NAME : B S SUDHEENDRA

EMAIL ID : bssudheendra2006@gmail.com

TOPIC : Mention all windows tools for debugging with screenshots.

Introduction

In Windows environments, troubleshooting application issues, installations, and security events often requires specialized utilities. The Sysinternals suite and other Windows tools provide deep insights into processes, registry activity, network connections, and system behavior.

This assignment explains key tools including

- LogonSessions,
- Autologon,
- ProcessExplorer,
- ProcessMonitoring,
- PsExec,
- PsTools,
- Whois,
- Sysmon.

LogonSessions

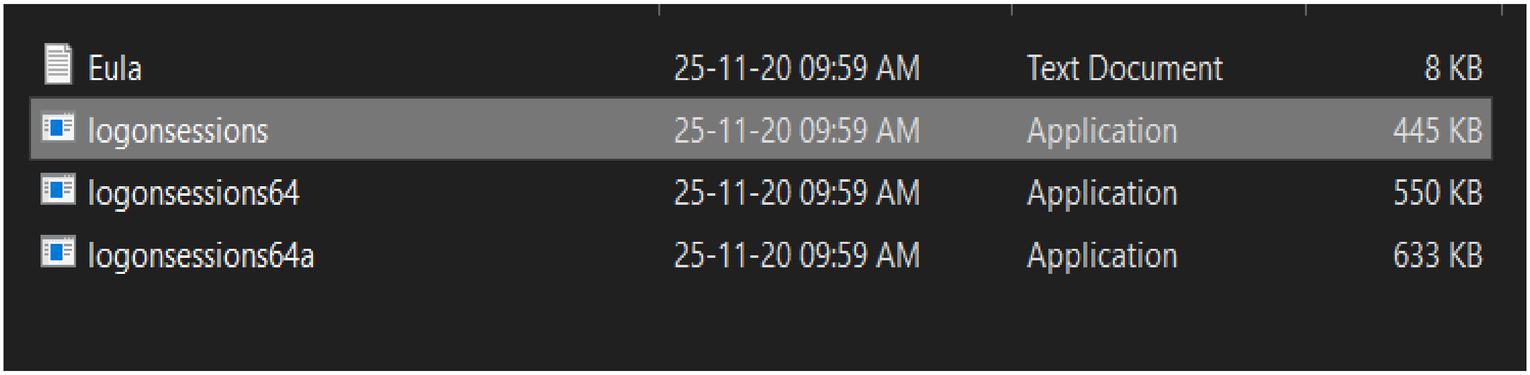
Purpose: Displays information about all active logon sessions on a computer.

Key Details:

- Shows logon session IDs, usernames, logon type (interactive, service, remote),and authentication method.
- Useful for auditing current and past user sessions.

Use in Debugging:

- Detects orphaned sessions that might lock resources.
- Helps trace suspicious logins during incident response.



Eula	25-11-20 09:59 AM	Text Document	8 KB
logonsessions	25-11-20 09:59 AM	Application	445 KB
logonsessions64	25-11-20 09:59 AM	Application	550 KB
logonsessions64a	25-11-20 09:59 AM	Application	633 KB

Autologon

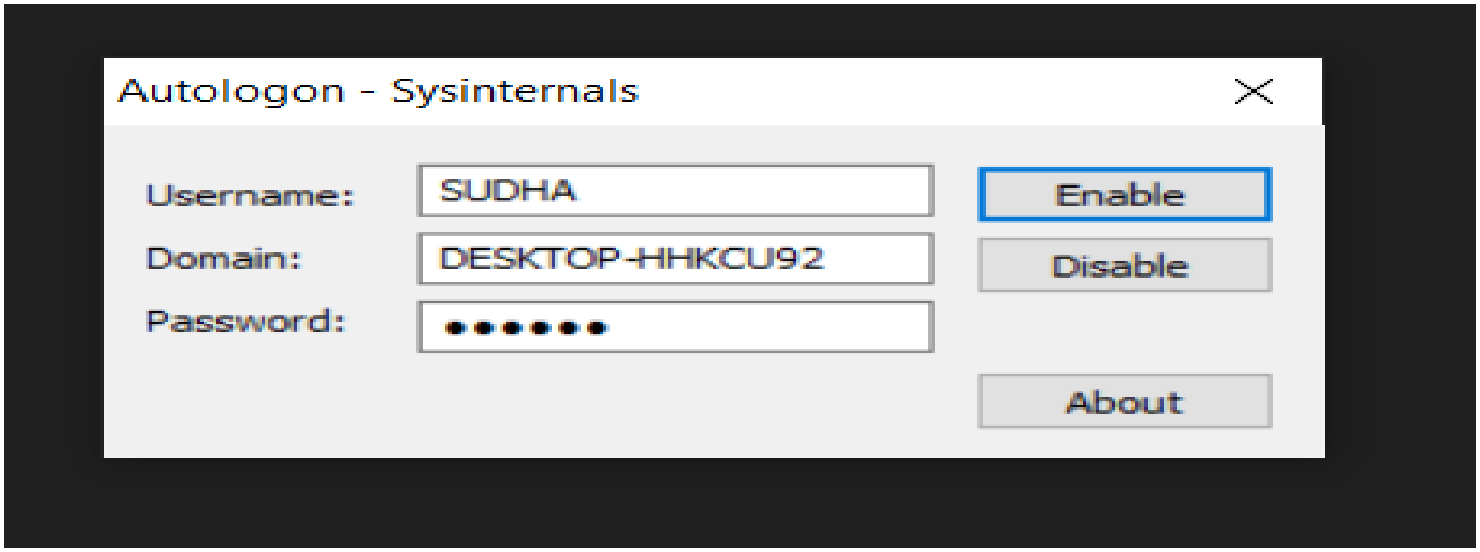
Purpose: Configures Windows to automatically log in with specified credentials.

Key Details:

- Credentials are encrypted in the registry and used during system startup.
- Removes the need for manual user input at every reboot.

Use in Debugging:

- Automates repeated testing cycles after system reboots in packaging environments.
- Speeds up virtual machine testing scenarios where manual logon delays progress.



Autologon - Sysinternals

Username: SUDHA

Domain: DESKTOP-HHKCU92

Password: ●●●●●●

Process Explorer

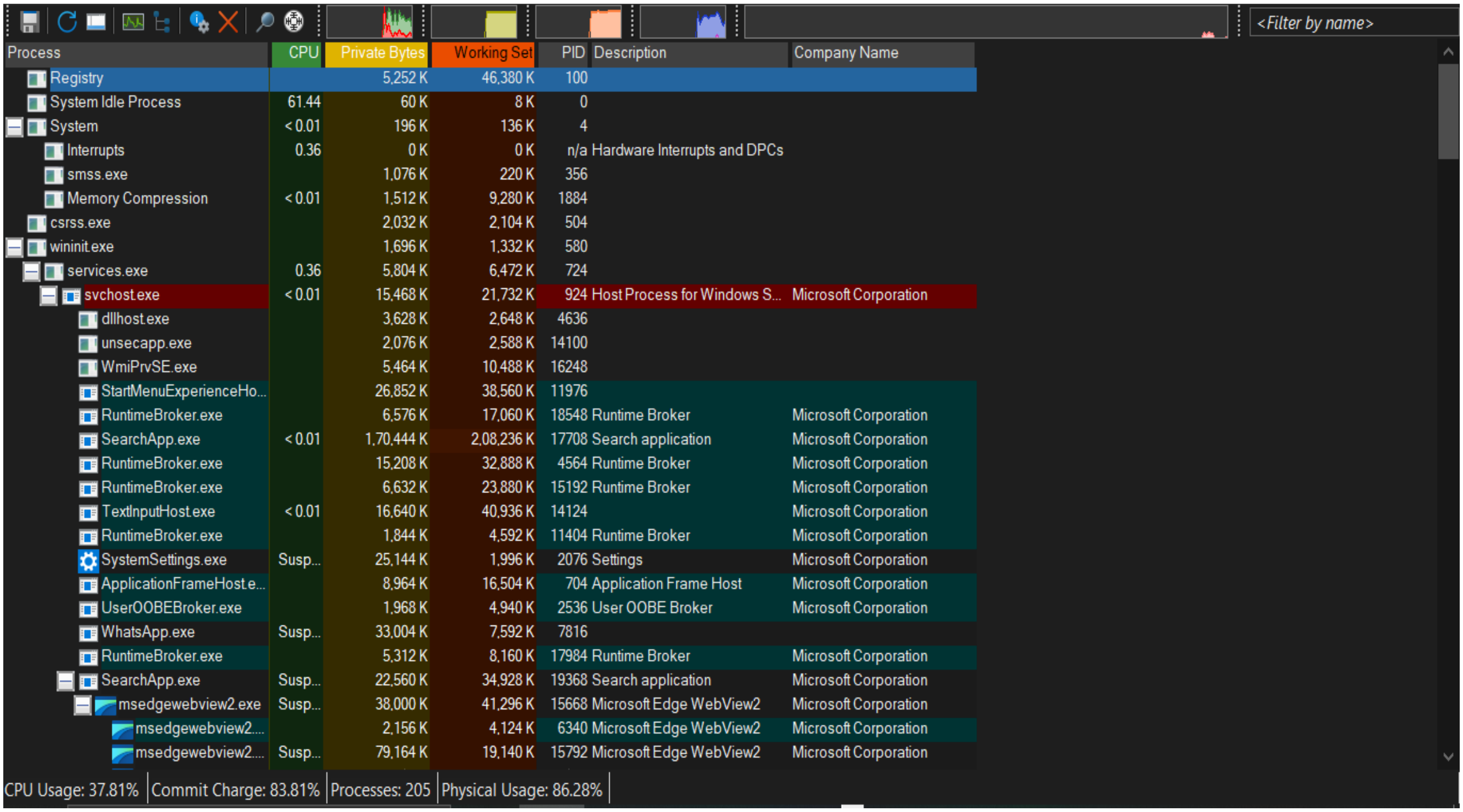
Purpose: Advanced process management tool, often referred to as “Task Manager on steroids.”

Key Details:

- Displays process hierarchy, open handles, loaded DLLs, CPU/memory usage, and verified signatures.
- Highlights recently launched or suspicious processes in real time.

Use in Debugging:

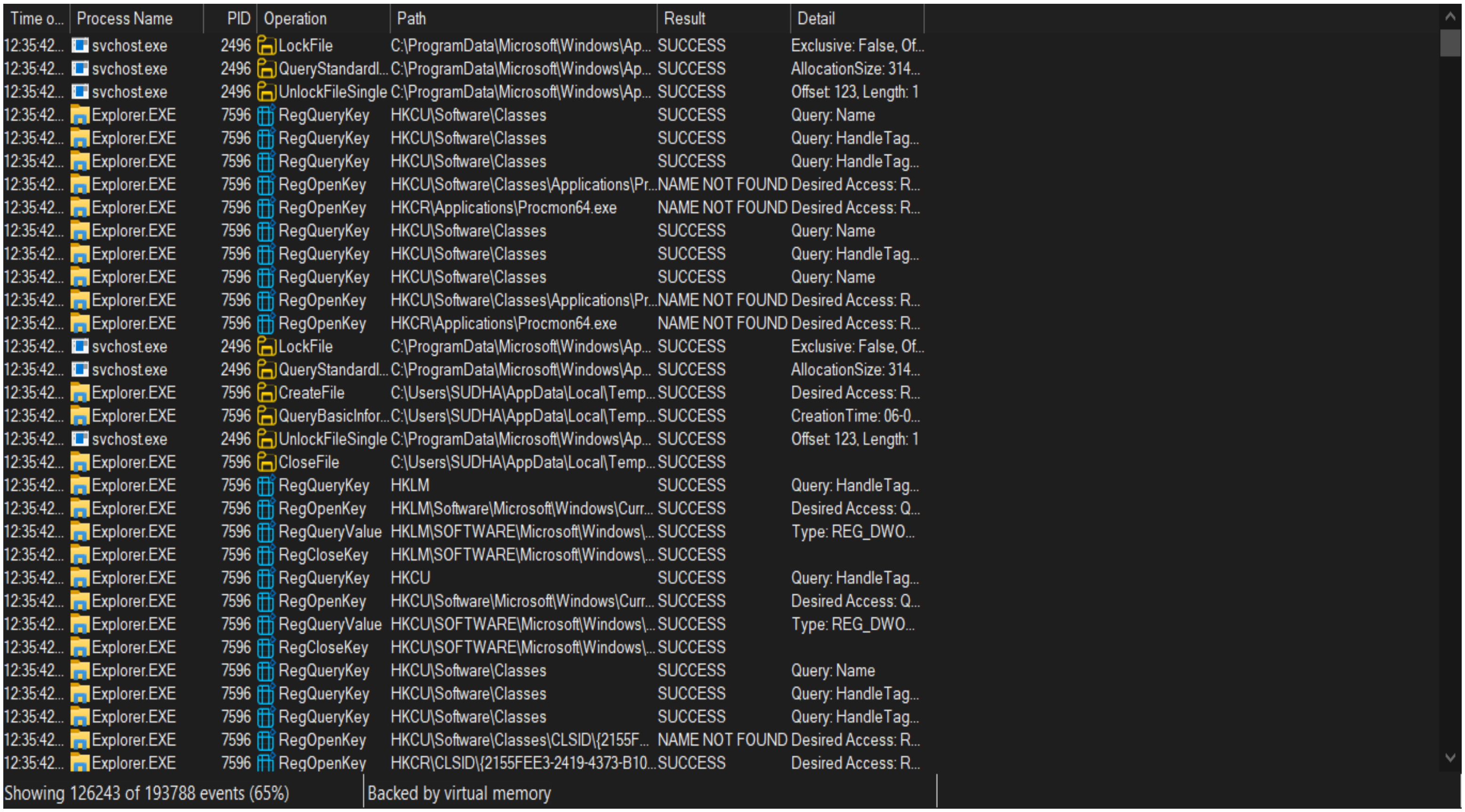
- Identifies which process is locking a file or preventing an installer from running.
- Checks for unsigned binaries or malicious software



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		5,252 K	46,380 K	100		
System Idle Process	61.44	60 K	8 K	0		
System	< 0.01	196 K	136 K	4		
Interrupts	0.36	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,076 K	220 K	356		
Memory Compression	< 0.01	1,512 K	9,280 K	1884		
csrss.exe		2,032 K	2,104 K	504		
wininit.exe		1,696 K	1,332 K	580		
services.exe	0.36	5,804 K	6,472 K	724		
svchost.exe	< 0.01	15,468 K	21,732 K	924	Host Process for Windows S...	Microsoft Corporation
dllhost.exe		3,628 K	2,648 K	4636		
unsecapp.exe		2,076 K	2,588 K	14100		
WmiPrvSE.exe		5,464 K	10,488 K	16248		
StartMenuExperienceHo...		26,852 K	38,560 K	11976		
RuntimeBroker.exe		6,576 K	17,060 K	18548	Runtime Broker	Microsoft Corporation
SearchApp.exe	< 0.01	1,70,444 K	2,08,236 K	17708	Search application	Microsoft Corporation
RuntimeBroker.exe		15,208 K	32,888 K	4564	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		6,632 K	23,880 K	15192	Runtime Broker	Microsoft Corporation
TextInputHost.exe	< 0.01	16,640 K	40,936 K	14124		Microsoft Corporation
RuntimeBroker.exe		1,844 K	4,592 K	11404	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	25,144 K	1,996 K	2076	Settings	Microsoft Corporation
ApplicationFrameHost.e...		8,964 K	16,504 K	704	Application Frame Host	Microsoft Corporation
UserOOBEBroker.exe		1,968 K	4,940 K	2536	User OOBE Broker	Microsoft Corporation
WhatsApp.exe	Susp...	33,004 K	7,592 K	7816		
RuntimeBroker.exe		5,312 K	8,160 K	17984	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	22,560 K	34,928 K	19368	Search application	Microsoft Corporation
msedgewebview2.exe	Susp...	38,000 K	41,296 K	15668	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....		2,156 K	4,124 K	6340	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2....	Susp...	79,164 K	19,140 K	15792	Microsoft Edge WebView2	Microsoft Corporation

CPU Usage: 37.81% | Commit Charge: 83.81% | Processes: 205 | Physical Usage: 86.28%

ProcessMonitoring



Time o...	Process Name	PID	Operation	Path	Result	Detail
12:35:42...	svchost.exe	2496	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive: False, Of...
12:35:42...	svchost.exe	2496	QueryStandardI...	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 314...
12:35:42...	svchost.exe	2496	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset: 123, Length: 1
12:35:42...	Explorer.EXE	7596	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:35:42...	Explorer.EXE	7596	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:35:42...	Explorer.EXE	7596	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:35:42...	Explorer.EXE	7596	RegOpenKey	HKCU\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
12:35:42...	Explorer.EXE	7596	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
12:35:42...	Explorer.EXE	7596	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:35:42...	Explorer.EXE	7596	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:35:42...	Explorer.EXE	7596	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:35:42...	Explorer.EXE	7596	RegOpenKey	HKCU\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
12:35:42...	Explorer.EXE	7596	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
12:35:42...	svchost.exe	2496	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive: False, Of...
12:35:42...	svchost.exe	2496	QueryStandardI...	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	AllocationSize: 314...
12:35:42...	Explorer.EXE	7596	CreateFile	C:\Users\SUDHA\AppData\Local\Temp...	SUCCESS	Desired Access: R...
12:35:42...	Explorer.EXE	7596	QueryBasicInfor...	C:\Users\SUDHA\AppData\Local\Temp...	SUCCESS	CreationTime: 06-0...
12:35:42...	svchost.exe	2496	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset: 123, Length: 1
12:35:42...	Explorer.EXE	7596	CloseFile	C:\Users\SUDHA\AppData\Local\Temp...	SUCCESS	
12:35:42...	Explorer.EXE	7596	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
12:35:42...	Explorer.EXE	7596	RegOpenKey	HKLM\Software\Microsoft\Windows\Curr...	SUCCESS	Desired Access: Q...
12:35:42...	Explorer.EXE	7596	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	Type: REG_DWO...
12:35:42...	Explorer.EXE	7596	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	
12:35:42...	Explorer.EXE	7596	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
12:35:42...	Explorer.EXE	7596	RegOpenKey	HKCU\Software\Microsoft\Windows\Curr...	SUCCESS	Desired Access: Q...
12:35:42...	Explorer.EXE	7596	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\...	SUCCESS	Type: REG_DWO...
12:35:42...	Explorer.EXE	7596	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\...	SUCCESS	
12:35:42...	Explorer.EXE	7596	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:35:42...	Explorer.EXE	7596	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:35:42...	Explorer.EXE	7596	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:35:42...	Explorer.EXE	7596	RegOpenKey	HKCU\Software\Classes\CLSID\{2155F...	NAME NOT FOUND	Desired Access: R...
12:35:42...	Explorer.EXE	7596	RegOpenKey	HKCR\CLSID\{2155FEE3-2419-4373-B10...	SUCCESS	Desired Access: R...

Showing 126243 of 193788 events (65%) | Backed by virtual memory

PsExec

Purpose: Executes processes on remote systems or under different user contexts.

Key Details:

- Allows launching commands as SYSTEM, administrator, or another user.
- Does not require manual login to the remote machine.

Use in Debugging:

- Testing MSI packages under SYSTEM context (similar to SCCM deployment).
- Troubleshooting permission-related installation failures.

PsTools

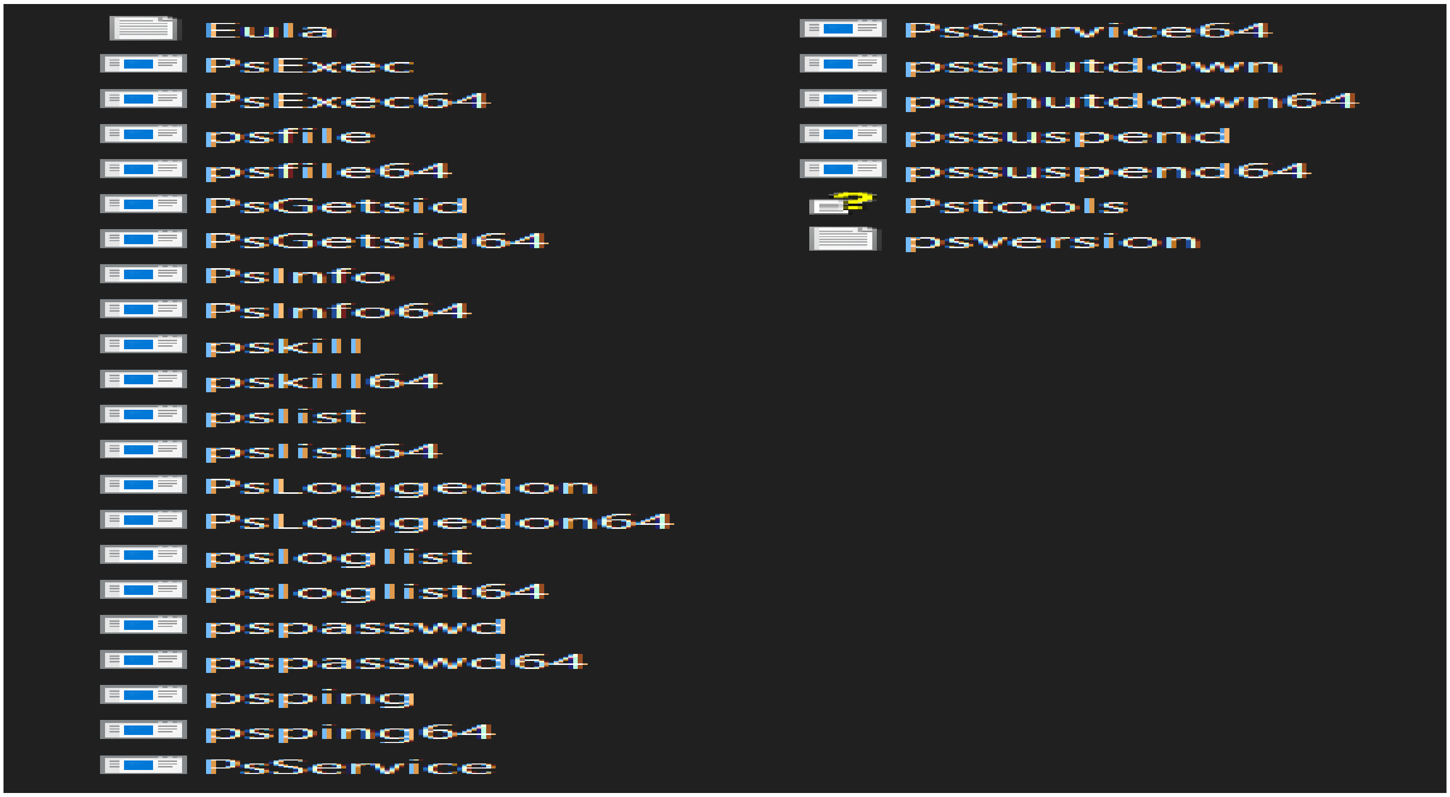
Purpose: A collection of command-line tools for remote administration.

Key Utilities in the Suite:

- **PsList :** View processes on remote systems.
- **PsKill :** Terminate processes remotely.
- **PsLoggedOn :** View logged-on users.
- **PsShutdown :** Reboot or shut down systems remotely.

Use in Debugging:

- Manage processes and sessions across multiple machines in a testing lab.
- Quickly restart services or kill problematic processes blocking an installation.



```
Eula
PsExec
PsExec64
psfile
psfile64
PsGetsid
PsGetsid64
PsInfo
PsInfo64
pskill
pskill64
pslist
pslist64
PsLoggedon
PsLoggedon64
psloglist
psloglist64
pspasswd
pspasswd64
psping
psping64
PsService
PsService64
psshutdown
psshutdown64
pssuspend
pssuspend64
Pstools
psversion
```

Whois

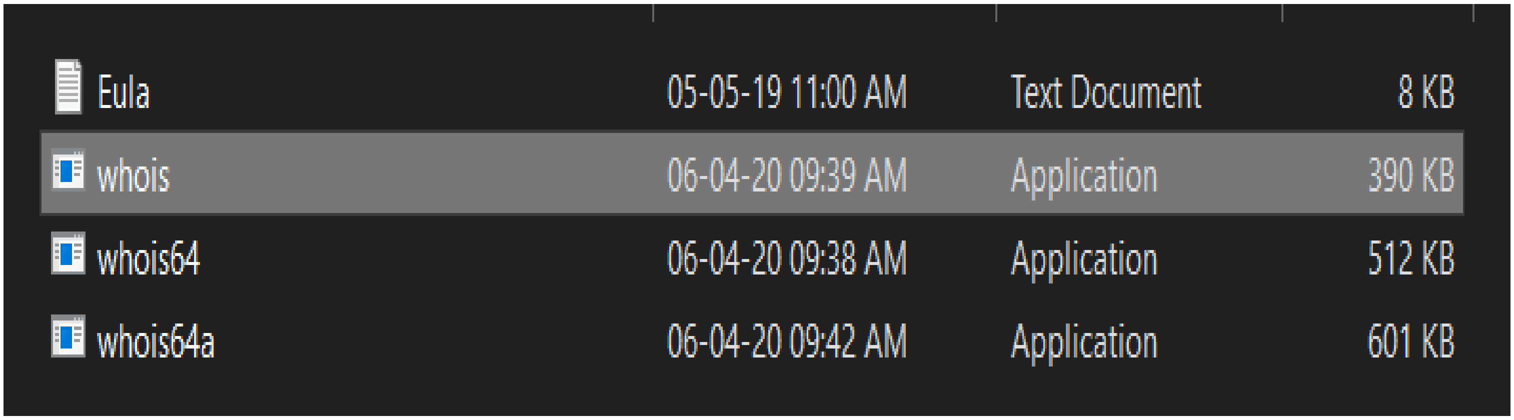
Purpose: Looks up registration details of a domain.

Key Details:

- Provides information on domain ownership, registrar, and contact details.
- Helps verify if a domain is legitimate.

Use in Debugging:

- Useful in security analysis when applications connect to suspicious external servers.
- Validates network endpoints used by software.



Eula	05-05-19 11:00 AM	Text Document	8 KB
whois	06-04-20 09:39 AM	Application	390 KB
whois64	06-04-20 09:38 AM	Application	512 KB
whois64a	06-04-20 09:42 AM	Application	601 KB

Sysmon

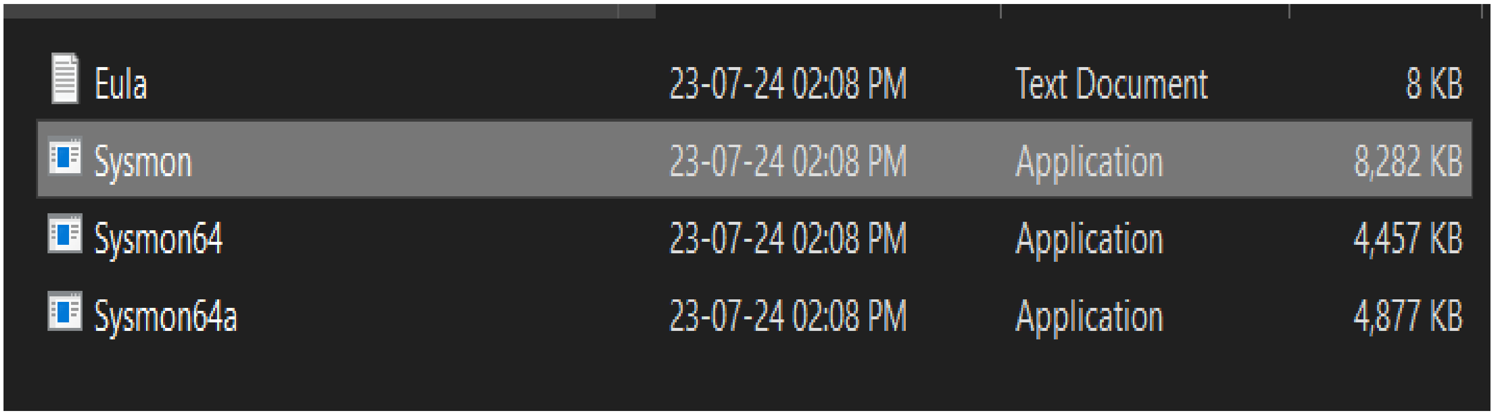
Purpose: A Windows service and driver for logging detailed system activity into Event Viewer.

Key Details:

- Records process creation (with hashes, command line), network connections, and file creation events.
- Supports custom configuration for filtering events of interest.

Use in Debugging:

- Tracks which processes and files are created by an installer or application.
- Detects unexpected or malicious activity that standard event logs miss.



Eula	23-07-24 02:08 PM	Text Document	8 KB
Sysmon	23-07-24 02:08 PM	Application	8,282 KB
Sysmon64	23-07-24 02:08 PM	Application	4,457 KB
Sysmon64a	23-07-24 02:08 PM	Application	4,877 KB

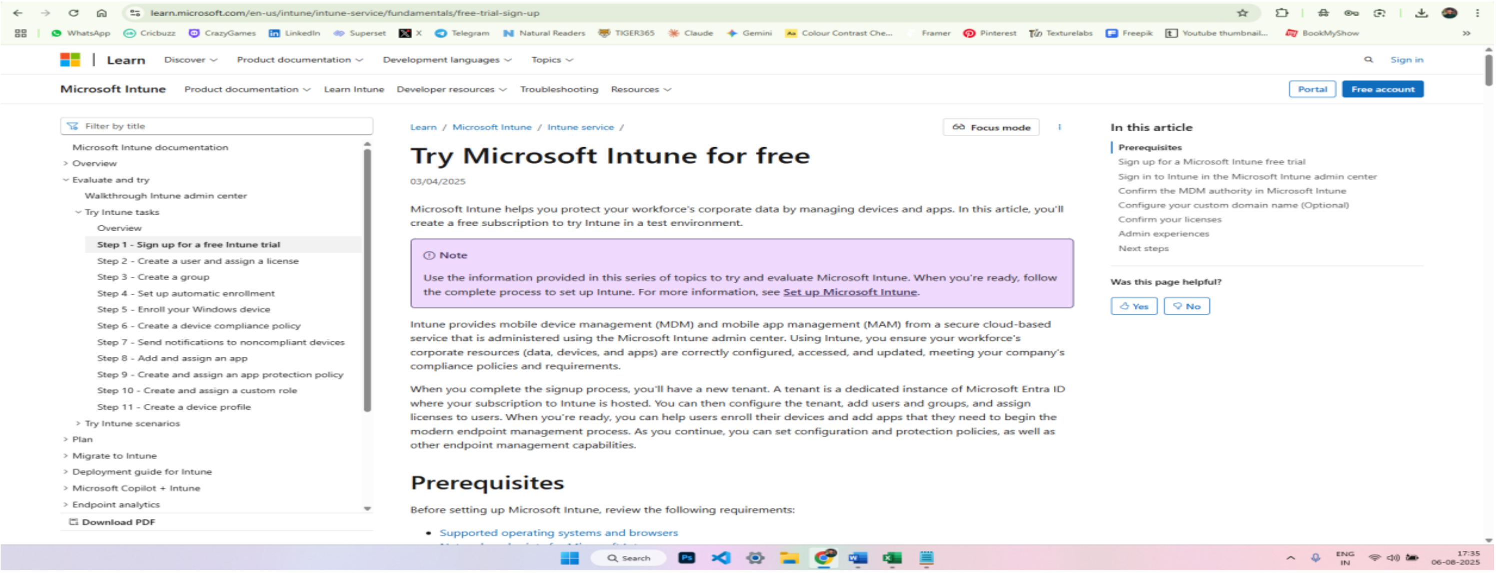
Conclusion

Each of these tools plays a vital role in application packaging, deployment, and security analysis. From monitoring process and registry activity (Process Explorer, RegMon, Sysmon) to managing remote executions (PsExec, PsTools) and session tracking (LogonSessions), they provide comprehensive visibility into Windows systems. Mastering these utilities helps in resolving installation issues, diagnosing application failures, and improving overall troubleshooting efficiency.

TOPIC : Steps to create for Microsoft intune portal.

1. Access the Intune Setup Account Page:

- Open a web browser and go to the Intune setup account page.


learn.microsoft.com/en-us/intune/intune-service/fundamentals/free-trial-sign-up
WhatsApp
Cricbuzz
CrazyGames
LinkedIn
Superset
X
Telegram
Natural Readers
TIGER365
Claude
Gemini
Colour Contrast Che...
Framer
Pinterest
Texturelabs
Freepik
Youtube thumbnail...
BookMyShow
Learn
Discover
Product documentation
Development languages
Topics
Sign in
Microsoft Intune
Product documentation
Learn Intune
Developer resources
Troubleshooting
Resources
Portal
Free account
Filter by title
Microsoft Intune documentation
Overview
Evaluate and try
Walkthrough Intune admin center
Try Intune tasks
Overview
Step 1 - Sign up for a free Intune trial
Step 2 - Create a user and assign a license
Step 3 - Create a group
Step 4 - Set up automatic enrollment
Step 5 - Enroll your Windows device
Step 6 - Create a device compliance policy
Step 7 - Send notifications to noncompliant devices
Step 8 - Add and assign an app
Step 9 - Create and assign an app protection policy
Step 10 - Create and assign a custom role
Step 11 - Create a device profile
Try Intune scenarios
Plan
Migrate to Intune
Deployment guide for Intune
Microsoft Copilot + Intune
Endpoint analytics
Download PDF
Learn / Microsoft Intune / Intune service /
Focus mode
In this article
Prerequisites
Sign up for a Microsoft Intune free trial
Sign in to Intune in the Microsoft Intune admin center
Confirm the MDM authority in Microsoft Intune
Configure your custom domain name (Optional)
Confirm your licenses
Admin experiences
Next steps
Was this page helpful?
Yes
No
Search
ENG
IN
17:35
06-08-2025

Try Microsoft Intune for free

03/04/2025

Microsoft Intune helps you protect your workforce's corporate data by managing devices and apps. In this article, you'll create a free subscription to try Intune in a test environment.

Note

Use the information provided in this series of topics to try and evaluate Microsoft Intune. When you're ready, follow the complete process to set up Intune. For more information, see Set up Microsoft Intune.

Intune provides mobile device management (MDM) and mobile app management (MAM) from a secure cloud-based service that is administered using the Microsoft Intune admin center. Using Intune, you ensure your workforce's corporate resources (data, devices, and apps) are correctly configured, accessed, and updated, meeting your company's compliance policies and requirements.

When you complete the signup process, you'll have a new tenant. A tenant is a dedicated instance of Microsoft Entra ID where your subscription to Intune is hosted. You can then configure the tenant, add users and groups, and assign licenses to users. When you're ready, you can help users enroll their devices and add apps that they need to begin the modern endpoint management process. As you continue, you can set configuration and protection policies, as well as other endpoint management capabilities.

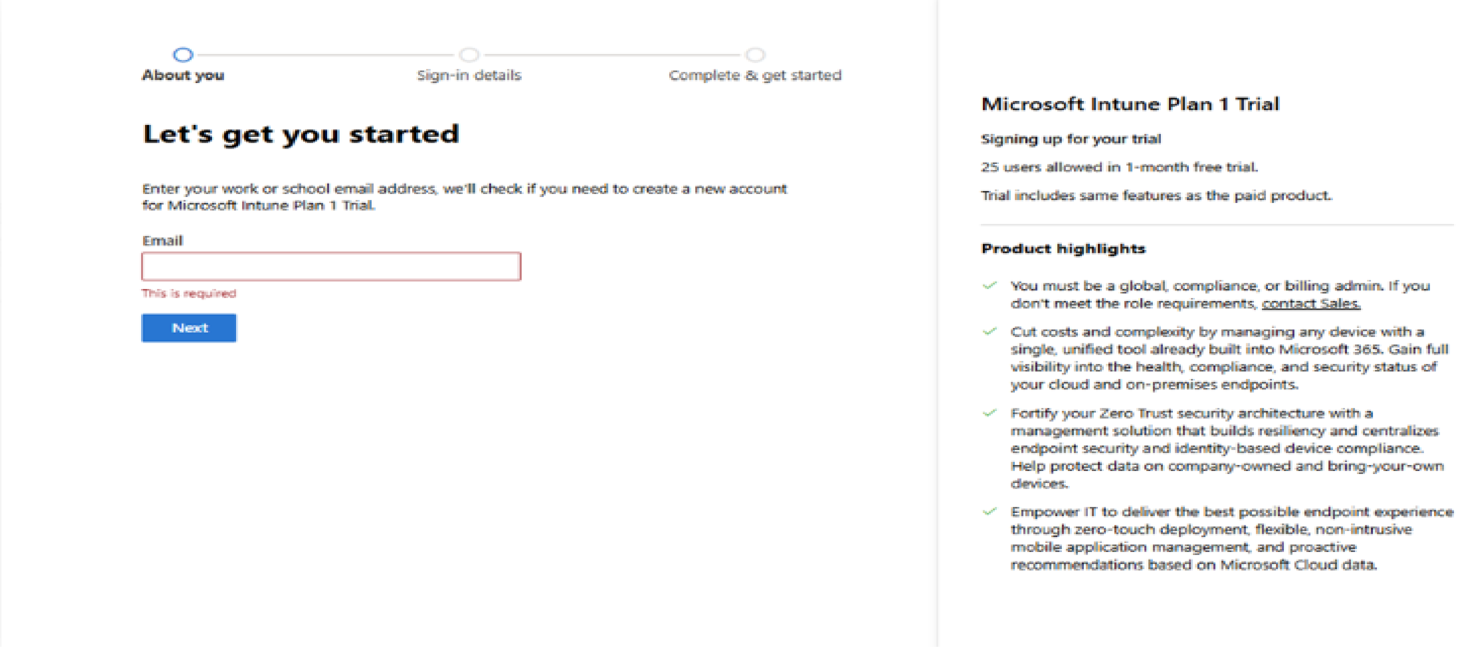
Prerequisites

Before setting up Microsoft Intune, review the following requirements:

- Supported operating systems and browsers

2. Sign Up or Sign In:

- For new users: Enter your email address and click "Next." Follow the prompts to create a new account and provide the necessary information.
- For existing users: Sign in with your existing work or school account.



Let's get you started

Enter your work or school email address, we'll check if you need to create a new account for Microsoft Intune Plan 1 Trial.

Email

This is required

Microsoft Intune Plan 1 Trial

Signing up for your trial

25 users allowed in 1-month free trial.

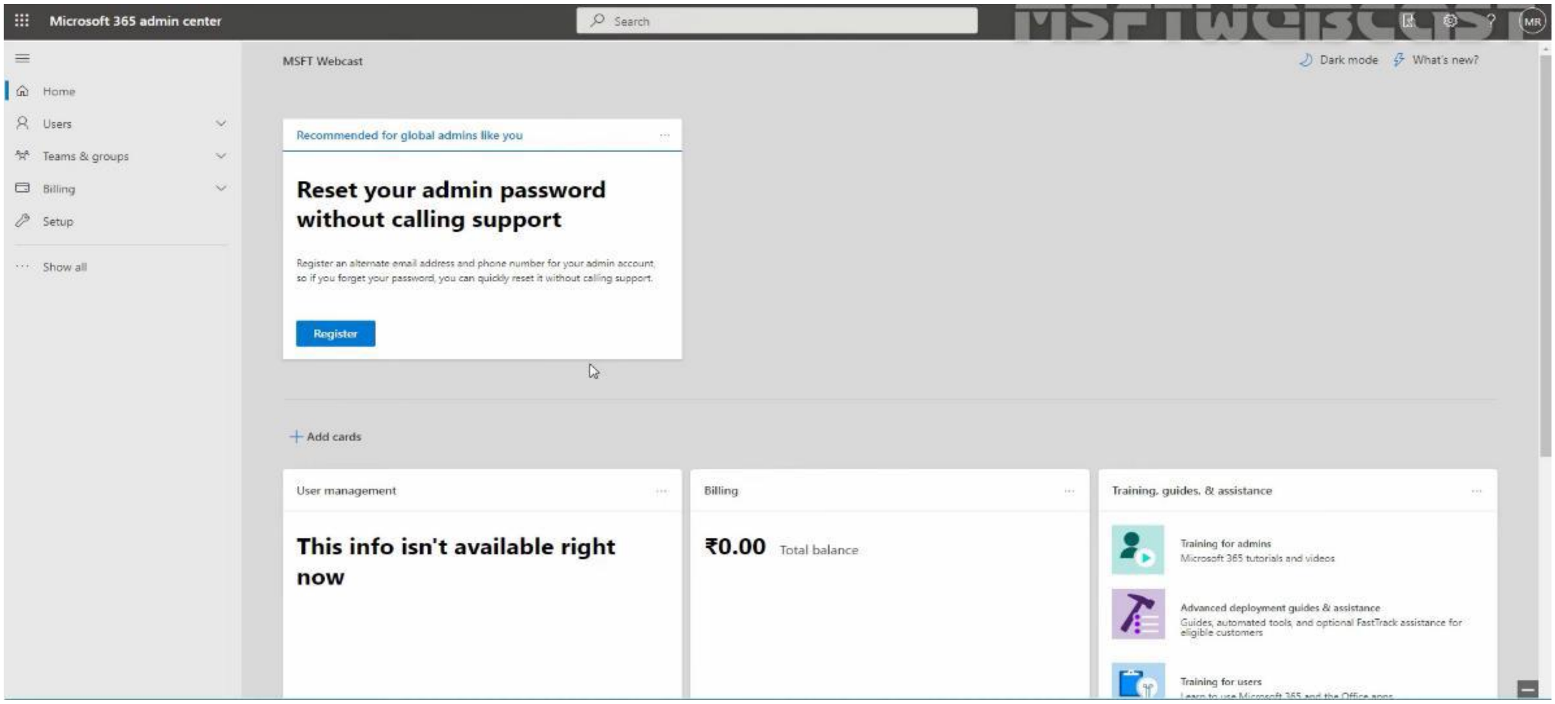
Trial includes same features as the paid product.

Product highlights

- ✓ You must be a global, compliance, or billing admin. If you don't meet the role requirements, contact Sales.
- ✓ Cut costs and complexity by managing any device with a single, unified tool already built into Microsoft 365. Gain full visibility into the health, compliance, and security status of your cloud and on-premises endpoints.
- ✓ Fortify your Zero Trust security architecture with a management solution that builds resiliency and centralizes endpoint security and identity-based device compliance. Help protect data on company-owned and bring-your-own devices.
- ✓ Empower IT to deliver the best possible endpoint experience through zero-touch deployment, flexible, non-intrusive mobile application management, and proactive recommendations based on Microsoft Cloud data.

3. Complete the Sign-Up Process:

- If creating a new account, you'll be asked to verify your email address and potentially provide additional information like your name, company details, and region.
- After signing up or signing in, you'll be directed to the Microsoft 365 Admin Center.



Recommended for global admins like you

Reset your admin password without calling support

Register an alternate email address and phone number for your admin account, so if you forget your password, you can quickly reset it without calling support.

User management

This info isn't available right now

Billing

₹0.00 Total balance

Training, guides, & assistance

Training for admins
Microsoft 365 tutorials and videos

Advanced deployment guides & assistance
Guides, automated tools, and optional FastTrack assistance for eligible customers

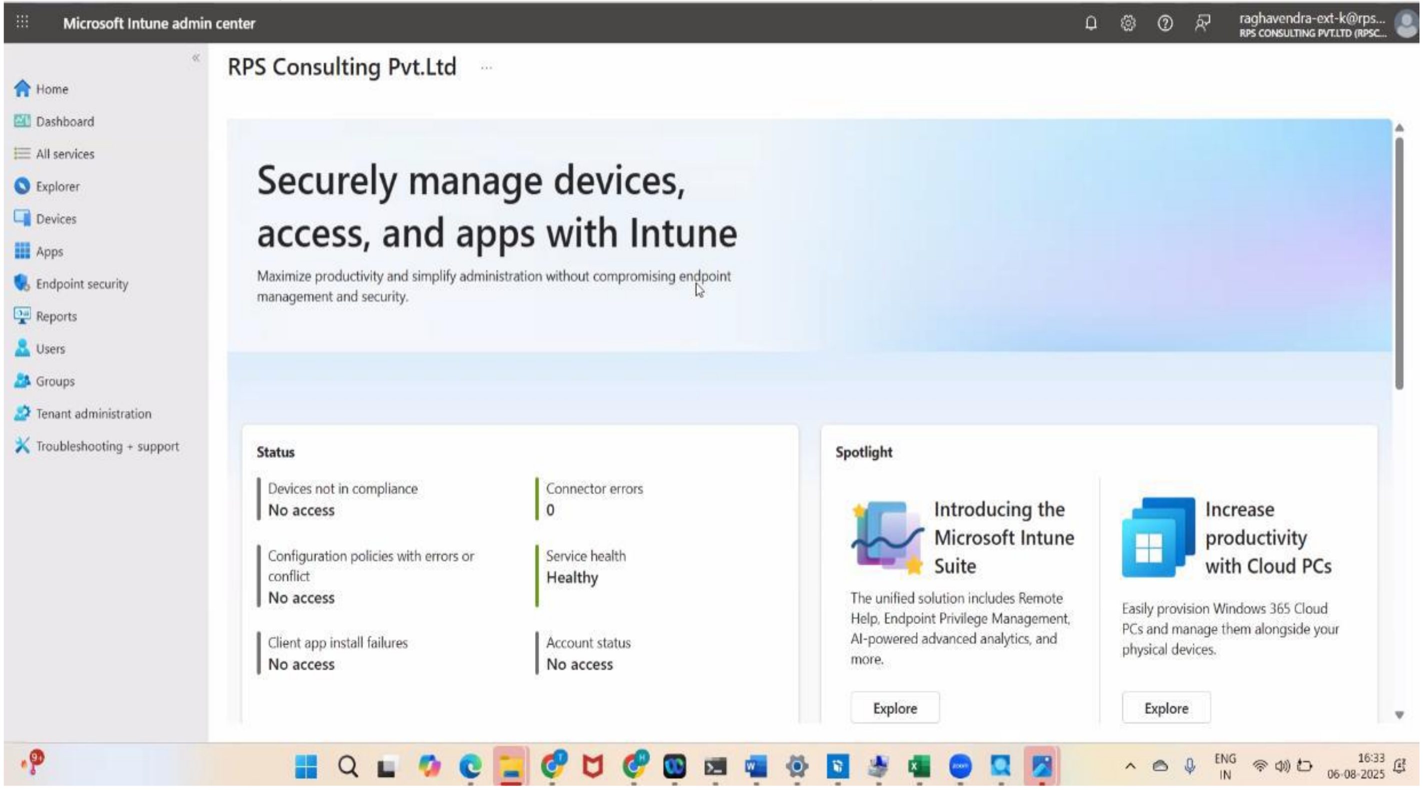
Training for users
Learn to use Microsoft 365 and the Office apps

4. Considerations for Existing Work or School Accounts:

- If you're using an existing work or school account, you might need to add Intune to your existing subscription.
- If you plan to use your organization's custom domain name or synchronize with on-premises Active Directory, you might need to close the browser window after the initial setup and configure these aspects separately.

5. Accessing Intune After Enrollment:

- Once the free trial is set up, you can access the Microsoft Intune Admin Center to manage the service.
- You can use any device with a supported browser to sign in.



RPS Consulting Pvt.Ltd

Securely manage devices, access, and apps with Intune

Maximize productivity and simplify administration without compromising endpoint management and security.

Status

Devices not in compliance
No access

Connector errors
0

Configuration policies with errors or conflict
No access

Service health
Healthy

Client app install failures
No access

Account status
No access

Spotlight

Introducing the Microsoft Intune Suite

The unified solution includes Remote Help, Endpoint Privilege Management, AI-powered advanced analytics, and more.

Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.