System Requirements Overview

This document is updated regularly. Please visit Doc-it.com/overview for the current version.

This document contains the minimum hardware and operating system requirements for implementing Doc.It Suite®. The specifics for your environments can influence our recommended minimum requirements.

Requirements at a Glance

	Doc.It Suite	Doc.It Explore	Doc.It Connect
Doc.It Server	☑	☑	☑
Scanning Workstation	☑	☑	
Doc.It Web Portal	☑		☑

We encourage you to discuss your environment with us should you have any questions on your existing hardware, purchasing new hardware or upgrading your hardware.

For more detailed information and guidelines on system requirements, please contact John Glynn (jglynn@doc-it.com) or Ron Allan (rallan@doc-it.com).

Doc.It®

info@doc-it.com | www.doc-it.com

Global Headquarters
1425 Cormorant Drive, Suite 201
Ancaster ON L9G 4V5
Canada

888.693.6248
905.547.1100

USA
7848 W. Sahara Ave.
Las Vegas, NV 89117
USA

888.693.6248
905.547.1100

United Kingdom
4th Floor, Euston House
24 Eversholt Street
London, NW1 1AD, UK

00 1 888 693 6248
00 1 905 547 1100

USERS	DOC.IT 4.6 SERVER (SUITE, EXPLORE, CONNECT)	PORTAL SERVER	WATCH SERVER
3-5	Windows 10 16 GB of RAM i7 CPU with 8 threads 500 GB SSD drive Ethernet network (no WiFi)	Windows 10*1 16 GB of RAM i5 CPU 500 GB disk DMZ recommended*2	Watch & OCR can run on Doc.It 4.6 Server in addition to the Doc.It Server Components*3
6-20	Server class OS (Domain Controller) Server class CPU 16 GB of RAM 2 TB disk*4 (SSD,RAID recommended but not enforced) Ethernet network (no WiFi)	Server OS Server CPU 16 GB of RAM 500 GB of disk	Windows 10 16 GB of RAM i7 CPU 500 GB of disk
20-40	Fully licensed MS SQL server Server class OS Server class CPU 32 GB of RAM 2 TB disk*4 (SSD,RAID recommended)	Server OS Server CPU 16 GB of RAM 500 GB of disk	Windows 10 16 GB of RAM i7 CPU 500 GB of disk
40+	**See above for basic guidelines.** **For more accurate discussion contact Doc.It** **John Glynn, IT Manager** **1-888-693-6248 Ext. 3225 or jglynn@doc-it.com**		

1 Windows 10 only allows a maximum of 20 concurrent SMB connections. Server operating systems do not have this limitation.

2 A hardware firewall appliance with a configurable DMZ zone is strongly recommended to prevent unauthorized outside access to the web portal system or the firm's LAN environment.

3 The "Watch & OCR" must run in a virtual machine. It cannot be installed on the physical Windows 10 desktop.

4 The server that is hosting the web portal must be reachable by Internet-based systems. This will require that an Internet-based IP Address (static) and Fully Qualified Domain Name (FQDN) be associated with the web portal host system. If the host is within the DMZ, then the IP address of the Firewall that is Internet-facing is used along with the FQDN to create the Internet DNS entry and the Firewall is configured to forward the appropriate "traffic" to the web portal host system.

Additionally, a Secure Sockets Layer (SSL) Certificate will be required if you wish to secure the traffic between Internet-based clients and the web portal system. An SSL certificate pair is used to encrypt all the traffic between the client system and the web portal system ensuring that the information passing between these systems cannot be intercepted and understood by any unauthorized individual. Certificates for the web portal must be available in a format acceptable to Microsoft's IIS and must be 256-Bit / 2048-Bit. Check with the various Certificate Authorities (CAs) regarding availability of certificate formatting (without having to perform conversion) of their SSL certificates.

The portal server will require the firm's SMTP email settings and an email address to be used as a relay. The portal server will require an SSL certificate. Also, ports 8733, 4021, 3050 and 137-139 will need to be opened between the DMZ and the internal network. Port 8033 needs to be open from the portal to the outside.

NOTE: Microsoft's Internet Information Server (IIS) is required to run the Doc.It Web Portal Server.

Doc.It®

info@doc-it.com | www.doc-it.com

Global Headquarters
1425 Cormorant Drive, Suite 201
Ancaster ON L9G 4V5
Canada

888.693.6248
905.547.1100

USA
7848 W. Sahara Ave.
Las Vegas, NV 89117
USA

888.693.6248
905.547.1100

United Kingdom
4th Floor, Euston House
24 Eversholt Street
London, NW1 1AD, UK

00 1 888 693 6248
00 1 905 547 1100

DOC.IT CLIENT WEB PORTAL SERVER

The Doc.It Web Portal Server, version 4.x, can be successfully run on a workstation if the firm has less than 15 users. The workstation must meet the same requirements listed for running the Doc.It Suite client. Storage requirements for the web portal will vary depending on the number of the firm's clients that become portal users and the amount of information (# of files) that is transferred – by the client and the firm – via the portal. It is conceivable that average client/firm disk utilization could require 100MB of disk space over a year; this estimate can be used to determine the expected disk space based on the number of clients that will become portal users.

If the firm is greater than 15 users the Doc.It Web Portal Server must be a Microsoft supported server-grade system running Windows Server 2008, or later, other than SBS Server. The Doc.It v4.x Client Web Portal Server comes as a complete package and does not require additional software on the hosting system to run.

> Note: Windows 7/8 desktop operating systems only allow 20 simultaneous connections to the portal. Each employee desktop requires one of the 20 connections. This is a hard limit within the operating system. Firms with more than 15 employees must run portal on a server.

A hardware firewall appliance with a configurable DMZ port is strongly recommended to prevent unauthorized outside access to the web portal system or the firm's LAN environment. The implementation of a firewall would be a requirement for any outsource/hosted solution. The system that is hosting the Doc.It v4.x Web Portal Server would be connected to the DMZ port of the Firewall device.

The system that is hosting the web portal must be reachable by Internet-based systems. This will require that an Internet-based IP Address (static) and Fully Qualified Domain Name (FQDN) be associated with the web portal host system. If the host is within the DMZ, then the IP address of the Firewall that is Internet-facing is used along with the FQDN to create the Internet DNS entry and the Firewall is configured to forward the appropriate "traffic" to the web portal host system.

Additionally, a Secure Sockets Layer (SSL) Certificate will be required if you wish to secure the traffic between Internet-based clients and the web portal system. A SSL certificate pair is used to encrypt all the traffic between the client system and the web portal system ensuring that the information passing between these systems cannot be intercepted and understood by any unauthorized individual. Certificates for the web portal must be available in a format acceptable to Microsoft's IIS and must be 256-Bit / 2048-Bit. Check with the various Certificate Authorities (CAs) regarding availability of certificate formatting (without having to perform conversion) of their SSL certificates.

> *NOTE: Microsoft's Internet Information Server (IIS)* ***is required*** *to run the Doc.It Web Portal Server.*

Doc.It®

info@doc-it.com | www.doc-it.com

Global Headquarters
1425 Cormorant Drive, Suite 201
Ancaster ON L9G 4V5
Canada

888.693.6248
905.547.1100

USA
7848 W. Sahara Ave.
Las Vegas, NV 89117
USA

888.693.6248
905.547.1100

United Kingdom
4th Floor, Euston House
24 Eversholt Street
London, NW1 1AD, UK

00 1 888 693 6248
00 1 905 547 1100