XEROX®

Version 50.xx, September 2005

701P25380

Xerox Document Services Platform Series
Common Controller

Security Guide

Prepared by:
Xerox Corporation
Global Knowledge and Language Services
800 Philips Road Bldg. 845-17S
Webster, New York 14580
USA

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

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).” SWOP® is a registered trademark of SWOP, Inc.

DocuSP includes use of GNU source and object code, which is subject to the terms of the GNU GPL. Please review the GNU GPL terms and conditions to understand the restrictions under this license. For more information on GNU, please go to http://www.gnu.org/licenses/gpl.txt.

As a requirement of the GNU GPL terms and conditions, source code of the above programs list can be found on the www.xerox.com website for the applicable DocuSP-based product or can be ordered from Xerox.

This information is provided for information purposes only. Xerox Corporation makes no claims; promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this document and disclaims all liability concerning the information and/or the consequences of acting on any such information. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

Product Recycling and Disposal

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

European Union

Some equipment may be used in both a domestic/household and a professional/business application.

Domestic/Household Environment

Application of this symbol on your equipment is confirmation that you should not dispose of the equipment in the normal household waste stream.

In accordance with European legislation end of life electrical and electronic equipment subject to disposal must be segregated from household waste.

Private households within EU Member States may return used electrical and electronic equipment to designated collection facilities free of charge. Please contact your local disposal authority for information.

In some Member States when you purchase new equipment your local retailer may be required to take back your old equipment free of charge. Please ask your retailer for information.

Professional/Business Environment

Application of this symbol on your equipment is confirmation that you must dispose of this equipment in compliance 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.

Prior to disposal please contact your local dealer or Xerox representative for end of life take back information.

Table of Contents

Introduction

The Security Guide provides the information needed to perform system administration tasks for maintaining the Xerox Document Services Platform (DocuSP) for printing systems.

About this guide

This guide is intended for network and system administrators responsible for setting up and maintaining Xerox printers with DocuSP software. System administrators should have an understanding of the Sun workstation, a familiarity with Solaris, and with basic UNIX commands. This includes the use of text editors such as vi or textedit and the ability to maneuver within the Solaris environment. To enable them to setup a customer site, system administrators are expected to have a working knowledge of Local Area Networks (LANs), communication protocols, and the applicable client platforms.

Contents

In general, this document covers information about the DocuSP that is not covered in the Online Help or other available guides.

The following list describes the contents of this guide:

- Gateway and Network Configuration
- Backup and Restore
- Security and Network Setup
- Printing
- Finishing
- Fonts
- MICR
- Tape Client
- Accounting and Billing
- Troubleshooting
- Hints and Tips

Conventions

This guide includes the following conventions:

- Angle brackets - Variable information that is displayed on your screen is enclosed within angle brackets; for example, “Unable to copy <filename>.”
- Square brackets - Names of options you select are shown in square brackets; for example, [OK] and [Cancel].
- Notes are hints that help you perform a task or understand the text. Notes are found in the following format:

NOTE: *This is an example of a note.*

Customer support

To place a customer service call, dial the direct TTY number for assistance. The number is 1-800-735-2988.

For additional assistance, dial the following numbers:

- Service and software support: 1-800-821-2797
- Xerox documentation and software services: 1-800-327-9753

Security

This section describes the DocuSP system-supplied security profiles. It outlines the characteristics of each profile and indicates how each can be customized to create user- defined profiles. The enhanced security features in DocuSP protect the system against unauthorized access and modification.

This section also addresses the options available to the administrator in setting up and managing user accounts.

Finally this section offers general guidelines to security-related procedures that can be implemented to improve the security of the DocuSP controller and the Solaris OS.

System supplied security profiles

The four system-supplied profiles are: none, low, medium, and high. The following table describes the characteristics of each security level and the configurable settings that restrict access to various devices and operating system services.The default setting is "Low."

Table 2-1 Security Profiles

Profile	Characteristics	User	Compatibility	Comments
None	Default Solaris and system security. All ports are open. Walkup users can reprint anything. Full workspace menu is available. Auto logon is enabled.	Physically closed environments.	Close to DocuSP 2.1 and 3.1. Similar to DocuSP 3.X "Medium".	Anonymous FTP is read-only and restricted. The Solaris desktop is removed from all settings except none.
Low	FTP is enabled. Telnet, rsh is disabled. NFS client is enabled. AutoFS is enabled. Walkup users can reprint from "Saved Jobs" and CD-ROM. Terminal window is password protected. Auto-login is enabled.	First choice setting for most environments.	Similar to DocuSP 3.x "High". Supports DigiPath workflow.	Anonymous FTP is ready-only and restricted. To enable telnet, go to [Setup], [FTP/ Remote Diagnostics]. "Low" is the default setting.

Profile	Characteristics	User	Compatibility	Comments
Medium	FTP is enabled. telnet, rsh is disabled. NFS client is disabled. AutoFS is disabled, e.g./ net/<hostname>and home/<username> are not automatically mounted. NFS server is filtered via RPC tab. Walkup user can reprint from CD_ROM. Terminal window is password protected.	Environments requiring high security but with a need to integrate DigiPath.	Supports DigiPath workflow.	Anonymous FTP is ready-only and restricted. To enable telnet, go to [Setup], [FTP/ Remote Diagnostics].
High	FTP is disabled. telnet, rsh is disabled. NFS client is disabled. AutoFS is disabled, e.g./ net/<hostname>and home/<username> are not automatically mounted. NFS server is disabled on customer network. Walkup users cannot reprint anything. Terminal window is password protected. Auto login is disabled (login is always required from GUI).	For government market.	Does not support DigiPath workflow.	File FTP is disabled. File transfer can be done via Secure FTP. For CFA support, that is FTP upload of outload, go to [Setup], [FTP/ Remote Diagnostics] menu.
Custom	Any profile can be edited to adjust to user needs			

NOTE: *Regardless of the security profile, anonymous FTP is Read-only with restricted access to /export/home/ftphome only.*

Enable and disable services

The following tables provide a list of the services that can be enabled and disabled from the DocuSP “Setup > Security Profiles” menu options.

Table 2-2 “System” tab

System Service	Description
Allow_host.equiv_plus	Background: The /etc/hosts.equiv and /.rhosts files provide the remote authentication database for rlogin, rsh, rcp, and rexec. The files specify remote hosts and users that are considered to be trusted. Trusted users are allowed to access the local system without supplying a password. These files can be removed or modified to enhance security. DocuSP is provided with both of these files deleted entirely. The setting All_host.equiv_plus is set to disabled, then anytime that security settings are applied, the + will be removed from host.equiv. IMPORTANT NOTE: Removing the + from the hosts.equiv file will prevent the use of the Xerox command line client print from remote clients. An alternative would be to remove the + and add the name of each trusted host that requires this functionality. Leaving the + will allow a user from any remote host to access the system with the same username
BSM	Enable or disable the Basic Security Module (BSM) on Solaris
Executable Stacks	Some security exploits take advantage of the Solaris OE kernel executable system stack to attack the system. Some of these exploits can be avoided by making the system stack non-executable. The following lines are added to /etc/system/fP file:set noexec_user_stack=1set noexec_user_stack_log=1
Remote CDE Logins	Deny all remote access (direct/broadcast) to the X server running on DocuSP by installing an appropriate /etc/dt/config/Xaccess file.
Router	Disable router mode by creating an empty the empty file: /etc/notrouter.
Secure Sendmail	Force sendmail to only handle outgoing mail. No incoming mail will be handled by sendmail.
Security Warning Banners	Enable security warning banners to be displayed when a user logins or telnets into the DocuSP server.

Table 2-3 “INIT” tab RC2 section

RC2 Service	Description
S40LLC2	Class II logical link control driver
S47ASPPP	Asynchronous PPP link manager. This service is re-enabled via enable-remote-diagnostics command.
S70UUCP	UUCP server
S71LDAP.CLIENT	LDAP daemon to cache server and client information for NIS lookups.
S72AUTOINSTALL	Script executed during stub JumpStart or AUTOINSTALL JumpStart
S72SLPD	Service Location Protocol daemon

RC2 Service	Description
S73cachefs.daemon	Starts cachefs file systems
S73NFS.CLIENT	NFS client service. Disables the statd service which is only required if your system is an NFS server or a client.
S74AUTOFS	The automountd service is only required if your system uses NFS to automatically mount file systems. Stopping the autofs subsystem will kill the running automountd daemon and unmount any autofs file systems currently mounted.
S80SPC	SunSoft Print Client daemon
S88SENDMAIL	The sendmail daemon is used to send mail over the internet. Sendmail has some security issues that are addressed by more recent Solaris patches than those currently loaded with the DocuSP software. If sendmail is not required, it can be disabled with the following procedure.
S90WBEM	CIM Boot Manager. Disables WBEM clients from accessing DocuSP server.

Table 2-4 "INIT" tab RC3 section

RC3 Service	Description
S15NFS.SERVER	NFS Server. Disable ability to export DocuSP Server file systems. This service is enabled if DigiPath and Decomposition Services (NetAgent) are enabled.
S17BWNFS.DAEMON	Secure mounted file systems. There are two shared file systems that are exported by DocuSP. The two directories are only required for anyone with XDOD version 3.0 or below. With the release of DigiPath Version 1.0, it is not necessary to export these file systems.
S76SNMPDX	Sun Solstice Enterprise Master Agent. Solaris SNMP services are disabled. This does not prevent DocuSP SNMP services from operating.
S77DMI	Sun Solstice Enterprise DMI Service Provider
S80MIPAGENT	Mobile IP agent

Table 2-5 "INETD" tab

INETD Service		Description
amiserv	RPC Smart Card Interface	Not used by DocuSP
cachefs	Cached File System server	Not used by DocuSP

INETD Service		**Description**
chargen	Character Generator Protocol server	Sends revolving pattern of ASCII characters. Sometimes used in packet debugging and can be used for denial of service attacks. Not used by DocuSP
comsat	Biff server	comsat is the server process which listens for reports of incoming mail and notifies users who have requested to be told when mail arrives. Not used by DocuSP
daytime	Daytime Protocol server	Displays the date and time. Used primarily for testing. Not used by DocuSP
discard	Discard Protocol server	Discards everything sent to it .Used primarily for testing. Not used by DocuSP
dtspc	CDE sub-process Control Service	CDE sub-process Control Service (dtspcd) is a network daemon that accepts requests from clients to execute commands and launch applications remotely. Not used by DocuSP
echo	Echo Protocol server	Echoes back any character sent to it. Sometimes used in packet debugging and can be used for denial of service attacks. Not used by DocuSP
exec	Remote execution server	Used by rexec(1) command. Potentially dangerous— passwords and subsequent session is clear text (not encrypted). Not used by DocuSP.
finger	Remote user information server	Display information about local and remote users. Gives away user information. Not used by DocuSP
fs	X font server	Used by CDE to dynamically render fonts. DocuSP uses bit-map fonts.
ftp	File transfer protocol server	This can be used to enable/disable the ftp server. This does not affect using the ftp client from the DocuSP server to another host running an FTP server. Note that DigiPath requires this service to be enabled.
kcms_server	KCMS library service daemon	Allows the KCMS library to access profiles on remote machines. Not used by DocuSP.
login	Remote login server	Used by the rlogin(1) command. Potentially dangerous— uses ~/.rhosts file for authentication; passwords and subsequent session is clear text (not encrypted).
name	DARPA trivial name server	in.tnamed is a server that supports the DARPA Name Server Protoco. Seldom used anymore. Not used by DocuSP

INETD Service		Description
rpc.cmsd	Calendar manager service daemon	rpc.cmsd is a small database manager for appointment and resource-scheduling data. Its primary client is Calendar Manager. Not used by DocuSP
rpc.rusersd	network username server	Gives intruder information about accounts. Not used by DocuSP.
rpc.rwalld	Network rwall server	Server that handles rwall(1M) command requests. Can be used for spoofing attacks. Not used by DocuSP.
rpc.sprayd	Spray server	Records the packets sent by the spray(1M) command. Can be used in denial of service attacks. Not used by DocuSP
rcp.ttdbserverd	RPC-based ToolTalk database server	The RPC-based tooltalk database server is required for CDE action commands. In particular, the CDE front panel has various menu items that rely on CDE actions. Late in the CP3.1 release, the Server UI team disabled the front panel. With the panel disabled, the need for the tooltalk database server no longer exists
rquotad	Remote quota server	Used by the quota (1M) command to display user quotas for remote file systems. Not used by DocuSP
sadmind	Distributed system administration daemon	Used by Solstice AdminSuite applications to perform distributed system administration. Not used by DocuSP.
shell	Remote execution server	Used by rsh(1) and rcp(1) commands.. The print command line client relies on the remote shell internet service being enabled since it uses the rcp(1) command to transfer files onto the DocuSP server. However, this service represents a security risk. Not used by DocuSP
talk	Server for talk program	The talk utility is a two-way, screen oriented communication program. Not used by DocuSP.
telnet	TELNET protocol server	This can be used to enable/disable the telnet server This does not affect using the telnet client from the DocuSP server to another host running an TELNET server
time	Time Protocol server	Outdated time service. Seldom used anymore. Not used by DocuSP
uucp	UUCP server	UNIX to UNIX system copy over networks. UUCP is not securely set up and can be exploited in many ways. Not used by DocuSP

User level changes

The following user-level changes are made:

- all users for at, cron, and batch are disallowed
- nuucp account is disabled
- listen account is disabled
- password entry locked for bin, sys, adm, uucp, nobody, noaccess, nobody4, and anonymous

Solaris file permissions

Secure File Permission options can be enabled or disabled through the DocuSP interface. Fix-modes include:

- fixmodes-xerox: fix file permissions for all packages to make them more secure. Available under the System tab under the “Secure File Permissions” drop-down menu.
- fixmodes-solaris: fix file permissions only for Solaris packages to make them more secure. Available under the System tab under the “Secure File Permissions” drop-down menu.

The fix-modes utility (from the Solaris Security Toolkit) adjusts group and world write permissions. It is run with the '-s' option to secure file permissions for Solaris files that were created at install time only. Customer-generated files are not affected.

NOTE: *When this command is run, a file called /var/sadm/install/content.mods is left. Do not delete this file. It contains valuable information needed by fix modes to revert the changes to the system file permissions if the security setting is changed back to medium.*

Disabling secure name service databases

The following databases are **disabled** when security is invoked:

- passwd(4)
- group(4)
- exec_attr(4)
- prof_attr(4)
- ser_attr(4)

Multicast routing disabled

Multicast is used to send data to many systems at the same time while using one address.

OS and host information hidden

The ftp, telnet and sendmail banners are set to null so that users in cannot see the hostname and OS level.

NOTE: *All of these services are prohibited with a 'high' security setting, but if they are re-enabled manually the hostname information will remain hidden.*

Sendmail daemon secured

Sendmail is forced to perform only outgoing mail. No incoming mail will be accepted.

Network parameters secured

Sun's nddconfig security tool is run. For additional information, view Sun's document, Solaris Operating Environment Network Settings for Security, at

http://www.sun.com/solutions/ blueprints/1200/network-updt1.pdf.

Executable stacks disabled

The system stack is made non-executable. This is done so security exploitation programs cannot take advantage of the Solaris OE kernel executable system stack and thereby attack the system.

NFS port monitor restricted

The NFS server normally accepts requests from any port number. The NFS Server is altered to process only those requests from privileged ports.   Note that with the high security setting, NFS is disabled; however if the service is re-enabled manually, the port restriction will still apply.

Remote CDE login disabled

The Remote CDE login is disabled.

DocuSP router capabilities disabled

The DocuSP router capabilities is disabled (empty/etc/notrouter file created).

Security warning banners

Security warning banners are displayed when a user logs in or telnets into the DocuSP server. This message explains that only authorized users should be using the system and that any others face the possibility of being monitored by law enforcement officials.

NOTE: *DRW (DocuSP Remote Workflow) is not impacted by security settings.*

Disabling LP anonymous printing

You can choose to disable anonymous printing on all existing LP printer queues that are associated with the DocuSP virtual printers. When anonymous LP is disabled, only systems that have their IP address in the DocuSP controller /etc/hosts table are authorized to submit LP requests. Answer “y” for yes to disable this printing option.

Remote shell internet service

If you are using the legacy Xerox print command line client (the software is not distributed with this release), you will need to use the remote shell internet service to transfer files to the DocuSP controller. However, if you are not using the Xerox print command line client, it is strongly recommended that the remote shell internet service is disabled. When these three questions are answered, all remaining aspects of the "High" security setting are implemented.

enable-ftp and disable-ftp

These options allow for enabling and disabling FTP alone. You must have FTP enabled when using a Continuous Feed system, or FreeFlow Production Print and NetAgent.

FTP is also required for the Call for Assistance (CFA) feature. This uses FTP to push IOT logs and a DocuSP outload back to the DocuSP controller.

NOTE: *Temporarily enable FTP through the DocuSP Setup > FTP/Remote Diagnostics menu option.*

Creating user-defined profiles

To create a customized profile, the administrator copies any security profile and edits the profile according to the needs of the customer environment. This new user profile can be selected, edited, set as current, and set as default.

Setting the current and default profiles

The administrator can select any profile and set it as the Current Profile. This Current Profile persists throughout reboot and software upgrades until it is changed by the administrator. Similarly, the administrator can select a Default Profile that remains in effect until it is changed by the administrator.

Account management

Any interaction between a user and the DocuSP is associated with a user account and is done via a logon session, which is the basis for granting access.

DocuSP user accounts are defined either locally at the device or remotely at a trusted network location like ADS. The local user account is composed of a logon user name and an assigned user group. A user account can be a member of one and only user group. It is the user group that is associated with a security profile that defines the privileges of the group.

Default user accounts are provided to allow easy transition from DocuSP versions 3.8 and earlier.

Local users and groups

Local user accounts are constructed based on the Solaris model, with its limitations and restrictions, using the [User & Group Management] selection on the DocuSP interface.

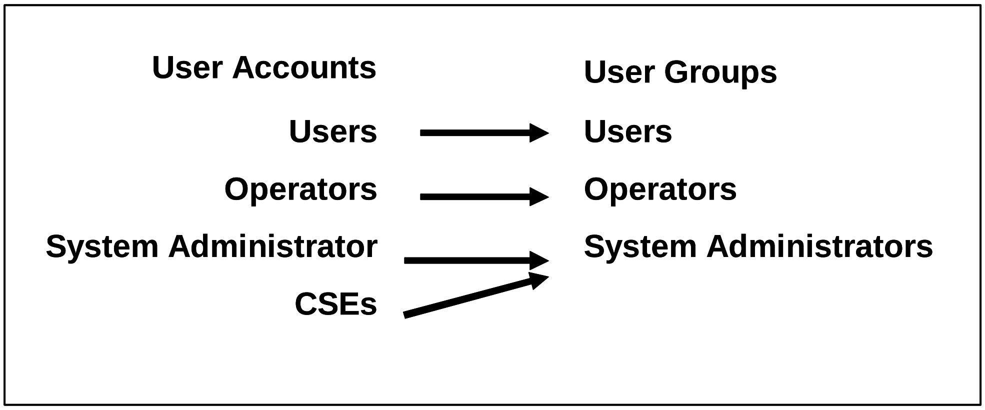
- Each local user account has an associated user name between 2-8 characters in length and is case sensitive.
- The user name is a string of characters from the set of alphabetic characters (a-z, A-Z), numeric characters (0-9), period (.), underscore (_), and hyphen (-); the first character must be alphabetic and the string must contain at least one lower case alphabetic character.
- Each account has the following attributes: user name, password, user group, account disabled/enabled, and comments.
- The maximum number of user accounts is 25,000.
- Each local user account has an associated user password that is a sequence of characters that is case sensitive and between 0 - 8 characters in length.

Default user groups and user accounts

DocuSP provides three default **user groups**: Users, Operators, and System Administrators. It also supplies four default **user accounts**: User, Operator, SA and CSE. User and Operator accounts correspond to User and Operator User Groups while SA and CSE both correspond to the System Administrators group.

.

Figure 1: Assignment to Groups



The User, Operator and SA user accounts cannot be edited, deleted, disabled, or removed from the assigned group. The CSE account can be removed from the System Administrator group and assigned to another group

Creating user accounts

The DocuSP user interface enables the Administrator to manage accounts easily by selecting [Setup], [Users & Groups], and the [Users] tab.

When the administrator selects the Users tab, a pop-up window appears that enables the administrator to create, edit, or delete an account and indicate whether the account should be enabled or disabled.

Group authorization

Job Management and Customer Diagnostics are two functions of DocuSP that the administrator may choose to restrict. From the Setup > Users & Groups menu option, select the “Group Authorizations” tab in the interface. The administrator can choose to enable or disable the service for a particular user group.

Table 2-6 Enable/disable from the “Group Authorizations” tab

Function	Users	Operators	Administrators(sa and cse)	Changeable via GUI	Comment
Job Management (release, hold, proof, promote, move, delete, … etc)	-	Enabled	Enabled	Yes	
Queue Management (New, Delete, Properties)	-	Enabled	Enabled	No	Possible to change this via GUI in DocuSP 4.2.
Queue Job Operations(Accept Jobs, Release Jobs, …etc)	-	Enabled	Enabled	No	

Function	Users	Operators	Administrators(sa and cse)	Changeable via GUI	Comment
Reprint Management	Enabled	Enabled	Enabled	No	The ”reprint_path” in Security Profile controls the directories that users can reprint. The defaults are:None -> everythingLow -> “saved”Med -> CD-ROMHigh -> nothing
Printer Manager(Finishing, Image Quality …etc)	-	-	Enabled	No	
Resource Managemen(LCDS Resources, PDL Fonts, Forms, ….etc)	-	Enabled	Enabled	No	Possible to change this via GUI in DocuSP 4.2.
Accounting, Billing	-	Enabled	Enabled	No	
System Preferences	-	Can set International,Job Processing, Stocks & Trays	Enabled	No	
Setup (System configuration, Gateways)	-	View & Print only	Enabled	No	
Setup (Feature licenses, Network configuration)	-	-	Enabled	No	
Setup (Security profile, SSL/ TLS, IP Filter)	-	-	Enabled	No	
Setup (Users & Groups)	-	-	Enabled	No	
Change password	Self	Self	Enabled	No	
Service Diagnostics	-	-	Enabled	No	

Function	Users	Operators	Administrators(sa and cse)	Changeable via GUI	Comment
Customer Diagnostics	Enabled	Enabled	Enabled	Yes	
Backup / Restore	-	Enabled	Enabled	No	

Password security

When the system is installed, the Change System Password dialog box appears and prompts users to establish all System Default Accounts with new passwords. For security reasons, **all system passwords must be changed.**

- **root:** has super user access to the workstation. The initial password for this account is set during installation of the operating system and should be obtained from the Xerox service personnel.

NOTE: *For security reasons, the root account password should be changed as soon as the Xerox service personnel have completed the installation.*

- The Xerox user name is the account from which the Xerox software runs. Enter the Xerox user password for this account. Contact your Customer Service Representative if this is unknown.

NOTE: *The administrator should verify access to the Xerox application for all levels before the service installation personnel leave the site*

- **ftp:** an account to permit some clients to retrieve their software from the DocuSP controller using the TCP/IP communication protocol. This account will be set to Read-only access to the /export/home/ftp directory

NOTE: *To maintain system security, it is recommended that any restricted access login be terminated as soon as the session has been completed.*

NOTE: *The user and group identifications, uid and gid, for the Xerox accounts that are listed above cannot be arbitrarily changed in the password and group files to new values because the software is based on the proper access to the Xerox supplied files.*

NOTE: *Please be aware that Xerox Customer Support Personnel must have access to the new root password for service and support. It is the customer's responsibility to ensure that the root and system administrator passwords are available for them.*

Strong Passwords

DocuSP provides additional security for users required to adhere to strict security guidelines. It provides a means in which a strong password policy can be enforced.

Strong Passwords can be Enabled and Disabled (default setting) via the Password Policies window.

Strong passwords must consist of ALL of the following

- A minimum of 8 characters in length
- Contain at least one capital letter
- Contain at least one number
- Contain at least one special character {!, @, #, $, %, ^, &, *}, including open and close parentheses { ( ) }, hyphen{ - }, underscore{ _ }, and period{ . }.

NOTE: *In DocuSP 4.x - The minimum password length is set in the security profiles. To enable the remaining requirements, the root (su) user must run the setstrongsecurity script located in the /opt/XRXnps/bin directory and reboot the system. Once the strong password feature is enabled, upon creation, new users will be forced to have a strong password assigned to their account. The passwords for existing users will remain the same and continue to work as before, but can be updated if necessary.*

NOTE: *The strong password requirements cannot be modified. A strong password cannot be set for root or any other Solaris user accounts that are not created by DocuSP.*

NOTE: *Remote Network Server: If running NIS+ name service, strong passwords would be enforced via the NIS + server.*
This policy can be set by using the -a <# of allowed attempts> argument with rpc.nispasswdd. For example, to limit users to no more than four attempts (the default is 3), you would type: rpc.nispasswd -a 4.

How to Enable/Disable Strong Password

- From the Setup menu select [Users and Groups]
- From the Policies drop down menu select [Password]
- Enable/Disable Strong Password from the Password Policies window. The default setting is “Disable”.

Login Attempts Allowed

DocuSP has provided a means to lockout users after reaching the maximum number of consecutive attempts. Once this is done, the user will need to apply (reset) a security policy and reboot the system.

The number of failed attempts and enable/disable is configurable via the Password Policy screen. When enabled, login attempts can be set from 1-6 attempts before the user is locked out. This function will only apply to failed login attempts via the DocuSP UI and does not apply to the root (su) user.

How to Enable/Disable Login Attempts

- From the Setup menu select [Users and Groups]
- From the Policies drop down menu select [Password]
- Enable/Disable Login Attempts from the Password Policies window. The default setting is “Disable”.

Password Expiration

The System Administrator can set a password expiration via the Solaris Management Control.

NOTE: *SMC (Solaris Management Control) has replaced AdminTool. AdminTool has been retired in Solaris 10.*

1. Open a terminal window and login as root
2. Type: smc &
3. Go to: System Configuration -> Users -> User Accounts-> <select user> -> Password Options tab
4. Enter values in the drop down menus associated with each password expiration parameter.

The DocuSP UI does not handle password expiration. Thus, DocuSP will not prompt the user to enter a new password if his/her password has expired. Instead, a message is posted indicating unknown user name or password. It is up to the customer to determine that the password has expired. To do so, the customer should open a terminal window and attempt to login as the user in question. If the password has expired, the system will prompt for the user to enter a new password.

Security Logs

User Activity on the System

When the High security profile is enabled, the Solaris Basic Security Module (BSM) is activated.

Date/Time User Login/Logout

This information is kept in the authlog and syslog in the /var/log directory. Login/Logout to DocuSP is tracked as well as Network Login/Logout.

Changing individual passwords

There are two ways to change passwords: Users can change their own passwords using the selection on the Logon menu and the administrator can change the password by double clicking on the user name in the User tab of [Users and Groups Management].

Accessing DocuSP through ADS

If DocuSP has been configured to join a Windows 2000 ADS domain, users may log onto the printer using their Microsoft Active Directory Services (ADS) user names.

To provide this option, the administrator must first configure DocuSP appropriately for the DNS gateway (see the “Gateway and Network Configuration” section of this guide). Additionally, the administrator must access the [ADS Groups] tab through [Users and Groups Management] and specify or edit the mapping of the ADS groups to the DocuSP user groups having permission to log on to the printer.

Configure DocuSP to Join the ADS Domain

To enable the ADS user accounts, DocuSP must have DNS enabled and joined to the appropriate ADS domain.

1. Logon to DocuSP as a member of the System Administrators. From the Network Configuration option, select the DNS tab, make sure that the Enable DNS check box is checked. Ensure that the DNS Server list is filled in with the IP addresses of up to three DNS servers to search when resolving host names to IP addresses. (This is part of the network configuration procedure).
2. Select the ADS tab, and enter in the fully qualified domain name of the ADS domain.
3. Click “Join…” button to join DocuSP to the ADS domain specified.

NOTE: *If DNS is not enabled, the “Join...” button will not be available.*

Map the ADS groups to the DocuSP user groups

From the Setup menu, Users & Groups option, select the ADS Groups tab. A member of the System Administrators group can specify, view and edit the mapping of ADS Groups to the three DocuSP user groups (Administrators, Operator, Users) permitted to log on to the printer.

Log on to the system with ADS user names

From the Logon menu, select ADS for authentication, then log on to the system with your ADS user name and password.

NOTE: *For this feature to work, Administrators must ensure that DNS is enabled, DocuSP is configured to join the ADS domain, and ADS groups are mapped to the DocuSP user groups.*

Troubleshoot ADS

Refer to the online help feature when troubleshooting ADS.

Limiting access

DocuSP provides options that allow the administrator to block or limit access to the system.

IP Filtering

IP Filtering allows the administrator to block IP addresses and provides access to services such as: LPR, IPP, HTTP, HTTPS, SMB Printing, Raw TCP Printing, and FTP Connections.

The administrator can limit access through the DocuSP interface [Setup > IP Filtering menu option]. The filter allows the blocking of specific IP addresses or a range of addresses from accessing the system. Available options include: Enable All Connections, Disable All Connections, Enable Specified Connections. Additional subnet mask can also be specified.

Refer to online help for detailed descriptions of IP Filtering property tabs such as: General tab, System tab, INIT tab, INETD tab, RPC tab.

Remote Workflow

Remote Workflow allows for a remote connection to the DocuSP controller.

The administrator can limit access through the DocuSP interface [Setup > System Preferences menu option]. Remote Workflow options include: Enable All Connections, Disable All Connections, Enable Specified Connections (by specific IP Address).

NOTE: *The default is Enable All Connections.*

Secure Socket Layer

DocuSP implements Secure Socket Layer technology using encryption, a secure port, and a signed digital certificate.

Secure Socket Layer (SSL) and Transport Layer Security (TLS) are two network security protocols that encrypt and transmit data via HTTP and IPP over the TCP/IP network. SSL is a protocol layer placed between a reliable connection-oriented network layer protocol and the application protocol layer.

The network client and the web server (printing system) decide which protocol to use for data transfer and communication.

The encryption level can be either secure or normal. Normal security in the SSL/TLS tab means that the user can access IPP or HTTP via http or https.

Using the DocuSP SSL/TLS Security Feature

The Secure Socket Layer (SSL) and Transport Layer Security (TLS) are two protocols used to provide a reliable end-to-end secure and authenticated connection between two points over a network. The DocuSP SSL/TLS feature allows a DocuSP System Administrator to do the following:

1. Create and use a self-signed SSL/TLS certificate
2. Use an existing certificate obtained from a certificate authority (i.e. VeriSign, Thawte, etc.)

Creating and Using a Self-Signed Certificate

– Logon to DocuSP as System Administrator or as a user who belongs to the System Administrator group.

– Go to Setup -> SSL/TLS

- If not already enabled, click the 'OK' button in the "Information" pop-up box
- Click on the 'Add Certificate Button'. This will launch the "Add Certificate Wizard".

  Step 1 - Select "Self-Signed Certificate"

  Step 2 - Select and enter either the server

  - Domain Name
  - IP Address
  - Other

  Step 3 - Enter the requested information:

  - Organization (required)
  - Organizational Unit (optional)
  - E-mail (optional)
  - Locality (optional)
  - State/Province (optional)
  - Country (required)

  Step 4 - Enter the length of time that the certificate will be valid for.

  Step 5 - Verify information entered in previous steps.

  Step 6 - A message will appear indicating that the self-signed certificate has been installed.

NOTE: *During steps 2-5, the user may go back and correct any mistakes made in previous steps.*

- Click on the 'Enable SSL/TLS' checkbox at the top of the SSL/TLS window.
- Select a SSL/TLS mode of operation:
  - Normal (Encrypted and Unencrypted Access)
  - Secure (Encrypted Access Only)
- Select encryption strength:
  - Normal (DES-MD5-56-bit)
  - Normal (DES-MD5-40-bit)
  - Normal (DES-MD5-128-bit)
  - Normal (3DES-MD5-128bit)
  - High (RC4-MD5-128-bit)
  - High (3DES-MD5-128-bit)

Using an Existing Signed Certificate from a Certificate Authority

- If SSL/TLS is not already enabled

- Click 'Add Certificate'

  Step 1 - Select "Signed Certificate from a Certificate Authority"

  Step 2 - Select and enter either the server

  - Domain Name
  - IP Address
  - Other

  Step 3 - Enter the requested information:

  - Organization (required)
  - Organizational Unit (optional)
  - E-mail (optional)
  - Locality (optional)
  - State/Province (optional)
  - Country (required)

  Step 4 - Browse to the location of the signed certificate (.pem file).

  Step 5 - Verify information entered in previous steps.

  Step 6 - A message will appear indicating that the certificate has been installed.

NOTE: *During steps 2-5, the user may go back and correct any mistakes made in previous steps.*

Digital Certificates

SSL/TLS cannot be enabled unless a digital certificate has been installed on the system, using the Add Certificate button. Installing a digital certificate can only be done by someone with administrator privileges.

The administrator selects SSL/TLS from the [Setup] Menu and clicks on the [Add Certificate] button. This invokes the Add Certificate wizard. There are two options regarding digital certificates. One option is “Self-signed certificate”. This is selected when no third party Certificate Authority is being used.

Another option is “Signed Certificate from a Certificate Authority”. In this case, the administrator needs to supply the fully qualified domain name, IP address, organization and country of the Certificate Authority.

If the choice is to use a Certificate Authority, all Certificate information needs to be held in a file and sent to the Certificate Authority. The Authority returns a valid certificate that must be installed on the system.

NOTE: *A self-signed certificate is not as secure as a certificate signed by a Certificate Authority. A self-signed certificate is the most convenient way to begin using SSL/TLS and does not require the use of a server functioning as a Certificate Authority or a third party Certificate Authority.*

Once the Digital Certificate has been installed, the Enable SSL/ TLS selection becomes available among the [Setup] options. At that time the administrator can select the mode of operation, Normal or Secure, from a drop-down menu.

Network Protocol

This section addresses Network Protocol, name service changes and the changes that occur when security is invoked.

The table below addresses the list of Network Protocols that are used by the DocuSP server software or Xerox client operations.

Table 2-7 Network Protocols

Network Protocol	Required
XSun	Required for functionality of DocuSP diagnostics software.
HTTP	Used when connecting to the server via the HTTP gateway. Connections can also be filtered using the IP Filter feature under Setup -> IP Filter.
Tomcat web server	Required for the functionality of the DocuSP Internet Services gateway and the Xerox Remote Services application.
IPP	Required for job submissions from the FreeFlow Print Manager and/or a Digipath (FreeFlow 2.0+) client. The IPP gateway can be enabled/disabled under Setup -> Gateways -> IPP tab. Connections can also be filtered using the IP Filter feature under Setup -> IP Filter.
Sun RPC	Used by many different clients, including DigiPath/FreeFlow and DocuSP Remote WorkFlow (DRW), and network services such as NIS+. Typically used to establish a connection to the server, which then redirects the connection to another open port using OS level port management. This service is shutdown when DocuSP security is set to high. Connections can also be filtered using the IP Filter feature under Setup -> Security Profiles -> <Any Profile> -> RPC tab
SNMP	Used for SNMP message exchange and traps. The SNMP gateway can be enabled/disabled under Setup -> Gateways -> SNMP.

Network Protocol	Required
WINS	Required when in an environment where connection to a WINS server is necessary. WINS service can be enabled/disabled under Setup -> Network Configuration -> WINS tab.
Socket (Raw TCP/IP) Printing	Required if jobs will be submitted via the socket gateway. The socket gateway can be enabled/disabled under Setup -> Gateways -> Socket. Connections can also be filtered using the IP Filter feature under Setup -> IP Filter.
LPD (LP/LPR)	Required for job submissions via the LP/LPR gateway (LP/LPR client, DocuSP Print Service (Reprint Manager), etc.). The port assigned to the LPD can be changed and/or the gateway can be enabled/disabled under Setup -> Gateways -> LPD.
SSH	Access the server via a secure shell (SSH, SFTP, etc.).
FTP	Access the server via FTP and/or submit jobs from a DigiPath/FreeFlow client via the Digipath/FreeFlow Print Manager. This service (ftpd) is shutdown when DocuSP security is set to high. In FreeFlow v2.0, the client has the ability to use secure FTP (sFTP) when DocuSP security is set to high and FTP is not available. Connections can also be filtered using the IP Filter feature under Setup -> Security Profiles -> <Any Profile> -> RPC tab.
SSL	Required when using the TLS/SSL security feature and/or a FreeFlow 2.0+ client with DocuSP security is set to high. Connections can also be filtered using the IP Filter feature under Setup -> IP Filter.
NFS	Necessary when using NFS mounted directories. This service is disabled when DocuSP security is set to high. Connections can also be filtered using the IP Filter feature under Setup -> Security Profiles -> <Any Profile> -> RPC tab.

NOTE: *The IP Filtering (Setup->IP Filter) feature can also help in limiting access to the server. This is DocuSP's GUI interface to the SunScreen Lite firewall that is part of the Solaris 8 Operating System. This feature allows the user to limit the number of clients who are allowed to access the server via services such as LPR, IPP, HTTP, HTTPS, SMB Printing, and FTP. By default, the firewall is disabled (all ports open), but can be enabled to either only allow specified connections (by IP address, IP address range, or subnet mask) or to close all ports. For DRW clients, this mechanism exists under System Preferences -> Remote Workflow -> "Enable Specified Connections".*

NOTE: *FreeFlow v2.0 and newer allows users to select whether or not the DocuSP server they connecting to will have high security enabled. If so, the client will use other communication paths such as sIPP (via SSL) for job submissions and sFTP for decomposition services (NetAgent).*

Roles and responsibilities

Xerox will make every effort to assist the administrator in ensuring that the customer environment is secure.

Xerox responsibilities

Xerox is committed to providing a level of security which will allow the DocuSP controller to be a good network citizen in response to current security intrusions. Additional security beyond this remains the responsibility of the customer.

Xerox is constantly evaluating the security of the DocuSP controller and the Sun Solaris operating system. Xerox is committed to providing the latest Solaris security patches provided by Sun Microsystems in each major DocuSP release. The DocuSP development team will also add Solaris security patches in between major release cycles. All OS security patches for applications that are added during a DocuSP install will be included, even if the application code is not normally used by DocuSP users. Security patches for applications that are not loaded by a DocuSP install will not be evaluated or included. Only the version of a patch impacting security will be included. If a security patch has a newer version that is not security related, then this patch will not be updated to the newer version. Any security patch that is determined to have a negative impact to DocuSP operation will not be added.

Customer Responsibilities

The administrator has the primary responsibility for maintaining the security of the network within the customer's site. It is important that network security is continuously monitored and maintained, and that appropriate security policies are established and followed.

The procedures outlined in this document assume a basic knowledge of UNIX, the vi editor, and general computing concepts. It is expected that the network administrator or system administrator responsible for network security understands the base commands (cd, chmod, cp, grep, kill, ln, ls, man, more, ps, etc.), and the UNIX directory path and filename structures shown in this document.

There is information within the text and in the appendix sections for reference to those who may not use UNIX often.

The DocuSP product operates on the default Solaris OS configuration and some additional Solaris patches required by DocuSP. Several scripts are used to provide additional security for the DocuSP. Not all scripts are public knowledge, only those that are public are defined in this document and these can be performed by the customer.

Xerox DocuSP engineering will evaluate the latest Sun Security Alert Packs issued by Sun Microsystems and integrate these patches into the DocuSP releases. Local customer support will be responsible for loading the latest DocuSP software.

Xerox strongly recommends that the customer change passwords from the default settings since the ultimate security of the printing system resides with the customer.

NOTE: *Please be aware that the Xerox Customer Support Personnel must have access to the new root password for service and support. It is the customer's responsibility to ensure that the root password is available for them.*

Security tips

The following recommendations will enhance security.

Document and backup

Always document and backup all files that you modify in case some unforeseen problem occurs. Example: #cp/etc/inet/inetd.conf   /etc/inet/inetd.conf.orig <RETURN>. If, for whatever reason, the DocuSP controller will not boot up after your modifications, you can restore the software to its original configuration by booting to single user mode. This is done by typing **boot -s** from the <ok> prompt. You will be prompted for the root password. Upon login as root, you can copy the original files back. For SPARC controllers running Solaris 8, this is done by typing boot -s from the <ok> prompt. For x86 controllers running Solaris 9, this is done by typing reboot -- -s in a terminal window.

If you are unfamiliar with the vi editor, you can use the GUI based Text Editor program. To launch the editor as root user, in a terminal window login as root and enter the following: #/usr/openwin/bin/textedit & <RETURN> Textedit leaves a backup of the modified file in the same directory. For SPARC controllers running Solaris 8, in a terminal window, as root, type: /usr/openwin/bin/textedit & <RETURN>. For x86 controllers running Solaris 9, in a terminal window, as root, type: /usr/dt/bin/dtpad & <RETURN>. This backup file will have a% after the name. This file can be deleted if you have already backed up the original file.

When you make a manual change to the /etc/inetd.conf file, to avoid rebooting the controller, you can retstart the inetd process. To do this, as root user type: ps -e | grep inetd <enter> and note the process ID returned. Then, type: kill -HUP #### (where #### denotes the process ID).

Online Help for security

A great deal of helpful security information can be found in Online Help. Sun's security tools and blueprints may be found at:

http://www.sun.com/solutions/blueprints/

Other security information, including alerts, may be found at:

`http://sunsolve.sun.com/pub-cgi/`
`show.pl?target=security/sec`

http://www.cert.org/nav/ index_main.html

http://www.cve.mitre.org/.