Product Security White Paper

XpressDox Document Automation

Last updated: August 2020

93 North Street, Johannesburg, South Africa

Table of Contents

Product Security White Paper

XpressDox has implemented reasonable administrative, technical and physical safeguards to help protect against security incidents and privacy breaches involving the XpressDox product, provided the product is used in accordance with XpressDox instructions for use.

However, as systems and threats evolve, no system can be protected against all vulnerabilities and we consider our customers the most important partner in maintaining security and privacy safeguards.

If you have any concerns, we ask that you bring them to our attention and we will investigate. Where appropriate, we will address the issue with product changes, technical bulletins and/or responsible disclosures to customers and regulators.

XpressDox continuously strives to improve security and privacy throughout the product lifecycle using practices such as:

- Privacy and Security by Design
- Product and Supplier Risk Assessment
- Vulnerability and Patch Management
- Secure Coding Practices and Analysis
- Vulnerability Scanning and Third-Party Testing
- Access Controls appropriate to Customer Data
- Incident Response

Clear paths for two-way communication between customers and XpressDox.

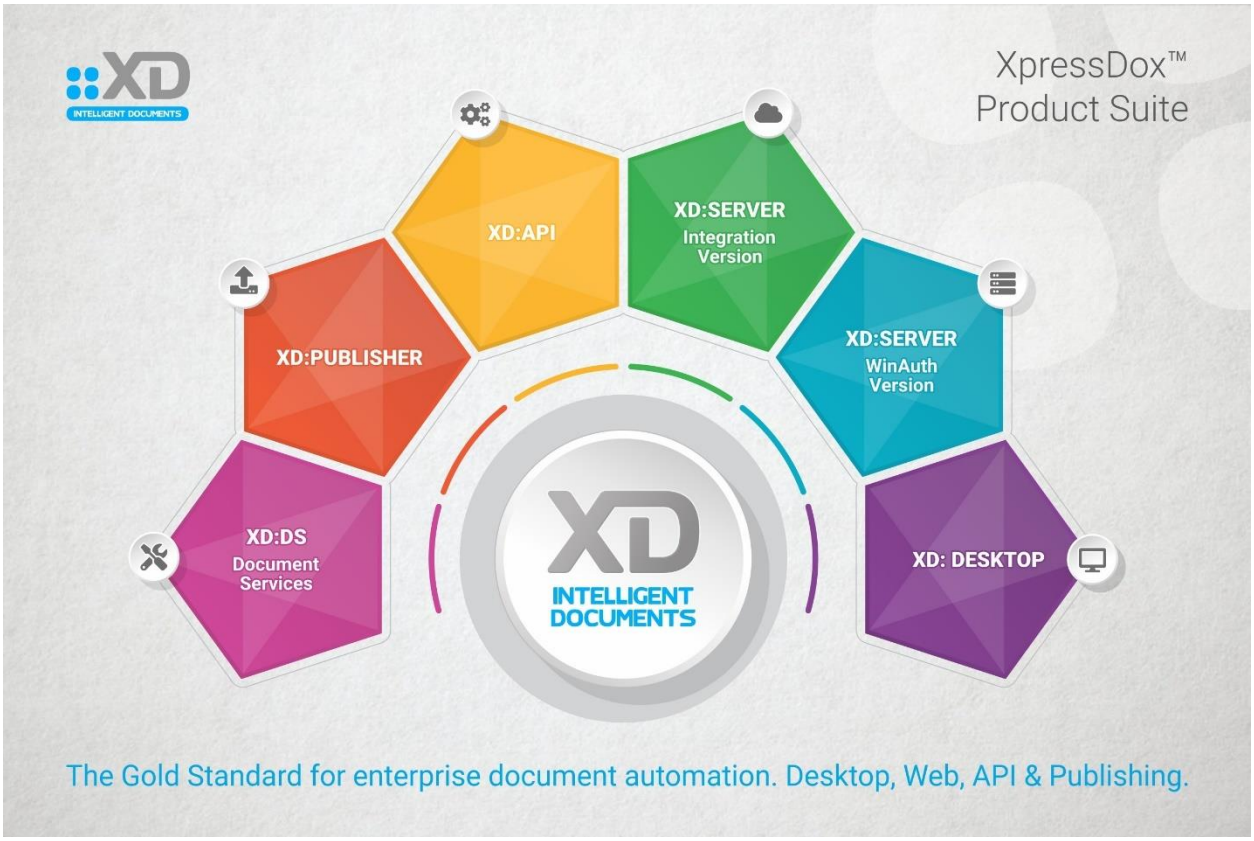
If you would like to report a potential product related privacy or security issue (incident, breach or vulnerability), please contact Chris Pearson at chris@xpressdox.com

The purpose of this document is to detail how XpressDox security and privacy practices have been applied to the XpressDox Product, what you should know about maintaining security of this product and how we can partner with you to ensure security throughout this product's lifecycle.

Product Description

XpressDox products are proven as the industry-leader in secure document automation. Our servers and software are designed for fast and easy deployment, and can be efficiently customized to your unique requirements. Integration of documents with your web sites and apps is unbelievably quick.

The XpressDox product suite includes:



XpressDox Desktop Products for MS Word

1. XpressDox Desktop **Supervisor** for MS Word

Supervisor manages authoring rights, where files are stored, and other configuration options.

Typically, a large firm will require only one Supervisor license.

2. XpressDox Desktop **Author/Developer** for MS Word

XpressDox Author allows template designers to build templates. XpressDox templates can be as basic or as sophisticated as you need them to be. For some requirements, all that is required are basic fields. But for others, you may wish to include sophisticated commands for Gender, Conditional Logic, Include Template, Repeating Items, Calculations, and even Database Access. XpressDox is right at home with every level of usage.

The Command Editor is included with XpressDox Author and it empowers the template author by providing an alphabetic list of all the XpressDox commands, with functionality which provides wizards for completion of the command as well as supplying examples of commands. The Command Editor also provides functionality for easily selecting the correct data element from a list of existing data elements. This helps the template author to develop templates more quickly. For large firms, a "basic" author license is also available which limits the functionality for departmental users who don't have the skills to develop "full-blown" templates.

3. XpressDox Desktop **Runner** for MS Word

XpressDox Runner allows users to run templates on their Microsoft® Word desktop. It includes no authoring commands, so users can only run templates. This means that less training is required for template runners, since the user-interface is limited to a handful of choices.

Secure, Customizable Document Automation Servers

XpressDox Servers are proven as the industry-leader in secure document automation. Our servers and software are designed for fast and easy deployment, and can be efficiently customized to your unique requirements.

XpressDox servers are available in two configurations: **Windows Authentication** servers and **Integration** servers. In addition to these server configurations, you can use the hosted XpressDox Cloud or host XpressDox servers in your own server facilities at Microsoft Azure, Amazon AWS, or the hosting provider of your choice.

The XpressDox **API** server ships as part of the Integration server on pricing plans of 50 or more users.

XpressDox servers include native data source compatibility, including SQL Server, ODBC-compliant databases, MySQL, Microsoft Office data sources such as Access, Excel, and Outlook, XML, text files and applications such as Salesforce.

1. **Windows Authentication** Server (Own-hosted)

Secure and Private Document Automation. Uses Windows Active Directory for complete control over user, folder and file access rights. No need to maintain yet another list of user credentials. Securely share configuration, brand and templates across your business.

2. **Integration** Server (Own-hosted or XD Cloud Hosted)

Document Automation in your Website and Mobile Apps. Perfect for secure app-to-server document automation integration to your websites, web apps and mobile apps. Various integration options to suit your deployment needs.

(a) XpressDox Server RESTful API

The XpressDox RESTful API exposes the full power of XpressDox document automation functionality to your apps.

With this API, you will be able to authenticate your app with your XpressDox Server (own hosted and hosted), explore folders and files, send data, assemble documents, and receive back links to completed documents.

File upload, download and delete functions are also supported.

Using the RESTful API for server-to-server communications will provide you with the most power and control, although it does require some development know-how.

(b) XpressDox-in-Word API

This API would be used specifically where you need to develop a custom user interface to capture data and select templates, but where you would still like to have access to the features made available by the Word Add-in.

Use of this API requires Word to be installed not only for rendering the merged documents, but for some of the other pre- and post-merging functions as well.

The API and documentation are installed along with the installation of the XpressDox Word Add-in. The documentation is provided in the Word document XpressDox In Word API Specification.doc which will have been installed into the My Documents\XpressDox folder the first time Word is loaded after XpressDox has been installed.

The specification document refers to a Word template in the My Documents\XpressDox\Samples folder. This Word template contains some Word VBA macros which demonstrate the usage of some of the XpressDox-in-Word API functions as called from within a VBA macro.

(c) XpressDox API for .NET

Typically you would use this API to embed the XpressDox document automation capability into systems such as accounting, practice management, work flow and any other system where there is a need for creating non trivial documents. The templates used can be sourced from the Windows file system, or from any other source such as a document management system.

If there is no need to render the merged documents on the machine on which the API will operate, then it is not necessary to have Word installed on that system. Word is needed in order to author templates, which in turn requires XpressDox Author, and to render the resulting merged document for printing or reading. The function of merging the template and data that XpressDox performs does not require Word.

The XpressDox API is embedded in the .NET assemblies, which are installed with the Word Add In instance of XpressDox, so no additional software is needed in order to use the API. A sample Visual Studio solution (in C#) can be downloaded, along with formal documentation on the use of the API.

(d) XpressDox API for COM

The second XpressDox API is for use by non .NET developers and it exposes an interface to XpressDox via COM. This interface is very similar to the XpressDox Engine API for .NET, the major difference being that templates are expected to reside somewhere on the Windows file system. This does not mean that they cannot actually be stored in a document management system or database, but that they will have to be moved onto the file system before the COM API will be able to access them.

Similarly to the XpressDox API for .NET, the COM API uses assemblies that are installed along with the Word Add-in instance of XpressDox. It also needs another assembly, which is downloaded and installed along with the XpressDox API in the download process referred to above. The COM API would be used in much the same circumstances as the XpressDox API for .NET.

(e) XpressDox Devkit

Using either of the two APIs, you are responsible for creating an XML data set, selecting a template, and storing the merged document created from them. It is necessary to note that much of the functionality available to the XpressDox Word Add-in is NOT available to the API user. This includes the dynamic data capture interview and all the features exposed via the Configuration user interface (e.g. Standard Folders for document and data storage, Data Sources, Standard Data Items, Configuration merging, etc.).

All commands that can be coded into templates which refer to these features (i.e. all the Data Capture commands in the Command Editor, as well as Data Source commands and commands in the Advanced document and file handling section of the Command Editor) will be ignored when the template merging is handled via either of the two XpressDox Engine APIs.

However, the XpressDox Devkit, which is a new addition (and can be downloaded from the same place as the API download) will make all of the above exclusions available to the developer—try it and see.

Hardware Specifications (On-premise hosted servers)

True Server Environment

- Processor: Intel XEON CPU 1.8 Ghz or faster. 4 Core with Hyperthreading (Minimum)
- RAM: 32 GB ECC Ram
- Hard drives: Minimum of 4 Hard drives configured in Raid 10. (Enterprise SSDs are recommended, but Enterprise SAS drives should suffice)
- Ethernet Connection: 1 GB port or faster
- Bandwidth: 50 Mbps or faster internet connection (Full Duplex) 50 Mbps Download and 50 Mbps Upload speed. (It will work on slower connections but with degraded performance)

Desktop Server Environment

- Processor: Intel Core i5 CPU 2 Ghz or faster. 4 Core with Hyperthreading (Minimum)
- RAM: 32 GB Ram
- Hard drives: Minimum of 4 Hard drives configured in Raid 10. (Enterprise SSDs are recommended, but Enterprise SAS drives should suffice)
- Ethernet Connection: 1 GB port or faster
- Bandwidth: 50 Mbps or faster internet connection (Full Duplex) 50 Mbps Download and 50 Mbps Upload speed.

Virtual Environment

- 4-8 vCPU (Depending on underlying CPU speed) If 1.8-2.0 Ghz we recommend 8 vCPU's. With 2.4 Ghz and faster 4 vCPU should suffice.
- 32Gb vRAM
- 150 GB Minimum Storage for Operating System and supporting software.
- 500 GB Storage for XpressDox data. These can be on one virtual drive or separate virtual drives, but it is important that the underlying hard drive infrastructure must have at least 6 drives in Raid 10, SSDs are also recommended here.

Hardware Specifications (XD Cloud-hosted servers)

Virtual Environment

- 3 Azure geo-redundant environments – locations United States, Canada, Germany
- For Azure compliance, see https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/

Recommended Hardware Architecture for Cloud Deployments

The architecture should follow international best practices and include all the relevant technology for redundancy purposes. All servers should include:

- Dual Power Supply Connection
- Dual Network Connectivity
- Multiple Hard drives for the purpose of redundancy and performance

For each server a failover server should co-exist within the same physical location. Failover for this location should be fully automated.

Software Requirements

- Microsoft Windows Server 2012, or higher
- Microsoft .Net Framework v4.5.2, or higher
- Internet Information Services (IIS) v7, or higher
- Microsoft SQL Server [Express] 2012, or higher, if XpressDox WinAuth Server or XpressDox Cloud Server (i.e. not XpressDox API Server) is being installed
- Optional: Access to your Windows network, only if Windows Active Directory user authentication is required

Network Ports and Services

It is recommend that all ports are blocked with the following exceptions:

- HTTPS on the default port 443
- Port 11000 which is used for the application's auto updating service
- Port 3389 can be opened on an ad hoc basis if remote access to the machine is required.

Sensitive Data Transmitted

The following sensitive data is transmitted through the application lifecycle:

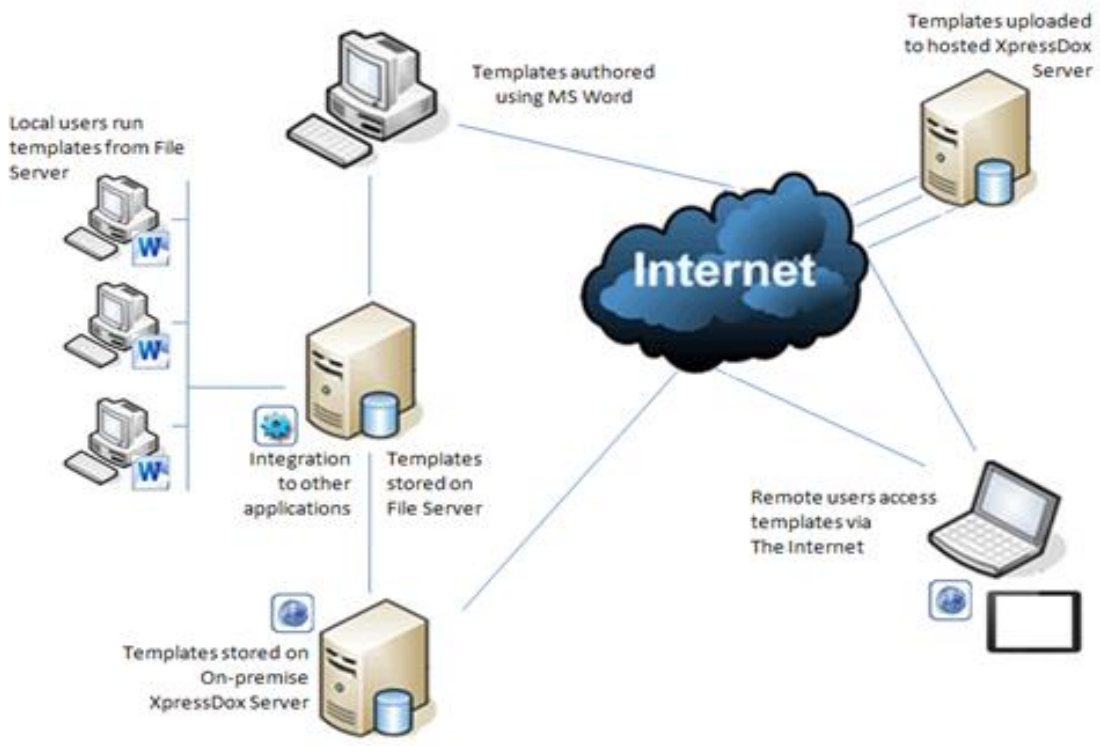
- Login credentials secured via HTTPS (Does not apply where Active Directory Authentication is used)
- Any other data which Client choose to include in their template design

Sensitive Data Stored

The following sensitive data is stored through the application lifecycle:

- Login credentials are stored in the database
- A SHA512 salted hashed version of the password is saved
- Client Templates are stored but can be encrypted if required
- Datasets and/or documents are stored subject to Client preference
- If stored, a Client choice exists for each document or dataset to be encrypted at rest

Typical Network and Data Flow Diagram



Internet Security Solutions (Antivirus and Malware Protection)

The following Internet Security Solutions are recommended:

- Monthly Windows updates for System Security
- An Enterprise Antivirus and Antimalware solution with real time monitoring and reporting enabled
- Software Restriction Policies should be enabled to prevent any other software from data access or interference

Authentication and Authorization

User Access

XpressDox supports Basic Authentication.

User Access: Username and Password is sent via an HTTPS POST request to the server and an encrypted Authentication cookie is returned to be used in subsequent calls.

The following functionality is available regarding management of passwords:

Forgotten Password - A reset link will be emailed to the user's registered email address on the system. This link will expire after a configurable time limit.

Change Password - An authenticated user will have the option to change their password at any given time.

API Access: Username and Password is sent via an HTTPS POST request from the integrating server to the XpressDox Server and a token is returned to be used in subsequent calls.

User Management

The user to register a new account on the system is automatically assigned as the administrator on the account.

Account administrators have access to add, edit and disable users within their accounts. The following user roles can also be assigned to any user restricting access to various functional areas.

Administrators, File Administrators, Template Runners

User Groups can also be defined and users assigned to these groups. Folder access can then be managed by allowing certain groups access to certain folders.

Network Controls

Besides the Port Restrictions mentioned above no additional firewall rules are necessary.

Encryption

The minimum recommended protocol for all network traffic is TLS 1.2 with AES256. Encryption at rest can be enabled by the Application Administrator.

Audit Logging

Comprehensive audit logging of who did what, when - saved into a SQL Server database. For example:

- User management
- Templates management
- Assemblies reporting management
- Authentication auditing
  - User login/logout
  - User login from multiple workstations
  - Client application connect/disconnect with IP address and port
  - Failed client connection attempts
  - Failed/successful attempts to access, modify, or delete roles, permissions, etc.
- Application logging
  - Service Start/Stop
  - Application errors
- Audit data permissions
  - System administrators

Remote Connectivity

RDP access can be granted on an ad-hoc basis if remote access to the machine is required

End-of-Life and End-of-Support

XpressDox provides support on the current version plus two previous major versions of its software. Note that the client can download the latest code version at any time without purchasing an upgrade, but their functionality in the upgraded product will be limited to the functions that were in the version they originally purchased.

This is unique as outright purchase clients are not forced to update their software, and as such no end of life notification is issued.

Supported versions of Microsoft Word (Office) are as published on the download page of the XpressDox website.

Privacy of Information

Information regarding our privacy policy can be found here: https://xpressdox.com/privacy/

Secure Coding Standards

We implement a Software Development Life Cycle (SDLC) that includes:

1. Security as a design requirement
2. Regular regression testing
3. Code reviews
4. Use of a framework where feasible and appropriate
5. If there is an application need to store or transmit sensitive data we make use of encryption in transit and at rest
6. Conducting Security and Privacy Impact Assessments, including inventory of applications, libraries on which they depend, application contacts/developers, data classifications, and data volume estimates.
7. Following secure coding practices such as minimizing risks identified by a Coding Vulnerability Checklist
8. Reviewing accounts & privileges regularly.
9. Separating Test environments from Production environments.
10. Separation of duties are established and monitored to ensure conflicting roles and access to all phases of the development and implementation process are not granted.
11. A risk assessment is performed prior to production for all applications that will store, access, create and/or transmit confidential or protected information.
12. All build and deployment development operations are automated to minimize human error.

System Hardening

- SQL Server database – default sys admin user is disabled
- Remote Desktop connection for the purpose of remote support is only available via VPN and not publicly available
- All incoming ports are disabled by default, and only HTTP and HTTPS are enabled; port 11000 is enabled for auto-updating
- All traffic is secured by SSL certificates
- RDP port 3389 is only opened on request for RDP connections

Penetration Tests

Date of scan: Sun Jul 26 20:31:44 2020 UTC

Type of Scan: Common Vulnerabilities and Exposure (CVE)

URL: https://cve.mitre.org

Risk Identified

Medium (CVSS: 5.0) 443/tcp NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (OID: 1.3.6.1.4.1.25623.1.0.108031)

Risk Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exist only on HTTPS services.

Vulnerability Detection Result

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution type: Mitigation

The configuration of these services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.

Disclaimer

The information contained in this Product Security White Paper is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify or supersede the terms and conditions of any written agreement between such customer and XpressDox, or XpressDox subsidiaries or affiliates (collectively “XpressDox”),

XpressDox does not make any promises or guarantees to the customer that any of the methods or suggestions described in this Product Security White Paper will restore customer’s systems, resolve any issues related to any malicious code or achieve any other stated or intended results.

The customer exclusively assumes all risk of utilizing or not utilizing any guidance described in this Product Security White Paper.