PagePack™ Assistant
Security and Evaluation Guide

Version: 2.0
Date: Nov 2008

PGPGL-03UA

Contents

List of Figures and Tables

1 Overview and "How to use this Guide"

1.1 Goals and Objectives

Network and data security is one of the many challenges that businesses face on a daily basis. Recognizing this, Xerox Corporation continues to engineer and design all of our products to ensure the highest level of security possible.

This document provides additional background on the Xerox PagePack software capabilities, and specifically focuses on the security aspects of PagePack Assistant client software - with the goal of ensuring that customers understand and feel confident how the PagePack Assistant functions are performed and that machine data is transmitted to Xerox in a secure, accurate and auditable manner. This guide is designed to help a customer certify, evaluate and approve the deployment of the PagePack Assistant software in support of their PagePack contract. The document combines sections of information related to the PagePack Assistant's potential impact to security and network infrastructure, with calculations of theoretical network traffic.

Xerox recommends that customers read this document in its entirety and take appropriate actions consistent with your information technology security policies and practices. Customers have many issues to consider in developing and deploying a security policy within their organization. Since these requirements will vary from customer to customer, the customer has the final responsibility for any and all implementations, re-installations and testing of security configurations, patches and modifications.

1.2 Intended Audience

It is expected that this guide will be used by the customer's network administrator prior to installing the PagePack Assistant software. In order to get the most from this guide, the readers should have an understanding of:

- The network environment where the PagePack Assistant will be installed
- Any restrictions placed on applications that are deployed on that network
- The Microsoft Windows Operating System

1.3 Using this guide

There are two main scenarios for using this guide. This guide can be used by a customer that does not have acceptance and evaluation procedures for this type of software. The other scenario is for a customer that has defined guidelines to evaluate software being introduced into their environment. In both cases, the three identified areas of concern are Security, Impact to the network infrastructure and what other resources might be required to install, use and support the PagePack Assistant software.

This guide should be used to gather information about these areas and determine if further investigation is needed. To that end this document is divided into five main areas for review.

1. This overview
2. An introduction to the PagePack Assistant including systems requirements
3. Potential impacts to a typical customer network deployment including:
   - Security information, implications and recommendations
   - Roles and permission requirements of the PagePack Assistant users.
4. Information about features that impact the network. These may include estimates of traffic generated, changes to the network infrastructure, or other resources required
5. PagePack Communication with Xerox PagePack Back Office System
   - Includes Web Data Interaction and Periodic Data Update Between PagePack Assistant and PagePack BOS.

1.4 Limits of this guide

The intent of this guide is to provide meaningful information to be used when evaluating the PagePack Assistant software. However this guide can in no way provide a complete information source for all customer network administrators. Therefore, this guide must propose a hypothetical customer printer environment in order to accomplish its goal. Where the customer's network environment differs from that which the guide describes, the customer's network administration team and Xerox PagePack Support representative will be left to subjectively understand the differences and decide on any certification modifications and/or future steps.

Additionally:

- Only those features within PagePack Assistant known to have some discernable impact to the overall customer network environment, whether it be the overall network, security, or other customer resources will be reviewed in this guide.
- The information provided is related to a specific PagePack Assistant version release. Although much of this information will remain constant through the software's life cycle, some of the data provided will be revision specific.

2 Introduction to the PagePack Assistant (PPA)

2.1 Product Overview

The PagePack Assistant application is a software package that discovers and monitors network printing devices, specifically Xerox PagePack office printers and multifunction devices. PPA features a built-in alert detection system and has the capability to send an email message to an appropriate user when certain conditions exist in the devices being monitored. PPA provides clear and concise status of all networked printers. Printer status conditions can be displayed and monitored by viewing the software user interface. Directly from PPA, the printer administrator can:

- Discover network connected PagePack printers
- Monitor printers for status and alert conditions and notify users (via email) when faults occur.

PPA supports industry-standard SNMP (Simple Network Management Protocol) MIBs, however, the amount and types of management that PPA can provide is dependant on the printer's level of conformance to those standards.

- Printer Management features covered by industry standards
  - Device Identity (i.e. model, serial number, manufacturer, etc.)
  - Device Properties (i.e. input trays, output bins, serial number, etc.)
  - Device Status including overall state, detailed status, UI messages, etc.
  - Consumables + levels (toner, fuser, print cartridge, + device unique parts)
  - Supported print protocols (LPD, HTTP, Port 9100)
  - TCP/IP protocol suite (SNMP, TCP, UDP, IP, NIC details)

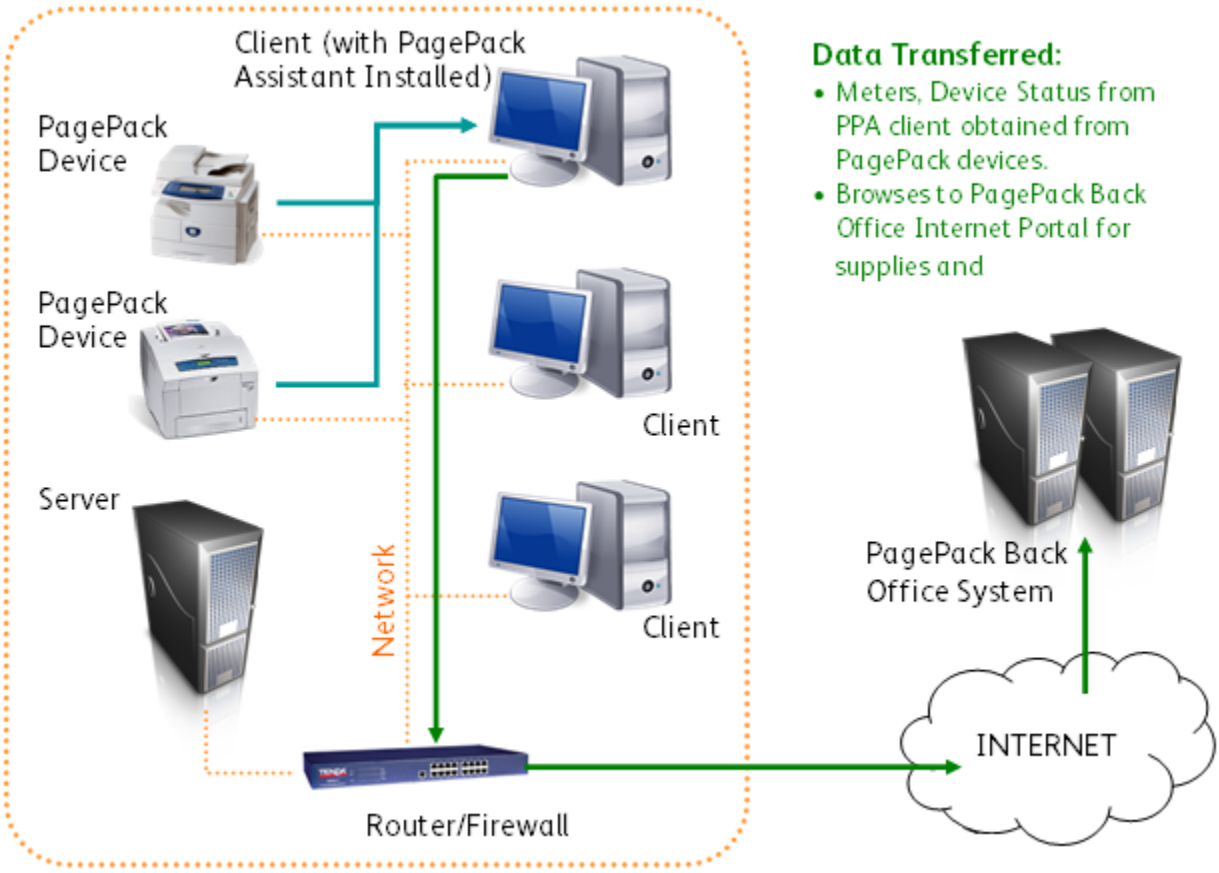
2.2 PPA Deployment Requirements

PPA is deployed by installing on a customer's desktop or laptop computer that shares the network with those printers to be monitored. For the PPA software to operate, the computer that has the PPA software installed on it should be turned on during normal business hours at least twice a week. The communication is run as a service and does not require a user to be logged on during those times.

Note: Depending on connectivity of PPA software, the scheduled events for meter reads and alert activity may be affected.

PagePack System Component Architecture

The diagram below shows a typical configuration within a customer's network that might be deployed. The PagePack Assistant software is installed on one of the customer's networked computers that can access the PagePack devices through the customer's local network.



Recommended Hardware Requirements

The hardware recommendation listed below is what would be expected when installing PPA on new equipment in a production server environment, but may not represent the minimum hardware needed. For those requirements, consult the PPA README documentation provided by the PPA installer.

Hardware	Requirement
Processor	Pentium IV Processor compatible executing at 1 GHz or faster
RAM Memory	256 MB (minimum), 512 MB (recommended)
Free Storage	100 MB (minimum for application and database)
Misc. Hardware	CD-RW/DVD, KBD, Mouse, Monitor, Ethernet connection

Table 1: Recommended Hardware Requirements

Note: In the event that PPA is to be installed on a rack mounted server, it is expected that a Keyboard-Video-Mouse terminal interface to the server be provided.

Server Software Requirements

Operating System Requirements

PPA can be executed on Microsoft Windows XP (Home or Professional) and server platforms (Windows 2003 SP1 and Windows 2000 Server/Pro with SP4).
Notes:

- It is always recommended that host computers be kept up to date with the latest critical patches and service releases obtainable from Microsoft.
- Network Transmission Control Protocol/Internet Protocol (TCP/IP) must be loaded and operational.

Database Requirements

PPA installs a Microsoft Access 2000 database file (*.mdb) within the installation directory that stores printer data and application settings. No database licensing is necessary for PPA itself.

Browser Requirements

Although the PPA is a windows application that does not require a web browser to view, the PagePack Back Office Portal is web based and requires the use of a browser to access. Optimal performance and security can be achieved when using Internet Explorer 6.0 and higher.

2.3 Printing Device Requirements

Network Printer Discovery / Monitoring Requirements

For successful management by PagePack Assistant, all SNMP-based printer devices should support the mandatory MIB elements and groups as defined by the following standards:

- RFC 1514/2790 (Host Resources MIB v1/v2)
- RFC 1759 (Printer MIB v 1)

3 PagePack Assistant Security

3.1 General Security Information

Security is an important consideration when evaluating tools of this class. This section is intended to provide some background into the security methods used by PagePack Assistant and provide some information on changing security related defaults, if required.

Windows Server Security

PPA is compatible with the security features built into Microsoft Windows Server OS incl.:

- User authentication and authorization
- Secure Terminal Services support
- Group policy deployment and management
- Internet Connection Firewall (ICF) including;
  - Security Logging settings
  - ICMP settings

Printer Security

PagePack Assistant has the ability to:

- Expose and display open TCP and UDP ports on any network printer. This can be used to identify potential security holes within the print environment.
- Lock the device console to prevent tampering
- Inspect printer protocols and service settings for unauthorized changes
- Turn on authentication for network scanning.
- Disable unused protocols and services on Xerox network printers
- Define Simple Network Management Protocol (SNMP) GET/SET/TRAP community names
- Manually add SNMPv3-compliant printers in order to authenticate & encrypt all communication between them.

SNMP Security

The SNMP is the most widely-used-network-management tool for communication between network management systems and the devices being managed. PPA uses SNMP during its Discovery operations to provide detailed information about printers it “finds” on the network. After Discovery, SNMP is used to monitor printers for faults, changes in status, to carry configuration set changes and support printer troubleshooting.

SNMP v1-v2 security

In its current form, SNMP's security is limited to three methods of access: READ-ONLY, WRITE-ONLY and READ-WRITE. Access from PPA to the devices is granted by the use of "community name strings," which are the names of the groups to which the devices belong. By default, PPA uses the community name string of “public” which is the printer manufacturer’s default setting. The user can elect to change this setting on the devices and has the ability to change the “community name string” that PPA uses to match the settings for the printers configured.

Required Permissions

There are no special account privileges requirements in order to execute the PagePack Assistant, as it will automatically execute upon log in for those accounts at Windows “User” account type or higher. To install the software, the user needs to have administrative account rights to the host system to allow system level changes to occur.

4

Network Impact in a typical PagePack Assistant Deployment

4.1 Systems Infrastructure

Network Ports Used by PPA

PPA relies on a number of TCP/IP network ports, all pre-defined by the Windows operating system as defaults to perform its activities. A table of PPA features, network protocols used and ports accessed with the data direction (related to the PPA client software) are defined below.

PPA Feature/Function	Protocol	Port # used	Data Direction
Network printer discovery + Retrieval of capabilities /status & usage counters + Single device configuration	SNMP v1, v3	161	Outgoing
Network printer web page	HTTPS	443	Outgoing
Network Printer Discovery + Troubleshoot	PING / ICMP	none	Outgoing

Table 2: Ports and Protocols Used by PagePack Assistant

Note: Some customer environments may restrict the routing of ICMP packets across routers using an access control list to avoid "denial of service" attacks and worms from impacting their network. As a result, the "[Add Printer] within [Printers] device view" feature will be adversely impacted:

4.2 General Discovery considerations

The Discovery function allows PPA to search for network printers on a customer's intranet. Printer discovery is a crucial part of the PPA application as it is the main method to get networked connected devices identified and stored in the local database. It is a compound operation that involves the generation of unique network addresses and the subsequent querying of those addresses (via SNMP) for printer type and general configuration information. Since this operation uses the network resource, consideration should be made as to what is to be detected and to configure the Discovery to achieve this goal with a minimum of network contention. PPA provides a number of methods to discover to gain the most information with the least impact to network bandwidth.

Device Discovery Methods Employed by PagePack Assistant

After being installed onto a networked computer, the PagePack Assistant will begin to automatically discover network print devices located on the same subnet of the host that it is installed on within the customer's network. Depending upon network configuration, this initial discovery could identify all of the network printers within the customer. The method used to perform this initial discovery is known as "local subnet discovery".

Once the registration process has completed between the PPA and the PagePack BOS, a list of one or more PagePack printers under contract will be automatically provided to the PPA by the PP BOS to find on the network. For those printers not already discovered during the initial broadcast discovery during installation, the PagePack Assistant seeks those devices within the customer's network by using a discovery method known as "PagePack Automatic Discovery". The PagePack Assistant also provides two other methods of allowing the customer to specify which printers to discover. The first method allows the customer to directly enter the network IP address into an advanced user mode screen if they know the printers network address and the other method allows the customer to enter a subnet address specification of the network where they expect to find PagePack printers.

The next sections describe each major Discovery method and its potential network impact.

4.3 Discovery Overviews

PagePack Automatic Discovery

Operation

Automatic Device Discovery is performed when the PagePack Assistant has been given the list of PagePack printers that are under contract to be discovered. This process will obtain IP addresses from the customer's network routers using SNMP queries to the router. These network addresses can be used to query a given network entity to determine if it is a printing device. PagePack Assistant maintains a mapping between all of the discovered devices and IP addresses currently discovered.

PagePack Automatic Discovery Method Details:

How PagePack Assistant performs this discovery method is as follows:

- An SNMP-based broadcast packet is sent out to the local subnet. In this packet, PagePack Assistant requests a single specific datum which PagePack Assistant uses to identify routers from the list of responses received. Devices that do not respond to this SNMP-based broadcast packet are automatically excluded.
- PPA will then create two lists based upon all responses received on the local subnet;
  - A list of live, non-router-related IP addresses (printers, computers, etc)
  - A list of devices identified as routers.
- At this point the PagePack Assistant will then began to query each non-router IP address for printer information given the network addresses gained during the 1st phase of the PagePack Automatic Discovery.
- Once all of the printers found within the initial phase of the PagePack Automatic Discovery have been queried, the list of contracted PagePack printer serial numbers provided by the PP BOS is compared to those serial numbers discovered. If a match occurs, that printer will be identified within the PPA user interface as being "Managed". If a serial number identified by the PP BOS is not in the generated list of

printers just discovered, the PagePack Assistant will attempt to extend its router discovery to include a second ring of routers, to identify network candidates to be discovered and interrogated to find a match with the contracted list of printers.

- In the event that this second round of PagePack Automatic Discovery fails to match up all of the serial numbers provided by the PP BOS, and third and last PagePack Automatic Discovery will be performed against a new list of routers. This 3rd PagePack Automatic Discovery "hop" is the last one performed and is expected to discover all of the printers identified by the PP BOS as being under contract.

Network Impact

Typically, the impact to the customer network is barely noticeable although a steady stream of packets can be seen. Also, router usage-related logs may grow in size due to this discovery method.

IP Sweep

IP Sweep Operation

The IP Sweep Discovery method is one of the methods to discover printers on a network within PagePack Assistant. A packet is sent to every IP address within the user-defined subnet or address range list. These address ranges should be known and provided before running the discovery.

The specific algorithm used within this discovery method is:

- A single packet is sent to each IP address contained within each subnet or address range defined within the PagePack Assistant "Find More Printers" advanced page. In this packet, PPA requests a value for a single SNMP-based identifier.
- For each device that responds to SNMP request, PagePack Assistant will add the network (IP) address of the response device into its list of "live" IP addresses.
- PagePack Assistant then queries those responding devices with live IP addresses for two more pieces of information . This enables the PagePack Assistant to identify the responding device as a printing device from non-printing devices.
- For those devices identified as printers, PagePack Assistant then continues to query the devices to obtain some basic attributes of the printer.
- Based upon the identity of each printing device, PagePack Assistant then queries the appropriate vendor-specific device database found within the device in order to obtain the printer's serial number

When to use

Within the PagePack Assistant, the IP Sweep Discovery method is provided within the "Find More Printers" tab in the "Advanced Settings" section. As the discovery of managed PagePack devices is expected to be automatically performed after installation, this method should only be needed in the event that a device under contract can not be discovered automatically. In order to use this method, the customer has to have knowledge of the IP subnet addresses where managed PagePack printers may exist.

Network Impact

The amount of network traffic generated by a sweep-based discovery is minimized because the requests are directed to specific IP addresses

Managing Discovery

The Discovery process can be managed in a number of ways.

- Discovery methods can be setup to perform specific actions (i.e. discover only printers; only Xerox printers, only those printers in a certain location, etc.). This "throttling" ability can be used to customize the discovery processes and reduce the amount and types of network traffic generated by PPA.
- It can be controlled by the use of SNMP community name strings to query certain network printers over others.
- The discovery will provide active status on its progress.
- Device timeout and retry parameters are pre-defined with a setting of five seconds for attempt tryout and 1 retry allowed to get print information from slower network subnets on a customer's network.

4.4 Discovery Network Data Calculations

As mentioned earlier, each printer discovered can create as much as 7KB of discovery-based traffic.

IP Sweep Network traffic calculations

To help understand network discovery and its impact to a network, the following are provided as assumptions:

- 10 network printers will be discovered
- The number of bytes transferred between PPA and the networked printer is 7KB.
- Discovery executes once per month.

The calculation for the network bandwidth loading for printer-based discovery over one month is: **1** cycles/month x **10** printers x **7186** Bytes/printer = **71860 bytes** = **70KB/month**

4.5 Network Impact Considerations of Printer Management

PPA communicates with the printers under management on a regular basis. Examples include Status Polling and Historical Data gathering (scheduled to run at certain times) and device generated alerts (occurring at random times). Each transaction consists of a series of "back-and-forth" SNMP queries with the device, beginning with an "are you there" query, then progressively asking for more information (with each device response) until the transaction purpose is complete.

Scheduled Communications Calculations

Status Polling Assumptions:

- Status Polling traffic averages 2 KB per transmission
- Status Polling occurs every day, once per every two hours (24x7)
- 10 printers are reporting

The calculation for the amount of net traffic generated during a month of status polling is: **10** printers x **12** polls x **30** days x **2048** Bytes = 7,372,800 bytes or approx. **7 MB per month**

Historical Data Gathering Assumptions:

- Historical Data Gathering traffic = 4KB per transmission
- Gathering occurs once daily
- 10 printers are reporting

The calculation for the amount of net traffic generated during a month of historical data gathering is: **10** printers x **30** days x **4096** Bytes = 1,228,800 or approx. **1.2 MB per month**

4.6 Total PPA Data Transfer Calculations

The next two traffic calculation examples show totals for both a typical and a more exaggerated network data transfer size during a one month period. Both totals include the use of regularly scheduled Discovery, Status Polling and Historical Data Gathering.
The first example estimates traffic based on the typical sizes of network communications used by PPA. This also assumes PPA is configured to business hours of 8 hours/day and 21 days/month. Using 7KB for discovery, 2KB for Status Polling, and 4KB for Historical Data Gathering, the network traffic could be as much as follows for the same 1,000 printers in a given month:

Discovery total
1 cycles/month x **10** printers x **7186**Bytes /printer = **71** KB/month

Historical Data Gathering total
30 days/month x **10** printers x **4096**/printer = **1228** KB/month

Status polling total
30 days/mo x **12** polls/day x **10** printers x **2048**/printer = **7372** KB/month

OVERALL (Typical) TOTAL
71 KB (discovery) + **1228** KB (historical) + **7372** KB (status polling) = **8671** KB/month (8 MB/month)

Email Data Comparison
The following email example can be used as a comparison to the amount of traffic generated by PPA. Assume an average size of 3 KB (essentially text-only) with 10 employees using email 20 times per day every business day a month.

Email Data - Assuming 3KB average size
30 days/month x 20 emails/person x 3072 Bytes/email x 10 people = 18,432 KB/month = approximately **18** MB of Email Data/month

The example above is based on text only emails and demonstrates the lower end of traffic. It does not include any attachments to email traffic that are typical.

Note: Although it is difficult to accurately determine the amount of network traffic generated and consumed by an application like PPA (and/or email) with all of its options and activity, the comparison above proposes that the PPA data created and transferred across the network is significantly lower than that created and consumed by a conservative email estimate.

5

PPA Communication with Xerox PagePack Backoffice System

5.1. Overview

The Xerox PagePack Assistant communicates directly to the Xerox PagePack Back Office System ("PagePack BOS") through the Internet, transferring associated printer and device information through a secure web services transfer mechanism (SSL) automatically. This device information is then used by BOS to update device status and meter reads.

The security of this communication method is protected by several mechanisms.

- The PagePack Assistant must be configured with both a valid PagePack BOS URL and a valid PagePack BOS company ID from the Xerox PagePack BOS administration. This data is pre-configured within the customer's PPA installer.
- After installation, the PagePack Assistant will automatically request registration with Xerox
- The Xerox PagePack Assistant to Xerox PagePack Back Office System web service communication method is further secured by the use of the HTTPS protocol (with 128 bit encryption) when configuring the web service communication method in XDM. HTTPS is http using a Secure Socket Layer (SSL). HTTPS is a communications protocol designed to transfer encrypted information between computers over the World Wide Web.
- PagePack Assistant initiates all contact with Xerox PagePack BOS. PagePack BOS does not send contact requests to the PagePack Assistant.

Web Service Data Interaction Between PagePack Assistant and PagePack BOS

PagePack Assistant "Ping" to PagePack BOS - periodically PPA will send a health status ping to PP BOS to "let it know" that it is still there and in good status. Ping data content includes Company ID, PagePack Assistant ID and "Hello" message. The data size is ~ 3 KB. Frequency is set to once every sixty minutes.

PagePack Assistant to PagePack BOS Periodic Data Update

Periodically PPA sends certain information it has about a device or devices to PP BOS. This "push" of data is needed to keep PP BOS up-to-date with new meters and status changes and contains the most amount of data that is transferred between the applications. For each device, the data content includes; Complete Device Record (~ 4KB), Device Alert Table (~400 Bytes). Differences information (i.e. changes since last "push") include: Historical Meters (approximately 4KB). The frequency of this communication is daily