

Closing the gaps with just4clicks (Co-Management)

Jörgen Nilsson
Onevinn



Key Takeaways

- What does Co-Management mean?
- Pre-requirements
- And most important! Why do we need it?
- Scenarios and Examples

Co-Management

Introduction

Co-Management

Properties



Enablement Workloads Staging

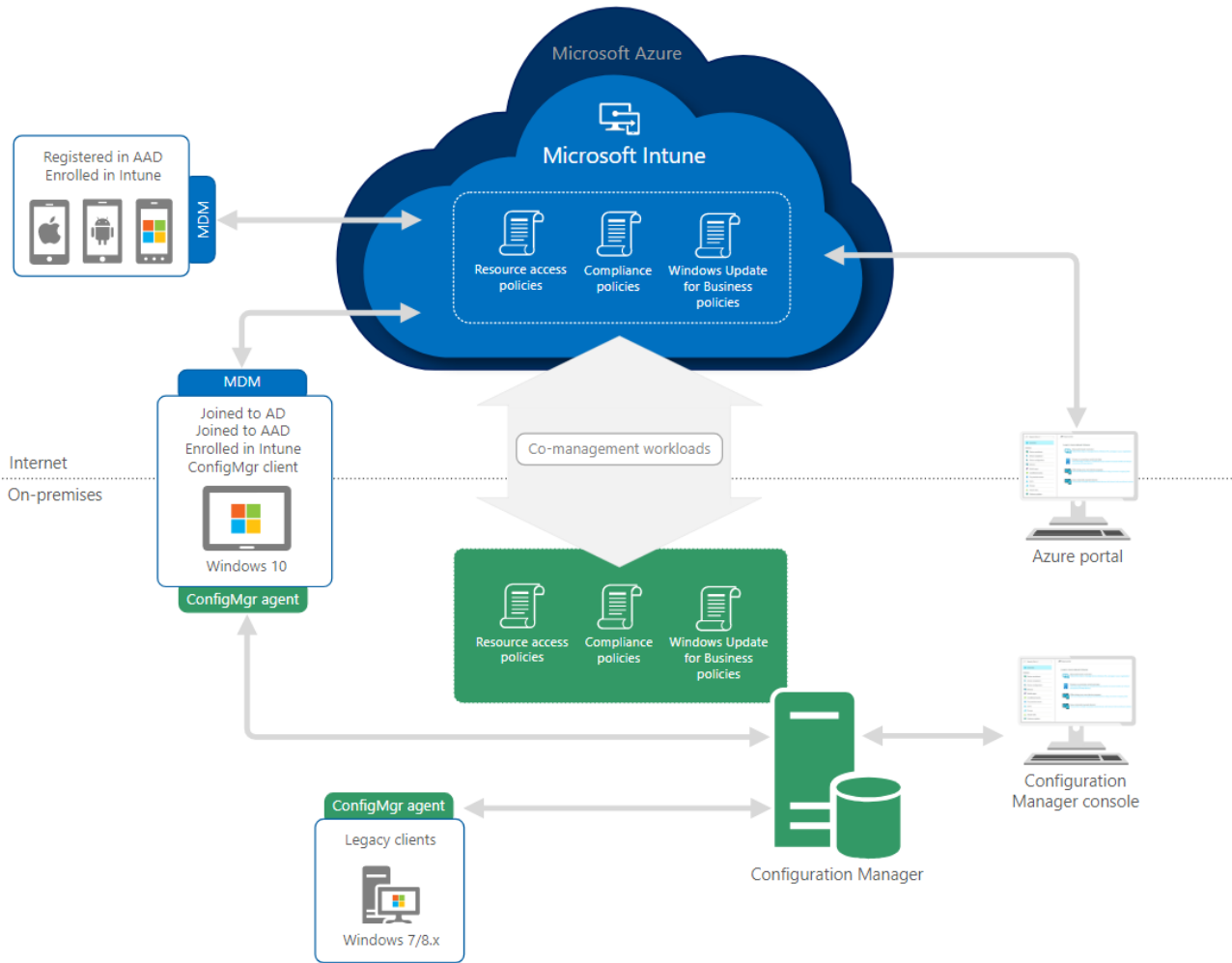
For Windows 10 devices that are in a co-management state, you can have Microsoft Intune start managing different workloads. Choose Pilot Intune to have Intune manage the workloads for only clients in the Pilot group (specified later in this wizard). If you are



OK

Cancel

Apply



Pre-requirements

Getting Started with Co-Management

- Configuration Manager version 1710 or later
- Azure AD
- EMS or Intune license for all users
- [Azure AD automatic enrollment](#) enabled
- Intune subscription (MDM authority in Intune set to **Intune**)

General Prerequisites

- Configuration Manager version 1710 or later
- Azure AD
- EMS or Intune license for all users
- Azure AD automatic enrollment enabled
- Intune subscription (MDM authority in Intune set to Intune)

Device Requirements

- Devices with the Configuration Manager client
 - Windows 10, version 1709 (also known as the Fall Creators Update) and later
 - [Hybrid Azure AD joined](#) (joined to AD and Azure AD)
- Devices without the Configuration Manager client
 - Windows 10, version 1709 (also known as the Fall Creators Update) and later
 - [Cloud Management Gateway](#) in Configuration Manager (when you use Intune to install the Configuration Manager client)

Azure AD Connector

- Must be up-to-date
- Computer Accounts must be included in the sync.

NAME	ENABLED	OS	VERSION	JOIN TYPE	OWNER	MDM	COMPLIANT
	✔ Yes	Windows 10 Enterprise	10.0 (14393)	Hybrid Azure AD joined	N/A	None	N/A
	✔ Yes	Windows 10 Enterprise	10.0 (16299)	Hybrid Azure AD joined	N/A	Microsoft Intune	N/A
	✔ Yes	Windows 10 Pro	10.0 (14393)	Hybrid Azure AD joined	N/A	None	N/A
	✔ Yes	Windows 10 Enterprise	10.0 (15063)	Hybrid Azure AD joined	N/A	None	N/A
	✔ Yes	Windows 10 Enterprise	10.0 (15063)	Hybrid Azure AD joined	N/A	None	N/A

Hybrid Azure AD Joined

- Troubleshooting client registration
- Command: dsregcmd /status

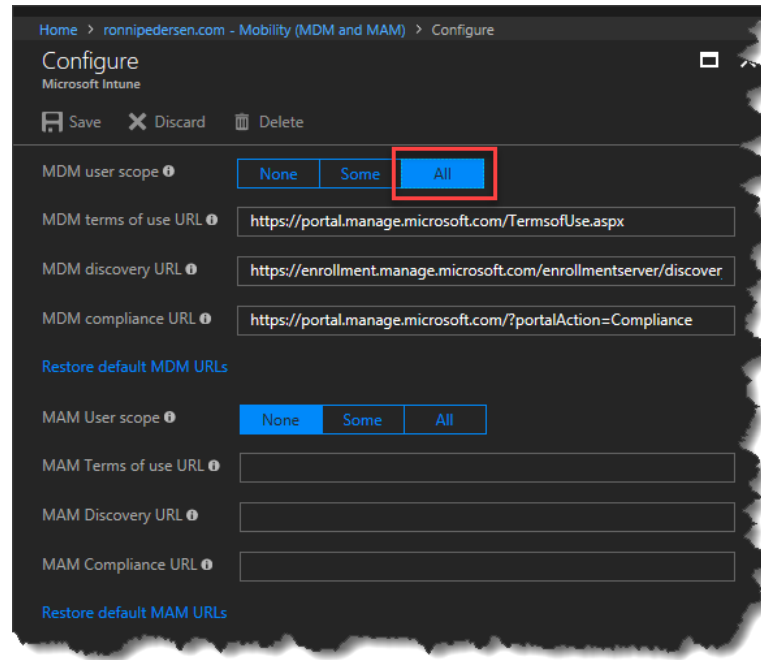
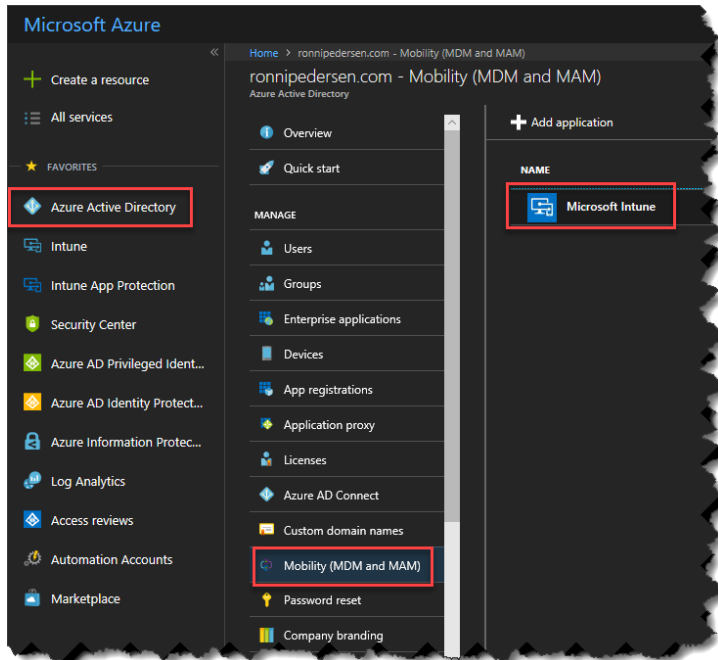
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>dsregcmd /status

-----+
| Device State |
-----+

AzureAdJoined : YES
EnterpriseJoined : NO
DeviceId : 6cec6a69-ea4d-4618-b903-98acc2e6d446
Thumbprint : 5EFE781E65C4743443066A37A70C2611A509E784
KeyContainerId : 73149bd0-2da3-4973-9b13-30dc45186db5
KeyProvider : Microsoft Software Key Storage Provider
TpmProtected : NO
KeySignTest : PASSED
    Idp : login.windows.net
    TenantId : 405cdaac-2a0c-4b96-ba7f-8f1cf4dcd76f
    TenantName : RONNIPEDERSEN.COM
    AuthCodeUrl : https://login.microsoftonline.com/405cdaac-2a0c-4b96-ba7f-8f1cf4dcd76f/oauth2/authorize
    AccessTokenUrl : https://login.microsoftonline.com/405cdaac-2a0c-4b96-ba7f-8f1cf4dcd76f/oauth2/token
    MdmUrl : https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc
    MdmToolUrl : https://portal.manage.microsoft.com/EnrollUse.aspx
```

Enable Azure AD automatic enrollment



Migrate from Intune Hybrid to Standalone

- 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

Intune data migration tool

- Collects data about the objects you select from your Configuration Manager hierarchy.
- Provides details about the objects you can select for import and information about why some objects cannot be imported.
- Imports selected objects into your Microsoft Intune tenant.
 - Configuration items
 - Certificate profiles
 - Email profiles
 - VPN profiles
 - Wi-Fi profiles
 - Compliance policies
 - Apps
 - Deployments

Enable Co-Management



Properties



Enablement Workloads Staging

To enable co-management for devices managed by Configuration Manager, configure automatic enrollment in [Microsoft Intune](#).

[Learn more](#)

Automatic enrollment in Intune

Pilot

- None
- Pilot
- All

To enable co-management for devices already enrolled in Intune, create an app in Intune to install the Configuration Client. Copy the following command line

[Learn more](#)

```
CCMSETUPCMD="/mp:https://CCMEJECTP1710.CLOUDAPP.NET/CM_Proxy_MutualAuth/72057594037927939  
CCMHOSTNAME=CCMEJECTP1710.CLOUDAPP.NET/CCM_Proxy_MutualAuth/72057594037927939 SMSiteCode=TP4  
SMSMP=http://CMTP4.INTRA.CCMEXEC.LOCAL
```

Copy

OK

Cancel

Apply

Workloads

- Compliance policies
- Resource access policies
- Windows Update policies
- Endpoint Protection(1802TP)

Properties

Enablement Workloads Staging

For Windows 10 devices that are in a co-management state, you can have Microsoft Intune start managing different workloads. Choose Pilot Intune to have Intune manage the workloads for only clients in the Pilot group (specified later in this wizard). If you are not ready to move workloads to Intune, select Configuration Manager.

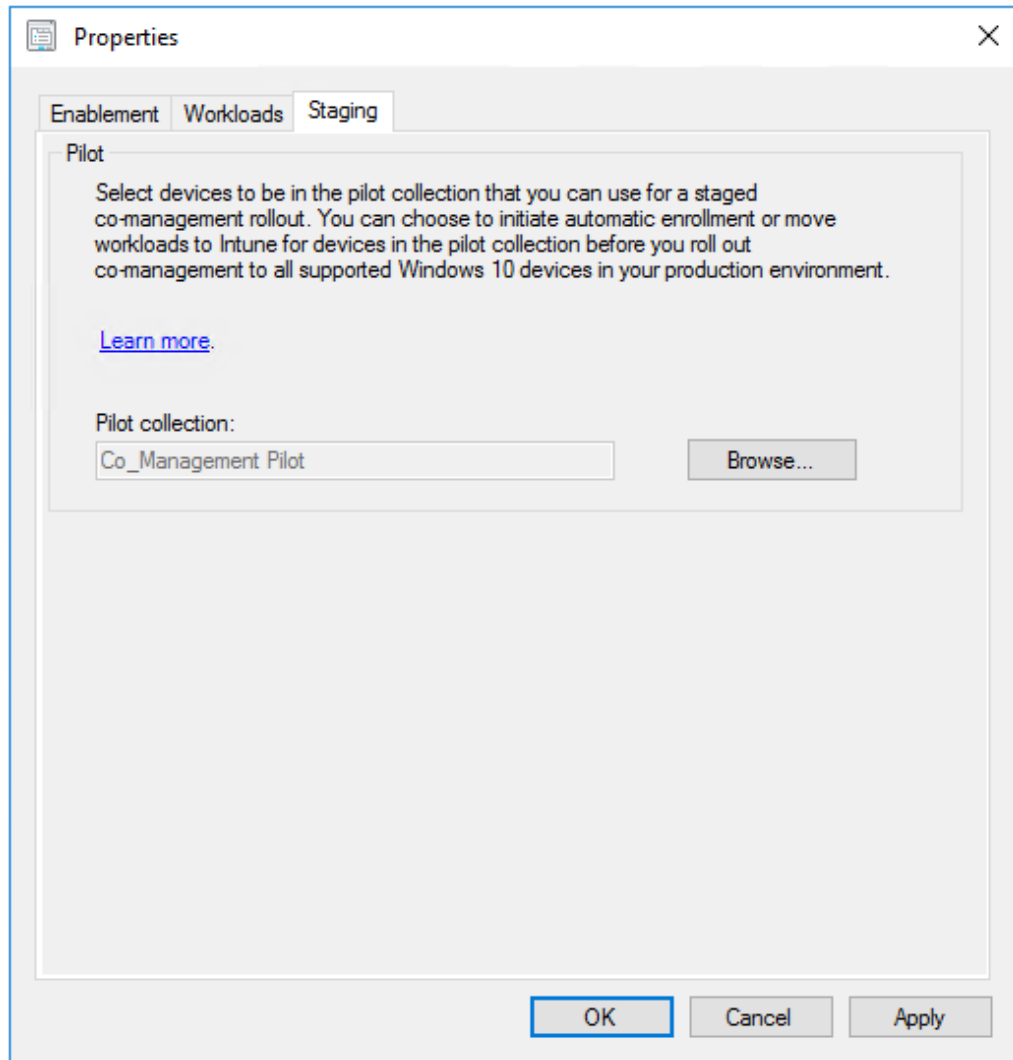
[Learn more](#)

	Configuration Manager	Pilot Intune	Intune
Compliance policies:			
Resource access policies:			
Windows Update policies:			
Endpoint Protection:			

OK Cancel Apply

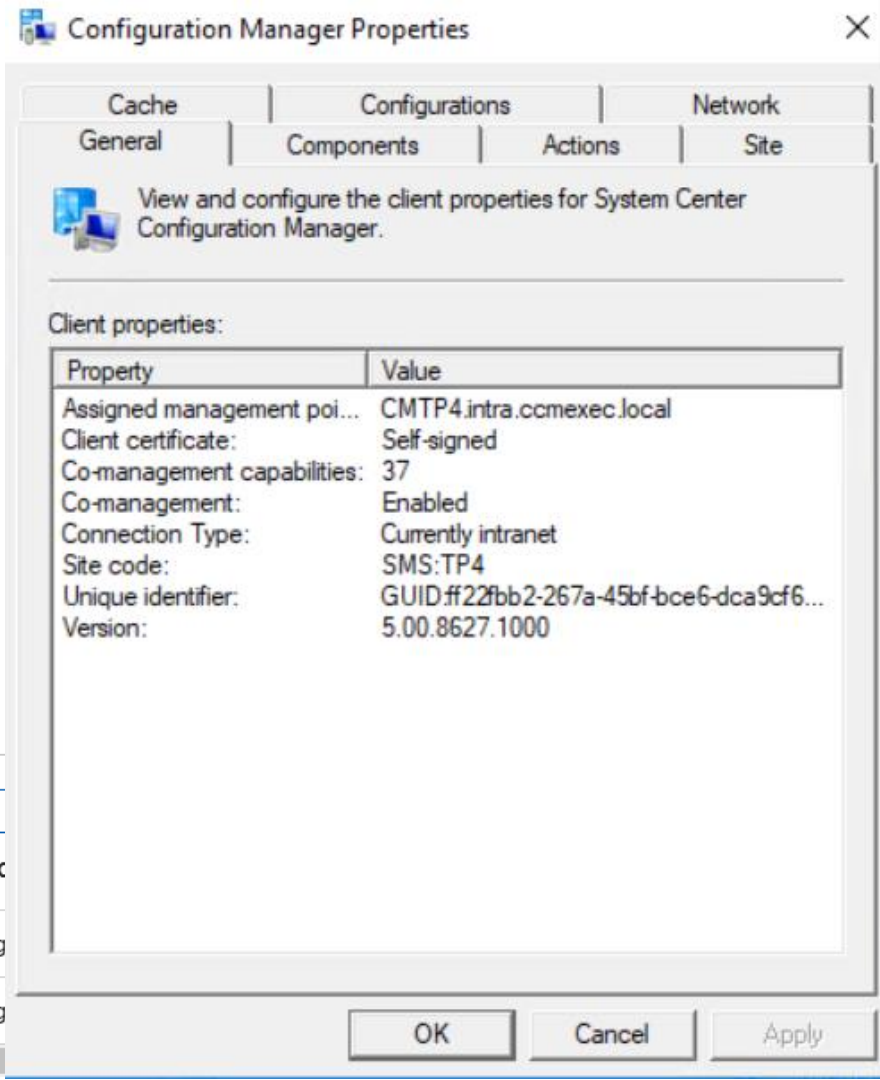
Staging

- Choose Pilot collection(if used)



Verifying

- Intune Portal
- Configuration Manager client
- Admin Console

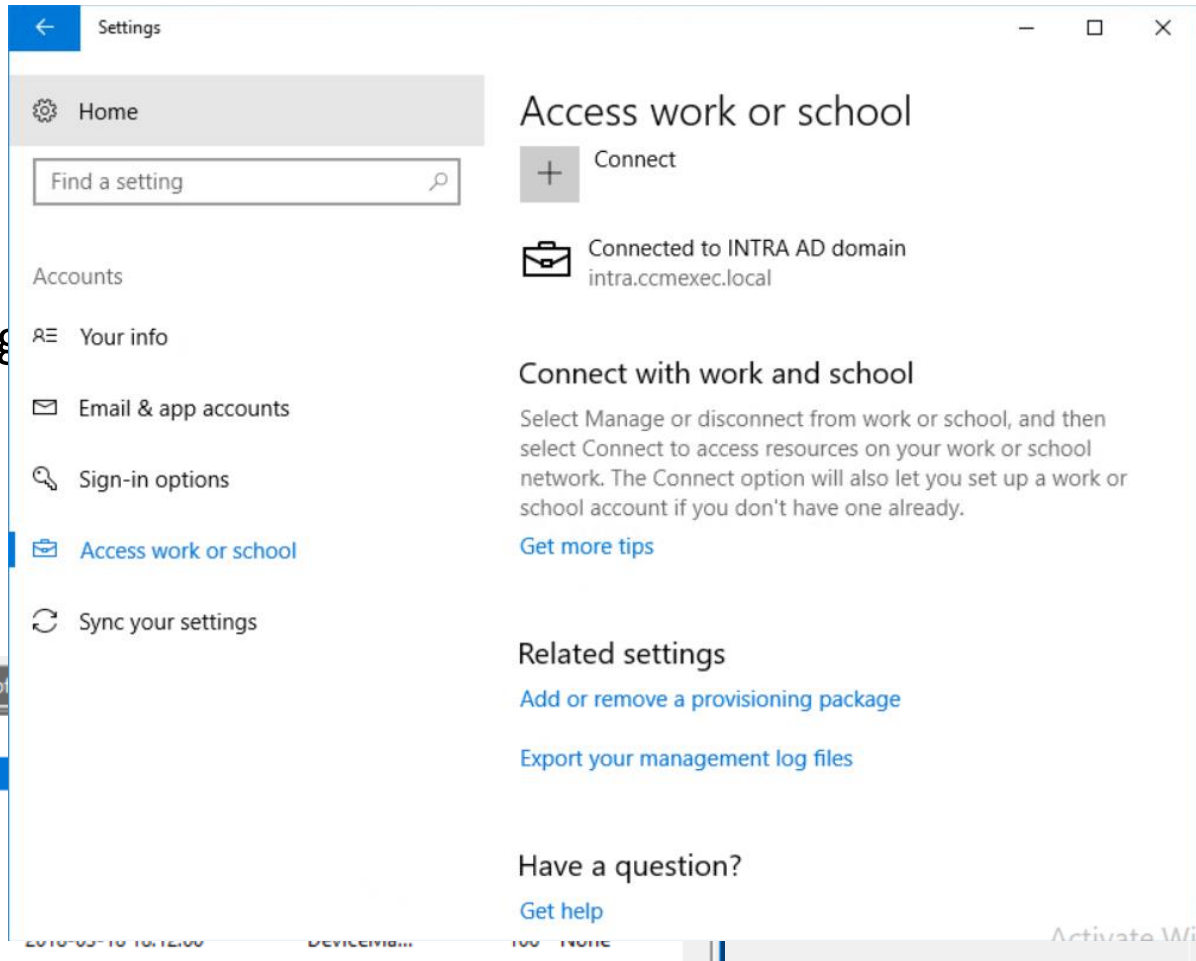
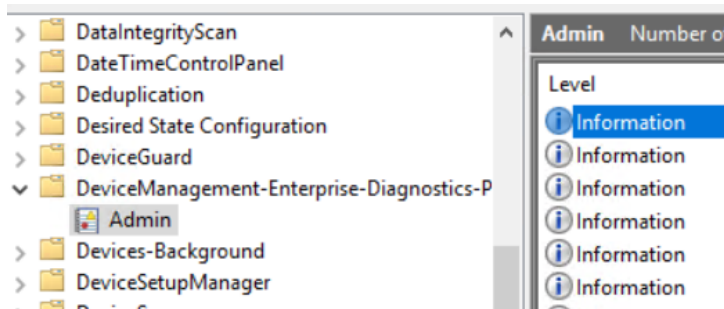


Search by Email, UPN or Device Name

DEVICE NAME	MANAGED BY	OWNERSHIP	COMPLIANCE
CMP001	MDM/ConfigMgr Agent	Corporate	See Config
CMP002	MDM/ConfigMgr Agent	Corporate	See Config

Troubleshooting

- New client log file:
CoManagementHandler.log
- Event log:
DeviceManagement-
Enterprise-diagnostics-
Provider



Common misunderstandings

- Co-Management requires Cloud Management Gateway and Cloud DP!
- Co-Management is only for AzureAD Joined computers
- Co-Management is to solve Intune shortcomings

Why Co-Management?!

Scenario – Azure AD Joined/Intune

- Windows Autopilot
- Make it possible to manage what Intune standalone cannot
 - Software Inventory
 - Reporting
 - Advanced App deployment
 -



ConfigMgr Client Setup Bootstrap - Properties

Intune Apps

Search (Ctrl+/)

GENERAL

Overview

MANAGE

Properties

Assignments

MONITOR

Device install status

User install status

* App type

Line-of-business app

* App package file
ccmsetup.msi* App information
Configure

App information

* Name

ConfigMgr Client Setup Bootstrap

* Description

Client Bootstrapper

* Publisher

Microsoft

Category

0 selected

Display this as a featured app in the Company Portal

Yes

No

Information URL

Enter a valid url

Privacy URL

Enter a valid url

Command-line arguments

AADTENANTID=E39472CF-EA87-4C62-B220-BE897985646C
AADTENANTNAME=Contoso

USER FAILURES

DEVICE FAILURES

0

0

Scenarios– domain joined

- Factory reset as long as the client have Internet connectivity
- Reboot action
- Compliance policies for Conditional Access

New in 1802 - Dashboard

Co-management

