**ASSIGNMENT:** Mention all windows tools for debugging with screenshots and steps to create for Microsoft Intune Portal

**BATCH ID:** DWS_B5_25VID2550

**NAME:** Sameer Moahanlal Katre

**RPS USER ID:** 34930

**MAIL ID:** katresameer27@gmail.com

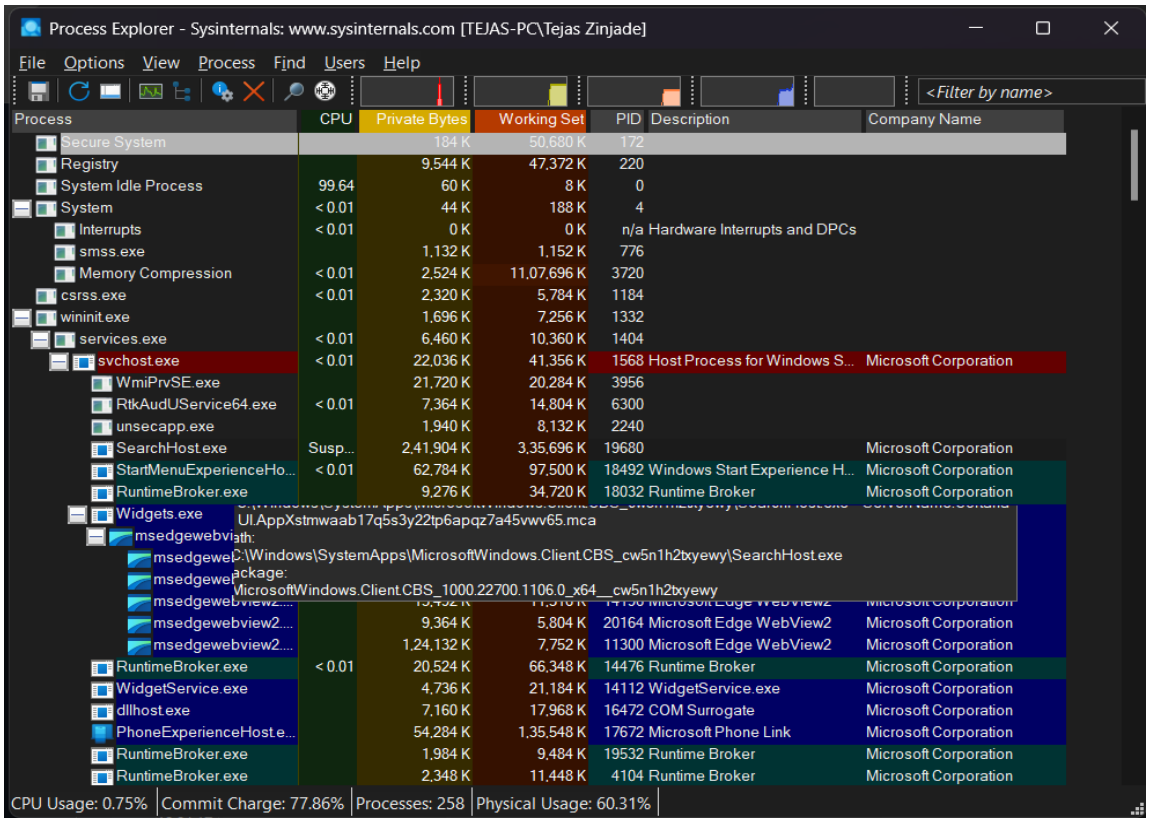
# WINDOWS TOOLS FOR DEBUGGING


## 1.Autologon

Autologon is a specialized utility developed by Sysinternals to simplify the automatic logon process on Windows systems. Instead of requiring a user to enter credentials each time a system boots, Autologon securely stores and manages the username and password needed for Windows authentication. The tool is particularly valuable for systems that must operate with minimal user intervention, such as kiosks, headless servers, or testing environments. Using its graphical interface, administrators can configure the specific user account that should be logged in automatically, ensuring that only authorized credentials are set up.

Autologon achieves this by securely editing the necessary registry keys in Windows, storing the credentials in a way that's resistant to casual snooping but still easily updateable through the tool itself. This means that IT staff can both automate and audit the use of autologon functions. Common uses include automatically logging in users for demonstration purposes, managing unattended machines, or setting up environments where certain applications must launch immediately after the system starts. However, while Autologon makes the process seamless, it's important to balance convenience with security, ensuring that the feature is only enabled in scenarios where physical or network access is already restricted and the risks are understood.

## 2. Process Explorer



Process Explorer is one of the most popular and powerful tools in the Sysinternals suite, offering a level of insight into running processes and system resources unavailable in the default Windows Task Manager. The interface provides a real-time, hierarchical view of all processes running on a system, allowing users to see parent-child relationships, detailed executable paths, and loaded modules (DLLs). For each process, Process Explorer displays extensive properties, including memory usage, CPU consumption, digital signature verification, open file handles, and network activity.

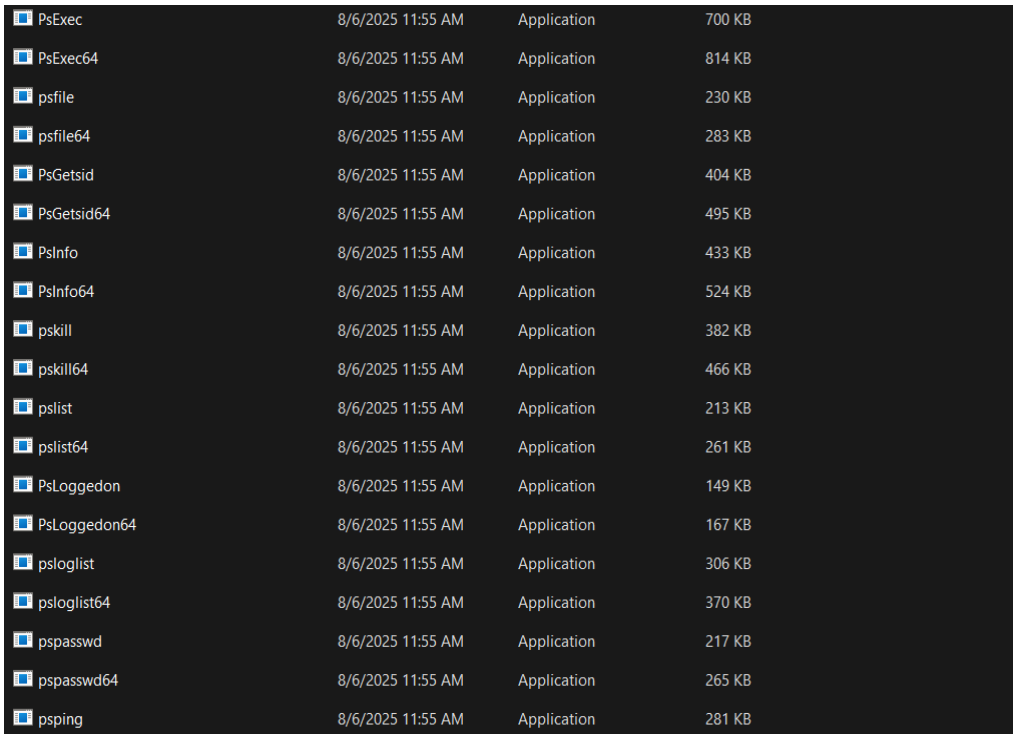
This detail is invaluable for IT professionals, developers, and security analysts alike. For example, when troubleshooting system slowdowns, Process Explorer enables users to quickly identify resource hogs or processes with memory leaks. Security experts frequently use it to spot suspicious processes, investigate malware, and discover unauthorized activity by inspecting process origins and system behavior. The tool also allows for advanced operations such as suspending, killing, or restarting processes and searching for open file handles, which is especially useful when trying to determine what is locking a particular file or resource. As a replacement for Task Manager, Process Explorer is regarded as indispensable for anyone who needs a deeper understanding of what's running on their computer.

## 3 .PsExec

PsExec is a command-line tool developed by Sysinternals that allows administrators to execute programs and commands remotely on Windows machines, as if they were running them locally. PsExec is lightweight and requires minimal setup, making it a preferred option for IT professionals who need to manage multiple systems from a central location. By simply specifying the target machine and the command to run, PsExec establishes a connection and relays the instructions securely.

With PsExec, functions like deploying scripts, installing updates, running diagnostics, and collecting system information become streamlined. The tool supports not only command execution but also the launching of full applications with interactive user interfaces, making remote troubleshooting possible. It also allows running commands with elevated privileges, useful for administrative tasks that require higher permissions. Security-wise, it respects account permissions, but users should exercise caution and only use it on trusted networks, as it can be leveraged for lateral movement by attackers if improperly secured. Overall, PsExec offers a powerful and flexible way to remotely control Windows systems, greatly reducing the need for physical or remote desktop access and significantly enhancing efficiency in large-scale IT operations.

# 4.PSTools



| | | | |
|---|---|---|---|
| PsExec | 8/6/2025 11:55 AM | Application | 700 KB |
| PsExec64 | 8/6/2025 11:55 AM | Application | 814 KB |
| psfile | 8/6/2025 11:55 AM | Application | 230 KB |
| psfile64 | 8/6/2025 11:55 AM | Application | 283 KB |
| PsGetsid | 8/6/2025 11:55 AM | Application | 404 KB |
| PsGetsid64 | 8/6/2025 11:55 AM | Application | 495 KB |
| PsInfo | 8/6/2025 11:55 AM | Application | 433 KB |
| PsInfo64 | 8/6/2025 11:55 AM | Application | 524 KB |
| pskill | 8/6/2025 11:55 AM | Application | 382 KB |
| pskill64 | 8/6/2025 11:55 AM | Application | 466 KB |
| pslist | 8/6/2025 11:55 AM | Application | 213 KB |
| pslist64 | 8/6/2025 11:55 AM | Application | 261 KB |
| PsLoggedon | 8/6/2025 11:55 AM | Application | 149 KB |
| PsLoggedon64 | 8/6/2025 11:55 AM | Application | 167 KB |
| psloglist | 8/6/2025 11:55 AM | Application | 306 KB |
| psloglist64 | 8/6/2025 11:55 AM | Application | 370 KB |
| pspasswd | 8/6/2025 11:55 AM | Application | 217 KB |
| pspasswd64 | 8/6/2025 11:55 AM | Application | 265 KB |
| psping | 8/6/2025 11:55 AM | Application | 281 KB |

PSTools is not just a single tool but a comprehensive suite of command-line utilities created by Sysinternals to help IT administrators perform a wide range of management tasks on both local and remote Windows systems. Among its most well-known members are PsList (for process listing), PsKill (for process termination), PsLoggedOn (to check who is logged onto a system), PsService (to control Windows services), and PsFile (to see which files are open remotely), among others. This toolkit streamlines many routine and advanced administrative chores, often replacing or augmenting Windows' built-in tools.

The beauty of PSTools lies in its consistency and flexibility. All tools are designed to be script-friendly, enabling their use in batch scripts and automated workflows. For example, system administrators can deploy patches, monitor uptime, gather status reports, and manage user sessions across hundreds of computers

from a single command console. The only requirement is suitable permissions and, in some cases, administrative shares must be enabled. This makes PSTools invaluable for managing enterprise networks, ensuring system consistency, and responding to incidents or emergencies quickly. For IT teams, PSTools reduces repetitive manual labor and helps maintain a stable, secure, and well-monitored infrastructure.

## 5. RegMon

RegMon, short for Registry Monitor, is a classic yet influential tool from Sysinternals designed to monitor real-time access to the Windows registry. The Windows registry is a vital database where settings and options for both the operating system and installed applications are stored, and observing its changes can be crucial for troubleshooting and security analysis. RegMon displays live streams of read, write, and delete operations occurring in the registry, identifying the processes responsible and the registry keys being accessed or modified.

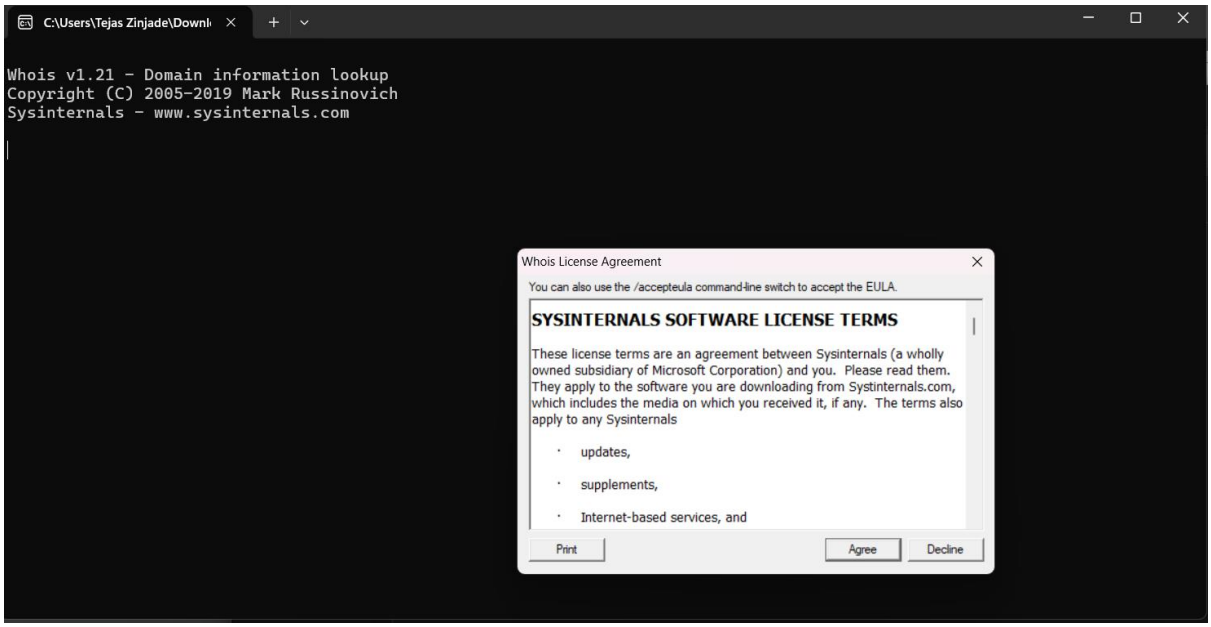
This information is essential when diagnosing application errors, tracking down the source of unexpected behavior, or analyzing the operations of potentially malicious software. Developers also benefit from RegMon by understanding how their software interacts with the system registry and identifying potential conflicts or bottlenecks. While integrated into newer tools like Process Monitor, RegMon remains iconic for visualizing registry activity in a user-friendly interface. It is a powerful aid in environments where system policies, user settings, or security controls are heavily reliant on registry values. Using RegMon, administrators gain a transparent and granular perspective on a critical area of Windows systems that is usually opaque, leading to faster resolutions and more secure configurations.

## 6. Sysmon

Sysmon (System Monitor) is an advanced system service and driver from the Sysinternals suite, engineered for continuous system monitoring and robust security analysis. Once installed, Sysmon logs detailed information about a wide variety of important system events, including process creations, network connections, file creation timestamps, and changes to the file system. The data collected is highly granular and structured to support forensic investigations, intrusion detection systems, and incident response workflows.

What distinguishes Sysmon is its ability to capture intricate details, such as command-line arguments for process executions, parent process relationships, and even hash values of executed files. This level of visibility is essential for early detection of abnormal or malicious activity, such as unauthorized lateral movement or the execution of suspicious binaries. Security teams often use Sysmon in conjunction with SIEM (Security Information and Event Management) systems to analyze behaviors and correlate events across an organization’s network. Sysmon's configuration is customizable, letting administrators choose which types of activity to monitor and log, reducing unnecessary noise. In summary, Sysmon transforms Windows systems into highly observable environments and is a foundational tool for anyone serious about securing and monitoring modern Windows infrastructures.

# 7. Whois




Whois is a widely used command-line tool, not exclusive to Sysinternals but often included with administrative toolkits, that provides essential information about internet domain names and IP addresses. By querying public Whois databases, the tool retrieves ownership details, registration status, contact information, and other metadata about a given domain or IP. This process is invaluable in network administration, cybersecurity, and IT support.

For network troubleshooting, Whois helps identify the party responsible for a problematic or unknown domain or IP address, allowing administrators to trace the origin of suspicious traffic or spam. It is also commonly used to verify domain availability during website launches or when purchasing new addresses. In security investigations, Whois data can reveal the registrant of a domain involved in phishing, helping teams connect the dots

and report abuse. While simple to use – just type the domain or IP as a parameter – Whois puts crucial intelligence at your fingertips and supports rapid response to network incidents. Its inclusion in toolsets alongside Sysinternals applications makes it a valuable companion for any IT professional seeking comprehensive visibility and control.

## ❖ STEPS TO CREATE FOR MICROSOFT INTUNE PORTAL

### Step 1: Prerequisites

Before you begin:

- You must have a Microsoft 365 account with Intune license (like Microsoft 365 E3/E5, Enterprise Mobility + Security E3/E5).
- You must be a Global Admin or Intune Admin.
- Have access to Azure AD and admin.microsoft.com.

### Step 2: Sign in to Microsoft Intune Portal

Go to:

https://endpoint.microsoft.com

This is the Microsoft Intune (Endpoint Manager) Admin Center.

### Step 3: Configure Basic Intune Setup

3.1 - Verify MDM Authority

- Go to: Tenant administration > Intune enrollment
- Ensure MDM Authority is set to *Microsoft Intune*
- If not set, click Set MDM Authority

---

## Step 4: Add Users & Groups

- Go to Users > All Users – Add or sync users from Azure AD / On-premises AD.
- Go to Groups > New Group to create security or M365 groups for targeting policies/apps.

---

## Step 5: Enroll Devices into Intune

5.1 - Windows Enrollment

- Go to: Devices > Windows > Windows enrollment
- Configure Automatic Enrollment for Azure AD-joined or Hybrid-joined devices.

5.2 - Android/iOS Enrollment

- Go to: Devices > Android/iOS > Enrollment
- Configure Android Enterprise, Apple MDM Push Certificate, Company Portal apps, etc.

## Step 6: Create Device Compliance Policies

- Go to: Devices > Compliance policies > Create policy
- Select Platform (Windows/iOS/Android)
- Define rules (like password policy, encryption, OS version)

## Step 7: Create Configuration Profiles

- Go to: Devices > Configuration profiles > Create profile
- Platform: Windows 10 and later
- Profile Type: e.g., Templates > Device Restrictions
- Configure settings like Wi-Fi, BitLocker, Defender, etc.

## Step 8: Deploy Applications

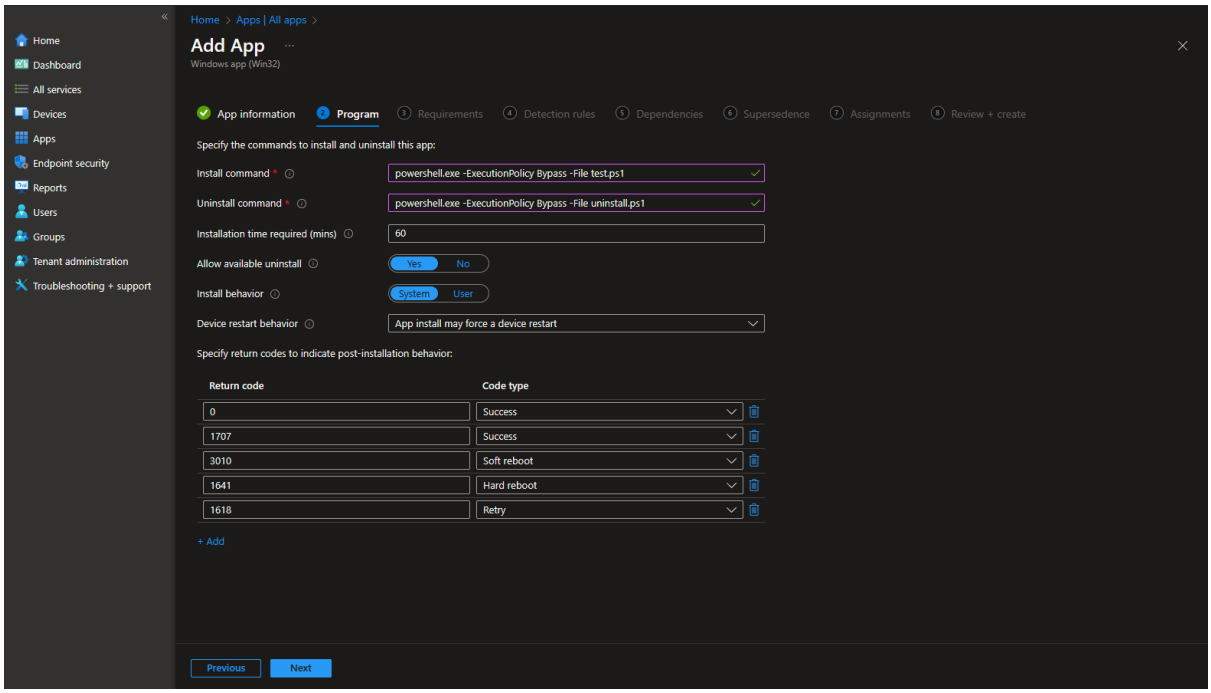
- Go to: Apps > Windows > Add
- Select app type:
    - .msi, .exe, .intunewin, Store app, etc.
- Configure deployment type (Required/Available) and assign to groups

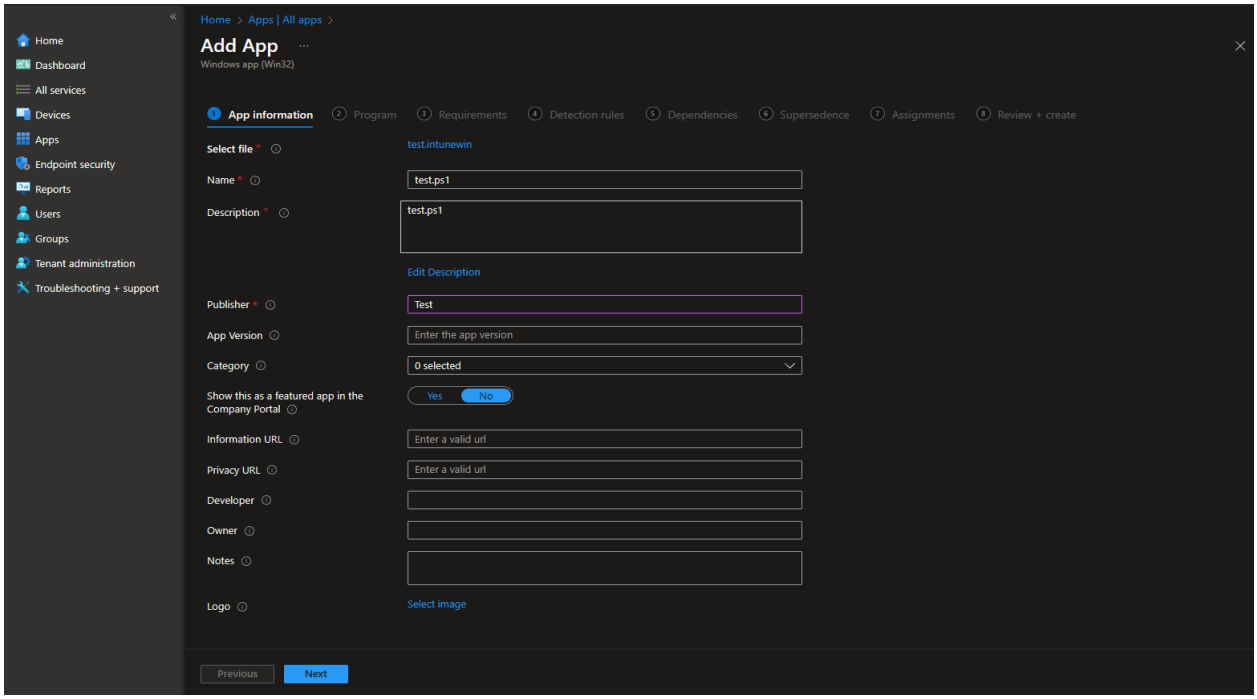
## Step 9: Create Scripts or PowerShell for Customization

- Go to: Devices > Scripts > Add
- Upload PowerShell scripts for automation (like registry edits, cleanup, installs)

## Step 10: Monitor & Report

- Go to: Reports, Endpoint analytics, or Devices > Monitor
- Check compliance status, deployment success/failure, app install status, etc.


Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Apps | All apps >
Add App
Windows app (Win32)
App information
Program
Requirements
Detection rules
Dependencies
Supersedence
Assignments
Review + create
Specify the commands to install and uninstall this app:
Install command *
powershell.exe -ExecutionPolicy Bypass -File test.ps1
Uninstall command *
powershell.exe -ExecutionPolicy Bypass -File uninstall.ps1
Installation time required (mins)
60
Allow available uninstall
Yes
No
Install behavior
System
User
Device restart behavior
App install may force a device restart
Specify return codes to indicate post-installation behavior:
Return code
Code type
0
Success
1707
Success
3010
Soft reboot
1641
Hard reboot
1618
Retry
+ Add
Previous
Next


Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Apps | All apps >
Add App
Windows app (Win32)
App information
Program
Requirements
Detection rules
Dependencies
Supersedence
Assignments
Review + create
Select file *
test.intunewin
Name *
test.ps1
Description *
test.ps1
Edit Description
Publisher *
Test
App Version
Enter the app version
Category
0 selected
Show this as a featured app in the Company Portal
Yes
No
Information URL
Enter a valid url
Privacy URL
Enter a valid url
Developer
Owner
Notes
Logo
Select image
Previous
Next