

# Who *really* needs admin rights?

## CSC 4: Controlled Use of Administrative Privileges

### Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.


Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.
Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.
Use Multi-Factor Authentication for All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.
Use Dedicated Workstations For All	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.
<b>Limit Access to Script Tools</b>	<b>Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.</b>
Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

<http://www.cisecurity.org/controls/>

# Limit access to Script Tools

## CSC 4: Controlled Use of Administrative Privileges

Binary	Functions	Type
<a href="#">Atbroker.exe</a>	Execute	Binaries
<a href="#">Bash.exe</a>	Execute AWL bypass	Binaries
<a href="#">Bitsadmin.exe</a>	Alternate data streams Download Copy Execute	Binaries
<a href="#">Certutil.exe</a>	Download Alternate data streams Encode Decode	Binaries
<a href="#">Cmd.exe</a>	Alternate data streams	Binaries
<a href="#">Cmdkey.exe</a>	Credentials	Binaries
<a href="#">Cmstp.exe</a>	Execute AWL bypass	Binaries
<a href="#">Control.exe</a>	Alternate data streams	Binaries
<a href="#">Csc.exe</a>	Compile	Binaries
<a href="#">Cscript.exe</a>	Alternate data streams	Binaries
<a href="#">Dfsvc.exe</a>	AWL bypass	Binaries
<a href="#">Diskshadow.exe</a>	Dump Execute	Binaries
<a href="#">Dnscmd.exe</a>	Execute	Binaries



Credit to LOLBAS Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts)