Device Management Solutions

Savian So
Academic Solutions Specialist

Microsoft

Get started with Active Directory

Windows Server

Device Management in
System Center Configuration Manager (SCCM)

Microsoft System Center 2012
Configuration Manager

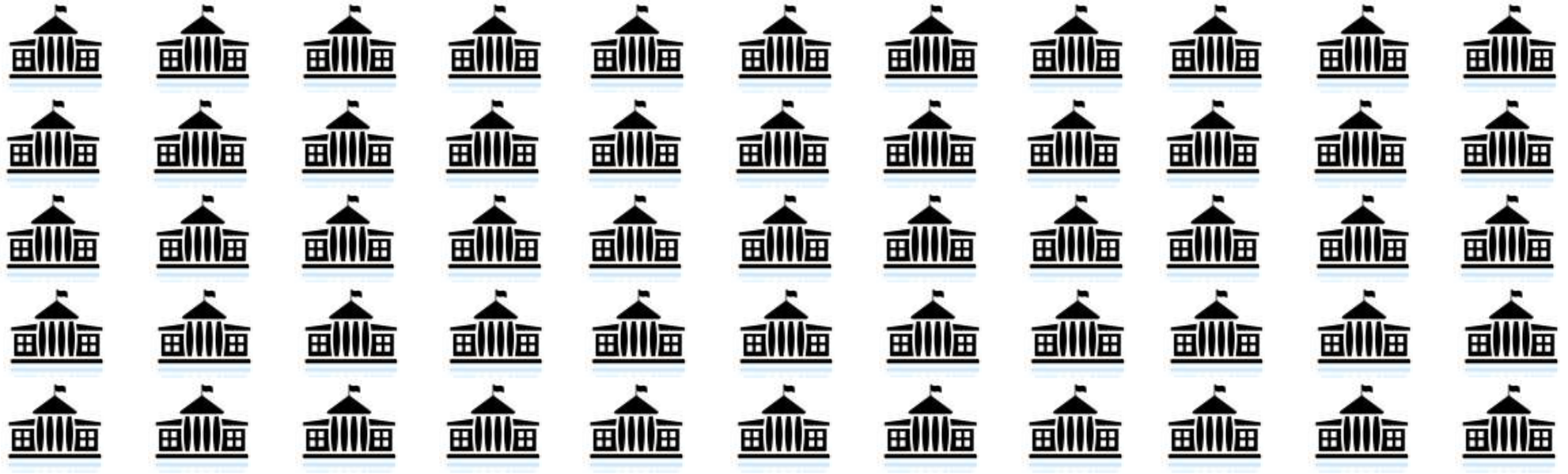
Windows Intune Connector for SCCM

Windows Intune

Microsoft

Before that

Using Active Directory (AD)?



The role of AD

- Manage Device Easily
  - Centralized Administration, Security Setting, Group Policy
- All About User Account
  - User profile, Roaming profile, Security Auditing
- Secure your share data
  - Share folder permissions, inheritance permissions

Microsoft

Group Policy ?

Microsoft

What is Group Policy?

- Infrastructure for managing user and machines in a Windows network
- Enables administrators to effect changes at targeted groups of machines and users

Microsoft

Examples

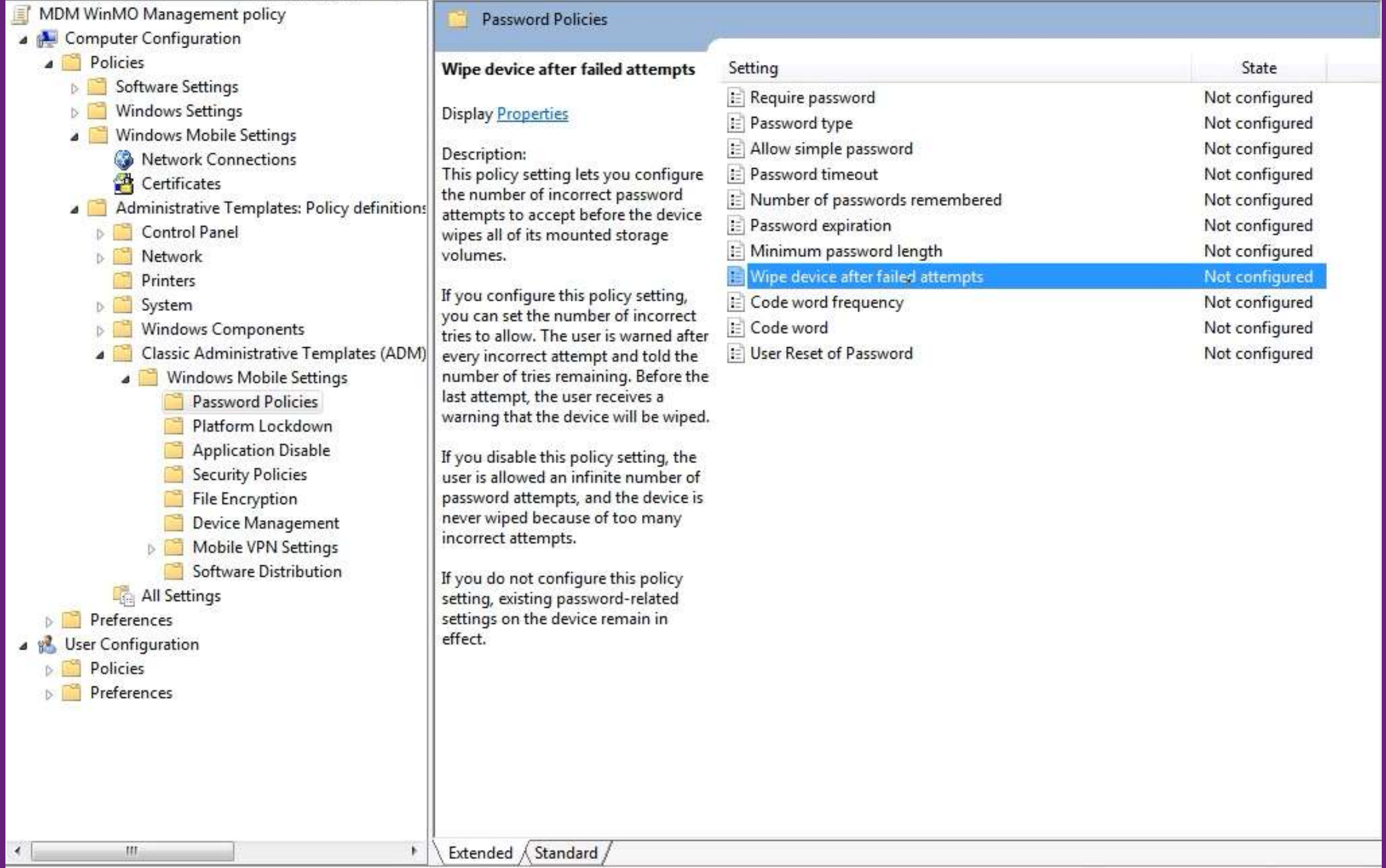
- Registry extension
- "Disable control panel," "Disable Remote Desktop"

- Software Installation
- "Show Add / Remove Programs"

- Security extension
- "Enable logon auditing"

- Folder Redirection
- "Put users' mydocs on the network"

Microsoft


MDM WinMO Management policy
Computer Configuration
Policies
Software Settings
Windows Settings
Windows Mobile Settings
Network Connections
Certificates
Administrative Templates: Policy definitions
Control Panel
Network
Printers
System
Windows Components
Classic Administrative Templates (ADM)
Windows Mobile Settings
Password Policies
Platform Lockdown
Application Disable
Security Policies
File Encryption
Device Management
Mobile VPN Settings
Software Distribution
All Settings
Preferences
User Configuration
Policies
Preferences
Password Policies
Wipe device after failed attempts
Display Properties
Description:
This policy setting lets you configure the number of incorrect password attempts to accept before the device wipes all of its mounted storage volumes.
If you configure this policy setting, you can set the number of incorrect tries to allow. The user is warned after every incorrect attempt and told the number of tries remaining. Before the last attempt, the user receives a warning that the device will be wiped.
If you disable this policy setting, the user is allowed an infinite number of password attempts, and the device is never wiped because of too many incorrect attempts.
If you do not configure this policy setting, existing password-related settings on the device remain in effect.
Setting
State
Require password
Not configured
Password type
Not configured
Allow simple password
Not configured
Password timeout
Not configured
Number of passwords remembered
Not configured
Password expiration
Not configured
Minimum password length
Not configured
Wipe device after failed attempts
Not configured
Code word frequency
Not configured
Code word
Not configured
User Reset of Password
Not configured
Extended
Standard

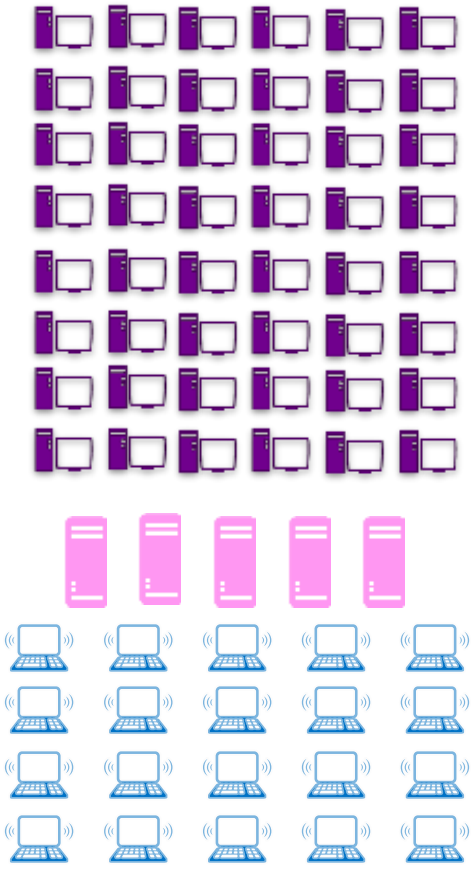
More Examples

- ON/OFF Wireless LAN
- Allow/Deny Removable Storage
- Enable/Disable Camera
- Block Application in ROM
- ON/OFF Application Notification
- Block Unsigned Applications Running on Devices
- Manage Certificates
- Device Encryption & Storage Card Encryption
- Configure the Windows Update for Windows Mobile Service

Microsoft


Microsoft
System Center 2012
Configuration Manager
Microsoft System Center 2012
Configuration Manager
Microsoft

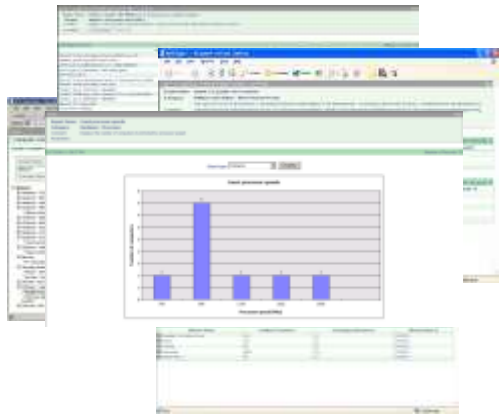
Microsoft SCCM 2012 Feature set overview



Discovery

Inventory

- Hardware
- Software
- Asset Intelligence
- Software Metering



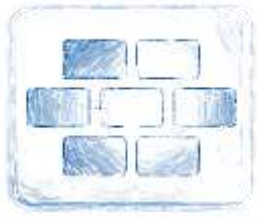
Reporting

Microsoft SCCM 2012 Feature set overview

OS Deployment
- Client or Servers
- Existing or new machine
- User parameters migration
- WIM image format
- Tasks sequencer
- Application compatibility

Application distribution and installation
- No Mandatory Packaging
- Dynamic Targeting based on user affinity and/or inventory
- Network Access Protection integration
- Wake-On-Lan

Update Management
- Microsoft security updates
- Hardware and software vendors catalogs
- Business Applications
- Maintenance Windows



Desired Configuration Monitoring
- Microsoft best practices
- Custom models
- Ability to remediate some settings

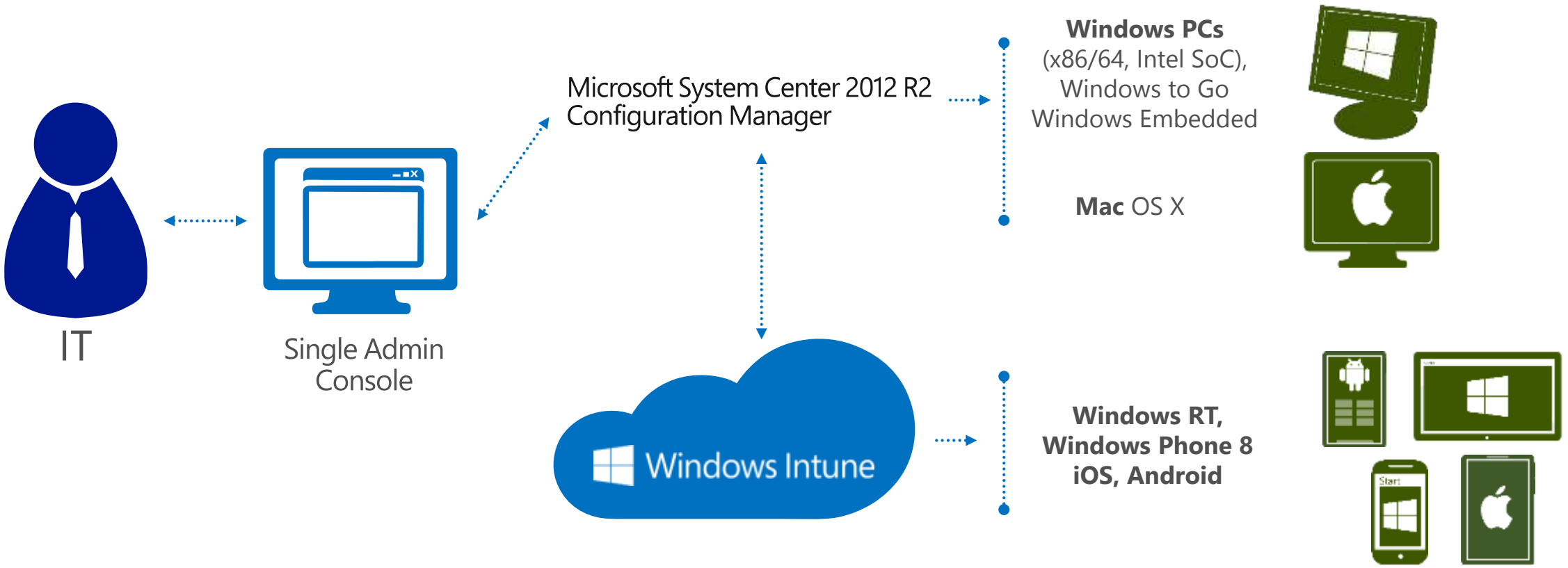
Microsoft

Windows Intune

Windows Intune Connector for SCCM

Microsoft

Windows Intune Connector Features



Windows Intune

Features of Window Intune

- Help Protect PCs from malware
- Deploy software & updates to PCs
- Proactively monitor PCs
- Set security policies
- Inventory hardware and software
- Track Microsoft & 3rd party licenses
- Integrate with Active Directory

- Management for Windows 8, Windows RT, Windows Phone 8, Android, and iOS devices.
- Set security policies
- Control Exchange ActiveSync (EAS) Security Policies
- Publish software to Users
- Inventory hardware
- Track LOB software deployment

Microsoft