Fusion3

EDGE 3D Printer

OPERATION:
LONG PRINTS & REMOTE ACCESS

Revision 3/15/2023

LONG PRINTS & REMOTE ACCESS

How to safely run long prints on EDGE.

IMPORTANT: Fusion3 recommends NEVER leaving a running 3D printer unattended for ANY length of time. Every print should be supervised in a manner that allows an operator to intervene if the print begins to fail or malfunction. Fusion3 may elect, at its discretion, to not cover damage caused by unattended prints under your warranty.

INTRODUCTION

We get it: large prints take a long time, sometimes multiple days, and it's not practical to have someone sit by a running printer 24/7 until the print is done. But in order to keep your Fusion3 warranty in force, and protect your equipment, personnel, and facilities, it's important to not let any 3D printer run unattended.

This document outlines a number of approaches to remotely monitoring your printer that allow you to intervene if needed, and stop or pause a print, without having someone physically next to the printer.

Any remote monitoring approach must have three components:

1. A way to **see** the printer and what it's doing in realtime.
2. A way to **intervene** to stop or pause a print that's having problems.
3. A **person** whose job it is to remotely monitor the print (continuously or multiple people in shifts).

We can provide some pointers on the first 2 points… The last one is up to you!

WAYS TO SEE THE PRINTER

You must be able to see the physical printer and the print chamber. Seeing the network interface is nice but not sufficient, because that information doesn't tell you if a print has failed due to coming off the bed, horizontal offset, etc.

- Webcam linked to third party app (ring, etc)
- Webcam hosted on your local network (would require remote outside-of-network access)
- (coming soon) Integrated webcam accessory (available through the network interface).

The camera should be positioned so that you can tell if a failure happens. Ideally you'll be able to see the entire print chamber, including the bed and print head, to catch all possible failure modes in frame.

WAYS TO INTERVENE

The goal of intervening is to prevent damage to the printer or facilities from a print that has failed, or is in the process of failing. There are several ways to do this:

- (low tech) Kill power using a "smart outlet".
- (med tech, secure) Configure a PC on your local network to accept Remote Desktop connections and connect to it from outside your network to use the network interface to control the printer.
- (med tech, not secure) Configure port forwarding to expose the printer's network interface to the wider internet.

Low Tech: Smart Outlet

Use a "smart outlet" that can be controlled remotely via an app (Belkin or similar) to temporarily kill power to the printer when you see a print fail. Don't forget to restore power so the printer can cool down normally.

Good:

- Does not require cooperation of your IT dept, beyond getting the outlet on your network
- Simplest to set up
- Does not expose a computer or the printer to the wider internet.

Bad:

- Limited control - your only choice is to let the print run or kill power completely
- You must be sure the smart outlet can support 6A continuous draw or brownouts may occur
- The webcam side of things must be an entirely separate thing

Remote Desktop Connections

This is our preferred solution to remotely controlling printers. It's a good balance of access to information and control, while remaining secure.

For more information on what Remote Desktop is and how it works:

- https://en.wikipedia.org/wiki/Remote_Desktop_Services#Remote_Desktop_Connection
- https://support.microsoft.com/en-us/windows/how-to-use-remote-desktop-5fe128d5-8fb1-7a23-3b8a-41e636865e8c

Good:

- Gives you full control over the network interface. You can pause or cancel prints, run gcode commands, etc.
  - This can give you some options to attempt to recover a print vs giving up and killing it completely.
- Can be integrated with a webcam over your local network or the optional EDGE accessory camera.
- You can control multiple printers on your network from a single PC. Good for remotely monitoring a farm!
- Does not require you to know/memorize your external IP address.

Bad:

- Requires your host PC to be running windows 10 or 11 professional.
- Requires the host PC be left running at all times.
- Requires that your local network / IT dept allow remote desktop connections.
- RDP is generally considered secure, but this does increase your IT vulnerability to hostile actors.

Alternatives to RDP

If you are not using win10/11 Pro, or want to use something else: https://rustdesk.com/ Rust has installed (requires admin privileges) and lightweight (no privileges needed) versions.

Port Forwarding (not recommended)

It is possible to port forward the printer's IP address (and thus the network interface) directly to the wider internet. Then, if you know your externally-facing IP address, you can access it from anywhere in the world.

Good:

- Gives you full control over the network interface. You can pause or cancel prints, run gcode commands, etc.
- This can give you some options to attempt to recover a print vs giving up and killing it completely.
- Can be integrated with a webcam over your local network or the optional EDGE accessory camera.
- Doesn't rely on a computer that runs Windows 10/11, or other devices on your network

Bad:

- This is **EXTREMELY INSECURE**. EDGE's network interface was not designed with this use case in mind, and it has not been hardened to the degree publicly-facing internet devices should be. It can dramatically increase your IT attack surface and give hostile actors an additional potential toehold onto your network.
- Only feasible on small networks, since generally only a few devices per (external) IP can be port forwarded.
- Requires administrative access to your network's routers, or cooperation from your organization's IT team (no IT team in their right mind should let you do this, by the way).
- You should enable the UI password if you do this. For more info, see "*Mode switches & options*".
- You must remember/memorize your external IP address. If this address changes, you'll have to keep track.

The only time port forwarding might be appropriate is on a small network with no critical infrastructure or data attached to it, AND it's used temporarily for a single print, and afterwards disabled again. This reduces the window potential attackers have to find and exploit the port forwarding.