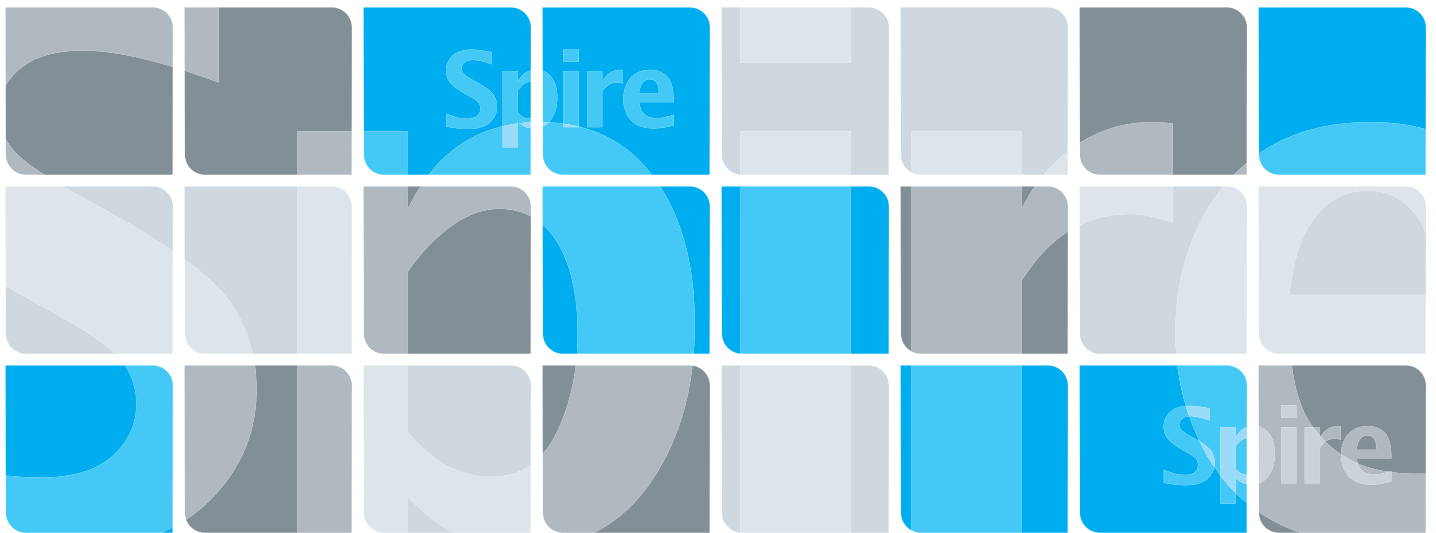




Xerox CX Print Server, Powered by Creo for the Xerox DocuColor 7000AP/8000AP Digital Presses



731-01276A-EN

Security White Paper
English

Copyright

© Creo, 2007. All rights reserved.

This document is also distributed in Adobe Systems Incorporated's PDF (Portable Document Format). You may reproduce the document from the PDF file for internal use. Copies produced from the PDF file must be reproduced in whole.

Trademarks

Creo is a trademark of Creo.

Adobe, Acrobat, Adobe Illustrator, Distiller, Photoshop, PostScript, and PageMaker are registered 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.

Kodak, Brisque, and InSite are trademarks of Kodak.

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

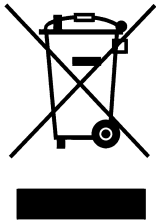
PEARL, PEARLsetter, PEARLhdp, PEARLdry, and PEARLgold are registered trademarks of Presstek, Inc.

XEROX is a trademark of XEROX CORPORATION.

FCC Compliance

Any Creo equipment referred to in this document complies with the requirements in part 15 of the FCC Rules for a Class A digital device. Operation of the Creo equipment in a residential area may cause unacceptable interference to radio and TV reception, requiring the operator to take whatever steps are necessary to correct the interference.

Product Recycling and Disposal



If you are managing the disposal of your Xerox product, please note that the product contains perchlorate, lead, mercury, and other materials whose disposal may be regulated due to environmental considerations in certain countries or states. The presence of perchlorate, lead and mercury is fully consistent with global regulations applicable at the time that the product was placed on the market.

Application of this symbol on your equipment is confirmation that you must dispose of this equipment with agreed national procedures.

In accordance with European legislation, end of life electrical and electronic equipment subject to disposal must be managed within agreed procedures.

Xerox operates a worldwide equipment take back and reuse/recycle program. Contact your Xerox sales representative (1-800-ASK-XEROX) to determine whether this Xerox product is part of the program. For more information about Xerox environmental programs visit <http://www.xerox.com/environment>.

For perchlorate disposal information, contact your local authorities. In the United States, you may also refer to the California Department of Toxic Substances Control (DTSC) or see <http://www.dtsc.ca.gov/hazardouswaste/perchlorate>.

This electronic information product complies with Standard SJ/T 11363 - 2006 of the Electronics Industry of the People's Republic of China.



Limitation of Liability

The product, software or services are being provided on an "as is" and "as available" basis. Except as may be stated specifically in your contract, Creo and its parents, subsidiaries, and affiliates expressly disclaim all warranties of any kind, whether express or implied, including, but not limited to, any implied warranties of merchantability, fitness for a particular purpose and non-infringement.

You understand and agree that, except as may be stated specifically in your contract, Creo and its parents, subsidiaries, and affiliates shall not be liable for any direct, indirect, incidental, special, consequential or exemplary damages, including but not limited to, damages for loss of profits, goodwill, use, data or other intangible losses (even if Creo has been advised of the possibility of such damages), resulting from: (i) the use or the inability to use the product or software; (ii) the cost of procurement of substitute goods and services resulting from any products, goods, data, software, information

or services purchased; (iii) unauthorized access to or alteration of your products, software or data; (iv) statements or conduct of any third party; (v) any other matter relating to the product, software, or services.

The text and drawings herein are for illustration and reference only. The specifications on which they are based are subject to change. Creo may, at any time and without notice, make changes to this document. Creo, for itself and on behalf of its parents, subsidiaries, and affiliates, assumes no liability for technical or editorial errors or omissions made herein, and shall not be liable for incidental, consequential, indirect, or special damages, including, without limitation, loss of use, loss or alteration of data, delays, or lost profits or savings arising from the use of this document.

www.pod-wf.com

Internal 731-01276A-EN

Revised October 2007

Contents

- Overview 1
- Network 2
 - Network Environments 2
 - Network Protocols 2
 - Network Types..... 2
 - Remote Access 2
 - Network Ports 3
 - Well known ports 3
 - * Part of IIS 4
 - Other ports 4
 - Physical Ports 5
 - CX8000AP platform 5
- Software Description 6
- Identification and Authorization 8
 - Users and User Rights 8
 - Potential Threats 8
 - What Can You Do? 8
- Access Control 9
 - Local DFE access..... 9
 - Potential Threats 9
 - What Can You Do? 9
 - About Remote Access 10
 - Microsoft Windows Sharing..... 10
 - RAS – Remote Access Server 11
 - Web Server Services 12
 - Remote Desktop Connection 12
 - FTP 12
 - Job Submission 13
 - Potential Threats 13
 - What Can You Do? 13
- Data Security..... 14
 - User Data (Job Data)..... 14
 - Ready to Print (RTP) Data 14

- Disk Wipe 14
- Format of Drives..... 14
- Potential Threats 15
- What Can You Do? 15
- Data Exchange 15
- Potential Threats 15
- What Can You Do? 15
- AntiVirus 15
- Potential Threats 16
- What Can You Do? 16
- System Integrity Protection 17
- Accountability (Audit Trails) 18

Overview

The purpose of this document is to describe the various access and security attributes of the Spire product line, specifically for the CX8000AP Server for the Xerox® DocuColor 7000AP/8000AP, and the potential threats to these attributes. Security relates to a collection of methods for access and integrity protection that a system provides in order to manage which users can access the system, and what features or data they can view or change.

Security threats are issues that relate to compromising the integrity of the system, hampering the integrity of job data, compromising secured feature access, or allowing unauthorized data access. The CX8000AP server relies mostly on the security of the Microsoft® Windows® operating system to provide these capabilities.

When describing security one has to address the following issues:

- Identification and authorization
- Access control (local and remote)
- Data Security
- System integrity
- Accountability (auditing)

This document is divided into two major parts:

- **Part 1:** A description of the product, network environment, software and hardware components.
- **Part 2:** A description of the identification and authorization, access control, data security, system integrity, and accountability (auditing) categories.

The Creo color server is a product line based on client/server architecture, printing to a variety of digital printers/copiers (output devices). The DFE (Digital Front End) receives input as a PDL (Printer Description Language) file and according to a “job ticket” (which is a set of parameters programmed by the client) produces an RTP (ready-to-print format) equivalent. The RTP format is then printed on the output device. The DFE controls the printer during the print process. The DFE server can concurrently handle multiple clients and processes.

The DFE is usually connected to the local area network (LAN), either in a Microsoft Windows (Workgroup or Domain), Novell®, or Macintosh® network environment.

Network

Network Environments

The DFE supports the following network environments:

- Microsoft Windows Network (Workgroup or Domain)
- Novell Network
- AppleTalk network

Network Protocols

The DFE supports the following network protocols:

- TCP/IP
- IPX/SPX
- NetBEUI
- AppleTalk

Network Types

- Ethernet

Remote Access

Remote access to the DFE can be established using a Microsoft Windows network client, a Novell client, a RAS client, a Web browser, a Microsoft Windows Remote Desktop Connection client or an FTP client.

For Certain remote applications, Creo's and external ones, which communicate via HTTP protocol on the server side, the DFE uses Web Server (IIS). IIS (Internet Information Services) is installed on the Server during the Operating system installation and is configured during Software installation. (See figure 1.)

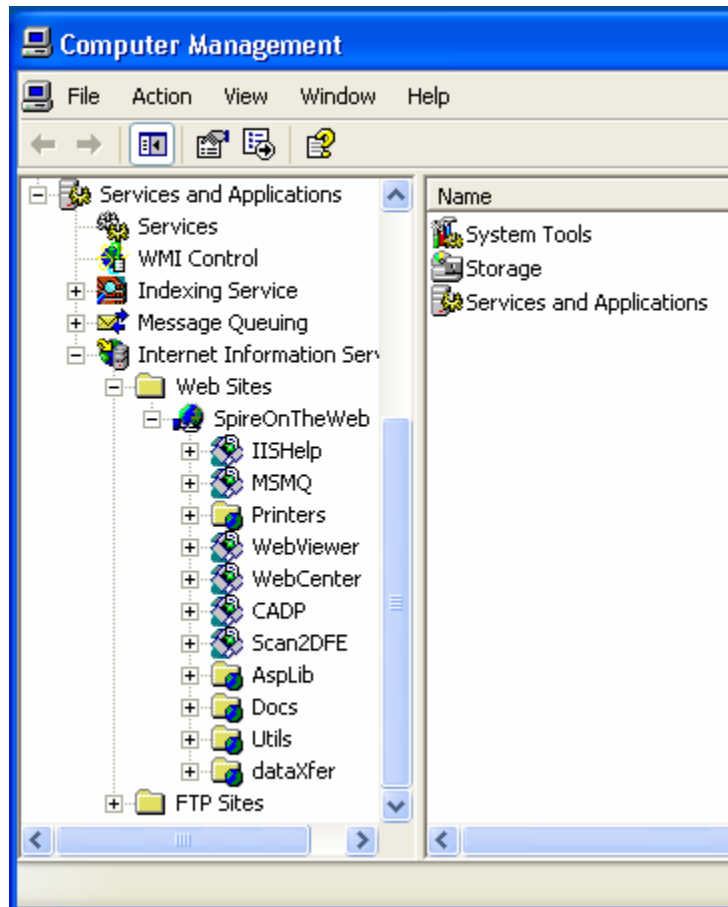


Figure1

Creo designed the DFE so remote access will be restricted to the required minimal operations and limit operations such as browse and write rights.

More information on remote access, see [About Remote Access](#) on page 8

Network Ports

Well known ports

Port	Application	Service	Protocol	Description
21	FTP server*	FTP	TCP	File Transfer Protocol

80	Web server*	HTTP	TCP	Connection to the <i>Spire</i> WebCenter/ WebViewer/Driver Extension,
135	RPC	epmap	TCP/UDP	DCE endpoint resolution
137	System	Netbios-ns	TCP/UDP	NETBIOS Name Service
138	System	Netbios-dgm	TCP/UDP	NETBIOS Datagram Service
139	System	Netbios-ssn	TCP/UDP	NETBIOS Session Service
427	System	svrloc	TCP/UDP	Server Location
515	tcpvcs	Printer	TCP/UDP	Spooler
3389	Remote Desktop Connection	svchost	TCP	Remote administration of the DFE

* Part of IIS

** More information on how the above applications use Port 80, see About Remote Access on page 10

Other ports

Ports 1025-1032 are ports that are not well defined or known. In general, some of these ports are used by the operating system for spooling purposes and are dynamic. The Microsoft Windows spooling process creates sockets using these ports, and they change according to the print activity of the DFE.

Physical Ports

CX8000AP platform

- Ethernet adapter #1– Connect to network
- Ethernet adapter – Not in use
- USB Port #1 – Connected to Mouse
- USB Port #2 – Connected to the color calibration device
- USB Port #3 (Front USB)– Not in use.

Software Description

The CX8000AP is based on the Microsoft Windows XP Professional (Service Pack 2) operating system.

Spire added-value software consists mainly of Creo developed software modules and a number of 3rd party drivers and utilities.

The following are services that are supported by the Spire platform:

- FTP Server
- Web Server
- RAS – Remote Access Service
- Macintosh print/file Access (3rd party service – ExtremeZ)
- LPR/LPD Printing (*UNIX*)
- Microsoft Windows file sharing
- Remote Desktop Connection

The following are the remote applications that can request information from the server:

- Web Viewer- Web HTML page, that uses Port 80 to get DFE information regarding Jobs queues, machine statuses etc.
- Web Center- Web HTML pages, that uses Port 80.
- Driver extension- GUI application, uses Port 80 for Online mode and get DFE parameters.
- FreeFlow applications- Uses Port 80, to query information from the DFE.

The following are 3rd party applications that run on the server:

- Adobe CPSI
- Java Virtual Machine
- Novell Network Client (optional)
- Adobe Acrobat
- Various device drivers (network board drivers, and so forth)
- 3rd party anti-virus applications (pending on product configuration and self purchase of anti-virus application)

The Spire platform DOES NOT include the following services:

- Rlogin / Telnet
- Email/POP3
- SMTP
- IMAP4 (143)

Identification and Authorization

The DFE uses the Microsoft Windows identification procedure for remote job submitters, connecting a Microsoft Windows security recognized user with a specific job. Access to the DFE does not apply any identification procedure, and there is no user differentiation.

Users and User Rights

Currently there is only one type of user role on the DFE itself, and that is the DFE administrator. An administrator has access to 100% of DFE functionality along with the user rights of a Microsoft Windows XP administrator. There is no change to any users or groups in the local security database. Other users belonging to different Microsoft Windows XP user groups cannot operate the DFE.

Potential Threats

When using the DFE locally, if the DFE is unattended, unauthorized personnel can use the DFE without any security mechanism blocking them. Both feature access and data security may be compromised. The DFE is not pre-configured with an auto lock mechanism.

What Can You Do?

Customers should not openly give out the username and password for the DFE, and should either secure the physical location of an unattended server, or lock the system when leaving the DFE unattended.

In addition, we suggest considering physical locks for the CD-ROM drive that are available for purchase on the open market.

Customers can also purchase a smart card system, which enables access only to specific personnel using personalized physical media.

Access Control

Local DFE access

- The DFE requires an administrator login to the Microsoft Windows operating system in order to operate the system.
- The administrator user referred to is the default local administrator defined by Microsoft Windows XP, which is member of the local administrators group.
- All DFE functionality is available to this user.
- Access to operating system functions is as defined by the built-in user group – Administrators.

Potential Threats

Usage of local peripherals can be used to load software that may compromise the security and integrity of the DFE. This can be done without the knowledge of the user. For example, an auto run CD can launch a virus-infected application, or running any executable that is infected with a “smart” virus can cause damage to the integrity of the DFE system, or the any existing job.

For information about unauthorized data access see [Potential Threats](#) on page 8.

What Can You Do?

Customers should run virus scans on all media for devices attached to the DFE (such as the DVD-ROM drive).

In addition, we recommend that you disable the guest account for local access.

About Remote Access

Microsoft Windows Sharing

Shared Volumes

Remote users are required to be logged in when a remote sharing session is requested.

There are two folders that are open to sharing by default:

- a. Utilities folder (client download of system utility applications)
- b. Shared Volume (mainly used for client upload of high-resolution files)

These volumes are accessible from Microsoft Windows and Macintosh clients. The permissions are Read/Write/Change to everyone. The DFE administrator can create higher levels of security for these volumes without hampering DFE operation.

Potential Threats

Many viruses enter the system through shared volumes using a guest account.

What Can You Do?

- Change the security permissions of the shared volumes to something other than the default guest account.
- Change the security permission of the utilities folder to read only.
- Disable the guest account entirely.
- Remove the “everyone” account from shared folder permissions.

Note: When reinstalling the Microsoft Windows operating system, these operations will need to be repeated.

RAS – Remote Access Server

Used mainly for diagnostic purposes. The customer has to purchase a modem separately, connect a phone line, and give this phone number to the support team. This connection can be encrypted and authenticated as provided by Microsoft Windows XP.

The RAS service runs by default but can be stopped by the administrator without affecting normal DFE operation.

Potential Threats

The remote access service can be a problem since it opens the DFE to users outside of the company LAN.

What Can You Do?

- Define which specific users can dial in, and verify that a password is required to login.
- Connect the modem only before usage, and disconnect immediately afterwards.
- Do not give out the phone number for the modem.
- Verify that the service requires Microsoft authentication and enable the “Require data encryption” check box in the RAS properties page.

Web Server Services

The web server service runs by default, and allows viewing of the DFE queues, storage folder, and alerts..

Potential Threats

The Web Server service can be a problem since it opens the DFE to users outside of the company LAN.

What Can You Do?

The DFE administrator can stop the web service without affecting DFE operation. If this service is disabled, Remote client applications and/or Web client access to the DFE features will be disabled.

Remote Desktop Connection

The DFE supports the Microsoft Windows XP Remote Desktop Connection utility for remote control of the DFE for administrative purposes. This connection is single user and password protected.

The DFE administrator can disable or enable this service.

FTP

The File Transfer Protocol (FTP) server service runs by default. Anonymous users are allowed access. The DFE administrator can stop the FTP service without affecting DFE operation.

Job Submission

TCP/IP Printing (LPR/LPD)

Netbios Printing

PAP/AppleTalk printing

Potential Threats

In general, any additional network service as listed above adds another remote access point to the DFE that can potentially allow an intruder to either damage the integrity of the system, or extract classified data. The DFE is not installed with any intruder detection system, or a firewall.

What Can You Do?

Customers should stop/disable any unnecessary network service (RAS, FTP, HTTP) or protocols (NetBEUI, AppleTalk, IPX\SPX), and then start these services or protocols only when needed.

Data Security

Data security refers to methods of protecting client data on the wire or on the computer system itself. There are several facets of data security, some relate to how to verify which users have access only to their own data, other facets relate to protecting client data overall.

User Data (Job Data)

User data is protected as any other data on the DFE, by limiting local and remote access to the DFE. The owner of job data is the administrator. There is no discrimination between specific clients. Any user who approaches the DFE can view all the current jobs.

Ready to Print (RTP) Data

Every job that has been successfully processed has RTP data associated with it. This data is saved on fast image disks that are defined as a *Microsoft Windows* stripe set. The file system format for the image disks is a proprietary *Creo* file system format. This file format is not accessible to the general public.

Disk Wipe

Normally, when you delete a file, the file's dictionary entry is removed but data still remains on the disk. The Disk Wipe utility clears previously deleted files. Disk Wipe eliminates the contents of deleted files by scanning all of the empty sectors on the *Spire* disk and replacing them with zeros. Nonempty sectors are left untouched. Disk Wipe eliminates the option to restore deleted information from the *Spire* disks.

Format of Drives

Creo supplies a special utility called: "Format Image Drives" that erases the database tables and the proprietary RTP files stored on the "stripe disk array". During normal production work, it is necessary to run this utility and clean these non-system disks. This routine affects the proprietary DISKS ONLY.

If a new PostScript file is ripped and new data is written to this "cleaned" partition – this will create a NEW proprietary database table that will make

it impossible to recreate the previous database and restore the old proprietary file system data.

Potential Threats

As described previously, the local DFE access is open to everyone if it remains unattended. Unauthorized personnel can view/extract classified jobs if no operator secures the DFE.

What Can You Do?

The operator of the DFE should lock the system when leaving the DFE unattended. If the SafeDisk option is installed the disks should be locked in a safe when the operator is not present.

Data Exchange

Data exchange refers to the exchange of data between secured computers. The DFE is not configured with any special tools to encrypt data on the wire. Microsoft Windows 2000/XP have such capabilities, which are not enabled by default.

Potential Threats

Job data being transferred on the wire is not encrypted and as a result, unauthorized personnel with the know how can collect live data sent to the DFE.

What Can You Do?

Define data encryption (IPSEC) on both ends of the transfer segment. This may not be possible in all network configurations and client operating system types.

AntiVirus

Pending on product configuration and purchase of a 3rd party anti-virus application, the DFE can run virus checks on incoming files. Creo recommends using the **McAfeeVirusScan** software and provides a Microsoft Windows XP installation and configuration guide for this

application. Always stay current with your virus definitions supplied by the antivirus product you choose.

Potential Threats

Viruses can affect system integrity and data integrity, and can penetrate the system either from an attached device such as a DVD-ROM drive. Viruses can compromise the system and data integrity.

What Can You Do?

Install an antivirus application on the Spire DFE. The most secure type of antivirus application is the “on-access” type. The DFE will be validated while running a virus scan application from a leading vendor of such applications. Customers will need to purchase this software separately from the antivirus vendor, install and configure it as defined in documentation supplied by the Spire team.

System Integrity Protection

System integrity protection refers to protecting the system from malicious attacks or unintentional breaks by the system users.

Resources	Description	Owner	Protected
Application files	exe, dll, and other files which make up the DFE application	Administrator	Not by default
Client data files	PDL, RTP, and other files which make up the client job	Administrator	Not by default, this should not be changed
Registry entries		Administrator	Not by default
Processes		Administrator	Not by default
Printers	Administrator can print, manage the printer, and manage documents	Administrator	Not by default

Accountability (Audit Trails)

Microsoft Windows XP provides security auditing capabilities as the DFE factory settings do not audit by default. Specific DFE events are not recorded in the system audit log.

Spire Spire Spire Spire Spire Spire Spire