

Re: Logon Type Identification

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-09/0683.html>

From: Steven L Umbach (*n9rou_at_n0-spam-for-me-comcast.net*)

Date: 09/28/05

Date: Tue, 27 Sep 2005 18:45:23 -0500

The link below will help. Type 7 means someone unlocked their computer and type 11 is a cached interactive logon which could be of concern unless it is found on laptop computers not connected to the domain. Cached logon means the user logged onto their computer with domain credentials even though a domain controller could not be contacted. For local network computers this could mean a network connectivity problem, dns misconfiguration for the domain controller or domain client, or the user may have intentionally unplugged their network cable to bypass logon/startup scripts and Group Policy refresh. Cached domain logons can be disabled via security policy. --- Steve

<http://www.windowsecurity.com/articles/Logon-Types.html>

Logon Type 7 – Unlock

Hopefully the workstations on your network automatically start a password protected screen saver when a user leaves their computer so that unattended workstations are protected from malicious use. When a user returns to their workstation and unlocks the console, Windows treats this as a logon and logs the appropriate Logon/Logoff event but in this case the logon type will be 7 – identifying the event as a workstation unlock attempt. Failed logons with logon type 7 indicate either a user entering the wrong password or a malicious user trying to unlock the computer by guessing the password.

Logon Type 11 – CachedInteractive

Windows supports a feature called Cached Logons which facilitate mobile users. When you are not connected to the your organization's network and attempt to logon to your laptop with a domain account there's no domain controller available to the laptop with which to verify your identity. To solve this problem, Windows caches a hash of the credentials of the last 10 interactive domain logons. Later when no domain controller is available, Windows uses these hashes to verify your identity when you attempt to logon with a domain account.

"Cindy" <Cindy@discussions.microsoft.com> wrote in message news:8969FBAA-4CF8-4557-B68C-8C1C73E561F0@microsoft.com...

> *Hi:*

> *I would like to know what the different logon type numbers in logon*

> *events.*

microsoft.public.security: Re: Logon Type Identification

- > *I know Type2 is interactive logon but type 7 and 11 also show up in event*
- > *logs on one of our laptops. I am not looking for the Event numbers,*
- > *rather*
- > *what type of logon was attempted by the different logon type #s.*
- >
- > *I searched Technet but could only find event numbers for that type 2 was*
- > *interactive logon.*
- >
- > *Thanks,*