

**SHARING KNOWLEDGE.
TOGETHER.**

**WORKPLACE
NINJA**

**SUMMIT
SUMMIT
SUMMIT
SUMMIT
SUMMIT**



Mastering shared Windows devices in your environment

Peter van der Woude



Glasssaal
room check-in



Thank you to our sponsors!



PLATINUM SPONSORS

glueck■kanja



Recast

2Pint



GOLD SPONSORS

control up



eido

THREATLOCKER®
ZERO TRUST PLATFORM

inforcer

baseVISION
Trusted Swiss Cybersecurity



nerdio

SILVER SPONSORS



Apento



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











What are we going to discuss?



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.

Concepts

Architecture and core concepts



Characteristics of shared devices

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

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.

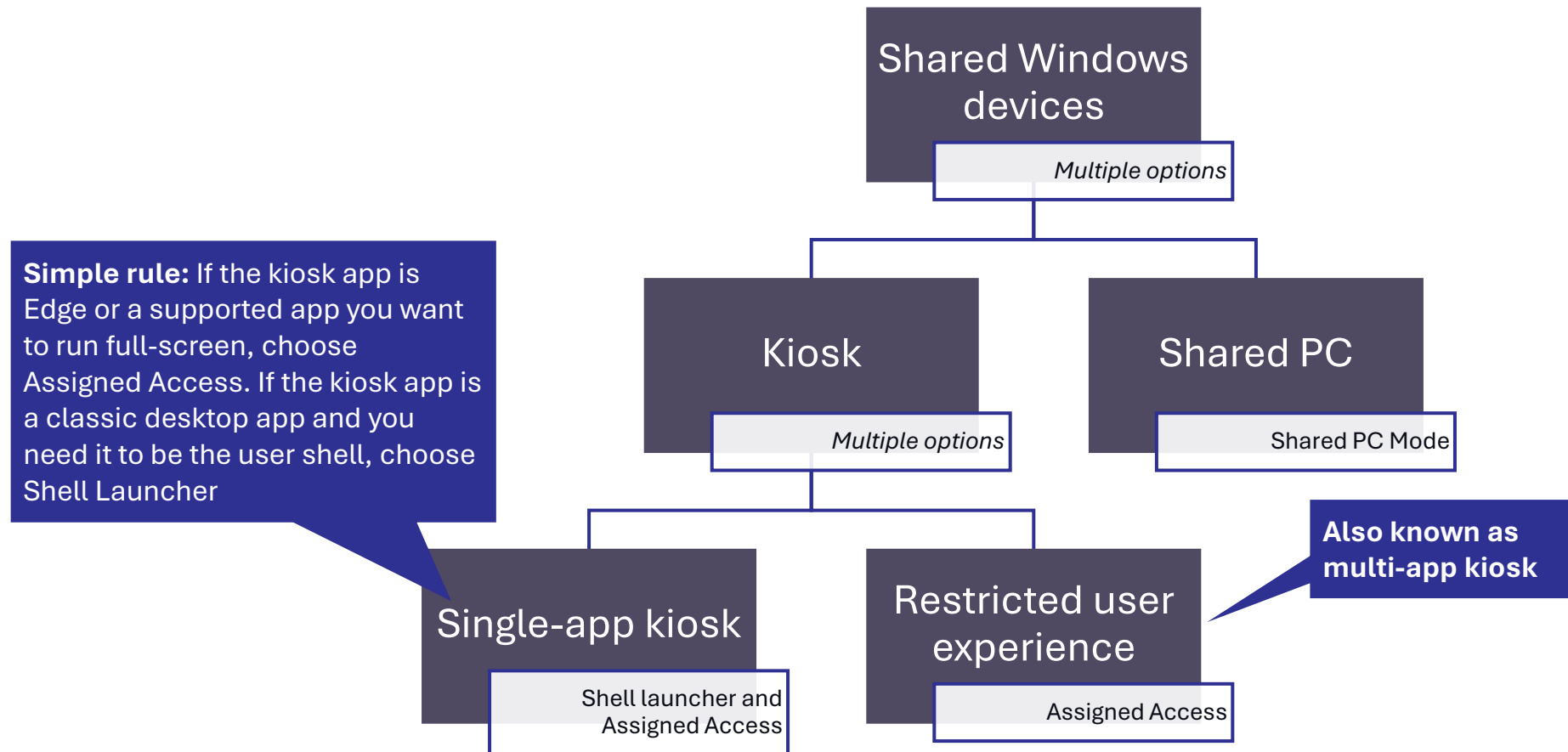
Configuration

Basic configuration options



Choosing the deployment model

What are the technical options for configuring shared devices?



Shared PC Mode basics

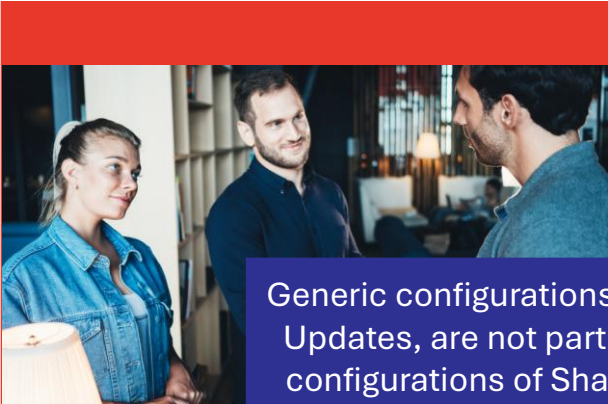
What are the main configurations that are part of Shared PCs?



Consider using Personal Data Encryption in combination with OneDrive

With or without OneDrive

Exclusions are possible
HKLM\SOFTWARE\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?

The screenshot displays the Microsoft Intune admin center interface. The top navigation bar includes the 'Microsoft Intune admin' logo, the 'Microsoft Intune admin center' title, and a user profile for 'PETERVANDERWOUDE.NL CORP ...'. The main content area is divided into three sections:

- Left sidebar:** Contains a navigation menu with icons for Home, Devices, Configuration, and Settings. The 'Configuration' section is expanded, showing a list of settings categories: Basics, Config (selected), Configure access, account, Windows 10 or later use, In organizations where m, Account manager setting, Click here for more info., Shared PC mode, Guest account, Account management, Local Storage, Power Policies, and Sleep time out (in seconds).
- Center pane:** Displays the 'Create profile' wizard for a 'Shared multi-user' profile. The wizard is in the 'Config' step. It shows a list of settings to be configured, including: Sleep Timeout (300), Inactive Threshold (30), Enable Shared PC Mode With One Drive Sync (Not configured), Enable Shared PC Mode (false), Enable Account Manager (false), Disk Level Deletion (25), Disk Level Caching (50), Deletion Policy (Delete at disk space threshold), and Account Model (Guest). Navigation buttons 'Previous' and 'Next' are at the bottom.
- Right pane:** Displays the 'Settings picker' for the 'Shared PC' category. It shows a search bar and a list of settings to be selected. The settings listed are: Account Model, Deletion Policy, Disk Level Caching, Disk Level Deletion, Enable Account Manager, Enable Shared PC Mode, Enable Shared PC Mode With One Drive Sync, and Inactive Threshold. A 'Select all these settings' button is at the bottom right.

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?



Microsoft Intune admin center

Home > Devices | Configuration

Custom ...
Windows 10 and later

Basics **2 Configuration settings** 3 Assignments 4 Applicability Rules 5 Review + create

OMA-URI Settings ⓘ

Add Export

Name ↑↓	Description ↑↓	OMA-URI ↑↓	Value
No settings			

Previous Next

Previous Next

Add Row X
OMA-URI Settings

Name * Multi-app kiosk mode configuration ✓

Description Kiosk mode configuration using Assigned Ac... ✓

OMA-URI * ./Vendor/MSFT/AssignedAccess/Configuration ✓

Data type * String

Value *
<Profile Id="{9A2A490F-10F6-4764-974A-53B19E722C23}">
<AllAppsList>
<AllowedApps>
<App
AppUserModelId="Microsoft.WindowsCalc
ulator_8wekyb3d8bbwe!App" />

Save Cancel

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
StartPins	Windows 11, version 22H2	v5	http://schemas.microsoft.com/AssignedAccess/2022/config
TaskbarLayout			
ClassicAppArguments	Windows 11, version 21H2	v4	http://schemas.microsoft.com/AssignedAccess/2021/config
ClassicAppPath			
AllowRemovableDrives	Windows 10	v5	http://schemas.microsoft.com/AssignedAccess/202010/config
GlobalProfile	Windows 10	v3	http://schemas.microsoft.com/AssignedAccess/2020/config
AutoLaunch	Windows 10	rs5	http://schemas.microsoft.com/AssignedAccess/201810/config
AutoLaunchArguments	Windows 10	default	http://schemas.microsoft.com/AssignedAccess/2017/config

Assigned Access XML profiles

<Taskbar ShowTaskbar="true"/>

Shows the taskbar in the kiosk experience
(can also be used to pin apps)

Each app specifies an app that is allowed
through AppLocker in the kiosk
experience

Each app specifies an app that is pinned
to the startmenu in the kiosk experience

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?

Microsoft Intune admin center

Home > Devices | Configuration

Custom ...

Windows 10 and later

Basics **2 Configuration settings** 3 Assignments 4 Applicability Rules 5 Review + create

OMA-URI Settings ⓘ Add Export

Name ↑↓	Description ↑↓	OMA-URI ↑↓	Value
No settings			

Previous Next

Add Row ×

OMA-URI Settings

Name * ✓

Description ✓

OMA-URI * ✓

Data type * ✓

Value *

```
<Config>
  <AutoLogonAccount
rs5:DisplayName="Kiosk user"/>
  <DefaultProfile Id="{9A2A490F-10F6-
4764-974A-53B19E722C23}"/>
</Config>
</Configs>
</AssignedAccessConfiguration>
```

Save Cancel

Recommendations

Additional configurations that should be considered



Recommendations

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

Microsoft Intune admin center

Home > Devices | Windows updates

Create Update ring for Windows 10 and later

Windows 10 and later

Enable pre-release builds * ⓘ Enable Not Configured

Select pre-release channel Windows Insider - Release Preview

User experience settings

Automatic update behavior ⓘ Auto install and restart at maintenance time

Active hours start * ⓘ 8 AM

Active hours end * ⓘ 5 PM

Option to pause Windows updates ⓘ Enable Disable

Option to check for Windows updates ⓘ Enable Disable

Change notification update level ⓘ Turn off all notifications, including restart warnings

Use deadline settings ⓘ Allow Not configured

Deadline for feature updates ⓘ Number of days, 0 to 30

Deadline for quality updates ⓘ Number of days, 0 to 30

Grace period ⓘ Number of days, 0 to 7

Auto reboot before deadline ⓘ Yes No

Previous Next

Auto install outside active hours or alternatively configure scheduled install times.

Turn off notifications

Remove power settings

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

Shared device configuration contains default power settings.

Microsoft Intune admin center

Home > Devices | Configuration

Create profile ...

Windows 10 and later - Settings catalog

Administrative Templates

System > Power Management > Sleep Settings

19 of 20 settings in this subcategory are not configured

Specify the system sleep timeout (plugged in) Disabled

System > Power Management > Video and Display Settings

5 of 6 settings in this subcategory are not configured

Turn off the display (plugged in) Disabled

Start Menu and Taskbar

102 of 103 settings in this subcategory are not configured

Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate Disabled

Previous Next

Settings picker

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

Search for a setting

Add filter

Browse by category

- Personal Data Encryption
- Personalization
- PKCS certificate
- PKCS imported certificate
- Power
- Printer Provisioning
- Printers
- Privacy

14 settings in "Power" category

Setting name

- ☐ Select Lid Close Action Plugged In
- ☐ Select Power Button Action On Battery
- ☒ Select Power Button Action Plugged In
- ☐ Select Sleep Button Action On Battery
- ☒ Select Sleep Button Action Plugged In
- ☐ Turn Off Hybrid Sleep On Battery
- ☐ Turn Off Hybrid Sleep Plugged In
- ☐ Unattended Sleep Timeout On Battery

Select all these settings

Prevent the device from falling asleep and/or being turned off.

Mostly Power and Power Management related settings.

Use Local Policies Security Options to remove permissions for shutdown.

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

Microsoft Intune admin center

Home > Devices | Configuration

Create profile

Windows 10 and later - Settings catalog

1 Basics 2 Configuration settings 3 Scope tags 4 Assignments 5 Review + create

+ Add settings ⓘ

^ Above Lock [Remove category](#)

1 of 2 settings in this category are not configured

Allow Toasts ⓘ ☐ Blocked ⓘ

^ Administrative Templates [Remove category](#)

System > Logon [Remove subcategory](#)

23 of 24 settings in this subcategory are not configured

Turn off app notifications on the lock screen ⓘ ☒ Enabled ⓘ

[Previous](#) [Next](#)

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.enrollmentP
rofileName -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

The scenario specific configuration that creates the main experience of the device.

Shared PC configuration

Assigned Access configuration

The application layer that contains scenario specific apps.

App

App

App

App

App

App

The recommended configuration layer that contains scenario specific configurations.

Recommended configurations

That includes at least the Windows updates, power settings, keyboard shortcuts, and notifications

The generic security baseline that is applicable to all devices.

Generic security baseline

That includes at least the Windows security baseline

Bonus: A few common challenges

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



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

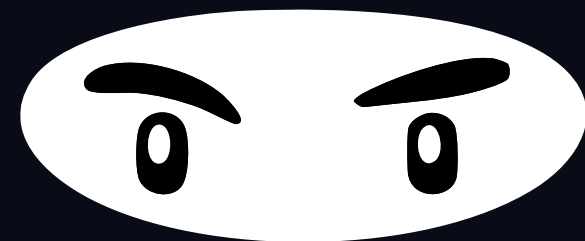
Start with the experience. Design the layers. Validate the complete lifecycle.

Thank You, Ninjas!

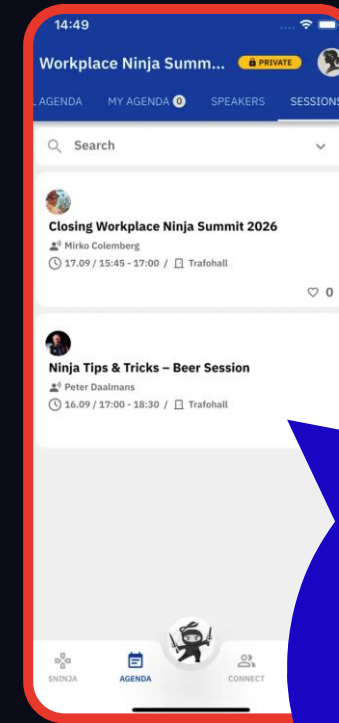
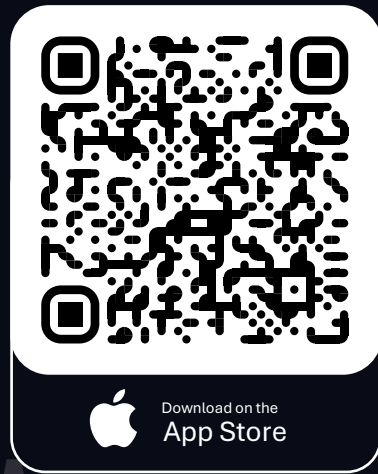


See You Next Year!

SUMMIT
SUMMIT
SUMMIT
SUMMIT
SUMMIT



Download the app and never miss any updates



We appreciate
your feedback!