PRINT AUDIT
INFINITE DEVICE MANAGEMENT

IDM Technical Overview

PA eBusiness

PRINT AUDIT
INFINITE DEVICE MANAGEMENT

Infinite Device Management Features

Minimal software to install

Infinite Device Management uses a small software program called the Information Collection Engine to perform periodic scans in the environment. The data is then sent to Print Audit and hosted on our servers here so no additional information is written to the computer's disk drives.

The Information Collection Engine is compatible with Internet proxy servers.

Security

No personal information is collected or sent from Infinite Device Management. Only the following information is gathered and transmitted to Print Audit's secure server:

- Printer name, make and model
- Location
- Serial number
- IP Address
- MAC Address
- Page Counts
- Toner levels
- Status / Alerts (e.g. out of paper, paper jam)

The Information Collection Engine creates the scan file in XML format and then encrypts it and sends it to our secure server as zipped file. Click here to view a Sample Data file (the sample file is the XML file in PDF format).

Data Storage

- Print Audit's server is located in a physically secure environment.
- Print Audit's server is located behind a dedicated hardware firewall that blocks all external access except that which is required for Infinite Device Management to function. The server is kept up to date with the latest operating system patches, security patches, and anti-virus updates.
- Server administration logins are restricted to a very limited number of authorized personnel who require access only for routine maintenance and backup purposes.
- Infinite Device Management is the only application running on this server and therefore there is no security threat posed by other programs.

Web Interface

- All external access is via secure login (username and password) and only through the secure web application at https://fm.printaudit.com.
- Infinite Device Management logins can be restricted to either a set of customers for a single dealer (a "dealer level" account) or a single customer (a "customer level" account). Advanced privileges can also be assigned to users.
- Access to the secure web application at https://fm.printaudit.com uses 256-bit SSL encryption.

Requirements

The Information Collection Engine requires the following:

- Internet Explorer 4.01SP2 or later installed.
- A TCP/IP based network.
- SNMP enabled network printers

Technical Overview of the Discovery Process

This topic is a technical overview of how the Information Collection Engine discovers printers on the network. Its main audience is IT personnel who want a greater understanding of how using the Information Collection Engine will impact their network.

Protocols Used

The Information Collection Engine uses SNMP (Simple Network Management Protocol) for the majority of its scanning. It uses SNMPv2 wherever possible to cut down on network “chatter”, but will fallback to SNMPv1 for devices that do not support SNMPv2. The Information Collection Engine also uses ICMP (ping) packets to aid in device discovery.

Discovery Process

The Information Collection Engine will gather networking information from the host computer (IP Address and Subnet) to determine a suggested scan range. The Information Collection Engine then uses ICMP (ping) to determine if there is a device listening at an IP address. The Discovery Scan then uses SNMP scanning within the internal network only, via the standard SNMP port (UDP port 161).
The Information Collection Engine uses unicast transmission to communicate to each IP address in the configured scan range. No broadcast packets are sent.
The Information Collection Engine does not send information out to the devices directly. A community string can be specified if need be.

The Information Collection Engine uses the following steps to scan each IP address when doing a Discovery scan.

1. The Information Collection Engine pings the IP address to see if it gets a valid response. It will wait the “Ping Timeout” as specified in the Advanced Discovery Settings, and if no valid response will retry the “Ping Retries” amount. If no valid ping response it assumes there is nothing listening at that IP address and moves to the next.
2. If there is a valid ping response, the Information Collection Engine then uses SNMP to try and retrieve a standard SNMP value from the device. If nothing is returned it will re-try with the “SNMP discovery” time out value set in the Information Collection Engine section of Infinite Device Management and will retry with the “SNMP retries” value. It will re-try this step for each community in the “Communities” list set in the Information Collection Engine section of Infinite Device Management. If there is nothing found, the Information Collection Engine stops scanning this IP address and assumes something is there, but it does not support SNMP.

3. If a valid SNMP value is returned the Information Collection Agent then attempts to get information from the public standard Printer MIB. Again, it will use the “SNMP discovery” timeout and the “SNMP retries” value for this. If nothing is found then the Information Collection Engine assumes this is a valid SNMP device, but not a printer/copier.
4. If information is found here, the Information Collection Engine then scans the device using the “SNMP request” and “SNMP retries” values.

Data Transmission Process

Once the data is collected, the Information Collection Engine creates an encrypted file containing the scan information from each device that is then sent to Print Audit to populate the Infinite Device Management web portal. Details on this process are included below.

The file size is approximately 5KB per device scanned.
The ICE connects to Print Audit’s server via an outbound connection only. There is no reverse connection made from Print Audit’s server to the ICE.
HTTPS is the default send method in the ICE configuration window. This ensures that the data is encrypted during transmission using standard internet security protocols (256 bit SSL on TCP port 443).
HTTPS (256-bit SSL) is the same security as is used in Internet banking or purchasing goods online from a merchant such as Amazon.
The server sends a simple acknowledgement that the data was received, but no other data is sent back to the ICE in response to the transmission. This response is also encrypted in the same manner as the transmission itself.

Why does Infinite Device Manger / Information Collection Engine not detect some of my devices?

If individual devices are not being detected by Infinite Device Manger, the following are the possible causes:

- The device has been powered down, physically disconnected from the network, or is otherwise offline.
- The device has been removed from the environment or permanently decommissioned.
- The device has experienced a failure that affects it’s network connectivity.
- The device does not support SNMP.
- The device has been reconfigured and SNMP has been disabled.
- The device has been moved to a new location, and it’s new IP Address is outside the range that the Information Collection Engine is configured to scan.
- The device is attached to a JetDirect box. We currently do not scan devices that are connected to HP Jet Direct boxes or any other network print server, we only scan directly attached networked printers.
- The device is a fiery device. Fiery devices do not provide enough information for the Information Collection Engine to gather and report on for the device.
- The device’s community string may have changed.

If none of the devices are being detected by Infinite Device Management / Information Collection Engine, the following are the possible causes:

- The Information Collection Engine is not configured with the correct IP addresses/ranges to properly to scan the devices.
- The Information Collection Engine is having problems communicating with devices on the network (for instance, a firewall is blocking SNMP traffic on the network).

What can I do to ensure that all of my devices are detected?

If individual devices are not being detected by Infinite Device Management / Information Collection Engine, try the following troubleshooting steps:

1. Check the device configuration, ensuring that it is powered on, online, and connected to the network.
2. Check the device's IP Address and confirm that it has not moved to a different subnet or to an IP address outside the scan ranges that The Information Collection Engine is configured to scan. If the device has been moved to an IP Address outside the ranges that the Information Collection Engine is configured to scan, change the Discovery Scan range in Infinite Device Management to include this IP address.
3. Open the devices' embedded webpage. If you can get to this page, the IP address for the device is correct. You should also confirm that port 161 is not being blocked for this device.
4. Ping the IP address to see if you get a response or not. If you do not get a response, the problem lies on the network and will have to be resolved before the Information Collection Engine can detect the device.

If none of the devices are being detected, try the following troubleshooting steps:

1. Double-check the Information Collection Engine configuration in Infinite Device Management and ensure it is set to scan the correct range(s) of IP addresses.
2. If there is a firewall present in the environment, ensure that it is not blocking SNMP communication (UDP port 161) between the Information Collection Engine and the devices you are tracking.
3. Confirm that the Community string set on the Information Collection Engine section of Infinite Device Management is the correct community that the devices are set to.

Is Network Traffic a Problem?

No, the packets are fairly small, and the scan runs for a short period of time.

- The Information Collection Engine does not create any network traffic until a scan is initiated.
- Once the initial discovery is complete, Infinite Device Management will perform a Refresh Scan instead of a Discovery Scan. A Refresh Scan re-uses community settings, etc. and can skip much of the discovery process. By default, full Discovery Scans are scheduled to occur every 12 hours. Refresh scans occur every 20 or 60 minutes depending on which version of ICE is installed.
- Once a scan has been initiated, the Information Collection Engine will create approximately 30 to 50 KB of bidirectional network traffic per device scanned.

How Do I Reduce Network Traffic If I Am Concerned?

There are a couple of things you can do to reduce traffic on the network that is caused by the discovery process. Each one is listed below along with pros and cons.

1. Limit the number of communities. As long as devices in the organization use the “public” community, or use a standard private community, then you should be able to get away with having only one or two “Communities”. The more communities you have, the longer the overall scan will take and the more SNMP requests are generated.
2. Lower the number of SNMP retries. You can lower the SNMP retries value to reduce overall traffic. However, it is possible that devices will be missed during the scan.
3. Enter the custom IP address ranges for the devices in the environment in the Information Collection Engine section of Infinite Device Management. You can avoid most of the traffic involved with discovery altogether if you only scan the IP addresses you know correspond to printers. For example, if you know you have five devices, adding those IP addresses can save hundreds of SNMP requests to IP addresses that are not associated with devices.