Kodak

InSite
Systems

DMZ Network Configuration Guide
English

719-00098G-EN Rev A

Copyright

© Kodak, 2008. All rights reserved.

Kodak, Creo, Prinergy, Connect, Powerpack, Brisque, and eCentral are trademarks of Kodak.

Acrobat, Adobe, Distiller, Illustrator, PageMaker, Photoshop, and PostScript are trademarks of Adobe Systems Incorporated.

Apple, AppleShare, AppleTalk, iMac, ImageWriter, LaserWriter, Mac OS, Power Macintosh, and TrueType are registered trademarks of Apple Computer, Inc. Macintosh is a trademark of Apple Computer, Inc., registered in the U.S.A. and other countries.

Hexachrome, PANTONE, PANTONE Goe, PANTONE Hexachrome, and PANTONE MATCHING SYSTEM are the property of Pantone, Inc.

PEARL, PEARLdry, PEARLgold, PEARLhdp, and PEARLsetter are registered trademarks of Presstek, Inc.

XEROX is a trademark of XEROX CORPORATION.

http://graphics.kodak.com/

Internal 719-00098G-EN Rev A

Revised February 2008

Contents

Introduction 1

What Is a DMZ? 1
About InSite Software 1

InSite in a DMZ Network Configuration 2

InSite DMZ Network Connection Requirements 4
Client to InSite Server 6
InSite Server to eCentral Server 6
InSite Server to Workflow Server 7
InSite Server to Distribution Server 7
InSite Server to File Servers 7
InSite Server to Support Server 7
Storefront Licensed for Credit Card Transactions 7
LAN Computers to InSite Server 8
Upgrading a Prepress Portal or Storefront System in a DMZ Configuration 8
Before Upgrading Prepress Portal or Storefront Software 8
Upgrading Prepress Portal or Storefront Software 8
About Strong Passwords 9

Introduction

This guide provides an overview of the network requirements that must be met before Kodak InSite™ software is installed in a demilitarized zone (DMZ) network configuration. A service representative will perform the installation.

What Is a DMZ?

A demilitarized zone (DMZ) is a special network segment that has controlled access to the Internet and that may have controlled access to the corporate local area network (LAN). This segment is carefully exposed to the Internet (usually via ports 80 and 443), and computers in this segment do not have open access to computers on the LAN. Computers in the DMZ may have limited access to specific LAN computers via controlled DMZ openings.

About InSite Software

The InSite family of products uses the Internet to connect directly to different parts of the workflow.

- The Kodak InSite Creative Workflow system provides a collaborative workspace, where design teams can manage and share images, artwork, and other files (known as elements) that make up a publication.

  Note: If Creative Workflow is in a stand-alone configuration, the server will reside in the DMZ. If Creative Workflow is integrated with Prepress Portal, the server will reside on the LAN.

- The Kodak InSite Prepress Portal system allows printers and their customers to work with print jobs, making the proofing, correction, and approval processes simple and efficient.
- The Kodak InSite Storefront system allows print buyers to order print jobs over the Internet.
- The Kodak InSite Variable Data Print (VDP) system allows users to personalize items over the Internet.

  Note: If VDP is in a stand-alone configuration, the server will reside in the DMZ. If VDP is integrated with Prepress Portal, the server will reside on the LAN.

InSite in a DMZ Network Configuration

Installing an InSite server within a DMZ network configuration means that the InSite server is located in the DMZ, and the workflow server (Kodak Prinergy® or UNIX® software file server) and distribution server (if used) are located on the LAN.

The workflow server has unrestricted access to the InSite server, but the InSite server's access to the workflow server is restricted to specific ports:

- Prinergy server: ports 135, 445, 1521, 6378, and 61234 (used for Rules-Based Automation)
- Server Message Block (SMB)-compliant file server: port 445, or when transmitted using NetBIOS over TCP/IP via ports 137, 138, and 139

The InSite server also needs access to the following servers:

- E-mail relay server via port 25
- Kodak eCentral®, the Internet portal server for software updates via port 80
- Distribution server (if applicable) via ports 135, 445, and 6379
- Kodak NexStation™ server (if applicable) via port 445

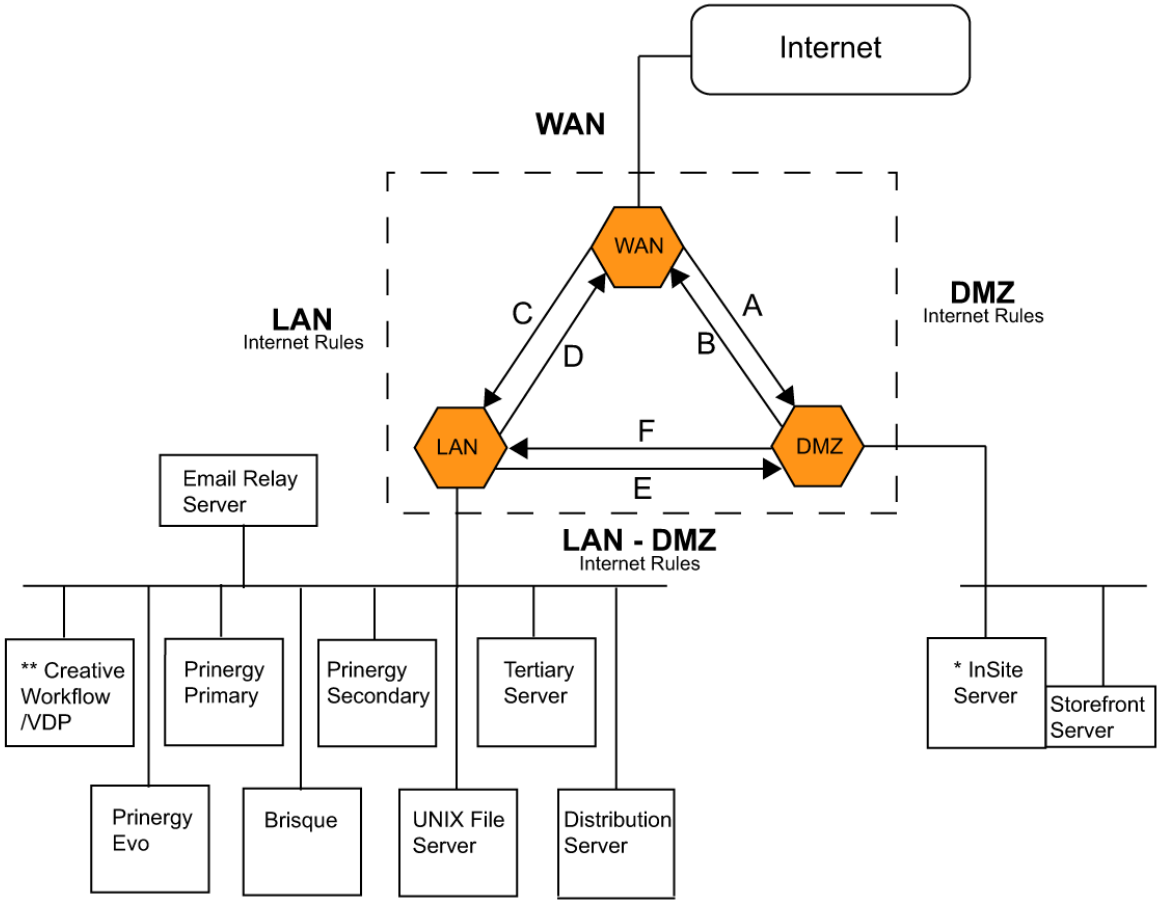
If applicable, the Prepress Portal or Storefront server needs access to the Creative Workflow or VDP server via ports 80 and 443.

If you have Storefront licensed for credit card transactions, you must:

- Install an SSL certificate on your Storefront server.
- Open port 443 on your Storefront server to two Cybersource servers.

Your service representative uses a configuration tool to install InSite software in a DMZ network configuration. This tool:

- Tests that the correct network ports are open between the InSite server and the workflow server
- Tests that the network has adequate available bandwidth—five megabytes per second or greater—between the InSite server and the file server
- Configures the InSite server
- Configures the Prinergy primary server, if applicable
- Configures the file servers where jobs reside
- Creates one non-domain account named InSiteService that is used by InSite, workflow servers, and all job servers, and uses a common password



Rule Set	Initiator to Recipient	Ports	Port Type
A	Internet to InSite server	Ports 80 and 443	TCP
B	InSite server to eCentral	Port 80	
	InSite server to Kodak support servers	Port 6503	
	Storefront server to Cybersource servers	Port 443	
C	Internet to LAN	No ports open	
D	LAN to Internet (optional)	Ports 80 and 443	
E	LAN to InSite server	All ports open	
F	InSite server to Prinergy primary server	Ports 135,445,1521,6378,61234	
	InSite server to Prinergy secondary/tertiary server	Port 445	
	InSite server to UNIX server with Samba (SMB over NetBIOS)	Ports 137-139	TCP and UDP
	InSite server to Windows server (native SMB)	Port 445	TCP
	InSite server to Creative Workflow/VDP server	Ports 80 and 443	
	Email relay server	Port 25	
	Distribution server	Ports 135,445,6379	

* InSite Server represents InSite Prepress Portal and/or InSite Storefront
** InSite Creative Workflow/Variable Data Print Server Integrated with InSite Prepress Portal/Storefront Server

Figure 1: DMZ Configuration Diagram

InSite DMZ Network Connection Requirements

The DMZ configuration must satisfy the following network connection requirements before InSite software can be installed or upgraded:

- InSite software must be installed on a separate server from the workflow server (Prinergy or other workflow system).
- The available bandwidth between the DMZ and LAN must be greater than five megabytes per second.
- The connection between the DMZ and LAN must be routed without packet modification. Network address translation (NAT) between the DMZ and LAN is not supported.
- If you are implementing InSite with the Kodak Brisque® workflow system:
  - For the Brisque 4.0 workflow system, you must have a second Network Interface Card (NIC) installed on the Brisque server and configured to the DMZ IP address.
  - For the Brisque 5.0 workflow system, Samba file server software must be installed on the Brisque server and configured to provide a NetBIOS export of the volumes to the DMZ.
- If the network uses a corporate proxy server, it must be configured to support ports 80 and 443.
- InSite must not be part of a domain if the workflow server on the LAN is part of a domain.
- The InSiteService account password must not contain certain special characters—see *About Strong Passwords* on page 9.
- Ports between the LAN and DMZ must not be filtered or blocked by a firewall or other security system.
- If you have Storefront software licensed for credit card transactions, you must have an SSL certificate installed on the Storefront server and you must have port 443 on the Storefront server open to two Cybersource servers.

The DMZ network configuration also requires the network connections shown in Figure 1.

Table 1: DMZ Network Connection Requirements

Connection	Source IP	Destination IP	Ports
Client to InSite server	Internet	InSite server (IIS IP address)	80—unencrypted access to InSite
	Internet	InSite server (IIS IP address)	443—encrypted access to InSite
	Internet	InSite server (Smart Review IP address)	443—encrypted access to Smart Review server
InSite server to the eCentral portal	InSite	ecentral.graphics.kodak.com	80—logs diagnostic and version information for support and automated software updates
InSite server to workflow server	InSite	Prinergy Connect™/ Powerpack™ primary or Prinergy Evo server	135—service control for a Remote Procedure Call (RPC)
	InSite	Brisque server (version 5.0 software with Samba)	137, 138, 139— TCP and UDP
	InSite	Prinergy Connect/Powerpack primary or Prinergy Evo server	445—Microsoft® Windows® 2000 file system
	InSite	Prinergy Connect/Powerpack primary server	1521—Oracle® database
	InSite	Prinergy Connect/Powerpack primary or Prinergy Evo server	6378—InSite services component (CSW Orb)
	InSite	Prinergy Connect/Powerpack primary server	61234—triggering Rules-Based Automation (RBA) actions
InSite server to distribution server	InSite	Distribution server	135—service control for RPC 445—Windows 2000 file system 6379—InSite services component
InSite server to file server	InSite	Windows file server	445—for any file server hosting InSite jobs or pages
	InSite	File server supporting SMB native	445—for any file server that supports SMB native (for example, UNIX with Samba version 3.x)
	InSite	File server supporting SMB over NetBIOS	137, 138, 139— TCP and UDP for file servers using SMB over NetBIOS (for example, UNIX with Samba version 2.x)

Connection	Source IP	Destination IP	Ports
InSite server to support server	InSite	CreoServiceport	6503—for remote service.
Storefront server to Cybersource	Storefront	ics2ws.ic3.com ics2wstest.ic3.com	443
Storefront server to NexStation server	Storefront	NexStation server	445
LAN computers to InSite server	All LAN IP addresses	InSite	All ports—computers on the LAN must be able to open a connection to the InSite server on any TCP/IP port.

Client to InSite Server

Client computers may be on the corporate LAN or on the Internet. In either case, they must be connected to the InSite server over TCP/IP ports 80 and 443.

If a corporate proxy server exists, any port can be used between the client computer and the proxy server, but the connection between the proxy server and InSite server must still be over ports 80 and 443.

LAN-based Clients to InSite Server

LAN-based InSite clients are typically staff users or InSite administrators. These clients connect to the InSite server over ports 80, 443, and 6377.

If you are using a corporate proxy server, disable the proxy server for access to the InSite server. The proxy server usually slows down access to InSite, and may also cause difficulties if it uses ports other than 80 and 443.

Internet-based Clients to InSite Server

InSite clients using the Internet are typically customer users. These clients need access to TCP/IP ports 80 and 443.

InSite Server to eCentral Server

The InSite server needs to periodically communicate with ecentral.graphics.kodak.com on TCP/IP port 80. The InSite server sends version and diagnostic information to eCentral to enhance support and to enable automatic InSite updates.

InSite Server to Workflow Server

InSite with Prinergy Connect or Prinergy Powerpack

InSite initiates connections on ports 135, 445, 1521, 6378, and 61234 to the Prinergy primary server. In response, the primary server opens connections on other ports back to the InSite server.

InSite for SMB-Compliant File Servers (for example, UNIX with Samba)

InSite initiates connections via SMB native on TCP port 445 or via SMB over NetBIOS on TCP and UDP ports 137, 138, and 139.

InSite Server to Distribution Server

When connecting to a distribution server, InSite opens a connection on ports 135, 445, and 6379. In response, the distribution server opens connections on other ports back to the InSite server.

InSite Server to File Servers

DMZ InSite Server to Windows File Server

When connecting to a Windows file server, InSite opens a single port (445) to the file server. In response, the file server opens connections on other ports back to the InSite server.

DMZ InSite Server to UNIX File Server

When connecting to a UNIX file server running Samba file server software version 3.x, InSite connects via SMB native on port 445. When connecting to a UNIX file server running Samba file server software version 2.x, InSite connects via SMB over NetBIOS and requires TCP and UDP ports 137-139. In response, the file server opens a variety of ports to the InSite server.

InSite Server to Support Server

For technical support, service representatives require port 6503 to be open on your firewall.

Storefront Licensed for Credit Card Transactions

With Storefront licensed for credit card transactions, you must have an SSL certificate installed on your Storefront server. You must also have port 443 open from the Storefront server to the following Cybersource servers:

- ics2.ic3.com
- ics2wstest.ic3.com

LAN Computers to InSite Server

See *InSite Server to Workflow Server* on page 7 and *InSite Server to File Servers* on page 7.

Upgrading a Prepress Portal or Storefront System in a DMZ Configuration

Once your Prepress Portal or Storefront software is in a DMZ configuration, you can update it easily through InSite Administration. During the update, the InSite Configuration Utility (ICU) will run to confirm your DMZ setup.

Before Upgrading Prepress Portal or Storefront Software

Before upgrading your system while it is installed in a DMZ configuration, you must:

- Ensure that all the hardware, software, and network components of your system are installed, configured, and operating correctly.
- Ensure that you are logged on to the InSite server as an administrator (with the user name Administrator or InSiteService).
- If you use Prinergy Powerpack or Prinergy Connect software, you must also:
  - ❒ Ensure that you know the password for the ARAXI account on the Prinergy primary server.
  - ❒ Ensure that you know the password for the InSiteService account.

    Note: Do not change the password for the InSiteService account while upgrading your InSite software. For assistance in changing the password, contact your service representative.
  - ❒ Ensure that all non-standard network mount points are disabled. To disable a mount point, if one exists:
    a. From the **Start** menu, select **Run**.
    b. Type cmd and click **OK**.
    c. Type net use /persistent:no
    d. Type net use * /d
    e. Type Y

Upgrading Prepress Portal or Storefront Software

Instructions for upgrading Prepress Portal or Storefront software are in the *InSite Prepress Portal and InSite Storefront Upgrade Guide*, available on the eCentral portal at https://ecentral.graphics.kodak.com.

Note: If you experience any errors during the upgrade, contact a service representative.

About Strong Passwords

It is recommended that you use strong passwords for your ARAXI and InSiteService accounts. A strong password must be at least eight characters long and contain three of the following classes: uppercase, lowercase, numbers, and non-alphanumeric “special characters” such as punctuation or symbols.

The password must not contain an:

& (ampersand)

‘ (apostrophe)

“ (quotation mark)

; (semicolon)

< (opening angle bracket)

> (closing angle bracket)

% (percent sign)

! (exclamation point)

Kodak

Eastman Kodak Company
343 State Street
Rochester, NY 14650 U.S.A.

© Kodak, 2008. All rights reserved.
TM: Kodak

To learn more about solutions from Kodak, visit http://graphics.kodak.com/.

Subject to technical change without notice.