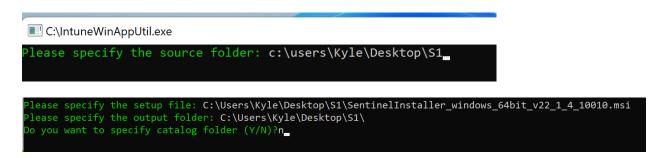
Step 1. Download the MSI of your choice from your Sentinel One Console (S1).



Step 2. Make sure you have download the win32 app wrapper from Microsoft. https://github.com/Microsoft/Microsoft-Win32-Content-Prep-Tool

Step 3. Wrap the msi you downloaded in step 1 with the tool you download in step 2.



Step 4. Take the .intunewin and upload to Intune.



App information Edit	
Name	Sentinel Agent
Description	Sentinel Agent
Publisher	Sentinel Agent
App Version	22.1.10010
Category	
Show this as a featured app in the Company Portal	Yes
Information URL	
Privacy URL	
Developer	**
Owner	**
Notes	**
Logo	
Program Edit Install command	msiexec /i "SentinelInstaller windows 64bit v22 1 4 10010.msi" /quiet
instali commanu	SITE_TOKEN=e 0=
Uninstall command	msiexec /x "(A699AEE8-B4E7-4474-A217-FDC1CC1C6784)" /qn
Install behavior	System
Device restart behavior	App install may force a device restart
Return codes	0 Success 1707 Success 3010 Soft reboot 1641 Hard reboot 1618 Retry
Requirements Edit	
Operating system architecture	x64
Minimum operating system	Windows 10 1607
Disk space required (MB)	**
Physical memory required (MB)	**
Minimum number of logical processors required	
Minimum CPU speed required (MHz)	
Additional requirement rules	**
Detection rules Edit	
Rules format	Use a custom detection script
Run script as 32-bit process on 64-bit	No

Enforce script signature check and run No script silently **Step 5.** Match these settings in Intune change the sitetoken to your own from the S1 console.

Step 6. Use this code to create a powershell script for a custom detection rule. Save it as *check_s1.ps1*

```
$A = 0
do {
    try {
        $Services = Get-Service -name
SentinelAgent
    }
    catch {
        $Services = $null
    }
    start-sleep -Seconds 30
    $A = $A + 30
} until (($null -ne $Services) -or ($A -ge 300))
if ($null -ne $Services) { Write-Host "Installed" }
else { exit }
```

Step 7. Done test your deployment.