SC-Wiki

`see last modified date at base of all pages`

Ninja Native Scripts

BowBlack Ninja offers a number of native scripts out-of-the-box in the Script Library that may be run on devices ad-hoc (either from the Search tab or from the play button icon on a device), via Scheduled Scripts, or via Scheduled Tasks.

Native Scripts

Clear DNS Cache 🪟
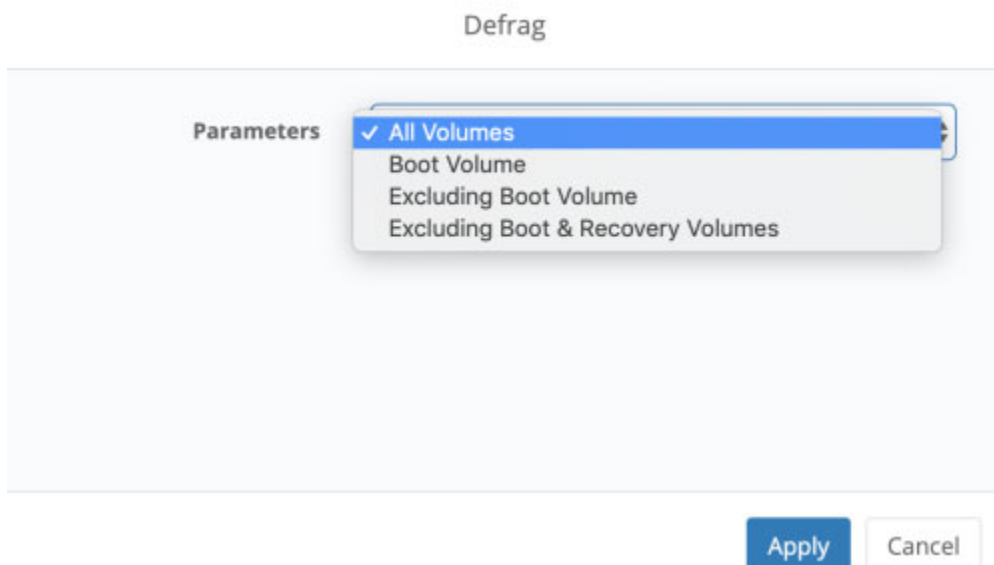This script runs the following command:

```
IPCONFIG /FLUSHDNS
```

Clear Event Logs File 🪟

This clears out all backup and security event logs for all users.

Defrag File 🪟
This runs hard drive defragmentation on the endpoints. You have the option to exclude the boot volume and/or the recovery volume.

Delete Temporary Files 🪟

This script deletes temporary file in the following locations (as long as not locked):

```
%WINDIR%\Temp
[PROFILES_DIRECTORY (c:\users\, c:\documents and settings, etc..]\
[USERNAMEFOLDER]\AppData\Local\Temp
[PROFILES_DIRECTORY (c:\users\, c:\documents and settings, etc..]\
[USERNAMEFOLDER]\Local Settings\Temp
```

Disable/Enable ARD (Apple Remote Desktop) 🍎

This script disables/enables ARD (Apple Remote Desktop) through use of the kickstart command-line utility.

Disable/Enable CD-ROM Drives 🪟

This toggles a registry key to disable/enable the respective drives.
Important Note : Depending on the OS, some machines may require a reboot to ensure this change is enforced.

Disable/Enable Firewall 🍎 🐧

This script disables/enables the firewall. There are options for both Mac and Linux.
For MacOS:
Firewall is disabled by running the following script:

```
#!/bin/bash\n sudo defaults write /Library/Preferences/com.apple.alf globalstate -int 0; exit 0
```

Firewall is enabled by running the following script:

```
#!/bin/bash\n sudo defaults write /Library/Preferences/com.apple.alf globalstate -int 1; exit 0"
```

Disable/Enable Floppy Drives 🪟

This toggles a registry key to disable/enable the respective drives.

Disable Mac Sleep 🍎

This script sets Mac system to never sleep.

Disable/Enable Sleep 🐧

This script sets the Linux system to never sleep, or enables the system to sleep.

Disable/Enable SSH (Secure Shell) 🍎 🐧

This script disables/enables SSH. For Mac, this is done through use of the systemsetup command-line utility.

Disable/Enable USB Drives 🪟

This script disables/enables the use of USB storage devices through a registry setting.

Disable/Enable User Access Control 🪟

This toggles the following registry key with a value of "1" (enable) or "0" (disable):

```
SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System
```

Disable/Enable VNC (Virtual Network Connection) 🍎

This script disables/enables VNC through use of the kickstart command-line utility.

Download updates, don't install

This script triggers the macOS update mechanism locally on the machine to download any available updates (but not install them yet).

Empty Recycle Bin

This allows you to run "empty recycle bin" on all drives/all users on the corresponding endpoints for Windows 7 and above. This script does not refresh the folder, so the icon may still show "full" until recycle bin is refreshed.

Empty Trash

This script empties the trash for each user on the device.

Enable Wake-on-LAN

This enables Wake-on-LAN capabilities through use of the systemsetup command-line utility.

Fix File System Errors

This script runs the following command:

```
CHKDSK /R
```

Important Note: Once this option is selected, you will need to schedule a reboot for this action to finish running.

Fix rebuild performance counters

This runs a script to clear and rebuild performance counters.

Flush DNS

This script clears the DNS cache using different command-line utilities dependent on OS version.

Force logout

This script forces logout for the currently-logged-in user.

Forced Reboot

This script utilizes WINAPI to run the'InitiateSystemShutdown' command with the forced parameter, and executes after 5 seconds.

Group policy force update

This runs the following command:

```
gpupdate /force
```

Install all available patches

This script triggers the update mechanism locally on the machine to download and install all available patches.

Install all available patches, restart if required

This script triggers the update mechanism locally on the machine to download and install all available patches. It then reboots the machine if a reboot is required following the install.

Important Note: For Mac devices, this script is only compatible with devices running macOS High Sierra and above.

Install Application 🪟 🍎

This script may be used to install an .EXE or .MSI on Windows devices, or a .PKG or .DMG on Mac devices. In order for the script to be successful, the installation must run silently.

1. In the 'Architecture' section, you can select the operating system type on the endpoints. You may specify either All, x86, or x64.

Important Note: If you select x86, it will skip all x64 machines in that policy.

- There are two ways you can provide the installer to Ninja. You can either upload it to the Amazon S3 server, or you can provide the path to the MSI or EXE by using a HTTPS URL.

Important Note: If you choose to upload the installer to the Amazon S3 server:

- There is a file size limit of 1GB.
- The MSI URL field will disappear.
- For security purposes, Ninja alters the name of the .msi or .exe when the file is uploaded to us. If an installer pulls information from that name, such as account or activation codes, it may be better to use an independent upload or a

custom script.

- Please specify the Application name. This is the name that will be displayed in the Activity Feed whenever the script is launched/deployed.
- List of any optional parameters that you want to run as a part of the installation process. If the installer requires a specific silent parameter, this where it should be added. For more information about parameters, please see: Script Library: Parameters.

1. **Important Note**: MSI installers are automatically run with the following parameters:
2. /quiet /qn /norestart /log {path to our script folder}ninjascript-output-{current-time}.txt
3. **Examples of common EXE silent parameters**: /silent /Silent /S /s -silent –silent
4. **Examples of common MSI silent parameters**: /quiet /qn /q

Lastly, you have an option to run the installation either under system, the current user, or utilizing the preferred Windows local or domain admin credentials from your credential store.

1. **Important Note**: Some software may require the install be deployed with specific credentials - for example, some antivirus software may prefer running as an Admin over the System user.

Install only recommended patches

This script triggers the macOS update mechanism locally on the machine to download and install only the recommended (as classified by Apple) patches.

Install only recommended patches, restart if required (requires 10.13.4 or newer)

This script triggers the macOS update mechanism locally on the machine to download and install only the recommended (as classified by Apple) patches, and then reboots the machine if a reboot is required following the install.

Important Note: This script is only compatible with devices running macOS High Sierra and above.

Install only security patches

This script triggers the update mechanism locally on the machine to download and install only the security (as classified by Linux) patches.

Install only security patches, restart if required

This script triggers the update mechanism locally on the machine to download and install only the security (as classified by Linux) patches, and then reboots the machine if a reboot is required following the install.

Kill Core Audio

This script resets the audio services daemons.

List all available patches

This script queries the update mechanism locally on the machine to provide a list of all available patches. The list will then be visible in the Activity Feed.
Important Note: If no available patches are found upon running this script, the 'Action: Completed' entry in the Activity Feed will simply state 'Finding available software' (with no actual patches listed).

List only security patches

This script queries the update mechanism locally on the machine to provide a list of available security patches. The list will then be visible in the Activity Feed.

Important Note: If no available security patches are found upon running this script, the 'Action: Completed' entry in the Activity Feed will simply state 'Finding available software' (with no actual patches listed).

Log Off Current User 🪟

This script allows you to log out all logged-in users from an endpoint.

Purge Disk Cache 🍎

This script clears the disk cache using the purge command-line utility.

Reapply user permissions 🍎

This script runs chown and chmod commands for all users.

Reboot 🪟 🍎 🐧

This script will reboot a device.

Important Notes:

1. For Windows devices, this script utilizes WINAPI to run the'InitiateSystemShutdown' command without the forced parameter, and executes after 30 seconds.
2. For Mac devices, this script uses the shutdown command line utility to force a reboot on a Mac device.

Reboot (pending reboot devices) 🪟

This script utilizes WINAPI to run the'InitiateSystemShutdown' command, and will only run on devices that have a pending reboot at the time when the script is run.

Release & Renew IP Address 🪟

This runs the following commands:

```
IPCONFIG /RELEASE and IPCONFIG /RENEW
```

Removable Media 🪟

This script allows you to disable/enable the use of USB, CD-ROM, and Floppy drives through a registry setting.

Removable Media

State   ✓ Disable
         Enable

Apply   Cancel

Remove Google/Yahoo toolbar 🪟

For these scripts, Ninja reads the uninstall key and then runs the uninstall string.

Repair Disk Perms 🍎

This script runs repair disk permissions on "/".

Repair SSH 🍎

This kills SSH connections and reinitializes the SSH daemon.

Repair TeamViewer 🍎

This script reinitializes TeamViewer, kills the service, and restarts it

Reset Launcher Services 🍎

This script resets launch services. For more information, please see this site.

Reset Printing 🍎

This script does the following:

- restarts/resets cupsd
- resets printer plists

Run Application 🪟

This script allows you to run an existing software on an endpoint.

Example: If you run CCleaner on endpoints, you can evoke that using Ninja.

1. In the 'Architecture' section, you can select the operating system type on the endpoints. You may specify either All, x86, or x64.

- **Important Note**: If you select x86, it will skip all x64 machines in that policy.

1. Provide the path to the .EXE (like "C:\program files\CCleaner\Ccleaner.exe").
2. Please specify the Application name, and also any optional parameters that you want to run alongside the application. For more information about parameters, please see: Script Library: Parameters
3. Lastly, you have an option to run the installation either under system (mostly used for applications that don't have a UI element to them), the current user, or utilizing credentials from your credential store.

Run Windows Cleanup 🪟

This runs the Windows Disk cleanup tool with the option **/SAGERUN:1**
The full command is:

```
(CLEANMGR /SAGERUN:1)
```

SFC Scannow 🪟

This script triggers an SFC Scan as the currently logged-in user. This requires Vista or greater OS, and a user with admin permissions must be logged in to the device.

System Restore 🪟

This script toggles the registry key to 0 or 1 to enable/disable the ability to perform a system restore.

The registry key that is responsible for system restore is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore
```
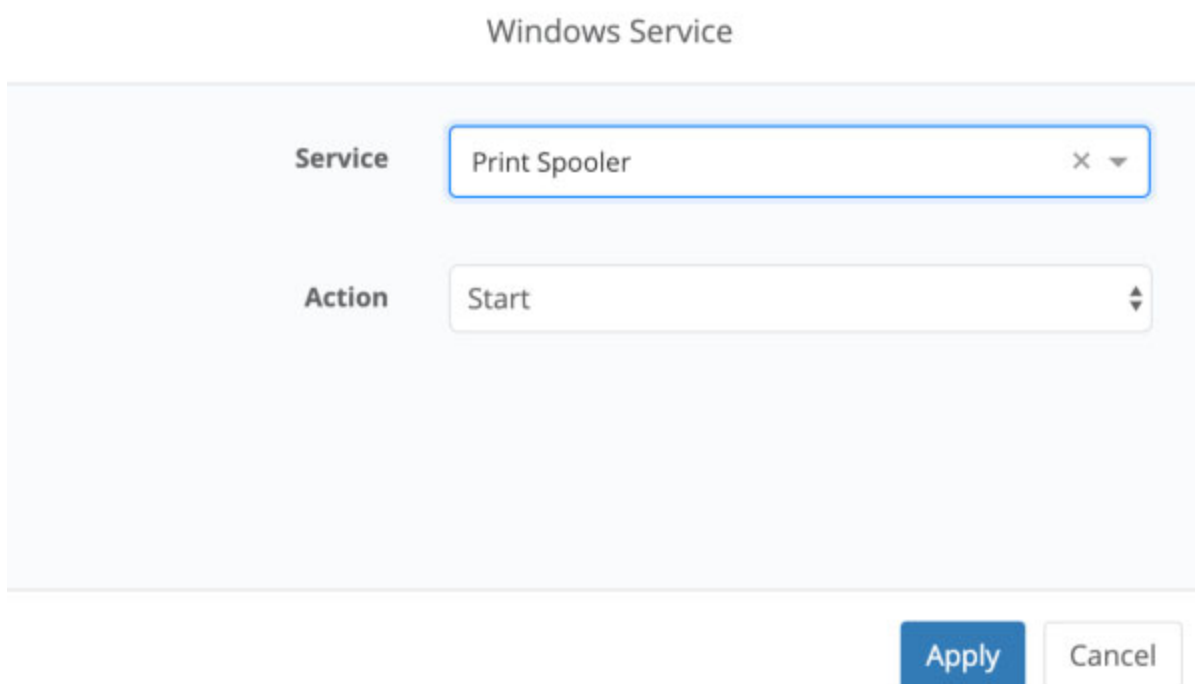
Turn Automatic Updates Off

This script sets the AutoUpdateRestartRequired setting in Preferences to "FALSE".

Wake Display Up

This script wakes the display through the use of the pmset command-line utility.

Windows Service

This allows you to start/stop a Windows Service.

The list of services that show up in the dropdown menu is created by cumulating all the service from all devices within your Ninja environment - so it's a superset of all the services for the devices in your environment.

PageName

Here we will explain …

Note: Simple & Logical.

```
Think Big to small
```

bowblack_ninja_remote_monitoring_and_management_ninja.txt · Last modified: 2022/10/21 11:58 by thesaint