

This document is intended for customers wishing to understand Printelligence™ deployment.
The full Deployment Guide is also available from your provider or the TechSource360 Portal.

Architecture

Hosted

Delivered as a hosted service, there are two components that make up Printelligence:

1. The Printelligence Client, which is deployed within your organization
2. The Printelligence Application Server (hosted by TechSource360 LLC)

The components communicate over the Internet. To ensure the highest level of security, all communication is encrypted using SSL (Secure Sockets Layer).

Printelligence Client

The Printelligence Client is deployed in your organization and is used to track printing activity. When a user prints, Printelligence tracks the printing and analyzes it, determining the number of pages, pages printed in color, page coverage, application, printer used, duplex selection, etc. The Printelligence client has been successfully deployed to over 5,000 organizations across the world.

Printelligence Application Server

The Printelligence Application Server is hosted by TechSource360. It is responsible for delivering the administration portal, as well as storing the meta-data about each print job. This architecture allows for the fast deployment of Printelligence into your organization.

Supported Operating Systems:

- Microsoft Server 2012
- Microsoft Windows 8 (32-bit and 64-bit)
- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows 2008 R2 Server (64-bit)
- Microsoft Windows 2008 Server (32-bit and 64-bit)
- Microsoft Windows Vista (32-bit and 64-bit)
- Microsoft Windows Server 2003 (32-bit and 64-bit)
- Microsoft Windows XP Professional (SP2 or later)
- Microsoft Windows 2000 Professional (SP4 or later)

**Printelligence had 5,000+ Installs
Worldwide**

**The print job NEVER
leaves your network**

No single point-of-failure

System Requirements

The following are the system requirements for both the print server and workstations:

Microsoft Windows .NET Framework (2.0 or later)

25 Mbytes Disk Space

Internet access over SSL (Secure Socket Layer)
*Name resolution between Printelligence-monitored
print servers and workstations*

Installs in Minutes

**One Client for All Installations
- Desktop, Server & Citrix**

Proxy Server

If your organization uses a proxy server, it is highly recommended the Printelligence service run with a Domain Service Account (DSA).

While Printelligence can run with the Network Service account, it rarely has sufficient authorization to navigate an organization's proxy server.

Using a Domain Service Account (DSA) with a proxy server creates many advantages:

The DSA can be set up to communicate through the proxy server to the hosted Printelligence Application Server

DSA communication can be restricted to a known IP address range.

The DSA can be set to a non-expiring password

Permissions can be restricted to only those needed to run Printelligence

The DSA can be centrally controlled

**Set up the Domain Service
Account before installing
Printelligence**

The account you select for Printelligence must have the ability to navigate through your organization's proxy server.

Some proxy servers restrict traffic for processes that are allowed to communicate to the Internet and to which IP addresses they can contact.

If your organization implements these server settings, you should allow the following processes: **prprn.exe** and **prprnct.exe** to communicate

to: <https://www.techsource360smart-print.com>

Account

Printelligence can be configured to use a Domain Service account or Network Service account.

Domain Service Account

If a Domain Service account is used for Printelligence, it must be able to communicate to the hosted Printelligence Application Server - SSL.

Be sure to set up the Domain Service Account prior to starting your Printelligence installation. Altering the

account information after installation is difficult and time-consuming, once you have installed Printelligence on all workstations in your organization.

Network Service Account

Printelligence can be installed to run under the Network Service account. The advantages of using the Network Service account are as follows:

Network Service is a built-in account defined on your workstations and servers.

The Network Service account has sufficient privileges to run Printelligence.

The disadvantage with using a Network Service Account is that information does not have permission to pass through the proxy server in most organizations. If your organization is contemplating moving to a proxy server in the future, you must then change the login credentials for every Printelligence client installed in the organization. Use the Local System Account for Windows 2000, as it does not have a Network Service Account.

Silent Deployment

Printelligence automatically detects new printers and users who have printed

Planning Checklist for Installation

Printelligence installation takes only minutes to complete. Before starting however, you will need some basic information about your organization's environment:

- 1. Registration Information:** The Company Name and Printelligence Registration Key
- 2. Proxy Information:** Confirm proxy information during installation, if required
- 3. Domain Service Account:** Domain Service Account information is required for organizations using dedicated service accounts to run Windows Services
- 4. Internet Access:** Printelligence requires Internet access to communicate with the hosted Printelligence Application Server. Internet access is tested during installation

Installation

Installation Package

The Printelligence installation package includes the following:

Standard MSI (Microsoft Windows Installer) package when deploying to the desktop.

An installation package that is the same for workstations and print servers.

No change to existing print drivers, print processors, port monitors

Always use a Domain Service account if one is available

Industry-standard installation procedures, including a completely automated uninstall procedure, should it be necessary.

Installation without the need to reboot the workstations or print servers.

The ability to be silently installed in many different ways, including SMS (Systems Management Server) or any other network-management technology that can use an MSI.

An application footprint which is only 25 Mbytes.

A custom print driver is not installed with Printelligence. Use the same print drivers you have already installed.

We do not change any of your existing print drivers, print processors, port monitors or any print-environment setting. You can be sure the print environment you have today will be the same environment after installing Printelligence.

When you add a new printer or driver, Printelligence automatically monitors it. You do not have to take any additional action for the printer or driver to be monitored by Printelligence.

We do not install a new print spooler. Continue to use the Windows print spooler.

Multiple Install

The recommended method to deploy the Printelligence application across your organization is to create an administrative installation point on a network server and run Setup from there.

An administrative install point consists of a folder containing an MSI file and several sub folders which contain the application files.

Note: Creating an administrative install point is sometimes known as “generating an MSI file”.

Security

Client Security

All data is encrypted during transmission using SSL (Secure Sockets Layer) with 2048-bit encryption. In addition, all locally cached data is encrypted.

The TechSource360 Data Center can only be accessed via biometric scans and has 24 x 7 security. In addition, intrusion detection systems are in place along with 24 x 7 monitoring. Finally, the hosting facility undergoes regular security scans to ensure that the highest level of security is maintained.

Application Security

Q. Do I need to open an incoming port in my Internet firewall?

No. At no time does the Printelligence Application Server “push” information to clients.

**Each customer’s data is stored separately
in a completely separate database**

Q. What coding practices are followed to ensure security?

TechSource360 regularly tests all components of code against buffer overflow, memory leaks and security vulnerabilities. We utilize automated tools as well as peer reviews to mitigate these risks.

No incoming port opened
2048-bit SSL Encryption

Data Center Security

Q. Do you utilize a third party to host the data center?

Yes. Microsoft Azure.

Please see <http://azure.microsoft.com/en-us/support/trust-center/security/> for information on data centers security.

Q. Is our data stored with other customers' data?

No. Each customer's data is stored separately in a completely separate database. All sharing capabilities between databases are disabled.

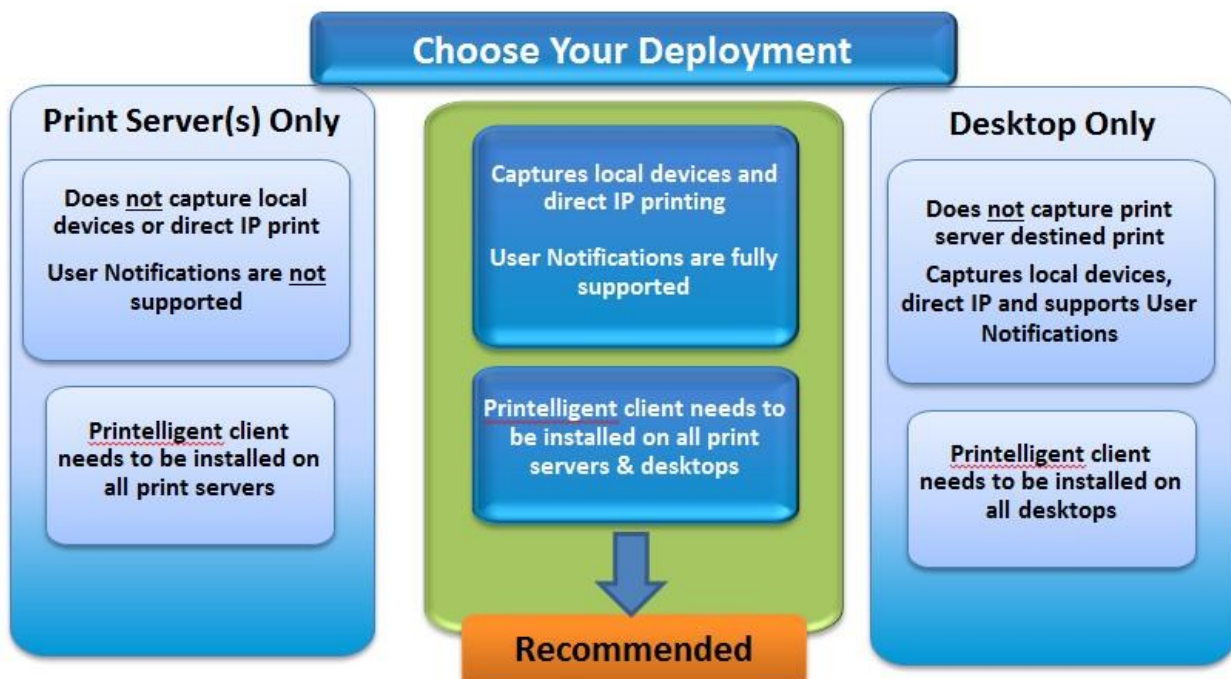
Q. Is there a Disaster Recovery plan in place?

Yes. A complete redundant site is provided with an uptime in less than 24 hours.

Q. What happens to my print environment if there is a loss of connectivity?

No impact during a down time, as Printelligence continues to operate and cache print information.

Understanding which deployment option best suits your organization is the best first step. Use the diagram below to help make that determination.



The full Deployment Guide is also available from your provider or the TechSource360 Portal.