Network Printing Best Practices

Here are some best practice steps for setting up a network-capable printer at MIT.

On this page:

- Setup
  - Change Admin Password(s)
  - Disable services that you do not need
  - Set an IP access filter on your printer
  - Ask IS&T to block outside traffic to your printer

- Security
  - Gather Information
  - If some computers cannot print to the printer
  - If the printer is printing garbage or acting strangely

Setup

Good setup advice is available at: Set Up a Printer on MITnet

The most important setup advice is to select a unique hostname for the printer, and request an IP address. See step #2 under "Set Up Instructions" on the above page.

Steps #3 and #4 from that page are optional. If desired, steps #3 and #4 let you request an Athena print queue for your printer, and configure your printer's MAC/hardware address into IS&T's bootp servers. If you don't know why you would need either of these, it should be safe to skip them.

(An Athena print queue is helpful if you frequently print from SAP. Registering your printer's MAC address for bootp is helpful for ensuring that a printer always gets its IP address when it boots, even after a reset.)

Security

Attackers regularly scan MIT's network looking for devices to exploit. A network-connected printer will be found, and probed for weakness. Here are steps you can take to protect your printer from attackers.

Change Admin Password(s)

If you take a printer out of the box and plug it into the network without changes, it may still have a default "admin" password, or might have no password at all. Attackers could get into the printer and change its settings.

- Protect your printer by setting a new admin password.
- Different printers will use different instructions for this.
  - Most network printers have a built-in web page. Go through the built-in web page and look for security settings or password settings.
- Don't lose your new password. Make a note of it, perhaps in your office manual, or even tape it to a note on the printer.

Disable services that you do not need

Printers can allow many different network services to support different ways of communicating with the printer. Each allowed service will be found and tested by attackers. Attackers testing your printer could cause it to print garbage pages, or could make it run so slow that it appears broken, or cause other problems.

- Protect your printer by turning off services that you do not need.
- Different printers will use different instructions for this.
  - Most network printers have a built-in web page. Go through the built-in web page and look for server settings.
- Very safe to disable:
  - Telnet - an old (pre-web) method of configuration
  - FTP - an old method of submitting print jobs
- Optional
SNMP
SNMP is used by Windows and Mac computers help the computer know the printer's status. But SNMP can also be abused by attackers. Disabling SNMP can make it harder for Windows or Mac computers to print to your printer.

Set an IP access filter on your printer

Many printers let you control which IP address is able to reach the printer. You may be able to use an IP filter to block off-campus attackers from even talking with your printer.

- Protect your printer by setting an IP filter to restrict access.
- Different printers will use different instructions for this.
  - Most network printers have a built-in web page. Go through the built-in web page and look for security settings, or access settings, or TCP/IP.
  - Most MIT computers use an IP address that starts with "18."
    - If the printer asks you to enter numbers as a high-low range, the most current information on ranges can be found here: What are MIT's IP ranges?
    - If the printer asks you to enter a CIDR range, the range is in the format "18.0.0.0/9" check What are MIT's IP ranges? for the current range.

Ask IS&T to block outside traffic to your printer

IS&T can block traffic originating outside MIT from getting to your printer. The steps to request this are:

- Send email to security@mit.edu.
- The mail should be from the listed printer owner.
- Give the printer's IP address or full hostname.
- Ask for the printer to be blocked from communicating with non-MIT IP addresses.

Support

If a network printer isn't working well, IS&T will try to help.

Gather Information

For most problems, IS&T will need to know the printer's make and model along with the printer's current IP address. You can find these by walking to the printer and using the buttons and menu on the printer to print a "settings page".

If some computers cannot print to the printer

Here are some tests that can help:

- Check that the printer has a properly assigned IP address.
- Check whether the IP is online, responds to pings, has a printer port open, or has an internal website.
- Check whether other computers can print to the printer.

If the printer is printing garbage or acting strangely

Check the steps in the "Security" section above:

- Change the admin password.
- Disable services that you do not need.
- Set an IP access restriction.

If the steps in the security section don't work, IS&T can block traffic originating outside MIT from getting to your printer. All packets coming from outside MITnet will be dropped at the border, this means no connections can be made with IPs outside MITnet. If anyone working from an non-MIT IP needs to print, they can join the VPN.

The steps to request this are:

- Send email to security@mit.edu.
- The mail should be from the listed printer owner.
- Give the printer's IP address or full hostname.
- Ask for the printer to be blocked from communicating with non-MIT IP addresses.