



Department for Levelling Up,
Housing & Communities

Cyber clinic

Active Directory Toolkit

2022



Agenda

Active Directory Tool

- Pre-requisites
- Download and installation
- Demo
- Staying in touch

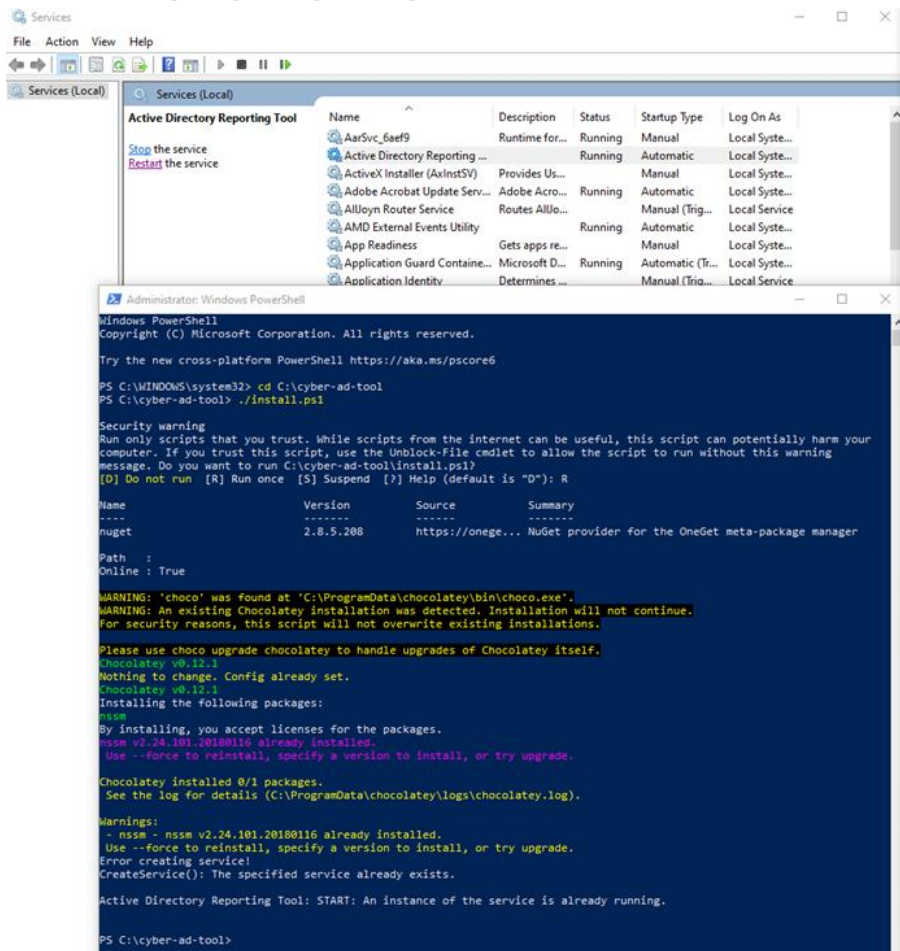
Prerequisites

- Windows device with local admin and connectivity to AD domain controller

Installation

- Download from : <https://github.com/communitiesuk/cyber-ad-tool>
- Extract .zip file contents
- Run install.ps1 as local admin
- Access via browser at <http://localhost:8080>

Installation



The screenshot shows the Windows Services console with the 'Active Directory Reporting Tool' service listed. Below it, an Administrator Windows PowerShell terminal window displays the execution of the installation script.

Services (Local)

Name	Description	Status	Startup Type	Log On As
AarSvc_6ae9	Runtime for...	Running	Manual	Local Syste...
Active Directory Reporting ...		Running	Automatic	Local Syste...
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Adobe Acrobat Update Serv...	Adobe Acro...	Running	Automatic	Local Syste...
Alloyn Router Service	Routes Allo...		Manual (Trig...	Local Service
AMD External Events Utility		Running	Automatic	Local Syste...
App Readiness	Gets apps re...		Manual	Local Syste...
Application Guard Containe...	Microsoft D...	Running	Automatic (Tr...	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\WINDOWS\system32> cd C:\cyber-ad-tool
PS C:\cyber-ad-tool> .\install.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\cyber-ad-tool\install.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R

Name                Version      Source                                Summary
----                -
nuget                2.8.5.208    https://onege... NuGet provider for the OneGet meta-package manager

Path :
Online : True

WARNING: 'choco' was found at 'C:\ProgramData\chocolatey\bin\choco.exe'.
WARNING: An existing Chocolatey installation was detected. Installation will not continue.
For security reasons, this script will not overwrite existing installations.

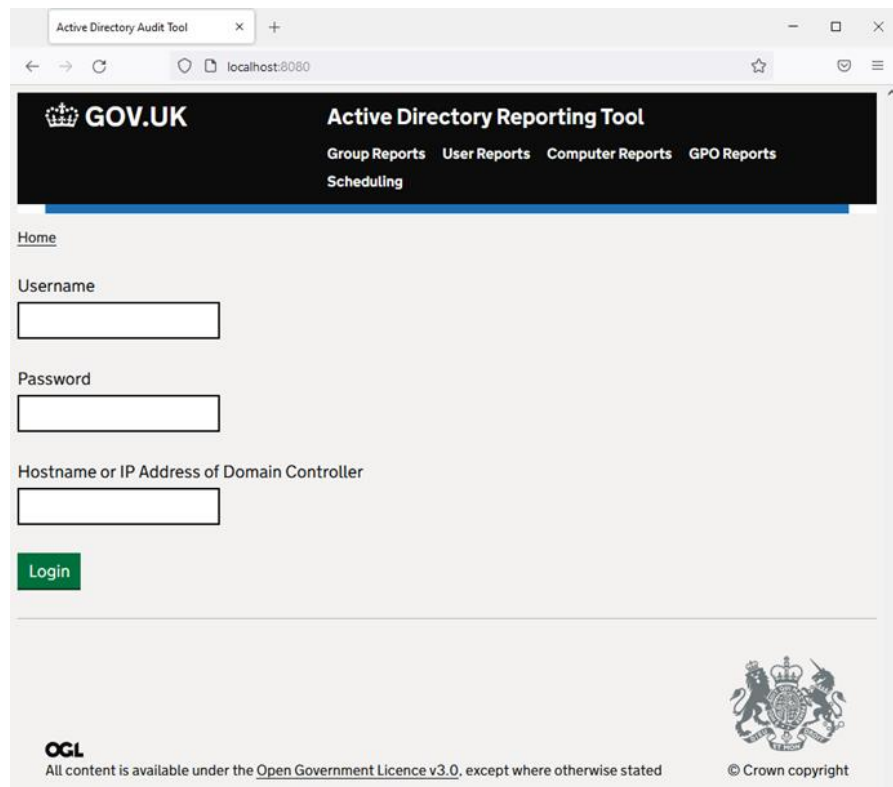
Please use choco upgrade chocolatey to handle upgrades of Chocolatey itself.
chocolatey v0.12.1
Nothing to change. Config already set.
chocolatey v0.12.1
Installing the following packages:
nssm
By installing, you accept licenses for the packages.
nssm v2.24.101.20100116 already installed.
Use --force to reinstall, specify a version to install, or try upgrade.

Chocolatey installed 0/1 packages.
See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).

Warnings:
- nssm - nssm v2.24.101.20100116 already installed.
Use --force to reinstall, specify a version to install, or try upgrade.
Error creating service!
CreateService(): The specified service already exists.

Active Directory Reporting Tool: START: An instance of the service is already running.

PS C:\cyber-ad-tool>
```



The screenshot shows the web interface of the Active Directory Reporting Tool. The header includes the GOV.UK logo and navigation links for Group Reports, User Reports, Computer Reports, GPO Reports, and Scheduling. The main content area has a 'Home' link and input fields for Username, Password, and Hostname or IP Address of Domain Controller, followed by a 'Login' button.

Active Directory Reporting Tool

Group Reports User Reports Computer Reports GPO Reports Scheduling

Home

Username

Password

Hostname or IP Address of Domain Controller

Login

OGL
All content is available under the [Open Government Licence v3.0](#), except where otherwise stated

© Crown copyright

Available reports

All Users

Users Never Logged On

Users Not Logged On for nn days

Locked Out Users

Disabled Users

Recently Created Users

Account Expired Users

Soon-to-expire User Accounts

Members of Domain Local Administrators Group

Members of Domain Admins Group

Users in more than one group

Recently deleted users

Recently modified users

Users with logon script

Users without logon script

Account never expires users

Recently logged on users

Dial in allowed users

All Computers

Recently Created Computers

Computers Not Recently Logged On

Domain Local Groups

Global Groups

All GPOs

Recently Created GPOs

User reports



Active Directory Reporting Tool

[Group Reports](#) [User Reports](#) [Computer Reports](#) [Group Policy Reports](#)

[Home](#) > [User Reports](#)

Select a Report

Users Not Logged On for nn days

Days to filter on

30

Run Report

Users Not Recently Logged On

Name

Last Logon

▼ Guest

Distinguished Name: CN=Guest,CN=Users,DC=mhclg,DC=gov,DC=uk

Object Guid: c2df73ec-031d-44d6-b55b-696e1fcfaa85

BadLogonCount: 0

Created: Sat Jan 16 2021 20:46:12 GMT+0000 (Greenwich Mean Time)

Deleted: null

Enabled: false

LockedOut: false

PasswordLastSet:

PasswordExpired: false

PasswordNeverExpires: true



Computer reports



Active Directory Reporting Tool

[Group Reports](#) [User Reports](#) [Computer Reports](#) [Group Policy Reports](#)

[Home](#) > [Computer Reports](#)

Select a Report

Computers Not Logged Onto for nn days

Select an OU

mhclg

Days to filter on

1

Run Report

Computers Not Recently Logged On

Name	IP address	OU	Operating System
eventcollector.mhclg.gov.uk	10.85.192.40	CN=EVENTCOLLECTOR;OU=mhclg;DC=mhclg;DC=gov;DC=uk	Windows Server 2019 Datacenter , 10.0 (17763)
client01.mhclg.gov.uk	10.85.192.51	CN=CLIENT01;OU=mhclg;DC=mhclg;DC=gov;DC=uk	Windows Server 2019 Datacenter , 10.0 (17763)

Total Count = 2

Export to CSV





Department for Levelling Up,
Housing & Communities

Demo

Active Directory Toolkit

Staying in touch - cyber support sessions

Cyber treatment plan & implementation support session available to book using this link: <https://calendly.com/andrea-baron/ad-hoc-call-with-council> .

These are longer 1:1 sessions between DLUHC cyber team and a council, available for any support, guidance or hands on help for the implementation of your cyber treatment plan.

Cyber support drop in sessions every Wednesday for 30 minute session between 2pm - 4pm. These regular 1:1 sessions are available for you to book anytime using the Calendly link: <https://calendly.com/andrea-baron/drop-in-support-session> .

Cyber clinics are occurring on the 3rd Thursday of the month between 11.30am - 12.30pm where a targeted cyber focus area will be presented, tool sets demonstrated and will be open to questions. Support, guidance and hands-on help is available to assist you in adoption and implementation.

Staying in touch

Follow our progress

- Read our fortnightly sprint notes on [Medium](#)
- Follow LDCU on Twitter ([@LDgovUK](#))
- Subscribe to our [Cyber newsletter](#) for progress updates and news relevant to those working in and around local government cyber security
- We'll also be sharing regular updates on the DLUHC Blog <https://dluhcdigital.blog.gov.uk/>

Have your say

We welcome further collaboration and input, so if you would like to share with us any strong evidence to support our research please email cybersupport@localdigital.gov.uk.



Department for Levelling Up,
Housing & Communities

Thank you

[We welcome feedback on our cyber support service](#)

 @LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

