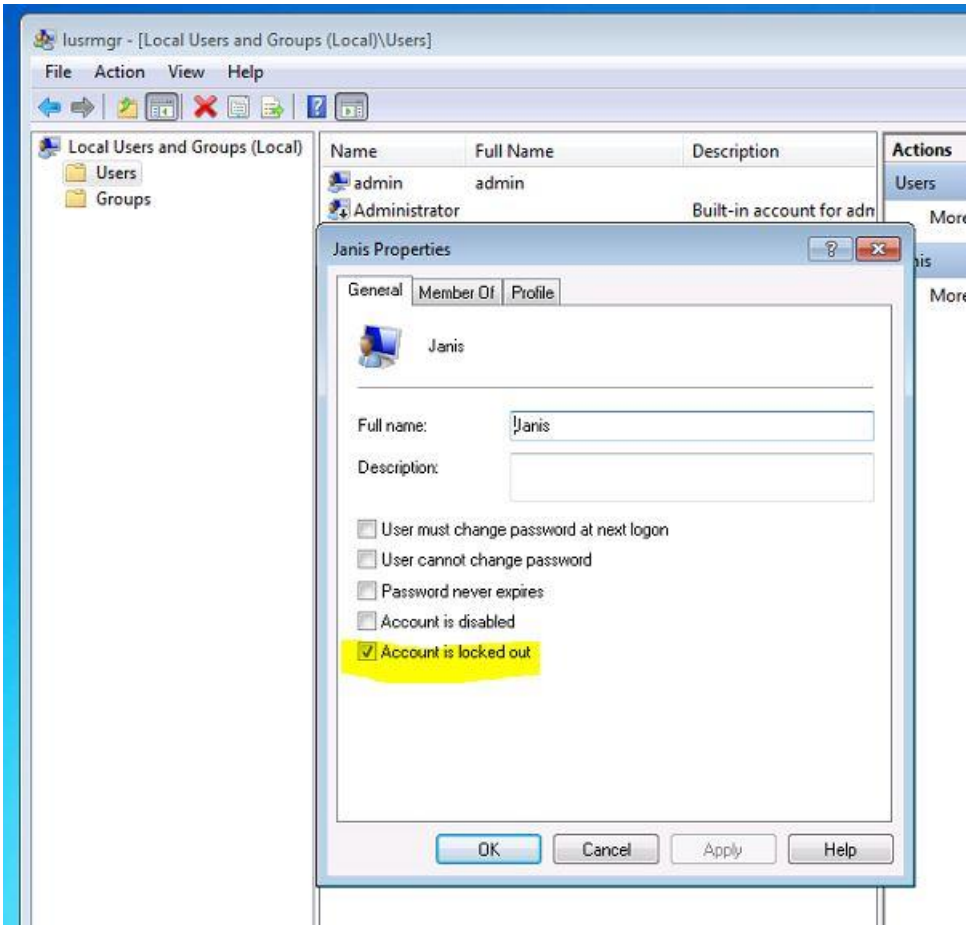



Paziņojums par bloķētu lietotāja kontu, ja izmanto Windows Remote Desktop programmatūru, lai pieslēgtos sistēmai attālināti

4. **Lietotāja konts atbloķēsies, kā arī neveiksmīgo mēģinājumu skaits *nonullēsies* automātiski pēc 15 minūtēm ( šīs vērtības tika norādītas šīs instrukcijas otrajā punktā). Gadījumā, ja ir nepieciešams kontu atbloķēt nekavējoties, sistēmas administratoram ir pieejama šāda opcija. To var izdarīt, lokālo lietotāju sarakstā atrodot nepieciešamo kontu un izņemot ķeksīti pie "Account is locked out" (šo var darīt arī izmantojot Powershell).**



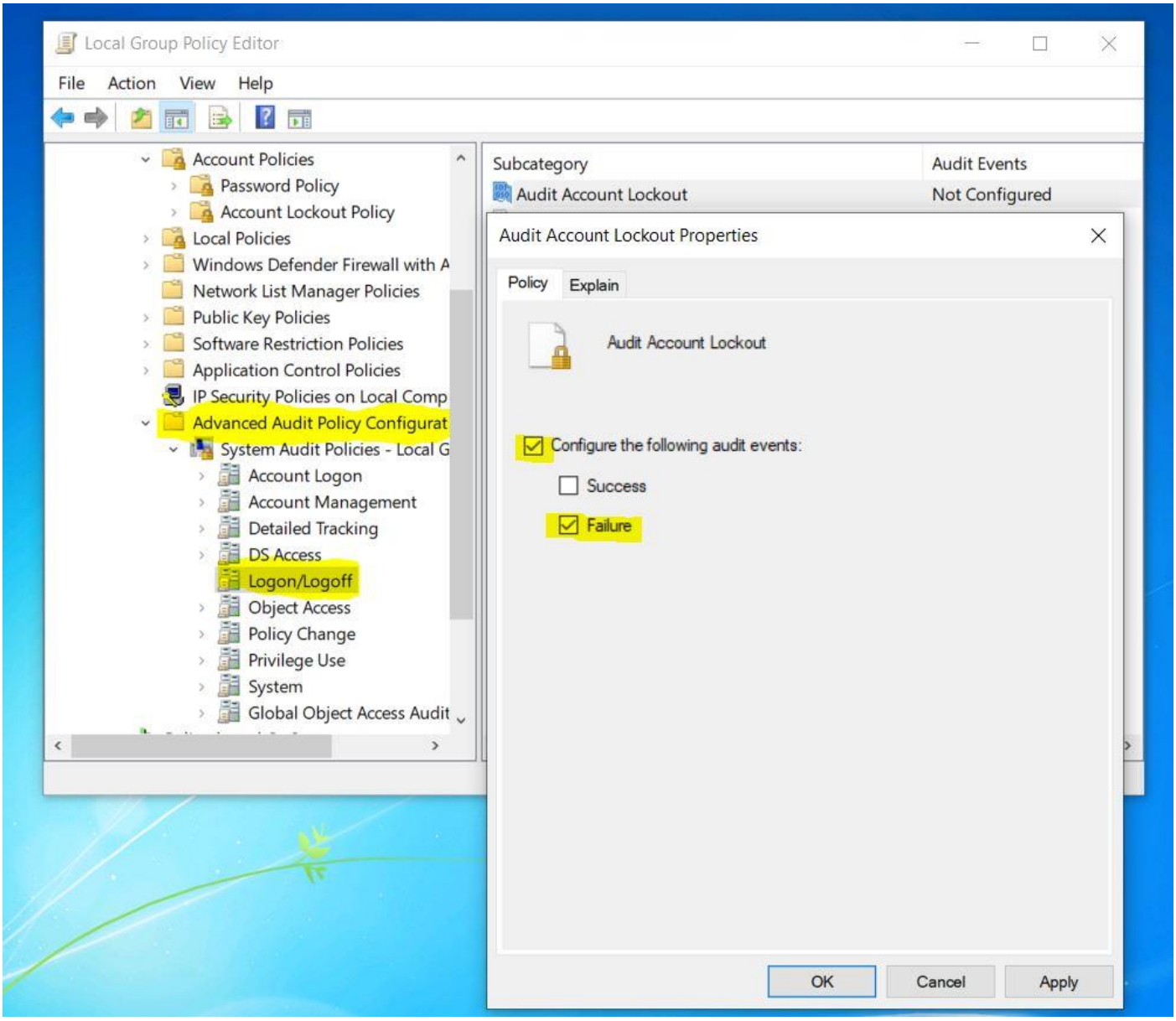

Atveram sistēmas lokālo lietotāju sarakstu, izmantojot meklēšanas funkciju – rakstam `local users`




Lietotāja atbloķēšana izmantojot grafisko saskarni – izņemam ķeksi no "`Account is locked out`"

PAPILDUS IETEIKUMS:

Rekomendējam uz Windows iekārtām ieslēgt arī auditācijas pierakstus, kas ir attiecināmi uz lietotāju kontu bloķēšanos. To var izdarīt, atverot iepriekš minēto "Local Computer Policy" (skatīt 2. punktu) un izvēloties **`Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies -> Logon/Logoff`**: `Audit Account Lockout – Failure.`




Tiks reģistrēti tikai Failure notikumi, t.i. neveiksmīgie pieslēgšanās mēģinājumi, kamēr konts ir bloķēts. Šie notikumi Windows žurnālierakstos tiek apzīmēti ar EventID:4625 ( par šo EventID vairāk var lasīt šeit: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625 )

!!! CERT.LV ir izstrādājusi rekomendācijas auditēšanas iestatījumiem Windows domēna infrastruktūrā (daļu no ieteikumiem var pielietot arī uz iekārtām, kas nav pievienotas domēnam), ar kurām varat iepazīties šeit: https://cert.lv/lv/2020/04/rekomendacijas-auditesanas-iestatijumiem-windows-domena-infrastruktura