


Adelaide Microsoft IT Pro Community | July 2024

Modern Provisioning and Update Management for Windows Devices

It's a journey, not a battle!

 Jesper Nielsen

 @dotjesper



Slide 1 [00:00:00]

Walk-in

//

Deck information

Deck Title: **Modern Provisioning and Update Management for Windows Devices**

Deck Topic: **It's a journey, not a battle!**

Deck URL: <none>

Last updated: **July 2, 2024**

Speaker: **Jesper Nielsen**

Audience: **IT Professionals & Technical Staff**

Event: **Adelaide Microsoft IT Pro Community | July 2024**

Delivery time: **45 minutes**

Content level: **300**

Slide 2 [Hidden]

Deck information

//

Abstract

Windows devices are essential for many organizations and businesses, but they also pose challenges in terms of provisioning and update management. How can IT professionals and administrators streamline the process of deploying, configuring, and updating Windows devices, while ensuring security, compliance, and user satisfaction?

This session will explore the latest technologies and Best Practices for Modern Provisioning and Modern Update Management for Windows devices, focusing on the topics: Windows Autopilot, Windows Autopilot device preparation (Windows Autopilot 2.0), and Windows Autopatch.

Windows Autopilot: Windows Autopilot is a cloud-based service that simplifies the deployment and configuration of new Windows devices, without requiring IT staff to physically touch each device. Windows Autopilot allows IT professionals and administrators to create and assign device profiles, which specify the settings, policies, apps, and features that should be applied to each device, reducing the time and cost of provisioning Windows devices, while improving the user experience and the security posture of the organization.

Windows Autopilot device preparation: Windows Autopilot device preparation (Windows Autopilot 2.0) is used to set up and configure new devices, getting them ready for productive use. Windows Autopilot device preparation aims to simplify device deployment by delivering consistent configurations, enhancing the overall setup speed, and improving troubleshooting capabilities, without device pre-registering or added as a Windows Autopilot device. Windows Autopilot device preparation is an improved profile experience that incorporates common customer asks, however it also comes with a few drawbacks.

Windows Autopatch: Windows Autopatch is a new feature that simplifies the update management of Windows devices, by automating the installation of quality and feature updates, as well as security patches, on Windows devices. Windows Autopatch allows IT professionals and administrators to configure and enforce update policies, which specify the frequency, schedule, and scope of updates that should be applied to each device. Windows Autopatch improves the performance, reliability, and security of Windows devices, while minimizing the disruption and the risk of update failures.

Slide 3 [Hidden]

Abstract

Windows devices are essential for many organizations and businesses, but they also pose challenges in terms of provisioning and update management. How can IT professionals and administrators streamline the process of deploying, configuring, and updating Windows devices, while ensuring security, compliance, and user satisfaction?

This session will explore the latest technologies and Best Practices for Modern Provisioning and Modern Update Management for Windows devices, focusing on the topics: Windows Autopilot, Windows Autopilot device preparation (Windows Autopilot 2.0), and Windows Autopatch.

Windows Autopilot: Windows Autopilot is a cloud-based service that simplifies the deployment and configuration of new Windows devices, without requiring IT staff to physically touch each device. Windows Autopilot allows IT professionals and administrators to create and assign device profiles, which specify the settings, policies, apps, and features that should be applied to each device, reducing the time and cost of provisioning Windows devices, while improving the user experience and the security posture of the organization.

Windows Autopilot device preparation: Windows Autopilot device preparation (Windows Autopilot 2.0) is used to set up and configure new devices, getting them ready for productive use. Windows Autopilot device preparation aims to simplify device deployment by delivering consistent configurations, enhancing the overall setup speed, and improving troubleshooting capabilities, without device pre-registering or added as a Windows Autopilot device. Windows Autopilot device preparation is an improved profile experience that incorporates common customer asks, however it also comes with a few drawbacks.

Windows Autopatch: Windows Autopatch is a new feature that simplifies the update management of Windows devices, by automating the installation of quality and feature updates, as well as security patches, on Windows devices. Windows Autopatch allows IT professionals and administrators to configure and enforce update policies, which specify the frequency, schedule, and scope of updates that should be applied to each device. Windows Autopatch improves the performance, reliability, and security of Windows devices, while minimizing the disruption and the risk of update failures.

//

Learning objectives

Learning objective 1. Getting knowledge about the use and Best Practice of Windows Autopilot, Windows Autopilot device preparation, including the top 3 tips to optimize any Windows Autopilot scenario.

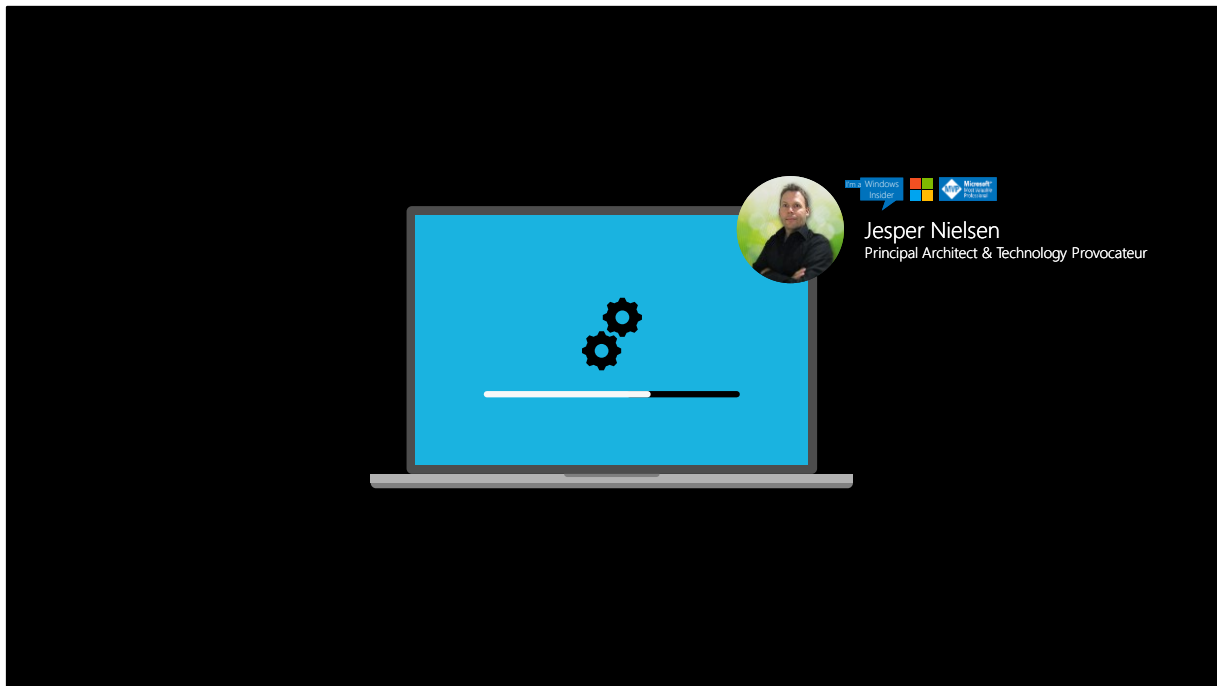
Learning objective 2. Getting knowledge about the benefits and pitfalls when moving either from WSUS or WU4B to Windows Autopatch.

Learning objective 3. Getting knowledge about the current, and coming, options and possibilities within Modern Provisioning and Update Management for Windows Devices using Microsoft Intune and MDM platform.

Slide 4 [Hidden]

Learning objectives

//



Slide 5 [00:00:00]

Booting...

//



Slide 6 [00:00:00]

Where you are...

//



Slide 7 [00:00:00]

Where I am...

//



Modern Provisioning and Update Management

Managing Windows devices, using Windows Autopilot and Windows Autopatch

Slide 8 [00:00:00]

Modern Provisioning and Update Management

Managing Windows devices, using Windows Autopilot and Windows Autopatch.

//



Slide 9 [00:00:00]

Modern Provisioning and Update Management

- Modern Provisioning - Windows Autopilot
- Modern Management (MDM) - Microsoft Intune
- Modern Update Management Windows Autopatch

//

A few words of attention

Are you Windows 11 ready yet? Well, are you even Windows 10 ready?

- No more hybrid-join and never hybrid Windows Autopilot
- More Self-Service, Less Required Apps

Are you Windows Hello for Business ready?



Slide 10 [00:00:00]

A few words of attention

//

Windows Autopilot - Today

19.6 M

Devices deployed with Autopilot

80%

Cloud joined only devices (Entra Joined)

73%

User Driven Deployments

"This week one of my users got a new desktop, which he setup using #autopilot. The user also went through the windows hello setup process, completely unassisted.

That user is 75 years old.

It was no big deal."

"Autopilot has saved us so much time, we use the base OEM image and provisioning happens in less than 30 minutes, before it would take 3 hours to get a device ready."

Slide 11 [00:00:00]

Autopilot – Today

//

3 ways to optimize any Windows Autopilot scenario.



Enable Windows Autopilot Enrollment Status Page (ESP)



Add five or less applications assigned to devices to the ESP block list, incl. a Desired State Configuration (DSC) package.



Disable the Account Setup phase of the Windows Autopilot Enrollment Status Page (ESP)

Slide 12 [00:00:00]

3 ways to optimize any Windows Autopilot scenario

- Enable Windows Autopilot Enrollment Status Page (ESP).
- Add five or less applications assigned to devices to the ESP block list, incl. a Desired State Configuration (DSC) package *.
- Disable the Account Setup phase of the Windows Autopilot Enrollment Status Page (ESP)

*) Need a Desired State Configuration (DCS) package, see the **Windows gecko** project, try it out or get inspiration: <https://github.com/dotjesper/windows-gecko/>

//

Ensure to be Windows Autopilot ready



Be Windows 11 ready
(and Windows 10 ready)



Windows Hello for Business
Controlled rollout



Enroll all existing devices into
Windows Autopatch
(Replace WSUS)

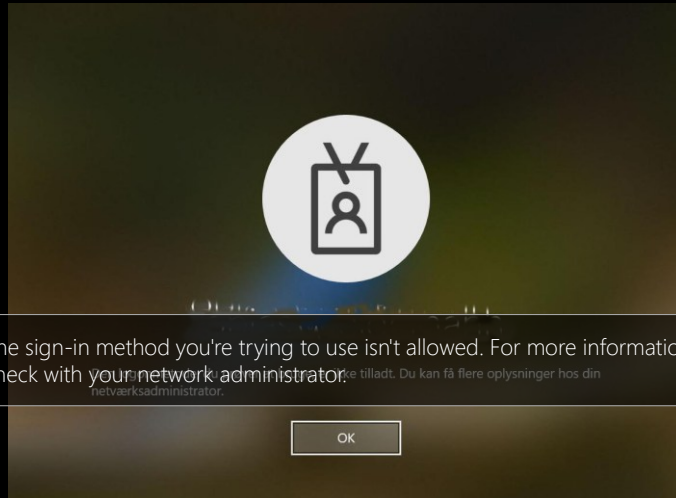
Slide 13 [00:00:00]

Ensure to be Windows Autopilot ready

- Be Windows 11 ready – and Windows 10 ready
- Windows Hello for Business - Controlled rollout
- Enroll all existing devices into Windows Autopatch - Replace WSUS

//

Being Windows Hello for Business ready

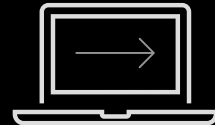


Slide 14 [00:00:00]

Windows Hello for Business ready

//

Going [Live]



Slide 15 [00:00:00]

3 ways to optimize any Windows Autopilot scenario

- Enable Windows Autopilot Enrollment Status Page (ESP).
- Add five or less applications assigned to devices to the ESP block list, incl. a Desired State Configuration (DSC) package *.
- Disable the Account Setup phase of the Windows Autopilot Enrollment Status Page (ESP)

Ensure to be Windows Autopilot ready

- Be Windows 11 ready – and Windows 10 ready
- Windows Hello for Business - Controlled rollout
- Enroll all existing devices into Windows Autopatch - Replace WSUS

//

Windows Autopilot device preparation

Slide 16 [00:00:00]

Windows Autopilot device preparation

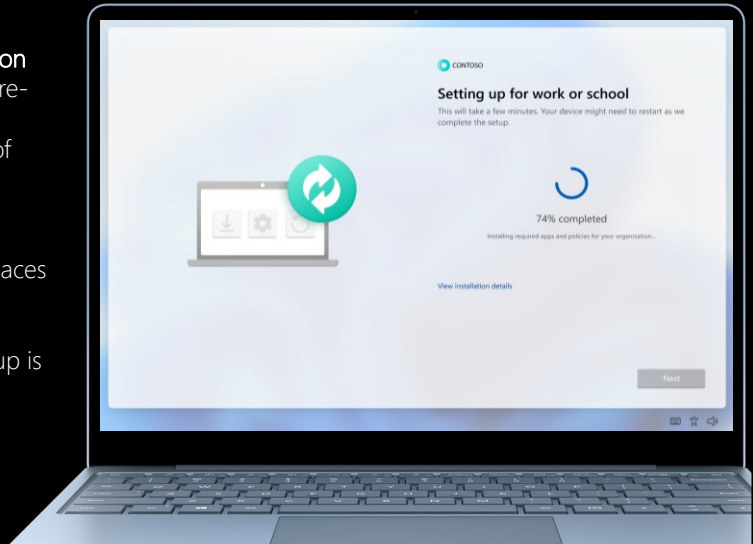
Windows Autopilot 2.0

//

Windows Autopilot - Tomorrow

Windows Autopilot device preparation

- Does not require hash-value or pre-registering (ish).
- Simplified OOBЕ view – show % of progress.
- More consistent experience with consumer flows.
- Improved grouping experience places devices in a group at the time of enrollment.
- Informs user when the OOBЕ setup is complete.

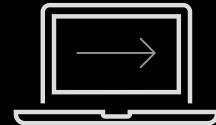


Slide 17 [00:00:00]

Autopilot – Tomorrow

//

Going [Live]



Slide 18 [00:00:00]

Windows Autopilot device preparation

- How to configure Windows Autopilot device preparation

//

Windows Autopilot device preparation limitations

Current limitations (Compared to Windows Autopilot)

- No computer naming options
- Limited to 10 managed apps and/or 10 scripts in ESP (per profile)
- Limited/delayed Microsoft Entra ID Dynamic Group usage - Enrollment time grouping is the solution
- No device assignment, User assignment only (it makes sense...)
- Currently require personal devices enrollment (no enrollment restriction)
- Currently corporate device identifiers is not supported/possible

Slide 19 [00:00:00]

Windows Autopilot device preparation limitations

Current limitations (Compared to Windows Autopilot)

- No computer naming options
- Limited to 10 managed apps in ESP (per profile)
- Limited/delayed Microsoft Entra ID Dynamic Group usage - Enrollment time grouping is the solution: No device assignment, User assignment only (it make sense...)
- Currently require personal devices enrollment (no enrollment restriction)
- Currently corporate device identifiers is not supported/possible

Links

Enrollment time grouping in Microsoft Intune:

<https://learn.microsoft.com/mem/intune/enrollment/enrollment-time-grouping>

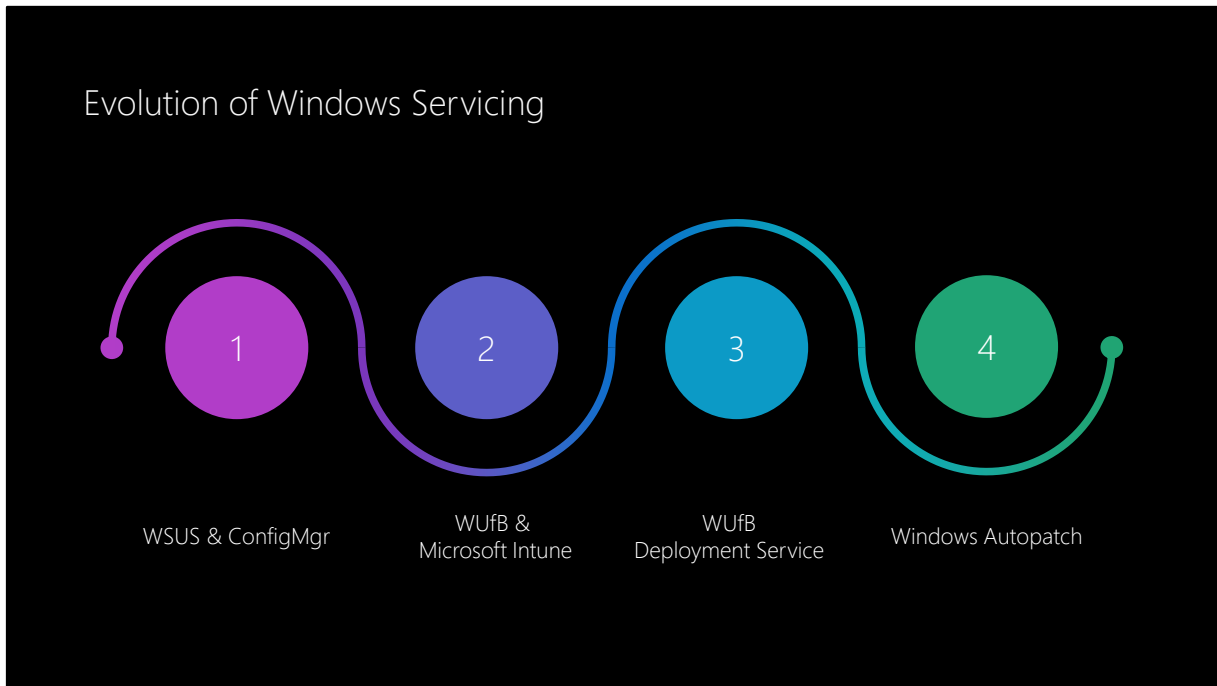
//

Modern Update Management using Windows Autopatch

Slide 20 [00:00:00]

Modern Update Management using Windows Autopatch

//



Slide 21 [00:00:00]

Evolution of Windows Servicing

//

Windows Autopatch is a cloud service that automates update management, to improve security and productivity across your organization.

Slide 22 [00:00:00]

What is Windows Autopatch?

Windows Autopatch is a cloud service that automates Windows, Microsoft 365 Apps for enterprise, Microsoft Edge, and Microsoft Teams updates, to improve security and productivity across your organization.

Rather than maintaining complex digital infrastructure, businesses want to focus on what makes them unique and successful. Windows Autopatch offers a solution to some of the challenges facing businesses and their people today:

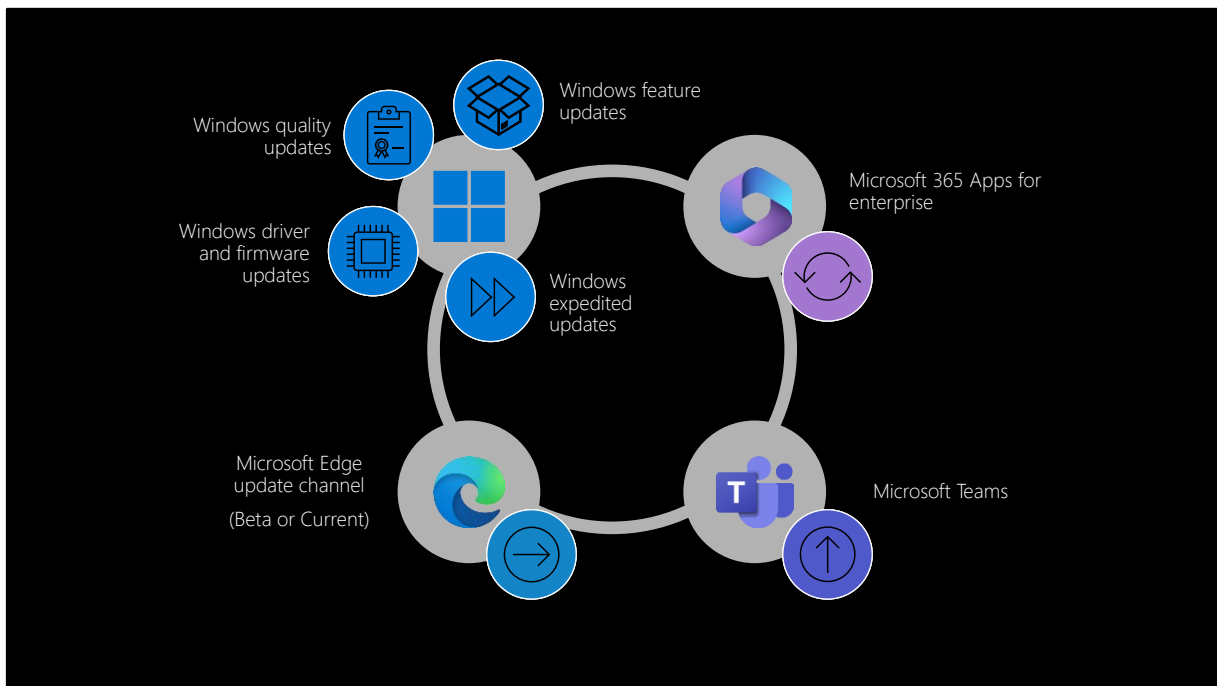
- Close the security gap: Windows Autopatch keeps software current, there are fewer vulnerabilities and threats to your devices.
- Close the productivity gap: Windows Autopatch adopts features as they're made available. End users get the latest tools to amplify their collaboration and work.
- Optimize your IT admin resources: Windows Autopatch automates routine endpoint updates. IT pros have more time to create value.
- On-premises infrastructure: Transitioning to the world of software as a service (SaaS) allows you to minimize your investment in on-premises hardware since updates are

delivered from the cloud.

- Onboard new services: Windows Autopatch makes it easy to enroll and minimizes the time required from your IT Admins to get started.
- Minimize end user disruption: Windows Autopatch releases updates in sequential deployment rings, and responding to reliability and compatibility signals, user disruptions due to updates are minimized.

<https://learn.microsoft.com/windows/deployment/windows-autopatch/overview/windows-autopatch-overview>

//



Slide 23 [00:00:00]

The anatomy of Windows Autopatch

<https://learn.microsoft.com/windows/deployment/windows-autopatch/overview/windows-autopatch-overview>

- Windows quality updates: Windows Autopatch aims to keep at least 95% of eligible devices on the latest Windows quality update 21 days after release.
- Windows feature updates: Windows Autopatch aims to keep at least 99% of eligible devices on a supported version of Windows so that they can continue receiving Windows feature updates.
- Microsoft 365 Apps for enterprise: Windows Autopatch aims to keep at least 90% of eligible devices on a supported version of the Monthly Enterprise Channel (MEC).
- Microsoft Edge: Windows Autopatch configures eligible devices to benefit from Microsoft Edge's progressive rollouts on the Stable channel.
- Microsoft Teams: Windows Autopatch allows eligible devices to benefit from the standard automatic update channel.

Manage Teams with policies: <https://learn.microsoft.com/microsoftteams/manage-teams->

with-policies

References

Windows quality updates: <https://learn.microsoft.com/windows/deployment/windows-autopatch/operate/windows-autopatch-groups-windows-quality-update-overview>

Manage Windows Autopatch groups:
<https://learn.microsoft.com/windows/deployment/windows-autopatch/deploy/windows-autopatch-groups-manage-autopatch-groups>

//

Changes made at tenant enrollment

The screenshot shows a web browser window displaying the Microsoft Learn article 'Changes made at tenant enrollment'. The page URL is <https://learn.microsoft.com/en-us/windows/deployment/windows-autopatch/references/windows-autopatch-changes-to-tenant>. The left sidebar contains a navigation menu with the following items: Windows Autopatch, Overview, Prepare, Deploy, Operate, References, Update policies, Changes made at tenant enrollment (highlighted), and What's new. The main content area has a heading 'Windows Autopatch will create the required Microsoft Entra groups to operate the service.' followed by a paragraph: 'The following groups target Windows Autopatch configurations to devices and management of the service by our [first party enterprise applications](#).' Below this is a table with two columns: 'Group name' and 'Description'. The table lists eight groups. To the right of the table is an 'Expand table' link. On the far right, there is an 'Additional resources' section with an 'Events' subsection showing a Microsoft Build event from May 21, 5 PM to May 24, 4 AM, with a 'Register now' link.

Group name	Description
Modern Workplace-All	All Modern Workplace users
Modern Workplace - Windows 11 Pre-Release Test Devices	Device group for Windows 11 Pre-Release testing.
Modern Workplace Devices-All	All Autopatch devices
Modern Workplace Devices-Virtual Machine	All Autopatch virtual devices
Modern Workplace Devices-Windows Autopatch-Test	Deployment ring for testing update deployments prior production rollout
Modern Workplace Devices-Windows Autopatch-First	First production deployment ring for early adopters
Modern Workplace Devices-Windows Autopatch-Fast	Fast deployment ring for quick rollout and adoption
Modern Workplace Devices-Windows Autopatch-Broad	Final deployment ring for broad rollout into the organization

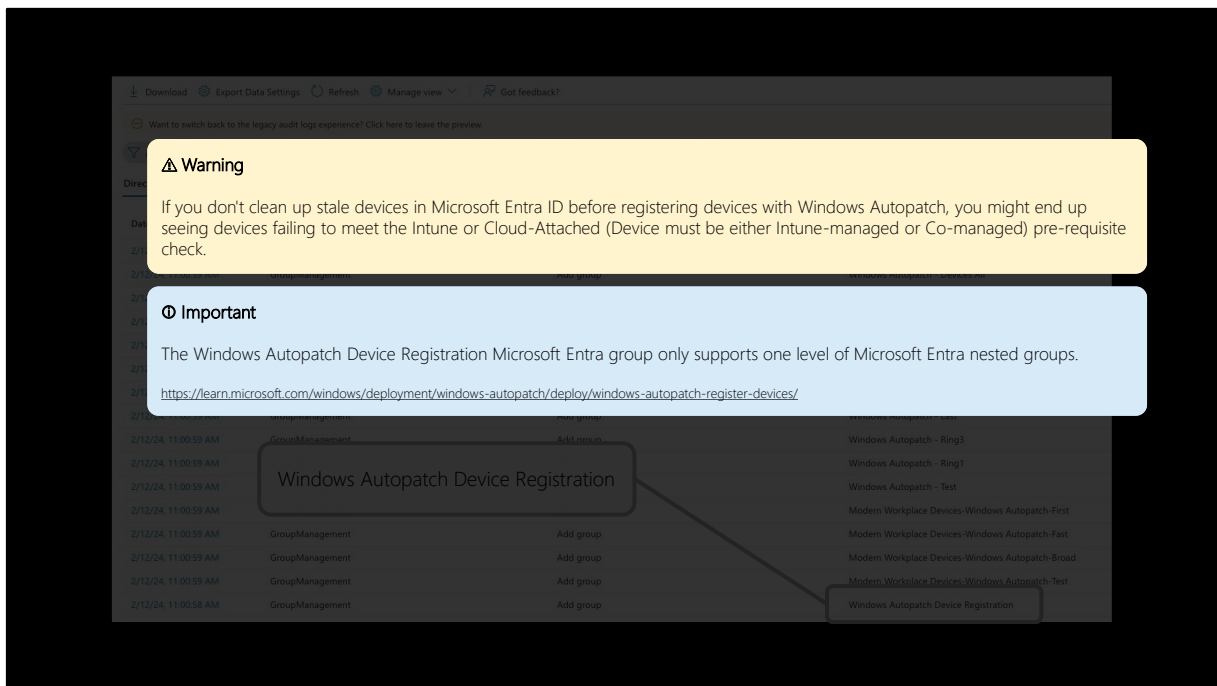
Slide 24 [00:00:00]

The anatomy of Windows Autopatch: Configuration profiles

Changes made at tenant enrollment:

<https://learn.microsoft.com/windows/deployment/windows-autopatch/references/windows-autopatch-changes-to-tenant/>

//



Slide 25 [00:00:00]

The anatomy of Windows Autopatch: Changes made at tenant enrollment

Changes made at tenant enrollment:

<https://learn.microsoft.com/windows/deployment/windows-autopatch/references/windows-autopatch-changes-to-tenant/>

The Windows Autopatch Device Registration Microsoft Entra group only supports one level of Microsoft Entra nested groups:

<https://learn.microsoft.com/windows/deployment/windows-autopatch/deploy/windows-autopatch-register-devices/>

//

The screenshot displays the Microsoft Entra ID audit logs interface. At the top, there are navigation links: Download, Export Data Settings, Refresh, Manage view, and Got feedback?. Below this is a warning banner: "Want to switch back to the legacy audit logs experience? Click here to leave the preview." The filter bar includes: Add filter, Show dates as: Local, Date range: 11.2.2024 - 13.2.2024, Service: All, Category: GroupManagement, Activity: Add group, and Reset filters. The table has two tabs: Directory (selected) and Custom Security. The table columns are Date, Category, Activity, and Target(s). The data shows multiple 'Add group' activities for 'GroupManagement' on 2/12/24 at 11:00:59 AM. Two callout boxes highlight specific activities: 'Windows Autopatch - Devices All' and 'Windows Autopatch Device Registration'. Arrows point from these boxes to their respective rows in the table.

Date	Category	Activity	Target(s)
2/12/24, 11:00:59 AM	GroupManagement	Add group	Modern Workplace Roles - Service Administrator
2/12/24, 11:00:59 AM	GroupManagement	Add group	Windows Autopatch - Devices All
2/12/24, 11:00:59 AM	GroupManagement	Add group	Modern Workplace Roles - Service Reader
2/12/24, 11:00:59 AM	GroupManagement	Add group	Modern Workplace Devices-Virtual Machine
2/12/24, 11:00:59 AM	GroupManagement	Add group	Modern Workplace-All
2/12/24, 11:00:59 AM	GroupManagement	Add group	Modern Workplace Devices-All
2/12/24, 11:00:59 AM	GroupManagement	Add group	Windows Autopatch - Ring2
2/12/24, 11:00:59 AM	GroupManagement	Add group	Windows Autopatch - Last
2/12/24, 11:00:59 AM	GroupManagement	Add group	Windows Autopatch - Ring3
2/12/24, 11:00:59 AM	GroupManagement	Add group	Windows Autopatch - Ring1
2/12/24, 11:00:59 AM	GroupManagement	Add group	Windows Autopatch - Test
2/12/24, 11:00:59 AM	GroupManagement	Add group	Modern Workplace Devices-Windows Autopatch-First
2/12/24, 11:00:59 AM	GroupManagement	Add group	Modern Workplace Devices-Windows Autopatch-Fast
2/12/24, 11:00:59 AM	GroupManagement	Add group	Modern Workplace Devices-Windows Autopatch-Broad
2/12/24, 11:00:59 AM	GroupManagement	Add group	Modern Workplace Devices-Windows Autopatch-Test
2/12/24, 11:00:58 AM	GroupManagement	Add group	Windows Autopatch Device Registration

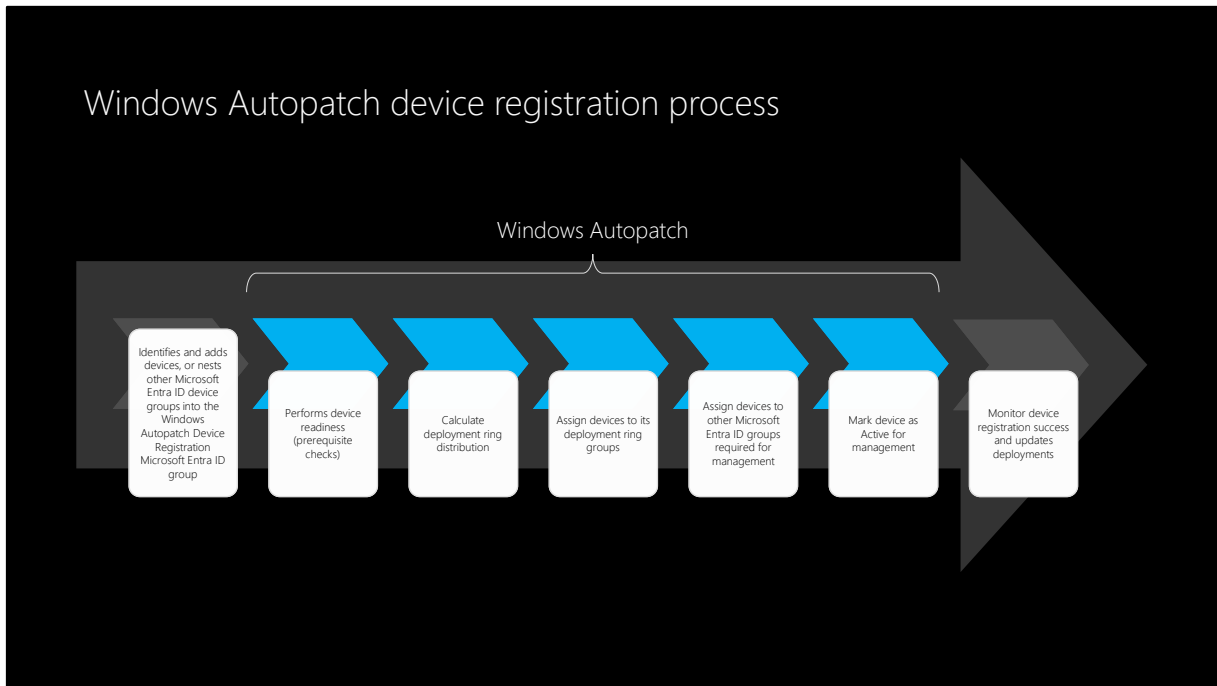
Slide 26 [00:00:00]

The anatomy of Windows Autopatch: Changes made at tenant enrollment

Changes made at tenant enrollment:

<https://learn.microsoft.com/windows/deployment/windows-autopatch/references/windows-autopatch-changes-to-tenant/>

//



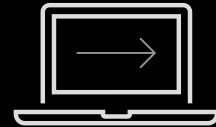
Slide 27 [00:00:00]

The anatomy of Windows Autopatch: Windows Autopatch device registration process

<https://learn.microsoft.com/windows/deployment/windows-autopatch/deploy/windows-autopatch-register-devices>

//

Going [Live]



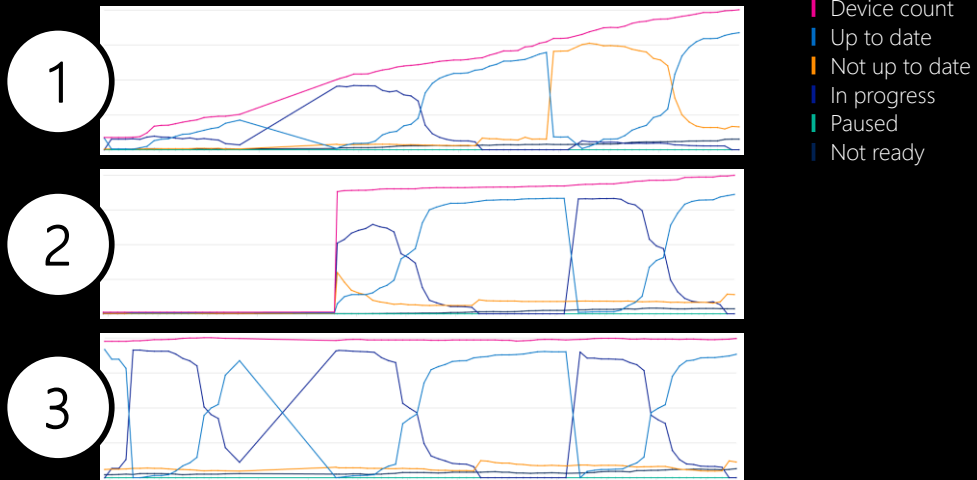
Slide 28 [00:00:00]

Windows Autopilot device preparation

- How to configure Windows Autopatch groups

//

Windows Autopatch enrollment scenarios



Slide 29 [00:00:00]

Windows Autopatch enrollment scenarios

//

Windows Autopatch for Microsoft Edge

Windows Autopatch does not come with a Microsoft Edge Update behavior configuration policy.

You should control Microsoft Edge Update behavior with your own configuration!



Slide 30 [00:00:00]

Windows Autopatch for Microsoft Edge

//

Windows Autopatch & Microsoft 365 Apps Update

Slide 31 [00:00:00]

Windows Autopatch & Microsoft 365 Apps Update

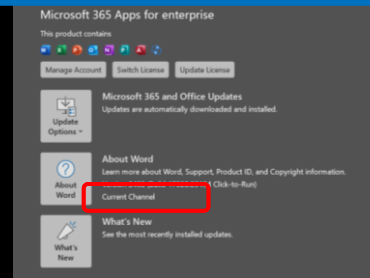
//

Microsoft 365 Apps Cloud Update policies

Windows Autopatch: Microsoft 365 Apps Monthly Enterprise Channel only



Windows Autopatch configured



Windows Autopatch configured
and Cloud Update configured

Slide 32 [00:00:00]

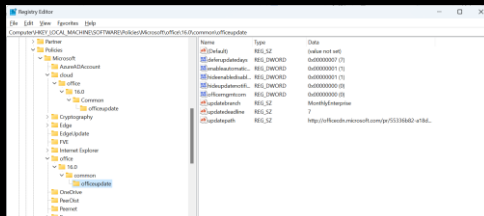
Microsoft 365 Apps Cloud Update policies

Cloud update is the successor to servicing profile.

Cloud update provides a modern update management solution for Microsoft 365 Apps. Use cloud update to address common servicing needs with features such as custom rollout waves, exclusion windows, pause, and rollback.

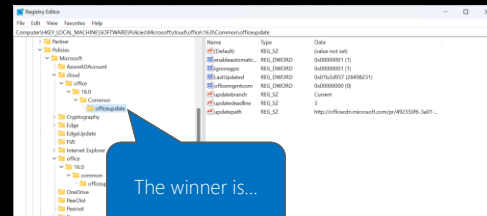
//

Microsoft 365 Apps Update settings



Microsoft 365 Apps Update policies:

1. Group Policies
2. Microsoft Intune
3. Microsoft 365 admin center



Microsoft 365 Apps Cloud Update policy:

1. Microsoft 365 Apps Admin Center
<https://config.office.com/>

Slide 33 [00:00:00]

Microsoft 365 Apps Update settings

Microsoft 365 Apps Update policies:

1. Group Policies
2. Microsoft Intune
3. Microsoft 365 admin center

Microsoft 365 Apps Cloud Update policy:

1. Microsoft 365 Apps Admin Center
<https://config.office.com/>

Cloud update is the successor to servicing profile.

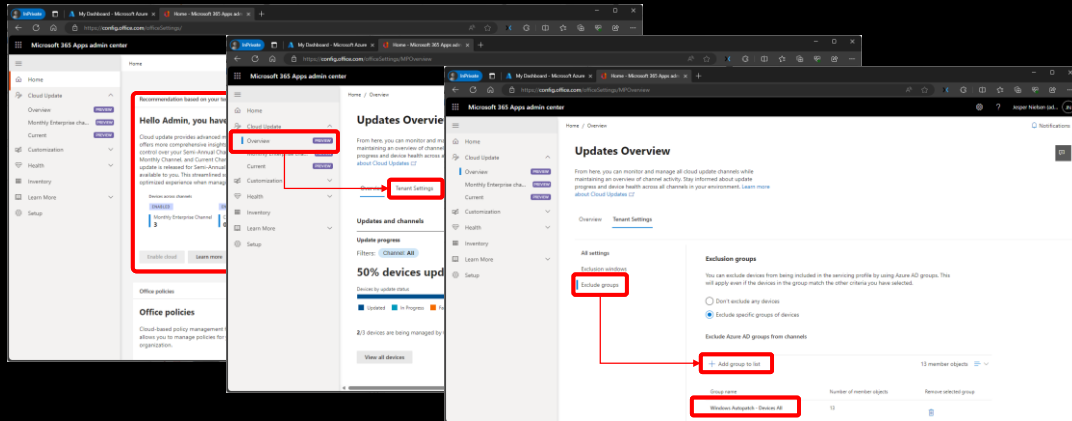
Order of assignment (who wins):

1. Microsoft 365 admin center
2. Group Policies
3. Microsoft Intune
4. Microsoft 365 Apps Admin Center

Highest number wins.

//

Microsoft 365 Apps Cloud Update policies – exclude devices



Slide 34 [00:00:00]

Microsoft 365 Apps Cloud Update policies

Cloud update is the successor to servicing profile.

Cloud update provides a modern update management solution for Microsoft 365 Apps. Use cloud update to address common servicing needs with features such as custom rollout waves, exclusion windows, pause, and rollback.

//



Modern Provisioning and Update Management | Extra

Slide 35 [00:00:00]

Modern Provisioning and Update Management | Extra

//

Modern Provisioning and Update Management | Extra



Microsoft Intune Config Refresh



New Company Portal



Set up enrollment notifications

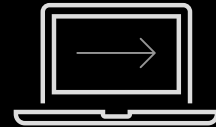
Slide 36 [00:00:00]

Modern Provisioning and Update Management | Extra

- **Microsoft Intune Config Refresh:** <https://techcommunity.microsoft.com/t5/windows-it-pro-blog/intro-to-config-refresh-a-refreshingly-new-mdm-feature/ba-p/4176921>
- **New Company Portal:** <https://techcommunity.microsoft.com/t5/intune-customer-success/new-look-for-intune-company-portal-app-for-windows/ba-p/4158755>
- **Set up enrollment notifications:**
<https://learn.microsoft.com/mem/intune/enrollment/enrollment-notifications>

//

Going [Live]



Slide 37 [00:00:00]

Modern Provisioning and Update Management | Extra

- Microsoft Intune Config Refresh
- New Company Portal
- Set up enrollment notifications

//

Summary

Slide 38 [00:00:00]

Summary

//

Q&A | Thank you!

Slide 39 [00:00:00]

Thank you

//



Jesper Nielsen

Principal Architect & Technology Provocateur

Microsoft Most Valuable Professional (MVP)

e: j.nielsen@windowsramblings.com | t: @dotjesper | b: <https://dotjesper.com/>

Slide 40 [Hidden]

About :: Biography

Who he is and what he do:

Jesper Nielsen is a Principal Architect and Technology Provocateur, Microsoft Most Valuable Professional (MVP)). He has been working hands-on with small- and large-scale IT-Infrastructure in many different industries for more than 20 years.

With a long background in supporting Windows technologies, Jesper Nielsen have designed and implemented several generations of Windows and is always happy to share his knowledge around this subject and related technologies.

Jesper Nielsen is the founder of the Everything Windows User Group, Denmark and is active in the community and can often be found at user group events as both speaker and attendee. He has been facilitating numerous seminars and events and has made several speaker appearances over the years were his passionate style of delivery, combined with his sense of humor, has made him a recognize speaker.

He does the work he does, because he is loving it, he likes the people he meets and is

always embracing the inner nerd and good presentation skills.

He finished a marathon around the four hours' mark, have been a gymnastics instructor for more than 30 years, he enjoying exploring technology and guide his kids into new technologies and is currently teaching himself C# for Windows app development.

He was awarded the MVP Status for Windows and Devices for IT for the first time, July 2016.

Find him:

E-mail: j.nielsen@windowsramblings.com

Follow him:

Blog: <https://dotjesper.com/>

Twitter: <https://twitter.com/dotjesper/>

GitHub: <https://github.com/dotjesper/>

LinkedIn: <https://www.linkedin.com/in/dotjesper/>

Microsoft MVP: <https://mvp.microsoft.com/en-us/PublicProfile/5002044/>

Join him:

Everything User Group Denmark: <http://wmug.dk/>

Workplace Ninja User Group Denmark: <https://wpninjas.dk/>

//

References

Slide 41 [:Hidden]

References

//