Evaluating Mobile Device Management for the University of Cincinnati

By

Matthew D. Rogers

Submitted to the Faculty of the Department of Information Technology in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Information Technology

University of Cincinnati
College of Education, Criminal Justice, and Human Services

April 2013
Evaluating Mobile Device Management for the University of Cincinnati

By

Matthew D. Rogers

Submitted to the Faculty of the Department of Information Technology in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Information Technology

© Copyright 2013 Matthew D. Rogers

The author grants to the Department of Information Technology permission to reproduce and distribute copies of this document in whole or in part.

Matthew Rogers
Matthew Rogers

Russell E McMahon
Professor Russell McMahon

4/19/2013
Date

4/16/2013
Date
Acknowledgements

I would like to take this opportunity to thank those who have given me assistance during this Senior Design project. First and foremost, I would like to thank Professor McMahon and Doctor Kumpf for finding me a new project with such short notice. Without their timely intervention my Senior Design may have been pushed back another year. I would also like to thank Professor McMahon for his continuous advising; he always had his door open any time I needed to talk about my project. Mark Faulkner and Diana Noelcke with UC IT are also to be praised for having this project in mind. Although they had been interested in an MDM solution, I provided the opportunity they had been waiting for to start the project. I would also like to thank Chris Edwards at the College of Nursing for being the catalyst to this project. This was an extremely rewarding experience.
Dedication

I would like to dedicate this Senior Design project to my loving wife, Kara Rogers. She has stuck with me through thick and thin as I worked towards completing my Bachelor’s Degree. As I bring a close to almost seven years of college, I am indebted to her for her patience, caring, and support. Without her, I never would have accomplished my goal.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgements</td>
<td>I</td>
</tr>
<tr>
<td>Dedication</td>
<td>II</td>
</tr>
<tr>
<td>Table of Contents</td>
<td>III</td>
</tr>
<tr>
<td>List of Illustrations</td>
<td>V</td>
</tr>
<tr>
<td>Abstract</td>
<td>VI</td>
</tr>
<tr>
<td>1. Statement of the Problem</td>
<td>1</td>
</tr>
<tr>
<td>2. Description of the Solution</td>
<td>1</td>
</tr>
<tr>
<td>3. Discussion</td>
<td>1</td>
</tr>
<tr>
<td>3.1. Requirements</td>
<td>1</td>
</tr>
<tr>
<td>3.2. Vendor Selection</td>
<td>3</td>
</tr>
<tr>
<td>3.3. Methodology</td>
<td>3</td>
</tr>
<tr>
<td>3.4. Hands On Evaluation</td>
<td>4</td>
</tr>
<tr>
<td>3.5. Budget</td>
<td>4</td>
</tr>
<tr>
<td>3.6. User Profile</td>
<td>5</td>
</tr>
<tr>
<td>3.7. Use Case Diagram</td>
<td>6</td>
</tr>
<tr>
<td>3.8. Gantt Chart</td>
<td>7</td>
</tr>
<tr>
<td>3.9. Deliverables</td>
<td>7</td>
</tr>
<tr>
<td>4. Analysis</td>
<td>8</td>
</tr>
<tr>
<td>4.1. Device Management</td>
<td>8</td>
</tr>
<tr>
<td>4.2. Asset Management</td>
<td>9</td>
</tr>
<tr>
<td>4.3. Application Provisioning and Management</td>
<td>10</td>
</tr>
<tr>
<td>4.4. Infrastructure Integration</td>
<td>11</td>
</tr>
<tr>
<td>4.5. Solution Implementation</td>
<td>12</td>
</tr>
<tr>
<td>4.6. Distribution of Management</td>
<td>13</td>
</tr>
<tr>
<td>4.7. Extensibility of API</td>
<td>14</td>
</tr>
<tr>
<td>4.8. Administrator and End User Experience</td>
<td>15</td>
</tr>
<tr>
<td>4.9. Reporting and Compliance</td>
<td>16</td>
</tr>
<tr>
<td>4.10. Cost Analysis</td>
<td>17</td>
</tr>
<tr>
<td>4.11. Additional Benefits</td>
<td>18</td>
</tr>
<tr>
<td>5. Background</td>
<td>19</td>
</tr>
<tr>
<td>5.1. AirWatch</td>
<td>19</td>
</tr>
<tr>
<td>5.2. Casper Suite</td>
<td>19</td>
</tr>
<tr>
<td>5.3. Meraki</td>
<td>19</td>
</tr>
<tr>
<td>5.4. MobileIron</td>
<td>19</td>
</tr>
<tr>
<td>6. Conclusion</td>
<td>20</td>
</tr>
<tr>
<td>6.1. Recommendation</td>
<td>20</td>
</tr>
</tbody>
</table>
## List of Illustrations

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1. Budget</td>
<td>4</td>
</tr>
<tr>
<td>Figure 2. User Profile</td>
<td>5</td>
</tr>
<tr>
<td>Figure 3. Use Case Diagram</td>
<td>6</td>
</tr>
<tr>
<td>Figure 4. Gantt Chart</td>
<td>7</td>
</tr>
</tbody>
</table>
Abstract

Management of mobile devices such as smartphones and tablets is an extremely important topic in the field of Information Technology. As the University of Cincinnati (UC) looks to the future, the need for a Mobile Device Management (MDM) solution is evident. Some of the most common functions of an MDM are: Device Management, Remote Wipe Capabilities, Private App Publication, and Security Settings. This project focused on the evaluation of several MDM vendors and the recommendation of one vendor for UC to pursue a Proof of Concept. Four vendors were chosen for this evaluation and recommendation. The field was narrowed in a collaborative effort between UC Information Technology and the UC College of Nursing. The four solutions are the Casper Suite, Meraki Systems Manager, Mobile Iron, and AirWatch. The four vendors were evaluated based upon criteria approved by UC IT, the UC IT Managers Committee, and the College of Nursing. The criteria categories include: Device Management, Asset Management, Application Provisioning, Infrastructure Integration, Solution Implementation, Distribution of Management, Extensibility of API, User Experience, Reporting, and Cost Analysis. After careful analysis and hands on evaluation, AirWatch was chosen as the best fit for the needs of the University of Cincinnati.
1. Statement of the Problem

The University of Cincinnati is looking towards the future and realizes that the ability to manage mobile devices, deploy applications to these devices, enforce security, etc. is essential to staying relevant in IT over the next few years. Currently aside from Exchange ActiveSync and an existing low level iOS only policy management solution, no product has been selected by the University of Cincinnati to fill this void.

2. Description of the Solution

The solution that can fix the problem listed above is a full feature mobile device management solution. This solution will enable management of a diverse array of mobile devices and specific functions such as email configurations and Application Stores.

3. Discussion

This section contains the background information regarding the project.

3.1. Requirements

Requirements for what the MDM solution needed to provide were a collaboration between UC IT, the College of Nursing, Apple Education, and industry best practices. The requirements are listed below.

I. Device Management
   a. Configurations
      i. Ability to push wireless configuration
      ii. Ability to push email configuration
      iii. Removal of all Corporate related items upon Enterprise Wipe
   b. Support for multiple phone operating systems
      i. Android
      ii. iOS
      iii. Windows Phone
iv. Blackberry

c. Security Policies
   i. Passcode
   ii. Lock Timeout
   iii. Encryption
   iv. Ability to encrypt transmission of restricted data
   v. Ability to require stored restricted data to be encrypted
   vi. Ability to force security settings
   vii. Ability to restrict downloading or storing of sensitive data (FERPA, HIPAA, etc.)

II. Asset Management
   a. Device location tracking
   b. Enterprise wipe capability
   c. Full wipe capability
   d. Remote lock capability
   e. Distinguish between Corporate and Personal devices
   f. Distinguish between Faculty and Students
   g. Distinguish between groups of devices for policy implementation
   h. Ability to set up location groups
   i. Ability to align location groups with AD user groups
   j. Additional security per application

III. Application Provisioning
   a. Custom App Store
      i. Internally developed applications
      ii. Marketplace applications
   b. Ability to push apps
   c. Ability to push web clips
   d. Ability to track app utilization
   e. Ability to remove applications
   f. Ability to reclaim VPP codes
   g. Does an application wrapping SDK exist

IV. Infrastructure Integration
   a. Integration with AD Users and Groups
   b. What platform can this be installed on
      i. Windows
      ii. Linux
      iii. Virtualized environment

V. Solution Implementation
   a. On Site vs. Cloud vs. Appliance
   b. Combination Implementation
   c. Number of Servers
   d. Ports that need to be opened up through the DMZ
VI. Distribution of Management
   a. Allow for colleges to manage their own devices
   b. Ability to delegate/restrict management of a device group based on login

VII. Extensibility of API
   a. Does an API exist

VIII. Administrator and End User Experience
   a. Self-enrollment option
   b. Web portal for end user
   c. Easy to use
   d. Branding capabilities

IX. Reporting and Compliance
   a. Ability to select reports by Location Group
   b. Ability to report on out of compliance devices
   c. Ability to report when policy violations occur

X. Cost Analysis
   a. System cost
   b. Cost per device
   c. Annual renewal per device

3.2. Vendor Selection

Four MDM vendors were chosen in a collaborative effort between UC IT and the College of Nursing. The first vendor, the Casper Suite, was selected by the College of Nursing. The Casper Suite is an iOS only vendor recommended by Apple. The second vendor, MobileIron, was selected by UC IT. MobileIron is an industry leader according to analysts such as Gartner and Forrester. The third vendor, Meraki, was selected by UC IT. Meraki is a free MDM solution provided by Cisco. The final vendor, AirWatch, was selected jointly by UC IT and the College of Nursing.

3.3. Methodology

The methodology used for the evaluation of vendors had several facets. An in depth analysis of features via white papers, user manuals, FAQs, webinars, walkthroughs, live demonstrations, and
conference calls. An in depth analysis of the experience occurred via the utilization of demo accounts and enrollment of devices into these demo accounts.

### 3.4. Hands On Evaluation

During the evaluation of the four vendors, various types of hands on evaluations were utilized. Demo accounts for AirWatch and MobileIron. A full-fledged Meraki Systems Manager was set up. The University of Cincinnati Blue Ash College has an onsite installation of the Casper Suite that was evaluated.

### 3.5. Budget

<table>
<thead>
<tr>
<th>Item</th>
<th>Retail</th>
<th>Actual Expense</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch Demo</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>Casper Suite Evaluation</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>Meraki Account</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>MobileIron Demo</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>Android Smartphone</td>
<td>$300.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>Apple iPad</td>
<td>$600.00</td>
<td>$0.00</td>
</tr>
</tbody>
</table>

| Total               | $900.00| $0.00          |

**Figure 1. Budget**
### 3.6. User Profile

<table>
<thead>
<tr>
<th><strong>Application:</strong></th>
<th>Mobile Device Management for the University of Cincinnati</th>
</tr>
</thead>
</table>
| **Potential Users:** | Level 4 UC IT Engineering  
Level 3 College Level IT Support  
Level 2 Support Center  
Level 1 Self Service |
| **Software and Interface Experience:** | Experience working with consoles such as WSUS, AD, ITMS, etc. |
| **Experience with Similar Applications:** | Altiris or ITMS console, SEP console, System Center console. Any console that allows management of thousands of endpoints in an Enterprise environment. On the device itself, any management application experience will be useful. |
| **Task Experience:** | Management of Enterprise Devices, reporting, etc. |
| **Frequency of Use:** | Daily for management of mobile devices, enrollment of new devices, monitoring of usage and statistics, etc. |
| **Key Interface Design Requirements that the Profile Suggests:** | Interface design is not editable. This is a console designed by a third party vendor for Enterprise usage. |

Figure 2. User Profile
3.7. Use Case Diagram

Figure 3. Use Case Diagram
3.8. Gantt Chart

![Gantt Chart Image]

3.9. Deliverables

The deliverables for this project were a written recommendation to UC IT concerning which MDM solution should be pursued for a Proof of Concept. This written recommendation would also include a detailed analysis of all four MDM vendors with comparisons of specific criteria.
4. Analysis

This section contains my personal analysis regarding each vendor based upon numerous documents reviewed, experiences, phone calls, interviews, etc. as described in the Methodology section. The documents can be found in my Reference section.

4.1. Device Management

Device management includes what breadth of mobile devices are supported, what types of configurations can be pushed to devices via the system, and whether a native client is required for management. AirWatch was the best vendor in terms of Device Management.

AirWatch: AirWatch supports a broad spectrum of devices such as iOS, Android, Windows Mobile, Windows Phone, Kindle Fire, Symbian, Blackberry, and Windows RT. Email configurations and wireless configurations can be pushed to devices. Depending on the platform, a native client is not required, but one is available for all platforms.

Casper Suite: The Casper suite supports only iOS devices. Email and wireless configurations can be pushed to devices. There is no native client for deployment to the devices.

Meraki: Meraki supports iOS devices and Android devices in an open beta. A native client is not available for iOS, but is required for Android. Wireless configurations can be pushed to devices.

MobileIron: MobileIron supports a diverse selection of devices including iOS, Android, Windows Mobile, Windows Phone, Symbian, and Blackberry. A native client is available depending upon the platform. Wireless and email configurations can be pushed to devices.
4.2. Asset Management

Asset management includes what security policies can be applied to the devices, remote control functionality, and distinguishing between corporate and personal devices. For the device management section, AirWatch is the frontrunner, closely followed by MobileIron.

**AirWatch:** AirWatch offers the full feature set of security policies possible for iOS devices including features only available in supervised mode. For Android devices, AirWatch offers advanced policy enforcement for Samsung SAFE devices and other vendor specific implementations. AirWatch also offers security profiles for all other supported devices. During the enrollment process, it is possible to determine personal versus corporate shared and corporate devices. Also, within the console itself, certain features can be universally turned off based upon device type.

**Casper Suite:** The Casper Suite offers the basic iOS security profile functionality. With the software it is possible to distinguish between corporate and personal devices.

**Meraki:** Meraki offers basic iOS and Android security profile functionality. There is no option for differentiating corporate and personal devices.

**MobileIron:** MobileIron offers iOS and Android security profile functionality, but does not offer vendor specific MDM capabilities. MobileIron also offers security profiles for all other supported devices.
4.3. Application Provisioning and Management

Application provisioning and management includes whether integration with the various App Stores exists, custom app stores, publication of internally developed applications, Volume Purchase Code redemption, and whether an Application Wrapping SDK exists. For the Application Provisioning and Management, AirWatch is the best selection.

**AirWatch:** AirWatch offers the ability to integrate with the iOS App Store, Amazon App Store, Google Play Store. For all platforms it offers the capability to host internally developed applications. Additionally, Apple VPP is possible from within the console and is handled in a very easy to use intuitive manner. An App Wrapping SDK exists which allows for easy manipulation of AD Security, App Usage statistics, Geo-fencing, etc.

**Casper Suite:** The Casper Suite offers the ability to integrate with the iOS App Store and host internally developed applications. Apple VPP is handled within the console in an intuitive manner.

**Meraki:** Meraki offers the ability to integrate with the iOS App Store and Google Play. Additionally, hosting of internally developed applications was recently added as a feature. Apple VPP is handled within the console.

**MobileIron:** MobileIron offers integration with the iOS App Store and Google Play Store. For all platforms supported in addition to those two it also offers the capability to host internally developed applications. Apple VPP is handled within the console.
4.4. Infrastructure Integration

Infrastructure integration includes integrations with Active Directory, User Groups, Exchange, and SharePoint. For the Infrastructure Integration, AirWatch is the best selection.

**AirWatch:** AirWatch offers direct integration with Active Directory users and groups. This can be utilized for device ownership and setting up location groups for devices. Additionally AirWatch can automatically provision exchange email accounts as well as IMAP, and POP3 email accounts. In terms of SharePoint integration, AirWatch offers direct integration of SharePoint with the Secure Content Locker feature.

**Casper Suite:** The Casper Suite offers direct integration with Active Directory users and groups. This can be utilized for device ownership and setting up location groups for devices. Additionally the Casper Suite can automatically provision exchange email accounts.

**Meraki:** Meraki offers partial integration with Active Directory, but not for management purposes. Additionally it does not offer the ability to automatically provision email configurations.

**MobileIron:** MobileIron offers direct integration with Active Directory users and groups. This can be utilized for device ownership and setting up location groups for devices. Additionally MobileIron can automatically provision exchange email accounts as well as IMAP, and POP3 email accounts. MobileIron offers integration with SharePoint as well.
4.5. Solution Implementation

Solution implementation includes whether the solution is onsite or cloud based, what platform it runs on, and the number of servers required. AirWatch was the best solution for this category.

**AirWatch:** AirWatch offers the ability to implement the solution as a hosted, SAAS, or on site full implementation. The on-site implementation only requires one server for up to 100,000 devices. The software is installable on a Windows platform and can be virtualized.

**Casper Suite:** The Casper Suite is available for on-site implementation only. The software can be installed on Windows or Mac OS X and can be virtualized under Windows. Only one server is required for initial implementation.

**Meraki:** The Meraki solution is entirely cloud based and has no option for on-site implementation.

**MobileIron:** MobileIron is offered as a Linux based hardware installation and is also available as a software Virtual Machine. The solution is only available preinstalled on a specific Linux distribution provided by Mobile Iron. One server is standard for initial implementation. MobileIron is available in both on-premise, Connected Cloud and hosted evaluation deployments.
4.6. Distribution of Management

This includes whether or not location groups can be tied directly to Active Directory user groups for management and usage. AirWatch is the best selection for Distribution of Management.

**AirWatch**: AirWatch offers the ability to setup a hierarchy of location groups similar to Active Directory. It also offers the ability to tie Active Directory groups directly to location groups for management.

**Casper Suite**: The Casper Suite does not offer a distributed management capability currently. The company has noted that the next release of the software will allow for location groups to be set up and Active Directory groups to be tied to these location groups for management.

**Meraki**: The Meraki solution does not offer full distributed management capability. It is possible to delineate some users as read access where other users have read write privileges.

**MobileIron**: MobileIron offers the ability to label devices into certain user defined groups for management purposes. It also offers the ability to link Active Directory users for management of those groups.
4.7. Extensibility of API

Extensibility of API includes whether a backend API exists for extending the solution capabilities and how extensive the API is. AirWatch and MobileIron are both equally good selections in this category.

**AirWatch:** AirWatch has a very robust backend API that can be used for customization and extension of the solution. The backend API is extremely extensive and the company offers significant documentation on how to utilize the API.

**Casper Suite:** The Casper suite does not offer a backend API.

**Meraki:** Meraki has no API.

**MobileIron:** MobileIron has a robust API that can be used to extend the capabilities of the system. The API is robust and should meet most any needs of the administrators.
4.8. Experience

Experience includes both the end user experience, self-service options, ease of use, branding capabilities, administrator console, upgrade options, and feel of the solution. AirWatch is the best solution in terms of experience.

**AirWatch:** From an end user experience, AirWatch is very good. A native application is installed on the device, and several additional applications such as a Secure Browser and Secure Content locker can be pushed. The applications are intuitive and visually appealing. The system also offers a self-service portal for users to manage their own devices. Most aspects of the applications and consoles can be branded with a corporate logo. The Administrator console is extremely intuitive, very in depth, and is customizable by the location group. When an upgrade to the system occurs, the Account manager is online with the Administrator during the entire process to ensure everything goes well.

**Casper Suite:** Casper Suite offers a very polished user experience with customized App stores and other applications.

**Meraki:** Meraki offers an end user experience that is reasonable. The applications are very straightforward, but very visually appealing. The administrative experience is fairly easy to navigate but not always intuitive. Also the console itself does not have a very polished feel.

**MobileIron:** MobileIron is on par with AirWatch from an end use experience. A native application and several initial web clips can be installed upon enrollment. The application is visually appealing and intuitive. The administrator console is not as intuitive to navigate and displays information in a manner consistent with network monitoring software. Upgrades to the software are performed via a button in the console.
4.9. Reporting and Compliance

Reporting and compliance includes reporting capabilities, automation capabilities, ability to select reports by location group, integration with existing reporting systems, and automatic compliance engine. AirWatch is the best solution in terms of reporting and compliance.

**AirWatch:** AirWatch offers a fully automated compliance engine that can be utilized at a global level or at specific location groups. By setting up criteria in regards to what is considered non-compliant, the system will not only notify the user and administrator, but can automatically begin deprovisioning the device to ensure security. AirWatch offers automated reporting via email for global and specific location groups.

**Casper Suite:** The Casper Suite does offer a semi-automated reporting and compliance engine that is slightly less customizable than MobileIron’s. Automated reporting is available via the console.

**Meraki:** Meraki offers basic reporting capabilities via email for specified software installation or removal of a device.

**MobileIron:** MobileIron offers a reporting and compliance engine, but it is primarily manual in operation. MobileIron does offer automated reporting via email for global and specific location groups.
4.10. Cost Analysis

Cost Analysis includes the system cost, server costs, server licensing, cost per device, and the cost of management. Meraki is the best solution in terms of cost.

**AirWatch:** AirWatch can be installed on premise in the form of an Appliance or a dedicated server. This server is a standard Windows server with standard licensing costs. The cost per device varies depending upon type of agreement and implementation and is negotiable to a certain extent. The typical cost is $9 per device per year. AirWatch offers an educational pricing scheme where for every one staff member under license, ten users are free. The staff price is a permanent $40.

**Casper Suite:** The Casper Suite is installed on either a Windows Server or a Mac Server. The typical costs of such a server stand. The cost per device per year is approximately $10.

**Meraki:** Meraki is entirely free in terms of devices and servers. The server is hosted externally at no cost and there is no cost for enrolling devices.

**MobileIron:** Meraki is installed onsite in a bundled Linux box. This costs $6000. Per device, the cost is typically $10. For education, all student devices are free, and only staff and faculty devices have an annual cost. The annual cost for devices is typically $40.
4.11. Additional Benefits

Additional benefits includes any additional features, functionality, partnerships, and or other items that do not fit in a preordained section. AirWatch and MobileIron both offer extensive additional benefits.

**AirWatch**: AirWatch has a dedicated Education team. In addition, AirWatch works closely with hardware and software vendors to ensure advanced feature functionality for the MDM. Also, AirWatch provides a great customer experience.

**Casper Suite**: The Casper Suite is constantly improving functionality and features to make itself more enterprise friendly. Also, Casper Suite is the only vendor available for resale directly from Apple.

**Meraki**: Meraki is continuously updating the feature set included with its product. During the few months I evaluated the solution, three or four key features were added. Additionally, due to its acquisition by Cisco, I would anticipate this product becoming even more competitive.

**MobileIron**: MobileIron offers a whole host of additional products that can be purchased to tie in to the MDM suite.
5. **Background**

5.1. **AirWatch**

AirWatch is an American Company based out of Atlanta, Georgia with a worldwide presence. AirWatch focuses on enterprise grade Mobile Device Management. (AirWatch, LLC. 2013) AirWatch is considered to be an MDM leader by Gartner and other analysts.

5.2. **Casper Suite**

JAMF Software is the parent company of the Casper Suite. JAMF Software is located in Minneapolis, Minnesota. The focus of the Casper Suite is management software for the Apple platform including Mac OSX and iOS. (JAMF Software, LLC. 2013)

5.3. **Meraki**

Meraki is a cloud based and cloud managed infrastructure organization based out of San Francisco, California. In November of 2012, Cisco Systems acquired Meraki. Systems Manager by Meraki is an entirely free and cloud based Mobile Device Management solution. (Cisco Systems Inc. 2013)

5.4. **MobileIron**

MobileIron is an American company based out of Mountain View, California with a worldwide presence. MobileIron focuses on simplification of the management of mobile devices. (MobileIron 2013)
6. Conclusion

6.1. Recommendation

The Mobile Device Management solution that best fits the needs of the University of Cincinnati is AirWatch. Overall, it met the largest selection of requirements and had the best user experience. Additionally, the support and feedback received from the company in addition to the dedicated Education team is invaluable.

6.2. Key Decision Making Factors

There were four key decision making factors in this decision: Application Provisioning and Management, Distribution of Management, Breadth of Device Support, and Administrator and End User Experience. UC IT considered Breadth of Device Support in addition to Distribution of Management to be of utmost importance. The College of Nursing considered Application Provisioning and Management to be the most important. Collectively, it was agreed that the Experience, both End User and Administrator, was of critical importance.

Application Provisioning and Management

- Custom App Store for each College
- iOS App Store, Google Play, and Amazon App Store
- Internally developed application capability
- Handles the Apple VPP redemption easily
- App Wrapping SDK for App Usage and AD Security, etc.

Distribution of Management

- Each College will be its own Location Group
- AD Groups can be tied directly to Location Groups
• College Level IT Staff will manage their own locations
• Policy can be inherited from upper level Location Groups

Breadth of Device Support
• iOS including Supervised Mode
• Android including Samsung SAFE, NOX, etc.
• Windows Mobile, Windows Phone 7, Windows Phone 8
• Symbian, Blackberry
• Windows RT
• Mac OS X

Administrator and End User Experience
• Secure Browser
• Customizable App Store based upon Location Group
• Secure Content Locker
• Dashboard View
• Location Group Specific Console
• Intuitive and easy to Use

6.3. Future Recommendations
Due to the constantly evolving and fast paced nature of mobile devices, it is imperative that the selection of software used for Mobile Device Management be revisited on a regular basis. On the same basis that other infrastructure solutions such as Asset Management and Software Delivery are reviewed should be the maximum length of time allowed between revisits. Given the fast past nature of mobility, an informal yearly review is recommended.
6.4. Implementation Recommendations

The implementation of an enterprise grade Mobile Device Management solution should be completed with extreme diligence. A yearlong Proof of Concept for load testing a real world feature testing should be implemented before actual full scale implementation of the solution. Additionally, a test environment and production environment should be set up so that new features, changes, and updates can go through acceptance testing. In terms of work load, it is recommended that a Senior Desktop Mobility Engineer and Junior Desktop Mobility Engineer be created as full time positions within UC IT due to the workload needed for management of an enterprise level Mobile Device Management solution.

6.5. Professional Feedback

UC IT

"Matt did a great job with his project. He was very detailed in his evaluation of the various vendors that offer a MDM product. The key to his success was understanding the requirements that the selected product needed to have and how each one would fit the needs of the university. Matt was very professional in his interaction with both his sponsors. I am very pleased with his recommendation."

- Diana Noelcke, UC IT
College of Nursing

“I have enjoyed working with you. I very much appreciate your hard work on the project and excellent communication. As I have shared previously, the MDM solution is critical for the College of Nursing's sophomore iPad initiative this fall. I think the final product is a clear reflection of your professionalism, attention to detail, and strong technical understanding of the topic. I felt like you carefully listened and reflected the requirements of both the College of Nursing and enterprise in your evaluation, resulting in a recommendation that positions the university to successfully address the challenges that surround mobile management.”

- Christopher Edwards, College of Nursing

Professional Colleague

"Matthew demonstrated attention to detail and professionalism of a very experienced IT professional. He considered all options available to him and worked diligently to prioritize the needs of his customers and mapped those needs to technology solutions. What impressed me most, however, is his ability to communicate his solution to his customers. At the end of his evaluation, he created a professional looking presentation that clearly articulated why he chose AirWatch and explained how easy it would be to maintain by the current campus Active Directory Administrators.”

- Jeff Wilson, Education IT professional with 12 years of IT experience.
7. References


Andrew, Barnes, interview by Matthew Rogers. *Software Applications Developer, Information Technology Department, Blue Ash College, University of Cincinnati* (2013).


Edwards, Christopher, interview by Matthew Rogers. *Assistant Dean for Information Technology and Communications, College of Nursing, University of Cincinnati* (2012-2013).

Faulkner, Mark, interview by Matthew Rogers. *Interim Senior Assistant Vice President Innovations and Partnerships, U.C. Information Technologies, University of Cincinnati* (2012-2013).


Hazem, Said, interview by Matthew Rogers. Associate Professor, Department of Information Technology, College of Education, Criminal Justice, and Human Services, University of Cincinnati (2012-2013).


Hofstetter, Dale, interview by Matthew Rogers. Information Technology Department, Blue Ash College, University of Cincinnati (2013).


Kumpf, Patrick, interview by Matthew Rogers. Associate Professor, Department of Information Technology, College of Education, Criminal Justice, and Human Services, University of Cincinnati (2012-2013).


McMahon, Russell, interview by Matthew Rogers. Associate Professor, Department of Information Technology, College of Education, Criminal Justice, and Human Services, University of Cincinnati (2012-2013).


Renner, Barbara, interview by Matthew Rogers. *Assistant Director Enterprise Communications, University of Cincinnati* (2013).


Stockman, Mark, interview by Matthew Rogers. *Associate Professor, Department of Information Technology, College of Education, Criminal Justice, and Human Services, University of Cincinnati* (2012-2013).


Thompson, Seth, interview by Matthew Rogers. *College of Nursing, University of Cincinnati* (2012).
