AUTOMATA

Technology Services

Planning Your Implementation

Evaluating MDM Solutions
Preparing Your Network
User Authentication Requirements
Security Strategy

Evaluating MDM Solutions

Lecture

Device Management Needs

- Device Management Goals
- Number and Type of Devices
- Identity Management & Authentication Needs
- Security & Compliance Requirements
- Pricing & Supportability

Device Management Goals

- Meet with all stakeholders & collect requirements.
- Determine your deployment model(s).
- Will you support BYOD?
- What kinds of Apps & Content will you deploy?
- Will you need a self-service portal or catalog for end-users?
- How large is your support team? Will multiple users need access to manage the MDM? Roles?
- If you are an education organization, do you need Classroom tools?

Device Type & Number

- What Apple platforms, OSes, and devices do you need to manage?
- How many devices do you need to support over the near and near-long term?
- How many sites / locations do you have?

Identity Management

- How many end-users does your organization have?
- Do you need to integrate a directory service like Active Directory / Entra ID with the MDM solution?
- Is your user authentication system on-premises only or also available in the cloud? Will you support SSO?
- Will end-users enroll personally owned devices? Do you want them to sign-in to do so via a portal?

Security & Compliance

- Some industries are highly regulated like health, finance or education.
- Is your organization okay with cloud-based solutions or is on-premises required?
- Do you need specific endpoint security?
- Internet and VPN policies?
- Security patches?
- Content filtering or restrictions?

Pricing & Support

- What is the pricing model and have you budgeted to account for growth?
- Is there a free trial or minimum license purchase?
- Is technical support and training included in the cost or is that an additional expense?

Network Requirements

Lecture

Evaluating Network Needs

- How complex is my organization's network infrastructure?
- How many wireless devices move around the campus / location daily?
- Do we support different networks for different users (faculty vs students or employees vs guests) ?
- How will we secure data and support remote users?
- Network security requirements?

MDM Network Configuration

- Is your MDM solution self-hosted / on-prem or is it cloud hosted?
- If self-hosted, consider the following…
  - DNS - must use a FQDN and resolvable both internally and externally.
  - Static IP
  - TLS / SSL certificate for encryption.
  - Firewall allows APN and HTTPS traffic.
  - Robust backup and disaster recovery solution.

Enterprise Networks

Lecture

Enterprise Networks

- Apple products require access to a variety of Internet hosts for many services.
- HTTPS Interception
- See the link in Resources for an exhaustive list of network configuration requirements for enterprise networks.

Wi-Fi Planning

Lecture

Wi-Fi Access

- Apple products support a host of authentication and encryption methods including…
  - Open, Captive, WPA2/3 Personal and WPA2/3 Enterprise
  - PSK, 802.1x and AES
  - RADIUS authentication
  - TTLS and PEAP
- Support wireless roaming via PMKID (Intel) and 802.11k,r,v in Apple Silicon Macs and iOS devices.

Wi-Fi Protocols

- 802.11ax (Wi-Fi 6, 6E)
- 802.11ac (Wi-Fi 5)
- 802.11n (Wi-Fi 4)
- 802.11g, 802.11b (Legacy)

Wireless Density

- Wireless Coverage
  - Placement of wireless access points.
  - Consider roaming. Think 3 dimensionally.
- Wireless Capacity
  - Consider gathering spaces.
  - Usage of devices, plan for growth.

Apple Network Support

Lecture

Built-In Network Services

- VPN Support
  - IKEv2
  - Cisco IPsec
  - L2TP over IPsec
- Content Filtering through MDM restrictions and proxies
- Cisco Support

Apple Push Notifications

- Your network must support APNs
  - Proxies are okay as long as they don't inspect network traffic to APNs.
- Ports and Hosts
  - TCP port 5223 to communicate with APNs
  - TCP port 443 or 2197 to send notifications from MDMs to APNs.
  - Whitelist 17.0.0.0/8 address block.

Bonjour

- Apple's name for the zero-configuration network standard.
- Allows devices to automatically find each other on a network.
- Bonjour-enabled services include…
  - AirPlay
  - AirPrint
  - AirDrop

User Authentication

Lecture

Single Sign On

- SSO process on iPhone, iPad, and Mac
  - Sign in once, a ticket is issued to access resources and doesn't authenticate again while the ticket is valid.
  - Kerberos SSO
  - Extensible to support SAML, OAuth 2.0, etc.
  - Platform SSO for macOS 13 and later.
    - Extends SSO functionality to the login window.

Identity Federation

- Supported via Apple Business / School Manager
  - Microsoft Entra ID (Azure)
  - Google Workspace
- Automatically generate Managed Apple IDs.
- End-Users then use their existing credentials to sign into services like iCloud.

User Authentication

- Binding a Mac to Microsoft Active Directory
  - Configure a Network Server for authentication.
  - Only acceptable in certain scenarios.
- Sign In with Apple
- Microsoft Exchange Server and M365
  - Microsoft Modern Authentication support
  - OAuth 2.0 for Microsoft 365
- Open Standards IMAP, POP, CalDAV, LDAP, CardDAV support.

Device, Data, App Security

Lecture

Device Security

- Balancing security policy and user productivity.
- Organization-owned devices
  - Ideally should be managed & supervised
- End-User owned devices
  - User enrollment in MDM, keeps organization apps and data separate. Can be removed.

MDM Security Features

Lecture

Managed Apps

- Apps installed by MDM are considered ‘Managed Apps’. A license is tracked for each.
- Can be configured as non-removable on iPhone and iPad.
- Excludes the App and it’s data from the user’s backup.
- App and it’s data are removed when it’s no longer managed.
- MDMs can also deploy and secure ‘Custom Apps’.

Managed Data

- Managed “Open In” on iOS/iPadOS
- Managed Notification Previews
- Managed Domains
- Managed Apple ID Security
- iCloud Security

MDM Security Settings

- Restrictions (similar to Screen Time restrictions).
- Passcode Requirements.
- Software Updates.
- Device Attestation.
- Remote Wipe, Remote Lock, Activation Lock.
- FileVault Encryption
- Smart Card (PIV) Integration

MDM Privacy

- MDM can only identify the following:
  - Device name
  - Serial number
  - Model name and number
  - Capacity and space available
  - Operating system version
  - Installed Apps

Digital Certificates

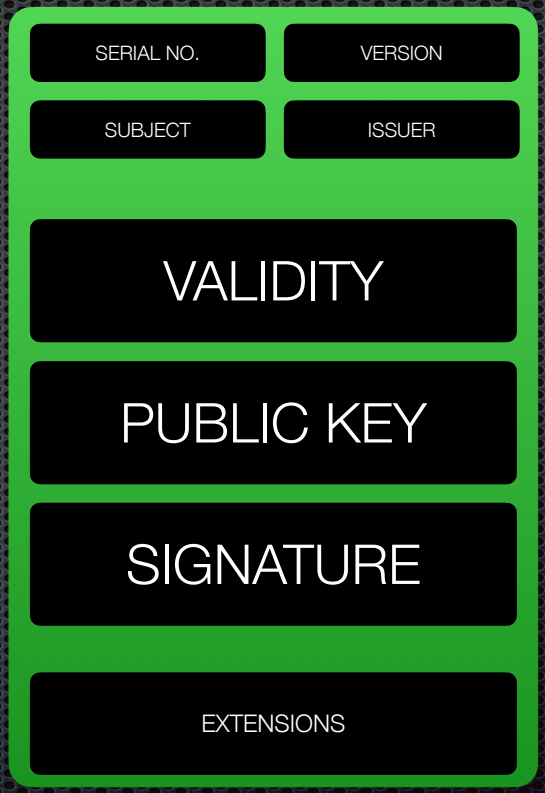
Lecture

Purpose

- Purpose
  - Used to establish trust between two sources for the secure exchange of data.
  - Encrypt network communications.
  - Authenticate users to networks and services without the need for usernames/passwords.

Structure

- Structure
  - Public Key
  - User Information
  - Certificate Authority Information



Anatomy of a Certificate

Certificate & Identity Formats

- A certificate and it's associated private key are known as an identity.
- Certificates can be freely distributed but private keys need to be kept secure. The public key must have a matching private key to decrypt.
- The private key is stored as a PKCS #12 - .p12 file.
- Apple supports .cer, .crt, .der, X.509 with RSA keys for certificate formats. They support .pfx and .p12 as identity formats.

Trusting & Verifying Certs

- A certificate is usually signed (verified) by a Certificate Authority.
- To evaluate a certificate's chain of trust, a device verifies the signature of the certificate and the root authority (anchor).
- Apple devices include a number of pre-installed root certificates called Trust Stores.

Trust Stores

- Categories
  - Trusted certificates
  - Always Ask certificates
  - Blocked certificates
- MDMs provide the ability for organizations to distribute certificates and establish the cert as a root that it trusts.
- MDMs also allow for a payload to automatically not accept untrusted certificates.