SHARING KNOWLEDGE.
TOGETHER.

WORKPLACE NINJA SUMMIT

SUMMIT
SUMMIT
SUMMIT
SUMMIT
SUMMIT

WORKPLACE NINJA SUMMIT

Mastering shared Windows devices in your environment

Peter van der Woude

WORKPLACE NINJA SUMMIT

Glasssaal room check-in

Thank you to our sponsors!

WORKPLACE NINJA SUMMIT

PLATINUM SPONSORS

glueck kanja

PATCH MY PC

Recast

2Pint

Microsoft

GOLD SPONSORS

control up

Admin By Request
ZERO TRUST PLATFORM

eido

THREATLOCKER®
ZERO TRUST PLATFORM

inforcer

baseVISION
Trusted Swiss Cybersecurity

robopack

EPIC FUSION
BRING IT ALL TOGETHER

nerdio

SILVER SPONSORS

systemcenterdudes

Apento

water
IT Security & Defense

ugurlabs

About Peter van der Woude

Focus

Modernizing endpoints

From

Groningen, Netherlands

Blog

https://petervanderwoude.nl

Workplace
Solution architect

Security
Windows and Device

Certifications

Microsoft 365 Certified: Enterprise Administrator Expert

Microsoft 365 Certified: Modern Desktop Administrator Associate

Hobbies

Spending time with my family

Playing and watching basketball

Building Lego and playing games

Contact

pvanderwoude@hotmail.com

@pvanderwoude

/peterwoude


POPCORN
POPCORN

What are we going to discuss?

WORKPLACE NINJA SUMMIT

Architecture and core concepts

Basic configuration options

Additional configurations that should be considered

Deployment options and assignment considerations

A successful shared Windows device is not a single configuration. It is the alignment of experience, identity, applications, security and deployment.

WORKPLACE NINJA SUMMIT

Concepts

Architecture and core concepts

Characteristics of shared devices

WORKPLACE NINJA SUMMIT

What are the main characteristics of shared devices?

Many different users

Same experience every time*

No personal device ownership

*Within the boundaries of the assigned role and configuration.

Important decisions to make

What are the important decisions to make before starting?

Managing expectation of the device

What configuration model should be used for the shared devices?

Shared PC
Multiple people sign in on the device, one at a time

Kiosk
Device is locked to a dedicated app or task

Handling identity of the user

What user account should be used for the shared devices?

Entra ID account
Local account

Conditional Access and MFA

Local storage of account information

Handling assignments to device

What would be the best assignments for shared devices?

No primary user
Be careful with applications and scripts that follow the user

Filters
Use filters, when possible, to target specific devices only

Thinking about device licensing

What licensing should be used for shared devices?

Often covered by existing licenses of users using the device. Especially when talking about Shared PCs

Might be required when device is used by users without eligible licenses, like: Temporary workers, local or shared accounts, public-access

Device licenses do not support Intune app protection policies, Conditional Access, and user-based management features.

Managing expectation of the device

What configuration model should be used for the shared devices?

Shared PC

Multiple people sign in on the device, one at a time

Kiosk

Device is locked to a dedicated app or task

Handling identity of the user

WORKPLACE NINJA SUMMIT

What user account should be used for the shared devices?

Entra ID account
Local account

Conditional Access and MFA

Local storage of account information

Handling assignments to device

What would be the best assignments for shared devices?

No primary user

Be careful with applications and scripts that follow the user

Filters

Use filters, when possible, to target specific devices only

Thinking about device licensing

WORKPLACE NINJA SUMMIT

What licensing should be used for shared devices?

Often covered by existing licenses of users using the device. Especially when talking about Shared PCs

Might be required when device is used by users without eligible licenses, like: Temporary workers, local or shared accounts, public-access

Device licenses do not support Intune app protection policies, Conditional Access, and user-based management features.

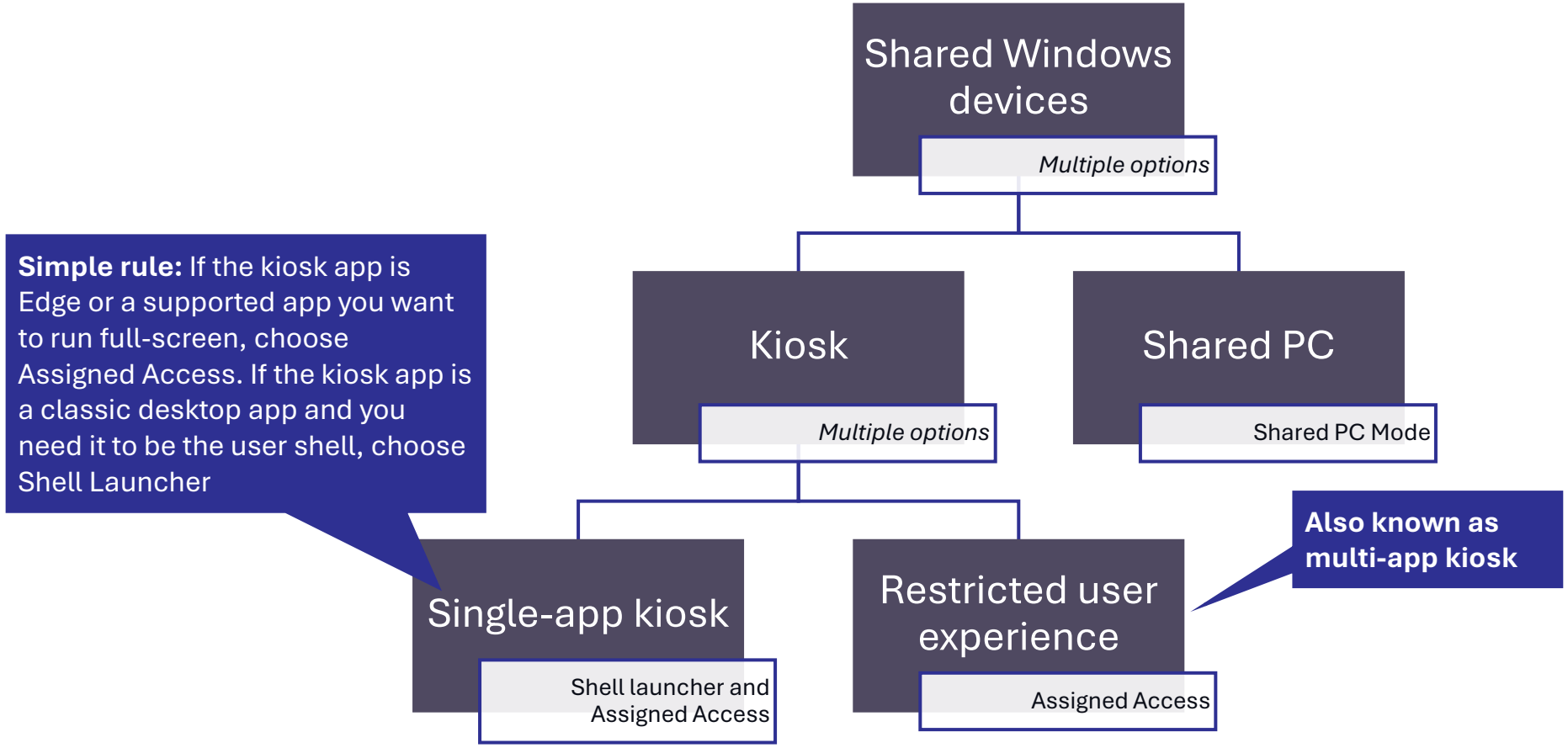
WORKPLACE NINJA SUMMIT

Configuration

Basic configuration options

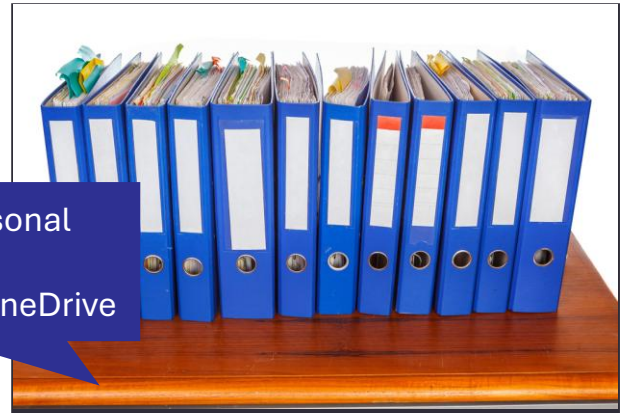
Choosing the deployment model

What are the technical options for configuring shared devices?



Shared PC Mode basics

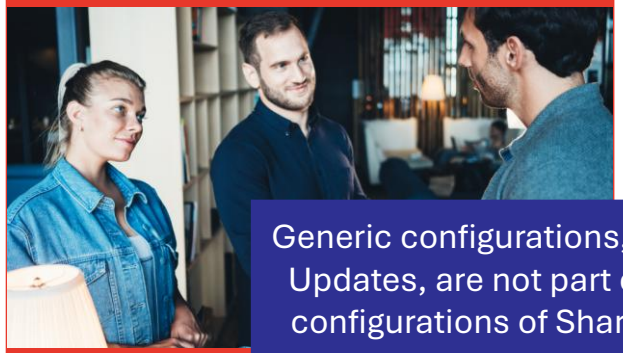
What are the main configurations that are part of Shared PCs?



Consider using Personal Data Encryption in combination with OneDrive

With or without OneDrive

Exclusions are possible HKLM\SOFTARE\Microsoft\Windows\CurrentVersion\SharedPC\Exemptions\



Generic configurations, like Windows Updates, are not part of the default configurations of Shared PC Mode.

Account management

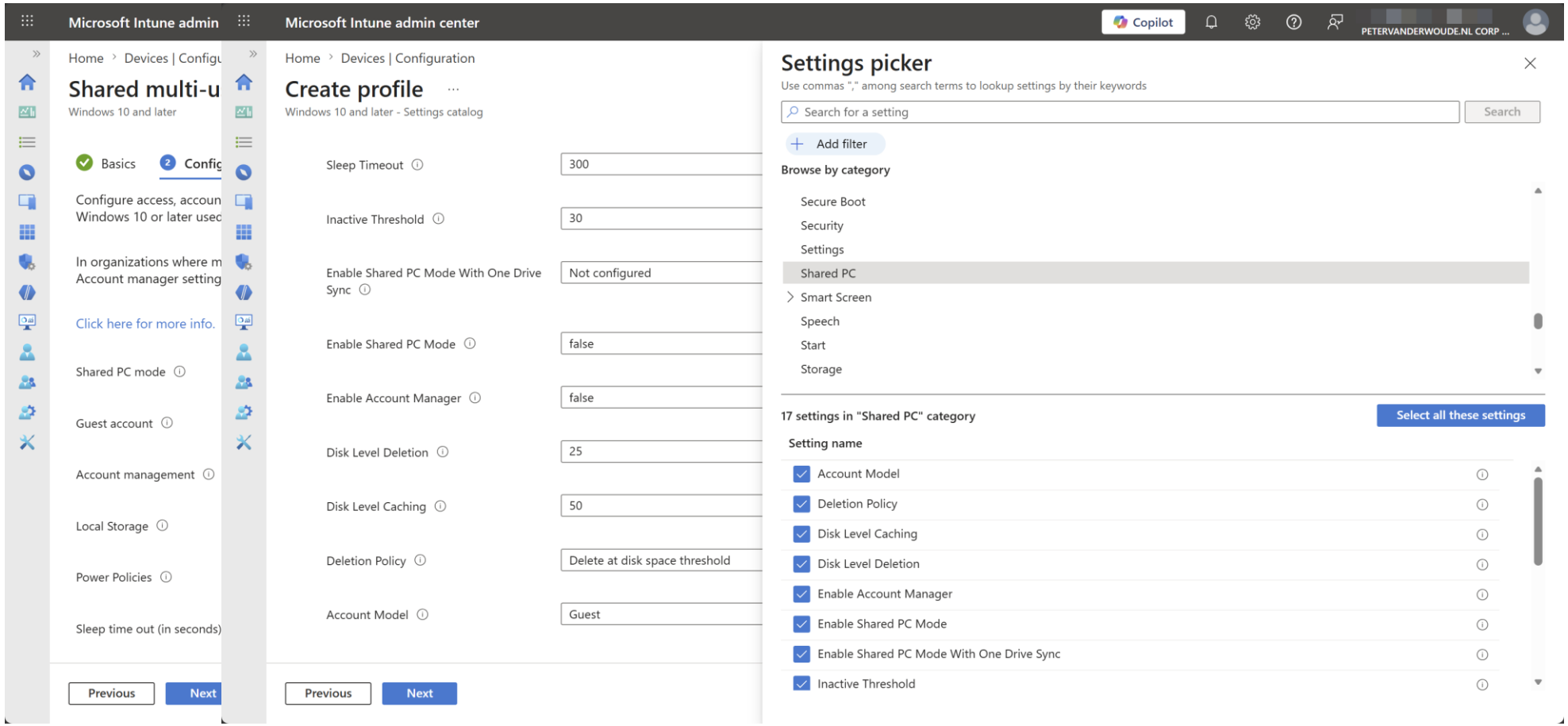
- Account manager
- Account model

Advanced customizations

- Power
- Sleep
- Sign-in
- Maintenance
- Pagefile
- Local storage

Technical reference: Shared PC technical reference | Microsoft Learn

What does it look like in Intune?



Assigned Access basics

Generic configurations, like Windows Updates and Power, are not part of the default configurations.

Profile

Allowed apps

Start layout

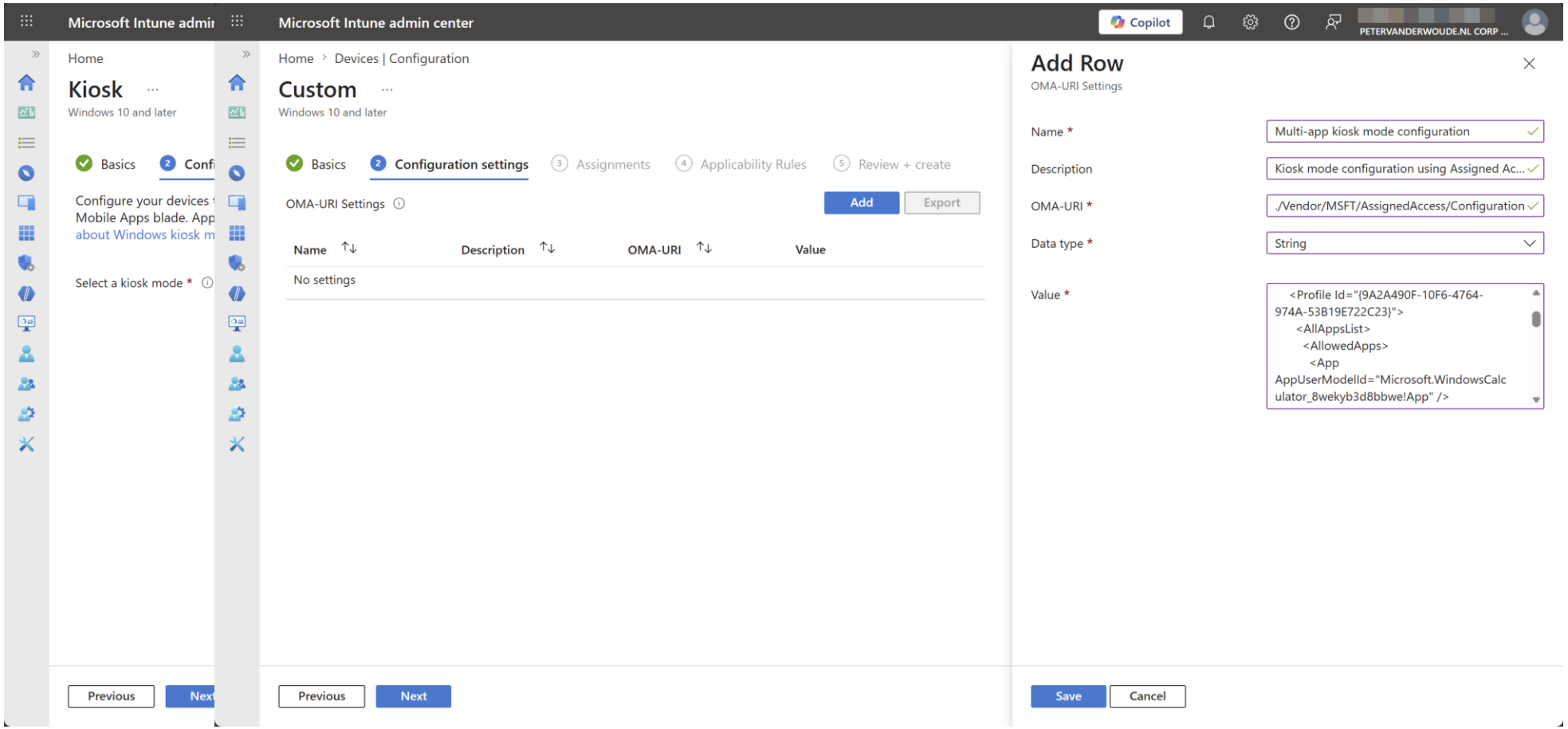
Taskbar

Account

Autologon

Technical reference: Assigned Access Policy Settings | Microsoft Learn

What does it look like in Intune?



Assigned Access XML basics

```
<?xml version="1.0" encoding="utf-8" ?>
<AssignedAccessConfiguration
xmlns="http://schemas.microsoft.com/AssignedAccess/2017/config">
  <Profiles>
    <Profile Id="{GUID}">
      <!-- Add configuration here as needed -->
    </Profile>
  </Profiles>
  <Configs>
    <Config>
      <!-- Add configuration here as needed -->
    </Config>
  </Configs>
</AssignedAccessConfiguration>
```

Each profile defines a set of applications that are allowed to run

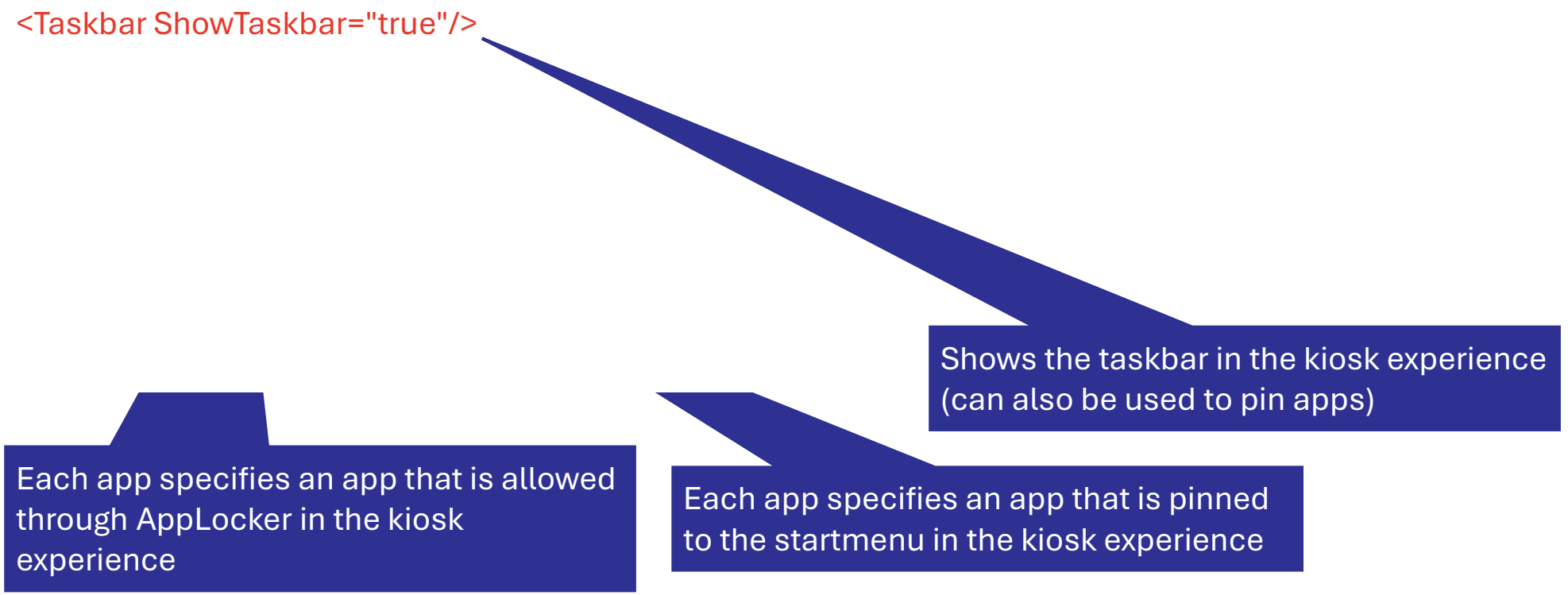
Each version is used to determine which features are available for the configuration

Each config associates a user account or a group to a profile

Assigned Access versioning

Version	Alias	Namespace
Windows 11, version 2H2	v5	http://schemas.microsoft.com/AssignedAccess/2022/config
Windows 11, version 21H2	v4	http://schemas.microsoft.com/AssignedAccess/2021/config
Windows 10	v5	http://schemas.microsoft.com/AssignedAccess/202010/config
Windows 10	v3	http://schemas.microsoft.com/AssignedAccess/2020/config
Windows 10	rs5	http://schemas.microsoft.com/AssignedAccess/201810/config
Windows 10	default	http://schemas.microsoft.com/AssignedAccess/2017/config

Assigned Access XML profiles



Assigned Access XML config

```
<Configs>
 <Config>
  <AutoLogonAccount rs5:DisplayName="Kiosk user"/>
  <DefaultProfile Id="{GUID}"/>
 </Config>
</Configs>
```

Uses an autologon account that will be automatically created.

```
<Configs>
 <v3:GlobalProfile Id="{GUID}"/>
</Configs>
```

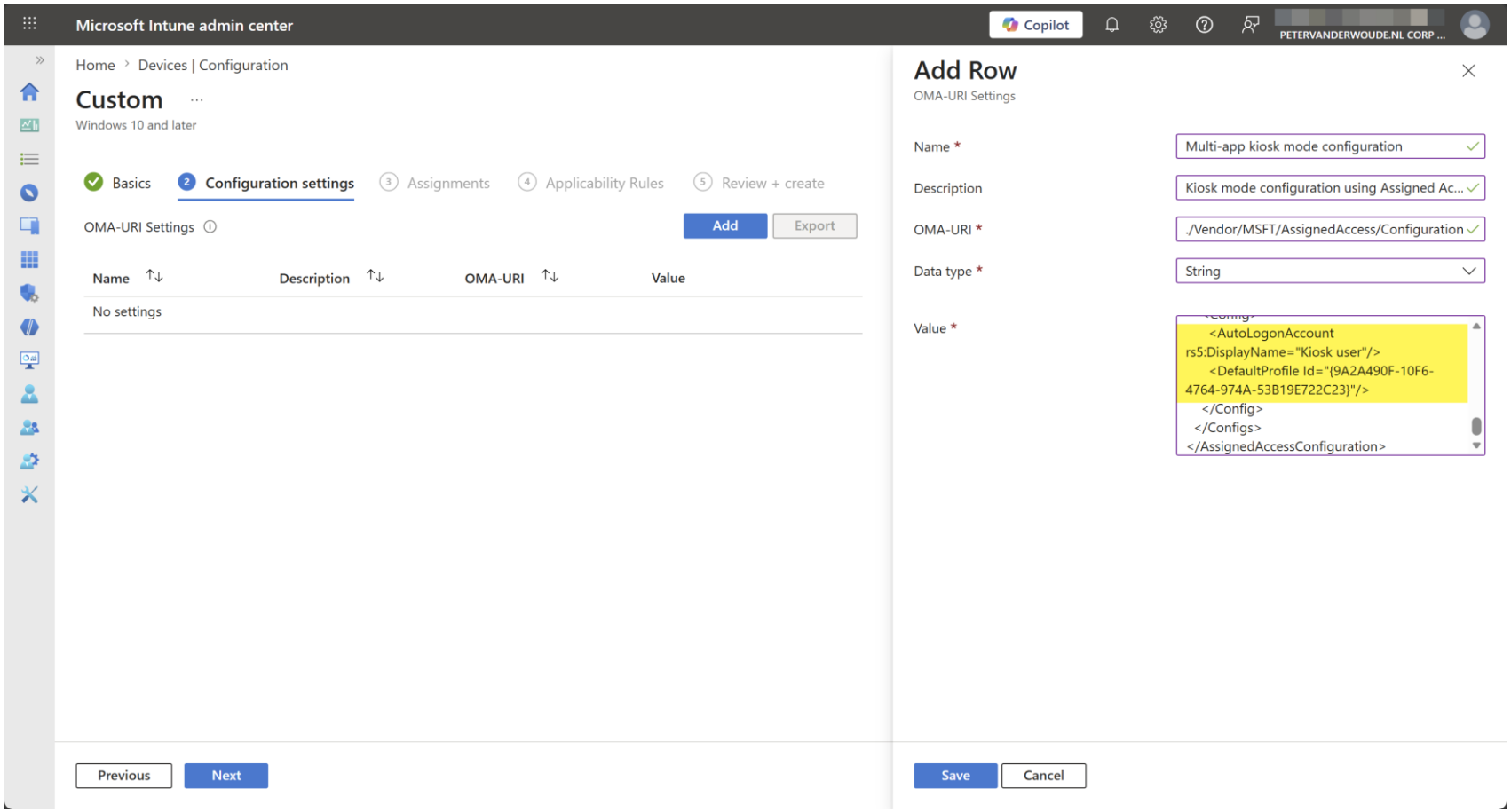
Uses the same configuration for every user that signs in.

```
<Config>
 <Account>AzureAD\user@contoso.onmicrosoft.com</Account>
 <DefaultProfile Id="{GUID}"/>
</Config>
```

Uses a specific configuration for the specified user or group.

Can be used for local user (.\user), Entra user (example), AD user (domain\user), and groups.

What does it look like in Intune?



WORKPLACE NINJA SUMMIT

Recommendations

Additional configurations that should be considered

Recommendations

WORKPLACE NINJA SUMMIT

Tuning Windows Updates

Removing power settings

Disabling keyboard shortcuts

Deploying apps

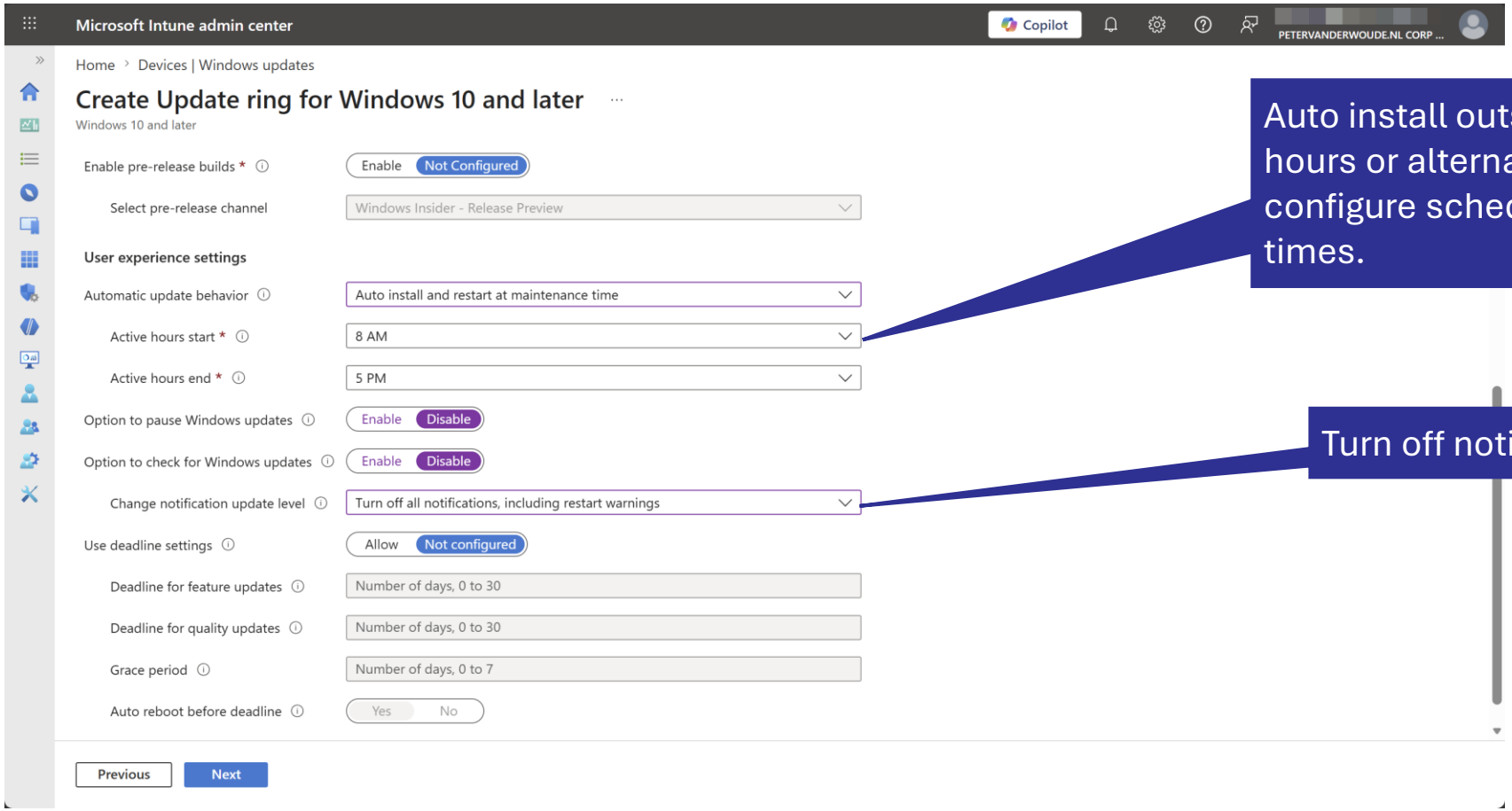
Preventing notifications

Troubleshooting and logs

Technical reference: Assigned Access Recommendations | Microsoft Learn

Tune Windows updates

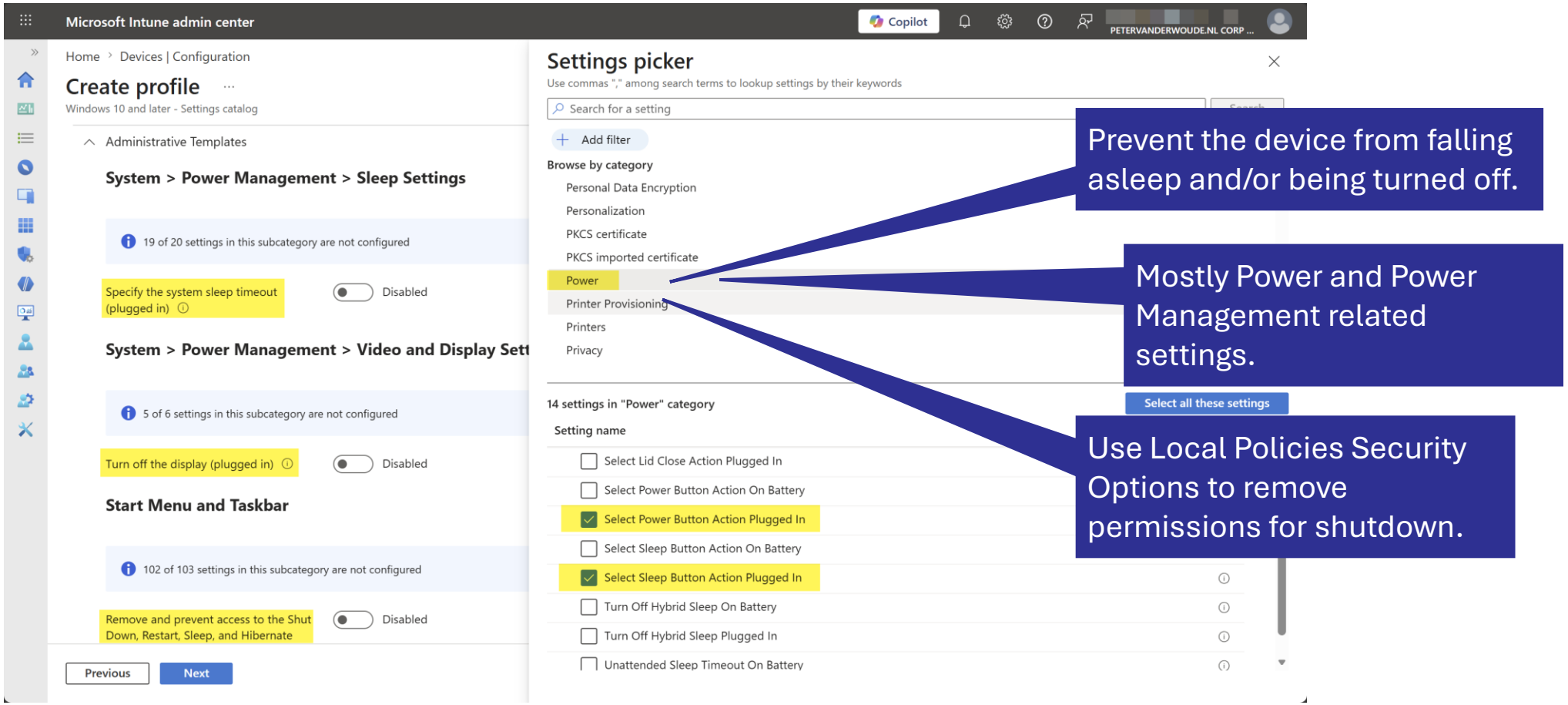
At least for kiosk devices and depending on the shared device usage



Remove power settings

At least for kiosk devices and depending on the shared device usage

Shared device configuration contains default power settings.



Disable keyboard shortcuts

At least for kiosk devices and depending on the shared device usage

The Keyboard Filter feature can be used to suppress specific unwanted key combinations, and it works with physical keyboards, the Windows on-screen keyboard, and the touch keyboard.

Enable the Windows feature.

```
Enable-WindowsOptionalFeature -Online -FeatureName Client-KeyboardFilter -All -NoRestart

$CommonParams = @{"namespace"="root\standardcimv2\embedded"}
$CommonParams += $PSBoundParameters
function Enable-Predefined-Key($Id) {
        $predefined = Get-WMIObject -class WEKF_PredefinedKey @CommonParams |
                where {
                        $_.Id -eq "$Id"
                };
        if ($predefined) {
                $predefined.Enabled = 1;
                $predefined.Put() | Out-Null;
                Write-Host Enabled $Id
        }
        else {
                Write-Error "$Id is not a valid predefined key"
        }
}
Enable-Predefined-Key "Alt+Tab"
```

Disable the specified key combinations.

Deploying apps

At least for kiosk devices and depending on the shared device usage

Apps that follow the user leave a trace of installations.

1. Deploy apps to devices

E.g. OneDrive on shared devices, or Explorer in kiosk mode.

2. Do not use an app that might expose (personal) data

Apps that are later installed cannot be used in configuration.

3. App must be installed before the configuration

4. Microsoft Edge has its own kiosk mode

Provides automatic limited experience.

5. App cannot launch another app in kiosk mode

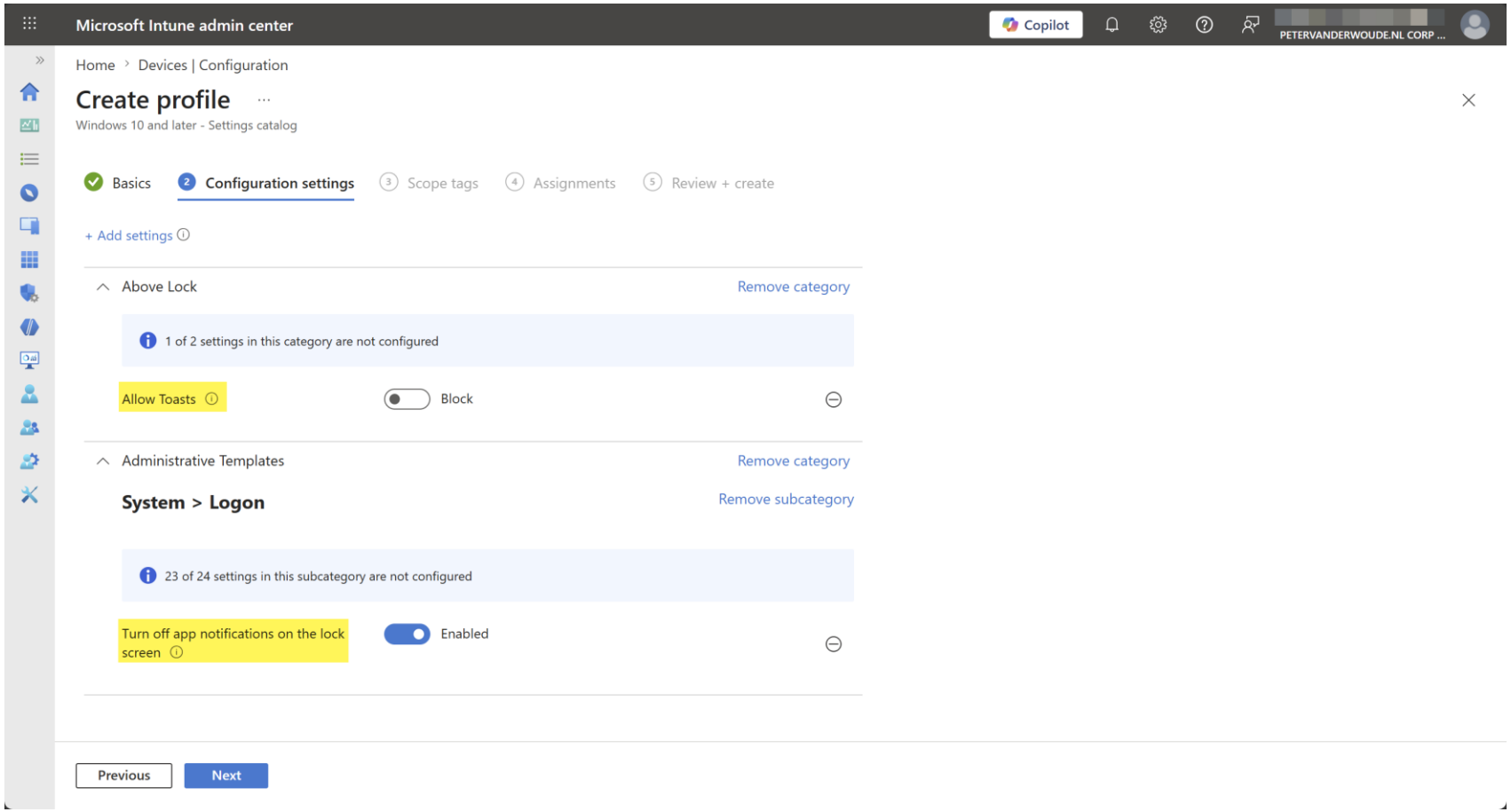
Breaks automatic behavior of kiosk.

6. Prevent apps that require user sign-in in kiosk mode

Kiosk mode is locked down with AppLocker.

Prevent lockscreen notifications

At least for kiosk devices and depending on the shared device usage



Troubleshooting and log locations

WORKPLACE NINJA SUMMIT

Shared PC

Log location

- C:\Windows\SharedPCSetup.log

Registry location

- HKLM\Software\Microsoft\Windows\CurrentVersion\SharedPC

Assigned Access

Log location

- Applications and Services Logs > Microsoft > Windows > AssignedAccess > Operational

Registry location

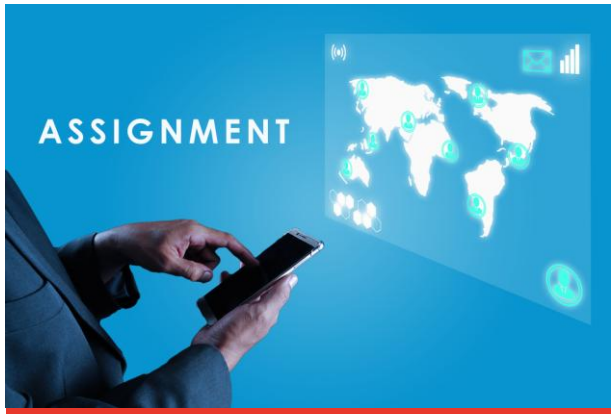
- HKLM\Software\Microsoft\Windows\AssignedAccessConfiguration
- HKLM\Software\Microsoft\Windows\AssignedAccessCsp
- HKCU\Software\Microsoft\Windows\AssignedAccessConfiguration

Deployment

Deployment options and assignment considerations

Deployment alignment

Deployment of the device



Assignments of the policies

Layering of policies

Self-deploying devices

Group devices using (device.devicePhysicalIds -any (_ -eq "[OrderID]:KIOSK"))

- No user interaction required for devices with Ethernet connection
- Joins the device to Entra ID and enrolls the device into Intune
- Provisions all policies, applications, certificates, and networking profiles on the device
- Relies on Enrollment Status Page to prevent access to the device
- No automatic primary user configuration for the device
- Requires TPM 2.0

Group/Filter devices (device.enrollmentProfileName -eq "Autopilot profile for Windows kiosk devices")

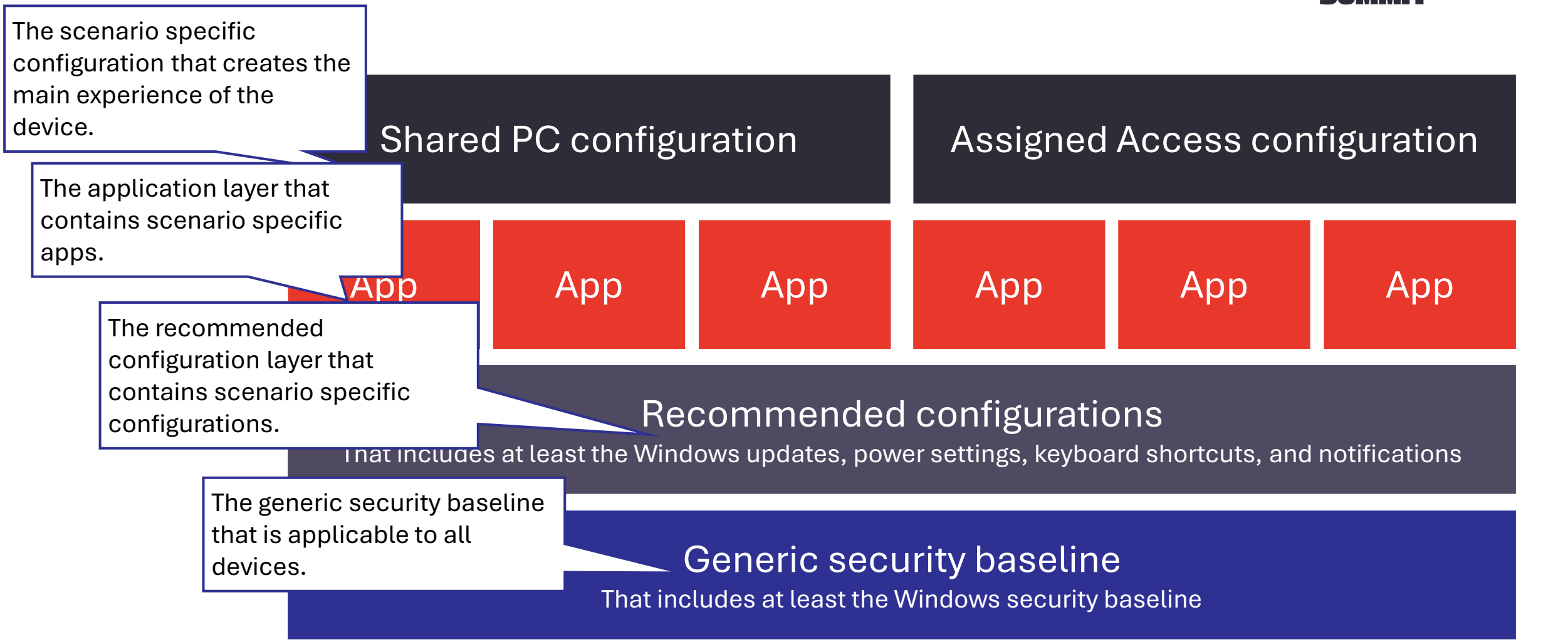
Handling assignments

Not easy to combine multiple filters

1. Always assign apps and configurations to devices
2. Use filters to exclude shared devices from user assignments
3. Deploy apps before applying configurations that require the apps
4. Don’t forget app specific configuration for shared devices

Think about the Microsoft 365 apps activation configuration for shared devices

Layering configurations



Bonus: A few common challenges

WORKPLACE NINJA SUMMIT

Autologon is not working on a Windows kiosk device

- Device lock configuration (often part of security baseline)
- Preferred Entra domain configuration
- Password policy as part of a compliance policy

OneDrive configuration is not working on shared Windows device

- Conflicting configurations
- Shared PC Mode was already enabled

Missing settings

./Device/Vendor/MSFT/Policy/Config/Start/HideRecommendedSection
./User/Vendor/MSFT/Policy/Config/Notifications/DisableAccountNotifications

Mastering shared Windows devices

A reliable shared device is the result of aligned layers, not a single configuration

WORKPLACE NINJA SUMMIT

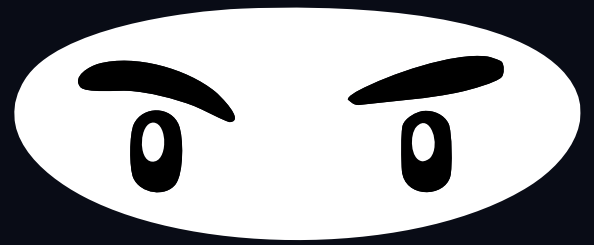
1	**EXPERIENCE**	**Choose the right experience** Shared PC | Single-app kiosk | Restricted user experience
2	**IDENTITY AND APPLICATIONS**	**Design for the user interaction** Identity | Licensing | Applications
3	**OPERATIONS**	**Keep the device reliable** Updates | Power | Notifications | Profiles | Troubleshooting
4	**SECURITY AND DEPLOYMENT**	**Build on a consistent foundation** Security | Compliance | Assignments | Deployment

Start with the experience. Design the layers. Validate the complete lifecycle.

Thank You, Ninjas!

SUMMIT
SUMMIT
SUMMIT
SUMMIT
SUMMIT

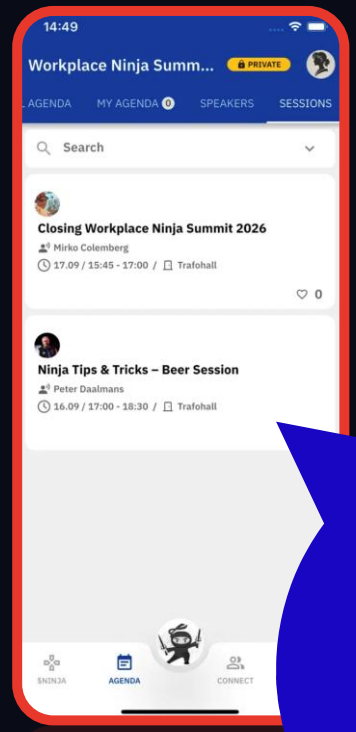
See You Next Year!



Download the app and never miss any updates

GET IT ON Google Play Store

Download on the App Store



We appreciate your feedback!