Thomas Kurth & Nicola Suter

CLASSIC ON-PREM SERVICES IN THE CLOUD

About us...

baseVISION

Thomas Kurth

Principle Workplace Consultant, baseVISION AG

Wirtschaftsinformatiker FH / EMBA
M365 Expert
IPMA & ITIL Zertifiziert

Contact Me

Twitter: https://twitter.com/ThomasKurth_ch
Blog: https://wpninjas.ch
Mail: thomas.kurth@basevision.ch

About us...

Nicola Suter

Workplace Engineer itnetX (Switzerland) AG

Informatiker EFZ

BSc student in computer science

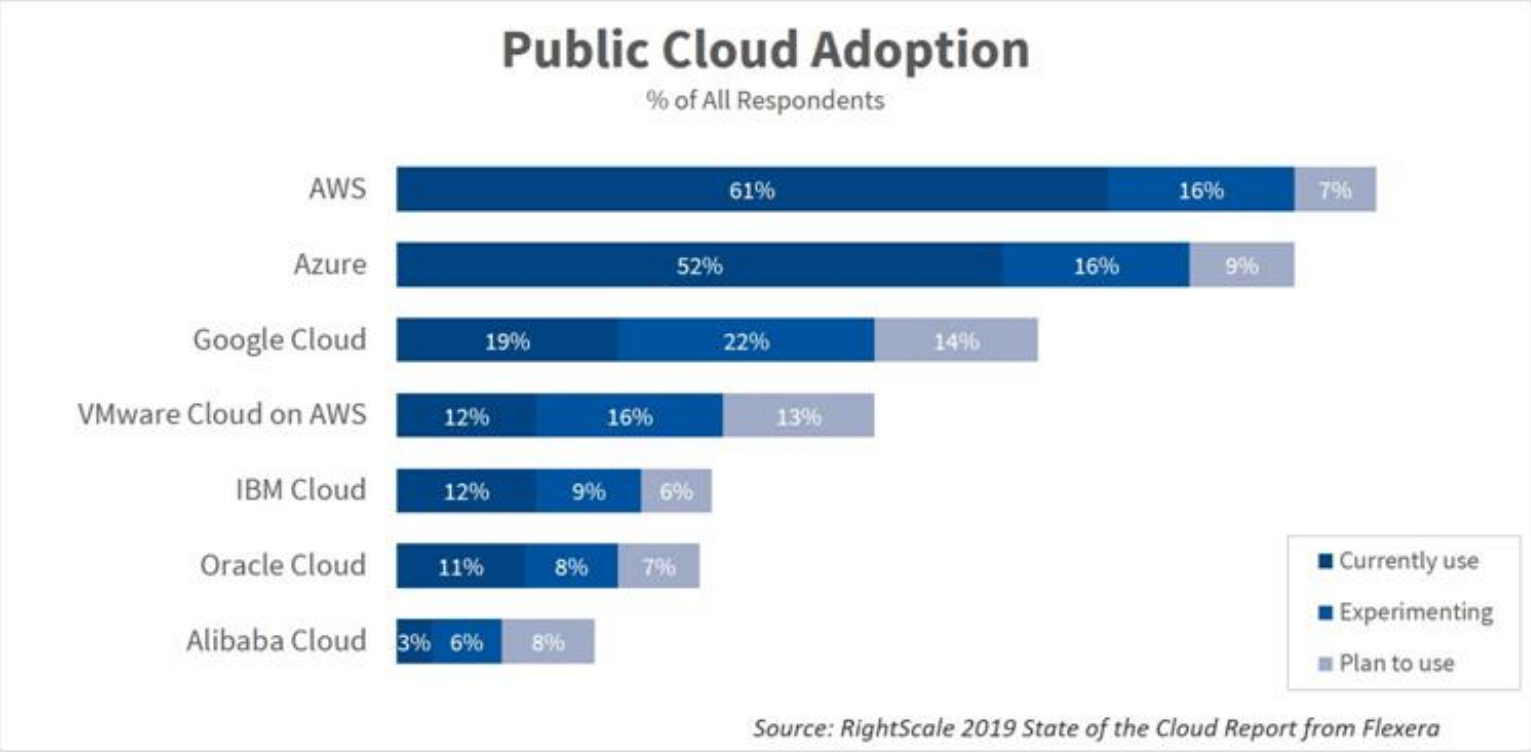
Contact Me

Twitter: https://twitter.com/nicolonsky
Blog: https://tech.nicolonsky.ch/
Mail: nicola@nicolasuter.ch

The story of cloud < 2017

The story of cloud 2019 - ???

- Still 30% are not using the cloud
- 50% of our customers are using some O365 services
- 20% of our customers are using M365 (Fast growing)



Why? Is it really not possible to use cloud only?

Microsoft offers cloud attached

- Cloud attached is the best from both worlds!
- ConfigMgr will stay as long you need it!
- Attach cloud-based intelligence and functionality as needed!

But before going this way you should check if you really have no cloud only option.

In this Session we will show you solutions for some of the "**fake blockers**"!

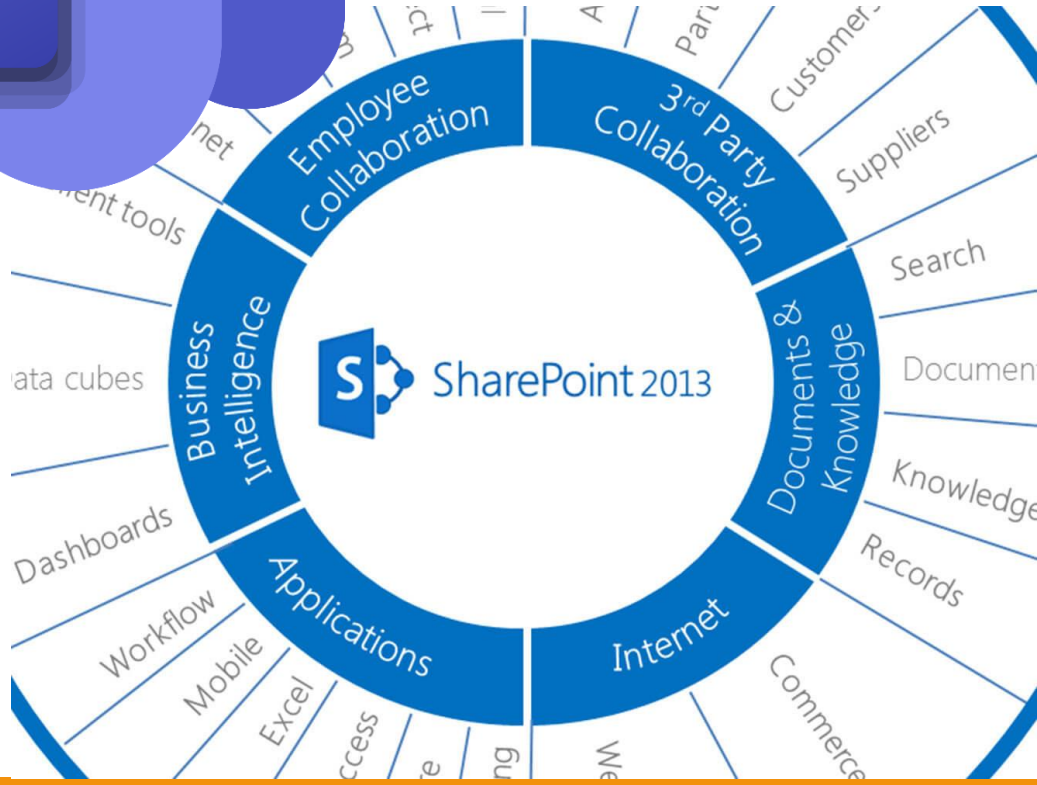
Traditional Fileshares

- Technologies used
  - NTFS
  - SMB
  - Kerberos
  - NTLM
- Devices
  - NAS Storage
  - Windows File Server
- Organization in folder trees

Traditional Fileshares → Modern World

- Technologies used
  - NTFS
  - SMB
  - Kerberos
  - NTLM
- Devices
  - NAS Storage
  - Windows File Server
- Organization in folder trees

Dropbox



But I still need file shares or other NTLM/Kerberos Resources!

Resources

- When a user signs into an Azure AD joined device in a hybrid environment:
  1. Azure AD sends the name of the on-premises domain the user is a member of back to the device.
  2. The local security authority (LSA) service enables Kerberos authentication on the device.
- During an access attempt to a resource in the user's on-premises domain, the device:
  1. Uses the domain information to locate a domain controller (DC).
  2. Sends the on-premises domain information and user credentials to the located DC to get the user authenticated.
  3. Receives a Kerberos Ticket-Granting Ticket (TGT) that is used to access AD-joined resources.

Details: https://docs.microsoft.com/en-us/azure/active-directory/devices/azuread-join-sso

Demo

PKI

- Local PKI with NDES and SCEP integrated in Intune

- Use cases
  - Wi-Fi Authentication
  - VPN Authentication
- Issues
  - Validating computer certificates on Windows Server with NPS role does NOT Work!
  - Still requires infrastructure

- Other options
  - SCEPMan
  - Cloud PKI Symantec --> Still requires SCEP Server

Printing – Windows Server capabilities

- Print server
  - Requires maintenance
  - Mapping printers is often overcomplicated
  - Intended to use with Active Directory

Printing – but I've heard there's Hybrid Cloud Print?

- Windows Server Hybrid Cloud Print
  - Complicated deployment and quite a few resources to deploy
  - Lots of PowerShell commands to add and manage printers
  - Even more servers running on premise

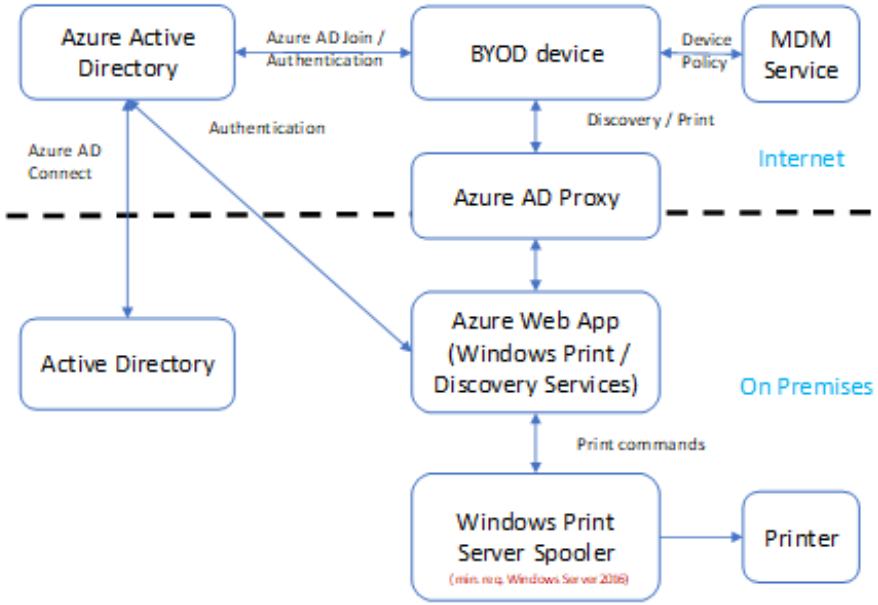


Image: Microsoft Docs: https://docs.microsoft.com/en-us/windows-server/administration/hybrid-cloud-print/hybrid-cloud-print-overview

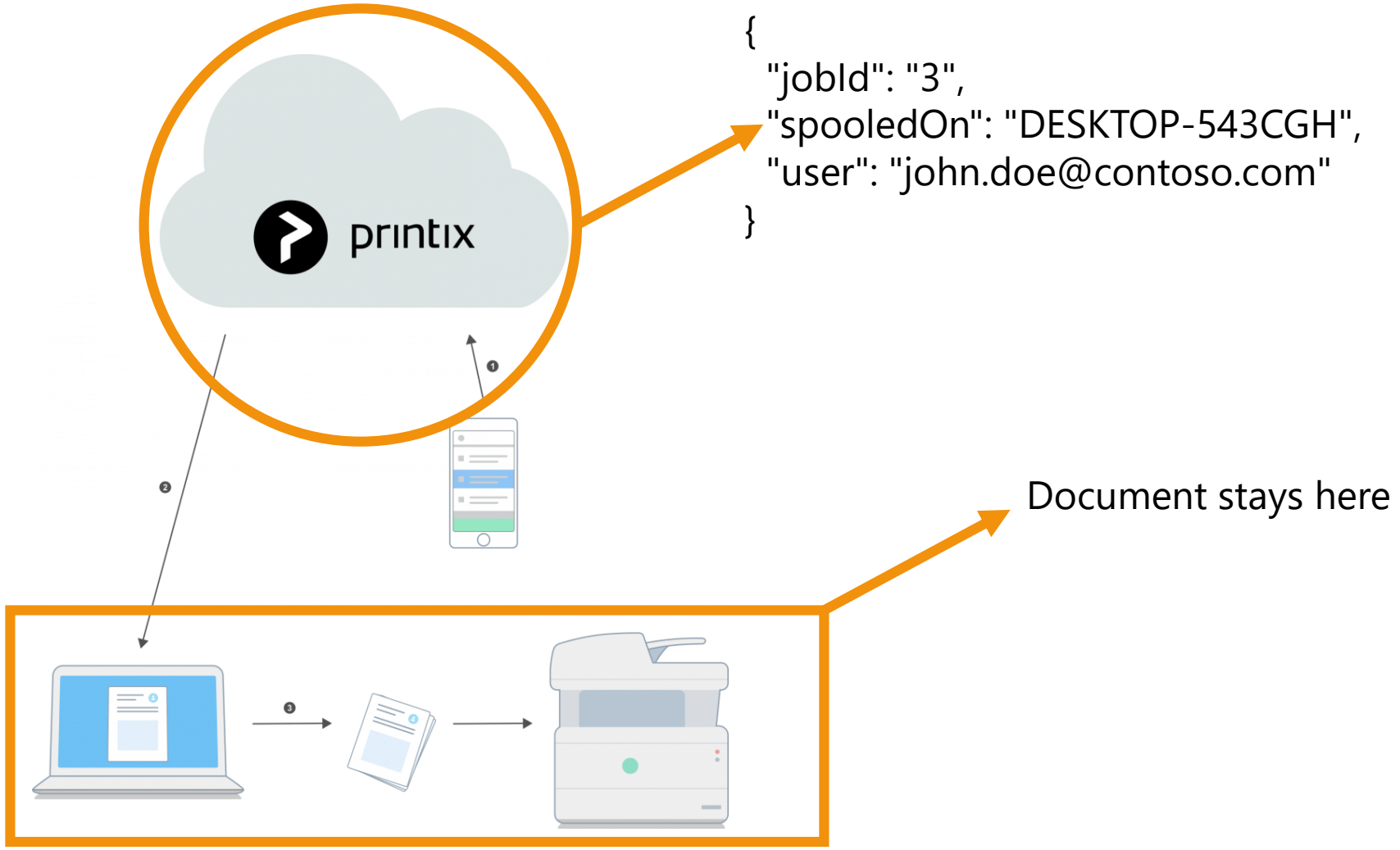
Printing – Microsoft's recommended 3rd party solution

- printix
  - "serverless" cloud printing (SaaS)
  - Available from Microsoft app source
  - Seamless Azure AD integration
  - Easy client agent deployment (single MSI)
  - Documents do not leave the corporate network
  - Vendor independent follow-me and secure printing
  - Easy onboarding because print queues from a print server can be migrated including custom settings on drivers
  - Supports Windows Virtual Desktop

Details: https://manuals.printix.net/administrator

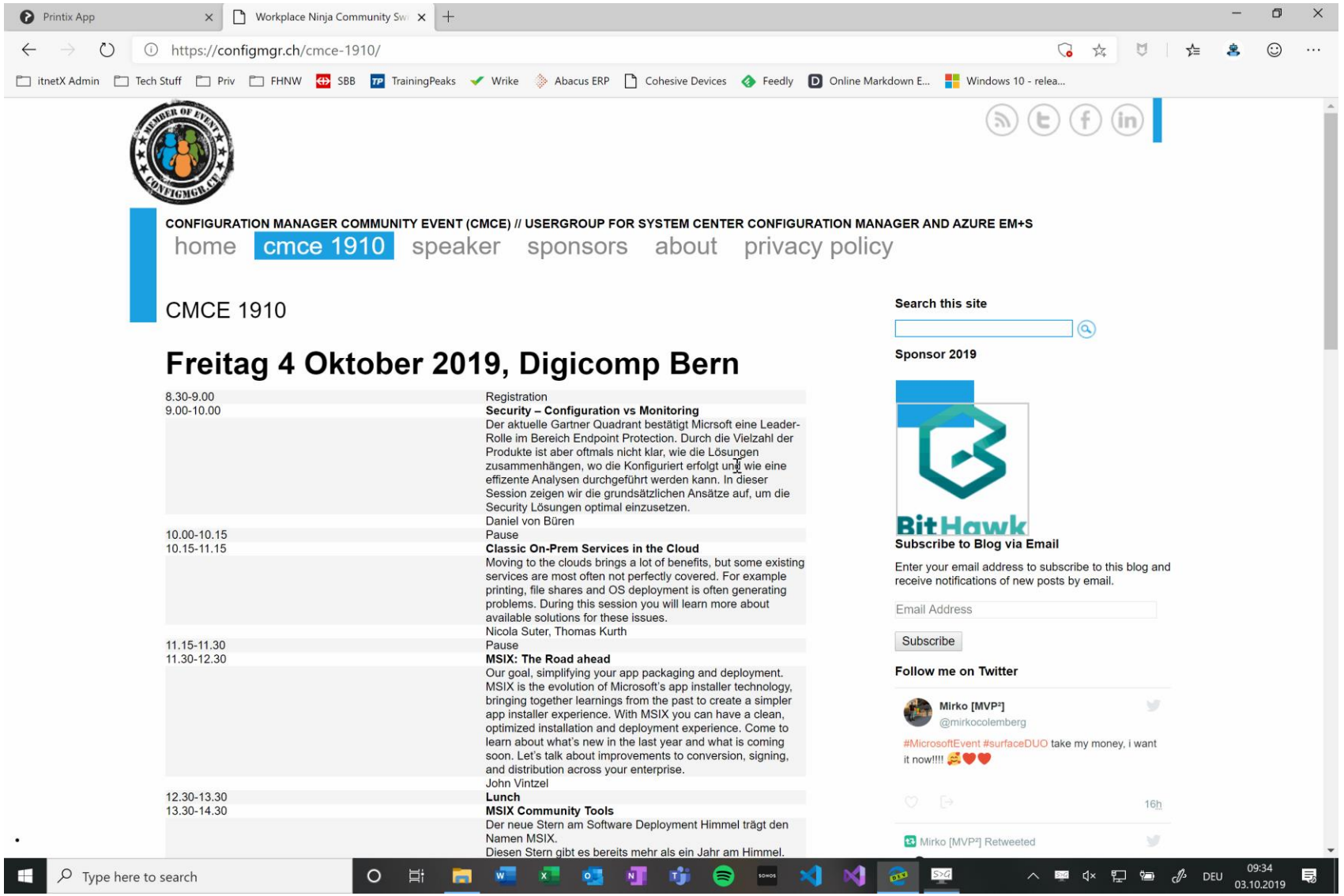
Printing – printix under the hood

- Documents do not leave the corporate network?

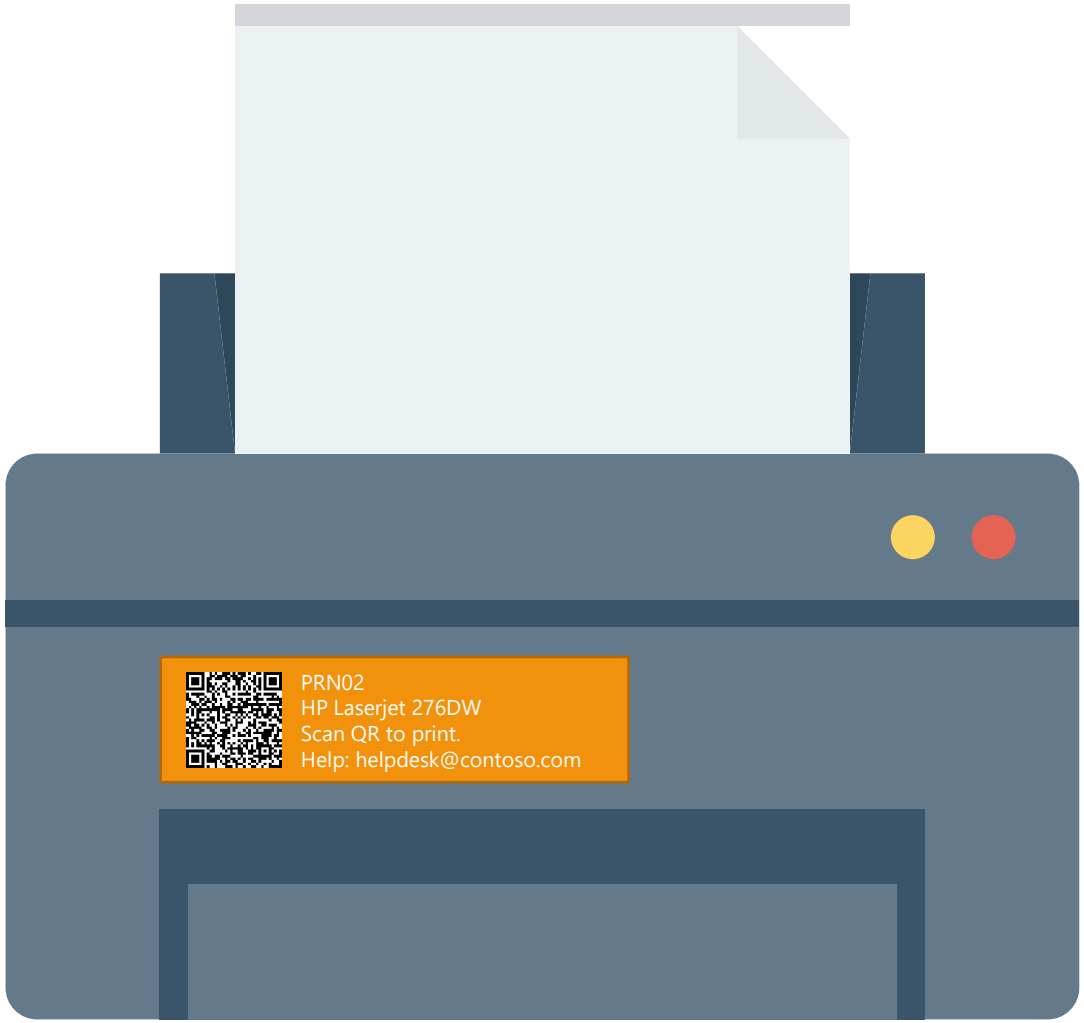


Demo

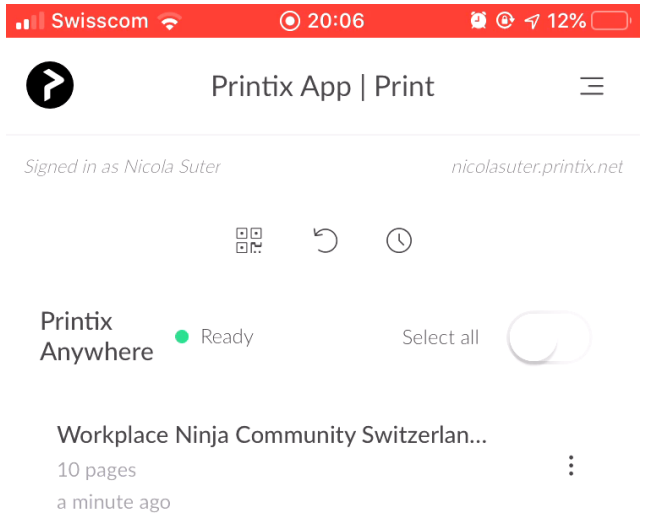
Printing – printix demo



Printing – printix demo



Printing – printix demo



I want my "normal" printers and have no need for follow-me printing?

Printing – printix challenges

- Real live feedback
  - No accounting (only Power BI reports)
  - No "scan to folder" capabilities
  - End user adoption

OS Deployment

2019 and still in need for Wipe and Load OSD?!

- Use cases from the field:
  - Integrate "old" devices into Autopilot and Intune
  - Upgrade TPM and UEFI-Firmware
  - Deploy a "clean" Windows for devices not shipped with a vanilla image or outdated Windows versions
  - Cloud Deploy from vendors

OS Deployment - mOSD

- Easy staging with Roger Zander's mOSD
  - Zero touch Windows 10 installation based on Autounattend.xml
  - Recommendation: Store your mOSD config within a git repository and enjoy a simplified configuration management

Latest mOSD sources: https://github.com/rzander/mosd

Documentation: https://rzander.azurewebsites.net/modern-os-deployment-mosd/

OS Deployment – mOSD hands-on

mOSD hands-on

Questions?

Share your ideas

- Share your voice / ideas!
  - http://microsoftintune.uservoice.com/
  - http://configurationmanager.uservoice.com/

Event Feedback:

Session Feedback:

Danke

Herzlichen Dank
@nicolonsky @ThomasKurth_CH @configmgr_ch #cmce_ch

Bewertung der Session: Configmgr.ch / azureems.ch

Xing: https://www.xing.com/net/cmce
Facebook: https://www.facebook.com/groups/411231535670608/
Linkedin: http://www.linkedin.com
Twitter: https://twitter.com/configmgr_ch

Nächster Event: Freitag 15. November, Zürich

baseVISION

BitHawk

RealStuff
Informatik AG

digicomp
Digital Competence. Made of People.