



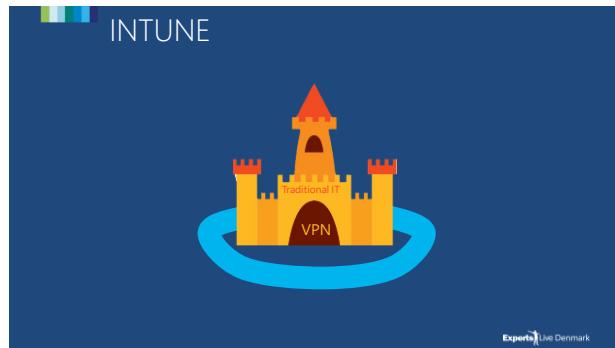
Revealing 10 Common INTUNE Errors and How to Avoid Them

Simon Skotheimsvik
Senior Cloud Consultant / CloudWay, Norway

1



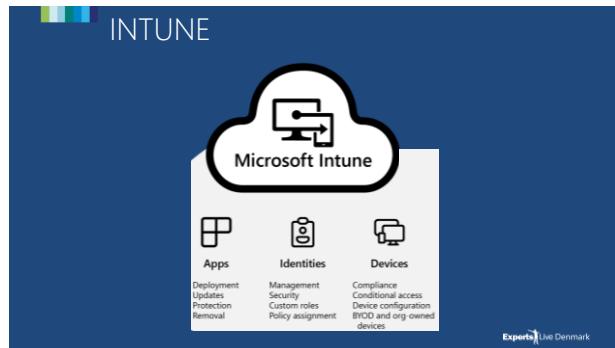
2



3



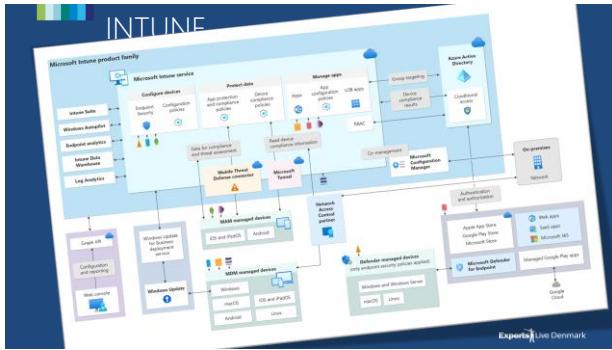
4



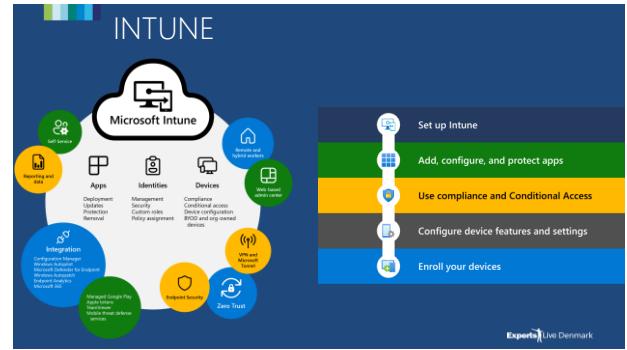
5



6



7



8

SIMON SKOTHEIMSVIK
Senior Cloud Consultant

@SSkotheimsvik skotheimsvik.no
<https://linktree/simonkothemsvik>

10

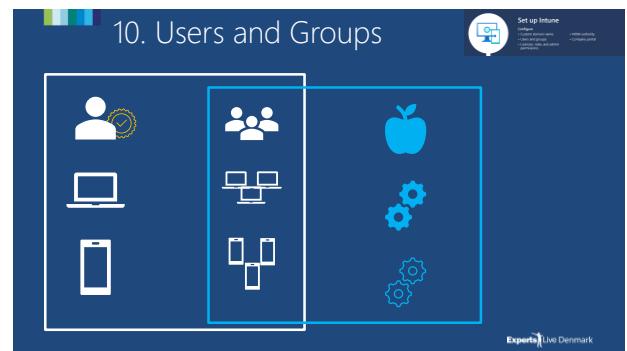


11

10 Users and Groups

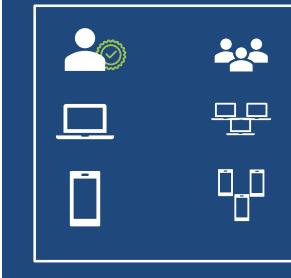
Revealing 10 Common Intune Errors and How To Avoid Them

12



13

10. Users and Groups



14



Groups All groups		
	Object Id	Group type
<input type="checkbox"/> Name 1	4220b5ef-c7ed-4db4-8a0f-bd4fb2056569	Microsoft 365
<input type="checkbox"/> All Company	4509b50b-ebe3-49bc-960b-68e5f58614d3	Distribution
<input type="checkbox"/> AE All Employees	6773a5dc-32c3-4667-aabb-1b8b01bd8e01	Security
<input type="checkbox"/> AU All Users	8df1a013-a380-4db4-8c1f-3ce085f6a29	Security
<input type="checkbox"/> AW AZ-Device-Intune-All Windows 10 Devices	ab0c35b0-3015-4043-957-4bae3538b28e	Security
<input type="checkbox"/> AW AZ-Device-Intune-All Windows 11 Devices	88d907b7-b10d-459e-9286-62c25ee1fc	Security
<input type="checkbox"/> AM AZ-Device-Windows-Patching-Early Release	98d907b7-b10d-459e-9286-62c25ee1fc	Security
<input type="checkbox"/> AV AZ-Device-Windows-Patching-IT Validation	9705ea01-b3ab-4db4-bee6-f7f0516d9683	Security
<input type="checkbox"/> AV AZ-Device-Windows-Autopilot-IE	b8kf02be-af0f-4d36-8e05-8703b1ff17c	Security
<input type="checkbox"/> AV AZ-Device-Windows-Autopilot-UK	casa02ee-374c-4b06-b3d-8703b40d0a	Security
<input type="checkbox"/> AJ AZ-Personal-CA-Administrators	0f100132-9f60-4025-a1a4-aae40ff9600	Security
<input type="checkbox"/> AJ AZ-Personal-CA-AbusingServiceAccounts	1ed83606-d01-4384-9fa3-fc343c20fc	Security
<input type="checkbox"/> AJ AZ-Personal-CA-BreakGlassAccounts	3c976647-2b04-4318-844c-8c28086beef	Security

15

Groups All groups		
	Object Id	Group type
<input type="checkbox"/> Name 1	4220b5ef-c7ed-4db4-8a0f-bd4fb2056569	Microsoft 365
<input type="checkbox"/> All Company	4509b50b-ebe3-49bc-960b-68e5f58614d3	Distribution
<input type="checkbox"/> AE All Employees	6773a5dc-32c3-4667-aabb-1b8b01bd8e01	Security
<input type="checkbox"/> AU All Users	8df1a013-a380-4db4-8c1f-3ce085f6a29	Security
<input type="checkbox"/> AW AZ-Device-Intune-All Windows 10 Devices	ab0c35b0-3015-4043-957-4bae3538b28e	Security
<input type="checkbox"/> AW AZ-Device-Intune-All Windows 11 Devices	88d907b7-b10d-459e-9286-62c25ee1fc	Security
<input type="checkbox"/> AM AZ-Device-Windows-Patching-Early Release	98d907b7-b10d-459e-9286-62c25ee1fc	Security
<input type="checkbox"/> AV AZ-Device-Windows-Patching-IT Validation	9705ea01-b3ab-4db4-bee6-f7f0516d9683	Security
<input type="checkbox"/> AV AZ-Device-Windows-Autopilot-IE	b8kf02be-af0f-4d36-8e05-8703b1ff17c	Security
<input type="checkbox"/> AV AZ-Device-Windows-Autopilot-UK	casa02ee-374c-4b06-b3d-8703b40d0a	Security
<input type="checkbox"/> AJ AZ-Personal-CA-Administrators	0f100132-9f60-4025-a1a4-aae40ff9600	Security
<input type="checkbox"/> AJ AZ-Personal-CA-AbusingServiceAccounts	1ed83606-d01-4384-9fa3-fc343c20fc	Security
<input type="checkbox"/> AJ AZ-Personal-CA-BreakGlassAccounts	3c976647-2b04-4318-844c-8c28086beef	Security

16

Groups All groups			
	Object Id	Group type	Membership type
<input type="checkbox"/> Name 1	4220b5ef-c7ed-4db4-8a0f-bd4fb2056569	Microsoft 365	Assigned
<input type="checkbox"/> All Company	4509b50b-ebe3-49bc-960b-68e5f58614d3	Distribution	Assigned
<input type="checkbox"/> AE All Employees	6773a5dc-32c3-4667-aabb-1b8b01bd8e01	Security	Dynamic
<input type="checkbox"/> AU All Users	8df1a013-a380-4db4-8c1f-3ce085f6a29	Security	Dynamic
<input type="checkbox"/> AW AZ-Device-Intune-All Windows 10 Devices	ab0c35b0-3015-4043-957-4bae3538b28e	Security	Dynamic
<input type="checkbox"/> AW AZ-Device-Intune-All Windows 11 Devices	88d907b7-b10d-459e-9286-62c25ee1fc	Security	Dynamic
<input type="checkbox"/> AM AZ-Device-Windows-Patching-Early Release	98d907b7-b10d-459e-9286-62c25ee1fc	Security	Assigned
<input type="checkbox"/> AV AZ-Device-Windows-Patching-IT Validation	9705ea01-b3ab-4db4-bee6-f7f0516d9683	Security	Assigned
<input type="checkbox"/> AV AZ-Device-Windows-Autopilot-IE	b8kf02be-af0f-4d36-8e05-8703b1ff17c	Security	Dynamic
<input type="checkbox"/> AV AZ-Device-Windows-Autopilot-UK	casa02ee-374c-4b06-b3d-8703b40d0a	Security	Dynamic
<input type="checkbox"/> AJ AZ-Personal-CA-Administrators	0f100132-9f60-4025-a1a4-aae40ff9600	Security	Dynamic
<input type="checkbox"/> AJ AZ-Personal-CA-AbusingServiceAccounts	1ed83606-d01-4384-9fa3-fc343c20fc	Security	Assigned

17

New Group

Got feedback?

Group type * Security

Group name * All Windows Devices

Group description * Group holding all devices with Windows Operating system

Microsoft Entra roles can be assigned to the group Yes No

Membership type * Assigned

Assigned
Dynamic User
Dynamic Device

18

Groups | All groups

Membership type * Assigned

Assigned
Dynamic User
Dynamic Device

AZ-Personal-CA-AbusingServiceAccounts

Object Id: 1ed83606-d01-4384-9fa3-fc343c20fc
Group type: Security
Membership type: Assigned

19

This screenshot shows the 'Groups | All groups' page in Microsoft Intune. A specific group named 'Dynamic Device' is selected. The 'Membership type' is set to 'Dynamic Device'. Below it, the 'Dynamic device members' section shows a table with three rows. The first row has a red highlight over the 'Assigned' column. The second row has a green highlight over the 'Assigned' column. The third row has a blue highlight over the 'Assigned' column.

20

This screenshot shows the 'Dynamic membership rules' configuration dialog. It displays a rule builder with an 'And/Or' condition. The 'Property' dropdown is set to 'deviceOSType', the 'Operator' dropdown is set to 'Contains', and the 'Value' dropdown is set to 'Windows'. Below the main dialog, a 'Rule syntax' section shows the generated query: '(device.deviceOSType -contains "Windows") and (device.deviceOSVersion -startsWith "10.0.22")'.

21

This screenshot shows the same 'Dynamic membership rules' configuration dialog as the previous one, but with a more complex rule. The 'Property' dropdown is set to 'deviceOSVersion', the 'Operator' dropdown is set to 'Starts With', and the 'Value' dropdown is set to '10.0.22'. The 'Rule syntax' section shows the query: '(device.deviceOSType -contains "Windows") and (device.deviceOSVersion -startsWith "10.0.22")'.

22

This screenshot shows the '10. Users and Groups' dashboard. It includes sections for 'All Windows 10 devices', 'All Windows 11 devices', 'All Autopilot devices with GroupTag like DK', and 'All users on Sales Department'. Each section has a corresponding icon and a detailed query description below it. The URL at the bottom is <https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>.

23

This screenshot shows the same '10. Users and Groups' dashboard as the previous one, but with a different layout. It includes sections for 'All Windows 10 devices', 'All Windows 11 devices', 'All Autopilot devices with GroupTag like DK', and 'All users on Sales Department'. Each section has a corresponding icon and a detailed query description below it. The URL at the bottom is <https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>.

24

This screenshot shows the '10. Users and Groups' dashboard. It includes sections for 'User group vs Device group'. Each section has a corresponding icon. The URL at the bottom is <https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#user-groups-vs-device-groups>.

25

10. Users and Groups

User group vs Device group

ariaupdated @ariaupdated
How do you group devices in your organization? #WindowsUpdate
#Management
User Groups
Device Groups
A combination of both
141 votes - 18 hours left
4:09 PM · Nov 7, 2023 · 1,132 Views

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#user-groups-vs-device-groups>

Experts Live Denmark

26

10. Users and Groups

User group vs Device group

ariaupdated @ariaupdated
How do you group devices in your organization? #WindowsUpdate
User Groups
Device Groups
Nickolaj Andersen [MVP] @NickolajA · 3h
Rarely ever do we assign anything towards a group that contains users.
99.9% of all targeting is towards device based groups.
4:05 PM · Nov 7, 2023 · 188 Views

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#user-groups-vs-device-groups>

Experts Live Denmark

27

10. Users and Groups

User group vs Device group

- If you want to apply settings to a user, regardless of the device
 - Assign your policies to a user group
 - Makes it easier for hardware replacements
- If you want to apply settings on a device, regardless of who's signed in
 - Assign your policies to a devices group.
 - Settings applied to device groups always go with the device, not the user.
 - Great for preprovisioning

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#user-groups-vs-device-groups>

Experts Live Denmark

28

10. Users and Groups

User group vs Device group

Assignments

Included groups: Add group, Add users, Add all devices

Group Members: Filter, None

Excluded groups: Filter, None

All Devices

Group Members: Remove

Groups: No groups selected

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#user-groups-vs-device-groups>

Experts Live Denmark

29

10. Users and Groups

User group vs Device group

- If you want to apply settings to a user, regardless of the device
 - Assign your policies to a user group
 - Makes it easier for hardware

! When excluding groups, you cannot mix user and device groups across include and exclude.

regardless of who's signed in

- Assign your policies to a devices group.
- Settings applied to device groups always go with the device, not the user.
- Great for preprovisioning

<https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#user-groups-vs-device-groups>

Experts Live Denmark

30

10. Users and Groups

User group vs Device group

I don't see membership changes instantly when I add or change a rule, why?

I configured a rule on a group but no memberships get updated in the group

Depending on the size of your Microsoft Entra organization, the group may take up to 24 hours for populating for the first time or after a rule change. This is a result of the asynchronous nature of the group's update process, which is determined by the number of members in the group. It can take 30 minutes or longer to populate.

<https://learn.microsoft.com/en-gb/azure/active-directory/enterprise-users/groups-troubleshooting-dynamic-memberships-for-groups>

Experts Live Denmark

31

10. Users and Groups

User group vs Device group

Dynamic groups are slow

Use Intune Filters!

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/filters>

Set up Intune

Experts Live Denmark

32

10. Users and Groups

Use Intune Filters!

Microsoft Intune admin center

Devices | Filters

Search: Create

Enrollment device platform restrictions:

- eSIM cellular profiles (preview)
- Policy sets
- Other
- Device clean up rules
- Device categories
- Filters

Filter name	Platform
WFLT001 - AAD joined	Windows 10 and later
WFLT002 - HAAD joined	Windows 10 and later
WFLT003 - AAD or HAAD joined	Windows 10 and later
WFLT004 - Windows 11 devices	Windows 10 and later
WFLT005 - Windows 10 devices	Windows 10 and later
WFLT006 - Windows devices	Windows 10 and later

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/filters>

Set up Intune

Experts Live Denmark

33

10. Users and Groups

Use Intune Filters!

Microsoft Intune admin center

Devices | Filters

WFLT004 - Windows 11 devices

Properties Associated assignments

Filter name: WFLT004 - Windows 11 devices
Description: 2023.09.26 - CloudWay template installed, Simon
Platform: Windows 10 and later

Rules Edit

(device.osVersion -startsWith "10.0.22")

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/filters>

Set up Intune

Experts Live Denmark

34

10. Users and Groups

Use Intune Filters!

Microsoft Intune admin center

Devices | Filters

WFLT004 - Windows 11 devices

Properties Associated assignments

Filter name: WFLT004 - Windows 11 devices
Description: 2023.09.26 - CloudWay template installed, Simon
Platform: Windows 10 and later

Rules Edit

(device.osVersion -startsWith "10.0.22")

WFLT001 - AAD Joined

Properties Associated assignments

Filter name: WFLT001 - AAD Joined
Description: 2023.09.26 - CloudWay template installed, Simon
Platform: Windows 10 and later

Rules Edit

(device.deviceTrustType -eq "Azure AD joined")

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/filters>

Set up Intune

Experts Live Denmark

35

10. Users and Groups

Use Intune Filters!

Windows Configuration profiles > **WDCP016 - OS - Disable News and Interests**

Edit profile - WDCP016 - OS - Disable News and Interests

Settings catalog

Assignments Review + save

Included groups: Add groups, Add all users, Add all devices

Groups: All Devices

Group Members: Filter mode, Edit filter, Remove

Filter mode: WRT005 - Windows 10 device include

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/filters>

Set up Intune

Experts Live Denmark

36

9

RBACs

Revealing 10 Common Intune Errors and How To Avoid Them

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/filters>

Set up Intune

Experts Live Denmark

37

9. RBACs

Intune Administrator

This role can create and manage all security groups. However, Intune Administrator does not have admin rights over Office groups. That means the admin cannot update owners or memberships of all Office groups in the organization. However, he/she can manage the Office group that he creates which comes as a part of his/her end-user privileges. So, any Office group (not security group) that he/she creates should be counted against his/her quota of 250.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference/intune-administrator>

Expert Live Denmark

38

9. RBACs

Intune Administrator

PRIVILEGED

This is a privileged role. Users with this role have global permissions within Microsoft Intune Online, when the service is present. Additionally, this role contains the ability to manage users and devices in order to associate policy, as well as create and manage groups. For more information, see Role-based administration control (RBAC) with Microsoft Intune.

This role can create and manage all security groups. However, Intune Administrator does not have admin rights over Office groups. That means the admin cannot update owners or memberships of all Office groups in the organization. However, he/she can manage the Office group that he creates which comes as a part of his/her end-user privileges. So, any Office group (not security group) that he/she creates should be counted against his/her quota of 250.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference/intune-administrator>

Expert Live Denmark

39

9. RBACs

Intune Administrator

This is a privileged role. Users with this role have global permissions within Microsoft Intune Online, when the service is present. Additionally, this role contains the ability to manage users and devices in order to associate policy, as well as create and manage groups. For more information, see Role-based administration control (RBAC) with Microsoft Intune.

This role can create and manage all security groups. However, Intune Administrator does not have admin rights over Office groups. That means the admin cannot update owners or memberships of all Office groups in the organization. However, he/she can manage the Office group that he creates which comes as a part of his/her end-user privileges. So, any Office group (not security group) that he/she creates should be counted against his/her quota of 250.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference/intune-administrator>

Expert Live Denmark

40

9. RBACs

Endpoint Manager roles | All roles

Name	Type
Application Manager	Built-in Role
Endpoint Security Manager	Built-in Role
Organizational Message Manager	Built-in Role
Endpoint Privilege Manager	Built-in Role
School Administrator	Built-in Role
Read Only Operator	Built-in Role
Endpoint Privilege Reader	Built-in Role
Intune Role Administrator	Built-in Role
Help Desk Operator	Built-in Role
Policy and Profile manager	Built-in Role

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference/intune-administrator>

Expert Live Denmark

41

9. RBACs

Endpoint Manager roles | Scope tags

Scope tags define groups of Intune resources that align with specific Intune Role assignments. For example, a "Seattle Office" scope tag could be used to associate policies, profiles or applications with administrators that only apply to the Seattle office.

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference/intune-administrator>

Expert Live Denmark

42

9. RBACs

Create Scope Tag

Basics

Scope tags define groups of Intune resources that align with specific Intune Role assignments. For example, a "Seattle Office" scope tag could be used to associate policies, profiles or applications with administrators that only apply to the Seattle office locations.

Name: iOS

Description: All iOS devices

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference/intune-administrator>

Expert Live Denmark

43

9. RBACs

The screenshot shows the Microsoft Intune admin center interface. The user is navigating through the 'Tenant admin | Roles > Endpoint Manager roles | Scope tags'. A new scope tag named 'AZ-Device-iOS' is being created. The 'Included groups' section shows a single group 'AZ-Device-iOS' selected. The 'Assignments' tab is active.

44

9. RBACs

The screenshot shows the configuration of a dynamic membership rule for the 'AZ-Device-iOS' scope tag. The rule specifies that devices must have either 'iPhone' or 'iPad' as their deviceOSType. The 'Configure rules' section shows the rule builder interface with two conditions: 'deviceOSType Equals iPhone' and 'deviceOSType Equals iPad'.

45

9. RBACs

The screenshot shows the creation of an iOS/iPadOS configuration profile named 'IDCP001 - OS - Device Restrictions'. The 'Profiles' section lists several profiles, including 'IDCP001 - OS - Device Restrictions' which is currently selected. The 'Platform: iOS/iPadOS' dropdown is set to iOS/iPadOS.

46

9. RBACs

The screenshot shows the configuration of a 'Device restrictions' setting for the 'IDCP001 - OS - Device Restrictions' profile. The 'Scope tag' dropdown is set to 'Default'. The 'Configuration settings' section shows the 'Device restrictions' setting is enabled.

47

9. RBACs

The screenshot shows the creation of a new role named 'Help Desk Operator' under the 'Endpoint Manager roles' section. The 'Manage' tab is selected, and the 'All roles' section shows the new role being added. The 'Name' field is populated with 'Help Desk Operator'.

48

9. RBACs

The screenshot shows the creation of a duplicate role named 'iOS Operator'. The 'Duplicate role' section indicates that the role is based on 'Help Desk Operator'. The 'Name' field is populated with 'iOS Operator'.

49

9. RBACs

Microsoft Intune admin center

Duplicate role

Copy role's existing description and permissions

Basics Permissions

Select a category below to configure settings.

Android Enterprise

Action	Yes	No
Read	Yes	No
Create	Yes	No
Delete	Yes	No
Assign	Yes	No
Update	Yes	No

Audit data Certificate Connector

50

9. RBACs

Microsoft Intune admin center

iOS Operator | Properties

Overview Basics

Name: iOS Operator

Description: Custom role based on Help Desk Operators perform remote tasks on applications or policies related to iOS.

Manage Properties Assignments

Permissions Edit

Permission	Read	Take application actions	Install Now
Certificate Connector	Read	Read	Read
Cloud attached devices	Read	Read	Read
Customization	Read	Read	Read
Device configurations	Read	Read	Read
Device compliance policies	Read	Read	Read
Device enrollment manager	Read	Read	Read

51

9. RBACs

Microsoft Intune admin center

iOS Operator | Assignments

Overview Manage Properties Assignments

Role assignments tie together a role definition with members and scopes. There can be one or more role assignments per role. This applies to custom and built-in roles.

+ Assign Refresh Export Columns

Name Description

52

9. RBACs

Microsoft Intune admin center

Add Role Assignment

iOS Operator

Basics Admin Groups Scope Groups Scope tags Review + create

Name: iOS Operator Assignment

Description:

Assigning users, scope groups and scope tags to custom role.

53

9. RBACs

Microsoft Intune admin center

New Group

Got feedback?

Group type: Security

Group name: AZ-Intune-CustomRole-iOS-Operators

Group description: Group holding users allowed to use the Intune Custom role iOS Operator

Microsoft Entra roles can be assigned to the group: No

Membership type: Assigned

54

9. RBACs

Microsoft Intune admin center

Add Role Assignment

iOS Operator

Basics Admin Groups Scope Groups Scope tags Review + create

Administrators in this role assignment can target policies, applications and remote tasks.

Included groups

Add groups: Add all users + Add all devices

Groups: AZ-Device-iOS Remove

55

9. RBACs

56

9. RBACs

57

9. RBACs

58

9. RBACs

Protecting Microsoft 365 from on-premises compromise

59

9. RBACs

Note

To be able to administer Intune you must have an Intune license assigned. Alternatively, you can allow non-licensed users to administer Intune by setting Allow access to unlicensed admins to Yes.

60

Set up Intune

Add, configure, and protect apps

Configure

- Baseline apps list
- Microsoft Outlook and Edge
- VPN

Use compliance and Conditional Access

Configure device features and settings

Enroll your devices

61

8 Application Distributions

Revealing 10 Common Intune Errors and How To Avoid Them

Exports Live Denmark

62

8. Application Distributions

Microsoft Intune admin center

Home > Apps > Apps | All apps

Search by name or publisher:

Name	Type	Status	Version
Adobe Acrobat Reader DC	Microsoft Store app (new)	Yes	
Company Portal	Microsoft Store app (new)	Yes	
M365 Apps for Enterprise	Windows app (Windows)	1.1	No
Microsoft Remote Desktop	Microsoft Store app (new)	Yes	
Microsoft To Do Lists, Tasks & Reminders	Microsoft Store app (new)	Yes	
Microsoft Whiteboard	Microsoft Store app (new)	Yes	
Teamviewer Remote Control	Microsoft Store app (new)	Yes	
Zip Utility - Win Zip compression	Microsoft Store app (new)	Yes	

63

8. Application Distributions

Microsoft Intune admin center

Home > Apps > Windows > Windows | Windows apps

Add Refresh Filter Export Columns

Search by name or publisher:

Name	Type	Status	Version	Assigned
Adobe Acrobat Reader DC	Microsoft Store app (new)	Yes		
Company Portal	Microsoft Store app (new)	Yes		
M365 Apps for Enterprise	Windows app (Windows)	1.1	No	
Microsoft Remote Desktop	Microsoft Store app (new)	Yes		
Microsoft To Do Lists, Tasks & Reminders	Microsoft Store app (new)	Yes		
Microsoft Whiteboard	Microsoft Store app (new)	Yes		
Teamviewer Remote Control	Microsoft Store app (new)	Yes		
Zip Utility - Win Zip compression	Microsoft Store app (new)	Yes		

64

8. Application Distributions

Microsoft Intune admin center

Home > Apps > Windows > Windows | Windows apps

Select app type

App type
Store app
Microsoft Store app (new)
Microsoft Store app (legacy)
Microsoft 365 App
Windows 10 and later
Microsoft Edge, version 77 and later
Windows 10 and later
Web Application
Windows with link
File link
Line of business app
Windows app (Windows)

65

8. Application Distributions

Microsoft Intune admin center

Home > Apps > Windows > Windows | Windows apps

Add Refresh Filter Export Columns

Search by name or publisher:

Name	Type	Status	Version	Assigned
Adobe Acrobat Reader DC	Microsoft Store app (new)	Yes		
Company Portal	Microsoft Store app (new)	Yes		
M365 Apps for Enterprise	Windows app (Windows)	1.1	No	
Microsoft Remote Desktop	Microsoft Store app (new)	Yes		
Microsoft To Do Lists, Tasks & Reminders	Microsoft Store app (new)	Yes		
Microsoft Whiteboard	Microsoft Store app (new)	Yes		
Teamviewer Remote Control	Microsoft Store app (new)	Yes		
Zip Utility - Win Zip compression	Microsoft Store app (new)	Yes		

66

8. Application Distributions

Microsoft Intune admin center

Home > Apps > Windows > Windows | Windows apps

Select app type

App type
Store app
Microsoft Store app (new)
Microsoft Store app (legacy)
Microsoft 365 App
Windows 10 and later
Microsoft Edge, version 77 and later
Windows 10 and later
Web Application
Windows with link
File link
Line of business app
Windows app (Windows)

67

8. Application Distributions

68

8. Application Distributions

69

8. Application Distributions

70

8. Application Distributions

71

8. Application Distributions

72

8. Application Distributions

73

8. Application Distributions

74

8. Application Distributions

75

8. Application Distributions

76

8. Application Distributions

77

8. Application Distributions

78

8. Application Distributions

13

8. Application Distributions

The screenshot shows the Microsoft Intune Enterprise Application Management interface. A modal window is open for purchasing a license. It displays the following information:

- Select license quantity:** 1
- Select billing frequency:** Pay monthly, annual commitment (radio button selected)
- Subtotal before applicable taxes:** €1,87
- Buy** and **Start trial** buttons
- Advanced Analytics** and **Available for trial or purchase** status indicators
- With full visibility into the state of your on-premises and cloud apps, deploy it quickly using a secure hosted enterprise catalog.**
- Microsoft Intune Advanced Analytics** and **Enterprise App Management** links

80

8. Application Distributions

The screenshot shows the Microsoft Intune admin center under the Tenant admin section. The **Capabilities** tab is selected. It displays the following sections:

- Tenant add-ons**: Shows a search bar and a list of available add-ons.
- Endpoint Privilege Management**: Shows a green status indicator and a brief description.
- Enterprise App Management**: Shows a green status indicator and a brief description.

81

8. Application Distributions

The screenshot shows the Microsoft Intune admin center under the Apps section. The **Windows | Windows apps** page is displayed. A modal window titled "Select app type" is open, showing a list of app types:

- Share app
- Microsoft Store app (new)
- Microsoft Store app (legacy)
- Company Portal
- Microsoft 365 App
- Microsoft Edge, version 77 and later
- Windows 10 and later
- Windows web link
- Web Application
- Microsoft To Do, To... Microsoft Store
- Microsoft Whiteboard
- Other
- Web link
- Line of Business app
- Windows app (Win32)
- Enterprise App Catalog app

82

8. Application Distributions

The screenshot shows the Microsoft Intune admin center under the Apps section. The **Add App** page is displayed for the "Windows catalog app (Win32)". The "App Information" tab is selected. The page includes fields for Name, Description, Publisher, App Version, Category, and a note about compliance requirements. Below the form, there is a "Search the Enterprise App catalog" input field and a list of published apps.

83

8. Application Distributions

The screenshot shows the Microsoft Intune admin center under the Apps section. The **Add App** page is displayed for "Putty (x64)". The "App Information" tab is selected. The page includes fields for Name, Description, Publisher, App Version, Category, and a note about compliance requirements. Below the form, there is a "Show this as a featured app in the Company Portal" checkbox and a "Information (0)" link.

84

8. Application Distributions

The screenshot shows the Microsoft Intune admin center under the Apps section. The **Add App** page is displayed for "Putty (x64)". The "Program" tab is selected. The page includes fields for Install command, Uninstall command, Installation time required (min), Allow available uninstall, Install behavior, and Device restart behavior. Below the form, there is a "Specify return codes to indicate post-installation behavior" section and a "Return code" and "Code type" table.

85

8. Application Distributions

The screenshot shows the Microsoft Intune Admin Center interface. A modal window titled "Add App" is open, specifically for a "Windows catalog app (WHIC2)". Under the "Detection rules" tab, a table lists a single rule: "Manually configure detection rules". The "Type" is set to "Path/Code" and the "File" path is "%ProgramFiles%PUTTY". The "Registry" path is listed as "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\PUTTY". The "Rules format" dropdown is set to "Manually configure detection rules".

86

8. Application Distributions

The screenshot shows the Microsoft Intune Admin Center interface. The left sidebar is expanded to show "Windows" and "Windows apps". The main pane displays a list of installed Windows apps. One entry, "PUTTY (64)", is highlighted in green. Other entries include Adobe Acrobat Reader, Microsoft Store app (new), Microsoft 365 Apps (Windows), Microsoft Remote Desktop, Microsoft Store app (new), Microsoft To Do List, Microsoft Store app (new), Microsoft Whiteboard, TeamViewer Remote, Zip UpZip - rar, 7z, zip ..., and Microsoft Store app (new).

87

8. Application Distributions

The screenshot shows the Microsoft Intune Admin Center interface. A session dashboard is displayed for a Microsoft 365 breakout session. The session details are: Morten Banke, 20th Mar 2024, 11:10am CET - 12:00pm CET, In Person Session. The title of the session is "Intune Suite - The good, the Bad an the Ugly". The session has 300 participants and is using Microsoft 365. The status bar at the bottom shows "2ip Unzip - rar, 7z, zip ... Microsoft Store app (new)".

88

8. Application Distributions

The screenshot shows the Microsoft Endpoint Manager (MSEndpointMgr) interface. The top navigation bar includes Home, Intune, Identity, Windows, Configuration, Policy, Tools, GitHub, and About us. A sub-menu for "Intune" is open, showing "App Factory". The main content area is titled "Intune App Factory" and describes it as an automated solution combining Azure DevOps Pipelines and Intune modules. It highlights features like "Application onboarding", "Continuous packaging", and "Latest application version available".

89

8. Application Distributions

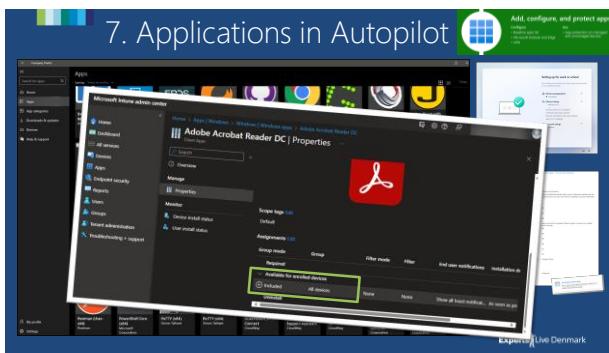
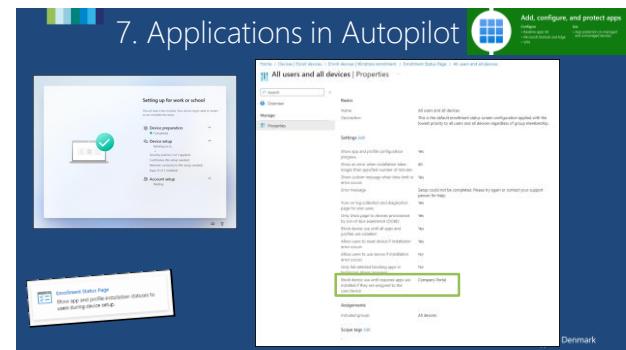
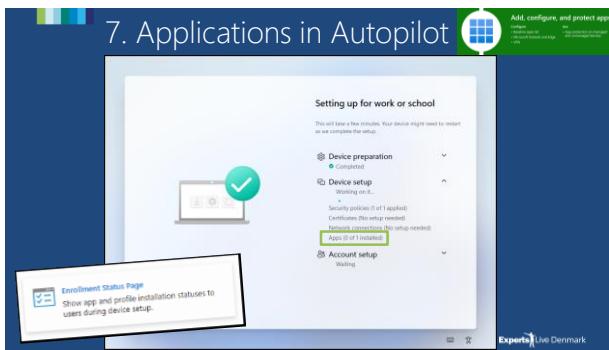
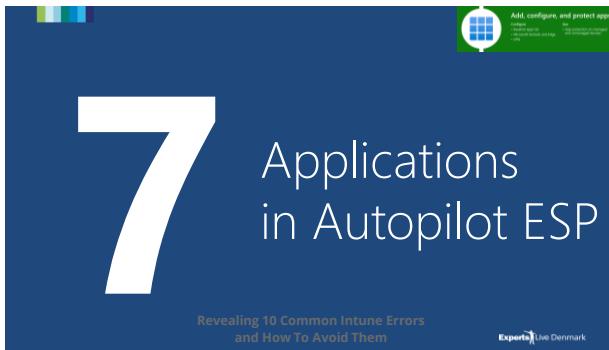
The screenshot shows the PATCH MY PC interface. The main heading is "We help you save time, money and improve your IT security". Below it, it says "Integrate Third-Party Patch Management in Microsoft ConfigMgr and Intune". There are two buttons: "Schedule a demo" and "Request a quote". A small inset window shows a Microsoft Intune session dashboard.

90

8. Application Distributions

The screenshot shows the PATCH MY PC interface. The main heading is "We help you save time, money and improve your IT security". Below it, it says "Integrate Third-Party Patch Management in Microsoft ConfigMgr and Intune". There are two buttons: "Schedule a demo" and "Request a quote". A large inset window shows a Microsoft 365 session dashboard. The session details are: Adam Cook, Liliu Barbat, 20th Mar 2024, 1:10pm CET - 2:00pm CET, In Person Session. The title of the session is "3rd Party Application Updates and Management and Advanced Insights for ConfigMgr and Intune".

91



6

Compliance Policies

Revealing 10 Common Intune Errors and How To Avoid Them

Exports Live Denmark

99

6. Compliance Policies

Microsoft Intune admin center

Compliance policies | Compliance policy settings

Mark devices with no compliance policy assigned as: Compliant

100

6. Compliance Policies

Microsoft Intune admin center

Compliance policies | Compliance policy settings

Mark devices with no compliance policy assigned as: Not compliant

101

6. Compliance Policies

Microsoft Intune admin center

Windows | Compliance policies

Policy name: WCOP001 - Device Health - BitLocker and Secure boot

Platform or OS: Windows 10 and later; Windows 8.1 and later

Policy type: Windows 10/11

WCOP001 - Device Health - BitLocker and Secure boot
WCOP002 - Device Properties - Minimum OS version
WCOP003 - System Security - Microsoft Defender
WCOP004 - System Security - Device Security
WCOP005 - System Security - Require encryption
WCOP006 - Microsoft Defender for Endpoint Risk Score

102

6. Compliance Policies

Microsoft Intune admin center

Windows | Compliance policies

WCOP001 - Device Health - BitLocker and Secure boot

Compliance policy - Windows 10 and later

Monitor Properties

Basics

Name: WCOP001 - Device Health - BitLocker and Secure boot
Description: 2023.09.26 - CloudWay template installed, Simon
Platform: Windows 10 and later
Profile type: Windows 10/11 compliance policy

Compliance settings

Device Health
Required
Secure Boot
Required
Code Integrity
Required

Actions for noncompliance

Action: Mark device noncompliant
Schedule: 2 Days

Message template

Additional recipients (via email)

None selected

103

6. Compliance Policies

Microsoft Intune admin center

Windows | Compliance policies

WCOP002 - Device Properties - Minimum OS version

Compliance policy - Windows 10 and later

Monitor Properties

Basics

Name: WCOP002 - Device Properties - Minimum OS version
Description: 2023.09.26 - CloudWay template installed, Simon
Platform: Windows 10 and later
Profile type: Windows 10/11 compliance policy

Compliance settings

Device Properties
Minimum OS version: 10.0.19044

Actions for noncompliance

Action: Mark device noncompliant
Schedule: Immediately

Message template

Additional recipients (via email)

None selected

104

6. Compliance Policies

105

6. Compliance Policies

106

6. Compliance Policies

107

6. Compliance Policies

108

6. Compliance Policies

109

6. Compliance Policies

110

The screenshot shows the Microsoft Intune Admin Center interface. The top navigation bar includes links for Home, Intune security, Conditional access, Conditional Access / Policies, Delete, View policy information, Control access based on all or specific network, Select what this policy applies to, Cloud apps, Include, Exclude, Select the cloud app to exempt from the policy, Edit filter (review), Target resources, All cloud apps included and if any excluded, Selected included cloud apps, Universal Store Service API and Web Application and API, Microsoft Intune, Microsoft Intune Conditional, Microsoft Intune Conditional (selected), Microsoft Intune Conditional (selected), Microsoft Intune Conditional (selected), and Microsoft Intune Conditional (selected). The left sidebar lists categories such as Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area displays a policy titled 'CA200-Internals-AllApps-AnyPlatform-CompliantorMFA-Grant' with sections for Control access based on all or specific network, Assignments, and Conditions. The bottom right corner features a shield icon with the text 'Use compliance and conditional access' and a link to 'Microsoft Intune Conditional access'.

111

Set up Intune

Add, configure, and protect apps

Use compliance and Conditional Access

Configure device features and settings

- Configure**
 - Security baseline
 - Access to organization resources
- Enhance**
 - Protections and configurations

Enroll your devices

112



5 Configurations

Revealing 10 Common Intune Errors
and How To Avoid Them



Configure device features and settings

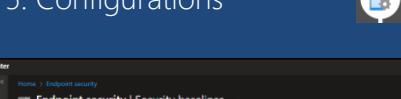
Intune configuration
Intune configuration
Intune configuration
Intune configuration



Expert Live Denmark

113

5. Configurations



The screenshot shows the Microsoft Intune admin center interface. The left sidebar includes Home, Dashboard, All services, Devices, App, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Endpoint security | Security baselines'. It features a search bar and navigation links for Overview, Overview (All devices), Security baselines, Security tasks, Manage, and Antivirus. A table lists security baselines: 'Security baseline for Windows 10 and later' (Last Published: 10/22/21, 12:00 AM), 'Microsoft Defender for Endpoint Baseline' (12/06/21, 12:00 AM), 'Security baseline for Microsoft Edge' (05/05/21, 2:00 AM), 'Windows 10S Security Baseline' (10/27/21, 12:00 AM), and 'Microsoft 365 Apps for Enterprise Security Baseline' (05/23/21, 2:00 AM). A top right corner shows a device icon with the text 'Configure device features and settings' and 'Intune Device Configuration'.

114

5. Configurations

The screenshot shows the Microsoft Intune interface for managing security baselines. At the top, it says "Available security baselines". Below that, a section titled "Windows 10 and later" lists several configurations such as "Microsoft Defender for Endpoint baseline", "Windows 10 and later", "Windows 11 and later", and "Windows 12 and later". Each item has a "View details" button. The "View details" button for the "Microsoft Defender for Endpoint baseline" is highlighted with a green box. Below this, there's a note about the baseline being implemented for physical devices and a warning against using it in cloud environments like Azure DevOps Pipelines. A "Next Step" button is present. On the right side, there's a sidebar with "Configure device features and settings" and a "Devices" section showing 1 device. At the bottom, there's a link to "Expertise Denmark" and a "Feedback" button.

115

The screenshot shows the Microsoft Intune 'Available security baselines' page. It highlights the 'Windows 10/11 MDM security baseline in Intune' and provides a link to 'List of the settings in the Windows 10/11 MDM security baseline in Intune'. The page includes sections for choosing a version (November 2021, December 2020, August 2020), viewing the baseline details, and navigating to device features and documentation.

116

117

118

5. Configuration

Available security baselines

The following security baseline options are available for use with Intune. Use the links to view the settings for each baseline.

- [Security Baseline for Windows 10 and later](#)
 - Windows 10
 - Windows 10 (S)
 - Windows 2000
 - Windows 2003
 - Windows 2008
 - Windows 2008 R2
 - Windows 2012
 - Windows 2012 R2
 - Windows 2016
 - Windows 2019
 - Windows 2022
- [Microsoft Defender for Endpoint baseline](#)
- [Microsoft Defender for Cloud baseline](#)
- [Microsoft Defender for Identity baseline](#)
- [Microsoft Defender for Microsoft 365 baseline](#)
- [Microsoft Defender for Endpoint security](#)
- [Microsoft Defender for Endpoint security \(Windows 10 and later\)](#)
- [Microsoft Defender for Endpoint security \(Windows 7 and later\)](#)
- [Microsoft Defender for Identity security](#)
- [Microsoft Defender for Identity security \(Windows 10 and later\)](#)
- [Microsoft Defender for Identity security \(Windows 7 and later\)](#)
- [Windows 10 App Guard](#)
- [Windows 10 App Guard \(Windows 10\)](#)
- [Windows Mail Baseline](#)
- [Windows Mail Baseline \(Windows 10 and later\)](#)
- [Windows Mail Baseline \(Windows 7 and later\)](#)
- [Windows Mail Baseline \(Windows 10 and later\)](#)
- [Windows Mail Baseline \(Windows 7 and later\)](#)
- [Windows Security Baseline](#)
- [Windows Security Baseline \(Windows 10 and later\)](#)
- [Windows Security Baseline \(Windows 7 and later\)](#)

Event Log Service

▪ Application log maximum file size in KB
Baseline default: 32768
Last modified: 10/26/2022

▪ System log maximum file size in KB
Baseline default: 20480
Last modified: 10/26/2022

Event Log Publishing

▪ Event log publishing interval in minutes
Baseline default: 10
Last modified: 10/26/2022

▪ Maximum log publishing length
Baseline default: 2
Last modified: 10/26/2022

▪ Number of log failures before stopping device
Baseline default: 3
Last modified: 10/26/2022

▪ Block simple password
Baseline default: No
Last modified: 10/26/2022

▪ Prevent minimum age in days
Baseline default: 1
Last modified: 10/26/2022

▪ Prevent use of screen
Baseline default: Enabled
Last modified: 10/26/2022

▪ Prevent idle show
Baseline default: Enabled
Last modified: 10/26/2022

DMA Guard

▪ Interruption of external devices incompatible with Kernel DMA Protection
Baseline default: Block all
Last modified: 10/26/2022

Device features

▪ Device configuration
Baseline default: Configuration
Last modified: 10/26/2022

Last Published

10/22/21, 10:00 AM
10/26/22, 10:00 AM
09/02/20, 11:00 AM
05/25/23, 200 AM
10/21/21, 10:00 AM
05/25/23, 200 AM

Denmark

119

120

The screenshot shows the Microsoft Intune Admin Center interface. The top navigation bar includes 'Home', 'Devices Windows | Windows', and 'Windows'. On the left sidebar, under 'Devices', 'Windows' is selected. The main content area displays 'Windows | Configuration profiles'. A search bar at the top has 'Search' and 'Windows device' dropdowns. Below it are 'Create profile', 'Refresh', 'Export', and 'Columns' buttons. A large blue arrow points from the 'Configuration profiles' section to the 'Profile name' column of the table. Another blue arrow points from the 'Profile name' column to the 'Platform' column.

Profile name	Platform	Profile type
WDS000001 - CS - Device Health and Virtualization Based Technology and OEM user	Windows 10 and later	Settings catalog
WDS000001 - CS - Security Baseline	Windows 10 and later	Settings catalog
WDS000001 - CS - Security Baseline - Internet Options	Windows 10 and later	Settings catalog
WDS000001 - CS - Windows Health Monitoring	Windows 10 and later	Settings catalog
WDS000001 - CS - Device Restrictions	Windows 10 and later	Settings catalog
WDS000001 - CS - Microsoft Defender SmartScreen	Windows 10 and later	Settings catalog
WDS000001 - CS - Windows Update For Business	Windows 10 and later	Settings catalog
WDS000001 - CS - Windows Update For Business reports	Windows 10 and later	Settings catalog
WDS000001 - CS - Device Optimization	Windows 10 and later	Settings catalog
WDS000001 - CS - Device Policy - Prescribed Policy for local accounts	Windows 10 and later	Settings catalog
WDS000001 - CS - Device Lock - Screen lock and 5 minutes	Windows 10 and later	Settings catalog
WDS000001 - CS - Lock Screen Image	Windows 10 and later	Settings catalog
WDS000001 - CS - Password must be locked screen	Windows 10 and later	Settings catalog

121

A screenshot of the Microsoft Intune Admin Center. The main title is "Intune Security baselines". Below it says "Creating and updating security baselines". A sub-section titled "Windows 10 and later" is selected. It shows a list of settings categories: "Settings catalog", "Windows hello", "Windows 10 and later", and "Windows 10 and later". On the left, there's a sidebar with navigation items like Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. At the bottom, there's a footer with "JoostGelijsteen.com" and icons for GitHub, LinkedIn, and YouTube.

122

5. Configurations

The screenshot shows the 'Endpoint protection' configuration page under 'Windows | Configuration profiles'. It includes sections for Microsoft Defender Application Guard, Microsoft Defender Firewall, Microsoft Defender SmartScreen, Windows Encryption (with sub-sections for Encrypt devices, Encrypt storage card (mobile only), BitLocker base settings, Warning for other disk encryption, Allow standard users to enable encryption during Azure AD join, and Configure encryption methods), and a summary of status for each setting.

123

5. Configurations

The screenshot shows the 'Create profile' page for 'BitLocker Drive Encryption' under 'Windows Components > BitLocker Drive Encryption'. It includes fields for selecting encryption methods (AES-256-CBC (Default), AES-256-XTS (Default), and AES-256-CBC-HMAC-SHA256 (Default)), choosing drive encryption method and recovery key location (Local Disk (E:) and User), and enabling or disabling full-drive encryption type on fixed drives.

124

5. Configurations

This screenshot shows a different view of the 'Create profile' page for 'BitLocker Drive Encryption', likely a previous step or a different configuration. It includes sections for BitLocker settings (Request Device Encryption, Allow Warning for Other Disk Encryption, Configure Recovery Password Method), and Administrator templates (Windows Components > BitLocker Drive Encryption > Operating System Drives).

125

5. Configurations

The screenshot shows the 'Create profile' page for 'Windows Components > Windows Hello for Business'. A note at the top states: 'If disabled, the user cannot provision Windows Hello for Business except on Azure Active Directory joined mobile phones where provisioning may be required. Not configured will honor configurations done on the client.' The configuration dropdown is set to 'Not configured' with options 'Not configured', 'Enabled', and 'Disabled'.

126

5. Configurations

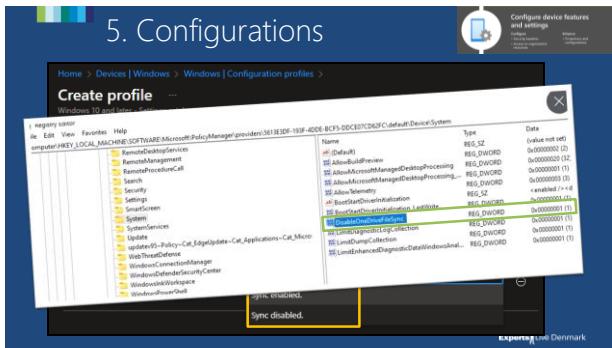
This screenshot shows the 'Create profile' page for 'Windows Components > Windows Hello for Business'. A note at the top states: 'If disabled, the user cannot provision Windows Hello for Business except on Azure Active Directory joined mobile phones where provisioning may be required. Not configured will honor configurations done on the client.' Below it, a note about OneDrive file sync is present: 'Configure Windows Hello for Business: Not configured' (dropdown with options 'Not configured', 'Enabled', 'Disabled'). A detailed note below explains the policy setting: 'Block Windows Hello for Business' and 'Windows Hello for Business is an alternative method for signing into Windows by replacing passwords, Smart Cards, and Virtual Smart Cards. If you disable or do not configure this policy setting, the device provisions Windows Hello for Business for any user.' At the bottom, a note says 'Block Windows Hello for Business' (dropdown with 'Disabled' selected).

127

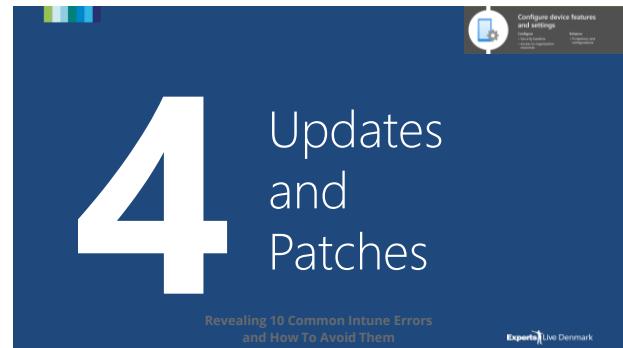
5. Configurations

The screenshot shows the 'Create profile' page for 'OneDrive file sync' under 'Windows | Configuration profiles'. It includes a note: 'This policy setting controls access to and features for managing files on OneDrive. If you enable this policy setting, users can't access OneDrive from the OneDrive app and the picker. Microsoft Store apps can't access OneDrive using the Win32 API. OneDrive doesn't appear in the navigation pane in File Explorer. OneDrive files aren't kept in sync with local files. Users can't automatically upload photos and videos to OneDrive from the picker. If you disable or do not configure this policy setting, apps and features can work with OneDrive file storage.' The configuration dropdown is set to 'Sync enabled' with options 'Sync enabled', 'Sync disabled', and 'Sync disabled'.

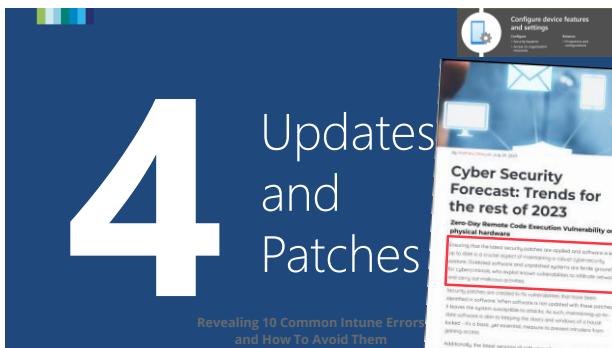
128



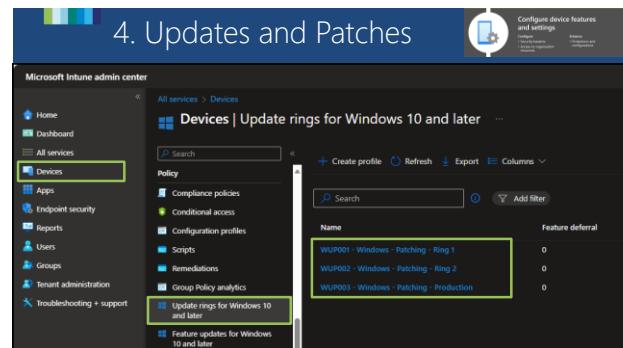
129



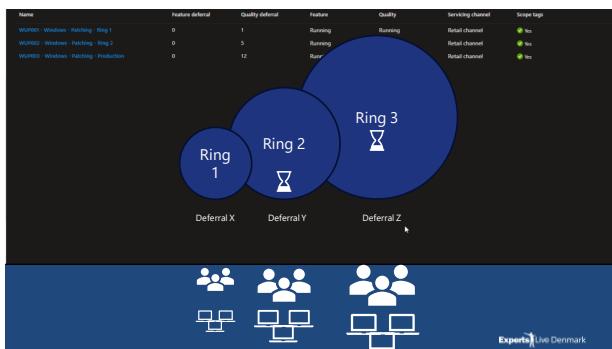
133



134



135



136



137

4. Updates and Patches

Microsoft Intune admin center

All services > Devices

Devices | Feature updates for Windows 10 and later

Name	Feature update version
WFLU001 - Windows10 - Ring 1	Windows 10, version 22H2
WFLU002 - Windows10 - Ring 2	Windows 10, version 21H2
WFLU003 - Windows10 - Production	Windows 10, version 22H2
WFLU004 - Windows11 - Ring 1	Windows 11, version 22H2
WFLU005 - Windows11 - Ring 2	Windows 11, version 22H2
WFLU006 - Windows11 - Production	Windows 11, version 22H2

138

4. Updates and Patches

Microsoft Intune admin center

All services > Devices

Devices | Feature updates for Windows 10 and later

Name	Feature update version
WFLU001 - Windows10 - Ring 1	Windows 10, version 22H2
WFLU002 - Windows10 - Ring 2	Windows 10, version 21H2
WFLU003 - Windows10 - Production	Windows 10, version 22H2
WFLU004 - Windows11 - Ring 1	Windows 11, version 22H2
WFLU005 - Windows11 - Ring 2	Windows 11, version 22H2
WFLU006 - Windows11 - Production	Windows 11, version 22H2

139

Microsoft Intune admin center

All services > Devices

Devices | Feature updates for Windows 10 and later

Name	Feature update version
WFLU001 - Windows10 - Ring 1	Windows 10, version 22H2
WFLU002 - Windows10 - Ring 2	Windows 10, version 21H2
WFLU003 - Windows10 - Production	Windows 10, version 22H2
WFLU004 - Windows11 - Ring 1	Windows 11, version 22H2
WFLU005 - Windows11 - Ring 2	Windows 11, version 22H2
WFLU006 - Windows11 - Production	Windows 11, version 22H2

140

Microsoft Intune admin center

Home > Devices | Feature updates for Windows 10 and later > WFLU004 - Windows11 - Ring 1 | Properties

Edit feature update deployment

Deployment settings Review + save

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

Name: WFLU004 - Windows11 - Ring 1
Description: 2023.09.26 - CloudWay template installed, Simon

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

141

Microsoft Intune admin center

Home > Devices | Feature updates for Windows 10 and later > WFLU004 - Windows11 - Ring 1 | Properties

Edit feature update deployment

Deployment settings Review + save

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

Name: WFLU004 - Windows11 - Ring 1
Description: 2023.09.26 - CloudWay template installed, Simon

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

142

Microsoft Intune admin center

Home > Devices | Feature updates for Windows 10 and later > WFLU004 - Windows11 - Ring 1 | Properties

Edit feature update deployment

Deployment settings Review + save

 Gabe Frost @bytnerd

See that new check box option under the Win11 version (the red box)? That is brand new (blog soon) and does the eligibility check automatically. So devices eligible for 11 get what you target, and ineligible get the latest 10.

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

143

4. Updates and Patches

Gabe Frost @tystenord
See that new check box option under the Win11 version (the red box)? That is brand new (blog soon) and does the eligibility check automatically. So devices eligible for 11 get what you target, and ineligible get the latest 10.

...so when you're ready for Win11 (and you should be by now) you can just use one Win11 feature update deployment policy to get ALL your Win10 & Win11 devices on the latest version.

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

144

4. Updates and Patches

All services > Devices
Devices | Driver updates for Windows 10 and later

Name	Assigned	Approval method
WOU001 - Driver Update - Ring 1	Yes	Automatic
WOU002 - Driver Update - Ring 2	Yes	Automatic
WOU003 - Driver Update - Production	Yes	Automatic
WOU004 - Driver Update - Manual update	Yes	Manual

145

4. Updates and Patches

Tenant admin | Tenant enrollment

Windows Autopatch

Windows Autopatch is an automated patch management service for Windows 10/11 Pro & Enterprise, Windows 365 clients, Microsoft 365 apps, Microsoft Teams, Microsoft Virtual Desktop, and Microsoft Edge. Windows 10/11 Enterprise E3 (or higher) is required to run the service. You must have the correct version of prerequisites. Learn more about our prerequisites. Windows Autopatch demos are available for all users regardless of prerequisites. Beta.

To check eligibility, start with the readiness assessment tool

The readiness assessment tool checks certain details of your Intune and Microsoft tenant to determine if you're eligible to begin testing when you enroll in Windows Autopatch. Run this tool whenever you want to confirm you've taken care of any reported issues.

We'll give you a list of things you need to do before enrolling in the tool. You must be signed in as at least Intune admin to run this tool. Some checks require administrative permissions.

146

4. Updates and Patches

Tenant admin | Tenant enrollment

This tool collects, assesses, and stores data in the service to perform the assessment. We do not collect or store personal data, nor share your data with other services. However, we do collect some data to provide you information to improve the service. We retain data for 12 months after you last use this tool to provide us improve the service. After 12 months, we retain it in de-identified form without company name. You can choose to delete the data we collect. Learn more about the privacy and review the privacy statement.

Select check box to allow Microsoft to assess and store results for the readiness assessment, and then select Agree.

Agree

147

4. Updates and Patches

Tenant admin | Tenant enrollment

Results

Run checks Export all Delete all data About this tool

This tool confirms that various Intune and Microsoft Intune settings are appropriate and meet prerequisites for Windows Autopatch. Learn more about Windows Autopatch.

Readiness status

LAST REFRESHED: 1/10/2023, 2:26 AM PM Ready

You are ready to enroll in Windows Autopatch, but you still have Advisory tasks. Complete these before you set up your first device.

Select Enroll to start your enrollment process.

Enroll

148

4. Updates and Patches

Windows Autopatch

- Create a Microsoft application that we use to run the Windows Autopatch service. Learn more about Windows Autopatch enterprise integration.
- Create the policies, groups and scripts necessary to run the service. This involves creating Windows Autopatch device groups, where specific policies and scripts are applied. To avoid conflicts, Windows Autopatch update policies must take precedence to avoid any conflicts. Learn more about changes made at tenant enrollment.
- Manage devices using Intune. Create and share info on usage, status, and compliance for devices and apps. Learn more about the data we collect.
- Store Windows Autopatch data securely in Azure data centers based on your data residency. Learn more about data storage and security.

I give Microsoft permission to manage my Microsoft Intune organization on my behalf.

Agree

149

4. Updates and Patches

Autopatch Operations can work with help you with issues that are outside the scope of your own IT operations.
We might have to contact this contact at any time, so choose contacts you're sure will be available. [Microsoft Privacy statement](#)

Provide contact info for your organization's Windows Autopatch admin.

Phone number: +47 91123260
Email: simon@skothemvalve.no
First Name: Simon
Last Name: Skothemvalve
Preferred Language: English

Primary Admin Secondary Admin

Next

150

4. Updates and Patches

Configure device features and settings

Windows Autopatch

Setting up Windows Autopatch

We're setting up policies and configuration for your tenant. This will take a few minutes.

151

4. Updates and Patches

Configure device features and settings

Windows Autopatch

Windows Autopatch setup is complete

Select Continue to start registering devices.

Continue

152

4. Updates and Patches

Configure device features and settings

Windows Autopatch

Devices

Autopatch groups set up is in progress

We're enabling Autopatch groups to manage in more detail how Windows Autopatch deploys updates. Learn more about Autopatch groups.

This could take up to 30 minutes. If you run into any issues, submit a support request.

153

4. Updates and Patches

Configure device features and settings

Devices | Overview

Preview upcoming changes to Devices and provide feedback.

Enrollment status Enrollment alerts Cloud PC performance (preview)

Windows Autopatch

By platform

Platform	Devices
Windows	23
iOS/iPadOS	8
Android	5
macOS	5
Linux	0
Windows Mobile	0
Total	41

154

4. Updates and Patches

Configure device features and settings

Devices | Overview

Windows Autopatch

By platform

Platform	Devices
Windows	23
iOS/iPadOS	8
macOS	5
Android	5
Chrome OS (preview)	0
Linux	0
Windows Mobile	0
Total	41

Quality Update Summary

No errors - Windows Autopatch can now apply quality updates to the following platforms: Windows, iOS/iPadOS, macOS, Android, Chrome OS (preview), Linux, and Windows Mobile.

As of 10/17/23 01:15 AM UTC, Windows Autopatch has successfully installed the October update between October 10 and 17, 2023, to the following platforms: Windows, iOS/iPadOS, macOS, and Android. In total, 41 devices were updated.

In fresh future updates, please turn on the Windows Autopatch Quality Update feature to receive notifications for updates. These include Windows Autopatch Quality Updates, which are designed to fix critical security vulnerabilities on Microsoft Azure. Windows Autopatch Quality Updates are more reliable than standard Windows updates.

155

4. Updates and Patches

156

4. Updates and Patches

157

4. Updates and Patches

158

4. Updates and Patches

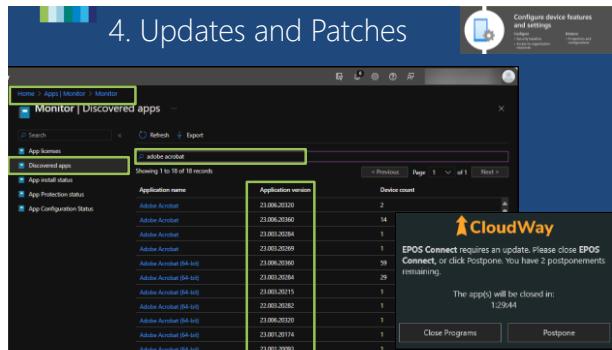
159

4. Updates and Patches

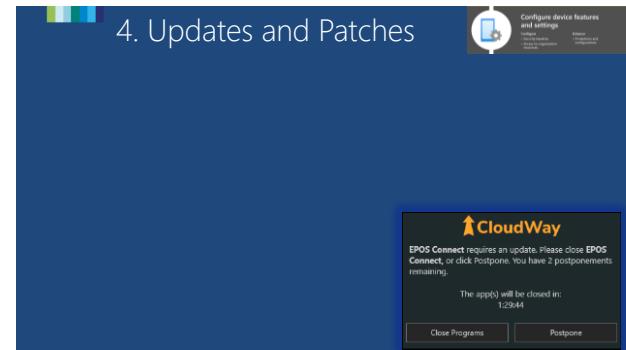
160

4. Updates and Patches

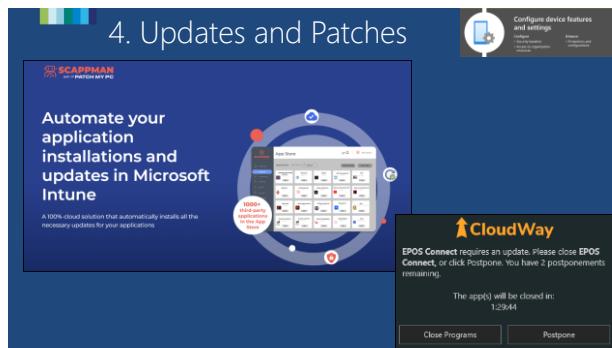
161



162



163



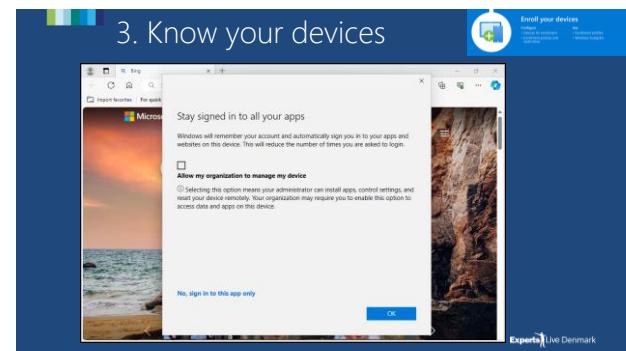
164



165



166



167

3. Know your devices

Welcome to the fresh look for Intune

Status

- Devices not in compliance: 0
- Configuration policies with error or conflict: 0
- Connector errors: 0
- Device health: Healthy
- Client app install failure: 0
- Account status: Active

168

3. Know your devices

Devices | Enrollment device platform restrictions

Windows restrictions | Android restrictions | macOS restrictions | iOS restrictions

Priority	Name	Assigned
Default	All Users	Yes

169

3. Know your devices

Edit restriction

Type: Windows (MDM)

Platform	versions	Personally owned	Device manufacturer
Allow	Block	Allow min/max range: Min: [] Max: []	Manufacturer name: []
Allow	Block	Allow min/max range: Min: [] Max: []	Manufacturer name: []
Allow	Block	Allow min/max range: Min: [] Max: []	Restriction not supported
Allow	Block	Allow min/max range: Min: [] Max: []	Restriction not supported
Allow	Block	Allow min/max range: Min: [] Max: []	Restriction not supported

170

3. Know your devices

Edit restriction

Type: Windows (MDM)

Platform	versions	Personally owned	Device manufacturer
Allow	Block	Allow min/max range: Min: [] Max: []	Manufacturer name: []
Allow	Block	Allow min/max range: Min: [] Max: []	Manufacturer name: []
Allow	Block	Allow min/max range: Min: [] Max: []	Restriction not supported
Allow	Block	Allow min/max range: Min: [] Max: []	Restriction not supported
Allow	Block	Allow min/max range: Min: [] Max: []	Restriction not supported

171

3. Know your devices

Edit restriction

Type: Windows (MDM)

Platform	versions	Personally owned	Device manufacturer
Allow	Block	Allow min/max range: Min: [] Max: []	Restriction not supported
Allow	Block	Allow min/max range: Min: [] Max: []	Allow [] Block []
Allow	Block	Allow min/max range: Min: [] Max: []	Restriction not supported

172

3. Know your devices

Devices | Overview

Enrollment status | Enrollment alerts | Cloud PC performance (preview) | Compliance status | Configuration

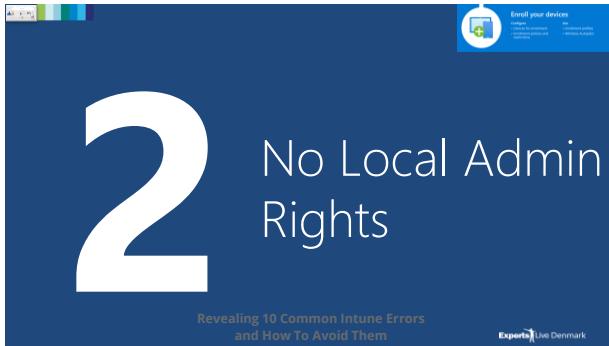
Intune enrolled devices last updated: 03/21/2024

Platform	Devices
Windows	23
iOS/PadOS	4
Android	5
macOS	2
Linux	0
Windows Mobile	0
Total	41

Enrollment failures by OS

Date	Windows	iOS/PadOS	Android	macOS	Linux	Windows Mobile
Mar 10	10	0	0	0	0	0
Mar 11	0	0	0	0	0	0
Mar 12	0	0	0	0	0	0
Mar 13	0	0	0	0	0	0
Mar 14	0	0	0	0	0	0
Mar 15	0	0	0	0	0	0
Mar 16	0	0	0	0	0	0
Mar 17	0	0	0	0	0	0
Mar 18	0	0	0	0	0	0
Mar 19	0	0	0	0	0	0
Mar 20	0	0	0	0	0	0
Mar 21	0	0	0	0	0	0

173



174



175



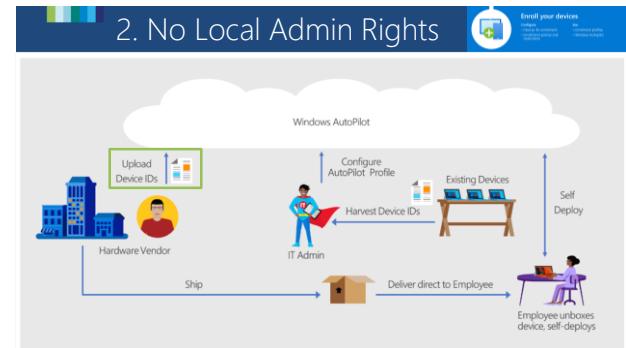
176



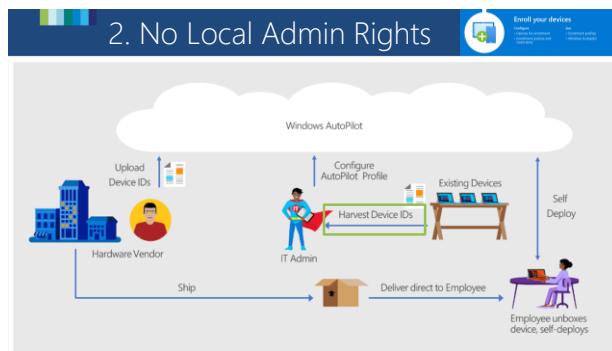
177



178



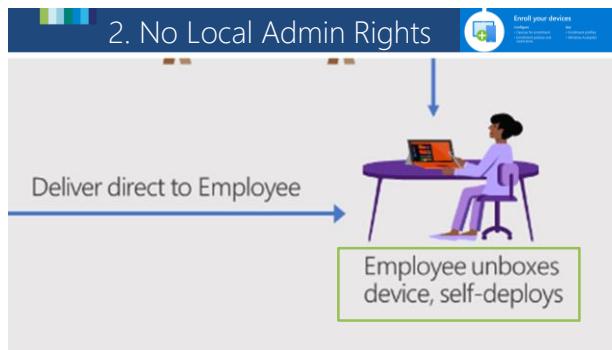
179



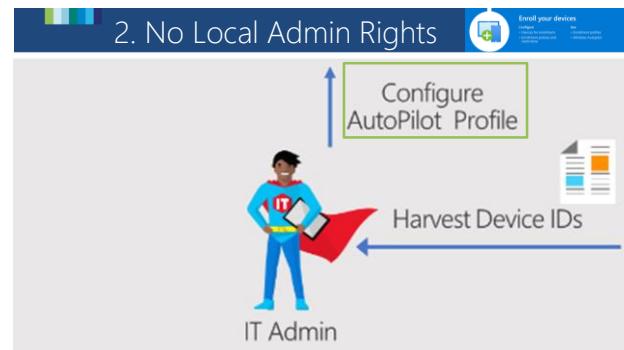
180



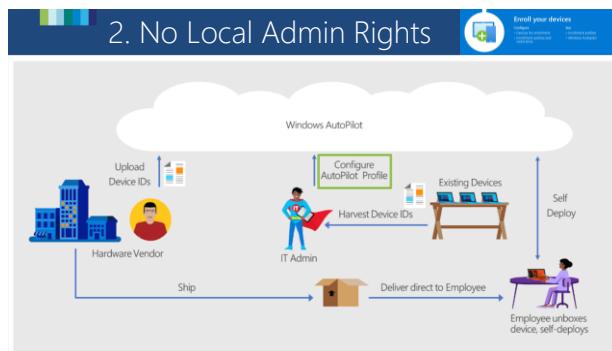
181



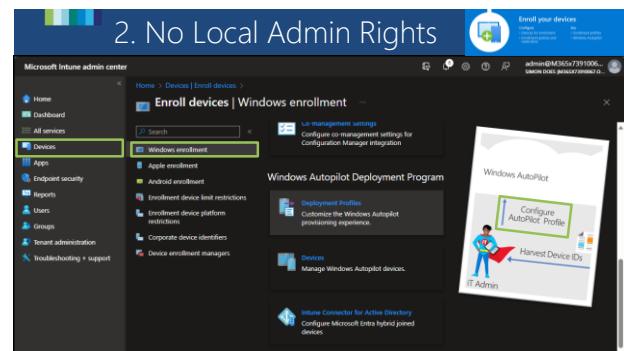
182



183



184



185

2. No Local Admin Rights

Microsoft Intune admin center

Home > Devices | Enrollment

Enroll devices | Windows enrollment

Windows Autopilot Deployment Program

Autopilot Profile | Configure Microsoft Intune hybrid joined devices

Devices | Manage Windows Autopilot devices.

186

2. No Local Admin Rights

Microsoft Intune admin center

Home > Devices | Enrollment

Enroll devices | Windows enrollment > Windows Autopilot deployment profiles > Autopilot Profile

Autopilot Profile | Properties

Autopilot Profile

No description

No

Windows PC

Out-of-box experience (OOBE) edit

User account type: Standard

187

2. No Local Admin Rights

Microsoft Intune admin center

Home > Devices

Devices | Device settings

Local administrator settings

Manage additional local administrators on all Microsoft Intune joined devices

Enable Microsoft Intune Local Administrator Password Solution (LAPS): No

188

2. No Local Admin Rights

Microsoft Intune admin center

Home > Devices | Windows | Scripts

WP5001 - Windows LAPS Account

Windows 10 and later

Script settings

Create LocalAdmin(LAPS).ps1

PowerShell script

Run this script using the logged on credentials

Enforce script signature check

Run script in 64 bit PowerShell host

Scope tag

Default

Assignments

Included groups: All Device-Intune-All Windows 10 Devices

Excluded groups: All Device-Intune All Windows 11 Devices

https://github.com/sandysang/MSIntune/tree/master/Intune-PowerShell/WindowsLAPS

189

2. No Local Admin Rights

Microsoft Intune admin center

Home > Endpoint security

Endpoint security | Account protection

Policy name: WESP01 - ACP - Windows Hello for Business

Policy type: Account protection (Preview)

Assigned

WESP02 - ACP - Windows LAPS

Local admin password solution (Windows LAPS)

Assigned

WESP03 - ACP - Local Administrators

Local user group membership

Assigned

190

2. No Local Admin Rights

Microsoft Intune admin center

Home > Endpoint security

Endpoint security | Account protection

Policy name: WESP01 - ACP - Windows Hello for Business

Policy type: Account protection (Preview)

Assigned

WESP02 - ACP - Windows LAPS

Local admin password solution (Windows LAPS)

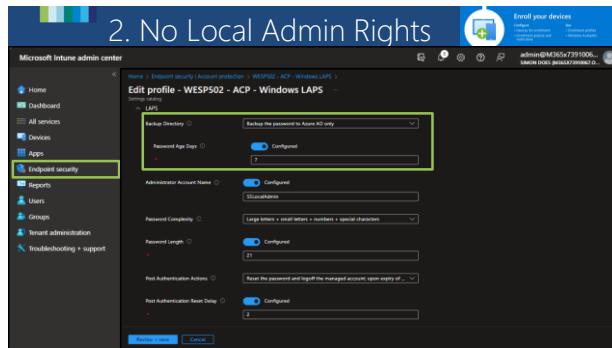
Assigned

WESP03 - ACP - Local Administrators

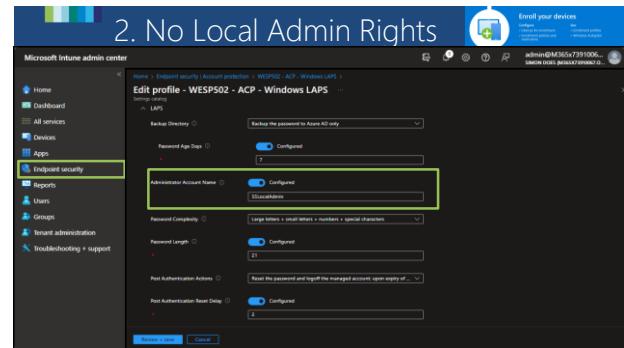
Local user group membership

Assigned

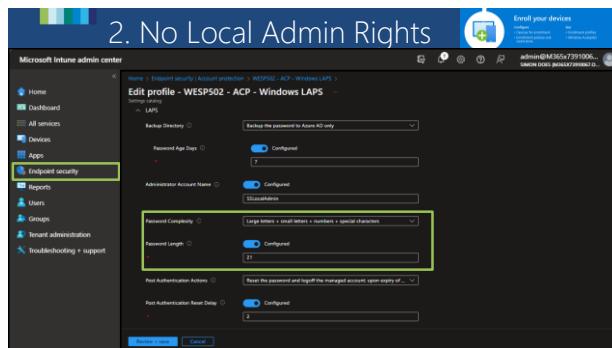
191



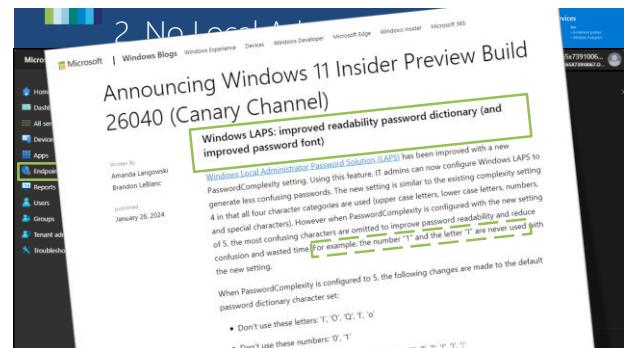
192



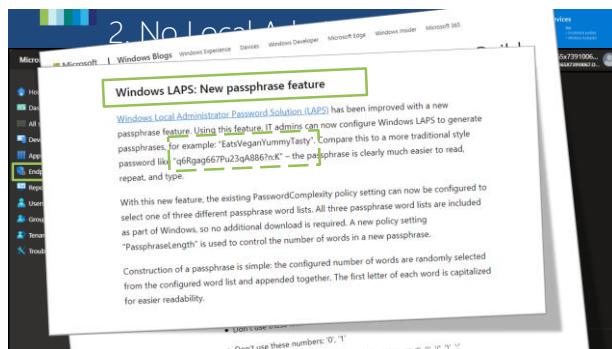
193



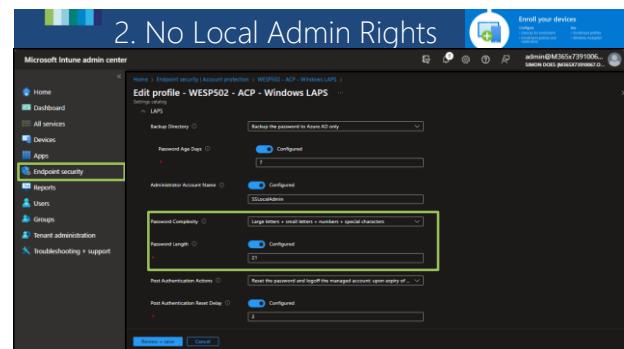
194



195



196



197

2. No Local Admin Rights

Microsoft Intune admin center

Edit profile - WESP02 - ACP - Windows LAPS

Post Authentication Actions: Reset the password and logoff the managed account upon expiry Post Authentication Reset Delay

Administrator Account Name: S\$localadmin

198

2. No Local Admin Rights

Microsoft Intune admin center

Endpoint security | Account protection

Policy name	Policy type	Assigned
WESP01 - ACP - Windows Hello for Business	Account protection (Preview)	Yes
WESP02 - ACP - Windows LAPS	Local admin password solution (Windows LAPS)	Yes
WESP03 - ACP - Local Administrators	Local user group membership	Yes

199

2. No Local Admin Rights

Microsoft Intune admin center

Edit profile - WESP03 - ACP - Local

Add users

Local users And Groups	Group and user action
Administrators	Add (Replace)
Administrator	Add (Replace)

LAPS Account
Builtin local Administrator

Entra ID Global Administrator Role and Entra ID Device Administrator Role

200

2. No Local Admin Rights

Microsoft Intune admin center

Edit profile - WDCP019 - OS - Disable Local Administrator

Configuration settings

Local Policies Security Options	
Accounts Enable Administrator Account	Disable
Accounts Rename Administrator Account	BuiltInAdmin

201

2. No Local Admin Rights

Microsoft Intune admin center

CLOUDWAY-875 | Local admin password

Local administrator password

Last password rotation: 10/25/2023, 10:00:13 AM
Next password rotation: 10/30/2023, 11:06:13 AM

202

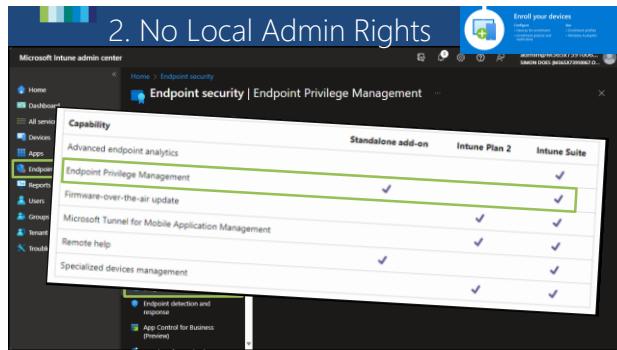
2. No Local Admin Rights

Microsoft Intune admin center

Endpoint security | Endpoint Privilege Management

Endpoint Privilege Management is now generally available. To use this add-on, your Global or Billing Administrator can start a trial or buy licenses.

203



204

2. No Local Admin Rights
If you don't have admin rights,
you can't break your computer!

75% 60%

less Helpdesk tickets less reinstallations

Experts Live Denmark

205



207

1 HYBRID

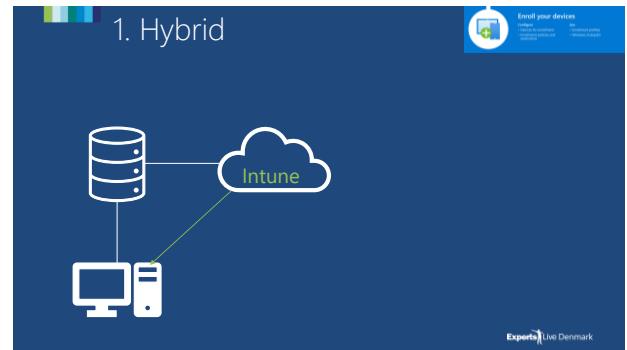
Revealing 10 Common Intune Errors
and How To Avoid Them

Experts Live Denmark

208



209



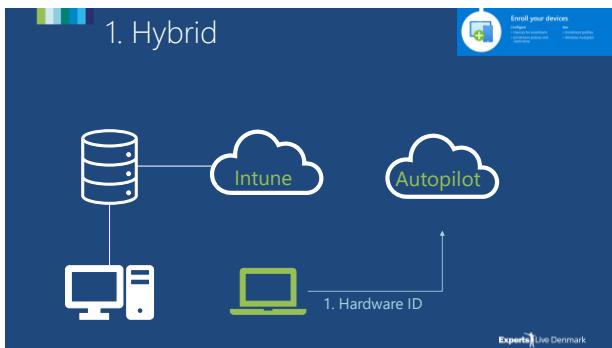
210



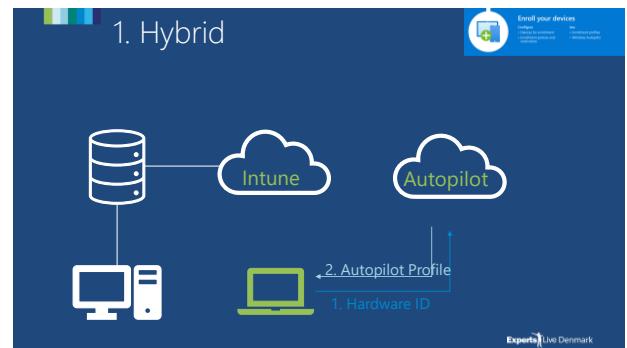
211



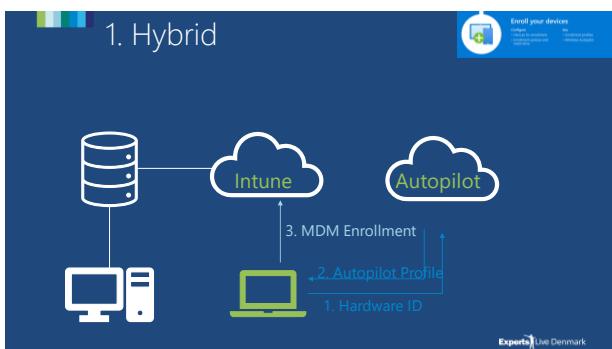
212



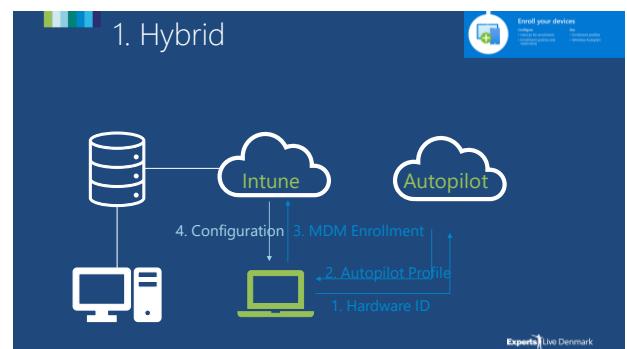
213



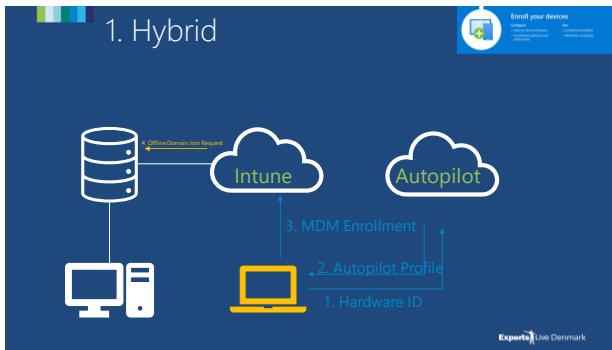
214



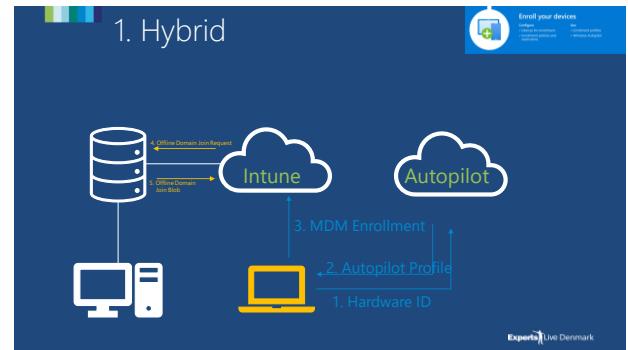
215



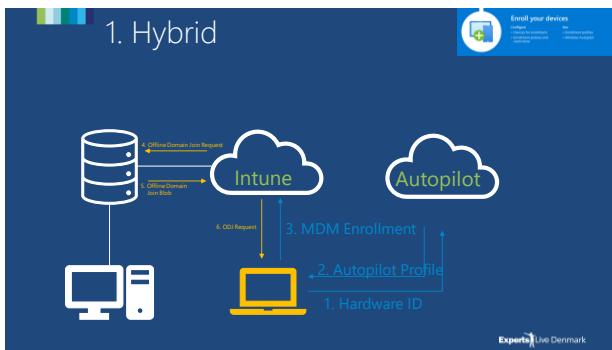
216



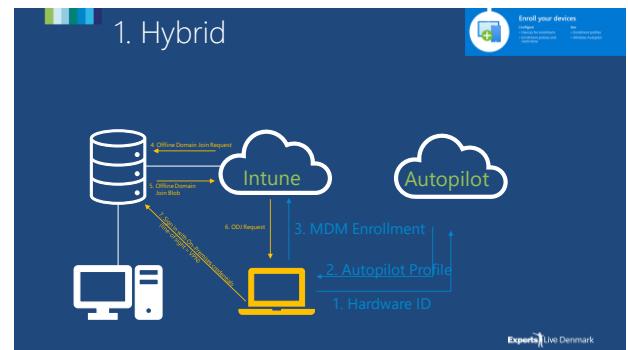
217



218



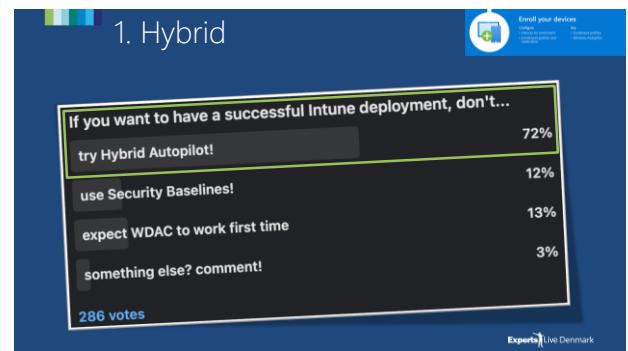
219



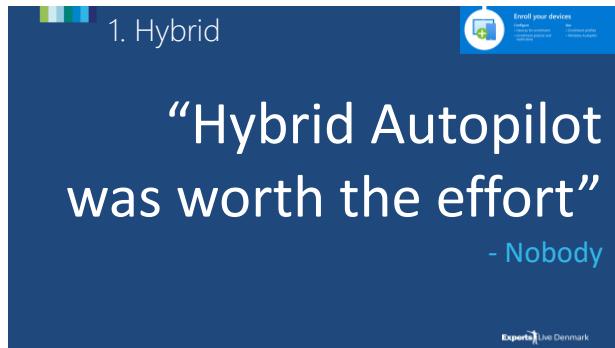
220



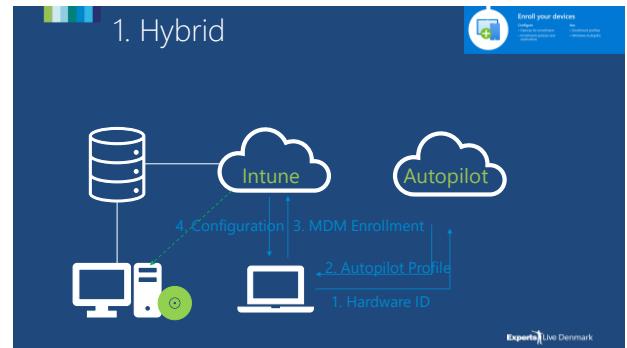
221



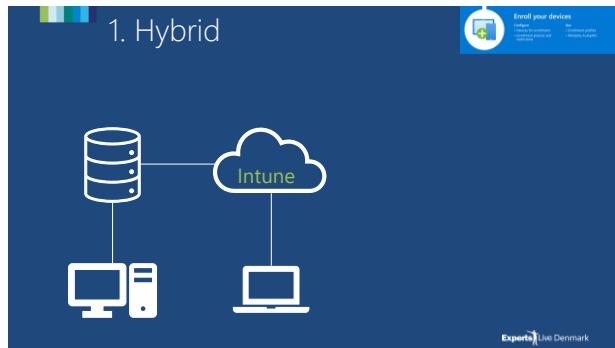
222



223



224



225



226

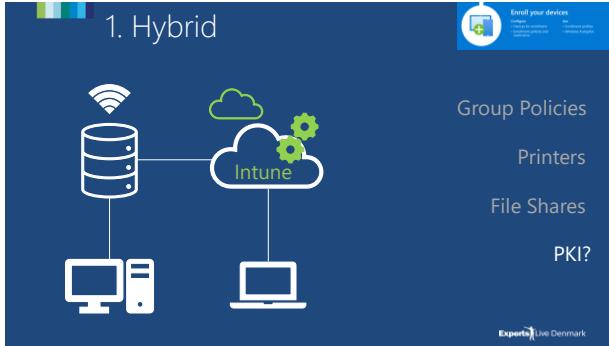


227

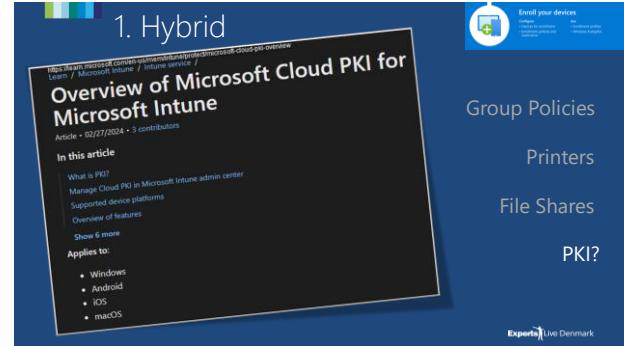


228

1. Hybrid



229

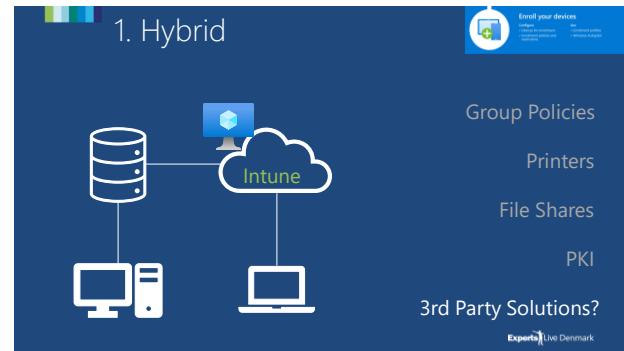


230

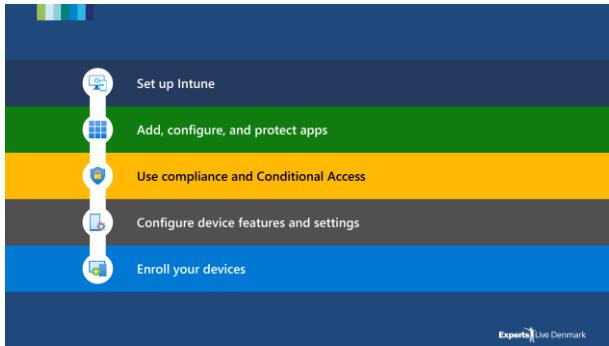
1. Hybrid

The screenshot shows a presentation slide titled "Overview of Microsoft Cloud PKI for Microsoft Intune". The slide includes a URL (<https://learn.microsoft.com/en-us/microsoft-365/cloud-pki-overview>), a date (April 16, 2022), and a location (Microsoft Ignite). It features a yellow header bar with "Security" and a "Breakout #2 - 1.06" button. The main content area contains a video player showing a speaker named Tbome Granheden, a timestamp (20th Mar 2024, 1:10pm CET - 2:00pm CET), and a session title ("Simplify your certificate management with Microsoft Cloud PKI"). To the right of the slide, there is a vertical sidebar with navigation links: "Group Policies", "Printers", "File Shares", and "PKI?". At the bottom right, there is a logo for "Experts Live Denmark".

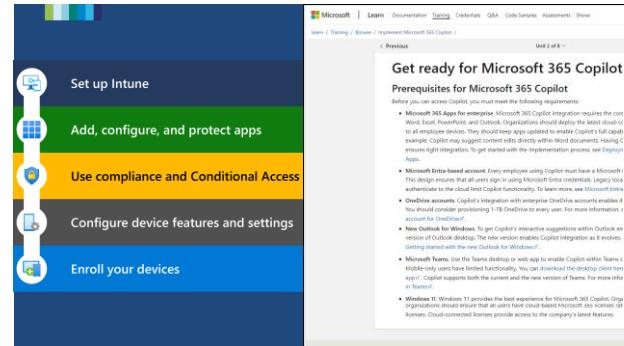
231



232



233



234



235

Get ready for Microsoft 365 Copilot

Prerequisites for Microsoft 365 Copilot

- Microsoft 365 Apps for Enterprise (current channel)*
- OneDrive
- New Outlook for Windows
- Windows 11 (preferred)
- Microsoft 365 E3 or E5 or Business Premium licences
- Microsoft Entrusted account
- Teams (either version)
- Loop



236



237



238