Cloud Connect

Stay ahead of the game:

What's new in Microsoft Enterprise Client Management

Jörgen Nilsson & Ronni Pedersen

Cloud Connect

Oslo Spektrum
November 7 - 9

About me

Ronni Pedersen

- Cloud Architect, APENTO
- Microsoft MVP: Enterprise Mobility
- MCSE/MCSA/MCITP/MCTS and more… ☺
- ITIL Foundation Certified
- Microsoft Certified Trainer (MCT)

Contact Info

- Mail: rop@apento.com
- Twitter (X): @ronnipedersen

About me

Jörgen Nilsson

- Principal Consultant, Onevinn
- Microsoft MVP: Enterprise Mobility
- MCSE/MCSA/MCITP/MCTS
- ITIL Foundation Certified
- Microsoft Certified Trainer (MCT)

Contact Info

- Mail: Jorgen.nilsson@onevinn.se
- X (Twitter): @ccmexec

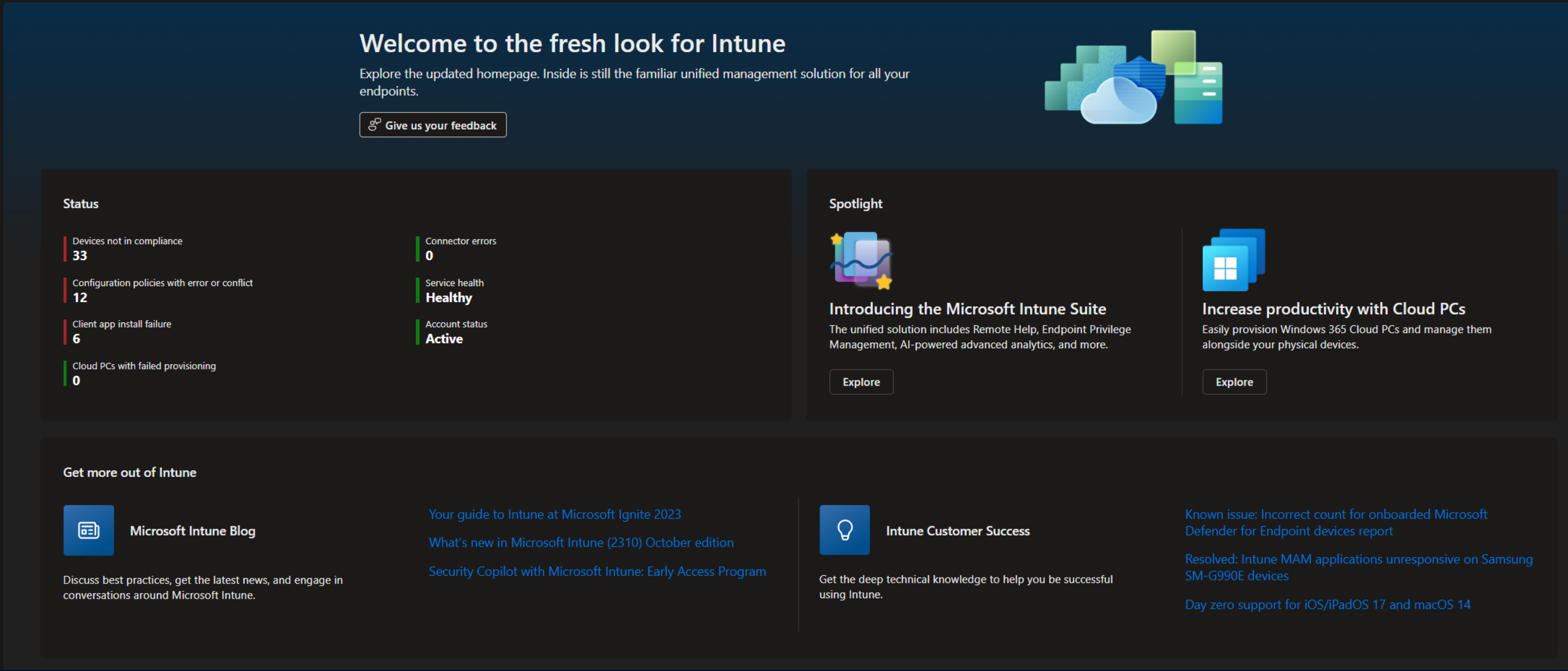
Agenda

- Intune what’s new in the latest releases?
- Intune what’s coming
- Microsoft Intune Suite
- What’s new in Configuration manager 2309
- Windows LAPS!
- Windows Autopatch
- What we learned during 2023

Cloud Connect

Intune what’s new in the latest releases?

New HomeScreen



Welcome to the fresh look for Intune

Explore the updated homepage. Inside is still the familiar unified management solution for all your endpoints.

Give us your feedback

Status

Devices not in compliance
33

Configuration policies with error or conflict
12

Client app install failure
6

Cloud PCs with failed provisioning
0

Connector errors
0

Service health
Healthy

Account status
Active

Spotlight

Introducing the Microsoft Intune Suite

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

Explore

Increase productivity with Cloud PCs

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

Explore

Get more out of Intune

Microsoft Intune Blog

Discuss best practices, get the latest news, and engage in conversations around Microsoft Intune.

- Your guide to Intune at Microsoft Ignite 2023
- What's new in Microsoft Intune (2310) October edition
- Security Copilot with Microsoft Intune: Early Access Program

Intune Customer Success

Get the deep technical knowledge to help you be successful using Intune.

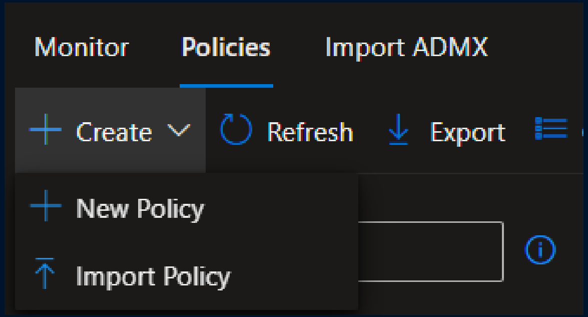
- Known issue: Incorrect count for onboarded Microsoft Defender for Endpoint devices report
- Resolved: Intune MAM applications unresponsive on Samsung SM-G990E devices
- Day zero support for iOS/iPadOS 17 and macOS 14

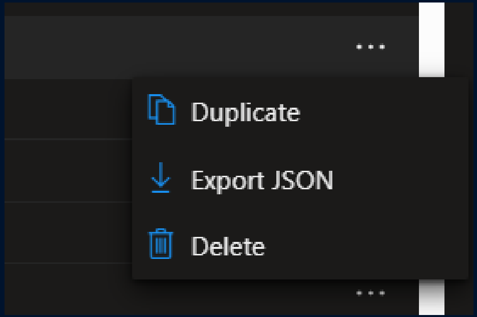
iOS/iPadOS/MacOS/Android

- Web based device enrollment with JIT registration for personal iOS/iPadOS devices
- Configure declarative software updates and passcode policies for Apple devices in the Settings Catalog
- New setting to block users from using the same password to unlock the device and access the work profile on Android Enterprise personally owned devices with a work profile
- Configuration scripts for unmanaged macOS PKG apps
- SSO support during enrollment for Android Enterprise fully managed and corporate-owned devices with a work profile
- Multiple Settings catalog addons for MacOS

Import and export settings catalog policies

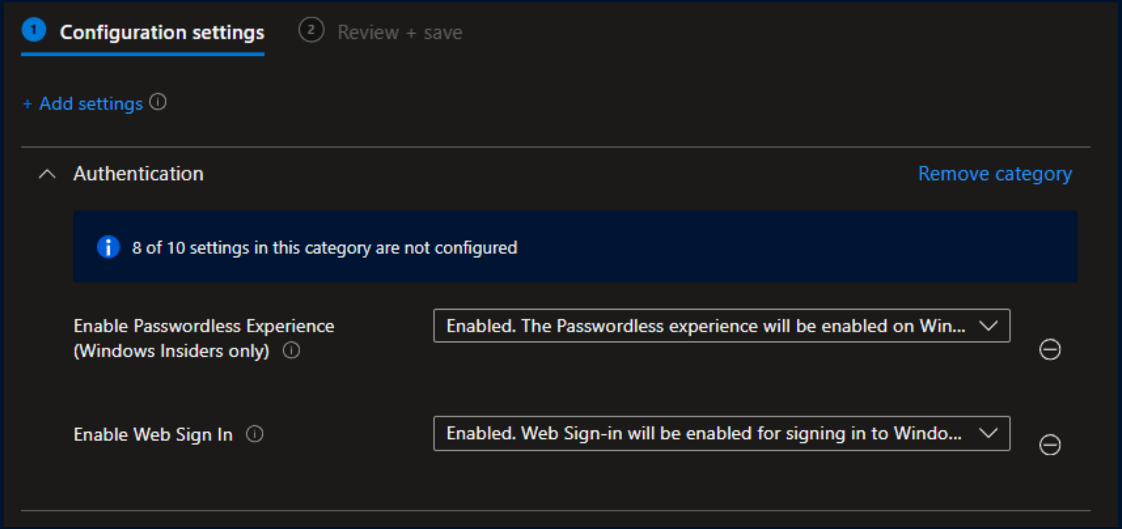
- Long awaited!
- Import/export Settings Catalog to JSON
- Have been possible with PowerShell/Graph





Windows 11 22H2 September CU - Passwordless

- Removes password option from login screen
- Local accounts still work with RunAS
- Settings catalog = only insiders
- Web-sign in and PIN reset to be able to recover



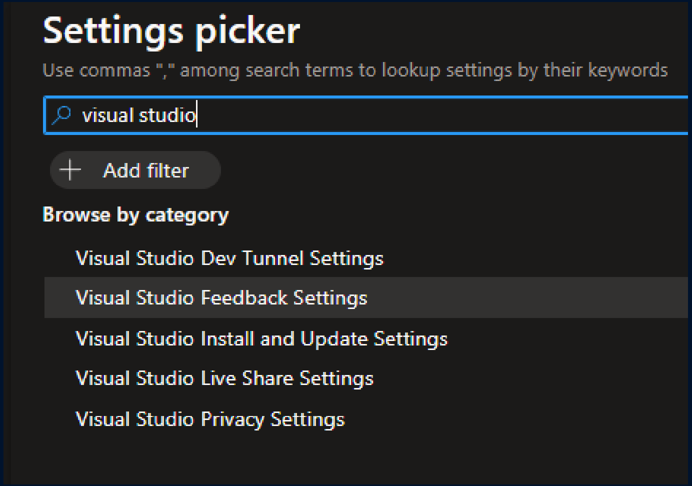
8 of 10 settings in this category are not configured

Enable Passwordless Experience (Windows Insiders only): Enabled. The Passwordless experience will be enabled on Win...

Enable Web Sign In: Enabled. Web Sign-in will be enabled for signing in to Windo...

Settings Catalog updates for Windows

- FSLogix
- Visual Studio



Settings picker

Use commas "," among search terms to lookup settings by their keywords

visual studio

Browse by category

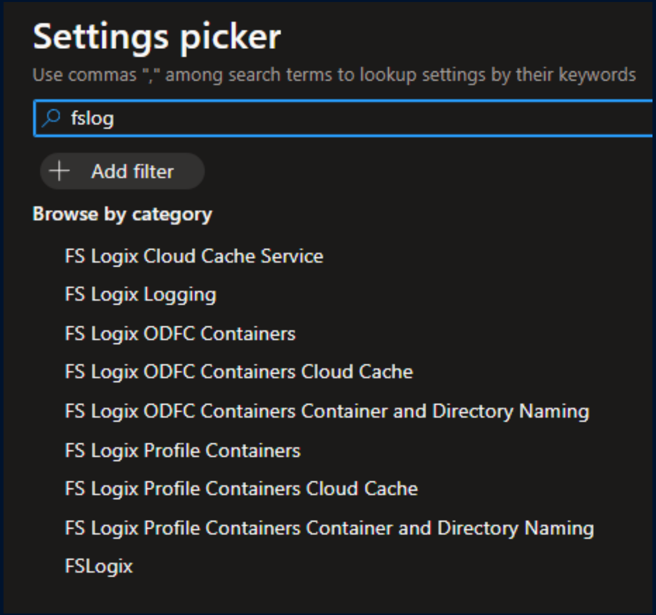
Visual Studio Dev Tunnel Settings

Visual Studio Feedback Settings

Visual Studio Install and Update Settings

Visual Studio Live Share Settings

Visual Studio Privacy Settings



Settings picker

Use commas "," among search terms to lookup settings by their keywords

fslog

Browse by category

FS Logix Cloud Cache Service

FS Logix Logging

FS Logix ODFC Containers

FS Logix ODFC Containers Cloud Cache

FS Logix ODFC Containers Container and Directory Naming

FS Logix Profile Containers

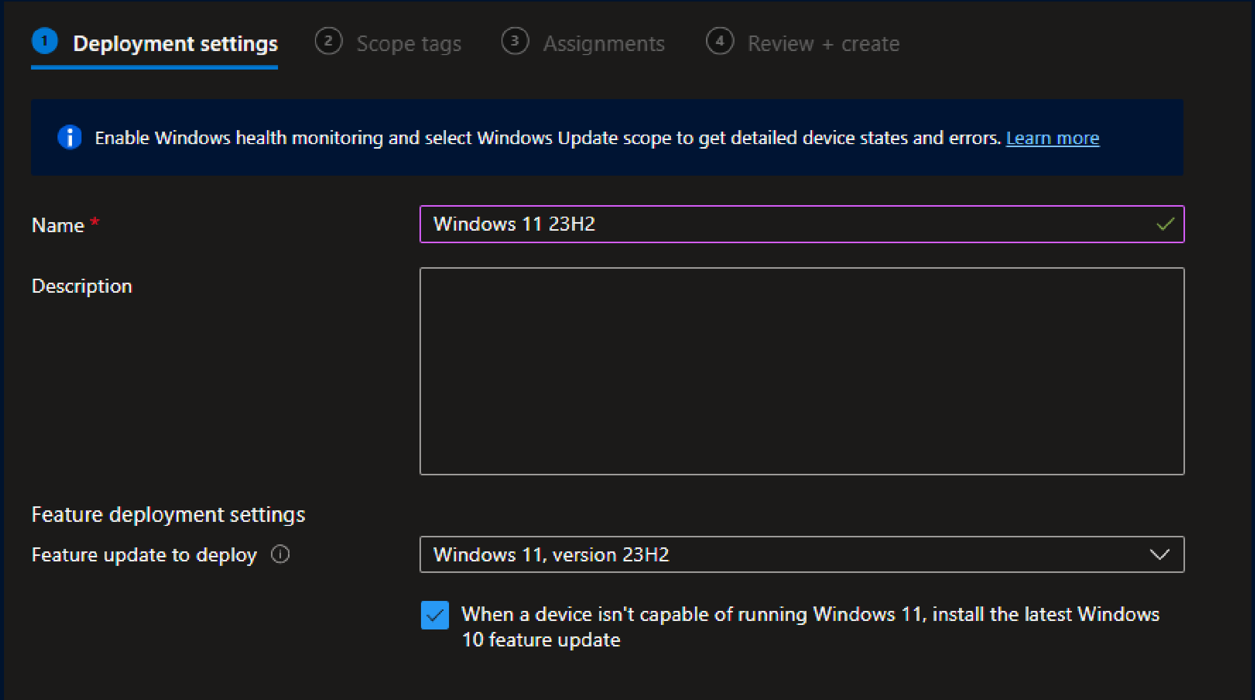
FS Logix Profile Containers Cloud Cache

FS Logix Profile Containers Container and Directory Naming

FSLogix

Upgrade Windows 11 23H2

- New settings to make sure Windows 10 versions used are supported
- With this we need less Feature Update policies



Enable Windows health monitoring and select Windows Update scope to get detailed device states and errors. Learn more

Name * Windows 11 23H2

Description

Feature deployment settings

Feature update to deploy: Windows 11, version 23H2

☑ When a device isn't capable of running Windows 11, install the latest Windows 10 feature update

Intune what’s coming

Coming - Updated Security Baselines

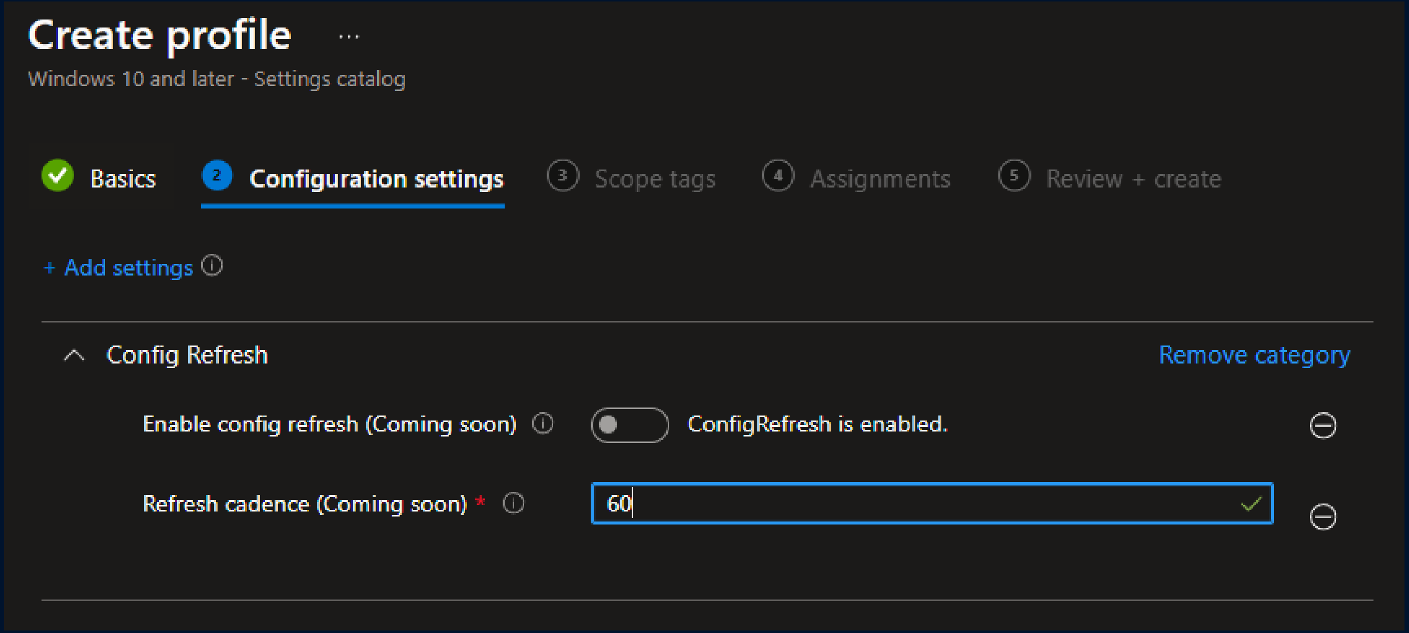
- Security baseline for Microsoft 365 Apps for Enterprise
- Security baseline for Windows 10/11

"Our engineering team has been working diligently to make sure we cover every single applicable setting in the Windows 11 22H2 baseline and ensure that the baseline template is up to quality. There have been major delays due to dependencies on other internal teams. Right now, we're nearing the end and are about 80% of the way there, so I anticipate we will be ready to release the Windows 11 22H2 baseline (which also supports Windows 10 settings) in January '24."

Windows 10/11 22h2 Security Baseline missing in Intune - Microsoft Community Hub

Config Refresh

- Refresh Intune policies on a schedule even when offline
- Important for Security policies!



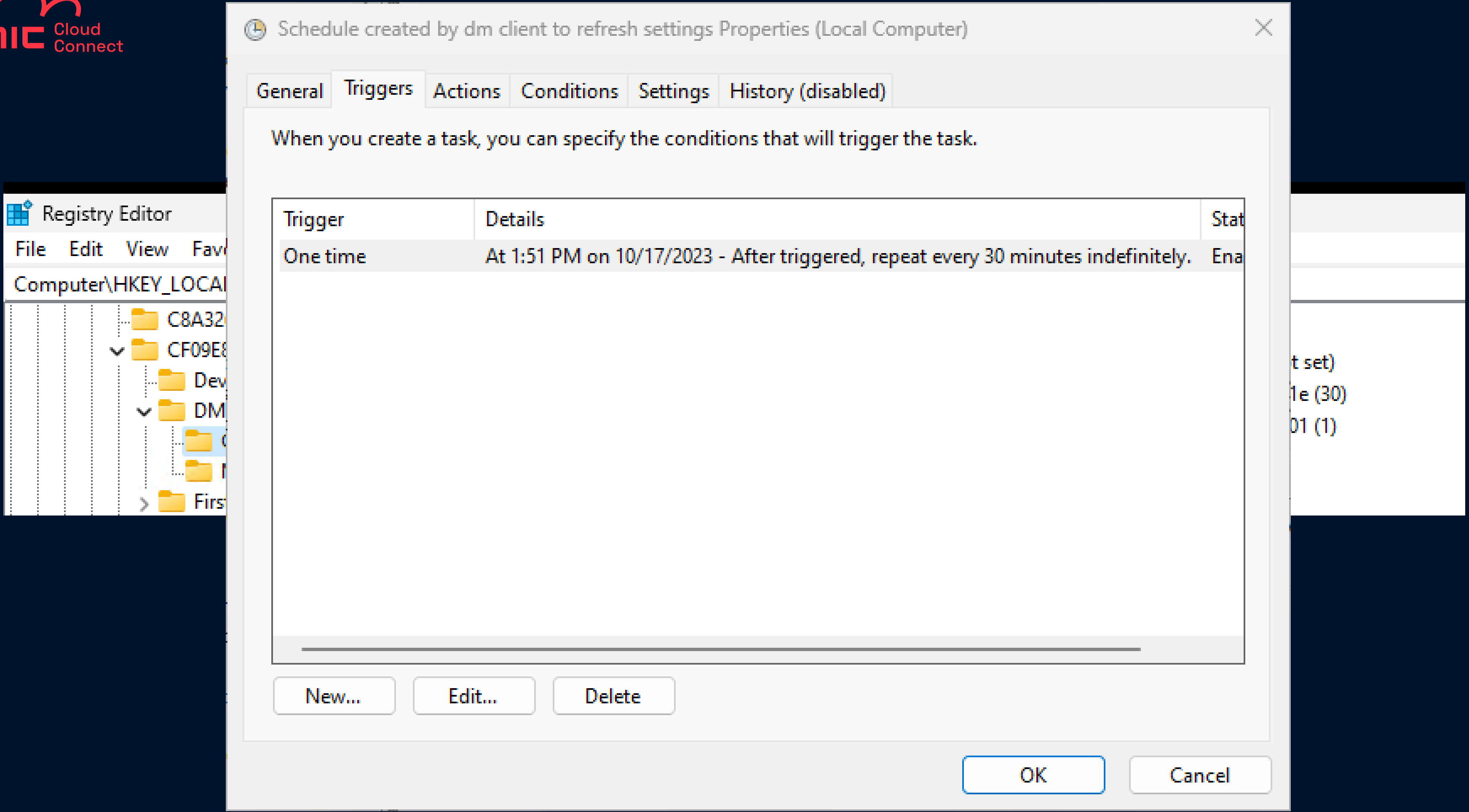
Create profile ···

Windows 10 and later - Settings catalog

Config Refresh

Enable config refresh (Coming soon) ⓘ ● ConfigRefresh is enabled.

Refresh cadence (Coming soon) * ⓘ 60 ✓



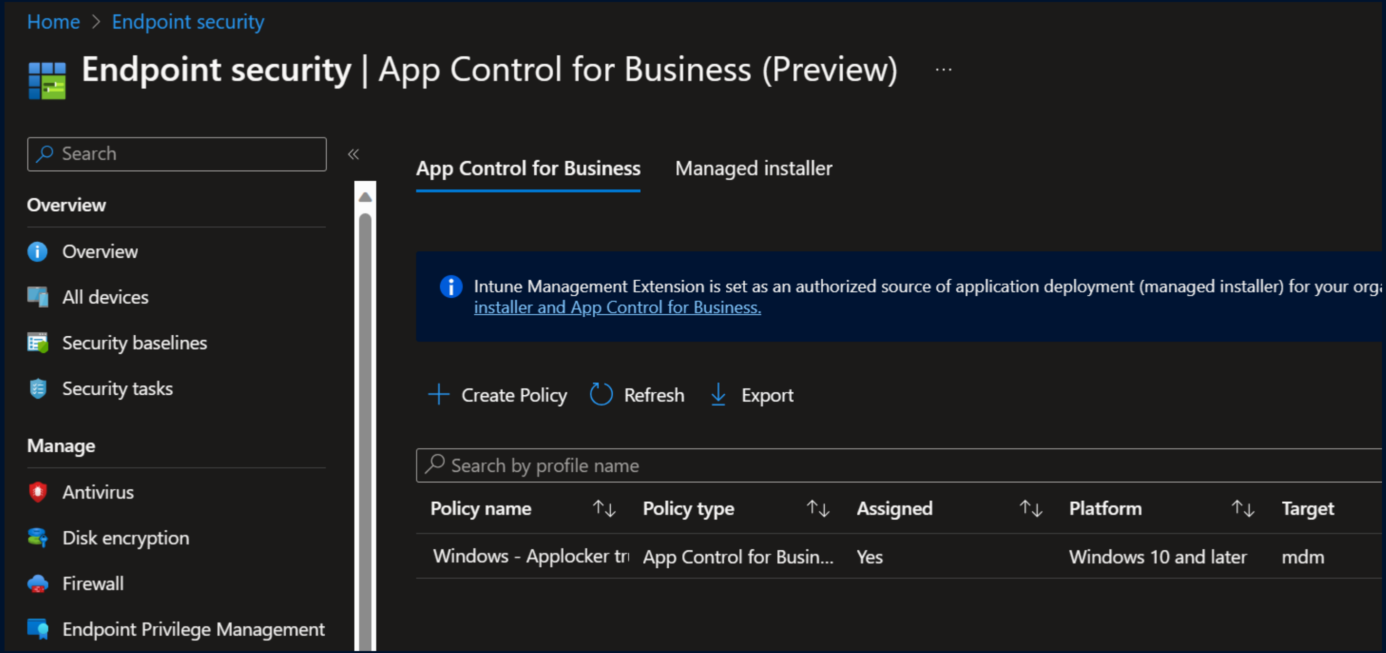
Schedule created by dm client to refresh settings Properties (Local Computer)

When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Stat
One time	At 1:51 PM on 10/17/2023 - After triggered, repeat every 30 minutes indefinitely.	Ena

Application control for business (preview)

- Intune - Managed Installer = Tenant wide
- Investments are being made in Application control for business



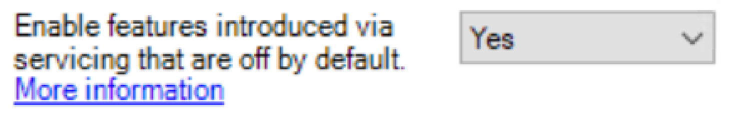
Endpoint security | App Control for Business (Preview)

Intune Management Extension is set as an authorized source of application deployment (managed installer) for your orga
installer and App Control for Business.

Policy name	Policy type	Assigned	Platform	Target
Windows - Applocker tri	App Control for Busin...	Yes	Windows 10 and later	mdm

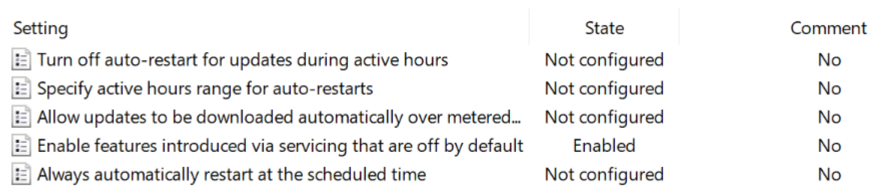
Continuous Innovation

- Adds control of how new features introduced in Monthly CU Windows 11 is deployed
  - Permanent enterprise feature control
  - Temporary enterprise feature control
- Bookmark: https://learn.microsoft.com/en-us/windows/whats-new/temporary-enterprise-feature-control

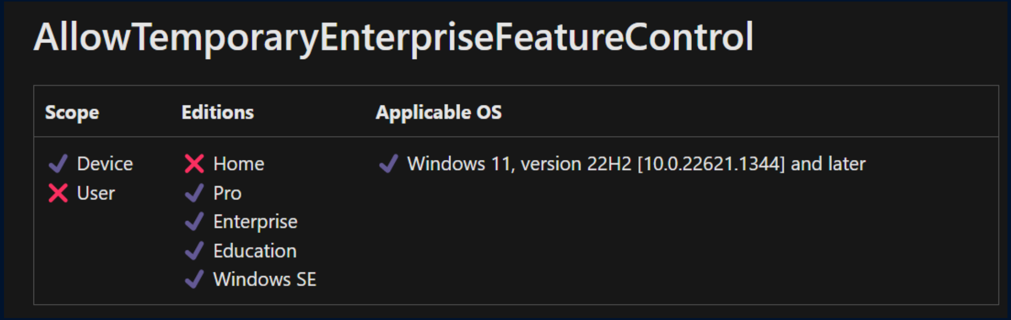


Enable features introduced via servicing that are off by default. Yes

More information



Setting	State	Comment
Turn off auto-restart for updates during active hours	Not configured	No
Specify active hours range for auto-restarts	Not configured	No
Allow updates to be downloaded automatically over metered...	Not configured	No
Enable features introduced via servicing that are off by default	Enabled	No
Always automatically restart at the scheduled time	Not configured	No



AllowTemporaryEnterpriseFeatureControl

Scope	Editions	Applicable OS
✓ Device ✗ User	✗ Home ✓ Pro ✓ Enterprise ✓ Education ✓ Windows SE	✓ Windows 11, version 22H2 [10.0.22621.1344] and later

Intune Suite

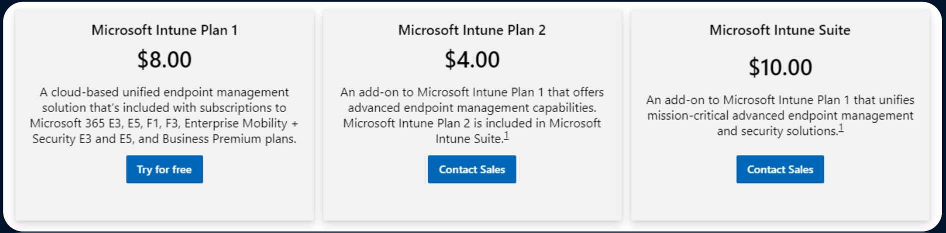
What is the Microsoft Intune Suite?

- Remote Help
- Endpoint Privilege Management
- Advanced Endpoint Analytics
- Microsoft Tunnel for Mobile App Management
- Management of specialty devices
- Advanced App Management
- Cloud PKI Management
- More to come....

More information at Microsoft Ignite 2023!

Intune Plans / License

Capability	Standalone add-on	Intune Plan 2	Intune Suite
Remote help	$ 3.50 ✓	✓	✓
Microsoft Tunnel for Mobile Application Management		✓	✓
Specialized devices management			✓
Microsoft Intune Advanced Endpoint Analytics	$ TBA ✓		✓
Microsoft Intune management of specialty devices		✓	✓
Microsoft Intune Endpoint Privilege Management	$ 3.00 ✓		✓
More advanced capabilities are on the way: • Advanced App Management • Cloud PKI	 $ TBA ✓ $ TBA ✓		 ✓ ✓



Microsoft Intune Plan 1

$8.00

A cloud-based unified endpoint management solution that's included with subscriptions to Microsoft 365 E3, E5, F1, F3, Enterprise Mobility + Security E3 and E5, and Business Premium plans.

Microsoft Intune Plan 2

$4.00

An add-on to Microsoft Intune Plan 1 that offers advanced endpoint management capabilities. Microsoft Intune Plan 2 is included in Microsoft Intune Suite.[1]

Microsoft Intune Suite

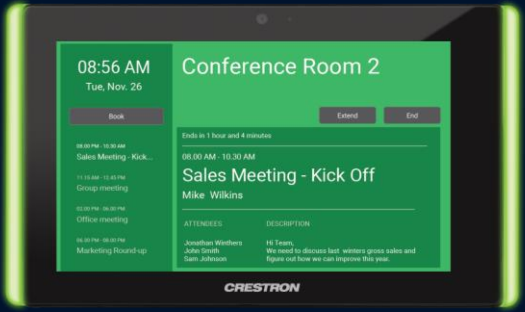
$10.00

An add-on to Microsoft Intune Plan 1 that unifies mission-critical advanced endpoint management and security solutions.[1]

Microsoft Intune management of specialty devices

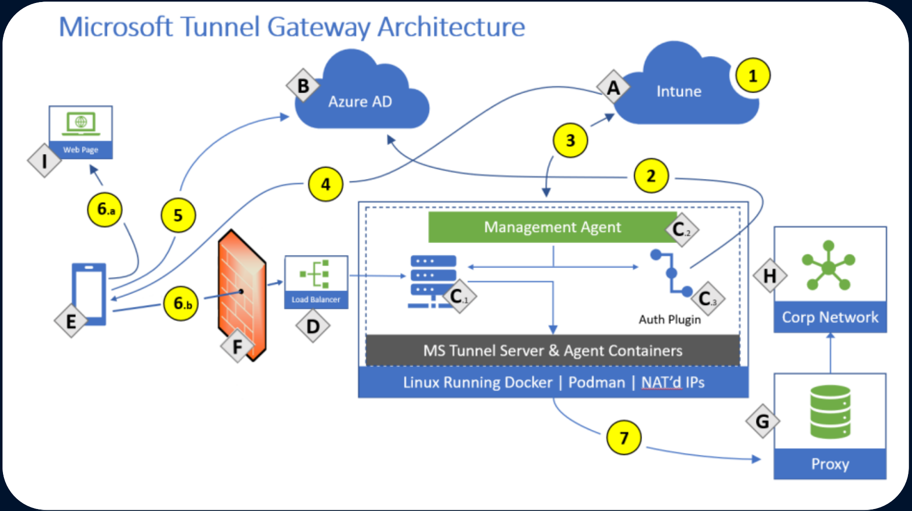
A set of device management, configuration and protection capabilities for special, purpose-built devices

- Augmented reality and virtual reality headsets
- Wearable headsets
- Large smart-screen devices (over 30" in size)
- Conference room meeting devices



Microsoft Tunnel for Mobile Application Management

- VPN gateway solution
- Runs in a container on Linux
- Allows access to on-premises resources from iOS/iPadOS and Android Enterprise devices
- Modern authentication
- Conditional Access


Microsoft Tunnel Gateway Architecture
B
Azure AD
A
Intune
1
Web Page
I
3
2
4
5
6.a
Management Agent
C.2
H
Corp Network
E
6.b
Load Balancer
C.1
C.3
Auth Plugin
D
F
MS Tunnel Server & Agent Containers
Linux Running Docker | Podman | NAT'd IPs
G
7
Proxy

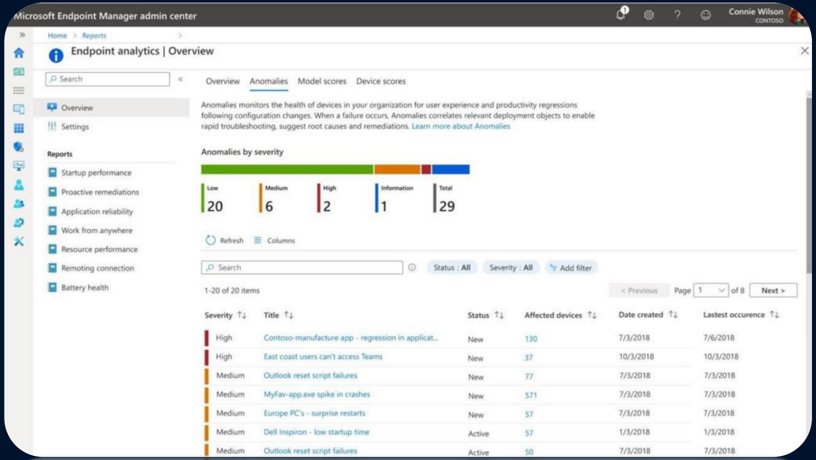
nic Cloud Connect

Advanced Endpoint Analytics

Microsoft Intune Suite

Advanced Endpoint Analytics

- A set of analytics-driven capabilities that help IT admins understand, anticipate, and improve end-user experiences.
- Initial features include customer device scopes, anomaly detection, and device timelines for troubleshooting.



Endpoint analytics | Overview

Anomalies monitors the health of devices in your organization for user experience and productivity regressions following configuration changes. When a failure occurs, Anomalies correlates relevant deployment objects to enable rapid troubleshooting, suggest root causes and remediations. Learn more about Anomalies

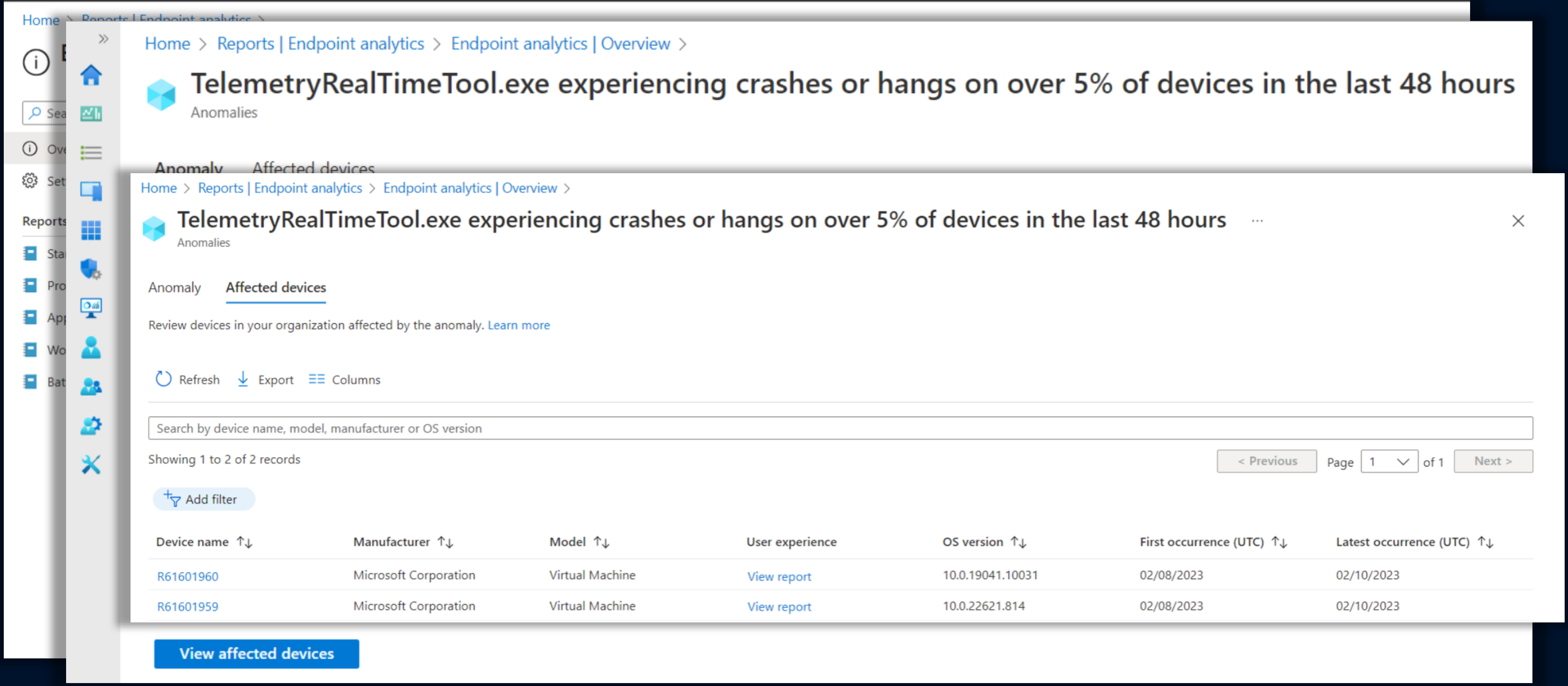
Anomalies by severity

Low	Medium	High	Information	Total
20	6	2	1	29

1-20 of 20 items

Severity ↑↓	Title ↑↓	Status ↑↓	Affected devices ↑↓	Date created ↑↓	Lastest occurence ↑↓
High	Contoso-manufacture app - regression in applicat...	New	130	7/3/2018	7/6/2018
High	East coast users can't access Teams	New	37	10/3/2018	10/3/2018
Medium	Outlook reset script failures	New	77	7/3/2018	7/3/2018
Medium	MyFav-app.exe spike in crashes	New	571	7/3/2018	7/3/2018
Medium	Europe PC's - surprise restarts	New	57	7/3/2018	7/3/2018
Medium	Dell Inspiron - low startup time	Active	57	1/3/2018	1/3/2018
Medium	Outlook reset script failures	Active	50	7/3/2018	7/3/2018

Anomaly Detection



Home > Reports | Endpoint analytics > Endpoint analytics | Overview >

TelemetryRealTimeTool.exe experiencing crashes or hangs on over 5% of devices in the last 48 hours

Anomalies

Anomaly Affected devices

Home > Reports | Endpoint analytics > Endpoint analytics | Overview >

TelemetryRealTimeTool.exe experiencing crashes or hangs on over 5% of devices in the last 48 hours ···

Anomalies

Anomaly Affected devices

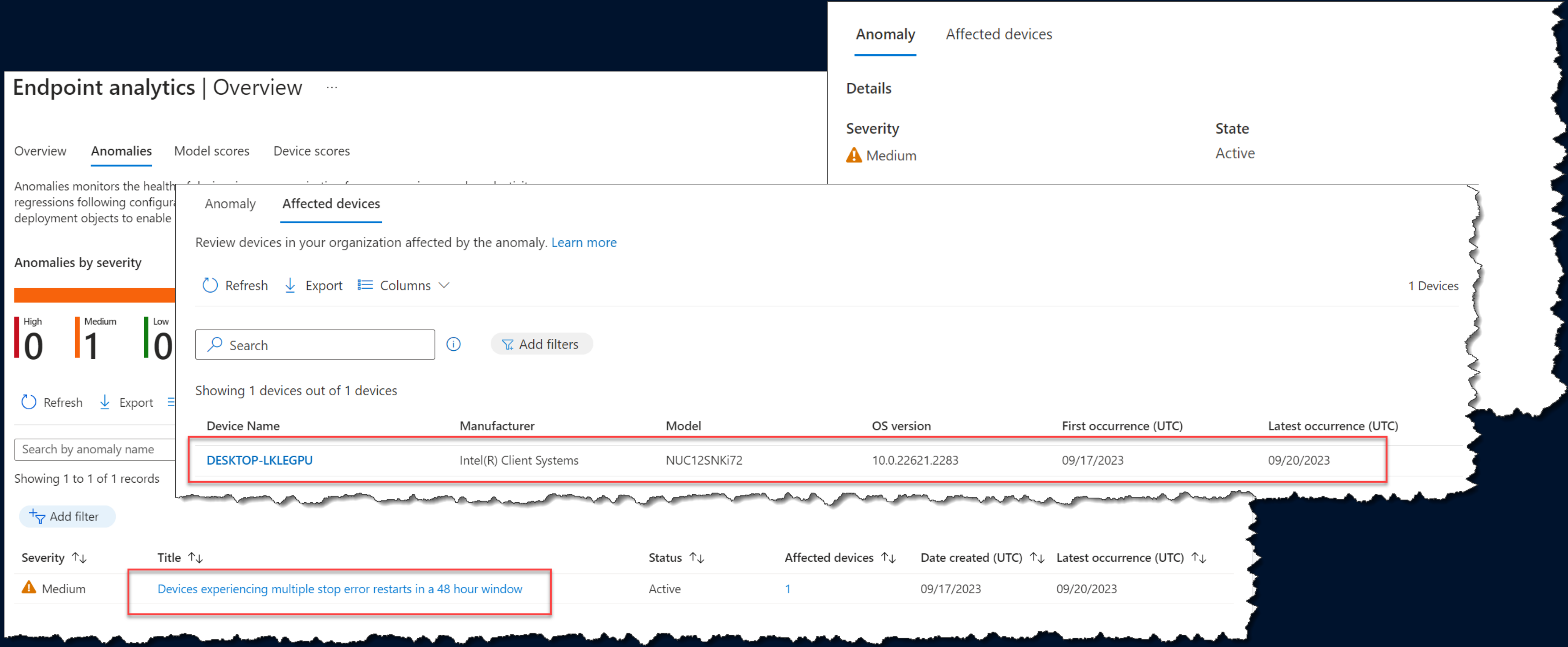
Review devices in your organization affected by the anomaly. Learn more

Search by device name, model, manufacturer or OS version

Showing 1 to 2 of 2 records

Device name ↑↓	Manufacturer ↑↓	Model ↑↓	User experience	OS version ↑↓	First occurrence (UTC) ↑↓	Latest occurrence (UTC) ↑↓
R61601960	Microsoft Corporation	Virtual Machine	View report	10.0.19041.10031	02/08/2023	02/10/2023
R61601959	Microsoft Corporation	Virtual Machine	View report	10.0.22621.814	02/08/2023	02/10/2023

Advanced Endpoint Analytics (Anomalies)



Endpoint analytics | Overview ···

Anomalies monitors the health
regressions following configura
deployment objects to enable

Anomalies by severity

High	Medium	Low
0	1	0

Showing 1 to 1 of 1 records

Severity ↑↓	Title ↑↓	Status ↑↓	Affected devices ↑↓	Date created (UTC) ↑↓	Latest occurrence (UTC) ↑↓
⚠ Medium	Devices experiencing multiple stop error restarts in a 48 hour window	Active	1	09/17/2023	09/20/2023

Details

Severity: ⚠ Medium

State: Active

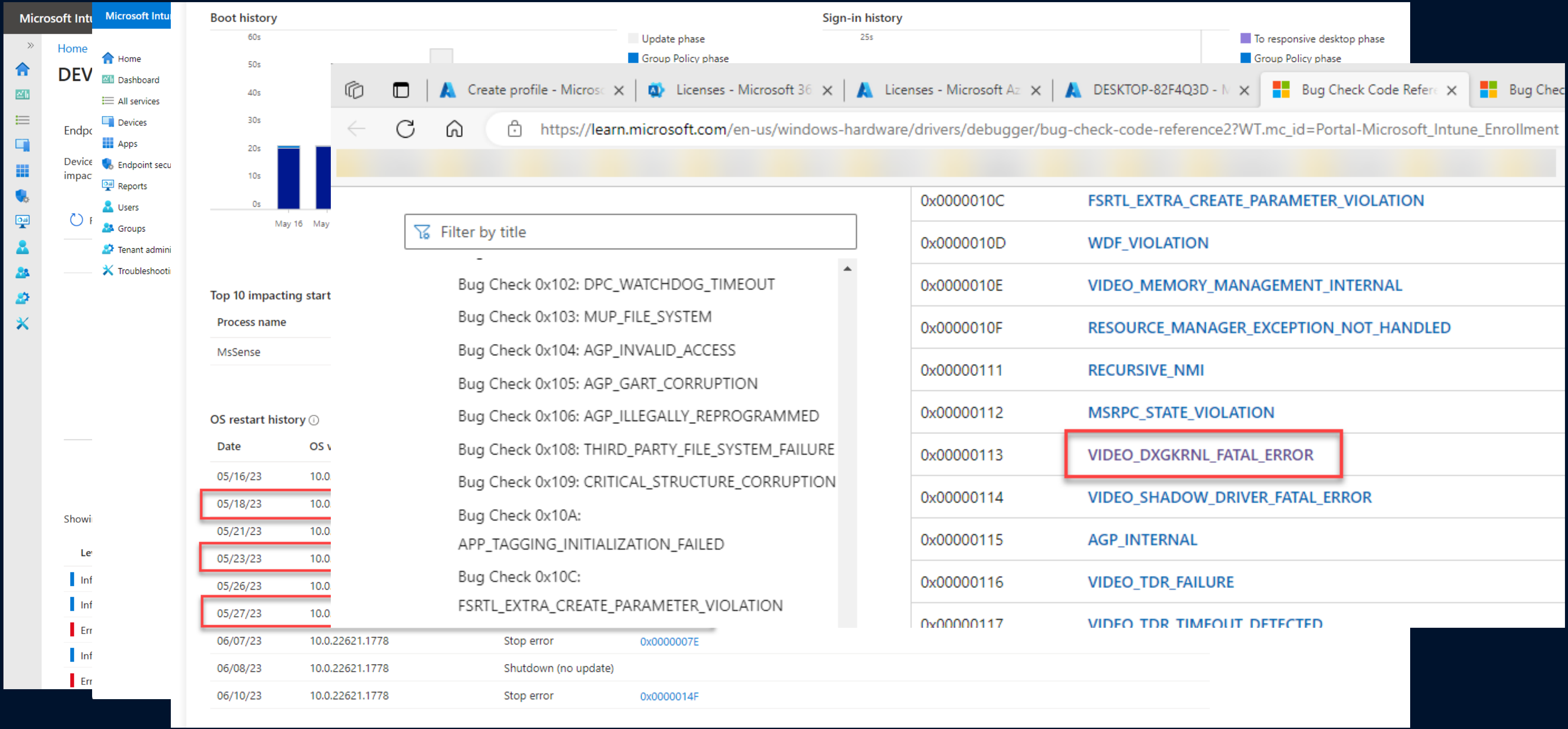
Review devices in your organization affected by the anomaly. Learn more

1 Devices

Showing 1 devices out of 1 devices

Device Name	Manufacturer	Model	OS version	First occurrence (UTC)	Latest occurrence (UTC)
DESKTOP-LKLEGPU	Intel(R) Client Systems	NUC12SNKi72	10.0.22621.2283	09/17/2023	09/20/2023

Enhanced Device Timeline



https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/bug-check-code-reference2?WT.mc_id=Portal-Microsoft_Intune_Enrollment

Bug Check 0x102: DPC_WATCHDOG_TIMEOUT
Bug Check 0x103: MUP_FILE_SYSTEM
Bug Check 0x104: AGP_INVALID_ACCESS
Bug Check 0x105: AGP_GART_CORRUPTION
Bug Check 0x106: AGP_ILLEGALLY_REPROGRAMMED
Bug Check 0x108: THIRD_PARTY_FILE_SYSTEM_FAILURE
Bug Check 0x109: CRITICAL_STRUCTURE_CORRUPTION
Bug Check 0x10A: APP_TAGGING_INITIALIZATION_FAILED
Bug Check 0x10C: FSRTL_EXTRA_CREATE_PARAMETER_VIOLATION

0x0000010C	FSRTL_EXTRA_CREATE_PARAMETER_VIOLATION
0x0000010D	WDF_VIOLATION
0x0000010E	VIDEO_MEMORY_MANAGEMENT_INTERNAL
0x0000010F	RESOURCE_MANAGER_EXCEPTION_NOT_HANDLED
0x00000111	RECURSIVE_NMI
0x00000112	MSRPC_STATE_VIOLATION
0x00000113	VIDEO_DXGKRNL_FATAL_ERROR
0x00000114	VIDEO_SHADOW_DRIVER_FATAL_ERROR
0x00000115	AGP_INTERNAL
0x00000116	VIDEO_TDR_FAILURE
0x00000117	VIDEO_TDR_TIMEOUT_DETECTED

OS restart history ⓘ

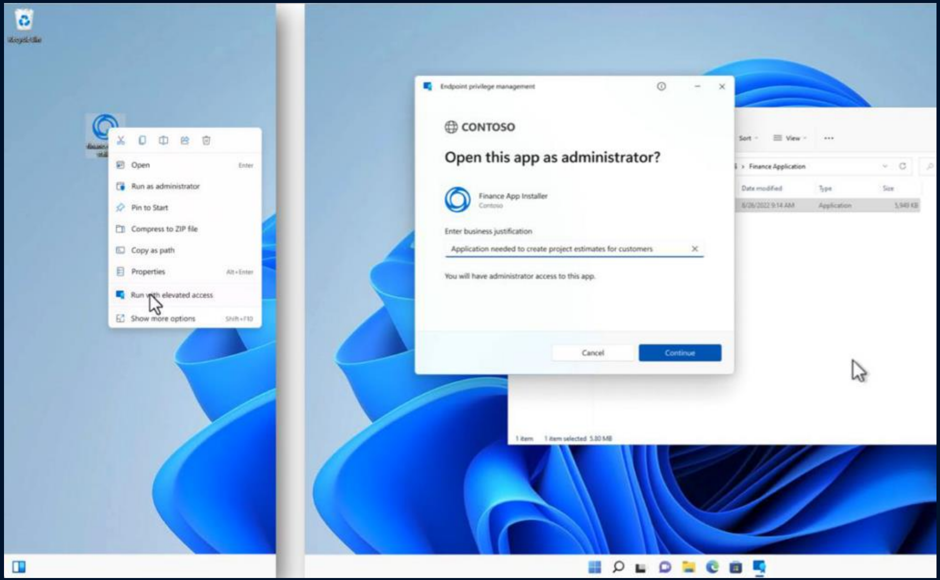
Date	OS v		
05/16/23	10.0		
05/18/23	10.0		
05/21/23	10.0		
05/23/23	10.0		
05/26/23	10.0		
05/27/23	10.0		
06/07/23	10.0.22621.1778	Stop error	0x0000007E
06/08/23	10.0.22621.1778	Shutdown (no update)	
06/10/23	10.0.22621.1778	Stop error	0x0000014F

Endpoint Privilege Management

Microsoft Intune Suite

Endpoint Privilege Management (EPM)

- Generally available!
- Intune add-ons
  - View the licensing options for EPM
- Free Trial
  - Up to 250 users for 90 days.



Open this app as administrator?

Enter business justification

Application needed to create project estimates for customers

You will have administrator access to this app.

Getting started with EPM

High-level process

- License Endpoint Privilege Management
- Deploy an elevation settings policy
  - Send elevation data for reporting
  - Reporting scope: Diagnostic data and all endpoint elevations
  - Default elevation response: Require user confirmation
  - Validation: Business justification
- Collection data
- Build and Deploy elevation rule policies

Start Now

Cloud Connect

Microsoft Intune Suite

Comming soon...

Cloud-based Certificate Management

- A cloud certificate management solution
  - Issue and manage VPN and Wi-Fi certificates from Intune to devices without on-premises infrastructure.
  - We expect to see more scenarios in the future…

- Release date: TBA - Most likely announed next week at Ignite!

https://www.microsoft.com/en-us/security/blog/2023/03/01/the-microsoft-intune-suite-fuels-cyber-safety-and-it-efficiency/

Advanced Application Management

- An enterprise catalog of applications that are easily accessible.
- Provides application update capabilities.

<u>Expected Release</u>:

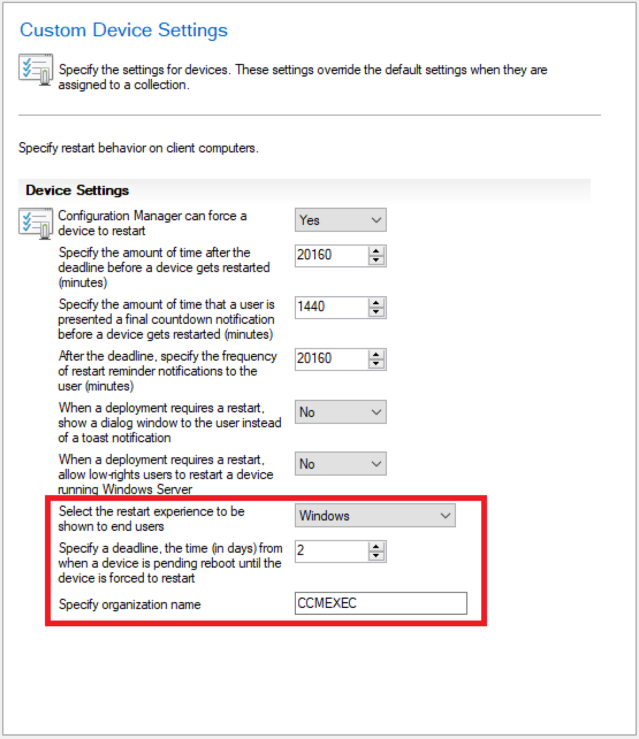
- The enterprise catalog
  - Available in public preview this year
- The application update capabilities
  - Available early 2024.

- More information next week (we hope) ☺

What’s new in Configuration manager 2309

Windows Update restart notification

- One of our favorite features now with Configuration Manager



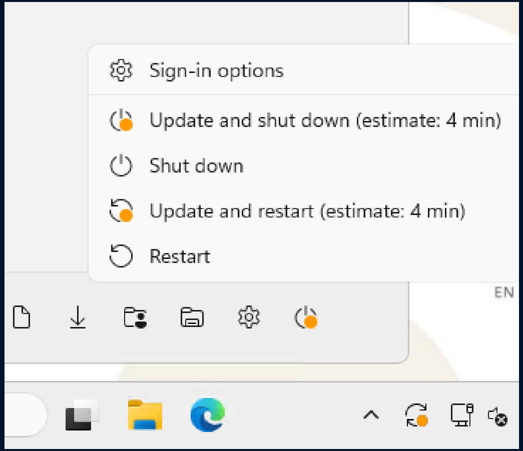
Custom Device Settings

Specify the settings for devices. These settings override the default settings when they are assigned to a collection.

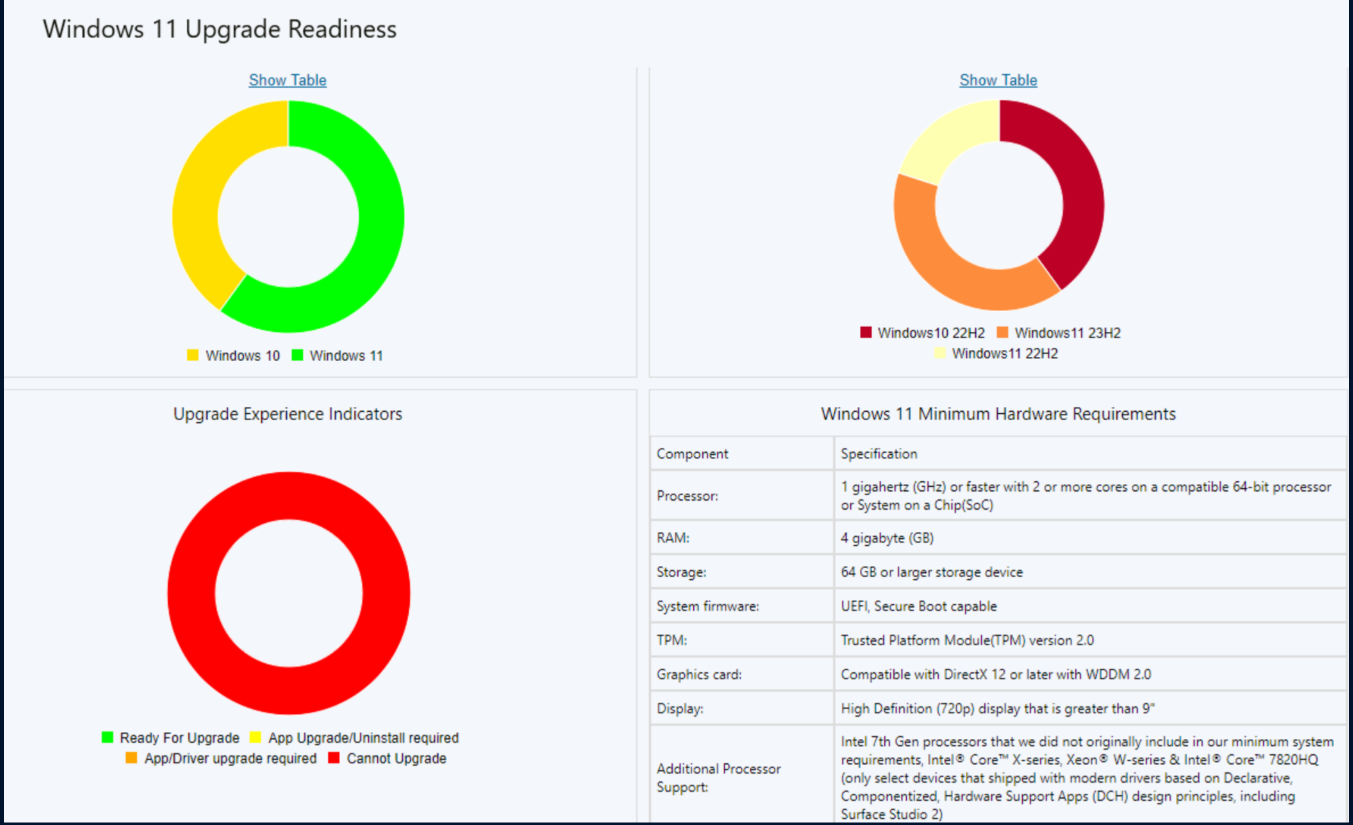
Specify restart behavior on client computers.

Device Settings

Configuration Manager can force a device to restart	Yes
Specify the amount of time after the deadline before a device gets restarted (minutes)	20160
Specify the amount of time that a user is presented a final countdown notification before a device gets restarted (minutes)	1440
After the deadline, specify the frequency of restart reminder notifications to the user (minutes)	20160
When a deployment requires a restart, show a dialog window to the user instead of a toast notification	No
When a deployment requires a restart, allow low-rights users to restart a device running Windows Server	No
Select the restart experience to be shown to end users	Windows
Specify a deadline, the time (in days) from when a device is pending reboot until the device is forced to restart	2
Specify organization name	CCMEXEC


Sign-in options
Update and shut down (estimate: 4 min)
Shut down
Update and restart (estimate: 4 min)
Restart
EN

Windows 11 Upgrade readiness Dashboard



Windows 11 Upgrade Readiness

Show Table

🟨 Windows 10 🟩 Windows 11

Show Table

🟥 Windows10 22H2 🟧 Windows11 23H2
🟨 Windows11 22H2

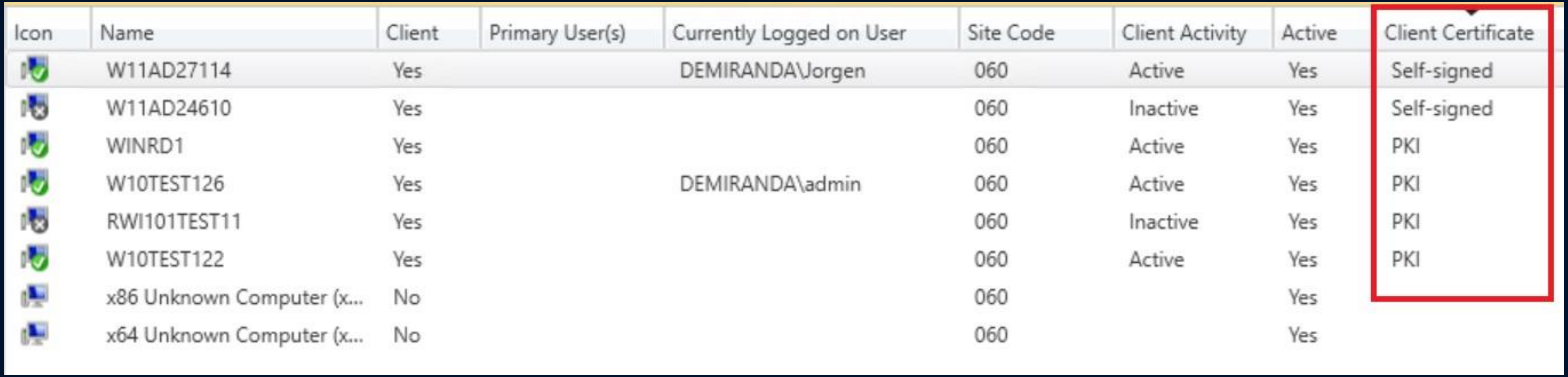
Upgrade Experience Indicators

🟩 Ready For Upgrade 🟨 App Upgrade/Uninstall required
🟧 App/Driver upgrade required 🟥 Cannot Upgrade

Windows 11 Minimum Hardware Requirements

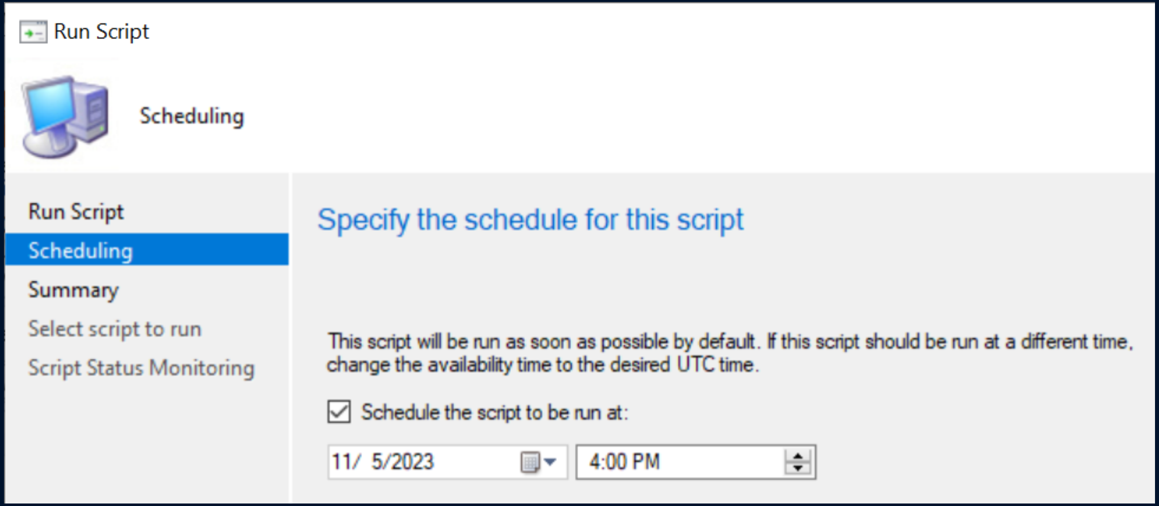
Component	Specification
Processor:	1 gigahertz (GHz) or faster with 2 or more cores on a compatible 64-bit processor or System on a Chip(SoC)
RAM:	4 gigabyte (GB)
Storage:	64 GB or larger storage device
System firmware:	UEFI, Secure Boot capable
TPM:	Trusted Platform Module(TPM) version 2.0
Graphics card:	Compatible with DirectX 12 or later with WDDM 2.0
Display:	High Definition (720p) display that is greater than 9"
Additional Processor Support:	Intel 7th Gen processors that we did not originally include in our minimum system requirements, Intel® Core™ X-series, Xeon® W-series & Intel® Core™ 7820HQ (only select devices that shipped with modern drivers based on Declarative, Componentized, Hardware Support Apps (DCH) design principles, including Surface Studio 2)

Client certificate shows correct information



Icon	Name	Client	Primary User(s)	Currently Logged on User	Site Code	Client Activity	Active	Client Certificate
✓	W11AD27114	Yes		DEMIRANDA\Jorgen	060	Active	Yes	Self-signed
✕	W11AD24610	Yes			060	Inactive	Yes	Self-signed
✓	WINRD1	Yes			060	Active	Yes	PKI
✓	W10TEST126	Yes		DEMIRANDA\admin	060	Active	Yes	PKI
✕	RWI101TEST11	Yes			060	Inactive	Yes	PKI
✓	W10TEST122	Yes			060	Active	Yes	PKI
	x86 Unknown Computer (x...	No			060		Yes	
	x64 Unknown Computer (x...	No			060		Yes	

Schedule Run script



Run Script

Scheduling

Specify the schedule for this script

This script will be run as soon as possible by default. If this script should be run at a different time, change the availability time to the desired UTC time.

☑ Schedule the script to be run at:

11/ 5/2023 4:00 PM

More news

- External service notification Run details from Azure Logic application
- New Site Maintenance task “Delete Aged Task Execution Status Messages”
- Maintenance window creation using PS cmdlet
- OSD preferred MP option for PXE boot scenario
- Enable Bitlocker through ProvisionTS
- Windows 11 Edition Upgrade using CM Policy settings
- Attack Surface Reduction (ASR) capability now marks Server SKU as compliant only after enforcement

Windows LAPS!

Benefits of using Windows LAPS

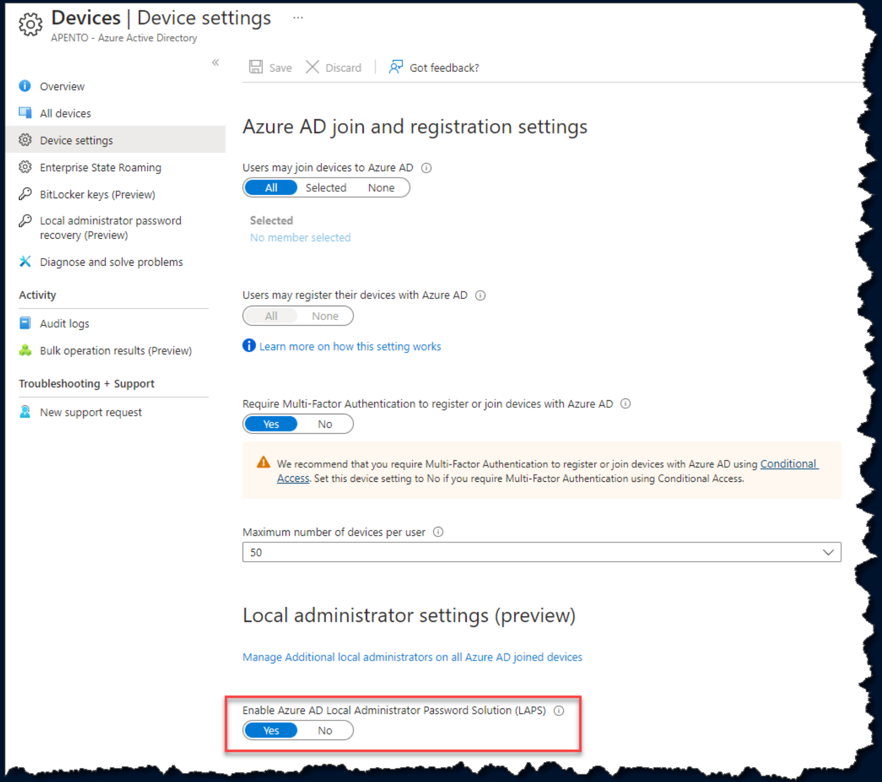
- Protection against pass-the-hash and lateral-traversal attacks

- Improved security for remote help desk scenarios

- Ability to sign in to and recover devices that are otherwise inaccessible

Enabling Windows LAPS with Azure AD

- Tenant wide configuration
- Cloud Device Administrator



Devices | Device settings ···
APENTO - Azure Active Directory
«
Save
Discard
Got feedback?
Overview
All devices
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Local administrator password recovery (Preview)
Diagnose and solve problems
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request

Azure AD join and registration settings

Users may join devices to Azure AD ⓘ
[✓ All] Selected None

Selected
No member selected

Users may register their devices with Azure AD ⓘ
All None

Learn more on how this setting works

Require Multi-Factor Authentication to register or join devices with Azure AD ⓘ
[✓ Yes] No

⚠ We recommend that you require Multi-Factor Authentication to register or join devices with Azure AD using Conditional Access. Set this device setting to No if you require Multi-Factor Authentication using Conditional Access.

Maximum number of devices per user ⓘ
50

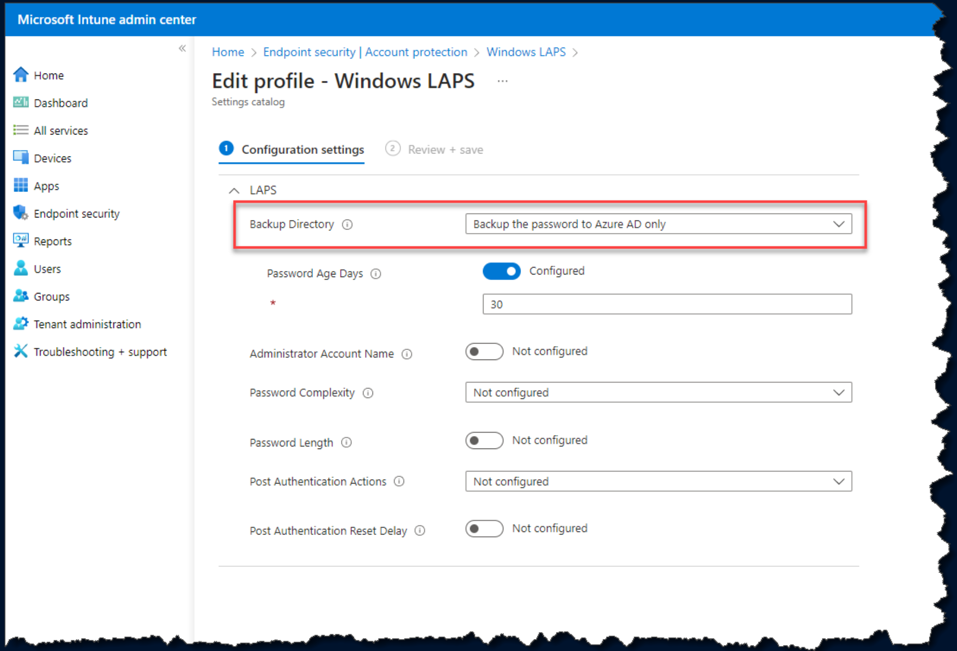
Local administrator settings (preview)

Manage Additional local administrators on all Azure AD joined devices

Enable Azure AD Local Administrator Password Solution (LAPS) ⓘ
[✓ Yes] No

Client-side configuration/policy

- Microsoft Intune
- Set the **BackUpDirectory** to be **Azure AD**.



Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Account protection > Windows LAPS >

Edit profile - Windows LAPS

Settings catalog

1 Configuration settings 2 Review + save

LAPS

Backup Directory: Backup the password to Azure AD only

Password Age Days: Configured

* 30

Administrator Account Name: Not configured

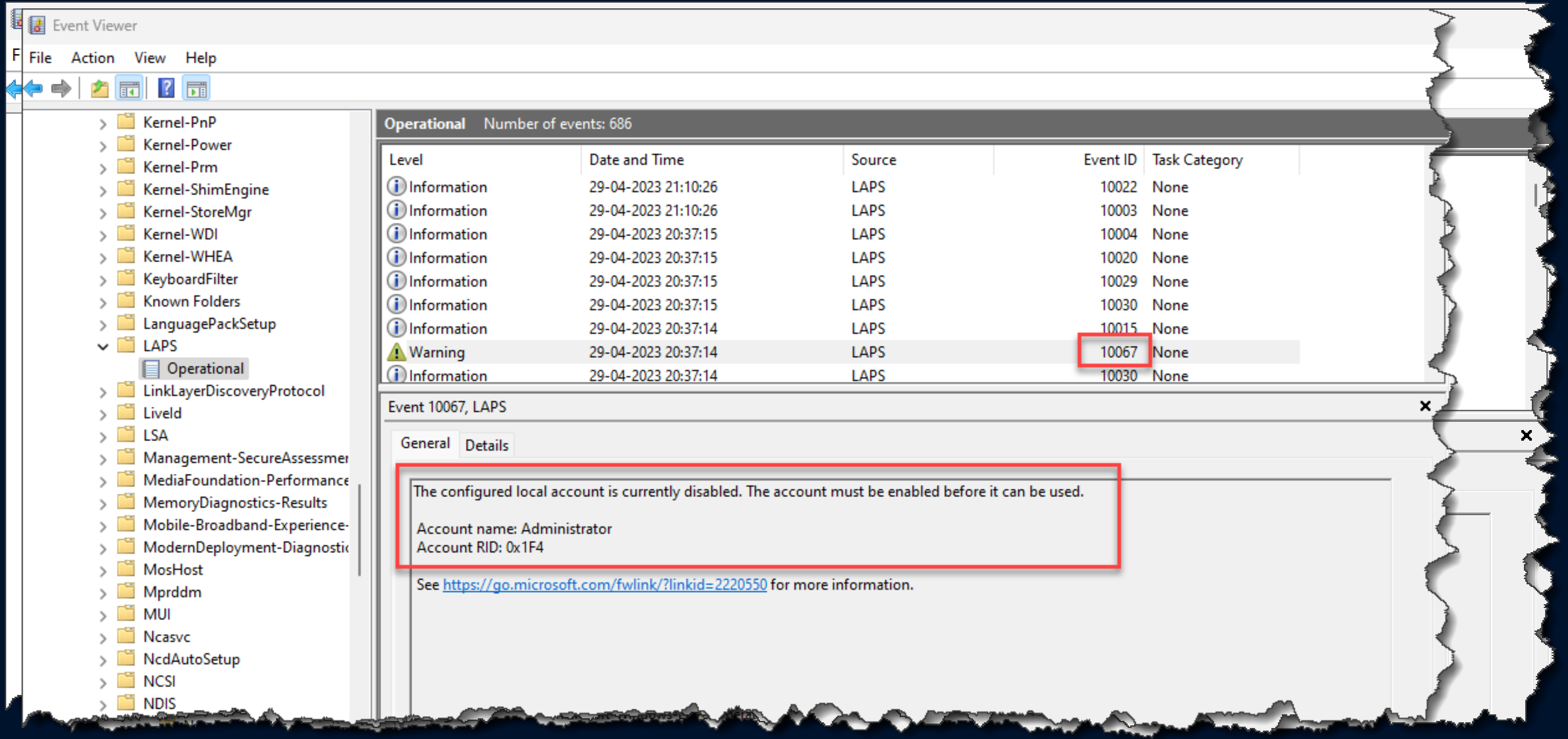
Password Complexity: Not configured

Password Length: Not configured

Post Authentication Actions: Not configured

Post Authentication Reset Delay: Not configured

Event Viewer



Operational Number of events: 686

Level	Date and Time	Source	Event ID	Task Category
Information	29-04-2023 21:10:26	LAPS	10022	None
Information	29-04-2023 21:10:26	LAPS	10003	None
Information	29-04-2023 20:37:15	LAPS	10004	None
Information	29-04-2023 20:37:15	LAPS	10020	None
Information	29-04-2023 20:37:15	LAPS	10029	None
Information	29-04-2023 20:37:15	LAPS	10030	None
Information	29-04-2023 20:37:14	LAPS	10015	None
Warning	29-04-2023 20:37:14	LAPS	10067	None
Information	29-04-2023 20:37:14	LAPS	10030	None

Event 10067, LAPS

The configured local account is currently disabled. The account must be enabled before it can be used.

Account name: Administrator
Account RID: 0x1F4

See https://go.microsoft.com/fwlink/?linkid=2220550 for more information.

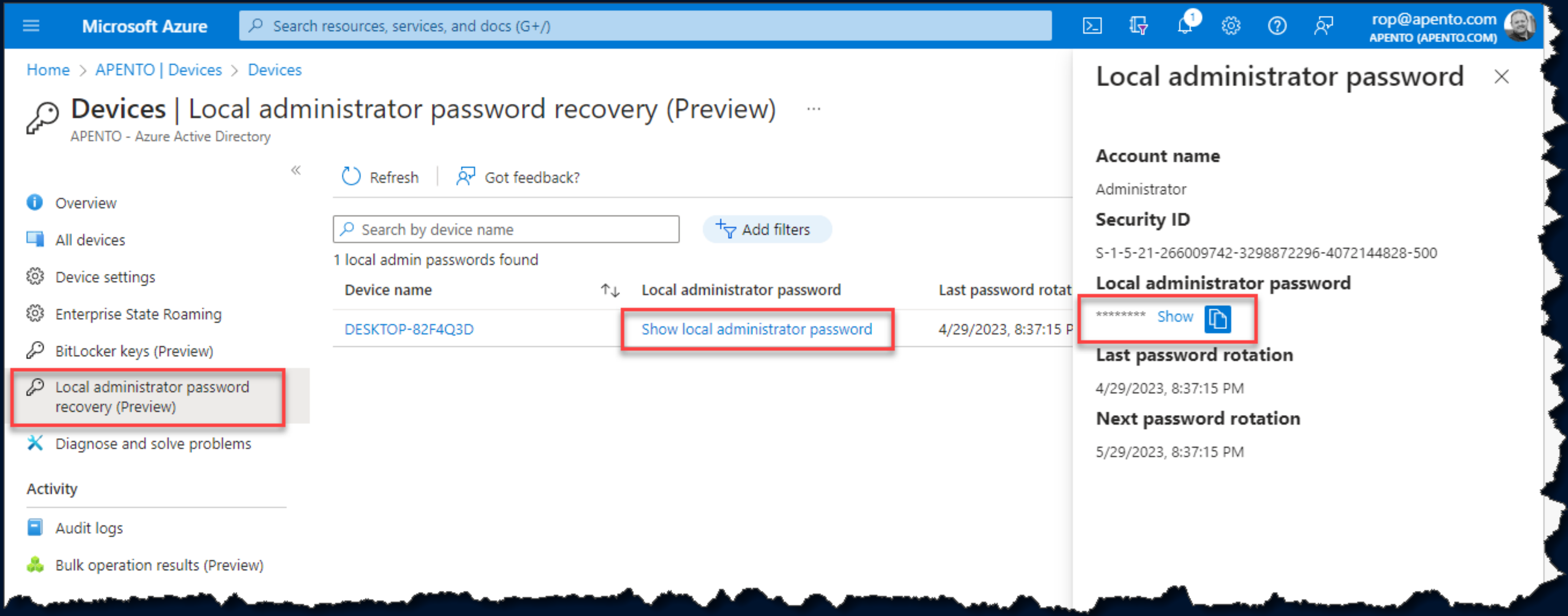
Recovering local admin password

- To view the local administrator password, you must be granted the **deviceLocalCredentials.Read.All** permission, and you must be assigned one of the following roles:

- Cloud Device Administrator
- Intune Service Administrator
- Global Administrator

List all Windows LAPS enable devices

- To list all Windows LAPS enabled devices in Azure AD, you can browse to **Azure Active Directory > Devices > Local administrator password recovery (Preview).**



Home > APENTO | Devices > Devices

Devices | Local administrator password recovery (Preview)

APENTO - Azure Active Directory

1 local admin passwords found

Device name	Local administrator password	Last password rotat
DESKTOP-82F4Q3D	Show local administrator password	4/29/2023, 8:37:15 P

Local administrator password

Account name

Administrator

Security ID

S-1-5-21-266009742-3298872296-4072144828-500

Local administrator password

******** Show

Last password rotation

4/29/2023, 8:37:15 PM

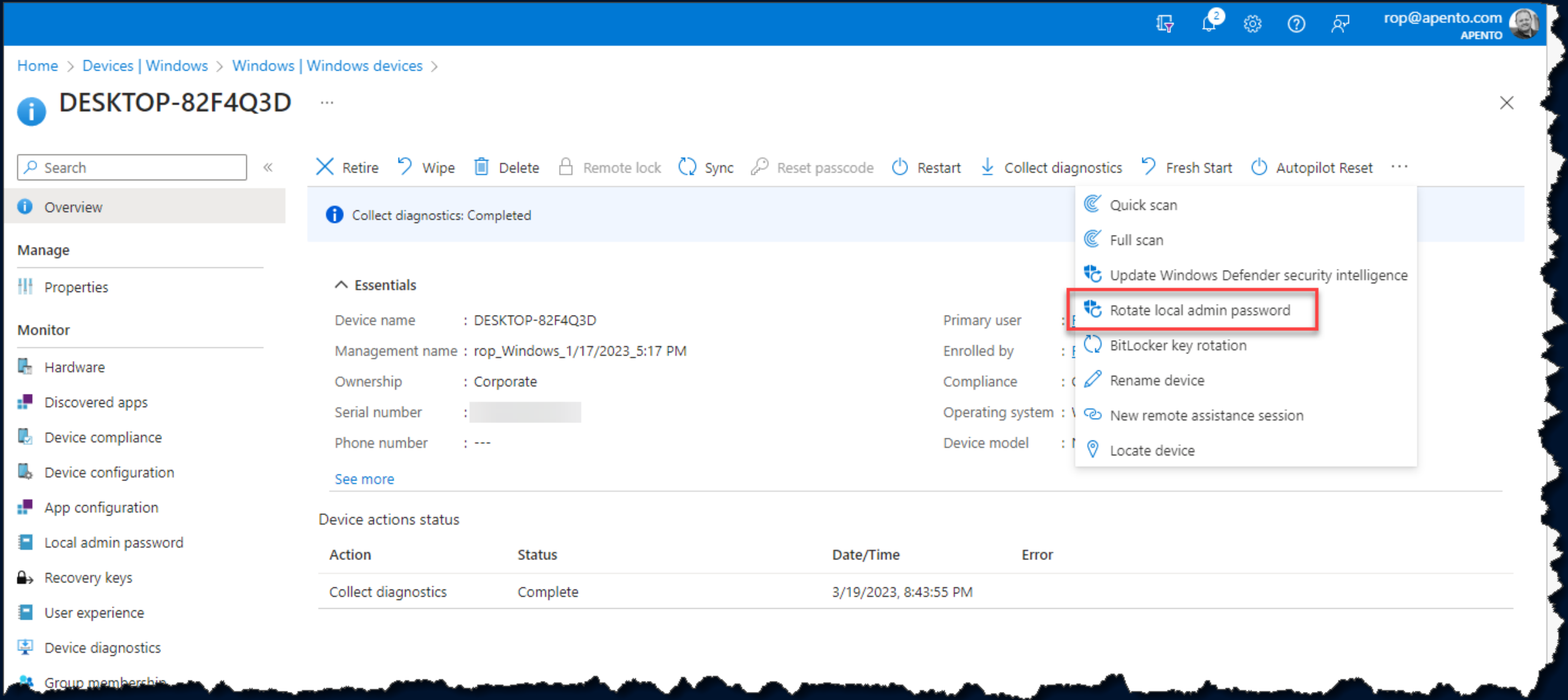
Next password rotation

5/29/2023, 8:37:15 PM

nic Cloud Connect

Reset local administrator password

- Microsoft Intune Admin Center



DESKTOP-82F4Q3D ...

Collect diagnostics: Completed

Essentials

Device name : DESKTOP-82F4Q3D
Management name : rop_Windows_1/17/2023_5:17 PM
Ownership : Corporate
Serial number : [redacted]
Phone number : ---

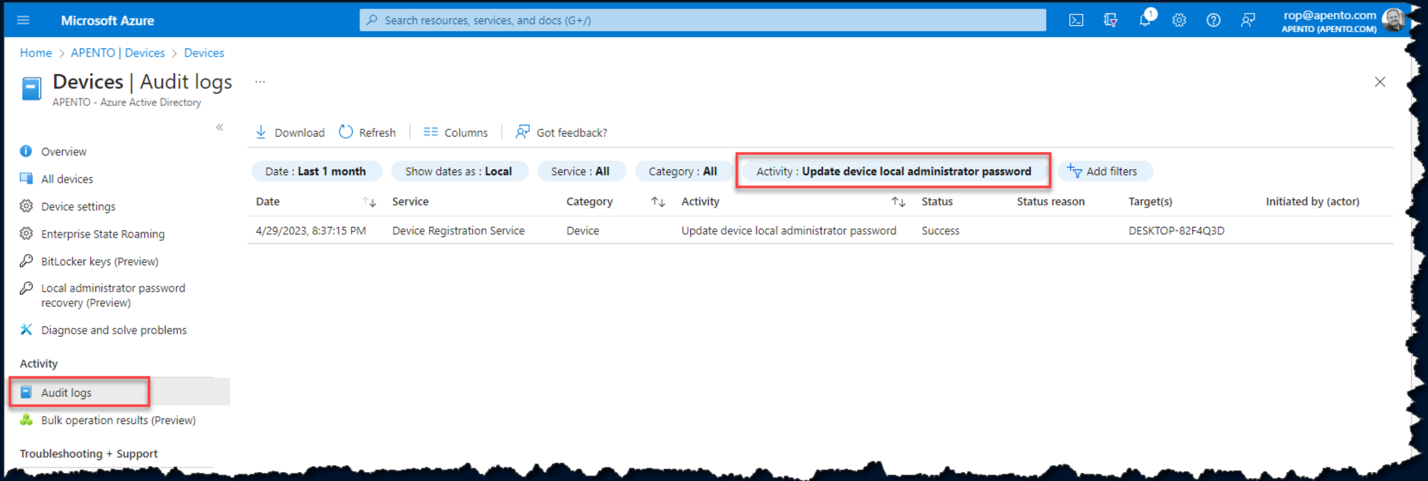
Primary user : F
Enrolled by : F
Compliance : C
Operating system : V
Device model : M

Device actions status

Action	Status	Date/Time	Error
Collect diagnostics	Complete	3/19/2023, 8:43:55 PM	

Audit Password Update and Recovery

- To view audit events, you can browse to:
  - Azure Active Directory > Devices > Audit logs
- Then use the **Activity filter** and search for:
  - “Update device local administrator password”
  - “Recover device local administrator password”



Home > APENTO | Devices > Devices

Devices | Audit logs

APENTO - Azure Active Directory

Date : **Last 1 month** | Show dates as : **Local** | Service : **All** | Category : **All** | Activity : **Update device local administrator password**

Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated by (actor)
4/29/2023, 8:37:15 PM	Device Registration Service	Device	Update device local administrator password	Success		DESKTOP-82F4Q3D	

Conditional Access policies for LAPS recovery

- Conditional Access policies can be scoped to the built-in roles like Cloud Device Administrator, Intune Administrator, and Global Administrator to protect access to recover local administrator passwords.

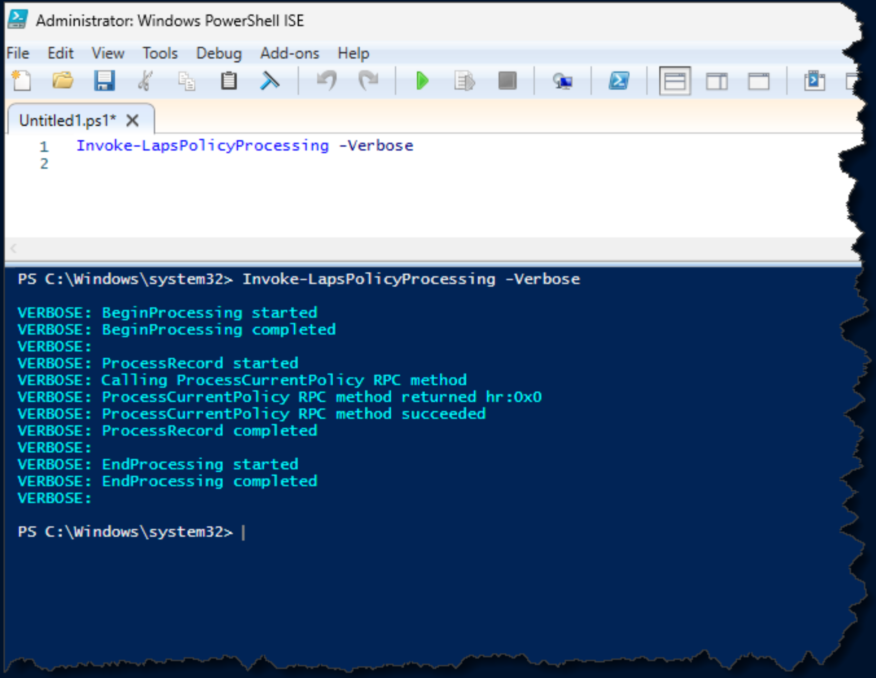
- You can find an example of a policy that requires multifactor authentication in the article, Common Conditional Access policy: Require MFA for administrators.

What happens when a device is deleted in Azure AD?

- When a device is deleted in Azure AD, the LAPS credential that was tied to that device is lost and the password that is stored in Azure AD is lost.

- Unless you have a custom workflow to retrieve LAPS passwords and store them externally, there’s no method in Azure AD to recover the LAPS managed password for a deleted device.

PowerShell / Windows LAPS



Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1*

```
Invoke-LapsPolicyProcessing -Verbose
```

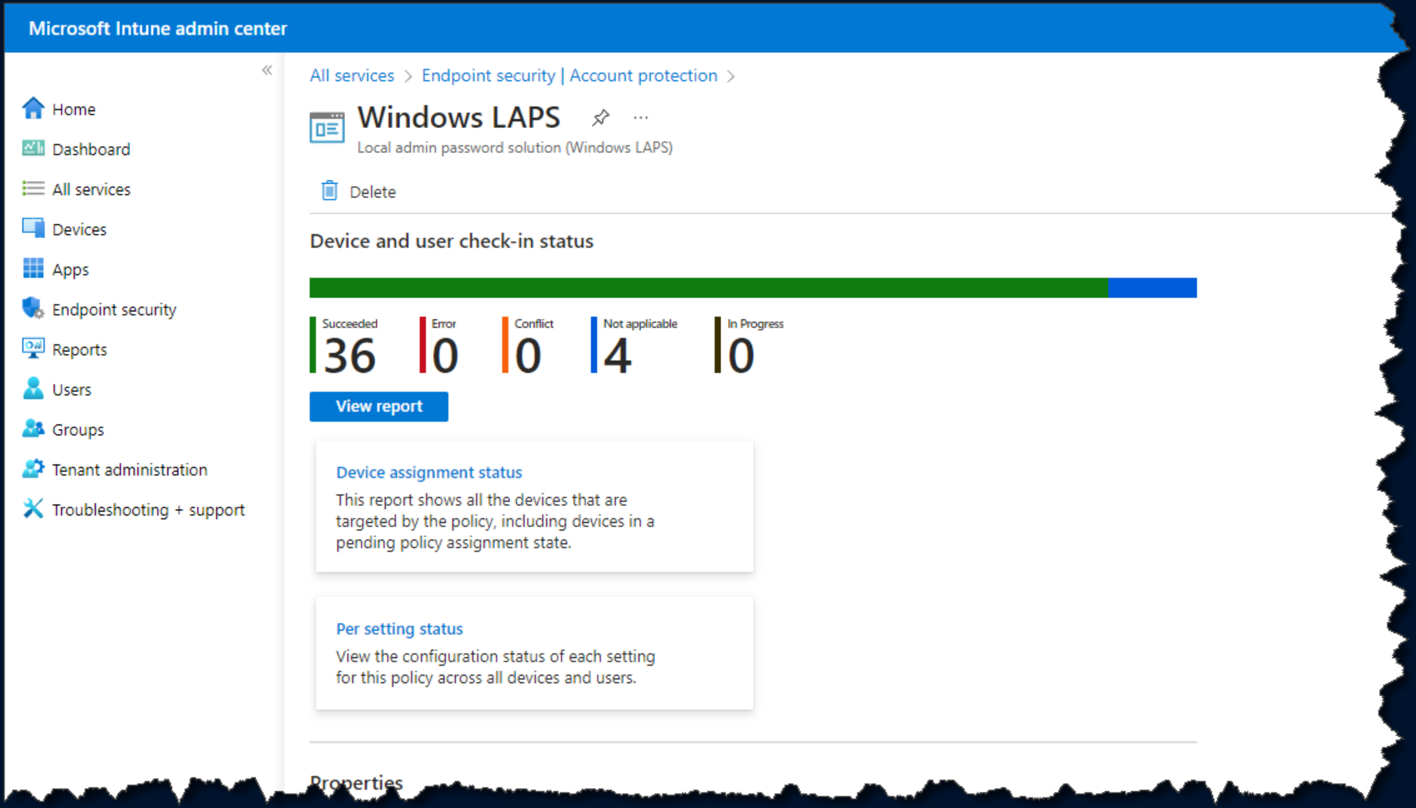
```
PS C:\Windows\system32> Invoke-LapsPolicyProcessing -Verbose

VERBOSE: BeginProcessing started
VERBOSE: BeginProcessing completed
VERBOSE:
VERBOSE: ProcessRecord started
VERBOSE: Calling ProcessCurrentPolicy RPC method
VERBOSE: ProcessCurrentPolicy RPC method returned hr:0x0
VERBOSE: ProcessCurrentPolicy RPC method succeeded
VERBOSE: ProcessRecord completed
VERBOSE:
VERBOSE: EndProcessing started
VERBOSE: EndProcessing completed
VERBOSE:

PS C:\Windows\system32> |
```

https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-scenarios-azure-active-directory

Using Microsoft Intune for Windows LAPS Management



Microsoft Intune admin center

All services > Endpoint security | Account protection >

Windows LAPS

Local admin password solution (Windows LAPS)

Device and user check-in status

Succeeded	Error	Conflict	Not applicable	In Progress
36	0	0	4	0

Device assignment status

This report shows all the devices that are targeted by the policy, including devices in a pending policy assignment state.

Per setting status

View the configuration status of each setting for this policy across all devices and users.

Properties

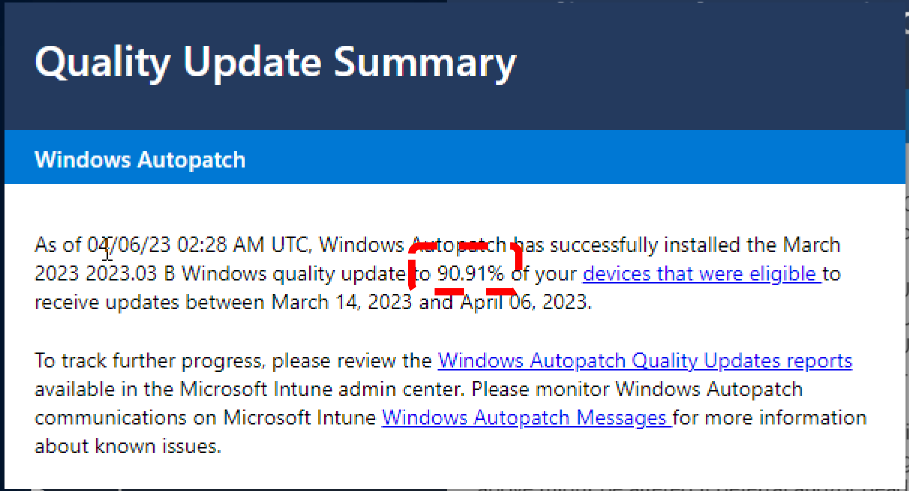
nic Cloud Connect

Windows Autopach

Windows Autopatch

Quality Update Schedule Notifications

- Test group:
- Broad group
  - Offered on: November 23
  - Deadline: November 28

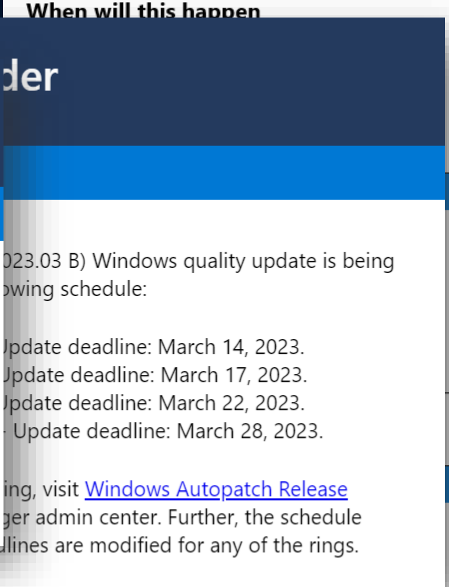


Quality Update Summary

Windows Autopatch

As of 04/06/23 02:28 AM UTC, Windows Autopatch has successfully installed the March 2023 2023.03 B Windows quality update to 90.91% of your devices that were eligible to receive updates between March 14, 2023 and April 06, 2023.

To track further progress, please review the Windows Autopatch Quality Updates reports available in the Microsoft Intune admin center. Please monitor Windows Autopatch communications on Microsoft Intune Windows Autopatch Messages for more information about known issues.

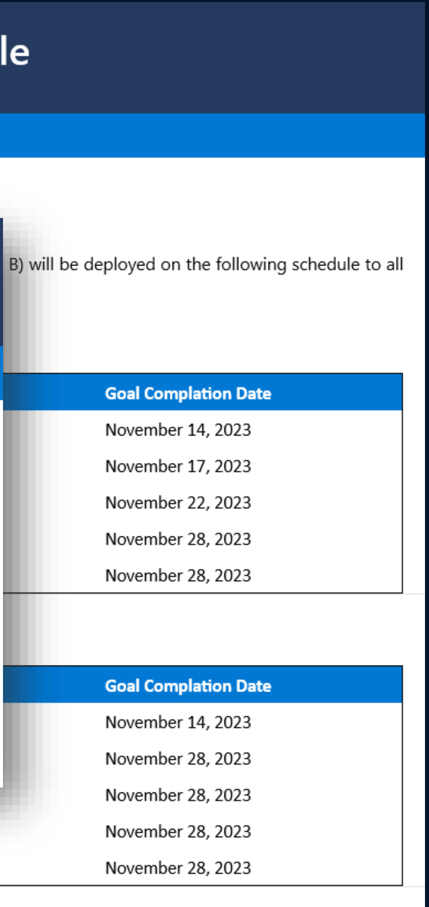


der

023.03 B) Windows quality update is being
owing schedule:

Update deadline: March 14, 2023.
Update deadline: March 17, 2023.
Update deadline: March 22, 2023.
Update deadline: March 28, 2023.

ing, visit Windows Autopatch Release
ger admin center. Further, the schedule
above might be altered if deferral and/or deadlines are modified for any of the rings.



Quality Update Schedule

Windows Autopatch

When will this happen

B) will be deployed on the following schedule to all

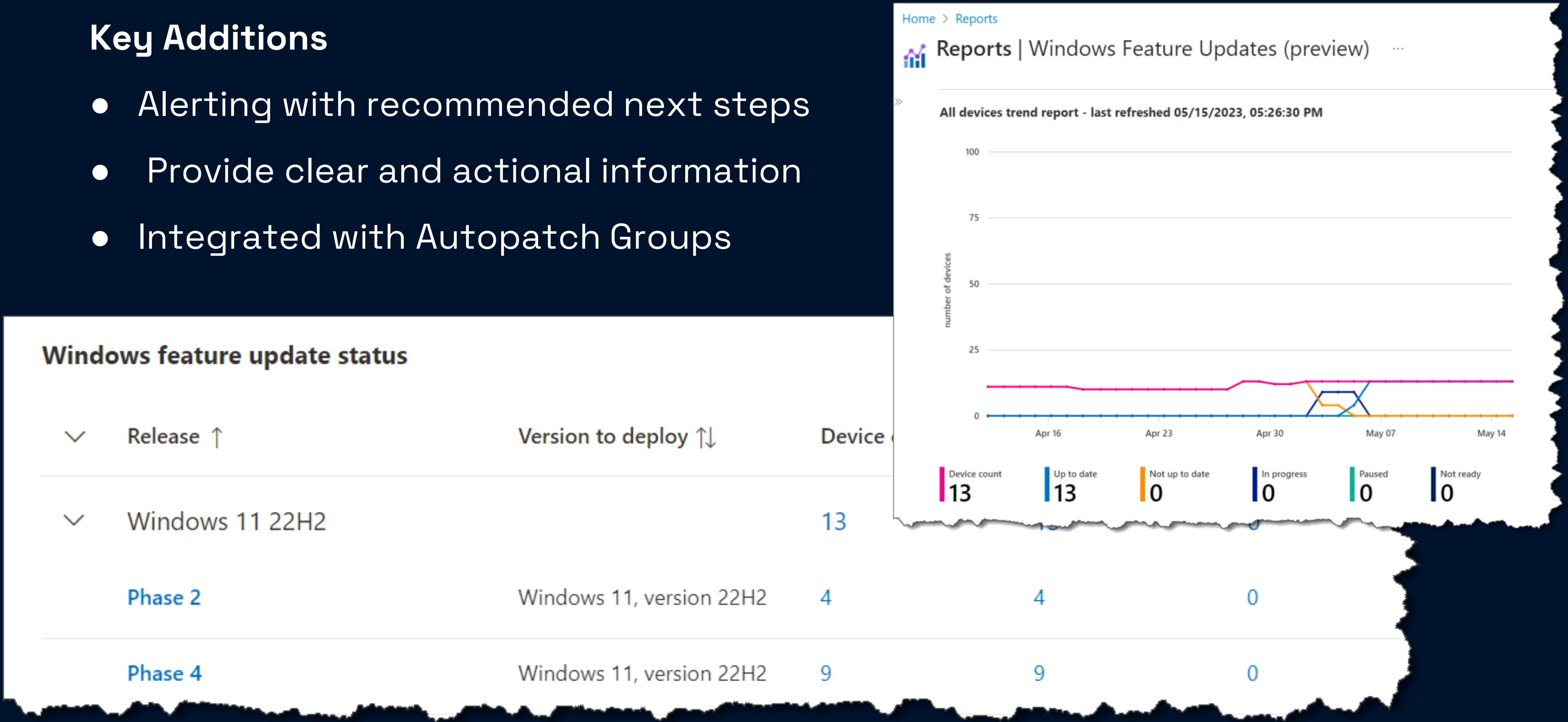
Goal Complation Date
November 14, 2023
November 17, 2023
November 22, 2023
November 28, 2023
November 28, 2023

		Goal Complation Date
		November 14, 2023
		November 28, 2023
Ring2	November 23, 2023	November 28, 2023
Ring3	November 23, 2023	November 28, 2023
Last	November 23, 2023	November 28, 2023

Windows Autopatch Reporting

Key Additions

- Alerting with recommended next steps
- Provide clear and actional information
- Integrated with Autopatch Groups



Home > Reports

Reports | Windows Feature Updates (preview)

All devices trend report - last refreshed 05/15/2023, 05:26:30 PM

Device count	Up to date	Not up to date	In progress	Paused	Not ready
13	13	0	0	0	0

Windows feature update status

Release ↑	Version to deploy ⇅	Device		
Windows 11 22H2		13		
Phase 2	Windows 11, version 22H2	4	4	0
Phase 4	Windows 11, version 22H2	9	9	0

What we learned during 2023

Windows 11 23H2 will be delivered as EKB

- Enablement packages are back!!
- Windows 11 22H2 –> 23H2

https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-client-roadmap-update-july-2023/ba-p/3871736

Windows 11 = Modern management, Cloud only

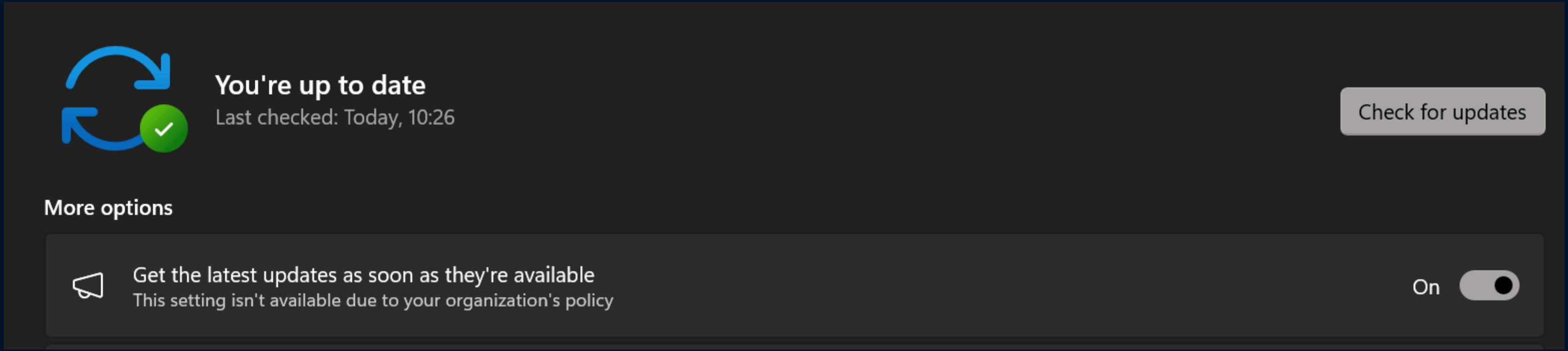
- We see 8 out of 10 Windows 11 projects includes the migration to Cloud Only

Driving factors:

- Windows Autopilot
- Work from Anywhere
- Driver/Firmware updates
- Security

Minimize risk by using the CU-preview release

- Released last Tuesday every month
- Includes all non-security related updates included in the coming CU
- Used way too little today!
- Deploy to your Pilot ring



You're up to date

Last checked: Today, 10:26

More options

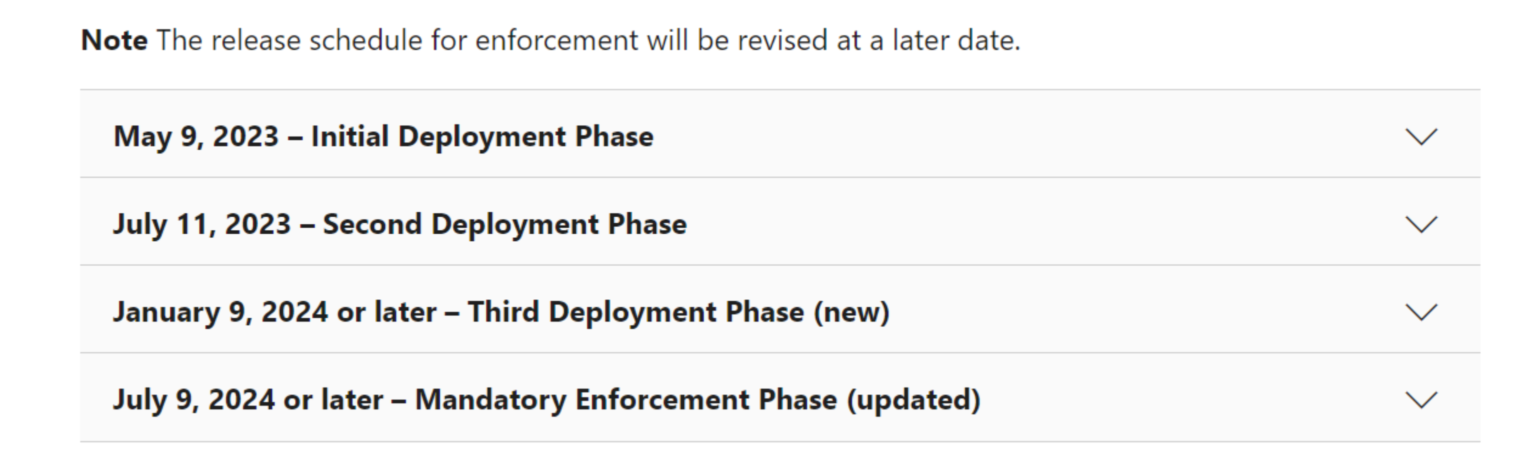
Get the latest updates as soon as they're available

This setting isn't available due to your organization's policy

On

CU which requires manual steps

- CVE-2023-21563 - January 2023 – BitLocker bypass
- CVE-2023-24932 - May 2023 – Secureboot bypass
- CVE-2023-32019 - June 2023 – Kernel vulnerability (enforced in August CU)



Note The release schedule for enforcement will be revised at a later date.

May 9, 2023 – Initial Deployment Phase

July 11, 2023 – Second Deployment Phase

January 9, 2024 or later – Third Deployment Phase (new)

July 9, 2024 or later – Mandatory Enforcement Phase (updated)

The year of the BitLocker PIN comeback

- BitLocker PIN made a comeback in 2023!
- Increases security
- Protects against, DMA, Physical, Memory and many more attack techniques.

https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/bitlocker-countermeasures

Summary of how to stay ahead of the game!

- Keep up and use the new features in Intune! All innovation is happening here!
- Start using the CU preview updates
- Use temporary feature control at least at IT to test what is coming
- Migrate to Windows LAPS! Legacy LAPS is deprecated!
- Use driver and firmware updates in Intune/WufB – Yes it works!
- Read through the CU – Knowledge base article each month – and take Action!
- Work with Secure Score – We are all in security now!