Quick Reference Guide

netwrix

Login/Logoff Auditing

This quick reference guide shows how to track user logins and logoffs to important workstations or servers in security event log.

Audit Policy Settings

- Run GPMC.exe (url2open.com/gpmc) create a new policy and link this GPO to an organizational unit (OU) that contains the computers in which you'd like to track user activity on. Once the GPO is created you must go into > Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies:
    - ■ *System > Audit Security State Change set to success*
    - ■ *Audit Policies > Logon/Logoff > "Audit Logon" and "Audit Logoff" and set to success and failure*
    - ■ *Audit Policies > Logon/Logoff > Audit other logon/logoff events set to success and failure*

Query The Security Event Logs of All Computers

- Edit and run the following code in Powershell ISE:

```
Get-ADComputer -SearchBase ‘OU=yourOU,DC=domain,DC=com’ -Filter * | Select-Object Name #query all of the target computers in the OU
$Computers = (Get-ADComputer -SearchBase ‘OU=yourOU,DC=domain,DC=com’ -Filter * | Select-Object Name).Name #Put all computers into a variable
$EventFilterXPath = "(Event[System[EventID='4647']] or Event[System[EventID='4648']])" #Query each computer and find all the instances of both the user logon event (ID 4648) and user logoff event (ID 4647)
foreach ($Computer in $Computers) {Get-WinEvent -ComputerName $Computer -LogName Security -FilterXPath $EventFilterXPath} #Use Get-WinEvent against each computer using this Xpath filter
$SelectOuput = @(    @{n='ComputerName';e={$_.MachineName}},
@{n='Event';e={if ($_.Id -eq '4648') { 'Logon' } else { 'LogOff'}}},
@{n='Time';e={$_.TimeCreated}},
@{n='Account';e={if ($_.Id -eq '4647') { $i = 1 } else { $i = 3 } [regex]::Matches($_.Message,'Account Name:\s+(.*)\n’).Groups[$i].Value.Trim()}}) #find both user logon and logoff events which user generated and from which computer the event came from
foreach ($Computer in $Computers) {
Get-WinEvent -ComputerName $Computer -LogName Security -FilterXPath $EventFilterXPath | Select-Object $SelectOuput | Format-Table -AutoSize}
```

Event ID Reference

■	4608	Startup
■	4609	Shutdown
■	4624	Logon
■	4625	An account failed to log on
■	4634	Logoff
■	4647	Begin Logoff
■	4648	Logon Attempt
■	4778	Session Reconnected
■	4779	Session Disconnected
■	4800	Workstation Locked
■	4801	Workstation Unlocked
■	4802	Screensaver Invoked
■	4803	Screensaver Dismissed
■	4768	A Kerberos authentication ticket (TGT) was requested.
■	4769	A Kerberos service ticket was requested.
■	4770	A Kerberos service ticket was renewed.
■	4771	Kerberos pre-authentication failed.
■	4772	A Kerberos authentication ticket request failed.
■	4776	The domain controller attempted to validate the credentials for an account.
■	4777	The domain controller failed to validate the credentials for an account.
■	5378	The requested credentials delegation was disallowed

Gain #completevisibility into who logged into what, when, and from where and get a video record of that session with Netwrix Auditor for Windows Servers: netwrix.com/go/trial-ws

Corporate Headquarters:
300 Spectrum Center Drive, Suite 1100,
Irvine, CA 92618

Toll-free: 888-638-9749

Int'l: 1-949-407-5125
EMEA: 44 (0) 203-318-0261

netwrix.com/social