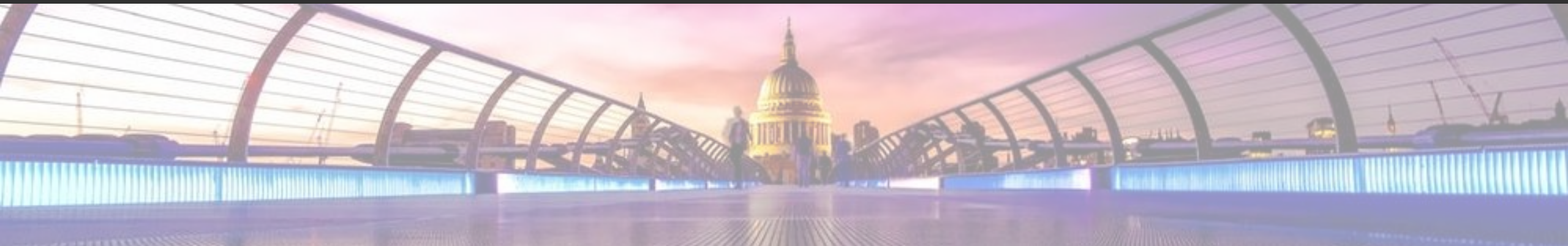
SCConfigMgr

Windows | EM+S | PowerShell

Use the power of Microsoft Cloud in your ConfigMgr environment with Co-management



Speaker introduction

@NickolajA

Nickolaj.andersen@truesec.se

Principal Consultant - TrueSec

@sandy_tsang

yinghua.ts@hotmail.com

System Architect - Valtori

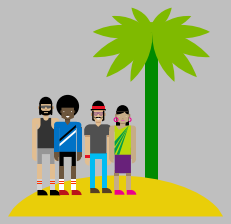
Key take aways

- What does Co-management mean?
- Why do we need it?
- Requirements and environment configuration
- Benefits with Co-managements
- Scenarios and examples

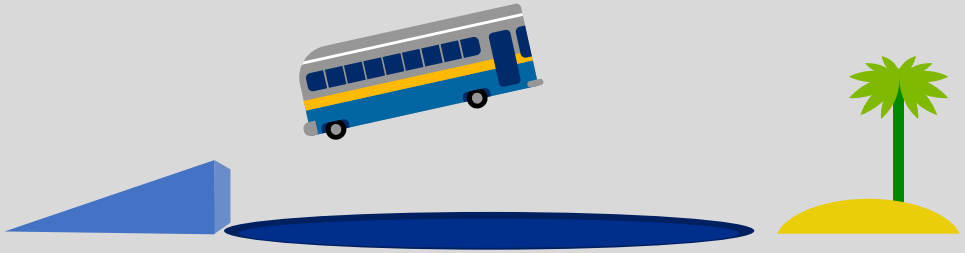
*"Configuration Manager helps customers build the **bridge** to **modern management** of Windows to lower the total cost ownership for managing Windows in the enterprise"*

Paths to Modern Management

Cloud-first



Big Switch Transition



Group by Group Transition

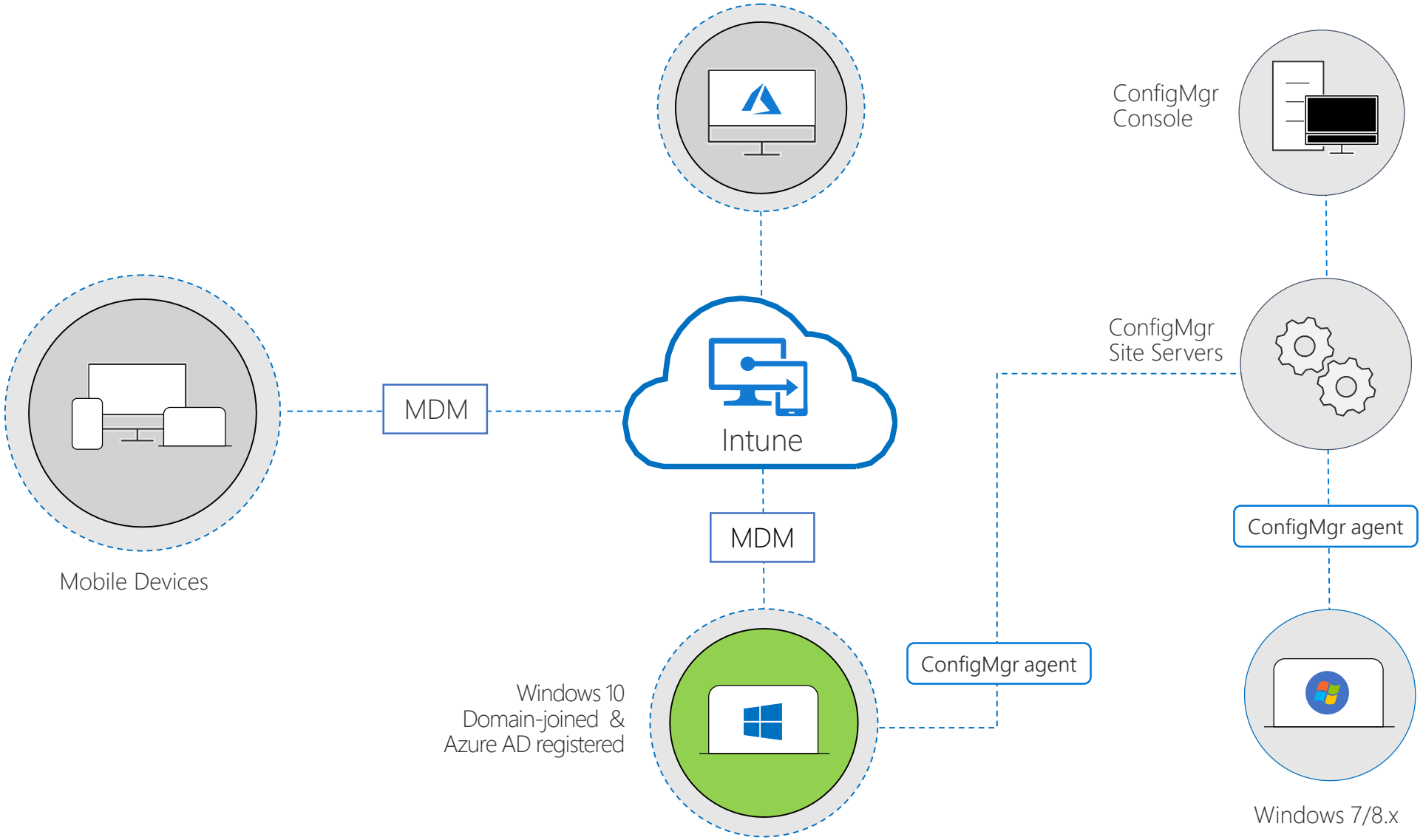
Leverage Co-management

Cloud-first

Workload transition (Co-management)

Group by Group Transition

What is Co-management



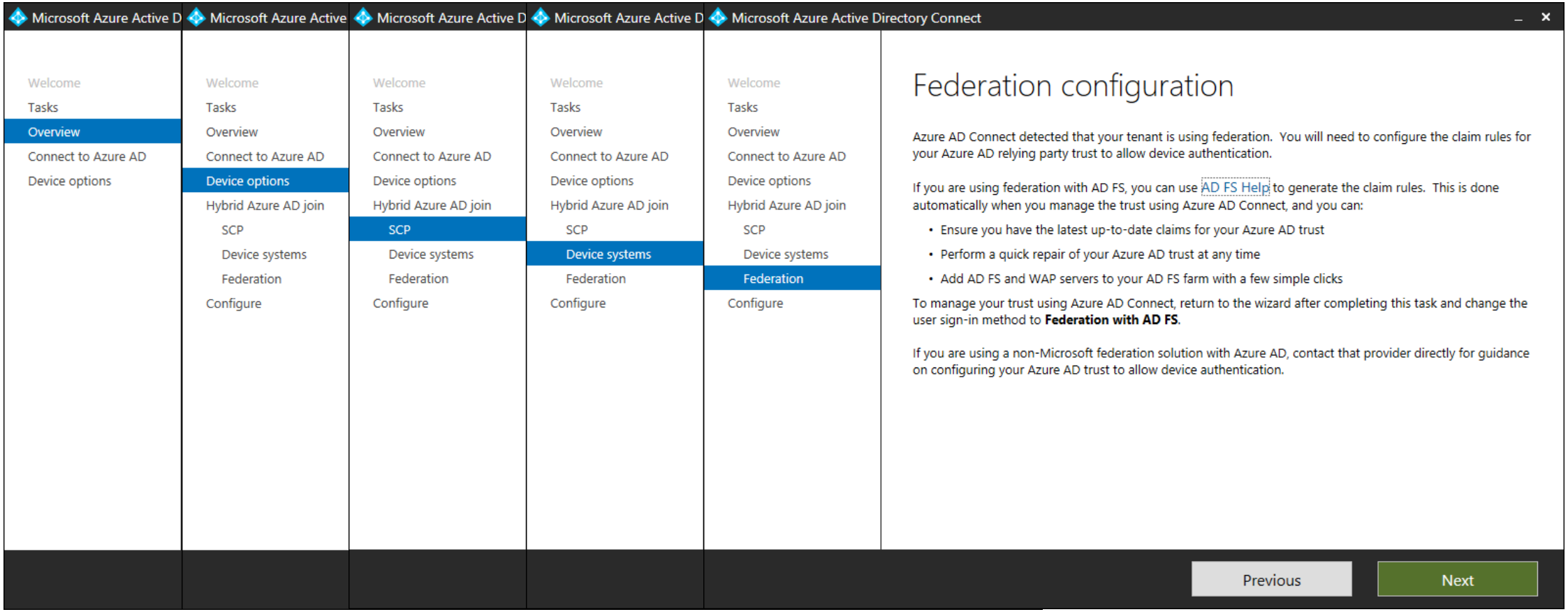
Common missunderstandings

- Co-management is to solve Intune shortcomings
  - It's a bridge to fill the gaps for modern management
- Co-management requires Cloud Mangement Gateway and Cloud DP
  - Optional for domain joined devices
- Co-management is only for domain joined devices
  - Support for Azure AD joined devices as well

What's required for Co-Management

- EMS or Intune licenses
- Configuration Manager 1710 or later
- Azure AD
  - Azure AD Connect
  - Auto-enrollment enabled
  - Hybrid Azure AD joined devices
- Intune subscription (MDM authority set to standalone)
- Windows 10 version 1709 or later
- Cloud Management Gateway (Cloud Distribution Point and Azure Services)
  - For Azure AD joined devices only

Hybrid Azure AD join



Migrate from Intune Hybrid

- Document and renew all certificates
  - APN, DEP etc.
- Import Configuration Manager data to Microsoft Intune
  - Applications, Policies, etc.
- Prepare Intune for user migration
  - AAD Groups, Install NDES, Exchange Connector etc.
- Change the MDM authority for specific users (mixed MDM authority)
  - Remove the user from the Intune collection in ConfigMgr
  - Userless devices can be migrated using a script
- Change your MDM authority to Intune standalone

DEMO

Enable Co-management

Get a device to a Co-management state

New or existing Windows 10 domain joined device

- Prerequisites
  - Traditional deployment through Configuration Manager
  - Configuration Manager client already installed
  - Hybrid Azure AD joined
  - Windows 10 version 1709 or later
  - *Optional - Cloud Management Gateway and Cloud DP*
- Actions
  - Stage device for Co-management (when piloting)
  - Auto-enrollment for Microsoft Intune (GPO or ConfigMgr agent)
  - Transitioned workload policies

DEMO

Domain joined device with Co-management

Get a device to a Co-management state

Windows 10 Azure AD joined devices (with or without AutoPilot)

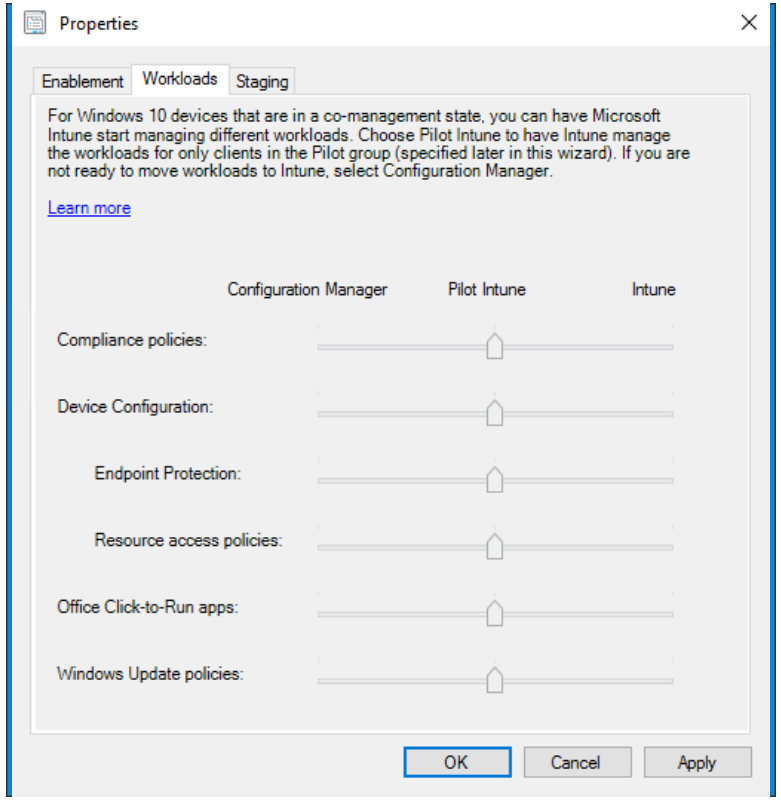
- Prerequisites
  - Azure AD joined and automatic Intune enrollment
  - Azure Services in Configuration Manager with Azure AD user sync
  - Logged on with an Azure AD identity or synced on-premise user
  - Cloud Management Gateway (Cloud Distribution Point)
  - Windows 10 version 1709 or later
- Actions
  - Configuration Manager client deployed through Intune
    - LOB app – bin\i386\ccmsetup.msi
  - Stage device for Co-management (when piloting)
  - Transitioned workload policies

DEMO

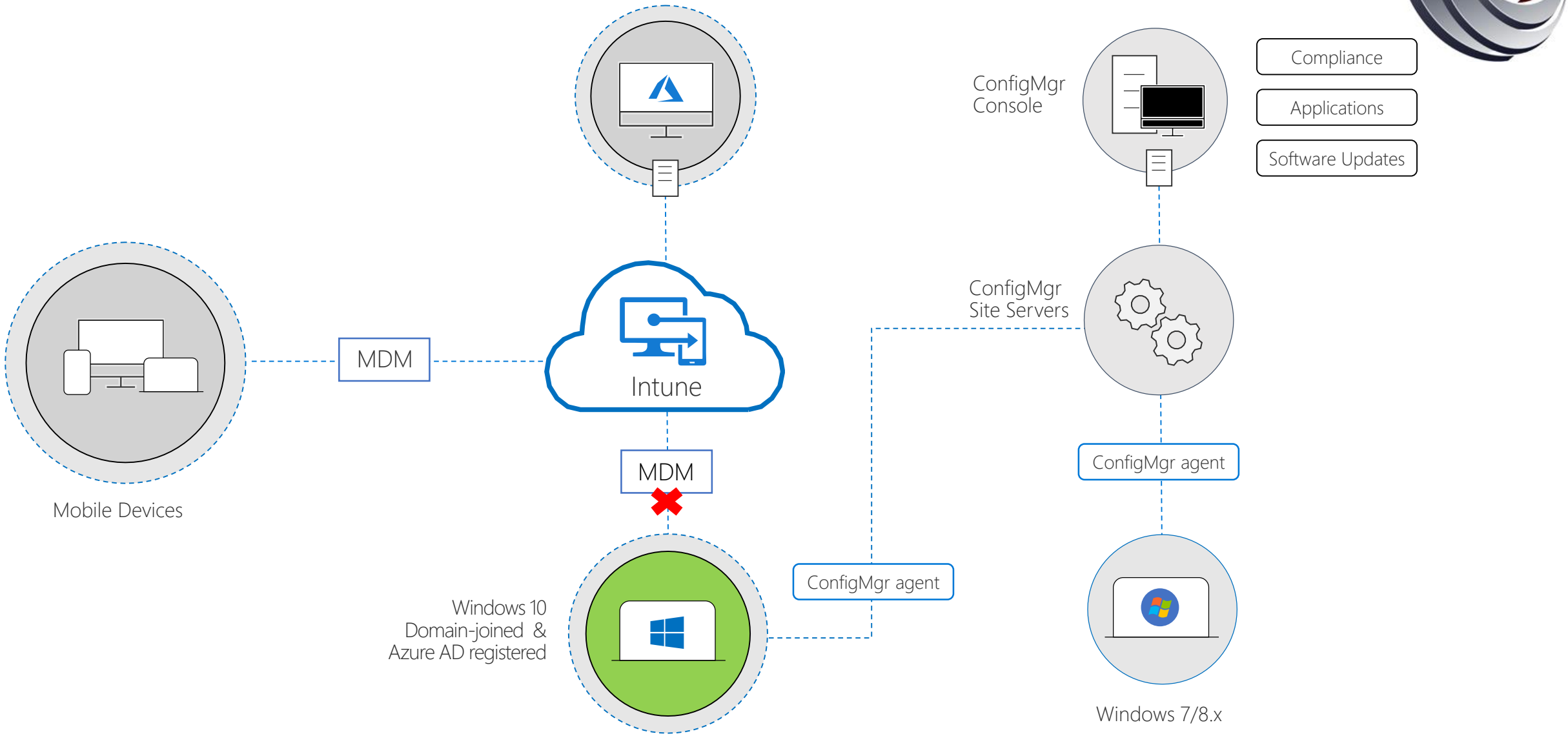
Azure AD joined device with Co-management

Co-management and workloads

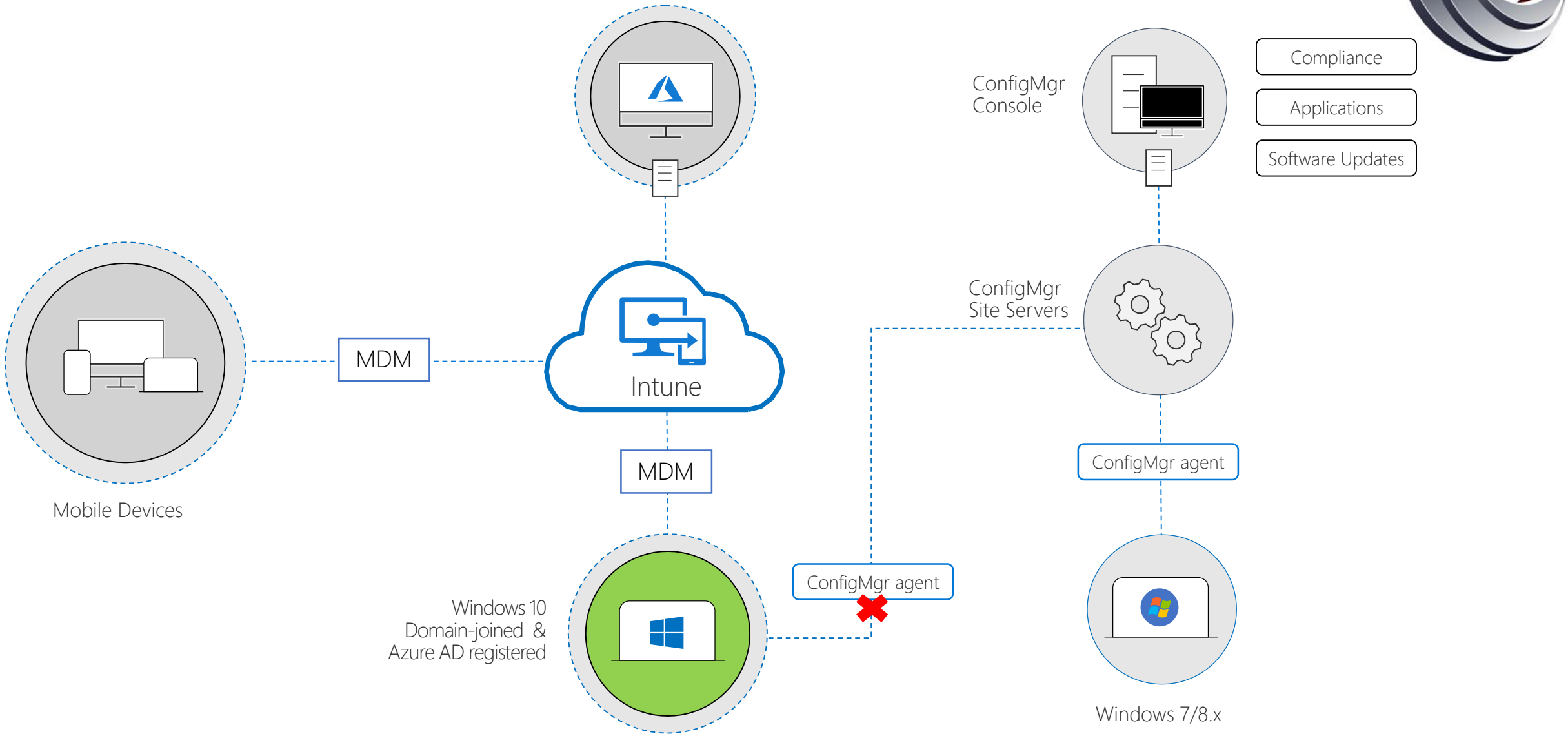
- Compliance policies
  - Compliance policies and rules evaluation
- Resource access policies
  - WiFi, VPN, Certificate and Email profiles and Windows Hello for Business
- Windows Update for Business policies
- Endpoint Protection policies
- Additional workloads in ConfigMgr 1806 TP
  - Device Configuration
  - Office Click-to-Run apps



Before workload transition



After workload transition



DEMO

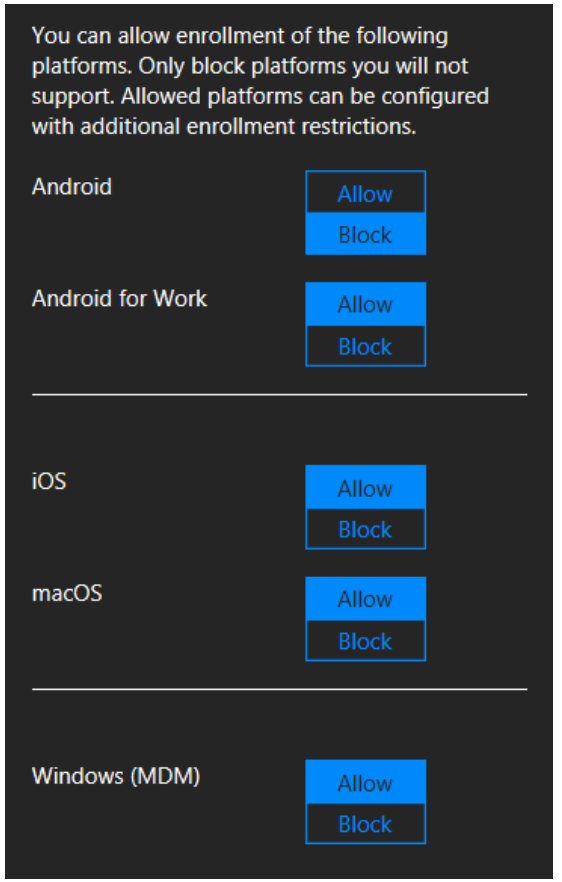
Transition Compliance policies

Troubleshooting Co-management

- Windows clients
  - C:\Windows\CCM\Logs\CoManagementHandler.log
  - C:\Windows\System32\config\systemprofile\AppData\Local\mdm
  - DeviceManagement-Enterprise-Diagnostics-Provider (event log)
  - dsregcmd.exe /status
- User needs an Intune license

Troubleshooting Co-management

- Cloud services
  - Enrollment restrictions (Windows (MDM)
  - Intune automatic enrollment enabled
  - Azure AD device registration enabled
- ADFS (optional)
  - Allow forms auth on Intranet authentication policies
  - Enable device authentication



Benefits with Co-management

- Conditional Access for traditionally managed devices
- Out of the box features like:
  - Remote actions
  - Factory reset
  - Restart device

Try it now

- Getting started with Co-management links:
- http://www.scconfigmgr.com/2017/11/23/how-to-setup-co-management-part-1/
- http://www.scconfigmgr.com/2017/11/23/how-to-setup-co-management-part-2/
- http://www.scconfigmgr.com/2017/11/24/how-to-setup-co-management-part-3/
- http://www.scconfigmgr.com/2017/11/24/how-to-setup-co-management-part-4/
- http://www.scconfigmgr.com/2017/11/24/how-to-setup-co-management-part-4/
- http://www.scconfigmgr.com/2017/11/29/how-to-setup-co-management-part-5/
- http://www.scconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/
- http://www.scconfigmgr.com/2017/11/30/deploy-configmgr-client-to-aad-device-from-intune/

Get in touch

@NickolajA

Nickolaj.andersen@truesec.se

Principal Consultant - TrueSec

@sandy_tsang

yinghua.ts@hotmail.com

System Architect - Valtori