Bring your own device is no longer just a trend—it is arguably the dominant workplace culture. More employees are using personal devices for work, creating a unique set of challenges for IT teams that must balance user convenience and data security. Core Services Engineering (CSE, formerly Microsoft IT) uses Enterprise Mobility Suite and other services to manage identity, devices, and applications. Now, simplified and integrated IT solutions enable employees to be productive on any device.

**Situation**

In a bring your own device (BYOD) work environment, users expect to be able to work from any location at any time, on the device of their choice. Moreover, users now typically have several identities, meaning that they use their devices in both work-related and non-work-related contexts. For example, they might bring a personal tablet to a business meeting and expect to access files on a team’s Microsoft SharePoint site, or they might present a Microsoft PowerPoint presentation over Microsoft Skype for Business. They’re likely to check both work and personal email accounts on their phone, and may use their phone camera to take photos of whiteboard sessions to help them remember what a work group collaborated on during a meeting. On both types of device, they’re likely to have a mix of apps, some for personal use and some for work.

But as the traditional boundaries between work and personal life blur the use of these devices, it’s critical that devices be managed in a way that is acceptable to the entire business. Data policies, such as encryption, password length, password complexity, and password duration, must provide corporate data security on all devices while maintaining the privacy of workers’ personal information.

IT must be able to identify, with certainty, who a user is and if a device should have access to corporate resources. Current trends suggest that workers change jobs and companies several times over the course of a career, so IT needs a way to account for this flux of people and devices. What should IT do if a device is lost or an employee leaves the company? What is the best way to ensure that corporate resources are wiped from a personal device that should no longer have access to them?

In short, the situation for IT is about managing data, managing access to that data, and handling the use of multiple accounts and identities on a device.

**Solution**

CSE approaches mobile device management as just one of a set of issues that are related to a mobile workforce. The first step is to make IT cloud-based and enable a mobile workforce. To address these, it is using the Enterprise Mobility Suite including solutions in Microsoft Intune and other Microsoft Azure services.

**Benefits**

- Low-cost, scalable solution
- Central location for users to access IT services
- Simplified administration via a single console
- Compliance and increased security
- Flexibility to meet user needs

**Products and technologies**

- Microsoft Intune
- Microsoft Enterprise Mobility Suite
- Active Directory Domain Services
- Microsoft Azure Active Directory
- Microsoft System Center Configuration Manager 2012
- Microsoft System Center Configuration Manager 1511
Solution

CSE has been involved in mobile device management (MDM) for several years and is evolving strategies and best practices to ensure the proper balance between convenience and security as BYOD becomes the norm in organizations of all sizes.

CSE approaches MDM a bit differently today than it did in the past. Even as recently as 2013, the focus was much more on providing access to applications. Now, however, the focus is on access as defined by certificate and profile provisioning. In the future, the focus will be on conditional access that is based on the state of the device as interpreted through the MDM system and Microsoft Azure Active Directory.

The Microsoft Intune and Microsoft Azure teams are working together to provide solutions so that CSE can address a range of related issues: identity and access management, mobile device and app management, and information protection. The first step is to make CSE cloud-based and enable a mobile workforce.

Identity and access management

For employees who use multiple devices for work, a key convenience—a requirement, even—is to have single sign-on (SSO) and a common identity, so that they can get their work done on whatever device suits them at the moment. A common identity enables application access management, regardless of whether those applications are on the device or in the cloud. This ensures that the user can have a consistent experience across devices and remain as productive as possible.

CSE is delivering identity and access management by providing that SSO experience, using federation to manage access to external resources, and consistently managing identities across on-premises and cloud-based identity domains. This helps CSE address the matter of managing access.

The following are some specific features:

- CSE provides users with a common identity across on-premises and cloud-based services through Microsoft Windows Server Active Directory and by connecting to Azure Active Directory.
- CSE uses Active Directory Federation Services (AD FS) to connect with Azure for a consistent, cloud-based identity.
- Through their accounts in Azure Active Directory, users have a common identity across Azure, Microsoft Office 365, and third-party applications.
- Developers can build applications that use the common identity model, integrating applications either with Active Directory Domain Services for on-premises applications or with Azure for cloud-based applications.

Azure Active Directory syncs with on-premises Active Directory Domain Services through Azure AD Connect. Azure Active Directory enables self-service password changes and resets, and self-service group management for internal users. It also supports multifactor authentication, so that internal users don’t have to carry around their smart cards.

Multifactor authentication provides an additional layer of security in case a device falls into the wrong hands or is used improperly. When a user attempts to log on or perform an action that is subject to multifactor authentication, the application or service confirms the user’s identity by sending a text, making a phone call, or using a mobile app. Typically, this additional authentication factor is a numeric code, such as a personal identification number (PIN), and may only be intended for a single use. The user must respond (usually within a limited period, such as 10 minutes) before the application or service allows him or her to proceed.
Credential caching enables enterprises to determine how long credentials can be cached on a device. This allows the enterprises to customize the user experience when users access applications and resources on devices. For example, enterprises can specify how long credentials pass through during logon or device registration, so that users do not have to enter their credentials so many times.

Mobile device management

Users prefer a consistent experience when they access and work with their line-of-business (LOB) apps, no matter what device they use, how often they use it, and what platform it runs. Device enrollment should be simple, and the process for finding and working with apps and other internal resources should be familiar. In addition, policies should help users feel secure that their personal data is protected on devices that they also use for work, and it should be possible to remove devices that users no longer want included in a managed environment.

Device enrollment

Users can enroll a device relatively quickly in Intune. Notably, the process is opt-in rather than opt-out. This sets a friendlier tone for the experience, because it doesn’t feel like a mandate. Users recognize the value of being able to use personal devices for work, and voluntarily enroll them.

Similarly, when users no longer want to use a device for work, they can easily remove it by using the Intune console (the web portal for information workers). For example, if a device has been lost or stolen, the user can either remove it for himself or herself, or request that CSE do so. When a device is removed, corporate assets are automatically removed from it. Devices can be completely wiped or just selectively wiped. See the “Device retirement/wiping” section later in this document.

Intune provides a single administrative console that it can use to manage all enrolled devices. One administrative advantage of this solution is the ability to create reports, such as security and audit reports.

Provisioning of the Company Portal

For users who connect to corporate resources on mobile devices, CSE now relies on its Company Portal to provide a kind of “one-stop shopping” experience for installing and using the Microsoft Windows or LOB apps that they need. Currently, users on iOS or Android platforms install the Company Portal from a separate site. For users on Windows or Windows Phone platforms, the Intune service pushes the Company Portal out to the device.

The Company Portal includes approximately 350 apps—and the number is growing at a rate of 10 to 15 new apps per month. Provisioning also includes updates of existing apps—as many as 35 to 40 are updated per month. Each month, there are approximately 30,000 application installations, and availability of the service has been more than 99 percent.

One goal that CSE has for the Company Portal is to create apps that package streams of content and functionality for specific roles and use cases. For example, for users in field sales and marketing, the GearUp app provides a quick reference to every product that Microsoft sells, including value propositions and competitive differentiation. For users who do a lot of business travel, an app is available to instantly track expenses while they are on the go, helping users complete expense reports more quickly for improved compliance.

Policies across mobile devices

Whether they are related to encryption, passwords, security, email management, or another fundamental issue, policies are the cornerstones of MDM in an organization. In Intune, users see a dialog box that informs them about policies. They can then select to allow apps and services from CSE, or they can cancel device enrollment.
Although users do not always fully appreciate this fact, policies are a form of protection for them too. Their own personal data on the devices that they use for work is more secure when other users and devices in the same environment are managed by policies. For more information about compliance settings for mobile devices, see the “Policy and security configuration” section.

Mobile application management

From an application standpoint, user and device provisioning is an important piece of the mobility landscape in organizations. For example, after app deployment, the app owner can use tools such as Operations Manager in Microsoft System Center to discover issues such as application dependencies, monitor application components, and isolate the cause of issues that are found during monitoring. They can even triage and remediate in Microsoft Visual Studio to fix any issues in the code. From an IT perspective, apps must be managed securely within the overall MDM service. LOB apps should be signed and should be accessed only by managed users.

Information protection

CSE has several goals for information protection, such as keeping corporate data secure, managing data rather than the user, and providing access to data on any trusted device. Techniques for achieving these goals include encryption and policies, as mentioned earlier.

Additionally, Intune enables access to company resources through certificate profiles. When certificate profiles are used to configure managed devices with the certificates that they need, device users can connect to on-premises company resources by using connections such as Wi-Fi or a virtual private network (VPN). When CSE deploys certificate profiles, it provisions devices with a trusted root certificate for the company’s public key infrastructure (PKI) and configures them to request device-specific certificates.

CSE will be offering conditional access features to help improve the precision of access and protection. For example, users who require just read-only access to a file or resource will be restricted from editing, printing, or forwarding it. One of the most significant scenarios for conditional access is email provisioning, but other scenarios include certificate provisioning and profile provisioning. Taken together, these techniques help address data management.

Deployment

Although CSE is evolving its approach to MDM, it’s important to consider, from a tactical perspective, how exactly it performs MDM. The information in this section describes, in detail, a deployment solution for a hybrid environment that includes both System Center Configuration Manager and Intune. Although smaller organizations might need only Intune (a stand-alone rather than hybrid environment), most medium to large organizations, including Microsoft, already have Configuration Manager and use it in combination with Intune.

Architecture

MDM consists of a series of components that work in concert:

- Configuration Manager provides the central administration console for administering both on-premises and cloud-based devices.
- The Intune subscription establishes the connection between Configuration Manager and Intune. It specifies the configuration settings for the Intune service, such as which users can enroll their devices and which mobile device platforms should be managed.
- Microsoft Intune Connector site system role, which is a Configuration Manager site role, acts as a gateway between Intune and on-premises Configuration Manager, sending settings and software deployment information to Intune, and retrieving status and inventory messages from mobile devices.
The following sections describe the various activities that are involved in the CSE MDM deployment.

Deployment process
CSE took a five-step approach to deploying MDM in its existing Configuration Manager environment.

Step 1: Build a Configuration Manager 1511 or SP1 environment
CSE added a Configuration Manager 1511 primary site that is specifically for MDM to the corporate domain hierarchy. Server hardware consisted of the following:

- A primary site server that uses a virtual machine with 12 gigabytes (GB) of RAM and four core processors
- A Microsoft SQL Server with 64 GB of RAM and six core processors

A separate site for MDM is not required. Because MDM can scale to large volumes of devices, most small and medium organizations will not need a separate site and can incorporate MDM into their existing site hierarchy.

Step 2: Provision users
CSE performed user discovery for the entire Microsoft corporate Active Directory forest by using the existing production Configuration Manager environment. This process took a few hours because of the large user base in Microsoft, but it ensured that all users were added to a user collection before MDM was enabled.
Organizations must consider the extent of their BYOD environment to determine if they need to perform a full user discovery, or whether the users who are allowed to enroll their mobile devices should be added manually to Configuration Manager.

**Step 3: Provision Intune services**

CSE worked with the Azure Active Directory team to provision Intune services for the Microsoft IT organizational user (tenant) account and set up the MDM services Admin (the account that is used for authentication when the Intune subscription is created in Configuration Manager). Microsoft IT also worked with the Active Directory team to configure Azure AD Connect and Active Directory Federation Services Windows Server 2012 R2. Azure AD Connect ensured that all users were synchronized into the cloud, and AD FS enabled users to use SSO to access all cloud services.

Microsoft had an existing tenant account because it already used Microsoft Office 365 and other cloud services; it also had Azure AD Connect and AD FS in place to synchronize data into the cloud. Companies that do not have these services in place will need to complete these tasks:

- Sign up for an Intune organizational (tenant) account.
- Deploy and configure Azure AD Connect to synchronize on-premises Active Directory users with the Azure AD Connect, creating the user ID that is used for cloud-based applications.
- Deploy AD FS to allow for a single identity for each user across both on-premises and cloud-based applications.

**Step 4: Set up DNS redirection**

Most companies will benefit from creating a Domain Name System (DNS) alias (CNAME record type) to redirect enterprise enrollment to <yourcompany>.com to allow for server auto discovery. This means that users will not need to know the actual server name when they enroll their device.

**Step 5: Acquire device-specific certificates**

Each device platform has different requirements for loading applications. CSE worked with the Microsoft App team to acquire the certificates that are required for the supported mobile devices.

**MDM configuration**

Enabling MDM requires creating an Intune subscription and defining an Intune Connector role in Configuration Manager. MDM is now equipped to work with any device platform, including iOS, Android, and Windows Phone. To set up and configure MDM, CSE completed these steps:

1. **Create a new Intune subscription.** In the Subscription Wizard, CSE selected Allow the Configuration Manager console to manage this subscription. This enabled Configuration Manager to become the authoritative source for managing all mobile devices, providing a single administration console for on-premises systems, cloud-connected devices, and application life cycle management.

2. **Define a user collection.** CSE created a custom user collection for all Microsoft employees, based on the users who were discovered during user discovery for the entire Microsoft corporate Active Directory forest. This ensured that members of this collection were licensed for enrollment in MDM.

3. **Configure the platform, certificates, and keys.** For each platform, CSE applied the required certificates.

4. **Assign a connector role.** CSE added the Intune Connector site server role to the Central Administration Site (CAS) server. The Intune Connector server role communicates directly with Intune and provides the communication gateway between Configuration Manager and Intune for all incoming and outgoing communication.
Cloud User Sync monitoring
After MDM is configured, a Configuration Manager component named Cloud User Sync provides communication between Configuration Manager and Intune. It monitors the collection of users for additions, synchronizes changes with Intune to license users, and enables users to enroll their devices.

CSE makes the following recommendations for Cloud User Sync monitoring:

- **Use delta user discovery and incremental updates.** When delta discovery is enabled in AD User Discovery settings, and incremental updates are selected in the collection settings, updates are synchronized more often. This ensures that licensing new users and removing licenses for disabled users occur quickly.

- **Use default Cloud User Sync settings.** Cloud User Sync synchronizes changes, such as when new users who have been added to the collection are licensed and enabled for enrollment or when the Intune license is revoked for users who have been removed from the collection. By default, synchronization occurs every five minutes and is a minimal burden on the Configuration Manager hierarchy and network.

- Monitor the following Intune Connector log files:
  - **Dmpdownloader.log** to monitor policy changes that are downloaded from Intune to Configuration Manager
  - **Dmpuploader.log** to monitor policy changes that are uploaded to Intune from Configuration Manager
  - **Cloudusersync.log** to monitor user licensing in Intune

- Use the CloudUserID field in the User_Disc table in Configuration Manager to identify whether users are licensed:
  - **Null** indicates that a user is not licensed to enroll devices.
  - **All zero GUID** indicates that a user was previously licensed but is no longer a member of the user licensing collection.
  - **Non-zero GUID** indicates that a user is licensed to enroll devices.

Users do not have to be licensed separately for each device. When a user is licensed, he or she is licensed for up to 20 devices.

Device enrollment
In addition to configuring the MDM architecture, CSE had to plan the user experience as part of its deployment. It wanted to ensure that the process for enrolling devices had these characteristics:

- It provides a good user experience, where users can enroll their devices, gain access to the Company Portal, and install LOB applications with minimal user intervention.

- It enables users to become productive quickly with LOB apps by providing a seamless SSO installation. AD FS enables Microsoft users to use the same credentials (their corporate user ID, email account, and network password), regardless of device.

When a user enrolls a device, CSE collects general information about the device, such as the manufacturer and any LOB apps that are installed from the Company Portal (but not from the Microsoft Store). The Company Portal is a required app for every newly enrolled device.
Troubleshooting enrollment
- CSE experienced enrollment failures because some users had a non-standard User Principle Name (UPN). The enrollment process is based on a user’s UPN, but the UPN of some Microsoft users deviated from the standard naming convention and also differed from their user alias. To resolve this issue, CSE created a DNS redirection.
- Because there are no client logs for enrollment troubleshooting, CSE needed to take a systematic approach to troubleshooting.
- CSE recommends that the following issues be verified when troubleshooting general device enrollment issues:
  - The Admin has configured MDM.
  - The Admin has enabled enrollment for specific device types.
  - The Admin has provisioned the user for mobile device enrollment.
  - The user is not trying to enroll several devices at the same time and has not enrolled more than 20 mobile devices in the system.
  - For Windows Phone 8.1 devices, the code signing certificate is configured properly.
  - For iOS devices, the Apple Push Notification Service certificate is configured and hasn’t expired, and the device is running iOS v5.0 or later.

Enrollment lessons learned
CSE learned lessons from a few issues that occurred during the enrollment process, particularly regarding user education requirements:
- Users were concerned about the type of information that CSE could see and collect about their personal devices. CSE needed to reassure users that it collects only general information about the device itself (such as the manufacturer) and any LOB apps that are installed from the Company Portal—and that it collects no personal information, such as phone numbers, personal apps, or apps that are installed from the Microsoft Store.
- Users were sometimes confused about differences in the enrollment process for the various mobile devices platforms (for example, one platform might have additional screens for adding management profiles on the device). To address this issue, CSE documented the enrollment process for each device and made this documentation available through the company support website, ITWeb.

Policy and security configuration
To help ensure that corporate security was maintained while also providing a good end-user experience, CSE had to coordinate with the following Microsoft teams:
- The Microsoft Security team, to define the policies that would enforce Microsoft corporate compliance settings on mobile devices, such as password policy and encryption settings.
- The Exchange team, to align policy settings between Exchange ActiveSync (EAS) and MDM.
- CSE took advantage of default compliance rules for mobile devices that are built into Configuration Manager. It created new configuration items (CIs) for mobile devices (different CIs for each device type, to make troubleshooting easier) and added built-in compliance rules whose values are based on CSE security requirements (see Table 1). It then created a configuration baseline for those CIs and targeted the configuration baseline to the collection of mobile devices.
Table 1. CSE compliance settings for mobile devices

<table>
<thead>
<tr>
<th>Corporate policy</th>
<th>Windows Phone</th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum password length</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Password expiration</td>
<td>70 days</td>
<td>Not set</td>
<td>Not set</td>
</tr>
<tr>
<td>Allow simple password</td>
<td>Not set</td>
<td>Not set</td>
<td>False</td>
</tr>
<tr>
<td>Number of failed logon attempts before device is wiped</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>File encryption on mobile device</td>
<td>True</td>
<td>True</td>
<td>Not set</td>
</tr>
<tr>
<td>Idle time before mobile device is locked</td>
<td>15 minutes</td>
<td>5 minutes</td>
<td>15 minutes</td>
</tr>
</tbody>
</table>

CSE makes the following recommendations for configuring mobile device policies:

- Align policies, such as password/PIN policies, across EAS and MDM to ensure the best end-user experience. Although the most restrictive policy will apply, different user experiences have the potential to increase support calls.

- If a policy does not apply to a particular device platform, the policy will report which platforms do not support it. Use common policies to simplify administration. For example, set the same password requirements across all mobile device platforms so that multiple CIs and different device collections are not required to support various password policies.

- Create custom device collections when policies cannot be aligned across platforms. The Configuration Manager console shows enrolled devices by device type. Use the Agent Edition attribute to create custom device collections and then target policy baselines to each collection.

- In both CIs and configuration baselines, to enforce compliance settings on the device, enable Remediates noncompliant settings. Otherwise, reports will reflect the current compliance state of enrolled devices but will not enforce compliance rules/settings on those devices.

Device retirement/wiping

Like other organizations, Microsoft needs a way to enforce security if users leave the company or lose a device. To help secure a lost device or retire a device from active use, CSE issues a wipe command to the device.

There are two types of wipe commands:

- A full wipe restores the device to its factory defaults. This removes all company and user data and settings. A full wipe can be performed on Windows Phone, iOS, and Android devices.

- A selective wipe removes only company data. The specific data that a selective wipe removes and the effect on data that remains on the device vary by device platform.

To limit which administrators can wipe or retire a device, CSE used role-based access control (RBAC) in Configuration Manager to restrict the view in the console for some administrators. After an MDM pilot has been conducted in a test hierarchy, it is important to retire all devices from the Configuration Manager console before the move to a production hierarchy.

IT Showcase Technical Case Study
Reporting
Configuration Manager includes many ready-to-use, built-in reports for MDM, including reports for apps, hardware inventory, and settings management, so it is not necessary to create custom reports. It is also not necessary to create separate reports for desktop device and mobile device management: the same report can be used to report on both types of environment.

CSE used built-in Configuration Manager reports to report on its MDM environment. In particular, two built-in reports provided CSE with insight into the application installation status and policy compliance status for MDM:

- **Security policy compliance report** (Home > ConfigMgr_<sitecode> > Compliance and Settings Management > Summary compliance by configuration baseline)
- **Application compliance report** (Home > ConfigMgr_<sitecode> > Software Distribution – Application Monitoring > Application compliance)

CSE also used Configuration Manager console monitoring to easily view and drill down to the asset level for the status of app deployment and security policy compliance.

Although custom reports were not needed because of the built-in reporting capabilities of Configuration Manager, CSE did create a custom Unified Device Management (UDM) dashboard for Microsoft executive management by using Microsoft SQL Server 2012 Reporting Services. This dashboard provides executive management with visibility into enrollment count trends through graphs, and also has a look and feel that are similar to other CSE dashboards.

Results
By creating a solution that streamlined the administration and deployment of devices and applications, CSE was able to increase the scope of its centrally managed devices by 10 percent at initial implementation, without having to add resources or administrative overhead. CSE expects this number to continue to increase at a rapid pace and sees potential for centrally managing more than 100,000 mobile devices.

Benefits
The benefits of mobile device management include:

- **Low-cost, scalable solution.** Intune integrates into the existing Configuration Manager environment without requiring new infrastructure, hardware, or network complexity in the CSE environment. It provides enterprise-level scalability, extending the reach of Configuration Manager to support management across device platforms.

- **Simplified administration.** The Configuration Manager console unifies device management, providing CSE administrators with a single console for administration, application management, and reporting across multiple device types.

- **Empowered users.** MDM provides a consistent end-user experience across device platforms. Microsoft users can enroll their personal devices, install internal business applications, and manage their mobile devices through the Company Portal, allowing them to be more productive from almost anywhere on almost any device.

- **Maintained compliance.** Compliance policies are maintained across multiple device platforms to meet Microsoft compliance and security requirements while providing a good end-user experience for Microsoft users. Security risks for lost, stolen, or retired devices are reduced, because CSE administrators can remove corporate data and applications from a device through Configuration Manager. Microsoft users can also remove data and applications for themselves, through the Company Portal.

Best practices
CSE recommends the following best practices for implementing MDM:

IT Showcase Technical Case Study
• Plan the deployment. Proper planning before deployment will increase deployment efficiency.
• Review the Configuration Manager hierarchy to determine how best to integrate MDM. Remember, MDM does not require a separate site in the Configuration Manager hierarchy.
• Understand which platforms the organization will support. This will help determine what types of certificates are required for app deployment.
• Acquire and deploy certificates and sideloading keys before user enrollment is enabled. Coordinate with other teams to streamline the app certification process.
• Identify and license specific users by using user discovery in Configuration Manager, and then add users to a custom collection that will synchronize these user accounts with Intune.
• Enable AD FS to allow users to use the same user name and password to access corporate resources.
• Work with the security and Exchange teams to align passwords and policies across device platforms to ensure a good user experience without compromising corporate security.
• Promote collaboration among all teams involved. Several different teams in the organization might need to be involved—including security, compliance, application developers, services, and infrastructure providers. It is important to ensure that all stakeholders can provide input at an early stage and that they can work together to ensure a smooth deployment.
• Develop a detailed communication and readiness plan. A well-developed support plan and documentation for user and helpdesk readiness can reduce support costs.
• Train help desk technicians before deployment. Have training and support content ready for modern device support, especially for any differences in the user experience across device platforms.
• Educate users. Provide users with documentation about the enrollment steps for each supported device platform to reduce support calls. Set expectations for any delays between enrollment and when Company Portal apps are available for installation. To reduce user concerns, make sure that users understand what is being inventoried on their devices. Create frequently asked questions (FAQs) for common questions, and document any known issues.
• Plan the enrollment process. To ensure a good user experience and reduce support costs, consider how the Company Portal and LOB apps will be deployed.
• Use categories to organize applications on the Company Portal and make them easier to find.
• Use security groups to limit what apps users can see, based on their role in the company.
• Determine which apps to publish on the Company Portal, based on business needs. Determine how long apps will be maintained on the Company Portal before they are retired.
• Evaluate which apps might change often, and consider using a deep link instead of deploying the full app.
• Use the Windows Phone emulator in the Windows Phone software development kit (SDK) to test the Windows Phone enrollment experience.

Resources
Manage Mobile Devices with Configuration Manager and Microsoft Intune

Microsoft Intune overview

IT Showcase Technical Case Study

Documentation Library for System Center 2012 Configuration Manager

System Center Technical Documentation

Directory synchronization roadmap

Related case studies

How Microsoft IT Deployed System Center 2012 Configuration Manager
https://www.microsoft.com/itshowcase/Article/Content/126

Microsoft IT Discusses Deployment of Unified Device Management

Building Reusable APIs in a Mobile First, Cloud First Business Environment
https://www.microsoft.com/itshowcase/Article/Content/493

Transforming IT into an Innovation Engine
https://www.microsoft.com/itshowcase/Article/Content/373

For more information

For more information about Microsoft products or services in the United States, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada Order Centre at (800) 933-4750. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information via the web, go to:

http://www.microsoft.com

© 2016 Microsoft Corporation. All rights reserved. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.