OpenText Fax Appliance Security

Overview of Features

Fax and Document Distribution Group
November 2010

Abstract

This whitepaper is intended to explain the inherent security embedded in the OpenText Fax Appliance (OTFA) with emphasis on how the appliance is protected from viruses and other malicious attacks.

Highlights:

– No Operating System Access

– Restricted Network Access

– Controlled Attachment Types

Contents

Introduction

Keeping data secure and the appliance functioning are the main purposes for the security method implemented on the OpenText Fax Appliance. In order to ensure these goals are enforced, the Fax Appliance is configured to have limited access so malicious and/or incompatible software is not installed - which could put it at risk.

What Makes the OpenText Fax Appliance Inherently Secure?

No Operating System Access

Even antivirus software can cause issues when installed. Since the Fax Appliance only sends faxes, **there is no risk of sending infected messages as could occur with email**. In order to ensure that no incompatible software is installed on the Fax Appliance, no access to the operating system is permitted. All administration is done through the web interface using Microsoft Silverlight.

The OpenText Fax Appliance is deliberately locked down to restrict access to the device. This protects the appliance configuration but also protects the sensitive nature of the faxes themselves. The U.S. Department of Health & Human Services (HHS) established a set of privacy and security rules called the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which regulates the handling of private health information. The HIPAA strongly recommends, "*placing the fax machine in a secure location to prevent unauthorized access to the information*"[i].

The OpenText Fax Appliance is a **secure device where unauthorized access is not possible**.

Restricted Network Access

The OpenText Fax Appliance uses very strict firewall rules to make sure the device is locked down and secure. Below is a list of the only open ports on the firewall.

Service	TCP	UDP
Email Delivery	25	25
Silverlight Client Access	80	80
Silverlight Client Access	81	81
Silverlight Client Access	82	82
Fax Delivery	5060	5060

[1] HHS. (2006, November 11). *Can a physician's office FAX patient medical information to another physician's office?* Retrieved from U.S. Department of Health & Human Services: www.hhs.gov/ocr/privacy/hipaa/faq/smaller_providers_and_businesses/356.html
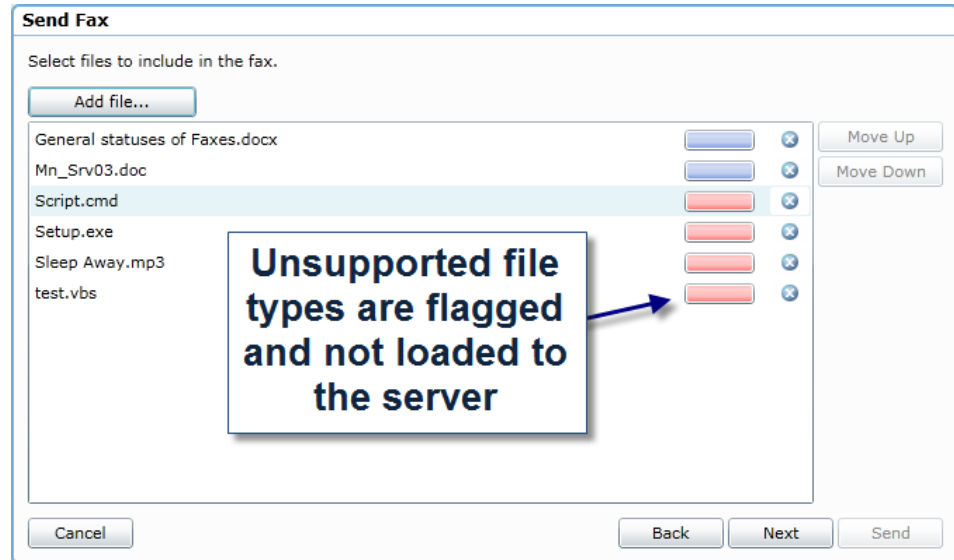
Controlled Attachment Types

Another security measure implemented by the OpenText Fax Appliance is the use of application whitelisting. This is where only a select number of document types are permitted as attachments to prevent conversion issues and potential risks. Even antivirus companies are seeing the value in moving beyond the old methods of pattern matching to newer solutions,

"If the growth of malicious software continues to outpace the growth of legitimate software, techniques like whitelisting - where we identify and allow only the good stuff to come in - will become critical." John Thompson, Symantec chief executive

Here is a list of the supported attachment type by the OpenText Fax Appliance:

Send Fax

Select files to include in the fax.

[Add file...]

General statuses of Faxes.docx	▭ ⊗	[Move Up]
Mn_Srv03.doc	▭ ⊗	[Move Down]
Script.cmd	▭ ⊗	
Setup.exe	▭ ⊗	
Sleep Away.mp3	▭ ⊗	
test.vbs	▭ ⊗	

Unsupported file types are flagged and not loaded to the server

[Cancel]   [Back] [Next] [Send]

Note: When sending a document using the Print-to-Fax Client, the document you are faxing is converting to a supported file type before it is sent. As a result, you can use any application with the Print-to-Fax Client without having to worry about unwanted malware or macros affecting the Fax Appliance.

For More Information

For more information on OpenText Fax Appliance visit http://faxsolutions.opentext.com or contact your OpenText sales representative at:

- North America: captaris.sales@opentext.com or (800) 304-2727

- EMEA: salesmea@opentext.com or +971 4 390 0281

- Western Europe: saleseurope@opentext.com or +31 (0)23 565 2333

About OpenText

OpenText is the world's largest independent provider of Enterprise Content Management (ECM) software. The Company's solutions manage information for all types of business, compliance and industry requirements in the world's largest companies, government agencies and professional service firms. OpenText supports approximately 46,000 customers and millions of users in 114 countries and 12 languages. For more information about OpenText, visit www.opentext.com.

www.**opentext**.com

North America	United States	Germany	United Kingdom	Australia
+800 304 2727	+1 847 267 9330	+49 89 4629 0	+44 0 1189 848 000	+61 2 9026 3400