CYSE 368 Internship Final Paper

Joey Whtimore
Professor Duvall
Old Dominion University
Network and Application Services
Fall 2024

Table Of Contents

Overview

During my time at ODU I had many rolls and many had to have to wear and it helped me develop to become a better cyber security professional and a better IT professional. This position helped me grow and learn how to manage my priorities and time and deal with customers from different demographics. this position also helped me to figure out how to turn technical language into more casual language. My time as a student lead really showed me how to use my Tier 1 customer support capabilities, leadership duties and technical expertise to another level to get the job done. As a tier one customer support professional I officially managed customer inquiries while adhering to our SLA (Service level agreement) .I also address technical challenges promptly ensuring smooth operation for on campus systems. My leadership duties really help me develop as a leader and help me learn how to keep everyone in on what I was thinking and how I would handle certain situations.I acted as a deputy to Senior Management and stepped in for higher level decision-making required. I had to lead weekly stand-ups to discuss project statuses and performance metrics and sharing it aligns with our goals we have set. I also supervised the team of students maintaining clarity of priorities and expectations for the week. As I develop my skills I realized I have gotten a lot of technical expertise for on-site support for Konica Minolta bizhub multifunction printers. I also provide technical support for cbord V100, v1000 ,and v200 door access control hubs and ensure they function seamlessly across campus. I also programmed key devices like v1000 and v200c board hubs to ensure reliable campus wide door access control. As I developed further in the position I eventually made a transition to a network technician. this network technician position is what I took this class for and I was able to learn how to handle tier 2 support and be a better leader among students. I also added more critical tasks like server maintenance and testing. As far as my tier 2 support and leadership I was promoted to handle complex tier two issues ensuring escalated adherence for escalated customer inquiries and these would be for VPs, project managers, and other important people around campus. I continued leadership by managing weekly stand-ups and leading a team of student employees. I also acted as a critical support figure for senior managers. As far as the server maintenance and testing went I conducted patching testing and troubleshooting for printer and biometric reader servers. I also focused on ensuring minimal downtime for essential University infrastructure. I also helped assist with the critical infrastructure of the University such as our electronic key box systems were up to date with patching and testing. I also provided training for the employees that were confused on how the workflow would be for these new devices.

Multi Function Printers(MFP)

My responsibilities at ODU regarding the MFP (Mulit Function Printers) would range from basic networking troubleshooting to doing basic maintenance. When I first began working with mfps I was known to just do basic troubleshoots regarding changing the toner or replacing the paper. whenever I went out and did these requests they were mundane rudimentary task that required little to no technical knowledge of the machine. I started advancing and learning the trouble codes of the mfps. I noticed that there was a certain pattern with a lot of the machines when they would run out of paper they would give the same trouble code or if the paper was filled up too high in the printer tray they would give a certain error code. With this constant learning and striving for greatness I eventually figured out that I could do more with printers and started asking more technical questions regarding them.

Tier 1 level support

The tier 1 level support for the printers would include me replacing the toner for them and replacing the paper. I noticed that most paper that would be in the MFPs were 8/11 ½ and would not cause jams like some of the thicker paper being used like cardstock. The paper would also have to be stored in a room temperature area with little to no humidity to make sure that it is still copy safe and would not damage the printer. The paper kept in these high humidity environments can cause the printer to jam more frequently and cause parts in the feeder tray to misfeed. With delivering the paper I was also tasked with delivering the paper to their respective locations and allowing people campus wide to print. This was an integral part of the job because all the printer paper requests went to us directly and there was no third part associated with this process. Another responsibility That I would like to harp on is tier 1 support for mfps is the management and delivery of toner supplies. the toner supplies that we would have were all directly through us and we had to manage it in our own Warehouse system. We had to make sure that we had a surplus of toners to provide to all of our satellite locations and are in House main campus locations. with this in mind it was an integral part of our job that we had to go out and make sure we gave all of our patrons the correct toner so we did not have to double back and make sure that we gave them the right toner.

Tier 2 level support

Tier 2 level support for the mfp service that I provide would actually be a more technical service that I would provide and would be more critical to the continuity of the campus if this tier 2 level support was not available. These services would include but not limited to

networking,management of supplies,vendor communication, and distribution of talent. When talking about the networking side of things in MFP services we have our own system of how we manage each device on our network so we have a load balance to our servers. We separate all our MFPs from student printers to admin or VIP printers. We make sure to separate these printers because we want multiple points of failure in our network and to ensure the health of our servers so they are not overloaded with requests. We also have a system where we would make use of VLAN's on our network to host our printer services on. We use a specific port number to regulate our printing services that I will not disclose for confidentiality purposes. In some areas we use a cloud based approach to manage the MFP traffic back to our servers but only in select locations we have tested this. Oftentimes I would have to change the VLAN on the specific port to the correct one and it allows us to run the traffic for the specific MFP protocols we have in place. This is essential for us to have correct ports because the protocols used are not only specific to that port but to the printers campus wide. Using the correct ports and protocols brings me to the deployment part of tier two support which can be categorized in management of supplies. When managing the supplies of MFPs or managing the MFP's in general we document almost everything we do so we can keep an accurate count of all our expenses and so we know how much we need to order when we make orders for toner supplies and paper. We use a third party application called Pharos to deploy and manage our MFPs we have on campus. Pharos allows us to manage users and charge users by making queries on our cbord server we have set up. When deploying MFP's my knowledge on Pharos has to be sufficient enough to also network the printer back to the correct server by assigning the Ip address using DHCP and route the traffic correctly so there is no mistranslation between printer and server. We use a third party to help manage our supplies as well and it is Konica Minolta. We use their web applications to not only order more supplies for the printers on campus but to also make service calls or service requests for each individual printer that has a valid contract with our vendor. When making service calls we have to communicate with their active technical assigned the call and this brings me to my next point of vendor communication. When dealing with the MFP's on campus we have to communicate what we need back and forth with the vendor and give them insight on some of the issues we have with the printers at the selected locations. We also serve as impromptu guides for the technicians at Konica Minolta because they may not know all of the ins and outs of the campus and would require proper guidance to get around. When I am tasked with the distribution of talent I go to the students and ask them to handle a tier 1 level request for me and I figure out which one to ask based on their interest and previous knowledge or skills from the requirements of the specific request. Since we handle almost 350+ printers on campus daily it is important for me to figure out which student is able to go the specific location and manage which issue the student could then handle based on the severity of the request. We aso now started using mobile credential scanners to help us use our phone to scan and pay for print jobs that we need down by the machine. As a tier 2 technician I make sure that the readers that we use are up to date with the correct configurations and that the reader itself is not damaged and routinely inspected for on campus use. A key issue we found with these readers is that they

would rest or damage the configuration on the card due to the printer losing power. We came up with a solution to let the reader have a backup power source when we configure the reader so it has proper wattage when we start setting it up initially.

Electronic Access Control (EAC)

Electronic access control is a critical task for our team and is usually handled by tier 2 or tier 3 technicians that can go out and handle these requests. These issue include user management,access control, and physical troubleshooting for the 200+ electronic doors on campus. Since ODU transferring most of the key access to be electronically controlled we have been very busy when it comes to user management as we have 15,000+ users actively using our system daily and more to come soon with our ongoing EVMS integration. When we manage users we use an application called cbord which is essentially the backbone of our campus and hosts multiple services from printing, electronic access control, and meal plans. Anything that requires the user to use their card or mobile credential device we have to use cbord. Managing the users using our cbord service allows us to track and audit the usage of their cards for what doors they use. We frequently collaborate with the card center to ensure the continuity of card usage. As I developed my troubleshooting skills I learned that some problems can be handled through the card center rather than having me directly involved such as the replacement of cards and troubleshooting the issues with some cards not being able to be scanned. Working with the card center also showed me that I had to be able to dim down the technical language and speak it in everyday speech when discussing a problem. Being able to bring myself down to explain technical issues in a non technical fashion was a valuable skill that ultimately allowed me to take my customer service skills to the next level and really understand the customer’s problem rather than throw jargon at them. This skill came full circle when I started to assists with the mobile credential integration for the whole campus. When assisting with the mobile credential launch I was part of the tier 1 and tier 2 support level for the launch. During this time I also assisted heavily when creating the FAQ that is used on the website to this day.

`

- How do I verify my Apple Watch device version?
- How do I verify and/or update my Apple Watch software version?
- On how many devices can I use my student ID in the Apple Wallet?
- Where do I go for questions about my Apple ID and/ or iCloud?
- How do I change or recover my Apple ID password?
- What happens if I lose my iPhone or Apple Watch? If I find it afterwards?
- What happens if I get a new iPhone or Apple Watch?
- Why can't I double-tap the home button or side button when my iPhone is locked to see my Monarch ID Card balances in Apple Pay?
- If I have a passcode on my phone, will I have to enter it every time?
- Can I use my Apple Student ID if my iPhone has a dead battery?
- Can I use my Monarch ID Card in Apple Wallet without cellular signal?
- Does it cost anything?
- Do I have to have a photo?
- I have my iPhone and Apple Watch set up. What if I lose one of them?

- What are the eligibility requirements to use Monarch ID Card via Google Pay Wallet?
- What are the device requirements?
- Can I use my Monarch ID Card without unlocking my phone?
- Can I use Google Pay Monarch ID Card ID if my phone has a dead battery?
- How many devices can I use my Monarch ID Card within Google Pay?
- What happens if I lose my Android device? If I find it afterward?
- Can I use my Monarch ID Card in Google Pay without a cellular signal?
- Does having my Monarch ID Card in Google Pay cost anything?
- Is a Monarch ID Card photo required?
- What is required to authenticate into the GET Mobile app?
- What if I have a passcode on my phone, will I have to enter it every time?
- How do I use my Monarch ID Card or Flex Points on my account from my phone?
- Will it work with off-campus merchants? (If applicable)
- I downloaded the Get App and have the Mobile ID but it's not scanning for me?

Some of the more advanced projects that I have worked on that include EAC would be the physical installation of the various readers around campus. Over at ITS we work with mt15,mt11,mt20,ad300, and ad400 card reader devices. These readers are produced by a vendor we work with closely called Schalge. Schalge produces these readers and gives us the readers with the most up to date firmware and it is up to us on how we want to integrate these into our environment. These readers use v100 and v1000 access control boards that go in our network closet and have to be properly configured before we put them in our environment as well. When we set up these readers we also assist with facilities management once in a blue moon to set up the strike relays to the doors since we handle the configuration and wiring of the v100 and v100 devices. When setting up a new door location we have to assign a new IP address to the controller and set it up using the cbord setup wizard gui. Then once the IP address is set up we then make sure we have our configuration cards for our new readers and go and install them on the selected location. Installing a new door location can take anywhere between 1 hour to 4 hours depending on the environment. We have been trying to have a uniform setup routine when it comes to installing new door locations but we ended up having to change up the wiring in some locations. We heavily cooperate with another department, Wiring and Infrastructure because they help us run the cables to all the IoT devices we control and many more campus wide. We usually have to consult with our Wiring and Infrastructure department when making plans to install new door controllers or readers so that they can make sure the cable is run seamlessly through the wall,conduit, or floor in some cases. After we set up the controller and reader our server side configurations have to be at our standards including VLAN setup, Switch Port management and node bounces on our server side as well. When dealing with the server side of EAC we have to bounce the nodes we have set up in our environment. This is essentially a shut and a no shut command that resets the network connection between the server and the web client that we interact with on a day to day basis. Here is a detailed view of the cbord web client we used called csgold.

I have my profile attached and this shows the address,phone number,and other card information we use to troubleshoot patron's accounts. This application is called csgold. This is where almost all tier 2 and tier 3 troubleshooting work is done. We can set door schedules, open and close doors remotely, and even set doors to be open or closed from our application.

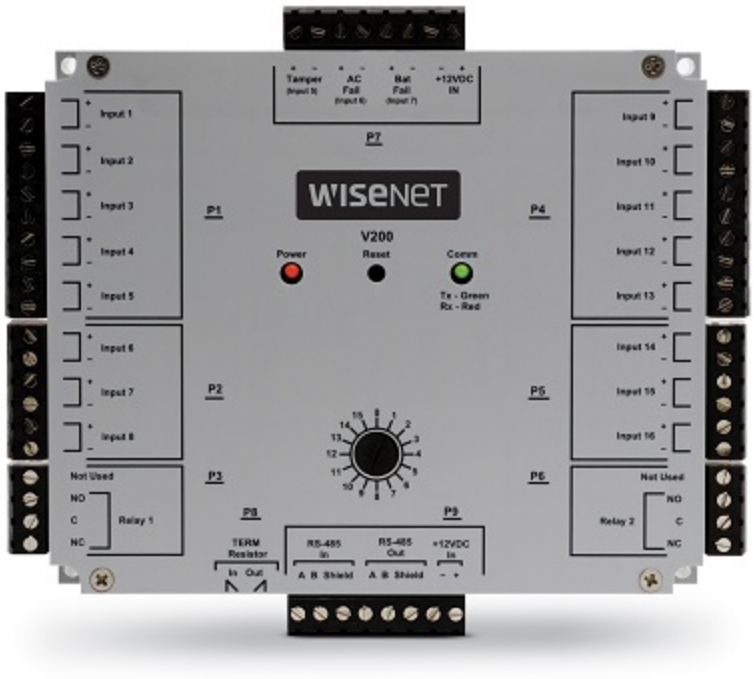
Patch Management

A responsibility that I want to incooproate that was used heavily in the development of my skills is the patch management process of my job. Every quarter I have to go out and make sure that all the newly patched devices are up and operational. when patches come out it is important that we are not caught off guard and address any problems before and after the Patch to make sure that any patches that are made to the systems are not pre-existing or happen because of the patch. Normally our patch management system that is ran by our magnificent server group will not cause any harm to our systems a lot of the problems that I have seen from the patches normally happen before the patch and is fixed by the patch. when I come out every quarter on Sundays the the systems that are patched are our mfp systems or servers our biometric finger scanning servers and normally but at times our csgold servers. All I do to make sure that our patches are sufficient is tested individualized systems so normally in an mfp patch test I will run a test print, and a biometric patch test I will scan my fingerprint to make sure that is logged on our server side, and finally and a door test I will make sure that my car is being logged and the doors are up and online.

Panic Buttons

As ODU becomes a more technically sound university as the years go on there is a great concentration on safety and security of the faculty,staff,and students on a daily basis. ITS has developed a way to safeguard and ease the minds of patrons at the university by implementing a panic buttons. With these panic buttons we allow faculty and staff to be able to silently alert authorities of threats to their safety as needed. The panic buttons send alerts to our public safety department and ODU Police Department's dispatch phone line operators. We also get alerts at ITS to handle the clearing of the alerts on our side. It is an important duty that we are responsible of as it can very well be the reason someone could get help or not. Public safety does quarterly check ups on theses buttons to make sure that they are in a working order.

This image above shows on of the panic buttons we have in our environments. Whenwe look at how the panic buttons are configured physically we attach them to the v200 which is another door controller similar to the v100 and v1000 series.



The v200 controller has to have power to make sure that the connection stays closed. When the panic button is initially set up we have to have a closed connection that is applied to the wiring. When we have the connections opened the panic button sends a signal back to the controller the controller then sends signals back to the server causing the alarm to go off. We tend to forget the physical labor aspect when it comes to mounting the panic buttons. We normally have to consult and plan our installs with the executive assistant of the department to determine the location of the panic button to go under the desk. We do this to make sure no false alarm are happening because we have had panic buttons that were not planned with the department and they accidentally press it because of the unfavorable location.

Camera Management

Managing cameras at ODU gives us a wide and diverse range of responsibilities for us to fulfill.When doing this task I had to incorporate my networking skills,disperse talent between myself and the students available.I also did some impromptu training for the configuration and troubleshooting of the cameras that we have on cams. From basic chores like a VLAN change or lens cleaning to more difficult difficulties like replacing a complete camera, the problems with our camera systems can range greatly in degree. Luckily, we avoided major hardware updates in readiness for the game, concentrating instead on networking changes and handling cleaning requirements. The cameras might get worn over time from environmental exposure. For example, strong storms or extended rain could cause cameras to turn off or suffer from lens grit or water marks, therefore degrading their image quality. Sometimes extended outage sets up further network problems. Should a particular camera be offline for more than a week, the network team may stop Power over Ethernet (PoE) on the related port or assign the VLAN for that port. These situations needed cooperation with the team in network engineering to reactivate ports and give impacted cameras back capability. I gave top emphasis to making sure our high-priority cameras those covering the stadium and university exteriors were running and delivering crisp photos. Given their necessary surveillance and monitoring powers, these cameras are rather important during events. I led some of the student team members to these important camera points often roofs and the tops of parking garages handle any problems. Equipped with microfiber towels and Windex cleaning agents, we gently cleaned the camera lenses to guarantee best view. I used these cleaning chores to teach the students on spotting high-priority cameras and grasping their importance for general campus security and event planning. Emphasizing the value of both fast troubleshooting and preventative maintenance was crucial to help to reduce downtime. For instance, I showed how to monitor the network dashboard for the condition of every camera and gave instances of how a problem, like a dirty lens, may drastically compromise stream quality. I then went over the actions required to rectify these issues such as physical cleaning, reactivating PoE, or networking repairs. Our efforts had clearly noticeable and significant effects. The display made evident the difference between a blocked or offline camera and a fully working one, therefore stressing the need of preventive maintenance. Comparisons between before and after provided a striking graphic depiction of the difference, highlighting how even seemingly little chores like lens cleaning may greatly increase the general performance of the system. Especially in readiness for important events like game days, this experience strengthened the need for collaboration, practical training, and meticulous attention to detail in preserving a strong and dependable monitoring system.

Facility Management Technical Support

When attacking the intricacies of the facility management support role at ODU its there is a lot of hats I have to wear in order to get the job done in an efficient manner. I normally will oversee the use of key boxes and the management of the keys for the key boxes and I also managed the users inside our own separate key box system hosted by our vendor gfms. when working with gfms they have been nothing but helpful and supportive as I transferred over to this new role and their Consultants always welcome our questions with open arms to make sure that we are always efficient whenever we use their key box systems. the key box systems that we have in place now are supposed to be temporary until we start using another vendor called key track. I work in tandem with a Facilities Management Department to make sure that when patrons go to get their fingerprint scanned for the key box system they have all of the required credentials. when using the key box we have to assign their pin and scan their fingerprint for them to access the key box. these instructions are normally unclear and the key box can be somewhat daunting to new users as the key box does not explicitly tell you how to use it. that is why I was a part of a team that created a guide for end users to use the key box. this guide has not been implemented yet but since I made it I will place it below.

Keybox Key Check In and Check Out How-To Guide:

Please start by creating an ITS Help Desk or ServiceNow ticket requesting access to a key box (757-683-3189,. itshelp@odu.edu, or https://oduprod.service-now.com/sp). In your ticket, please give us your first and last name, UIN, MIDAS, and ODU email address.

Checking Out Keys:

1. Make sure that the keybox says "PIN" before you type in your credentials:

2. Type in you pin number (usually your UIN)
3. The screen will say next "FP Ready":

4. Place your finger on the scanner and wait for it to say "FP Verified":

5. Then lift the latch then pull it back to open the keybox door,
6. When you scan your finger in, the lights on the top of the key should flash green showing that you can turn the key left and check it out:

7. Turn the key to the left to make the key horizontal to pull and check out the key.

Returning Keys:

1. Make sure that the key is turned VERTICALLY and not HOIZONTALLY for it to be registered as checked in,
2. This key has been turned vertically and has been returned successfully to the key box:

3. This key is still been logged as checked out by a user (the key must be turned horizontal be be checked in):

For help: 757-683-3189, or itshelp@odu.edu

Using this guide, users should have a seamless and easier experience using these key boxes. When configuring accounts I normally will get a request directly from email from housing or any other department saying that the specific user needs to access the key box. When I get these requests I will have to RDP into the key box server and make sure that I do an addition to the sequel database table that our key box prod server runs on. After I make sure that all the account information is correct I make sure that I execute my command and I will see the account on our web page.