SR16491534 ##3H23H4772H##

Service Request

Interface Security
170 Chastain Meadows Ct
Kennesaw, GA 30144

CTN3080033 SR16491534 Rev 0

ISS Helpdesk #: See guide

SR Type: Smashburger - Network Conversion

Dispatch Type: (TM)

Reference Number: SMSH01481 End User Reference: I0456572

Date: 11/10/2020 Window: 09:00 to 09:00 EST Expected Duration: 682 PO#: ISS_501996

Site Contact: MOD Phone: (914) 777-3370 Alt. Phone:
Company: SMASHBURGER #1481- Address: 448 MAMARONECK AVE. 448 MAMARONECK AVE.
City: MAMARONECK State: NY Zip: 10543

TAC: 404.536.4721 (AT&T) | 678.332.8358 (Verizon) | 678.460.2530 (Other)

SR DETAILS

If Hard ETA needed, please specify ETA date: 11/6/2020 **If Hard ETA needed, please specify ETA time**: 08:00
Interface PM email: Angela.Stringer@interfacesys.com

DESCRIPTION OF WORK

Smashburger - Network Conversion: Call TAC for Details

SR CHECKLIST

1. Upon arrival, log on with Onepath (via myESP or calling +1.800.493.0016).
2. Refer to the attached install guide for specific installation instructions.
3. Contact the appropriate customer helpdesk by chat or phone.
4. Verify all installation areas are clean and that you properly dispose of all trash.
5. Submit deliverables via myESP.
6. If any deliverables or the signed SR are still outstanding, submit via myESP or ESP within 24 hours.

To be completed by the Field Engineer (FE): 43398

Call Result: [ ] Successful [ ] Incomplete

Incomplete Reason:

Materials Used:

Description	Qty

Required for all calls:

Time at Log-on: _____:_____ EST

Time at Log-off: _____:_____ EST

Customer Heldesk Rep. Name: _____

Customer Call Closure Code: _____

Onepath TAC Rep. Name: _____

Onepath TAC Closure Code: _____

Installed Equipment:

Make/Model	Serial Number

RMA Equipment:

Make/Model	Serial Number

FE Initials | End-User Name (Please Print) | Title | End-User Signature | Date

SR16491534 ##3H23H4772H##

Description: Complete a network and VoIP conversion at a Smashburger location. The primary installation activities will consist of: 1) locating an acceptable installation location for an Interface broadband cabinet, 2) testing Cradlepoint backup service, 3) apply power to the cabinet and commission the equipment, 4) completing the cabinet installation, 5) connect the customers networking devices (see the provided port mapping of existing connections) and the WAPs, 6) perform a full system test on backup, 7) verify broadband service and bring the site online with the primary connection, 8) convert voice and 9) cleanup and closure.
Required Tools: Standard Telco + Label Maker
Required Materials: Standard Telco
Required Skills: Telecom & Networking
RMA Handling: Do NOT take any existing devices offsite. Box up the old Smashburger router, switch, and any existing patch cables that are no longer used and leave with the MOD for return. If there are defective or unused Interface provided parts, write down the make, model and serial number on the equipment return form. Neatly and securely place the parts in a box (NOT the same box as the old Smashburger equipment) and seal the box. Advise the MOD that FedEx will arrive onsite in 1-5 business days to retrieve the package. FedEx will bring the label, so all the MOD has to do is hand the box to the FedEx rep.
FE Overage Threshold: 2 hours

Notes:: Supplier = Verizon - FIOS
PLease Ship the Equipment to arrive on or Before 11/5/20. Please schedule the FE for the install on 11/6/20 at 8AM,

---

Equipment:

ONEPATH The easier way to get hard things done™

March 25, 2020

Re: COVID 19 - City/County/State/Federal Orders

To whom it may concern:

Please be informed that the bearer of this letter is subcontracted by Onepath Systems, LLC, a communications and information technology company providing essential critical infrastructure as outlined by the Cybersecurity and Infrastructure Security Agency (CISA); an agency operating under the Department of Homeland Security.

Under CISA guidelines, these workers must be able to travel to and gain access to infrastructure facilities and offices during curfews and restricted travel periods. CISA identifies the following list as essential to continued critical infrastructure:

Communications:

• Maintenance of communications infrastructure- including privately owned and maintained communication systems- supported by technicians, operators, call-centers, wireline and wireless providers, cable service providers, satellite operations, undersea cable landing stations, Internet Exchange Points, and manufacturers and distributors of communications equipment

• Workers who support radio, television, and media service, including, but not limited to front line news reporters, studio, and technicians for newsgathering and reporting • Workers at Independent System Operators and Regional Transmission Organizations, and Network Operations staff, engineers and/or technicians to manage the network or operate facilities

• Engineers, technicians and associated personnel responsible for infrastructure construction and restoration, including contractors for construction and engineering of fiber optic cables

• Installation, maintenance and repair technicians that establish, support or repair service as needed

• Central office personnel to maintain and operate central office, data centers, and other network office facilities

• Customer service and support staff, including managed and professional services as well as remote providers of support to transitioning employees to set up and maintain home offices, who interface with customers to manage or support service environments and security issues, including payroll, billing, fraud, and troubleshooting

• Dispatchers involved with service repair and restoration

Information Technology:

• Workers who support command centers, including, but not limited to Network Operations Command Center, Broadcast Operations Control Center and Security Operations Command Center

• Data center operators, including system administrators, HVAC & electrical engineers, security personnel, IT managers, data transfer solutions engineers, software and hardware engineers, and database administrators

• Client service centers, field engineers, and other technicians supporting critical infrastructure, as well as manufacturers and supply chain vendors that provide hardware and software, and information technology equipment (to include microelectronics and semiconductors) for critical infrastructure

• Workers responding to cyber incidents involving critical infrastructure, including medical facilities, SLTT governments and federal facilities, energy and utilities, and banks and financial institutions, and other critical infrastructure categories and personnel

• Workers supporting the provision of essential global, national and local infrastructure for computing services (incl. cloud computing services), business infrastructure, web-based services, and critical manufacturing

• Workers supporting communications systems and information technology used by law enforcement, public safety, medical, energy and other critical industries

• Support required for continuity of services, including janitorial/cleaning personnel

All persons performing critical operations have been instructed to comply with hygiene and social distancing requirements as established by the Centers for Disease Control and Prevention.

Please do not hesitate to contact me should you have any questions regarding this letter or our operations.

Sincerely,

D. Christopher Lewis

D. Christopher Lewis

President and Corporate Safety Officer, Onepath

Cybersecurity & Infrastructure Security Agency
Washington, DC 20528

May 27, 2020

To Whom It May Concern:

The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issues this letter to facilitate work in the interest of homeland security by Communications Sector workers identified in the CISA Essential Critical Infrastructure Workers advisory guidance, dated May 19, 2020.[1] CISA requests any courtesy that can be extended to essential workers involved in communications infrastructure operations, maintenance and restoration **in response to the COVID-19 Pandemic and any other regional disasters (e.g., hurricanes, tornadoes, wildfires, earthquakes) that may occur during any COVID-19 response phase**.

CISA developed the **Essential Critical Infrastructure Workers** advisory guidance identifying workers that conduct a range of operations and services deemed essential to continued critical infrastructure viability. This list is intended to support State, local, tribal, and territorial officials' decision-making as they work to protect their communities, while ensuring continuity of functions critical to public health and safety, as well as economic and national security.

In developing this advisory guidance, CISA determined that essential workers need access to jobsites based on our judgment that organizations affiliated with the Communications Sector engage in activity that could reasonably be included within the scope of "critical infrastructure" as that term is defined in law; and critical communications infrastructure is necessary to ensure first responder, emergency responder, and 911 communications capabilities are functional during this response and recovery period. In the course of providing this support, identified Essential Critical Infrastructure Workers in the Communications Sector should be able to travel to and access necessary critical infrastructure facilities in order to prevent loss of service or restore critical communications services.

CISA greatly appreciates your cooperation. For any questions or concerns related to this request, please contact the CISA at 888-282-0870 or CISAservicedesk@cisa.dhs.gov.

Sincerely,

Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency (CISA)

[1] "Guidance on the Essential Critical Infrastructure Workforce," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/publication/guidance-essential-critical-infrastructure-workforce.

Certificate of Completion and Acceptance

Your system was installed by trained technicians to meet the high standards of our quality assurance program.

Customer Name:_____ Account #:_____

Installation Address: _____

City:_____ State:_____ Zip: _____

Confirmation #: _____ Branch #: _____

Type of System:
❒ Secure Broadband ❒ Access Control ❒ Managed Access ❒ Structured Cabling
❒ Digital Voice ❒ Fire/Life Safety ❒ Camera Surveillance ❒ Supervisory System
❒ Intrusion ❒ Interactive Video ❒ Other:_____

Monitoring: ❒ Not Monitored ❒ Monitored by UL Listed Central Station ❒ Remote Video Monitoring
If Monitored, type of transmission link: ❒ Phone Lines ❒ Radio/Cellular/Broadband Backup

UL Listing *(if required):* _____ Type of Listing: _____ Certificate #: _____

I have received and understand the following:

❒ System Training & Operation ❒ Emergency Contact List ❒ Referral Program Details
❒ System User's Guides ❒ Backup Options ❒ Alarm Permit Information
❒ Monitoring Procedures ❒ Keys to Panel ❒ Other: _____

Was installation completed in accordance with the Agreement?	❒ Yes	❒ No
Were decals and/or signs installed to your satisfaction?	❒ Yes	❒ No
Was the installation completed to your satisfaction?	❒ Yes	❒ No
Are camera image views to your satisfaction? ❒ N/A	❒ Yes	❒ No
Was technician wearing protective shoe coverings when entering your location? *(Residential Only)*	❒ Yes	❒ No
Was the work area left clean and in order?	❒ Yes	❒ No
Were you properly instructed on the operation of the system?	❒ Yes	❒ No
Were our installers knowledgeable and helpful?	❒ Yes	❒ No
Did we meet your expectations?	❒ Yes	❒ No
Would you refer us to a friend or associate?	❒ Yes	❒ No
Are phones working properly?	❒ Yes	❒ No

Comments: _____

_____

_____

The customer named below hereby certifies that all equipment referred to in the Agreement, Schedule of Protection or Addendum has been delivered, is fully installed and it is in good operating order. Customer unconditionally accepts the equipment and authorizes commencement of billing in accordance with the Agreement.

_____ _____
Customer or Company Representative Signature *Date*

_____ _____
Customer or Company Representative Name Printed *Title*

Interface
The Leader in Secure Managed Cloud Services

and other Interface Companies
Interface Systems
ACO 7245, 6860 Lic. # 469046

Interface Security Systems - Equipment Return Form

Instructions: Please fill out this form for defective/unused **NEW** devices (anything that was included in the cabinet shipment that was non-functional that needs to be returned). The LEGACY devices you boxed up will remain onsite with the MOD and should not be included in the FedEx shipment. You will be responsible for completing the following for defective/unused **NEW** devices:

1. Record the make, model and serial number of each return device in the EQUIPMENT INFORMATION section below.
2. Record the equipment type in the EQUIPMENT INFORMATION section below. "Defective" refers to an out-of-box failure for Interface supplied equipment. "Unused" refers to gear that was shipped to site by Interface but was not used (this should be *extremely* rare).
3. Securely pack the return CPE in the box the new equipment came in and upload a photo of the equipment in the box before sealing to myESP.
4. Seal the box and explain to the Manager on Duty (MOD) that you are leaving the equipment onsite for a FedEx call tag dispatch. Advise them FedEx will be onsite in 1-5 business day with a label to retrieve the equipment. All the MOD has to do is hand them the box.
5. Fill out the RETURN CONFIRMATION section and ask the MOD to sign the equipment return form to indicate acceptance and understanding of the equipment return process.

LEGACY EQUIPMENT INFORMATION – TO BE LEFT WITH THE MOD

Make/Model	Serial/ID No.	Equipment Type (circle one)
Router:		**Decommissioned Legacy Gear (LEFT WITH MOD)**
Switch:		**Decommissioned Legacy Gear (LEFT WITH MOD)**

DEFECTIVE NEW EQUIPMENT INFORMATION – TO FOLLOW THE FEDEX CALL TAG PROCESS DESCRIBED ABOVE

Make/Model	Serial/ID No.	Equipment Type (circle one)
		Defective NEW Gear | Unused NEW Gear
		Defective NEW Gear | Unused NEW Gear
		Defective NEW Gear | Unused NEW Gear
		Defective NEW Gear | Unused NEW Gear
		Defective NEW Gear | Unused NEW Gear
		Defective NEW Gear | Unused NEW Gear
		Defective NEW Gear | Unused NEW Gear

RETURN CONFIRMATION

Today's Date:	
SR Number	
Installer Name	
Installer Signature	

MOD Name	
MOD Signature	

INSTALLATION TEST RESULTS
RECORD YOUR TEST RESULTS ON THIS PAGE AND FAX IT BACK WITH YOUR CLOSE-OUT PAPERWORK

1. Store Number: _____ Store Address: _____
2. Temporary VoIP telephone number: _____
3. Broadband information:
    a. PPPoE:
        i. Username: _____
        ii. Password: _____
    b. Static:
        i. IP address: _____ (If a range, use the 2nd useable)
        ii. Subnet Mask: _____
        iii. Gateway: _____
4. Primary Broadband type: DSL Cable T1 Granite Grid: _____
5. Primary broadband circuit ID: _____
6. Primary broadband test results (***From Fortigate DMZ port***):

	Ping Time	**Download**	**Upload**
Test 1			
Test 2			
Test 3			

7. 4G RSRP: _____ 4G RSRQ: _____
8. Back-up broadband results:

	Ping Time	**Download**	**Upload**
Test 1			
Test 2			
Test 3			

9. TTU close out Date and time: _____ Close Code: _____

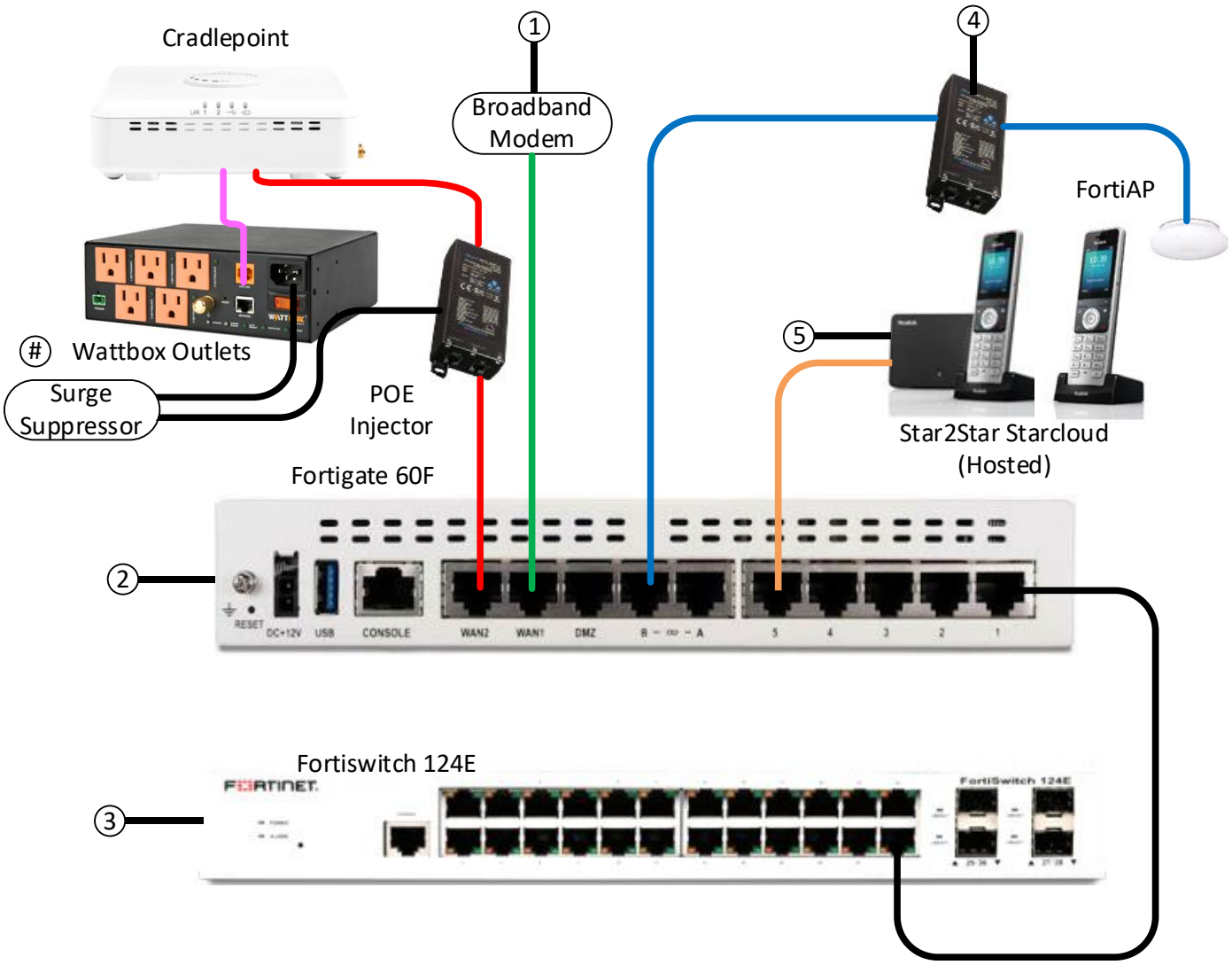
10. Issues Encountered:_____
_____
_____
_____

OVERVIEW: You will be converting this location form the current network to a new ISS provided Fortigate system. The new system is self-contained in a network cabinet, replacing the shelf current mounted design.

You will be:

- Prep work:
  - Determining the location where the cabinet will be installed.
  - Identifying and labeling connections to the existing system.
  - Unpacking the new cabinet, place it on the floor (on foam pieces) and power it up.
- Converting the network
  - Contacting ISS TTU to verify the new Fortinet router is on-line and run activation scripts.
  - Mounting the cabinet and connecting customers equipment.
  - Verifying network operations.
  - Removing the old network equipment.
  - Replacing the existing wireless access point.
- Installing new telephones
  - Verifying operation of new cordless phones
  - Installing charging bases

Contents



EQUIPMENT LAYOUT AND CONNECTIONS POST CONVERSION

REQUIRED TOOLS AND MATERIALS:

- Laptop with wired network and serial connection
- Ladder
- Label maker and supplies
- Fish tape
- Cell phone with camera
- Miscellaneous mounting hardware
- Hand tools
  - Flashlight
  - Punch Down Tool
  - Crimp Tool
  - Pliers
  - Screwdriver (flat and Phillips)
  - #1 Phillip screwdriver
  - Toner
  - Lineman's Set (Butt Set)
  - Wire loom wrap
  - Level

SUPPLIED EQUIPMENT:

- New ISS cabinet, containing:
  - Fortigate router
  - Fortiswitch switch
  - Cradlepoint CBA850
  - Wattbox
  - POE Injectors
- Two 12-Port CAT5e RJ45 passthrough patch panels.
- Twenty 14' Patch cords – 11 black, 1 gray, 10 white. (See instructions for color use)
- Surge suppressor and child-proof outlet covers
- FortiAP wireless access point (WAP)
- Yealink cordless phone base with two handsets and charging bases.

REVISION CONTROL:

- Previous version: 0.2.1 (10/14/2020)
- Current version 0.2.2 (10/15/2020)
  - Phones should be pre-registered.
  - Changed phone from Grandstream to Yealink in parts list.

PHONE NUMBERS:

- **ISS TTU: 1-800-554-9875, Option 1, Option 1**: THIS NUMBER SHOULD BE USED FOR NETWORK AND TELEPHONE SYSTEM PROGRAMMING AND TESTING.

1. **MILESTONE 1: ARRIVE ON-SITE, VERIFY EQUIPMENT AND DETERMINE INSTALLATION LOCATION.**
    a. Check in
        i. Arrive on site and check in
            1. Before entering the premise, contact TTU to obtain the broadband type and PPPoE / static IP information and temporary VoIP telephone number. Record this on the "Installation Test Results Page".
        ii. Enter the premise and introduce yourself as a representative of Interface Systems and explain that you are there to install the new network and digital voice system.
        iii. Ask for the Site Contact or Manager on Duty (MOD)
            1. Present your photo ID to the Site Contact and re-identify yourself as a representative of Interface Systems.
            2. The Site contact may require a passphrase prior to allowing you to perform any work on their site. The passphrase will be on your SR coversheet.
        iv. Quickly review with the MOD what work you will be performing, what areas you will be working in, and where you will require access to.
        v. Verify with the Site Contact that all the Point of Sales (POS) terminals and telephones are functioning correctly. If any are not, record this in the "Comments / Issues encountered" section of the "Installation Test Results Page" and your SR notes. Explain to the Site contact that our operations are not intended to fix any of these issues, and they need to follow their normal procedure to have their system repaired.
        vi. Ask the MOD to show you the locations for the following:
            1. Existing network equipment
            2. Any equipment broadband carrier's technician installed during last visit.
            3. Location of all telephones.
        vii. Ask MOD for the best location to use as a small staging area to place tools, equipment, and ladders, while working in the store.
    b. Verify the equipment
        i. Ask the MOD for the location of all equipment they received for this installation.
        ii. Make sure all equipment is present and in good shape.
        iii. If there are any issues, contact the ISS PM.
    c. Charge the cordless phones.
        i. Unpack the cordless phones and install the supplied battery in each one.
        ii. Unpack the charging bases, plug them in to power outlets and place the phones on the charging bases. Verify they are charging.

d. Work with the MOD to determine a location to install the new ISS cabinet.
    i. The ISS Network cabinet must be installed within 10' of the existing network equipment to allow installation of the interconnecting cables to the new cabinet.
    ii. The new cabinet will require a wall space that is a minimum of 21 inches wide by 30 inches high, including space for the cellular antennas.
    iii. An additional 3 inches will be required to the left to allow the cabinet door to open.
    iv. The cabinet must be located within 6 feet of an unswitched power outlet.
    v. The cabinet must be located where the existing network and phone cables can neatly reach. If this is not possible, new cables will be needed prior to installing the new cabinet.

NOTE: If there is enough space, the new ISS equipment cabinet will be installed in place of the existing network equipment and shelf. The existing equipment will stay in place while the new ISS equipment is prepared.

e. **COMPLETE MILESTONE 1.**
    i. Take photographs of:
        1. All equipment shipped to the site for your installation
        2. Space provided / available for the cabinet.

2. MILESTONE 2: CABLING

a. Identify ***and label*** all cables form the existing equipment.
    i. Do not unplug any cables
    ii. Existing router
        1. WAN – Label as "**Old WAN**"
        2. Wireless Access Point – Label as "**WAP**"
    iii. Existing switch:
        1. Printers – Label as "**Print 1**" through "**Print 4**"
        2. Payment Terminals – Label as "**POS / EMV 1**" through "**POS / EMV 3**"
        3. Kitchen Controllers – Label as "**Kitchen 1**" through "**Kitchen 3**"
        4. Point of Sales Servers – Label as "**POS Server Internal**" through "**POS Server External**"
        5. Thermostat – Label as "**Thermostat**"
        6. Menu Boards – Label as "**Menu 1**" through "**Menu 5**"
        7. Manager's Workstation – Label as "**Manager PC**"
        8. Digital Video Recorder – Label as "**DVR**"
        9. Music Player – label as "**Music**"

b. **COMPLETE MILESTONE 2.**
    i. Take photographs of:
        1. All labeled cables
        2. Existing equipment as currently installed / connected.

3. MILESTONE 3: PREPARE THE NEW SYSTEM

a. Prep

i. Unbox the ISS equipment cabinet and place it on the floor in front of the existing equipment, on the packing foam from the box.

ii. You will need to flatten the foam by folding the “ears” back into the frame of the foam. See picture below.

iii. Open the cabinet (combination is 3-2-3) and inspect the contents. Make sure that:
   1. All equipment is securely in place
   2. All cables are connected
   3. All power cords are securely seated

iv. Connect the AP
   1. Unbox the FortiAP wireless access point
   2. Plug the blue “WAP” CAT5e cable to the FortiAP.
   3. Place the FortiAP on top of the cabinet.

v. Attach the 2 Cradlepoint ‘paddle’ antennas to the SMA connectors on the top of the door.

vi. Unbox the surge suppressor and connect it to an outlet
   1. Route the power cords through the bottom of the cabinet
   2. Plug the “BKUP CP” in to one of the outlets on the surge suppressor.
   3. DO NOT plug the “WB” in until the cell signal / Internet connection has been verified.
   4. Apply power to the surge suppressor with the rocker switch.

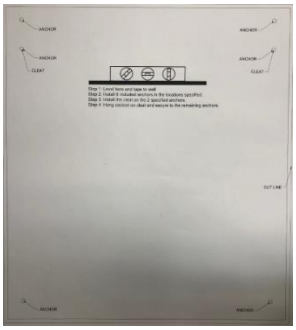
b. Verify 4g connectivity
    i. Verify the Cradlepoint POE injector is plugged into the surge suppressor and the Cradlepoint is powered on.
    ii. Verify the cellular signal.
        1. Disconnect the pink CAT5e cable from the Wattbox and connect it to your laptop and obtain a new IP address. Record your gateway address here: ____._____._____._____
            a. Verify the Cradlepoint is connected (Green antenna LED) and has at least 2 bars.
            b. Navigate to http://www.ipchicken.com.
                i. Record the WAN IP address it shows you here: ____._____._____._____
            c. Perform a speed test on the Cradlepoint
                i. Open a web browser and verify that you can navigate to multiple websites. Make sure you are not loading cached websites.
                ii. Navigate to a speed test site like www.speedtest.net and perform three separate speed tests. Record them on the "Installation Test Results Page"
            d. Contact ISS TTU to have the cellular signal checked. They may disable the SIM in slot 1 to switch over to the alternate carrier – this takes several minutes. ISS TTU will provide the values to write in the Installation Test Results page. They will be looking for the best signal based on this chart:

Technology	LTE		HSPA+ and EVDO
	RSRP (dBm)	RSRQ (dB)	EC/Io (dB)
Excellent	**> -84**	**> -5**	**> -2**
Good	**-85 to -102**	**-9 to -5**	**-2 to -5**
Fair	**-103 to -111**	**-12 to -9**	**-6 to -10**
Poor	**< -111**	**< -12**	**< -10**

    iii. If these minimums cannot be obtained:
        1. Relocate the Cradlepoint to where the RSRP and the RSRQ are better. (See Appendix B)
        2. A higher gain antenna may be required. (See Appendix C)
    iv. If you cannot connect to the internet, contact ISS TTU.
    v. Reconnect the pink cable to the Wattbox.
    vi. **Plug the "WATTBOX" power cord in to one of the outlets on the surge suppressor.**
    vii. **Turn the Wattbox power switch on**.
    viii. Verify all other equipment in the cabinet powers on, **including the Wireless access point**.
c. Have the system scripted
    i. Contact ISS TTU to have the Fortigate activation scripts run on this location.
    ii. While the scripts are running, route the cables from the Fortinet switch out one of the cable holes in the cabinet and to the existing router.
d. **COMPLETE MILESTONE 3**
    i. Take photographs of:
        1. Cabinet on the floor, connected the Internet through the Cradlepoint.

4. MILESTONE 4 MOUNT THE NEW SYSTEM AND CONVERT

a. Mount the cabinet
   i. The ISS Network cabinet must be installed within 10’ of the existing network equipment to allow installation of the interconnecting cables to the new cabinet.
   ii. Disconnect the FortiAP221 WAP.
   iii. Place the included template on the wall, so the top is 6’ off the ground.



   iv. Install the included anchors at the 6 locations indicated on the template.
   v. Mount the included cleat as indicated on the template.
   vi. Carefully hang the cabinet on the cleat.
      1. Open the door on the cabinet, carefully lift it, keeping all cables safe and align the mounting holes with the anchors.
      2. Secure the cabinet to the wall with the included hardware.

b. Mount the DK-8FF outlet strip / surge suppressor to the wall below the cabinet.

c. Install the patch panels
   i. The patch panels will be the physical interface between the existing wiring and the new ISS network switch / cabinet. They will mount in a location that all the existing network cabling can neatly plug into the front of the patch panels.
   ii. Mount the patch panels.
      1. Un-snap the patch panels from their mounting brackets.
      2. Neatly mount the brackets to the wall, straight and level. The two patch panels can be mounted either next to each other or vertically stacked, depending on the room available. Leave enough room between the brackets so the path panels can easily snap on and off.
   iii. Install the new ISS supplied 14-foot patch cords to the rear of the patch panel.
      1. See chart on nest page for patch panel port usage.
      2. Connect the black cables to ports 1 – 11 on the rear of the 1st patch panel. Label the other end of the patch cable for its use (See chart on next page).
      3. Connect the gray cable to port 12. Label this as “POS External NIC”.
      4. Connect the white cables to ports 1 – 10 on the 2nd patch panel. Label the other end of the patch cable for its use (See chart on next page).
      5. Snap the patch panels to their mounting brackets.
      6. Label each port on the front of the patch panel for its use.
      7. Neatly run these cables to the new ISS cabinet, tie wrapping and anchoring at regular intervals. Land them on the Fortiswitch ports listed in the table on the nest page.

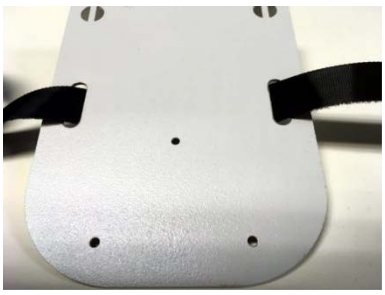
d. Connect the store to the new router
    i. Convert the store:
        1. Work with the MOD. Explain that this process will cause a temporary service interruption.
        2. You will move the cables for the first patch panel first – this is all the point-of sales and back-of-house systems. Once this is moved over, work with the MOD to verify system operation.
            a. One at a time, move the cables from the existing network equipment to the front of the first (POS) patch panel, connecting to the ports as you previously labelled the cables.

Switch Port	Device	Patch Panel	Cable Color	VLAN	Cable
1	Printer	1-1	Black	11	Print 1
2	Printer	1-2	Black	11	Print 2
3	Printer	1-3	Black	11	Print 3
4	Printer	1-4	Black	11	Print 4
5	Payment Terminal	1-5	Black	11	POS / EMV 1
6	Payment Terminal	1-6	Black	11	POS / EMV 2
7	Payment Terminal	1-7	Black	11	POS / EMV 3
8	Kitchen Controller	1-8	Black	11	Kitchen 1
9	Kitchen Controller	1-9	Black	11	Kitchen 2
10	Kitchen Controller	1-10	Black	11	Kitchen 3
11	POS Server	1-11	Black	11	POS ***Internal*** NIC
12	POS Server	1-12	Gray	10	POS ***External*** NIC
13	Thermostat	2-1	White	40	Thermostat 1
14	UNUSED	N/A	N/A	N/A	N/A
15	Menu Board	2-2	White	40	Menu 1
16	Menu Board	2-3	White	40	Menu 2
17	Menu Board	2-4	White	40	Menu 3
18	Menu Board	2-5	White	40	Menu 4
19	Menu Board	2-6	White	40	Menu 5
20	Manager's PC	2-7	White	40	Manager's PC
21	DVR	2-8	White	40	DVR
22	N/A	N/A	N/A	40	N/A
23	Music Player	2-9	White	40	Music
24	Uplink to Router	2-10	Black	TRUNK	Do not change please

   b. Work with the MOD to verify operation of all systems you connected to the new router, including:
      i. Point of Sales operation
      ii. Payment card reader operation
      iii. If there are any issues, contact ISS TTU for support.
3. Once sales operations have been verified, move the other equipment to the 2nd patch panel.
   a. Work with the MOD to verify operation of all systems you connected to the new router, including:
      i. EMV connection / status
      ii. DVR connection / Live video
      iii. Music system loading new music
      iv. If there are any issues, contact ISS TTU for support.
4. Once everything is verified, power down and remove the old router and switch.

e. Mount the included modem mounting bracket.
   i. Thread the receptacle end of the “Modem” power cord through the grommet in the bottom of the cabinet.
   ii. Mount the modem bracket in a location where the “Modem” power cord will reach.

f. Connect the primary broadband
   i. If there is no broadband circuit, the location will be brought up on dual Cradlepoints. See Appendix F.
   ii. Move and secure the broadband modem to the modem bracket, utilizing the included straps.
   iii. Thread the included Velcro strap through the modem bracket and strap the modem to the bracket.



   iv. Power the modem with the “1 - MODEM” cord from the cabinet.
   v. Reconnect the green cable to the WAN 1 port on the Fortigate router.
   vi. Connect the green WAN cable to the broadband modem / Ethernet jack.
   vii. Contact ISS TTU to verify the system switches over tot eh primary connection.

g. Install the new FortiAP access point
    i. Replace the existing access point with the FortiAP
    ii. Connect the blue cable to the "WAP" connection you previously labeled.
        1. Verify the FortiAP power up.
    iii. Test the access point
        1. ISS TTU will perform a verification script to make sure the new access point is online and has been activated correctly.
        2. On your laptop, download and install the (free) Wi-Fi Analyzer form the Microsoft store. https://www.microsoft.com/en-us/p/wifi-analyzer/9nblggh33n0n?activetab=pivot:overviewtab
        3. Open this application, select your country, and click on the "Networks" tab.
        4. Locate the store's SSID on the list and verify there is adequate coverage over the entire store, especially the sales floor.
        5. If there is not, the WAP will need to be relocated to a location that will provide coverage to the entire store.
h. Perform a speed test
    i. Connect your laptop to the "DMZ" port on the Fortigate router.
    ii. Your laptop should obtain an IP address in the 172.16.130.129/29 network.
    iii. Perform the speed test
        1. Navigate to https://www.ipchicken.com
            a. Record the WAN IP address it shows you here: _____._____._____._____
            b. Verify the IP address it gives you is NOT the backup Cradlepoint IP address.
            c. If it is the Cradlepoint IP address, wait a minute and try again. If this does bit change to the broadband IP address, contact ISS TTU for assistance.
        2. Open a web browser and navigate to http://www.speedtest.net
            a. You should be redirected to a Fortigate Login page.
            b. Use this login information:
                i. Username: speedtest
                ii. Password: $p33dt3$t
    iv. Verify that you can navigate to multiple websites. Make sure you are not loading cashed websites.
    v. Navigate to a speed test site like www.speedtest.net, www.speedtest.centurylink.net, or www.speedof.me (non-flash), and perform three separate speed tests.
    vi. Record your results on the "Installation Test Results" page.
    vii. Test the DVR
        1. ISS TTU will contact the customer to verify they can connect to the DVR using the "Wanzilla" DNS name.
i. **COMPLETE MILESTONE 4**
    i. Take photographs of:
        1. The equipment mounted:
            a. Cabinet mounted to the wall.
            b. Surge suppressor showing what outlets the cords are plugged into.
            c. Broadband modem, mounted to the bracket
        2. FortiAP

5. MILESTONE 5: VOICE

NOTE: If you need to access to the Yealink base, connect your laptop to port 2 on the Fortigate router.

a. Configure the IP Phones
   i. The Yealink base should be already mounted to the side of the cabinet and connected to port 4 on the Fortigate router.
   ii. Plug the power cord for the Yealink base into the extension coed in the cabinet labelled “Voice”
      1. If the base is already powered up, power cycle it by unplugging the power cord and plugging it back in.
   iii. The phones system may download firmware and configuration files. This may cause the phones and base to reboot several times.

b. Test the phone system.
   i. Once all phones have loaded their configurations, have the current time and date displayed and show line registration you can test functionality.
      1. Verify outbound calling from all three VoIP phones by calling an ANAC (1-800-444-4444, for example). Record the number the ANAC replies with.
      2. Verify inbound calling to the temporary telephone number (you recorded above) by calling it from your cellular phone. Verify all three VoIP phones ring.
      3. Test the phone operation in various locations in the store, trying to get as far from the base station as you can. If there is drop-outs and/or interference, the base station may need to be relocated to a more centralized area. Contact ISS TTU for assistance.

c. Install the phones in their final location
   i. Install the charging bases next to where the existing phones are. This will require local 110VAC for the bases.

d. **COMPLETE MILESTONE 5**
   i. Take photographs of:
      1. All phones installed in their final location (next to the existing analog phones)
      2. Yealink base station installation if it was relocated.

6. MILESTONE 6: COMPLETE INSTALLATION

a. Clean up and take photos
   i. Clean up all areas you worked in.
   ii. Remove all debris and packaging from all areas you worked in.
   iii. Remove any cables that are no longer in use.
   iv. Straighten up and neatly tie-wrap ALL cables for the point-of-sales, network, and telephone systems, even if you did not install these cables.
   v. Take photos of all your paperwork
      1. Signed COC
      2. Installation Test Results

b. **COMPLETE MILESTONE 6.**
   i. Email all images to ISS PM
   ii. Submit the COC to Building Reports or email to ISS PM
   iii. Close out with ISS TTU.