Implementing Mobile Device Infrastructure

Crowley

Ch 7

Topics

- Installing and deploying mobile device management solutions
- Mobile device on- and off-boarding processes
- Managing mobile device operations
- Configuring and deploying mobile device technologies

Mobile Device Infrastructure Scope

- Install and Configure Requirements-Based Mobile Solutions
- MDM installation considerations
- User base
- Infrastructure size and complexity
- Organizations interoperability requirements.

- User profiles
- Directory services for the new mobile infrastructure
- Establishing certificate policies
- Reviewing end-user licensing agreements

Business and Technical Aspects

- Both policy and technical aspects of setting up security features such as containerization and sandboxing.
- Group profiles need to be set up in advance
  - Include groupings of particular types of users such as executives, consultants, and so forth.
- Consider a pilot program
- Final approval for the implementation from upper management
- Document policies, plans, and procedures for implementation.
- Train users and administrators
- Consider program's life cycle
  - In terms of equipment and service acquisition.

Infrastructure Support and Coordination

- Best practice make sure you have everything in place to support MDM infrastructure.

May mean:

- Buying additional servers or provisioning additional bandwidth to accommodate added capacity.
- Upgrading server operating systems or adding security devices.
- Test all additions, as well as existing infrastructure
  - Make sure they can handle the increase in network traffic and server load.

Directory Services Setup

- As most MDM solutions, as well as mobile devices, integrate with the organization's existing directory services structure, directory services may need modifications.

- Lightweight Directory Access Protocol (LDAP) structure, such as Microsoft's Active Directory, likely will require a review of directory containers and policies.

Initial Certificate Issuance

- Prior to rolling out MDM , plan for PKI certificates.
- Develop policy regarding mobile device and user certificates.
- Consider setting up an automatic enrollment process using a self-service or captive portal, or even third-party enrollment if you use outsourced certificate services.
- The user's personal certificate will also need to be installed on the mobile device, as well as the device certificate itself, if it is used to authenticate itself to other devices.

End User Licensing Agreements

Review

- End user licensing agreements (EULA) to ensure compliance with laws and contracts with software vendors.
- Licensing agreements covering enterprise and volume licenses.
- Multi-instance software licenses.
- Organizational policies should mention and implement technical measures, such as license servers, to keep track of organizational and user compliance with those policies.

Sandboxing

- Technique used to keep apps separate by allowing them to run in their own restricted memory space
  - With restricted resources and limited access to other apps and hardware.
- Make sure that the needed technical infrastructure is in place.

Containerization

- Containerization is a method of separating data, and is commonly used to keep corporate and personal data separate on both organizationally owned as well as personally owned devices.
- Make sure that the MDM solution you are going to use supports containerization.
- End users also need to be trained on how containerization works and how they can use it to protect their own personal data and keep it private, as well as protect corporate data that resides on the device.
- Developing organizational policy on how containerization will be implemented, what data will be segregated, and so on is also important.

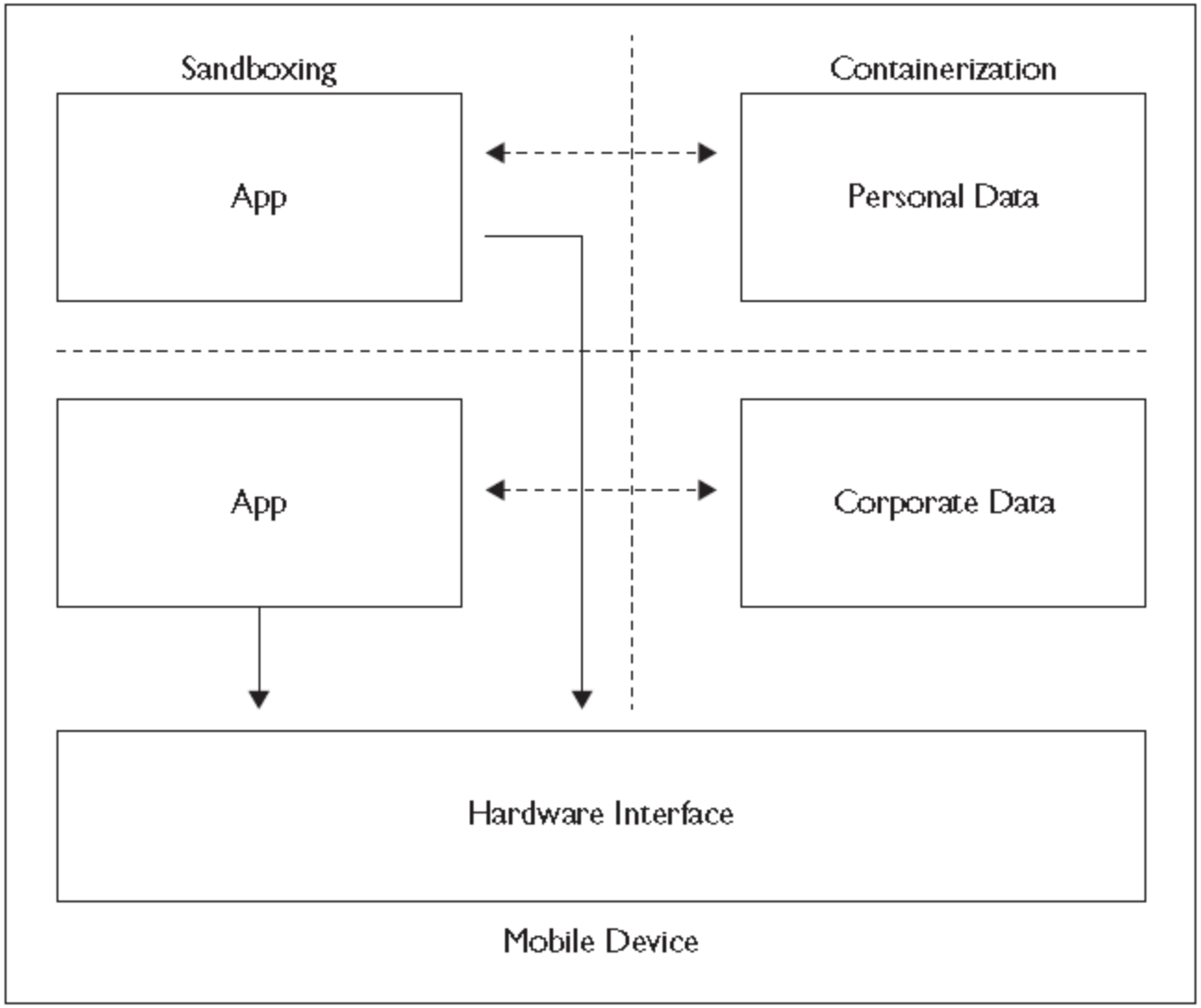


Figure 7-1 Illustration of sandboxing and containerization concepts

Device and Group Profiles

- A profile is a collection of configuration and security settings that an administrator has created in order to apply them to particular categories of users or devices.
- A profile can be created in several different ways.
  - Including through the MDM software
  - Or in a program such as the Apple configurator.
- Profiles are typically text-based files
  - Usually in an eXtensible Markup Language (XML) format, and are pushed out to the different devices that require them.
- Profiles should be based upon organizational needs.
- Profile may be device-specific or O/S specific.
- Profiles may be specific to different user categories or management groupings.

Profiles

- A group-specific profile applied to these external users may give them particular network configuration and security settings so that they can access a business extranet, for example, or use specific VPN settings.
- May also require access to particular enterprise or business-to-business (B2B) apps hosted on your organization's servers.
- In any case, both device-and user-specific profiles can be very helpful in managing larger groups of users, delivering uniform security and configuration settings to their devices based upon different mission or business requirements.

- Figure 7-2 displays configuration and security settings that can be included in a profile.

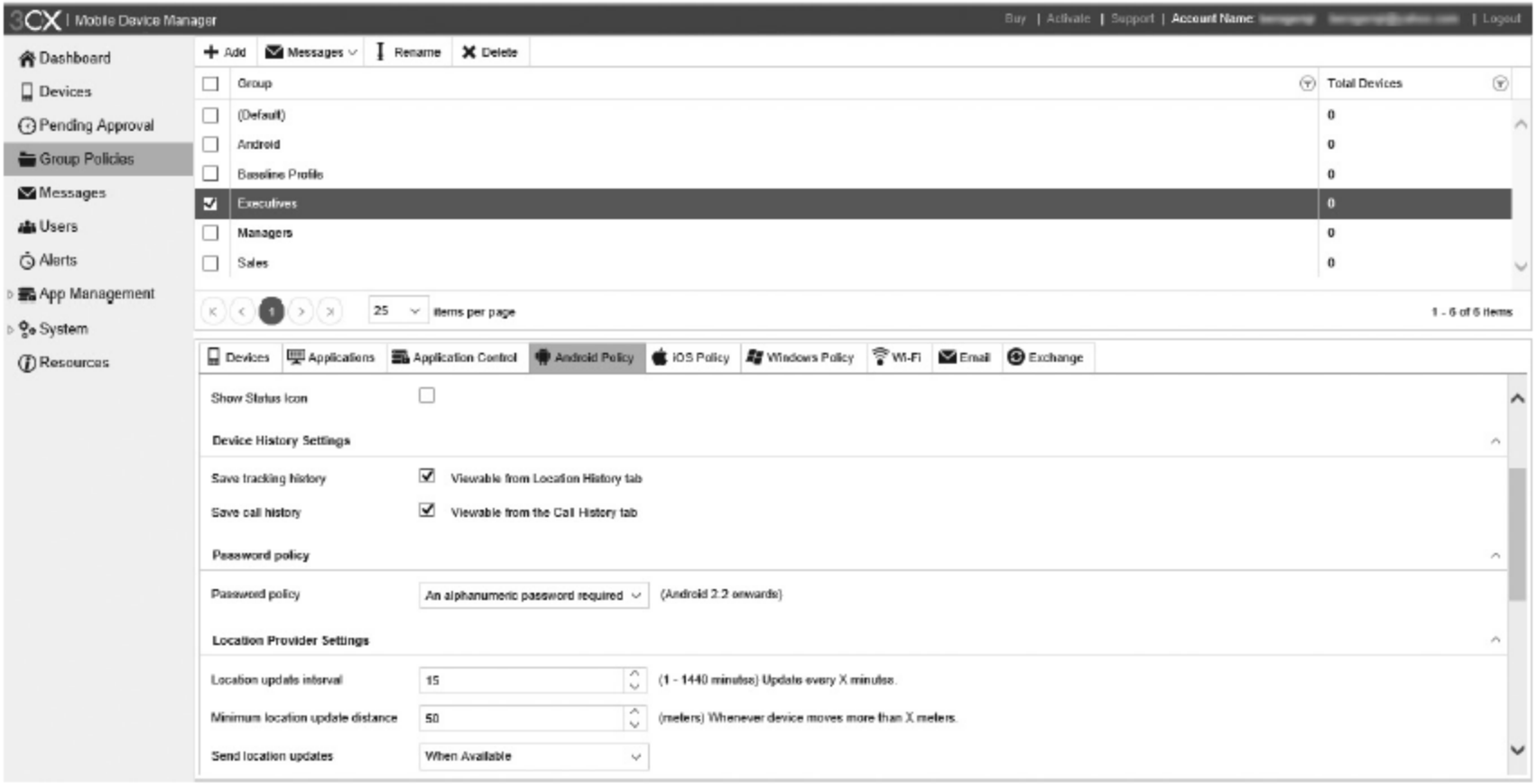


Figure 7-2 Configuration and security settings for a profile

- Depending upon your organizational needs, you could conceivably apply several different profiles to a device at once
  - Based upon platform, user group, and so forth.

Different Profiles

- You may decide to configure settings precedence in the MDM server to resolve conflicts based upon a number of criteria.
  - Including user group membership, or security requirements, for example.
- In addition to vendor or OS platform–specific profiles, you should also develop profiles that may apply to corporate-owned versus personally owned devices.
- A profile applied to a device in a BYOD environment may be considerably different than one applied to an organizationally owned device.
- Figure 7-3 shows how you can conceptually apply different profiles to different device and user groups.

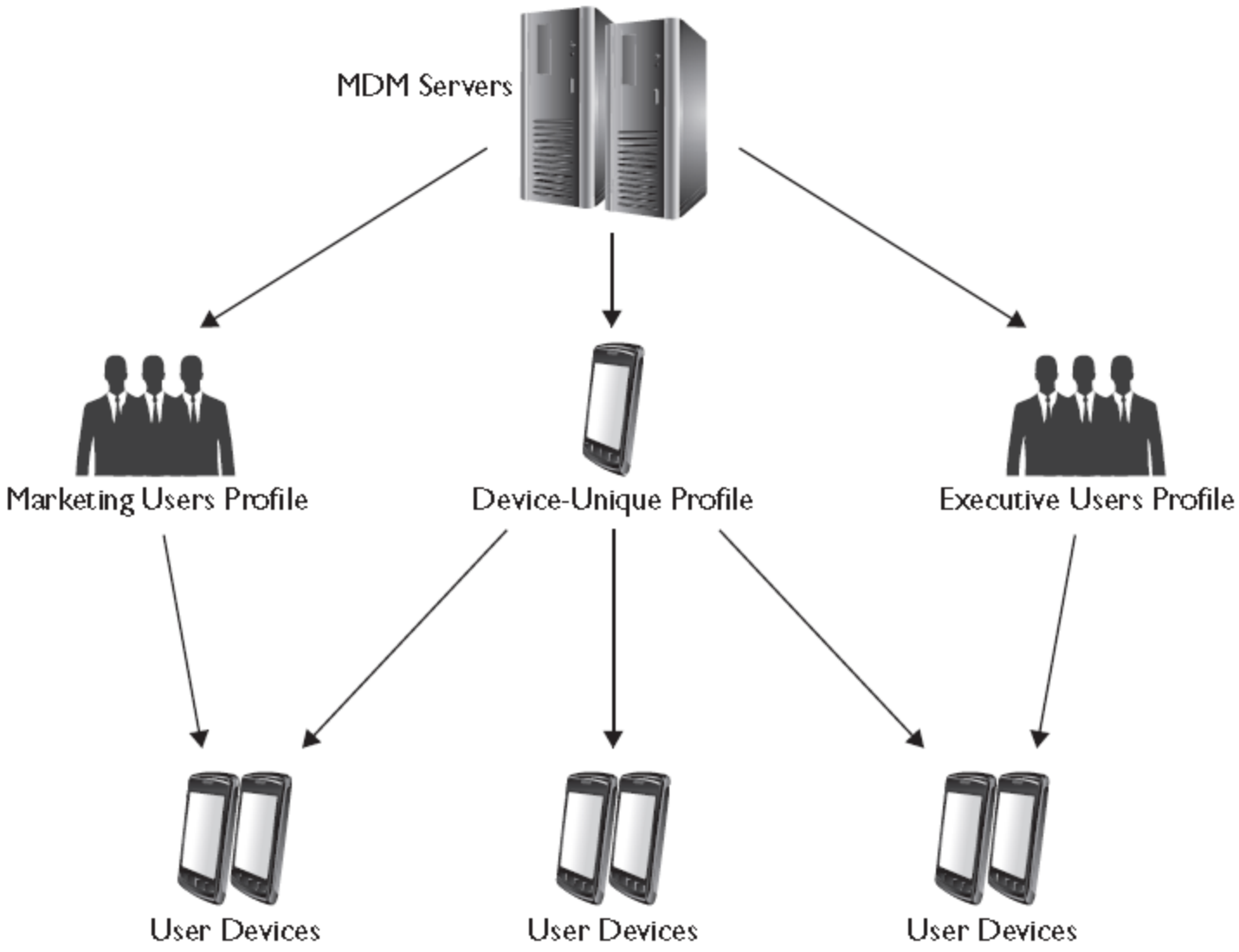


Figure 7-3 Applying profiles to different device and user groups

Conducting a Pilot Test and Evaluation

- In a pilot program, you would implement your MDM solution on a small-scale test basis.
- Examine problems in implementation.
  - Solve them before rolling it out to the general population.
- Participants should be carefully selected and then briefed on what the expectations are of the pilot test.

Pilot

- The pilot test should normally last as long as it takes to get a really good idea of how the actual rollout will go; depending upon the scale of the pilot test, this may take a month or two.
- For example, if it takes you a full week to roll out to a small pilot test group—to include device provisioning and issuance, certificate enrollment, profile configuration, and so on—then you could reasonably estimate the time required to roll out the solution to the general population, based upon the proportional number of users and devices involved.

Lesson's Learned

- Pilot enables you to learn from the experience
  - Implement the MDM solution more efficiently.
- Brief pilot group users to enable feedback, both formally and informally, to administrators and management concerning program.
  - Use feedback to gauge the effectiveness of the rollout.
  - Report any issues or problems test users had during the pilot
  - Offer suggestions for improvement.
- Once you have feedback from all participants, you should summarize the results and present to management.
- There may be some some changes to the process
  - May include some configuration changes to the MDM software or infrastructure.

Documentation

- Should include architecture, procedures, configuration and security settings, individual device information and inventory, and so on.
- Some documentation could also be used to enhance the overall architecture documentation for the enterprise, including the fixed desktop, server, and network device documentation.
- Documentation should be updated as needed, based upon changes in the infrastructure.

Program Launch

- There will always be unanticipated events in any major scale infrastructure implementation.
- When necessary, get approval from management for needed contingencies and adjustments.
- May mean approval for extra money in the budget if something needs to be purchased on-the-fly.
- May mean approval to make configuration changes in the existing network when implementing the solution.

Training

- Everyone in the organization should be trained on policies.
  - Will affect how they use their mobile devices from that point forward.
- May also be technical training required that is specific to device use, especially if users are migrating to a different platform or OS.
- There should also be training for the administrators who will manage the program.
- Training can come in the form of user manuals, handouts, short presentations, intranet sites, or even full scale vendor training classes for administrators whose daily job it will be to manage the MDM infrastructure.

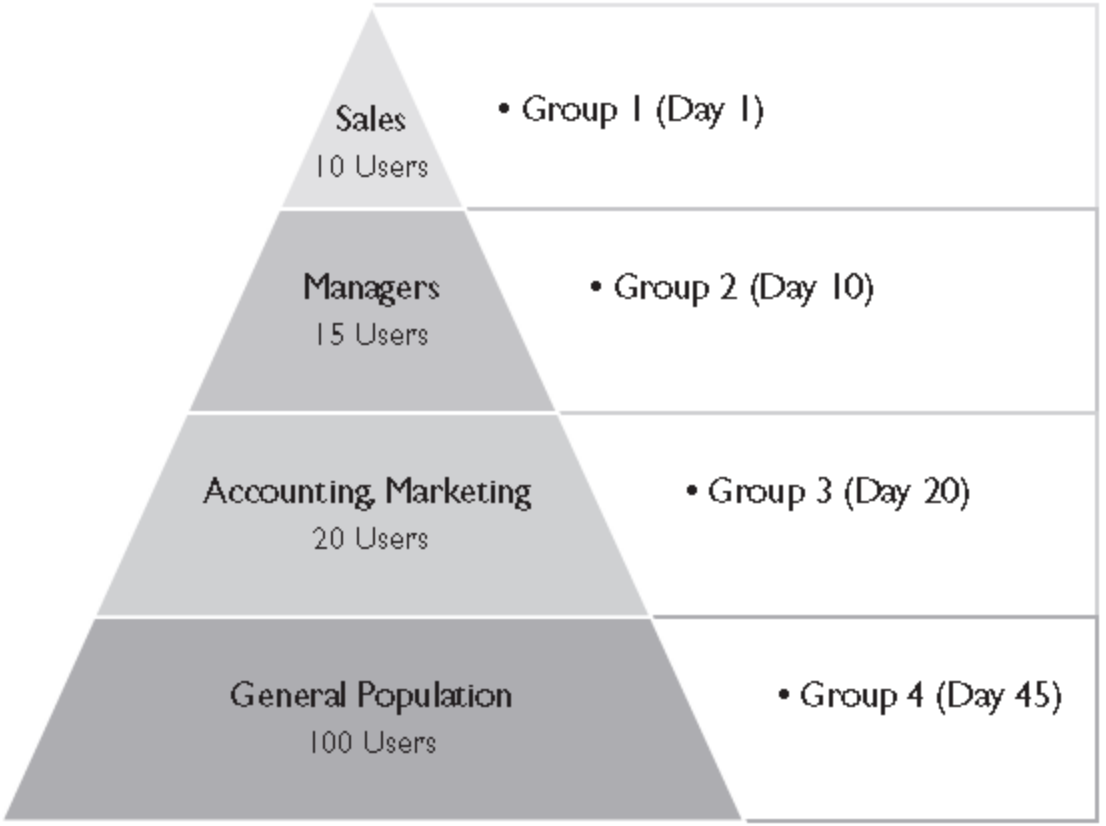
Scaling Numbers of Devices and Users

Two important considerations in deploying your mobile device management solution are the:

1. Numbers of users
2. Numbers and types of devices

- If you're dealing with a small number of users and devices, then deploying to everyone at once may not necessarily be a big deal in your organization.
- If, however, you are in a large organization, it may not be a good idea to deploy to everyone at once.
  - Likely going to be problems that crop up during a large-scale MDM implementation.
- Deploying to everyone at once could cause even smaller problems to become enterprise-wide issues and require a lot of attention from the limited number of technical personnel you may have available for the rollout.

Figure 7-4 A conceptual way to deploy MDM based on scale



- In large populations, prudent to deploy to small groups first.
- Scale rollout incrementally to different smaller groups

Level of Control

- Users who have already been using mobile devices prior to formal deployment, may get a little bit of "sticker shock" when the solution is first deployed and they figure out that they don't have as much control over their device as they previously did.
- May have some issues with people that may require you to scale back the level of control over devices temporarily and increment it slowly.
- This may not only be due to the users' resistance to change, but may also may come from a practical perspective of not having line-of-business applications or business processes ready for a stricter level of control and security requirements.

Infrastructure Considerations

- There also may be other technical reasons, however, for initially loosening control.
  - You may not have the proper infrastructure to manage that level of control over devices.
  - For example, you may choose to not initially impose content filtering on devices if you don't have the right content filtering infrastructure when the rollout occurs.
- Best solution is to have that infrastructure already in place, but this isn't always possible due to resource constraints or even organizational issues.
- In any case, scaling back the level of control when you initially deploy a solution may be something your organization considers for various reasons.

Mobile Device On-Boarding and Off-Boarding

- On-boarding and off-boarding are two of the most common processes that organizations have to go through on a fairly regular basis.
  - Employees and other members of the organization come and go, and when they do, there are a lot of checklist items that must be accomplished.
  - Among these are getting their mobile devices set up or, in the case of those that leave the organization, turned in and deprovisioned.
- Important to establish a defined, documented process for these two activities.

Device Activation

- If a previously used device is being issued to a new user, the device may simply have to be reprogrammed with a new telephone number and reloaded with the baseline operating system and apps.
- If the device is brand-new, it likely requires some sort of over-the-air (OTA) programming on the part of the carrier.
- A simple process and can be performed by the user or by the mobile device administrator.
- Devices can also be activated on a larger scale, with coordination from the carrier as the devices may be preprogrammed and activated prior to shipment to the organization.

Device Activation on Cellular Networks

- The user may need only to dial a number to get the phone activated with the carrier.
- Now, iPhones can be activated simply by dialing a number, which initiates an over-the-air programming process.
- There are other things that iTunes can still be used for during the initial setup for devices not centrally managed, such as synchronization, restoring from a backup, and app and content management, but in an enterprise situation, this should all be done using MDM software and techniques.

Other Mobile Hardware Facilitating OTA Access

- Aside from activation on a cellular network, devices can be activated and provisioned as well using different types of mobile communications hardware that can be used for OTA activation, provisioning, and programming.
- These types of hardware include built-in or removable (SD or USB) wireless cards and cellular cards, for those (rare) devices that don't have those capabilities included.
- Most of the scenarios involving OTA access using connectivity other than cellular technologies usually involve the organization versus the telecommunications carrier.

Provisioning

- Means to initially configure a device according to the corporate mobile device policy and make sure that it has the proper network, app, device, user, and security settings.
  - Entails installing the baseline set of apps the user requires for their job.
  - Can be done by the administrators before the device is even issued to the user.
  - Or it can even be done by the end user when he or she first uses the device.
- During the life of the device that additional provisioning actions take place, in the form of patches, operating system upgrades, installing new apps, and so on.
- Actions usually take place over-the-air, when the device is connected to the corporate network.
  - May happen by allowing the user to connect to the vendor's app store.

On-Boarding and Provision Process

Entails:

1. Assigning a device to a user
2. Activating the device
3. Provisioning the device based on the corporate policies and requirements
4. Making sure that the device functions as it needs to for the user.

- Different ways, include having the mobile device administrators perform this function, or even the users themselves.
- Some of the particular on-boarding and provisioning items that must be accomplished include setting up app stores, both vendor and enterprise controlled, as well as corporate email services.

On-Boarding

- Digital certificates used for authentication to enterprise services will also have to be provisioned.
- Backup services, including apps and policies, should also be deployed.
- Device will have to be entered into the MDM inventory tracking process, as well as any other organizational equipment inventory systems.
- For corporate-owned devices, the user should also have to physically sign for the device and take responsibility for it so that the user can be held accountable for loss or damage to the device.
- User should also be briefed on his or her responsibilities, both in the care and the acceptable use of the device.
- For personally owned devices, corporate policies will dictate what level of provisioning and on-boarding activities take place.

IMEI, ICCID, and IMSI Numbers: Three Identifiers

International Mobile Equipment (IMEI)

- 15-digit number used to uniquely identify a mobile device, typically a smartphone or other device that connects to a cellular network.
- Unique to the GSM family of devices
- Include devices that descended from GSM technologies (including current day 4G LTE and LTE-Advanced).

IMEI

- Typically, this number is printed inside battery compartment
- Some operating systems publish in in the device configuration settings.
- Can be used to identify a specific device and even to block that device from accessing the carrier's network.
- So, if the device is lost or stolen, the user can notify their carrier, and the carrier can make sure that the device can't be used on the network.

Integrated Circuit Card Identifier

- ICCID uniquely identifies a SIM.

International Mobile Subscriber Identity (IMSI) number.

- Also included on the SIM, but represents the actual user associated with the SIM.
- Typically, during the device provisioning process, those identifiers, as well as other information particular to the device, such as telephone number and MAC address, are collected by the server and stored in inventory.

Figure 7-5
IMEI and ICCID numbers

- Figure 7-5 shows how IMEI and ICCID numbers are listed for a newer Android device in the device settings.

Profile Installations

- Profile is a set of configuration settings applicable to a particular device or group of users.
- Can contain security information, such as authentication and encryption settings, network settings relating to connecting to a particular MDM server or to a VPN, for example.
- Provisioning involves sending these profiles to the device.
  - Can be done using a variety of methods.
- Administrators can provision a device with the appropriate profiles, or the user can actually do it himself under certain circumstances.

Profiles

- Typically utilize small configuration files formatted as an XML file.
  - Apple has the iPhone configuration utility.
  - Other vendors have their own configuration utilities as well
- For the sake of consistency across the enterprise and the ability to generate profiles for multiple device and user groups, it's probably more effective to use MDM software to create device and user profiles.
- Figure 7-6 shows an example of an XML configuration file for a device.
- Figure 7-7 shows an example screen from the iPhone configuration utility.

```
<plist version="1.0">
<dict>
      <key>ConsentText</key>
      <dict>
            <key>default</key>
            <string>This profile is mandatory for all MH mobile
devices.</string>
      </dict>
      <key>PayloadContent</key>
      <array>
            <dict>
                  <key>PayloadDescription</key>
                  <string></string>
                  <key>PayloadDisplayName</key>
                  <string>Restrictions</string>
                  <key>PayloadIdentifier</key>
                  <string>
MH_Baseline_Profile.restrictions1</string>
                  <key>PayloadOrganization</key>
                  <string>McGraw Hill</string>
                  <key>PayloadType</key>
                  <string>com.apple.applicationaccess</string>
                  <key>PayloadUUID</key>
```

Figure 7-6 An example of an XML configuration file

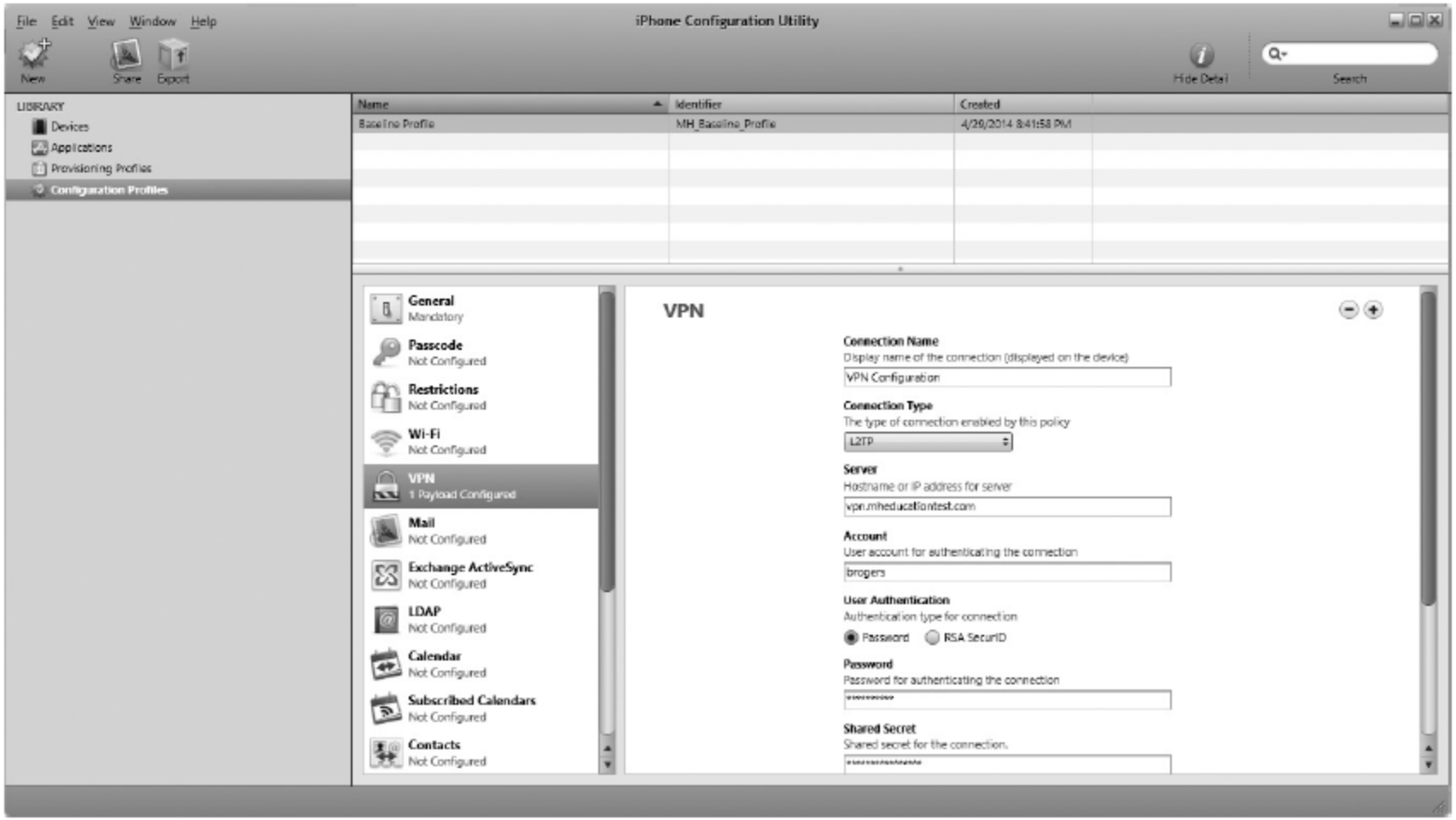


Figure 7-7 The iPhone Configuration Utility

Profiles

- Profiles can be sent to a device several ways.
- Manual on-boarding and provisioning is typically done by the administrator, who may have the device connected to a USB cable and a computer.
- Administrator could also provision a device by manually installing an XML file via an SD card.
  - Which contains all the configuration settings needed to get the initially set up for the MDM infrastructure.
  - Can be a time-consuming if there are a great many users to provision at the same time.
  - May be necessary for the occasional user having difficulty getting the device set up.

Self-Service Provisioning

- Self-service provisioning is a method by which the user assists in the provisioning process by going to a website and clicking on a link provided by the mobile device administrator.
  - Link could be provided via email or SMS text message.
  - Link would then initiate the provisioning process for the user, who may have to answer a few prompts or perform a few actions.
- User could also self-provision using a pre-installed app on the device, which would take the user through the various provisioning steps that the user must provide input for, such as their own username and password or passcode.
- Figure 7-8 shows the URL and temporary passcode as sent via email to the user for a new self-service device enrollment.

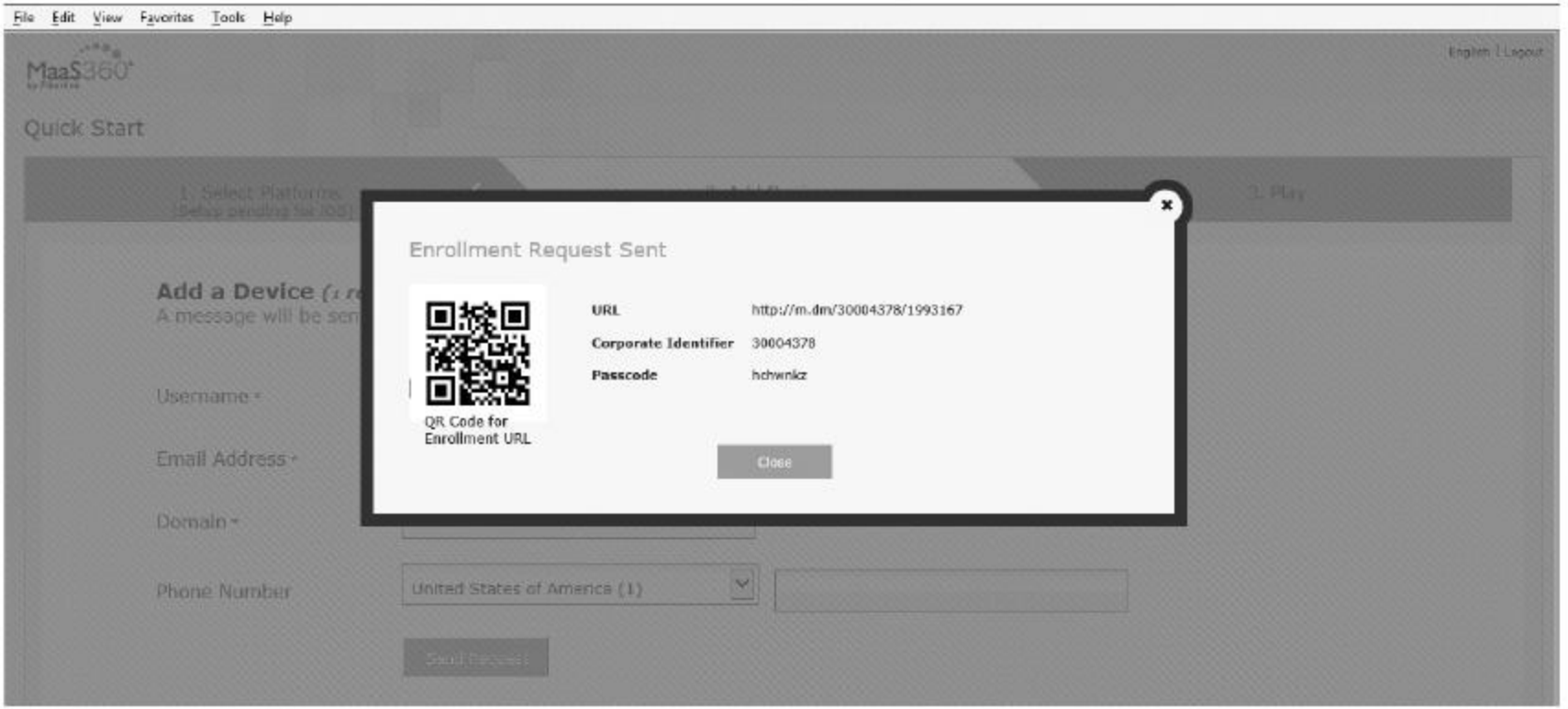


Figure 7-8 URL and temporary passcode sent to a user for device enrollment

Batch Provisioning

- Could be done by sending mass emails to users, which contain URLs and other settings they need in order to connect to a centralized provisioning website.
- Can also be accomplished by running scripts on the MDM server that contain the device IMEI or ICCID numbers for the applicable devices.
- Another way might be to send bulk SMS messages out to the users.
- Typically, batch provisioning might be done for a particular set of devices or users requiring a specific device or group profiles.

Remote Provisioning

- Involves sending provisioning profiles to the remote device using cellular or Wi-Fi.
- XML files provide the data necessary to provision a device, and can be sent in small bursts as individual files or as one large file.
  - XML file doesn't require a great deal of time or bandwidth to push to a smart device.
- Remote provisioning may sometimes require that the administrator temporarily assume control over the device.
- May be more useful after initial provisioning has been accomplished, to provision updates or changes to the configuration settings or profiles.

Secure Device Enrollment with SCEP

- One way to enroll devices is through a secure portal or other method that uses the Simple Certificate Enrollment Protocol (SCEP).
  - Protocol designed to deliver secure, encrypted settings to devices (both mobile and traditional) so they can securely communicate with the infrastructure.
- Both Apple and Microsoft make use of SCEP, albeit differently.
- SCEP is used to push a secure profile to a device that contains authentication credentials for the infrastructure.
- SCEP contains certificate information from the server so that the device and the server can negotiate secure communications.

SCEP Standard

- SCEP is still only a draft standard, published by the Internet Engineering Task Force, or IETF.
  - Not fully developed or implemented in many infrastructures or with all vendors.
- Using SCEP is not the only way to securely register a device; other protocols can be used as well, including SSL.
- Figure 7-9 shows an example of the SCEP configuration screen in the Apple iPhone configuration utility.

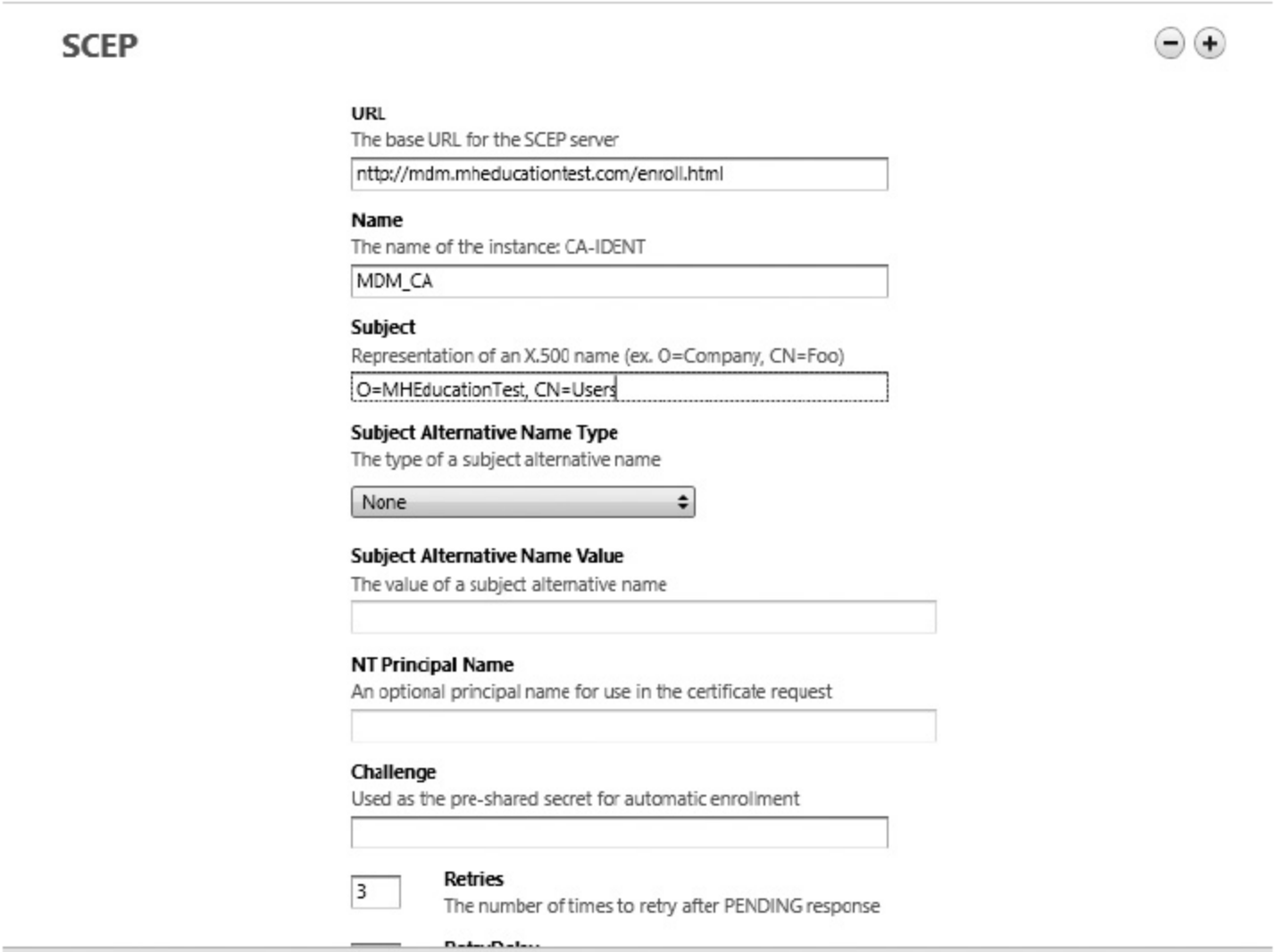


Figure 7-9 SCEP configuration screen in the Apple iPhone configuration utility

Off-Boarding and De-Provisioning

- Off- boarding and de-provisioning a mobile device with an employee who is leaving the organization is important.

Some needed processes:

- Get the device from employee
- Transfer contents
- Sanitize device
- Either dispose of it or return it into active inventory.

Employee Terminations

- When an employee leaves the organization, there is usually an orderly process for terminating network access and retrieving any organizationally owned equipment….
- One step is for the mobile device administrator to take possession of device, checking to make sure it has not been damaged and is still operational, transferring any organizational data from it, and wiping the device so it can be disposed of or reloaded.
  - If there's any personal data on the device, arrangements should be made to get the data from the device and return it to user.
- Once the organization has the device, the device should be reloaded back to its approved baseline and reissued to another member of the workforce.
- If the device is a smartphone, it may be a good idea to have the device phone number changed to a new one.

Migrations

- Employees may need to turn in to upgrade device.
- Data should be migrated to replacement.
- Typically means backing up the data separately from the operating system and apps on the old device so that it can be restored to the new device.
- Additionally, settings such as contacts, files, media, URLs, and other information should be migrated to the new device, via a data backup, or using vendor tools created just for that purpose.
- MDM software may also have the functionality needed to migrate user data from an old to a new device.

Application Considerations

- Uninstalling an app on a device that is to be de-provisioned may free up available licenses in an environment where there are limited volume licenses available for users.
- For some applications, particularly multi-instance software, the administrator may need to go in to that software and remove the device from the list of allowed devices.
- If licenses are tightly controlled, app may need to be uninstalled first from the old device before it can be reinstalled on a new device.
- Additionally, this may be a good opportunity to upgrade apps if there are any new versions available that the organization would like to include in its mobile device baseline.

Content

- Any data or content on the device should be examined to determine if it is corporate property or personal data.
- Organizational data should be backed up to a centralized location.
- With Personal data, user should be given the opportunity to retrieve it.
- In some cases, the organization may find content on the device of a prohibited nature.
  - In this event, the organization would need to determine whether it needs to retain the data as part of an investigation or simply delete the data from the device.

Deactivation

- Finally, if the device is not going to be reused, it should be deactivated and disposed.
  - Process may depend upon device or telecommunications vendor.
  - In some cases, the device may be returned to the vendor.
- Deactivation may require organization remove the SIM, if applicable, and return or destroy it, as well as contact the carrier to inform them that device is being deactivated and should not be allowed to connect to the carrier's network.
- As telephone numbers can be ported from device to device, this is another consideration when deactivating a mobile device because the number should be ported before device is deactivated.

Implementing Mobile Device Operations: Management Considerations

- Considers both the near- and long-term aspects of managing the infrastructure's life cycle, such as:
  - Managing certificates
  - Upgrading equipment
  - Implementing changes in the infrastructure
  - Even managing the retirement and disposal of devices and equipment.

Centralized Content and Application Management and Distribution

- Employees may remove data from corporate infrastructure and store it on devices or in the cloud via personal services.
  - For the most part, removing this data from its corporate boundaries is usually done to facilitate a legitimate business need.
  - Usually, when users resort to these unapproved means of content transfer and distribution to get their jobs done, it means that the organization hasn't done its job in developing approved methods of content distribution and use.
- Unfortunately, these unofficial methods used by employees put the organization at risk because of the possibilities of data loss, unauthorized access, malicious or unapproved content, and so on.

Apps

- Likewise, employees may also obtain apps and other content from sources other than those officially approved by the organization.
- Raises issues concerning an organization's ability to properly control both inbound (apps and approved content) and outbound (company sensitive data) content from mobile devices.
  - The solution is an enterprise solution for content management and distribution.
- Of course, apps can be distributed through a centralized MDM and MAM solution, through the initial provisioning of the device, by using device profiles, and by providing either on-demand or forced installation, usually through an enterprise app store.
  - Other content, however, may need to be considered, and the organization may need to implement a centralized content management and distribution solution to meet those requirements.

Solutions

- As with all enterprise solutions, content management and distribution systems should be integrated with the existing infrastructure, leveraging existing methods and technologies.
- Mechanisms—such as Active Directory's centralized authentication and resource access control, as well as content filtering, device and user profiles, and other centralized services—can be used together to help make content management work.

Distribution Methods

- On-premise models usually involve servers that contain content in shared folder locations, and can be, at the simplest level, accessed through share mapping.
  - Content can be files such as documents, spreadsheets, databases, slide presentations, media, and even executable files.
- More sophisticated models include Microsoft's SharePoint, which serves as both a content repository and access interface, providing location, indexing, and searching methods and structures.
- On-premise server- based solutions can also use custom-built web applications to manage and distribute content to its users.
- Cloud-based services are also viable distribution models for enterprise content.

Content Updates and Changes

- In addition to managing aspects of content that include storage, security, and delivery to the user, content management also includes controlling content.
- Covers content change and updates, as well as versioning control between those changes.
- Ensures that not only are files kept up-to-date and records of changes maintained but that file inconsistency and concurrent use issues are prevented and resolved when they occur.
- Could be implemented using permissions, file locks, or other mechanisms.

Application Management

- May also be controlled by the enterprise app store in conjunction with or as part of the content management system.
  - In the case of vendor or third-party apps, content management and distribution solutions could centrally manage which users and devices get which apps, of course
  - Could also be useful in maintaining multiple versions of apps if these are required for supporting business processes.
- The solution could also be used to maintain changes and updates for vendor apps and ensure that devices get the most current version.
- Could also assist in managing licensing requirements because there may be limitations on the number of concurrent or total licenses in use that the organization may have through their agreements with the vendors that provide those apps.

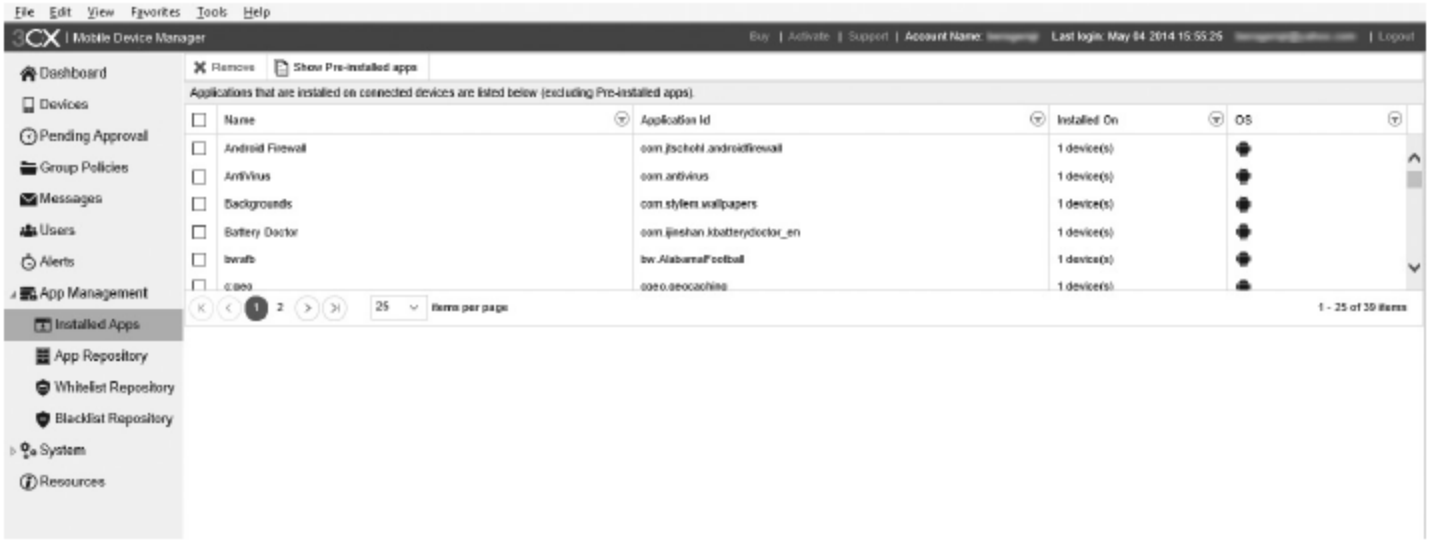


Figure 7-10 Listing and managing apps on an enrolled device

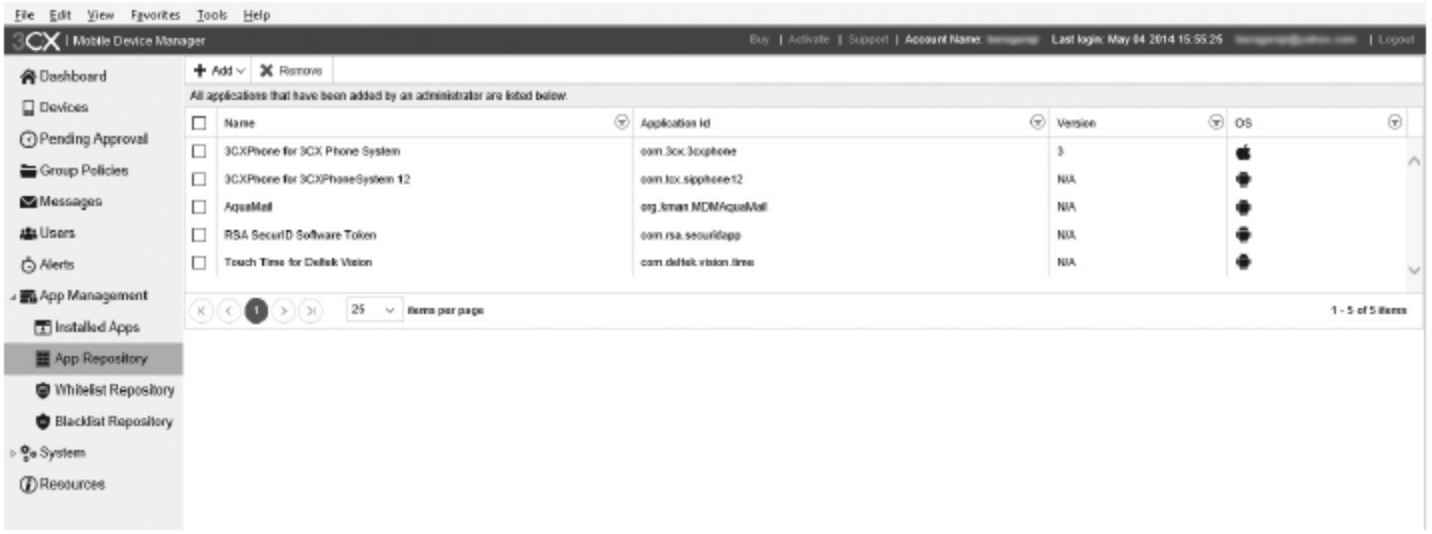


Figure 7-11 An example of an app store repository for an organization with required apps

Figure 7-10 shows an example of listing and managing the applications on an enrolled Android device. Note the options in the left-hand pane that allow different management tasks.

- Figure 7-11 shows how an enterprise app store might be configured in an MDM structure, with required apps in its repository.

Security and Access Control

- Most content management systems integrate with existing security mechanisms, such as LDAP authentication, HTTPS encryption, PKI, and file permissions to secure content.
- Like most other networked resources, content should be secured by those supplemental mechanisms based upon need-to-know and job requirements.
- Other restrictions designed to control access to content may be applied, such as time-of-day restrictions, role-based access control, and granular permissions (editing versus reading, and so on).

Implementing Remote Capabilities

- Mobile device administrators must be able to manage the device using over-the-air methods for a wide variety of tasks, including security, configuration, updating, and other day- to-day administrative reasons.
- Over-the-air management is one of the primary means that administrators use to configure and secure devices.
- Impractical to have the user bring his device in on a recurring basis to connect it to a USB cable and a computer.

Lock/Unlock

- Remotely locking the device will prevent unauthorized personnel from accessing it while it's out of the user's hands.
  - Could also be used in those instances where the user is using the device in a manner inconsistent with organizational security policy.
- Remotely unlocking a device, on the other hand, is something the organization may want to employ if the user has forgotten her passcode or personal identification number, and the device is locked.
- While remotely locking a device is used to protect data confidentiality and prevent unauthorized access, remotely unlocking a device can be used to protect data availability.

Remote Wipe

- Remotely wiping a device is done to prevent unauthorized access to data.
- Typically, the data on the device is so sensitive that unauthorized access or disclosure would be detrimental to the organization.
- This could also be the case if the data is of a personal nature and could result in harm to an individual or identity theft, for example.
- Of course, unless the device has been backed up recently, any data on the device is going to be lost forever once it is wiped.
- Remote wipe can be easily accomplished if the device has been enrolled in the MDM infrastructure and the policy is set up to allow for remote device wipe.

Remote Control

- Several reasons an organization may want remotely control capability.
  - Most obvious reason is to help a user who is having issues.
- Another reason for using remote control features may be to configure the device or change its settings.
- Several different ways that an administrator could remotely control the device.
  - Some of which involve putting an app on the device and enabling settings that allow remote control.

Location Services

- Mobile device administrators can use the same location services to locate a lost or missing device, or track its previous locations to ensure that it has been used in accordance with policy.
- Geo-fencing is another use of location services a mobile administrator may employ in order to track and manage mobile devices that are on the organization's premises.

Figure 7-12 Locating and remotely managing a device

Figure 7-12 shows how MDM can locate and remotely manage a device.

Reporting

- Reporting on a mobile device's status is one way that mobile administrators make use of remote capabilities so that they can keep track of device's:
  - Location
  - Use
  - Security and configuration settings.
- MDM software may have remote monitoring and reporting features, but this is also device- dependent.
  - In some cases, the type of device used may not provide for remote monitoring and reporting, or it may require the installation of an agent, on the device, or even an app that can provide remote monitoring and reporting capabilities.

Life-Cycle Operations

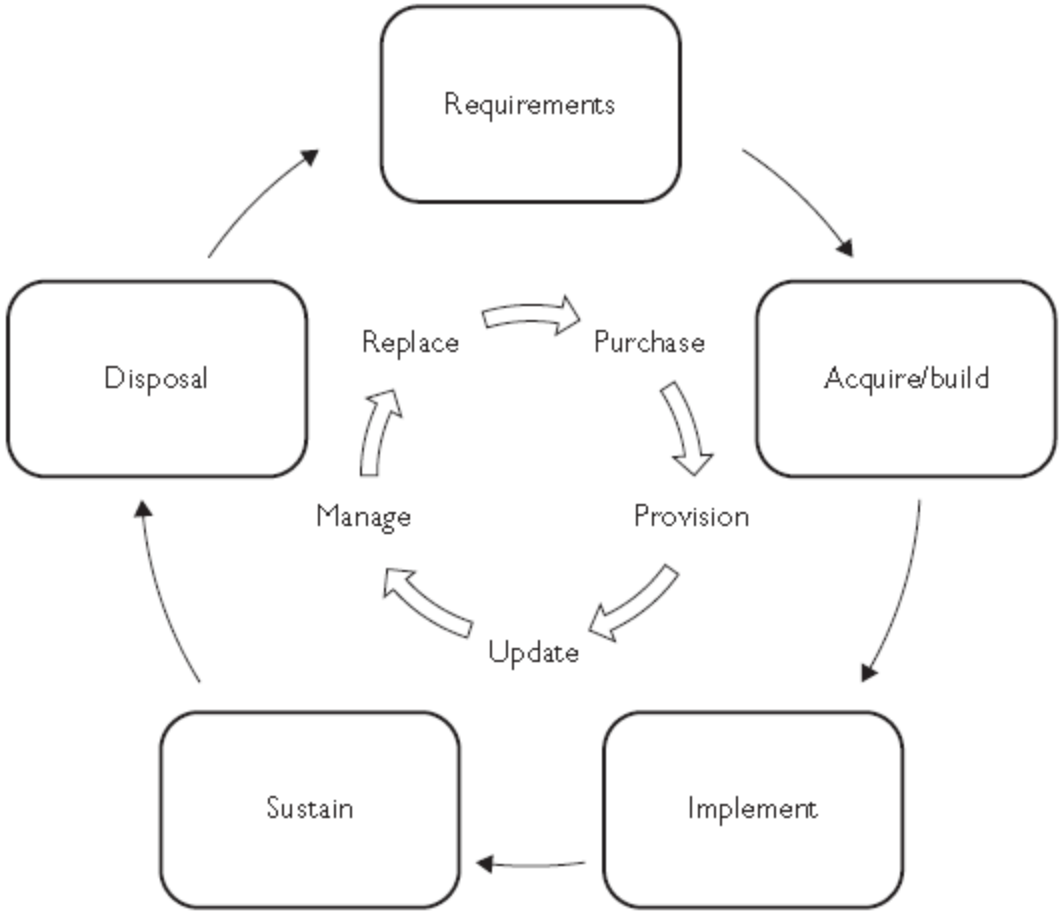
- The life cycle refers to the beginning-to-end process of planning, acquiring, developing, implementing, maintaining, and disposal of both MDM systems and related software.
- Both software and systems development life cycles (SDLC) provide a framework and structure for managing assets.

Software/System Development Life Cycle

- Requires that management maintain visibility on all assets in the enterprise, including purchase date, maintenance history, testing, and other relevant data.
- Organization should develop a process for periodically examining the different aspects of the MDM infrastructure.
  - Devices and other equipment, as well as software and apps, in order to ensure that those assets are still fulfilling their required functions.
- Organization may need to develop a policy that states that it will review devices for upgrade or replacement every three years.

SDLC

Figure 7-13 Conceptual diagram of mobile device life-cycle management



Certificate Expiration/Renewal

- Certificates must be renewed periodically.
  - May be via an internal self-service enrollment web site.
  - Or may be a process whereby device is remotely provisioned.
- Certificates can be sent via profiles to the device as well.
  - May be via a push action from the MDM servers, or even using a pull method from the device itself, when the certificate is within a certain amount of time of expiration.

Updates, Patches, and Upgrades

- Must be managed.
- While the latest upgrade or patch may be a necessity to restore broken functionality or to fix a security issue, the organization must keep track of what updates, patches, and upgrades actually do for them.
- Device and infrastructure stability is an important consideration, and constantly updating, upgrading, and patching devices when there is no justifiable business, functional, or security case doesn't necessarily contribute to the stability of the enterprise.
- All of these should be considered for interoperability with existing equipment and software, as well as the resources required to perform the updates.
- All of these considerations directly relate to the concept of change management.

Change Management

- A formalized organizational process used to ensure that any changes in the device or infrastructure baselines are appropriately considered, approved, and documented.
- Degree to which change management is formally implemented in the organization depends upon several factors.
  - Most important is the level of change and the level of impact it may have on the organization.
- Typically, a change control board (CCB) is formally created and responsible for overseeing the change management process, and usually consists of both technical personnel and managers, who evaluate proposed changes to the infrastructure for impacts on interoperability, availability, and even security.
- The change is normally tested first, in a nonproduction environment, to ascertain what effects the change would have on the existing infrastructure.
- When the change is evaluated, the board is responsible for approving the change and directing its implementation.
- If approved, the change is implemented and documented as part of the infrastructure architecture.
- Like all other aspects of managing the enterprise infrastructure, change management should be implemented according to policy developed and approved by senior management.

End-of-Life

- How organizations manage the end-of-life cycle for platforms is critical to making a smooth transition to new technologies.
- Operating systems will have to be upgraded from older versions to new versions.
  - Often requires moving to newer hardware.
- Likewise, moving to new applications may require also moving to new hardware.
- As you transition to new technologies and platforms, you'll need to plan on how to deal with the older hardware and software you are retiring.
- Obviously, you'll want to securely wipe all legacy devices that you are replacing, to ensure that there are no data remnants on the devices.

Proper Asset Disposal

- Some organizations choose to donate their old mobile devices to charitable organizations or schools, for example.
  - The devices should be taken to an authorized recycle facility that deals in recyclable electronics.
- Some organizations may choose to destroy their old devices to prevent them from being used improperly or accessed by unauthorized persons after disposal.
  - The organization will need to make sure that the disposal method complies with the law and is environmentally sensitive.

Configuring and Deploying Mobile Applications Messaging Standards

- email typically uses standardized protocols, ports, and configuration settings.
  - Each protocol performs a particular function that must be configured appropriately.

MAPI

- Microsoft's Messaging Application Programming Interface (MAPI) more of a programming interface.
  - Allows different clients to connect with email services for a variety of features.
  - Useful for enabling programs that wouldn't otherwise be email-aware to connect to email services.
  - Fully integrated with Microsoft clients, Exchange servers, and Active Directory services, and allows them to use non-email content and services as well.
- Because MAPI isn't a network protocol, it doesn't use any specific network port.
- MAPI communicates over other network services, such as remote procedure calls, to remote servers and clients that also use MAPI.

IMAP

- A networking protocol that handles the receipt and management of email messages.
- Works on the client side
- Supported by most popular email clients.
- Supports multiple connections to any mailbox at once, as well as by multiple clients simultaneously.
- Allows you to receive new messages automatically, almost in real time, without requiring you to reconnect to the server.
- Most current version, IMAP4, uses TCP port 143, but can also be used over a secure connection via SSL or TLS, and then uses TCP port 993.
- Often protocol of choice on mobile devices.

POP

- Also a client-side networking email protocol that provides for receiving and managing email message from the centralized email server.
- Most current version is POP3
- Considered a legacy protocol because the newer IMAP4 is much more feature-rich and enables more granular control over email.
  - For example, POP3 doesn't automatically deliver email messages to the client; it requires periodic reconnection from the client to the server, usually on a timed or polling basis.
  - POP3 also doesn't allow for multiple simultaneous clients or connections to an email account.
- POP3 downloads emails from the server and then deletes them from the server inbox.

Differences

- IMAP4 downloads a copy of the email to the client.
- Leaves original email intact on the server.
  - Can create issues on mobile devices if the user with POP3 configured as the email client protocol expects to be able to access her email later from a different device connecting to the server, and that email is missing or deleted.
- Like IMAP4, POP3 is supported by a wide variety of email clients and servers.
- Almost always a configuration option as well when configuring client email programs.
- POP3 uses TCP port 110, but can also use SSL or TLS over TCP port 995.

SMTP

- Simple Mail Transfer Protocol (SMTP) is the server-side email protocol.
- Uses TCP port 25 (and sometimes TCP port 587).
- Supported on practically every email service.
- Interoperable with almost every email service, including, of course, Microsoft Exchange, Unix's Sendmail, and others.
- SMTP can be secured by sending it over SSL as well (called SMTPS), using TCP port 465.
- Most mobile device email clients can be configured to communicate with SMTP or SMTPS over their standard ports.

Vendor Proxy and Gateway Server Settings

- If you use outsourced services that integrate into your enterprise infrastructure and mobile device management environment, then you should take into consideration some of the network settings you may have to push down to your devices.
- Some of these include proxy and gateway server settings for your devices that they will need to be able to access these third-party services.
- Some of these services could include vendor app stores, cloud-based storage services, or even cloud-based mobile device management services.

Configuration Considerations

- In some cases, your devices may be required to go through your own network infrastructure in order to communicate with these exterior services.
- In many cases, however, because your devices are mobile, it's possible they'll need to access the services regardless of where they are connecting from or over any type of connectivity, be it cellular or Wi-Fi, whether it's from home, the office, or on the road.
- To make this happen efficiently, you may need to configure certain apps or network connections on the device with vendor-specific network settings.

Configurations

- May include default gateway settings, VPN server addresses, proxy server addresses, and so forth.
- It may also include configuring nonstandard port numbers for communications with vendor or cloud services.
- Along with vendor network settings, you may also have to configure encryption and authentication settings on the device in order to access the services securely.
- Examples may include trusted certificates from the vendor in order to establish a secure connection with the vendor's infrastructure.

Considerations

- When integrating the mobile device management infrastructure into existing network, considerations include:
- Placement of network access control (NAC) devices, upgrading existing devices to add more traffic capacity for your mobile devices
- Adding additional equipment that is specific to mobile device implementation efforts, such as wireless LAN controllers, cellular repeaters, and so forth.

Capacity Planning

- Consider altering existing design in order to accommodate the new mobile device infrastructure.
  - Some of the changes to consider include examining include addition of wireless access controllers, security devices, and even entry points into the network, such as VPN concentrators.
- New entry points will need to be secured.
- Another consideration in managing the traffic flow for mobile devices is that it should be routed through specific devices, both to reduce latency and load-balance the traffic capacity throughout the network.

Hosting Solutions

- Different hosting solutions are available.
- Hosting services on the organization's premises is typically the traditional way to deploy services to the enterprise.
- Largely an issue of control, in that the organization has a much larger degree of control over services and infrastructure that are located within its own physical and logical boundaries.
- Most traditional infrastructure models have dictated that both servers and the services they provide physically reside on the organizational network.

Control vs Cost

- Control is certainly an advantage to be gained from this model.
- Disadvantages include both the technical and managerial overhead involved with maintaining the services.
- On-premise hosting requires dedicated staff and resources to make sure that the services are kept running, secured, and available at all times.

Cloud Options

- Recently, however, the traditional model has given way …
- For example, some servers, services, and now even entire infrastructures can be hosted off-premise by a trusted third party that the organization has contracted with.
- This business model is viable because the organization can take advantage of third parties that have built their entire businesses on hosting other organizations' infrastructures, so they can leverage economy of scale with those third-party providers.
- Now it's possible for even a small business to have an enterprise-level infrastructure hosted by a third party.
  - Without having to dedicate their own physical space, facilities, or staff to maintaining those services.
- Some of these cloud-based services include storage, infrastructure, and even mobile device management services.

Cost vs Control

- While cost savings and efficiency are the advantages to third-party hosting, lack of control is sometimes the disadvantage.
- This issue can be resolved by establishing a solid SLA with a third-party provider that includes reassurances of proper security, backups, load balancing, redundancy, and so forth.
- These assurances can contribute to the organization's perception of having greater control over these outsourced assets.
- Understand that the service-level agreement (SLA) is the key to establishing the organization's requirements and control over issues such as security, access controls, protection of data, frequency of backups, and so forth for data stored with a cloud service provider or third-party host.

Types of Mobile Applications

- From the user perspective, every function that can be performed on a mobile device is done through an app, which is basically just a program that runs on the device.
- But mobile apps have a different paradigm in terms of development, management, and security.
- Mobile apps usually have a different development focus, as they are designed with the mobility of the device taken into account.
- Apps are also developed to be more independent so that they don't need to rely as much on services, functions, and even data from other apps.

Native Apps

- Native apps are developed for a specific hardware or device platform, or even for a specific mobile operating system.
- Native apps are usually designed to take advantage of a particular piece of hardware and its lower-level device functions, as well as the API and other software hooks of a particular operating system.

Web Apps

- Web apps are developed from the perspective that a mobile device user will use specific,standardized protocols to access Web-based content in a browser.
- Usually delivered through a user's browser the app experience.
- Independent of the device's OS and hardware.
  - Some web apps may be better suited for one particular platform than another, but the development goal is to deliver a uniform experience to the user, regardless of platform.
- Some web apps may occasionally still have some device-specific code that is rendered or delivered to the device on-the-fly to ensure that the content is properly displayed or accessible based upon the device, but this is usually kept to a minimum.

Hybrid Apps

- In theory, offers the best of both the native and the web app worlds.
- It's an app that resides on the device platform itself, but it is written using web-based technologies that are common across most platforms and operating systems.
- This enables a common user experience, regardless of platform or device.
- Allows for cross-platform support and permits developers to develop one main code base that can be used on different devices.
- May not fully take advantage of a specific operating system's APIs or device hardware features because they are written with web technologies that communicate to the device through an abstraction layer in the operating system.

In-House Application Requirements

- Many apps provided in vendor app stores may work just fine for a business.
  - There are also third-party app developers out there that provide apps for specific business sectors and markets.
- Disadvantages of either vendor app stores or third-party apps include the fact that the organization must pay for these apps, as well as licensing them on a volume basis for its users.
- Depending upon the size of the MDM implementation in the organization, this may not be cost- effective.
- As another example, the organization may have very unique business needs that third-party apps don't address.
- For whatever reason, the organization may decide that it is more cost-effective to create organization-specific in-house apps.

App Publishing 1

- Several factors contribute to the effectiveness of app publishing.
- First, the organization requires personnel with skill sets in several aspects of technology, including networking, security, and not the least of these, programming.
- Depending on the type of app that the organization wants to produce, each may require different programming skills and knowledge of different programming languages.
- For example, producing a native app strictly for the iPhone or iPad requires a certain level of knowledge specific to programming languages used to create apps for these devices, as well as knowledge of the operating systems that run on these devices.

App Publishing 2

- Second, the organization needs to have infrastructure in place to deploy its own in-house development shop.
- In addition to personnel, there's equipment, software, and other materials that are required.
- Finally, the organization also has to have the infrastructure in place to deploy apps to the devices they are programmed for.
  - This is where an MDM infrastructure comes in, as well as a MAM capability, coupled with a content management and distribution solution.

Platforms

- You may have only Apple devices in the infrastructure, so you'd obviously need someone with development skills to support iOS devices.
- If you have Android devices in the infrastructure, then of course you need someone to be able to program in the relevant languages and understand the operating system.
- Same would apply to any other platform you have in the organization, such as BlackBerry or Microsoft.
- If you must provide support for more than one platform, then you probably need to increase the number of people for development.
- Remember that they also should have knowledge and skills in networking, security, and other technologies.
- In addition to being able to support a particular operating system platform, such as iOS or Android, you may also have to look at supporting specific hardware devices.

App Programming

- Not only does the programmer have to be familiar with the operating system and environment she is programming for, but also the hardware device.
- In the case of Apple devices, this may not be a huge issue, but because both Android and Microsoft operating systems can be ported to a variety of devices, developers may need to have some hardware knowledge as well.
- Probably more true on the Android side because each device vendor tends to customize the Android operating system a bit for its particular device.
- Microsoft devices, on the other hand, are likely to be easier to program for because they must meet stricter compatibility requirements to support Windows operating systems.

Vendor Requirements

- With Android developers, Google doesn't impose as strict requirements as Apple.
- Similar to operating system vendor requirements, there may also be requirements that hardware vendors impose on enterprise development shops.
- A hardware vendor, for example, could impose device certification requirements on a developer, requiring the developer to "certify" the app for security or compatibility with the device platform.
- In turn, the hardware developer may also have to provide the developer information on hardware hooks or other critical information the developer may need to build for that platform.
- This may only be the case if the organization intends to market their apps for that particular platform, but may also be required if organization requires lower-level proprietary information from the hardware vendor in order to write the apps for the device.

Certificates

- Digital certificates help identify and authenticate an entity.
- Can be used to verify that an app was developed and published by the owner of the digital certificate.
- App can be digitally signed by the developer, which not only identifies the developer, but also proves to the user that the app comes from a trusted source.
- In terms of enterprise app development, it's usually a good thing for the organization to acquire software signing digital certificates from a trusted source, usually from a third party that specializes in issuing digital identities.
  - VeriSign and Thawte are just two.
- Organization can always issue its own self-signed digital certificate with which to sign software and apps.
  - Doesn't have a solid anchor (or chain of trust, as it is known in the business) to another trusted third party, so its value to anyone outside the organizational boundaries may be questioned.
- If the software or app is going to be used only by employees and users inside the enterprise, a self-signed certificate may be a valid option.
- If, however, the enterprise app store is going to distribute this app outside of the organization, obtaining a digital certificate from a trusted third party is probably a better way to go.

Data Communication

- App developers must account for the mobile nature of devices when programming their apps so their apps should support a common occurrence of leaving one network and joining another dynamically.
- They must include provisions for the app to be able to connect to both wireless and cellular networks, and may need to include methods to connect to Bluetooth or other types of networks as well, depending upon the requirements of the app.
- If a developer hard- codes a specific port to be used by the app when communicating on the network, this may present problems if that port happens to be blocked on the firewall, or otherwise prevented from being used on the network.
- A better scenario may be to provide for a configuration method that the user or administrator could use to configure network settings dynamically, based upon how the network is set up.
- This might be as simple as a configuration screen in the app, or an XML file that an administrator can edit.

Secure Code

- Developers must make efforts to produce secure code by thoroughly testing it and taking into account specific vulnerabilities that may be associated with app programming.
- For example, developers should take into account input validation, as well as bounds checking, to ensure that any user input or action doesn't affect the app or its resources in a negative way.
- Faulty input validation has been known to cause issues such as injection attacks, and lack of bounds checking can result in application buffer overflows.

Security

- Other security requirements include encryption and authentication is another consideration.
- If the service uses password or certificate based authentication, the appropriate authentication mechanisms should be built into the app to support those methods.

Push Notification Technologies

- Push notifications are small messages sent to a device from a central communications server. Notifications require that the device have a constant or always-on network connection, such as a Wi-Fi or cellular connection.
  - Push notifications have been used since the first BlackBerry devices.
- Recent advances in MDM technologies, allow push notifications to perform a wide variety of management functions.
  - Could include notifications concerning updates, policy changes, and even configuration settings.
  - Notifications can also be used to tell an app to schedule an update at a given time or under given circumstances.
- While notifications don't typically carry huge amounts of data, they are able to direct an app to perform a function or make a connection back to the central MDM services.
- Unlike "pull messages," which was an older technique that used and involved apps that simply initiated connections to the server to check for updates, push notifications don't use up as much battery power as the older pull messages did, because they ran constantly in the background.

SMS

- Note that push notifications aren't the only way to send control messages and management commands to devices; the Short Message Service (SMS) can also be used.
- Because SMS doesn't require robust data services, it can be used to send messages to the device in the event that the infrastructure can't easily communicate with the device, which might be the case in the event that Wi-Fi data services, are turned off, or a device has a very weak cellular connection.

Three push notification services:

1. Apple Push Notification Service that is unique to Apple devices,
2. Google Cloud Messaging services that are used by Android,
3. ActiveSync, which is a Microsoft protocol.

Apple Push Notification Service

- Apple Push Notification service (APNs) pushes notifications down to iOS devices.
  - These come from Apple's central notification servers for apps downloaded from iTunes, of course, but also from Apple even for enterprise-level app notifications.
- In earlier versions of iOS, APNs was very limited in what it could do in terms of messaging, managing, and controlling the behavior of apps.
- With the iOS 7 feature improvements, however, APNs allows a much wider variety of messages and the ability to control apps on a much more granular level.
- APNs notifications are 256 bytes in size, and the protocol uses TCP port 2195.
- An additional protocol used by APNs is the APNs Feedback service, which uses TCP port 2196, and is used for failed notification delivery in the event the receiving device doesn't respond to the notifications.

Google Cloud Messaging

- Google Cloud Messaging (GCM) services were previously known as the Cloud-to-Device Message (C2DM) service, but was revamped and re-released as GCM in 2012.
- GCM performs functions similar to APNs, but is able to carry larger messages to its devices.
- Organizations that wish to use GCM must also go through Google's servers to forward messages to their devices.
- GCM messages can be used to send simple notifications to the device, or even send up to 4KB (kilobytes) of data.
- GCM uses TCP ports 5228–5230 for communications between devices and the Android Marketplace.

Exchange ActiveSync

- Exchange ActiveSync (EAS) is a Microsoft protocol widely used across a range of mobile operating system platforms and hardware vendors.
  - Originally developed as a synchronization protocol for Microsoft Exchange corporate users
  - Evolved over time to include more device control and management features.
- While not a full-fledged MDM solution, many organizations use it to perform some device management functions.
- EAS has the ability to set up and configure network connectivity and secure email options for clients that connect to Microsoft Exchange corporate servers, but it also has the ability to control the much wider range of functions.
- Some of these functions include the ability to set password policies, remotely wipe or lock a mobile device, and control some device settings.
- EAS can't, however, impose any management control on other apps or control the nature of secure network connections with most devices, so it's not a full MDM solution, but it could be used as a small part of one.
- EAS uses TCP port 2175 for its network communications.

Questions???