What is HP Remote Monitoring?

HP Remote Monitoring is an efficient, secure means of collecting and reporting usage data from your printing and imaging output environment. Remote Monitoring is a scalable and equally well suited to small-, medium-, and large-sized enterprise customers. With its automated data collection and convenient reporting features, Remote Monitoring makes it easy for you to manage your imaging and printing environment and make cost-effective decisions about it.

How do I acquire it?

HP Remote Monitoring is a value-added service offered to you when you purchase HP Pay per use for Imaging and Printing or Managed Services for Imaging and Printing.

What types of remote monitoring tools are in use?

The two types of data collectors used with HP Pay per use for Imaging and Printing or Managed Services for Imaging and Printing; they are appliance-based and printer-based (embedded) remote monitoring technologies.

Printer-based remote monitoring is installed within a printer and is suited for small environments with up to 50 devices. The advantage of using this tool is that it helps reduce costs by not requiring an external box at the customer site to perform data collection. You must have a compatible printer in which to install the printer-based data collector technology. In a large printing and imaging environment, you are better off using the appliance-based tool.
Suited for environments with more than 50 devices, the appliance-based data collector is a stateless machine that resides within your firewall. It does not collect data from your printing and imaging devices until it is instructed to by the HP Data Repository, which the data collector contacts every hour for instructions. The appliance-based data collector itself contains no data other than the network configuration required to log onto your network to securely contact the HP Data Repository.

How does it work?
It takes less than an hour to install the data collectors. These data collectors reside inside your firewall and capture device, consumables, and maintenance-kit usage–related data from predefined management information bases (MIBs) using Simple Network Management Protocol (SNMP) gets. Once the data is authenticated, the data collectors will be configured to send it to HP. Then, using either the predefined IP addresses or host names of the printers (there is no broadcasting over the network), the data collectors capture usage data from the device and send it on to HP in the same session. The data collected is then used to generate reports that can be viewed and downloaded by you.

How do I view reports?
When you are ready to view usage information, simply access the HP Services portal through a highly secure URL. You can choose among several report types, including a device usage summary and reports for individual devices by model name, page size, and other attributes. To generate a report, select your preferred report format (order-history, services-history, supplies-usage history, and supplies-per-printer reports are available in HTML or CSV formats; usage reports are available in HTML, CSV, or PDF formats). Then select a report, and the data is pulled from the database and displayed in the report on the Web site for your view and download. You can also specify report start and end dates for those reports that provide for this input, and you can generate online charts and graphs automatically from your reports.

How about my company’s security?
HP Remote Monitoring is designed to protect confidential information. The only information contained on the data collector is the network configuration information that allows it to be on your network and to securely contact only the HP Data Repository (to get its printer fleet data collection instructions). The appliance-based and printer-based data collectors contain no knowledge of the installed devices—they contain only the instruction code that enables them to get usage information from devices and pass that information on to the HP Data Repository. The data collector receives work instructions from HP on what devices need data collection, and where those devices are located. Once the data collector receives work orders from HP, it uses directed packets (specific IP or Hostname) to route them to the appropriate devices. Using “SNMP gets” the data collector queries the device, using predefined Management Information Base entries (MIBs) so that they are not “MIB-walking” through the device. The only MIBs queried are those specific to what the device type is, its serial number, page size, page type, and quantity of pages printed. Once the data is collected, it is passed on to HP in the same session that was initially opened, and the session is then closed.

For greater security, the data collector connects to HP via HTTPS (port 443)—the universal standard in secure transactions—using 128-bit encryption, and then authenticates with HP. Plus, the data collector always initiates communication with your network—communication is never initiated from outside. Further, with the exception of port 443, all ports such as SSH, Telnet, FTP, and SendMail are inaccessible (note: these ports are always turned off). Authentication of the data collector prior to communicating with the HP Data Repository provides additional security. Also, the data collector IP and host name can be set so it will communicate only with specific devices or a range of IPs. Finally, HP appliance-based Remote Monitoring uses intrusion detection to bolster the integrity of the data collector tools and data.
Key benefits

HP Remote Monitoring can help you save your organization money, rationalize device utilization, and boost user productivity.

- **Data gathering and reporting**—facilitates making print environment management decisions that can save your organization money, rationalize device utilization, and boost user productivity.

- **Improved device utilization**—allows you to move users from overutilized to underutilized devices, use high-cost-per-page and low-cost-per-page devices appropriately, and position devices for reduced user traffic.

- **Operations control**—offers improvements in working processes, better asset management, reduced supplies inventory, increased hardware reliability, tighter control over costs, and a clearly identified budget for printing operations.

- **Proactive maintenance and replenishment**—provides the assurance of continuous printing and administrative efficiency. There is no monitoring necessary on your part, no unplanned printer downtime, and no need for storage of spare supplies. This reduces overheads resulting from an overstocked supplies inventory and keeps production flowing smoothly by delivering exactly the right supplies and device maintenance at the right time.

- **Proactive support and device monitoring**—monitors your page counts, so you don’t have to, and proactively alerts you about preventive maintenance kit replacement needs at prescribed intervals. This increases hardware reliability and uptime, keeps devices working at peak operating conditions, and helps extend the life of your printing devices.

- **Online reports and service requests**—all contract details are available to view online at any time, and the entire process of managing contracts is fast and efficient. Instead of calling HP, you can use the Web-based ordering capabilities to obtain supplies and printer-maintenance kits or even to request service. This cost-effective process is considerably more efficient and is available 24/7. Online reports provide valuable device-usage information, enabling you to optimize printer-hardware usage. With this vital information, you are able to make better business decisions in real time and enjoy peace of mind.
Customer requirements for data collectors

Customers are required to provide the following:

- Host name
- Fully qualified domain name
- IP address
- DNS entries (primary and secondary)
- Subnet mask
- Default gateway
- Proxy name and port number (if required for Internet access)
- Port 443 access
- No SNMP traffic blocks for the gets
- Suitable host device (if printer-based) with administrator password for the installation

Key features of the data collector technology

- The data collector resides within your firewall and initiates communication to HP over HTTPS port 443, using 128-bit encryption.
- It takes one hour or less to install and configure the data collector.
- When instructed to work, the data collector captures usage data from devices and then sends it to HP in the same session.
- The data collector supports most HP network printers and some multivendor products. (Note that non-network HP printers can potentially be supported by manually collecting and submitting printer information.)
- The data collector set is scalable for small, medium, and large enterprises.
- Reports are accessed from the HP Service Portal through a highly secure URL using a browser.
- Reports generated include device-usage summary reports and installed-device reports by model name; by color, mono, and duplex; and by page size.
- The data collector can support a single device or thousands of devices.
- The data collector contains only configuration information; no customer data or device usage data resides on the data collector.
- Network traffic generated is as follows:
  - 7.46 MB/day—communication with HP
  - 1.2 MB/day—status messages (heartbeat)
  - 100 bytes/day—request for data collection (plus 5 KB in overhead/50 devices)
  - 200 bytes/day—network queries for MIB (5–40 queries, depending on device)
  - 10 KB/day—response to request for data collection from the data collector to HP (based on 50 printers)
Additional features of embedded (printer-based) technology

• Implemented as a Chailet-based printer plug-in (software):
  – Chai is HP’s implementation of Java™, available in many HP LaserJet printers.
  – The Chailet needs to be installed and configured on one of the printers in the fleet.
  – The embedded web server (EWS) MUST be enabled for the printer hosting the tool.

• Automated tool failure detection:
  – The tool fully recovers from power cycles of the host device.
  – There is an automatic failover mechanism if the tool is installed in more than one device in the fleet.
  – Loss of communication generates an event that can be viewed in the service center.

• Automatic software update (for customers who are comfortable with this feature):
  – New versions of the tool are detected and downloaded to the printer for installation.
  – New binaries are installed, and the tool is restarted to invoke the new version.
  – Software updates typically include support for new devices and defect fixes.

• Viewing data collections:
  – Data sent to HP for the last three data collections is maintained on the device and can be viewed by the customer through the tool user interface via the EWS.

• Viewing log files:
  – The tool maintains its own local log on the hard disk and records all transactions.
  – The log is accessible to HP personnel only through the tool interface via the EWS.

• Note that the printer based technology will only power cycle the printer under the following conditions:
  – Only when an update has been done (typically once every six weeks) or communication has stopped and we try to recover
  – When the printer has been idle for 1 hour (if this “one hour idle” condition is not reached within 24 hours of it needing a reboot, we wait for the current job (if any) to be finished and then reboot)
Why is it recommended to migrate from RPM to Remote Monitoring?

It is recommended that customers migrate from Remote Print Manager (RPM) to Remote Monitoring because HP Remote Monitoring provides all the benefits that exist in RPM plus the following:

• Data security:
  – HP Remote Monitoring is more secure in terms of data transport and its ability to better protect access to the data collector. This is where customers are using SMTP as a transport.

• Authentication:
  – Certificates are used between the data collector and the backend.
  – User name and password are authenticated.
  – PIN code is authenticated.

• Asset tracking/Asset management:
  – Trend analysis monitoring is done via historical usage information.
  – Device physical locations that have changed are tracked (requires Account Center/Device Center (ACDC) to be updated and maintained).
  – Manual data entry capability:
    – Data entry can be done for multivendor products
    – Data must be entered into service center once the customer has provided the information to HP.

• Future printers are going to be developed around Remote Monitoring and no further development will be done with RPM.

• Future technology road map:
  – Built around Remote Monitoring, which means Remote Monitoring will continue to grow and expand with the HP Services portfolio.

For more information

To learn more about HP Remote Monitoring and the HP Pay per use for Imaging and Printing solution, contact your local HP sales representative or visit our Web site at: www.hp.com/hps/printer/pr_advantage.html.