IT 5001 Senior Design Management II

CECH Mobility Solution

By

Ryan Moore

Submitted to
The Faculty of the School of Information Technology
In Partial Fulfillment of the Requirements for
The Degree of Bachelor of Science
In Information Technology

University of Cincinnati
School of Information Technology
College of Education, Criminal Justice, and Human Services

April 2014

Learner’s signature: ___________________________ Date: ___04/17/2014_____
Learner’s printed name: ______Ryan Moore_____.

Advisor’s signature: ___________________________ Date: ___04/17/2014_____
Advisor’s printed name: ______Professor Mark Stockman_____.
Abstract

Consumer technologies including tablets, smartphones, and 4G mobile data are being utilized by workers to increase productivity. However, most current IT departments are not equipped to provide secure, easy access to enterprise resources for the mobile user. Consequently, many users are creating their own mobility solutions that may cause loss of data integrity and potential security risks.

The College of Education, Criminal Justice, and Human Services (CECH) is in need of a mobility solution that offers users easy access to college resources while providing security and management tools. This project implements two new systems that integrate with existing systems. The first of these systems, Novell Filr, gives users “Drop Box like” access to data stored on a secured internal SAN. The second system, Airwatch Mobile Device Management, provides security features including remote wipe, location tracking, asset management and enterprise app deployment to mobile devices.
Acknowledgements

I would like to thank all of those who shared their time and expertise in the process of developing and implementing this project. Special thanks goes to Professor Patrick Kump, Professor Mark Stockman, and the rest of the faculty and staff in the School of Information Technology for all the time and knowledge they have shared over the years.

I would also like to thank the industry experts that took time out of their busy schedules and shared their expertise with me along the way. From Novell, I would like to thank Pat Hynds, Thayne Peterson, and Joe Marton. From Airwatch, I would like to thank Jason Hart.

Finally, I would also like to give my gratitude to my colleagues here at the University of Cincinnati for their help and support. From the UCIT Network Operations center, I would like to thank Chris Keith for his assistance with the Airwatch setup. From the College of Nursing, I would like to thank Seth Thompson for sharing his experiences. Last but not least, I would like to thank Brian Verkamp, Director of IT at the College of Education, Criminal Justice, and Human Services, for all of his support and encouragement through the years.
Table of Contents

ABSTRACT .................................................................................................................................................. I

ACKNOWLEDGEMENTS ............................................................................................................................. II

TABLE OF FIGURES ................................................................................................................................. IV

INTRODUCTION ............................................................................................................................................ 1

PROJECT DESCRIPTION .............................................................................................................................. 3

DESIGN PROTOCOLS ................................................................................................................................. 4

User Profile ................................................................................................................................................... 4

SOFTWARE AND INTERFACE EXPERIENCE .............................................................................................. 4

CECHCloud (File) ........................................................................................................................................... 4

Airwatch MDM ............................................................................................................................................... 5

TASK EXPERIENCE ..................................................................................................................................... 6

CECHCloud ..................................................................................................................................................... 6

Airwatch ....................................................................................................................................................... 6

FREQUENCY OF USE .................................................................................................................................... 7

TECHNICAL DESCRIPTION ......................................................................................................................... 8

OVERVIEW ..................................................................................................................................................... 8

CECHCloud (Novell Filr) .............................................................................................................................. 9

AIRWATCH (MDM) ...................................................................................................................................... 18

DELIVERABLES ............................................................................................................................................. 17

PROJECT PLANNING ..................................................................................................................................... 18

COST ANALYSIS .......................................................................................................................................... 20

TESTING REPORT ......................................................................................................................................... 22

SYSTEM REQUIREMENTS - CECHCloud (Novell Filr) .................................................................................. 22

TEST PLANNING .......................................................................................................................................... 23

TEST RESULTS .............................................................................................................................................. 26

BETA TESTING ............................................................................................................................................. 36

KNOWN ISSUES ........................................................................................................................................... 36

SYSTEM REQUIREMENTS – AIRWATCH ....................................................................................................... 37

TEST PLANNING .......................................................................................................................................... 38

TEST RESULTS .............................................................................................................................................. 41

KNOWN ISSUES ........................................................................................................................................... 47

CONCLUSION & RECOMMENDATIONS ......................................................................................................... 48

REFERENCES ............................................................................................................................................... 50

APPENDIX A-1 – CECHCloud Quick Reference Guide ............................................................................... 52

APPENDIX A-2 – CECHCloud Web Interface User Guide ......................................................................... 54

APPENDIX A-3 – CECHCloud Desktop User Guide ................................................................................... 70

APPENDIX A-4 – CECHCloud iOS User Guide .......................................................................................... 82

APPENDIX A-5 – CECHCloud Android User Guide .................................................................................. 95
Table of Figures

Figure 1: Novell Filr (CECHCloud) Use Case Diagram ................................................................. 5
Figure 2: Airwatch Use Case Diagram ........................................................................................... 6
Figure 3: Overview Network Diagram ........................................................................................... 9
Figure 4: Novell Filr Network Diagram .......................................................................................... 11
Figure 6: Airwatch System Network Diagram ............................................................................... 14
Figure 7: Fall Semester Planning Gantt chart ................................................................................. 20
Figure 8: Spring Semester Planning Gantt chart ............................................................................. 20

Table 1: CECHCloud Server Configuration ...................................................................................... 10
Table 2: Project Costs .................................................................................................................... 21
Table 3: CECHCloud Overall Test Results ..................................................................................... 26
Table 4: CECHCloud Web Interface Test Results .......................................................................... 29
Table 5: CECHCloud Desktop Client (Windows) Test Results ....................................................... 32
Table 6: CECHCloud iOS App Test Results .................................................................................... 33
Table 7: CECHCloud Android App Test Results ............................................................................ 34
Table 8: Airwatch BYOD Test Results .......................................................................................... 41
Table 9: Airwatch Department Owned, Single User Test Results .................................................. 43
Table 10: Airwatch Department Loaner Device Test Results ......................................................... 46
Introduction

In recent years, consumer technologies have begun to change how people work and connect. Devices like smartphones, tablets, and ultra-books combined with affordable broadband internet, 4G high-speed data connections, and a seemingly unending amount of Wi-Fi hotspots allow users to be connected just about anywhere, at any time. These anytime, anywhere workers, also being referred to as the hypermobile workforce, is on the rise. According a Forrester Forrsights Global Workforce survey taken in 2012, that number has more than doubled in 18 months and continues to grow. (Schadler, 2013)

This new idea of a hypermobile workforce is largely being created by the users themselves. An increasing number of people are purchasing mobile devices to connect them to enterprise resources. However, many IT departments are still in the early stages of learning how to manage, secure, and offer enterprise resources to mobile users.

Since there is a lack of support from their IT departments, users are finding their own way to create the mobile experience they desire. Many are starting to use third-party cloud based storage solutions such as Dropbox, Google Drive, or Microsoft’s OneDrive to store and access work related documents and data. (Novell, Inc, 2013) This creates many issues concerning data integrity, availability, and security. Users are also seeking applications for these devices on their own, creating potential compatibility and security issues. Furthermore, users are not properly securing their devices. Tablets and smartphones are very easy to misplace and are a very tempting targets for thieves. Without proper password protection, encryption, and
remote wiping capabilities, data stored or accessed from these devices could easily fall into the wrong hands.

At the College of Education, Criminal Justice, and Human Services (CECH), the Technology Support Services (TSS) department is in the early stages of figuring out the mobile dilemma. Approximately 30% of the faculty and staff in CECH have been provided with an iPad and another 40% have laptops to work with off-campus. (Verkamp, 2013) While there are some options for mobile CECH users to access college resources, such as network storage and licensed software applications, these solutions are cumbersome and not very user friendly. Similar to other mobile users, CECH faculty and staff have started to create their own on-the-go solutions.

Besides giving users easy and secure access, the CECH Technology Support Services department also needed the ability to be able to track, manage, and secure mobile devices that they provide to faculty and students. CECH has 50 iPads and several other devices available on loan, in addition to a further 30 iPads on order for the CECH Library. (Verkamp, 2013) The asset management of mobile devices was almost non-existent. If one of these devices goes missing, there would be no way to locate and/or secure the device.

Because of these many reasons, the CECH Technology Support Services decided to create a “Mobility Solution”. Not only does this solution include mobile device management for BYOD and college-owned devices, it also provides users seamless and ubiquitous mobile access to college resources, such as existing personal and shared storage, licensed apps, and network printing.
Project Description

This project two new systems to provide different mobility functionality. These systems are mutually independent, but together they create a complete mobility solution for users. Each system will utilize existing infrastructure managed by the Technology Support Services department, including the VMware vSphere cluster, Storage Area Network, and LAN.

The first of these systems, nicknamed CECHCloud, is powered by Novell’s Filr technology. Filr creates a front end for users to access data stored on internal OES file servers from several different interfaces and devices over an internet connection. This creates a “Dropbox” like experience for users to access their files easily and securely via a Web based application, Desktop sync client (Windows or MAC OSX), or mobile app (iOS, Android, or Blackberry 10). (Novell, Inc, 2013)

The second portion of this project consisted of configuring the policies, profiles, and procedures for CECH to utilize an existing University level Airwatch Mobile Device Management (MDM) system. Airwatch was integrated with the existing Apple Configurator setup that allows the quick and easy provisioning and updating of devices.

This new integration allows the TSS department to better support, manage, and secure mobile devices used by faculty and staff. Both BYOD (Bring your own device) and University owned devices, such as iPads, iPhones, Android phones and tablets, Blackberry’s, and Windows based devices are managed with separate policies.

One of the main functions for the Airwatch system is asset management of devices. The TSS staff will have the ability automate the process of keeping track of every device. The TSS
staff can implement security features based on the policies defined, including password requirements for devices, encryption, blocking apps, and controlling device features.

Besides offering better security, Airwatch also provides users with a better mobile experience. Bring Your Own Device (BYOD) users will be able to access commonly used, College licensed, and in-house apps through a custom app catalog. BYOD users will also be able to get help with configurations such as University e-mail, VPN, and wireless access.

**Design Protocols**

**User Profile**

Users of the CECH Mobility Solution include faculty and staff members of the college. While a major portion of the users are on mobile devices, not all aspects of the project require a mobile device, rather the prerequisite to be productive from outside of the office. Also, some third party affiliates, such as police departments involved in the Criminal Justice Epics program utilize parts of the project.

**Software and Interface Experience**

**CECHCloud (Filr)**

CECHCloud offers several different interface access options. All users need to be familiar with browsing file systems through GUI based applications such as Windows Explorer or Mac OSX Finder. Desktop users will also need to be familiar with a web browser such as Internet Explorer, Firefox, Chrome, or Safari. Mobile users need to be familiar with the app store of their respective mobile OS.
The Use Case Diagram in Figure 1 shows the different tasks for each user actor. The web interface is the main interface option for all users. All administrative tasks are performed from the web interface as well. External users are limited to web interface access, where internal faculty and staff can perform tasks on all interfaces.

![Use Case Diagram](image)

**Figure 1: Novell Filr (CECHCloud) Use Case Diagram**

**Airwatch MDM**

The Airwatch system requires users to be familiar with their mobile OS platform, but most tasks will be performed automatically without user interaction. There will also be a web based user portal for BYOD users.
The use case diagram shown in Figure 2 shows the assortment of tasks that can be completed by different users through the Airwatch system. These tasks can be completed via a web interface or an agent installed on the mobile device.

![Airwatch Use Case Diagram](image)

**Figure 2: Airwatch Use Case Diagram**

**Task Experience**

**CECHCloud**

End users need to be very comfortable browsing, viewing, and editing files from the web or desktop interfaces. There will be a small learning curve for users who wish to edit files on a
mobile device that depends on users’ experience with mobile apps used for editing. CECHCloud will provide some new functionality for user collaboration with the ability to share files with internal and external users.

TSS support staff need to be familiar with NFS file systems, file permissions, and user management via eDirectory and LDAP. Most administrative tasks will be performed on the existing file system to create directories and add permissions based on group memberships.

Airwatch

End user need to be familiar with the mobile OS of their device and installing apps via the app store of their device.

TSS support staff will need to be familiar with Apple Configurator as well as installing apps and profiles on multiple mobile OS systems.

Frequency of Use

CECHCloud is used on a regular basis by end users who are often out of the office or work from home. End users who do a majority of the work from their office workstation will only use the CECHCloud on special occasions.

Airwatch is used on a regular basis by the TSS support staff for asset management and provisioning the pool of shared devices. Additionally, when a new device is purchased for a faculty or staff member, the TSS support staff will use the system to configure the new device. At this time, BYOD devices will only be enrolled if the user requests access to a college-
purchased app for iOS. Updated TSS policies may require enrollment of additional BYOD devices in the future.

Technical Description

Overview

This solution integrates two new systems - Novell Filr and Airwatch - into existing systems, including Novell OES file servers and eDirectory/OpenLDAP servers. The new systems consist of several virtual machines hosted on an existing VMware vSphere cluster located in the CECH data center. Workstations and Printers on UC’s Local Area Network and behind the UC firewall have access to this system. Web portals and proxy servers are located in the DMZ to provide off-campus devices access to the new systems. Figure 3 shows a network diagram of the complete solution.
CECHCloud (Novell Filr)

The CECHCloud system requires three different servers: an Application server, a Lucene search index server, and a MySQL server. In the interest of scalability and high availability, an additional Lucene search index and application server was added in a clustered format to provide load balancing and failover. An Apache server was configured as a reverse proxy and a round-robin load balancer and placed in the DMZ. This provides additional security by removing the application servers from the DMZ, yet allows them to be accessed outside the firewall. This
also helps balance the load from incoming requests to the two application servers. All of the servers are virtual with the following configurations:

<table>
<thead>
<tr>
<th>Server</th>
<th>DNS Name</th>
<th>IP Address</th>
<th>Independent Disk</th>
<th>Hardware Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FilrProxy</td>
<td>Cechcloud.uc.edu</td>
<td>10.132.5.128</td>
<td>N/A</td>
<td>CPU - 1 Socket, 2 cores; Memory 2GB</td>
<td>Apache Reverse Proxy</td>
</tr>
<tr>
<td>FilrCechCloud1v1.0.1</td>
<td>Cechcloud1.uc.edu</td>
<td>10.132.5.113</td>
<td>[FC-DATASTORE-RAID10]FilrCechCloudFilrCechCloud_1.vmk</td>
<td>CPU - 2 Socket, 2 cores; Memory 12 GB</td>
<td>Filr VA Cluster Node</td>
</tr>
<tr>
<td>FilrCechCloud2v1.0.1</td>
<td>Cechcloud2.uc.edu</td>
<td>10.132.5.112</td>
<td>[FC-DATASTORE-RAID10]FilrCechCloud2FilrCechCloud2_1.vmdk</td>
<td>CPU - 2 Socket, 2 cores; Memory 12 GB</td>
<td>Filr VA Cluster Node</td>
</tr>
<tr>
<td>FilrSearch1v1.0.1</td>
<td>Filrsearch.cech.uc.edu</td>
<td>10.132.5.118</td>
<td>[FC-DATASTORE-RAID10]FilrsearchFilrsearch_1.vmdk</td>
<td>CPU - 2 Socket, 2 cores; Memory 8GB</td>
<td>Lucene Search VA Node</td>
</tr>
<tr>
<td>FilrSearch2v1.0.1</td>
<td>Filrsearch2.cech.uc.edu</td>
<td>10.132.5.120</td>
<td>[FC-DATASTORE-RAID10]FilrSearch2v1.0.1FilrSearch2v1.0.1.vmdk</td>
<td>CPU - 2 Socket, 2 cores; Memory 8GB</td>
<td>Lucene Search VA Node</td>
</tr>
<tr>
<td>FilrSQLv1.0.1</td>
<td>FilrSQL.cech.uc.edu</td>
<td>10.132.5.121</td>
<td>[FC-DATASTORE-RAID10]FilrMySQLFilrMySQL_1.vmdk</td>
<td>CPU - 2 Socket, 2 cores; Memory 8GB</td>
<td>MySQL Server</td>
</tr>
</tbody>
</table>

The Filr application, search, and MySQL servers are distributed as preconfigured virtual appliances by Novell. This allows Novell to simplify the deployment, management, and maintenance for the servers. Each appliance is built on specific and tuned operating systems (SLES 11.2), therefore the administrator does not have to install the OS, packages, or other components since everything is included and ready to configure and run. (Novell, Inc., 2013)

An independent virtual disk was configured that contains specific configuration for the deployment on each server. This process helps with maintenance and upgrades. The appliances do not require support packs or patches. As new enhancements and upgrades are released, the Administrator simply deploys the new virtual appliances and then attaches the independently
configured virtual disks. All configuration settings are then transferred to the new virtual appliances.

Figure 4 above, shows the network diagram of the Filr clustered environment. The Filr system will work with Windows Server, Novell Netware, or Novell OES file servers. In the case for the CECH deployment, Novell OES file servers were used. No changes to the file systems or servers were required. All data remains stored and secured on the file servers behind the firewall. The Filr system indexes file metadata on the Luence Search servers. Active Directory or
eDirectory permits user authentication and honors the file system trustee rights and attributes (CECH uses eDirectory for user authentication). Local and external user identities can be created independent of any LDAP source. For the CECH deployment, we permit users to share with external users who need to register their own accounts once a share has been created.

When a user first logs into the system, their home directory is indexed based on the home directory attribute of the users eDirectory account. This is displayed to the user as “My Files” (Personal Storage). Based on eDirectory group membership access rights, the user is also provided access to “Net Folders” (Shared Storage) directories on CECH’s shared network storage.

A user can then browse their files from the web interface or through the mobile application. Files remain on the OES file server unless the user directly downloads the file to their device. A user may then edit the file and upload it back to Filr. This will replace the original file with the newly edited file. At this time, Filr does not support versioning of files, but this is on the roadmap for future releases. (In the meantime, the OES file servers do allow users to “salvage” older versions of files. This has to be accomplished directly on the file servers from the user’s desktop).

Users may also share files with internal or external users from the web interface and mobile applications. When a user creates a share, they have the ability to give either Viewer, Editor, or Contributor (on folders only) rights. They also can set an expiration date/time on the share. When a file is shared with another user, an e-mail will be sent to that user with a link to the file. The link permits internal users to simply log in to access the file. External users are
required to register an account. (Once the share has expired, an external user’s account is removed).

Filr also has a desktop application that can be installed on laptops and home desktop computers on both Windows and Mac OSX operating systems. This desktop sync client creates a local copy of the user’s files on their desktop computer. Changes to local files will be instantly synced with the copy on the server. Changes made to files on the servers will sync with local copies in 15 minute intervals.

Airwatch (MDM)

The Airwatch system was implemented with a SaaS (Software as a Service) configuration. The University of Cincinnati’s Network Operations Center (NOC) hosts an Airwatch deployment that is available to university departments and colleges to utilize. Currently, the College of Nursing is the only other unit on campus taking advantage of this system. Their use cases are similar to those of CECH, including asset management of iPads and distribution of apps via Apple’s Volume Purchase Program (VPP). (Thompson 2014).

The system hosted by the NOC consists of a single Windows Server 2012 system with the Airwatch application installed. This system has a network connection in the DMZ that permits communications with devices and through the web portal off-campus without the need for a VPN connection. The system ties into a MSSQL database server as well as the University’s Active Directory for user authentication (Keith 2013). The CECH implementation will also integrate an Apple Configurator setup used to provision devices to a basic settings level.
CECH has full administrative control over an Organization Group (OG) within the Airwatch system to add Sub-Organization Groups, devices, profiles, apps, and make other configuration changes to manage devices. The UCIT NOC will manage the hardware, network, and licensing for the system.

Although Airwatch can manage many different types of devices with numerous configuration settings, at this time CECH will only manage Apple iPads. Airwatch will be used as an asset management system for college-purchased devices and to push VPP apps to BYOD.
devices on a per request basis. Some security features such as setting a passkey, encryption, location tracking, and remote lock/wipe capabilities are enforced on college-owned devices.

BYOD devices will not require any profile changes besides being enrolled in the Airwatch system for delivery of apps via VPP. BYOD devices can be disenrolled at any time on their own, but will lose access to the VPP apps purchased by the college. BYOD devices will neither have location tracking turned on nor will administrators have the ability to remotely wipe these devices. The capabilities can be enabled in the future if a need is identified.

There are three use cases that will have their own procedures in place. Detailed instructions for these procedures can be found in Appendix B.

The first of these work flows is for college loaner devices. This a pool of fifty iPads that are lent out to faculty for classroom use or personal use while traveling. These devices will be provisioned with a standard image through the Apple Configurator. They will be automatically enrolled for Multi-User Staging in the Airwatch system with the Airwatch agent preinstalled. A generic Apple ID will be set up on the device in order to enable the users to download apps to the device without having to enter their personal Apple ID.

After the device is provisioned, it is placed into an Organization Group (OG) in Airwatch that installs a profile to lock the device into Single App mode with the Airwatch agent. This locks the device into a login screen within the Airwatch agent. Users will not be able to leave this screen and make any changes to the device until they enter valid user credentials from UC’s active directory.
Once authenticated, the device will be placed into another Organization Group based upon Active Directory group membership. This allows devices to have different profile settings installed based on the user’s role. Also, Apps requested by the user will automatically be installed. For example, if a student logs in, they cannot change the Apple ID or install any apps directly from the Apple App Store. However, if a faculty member signs in, they will have the ability to enter their personal Apple ID and install personal apps.

When the device is returned, the user will log off the device through the Airwatch Agent. The devices will then be automatically moved back to the staging OG. All profiles and apps installed by the user OG will be removed and the device will once again be locked into single app mode and made ready for the next user.

The second workflow is for college-purchased devices that will be dedicated to a single user. These devices will also be provisioned on the Apple Configurator with a base image and automatically enrolled into single user staging with the Airwatch Agent preinstalled. When the faculty or staff member is first given the device, a technician will instruct them to log into the agent. This will move the device into an Organization Group based on the user’s Active Directory group membership. Based on this OG, profiles will be installed for different configuration settings, such as e-mail, wireless network, and VPN. These users will also have access to the CECH app catalog with commonly used public apps and any purchased apps assigned to the user.

The final workflow is for BYOD devices. In this use case, users will enroll via the web portal. There will be no need to install the agent on the device. The user is instructed to choose
‘Employee Owned’ device and will be placed into an Organization Group based on Active Directory group membership. No profiles or settings will be installed on the device outside of the enrollment profile. The user will then have permission to install VPP apps from the CECH app catalog.

**Deliverables**

The deliverables for this project include a fully functional, in-production, Novell Filr system branded as CECHCloud. This system ties into the CECH OES file system. All CECH faculty and staff will have complete access to their files and data stored on their personal storage and assigned shared storage. This system has a web user interface that can be accessed on or off campus without the use of a VPN. There are also Novell Filr Apps available through the Apple App Store, Google Play store, and Blackberry 10 App store. A desktop client can be downloaded and installed on personal computers through the web interface. (The MAC client is still in beta and users are being advised to not use it at this time. It will be out of beta in the next update; that update will not be applied until after this project is complete). Complete user guides for CECHCloud will also be available online on the CECH Technology Support Services web site. These guides can be viewed in Appendix A.

The Airwatch deliverables also include a fully functional system with the previously mentioned capabilities. iPads that demonstrate the different use cases will also be provided. An administrative web portal will be completed and branded. The end user self-service web portal is available, but will not be utilized at this time. The Airwatch agent is available for download through both the Apple App Store and Android Play Store, but will be automatically installed on devices through Apple Configurator. Also, an Apple Configurator setup with preconfigured iPad images to provision multiple devices at a time will be delivered. Finally, user and technician guides have been created for each workflow.
Project Planning

The idea for this project first came about in February of 2013 at Novell’s Brain Share conference in Salt Lake City, Utah. At the conference, my colleagues and I was introduced to an early beta version of the Novell Filr system. We were given access to a Filr system that gave us access to all of the conference documents and presentations. The system seemed a good replacement for our aging remote file access system called DocXchanger (Coundrey Corporation). This aging system ran on an End-of-Life Novell Netware system and a replacement was in need as the system was no longer stable and did not offer the features we needed in a remote file access system. Many of our users requested a better solution and there were talks of a University wide Box.net or DropBox system, but nothing could be agreed upon.

The Novell Filr system was included in the CECH Academic License Agreement with Novell and could be run on the existing virtual environment. With this information and the previous exposure to the system, it was decided by the IT Director, Brian Verkamp, to implement this solution. The second release of Filr (version 1.01) was released in late August 2013 and I was given the project.

The idea for setting up a Mobile Device Management system was considered, due to the constant increase in mobile devices in use. At the time, CECH lacked the ability to track usage of iPads or deliver licensed apps to the devices. The idea of adding an MDM solution to the project was presented to the IT director. He agreed that Filr may increase the demand for mobile devices and we were in need of a solution, as long as there was a cost-benefit.

In September 2013, I started with a Proof-of-Concept for Filr and began to research different MDM solutions. I looked into many different MDM solutions including Symantec, Airwatch, Mobile Iron, Citirx XenMobile, and Novell Zenworks Mobile Device Management. Many of these systems offered very similar features, mainly because they were limited by what Apple would allow them to do. I narrowed the field down to two different systems to setup Proof-of-Concepts for Airwatch and Novell Zenworks.
I picked Novell Zenworks MDM due to our relationship with Novell and the many different products we use from them. They offered very competitive pricing with our ALA agreement and promised integration with the Zenworks Configuration Management system we currently use for desktop management.

Airwatch was in consideration due to the industry acclaim it has received and the fact that the University was hosting a deployment of it. If the University decided down the road to implement a mobile device policy, we would be one step ahead in order to be in compliance.

While both of these systems POC test proved to provide the desired functions, Airwatch was finally picked as the final solution. Novell’s Zenworks MDM turns out it was a rebranded third party application rather than a home grown solution. My experience with these types of products offered from Novell has not been ideal. It is often hard to get good support or promised features. One of these promised features was integration with Zenworks Configuration Management. At this point in time this feature includes a link to the MDM system from ZCC and nothing else. They continue to promise database and reporting integration, but those features have been delayed for some time.

Airwatch costs would be less as there would be no hardware or virtual computing power needed by CECH to implement. Most of the management of the system would be provided by UCIT as well. Finally, the per-device cost per year was also less.

The project was broken down into two parts. The first semester was focused on implementing and testing Novell’s Filr with research into the MDM on the side. The second semester focused on the MDM system with minimal tweaking done to the Filr system. The following charts are the planned schedule for various parts of the project.
Cost Analysis

The first phase of the project, Novell Filr, did not have any additional costs. The Filr software is included in the Open Enterprise Server Academic Licenses Agreement (ALA) that CECH currently has with Novell. All servers required for this portion of the project are provided as virtual appliances as part of the package and will be hosted on CECH’s existing vSphere infrastructure.

The Airwatch implementation had minimal costs associated with it as well. Since the application is hosted by UCIT there were no hardware or software costs. The only cost to the
college is a per device cost on an annual license. The standard price per device for Airwatch is $39 annually, but UC currently receives a 50% discount. This discount may be renegotiated as other departments begin to license devices.

This project required the use of equipment for testing purposes. I have included the prices for this equipment as well as personnel costs based on my salary at approximately 20 hours per week spent working on the project. The following table shows a breakdown of all costs for the project.

<table>
<thead>
<tr>
<th>Overall Costs</th>
<th>Cost per unit</th>
<th>Number of units</th>
<th>Total Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airwatch License</td>
<td>$19.50</td>
<td>100</td>
<td>$975.00</td>
</tr>
<tr>
<td>iPad 2</td>
<td>$399.00</td>
<td>2</td>
<td>$798.00</td>
</tr>
<tr>
<td>iPod Touch</td>
<td>$185.00</td>
<td>1</td>
<td>$185.00</td>
</tr>
<tr>
<td>Samsung Galaxy Tab 10.1</td>
<td>$350.00</td>
<td>1</td>
<td>$350.00</td>
</tr>
<tr>
<td>Microsoft Surface RT</td>
<td>$499.00</td>
<td>1</td>
<td>$499.00</td>
</tr>
<tr>
<td>Estimated Personnel Costs</td>
<td>$23/hr.</td>
<td>640</td>
<td>$14,720.00</td>
</tr>
<tr>
<td><strong>Total Project Cost</strong></td>
<td></td>
<td></td>
<td><strong>$17,527.00</strong></td>
</tr>
</tbody>
</table>
Testing Report

System Requirements - CECHcloud (Novel Filr)

Overall
1. User authentication with CLS credentials via LDAP
2. User home directory synced with “My Files”
3. Share folders accessible under “Net Folders” per existing file system rights
4. Sharing of files and folders to both internal and external users
5. Load balancing and fail over via reverse proxy

Web Interface
1. Accessible from on- and off- campus
2. Accessible from multiple web browsers/versions
3. File search and file retrieval within acceptable times
4. Download files to local workstation
5. Upload files from local workstation
6. Replace existing files on server
7. Share files with both internal and external users

Desktop Client (Windows)
1. Install on Windows 7 and Windows 8
2. Create local file directories for Filr
3. Synchronize home folder and selected share folders (15 Min)
4. Max file size to sync 1000MB
5. Connects and syncs on- and off-campus

iOS App
1. Accessible from on- and off-campus
2. Does not remember user password
3. File search and retrieval within acceptable times
4. View files from home directory, share folders, and shared files in respective locations
5. Search for files by name
6. Download files to local workstation
7. Upload files from local workstation
8. Replace existing files on server
9. Share files with both internal and external users

Android App
1. Accessible from on- and off-campus
2. Does not remember user password
3. File search and retrieval within acceptable times
4. View files from home directory, shared, and shared files in respective locations
5. Search for files by name
6. Download files to local workstation
7. Upload files from local workstation
8. Replace existing files on server
9. Share files with both internal and external users

External Users
1. Receive e-mail when being shared a file
2. Click link in e-mail to be directed to CECHCloud site
3. Register an account with Filr
4. Login to Filr with self-created account
5. View shared files under ‘Shared with Me’ view
6. Edit files with editor or contributor rights
7. Unable to access after all shares have expired or removed

Test Planning

Overall
1. Test internal user authentication
   a. Login with LDAP accounts via web interface
   b. Login with LDAP accounts via mobile app
   c. Login with LDAP accounts via desktop client
   d. Change password through PSS, then login to Filr system
2. Home directory should populate under ‘My Files’ Net Folder
   a. Login and verify home folder is accessible to user
3. Share folders and sub folders accessible based on NFS file system rights under “Net Folders”
   a. Login and verify share folders are accessible with appropriate sub folders
4. Internal users should be able to share files and folders with both internal and external users
   a. Share items from “My Files” with internal user
   b. Share items from “Net Folders” with internal user
   c. Share items from “My Files” with external user
   d. Share items from “Net Folders” with external user
   e. Test expiration of shared items
5. Load balancing and fail over protection should be provided by cluster
   a. Login to multiple instances of CECHCloud. Verify alternation between cechcloud1 and cechcloud2 servers.
   b. Shut down cluster nodes and test for issues with access
   c. Shut down search index nodes and test for issues

Web Interface
1. Functions properly in different browsers
   a. Perform all tests in Internet Explorer 11, Chrome 30, Firefox 25, and Safari
2. Should be accessible from both on campus networks and off campus without VPN
   a. Test connection on campus network
   b. Test connection from off campus
3. File search and download should be without log delays
   a. Test search times on “My Files”
   b. Test search times on “Net Folders”
   c. Test download times of multiple file types and sizes
4. Working with files
   a. Test downloaded files to local workstation
   b. Test uploading files from local workstation
   c. Verify the replacement of existing files on server after upload
   d. Test In-Place-Edit of office files
5. Sharing files
   a. Test share files from web browser with internal users
   b. Test share files from web browser with external users
   c. Test created shares appear in “Shared by Me”
   d. Modify shares
      i. Change expiration
      ii. Add/Remove users
      iii. Remove shares

Desktop Client (Windows)
1.Client should work on both Windows 7 and Windows 8
   a. Test install on Windows 7
   b. Test install on Windows 8
2. Client should create and sync “My Files”, “Shared with Me”, and selected “Net Folders” files to a local directory
   a. Verify local directory creation
   b. Verify all files (under 1GB) are synced
3. Files should sync from the desktop client in 15 minute intervals
   a. Test new files sync back with the server
   b. Test edited files sync new version back to server
   c. Test new files created on server sync with local directory
   d. Test new files edited on server sync new version with local directory
4. File sync should work both on and off campus
   a. Test file sync connection on campus network
   b. Test file sync connection off campus

iOS App
1. Should be accessible from both on campus networks and off campus without VPN
   a. Test connection on campus network
   b. Test connection from off campus
2. App should not cache the users password
   a. Verify the app does not remember the users password on logoff
3. File search and download should be without log delays
   a. Test search times on “My Files”
   b. Test search times on “Net Folders”
   c. Test download times of multiple file types and sizes
4. Working with files
   a. Test downloaded files to device
   b. Test uploading files from device
   c. Verify the replacement of existing files on server after upload
5. Sharing files
   a. Test share files from app
   b. Test created shares appear in “Shared by Me”

Android App
1. Should be accessible from both on campus networks and off campus without VPN
   a. Test connection on campus network
   b. Test connection from off campus
2. App should not cache the users password
   a. Verify the app does not remember the users password on logoff
3. File search and download should be without log delays
   a. Test search times on “My Files”
   b. Test search times on “Net Folders”
4. Working with files
   a. Test downloaded files to device
   b. Test uploading files from device
   c. Verify the replacement of existing files on server after upload
5. Sharing files
   a. Test share files from app.
   b. Test created shares appear in “Shared by Me”
# Test Results

<table>
<thead>
<tr>
<th>Req. No.</th>
<th>Item No.</th>
<th>Test Case No.</th>
<th>Input</th>
<th>Expected Output</th>
<th>Actual Output</th>
<th>Pass/Fail</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.a</td>
<td>1</td>
<td>cechuser</td>
<td>Login successful</td>
<td>Login successful</td>
<td>Pass</td>
<td>Test user Login success</td>
</tr>
<tr>
<td>1</td>
<td>1.a</td>
<td>2</td>
<td>moorern</td>
<td>Login successful</td>
<td>Login successful</td>
<td>Pass</td>
<td>CLS user login success</td>
</tr>
<tr>
<td>1</td>
<td>1.a</td>
<td>3</td>
<td>testuser</td>
<td>Sign in failed, please try again</td>
<td>Sign in failed, please try again</td>
<td>Pass</td>
<td>Non-user account denied access</td>
</tr>
<tr>
<td>1</td>
<td>1.b</td>
<td>1</td>
<td>cechuser</td>
<td>Login successful</td>
<td>Login successful</td>
<td>Pass</td>
<td>Test user Login success</td>
</tr>
<tr>
<td>1</td>
<td>1.b</td>
<td>2</td>
<td>moorern</td>
<td>Login successful</td>
<td>Login successful</td>
<td>Pass</td>
<td>CLS user login success</td>
</tr>
<tr>
<td>1</td>
<td>1.b</td>
<td>3</td>
<td>testuser</td>
<td>Sign in failed, please try again</td>
<td>Sign in failed, please try again</td>
<td>Pass</td>
<td>Non-user account denied access</td>
</tr>
<tr>
<td>1</td>
<td>1.c</td>
<td>1</td>
<td>cechuser</td>
<td>Login successful</td>
<td>Login successful</td>
<td>Pass</td>
<td>Test user Login success</td>
</tr>
<tr>
<td>1</td>
<td>1.c</td>
<td>2</td>
<td>moorern</td>
<td>Login successful</td>
<td>Login successful</td>
<td>Pass</td>
<td>CLS user login success</td>
</tr>
<tr>
<td>1</td>
<td>1.c</td>
<td>3</td>
<td>testuser</td>
<td>Sign in failed, please try again</td>
<td>Sign in failed, please try again</td>
<td>Pass</td>
<td>Non-user account denied access</td>
</tr>
<tr>
<td>1</td>
<td>1.d</td>
<td>1</td>
<td>moorern</td>
<td>Login successful</td>
<td>Login successful</td>
<td>Pass</td>
<td>CLS user login success</td>
</tr>
<tr>
<td>2</td>
<td>2.a</td>
<td>1</td>
<td>moorern</td>
<td>Home Dir. under My Files</td>
<td>Home Dir. under My Files</td>
<td>Pass</td>
<td>Expected files available</td>
</tr>
<tr>
<td>2</td>
<td>2.a</td>
<td>2</td>
<td>cechuser</td>
<td>Home Dir. under My Files</td>
<td>Home Dir. under My Files</td>
<td>Pass</td>
<td>Expected files available</td>
</tr>
<tr>
<td>2</td>
<td>2.a</td>
<td>3</td>
<td>eurkaepics</td>
<td>My Files functions unavailable</td>
<td>My Files functions unavailable</td>
<td>Pass</td>
<td>Users without assigned home directory's default to “Shared with Me”</td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>1</td>
<td>moorern</td>
<td>Correct Share dir. under Net Folders</td>
<td>Correct Share dir. under Net Folders</td>
<td>Pass</td>
<td>All assigned folders accessible</td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>2</td>
<td>cechuser</td>
<td>Correct Share dir. under Net Folders</td>
<td>No folders under Net Folders</td>
<td>Fail</td>
<td>User must be added to “Q Drive” group</td>
</tr>
<tr>
<td>---</td>
<td>-----</td>
<td>---</td>
<td>---------</td>
<td>-------------------------------------</td>
<td>-----------------------------</td>
<td>------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>3</td>
<td>eurkaepics</td>
<td>Correct Share dir. under Net Folders</td>
<td>No access to folders assigned direct rights</td>
<td>Fail</td>
<td>Refer to Known Issue 1</td>
</tr>
<tr>
<td>4</td>
<td>4.a</td>
<td>1</td>
<td>Share test folder from My Files with internal user with moorern account</td>
<td>Internal user receives e-mail with link to folder.</td>
<td>Internal user receives e-mail with link to folder.</td>
<td>Pass</td>
<td>When user click link, they must login to access file</td>
</tr>
<tr>
<td>4</td>
<td>4.a</td>
<td>2</td>
<td>Share test file from My Files with internal user with moorern account</td>
<td>Internal user receives e-mail with link to file.</td>
<td>Internal user receives e-mail with link to file.</td>
<td>Pass</td>
<td>When user click link, they must login to access file</td>
</tr>
<tr>
<td>4</td>
<td>4.b</td>
<td>1</td>
<td>Share test folder from Net Folders with internal user with moorern account</td>
<td>Internal user receives e-mail with link to folder.</td>
<td>You do not have the rights to share your selections.</td>
<td>Fail</td>
<td>Refer to Known Issue 2</td>
</tr>
<tr>
<td>4</td>
<td>4.b</td>
<td>2</td>
<td>Share test file from Net Folders with internal user with moorern account</td>
<td>Internal user receives e-mail with link to file.</td>
<td>Internal user receives e-mail with link to file.</td>
<td>Pass</td>
<td>When user click link, they must login to access file</td>
</tr>
<tr>
<td>4</td>
<td>4.b</td>
<td>3</td>
<td>Share test file from Net Folders with internal user with eurkaepics account</td>
<td>You do not have the right to share you selections.</td>
<td>You do not have the right to share you selections.</td>
<td>Pass</td>
<td>User does not have rights to share.</td>
</tr>
<tr>
<td>4</td>
<td>4.c</td>
<td>1</td>
<td>Share test folder from My Files with external user with moorern account</td>
<td>External user receives e-mail with link to folder.</td>
<td>External user receives e-mail with link to folder.</td>
<td>Pass</td>
<td>When user click link, they must create an account if they don’t already have one</td>
</tr>
<tr>
<td>4</td>
<td>4.c</td>
<td>2</td>
<td>Share test file from My Files</td>
<td>External user receives e-mail with link to folder.</td>
<td>External user receives e-mail with link to folder.</td>
<td>Pass</td>
<td>When user click link, they must</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4.d</td>
<td>1</td>
<td>Share test folder from Net Folder with internal user with moore account</td>
<td>Internal user receives e-mail with link to folder.</td>
<td>You do not have the rights to share your selections.</td>
<td>Fail</td>
<td>Refer to Known Issue 2</td>
</tr>
<tr>
<td>4</td>
<td>4.d</td>
<td>2</td>
<td>Share test file from Net Folders with external user with moore account</td>
<td>External user receives e-mail with link to file.</td>
<td>You do not have the rights to share your selections.</td>
<td>Fail</td>
<td>Refer to Known Issue 2</td>
</tr>
<tr>
<td>4</td>
<td>4.e</td>
<td>1</td>
<td>Set Expiration on Share</td>
<td>Share removed and not accessible by share members after expiration</td>
<td>Share removed and not accessible by share members after expiration</td>
<td>Pass</td>
<td>When user click link, they must create an account if they don’t already have one.</td>
</tr>
<tr>
<td>5</td>
<td>5.a</td>
<td>1</td>
<td>Login to Multiple instance of CECHCloud</td>
<td>Each instance alternates between cechcloud1 and cechcloud2</td>
<td>Each instance alternates between cechcloud1 and cechcloud2</td>
<td>Pass</td>
<td>The reverse proxy uses round robin load balancing that alternates cluster nodes.</td>
</tr>
<tr>
<td>5</td>
<td>5.b</td>
<td>1</td>
<td>Shutdown Cechcloud1</td>
<td>Connection to the server on multiple instances.</td>
<td>Connection to the server on multiple instances.</td>
<td>Pass</td>
<td>Each instance was automatically directed to cechcloud2.</td>
</tr>
<tr>
<td>5</td>
<td>5.b</td>
<td>2</td>
<td>Shutdown Cechcloud2</td>
<td>Connection to the server on multiple instances.</td>
<td>Connection to the server on multiple instances.</td>
<td>Pass</td>
<td>Each instance was automatically directed to cechcloud1.</td>
</tr>
<tr>
<td>5</td>
<td>5.c</td>
<td>1</td>
<td>Shutdown Filrshare1</td>
<td>System should function normally</td>
<td>System should function normally</td>
<td>Pass</td>
<td>With heavy usage, performance may be slowed.</td>
</tr>
<tr>
<td>5</td>
<td>5.c</td>
<td>2</td>
<td>Shutdown Filrshare2</td>
<td>System should function normally</td>
<td>System should function normally</td>
<td>Pass</td>
<td>Performance may be slowed.</td>
</tr>
<tr>
<td>Req. No.</td>
<td>Item No.</td>
<td>Test Case No.</td>
<td>Browser</td>
<td>Input</td>
<td>Expected Output</td>
<td>Actual Output</td>
<td>Pass/Fail</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>---------------</td>
<td>---------</td>
<td>-------</td>
<td>-----------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>2</td>
<td>2.a</td>
<td>1</td>
<td>n/a</td>
<td>Test Connection on Campus</td>
<td>Web Interface displayed</td>
<td>Web Interface displayed</td>
<td>Pass</td>
</tr>
<tr>
<td>2</td>
<td>2.b</td>
<td>2</td>
<td>n/a</td>
<td>Test connection off campus</td>
<td>Web Interface displayed</td>
<td>Web Interface displayed</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>1</td>
<td>IE</td>
<td>Test Search Times for My Files</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>2</td>
<td>Chrome</td>
<td>Test Search Times for My Files</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>3</td>
<td>Firefox</td>
<td>Test Search Times for My Files</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>4</td>
<td>Safari</td>
<td>Test Search Times for My Files</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>3.b</td>
<td>1</td>
<td>IE</td>
<td>Test Search Times for Net Folders</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>3.b</td>
<td>2</td>
<td>Chrome</td>
<td>Test Search Times for Net Folders</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>3.b</td>
<td>3</td>
<td>Firefox</td>
<td>Test Search Times for Net Folders</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>3.b</td>
<td>4</td>
<td>Safari</td>
<td>Test Search Times for Net Folders</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.a</td>
<td>1</td>
<td>IE</td>
<td>Download Test file to local workstation</td>
<td>File downloaded successful</td>
<td>File downloaded successful</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.a</td>
<td>2</td>
<td>Chrome</td>
<td>Download Test file to local workstation</td>
<td>File downloaded successful</td>
<td>File downloaded successful</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.a</td>
<td>3</td>
<td>Firefox</td>
<td>Download Test file to local workstation</td>
<td>File downloaded successful</td>
<td>File downloaded successful</td>
<td>Pass</td>
</tr>
<tr>
<td>---</td>
<td>-----</td>
<td>----</td>
<td>---------</td>
<td>----------------------------------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
<td>------</td>
</tr>
<tr>
<td>4</td>
<td>4.a</td>
<td>4</td>
<td>Safari</td>
<td>Download Test file to local workstation</td>
<td>File downloaded successful</td>
<td>File downloaded successful</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.b</td>
<td>1</td>
<td>IE</td>
<td>Upload Files from local workstation</td>
<td>File successfully uploaded and appears on server immediately</td>
<td>File successfully uploaded and appears on server immediately</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.b</td>
<td>2</td>
<td>Chrome</td>
<td>Upload Files from local workstation</td>
<td>File successfully uploaded and appears on server immediately</td>
<td>File successfully uploaded and appears on server immediately</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.b</td>
<td>3</td>
<td>Firefox</td>
<td>Upload Files from local workstation</td>
<td>File successfully uploaded and appears on server immediately</td>
<td>File successfully uploaded and appears on server immediately</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.b</td>
<td>4</td>
<td>Safari</td>
<td>Upload Files from local workstation</td>
<td>File successfully uploaded and appears on server immediately</td>
<td>File successfully uploaded and appears on server immediately</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.c</td>
<td>1</td>
<td>IE</td>
<td>Upload edited existing files from local workstation</td>
<td>File overwrites file on the server</td>
<td>File overwrites file on the server</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.c</td>
<td>2</td>
<td>Chrome</td>
<td>Upload edited</td>
<td>File overwrites</td>
<td>File overwrites</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.c</td>
<td>3</td>
<td>Firefox</td>
<td>Upload edited existing files from local workstation</td>
<td>File overwrites file on the server</td>
<td>File overwrites file on the server</td>
<td>Pass</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---------</td>
<td>-------------------------------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>4</td>
<td>4.c</td>
<td>4</td>
<td>Safari</td>
<td>Upload edited existing files from local workstation</td>
<td>File overwrites file on the server</td>
<td>File overwrites file on the server</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.d</td>
<td>1</td>
<td>IE</td>
<td>Edit Office document with Edit-In-Place feature</td>
<td>Document opens on local workstation and changes are saved directly to the file server</td>
<td>Document opens on local workstation and changes are saved directly to the file server</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.d</td>
<td>2</td>
<td>Chrome</td>
<td>Edit Office document with Edit-In-Place feature</td>
<td>Document opens on local workstation and changes are saved directly to the file server</td>
<td>Document opens on local workstation and changes are saved directly to the file server</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>4.d</td>
<td>3</td>
<td>Firefox</td>
<td>Edit Office document with Edit-In-Place feature</td>
<td>Document opens on local workstation and changes are saved directly to the file server</td>
<td>Document opens on local workstation and changes are saved directly to the file server</td>
<td>Pass</td>
</tr>
<tr>
<td>Req. No.</td>
<td>Item No.</td>
<td>Test Case No.</td>
<td>Input</td>
<td>Expected Output</td>
<td>Actual Output</td>
<td>Pass/Fail</td>
<td>Notes</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>---------------</td>
<td>-------</td>
<td>-----------------</td>
<td>---------------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>1</td>
<td>1.a</td>
<td>1</td>
<td>Install Client on Windows 7</td>
<td>Successful Install</td>
<td>Successful Install</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1.b</td>
<td>1</td>
<td>Install Client on Windows 8</td>
<td>Successful Install</td>
<td>Successful Install</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2.a</td>
<td>1</td>
<td>Sync all files to local directory, Windows 7</td>
<td>All files sync</td>
<td>All files sync</td>
<td>Pass</td>
<td>Files over 1GB do not sync. User must select which Net Folders files sync</td>
</tr>
<tr>
<td>2</td>
<td>2.a</td>
<td>2</td>
<td>Sync all files to local directory, Windows 8</td>
<td>All files sync</td>
<td>All files sync</td>
<td>Pass</td>
<td>Files over 1GB do not sync. User must select which Net Folders files sync</td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>1</td>
<td>Create new file in</td>
<td>File is synced to</td>
<td>File is synced to</td>
<td>Pass</td>
<td></td>
</tr>
</tbody>
</table>

**Table 5: CECHCloud Desktop Client (Windows) Test Results**
### Table 6: CECHCloud iOS App Test Results

<table>
<thead>
<tr>
<th>Req. No.</th>
<th>Item No.</th>
<th>Test Case No.</th>
<th>Input</th>
<th>Expected Output</th>
<th>Actual Output</th>
<th>Pass/Fail</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.a</td>
<td>1</td>
<td>Test connection on campus</td>
<td>Successful connection and login</td>
<td>Successful connection and login</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1.b</td>
<td>1</td>
<td>Test connection off campus</td>
<td>Successful connection and login</td>
<td>Successful connection and login</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2.a</td>
<td>1</td>
<td>Logoff, reopen app</td>
<td>User password required to login again.</td>
<td>User password required to login again</td>
<td>Pass</td>
<td>No option to save password after initial login</td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>1</td>
<td>Test search times on My Files</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>Req. No.</td>
<td>Item No.</td>
<td>Test Case No.</td>
<td>Input</td>
<td>Expected Output</td>
<td>Actual Output</td>
<td>Pass/Fail</td>
<td>Notes</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>---------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1</td>
<td>1.a</td>
<td>1</td>
<td>Test connection on campus</td>
<td>Successful connection and login</td>
<td>Successful connection and login</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1.b</td>
<td>1</td>
<td>Test connection off campus</td>
<td>Successful connection and login</td>
<td>Successful connection and login</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2.a</td>
<td>1</td>
<td>Logoff, reopen app</td>
<td>User password required to login again.</td>
<td>User password required to login again</td>
<td>Pass</td>
<td>No option to save password after initial login</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>1</td>
<td>Test search times on My Files</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3.b</td>
<td>1</td>
<td>Test search times on Net Folders</td>
<td>&lt;1s</td>
<td>&lt;1s</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4.a</td>
<td>1</td>
<td>Download file</td>
<td>File downloads to local device. Viewable from downloads tab.</td>
<td>File downloads to local device. Viewable from downloads tab.</td>
<td>Pass</td>
<td>Tapping a file only brings up a preview. Does not save to device.</td>
</tr>
<tr>
<td>4</td>
<td>4.b</td>
<td>1</td>
<td>Upload a file from device</td>
<td>File available on server instantly</td>
<td>File available on server instantly</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4.c</td>
<td>1</td>
<td>Download file, edit it, and upload</td>
<td>File is replaced on server with new version</td>
<td>File is replaced on server with new version</td>
<td>Pass</td>
<td>An App to edit the file must be installed on device</td>
</tr>
<tr>
<td>5</td>
<td>5.a</td>
<td>1</td>
<td>Share file from app</td>
<td>All sharing functionality is available</td>
<td>All sharing functionality is available</td>
<td>Pass</td>
<td>Must have version 1.0.1 or greater of the app</td>
</tr>
<tr>
<td>5</td>
<td>5.b</td>
<td>1</td>
<td>View shared files</td>
<td>Shared files appear in the Shared by Me tab</td>
<td>Shared files appear in the Shared by Me tab</td>
<td>Pass</td>
<td></td>
</tr>
</tbody>
</table>
Beta Testing

Beta testing was done with two different groups at CECH which are significant stakeholders in the Filr project. The first group is from the American Sign Language (ASL) program. Professors from this department utilized the CECHCloud program to create share folders with students (external users). These shares gave the students a place to upload large video files and other documents to turn in for assignments. The shares would then expire after the due date of the assignment and the students account removed.

During this beta test, it was discovered that the students accounts were being deleted after only a day, however the shares were not expired. This was the result of a default setting to remove non-LDAP accounts from the Filr directory when the LDAP was synced overnight. The resolution was a simple change in the configuration of the LDAP sync settings.

The second significant beta test involved a larger group of users from the Criminal Justice department and their EPICS program. The users in this test group included professors and graduate assistants, and third party sites around the country. The third party sites have affiliate accounts that allow them access to a specific folder where they can upload audio files from interviews. These interviews are then access by the GA’s to be transcribed and coded for research.

During the beta test with this group a couple of different issues were discovered. Known issue #1 was discovered by GAs who were given direct trustee permissions to individual sub folders. Some of the GAs and professors access the share folder from Apple Mac OSX devices. The OSX operating system creates hidden files known as “apple double” files that contain metadata. These files however were not hidden on the NFS file system and when accessed through the Filr web interface or iOS app, appeared as the actual file with a “._” before the name. When users attempted to open these files, they were unable to be read by the corresponding programs.

The “apple double” files have been deprecated in newer programs and are not necessary. In order to solve this issue, I leveraged Novell’s Storage Manager Software to “groom” the file servers and remove any of these “apple double” files and scheduled grooming for future files that are created.

Known Issues

1. Some users are unable to see some Share sub-folders that they have direct trustee rights to in eDirectory.

Cause:

When shared sub directories were created using Novell Storage Manager, the Group with access to the directory was assigned as the Owner for that share. Filr is unable to read the ACL’s for folders that have the Group set as the Owner.

Resolution:

Bug has been reported to the Novell Filr engineers. A workaround was set to change the attribute of the Owner of these affected folders to User. When new shares are created with Novell Storage Manager, the Owner will need to be changed as well.
2. Users cannot share Folders in Net Folders.

Cause:
This is a feature that has not been added to the system yet.

Resolution:
This feature will be added in an upcoming release. Until then, user can create folders under their Home Directories (My Files) and share entire folders from there.

3. Branding on the login page does not always show up

Cause: Unknown

Resolution:
This is a known issue by the Novell Filr engineering team. It is expected to be fixed in the next release.

4. Files are not able to be sorted by the last modified date in the Filr web interface

Cause:
Filtr attempts to sort the files by the date they were originally indexed with the Filr system, rather than the last modified date from the files metadata.

Resolution:
This bug has been reported to the Novell Engineering team and is expected to be fixed in the next release.

System Requirements – Airwatch

BYOD – Employee Owned Devices
Organization Group – BYOD – CECH

1. User can self-enroll using CLS Credentials
2. Device and be unenrolled without authorization
3. User can access and install public and assigned VPP apps through CECH App Catalog
4. Managed Apps removed when device unenrolled
5. UC Exchange e-mail configuration
6. Junos Pulse VPN settings
7. Location Tracking not available in Airwatch
8. Remote Full Wipe not available in Airwatch
9. Lock device remotely
10. Clear passcode remotely
11. Enterprise wipe (remote disenrollment)
12. User access to self-service portal
**Department Owned – Single User Device**
Organization Group – Department Owned – CECH

1. User enrollment with CLS Credentials
2. Device cannot be unenrolled without authorization
3. User can access and install public and assigned VPP apps through CECH App Catalog
4. Managed Apps removed when device unenrolled
5. UC Exchange e-mail configuration
6. Junos Pulse VPN settings
7. Location tracking
8. Remote full wipe
9. Enterprise wipe
10. Lock Device remotely
11. Clear passcode remotely
12. User access to self-service portal

**Department Loaner Devices**
Organization Groups – Loaner Faculty and Staff & Loaner Students – CECH

1. Post enrollment with Airwatch Enroll web clip
2. Device cannot be unenrolled without authorization
3. Device locked to agent login screen while checked in
4. Device unlocked from agent while checked out
5. Faculty, staff, and students can login for checkout using CLS credentials
6. Proper Organization Group and user assignment during check in/check out process
7. Assigned Public and VPP apps install automatically (by request)
8. Prevent Apple ID account changes
9. Location Tracking
10. Remote full wipe
11. Enterprise wipe
12. Lock Device remotely
13. Clear passcode remotely
14. No user access in self-service portal

**Test Planning**

**BYOD – Employee Owned Devices**
Organization Group – BYOD – CECH

1. Test user self-enroll using CLS Credentials
   a. Enroll BYOD device via web enrollment
   b. Enroll BYOD device via agent
2. Test device enrollment removal
   a. Remove BOYD device
3. Test access to apps via CECH App Catalog
   a. Install public app via catalog
   b. Install VPP app via catalog
4. Test managed app removal with device unerollment
   a. Remove BYOD device
5. Test UC Exchange email configuration
   a. Check configuration without prior settings
   b. Check configuration with prior settings
6. Test Junos Pulse VPN Settings
   a. Install Junos Pulse, check settings without prior configuration
   b. Install Junos Pulse, check settings with prior configuration
   c. Connect to VPN with Junos Pulse
7. Test the lack of ability to track location via Airwatch
   a. Check location of BYOD via Airwatch console
   b. Check location of BYOD via self-service portal
8. Test the lack of ability to perform a full wipe via Airwatch
   a. Attempt to perform a full wipe on a BYOD device via Airwatch console
   b. Attempt to perform a full wipe on a BYOD device via self-service portal
9. Test remote lock of device
   a. Perform a remote lock via Airwatch
   b. Perform a remote lock via self-service portal
10. Test clear passcode remotely
    a. Attempt to clear passcode via Airwatch
    b. Attempt to clear passcode via self-service portal
11. Test enterprise wipe
    a. Attempt an enterprise wipe via Airwatch
    b. Attempt an enterprise wipe via self-service portal
12. Test user access to self-service portal
    a. Log into self-service portal as user, verify devices

**Department Owned – Single User Device**

Organization Group – Department Owned – CECH

1. Test user enrollment with CLS Credentials
   a. Enroll device via web enrollment
   b. Enroll device via Airwatch agent
2. Test device cannot be unenrolled without authorization
   a. Attempt to remove a device
3. Test user can access and install public and assigned VPP apps through CECH App Catalog
   a. Install a public app via CECH App Catalog
   b. Install a VPP app via CECH App Catalog
4. Test managed apps removed when device unenrolled
   a. Remove device and verify managed apps removed
5. Test UC Exchange e-mail configuration
   a. Check configuration without prior settings
   b. Check configuration with prior settings
6. Test Junos Pulse VPN settings
   a. Install Junos Pulse, check settings without prior configuration
   b. Install Junos Pulse, check settings with prior configuration
   c. Connect to VPN with Junos Pulse
7. Test Location tracking
   a. Check location of device via Airwatch Console
   b. Check location of device via self-service portal
8. Test Remote full wipe
   a. Attempt to perform a full wipe on device via Airwatch console
   b. Attempt to perform a full wipe on device via self-service portal
9. Test Enterprise wipe
   a. Attempt an enterprise wipe via Airwatch
   b. Attempt an enterprise wipe via self-service portal
10. Test lock device remotely
    a. Perform a remote lock via Airwatch
    b. Perform a remote lock via self-service portal
11. Test clear passcode remotely
    a. Attempt to clear passcode via Airwatch
    b. Attempt to clear passcode via self-service portal
12. Test user access to self-service portal
    a. Log into self-service portal as user, verify devices

Department Loaner Devices
Organization Groups – Loaner Faculty and Staff & Loaner Students – CECH

1. Test post enrollment with Airwatch Enroll web clip
   a. Open Airwatch Enroll web clip, verify agent settings
2. Test device cannot be unenrolled without authorization
   a. Attempt to remove a device
3. Test device locked to agent login screen while checked in
   a. Attempt to leave Airwatch agent on a checked in device
4. Test device unlocked from agent while checked out
   a. Check out a device, attempt to leave agent
5. Test faculty, staff, and students can login for checkout using CLS credentials
   a. Test different user accounts for login
6. Test proper Organization Group and user assignment during check in/check out process
   a. Login with faculty staff account, verify user and OG
   b. Login with student account, verify user and OG
   c. Logout with accounts, verify user and OG
7. Test assigned Public and VPP apps install automatically (upon request)
   a. Assign apps to users and login to device
8. Test prevent Apple ID account changes
   a. Attempt to change the Apple ID
9. Test Location tracking
   a. Check location of device via Airwatch Console
10. Test lock device remotely
    a. Perform a remote lock via Airwatch
11. Test clear passcode remotely
    a. Attempt to clear passcode via Airwatch
12. Test Enterprise wipe
    a. Attempt an enterprise wipe via Airwatch
13. Test Remote full wipe
    a. Attempt to perform a full wipe on device via Airwatch console

Test Results

Table 8: Airwatch BYOD Test Results

<table>
<thead>
<tr>
<th>Req. No.</th>
<th>Item No.</th>
<th>Test Case No.</th>
<th>Input</th>
<th>Expected Output</th>
<th>Actual Output</th>
<th>Pass/Fail</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.a</td>
<td>1</td>
<td>Airwatch test</td>
<td>Enrolled successfully</td>
<td>Enrolled successfully</td>
<td>Pass</td>
<td>AD test user login success</td>
</tr>
<tr>
<td>1</td>
<td>1.a</td>
<td>2</td>
<td>moorern</td>
<td>Enrolled successfully</td>
<td>Enrolled successfully</td>
<td>Pass</td>
<td>CLS user login success</td>
</tr>
<tr>
<td>1</td>
<td>1.a</td>
<td>3</td>
<td>testuser</td>
<td>Failed to validate user credentials</td>
<td>Failed to validate user credentials</td>
<td>Pass</td>
<td>Non-user account denied access</td>
</tr>
<tr>
<td>1</td>
<td>1.b</td>
<td>1</td>
<td>Airwatch test</td>
<td>Enrolled successfully</td>
<td>Enrolled successfully</td>
<td>Pass</td>
<td>AD test user login success</td>
</tr>
<tr>
<td>1</td>
<td>1.b</td>
<td>2</td>
<td>moorern</td>
<td>Enrolled successfully</td>
<td>Enrolled successfully</td>
<td>Pass</td>
<td>CLS user login success</td>
</tr>
<tr>
<td>1</td>
<td>1.b</td>
<td>3</td>
<td>testuser</td>
<td>Failed to validate user credentials</td>
<td>Failed to validate user credentials</td>
<td>Pass</td>
<td>Non-user account denied access</td>
</tr>
<tr>
<td>2</td>
<td>2.a</td>
<td>1</td>
<td>Remove profile</td>
<td>Profile removed, console shows device unenrolled</td>
<td>Profile removed, console shows device unenrolled</td>
<td>Pass</td>
<td>Device not delete from console</td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>1</td>
<td>Install Novell Filr app</td>
<td>Install app</td>
<td>Install app</td>
<td>Pass</td>
<td>User Prompted to confirm install</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3.b</td>
<td>1</td>
<td>Install Math 42 app</td>
<td>Install app</td>
<td>Did not install</td>
<td>Fail</td>
<td>See Known Issue 1</td>
</tr>
<tr>
<td>4</td>
<td>4.a</td>
<td>1</td>
<td>Remove enrollment profile</td>
<td>Managed apps removed</td>
<td>Managed apps removed</td>
<td>Pass</td>
<td>Apps installed via App Store not affected</td>
</tr>
<tr>
<td>5</td>
<td>5.a</td>
<td>1</td>
<td>Open Mail app without prior configuration</td>
<td>Settings configured, password required</td>
<td>Settings configured, password required</td>
<td>Pass</td>
<td>Once password was entered, mail and contact were sync with exchange</td>
</tr>
<tr>
<td>5</td>
<td>5.b</td>
<td>1</td>
<td>Open mail app that was configured prior to enrollment</td>
<td>Existing exchange profile over written</td>
<td>A second, identical profile is created</td>
<td>Fail</td>
<td>Consider removing this feature from BYOD devices.</td>
</tr>
<tr>
<td>6</td>
<td>6.a</td>
<td>1</td>
<td>Install Junos Pulse after enrollment</td>
<td>Sslvpn connection settings preconfigured</td>
<td>Sslvpn connection settings preconfigured</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6.b</td>
<td>1</td>
<td>Install and configure Junos Pulse prior to enrollment</td>
<td>Sslvpn connection settings overridden</td>
<td>Sslvpn connection settings overridden</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6.c</td>
<td>1</td>
<td>Connect to SSLVPN with configured Junos Pulse app</td>
<td>Connected successfully</td>
<td>Connected successfully</td>
<td>Pass</td>
<td>User needs to provide password</td>
</tr>
<tr>
<td>7</td>
<td>7.a</td>
<td>1</td>
<td>Locate device via console</td>
<td>Data not collected due to privacy settings.</td>
<td>Data not collected due to privacy settings.</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7.b</td>
<td>1</td>
<td>Locate Device via self-service portal</td>
<td>Hidden For Privacy</td>
<td>Hidden For Privacy</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8.a</td>
<td>1</td>
<td>Perform full wipe from console</td>
<td>Option not available</td>
<td>Option not available</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8.b</td>
<td>1</td>
<td>Perform full wipe from self-service portal</td>
<td>Option not available</td>
<td>Option not available</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>Req. No.</td>
<td>Item No.</td>
<td>Test Case No.</td>
<td>Input</td>
<td>Expected Output</td>
<td>Actual Output</td>
<td>Pass/Fail</td>
<td>Notes</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>---------------</td>
<td>-------</td>
<td>----------------------------------</td>
<td>---------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1</td>
<td>1.a</td>
<td>1</td>
<td>Airwatch test</td>
<td>Enrolled successfully</td>
<td>Enrolled successfully</td>
<td>Pass</td>
<td>AD test user login success</td>
</tr>
<tr>
<td>1</td>
<td>1.a</td>
<td>2</td>
<td>moorern</td>
<td>Enrolled successfully</td>
<td>Enrolled successfully</td>
<td>Pass</td>
<td>CLS user login success</td>
</tr>
<tr>
<td>#</td>
<td>1.a</td>
<td>3</td>
<td>testuser</td>
<td>Failed to validate user credentials</td>
<td>Failed to validate user credentials</td>
<td>Pass</td>
<td>Non-user account denied access</td>
</tr>
<tr>
<td>----</td>
<td>-----</td>
<td>---</td>
<td>----------</td>
<td>-------------------------------------</td>
<td>-------------------------------------</td>
<td>------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>1.b</td>
<td>1</td>
<td>Airwatch test</td>
<td>Enrolled successfully</td>
<td>Enrolled successfully</td>
<td>Pass</td>
<td>AD test user login success</td>
</tr>
<tr>
<td>1</td>
<td>1.b</td>
<td>2</td>
<td>moorern</td>
<td>Enrolled successfully</td>
<td>Enrolled successfully</td>
<td>Pass</td>
<td>CLS user login success</td>
</tr>
<tr>
<td>1</td>
<td>1.b</td>
<td>3</td>
<td>testuser</td>
<td>Failed to validate user credentials</td>
<td>Failed to validate user credentials</td>
<td>Pass</td>
<td>Non-user account denied access</td>
</tr>
<tr>
<td>2</td>
<td>2.a</td>
<td>1</td>
<td>Remove MDM profile</td>
<td>Password required for removal</td>
<td>Profile removed</td>
<td>Fail</td>
<td>See Known issue 2</td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>1</td>
<td>Install Novell Filr app</td>
<td>Install app</td>
<td>Install app</td>
<td>Pass</td>
<td>User Prompted to confirm install</td>
</tr>
<tr>
<td>3</td>
<td>3.b</td>
<td>1</td>
<td>Install Math 42 app</td>
<td>Install app</td>
<td>Did not install</td>
<td>Fail</td>
<td>See Known Issue 1</td>
</tr>
<tr>
<td>4</td>
<td>4.a</td>
<td>1</td>
<td>Remove enrollment profile</td>
<td>Managed apps removed</td>
<td>Managed apps removed</td>
<td>Pass</td>
<td>Apps installed via App Store not affected</td>
</tr>
<tr>
<td>5</td>
<td>5.a</td>
<td>1</td>
<td>Open Mail app without prior configuration</td>
<td>Settings configured, password required</td>
<td>Settings configured, password required</td>
<td>Pass</td>
<td>Once password was entered, mail and contact were sync with exchange</td>
</tr>
<tr>
<td>5</td>
<td>5.b</td>
<td>1</td>
<td>Open mail app that was configured prior to enrollment</td>
<td>Existing exchange profile over written.</td>
<td>A second, identical profile is created</td>
<td>Fail</td>
<td>This use case only applies to new devices</td>
</tr>
<tr>
<td>6</td>
<td>6.a</td>
<td>1</td>
<td>Install Junos Pulse after enrollment</td>
<td>Sslvpn connection settings preconfigured</td>
<td>Sslvpn connection settings preconfigured</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6.b</td>
<td>1</td>
<td>Install and configure Junos Pulse prior to enrollment</td>
<td>Sslvpn connection settings overridden</td>
<td>Sslvpn connection settings overridden</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6.c</td>
<td>1</td>
<td>Connect to SSLVPN with configured</td>
<td>Connected successfully</td>
<td>Connected successfully</td>
<td>Pass</td>
<td>User needs to provide password</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7.a</td>
<td>1</td>
<td>Locate device via console</td>
<td>Device location shown in console</td>
<td>Device location shown in console</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7.b</td>
<td>1</td>
<td>Locate Device via self-service portal</td>
<td>Device location shown in console</td>
<td>Device location shown in console</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8.a</td>
<td>1</td>
<td>Perform full wipe from console</td>
<td>Option not available</td>
<td>Option not available</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8.b</td>
<td>1</td>
<td>Perform full wipe from self-service portal</td>
<td>Option not available</td>
<td>Option not available</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>9.a</td>
<td>1</td>
<td>Perform a remote lock via console</td>
<td>Device locked</td>
<td>Device locked</td>
<td>Pass</td>
<td>Device can be unlocked with user passcode</td>
</tr>
<tr>
<td>9</td>
<td>9.b</td>
<td>1</td>
<td>Perform a remote lock via self-service portal</td>
<td>Device locked</td>
<td>Device locked</td>
<td>Pass</td>
<td>Device can be unlocked with user passcode</td>
</tr>
<tr>
<td>10</td>
<td>10.a</td>
<td>1</td>
<td>Clear passcode via console</td>
<td>Passcode removed</td>
<td>Passcode removed</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10.b</td>
<td>1</td>
<td>Clear passcode via self-service portal</td>
<td>Passcode removed</td>
<td>Passcode removed</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>11.a</td>
<td>1</td>
<td>Perform an Enterprise wipe from console</td>
<td>Device unenrolled, profiles removed, managed apps removed</td>
<td>Device unenrolled, profiles removed, managed apps removed</td>
<td>Pass</td>
<td>Device is not deleted from console</td>
</tr>
<tr>
<td>11</td>
<td>11.b</td>
<td>1</td>
<td>Perform an Enterprise wipe from self-service portal</td>
<td>Device unenrolled, profiles removed, managed apps removed</td>
<td>Device unenrolled, profiles removed, managed apps removed</td>
<td>Pass</td>
<td>User no longer sees device in portal</td>
</tr>
<tr>
<td>12</td>
<td>12.a</td>
<td>1</td>
<td>Test user access to self-service portal</td>
<td>User can log into and see enrolled devices</td>
<td>User can log into and see enrolled devices</td>
<td>Pass</td>
<td>User can log in without device enrolled</td>
</tr>
</tbody>
</table>
Table 10: Airwatch Department Loaner Device Test Results

<table>
<thead>
<tr>
<th>Req. No.</th>
<th>Item No.</th>
<th>Test Case No.</th>
<th>Input</th>
<th>Expected Output</th>
<th>Actual Output</th>
<th>Pass/Fail</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.a</td>
<td>1</td>
<td>Open Web Clip</td>
<td>Airwatch Agent configuration</td>
<td>Airwatch Agent configuration</td>
<td>Pass</td>
<td>Configuration complete when agent is at login screen</td>
</tr>
<tr>
<td>2</td>
<td>2.a</td>
<td>1</td>
<td>Remove MDM profile</td>
<td>Password required for removal</td>
<td>Profile removed</td>
<td>Fail</td>
<td>See Known issue 2</td>
</tr>
<tr>
<td>3</td>
<td>3.a</td>
<td>1</td>
<td>Hit home screen button</td>
<td>No response</td>
<td>No response</td>
<td>Pass</td>
<td>iPad is locked into login screen until user logs in</td>
</tr>
<tr>
<td>4</td>
<td>4.a</td>
<td>1</td>
<td>Login with user moorern</td>
<td>Login successful, unlocked from Airwatch agent</td>
<td>Login successful, unlocked from Airwatch agent</td>
<td>Pass</td>
<td>After login, device is moved to new OG, removing single app mode profile</td>
</tr>
<tr>
<td>5</td>
<td>5.a</td>
<td>1</td>
<td>Login with Airwatch test</td>
<td>Successful login</td>
<td>Successful login</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5.b</td>
<td>1</td>
<td>Login with testuser</td>
<td>Failed to validate user credentials</td>
<td>Failed to validate user credentials</td>
<td>Pass</td>
<td>User must have account in AD</td>
</tr>
<tr>
<td>6</td>
<td>6.a</td>
<td>1</td>
<td>Login with account moorern</td>
<td>Device moved to OG Students</td>
<td>Device moved to OG Students</td>
<td>Pass</td>
<td>Based on AD group membership, moorern account is placed into Students</td>
</tr>
<tr>
<td>6</td>
<td>6.b</td>
<td>1</td>
<td>Login with account Airwatch test</td>
<td>Device moved to OG Faculty and Staff</td>
<td>Device moved to OG Faculty and Staff</td>
<td>Pass</td>
<td>Based on AD group membership, Airwatch test account is placed into Faculty and Staff</td>
</tr>
<tr>
<td>6</td>
<td>6.c</td>
<td>1</td>
<td>Logout</td>
<td>Device moved to staging OG</td>
<td>Device moved to staging OG</td>
<td>Pass</td>
<td>Staging OG is the default</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>7</strong></td>
<td><strong>7.a</strong></td>
<td><strong>1</strong></td>
<td>Assign UC Mobile App to Airwatch test user</td>
<td>App installs when user logs in</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>App installs when user logs in</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pass</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>8</strong></td>
<td><strong>8.a</strong></td>
<td><strong>1</strong></td>
<td>Change Apple ID</td>
<td>Option not available</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Option not available</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pass</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>9</strong></td>
<td><strong>9.a</strong></td>
<td><strong>1</strong></td>
<td>Locate device via console</td>
<td>Device location shown in console</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Device location shown in console</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pass</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>10</strong></td>
<td><strong>10.a</strong></td>
<td><strong>1</strong></td>
<td>Perform a remote lock via console</td>
<td>Device locked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Device locked</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pass</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Device can be unlocked with user passcode</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>11</strong></td>
<td><strong>11.a</strong></td>
<td><strong>1</strong></td>
<td>Clear passcode via console</td>
<td>Passcode removed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Passcode removed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pass</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>12</strong></td>
<td><strong>12.a</strong></td>
<td><strong>1</strong></td>
<td>Perform an Enterprise wipe from console</td>
<td>Device unenrolled, profiles removed, managed apps removed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Device unenrolled, profiles removed, managed apps removed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pass</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Device is not deleted from console</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>13</strong></td>
<td><strong>13.a</strong></td>
<td><strong>1</strong></td>
<td>Test user access to self-service portal</td>
<td>User can log into and see enrolled devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>User can log into and see enrolled devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pass</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>User can log in even without devices enrolled, but can only register a device</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Known Issues**

Known Issue 1: Apple VPP License is not fully implemented

Airwatch has acknowledged limited functionality of the Apple VPP License system. License apps can be added to Airwatch and distributed once to users. Once distributed, the license cannot be reclaimed or reinstalled via Airwatch, but can be reinstalled using the user’s Apple ID and Apple app store. Full functionality is expected to be available in version 7.1.
Known Issue 2: Apple does not allow preventing the removal of MDM Profiles

Currently, Apple restricts the ability to prevent the removal of an MDM profile unless the device was purchased directly from Apple and the profile was preloaded onto the system. This functionality should be available in a future release of iOS for supervised devices, but no time-frame has been provided as to when this feature will be available.

Conclusion & Recommendations

With Novell Filr and Airwatch Mobile device management now up and running, CECH is two steps closer to solving the mobile dilemma. These solutions address many of the issues Technology Support Services have encountered while trying to keep up with the new hypermobile faculty and staff. Users now have easy, secure access to their data and do not have to resort to less secure third party solutions. Also, the TSS department can now begin to manage mobile devices and is prepared to implement new policies in the future, as the need will surely arise.

While these solutions are a good start, the work in reigning in the mobile infrastructure is incomplete. During this project, some of the promised features in the systems were not complete. For the Novell Filr implementation, the missing features and bugs of the system will not delay the full rollout to all faculty and staff. For several months now, the CECHCloud system has been in an open beta test for any user who would like to use it. It will be officially launched after the next update. That update should be available shortly and should fix several bugs.

The Airwatch system did not completely deliver as promised on some features, and therefore, I am making the recommendation to hold off on deploying this system for the time being. Airwatch’s inability to remove certain user data and settings, such as the Apple ID, from a multi-user device without a complete wipe of the device is particularly troublesome. I recommended that the system be
implemented during the Summer of 2014 when the college will be relocating computer labs and offices. This will allow for more time to expose users to the new process. Also, the lack of the fully functional VPP program causes Airwatch to lose a majority of its value. Until these issues are resolved, I cannot recommend purchasing Airwatch licenses for BYOD devices.
References

Airwatch, LLC. (2012). *Enabling Bring Your Own Device (BYOD) In the Enterprise*. Airwatch, LLC.


Marton, J. (2013, October 9). Telephone interview.


Cincinnati, OH: University of Cincinnati. Retrieved October 2013, from

http://hdl.handle.net/2374.UC/702723


*Novell Mobility Webinars.*


Appendix A-1 – CECHCloud Quick Reference Guide

About CECHCloud

CECHCloud is a service provided by the CECH Technology Support Services department that is powered by Novell’s Filr. This service gives you access to all the files stored securely on your U:, Q:, and R: drives from the “Cloud” on just about any device without having to connect with the VPN.

Accessing CECHCloud

**NOTE:** CECHCloud can be accessed from any web browser, on or off campus without the VPN.

1. Go to the URL [https://cechcloud.uc.edu](https://cechcloud.uc.edu).
2. Enter your UC Central Login User Name and Password and click Sign In.

Accessing Different Storage locations

- The **My Files** icon takes you to your **U: Drive**.
- The **Shared with Me** icon shows files others have shared with you.
- The **Shared by Me** icon shows files you have shared with others.
- The **Net Folder** icon takes you to files the **Q: and R: drives**.

Working With Files and Folders

**Sharing Files and Folders** - You can only share Folders that are located in **MY Files (U: Drive)**

**Adding Folders** - Create new folders inside U: Drive and Q: Drive inside CECHCloud.

**Download Files** - Download files from CECHCloud web browser.

**Editing a File** - It is recommended to download a file, edit, and then re-upload to CECHCloud.

**Viewing Files in Read-Only Mode** - View files inside web browser.

Desktop Sync

Use **Novell Filr Desktop Sync** application to sync your network storage with your home computer or laptop. This application will create a copy of each file on your local computer that will automatically sync back to the server. Any changes made to files on your local computer will be changed
on the server. (It is recommended to have a secure login to any machine with the Desktop Sync installed)

Mobile Devices

CECHCloud can be accessed on Apple iOS, Android, and Blackberry 10 mobile devices. Download the mobile app by searching for “Novell Filr” from the app store.

Further Documentation visit http://cech.uc.edu/itservices/cech-guides/filr-cech-cloud.html
Appendix A-2 – CECHCloud Web Interface User Guide

Using CECHCloud from a Web Browser

About CECHCloud

CECHCloud is a service provided by the CECH Technology Support Services department that is powered by Novell’s Filr. This service gives you access to all the files stored securely on your \textit{U, Q, and R: drives} on most devices without having to connect to the UC network using the VPN.

The follow guide is a basic introduction to some of the key features of the CECHCloud service when accessing it through a web browser such as Internet Explorer, Safari, Google Chrome, or Mozilla Firefox. For additional information, you can click your name in the top right corner of any page to access more detailed help documentation.

For additional technical support please contact the CECH Technology Support Services Department.

Accessing CECHCloud

\textbf{NOTE: CECHCloud can be accessed from any web browser, on or off campus without the VPN.}

1. Launch a web browser, such as Google Chrome, Mozilla Firefox, or Internet Explorer.
2. Go to the following URL: \url{https://cechcloud.uc.edu}.
3. Enter your \textit{UC Central Login User Name and Password} and click \textbf{Sign In}.  

\begin{figure}[h]
  \centering
  \includegraphics[width=0.5\textwidth]{cechcloud.png}
  \caption{CECHCloud User Interface}
  \end{figure}
4. When you first launch CECHCloud, you will see the My Files page. This is where you can access files and folders on your U: Drive.

Using CECHCloud to View, Edit, and Share Files and Folders

Navigating CECHCloud

Accessing Different Storage locations

To navigate to other files and folders, such as the Q: and R: Drives, use the icons at the top.
• The **My Files** icon takes you to your *U: Drive*.

• The **Shared with Me** icon shows files that others have shared with you.

• The **Shared by Me** icon shows files you have shared with others.

• The **Net Folder** icon shows you files on the *Q: and R: drives*.

When you select **Net Folders**, you will see the network shared drives (*Q: drives*) of the departments you have access to.

If you normally use the *R: Drive*, this will look familiar. If you only use the *Q: Drive*, simply click your department’s folder name and you will see the files in the *Q: Drive*.

**Browsing Folders and Files**

1. To browse the file system, click the name of the folder you would like to open.
2. This will display the contents of the folder selected. From here you can browse further, create a new folder, add, view, share, and download files for editing.

3. To navigate back up the folders, you can click the up arrow next to the Current Folder name or click the folder name in the Folder Path at the top of the page.

**NOTE:** By default, only 25 items are displayed per page. If there are more than 25 items in a folder, use the Page Navigation arrows at the bottom of the page to view more items.

**Working with Files and Folders**

**Sharing Files and Folders**
Understanding Access Rights

Access rights are how you define which users are allowed to do what with the files and folders that you share with them. You can grant users the following rights when you share files and folders with them:

- **Viewer:** Users can view individual files that are shared with them, or all files within the folder that is shared with them.
- **Editor:** Users can view and modify individual files that are shared with them, or all files within the folder that is shared with them.
- **Contributor:** (Applies only when sharing folders) Users can create files in the folder, rename existing files, modify files, move files, and delete files inside the folder. Users cannot perform actions on the folder itself.

Creating a Shared Files and Folders

NOTE: Folder Sharing is currently limited to My Files *(U: Drive)*. You can share individual or multiple files from the *Q: and R: Drives*, but not entire folders. This function will be made available after a future update.

1. Navigate to the folder that contains the files that you want to share.
2. Select the files you want to share by checking the box next to the file, then click **Share**.

Or

Click the drop-down arrow next to the file that you want to share, then click **Share**.

The **Share** dialog box is displayed.
3. To share with another **CECH Faculty or Staff member**, begin typing their name or username into the **Share with** field. Click the name of the person when it appears in the drop down list.

4. Select the **Share Rights** to give to the user and click **OK**.

5. To share with an **external user (anyone that is not CECH Faculty or Staff)**, enter their e-mail address in the **Share with** field and click the plus sign (+).

6. Select the **Share Rights** to give to the user and click **OK**.

**NOTE:** By default, Shared Rights do not expire. It is recommended to place an expiration time on Shared Rights, especially when sharing with external users.

7. To set an expiration on the Share Rights, click **Never** under the **Expires** column. Choose to have the share expire on a certain date by selecting **on** and choosing a date or after a period of time by selecting **after** and setting the number of days. Click **Ok**.
8. To add a note to the share, click **none** under the **Note** column. Enter text into the **Edit Note** field. Click **Ok**.

9. To ensure that a notification e-mail is sent to the people you are sharing with, check the box next to **Notify**.
10. Click **Ok**.

**Modifying or Removing a Share**
1. Click the **Share by Me** icon from the top of any page.

2. Check the box next to the file(s) that you want to modify and then click **Share**.

   Or

   Click the drop-down arrow next to the file that you want to modify, then click **Share**.

   ![Shared by Me](image)

   The **Share** dialog is displayed.

   ![Share dialog](image)

3. To modify the **Share Access Right** click the down arrow under the **Access** column and choose the new rights.

4. To modify the expiration click the drop down arrow under the **Expires** column and select a new expiration time.

5. To remove the user from the share, click the icon in the table next to the person you want to remove. To completely remove the share, remove all users from the share.

   ![Adding Folders](image)

   **Adding Folders**

   1. To create a new folder, click the **New Folder** button.
2. Enter the name of the folder in the *Folder Name* window that appears, click **OK**

![New Folder](image)

Adding Files

Too add a file or folders click the **Add Files** button.

![Add Files](image)

(Firefox, Chrome, or Safari browsers)
A blue overlay will appear. You can simply drag files into this area, and they will be uploaded or you can click **Browse** to find the files on the local file system.
NOTE: If the file already exists, a File Conflict window will appear. If you choose to Overwrite Files, it will replace the current file on the server.

Or

Choose Cancel Copying, rename the file and try adding it again.

(Internet Explorer)

A Java Applet window will appear. You may receive the following security warning, if so, click Run.
Once the Java Applet Loads, the Add Files window will appear.

Drag files that you want to upload into the folder icon in the window.

NOTE: If the file already exists, a File Already Exists window will appear. If you choose to Yes, it will replace the current file on the server.

Or

Choose No, rename the file and try adding it again.
Editing a File

There are two ways to edit a file. You can download a file to your workstation to edit it or you can edit the file in place on the CECHCloud site.

Editing Files with Edit-in-Place

**NOTE:** *Edit-in-Place* feature only allows you to edit certain document types if the specific application is installed on the workstation. For example, to edit a .doc file, you must have Microsoft Word. Currently the only applications that support *Edit-in-Place* are Microsoft Office on Windows and Open Office/LibreOffice on both Windows and Mac OSX.

1. Navigate to the location of the file you want to edit.
2. Click the drop-down arrow next to the file that you want to edit, then click View Details.
3. Click **Edit This File**.

This will open the file editor application specified for the file type. (For example, .doc file will open in Microsoft Word, and .ppt file will be open in Microsoft Power Point).

4. You may receive the following Java security warning, Click Run.

5. When the Application opens, proceed to edit the document.

**NOTE:** If you are using Microsoft Office, it may open the file in **Protected View**. If you see the following banner at the top of the page, click **Enable Editing**.

6. Once you have finished editing the file, save your changes, then exit the editing application.

   The changes will be now available on the file in CECHCloud.
Downloading and Editing a File

1. Navigate to and open the folder that contains the file you want to edit.
2. Click the name of the file you want to edit.
3. Save the file to your workstation with the original name.

NOTE: Firefox and Chrome require Popups to be enabled for *.uc.edu.

Or for Internet Explorer, choose Save or Save as to select a location.
4. Edit the file and save it.

5. In CECHCloud, navigate to the folder where the file is located, then click Add Files.

6. Follow the instructions on Adding Files to upload the file back to the CECHCloud server.

Viewing Files in Read-Only Mode

If you want to quickly view a file, you can view it in HTML format in your Web Browser.

NOTE: Some file types cannot be viewed in HTML format such as PNG, JPG, GIF, and PDF. Also, if files are too large, the request times out after 30 seconds and the file is not displayed.

View the File

1. Navigate to the file that you want to view.
2. Click the drop-down arrow next to the file that you want to view, then click View HTML.
3. The file will open in another window as a Read-Only file.
Appendix A-3 – CECHCloud Desktop User Guide

Using the Filr Desktop Sync Application with CECHCloud

Windows Version

About CECHCloud

CECHCloud is a service provided by the CECH Technology Support Services department that is powered by Novell’s Filr. This service gives you access to all the files stored securely on your U:, Q:, and R: drives from the “Cloud” on just about any device without having to connect with the VPN.

The following guide shows how to install and use the Novell Filr Desktop Sync application to sync your network storage with your home computer or laptop. This application will create a copy of each file on your local computer that will automatically sync back to the server. Any changes made to files on your local computer will be changed on the server.

NOTE: Please do not install this application on your office computer, instead continue to access files directly through the U:, Q:, and R: Drives.

Downloading and Installing the Filr Application

5. Launch a web browser, such as Google Chrome, Mozilla Firefox, or Internet Explorer.
7. Enter your UC Central Login User Name and Password and click Sign In.

8. Click on your name in the upper right hand corner of the page.
9. From the popup window, Click Download Filr Desktop App.
10. Click the link for the **Windows x86 Client** or **Windows x64 Client** depending on whether you have a 32-bit or 64-bit operating system. 

   Click here to determine if you are running a 32-bit or 64-bit version of Windows.

11. Choose to **Save** the file.

12. Once the download is complete, browse to where you saved the file and double click it to start the install.

13. If prompted by a security warning, click **Run**.

14. If *Microsoft.NET Framework 4* is not currently installed, the application will prompt you to install it.

15. Review the **License Agreement** and click **Accept**.
16. Once *Microsoft.NET* is installed, click **Next** to start the Filr installation.

17. Review the *License Agreement*. Check the box next to "*I accept the terms in the License Agreement*", then click **Next**.

18. Click **Next** to accept the default installation location.
19. Click **Install** to begin the installation.

20. Once the install completes, click **Finish**.

### Configuring Novell Filr for the First Time

Now that the client is installed, the client must be configured for the first time.

1. When the “Welcome to Novell Filr” window appears, click **Start**.
2. In the Account Information screen, enter https://cechcloud.uc.edu for the Server URL.
3. Enter your UC Central Login User Name and Password, then click Next.

4. On the Synchronized Folders screen you can add and remove folders that need to be synchronized.

By default, the My Files (which is the U: Drive) and Shared with Me Folders are selected. The size of every file is shown to the right of each folder. This is the amount of space that will be taken up on your local hard drive.

Adding Synchronized Folders

1. To add folders from the Q: and R: Drives, click Add.

IMPORTANT NOTE: Do not choose to sync the entire department share folders (Q: Drive). This would take up most, if not all of your local hard drive. ONLY SELECT THE FOLDERS THAT YOU NEED REGULAR ACCESS TO.
2. Select **Net Folders** from, then browse to the folder you would like to sync by clicking the folder name to open each folder.

3. Once you have located the folder you would like to sync, click the arrow next to the folder name. It will change into a check mark indicating it has been selected. Continue until you have selected all the folders you would like to sync and click **OK**.

![Net Folders Screen](image)

4. In the *Synchronized Folder* screen, the folders you have added will appear. In a moment, it will calculate the size.

![Synchronized Folders Screen](image)

**NOTE:** If the size is colored red, this means the folder is very large. Make sure you have enough space on your local hard drive. Also, it may take a while for the initial sync to occur.

**TIP:** To add or remove folders after the initial setup, right click on the *Filr Icon* in the *System Tray* located in the bottom right corner of your desktop, then select “*Open Filr Console*”.

![Filr Icon](image)
The *Console* window will open, select “Synchronized Folders” to Add or Remove Folders.

Deleting Synchronized Folders

1. To stop a folder from being synced, highlight the folder and click **Remove**.

2. The folder is removed and the contents will be deleted from your system upon the subsequent sync.

**NOTE:** If a folder is very large, it may be a good idea to remove it and then add smaller sub-folders if possible.
5. Once you have selected the folders you would like to sync, click next.
6. If you have selected one or more larger folders, the following warning will appear. Click Continue once you have verified that you have enough free disk space.

![Disk Space Warning]

7. On the General Settings page, ensure the Start Novell Filr at login box is checked and click Next.

![General Settings]

8. Confirm the settings at the Summary Screen, then click Finish.
9. Filr will now begin syncing your files. This may take some time depending on the size of the files being synced.

Using the Filr Desktop Sync Application

Viewing Synced Files on the Computer

Synced files are stored by default to the C:\Users\<username>\Filr\ directory on your local machine. If you open “Computer” from the Start menu or Desktop icon, you will see Novell Filr has been automatically added to your Favorites and a Novell Filr Library has be created.
Either of these short cuts will take you to the Filr Directory. From there you can browse your U: Drive under “My Files” or Folders from the Q: and R: Drives under “Net Folders”.

From here you can browse, open, edit, and save files like any other files on your computer. Any changes made will sync back to the server and overwrite the existing file.

**Sharing Files from the Desktop Application**

To share a files, right click on the file or folder and select **Share**.
Another window will open, login with your UC Central Login Username and Password.

The Share dialog box is displayed.

11. To share with another CECH Faculty or Staff member, begin typing their name or username into the Share with field. Click the name of the person when it appears in the drop down list.

12. Select the Share Rights to give to the user and click OK.
13. To share with an external user (anyone who is not CECH Faculty or Staff), enter their e-mail address in the Share with field and click the plus sign \( + \).

14. Select the Share Rights to give to the user and click OK.

NOTE: By default, Shared Rights do not expire. It is recommended to place an expiration on Shared Rights, especially when sharing with external users.

15. To set an expiration on the Share Rights, click Never under the Expires column. Choose to have the share expire on a certain date by selecting On and choosing a date or after a period of time by selecting After and setting entering the number of days. Click Ok.

16. To add a note to the share, click none under the Note column. Enter text into the Edit Note field. Click Ok.
17. To ensure that a notification e-mail is sent to the people you are sharing with, check the box next to Notify.

18. Click Ok.
Appendix A-4 – CECHCloud iOS User Guide

Using Novell Filr App to Access CECHCloud on an iPad or iPhone

About CECHCloud

CECHCloud is a service provided by the CECH Technology Support Services department that is powered by Novell’s Filr. This service gives you access to all the files stored securely on your U:, Q:, and R: drives on most devices without having to connect to the UC network with the VPN.

The following guide is a basic introduction to some of the key features of the CECHCloud service when accessing it through the Novell Filr App on an iPad or iPhone. Before starting this guide, make sure you go to https://cechcloud.uc.edu from a web browser and sign in, if you have not already done so.

Installing and Configuring the Novell Filr App

Open the App Store and Search for “Novell Filr”.

Tap the Cloud Icon to install

Once the app is installed, click Open.
Enter your **UC Central Login User Name** for **User ID**.

Enter your password

Enter **cechcloud.uc.edu** for **Server IP Address**

Tap **Sign In**

This will bring up the Filr App Main Screen
Navigating the Filr App

From the main screen you will see recently viewed documents under the three main headers:

**My Files** is files located in your *U: Drive*.

**Share with Me** are files other users have shared with you.

**Net Folders** contain files from the *Q: and R: drives* you have access to.
On the bottom of the main screen there are Five Options:

- **What’s New** – Shows newly added or edited files.
- **Shared by Me** – Shows files you have shared with others.
- **Downloads** – Files you have downloaded to your device
- **Search** – Allows you to search for Files with key words.
- **Settings** – Change application settings.

Tap the icon for the location you would like to browse

This will bring up a list of Folders and Files for that location.
Simply tap a folder to view the contents of that folder.

Tap a file name to bring up a preview of that file.
Tap the back arrow in the top left corner to move up a level.

Tap the Home Icon to return to the main screen.

To move to another file location, use the icons at the bottom left of the page to navigate between My Files, Shared With Me, Net Folders, and Downloads.

**Working with Files**

**Viewing Files**

When you have located the file you would like to view, simply tap the file to open a preview of the file.
NOTE: Not all file types can be viewed from the app. Microsoft Office Files, Adobe PDF, and Images can all be viewed.

To expand the preview size, tap the arrow at the top of the preview window.

Open a file with another application

NOTE: To edit a file, you must have an app installed that can edit the file type.

To open the file with another application, tap the actions icon.

Choose Open in.
This will bring up a list of available apps that can open this file type, tap the icon of the app you would like to use. The file will then be opened by that application.

Make any edits with the app and then save. Use the Action icon and choose Open In.

Select Open in Novell Filr.
Select the destination of the original file or another location where you would like to save the new file.

![Destination selection interface](image)

Tap **Upload**.

If saving in the same location, Filr will prompt you to confirm that you want to overwrite the original file.

![Confirmation dialog](image)

Tap **Yes**.

### Downloading a file to work with offline

If you would like to save a file to your device, so that you can access it when not connected to the internet, select the file you would like to download.

Tap the **download** icon at the top of the preview window.
The file will be downloaded to the device’s local memory.

To view or edit the downloaded files, go to the download location from either the file browsing window or the main screen.

From here, you can view or open the file in another application, even when offline.

Sharing files

Browse to the file you would like to share.

Tap the **Arrow** next to the file name.

Tap the **Share** button.
Begin typing the name of the person you want to share the file with, then select their name from the list or type in the e-mail address of an external user.

Highlight each user to set Access rights and Expiration times.

Tap **Access** to select from **Viewer** or **Editor**.

Tap **Expires** and choose an expiration time.

Enter a **Note** if desired.

Tap **Save** to save the share. An e-mail will be sent to all share users notifying them of the shared item.
To remove a share, tap the arrow next to the file name,

Tap the **Share** button.

Tap **Remove** next to the user name.
Tap *Save*.

<table>
<thead>
<tr>
<th>Access</th>
<th>Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expires</td>
<td>Never</td>
</tr>
</tbody>
</table>

**externaluser@emailprovider.com**

**Remove**
Appendix A-5 – CECHCloud Android User Guide

Using Novell Filr App to Access CECHCloud on an Android Device

About CECHCloud

CECHCloud is a service provided by the CECH Technology Support Services department that is powered by Novell’s Filr. This service gives you access to all the files stored securely on your U:, Q:, and R: drives from the “Cloud” on just about any device without having to connect with the VPN.

The follow guide is a basic introduction to some of the key features of the CECHCloud service when accessing it through the Novell Filr App on an Android device. Before starting this guide, make sure you go to https://cechcloud.uc.edu from a web browser and sign in, if you have not already done so.

Installing and Configuring the Novell Filr App

1. Open the Google Play store and Search for “Novell Filr”.

![App Store Screenshot](image-url)
2. Tap Install.

3. Tap Accept to allow the App permissions.

4. Once the installed, tap Open or locate and tap the Novell Filr icon from the home screen.
5. Review the License Agreement and tap Accept.

6. Enter your UC Central Login User Name and Password. Enter cechcloud.uc.edu for Server IP Address. Tap Sign In.
Navigating the Filr App

On the main screen you will see recently viewed documents under the three main headers:

- **My Files** are files located in your **U: Drive**.
- **Share with Me** are files other users have shared with you.
- **Net Folders** contain files from the **Q: and R: drives** you have access to.

On the bottom of the main screen there are Five Options:

- **What’s New** – Shows newly added or edited files.
- **Shared by Me** – Shows files you have shared with others.
- **Downloads** – Files you have downloaded to your device
- **Search** – Allows you to search for Files with keywords.
- **Settings** – Change application settings.

1. Tap the icon for the location you would like to browse.
   This will bring up a list of Folders and Files for that location.
2. Tap a folder to view the contents of that folder
3. Tap a file name to select the file.
4. Tap “Generate online preview” to view the document in the preview screen.
5. Tap the *Up to <folder>* to move back up a level.

6. To move to another file location, use the icons at the top of the page to navigate between *My Files, Shared With Me, Net Folders, and Downloads*.

![Up to Senior Project](image)

**Viewing Files**

When you have located the file you would like to view, simply tap the file to open a preview of the file.

**NOTE:** Not all file types can be viewed from the app. Microsoft Office files, Adobe PDF, and Images can all be viewed.

1. To expand the preview size, tap the arrow at the top of the preview window.

Using CechCloud from a Web Browser

About CechCloud
Accessing CechCloud

Open a file with another application
NOTE: To edit a file, you must have an app installed that can edit the file type.

1. To open the file with another application, tap the actions icon.

2. The file will download to the device. The “Complete action using” window will appear, showing compatible apps that can open the file. Select the App you would like to use and tap either Always or Just Once.

3. After you make any edits with the App, save the changes. Use the Send feature of the App (this is generally found under the app menu icon.) The “Choose an action” menu appears, select Novell Filr.

4. The Filr App will display the Upload screen. Tap Browse to choose the location to save the file.
5. Choose the location you want to save the file, then tap **Select**.

6. If saving in the same location as the original file, you will be prompted to overwrite the file.

| A file with the selected name already exists. Do you want to continue and overwrite it? |
|------------------|------------------|
| **No**            | **Yes**          |

**NOTE:** If you click Yes, this will overwrite the original file on the server. To avoid this, click No; save the file with a different name, and then upload it again.
Downloading a file to work with offline

If you would like to save a file to your device so that you can access it when not connected to the internet, select the file you would like to download.

1. Tap the download icon at the top of the preview window.

2. The file will be downloaded to the device's local memory.
3. To view or edit downloaded files, go to the download location from either the file browsing window or the main screen.

4. From here you can view or open the file in another application, even when offline.

Sharing files

1. To share a file, browse to the file you would like to share.
2. Tap the Arrow next to the file name.
3. Tap the Share button.
4. Begin typing the name or the person you want to share with, then select their name from the list.

Or

Type in the e-mail address of an external user.

5. Highlight each user to set Access rights and Expiration times.
6. Tap Access to select from Viewer or Editor.
7. Tap Expires and choose an expiration time.
8. Enter a Note if desired.
9. Tap Save to save the share. An e-mail will be sent to all share users notifying them of the shared item.

1. To remove a share, tap the arrow next to the file name,
2. Tap the Share button.
3. Tap **Remove** next to the user name.

4. Tap **Save**.
Filr Update Process

1. Download the latest Virtual Appliances from the Novell Customer Center and extract to the management workstation.

2. Bring down Filr VA’s first (cechcloud1 and cechcloud2), then the search appliances (filrsearch1 and filrsearch2), then the MySQL appliance (filrsql) last.

3. Follow these instructions for the VA’s in this order, FilrSQL, Filesearch1&2, Filrcechcloud1&2.

4. In the VSphere Client click File>Deploy OVF Template and select the .ovf file for the new VA.

5. In the Name Field, rename the Filr Appliance to <servername>v<version number>. I.e., FilrCechcloud1v1.0.1.

6. Accept the default disk format and click finish. **Do not power one yet.**

7. Edit settings on the new virtual machine to match the Hardware Configuration in the Servers Table.

8. On the Hardware Tab, click add, and select Hard Disk

9. Choose Use an existing virtual disk

10. Browse the Disk File Path to the datastore location for the Independent Disk in the Servers Table.

11. In the Virtual Device Node section, select SCSI (1:0) from the drop down

12. In the Mode section, select Independent, select Persistent. Finish.
13. Go to the Old version of this VA and edit settings to remove the second independent disk. Double check to make sure this machine is powered off.


15. Accept the License Agreement.

16. Specify the same configuration information as the original install. See Server Table for IP and hostnames.

17. The data storage location (/vastorage) should be the same, Hard Disk, sbd1. Click Next.

18. (For Filr Appliance, select Remote NFS for the /vashare storage location. NFS server hostname is basin.cech.uc.edu and remote directory is /vashare).

19. Click Configure.

20. In a browser, navigate to https://ip_address:9443

21. Log into the appliance. Make sure all settings are set the way they were.

22. (Conditional) If you are updating the search appliance:

   a. Click the Filr Search Appliance Configuration icon.

23. The Search Settings page is displayed.

   a. Ensure that all of the settings are set to your desired specifications.

24. (Conditional) If you are updating the database appliance:
a. Click the *phpMyAdmin* icon.

b. Verify that the database is populated.

25. (Conditional) If you are updating the **Filr appliance**:

   a. Click the *Filr Server Configuration* icon.

26. The Filr Configuration Wizard is displayed.

   a. Click *Finish* to update the appliance.

27. Depending on the size of your database, the update process can take over an hour to complete. For example, a 14 GB database might take 30 minutes to complete, and a 30 GB database might take an hour or more.

28. Repeat these steps for each Appliance.

29. Once the Filr Appliances are running, go into YAST through the console window and open port 8009 on the firewall.

30. The search appliances will need to be re-indexed.
Appendix B-1 – Airwatch User BYOD Guide

Enroll Employee-Owned iPad into Airwatch

What you will need:

- iPad 2 or newer with iOS 7 or greater
- University of Cincinnati Central Login (6+2)
- Wireless internet connection
- Apple ID

What is Airwatch?

Airwatch is a Mobile Device Management (MDM) system that provides CECH Faculty, Staff, and the Technology Support Services department with easier setup, security, and management of mobile devices. Some of the many features added by enrolling in Airwatch include:

- Automatic configuration of settings such as e-mail and VPN
- Self Service portal for security features such as locking or wiping a device
- Device encryption to protect sensitive data
- Custom CECH App store with easy access to popular public apps
- Access to Apple’s Volume Purchase Program (VPP) for college purchased apps

How to enroll your iPad

1. Ensure your iPad is connected to a wireless network.
2. Open the Safari browser and navigate to https://www.Airwatch.uc.edu/enroll
3. When the page loads, enter the Group ID “CECH”
4. Tap Next
5. Enter your Central Login Username and Password

6. Tap Next
7. From the drop down menu, select Employee-Owned then tap next.

8. Airwatch will begin to install profiles on the device. You must tap install and accept these profiles.
9. If you have not already signed into your iTunes account, you will be prompted to sign in. If you do not already have an account, you can create one now.

10. After all the profiles have installed, you can close Safari.

**How to set up your iPad after enrollment**

1. A new app will appear on your iPad that opens the CECH App Store.

2. The CECH App Store contains popular UC related public apps. Just tap “Free” to install. The “Purchased” tab contains apps that have been purchased through Apple’s VPP that you can install.
3. After selecting your apps, you will be prompted to install them.

4. Securewireless, e-mail, and VPN (Junos Pulse app required) will all be configured for you. You will need to enter your password when prompted.
How to remove your device from Airwatch

If you have enrolled your personal device in Airwatch, you may remove it at any time. However, any apps that were installed or settings that were configured through Airwatch will be removed as well. Public apps may be reinstalled through the iTunes App Store.

1. Open the Settings app and select General from the left hand side, then select Profiles from the right.

2. Select the “MDM Profile/V_2” profile
3. Tap Remove. This will remove all profiles installed by Airwatch

How to manage your device through the web self-service portal

1. From any web browser, go to https://www.airwatch.uc.edu/MyDevice
2. Enter the Group ID “CECH” and your Central Login username and password
Appendix B-2 Technician’s Guide – Department Owned Single User Device

Set up a College Purchased iPad for a Single User

Initial Setup

1. Connect the iPad to the Apple Configurator
2. Give the iPad the name <username>’s iPad
3. Make sure Supervision is turned off
4. Select “When update is available” for Update iOS
5. Check “Erase before installing”
6. Choose as the Restore image

7. Click Prepare
8. Apple Configurator will restore the backup image to the device. This may take several minutes.

User Setup
NOTE: The following instructions steps should be done with the user.

1. Go to Settings>Wi-Fi and have the user log into Securewireless

2. Open the Safari Browser and navigate to https://www.Airwatch.uc.edu

3. Enter the Group ID “CECHDO”
4. Tap Next
5. Have the user log in with their Central Login credentials
6. Tap Next

7. Select Corporate – Dedicated from the Device Ownership drop down
8. Enter the ED Tag number for the device in the Asset Number field
9. Install the Enrollment Profile and accept all prompts

10. Once the enrollment is complete, it will prompt to sign into iTunes with their Apple ID

   **NOTE:** If the user does not have an Apple ID, one can be created now

11. The user will then be prompted to create a passcode

   **NOTE:** This is required and must be at least 4 characters long

12. Open Settings, the user will be prompted for their “Exchange Active Sync” password

   **NOTE:** This is their e-mail password. Once entered, their e-mail is set up.
13. In Settings, go to General > Profiles > Web Clip URL. Remove this profile.

14. Users can then install apps from the CECH App Catalog or Apple App Store

   NOTE: If they are assigned a purchased app, it will be found in the “Purchased” tab in the CECH app Catalog.
Setting up and Enrolling Loaner iPads

Supervise the device with Apple Configurator – This can be done in groups

1. Use the Name CECH iPad
2. Check “Number sequentially starting at 1”
3. Turn Supervision to “On”
4. Enter Organizational Info
5. Check “Allow Devices to connect to other Macs”
6. Choose “CECH iPad Shared” for the backup to restore
7. Select Enrollment and Wi-Fi Profiles

8. Select Airwatch MDM Agent from Apps
9. Click Prepare

**Enrollment and setup**

1. Once the device is prepared, open Settings
2. Go to iTunes & App Store
3. Enter Apple ID for the iPad Group (i.e., Teched10@ucmail.uc.edu for iPads 1-10)
4. Turn on Automatic Updates for Apps and Updates
5. Open the Enroll App to configure the Airwatch Agent

6. When the Agent is finished configuring, the log in screen will appear

7. Go to the Airwatch Management portal at https://www.Airwatch.uc.edu
8. Log in with ad.uc.edu\<username> and CLS password
9. Go to Menu> Dashboard
10. Find the device(s) that you just enrolled. They will be in the “College of Ed, CJ, HS” Organization Group
11. Click the name of the device
12. This brings up the details on the device. Once again click on the name of the device

13. This takes you to the device details page
14. Go to Admin > Change Organization Group
15. Change the Location to “Staged Devices – CECH default” and Save

16. In a moment, the device will receive new profiles based on this group. It will lock the device into single app mode for the Airwatch agent. Make sure you cannot use the home button.

The device is now staged for multi user deployment.

Checking out a device

**NOTE:** Any faculty, staff member, or student may sign out a device.

1. Log into the Airwatch agent with the users CLS credentials
2. Accept any notification prompts
3. The agent status page will appear
4. Hit the home button to get to the home screen
5. It will prompt you to enter a passcode. This passcode can be anything, but must be at least 4 characters.

6. Any apps associated to the user account will automatically install

**NOTE:** The iPad is originally connected to a hidden secured network that may not be available outside of classrooms. The user may log into Securewireless or any other wireless network. These settings will be removed on check in.

**Checking in a device**

**NOTE:** When finished with the device, it is important to log out of the device. This will remove any personal data, history, apps, or settings you have put on the device and prepares it for the next user.

1. Open the Airwatch agent
2. Click Log out

3. It will prompt you to make sure you want to log out, tap yes

Once you are logged out, the device will be once again locked at the login screen