Kofax ControlSuite

Administrator’s Guide – Security

Version: 1.1.0

Date: 2020-01-16

KOFAX

Table of Contents

Preface

This document describes the security model for Kofax ControlSuite 1.1.0 and provides architecture diagrams and details related to ControlSuite product components.

Note The information in this document relates to the security model for Kofax ControlSuite. For details about ControlSuite features and functionality, please consult your Kofax professional.

Getting help for Kofax products

The Kofax Knowledge Base repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Base to obtain answers to your product questions.

To access the Kofax Knowledge Base, go to the Kofax website and select Support on the home page.

Note The Kofax Knowledge Base is optimized for use with Google Chrome, Mozilla Firefox, or Microsoft Edge.

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need.

  Type your search terms or phrase into the Search box, and then click the search icon.

- Product information, configuration details and documentation, including release news.

  Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.

- Access to the Kofax Customer Portal (for eligible customers).

  Click the Customer Support link at the top of the page, and then click Log in to the Customer Portal.

- Access to the Kofax Partner Portal (for eligible partners).

  Click the Partner Support link at the top of the page, and then click Log in to the Partner Portal.

- Access to Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

  Scroll to the General Support section, click Support Details, and then select the appropriate tab.

Security and encryption terminology

Access Control List (ACL): Identifies a user (trustee) and specifies the access rights allowed, denied, or audited for that trustee.

Active Directory (AD): Technology created by Microsoft to provide a centralized and standardized system that automates network management of user data, security and distributed resources, and enables interoperation with other directories.

Encrypting File System (EFS): System-level file encryption used to protect data from attacks by unauthorized users who gain physical access to a computer.

Hypertext Transfer Protocol Secure (HTTPS): The use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under standard HTTP application layering. HTTPS encrypts and decrypts user page requests and the pages that are returned by the Web server.

Internet Printing Protocol Secure (IPPS): Secure/encrypted version of the Internet Printing Protocol, to support the secure transmission of documents for print.

JSON Web Token (JWT): Security token used to authenticate user and service credentials, and permissions to other components within the system.

Public Key Infrastructure (PKI): A security framework that uses two different cryptographic keys, a public key and a private key, to protect communications between clients and servers.

Secure Sockets Layer (SSL): A certificate-based cryptographic protocol that provides encrypted communication and authentication between two entities over the network during transit**.**

SSL Certificate: A security certificate issued by a trusted authority to validate encrypted data.

Transparent Layer Security (TLS): A certificate-based cryptographic protocol that provides encrypted communication and authentication between two entities over the network during transit. TLS is an upgraded successor to SSL.

Overview

The Kofax ControlSuite security model relies on industry-standard technologies such as Active Directory or LDAP services for authentication and authorization privileges, secure data transmissions using SSL/TLS and encryption such as EFS (Encrypted File System). Information in this document tells how Kofax handles the following aspects of ControlSuite security.

- Authentication and Authorization mechanisms
- Data in transit
- Data at rest

Security Development Lifecycle

Implementation of a Security Development Lifecycle helps software development companies reduce the number of security-related design and coding defects, and the severity of security defects that have not been identified.

The Kofax Security Development Lifecycle is focused on the following areas to ensure security against key vulnerabilities.

- **Risk**: Identify primary and secondary software security risks
- **Product Design**: Address identified risks based on Kofax Security Requirements
- **Verification Techniques**: Use of Kofax tests and activities to verify the corresponding security requirements and vulnerabilities

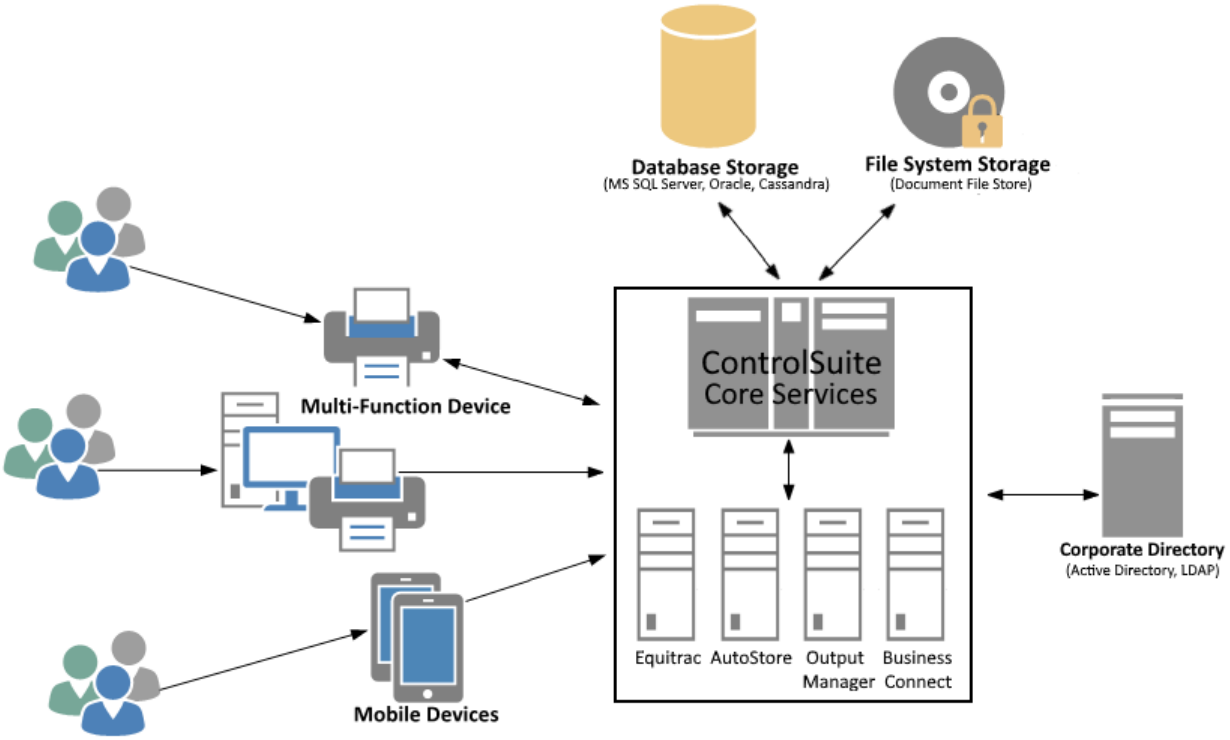
Implementation

Kofax has implemented the following software security best practices.

- Address security considerations across all phases of product development and implementation, including training, planning and design, risk assessment, implementation, verification and testing, and release.
- Regularly review security considerations to ensure continual security improvements.
- Test early and often with a variety of vulnerability tools, network monitoring, and intelligent test cases.

Kofax ControlSuite security model

Kofax ControlSuite architecture



User login and authentication

Category	Authentication and Authorization
Description	User provides login credentials for Kofax ControlSuite application.
Security Details	Kofax ControlSuite supports synchronizing users/groups with Active Directory/LDAP. This approach allows Kofax ControlSuite to take advantage of the corporate infrastructure for authentication and credential management. Kofax ControlSuite also offers application-specific authentication and authorization mechanisms for convenience and added security. These mechanisms include credential management and storage. Stored passwords are encrypted. Once a user has been authenticated, applications send the authenticated user's credentials to the ControlSuite Core Services for authorization. The ControlSuite Core Services first ensure that the application itself is trusted, then generate, sign, and respond with a JSON Web Token (JWT) containing the identity of the user and the roles the user can perform. The application can then call appropriate subcomponents with the JWT authorization. Subcomponents verify the received JWT is signed by a trusted service and contains the necessary permissions to access protected resources. The user's actual credentials are never sent directly to other subcomponents.

Service login and authentication

Category	Authentication and Authorization
Description	ControlSuite service provides credentials to another ControlSuite service.
Security Details	A ControlSuite service will send its credentials to the ControlSuite Core Services, which authenticate the service. The ControlSuite Core Services generate, sign, and respond with a JSON Web Token (JWT) containing the identity of the service and the roles it can perform. The service will then be able to make requests of other ControlSuite services, passing the JWT authorization in place of the credentials. The ControlSuite service receiving the request verifies the received JWT is signed by a trusted service and contains the necessary permissions to access protected resources. The service's actual credentials are never sent directly to other ControlSuite services.

ControlSuite Server transmits to another ControlSuite server

Category	Data in transit
Port	Configurable. Defaults to 8181.
Protocol	HTTPS
Description	Kofax ControlSuite server transmits to/from another ControlSuite application or server.
Security Details	All Kofax ControlSuite components are configured to use secure encrypted communication (TLS) with custom or administrator supplied certificates. The TLS protocol and cyphers can be configured using Windows settings.

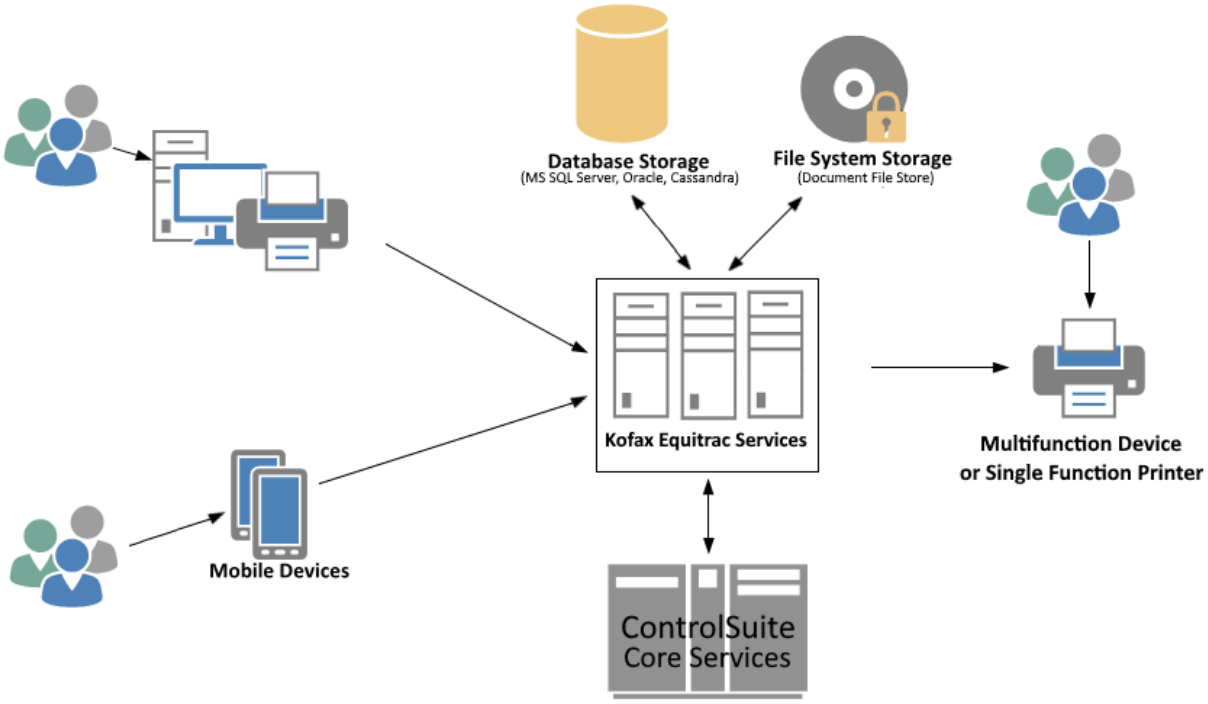
ControlSuite Core Services transmit to Cassandra Database server

Category	Data in transit
Port	7001, 9042, 9160
Protocol	HTTPS
Description	ControlSuite Core Services transmit to/from Cassandra distributed database nodes.
Security Details	Communication from ControlSuite Core Services to Cassandra database and between distributed database nodes is configured to use secure encrypted communications with custom self-signed certificates.

Data storage

Category	Data at rest
Description	Secure storage of component credentials and configuration.
Security Details	ControlSuite service credentials are stored on disk and encrypted. Access control lists (ACLs) limit access to authorized users and services. The configuration for ControlSuite Core Services is stored in the file system and protected by the ACLs.

Kofax ControlSuite Office Print (Equitrac) architecture



Print Subsystem transmits to Kofax Equitrac server

Category	Data in transit
Port	Configurable. Defaults to 8181.
Protocol	HTTPS
Description	Windows print spooler transmits print documents to, and receives configuration from, a Kofax Equitrac server.
Security Details	All Kofax ControlSuite components, including Equitrac, are configured to use secure encrypted communication (TLS) with custom or administrator supplied certificates. The TLS protocol and cyphers can be configured using Windows settings.

Kofax Equitrac server transmits to MFD or Single Function Printer

Category	Data in transit
Port	9100, 515 or 631, depending on protocol
Protocol	RAW, LPR, IPP
Description	Kofax Equitrac server transmits print documents to a Multifunction Device (MFD) or Single Function Printer for print.
Security Details	The Kofax Equitrac server must connect to the MFD or Single Function Printer to send documents for print . For secure encrypted transmissions, the MFD must support IPPS. Please see the *Print Stream Encryption* document for details on how to configure the print system.

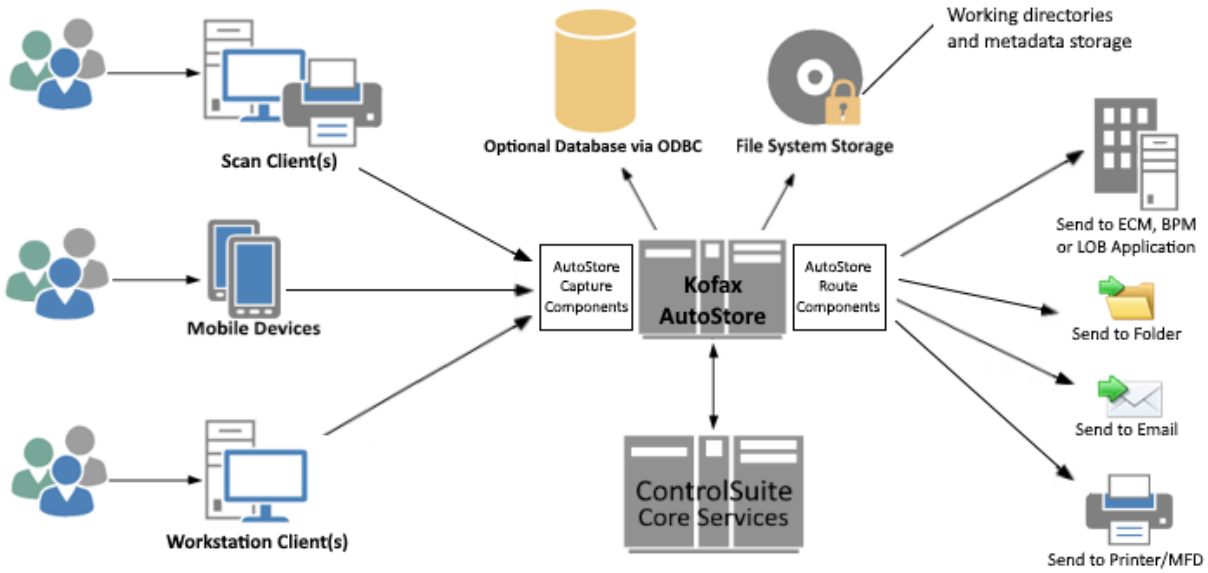
Kofax Equitrac Server transmits to Database server

Category	Data in transit
Port	Varies, depending on protocol
Protocol	TCP/IP or named pipes
Description	Kofax Equitrac servers transmit to/from database.
Security Details	Kofax Equitrac servers connect to a SQL database. Typically, the database server system is co-located with the Equitrac servers that connect to the database.

Data storage

Category	Data at rest
Description	Print documents and metadata stored on disk for secure document release
Security Details	The Kofax Equitrac server needs to store printed documents on disk to support page counting and secure document release. Windows Encrypting File System (EFS) should be used to protect the data at rest. Please see the *Print Stream Encryption* document for details on how to configure the print system.

Kofax ControlSuite Capture (AutoStore) architecture



Client transmits to Kofax AutoStore server

Category	Data in transit
Port	Configurable and depends on the client; see the *AutoStore Communication Port Reference* for details.
Protocol	Depends on the client
Description	Kofax AutoStore client transmits to Kofax AutoStore server.
Security Details	Kofax AutoStore capture components can be configured to use secure encrypted communication (TLS) with custom or administrator supplied certificates. The details can be configured using Windows settings.

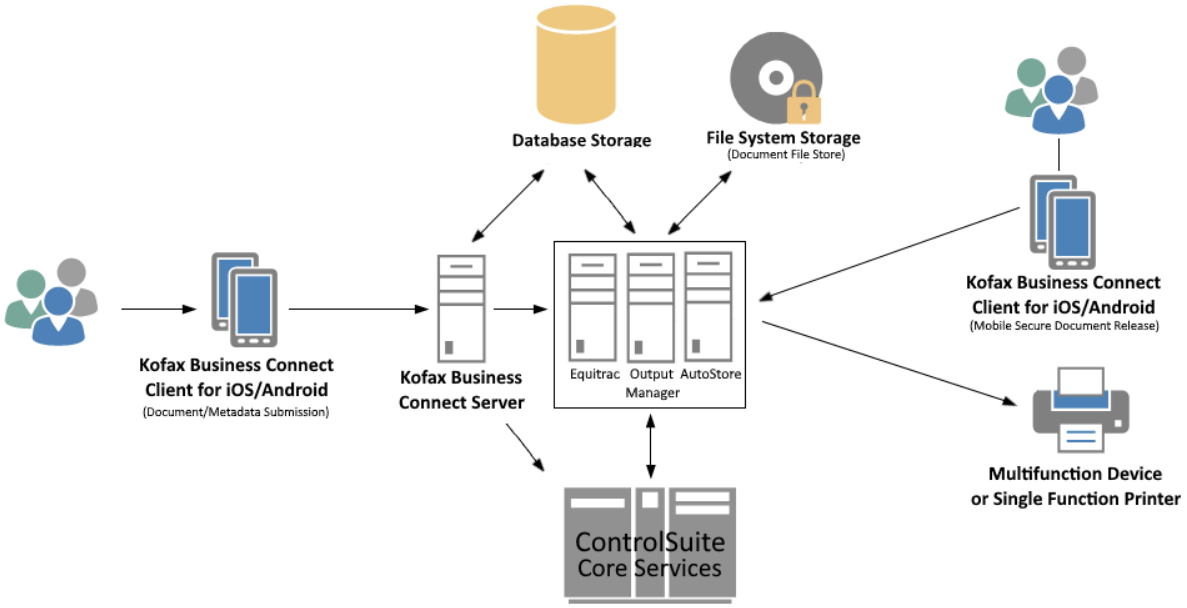
Kofax AutoStore Server transmits to Database server (optional)

Category	Data in transit
Port	See *AutoStore Communication Port Reference*
Protocol	TCP/IP or named pipes
Description	Kofax AutoStore server transmits to/from database
Security Details	Kofax AutoStore servers can optionally connect to SQL databases. Kofax AutoStore uses external databases for data lookup, and does not utilize any internal databases.

Data storage

Category	Data at rest
Description	Workflow data stored on disk
Security Details	Documents and metadata submitted to a Kofax AutoStore workflow are stored on disk during the workflow execution. Stored passwords are encrypted. Windows Encrypting File System (EFS) should be used to protect the data at rest.

Kofax ControlSuite Mobile (Business Connect) architecture



Kofax Business Connect mobile application transmits to server

Category	Data in transit
Port	443
Protocol	HTTPS
Description	The Kofax Business Connect mobile app transmits to Kofax Business Connect server.
Security Details	Kofax Business Connect can be configured to use secure encrypted communication (TLS) with custom or administrator supplied certificates. The details can be configured using Business Connect Configuration Manager, IIS Manager and Windows settings. The only officially supported mode for a production environment is to use an SSL Certificate issued by a trusted Certificate Authority. Self-signed certificates require additional configuration for mobile devices and are not supported. In addition to TLS encryption, user credentials are always encrypted with Public Key Infrastructure (PKI) encryption between the mobile app and the server.

Kofax Business Connect server transmits to ControlSuite server

Category	Data in transit
Port	82
Protocol	HTTPS
Description	Kofax Business Connect server transmits to/from other Kofax ControlSuite server(s).
Security Details	All Kofax ControlSuite components are configured to use secure encrypted communication (TLS) with custom or administrator supplied certificates. The TLS protocol and cyphers can be configured using Windows settings.

Kofax Business Connect server transmits to AutoStore WebCapture component

Category	Data in transit
Port	Configurable. Defaults to 3291.
Protocol	HTTPS
Description	Kofax Business Connect server transmits to/from AutoStore WebCapture server.
Security Details	Communication with the AutoStore WebCapture component can be configured to use secure encrypted communication (TLS) with custom or administrator supplied certificates. The TLS protocol and cyphers can be configured using Windows settings.

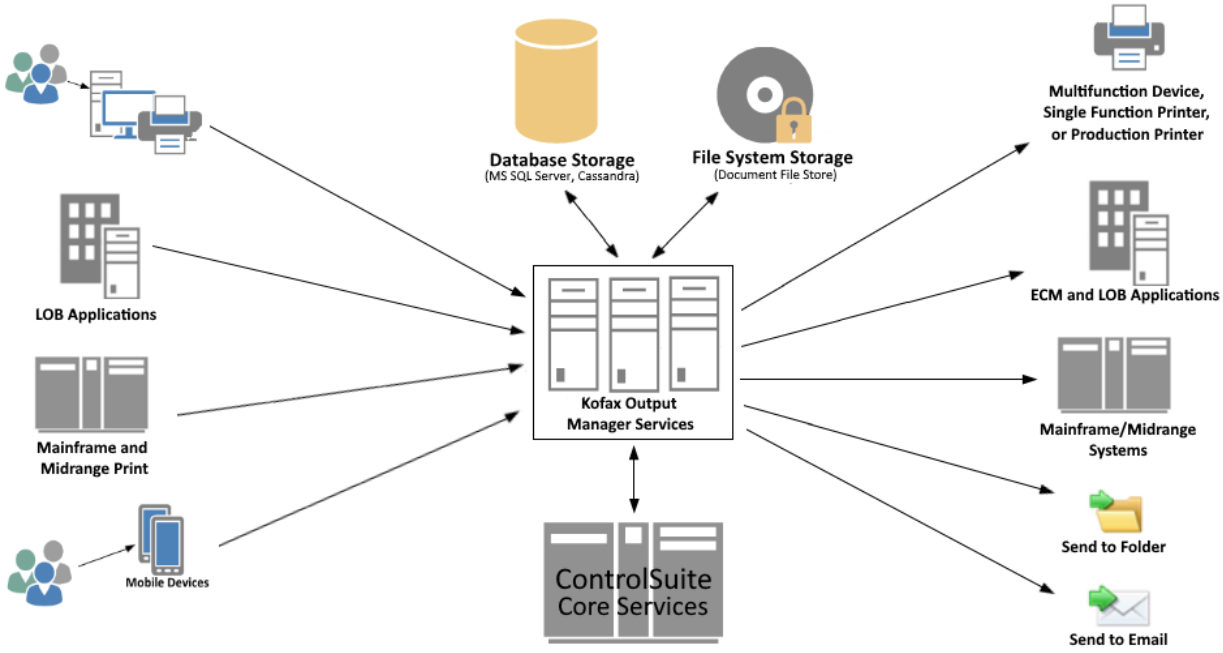
Kofax Business Connect server transmits to Database server

Category	Data in transit
Port	Varies, depending on protocol
Protocol	TCP/IP or named pipes
Description	Kofax Business Connect server transmits to/from database.
Security Details	The Kofax Business Connect server can connect to Microsoft SQL Server if the SQL Server database is configured instead of the default embedded Microsoft SQL Server Compact Edition database.

Data storage

Category	Data at rest
Description	Primary storage is Microsoft SQL Server Compact Edition database or Microsoft SQL Server database. Also, Kofax Business Connect stores configuration and some temporary operational data (documents, metadata) in folders that reside within the Windows file system during the workflow execution.
Security Details	By default, the Microsoft SQL Server Compact Edition database is used. The database is always encrypted. Kofax Business Connect server can also be configured to use Microsoft SQL Server database. Kofax Business Connect servers do not store any credentials or other sensitive data in the database. The Windows Encrypting File System (EFS) should be used to protect the data set stored in the Windows file system at rest.

Kofax ControlSuite Output Management (Output Manager) architecture



Applications and clients transmit to Kofax Output Manager server

Category	Data in transit
Port	Depends on the client. Common ports include 9100 (Socket), 515 (LPR/LPD), and 631 (IPP)
Protocol	Depends on the client
Description	Kofax Output Manager receives data from other applications, clients, and devices through multiple protocols including Native IP Socket, LPR/LPD, and IPP(s). Output Manager receives encrypted information from IPPS clients over secure (TLS) channels.
Security Details	When receiving data from other ControlSuite components, HTTPS is used and secured using custom or administrator supplied certificates. When receiving data from IPP clients, the customer can configure the server to require IPPS (TLS).

Kofax Output Manager server to MFD

Category	Data in transit
Port	9100, 515 or 631, depending on protocol
Protocol	RAW, LPR, IPP
Description	Kofax Output Manager server transmits documents to an MFD for print.
Security Details	The Kofax Output Manager service needs to connect to the MFD to send print jobs submitted through the system. IPP devices can be configured to support IPPS and Output Manager can be configured to send to these devices over secure (TLS) channels.

Kofax Output Manager server transmits to Database server

Category	Data in transit
Port	Varies, depending on protocol
Protocol	TCP/IP or named pipes
Description	Kofax Output Manager server transmits to/from the Database server.
Security Details	The Kofax Output Manager server connects to the Microsoft SQL Server database as configured by the Database Administrator.

Data storage

Category	Data at rest
Description	Kofax Output Manager stores data in one or more file store folders that reside within the Windows file system.
Security Details	Kofax Output Manager provides the ability to encrypt the file store folder using Windows Encrypting File System (EFS).