Technical Tip

How to Remotely Access DIGIOP

Revision 9.14.2018

Table of Contents

1.0 TCP/IP Port Configurations

You can access DIGIOP Control and DIGIOP Connect from a location that is outside of the Local Area Network of the DIGIOP Server you are using. If there is a firewall between the DIGIOP Server and the PC at the remote site, you must forward ports in your router and in any software firewalls to allow communications. All necessary changes are made to the Windows Firewall by the DIGIOP Server Installer. The information below includes TCP/IP port settings and router port forwarding settings for a basic DIGIOP server setup. For more advanced configurations, including custom port configuration for multiple servers behind the same public IP address, see section 2.

1.1 DIGIOP Connect Remote Access TCP/IP Settings

To be able to launch Connect and view video remotely, the following inbound ports must be forwarded:

Web Service Port: 24752 TCP

Video Service Port: 24754 TCP

1.2 DIGIOP Elements TCP/IP Settings

Systems hosted by DIGIOP Elements Cloud Hosting also utilize outbound ports. Most firewalls do not restrict outbound access, but if your location has outbound restrictions, you must allow outbound access for the following ports:

DIGIOP Elements Tunnel: 24753 TCP

Web Service Port: 24752 TCP

1.3 DIGIOP Control Remote Access TCP/IP Settings for Locally Hosted Systems

If your server is hosted locally, to be able to access DIGIOP Control from a remote computer, the following inbound port must be forwarded:

Configuration Port: 80 TCP

1.4 DIGIOP™ Mobile Access

To be able to view video remotely from a mobile device, the following inbound ports must be forwarded:

DIGIOP GoMobile App for Apple iOS devices: Utilizes the same Video Service Port as Connect (configured above)

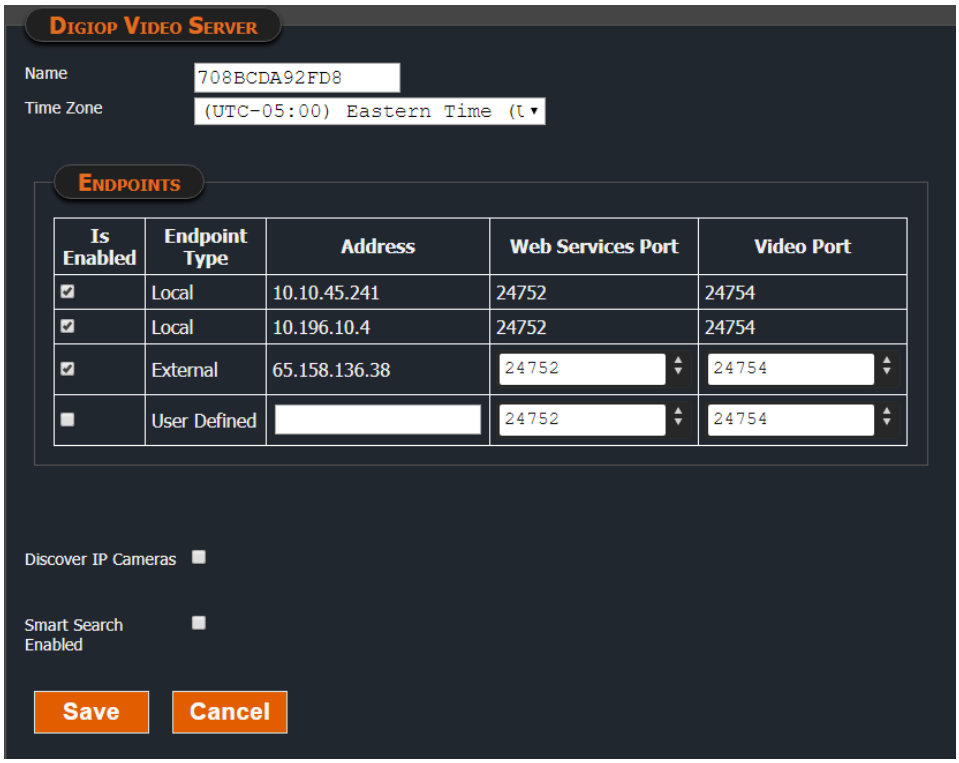
2.0 DIGIOP Advanced Networking Configuration

DIGIOP also includes the ability to configure custom ports. This is useful if you have another application already using the default ports, or if you need to be able to configure multiple DIGIOP Servers behind the same firewall.

2.1 Configuring Custom Ports

Custom ports will need to be configured in DIGIOP Control and then forwarded in all firewalls.

1. Launch DIGIOP Control and Login.
2. Highlight the video server and select **Edit**. The DIGIOP Video Server configuration page will appear, including the Endpoints configuration box.



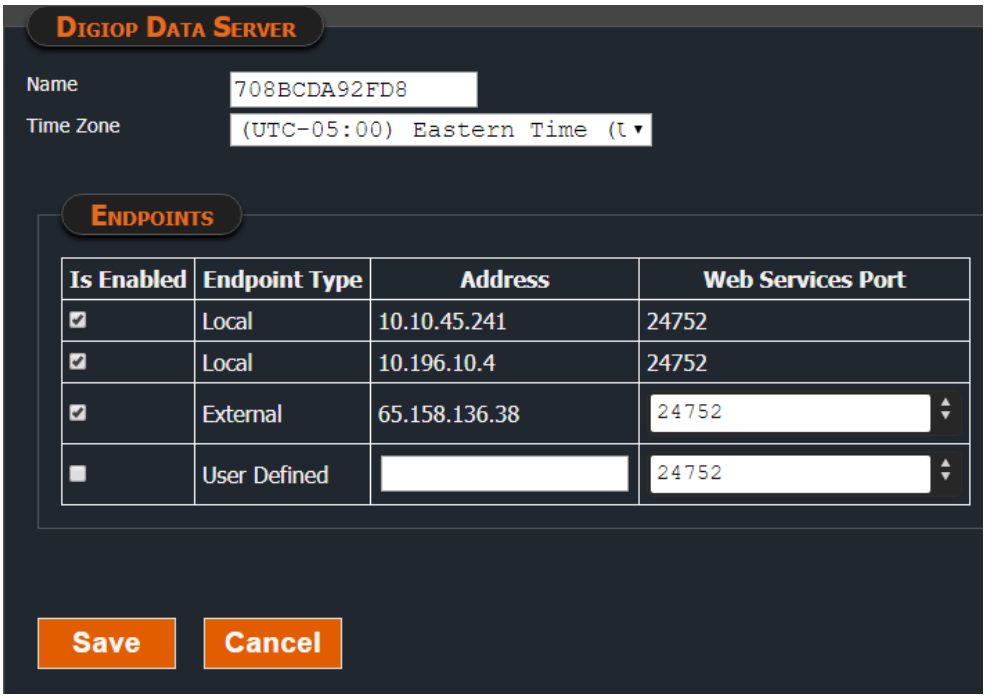
3. Use the up and down arrows to modify both the Web Services Port and Video Port to the desired ports.

NOTE 1. Only the External and User Defined ports will be modified. The Local ports will remain 24752 for the Web Services Port and 24754 for the Video Port.

2. If utilizing a User Defined address, its custom ports will need to match the custom ports of the External address.

4. Click **Save** to save all configurations.

5. Highlight the data server and select **Edit**. The DIGIOP Data Server configuration page will appear, including the Endpoints configuration box.



6. Use the up and down arrows to modify the Web Services Port. The port you configure here should match the same port used to configure the Web Services Port in Step 3.

2.2 Viewing Video from an External Network with Custom Ports

The ports configured in 2.1 will need forwarded in the router.

2.2.1 DIGIOP Server Inbound Connections

No changes will need to be made to Windows Firewall or any software firewalls as the Local internal ports have remained the same.

2.2.2 DIGIOP Server Outbound Connections

No changes will need to be made to Windows Firewall or any software firewalls as the Local internal ports have remained the same. If utilizing DIGIOP Elements, TCP ports 24752 and 24753 will still need to be allowed for outbound access as in Section 1.

2.2.3 Router/Hardware Firewall Inbound Connections

The custom configured ports defined in section 2.1 will need forwarded.

1. Web Services Port – Forward the custom defined Web Services port on the Public external IP to port 24752 on the Local internal IP.
2. Video Services Port – Forward the custom defined Video Services port on the Public external IP to port 24754 on the Local internal IP.

If your server is hosted locally, and you would like to be able to access DIGIOP Control remotely, port 80 will still need forwarded.

1. Port 80 – Forward port 80 on the Public external IP to port 80 on the Local internal IP.

If you would like to be able to view video remotely from a Mobile device, the following ports will still need forwarded.

1. DIGIOP GoMobile App for Apple iOS devices: Utilizes the same custom Video Service Port as Connect (configured above)
2. Mobile Web support for Android devices: Forward port 80 on the Public external IP to port 80 on the Local internal IP.

2.2.4 Router/Hardware Firewall Outbound Connections

Servers hosted remotely by DIGIOP Elements:

If your router/hardware firewall restricts outbound connections, you will still need to allow outbound connections for ports 24752 and 24753 as in Section 1.

Servers hosted locally:

There are no outbound ports required.

2.2.5 DIGIOP Connect Workstation

There are no inbound or outbound ports required.

2.3 Multiple DIGIOP Servers Behind the Same Firewall

Multiple servers can be located behind the same firewall by using custom ports.

2.3.1 Assign Custom Ports

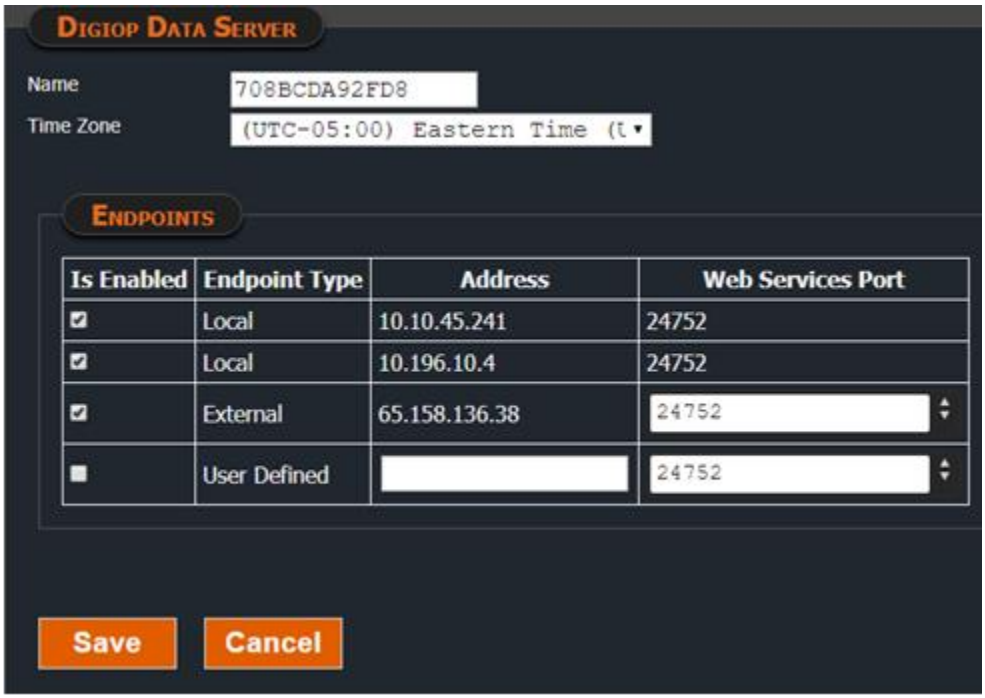
Each server will need its own unique set of custom ports. As a best practice, it is recommended that you do not use 24752, 24753, or 24754 for your custom Web Services or Video Ports. Follow the steps in 2.1 to assign unique ports to each server.

2.3.2 Port Forwarding

The ports configured in 2.3.1 will need forwarded in the router. Follow the same steps as in Section 2.2 to forward the needed ports. In this instance, the Public external IP address will be the same for each port forwarding rule, but rules will need to be created for each custom defined port for each Local internal IP address.

2.4 User Defined Endpoints

All network endpoints discovered by DIGIOP are added and enabled in Control by default. You also have the ability to add custom User Defined endpoints. This is useful, for example, for locations where DIGIOP was not able to discover a needed IP address, or for locations that have multiple external/public IP addresses. Control allows you to enter the User Defined endpoint and the ports you would like to use.



2.5 Disabling Endpoints

All network discovered endpoints are enabled by default. In DIGIOP Control you can uncheck the “Is Enabled” box in order to disable an endpoint. DIGIOP will no longer try to use that IP address to make network connections. This is useful, for example, for locations that have multiple external/public IP addresses. DIGIOP will often discover the Public IP that the router is sending out. You may not want to use this address, but rather one of your other Public IP addresses. You can enter the Public IP address as a User Defined address, then uncheck the box next to the discovered External address so that it is no longer used.

3.0 Legacy TCP/IP Port Configurations

Earlier versions of DIGIOP Server utilized a different TCP/IP Port Configuration scheme. For versions 8.0 - 9.0, inbound port forwarding is needed on the following ports.

Port Number	Protocol	Definition
7000	TCP	Logon
8000, 8001	TCP	Live Video Transmission
8002	TCP	Checking Server
9000, 9001	TCP	Video On Demand (Search)
24752		DIGIOP™ Data, Camera Configuration, Connect Updating Systems List, Connect Updates, Event Notifications
80	TCP	DIGIOP™ Control
4165, 5353, 4022, 6055, 52220, 69, 10000, 43282, 31001,2380	UDP	IP Camera Discovery (Optional)

3.1 DIGIOP Elements TCP/IP Settings

Systems hosted by DIGIOP Elements Cloud Hosting also utilize outbound ports. Most firewalls do not restrict outbound access, but if your location has outbound restrictions, you must allow outbound access for the following ports:

DIGIOP Elements Tunnel: 24753 TCP

Configuration Port: 24752 TCP