Microsoft

System Center 2012 R2 Configuration Manager and Microsoft Intune

Manage PCs, servers, and mobile devices, all from a single management console

Users

- Demand their own choice of device
- Expect anywhere connectivity and productivity

IT

- Needs to maintain compliance and data protection
- Must avoid the complexity and cost associated with many discrete management infrastructures

Facts

- The worldwide smart connected device space will continue to surge, with overall shipments surpassing 2 billion units by the end of 2015 with a market value of $735.1 billion.[1]
- 61% of global enterprises provide IT support for company-owned smartphones and tablets, up from only 27% in 2011. This contrasts with 17% supporting employee-owned smartphones and tablets.[2]
- For company-owned smartphones, only 55% of decision-makers say that their company has security policies and sufficient tools, 35% say that they lack tools, and 6% lack a security policy and tools.[2]
- Only 30% of firms have policies and sufficient tools for employee-owned smartphones; 15% lack a policy entirely.[2]

With the consumerization of IT trend gaining momentum and mindshare, organizations are faced with the challenge of finding the right balance between allowing their employees to choose which devices they use, while making sure those devices have access to the right set of applications while meeting corporate data protection and compliance requirements.

Microsoft's solution builds on market-leading client management by combining System Center 2012 R2 Configuration Manager with Microsoft Intune to provide organizations with a comprehensive, cross-platform, and user-centric way to deploy applications and manage users' devices whether they are corporate-connected or cloud-based.

With Configuration Manager and Intune, organizations can enable their employees to choose their devices, unify their management infrastructure, and simplify IT administration. IT can deliver and manage consistent application experiences for employees based on their corporate identity, network connectivity, and device type, helping maintain productivity as employees use various devices throughout their day. Through a single infrastructure and administrative console, they can manage PCs, mobile devices, endpoint protection, and virtual machines across platforms, including Windows, Windows Phone, Mac OS X, iOS and Android.

Simplified server and client deployment, streamlined updates, and consolidated reporting enable your IT staff to easily manage your mobile, physical, and virtual client environments, reducing costs and increasing efficiency through comprehensive application and device management. Unified security, including System Center Endpoint Protection, protects your corporate information and helps you better manage risk by deploying software updates and antimalware definitions to PCs, as well as enabling selective wipe of mobile devices.

Enable users

Users can self-provision applications through a company portal. Users can view, install, and run corporate applications across devices, including corporate LOB applications, web applications, and links to IT-recommended applications available from public application stores.

Consistent self-service access to applications	Users can install applications from a Company Portal which is consistent across devices and platforms.
Automatic access configuration	Provides automatic VPN, Wi-Fi profiles, and authentication settings and manages and distributes certificates, giving end users access to company resources.

Unify IT management infrastructure

Configuration Manager and Intune enables you to streamline operations by consolidating all client management and security in a single infrastructure.

Unified device management	Enables you to manage Windows PCs, Macs, and Unix/Linux servers, as well as mobile devices running Windows Phone, iOS, and Android – all through a single infrastructure and administrative console.
Comprehensive settings management	Improves functionality by setting and enforcing configurations, triggering console alerts, providing richer reporting, and utilizing pre-built industry standard baseline templates. IT also gains visibility into at-risk devices through jailbreak and root detection for iOS and Android.
Integrated antimalware protection and management	Integrates desktop security and compliance management to protect against malware through System Center 2012 R2 Endpoint Protection, remediate vulnerabilities, and deploy updates.
Reduced infrastructure requirements	Lowers the number of physical servers and primary and secondary sites and provides scalability enhancements. Uses in-console monitoring to track software distribution and report on infrastructure utilization to help reduce cost and complexity.

Simplify IT administration

Configuration Manager and Intune make it easier and faster for you to keep systems well managed and compliant.

User-centric app delivery	Enables IT to provide applications to people while defining the best delivery mechanism for each application to a device based on the platform being used. Provides the ability to differentiate application installs between corporate and personal devices.
Software update management	Identifies which devices are not up-to-date; delivers and installs the required updates and reports.
Role-based administration	Enables IT to access tools and information based on scope of activity and span of control.
Multiple OS deployment method support	Provides support for PXE-initiated, multi-cast network-based installations, stand-alone media, and pre-staged media deployment.
Client activity and health	Offers an in-console view of client health, threshold-based console alerts, hardware/software inventory and status, and remediation.

For more information about Configuration Manager, visit www.microsoft.com/configmgr.