



CirrusPrint™

Cloud and Network Printing

© 2014 Synergetic Data Systems Inc.

CirrusPrint™

Cloud and Network Printing Software

CirrusPrint simplifies and streamlines network printing. As companies move their computer operations to the cloud, or as they add remote locations connected over the Internet or VPN, printing configuration becomes complex and print speed becomes troublesome. Documents that printed instantly locally take many seconds or even minutes to print remotely.

CirrusPrint enables patent-pending compression techniques to reduce data in your print jobs, and provides simplified configuration of printing between locations in a network or in the cloud.

Table of Contents

Foreword	0
Part I Introduction	5
Part II Architecture	7
Part III Installation	9
1 Install On Unix.....	10
2 Install On Windows.....	12
3 Licensing.....	13
4 Uninstalling.....	14
5 Firewall and NAT Configuration.....	15
6 Updating to 1.0.07 or higher.....	16
Part IV Operation	17
1 Running on Unix or Linux.....	18
Automatic Startup	19
Licensing Script	20
Browser-based Operation	21
2 Running on Windows.....	22
Status Tab	23
Port Configuration Tab	24
License Tab	25
Part V Getting Started	27
Part VI Browser Interface	29
1 Login.....	30
2 Menu Options.....	31
3 Configuration.....	32
Remote Locations	33
Remote Devices	34
Local Ports	37
Local Paths	38
Service Settings	39
Users	41
4 Monitoring.....	42
Status	43
Log Viewer	44
Job History	45
Part VII Remote Location Clients	46
1 Installation on Unix.....	47

2	Installation on Windows.....	49
---	------------------------------	----

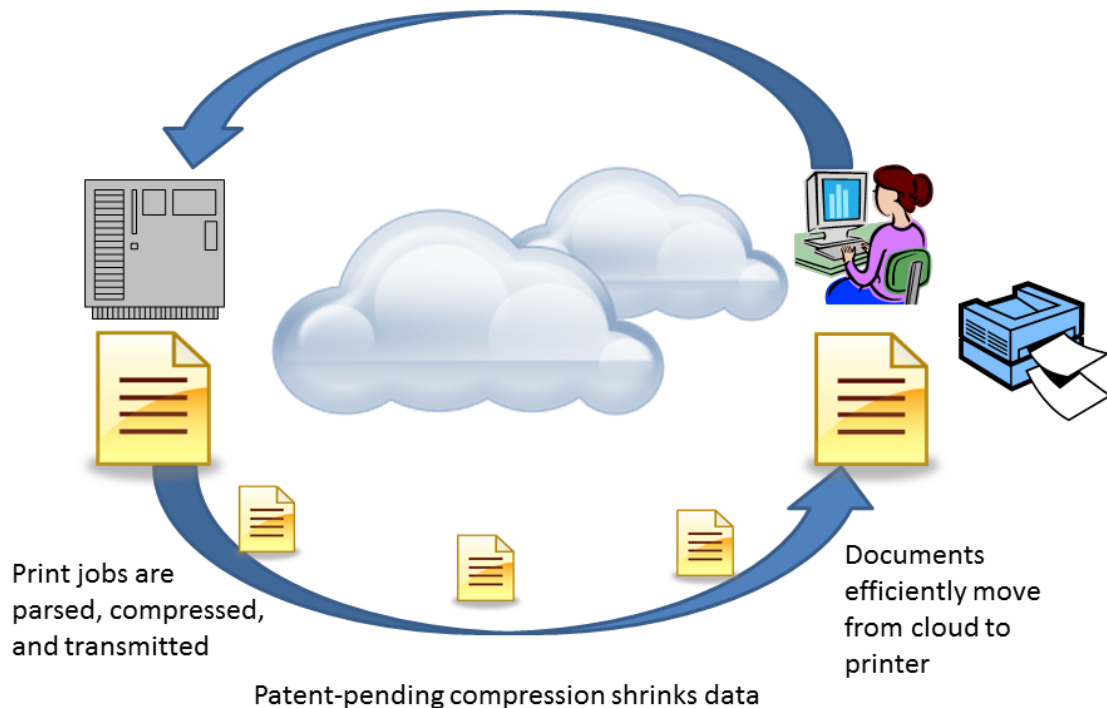
Part VIII Additional Information 50

1	Autosend Paths.....	51
2	Transferring To A New Server.....	52

1 Introduction

Welcome to CirrusPrint™, software to manage and streamline remote printing and document transfer between your cloud-based computer systems and local printers and file storage systems.

CirrusPrint™ Cloud and Network Printing



The Problem

As companies move their computer systems and business applications to cloud and hosted systems outside of their own networks, they find printing slows down and becomes difficult to manage. Unlike software applications, printers must remain local to the users they serve. Printing over the Internet or any wide area network, with its relatively low speed, becomes a bottleneck. Users wait longer than before for their documents to print, and the act of printing adds to the overall network usage. In addition, print data must be secured so that as it travels over the Internet, it can't be captured by third parties.

And these same issues can also apply to file-oriented documents, where there is a need to transfer them securely and efficiently between systems across the Internet.

The Solution

With CirrusPrint, the systems that create your documents can be anywhere, and you can still print and store those documents locally. Document distribution is also easy to manage, so that one print run can appear in multiple locations or on multiple printers.

Security is maintained as documents are transferred across the network, using SSL, an important feature when using the public cloud. SSL is optional, however, in cases where document security is

maintained in other ways, such as a VPN.

When documents are transferred, CirrusPrint uses both standard compression and patent-pending anti-redundancy techniques. This makes the data transfer as efficient as possible, with significant byte count reductions to reduce the time and overhead of document transfer.

Key Features

- High performance wide-area network printing
- Very high compression ratios through patent-pending anti-redundancy techniques, even of already compressed PDF documents
- One to one, or one to many, document distribution features: one file to many desktops, for example
- Secure document transmission using SSL
- Stateless design, so document transmission can occur as remote sites are available
- Exact replication retains features such as duplex and tray control
- Server-centric configuration via browser interface

2 Architecture

A CirrusPrint server listens on ports and paths for print jobs produced by a server application. As jobs arrive, they are parsed and compressed, and delivered to remote locations. Those locations run CirrusPrint client software designed to monitor for jobs, receive and uncompress them, and deliver them to printers and files at the remote locations.

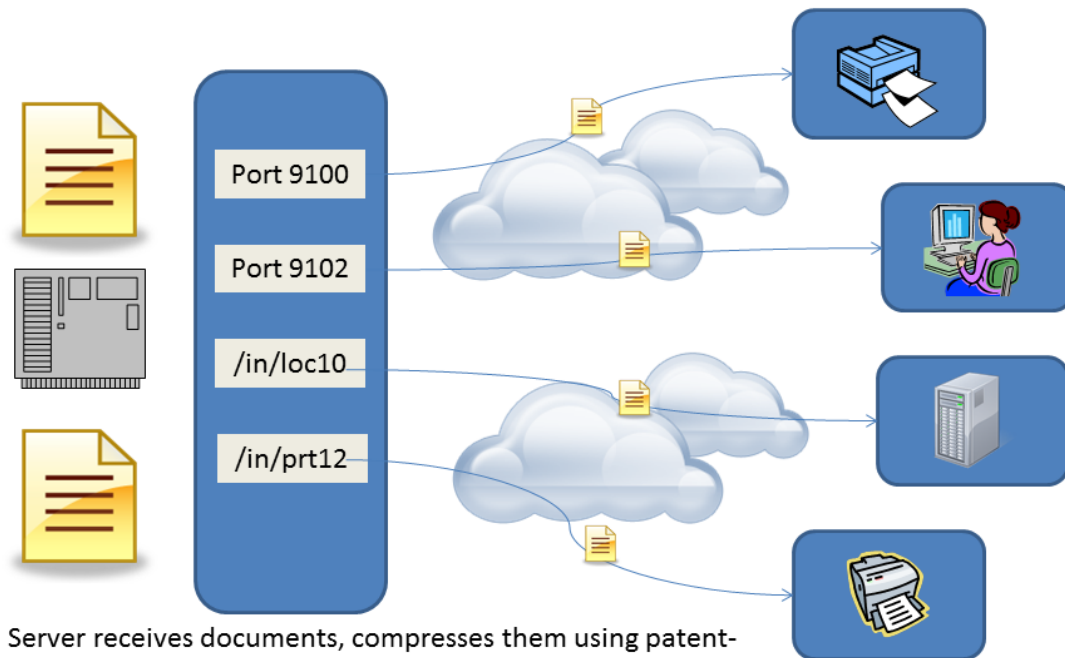
Ports

The server is configured to listen on any number of ports. These ports behave like a raw print port on a network printer. Once configured, system printers can be configured to print to the ports on the CirrusPrint machine rather than a port (typically 9100) on the printer itself. As print jobs arrive on these ports, they are forwarded to the remote devices configured for each port.

Paths

The server can also be configured to monitor paths, for all or selected files that appear in those paths. Files can be selected by wildcard patterns, like *.pdf for only PDF files, or invoice* for any files starting with "invoice". As files arrive in the paths, they are picked up and forwarded to remote devices or files configured for each path.

CirrusPrint™ Architecture



Server receives documents, compresses them using patent-pending techniques, then distributes them to remote network locations, where they are uncompressed and printed or stored.

Server

The Server is generally installed on a system where the printing application is running, though it could also be installed on another system on the local network where that application runs, or on an out-of-

network machine that provides high network performance. Data transferred from the application system to the Server is not compressed, so high speed and low cost bandwidth is important.

The following elements are configured at the Server:

- [Remote locations](#) - systems where CirrusPrint clients are installed, including authentication information.
- [Remote devices](#) - printers or file destinations at the remote locations.
- [Local Ports](#) - network ports that simulate a network printer and forward documents to one or more remote devices.
- [Local Paths](#) - file system locations where documents are picked up and forwarded to one or more remote devices.

Location Clients

Clients are configured to connect with a Server. When started, the Client opens a secure connection to a Server, logs in, and waits for document deliveries. The Client and Server communicate using techniques to reduce the amount of data that is transferred. Both standard compression and patent-pending anti-redundancy techniques are used to dramatically reduce the amount of data that is transferred between the application and remote printers or files.

Browser Access

The server includes an internal web server, used for configuration and monitoring. You can connect to this server using any modern web browser, specifying the listening port in the address, such as <http://192.168.1.12:8285>.

A login screen is presented, followed by a [menu](#) offering server monitoring tools, and if you are logged in as an administrator, configuration tools. The default admin login is "admin", password "admin". This administrative login should be changed as part of the initial configuration, using the [Users](#) tool.

3 Installation

The CirrusPrint server is available for Windows and many Linux or Unix systems. Installation is a simple, quick process, following instructions in these chapters:

[Install on Unix](#)

[Install on Windows](#)

After installation, read the following chapters regarding running the server. These instructions also include sub-chapters on licensing:

[Running on Unix](#)

[Running on Windows](#)

There are separate chapters regarding installation of the CirrusPrint remote location client software:

[Install Client on Unix](#)

[Install Client on Windows](#)

3.1 Install On Unix

The Unix installation process involves a few steps with the command line, and assumes you have the installation tar.Z file available on the system. You should be the superuser (root) to perform the installation.

1. Create a directory to install the software in, and make it the current directory. This should be on a file system with at least 100MB of free space, though actual disk space need can vary considerably depending on many factors, such as they variety and types of documents you print, and how high or low log and cache purge settings are defined. If you aren't sure, just pick the file system with the most available space.

If there are multiple installs on this machine, choose directory names based on how you wish to identify the different installations, such as by tenant name. The last element of the directory is used to create a unique script for this install. In the examples below, the name "install1" is used. **Be sure the final segment of the install path is unique to avoid script conflicts.** To see existing names, use `ls /usr/bin/cp10_*`.

If you are updating an existing 1.0 installation, use the existing installation directory.

```
mkdir -p /data/cirrus/install1  
chmod 777 /data/cirrus/install1  
cd /data/cirrus/install1
```

2. If the server is already installed in this location, you should stop it at this point:

```
cp10s_install1 stop
```

3. Uncompress and extract the contents of the downloaded tar file. For example, if the tar file is available in the /tmp directory:

```
uncompress /tmp/cp10_linux_x86_tar.Z or gunzip /tmp/cp10_linux_x86_tar.Z  
tar xvf /tmp/cp10_linux_x86_tar
```

Some Linux systems do not have the uncompress command, but you can use gunzip in place of uncompress.

Some systems support a "z" option on the tar command, which performs decompression automatically, so you could enter just one command:

```
tar xvzf /tmp/cp10_linux_x86_tar.Z
```

4. If this is a new installation, run the setup.sh script. This script will prompt you to view and accept the CirrusPrint license agreement.

```
./setup.sh
```

5. Also if this is a new installation, or you have upgraded your license count and require manual licensing, run the license.sh script to activate the software as a demo or live product.

```
./license.sh
```

6. Start the server with the following command:

cp10s_install1 start

When the server is running, you can use the [browser interface](#) for monitoring and configuration. The browser interface provides extensive monitoring and configuration tools. This interface includes extensive browser-based help.

CirrusPrint uses two ports, one for the service for clients, and one for browser management. This default ports are 8284 and 8285, respectively. If another program or another CirrusPrint install uses the default ports, you must edit cp10s.ini in the install directory to have this instance use different ports, or different bind addresses. Edit the port= lines and/or bindto= lines in the [service] and [httpd] sections.

Remote clients must be configured to connect to the correct address and port for this installation instance.

3.2 Install On Windows

Run the cp10s_setup.exe program to install CirrusPrint on a Windows server. This will run an installation wizard, including panels for acceptance of the license agreement and the install location. The default installation location is C:\SDS\cp10\server, which is the recommended location for single-tenant installations.

There can be many installations of the server on one system, each to its own directory and managed independently. The last element of the directory name is used in shortcuts and services, to identify which installation is being operated on, so check for existing names before choosing a location for a new installation. To update an installation to the current version, install over the top of an existing install folder. Note that a CirrusPrint server must be stopped in order to update it.

Be sure the final segment of the install path is unique to avoid service name conflicts. To see existing names, use the Windows services manager and look for services starting with CirrusPrint 1.0 Server.

Do not choose a "Program Files" location to avoid security issues with Windows. Be sure to choose a disk that has plenty of disk space available, as CirrusPrint utilizes disk for caching and logging. At a minimum, the disk should have 100MB or more free space, though the needs of CirrusPrint can vary widely based on job volume and content.

The setup program installs the software for the user who runs it. This is typically an Administrator, so login appropriately before running the setup.

Once the setup is complete, there will be some new entries on the Start, Programs menu, under CirrusPrint 1.0 Server. One or more of these is the CirrusPrint Manager (*location*), which is used to perform some key functions for this installation:

- License the server for demo or live use
- Configure the server's ports, if necessary to avoid conflicts with other applications or other CirrusPrint installations on this machine
- Start and Stop the server
- Install or uninstall the server as a service
- Access the server's [browser interface](#) when the server is running

There is help available for the CirrusPrint Manager within the program, by clicking the help icon on the toolbar.

The browser interface also includes a help system. The browser interface provides extensive monitoring and configuration tools.

3.3 Licensing

There are three types of licenses: demo, permanent, and emergency.

A demo activation is available at any time and without a serial number and PIN code. This type of activation is limited to 30 days of use and 5 devices, and is used to evaluate the software.

A permanent or emergency license is assigned a serial number and PIN code specific to the machine it is installed on. Part of this license is the number of active devices the license supports. See License Counts, below, for details.

A permanent license will run perpetually on the machine and in the location where it is installed, and will deliver jobs to remote locations so long as the license period has not expired. A System ID and machine class identify the machine the software is installed on and is required to obtain a permanent license, as they are used to generate the permanent activation keys. Note that if you move it to a new machine, or even to a new location on the current machine, the system ID to which the permanent keys are linked will change and a license reset is required.

An emergency license is available in cases where you have a serial number and PIN code, and need to get a new machine up and running right away, without waiting for a reset. The System ID and machine class are not used to generate an emergency license. This license will run for 30 days, by which time you must obtain the reset and activate the license as permanent.

View the [Licensing Script](#) and [License Tab](#) chapters for details on licensing for Unix and Windows, respectively.

If there are multiple installations on a single machine, each installation has its own system ID and must be licensed separately, using unique serial numbers.

License Counts

A permanent or emergency license is granted a license count, which indicates how many active devices can be configured. A device represents a remote location printer or file path definition, specifying anywhere a print job or document file can be delivered. Inactive devices, and the automatic "autosend" devices, are not counted in this limit.

License Periods

Licenses have an expiration date, and are generally renewed monthly via an automatic process. When a license approaches its expiration date, it should be renewed. There is a seven-day grace period during which the software will function normally after the expiration date, but after seven days, and up to thirty days, the software will delay job delivery by up to one minute, and licenses over thirty days beyond their expiration date stop delivering jobs (though jobs will continue to be spooled).

License data is downloaded whenever the server is started, and also on a daily basis, to ensure continuous operations. Internet access to the cirrusprint.com website from the server is required.

When a license has expired, events are logged in the server logs, and if email information has been configured in the browser interface [Service Settings](#) screen, notices are also sent by email.

Licenses are also available without expiration dates, for a one-time license fee, plus annual maintenance fees to enable access to new versions.

3.4 Uninstalling

To remove CirrusPrint from a machine, follow these instructions:

Unix

Remove the `/usr/bin/cp10s` script.

Remove the install directory and subdirectories.

Windows

Use Control Panel, Programs and Features. Select the CirrusPrint Server that references the install folder you want to remove, and click Uninstall. This will attempt to automatically stop and remove the CirrusPrint service first, but you may choose to manually perform these steps first, using the CirrusPrint Server Manager.

In most cases, this will remove all installed files from the installation folder, and the server's Start, Programs menu folder. However, if permission settings prevent this, or a CirrusPrint program is running or folder is open, this can be performed manually at later time.

3.5 Firewall and NAT Configuration

Firewall Configuration

Each CirrusPrint server uses two network ports, one for remote clients and one for the browser interface, which is used to configure and monitor the system. By default, these two ports are 8284 and 8285, respectively. Additional installations on one machine are configured to use different ports and/or different 'bindto' addresses. These ports must allow connections from external systems, and it is common for a firewall to block access to these ports. Therefore, a system administrator should configure the firewall on the system where CirrusPrint is installed to allow access from the systems that will run client software or access the browser interface.

In some cases, only the client port needs to be opened up. If the browser interface will only be accessed from the CirrusPrint machine itself, or an open local network address, a firewall change might not be needed for that port.

If you do open the browser interface port to the Internet, consider turning on SSL security for the browser interface in [Service Settings](#).

NAT Configuration

If a CirrusPrint server resides on a system behind a router, and remote clients need to access it through that router, then an administrator will need to configure the router to forward these ports to the CirrusPrint machine. Most routers provide a browser interface to configure this, often calling ports "services", since many common services are associated with specific ports (like port 80 for HTTP).

3.6 Updating to 1.0.07 or higher

CirrusPrint 1.0.07 adds multi-install capability, through changes that allow multiple installations on a single machine, where each installation can be independently operated. There were modifications to the installation and setup to utilize the installation path, more specifically the last segment of it, as a name for the Windows Service or `/usr/bin/cp10s_install` script name.

For example, if you installed CirrusPrint to `C:\SDS\cp10\acme`, the Windows Service for that installation will be named "CirrusPrint 1.0 Server (acme)". Likewise, on Linux, if you installed to `/usr/local/cp/acme`, the management script would be called `/usr/bin/cp10s_acme`. Note the default installation path on Windows is `C:\SDS\cp10\server`, so the resulting default service name and shortcuts all have "(server)" in their name.

Each server requires two unique ports to listen on (or optionally unique IP addresses if configured to bind to a particular address on a multi-address machine). Therefore, before starting a CirrusPrint installation, you need to ensure that it is configured to listen at unique address/port values. The Windows CirrusPrint manager provides a configuration tab for this purpose. On Unix, you can edit the `cp10s.ini` file located in the install directory, editing `port=` lines and/or `bindto=` lines in the `[service]` and `[httpd]` sections.

Updating Existing Directory

On Windows, the previous service name of "CirrusPrint 1.0" is not detected by the CirrusPrint server manager. This will enable the toolbar button to install the service, and this process will remove the old name from services before installing the new name. Note that the systems Programs and Features will show two installations, both the old and new. Leave both present, since uninstalling either will remove the contents of the directory they both point to.

On Unix, the `/usr/bin/cp10s` script is removed as the new `cp10s_install` script is added, when you run `setup.sh`.

Adding New Directory

If you install 1.0.07+ in a new location, and an older installation exists elsewhere, the old Windows service remains active, starting CirrusPrint in the old directory, and the new install-specific service is added. Likewise, on Unix the old `/usr/bin/cp10s` script remains and can still be used to manage the older installation directory.

Transition to New Directory

You can quickly transition to a copy of an older installation in a new directory, with minimal disruption to operations, following these steps:

- Install to the new directory
- License the new installation, using an emergency temp license request (or pre-request a license reset)
- Copy the `cp10s.ini` file and the contents of the "data" directory from the old installation location to the new location, which will provide a duplicate configuration (note that only one instance of the server can run at a time, since they would attempt to listen on duplicate ports)
- Stop the old server, and start the new server
- Once you've confirmed proper operation, uninstall the old server
- Request a license reset, then license the new installation as a permanent license (if you used an emergency temp license previously)
- On Windows, install the new instance as a service

4 Operation

The CirrusPrint server includes tools to start and stop the server, and to install it to run automatically as a service.

Instructions are available for both [Unix](#) and [Windows](#).

4.1 Running on Unix or Linux

The CirrusPrint server can be started and stopped from the Unix command line. Each install location has its own script in the /usr/bin directory.

cp10s_install start	Starts the server
cp10s_install stop	Stops the server
cp10s_install restart	Stops, then restarts the server

Once running, CirrusPrint will listen for location connections on one port and browser connections on a second port. These ports are configured in the cp10s.ini file, so if you need to manually adjust the ports, edit that file before starting the server.

The default port for location connections is 8284, and for the browser interface is 8285, so from a browser, use a URL like `http://192.168.1.10:8285` or `http://printserver:8285` in your browser. If the configuration indicates the browser interface is secure, use "https" rather than "http" in the URL. The secure setting is defined in the [httpd] section of cp10s.ini.

4.1.1 Automatic Startup

You can also configure the system to automatically start CirrusPrint when it boots. There are two techniques for this, and they can vary by your exact operating system.

- Add a line to `/etc/inittab` to run `cp10s_install` start one time at all regular run levels

```
cp10_install:2345:once:/usr/bin/cp10s_install start
```

- Create a script `S99cirrus`, and place this script in any `/etc/rc#.d` directory associated with normal run levels (typically `/etc/rc2.d`, `/etc/rc3.d`, or `/etc/rc5.d`). It doesn't hurt to place the script in levels 2, 3, and 5. The script can be as simple as:

```
#!/bin/sh
cp10s_install start
```

If there are multiple installations on a single machine, each install has its own script and all should be started. Simply add more lines to `/etc/inittab` or the startup script code.

4.1.2 Licensing Script

The `license.sh` script is used for licensing CirrusPrint on Unix or Linux systems. To run this, login as the root user and make the CirrusPrint server directory the current directory. Then use `./license.sh`.

This presents the following menu:

```
CIRRUSPRINT LICENSING OPTIONS
```

```
Use the following options if this machine is connected to the Internet:
```

- ```

1 - Permanent Activation (requires serial number and PIN code)
2 - Emergency Temporary Activation (also requires SN and PIN)
3 - 30-Day Demo Mode Activation
```

```
Use the following options for manual activation. Activation keys
can be obtained from http://synergetic-data.com/cplic.cgi.
```

- ```
-----  
4 - Display System ID and machine class (needed for option 5)  
5 - Enter Permanent Activation  
6 - Enter Emergency Temporary Activation  
7 - Enter 30-Day Demo Mode Activation
```

Options 1, 2, and 3 use the Internet to obtain activation information, and automatically activate the product. Options 5, 6, and 7 are the equivalent but require you to obtain activation information from another computer that does have Internet access, and type it (or copy/paste it if possible) into the CirrusPrint system. Option 4 provides the active system ID and machine class, if you need to obtain a permanent activation manually.

For more details about types of licenses, see the [Licensing](#) chapter.

4.1.3 Browser-based Operation

The Unix/Linux `setup.sh` script creates an Apache include file `web/cirrusprint.conf`. On systems with an Apache web server, this file can be copied to the `/etc/httpd/conf.d` directory. Once the Apache server is restarted, open the <http://hostname/cirrusprint> URL to perform select server operations. You can edit this script if you need to enable `VirtualHost` directives. The `Server` button of this page presents a sub-page with several options, including:

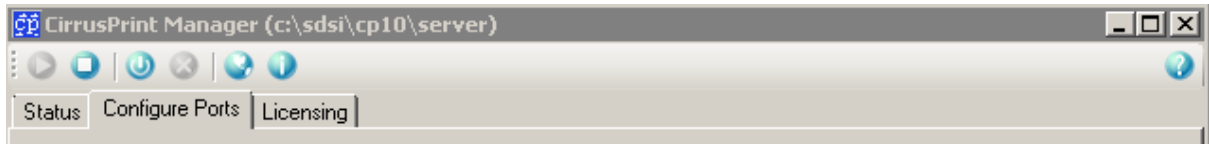
- A link to the internal server manager, which listens on port 8485 by default
- Options to stop and start the server
- Options to license the server in demo, permanent, or emergency temp mode.

In addition, there are `About` and `Manual` buttons to display some general CirrusPrint information and view this manual.

Open Access

By default, this include file provides open access to the `/cirrusprint` URL. If this is a publicly accessible server, you probably want to limit access. Follow Apache guidelines for securing this path, via access control or authentication. The `cirrusprint.conf` file contains commented lines to assist in access control. Authentication must be set up by the Apache administrator.

4.2 Running on Windows



You can use the CirrusPrint Manager application for any given installation, available from the Start, Programs menu, to manage operation of the CirrusPrint server on Windows.

At the top of the manager window is a toolbar offering several options. From left to right:

- Start the server running
- Stop the server
- Install the server as a service
- Uninstall it as a service
- Access the browser interface
- View the manual
- Help (at the far right of the toolbar)

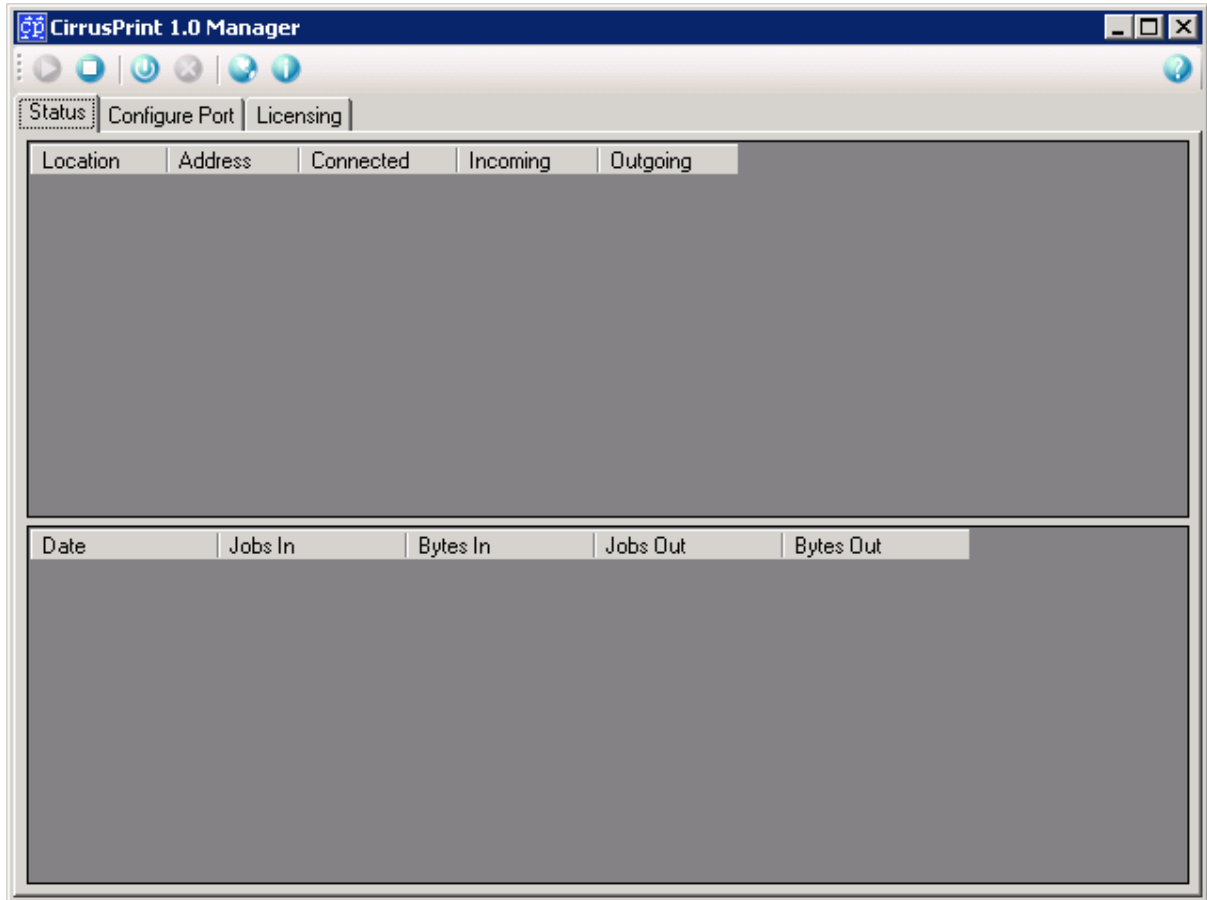
Different options may be available at different times. For example, if the server is not running, the stop and browser access buttons are disabled.

There are three tabs available with varying information.

- [Status](#)
- [Configure Ports](#)
- [Licensing](#)

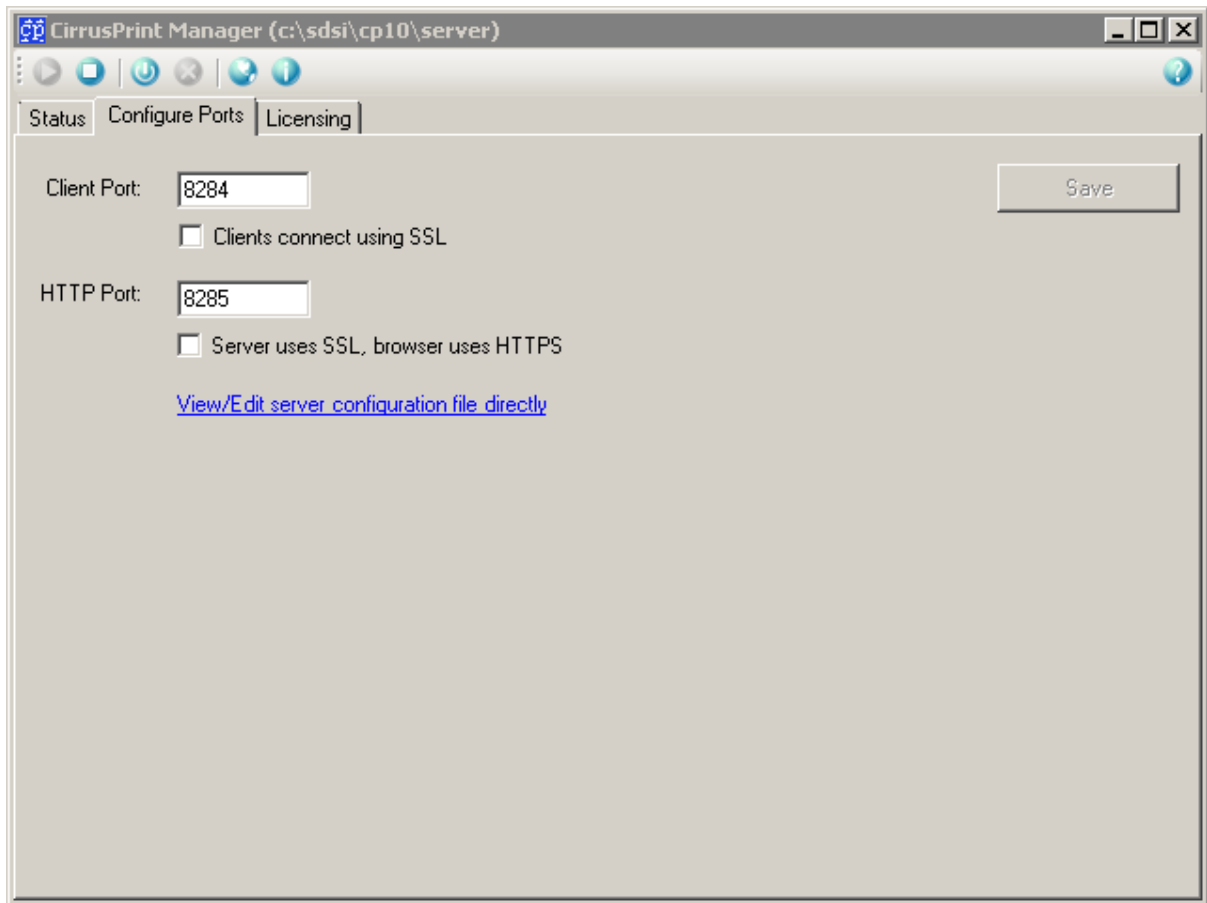
4.2.1 Status Tab

This tab provides a periodic snapshot of server information when the server is running. It shows remote location connections in the upper table, and summary job statistics in the lower table. More detailed information, such as logs and individual job history, can be accessed in the [browser interface](#).



4.2.2 Port Configuration Tab

In cases of port conflict, such as when multiple installations are on the same machine, it is necessary to change the client and HTTP ports from their defaults. If so, you can edit the value and Save it here. You can also view and edit the complete configuration file (cp10s.ini) by clicking the link on this tab.



4.2.3 License Tab

This tab is used to license the server. If you have an Internet connection on this machine, it is easiest to use the automatic activation features. If not, you can use the Manual Licensing feature in conjunction with the license server at <http://cirrusprint.com>, which you can access on another machine that does have Internet access.

Demo License

Click Automatic Activation if the system is connected to the Internet. Two activation keys are downloaded and installed automatically.

For manual activation, obtain current demo keys from the Internet on another machine, and copy/paste them into the Key 1 and Key 2 fields, then click Activate.

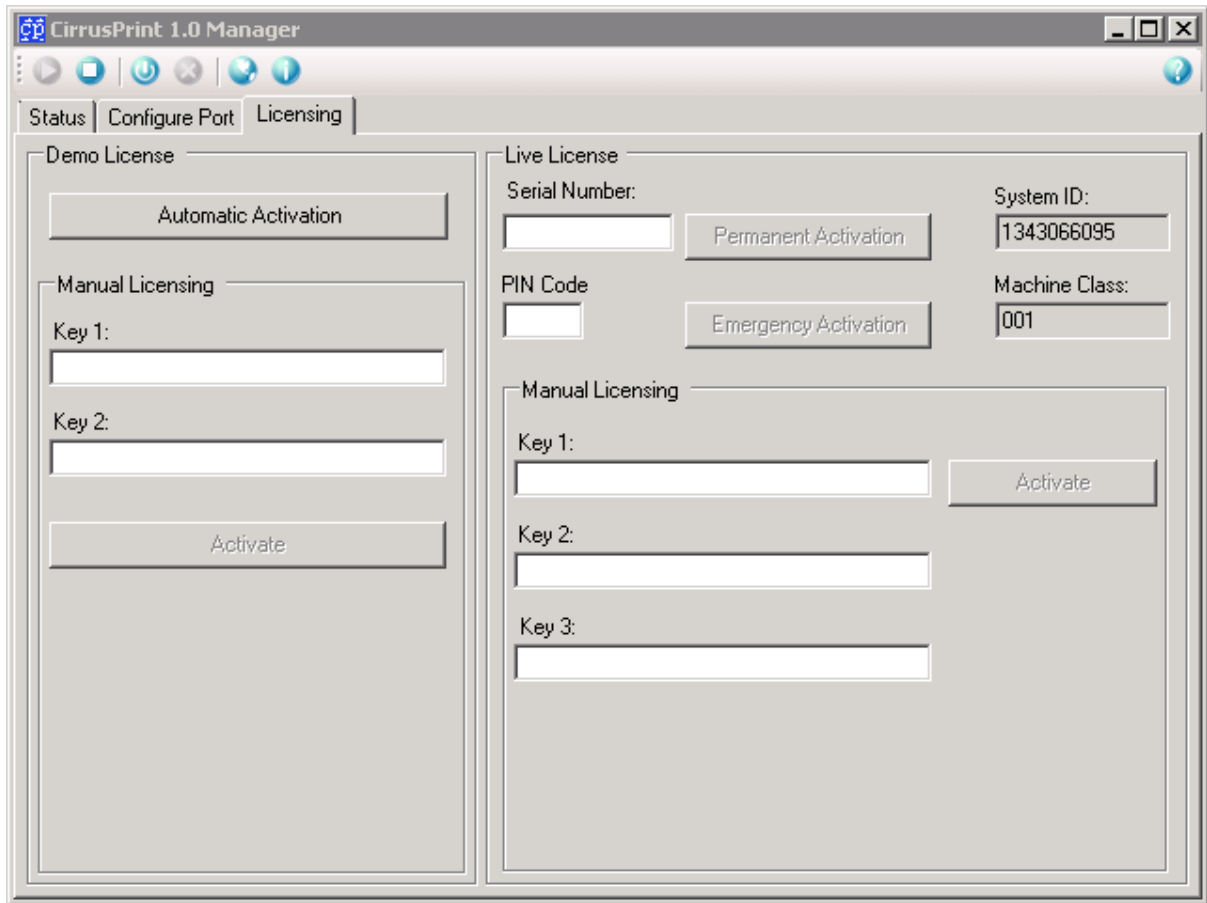
Permanent or Emergency License

Enter the serial number and PIN code provided with your license, then:

For automatic activation, and click the appropriate Permanent or Emergency button. Three keys are downloaded and installed automatically.

For manual activation, use a system that is connected to the internet. With your serial number and PIN code, and for a permanent activation the system ID and machine class displayed here, and obtain activation keys, then paste them in to the fields for Key 1, Key 2, and Key 3, and press Activate.

For more details about types of licenses, see the [Licensing](#) chapter.



5 Getting Started

Once CirrusPrint is installed and started, the next step is to configure it to print or transfer files to one or more remote locations. This involves several browser interface screens.

Configure a Remote Location

Remote locations are systems that will run the remote location client software, designed to receive and process files and print jobs sent from the CirrusPrint server. The server assigns an ID and password to each remote location, and clients are installed and configured to login to the server using that ID and password. To set up one or more remote locations, use the [Remote Locations](#) menu option.

Once a location has been configured, install the [client software](#) on a system at that location, and configure it to connect to the CirrusPrint server, using the location ID and password. As soon as that location connects successfully, it will upload a list of printers to the server, assisting in the next configuration step.

Configure a Remote Device

Remote devices are where files or print jobs are delivered. A remote device can be a printer, such as a Windows printer or a Linux spool queue, or it can be a file, where the file name can include parameters to ensure uniqueness or produce a logical naming convention. It can also be a command on the remote system, where the file is passed to a command line for processing.

Remote devices are given an ID, a device type, and a device path or name. When configuring a device, the list of printers provided by the remote location is presented, allowing simple copy/paste of printer names when configuring printers. The following types of devices are supported:

- **File** - a file is created on the remote system, based on a path and substitution parameters.
- **Command** - A command line is run, typically with the substitution parameter {file} to use the file created at the remote location. This type of device can easily print to a Unix or Linux spool queue.
- **Win Printer** - A Windows printer name when the client runs on a Windows system. Note that jobs sent to this printer must be compatible with the printer, so care is required to select a compatible print driver when printing jobs that go to this device.
- **Network Printer** - A network name or address of a printer.
- **Open Document** - A file is created, typically in a temp or work directory, and the client opens the document when received. This type of device is effective when location clients are installed on user desktop computers.

Each remote location can have any number of devices configured. One device, a file transfer device called "autosend", is automatically created (and not counted for licensing purposes). To set up remote devices, use the [Remote Devices](#) menu option. First select a location, then edit or add devices for that location.

Configure Local Ports

Local ports provide one of the two ways jobs can be submitted to the CirrusPrint server and delivered to a remote device. Typically, ports are used for print jobs. System spoolers and many applications can print to a network printer, and that is exactly how a CirrusPrint local port operates. When a print job arrives on a port, CirrusPrint stores and parses the job, then queues it for a specific remote location

device (or more than one device if you configure it that way). If a remote location is connected, it receives jobs immediately. If not, the server keeps the job until the location connects and receives it.

Ports are configured with an ID and a TCP/IP port number. Network printers typically listen on port 9100, so it is common to use a range of ports in the 9000 range for CirrusPrint, but in fact, any available ports can be used, from 1025 through 64000. Ports are also configured to target one or more remote devices. Whenever a job arrives on the port, these are the devices where the job gets delivered.

To set up local ports, use the [Local Ports](#) menu option.

On Windows, once a port has been configured, a Windows printer port is added named "cp_portid". When updating printer definitions on the server, simply select this port for the printer. On other systems, printers are simply configured to print to a network printer, specifying the CirrusPrint server and port as the "printer" and port number. When configuring a printer to print to the port, be sure to use a print driver that is compatible with the target device. If possible, use the manufacturer's print driver.

Configure Local Paths

The CirrusPrint server can monitor directories for files to arrive. Typically paths are used to transfer document files to remote locations, for storage or viewing. When a new file appears in a directory, it is picked up, parsed, and queued for a specific remote location device. If a remote location is connected, the file is delivered immediately. If not, the server keeps the job until the location connects and receives it.

Paths are configured with an ID, a directory name, and an optional wildcard mask to limit what files are picked up by that path definition. Paths are also configured to target one or more remote devices. Whenever a job is picked up for this path definition, these are the devices where the job gets delivered.

To set up local paths, use the [Local Paths](#) menu options.

6 Browser Interface

The CirrusPrint server includes an internal HTTP server, accessed by any web browser. This interface is used to monitor the server and manage its configuration.

6.1 Login

In order to view server activity or edit the server's configuration, you must login with a user ID and password. An administrator user can set up user logins and edit the configuration.

When first installed, there is an administrative login defined (login=admin, password=admin). Logging in with this initial user will allow other users to be defined, and the admin account password to be changed.

6.2 Menu Options

The main menu is accessed with any modern web browser, pointed to the server and configured listening port. The default port is 8285, so a URL to access the server would look like: `http://x.x.x.x:8285`, where `x.x.x.x` is replaced with the IP address or host name of the server. The default login is `admin`, password `admin`.

All Users

- [Status](#) is used to view license, connection, and data summary information.
- [Logs](#) is used to view the daily server logs, which display server activity.
- [Jobs](#) is used to monitor recent jobs, to see completion status and document transfer efficiency levels.

Administrators

- [Remote Locations](#) is used to create, edit, and delete remote locations. Each remote location will have a CirrusPrint location client installed and configured to communicate with this server.
- [Remote Devices](#) is used to create, edit, and delete remote devices. Each remote location can have one or more devices. Devices is a term used loosely, as a *device* can be a printer, a command line, or a file at the remote location.
- [Local Printer Ports](#) is used to create, edit, and delete printer ports. A printer port is a raw listening port that a print spooler or other application can print to. These ports simulate a network printer interface. Each port can be configured to forward the print job to any number of remote devices.
- [Local Paths](#) is used to create, edit, and delete path monitors, which watch for files to arrive in specific paths. Those files are then forwarded to any number of remote devices.
- [Service Settings](#) is used to edit server configuration settings.
- [Users](#) is used to create, edit, and delete users who have access to the server's browser interface.
- **Restart** is used to restart the server after a configuration change. This supplements the system-level operation programs, which can be used to stop, start, or restart the server.

6.3 Configuration

Administrative users can configure the server using various options from the main menu.

- Server operation options, such as the main listening port and logging details, are configured using [Service Settings](#).
- Users, both admin and standard users, can be edited using [Users](#).
- Remote locations, including the shared secret password a location uses when connecting, are edited using [Remote Locations](#).
- Each remote location can have one or more devices, configured in [Remote Devices](#). Devices include printers, command lines, and file system locations where documents can be delivered.
- Local printer ports are listening sockets that wait for print jobs to be received. This simulates a network printer, so any system that can print to a network printer can send print jobs to the server. When print jobs arrive, they are transported to configured remote devices at one or more locations. Ports are configured using [Local Ports](#).
- Paths on the local file system can be monitored for document files. As files arrive, they are transported to configured remote files or devices at one or more locations. Paths are configured using [Local Paths](#).

6.3.1 Remote Locations

To receive jobs from the server, a remote location must connect and login to the server. The server must have a table of known locations and their passwords in order to authenticate the connection. The locations are identified by a location ID and a password.

A location ID might also be thought of as a user ID, in cases where different users at one location might have individual connections to receive jobs. It is possible, therefore, to have jobs sent to personal printers or user folders or desktops.

The initial screen is a list of known location ID's. From this screen, you can select a location to edit, or add a new location by pressing the New button.

Location ID is the unique ID for a given location. The client software at this location must be configured with this ID when it connects to this server.

Description is an information field.

Password is the password the location client must provide when connecting to this server. The client software at this location must be configured with this password. This entry is obscured when editing. Click the Show Me button to see the password text.

Location is inactive, if checked, indicates this location can't connect, though the location record remains on file.

Allowed IP is a semi-colon delimited list of IP addresses or wildcards. If this value is filled in, the location must connect from an address matching one of the values. Note that this is the IP address from the server's viewpoint, which may differ from the remote client's internal IP address if access is through a router that does address translation. If you aren't sure what a location's IP address is from the server's viewpoint, temporarily leave this field blank, then monitor server logs as the location connects, and its IP address will be visible. Note also that IP addresses can be dynamic, though in that case they will likely be from a range, so a wildcard might be appropriate.

Press the Save button to save any changes, or the Delete button to remove an existing record.

When a location created, an "autosend" local path and remote device is created, named to match the location ID.

6.3.2 Remote Devices

When jobs are received by the server and delivered to a remote location, they are delivered to a *remote device*, a term used somewhat loosely. A remote device is a printer, file, or command line that is printed to, copied to, or executed when a job's data is delivered.

An autosend remote device is automatically configured for each location. This moves files from the server's "autosend/*locationID*" path to the location client's "autosend/*server*" path.

To edit or add a remote device, first select a location, then select an existing device ID or add a new one using the New button. Locations are defined in the [Remote Locations](#) tool.

Device ID is an identifier for this device at the location specified. It must be unique for the location.

Description is an information field.

Device defines the type of device and the value or name of the device.

There are five types of devices:

- File
- Command
- Win Printer
- Network Printer
- Open Document

A File device creates a file on the remote system. The value will typically be a path with substitution parameters used to generate a file name. For remote location clients running Unix or Linux, the file may start with | or > to send the file to a command rather than the file system. For example, to print to a spooler destination named "hp4000", device might be: **|lp -dhp4000 -oraw**". On Windows, this can also be the name of a shared printer, such as \\Server\Printer1.

A Command device runs a command line defined as the value. The command line will contain one or more substitution parameters so the command can operate on the delivered data file. This is generally used to execute a spooler command to print the job file, for example: **lp -dhp4000 -oraw {file}**.

A Win Printer device is a Windows spool queue name. The job is sent to the Windows spooler as a raw print job. Note this is not a printer share name (a UNC path such as \\ptrsv\printer1). For that type of name, use a File device type.

A Network Printer value is an IP address or hostname, with an optional *:port* suffix. The default port is 9100, which is what printers with network interfaces normally listen on.

An Open Document device works just like a file device, except once the file is created, it is opened using the client operating system facilities. Only known document and image file types are supported, and the client can't be running in background or as a service. Note that the file is not automatically deleted, as the viewing application requires access for an unknown amount of time, and the client will not wait for it to close.

For convenience, when a remote location client connects to the server, it reports known printers for that location ID, and that list is provided at the bottom of the Device entry. For Windows clients, this is a list of Windows printer names. For Unix/Linux clients, it is the result of the 'lpstat -s' command.

Substitution Parameters

The following parameters are available in remote device value fields. Some parameters are most applicable in File type devices, and some are available only from local path sources or from local port sources. In addition to these fixed parameters, there are soft parameters that can be supplied by an application that performs local path transfers. See notes about soft parameters below.

To reference a substitution parameter in a device value, use its name in curly braces. For example, to specify a file path based on the server, date and time, a sequencer, and a file extension, a value could look like this: `/data/arc/{server}-{ymd}-{hh}{mm}-{#}.{ext}`

- **file** is the name of the client-side work file. This is helpful with command type devices, where the name of the job file is needed for a command line program.
- **errfile** can be used in command type devices. It refers to a dynamically generated file whose contents can contain error messages. If this file has content after the command is executed, the error message content is logged on the client and also at the server in job history. In addition, the job is retained on the client to retry a short time later.
- **respfile** can be used in command type devices. It refers to a dynamically generated file whose contents can contain information messages that are logged on the client and also at the server in job history. This information could be used, for example, to identify a spool job number in job history.
- **yyyy** is the current 4-digit year
- **yy** is the current 2-digit year
- **mm** is the 2-digit current month
- **dd** is the 2-digit current day of the month
- **hh** is the 2-digit current hour in 24-hour time
- **mn** is the 2-digit current minute
- **ss** is the 2-digit current second
- **ymd** is the same as `{yyyy}{mm}{dd}`
- **jobid** is the job ID number
- **server** is the server hostname or address the client received the job from.
- **#** a unformatted file sequence number, used to guarantee uniqueness when File type output is specified.
- **##, ###, ####, #####** a zero-filled, 2 to 5 digit sequence number, used to guarantee uniqueness when File type output is specified. If the sequencing required exceeds the digits allowed, an unformatted sequence number results.
- **temp** is a temporary directory for workfiles, from environment variable TEMP on Windows, or the user's home `.cp10/tmp` path on Unix.

On Windows clients, the following symbolic folder names are also available:

- **desktop** for the running user's Desktop folder.
- **commondesktop** for the Desktop folder for all users.
- **documents** for the running user's Documents folder.
- **commondocuments** for the Documents folder for all users.

The following parameters are also available if the job arrived from a [local path](#) source.

- **filename** is the source file name, without a directory path.
- **path** is the directory path, with a trailing slash, of the source file.
- **ext** is the file extension of the source file name.
- **owner** is the Unix or Linux owner name of the source file.
- **group** is the Unix or Linux group name of the source file.

The following parameters are also available if the job arrived from a [local port](#) source.

- **fromip** is the IP address of the machine that printed to a source port.
- **port** is the source port number.
- **ext** is an inferred file name extension based on the content of the print data that was received by the source port, such as "ps", "pcl", or "pdf".

Soft Parameter Substitution

Soft parameters are supplied via an INI file associated with the local path file (*path.ini*), in an [info] section with *name=value* pairs. For example, if a file 12345.pdf is placed in a monitored path, a file 12345.ini could be placed there as well, and any name/value pairs in the file's [info] section will be transferred to the remote clients. Any {*name*} string found in the device's value field will be replaced with its *value*.

Protected Directories

To prevent accidental destruction of important system information, all files must contain at least two directory delimiters, and the following directories are protected and can't be written to:

Unix:

- The /etc/ directory
- Any directory containing /bin/
- Any directory containing /sbin/

Windows:

- The Windows (%systemroot%) directory
- The Program Files or Program Files (x86) directories

License Limit Notification

If you create or enable a device so that more devices are configured than licensed, the system will automatically disable a device and display a message indicating which device was disabled.

6.3.3 Local Ports

A local port is a network port on which the Server listens for print jobs to arrive. This port works in a manner similar to that of a network printer, so any system that can print to network printers, such as print spoolers, can deliver print jobs to the Server. All that is needed is to configure the "printer" to print to the address or host name, and port, which the Server is configured to listen on.

There can be many such ports configured, and any available listening port can be used. Each port is also configured to deliver the incoming data to [remote devices](#) at [remote locations](#). There can be one, or many of these devices, so it is possible for one print job to be distributed to multiple devices, files, or programs.

Note that as identical data is distributed to each remote device, those devices must all support the data format being distributed. For example, if a job arrives in the PostScript 3 print language, the remote devices must support that version of PostScript. It may be possible to use command line devices to run data through a conversion process, but that is a functionality outside the scope of CirrusPrint.

Port ID is a unique identifier for this port definition.

Port is the TCP/IP port number on which the server listens for print jobs. Only one port ID can listen on a given port, and you are notified if there is a duplication of assignment. The port number must be between 1024 and 65535. Common port ranges are 9101 to 9999, representing an extension of the standard port 9100 that most network printers listen on. Note that if the server's client connection port is configured to bind to a particular IP address, then the port monitor will bind to that same address. This allows multiple instances of CirrusPrint on a machine with multiple addresses to use the same local port numbers, as long as they bind to different IP addresses.

Description is an information field.

Port is inactive, if checked, indicates the server will not listen for jobs on this port.

Target(s) is used to specify which remote devices receive deliveries of jobs that arrive on this port. To add a remote device, choose a location, then choose a remote device, and click the add button (<). To remove a device, select it and click the delete button (x).

Allowed IP is a semi-colon delimited list of IP addresses or wildcards. If this value is filled in, the systems printing to this port must have a matching IP address. Note that this is the IP address from the server's viewpoint, which may differ from the machine's internal IP address if access is through a router that does address translation.

Once a port is configured and listening, you can configure printers in your spooling system to print to the local port on the CirrusPrint server machine, as if it were a network printer. Print jobs received on the port are forwarded to the target devices at remote client locations.

On Windows servers, when a port is added, updated, or deleted, a corresponding Windows printer port is added, updated, or deleted, if permissions allow. The port name is "cp_install_portid". This action is performed by using the prnport.vbs script provided with modern Windows systems in the System32 directory, or the System32\Printing_Admin_Scripts\en-US directory. It is then simple to change the properties of any printer to use this port.

6.3.4 Local Paths

A local path is a directory that the Server monitors. When new files arrive, or files that match a wildcard pattern, those files are picked up and transferred to one or more remote device targets. The files are removed from the monitored directory when picked up.

There can be many such paths configured. Each path is also configured to deliver the incoming data to [remote devices](#) at [remote locations](#). There can be one, or many of these devices, so it is possible for one file to be distributed to multiple devices, files, or programs.

An autosend path is automatically defined for each location that is configured. The monitored path for the location is in the server's "autosend/*location/D*". This path is automatically configured to send jobs to the client's "autosend/*server*" path.

In addition to transferring files, it is possible to transfer information related to those files, via a same-named .ini file. Name/value pairs found in the [info] section of that file are transferred to the remote devices, and can be used as substitution parameters.

Path ID is a unique identifier for this path definition.

Directory Path is a directory or folder to be monitored.

Wildcard is one or more wildcard specifications that limit what files will be picked up from the directory. Multiple wildcards can be specified delimited by a semicolon. For example, *.ps;*.pcl will watch for files with both .ps and .pcl extensions.

Path is inactive, if checked, indicates the server will not monitor for jobs in this path.

Target(s) is used to specify which remote devices receive deliveries of jobs that arrive on this port. To add a remote device, choose a location, then choose a remote device, and click the add button (<). To remove a device, select it and click the delete button (x). Path definitions can target "file" and "open document" device types.

When writing programs or scripts to create files for pickup in a local path, it is important the file is complete before picked up. To ensure this occurs, create the file using a working path or name that will not be picked up, then when the file is ready, rename it to the final name for pickup. In addition, if a INI file is also to be supplied, create that before the rename operation. Also, ensure that full permission, including delete permission, is available to the server user. Otherwise, the server will be unable to remove the files picked up.

6.3.5 Service Settings

These settings control how the server operates and manages itself. All settings are stored in the server's configuration file, cp10s.ini, and can be maintained there manually or via the browser interface.

Remote Location Access

Server Port specifies the port on which the server is accessed from remote location clients. The clients must be configured to connect to this port. Location IDs and their associated passwords are defined in the [Remote Locations](#) page. Note that the system's firewall might need to be configured to allow connections from remote locations to this port. In addition, if the server resides behind a NAT address translation, the router must forward this port into the CirrusPrint server machine in order for remote location clients to reach the server via the router's public address.

Secure is an on/off option. If set on, the server listens using SSL to encrypt transmission. Remote locations must be configured to match this setting. The default is "on". Most platforms support SSL. Without SSL enabled, documents are transferred between the server and remote locations without encryption. In cases where communication between the server and remote locations is over a VPN, you might not want to enable security, since there the data is already encrypted as it crosses the network.

Bind to allows setting of a bind to IP address. The default, if left blank, is to listen on all addresses supported by the machine. If set, the service will only listen on the specified IP address.

Browser Access

HTTPD Port specifies the port used to access the server's internal web server, used for configuration and monitoring by an administrator.

Secure is an on/off option that determines if a browser must use the "https:" protocol for encrypted web browsing. By default, the server provides a self-signed certificate for this connection, so browser users will have to accept the unverified certificate when they connect to the server.

Bind to allows setting of a bind to IP address. The default, if left blank, is to listen on all addresses supported by the machine. If set, the httpd service will only listen on the specified IP address.

Session Lifespan specifies the number of hours that a given browser session runs before requiring a login. This is typically set to 12 hours, to force a login once per work day. If set to 0, a login is required whenever the browser is closed and restarted.

Logging

Log Path defines the directory or folder where log files are kept. There is a log file for each day. The default is the "logs" directory under the server installation directory.

Log Details defines how much detail is maintained in the log files for job transactions and for HTTP (browser) access. There are three levels of detail: Normal, Detailed, and Very Detailed. Detailed and Very Detailed settings are used primarily for analysis and debugging purposes, as they generate a large amount of data.

Purging

Job Purging defines how many days job history is kept and also how long undelivered job files are kept, before automatic deletion. If a remote location fails to pick up a job immediately, the job data file is retained until the location successfully connects and picks up the job, or until this amount of time passes.

Workfile Purging defines how many days work files are kept. Work files are normally cleaned up automatically as jobs are processed, but if jobs terminate abnormally, files can be left behind. Work files should generally be cleaned up quickly unless needed for debugging purposes.

Cache Purging defines how many days a cache entry can remain unused before purged. Object caching is used to increase performance of job delivery to remote locations. However, if a cache entry is unused, it occupies space for no reason, so it can be removed to free that space.

Log Purging defines how many days log files are kept. A log file is created for each day.

Email Server Configuration

SMTP Server names the mail server to connect to when sending emails. The server may contain a "ssl:" prefix to indicate the server uses SMTPS rather than plain or enhanced SMTP. It may also contain a *:port* suffix if the server's port is not 25 for SMTP or 465 for SMTPS. Many servers use port 587 in conjunction with STARTTLS protocol. The server supports STARTTLS starting with version 1.0.07 on platforms where SSL is supported.

To Address is the address to send email notifications to. Notifications relate to license thresholds being reached. There is also an option to enable sending such notifications to the publisher as well.

From Address is the address that will appear in the From header of the email.

Login and **Password** must be filled in if the mail server requires authentication.

When you've configured email settings, you can use the Send Test button to send a test email to the To Address value. A message will indicate success or failure, and after the test, a detailed SMTP log is available with the Test Log button. Note that the Send Test button does not save the configuration settings.

6.3.6 Users

To use the browser interface of the server, a user provide a login and password. This tool is used to add, edit, and delete such user profiles. Users can be regular users or administrators. Regular users can monitor the server and view logs, and administrators can configure the server.

The initial screen is a list of known user ID's. From this screen, you can select a user to edit, or add a new user by pressing the New button.

User ID is the name the user logs in under.

User Name is an information field.

Password is the password the user must provide when logging in. This entry is obscured when editing. Click the Show Me button to see the password text.

Date Format indicates the format that this user enters dates in. Specifically, the order of month, day, and year values are specified so the server knows how to interpret a date entry.

Admin user, if checked, indicates this user is an administrator.

User is inactive, if checked, indicates this user can't log in, though the user record remains on file.

Allowed IP is a semi-colon delimited list of IP addresses or wildcards. If this value is filled in, the user must login from an address matching one of the values. Note that this is the IP address from the server's viewpoint, which may differ from the user's internal IP address if access is through a router that does address translation. Also, users who access the server via the Internet will likely have dynamic IP addresses. This option is most useful for internal networks where IP addresses are managed by an administrator.

Press the Save button to save any changes, or the Delete button to remove an existing record.

6.4 Monitoring

Several options are provided for monitoring the operation of the server, including the Status page, which shows summary and daily job and license information, the Log Viewer, and Job History.

6.4.1 Status

The status window shows three tables of information. The first is the server serial number and license information, including month-to-date job usage. The second is a list of connected clients. The third shows recent job and byte count summaries.

6.4.2 Log Viewer

The log viewer allows selection of a daily log file, and then displays recent lines of the server's daily log file. Log files are purged after a [configured](#) number of days.

- The view can be refreshed automatically by checking the Auto Refresh box, or manually.
- The number of lines viewed can be adjusted using the Most recent lines drop box.
- The whole log file can be exported as a CSV file by pressing the Export button.
- You can filter the log to show lines of a certain type, process ID, job number, date range, or message content, by pressing the Filter button.
- You can view a summary of the daily activity by pressing the Summary button. When in the Summary view, press the Monitor button to return to the detail view.

6.4.3 Job History

Job history displays the jobs received from local ports and paths, and where those jobs are delivered. For each location the jobs are delivered to, document size and transfer size information is displayed. Below each location, the remote device(s) the job was delivered to is displayed.

The columns represent the following information:

Server Information Columns

- Job No is the unique identifier for the job, composed of date, time, and sequence information.
- Source is the port number or path ID the job was received from.
- Submitted is the date and time the job was received by the server.
- Job Size is the size, in bytes, of the document received on the port or path.

Remote Location Columns

These rows display information related to the transfer of the job's data to the remote location. Once there, it is delivered to all the devices configured for the job's source at that location. Depending on the job's source, there may be one or more location rows per job.

- Location ID is the remote location ID that the job was delivered to.
- Received is a date and time stamp of when the job was fully received at the remote location.
- Bytes Sent is the number of bytes, after compression, that were transferred from the server.
- Message will display error messages related to the location.

Remote Device Columns

These rows, under the associated location row, display details about where the job was delivered, such as spoolers or file names. Depending on the job's source, there may be one or more devices per location per job.

- Dev ID is the remote device ID, at the location displayed above, to which the job was transferred. There may be more than one device, even at a single remote location, to which the job is transferred (for example, one device might be a printer, another might be a print history folder). As a result, there may be more than one row of device information under each location.
- Delivered is the date and time when the document was delivered to the device.
- Output is the file, command, or printer that was the device's target, where the document was actually delivered.
- Message will display error messages related to the device.

7 Remote Location Clients

CirrusPrint client software must be installed at each remote location that will receive jobs from the server. Each client can be configured to connect to the server and accept jobs for a given location ID. The location ID can be considered an actual location, servicing printers and files for all users of a system, or different users can be assigned unique location ID's and run their own copies of the client software. In either case, the client receives jobs and delivers them to local printers or files.

The Unix client is written in Perl, so you must have a Perl 5.6 or later interpreter installed on the client system. This software is installed on most Linux systems, as well as AIX, HP/UX, OS/X, SCO, and other Unix variants. For information about Perl, and access to downloads for many platforms, visit <http://perl.org>.

The Windows client is derived from the Unix Perl program, and provided as a console executable, along with a Windows manager program and service program.

7.1 Installation on Unix

The Unix installation process involves a few steps with the command line, and assumes you have the installation tar.Z file available on the system. You should be the superuser (root) to perform the installation.

1. Create a directory to install the software in, and make it the current directory. This should be on a file system with at least 100MB of free space, though actual disk space need can vary considerably depending on many factors, such as they variety and types of documents you print, and how high or low log and cache purge settings are defined. If you aren't sure, just pick the file system with the most available space.

If you are updating an existing 1.0 installation, use the existing installation directory.

```
mkdir /data/cirrus_client  
chmod 777 /data/cirrus_client  
cd /data/cirrus_client
```

2. If the client is already installed and running, you should stop it at this point:

```
cp10c stop
```

3. Uncompress and extract the contents of the downloaded tar file. For example, if the tar file is available in the /tmp directory:

```
uncompress /tmp/cp10c_tar.Z or gunzip /tmp/cp10c_tar.Z  
tar xvf /tmp/cp10c_tar
```

Some Linux systems do not have the uncompress command, but you can use gunzip in place of uncompress.

Some systems support a "z" option on the tar command, which performs decompression automatically, so you could enter just one command:

```
tar xvzf /tmp/cp10c_tar.Z
```

4. If this is a new installation, run the setup.sh script. This script will prompt you to view and accept the CirrusPrint license agreement, confirm the location of the Perl interpreter, and create the /usr/bin/cp10c script.

```
./setup.sh
```

5. Also if this is a new installation, configure the client. The script will prompt you for server and location login information, and store that information in a private file in your HOME directory.

```
cp10c -config
```

6. Start the server with the following command:

```
cp10c -start
```

Complete documentation is available from the command line, **cp10c -help**, and also in html and PDF

format in the "man" subdirectory under the client installation directory.

7.2 Installation on Windows

Run the cp10c_setup.exe program to install the CirrusPrint Client on a Windows computer. This will run an installation wizard, including panels for acceptance of the license agreement and the install location. The preferred location for the installation is the default one. Overriding this and choosing a Program Files location will require extensive manual folder security modifications. Be sure to choose a disk that has plenty of disk space available, as CirrusPrint utilizes disk for caching and logging. At a minimum, the disk should have 100MB or more free space, though the needs of Cirrus can vary widely based on job volume and content.

The setup program installs the software for the user who runs it. This is typically an Administrator, so login appropriately before running the setup.

Once the setup is complete, there will be some new entries on the Start, Programs menu, under CirrusPrint 1.0 Client. One of these is the CirrusPrint Client, which is used to perform some key functions:

- Start, Stop the client software or service
- Install, Uninstall the client as a service
- Install, Uninstall the client on your Startup menu so it starts when you login
- Configure the client with server and location login information
- Monitor the client operation

The Client manager provides help, available by clicking the Help toolbar button.

8 Additional Information

This chapter contains additional CirrusPrint information.

8.1 Autosend Paths

When [remote locations](#) are configured using the server's browser interface, a [local path](#) named for that location is also created. The disk path for this local monitored path is the "autosend/*location/D*" path under the server installation directory. In addition, a [remote file device](#) is defined for the location as well, with a client-side path of "autosend/*server*".

This allows for immediate file transfers from the server to any configured location, without explicit path configuration.

8.2 Transferring To A New Server

If you need to move the CirrusPrint server installation to a new machine, follow these steps:

- Install a current version of CirrusPrint on the new system.
- License it using an emergency temp license, which provides up to 30 days of use.
- Start the new server to ensure operation. Stop it to proceed.
- Copy the *.dat files from the existing server's "data" directory to the data directory on the new server. This copies all configuration data to the new installation.
- Optionally copy the cache directory structure to the new directory. This can be quite large and you might choose to let the cache be recreated with use.
- When all operations have moved to the new server, request a license reset, permanently license CirrusPrint on the new server, and stop/uninstall it on the old server.