Information Technology Support for Pyxis® Dispensing Products

A CareFusion Marketing Publication

carefusion.com

CareFusion

Information Technology Support for Pyxis Dispensing Products

CareFusion provides this document for use as a general resource only. Anyone using this document should determine whether it is compatible with applicable state laws, regulations, professional practice guidelines, and accreditation standards. Use of this document should be at all times governed by the professional judgment of the user.

Purpose

This document outlines the typical information technology (IT) requirements to implement the Pyxis® Dispensing Products in a care facility.

Related Documents

- 10000184410 *Pyxis Medstation® 4000 System Specifications Guide*
- 10000128323 *Pyxis MedStation 4000 System Implementation Planning Guide*

CareFusion Pyxis Products Support Overview

CareFusion Pyxis products referenced above are turnkey systems. These products are supported by our Pyxis technical support and field-based service teams.

Pyxis Dispensing products are designed for ease of use and to be as unobtrusive as possible to a facility's IT infrastructure. With thousands of customers worldwide, CareFusion must maintain a level of consistency with the way its systems are offered and maintained. The operating system, device settings, and supporting software are imaged prior to shipment to the facility.

By maintaining this consistency, we ensure that our products are supportable through our centralized support center. For these same reasons, the installation of unauthorized third-party software by customers is contrary to company policy due to the installation of agents, services, or applications affecting the integrity of the shipped image. This compliance is detailed in the Master Support Terms and Conditions and can void the Carefusion Support responsibilities for altered products.

CareFusion understands the implications of the impact our systems can potentially have on a facility and we have designed our systems with security as a priority. The sections below outline our solutions for maintaining this level of security.

NOTE:
The information provided in this document is an overview of the information technology requirements for the Pyxis Dispensing Products. To obtain more details about the requirements, contact your CareFusion Sales representative, who will schedule a meeting. CareFusion looks forward to our partnership and to providing you the highest level of service.

Pyxis Dispensing Products consist of the following components that provide a stable and secure system for the automated dispensing of medication:

- One or more Pyxis Dispensing Product units (stations), which are computer-based automated dispensing cabinets
- Database servers
- Pyxis Workstations (remote server consoles)
- Interface equipment
- Security systems (patch management and virus management)

Hardware

Hardware for the Pyxis Dispensing Products consists of at least one database server and at least one station.

If you determine that additional access points are needed for pharmacy staff, you can lease or purchase a workstation that serves as an additional database server terminal for system administration.

Database server hardware

Typical specifications for the Pyxis-provided database server hardware are as follows:

- Processor—Intel® Xeon® 2.40 GHz (Quad Core)
- Memory—6 GB, DDR3-1333
- Storage—RAID-10 SATA array with global hot spare, SATA standalone backup drive
- NIC—Dual-gigabit Ethernet ports
- Removable drives—DVD/RW
- Rack size—6U or 2U† Tower available—6U model only

† U (or RU) is the abbreviation for "Rack Unit" the measure that describes the height of rack-mounted equipment.

Typical Station hardware

Typical specifications for the Pyxis-provided station and workstation are:

- Windows 7 Embedded OS
- 1–2 GB RAM
- 60 GB Solid State Drives (SSD)
- Speakers (optional)
- CD/DVD (optional)
- Wireless Networking (optional)

Operating system

The Pyxis Dispensing Products use Windows® operating systems, including Windows XPe. CareFusion will continue to provide support for your existing Pyxis technologies on the Windows XPe OS per the terms and conditions of your current support agreement. A database engine is present on nearly all Pyxis Dispensing Products, as well as a complete managed antivirus solution.

Pyxis Product	Operating system (server/station)	Database software (server/station)	Antivirus solution (server/station)
CUBIE® Replenishment Station	Windows XP Embedded operating system	Sybase® 10	
Pyxis Anesthesia System 3500	Windows Server® 2003/ 2008 operating system/ Windows XP Embedded operating system/ Windows 7 operating system	Sybase 9	ESET® Endpoint Antivirus (Stations); ESET File Security (Console)
Pyxis CathRack	Windows 7, Windows 2008	Sybase11	
Pyxis C^{II}Safe® v7.x system	Windows 7 operating system	Sybase 9	
Pyxis Connect v2.9	Windows XP operating system Windows 2003 operating system	MS SQL® 2005 Workgroup	
Pyxis Connect v3.0	Windows 7 operating system Windows 2008 operating system	MS SQL 2005 Workgroup	
Pyxis DuoStation	Windows XP Embedded operating system	Sybase 9	ESET Endpoint Antivirus (Stations); ESET File Security (Console)
Pyxis EcoStation	Windows CE/Windows 2008 32-bit	MS SQL 2005 Express	
Pyxis MedStation® 2000 system	Windows Server®2003 operating system SP1/ Windows NT operating system 4.0 SP6a	Sybase 9/Sybase 7	Symantec® AntiVirus 9/ Norton® AntiVirus 7.5
Pyxis MedStation 3000 system	Windows 2000 Server operating system/ Windows 2000 operating system	Sybase 9	ESET Endpoint Antivirus (Stations); ESET File Security (Console)
Pyxis MedStation 3500 system	Windows Server 2003 operating system/ Windows XP Embedded operating system	Sybase 9.02	ESET Endpoint Antivirus (Stations) ESET File Security (Console)
Pyxis MedStation 4000 system; Pyxis Anesthesia system 4000; Pyxis DuoStation; Pyxis SupplyClient; Pyxis SupplyRoller system;	Windows Server 2008 operating system/ Windows Server 2003 operating system/ Windows XP Embedded operating system/ Windows 7 operating system	Sybase 11	ESET Endpoint Antivirus (Stations) ESET File Security (Console) for devices using Windows 7 and Windows Server 2008

Pyxis Product	Operating system (server/station)	Database software (server/station)	Antivirus solution (server/station)
Pyxis Order Entry Station v2.9, v3.0	Windows XP operating system		
Pyxis PAR$_X$® system	Windows XP operating system	Sybase 9 Apache Tomcat® v6.0 3COM® TFTP Server v2.0.10	
Pyxis ProcedureRoller® system	Windows 7/Windows 2008	Sybase 11	
Pyxis ProcedureStation® half-height system	Windows 7/Windows 2008	Sybase 11	
Pyxis ProcedureStock® system	Windows 7/Windows 2008	Sybase 11	
JITrBUD® system	Windows 7/Windows 2008	Sybase 11	
Pyxis ScanStation®	Windows XP Embedded operating system		
Pyxis ScanStation+	Windows XP Embedded operating system		
Pyxis ScrubStation® v7.x system	Windows XP Embedded operating system Windows 2003 operating system	Sybase 10	
Pyxis SpecialtyStation® v4.x system	Windows 2000 operating system	Sybase 9	
Pyxis StockStation® system	Windows 7®/Windows 2008	Sybase 11	
Pyxis SupplyCenter system v9.x	Windows 7/Windows 2008	Sybase 11	
Pyxis SupplyRoller® system	Windows 7/Windows 2008	Sybase 11	
Pyxis SupplyStation® half-height system	Windows 7/Windows 2008	Sybase 11	
Pyxis SupplyStation mains	Windows 7/Windows 2008	Sybase 11	
VTS Host	Windows 2008 operating system		

***** The information provided in this document for the Pyxis DuoStation system pertains to the system being configured in “Med” only mode.

Security

The Pyxis Dispensing Products include a managed antivirus solution and a managed patch solution for the Windows operating system provided by CareFusion Security Module 2.0. Security Module 2.0 is an implementation of ESET Endpoint Antivirus and Administration and Windows Server Update Services 3.0. This server is wholly managed by CareFusion. The Pyxis Security Module 1.0 is an implementation of Symantec Antivirus Server 10.1 or Symantec Endpoint Protection 11 and Windows Server Update Services 2.0, or Windows Server Update Service 3.0. This server is wholly managed by CareFusion.

Networking

The following sections outline the specific network protocols, technologies, and port usage required to implement a typical Pyxis Dispensing Product Solution.

Addressing

The Dispensing device requires a standard internet protocol (IP) address assignment to function. This IP address may be assigned statically or by means of a dynamic host configuration protocol (DHCP) server reserved MAC address assignment. At this time, CareFusion does not support DHCP with DNS (except for Pyxis MedStation 4000 and ScrubStation stations), Active Directory membership, or facility domain membership.

All stations are deployed with a standard network interface card (typically Intel PRO/100 S Desktop Adapter or Intel PRO/100 M Desktop Adapter). Wireless networking is available on most stations.

The following products have the option of connecting wirelessly to the hospital network:

- Pyxis MedStation 3000 system
- Pyxis Medstation 3500 system
- Pyxis Medstation 4000 system
- Pyxis DuoStation
- Pyxis Anesthesia system 3500
- Pyxis Anesthesia system 4000 Station
- Pyxis SupplyClient
- Pyxis SupplyRoller system

Supported protocols for wireless devices

The following tables list the supported protocols for wireless communication, encryption, and authentication for wireless devices that are available for Pyxis Medstation Dispensing products, Pyxis DuoStation or Pyxis Anesthesia system.

Wireless device	Supported protocol
134513-01 PCBA WIRELESS ADAPTER WIN7	802.11 b/g/n CSMA/CA with ACK WEP, WPA/WPA2 WPA-PSK/WPA2-PSK(TKIP/AES)
35301-01 PCBA WIRELESS ADAPTER WIN7 (DOD)	802.11 Dual Band a/b/g/n WPA, WPA2, 802.1X (EAP-TLS, TTLS, PEAP, LEAP, EAP-FAST), EAP-SIM, EAP-AKA authentication PAP, CHAP, TLS, GTC, MS-CHAP, MS-CHAP v2 authentication protocols 64-bit and 128-bit WEP, AES-CCMP, TKIP encryption protocols FIPS, FISMA compliance

Network port usage

The Security Module 2.0 uses TCP ports to interact with several computers including the host system server and remote diagnostic server in your facility. Security Module 2.0 uses the following ports:

Common Pyxis Communication Ports

Port	Protocol	Internal / External	Service
25	TCP	External	Simple Mail Transfer Protocol (SMTP)
80	TCP	Internal	WSUS/Security Module 2.x
123	TCP	Internal	Network Time Protocol (NTP)
443	TCP	Internal	Remote Support Services / ESET Updates
445	TCP	Internal	Windows File Share
2221	TCP	Internal	ESET AntiVirus Updates/Administration
2222	TCP	Internal	ESET AntiVirus Updates/Administration
2638	TCP	Internal	Sybase Database ODBC/Administration
5631	TCP	Internal	PCAnywhere® (optional)
8042	TCP	Internal	EcoRex Configuration Tool (EcoStation only)
8052	TCP	Internal	EcoRex Report Generation Tool (EcoStation)
8531	TCP	Internal	WSUS/Security Module 1.0
9556	TCP	Internal	HL7 Connect (EcoStation only)
18000	TCP	Internal	Ntcomm to Notifier
18001	TCP	Internal	Timegod
18002	TCP	Internal	Notifier to Ntcomm
18003	TCP	Internal	Brain Transplant
18004	TCP	Internal	Console Application

Common Pyxis Communication Ports

Port	Protocol	Internal / External	Service
18006	TCP	Internal	Notifier to Launcher
18007	TCP	Internal	Maintain
18008	TCP	Internal	Notifier to Ntcomm
18009	TCP	Internal	Pcomm
18010	TCP	Internal	Query Manager
18050	TCP	Internal	Comm Status Console to Notifier
6000-7000	TCP	Internal	Connect Server/View station Devices Connect port (configurable, 1 port per system user required).

CareFusion® Coordination Engine

The CareFusion Coordination Engine (CCE) is a common platform for interoperability between our devices and hospital IT systems. CCE enables new offerings by leveraging data assets across our products, including integration of our workflow applications such as (Point-of-Care), analytics (KP) and surveillance (MedMined). Hardware for the CCE is optional and may be purchased by the customer. The CCE may also be purchased as a software-only solution.

Port	Protocol	Internal or External to MTF	Service
80	HTTP	Internal	Communication with CareFusion products.
443	HTTPS	Internal	Communication with CareFusion products. Requires constant outbound internet access from the device for remote support.
808	Net.TCP	Internal	Communication with CareFusion products.
1200-49000	TCP	Internal	Web service to other CCE components.

For each CCE service configured at the site, an additional port in the range [1200-49000] is required.

For each interface configured at the site, an additional port in the range [1200-49000] is required.

Disaster Recovery Design

The Pyxis MedStation and Pyxis SupplyStation system consoles utilize a RAID-10 storage array with a hot spare drive to provide redundancy for up to two hard disk failures. The active running database and the most recent copy of the database backup reside on the

RAID-10 Storage Array. The system consoles also utilize a single standalone RAID-0 drive to maintain additional copies of the database, including the most current copy, and have a mirror of the database transaction log resident as well. Lastly, the system consoles are capable of copying the database backup files and transactional archive files to an external DVD or a network file share. See *Network storage* on page *8 of 10* for additional details.

Recovery

If the Pyxis MedStation system console or the Pyxis SupplyStation system console fails, the Technical Support Center for Pyxis Products will work with a local CareFusion technician to attempt recovery of the system and its hard drive contents with a replacement server. If recovery of the hard drive contents is not possible, the Technical Support Center can utilize the database and transactional archive information copied to either a DVD or network file share to bring the system back online using a recovery process executed by the Technical Support Center.

Network storage

Most versions of Pyxis Dispensing Products allow you to back up the database and the transactional archive over the network if a network shared drive is available to the Pyxis system server (only servers have the option of network backups).

Network drive capabilities

In order to back up the database and transactional archive to the network, the Pyxis MedStation and Pyxis SupplyStation system servers must be able to map a drive on the network storage system at your facility. The Pyxis system server can automatically map the drive because it stores user credentials. User credentials can be the default credentials that are provided by CareFusion, a set of local user credentials, or domain user credentials. These credentials should not change after initial setup.

Network storage requirements

The following table contains the network storage requirements that you need in order to back up the database or transactional archive to the network.

Type of backup	Disk space required	Number of copies stored	Frequency
Database	100 MB–1 GB	7–365*	Nightly
Transactional archive	1 MB–15 MB	Not applicable**	Manually (initiated by user)
Supply	10 GB		15 days

* Configurable on Pyxis MedStation 2000 system with console software version C6.0.1.016 or later, Pyxis MedStation 3000 system, and Pyxis MedStation 3500 system, and Pyxis Anesthesia System 3500. For MedStation 4000, the auto-archiving to the network process is activated during system setup by a CareFusion employee and runs within the existing database backup at 11:00 p.m. local time.

Auto-archiving is enabled if a valid external path is configured in the System Setup Utility for the Archive Export Destination. Because new archive files are created at 1:30 am every day and the archive to network runs at 11 p.m. local time, archive files on the network share site will be one day behind. The database backup network location should be different from the archive backup network location.

** A set of transactional archive files is created each day. The files are typically kept for as long as is required by local regulations.

Patches

Pyxis Dispensing Products are a dynamic system that uses the OEM/embedded implementation of the Windows operating system, so a thorough quality test cycle is performed on all released patches for the Windows operating system. This practice ensures compatibility with support for Pyxis Dispensing Product devices.

Therefore, the process of approving and deploying patches for the Windows operating system is managed exclusively by CareFusion via the Security Module. Scheduled deployment of these patches is created with an agreement between CareFusion and your IT group.