



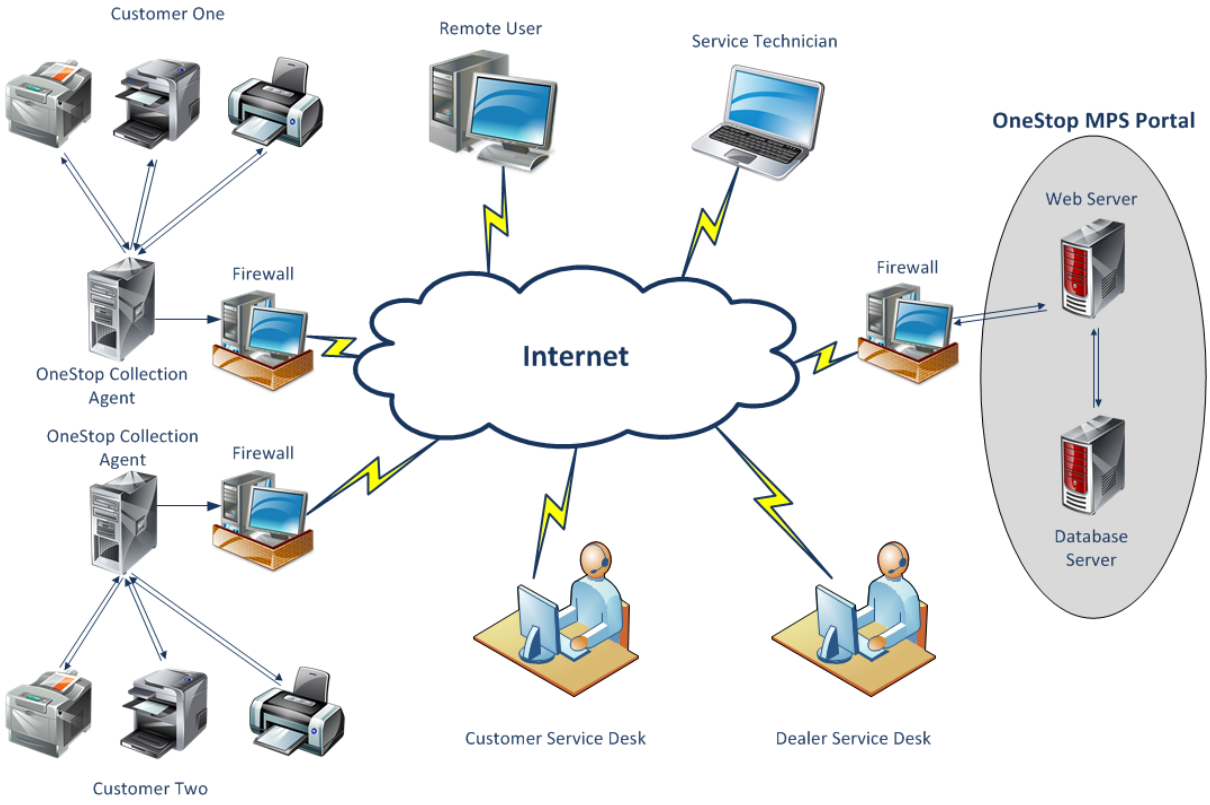
# OneStop Collection Agent Security White Paper

# OneStop Collection Agent Service

The OneStop Collection Agent is designed to collect device data from the MIB of networked print devices. The data is then uploaded to a specific OneStop website. The OneStop Collection Agent tool is a read only tool. At no point does it write any information or make any changes to any device it connects to.

# OneStop Overview

- OneStop MPS Portal provides an efficient method of remotely monitoring device usage and status
- Flexible security model allows the same system to be deployed to multiple customers
- Enables the dealer to deliver pro-active service to the customer
- Delivers the ability to reduce costs through just in time consumables
- Reduces overall fleet cost via enhanced availability



# General Information

## What protocols does the OneStop Collection Agent use?

OneStop uses the Simple Network Management Protocol (SNMP) and Ping (ICMP). These are industry standard protocols used to set and retrieve information from network enabled devices.

## Where should the OneStop Collection Agent be installed?

The OneStop Collection Agent should be installed on a server or PC that is running 24/7 which is able to ping all the devices you want to collect information from. You will also need internet access from this PC or server. The OneStop Collection Agent is installed as a service.

## How often will the OneStop Collection Agent collect information?

The OneStop Collection Agent is configured differently for each customer's site. There are 2 different types of information collected. The first is a general scan to discover devices and collect meter readings. This scans the networks for IP Addresses configured for the site at a set time of the day. The second is to check on the current device status which will only scan devices that OneStop is aware of at a set interval, for example every 10 minutes.

## What ports does OneStop Use?

Depending on which website protocol is being used will decide what port number will be used, PORT 80 = HTTP

PORT 443 = HTTPS (Outgoing only)

PORT 161 = SNMP

## What is the size of data being sent out to OneStop?

Size varies dependent upon the number of devices being monitored, for 5 or less devices, average data sizes are 10KB, 20 devices being 40KB.

## What file types are uploaded?

.XML files containing device data (Description, IP address, Serial number, MAC address, Status, meter readings and consumable levels) are compressed and uploaded to your dealers OneStop website in .ZIP format.

### What Encryption is used?

Secure Sockets Layer (SSL) is used (Provided this was specified by your dealer when OneStop was initially implemented), this will be evident in that the URL will begin with HTTPS, not HTTP.

### Why does the agent run as a service?

The Agent runs as a service as it is designed to run in the background and be as non-invasive as possible, As a service is run by a service account, this allows the agent to perform its duties completely automatically without the need for user intervention beyond installation and it has no need for a user to be logged in, which is why the agent does not run as an app.

### Why is it required that the agent be installed as administrator?

Due to the nature of windows, services can only be installed with admin rights. Even when running on an admin account we advise that installation is done via 'Run as admin' which ensures the service is installed correctly.

## Networked Printers and Copiers

What information does the OneStop Collection Agent collect?

The IP address, MAC address, device description, device status, consumable usage and meter reading information are collected. No other information is retrieved from the device.

### How is this information stored?

The information is stored in an XML file, which is stored locally before being uploaded to the dealer's website where it is processed and stored in a secured SQL database.

### Where is the information sent?

The information gathered by the OneStop Collection Agent is uploaded to the dealer's web site.

## SNMP v3 Support

SNMP v3 is fully supported, with the following options available:

- SNMPv3SecurityLevel, level of encryption. Possible values:
  - NoAuthNoPriv - no authentication and no encryption
  - AuthNoPriv - messages are authenticated but not encrypted
  - AuthPriv - messages are authenticated and encrypted
- SNMPv3AuthenticationEncryption, encryption used for authentication. Possible values:
  - MDS
  - SHA
- SNMPv3PrivacyEncryption, encryption used for data. Possible values:
  - DES
  - 3DES
  - AES
- SNMPv3UserName
- SNMPv3AuthenticationPassword
- SNMPv3PrivacyPassword

## OneStop Standalone Agent

The OneStop Standalone Agent has been designed to work in the same way as our regular OneStop Agent Service, using the same technology, the only difference is that the Standalone Agent does not rely on a computer being present onsite to run, making it ideal for sites with strict security policies and sites with no terminals.

Once the Standalone Agent has been configured, it can be connected to the chosen network and will monitor the specified IP addresses at regular intervals which are set within the OneStop MPS Portal website.

As the OneStop Standalone Agent uses the same technology to monitor print devices as the OneStop Agent Service, the only additional technical points to consider are below.

### Standalone (Raspberry Pi) Data Collection Agent Information

The OneStop Standalone Agent uses the following ports;

PORT 161 = SNMP

PORT 23998 = HTTP REQUESTS

PORT 23999 = DEVICE DISCOVERY

### What is required to use the OneStop Standalone Agent?

The OneStop Standalone Agent requires an RJ45 network cable, a free RJ45 network point and power. A power supply is included with the package.

## Agent Operation Guidelines

The below document will cover the basic functions of the agent and what is required for consistent operation.

### Installation and service:

The agent should be installed as administrator always, this is because the agent runs as a service and only an administrator can install services to the service manager, running as admin also ensures the agent receives the permissions it needs to run and send readings to the portal.

### Permissions and protocols

The agent will by default use the Local System service account to run, however, if local system has had its permission set edited or a custom service account is preferred, any service account can be applied to the agent as long as the following permissions are assigned to said account:

- Rights to scan the local network – our agent will need to scan the local and connected networks in order to scan and return data from Printer devices. The agent needs Read permissions on the network, not write, the agent never writes to any devices.

- Rights to create and send XML files to upstream server – The agent writes the data it returns from devices to xml files which it will then upload to the portal, these XML files need to be allowed through any local firewalls and the agent needs the read/write/modify permission on its agent folders:

  C:\ProgramData\Business I.T. Systems Ltd\OneStop Collection Agent
  C:\Program Files (x86)\Business I.T. Systems Ltd\OneStop Collection Agent

- Ports need to be open – The agent needs the rights to Read the devices over Port 161 SNMP and to be able to ping devices over ICMP. Outbound ports to the server are 80 HTTP and 443 HTTPS, one of these ports needs to be open.
- The agent is equipped to use TLS 1.2, making sure this channel is enabled on the local network will allow the agent to utilise this secure channel.

## SNMP Settings

In order for the agent to be able to read the machines, SNMP settings need to match on both the device and agent. For SNMP v1/2 the only value in consideration is the community string which, by default should be set to 'public'. The agent will have this string set by default to so if the community string has been changed to a custom string, please update the agent's SNMP settings.

For SNMP v3 the same applies, all values need to match however in v3 there are 2 passwords, an encryption type and a context name that need to be specified, ensure these are all the same and the agent will be able to connect.

## Install location and Devices

The agent should preferably be installed on a server, however, if the agent is installed on a computer, ensuring that this PC is turned on 24/7 will limit the interruptions to the service.

The agent will perform a meter reading scan once per day, at this time all Printers on the network will need to be turned on and contactable, any machines switched off during this

time will miss the meter reading, as such it is advisable to set the scan time for a point where machines are likely to be switched on.

### .NET Framework

The latest OneStop Collection Agent is version 2.3. This agent version requires a minimum of Microsoft .NET Framework version 4.5.2 which is the minimum supported framework version by Microsoft. If a v2.3 agent is installed on a site without this framework or greater installed, the agent will fail to run.

Operating systems and applications that are running versions older than this are at a potentially substantial security risk and should consider updating when possible.

The earliest operating systems that can support 4.5.2 is Windows 7 Service Pack 1 and Windows Server 2008 R2 SP1. Any systems prior to this such as XP and Windows Service 2003 are unable to support versions post Framework v4 and will be unable to run the new agent.

### Antivirus:

When you are installing the OneStop Collection Agent on a PC/server that has anti-virus software installed, in some cases the anti-virus software will stop the agent service from running and thus no readings can be taken. To overcome this issue, you will need to make sure that you exclude the Agent in the AV software.

## Remote command queuing

Commands can be queued on the OneStop server for each agent. The agent will check for new commands at a pre-determined interval, and action the commands.

### How are the Agent commands sent?

The agent makes a request to the OneStop Importer Web Service, requesting any queued commands. If there are any present, they are queued on the agent, and results uploaded to the server if needed. If the Agent command interval is set to 0, the agent will not check for commands

The commands consist of a numeric value instruction the agent what to do, and an option string parameter, such as IP address when the MIB walk is requested

Currently, the following commands are supported:

### Restart Agent

This will restart the OneStop Collection Agent Service.

### Force Discovery Scan

This will force a device discovery scan and will upload the devices readings to OneStop.

### Upload Log Files

This will send the log files to a .zip file and upload the agents log files to the OneStop server

### Delete Log Files

This will delete the agents log files.

### Set Log Mode

This will change the agent log mode.

### Walk MIB

This will check the printer MIB (Management Information Base) for the IP Address specified, if available, then a MIB walk will be performed and the MIB information will be stored into a .txt file. This file is then sent to a .zip file and uploaded to the OneStop server.