

Print Tracker discovers network devices that respond to Simple Network Management Protocol (SNMP) requests. A version of SNMP (either v1, v2 or v3) must be enabled for Print Tracker to capture device information. If an end user turns off SNMP entirely, metering software will be unable to capture information from devices.

By default, all Print Tracker installations capture information from devices that have SNMP v1 & v2 enabled. SNMP versions 1 and 2 send passwords in clear text across the local intranet when gathering meters. All devices are shipped with SNMP v1 & v2 enabled.

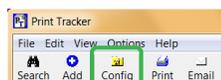
SNMPv3 encrypts the data and is the most secure protocol available. SNMPv3 is a relatively new protocol and only the newest imaging machines offer this support. SNMPv3 is disabled when devices are shipped from manufacturers.

Information from SNMPv3 enabled devices can be captured by Print Tracker by granting permissions.

Permitting Print Tracker to capture information from SNMP enabled devices

1. Install Print Tracker on a workstation or server to capture SNMP v1 & v2 enabled devices.

In environments with SNMPv3 devices, DO NOT send a report when prompted.

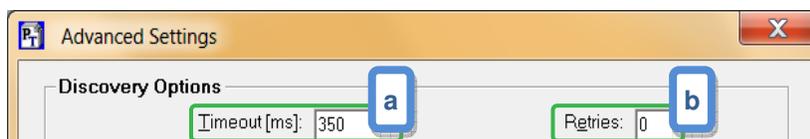


2. Click the 'Config' button in the upper left corner of Print Tracker to open the settings dialog.



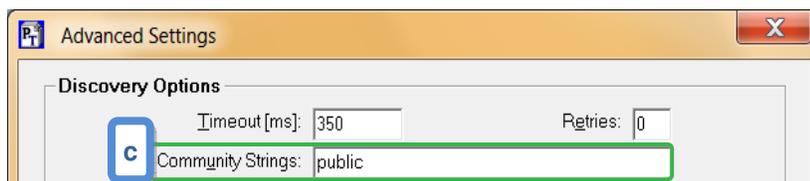
3. Click the 'Advanced Settings ...' button of the 'Settings' dialog to open 'Advanced Settings > Discovery options'.

The 'Advances Settings' dialog will open.



- a. Timeouts of 350ms pings devices for about 1/3 second.
- b. The default retry is "0".

If a network device is in a suspended mode, it may take longer to get a response. The timeout and retries settings allow the device to be queried more than once if the first response is not received.



- c. Sometimes devices are setup with a security password called a community string. The default community string is "public" in lower-case letters. Community strings are case-sensitive. Enter multiple community strings comma-separated, without spaces. For example, the community sting setting may be 'public,PUBLIC,SeCuRe'.

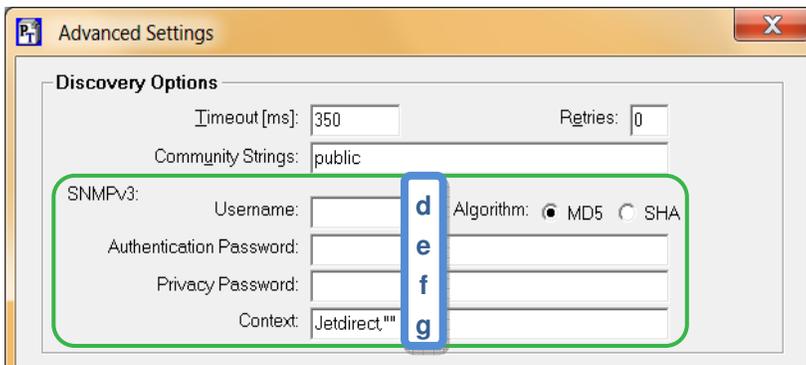
Permitting Print Tracker to capture information from SNMPv3 enabled devices

 **NOTE** – SNMPv3 enabled device capture CANNOT be set from the Admin console.

SNMPv3 enabled devices can be discovered and their meter and status information captured by allowing the functionality in the Print Tracker collection software.

If devices use SNMPv3, enter the authentication information as it appears on the imaging devices. Separate multiple values with commas and enclose values containing commas with quotes. Common SNMPv3 contexts include Jetdirect (HP devices), mfpdirect (Sharp devices), or "" (Samsung devices).

 **NOTE** – If the SNMPv3 enabled device does not show a context, use "".



The SNMPv3 settings may appear as follows:

- d. User Name: admin
- e. Authentication Password: the brown fox
- f. Privacy Password: ate the hen
- g. Context: Jetdirect

Examples of multiple authentication sets might appear as:

User Name: admin,admin

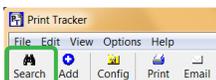
Authentication Password: the brown fox, the wolf

Privacy Password: ate the hen,"ate the fox, then died"

Context: mfpdirect, ""

To find and begin reporting on the newly enabled SNMP devices

4. Return to the Print Tracker main screen by clicking 'OK' on both the 'Advanced Settings' and 'Settings' dialogs.



5. Click the 'Search' button to search for SNMPv3 enabled devices.

6. When prompted, send an email meter report.



Warning – SNMPv3 discovery and reporting tends to be much slower than SNMP versions 1 and 2 due to the added load of encryption / decryption. Only include the contexts and values that are required by the devices that require monitoring and place the contexts and values that most devices use first in the list.