CFS & Affiliated IP Phones

From: M Bret Blackford (bret_blackford@yahoo.com)

To: bret_blackford@yahoo.com

Date: Sunday, April 12, 2026 at 08:52 AM CDT

MEMO to FILE

From: Michele <michele@hawkisg.com>
Sent: Wednesday, April 8, 2026 12:31 PM
To: Mary Ennis <mennis@cfserve.org>
Subject: RE: CFS

Mary,

I have not heard back from Kevin. I was looking for an email address to send him information – I have not received one yet. So here is the information you all need to make the changes on your network setup.

1. I have attached the new Firewall settings that will need to be made
2. The Mikrotik router is currently on a monthly rental through Affiliated. Please return this to:

Affiliated Communications
800 Jupiter Rd. Suite 200
Plano, TX 75074

Once the device has been received, your invoicing will be adjusted.

3. QoS should be prioritized traffic to atidevelopers.com and atidevelopers.net and pass STUN

Please let me know if Kevin needs anything else.

We are currently troubleshooting our voicemail issue.

Thank you,

M. Michele Gooch

Hawk iSolutions Group, Inc.
16227 Quail Valley Dr.
Wildwood, MO 63005
Office: (314) 727-1174 x 6303
Fax: (636) 230-9905
hawkisg.com | Facebook | Twitter | LinkedIn

From: Michele <michele@hawkisg.com>
Sent: Wednesday, April 8, 2026 8:54 AM
To: Mary Ennis <mennis@cfserve.org>
Subject: RE: CFS

Mary,

I just wanted to follow up with you and let you know that I have spoken to Kevin this morning.
Thank you,

M. Michele Gooch

Hawk iSolutions Group, Inc.
16227 Quail Valley Dr.
Wildwood, MO 63005
Office: (314) 727-1174 x 6303
Fax: (636) 230-9905
hawkisg.com | Facebook | Twitter | LinkedIn

From: Mary Ennis <mennis@cfserve.org>
Sent: Wednesday, April 8, 2026 8:20 AM
To: Michele <michele@hawkisg.com>
Subject: CFS

Good morning,

I tried to call John this morning and did not get his voicemail. I called your number as well and did not get voicemail either. Can you please have John call Kevin Romain at 731-343-2382.

Thank you,

Serving for Life

Mary Ennis
Office Manager
Christian Family Services, Inc.
7955 Big Bend Blvd
St Louis MO 63119
(314) 968-2216
Fax: (314) 968-2335
www.stlcfs.org

ClearCloudSOLUTIONS_FirewallConsiderations_2026.pdf
316.7 KB

AFFILIATED ComNet

Clear Cloud SOLUTIONS

Firewall Considerations

The information below is intended to provide an overview of Firewall settings and dependencies for customers desiring to deploy the Clear Cloud ACCESS or Clear Cloud UNISON solutions:

- ✓ Standard Firewall configurations often allow any traffic, UDP or TCP outbound. This is generally sufficient.
- ✓ The UDP session timer in the firewall must be at least 120 seconds.
- ✓ SIP ALGs, Transformations, helpers, etc. should be turned off.

If the network administrator blocks outbound connections, please ensure the following items are adhered to in order for proper operation:

- ✓ Outbound UDP sourced from port 5060 to any UDP port (used for SIP signaling)
- ✓ Outbound UDP sourced from port 5004 and 5005 to any UDP port (used for the voice path - RTP and RTCP)
- ✓ Outbound UDP from any port to port 123 (Used for time source).

  NOTE: This can be omitted if using an internal NTP source on the network)
- ✓ Outbound TCP from any port to port 65002 through 65090 (Used for HTTP-based provisioning and phonebook updates to the phone) 65052 is our PBX - so it can be limited to that port.
- ✓ Prioritize UDP Traffic above all other Data to atidevelopers.com(74.120.80.132) , atidevelopers.net (74.120.83.116), ~~74.120.83.65 and 74.120.80.161.~~

NOTE: No inbound connections are required.

Regardless of the customer's configuration, please feel free to engage the Clear Cloud team in any opportunity - as there are many more dependencies, unique customer requirements, and considerations than those listed here. The Clear Cloud SOLUTIONS team may be reached any time day or night at 214.382.9944, or Cloud@Affiliatedcom.com.

CFS UDR7 Testing Summary

April 11, 2026 — concise status report for next steps

Main win	We proved the UniFi UDR7 can run directly from the Spectrum/Charter EN2251 cable modem after a modem reboot, and we also partially integrated the UDR7 into the live 192.168.44.x CFS network with both Wi-Fi and Ethernet clients working under test conditions.
Main roadblock	DNS was the main limiter. Using only 192.168.44.100 as DNS did not produce reliable external resolution for UDR7 clients. Adding 1.1.1.1 as fallback restored practical UDR7 Wi-Fi and Ethernet access. Cisco firewall behavior still needs review as a possible hidden constraint.
End-of-night state	Production was returned to the prior path and phones were tested successfully. The one material exception is that the UDR7 was left on 192.168.44.x rather than being reverted to 192.168.10.x.

What was tested

- Confirmed an isolated baseline with the UDR7 providing DHCP and internet when using public DNS on the earlier 192.168.10.x test network.
- Moved the EN2251 cable modem directly to the UDR7 WAN. A hot swap did not immediately work, but after power-cycling the EN2251, the UDR7 came online with a public WAN IP. This proved that EN2251 → UDR7 is viable.
- Changed the UDR7 LAN to 192.168.44.1/24 with DHCP range 192.168.44.50–99 to rehearse a production-style cutover.
- Temporarily disconnected the MikroTik RouterBoard and connected the CFS switch path into the UniFi switch. This gave the UDR7 / UniFi side visibility into the live 192.168.44.x environment and showed partial success with real CFS devices.
- Tested UDR7 clients on both Wi-Fi and Ethernet. Clients received 192.168.44.x addresses, could reach 192.168.44.1 and 192.168.44.100, and later worked for internet after DNS fallback was added.

What looks good

Area	Finding	Meaning
Cable modem test	UDR7 obtained public WAN after EN2251 reboot.	Direct modem connection is feasible for future cutover.
192.168.44.x rehearsal	UDR7, switch, and clients operated on the CFS subnet.	Partial live-network integration succeeded.
Client path	Both UDR7 Wi-Fi and Ethernet worked after DNS fallback was added.	The UDR7 itself is not the primary blocker.

Rollback	Phones worked after returning production to prior routing.	The rollback appears successful enough for Monday use.

Roadblocks and open questions

• DNS is the clearest unresolved issue. 192.168.44.100 was reachable, but by itself it did not provide reliable external resolution for UDR7 clients during this session. Adding 1.1.1.1 fixed the practical problem, but that is not yet a clean long-term AD/production design.

• The Cisco firewall / ASA remains a likely hidden variable. It may still contain routing, NAT, or rule logic tied to the old topology and could be acting as a silent drop point or “black hole” for some traffic.

• The UDR7 was not fully cleaned back to isolated lab mode. It still sits on 192.168.44.x instead of 192.168.10.x, which should be corrected in a future maintenance window.

How the system was left

• Production connections were restored to the prior path: cable modem → Spectrum/Charter router → MikroTik RouterBoard, with production service apparently functioning again.

• Phones were tested by placing an outbound call and audio quality was good.

• The UDR7 remained powered on and online for testing, still configured for 192.168.44.0/24. This is the key exception to “fully back to prior state.”

• Because of the DNS fallback setting, the UDR7’s own Wi-Fi and direct Ethernet tests were working by the end of the session.

Recommended Monday follow-up: (1) verify whether the UDR7 should be returned to an isolated 192.168.10.x lab state; (2) review the DNS/DC host at 192.168.44.100, including forwarding and default gateway behavior; (3) map the Cisco firewall interfaces/rules to determine whether it is still required and whether it is affecting routing.