

FREE PRINTER MONITORING SOFTWARE

Installation Instructions

ICE is our free printer monitoring software. It installs in minutes on any Windows workstation or server, reads the printers on your own network, and sends what they report to a secured web server over a secured Internet connection. It is what fills in your free printer app with live information and current alerts.

Is it safe? Yes. ICE reads only what each printer reports about itself: its name and location, make and model, serial number, network address, page counts, toner levels and status alerts such as a paper jam. It never sees the documents you print, and no personal information is read or sent. ICE starts every connection itself, the way your computer sends an email. Nothing from outside can connect in to your network through it, and the information travels encrypted, the same protection used for online banking.

1. Choose a computer to host ICE

The computer you choose should be one that is always turned on. This might be a server, but it does not have to be. It also needs to meet these minimum requirements:

- Windows 7 or later, or Windows Server 2008 or later, 32-bit or 64-bit
- Processor and memory as required by the operating system
- 20 MB of hard disk space

2. Download ICE

Use this link to download the latest version of ICE: <https://theprinterdoctor.ca/ice.html>

3. Install ICE

1. Go to where you saved the PaFmIceSetup.exe file in the step above.
2. Double-click the file to begin the installation.
3. Click **Run** to begin the wizard.

4. Activate ICE

1. If your antivirus software asks about ICE, choose to allow it so that it is not blocked.
2. Launch the **ICE Administrator** from your programs.
3. In the **ICE Administrator Licensing** dialog, enter the activation code we sent you. If you have not been given an activation code, please email service@theprinterdoctor.ca for one.
4. Click **Activate**.
5. The ICE License Agreement is then displayed. Select **I Agree** to proceed.

6. A message then confirms that the licensing has succeeded. If it has not, please try to activate a second time.
7. If it still does not succeed, a proxy server or a firewall may be in the way. See the firewall and proxy information further down.
8. Once activated, open the **Tools** menu and select **Scan Now**.
9. Email service@theprinterdoctor.ca to let us know ICE is installed, and a representative will contact you to confirm the printers now being monitored.

Firewall and Proxy Server Information

In most offices nothing here needs to be changed. This section is for networks with tighter security, and for the IT team that looks after them.

If ICE cannot reach the secured web server, it cannot activate or send its data. If you have installed ICE but cannot activate it, please review the information below.

Firewalls (software and hardware)

ICE makes three kinds of connection. None of them opens your network to the outside.

- **Reading your printers: UDP port 161 (SNMP).** This is the standard channel printers use to report their own status, and ICE uses it only between the ICE computer and the printers on your own network. It never crosses the Internet, so nothing needs to be opened on your Internet firewall. It needs attention only if security software on the ICE computer, or an internal firewall between that computer and the printers, is blocking it. (ICE also sends a standard ping to find which addresses have a device.)
- **Sending the data: TCP port 443 (HTTPS), outgoing only.** This is the same kind of outgoing connection a web browser makes to a secure website, and most firewalls already allow it.
- **Automatic updates: TCP port 80, outgoing only.** ICE uses this to check whether a newer version of itself is available. Automatic updates can be turned off in ICE if your IT policy requires it.

No incoming ports need to be opened. Every connection is started by ICE itself, and nothing connects in to ICE.

Proxy settings

If your network uses a proxy server and does not allow direct access to the Internet, the proxy settings in the ICE Administrator must match your network's proxy.

When first installed, ICE tries to reach the Internet directly, with no proxy, for updates and for sending its scan data. ICE supports HTTP proxy servers only. It does not support SOCKS proxy servers.

To set the proxy settings for ICE:

1. Open the **ICE Administrator** from your programs.
2. Click the **Proxy Settings** button. The Proxy Settings window appears.
3. Select the type of proxy from the **Proxy type** box.
4. Enter the information for your network's proxy server.
5. Click **OK**.

You will need to stop and start the ICE and Updater services for them to use the new proxy settings.

If you do not know the proxy settings, select the **Detect** button and ICE will try to detect the proxy settings already set in Windows. We recommend confirming the correct settings with your IT department before applying them.

You can also test the proxy settings by selecting the **Test** button.

Detailed information on the Proxy Settings window

Proxy types are as follows:

No Proxy: ICE contacts the Internet directly. This is the default setting, and it works where an organization does not use a proxy server.

Custom: You enter the address and port of your organization's proxy server yourself. We recommend this option because it makes it very clear what is going on. If your proxy server requires authentication, tick the **Proxy requires authentication** box and enter the login name and password.

Auto Discover: Uses the Web Proxy Auto Discovery Protocol (WPAD) to find the correct proxy server. If ICE cannot find one using WPAD, it falls back to No Proxy. This option can increase the time Internet calls take if your network is not configured for WPAD. If your proxy server requires authentication, tick the **Proxy requires authentication** box and enter the login name and password.

Logged In User: Provided for backwards compatibility with earlier versions of ICE. It uses the proxy settings set in Windows for a particular user. To use it, the ICE and Updater services must be configured to log on as the user named in the Login box. We recommend the Custom option instead wherever possible.

Address: The server address of the proxy server. Used only for the Custom proxy type.

Port: The port the proxy server listens on. Used only for the Custom proxy type.

Proxy requires authentication: Tick this box if your proxy server requires user authentication. Required for the Logged In User proxy type.

Login: The user name required to log in to the proxy. For some proxy servers and network configurations you may need to enter it in the DOMAIN\USERNAME format.

Password: The password required to log in to the proxy server.

Custom Scan IP Ranges

To set custom IP ranges to scan, open the ICE Administrator, go to **File**, then **Configuration**, and select **Use Local Configuration Only**. Once a checkmark shows beside it, select **View/Edit Configuration**. Here you can set the IP ranges.

By default, ICE uses the IP address and subnet mask of the computer it runs on to decide which addresses to scan, and to work out the broadcast and network addresses.

With a custom scan range, the subnet mask is used only to work out the broadcast and network addresses so that ICE does not scan them. To limit the range of addresses, use the start and end of the range, not the subnet mask.

ICE accepts a scan range of a single address.

Best practices

Limit scanning to the subnets where printers will be found. If the network is made up of many subnets, scan only those that have printers.

Within a subnet, limit scanning wherever possible to the address range where printers will be found. If printers are always given IP addresses above 200 on a class C subnet, do not scan all 254 addresses. Configure ICE to scan just the 54 addresses where printers will be found.

If you have any further questions, please contact Technical Support at service@theprinterdoctor.ca