Rapid Assessment Key v2
Technical Overview

Overview

The Rapid Assessment Key v2 is an extremely easy to use USB device that quickly collects data on networked imaging devices. The key allows office equipment dealers to easily gather meter reads, discover devices and troubleshoot document output issues in minutes.

Print Audit is the ONLY print management company that has been given access to all of the major office equipment manufacturers' device information. This gives Print Audit the most accurate scan results in the industry.

Rapid Assessment Key v2 Features

No software to install

The Rapid Assessment Key v2 resides on a USB drive that is plugged into an available USB port on the network (USB version 2.0 is recommended for better performance; USB version 1.1 or higher is supported).

No information written to host computer

The program uses the RAM on the host computer to operate, but does not write any information to the computer’s disk drives. The Rapid Assessment Key v2 requires a minimum of 10MB free on the key.

Security

No personal information is collected or sent from the Rapid Assessment Key v2.

Virus Protection

The Rapid Assessment Key v2 is digitally signed to ensure the integrity of the software. We recommend ensuring that the key is virus free by periodically scanning the key with an antivirus program.

Internet Connection

The program does not require Internet access each time the key is launched. The key will launch 5 times without Internet access before it is locked and requires Internet access to validate the license.

The key is compatible with Internet proxy servers. The proxy settings must be configured in Internet Explorer prior to launching the key.

Requirements

Using the Rapid Assessment Key v2 requires the following:

- Windows 2000 or newer operating system with Internet Explorer 4.01SP2 or later installed.
- An available USB 1.1 or 2.0 port.
- A minimum of 10MB free on the USB key and on the computer running the software.
- A TCP/IP based network.
- SNMP enabled network printers

Technical Overview of the Discovery Process

This topic is a technical overview of how the Print Audit Rapid Assessment Key v2 discovers printers on the network. Its main audience is IT personnel who want a greater understanding of how using the Rapid Assessment Key v2 will impact their network.

Protocols Used

The Rapid Assessment Key v2 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 Rapid Assessment Key v2 also uses ICMP (ping) packets to aid in device discovery.

Discovery Process

The Rapid Assessment Key v2 will gather networking information from the host computer (IP Address and Subnet) to determine a suggested scan range. The Rapid Assessment Key v2 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 Rapid Assessment Key v2 uses unicast transmission to communicate to each IP address in the configured scan range. No broadcast packets are sent.

The Rapid Assessment Key v2 does not send information out to the devices directly. A community string can be specified if need be.

The Rapid Assessment Key v2 uses the following steps to scan each IP address when doing a Discovery scan.

1. The Rapid Assessment Key v2 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 Rapid Assessment Key v2 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 in the Advanced Discovery Settings and will retry with the "SNMP retries" value. It will re-try this step for each community in the "Communities" list in the Advanced Discovery Settings. If there is nothing found Rapid Assessment Key v2 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 Rapid Assessment Key v2 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 Rapid Assessment Key v2 assumes this is a valid SNMP device, but not a printer/copier.

4. If information is found here, the Rapid Assessment Key v2 then scans the device using the "SNMP request" and "SNMP retries" values.

Why does the Rapid Assessment Key v2 not detect some of my devices?

If individual devices are not being detected by Rapid Assessment Key v2, 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 Rapid Assessment Key v2 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 Rapid Assessment Key v2 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 Rapid Assessment Key v2, the following are the possible causes:

- Rapid Assessment Key v2 is not configured with the correct IP addresses/ranges to properly to scan the devices.

- Rapid Assessment Key v2 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 Rapid Assessment Key v2, 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 Rapid Assessment Key v2 is configured to scan. If the device has been moved to an IP Address outside the ranges that Rapid Assessment Key v2 is configured to scan, change the Discovery Scan range 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 Rapid Assessment Key v2 can detect the device.

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

1. Double-check the Rapid Assessment Key v2 configuration 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 (TCP port 161) between Rapid Assessment Key v2 and the devices you are tracking.

3. Confirm that the Community string set on Rapid Assessment Key v2 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 Rapid Assessment Key v2 does not create any network traffic until a scan is initiated.
- Once a scan has been initiated, the Rapid Assessment Key v2 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" in the Advanced Discovery Settings. 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. Load a list of specific IP addresses into the Discovery Scan Window. You can avoid most of the traffic involved with discovery altogether if you load the list of IP addresses you know correspond to printers into the Discovery scan window. For example, if you know you have five devices, adding those IP addresses via file import or manual entry can save hundreds of SNMP requests to IP addresses that are not associated with devices.

4. Once the initial discovery is complete, do a Refresh Scan instead of a Discovery Scan. A Refresh Scan re-uses community settings, etc. and can skip much of the discovery process.

Technical Support

In North America, you can call our toll-free number at 1-877-41-AUDIT (28348) or click here to Contact Print Audit. Please visit our website at http://www.printaudit.com for our worldwide support options and for our online knowledge base.