



## AD Account 10 Stunden nach letzten Logon deaktivieren

Mit diesen beiden Beispiel-Skripten können wir AD Konten nach einer beliebigen Zeit deaktivieren. Mein Ziel war es, AD Konten von externen Support Mitarbeitern 10 Stunden nach dem letzten Logon zu deaktivieren.

Aktuell habe ich nur einen User dessen letzter Logon mehr als 1 Stunde her ist. Dieser würde jetzt deaktiviert werden.

### Skript 1)

```
# Jörn walter https://www.der-windows-papst.de
clear
$domain = "ndsedv.de"
$HoursInactive = 10
$time = (Get-Date).AddHours(-($HoursInactive))

Get-ADUser -Filter {LastLogon -lt $time -and enabled -eq $true} -Properties
LastLogon -Server dc01 -SearchBase "OU=User
Accounts,OU=User,OU=ORG,DC=ndsedv,DC=de" |
select-object samaccountname,@{Name="LastLogon";
Expression={[DateTime]::FromFileTime($_.lastLogon).ToString('dd-MM-yyyy
hh:mm:ss')}} | export-csv C:\Temp\inactiveUser.csv -notypeinformation

Import-Csv "C:\Temp\inactiveUser.csv" | ForEach-Object { $samAccountName =
$_."samAccountName" Get-ADUser -Identity $samAccountName | Disable-ADAccount }
```

### Skript 2)

```
# Jörn walter https://www.der-windows-papst.de
$time = [DateTime]::Now.Subtract([TimeSpan]::FromHours(10)).ToFileTime()
Search-ADAccount -accountinactive -useronly -SearchBase "OU=User
Accounts,OU=User,OU=ORG,DC=ndsedv,DC=de" | where {$_.lastlogon -lt $time} |
Disable-ADAccount -whatif
```

### Ausgangssituation:

Das sind die aktuellen Timestamps folgender User:

Der User adm\_jwalter hat sich erst gerade authentifiziert.

The screenshot shows the Active Directory console with the user 'adm\_jwalter' selected. The 'Eigenschaften von adm\_jwalter' dialog box is open, displaying the 'Attribute' tab. The 'lastLogon' attribute is highlighted with a red arrow, showing a value of '06.10.2017 23:43:52'. Other attributes include 'displayName', 'distinguishedName', 'lastLogoff', 'lastLogonTimestamp', and 'logonCount'.

Attribut	Wert
displayName	adm_jwalter
distinguishedName	CN=adm_jwalter,OU=User Accounts,OU=Us
dScorePropagationD...	05.10.2017 21:30:46 Mitteleuropäische Som
instanceType	0x4 = ( WRITE )
lastLogoff	(nie)
lastLogon	06.10.2017 23:43:52 Mitteleuropäische Som
lastLogonTimestamp	05.10.2017 20:45:30 Mitteleuropäische Som
logonCount	11
msDS-SupportedEncr...	0x0 = ( )
name	adm_jwalter
objectCategory	CN=Person,CN=Schema,CN=Configuration,I
objectClass	top; person; organizationalPerson; user
objectGUID	dda02529-6415-4aca-b23e-5e6bd8234b09
objectSid	S-1-5-21-1114462570-1726162390-2557311



## AD Account 10 Stunden nach letzten Logon deaktivieren

Der User CAAdmin hat sich vor gut 17 Tagen zuletzt authentifiziert.

The screenshot shows the Active Directory console with the 'Eigenschaften von CAAdmin' dialog box open. The 'lastLogon' attribute is highlighted with a red arrow. The attribute list is as follows:

Attribut	Wert
displayName	CAAdmin
distinguishedName	CN=CAAdmin,OU=User Accounts,OU=User,...
dScorePropagationD...	06.10.2017 23:39:34 Mittteleuropäische Som...
instanceType	0x4 = ( WRITE )
lastLogoff	(nie)
lastLogon	10.09.2017 23:01:48 Mittteleuropäische Som...
lastLogonTimestamp	10.09.2017 18:57:41 Mittteleuropäische Som...
lockoutTime	0
logonCount	36
name	CAAdmin
objectCategory	CN=Person,CN=Schema,CN=Configuration,...
objectClass	top; person; organizationalPerson; user
objectGUID	02082424-1a21-469d-aea3-1aDe49c1281f
objectSid	S-1-5-21-1114462570-1726162390-2557311

Der User Test hat sich vor gut 10 Monaten zuletzt angemeldet.

The screenshot shows the Active Directory console with the 'Eigenschaften von Test' dialog box open. The 'lastLogon' attribute is highlighted with a red arrow. The attribute list is as follows:

Attribut	Wert
displayName	Test
distinguishedName	CN=Test,OU=User Accounts,OU=User,OU=...
dScorePropagationD...	05.10.2017 19:17:19 Mittteleuropäische Som...
homeMDB	CN=Mailbox Database 0908720125,CN=Dat...
instanceType	0x4 = ( WRITE )
lastLogoff	(nie)
lastLogon	21.11.2016 14:25:25 Mittteleuropäische Som...
lastLogonTimestamp	21.11.2016 14:25:25 Mittteleuropäische Som...
legacyExchangeDN	/o=NDSedV/ou=Exchange Administrative G...
logonCount	1
mail	test@ndsedv.de
mailNickname	test
mDBUseDefaults	TRUE
msDS-SupportedEncr...	0xD = ( )



## AD Account 10 Stunden nach letzten Logon deaktivieren

Der User Test1 und Test2 waren noch nie angemeldet.

Active Directory-Benutzer und -Computer

Name | Typ

- adm\_jwalter | Benutzer
- CAAdmin | Benutzer
- Test | Benutzer
- Test1 | Benutzer
- Test2 | Benutzer

Eigenschaften von Test1

Attribut	Wert
dScorePropagationD...	0x0 = ( )
instanceType	0x4 = ( WRITE )
lastLogoff	(nie)
lastLogon	(nie)
logonCount	0
name	Test1
objectCategory	CN=Person,CN=Schema,CN=Configuration,...
objectClass	top; person; organizationalPerson; user
objectGUID	47b33d5d-018e-488d-9dc6-3011fec8b660
objectSid	S-1-5-21-1114462570-1726162390-2557311
primaryGroupID	513 = ( GROUP_RID_USERS )
pwdLastSet	11.09.2017 12:28:03 Mitteleuropäische Som...
repPropertyMetaData	AttrID Ver Loc.USN Org.DSA
sAMAccountName	Test1

Active Directory-Benutzer und -Computer

Name | Typ

- adm\_jwalter | Benutzer
- CAAdmin | Benutzer
- Test | Benutzer
- Test1 | Benutzer
- Test2 | Benutzer

Eigenschaften von Test2

Attribut	Wert
cn	Test2
codePage	0
countryCode	0
department	Admin
displayName	Test2
distinguishedName	CN=Test2,OU=User Accounts,OU=User,OU...
dScorePropagationD...	11.09.2017 13:03:22 Mitteleuropäische Som...
instanceType	0x4 = ( WRITE )
lastLogoff	(nie)
lastLogon	(nie)
logonCount	0
msDS-SupportedEncr...	0x0 = ( )
name	Test2
objectCategory	CN=Person,CN=Schema,CN=Configuration,...



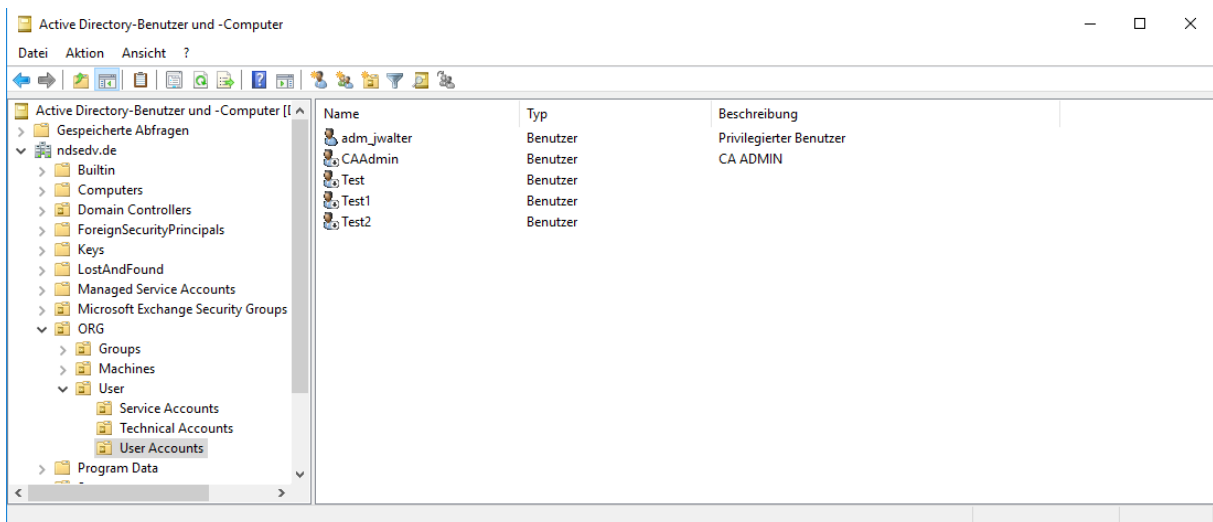
## AD Account 10 Stunden nach letzten Logon deaktivieren

Starte ich nun das Skript, werden alle User bis auf den User adm\_jwalter deaktiviert.

```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Disable Inactive Users.ps1 Disable Inactive User.ps1 X
1 # Jörn Walter 07.10.2017 https://www.der-windows-papst.de
2 clear
3 $time = [DateTime]::Now.Subtract([Timespan]::FromHours(10)).ToFileTime()
4 Search-ADAccount -accountinactive -useronly -SearchBase "OU=User Accounts,OU=ORG,DC=ndsedv,DC=de" | where {$_.lastlogon -lt $time} | Disable-ADAccount -whatif

WhatIf: Ausführen des Vorgangs "Set" für das Ziel "CN=CAAdmin,OU=User Accounts,OU=ORG,DC=ndsedv,DC=de".
WhatIf: Ausführen des Vorgangs "Set" für das Ziel "CN=Test1,OU=User Accounts,OU=ORG,DC=ndsedv,DC=de".
WhatIf: Ausführen des Vorgangs "Set" für das Ziel "CN=Test2,OU=User Accounts,OU=ORG,DC=ndsedv,DC=de".
PS C:\Windows\System32>
```

### Das Ergebnis:



Name	Typ	Beschreibung
adm_jwalter	Benutzer	Privilegierter Benutzer
CAAdmin	Benutzer	CA ADMIN
Test	Benutzer	
Test1	Benutzer	
Test2	Benutzer	



## AD Account 10 Stunden nach letzten Logon deaktivieren

### Final Skript:

```
# Jörn walter 07.10.2017 https://www.der-windows-papst.de
clear
$From = "DisableExternalAccounts@ndsedv.de.de"
$To = "joern.walter@ndsedv.de.de"
$smtpServer = "172.18.32.107"
$reportfile = "C:\Install\inactiveUsers.csv"

write-Host "-----" -ForegroundColor Red
write-Host "Delete old File: $reportfile" -ForegroundColor Red
write-Host "-----" -ForegroundColor Red
if (Test-Path $reportfile) {
    Remove-Item $reportfile -ErrorAction SilentlyContinue
}

write-Host "-----" -ForegroundColor Yellow
write-Host "Current Time -10 Hours" -ForegroundColor Yellow
$HoursInactive = 10
$InactiveDate = (Get-Date).AddHours(-($HoursInactive))
$InactiveDate2 = [DateTime]::Now.Subtract([TimeSpan]::FromHours(10)).ToFileTime()
write-Host "Lockdown Time is: $InactiveDate" -ForegroundColor Yellow
write-Host "Lockdown Time is: $InactiveDate2" -ForegroundColor Yellow
write-Host "-----" -ForegroundColor Yellow

$dc = "dc01","dc02"
Get-ADUser -Server $DC -SearchBase "OU=RemoteSupport,OU=Externe
MA,OU=SITES,OU=\#KONFIGURATION,DC=ndsedv,DC=de" -Filter { LastLogon -lt
$InactiveDate2 -and Enabled -eq $true } -Properties LastLogon | Select-Object @{
Name="SamAccountName"; Expression={$_.SamAccountName} }, LastLogon | Export-Csv
C:\Install\InactiveUsers.csv -NoTypeInfoInformation -append
Get-ADUser -Server $DC -SearchBase "OU=RemoteSupport,OU=Externe
MA,OU=SITES,OU=\#KONFIGURATION,DC=ndsedv,DC=de" -Filter { LastLogon -notlike "*" -
and Enabled -eq $true } -Properties LastLogon | Select-Object @{
Name="SamAccountName"; Expression={$_.SamAccountName} }, LastLogon | Export-Csv
C:\Install\InactiveUsers.csv -NoTypeInfoInformation -append
write-Host "-----" -ForegroundColor White
write-Host "Connect $DC" -ForegroundColor White
write-Host "-----" -ForegroundColor White

#Alternative
#$Users = Search-ADAccount -AccountInactive -TimeSpan "00.10:00:00" -UsersOnly -
SearchBase "OU=RemoteSupport,OU=Externe
MA,OU=SITES,OU=\#KONFIGURATION,DC=ndsedv,DC=de" | where {$_.Enabled -eq "True"} |
Select-Object @{ Name="SamAccountName"; Expression={$_.SamAccountName} } | Export-
Csv C:\Install\InactiveUsers.csv -NoTypeInfoInformation -append
#$Users = Search-ADAccount -AccountExpired -UsersOnly -SearchBase
"OU=RemoteSupport,OU=Externe MA,OU=SITES,OU=\#KONFIGURATION,DC=ndsedv,DC=de" |
where {$_.Enabled -eq "True"} | Select-Object @{ Name="SamAccountName";
Expression={$_.SamAccountName} } | Export-Csv C:\Install\InactiveUsers.csv -
NoTypeInfoInformation -append
#$Users = Search-ADAccount -PasswordNeverExpires -UsersOnly -SearchBase
"OU=RemoteSupport,OU=Externe MA,OU=SITES,OU=\#KONFIGURATION,DC=ndsedv,DC=de" |
where {$_.Enabled -eq "True"} | Select-Object @{ Name="SamAccountName";
Expression={$_.SamAccountName} } | Export-Csv C:\Install\InactiveUsers.csv -
NoTypeInfoInformation -append

write-Host "-----" -ForegroundColor Yellow
write-Host "write file" -ForegroundColor Yellow
write-Host "-----" -ForegroundColor Yellow

If ((Get-Item $ReportFile).length -gt 0kb) {
write-Host "Variable is OK"
}else{
write-Host "-----" -ForegroundColor White
write-Host "No Users found to Disable" -ForegroundColor White
write-Host "-----" -ForegroundColor White
exit
}

write-Host "-----" -ForegroundColor Yellow
write-Host "Disable Accounts" -ForegroundColor Yellow
write-Host "-----" -ForegroundColor Yellow

Import-Csv "C:\Install\InactiveUsers.csv" | ForEach-Object {
    $samAccountName = $_.samAccountName
```



## AD Account 10 Stunden nach letzten Logon deaktivieren

```
Get-ADUser -Identity $samAccountName |
Disable-ADAccount }
$ReportFiles = 'C:\Install\InactiveUsers.csv'

IF (Test-Path $ReportFiles){
  If ((Get-Item $ReportFiles).length -gt 0kb) {
    write-Host "-----" -ForegroundColor green
    write-Host "Send Mail to Admin" -ForegroundColor green
    write-Host "-----" -ForegroundColor green
    Send-MailMessage -SmtpServer $smtpServer -To $To -From $From -Subject "Disable
External Inactive Users" -Body "Daily Report about External Inactive Users - IT-
Operations" -Attachments $reportfiles -Priority High -Encoding "UTF8"
  }
} else {
  write-Host "-----" -ForegroundColor red
  write-Host "No File no E-Mail" -ForegroundColor red
  write-Host "-----" -ForegroundColor red
}
}
```