Xerox Device Data Collector 1.3

Security and Evaluation Guide

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

Table of Contents

Table of Figures

Overview and How to Use this Guide

Goals and Objectives

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

This document provides additional background on the Xerox Device Data Collector (XDDC) software capabilities, and specifically focuses on the software's security aspects. This document will help you better understand how XDDC functions and help you feel confident that XDDC transmits device data in a secure and accurate manner. This guide will help you certify, evaluate, and approve the deployment of XDDC in support of your contract. It includes information on XDDC's potential impact on security and network infrastructure as well as calculations of theoretical network traffic.

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

Intended Audience

It is expected that this guide will be used by your network administrator before installing XDDC. In order to get the most from this guide, you should have an understanding of:

- the network environment where you will install XDDC,
- any restrictions placed on applications that are deployed on that network, and
- the Microsoft Windows® operating system

Using This Guide

There are two main scenarios for using this guide: if you are a customer who does not have acceptance and evaluation procedures for this type of software or if you are a customer who has defined guidelines. In both cases, the three identified areas of concern are security, impact to the network infrastructure, and what other resources might be required to use XDDC.

Use this guide to gather information about these areas and determine if you need to investigate XDDC further. This document is divided into these areas:

1. This overview

2. An introduction to XDDC
3. Potential security-related impacts to a typical customer environment including:
   - Security information, implications, and recommendations
   - Roles and permission requirements of XDDC users
4. Information about features that impact the network, which may include estimates of generated traffic, changes to the network infrastructure, or other required resources.

Limits to this Guide

This guide is meant to help you evaluate XDDC, but it cannot be a complete information source for all potential customers. This guide proposes a hypothetical customer printer environment; if your network environment differs from the hypothetical environment, your network administration team and Xerox Support Representative must understand the differences and decide on any certification modifications and/or future steps. Additionally:

- This guide only describes those features within XDDC that have some discernable impact to the overall customer network environment, whether it be the overall network, security, or other customer resources.
- The guide's information is related to the current XDDC release. Although much of this information will remain constant through the software's life cycle, some of the data is revision-specific, and will be revised periodically. IT organizations should check with the Xerox Support Representative to obtain the appropriate version.

Xerox Device Data Collector Tool Overview

Product Overview

XDDC discovers network and direct printing devices, specifically office printers and multi-function devices.

XDDC may be used to support pre-sales device data gathering activities, primarily involving network device identification and the sampling of their usage counters to help in estimating the output volumes at a customer's site. The XDDC Data Collector is accessed at the customer's site via a Web browser through a pre-defined Xerox Internet link URL and as a result, does not require installation using the Windows® Add/Remove program utility.

The XDDC tool can discover network printing devices using industry-standard Simple Network Management Protocol (SNMP) MIBs to collect the current meter reads of those devices scanned. After loading the XDDC Data Collector into their Web browser, the end-user must initiate the XDDC Device Discovery before the software will discover any devices because the process is not automatic. Discovered device information, which the end-user can access through the Internet, is automatically uploaded to the XDDC server located within the Xerox hosting facility. At a later date, the end-user will have to perform a second execution of the same Data Collector to get a second set of meter reads from the discovered devices, which again will be automatically uploaded to the XDDC server. With at least two meter read samples from the network devices, the pre-sales analyst can estimate the output volume at the customer's site and use this information to develop a proposal.

You can do the following from XDDC:

- Discover network-connected printers
- Discover direct-connected printers
- Get network printer information based on industry-standard Simple Network Management Protocol (SNMP).

XDDC Deployment Requirements

XDDC requires the installation of the Microsoft ClickOnce-based application. For more information on the deployment requirements, see the Security section.

The creation of an XDDC Data Collector within the XDDC server enables end-users to use XDDC. The Data Collector contains a signed Microsoft® ClickOnce-based application that the end-user accesses from a Web browser via the automatically created URL, which the XDDC server produces during the collector's creation. The individual who creates the Data Collector sends the end-user the Data Collector's URL via e-mail.

Once the end-user accesses the XDDC Data Collector link in the Web browser, the XDDC End User License Agreement (EULA) will display, requiring the end-user to acknowledge and accept the terms and conditions for

using the Data Collector. After the end-user accepts the EULA, XDDC will display a message, prompting the end-user to allow the application to run. The end-user will only see this message if this is the first time that the XDDC application is being used for this user on this computer. If allowed, the Data Collector application will run from the end-user's Web browser and start collecting local subnet identification.

Xerox Device Data Collector System Component Architecture

This diagram shows a typical configuration that a customer may deploy within their network. In this example, XDDC runs on a networked computer that can access the printers through the local network.

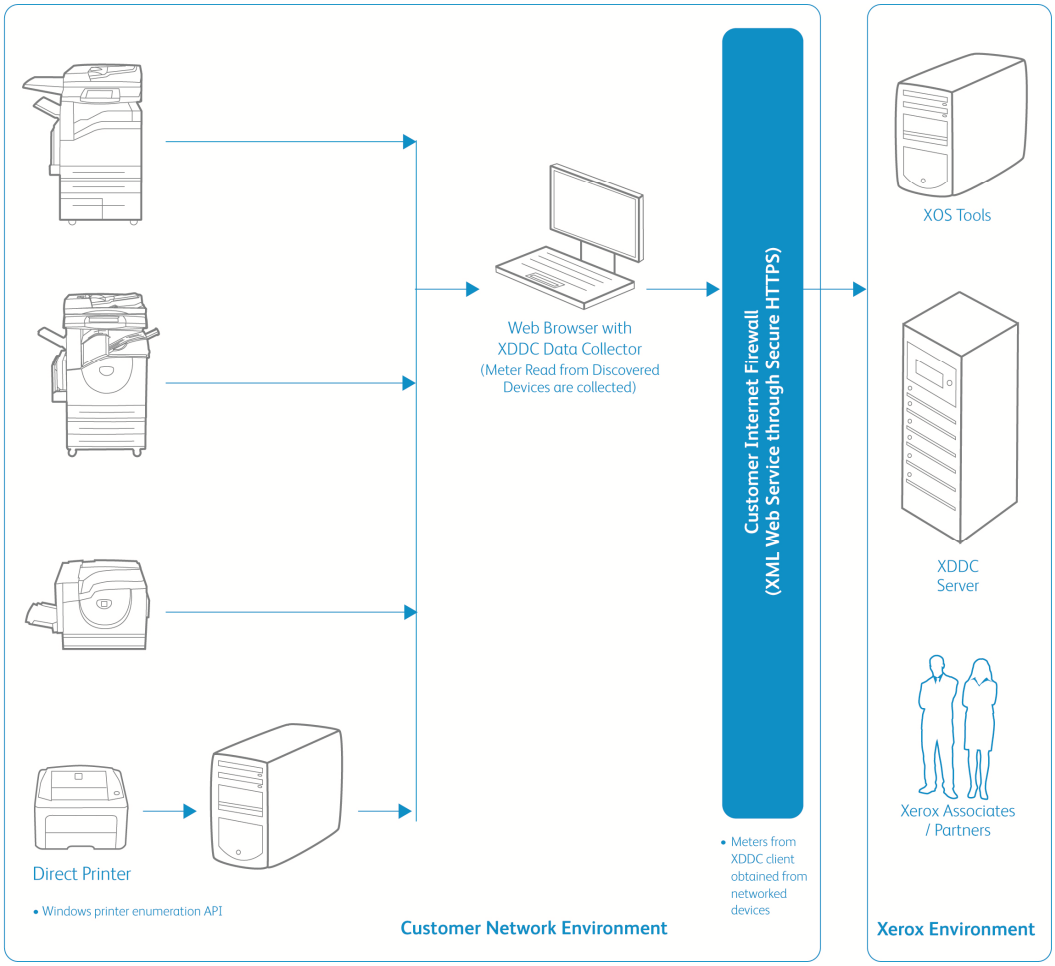


Figure 1: Typical Xerox Device Data Collector Deployment

Browser Requirements

XDDC requires the use of Microsoft Internet Explorer® versions 6.0, 7.0, or 8.0 or Mozilla Firefox® versions 3.5 or 3.6. You must add the XDDC URL to your trusted sites list.

Recommended Hardware and Operating System Requirements

Operating System (32-bit and 64-bit)

- Windows® XP Professional with Service Pack 3
- Windows Server® 2003 with Service Pack 2
- Windows Server® 2008 and 2008 R2
- Windows® 7 Professional and Ultimate
- Windows Vista® Service Pack 1 Professional and Ultimate

Memory

- Minimum 512 MB RAM (1 GB RAM Recommended) for Windows® XP and Windows Server® 2003
- Minimum 1 GB RAM (1.5 GB RAM Recommended) for Windows Vista®, Windows® 7, and Windows Server® 2008 and 2008 R2

Processor: 1.7 GHz processor or better

Hard Disk: minimum free space is approximately 100 MB for the application and up to 500 MB for the Microsoft®.NET framework, if not previously installed.

Minimum Resolution: 1024x768

Internet connection: Required

Notes:

- We recommend that you update your host computers with the latest critical patches and service releases from Microsoft Corporation.
- The Network Transmission Control Protocol/Internet Protocol (TCP/IP) must be loaded and operational.
- Requires SNMP-enabled devices and the ability to route SNMP over the network. It is not required to enable SNMP on the computer where XDDC will be installed or any other network computers.
- Add the Device Data Collector's site to the trusted zone.
- Do not set the security settings for the trusted zone too high; set them to the next lowest level, which depending on the operating system, is either Medium or Medium-High.
- Install Microsoft®.NET 2.0 (minimum requirement), 3.0, or 3.5 on the client machine if it is not already installed. Microsoft® .NET 3.0 and 3.5 will often come pre-installed on the latest Microsoft operating systems.
- If you make any changes to the client security or configuration, restart Microsoft Internet Explorer® to ensure the new settings are applied successfully.

Unsupported Configurations

Any version of Macintosh® operating system, Unix® operating systems, Windows NT® 4.0, Windows® Media Center, and Windows® 2000.

Database Requirements

XDDC installs temporarily Microsoft SQL Server® 2005 Compact Edition (SQL CE) database engine and database files that store printer data and application settings within the end-user's temp directory. No database licensing and installation is necessary for XDDC.

Printer Requirements

Network Printer Discovery/Monitoring Requirements

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

- RFC 1157 (SNMP Version 1)
- RFC 1213 (MIB-II for TCP/IP-based Internet)
- RFC 2790 (Host Resources MIB v1/v2)
- RFC 1759 (Printer MIB v 1)
- RFC 3805 (Printer MIB v 2)

Direct Printer Requirements

- Queue-based discovery depends on user permissions on domain and/or across computers, NetBIOS File and Printer Sharing, Network Discovery, and WMI.

Security

Since security is an important consideration when evaluating tools of this class, this section provides information about the security methods used by XDDC.

Application

XDDC relies on a signed Microsoft® ClickOnce-based application to gather data, and submit to the XDDC server. The user interface that displays the gathered data is accessible only to the specific Data Collector used to discover the devices.

Install

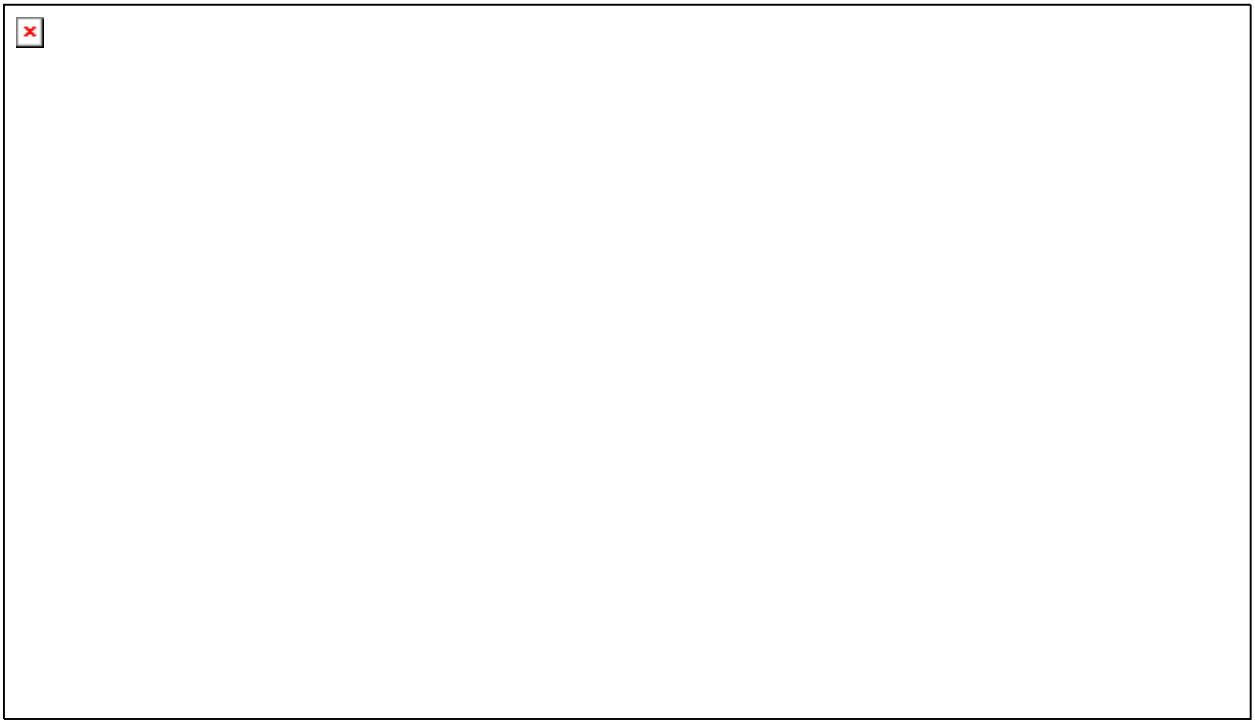
A Microsoft® ClickOnce-based application is used to run the XDDC application. Although the data collector does not require administrative permissions for installation and use, the end-user and the browser need to have the required permissions to run the Microsoft® ClickOnce-based XDDC application. To ensure XDDC will run, add the XDDC URL to the trusted sites list and log in as a system administrator. However, adding the XDDC URL to the trusted sites list is not required; depending on the individual system setup, XDDC can also run as a non-administrator user. XDDC has been tested to work with the Windows® firewall, so there should be no problem with most security configurations.

Temporary File Storage

The temporary file storage is where the ClickOnce application files are stored after being downloaded and are executed from this location. This location is managed by the browser.

Licensing

Consent and acceptance of the XDDC Data Collector End User License Agreement is required to execute the Data Collector.



Network Printer

The Simple Network Management Protocol (SNMP) is the most widely-used-network-management tool for communication between network management systems and the networked printers. XDDC utilizes SNMP during discovery operations to retrieve detailed data from output devices detected on the network. XDDC supports SNMP version 1 and version 2 protocols. The following application properties will help you better understand the impact of XDDC on printer security:

- it does not modify the settings on the printer; it only reads them.
- it does not register for SNMP traps.
- it does not gather device status data
- it does not gather any print job or user data.
- Once the XDDC Data Collector browser session is dismissed, no further activity will occur from the Data Collector.

SNMP v1-v2 Security

Access from XDDC to the devices is granted by the use of community name strings. Although usually referred to as the password, for SNMP operations, the community name provides a very simple level of authentication for all PDU operations. By default, XDDC uses the community name string of public, which is the printer

manufacturer's default setting. You can elect to change this setting on the printers and you have the ability to change the community name string that XDDC uses to match the settings for the configured printers.

XDDC does not support SNMP v3 only configured devices. in order to communicate with printers that have SNMP v3 enabled, the printers must also have SNMP v2 enabled for XDDC to communicate with them.

Xerox Device Data Collector Server Integration

XDDC communicates with the XDDC server multiple times during a scan. It is important to recognize that XSM is hosted in an ISO 27001-compliant facility. The data exchanged during such communications is compressed and encrypted. The security of this communication is protected by several mechanisms.

- The XDDC server database sits behind a secure firewall and is not accessible from the Internet.
- The Xerox Device Data Collector to XDDC server Web service communication method is secured by the use of the HTTPS protocol (with 128-bit encryption). HTTPS is HTTP using a Secure Socket Layer (SSL).
- XDDC initiates all contact with the XDDC server on the client computer through ClickOnce and no special firewall configuration on the site is required to enable communications.
- Collected data can only be accessed per collector within XDDC. Access to data across collection is only accessible within XSM according to the account access permissions.
- Printer Data Export: occurs by default once scan has ended.

Device Information Communicated to XDDC Server

The data that is sent to the XDDC server and ultimately to XSM is printer-specific, which is mostly billing counters and printer attributes. Here is the list of printer fields sent to XSM:

IP Address	Fuji Xerox Meter 1
MAC Address	Fuji Xerox Meter 2
Serial Number	Fuji Xerox Meter 3
Manufacturer	Fuji Xerox Meter 4
Model Name	Images Sent
2 Sided Sheets	Internet Fax Images Received
Black + Color Level 1 Impressions	Internet Fax Impressions
Black Copied Impressions	Large Impressions
Black Copied Large Sheets	Level 1 Impressions
Black Impressions	Level 2 Impressions
Black Large Impressions	Level 3 Impressions
Black Printed Impressions	Network Scanning Images Sent
Black Printed Large Sheets	Page Count
Color Copied Impressions	Printed 2-sided Sheets
Color Copied Large Sheets	Printed Impressions
Color Impressions	Printed Large Sheets
Color Large Impressions	Scanned Images Stored
Color Level 2 Impressions	Server Fax Images Sent
Color Level 3 Impressions	Server Fax Images Received
Color Printed Impressions	Server Fax Impressions
Color Printed Large Sheets	Sheets
Copied 2-sided Sheets	Total Impressions
Copied Impressions	Port Type
Copied Large Sheets	Printer Type
E-mail Images Sent	Queue Name
Embedded Fax Impressions	Share Name
Embedded Fax 2-sided Sheets	Shared
Embedded Fax Images Sent	Driver Name
Embedded Fax Images Received	Port Name
Embedded Fax Large Sheets	Port Monitor Name
Fax Images Received	Comment
Fax Impressions	Computer Name
	Average Yellow Coverage Percentage
	Average Cyan Coverage Percentage
	Average Magenta Coverage Percentage
	Average Black Coverage Percentage

Table 1: Printer Data Communicated to XDDC Server

XDDC Site Information Sent to XDDC Server

The IP and subnet of the client are gathered, so the local subnet can be added to the scan settings. There is an option to delete or hide printer IP and MAC addresses if the data collection administrator configures this option.

Network Impact

Company network guidelines will typically enable or disable specific network ports on routers and/or servers. Your IT department will mostly be concerned with the ports used by XDDC for outgoing traffic. Disablement of specific ports may impact the functionality of XDDC. Refer to the table below for specific ports used by XDDC processes.

Port Number	Port Name	Comment
161 (typical)	SNMP	Network printer discovery, retrieve usage counters
135	RPC	Microsoft Windows® Remote Procedure Calls (RPC) for computer or direct printer discovery
80 (typical)	HTTP	XDDC server data transfer
443	HTTPS	Secure XDDC-to-XDDC Server data transfer
n/a	ICMP (ping)	Network Printer Discovery, Troubleshoot

Table 2: Xerox Device Data Collector Outbound Ports

XDDC does not require any incoming ports to be opened up on the installed machine. This means that the firewall on the machine should not require any modification.

Discovery

The discovery function allows XDDC to search for network printers on a customer's intranet. Printer discovery is a crucial part of the XDDC application because it is the main method to identify networked-connected devices and store them in the local database. It involves the generation and querying of network addresses (via SNMP) for printer type and general configuration information. Since this operation uses the network resources, you should consider what you want to detect and then configure the discovery to achieve this goal with a minimum of network contention.

Device Discovery Method Employed by Xerox Device Data Collector

After you have downloaded the XDDC Data Collector within a Web browser, it will be ready to discover network printers located on the same subnet as the host.

The Xerox Device Data Collector also allows the end-user to perform the discovery upon a different IP address range. For this purpose, the end-user can specify a range of addresses that will be searched.

Note: As a rule of thumb, each discovered printer might generate as much as 50 KB (maximum) of network message traffic including usage counters.

IP Sweep Operation

IP Sweep Discovery method is the preferred method of accurately discovering printers on a network. A packet is sent to every IP address in the user-defined address or address range list. The address list should be known and provided before running the discovery.

Specifically:

- A single packet is sent to each IP address contained within each subnet or address range defined within the current IP address for the current IP Sweep. In this packet, XDDC requests a value for a single SNMP-based RFC 1213 Object Identifier (OID).
- For each device that responds to the RFC 1213 OID, XDA will add the IP address of the response packet into its list of live IP addresses.
- XDDC then queries those devices with live IP addresses for two more OIDs: one RFC 1213 OID and one RFC 3805 OID. This enables XDDC to identify printing devices from non-printing devices. Both groups of devices are stored within the XDDC database, however, only printing devices are exposed via the XDDC UI.
  - For those printer devices that respond to the RFC 3805 OID query, XDDC flags them as printers.
  - For those devices that do not respond to the RFC 3805 OID query, XDDC then checks an RFC 1213 OID value against database values to determine if the device is in fact a known printer. This is necessary because some printing devices (i.e. printers using external print server boxes, older printers, etc.) do not support RFC 3805 – the Printer MIB.
    - The database contains RFC 1213 values for several known supported and unsupported printers.
- XDDC then queries all live IP addresses for three RFC 1213 OIDs and one RFC 2790 OID.
- For those devices identified as printers, XDDC queries three more RFC 2790 OIDs and four more RFC 3805 OIDs to obtain some basic attributes of the printer.
- Based upon the identity of each printing device, XDDC then queries the appropriate vendor-specific OID and an OID from the Printer MIB in order to obtain the printer's serial number.
- XDDC then queries 3 RFC 3805 OIDs in order to display the printing device's rated speed in pages per minute (PPM).
- Based upon the identity of each printing device, XDDC then queries the appropriate OID(s) to obtain the printing device's software/firmware level.

Network Impact

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

Accuracy

The IP Sweep method produces a controlled and orderly flow of data between the printers and the server, reducing network packet collisions that can introduce errors in the printer information.

Managing Discovery

The Discovery process can be managed by:

- Configuring the discovery IP address range.
- Updating the SNMP community name string according to network printer configuration.
- Monitoring the active status of the discovery progress.

Discovery Network Data Calculations

As mentioned earlier, each discovered printer could create as much as 50KB of discovery-based traffic. IP Sweep discovery sweeps all of the addresses in the ranges supplied.

Device Discovery Data Set Magnitudes on Typical Printers

The amount of data transferred during an operation, such as discovery, is a function of the device's capabilities. Measurements made on typical devices show the variability of these parameters. It is highly unlikely that any one network would be populated with only one device type. Instead, the typical case is a variety of devices that are dependent upon the particular needs of individuals or groups on the network. Here are three printer examples to demonstrate the variability in both the amount of collected data and the data transfer rate for typical devices.

Machine Model	Discovery
Xerox WorkCentre® Pro 245	49.2 KB
Xerox Phaser® 8560 DN	15.3 KB
HP LaserJet 4345 MFP	29.1 KB
Average	*31 KB*

Table 3: Xerox Device Data Collector Discovery Data Sizes

Assuming that XDDC will discover a thousand network devices on the network and each device discovery data set size is 31 KB, this set of devices is expected to retrieve the following printer-based discovery data per scan:

- 1 discovery x 1,000 printers x 31 KB/printer (Discovery data set size) is approximately 31 MB

Total XDDC Data Transfer Calculations

The next traffic calculation example shows totals for an exaggerated network data transfer size for a scan.

The calculation is inflated to show an above-the-limits traffic estimate. It assumes that every discovery requires 50 KB of traffic to complete (except non-printer discovery). This demonstrates the extreme upper limits for a network with 1,000 print devices being scanned.

Discovery Total

1,000 printers x 50 KBytes/printer = 50 MB

Discovery Traffic to Non-print Devices during a Sweep

65,534 IP Address x .2 KBytes/device = 12 MB

Overall (Exaggerated) Total

50 MB + 12 MB = 62 MB

Xerox Device Data Collector Server Integration

The Xerox Device Data Collector communicates directly to the XDDC server through the Internet, transferring associated printer and device information through a secure Web services transfer mechanism automatically (Refer to the Section 2: Security for more information on security). This device information is then used by XDDC server to update meter reads.

Device Information Export

XDDC exports device information to the XDDC server via Web services. The device information includes device identity information and usage information. The data packet size is roughly 35 KB per 100 devices.