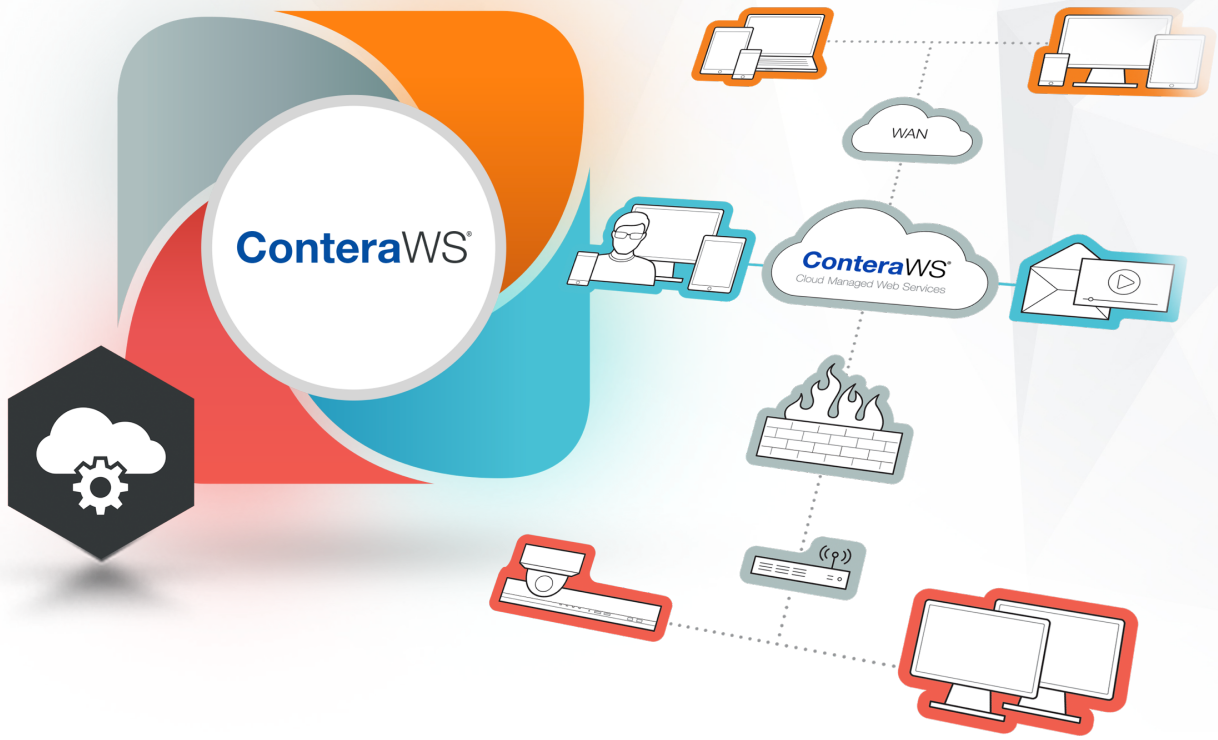
ContteraWS®

ContteraWS® Cloud Managed Web Services



IT Network Pre-Deployment Requirements

Arecont Vision®
A COSTAR COMPANY

+1.818.937.0700 | www.arecontvision.com | avsales@arecontvision.com

Arecont Vision®
A COSTAR COMPANY

Table of Contents

Introduction

ConteraWS (web services) is a secure and powerful Web-enabled platform that reduces maintenance costs and streamlines the management of video surveillance systems. Customers using ConteraWS (web services) can manage user groups, access live and recorded video, and export video incidents to cloud servers without fear of exposing their security system to potential threats. Our service ensures the security and integrity of your data by implementing technologies designed to prevent a wide range of hacking and data loss scenarios.

This document has been created to work as a guide to ensure your installation goes smoothly.

Nomenclature

ConteraWS® = Contera Web Services (Thin Client and Management)
ConteraVMS® = Contera Video Management Server Software (Local Recording and Thick Client)
ConteraMobile® = Contera Mobile App for iOS and Android OS
ConteraCMR® = Contera Cloud Managed Recorder

Ensuring Remote Access Through ConteraWS (Web Services)

ConteraWS (web services) utilizes a relay system that does not require port forwarding, thereby reducing maintenance and complexity. While no additional network configuration should be required, some specific ports cannot be blocked for outgoing traffic.

To ensure the successful commissioning of your ConteraWS (web services) enabled recorder:

Incoming	Outgoing
None required	These ports do not need to be forwarded (but cannot be blocked)
	TCP port 80 (Required) - Used for ConteraWS relay
	TCP port 443 (Required) - Used for ConteraWS relay

Network Whitelist Requirements

If the network is preventing the recorder from communicating with ConteraWS, it will prevent the service from making the necessary connection required for authenticating the recorder. This will require a Network Administrator to whitelist the hosts that the recorder will reach out to in order to make a connection to ConteraWS.

Note: We recommend adding the domains as documented below to your network whitelist instead of the IP address the domains resolve to. If your network filter uses reverse DNS, it is recommended to add your recorder to an exclusion range that is not filtered as our IP range will resolve to amazonaws.com.

Note: Communication with the relay service u5fgb.com uses a payload of message/http. This is an embedded HTTP response message from the recorder to the client software. If your network filter is blocking traffic to u5fgb.com you must allow "Content-Type" of "message/http" in your network filter.

The Following Locations are REQUIRED	
***.us-west.u5fgb.com** (for recorders located in the West Coast)	TCP 443 TCP 80
***.us-east.u5fgb.com** (for recorders located in the East Coast)	TCP 443 TCP 80
***.*.u5fgb.com *and* *.u5fgb.com** (for communication with relay service) *Note: Adding *.*.u5fgb.com will allow communication to new relay services as they become available.*	TCP 443 TCP 80
***.gp4f.com** (for communication with API services and branding portal)	TCP 443
Arecontvision-ws.com (for ConteraWS login portal)	TCP 443

The Following Locations are OPTIONAL	
stun.u5fgb.com (for peer to peer connections to improve performance)	UDP 3478
***.arecontvision.com** (for support of future enhancements)	TCP 443

The Following Locations are for ReportStar	
hw.mymanagedvideo.com (for communication with ReportStar service)	TCP 443
***.reportstar.com** (for ReportStar login portal)	TCP 443

Note: Cisco Iron Port devices may need a "Cisco Data Security" policy setup to allow POST traffic through. This will resolve issues with live video showing black when using relay.

Email Whitelist Requirements

When using an email service that filters emails based on a whitelist, it is possible that communication from ConteraWS will be blocked. Configuring your email server whitelist to accept incoming emails from ConteraWS servers will prevent missed communication from ConteraWS.

The following servers are required:

- *@arecontvision-ws.com
- *@gp4f.com

Bandwidth Recommendations

Arecont Vision recommends an NVR site upload bandwidth speed of 5 Mbps for an optimal experience when remotely viewing video over the WAN (Internet). This will result in a positive user experience when reviewing video from one 4MP high definition stream, or up to 9 standard definition streams. In instances where less than 5 Mbps is available remote users should plan to utilize standard definition streams for retrieving video over the WAN.

While the ConteraWS platform is highly configurable to meet exact bandwidth usage requirements the following table may be referenced as a typical use case:

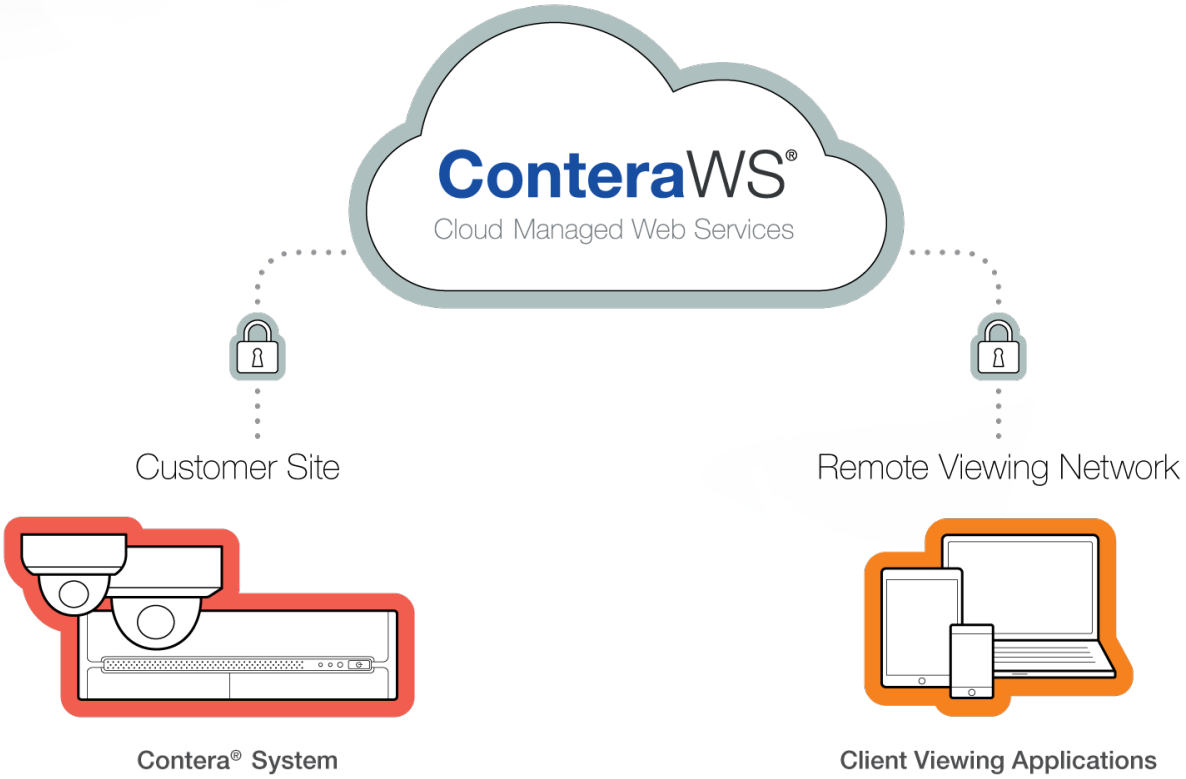
Channel Count	Live & Search SD Playback	Live & Search HD Playback
Single channel	500 Kbps	5 Mbps
4 channel grid	2 Mbps	Not Applicable
9 channel grid	5 Mbps	Not Applicable
16 channel grid	8 Mbps	Not Applicable

Average Bandwidth Usage Based on D1/4MP, 6,000Kbps, 15 IPS, 15 GOP IP Cameras

Note: The Arecont Vision ConteraWS platform dynamically chooses HD or SD streams for viewing based on the client display configuration selected by the user.

For example, a 4CH view will deliver SD video by default while a single channel view will automatically deliver the HD stream. Stream selection may also be manually controlled using the stream selection control at the top of the applicable display screen.

ConteraWS Relay Communication Diagram



Using LAN Smart Forwarding

LAN Smart Forwarding is a feature of ConteraWS (web services) which will keep most traffic within a local network when both the client and the recorder are on the same network. When the client initiates a connection to a recorder through ConteraWS, the external IP addresses of the client and recorder are provided to ConteraWS. If they match, ConteraWS will instruct the client application to connect directly to the recorder using the local IP Address. Even in a large corporate environment with

multiple subnets, you can configure IP ranges to allow LAN Smart Forwarding to acknowledge that both the client and the recorder still reside on the same network.

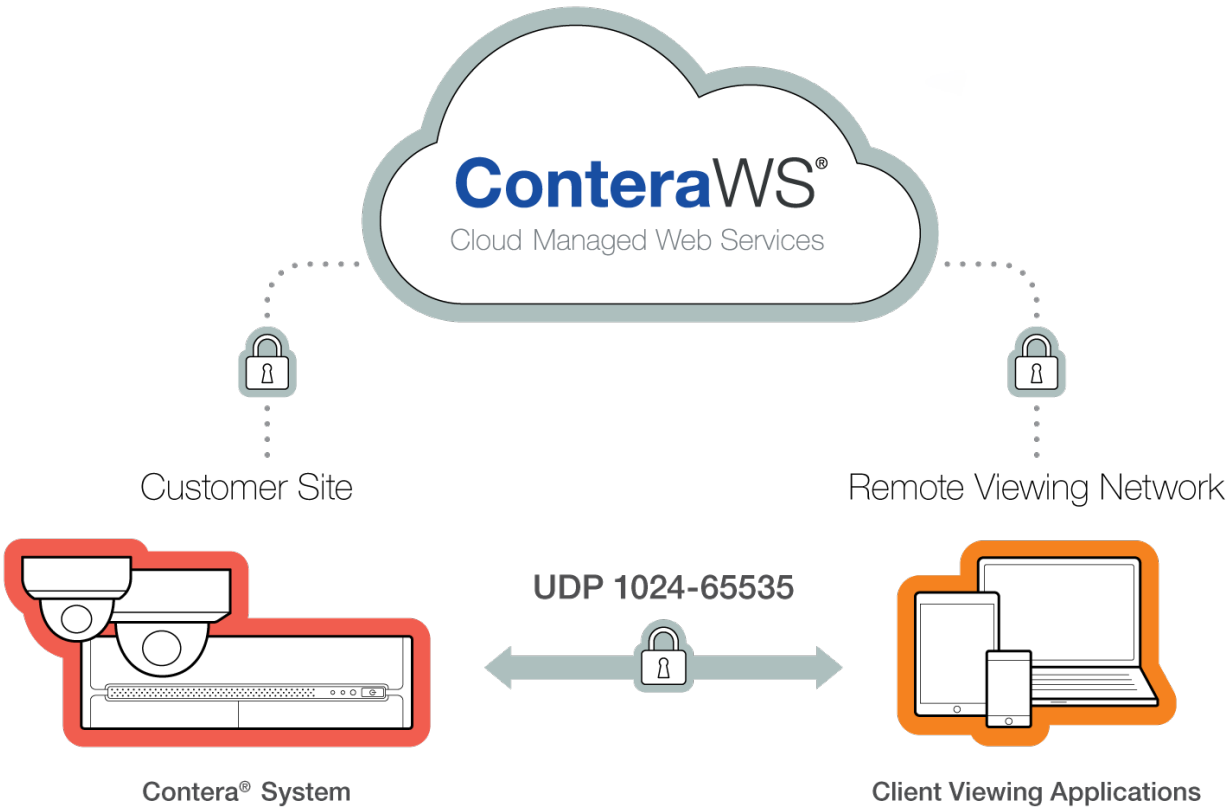
You can enable LAN Smart Forwarding within ConteraWS (web services) under My Recorders, then select the desired recorder, and Remote Network Settings. This feature is enabled by default for new recorders added to ConteraWS.

Web Services Peer-To-Peer Connection

Video streaming performance is typically best when video is sent directly from the recorder to the client. When the client initiates a connection through ConteraWS, the client attempts to connect directly to the recorder using STUN and ICE protocols. If this succeeds, then a direct video connection is established; if not, the connection will automatically fall back to the Relay method.

Peer-to-Peer connections are optional but will provide improved performance over utilizing the relay service. A Peer-to-Peer connection utilizes one random UDP port per connection in the 1024-65535 range (incoming and outgoing.) If UDP is unconditionally blocked in either direction on any ports within the range, Peer-to-Peer will be unreliable, or not work at all. Additionally, locking down (i.e. blocking outgoing UDP traffic) on all but one port will not succeed because ConteraWS (web services) relies on dynamic per-session UDP port mapping. If Peer-to-Peer fails, you will automatically fall back to the Relay method.

ConteraWS Peer-To-Peer Communication Diagram



Using Manual NAT for Best Performance

While most users find the performance of the previously discussed connection methods acceptable, users wishing to achieve the absolute best video streaming performance will want to consider using Manual NAT. Manual NAT is when you specify an IP address for clients to use when connecting

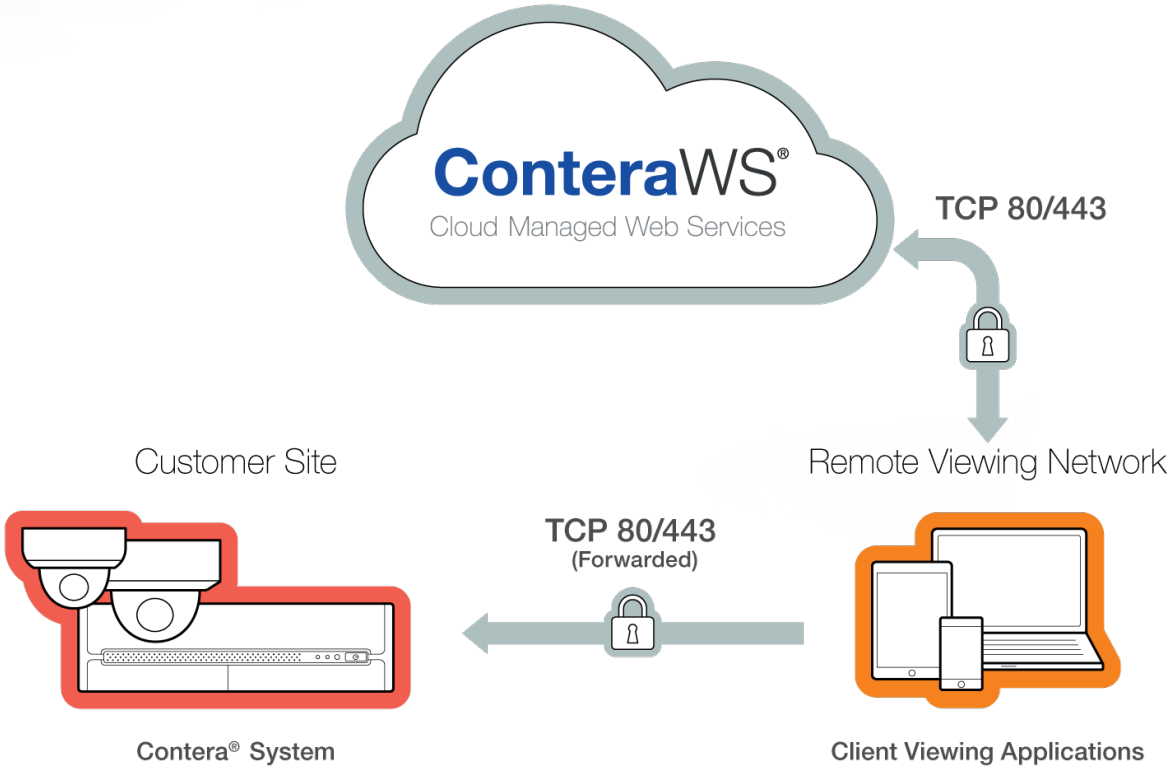
to the recorder. By using an external IP address or URL, and forwarding the following ports to the recorder, you will connect directly to the recorder in all cases.

Incoming
These ports need to be opened and forwarded to the recorder
TCP port 80 (Required) - Used for ConteraWS Thin Client, ConteraVMS (Thick Client), and ConteraMobile (iOS/Android App)

Note: 80 is used by default, but HTTPS (443) can be set up for Manual NAT by entering https://<ipaddress> in Manual NAT address field.

Once the recorder is configured you can enable Manual NAT within ConteraWS (web services) under My Recorders, then select the desired recorder, and Remote Network Settings. You can enter the IP address (or Domain) and the port to ensure ConteraWS (web services) uses a direct connection.

ConteraWS Manual NAT Communication Diagram



Direct Connection

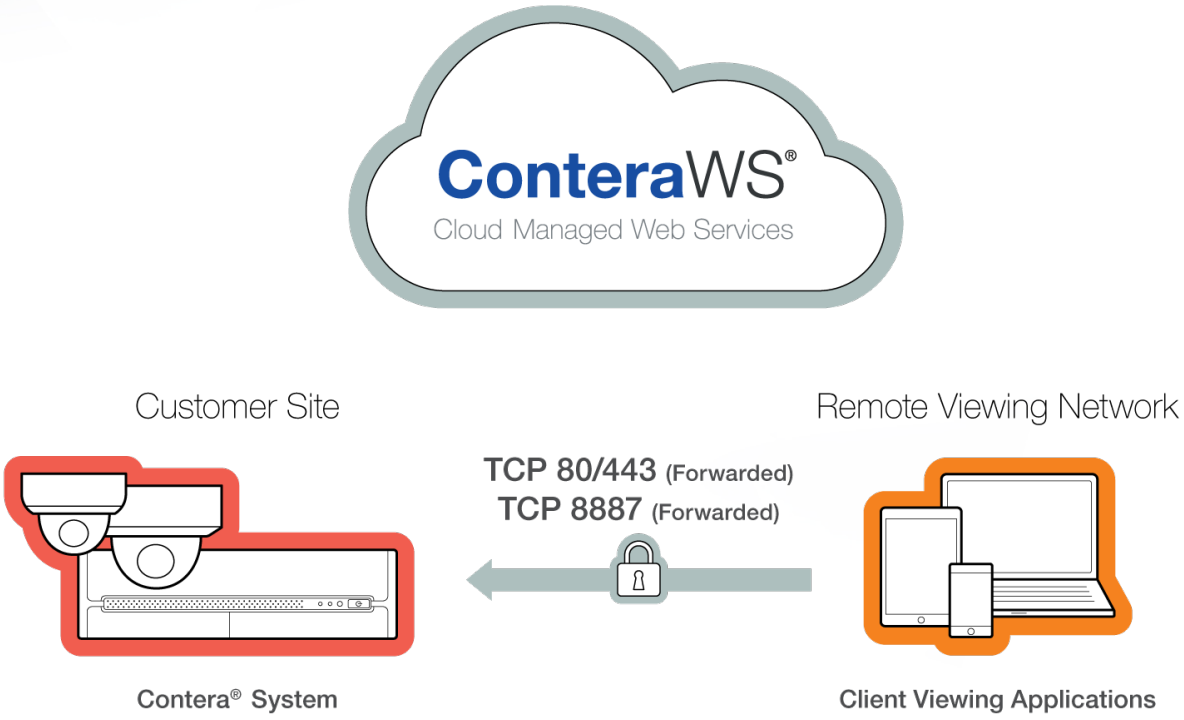
It is possible to create a direct connection to your ConteraCMR recorder by utilizing an external IP and forwarding ports to the recorder. This will allow you to bypass ConteraWS (web services) and directly type the IP address or Domain of your recorder in your browser address field. Doing this, however, will negate the benefits of ConteraWS (web services) such as single sign-on, group and user management, cloud backup, etc.

To establish a direct connection the following ports need to be forwarded:

ConteraWS (Thin Client)	ConteraVMS (Thick Client)	ConteraMobile (Mobile Client)
Port 80 or 443 - webpage / video streaming	**Port 443** - for authentication	**Port 443** - for authentication
	Port 8887 - for video streaming	**Port 8887** - for video streaming

Note: 80 is used by default, but HTTPS (443) can be used by typing "https" in the URL instead of "http." Doing so will display a certificate warning.

ConteraWS Direct Connection



ConteraWS Proxy Server Support

ConteraWS (web services) supports the use of network proxy services to securely aggregate HTTP communication in corporate environments. ConteraWS requires an HTTP 1.1 compliant proxy and can accommodate null, basic, or digest authentication.

Note: Depending on the ConteraWS connection method, some performance latency may be incurred. Relayed connections will route all video traffic through the proxy host, while a peer-to-peer negotiated connection will deliver video directly from the recorder to the client. Control messages will remain routed through the proxy.

Estimated Usage

Example 1 — User pulling / exporting 1 camera at 1920x1080 (High bandwidth review of a single camera)

- 2.24mbps

Example 2 — User pulling / exporting 1 camera at 640x480 (Low bandwidth review of a single camera)

- 250kbps

Additional Resources

- ConteraWS Architecture Overview Sheet

Arecont Vision®
A COSTAR COMPANY

The information in this publication is believed to be accurate in all respects. However, Arecont Vision cannot assume responsibility for any consequences resulting from the use thereof.

The information contained herein is subject to change without notice. Revisions or new editions to this publication may be issued to incorporate such changes.

+1.818.937.0700 | www.arecontvision.com | avsales@arecontvision.com