Security Considerations

WITH VIDESTRA SYSTEMS

Dan Desjardins
VIDESTRA |WWW.VIDESTRA.COM | SUPPORT: 608.999.9003

Contents

Security Considerations with Videstra

Overview

Installing a new system that involves computers that will become part of your enterprise network will undoubtedly raise issues and security considerations. This will be no different with Videstra. The following pages discuss the details of many of those security issues. This document is not too lengthy, however here is an executive summary of the things you should know about Videstra.

Executive Summary

- Shares are used. Most are read-only, some are read-write.
- No *incoming* connections from outside your network are required.
- Some *incoming* connections are necessary only from within your private subnet.
- The following default ports are used, and *outgoing* connections must be permitted:
  - 21 (FTP)
  - 22 (SFTP)
  - 80 (HTTP)
  - 554 (RTSP)
  - 8080 (V-Streamer REST API)
  - 53608 (TCP/IP VestraView Client Connection)

  Any of the above ports can be changed if/when necessary.
- The OS's used are Windows 10 LTSC and Ubuntu 18.04 LTS

For more details on all security aspects of your Videstra system you may continue reading the following sections. If you have additional questions please feel free to reach out to support@videstra.com or call us at 608.999.9003 M-F 9AM to 5PM CST.

Operating Systems (V-Manager & V-Streamer)

The Videstra **V-Manager** is running Windows 10 LTSC. This is an IoT version of Windows designed for Windows based appliances. Windows LTSC receives only security and stability updates. It does not receive new Windows features, nor does it offer an automatic path for upgrading to Windows 11. Depending on your installation you will be running one of the following Windows 10 LTSB (Long Term Service Branch) or LTSC (Long Term Service Channel) Releases:.

Version	Release Date	Extended support end date
1607 LTSB	2016-08—02	2026-10-13
1809 LTSC	2018-11-13	2029-01-09
21H2 LTSC (current release)	2021-11-16	2027-01-12

> *Note: LTSB and LTSC are both Long Term Service releases; Microsoft just changed the name sometime in 2019 to better conform with their IoT Strategy.*

As of the date of this writing 21H2 is the latest LTSC version of the Windows operating system available. A Windows 11 LTSC version is expected to be released sometime in late 2023. Upgrades to this version can be provided at additional cost. Contact Videstra if this is important to you.

The Videstra **V-Streamer** is running Ubuntu Linux Version 18.04 LTS. We plan to update this to version 22.04 by the end of 2023.

> *Note: Security patches for the V-Streamer can be installed, however no patches to the kernel are allowed. Patches to the kernel will disable the interface to the AJA Corvid HD-SDI card. The Unattended upgrades settings are set for manual and should be set to blacklist all kernel update. It will be best to let Videstra support run any security updates if desired. The security update process can take up to one hour.*

Code Signing Certificate

As of Version 2.3.16 Videstra software uses a *Sectigo® EV Code Signing Certificate* with a hardware security token. Prior to 2.3.16 Videstra used a Comodo® OV signed certificate.

Shares

Videstra makes use of several Windows Shares. Below is a list of shares used by Videstra:

Rolling Temporary Shares

Whenever a user enters the Timelapse Factory™ or Clip Factory™ a *temporary read-only share* is created on the V-Manager. It will be given a random name (e.g., “A1B2C6F0”). This is a read-only share and is known only to the client on which the Timelapse or Clip Factory have been started. It is used by the client to copy images from the V-Manager to create the time lapse movie (Timelapse Factory) or to view index frames for accessing clips from Axis cameras (Clip Factory).

Once the user exits the Timelapse Factory, or Clip Factory the share is automatically deleted from the V-Manager. If the client stops unexpectedly the share will automatically be deleted after 6 minutes of nonuse.
Timelapse Factory and Clip Factory share names are never re-used. The share name is a randomly generated temporary GUID (Globally Unique IDentifier).

Client Software Updates (VidestraUpdater Share)

Client Software Updates are done over a *read-only* share on the V-Manager called VidestraUpdater. Permissions are set to "Everyone." Older installations may also have a VidestraUpdater$ share still in place. Under Windows the trialing $ denotes it as a hidden share. On current Videstra versions this is no longer used. The hidden share was abandoned due to many customers disabling hidden shares on their networks. If you find this share on your system you may safely delete it.

Weather Graphics System Shares

An open (Read/Write) share is used to copy time lapse movies to The Weather Company MAX and Baron Lynx systems. The path to the share will vary from system to system.

> On MAX Systems from The Weather Company™ the share will look something like this:
> **[CALL LETTERS]-TVDC2\DigitalMedia\Custom\Content\Videos\Timelapse**
> Access to this share is limited to valid MAX users (either Producer or truvuadmin)
>
> On Lynx systems from Baron™ the share must be created for Videstra and will look like this:
> *[CALL LETTERS]-LYNX\Lynx\Graphics\Time Lapses* ← *note there is a space in Time Lapses*
> Access to this share can be limited to Videstra after user Videstra is created on Lynx – otherwise it will be set to Everyone.

Outgoing Connections to Public Addresses

Various connections to public IP Addresses are common with the Videstra system. No *incoming* connections are used or necessary. All connections are on outgoing ports only. Some IT departments will routinely block outgoing port connections and if that is the case in your facility here are some things to keep in mind:

RTSP (Normally Port 554)

RTSP (Real Time Streaming Protocol) is used to get h.264 or h.265 video from most cameras. Outgoing ports used to connect to a cameras RTSP stream must be open (again – outgoing only). By default, this will be port 554, but it can be set up to be most any other port. You will likely have more than one camera and all, or only some of the cameras may use port 554. Make sure you allow outgoing connections on rtsp ports used by all the cameras.

HTTP (Normally Port 80)

HTTP is used chiefly for connections to camera services such as internal web pages, images and even to control the camera (Pan/Tilt/Zoom) functions. By default, this will be port 80, but like RTSP it can be configured to most any other port. And, once again, this is only for *outgoing* connections.

Both the RTSP and HTTP Connections will be made from the V-Manager, the V-Streamer *and* any Windows computers running a copy of the VestraView client software.

FTP (Port 21) and SFTP (Port 22)

Videstra uses both FTP and SFTP for updating DOT database files and backing up the critical files for recovery should you experience catastrophic hardware failure. The V-Manager uses both FTP as well as SFTP to connect to videstra.net for these purposes. As stated many times herein – these are outgoing connections only. FTP Connections are *passive*.

Web Publishing (FTP/SFTP/FTPS)

Web Publishing is typically done using SFTP (port 22 via SSH), however some legacy operations may still be using FTP (port 21). Videstra supports FTP, SFTP and even FTPS. Ports for any FTP type can be customized if necessary. Some Web publishing utilizes an HTTP Upload via a very secure, but proprietary key exchange. This is used for updating overlays used with the Videstra LiveShare™ service. This update is done over port 80 on an outgoing connection only.

V-Streamer API (Port 8080)

The V-Manager communicates with the V-Streamer over Port 8080. The V-Streamer must allow for incoming connections on port 8080. Since this is only for connections within your private subnet this is not considered to be a security risk.

V-Streamer Setup Pages (Port 80)

When you connect to the V-Streamer with a web browser that is done over port 80 via the HTTP protocol. The V-Streamer must allow incoming connections on port 80. Since this is only for connections within your private subnet this is not considered to be a security risk.

VestraView Client (Port 53608 and 53609)

The VestraView client connects to the V-Manager over port 53608 via TCP/IP. The V-Manager must allow incoming connections on port 53608. This can be changed if necessary. Communications between the VestraView Client and the V-Manager are encrypted. Since this all takes place within your private subnet this is not considered to be a security risk.
In some installations multiple V-Managers may be used – in which case a secondary connection port must be allowed. This is usually 53609 but can be changed as necessary to avoid any conflicts.

ICMP Echo (Pings)

Some functions in Videstra may use ICMP Echo Requests to verify the presence of a machine providing a service. This is entirely optional (this can be turned off). Devices include:

1. The V-Streamer
2. The V-Manager
3. The Weather Graphics Machines (The Weather Company Max or Baron Lynx)

When setting up a camera connection a ping test is part of the setup. If the Ping fails, however, this can be ignored. A ping is a good positive test, but an unreliable negative test because many network administrators routinely disallow ICMP echo requests on routers within their networks.

User Account

The V-Manager will have a specific user account called **VestraView**. Do not delete this account or change the password. This account is used by the server for acquiring various services. It has limited access.

Are There Any Backdoors in Videstra

There is no backdoor in the V-Manager (The Windows based box). There is an *optional* backdoor that can be enabled only on-site in the V-Streamer. By default, it is off. No one outside of your firewall can open this backdoor – it *must* be done by someone in your facility.

Best Practices

Videstra has published numerous Best Practices documents on our website available at: https://www.videstra.com/support. There are a few security-based Best Practices documents, but one important one is for securing cameras that you have deployed. That document can be accessed at the following direct URL: https://videstra.com/bestpractices/bp-security.pdf