Security White Paper

PRISMAprepare 7.1 - version 003

Copyright and Trademarks

Copyright

Trademarks

Table of content

Foreword

This document describes the security features of PRISMAprepare. It discloses which data PRISMAprepare handles and how its security works.
Firstly, this document provides an overview of PRISMAprepare. Secondly, it details all security related issues. For example, which data the application handles and which network protocols and ports are used.

IT administrators are the target group for this security white paper.

Canon can deliver this document to sales companies worldwide. Sales companies can edit the contents of the document before disclosing any of the information to customers.

1 What is PRISMAprepare

PRISMAprepare is a document preparation solution. The PRISMAprepare product targets both the corporate and the commercial printing environment.

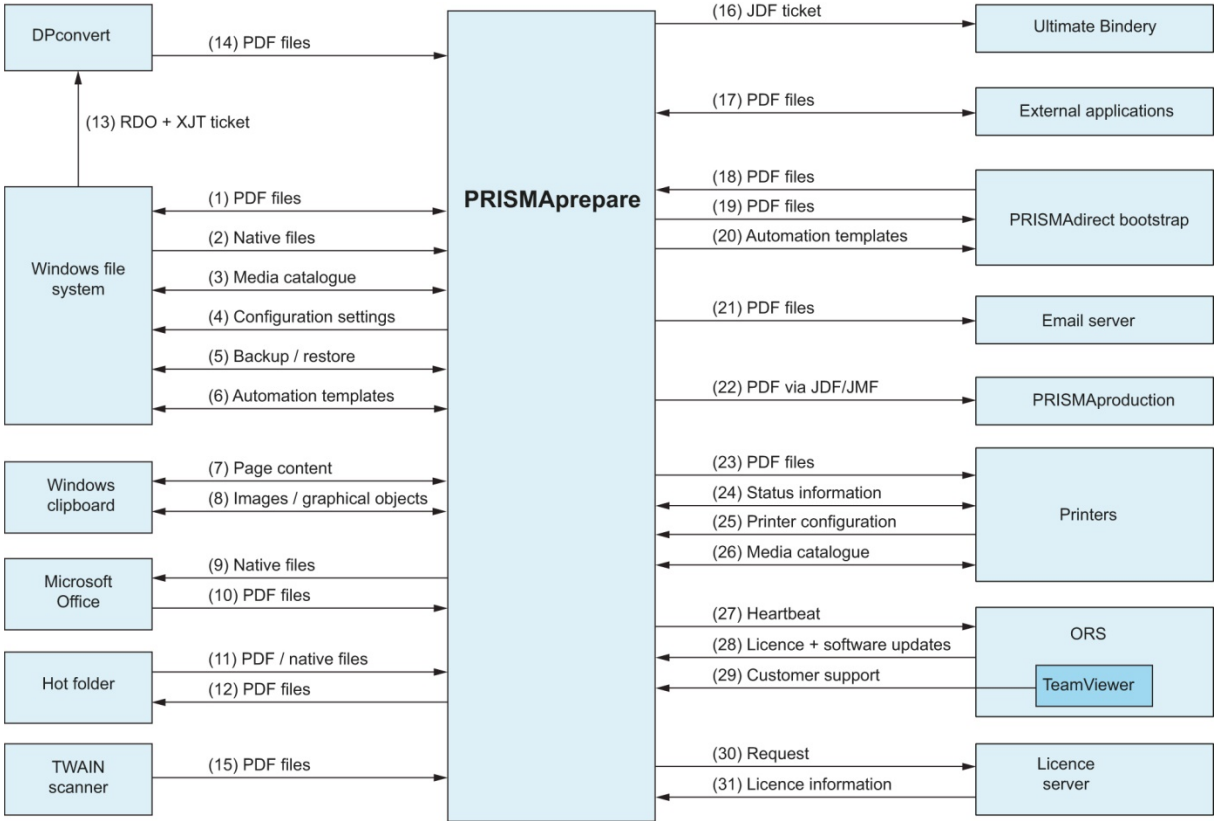
PRISMAprepare can be sold together with PRISMAdirect. PRISMAdirect serves as a:

- Web shop / order submission client for the end user
- Order management / production workflow solution for the print room operator.

An interface exists between these two products. Documents submitted to PRISMAdirect can be page programmed and printed using PRISMAprepare.

1.1 PRISMAprepare and its environment

PRISMAprepare is a desktop application. The following diagram illustrates the interactions between PRISMAprepare and its environment. The licence server can be installed on a different computer than the PRISMAprepare computer. In this case, it is called a remote licence server.



The data interactions in the diagram contain numbers enclosed by round brackets. The numbers match the data transmitted between PRISMAprepare and its components in the text below.

PRISMAprepare transmits data to and from the file system:

- Open and save PDF files (1).
- Open native files (2).
- Import / export the media catalogue file (3).
- Storage of the configuration settings (4), including the name and port number of the licence server and the configuration of the log level.
- Backup / restore of the configuration (5) of PRISMAprepare.
- Storage of the automation templates (6) for automated page programming.

PRISMAprepare copies data to and from the clipboard:
- Page content (7), including any VDP frames, but excluding any page programming.
- Images and graphical objects (8).

PRISMAprepare can open Microsoft Office documents and documents supported by Microsoft Office (9). PRISMAprepare converts these documents automatically to PDF (10) by calling the related Microsoft Office application.

PRISMAprepare can process files directly from the file system using a hot folder:
- Import native files and/or PDF files (11).
- Export the original PDF file, modified PDF file (12) and the log file to the destination folder.

The DPconvert module can convert Xerox RDO archive files (13) into PDF files (14).

Scanned jobs (15) can be received through the TWAIN interface.

PRISMAprepare can send JDF tickets (16) to Ultimate Bindery using a hot folder.

PRISMAprepare allows the operator to edit a PDF file (17) in an external application, e.g. Adobe Acrobat. The changed file is sent to PRISMAprepare again.

PRISMAprepare can be called on a .NET interface by the PRISMAdirect bootstrap.
- The bootstrap allows the operator to page programme a PDF file (18), or to print a PDF file via PRISMAprepare.
- The bootstrap can return a page programmed PDF file (19) to PRISMAdirect.
- A service of the PRISMAdirect bootstrap synchronizes the automation templates (20) from PRISMAprepare to PRISMAdirect.

PRISMAprepare uses an email server to send proof PDF files (21) to customers.

Optionally, PRISMAprepare can send jobs (22) to PRISMAproduction using the printer driver of PRISMAproduction. The communication is one-way only. No status information is sent back from PRISMAproduction to PRISMAprepare.

PRISMAprepare can send page programmed PDF files (23) to the printers and receive status information (24). PRISMAprepare can retrieve the printer configuration (25) of a number of printers.

PRISMAprepare can import the media catalogue (26) from PRISMAsync controllers and EFI controllers. The media catalogue of PRISMAprepare can be exported to a file or to a printer.

PRISMAprepare sends a heartbeat (27) to Océ Remote Service (ORS) to check the connection. ORS pushes license and software updates (28) to PRISMAprepare.

TeamViewer is used for remote customer support (29). TeamViewer is installed by the remote assistance feature and can only be used in combination with ORS.

PRISMAprepare sends a request (30) for license information to the license server. The license server sends a string containing the licensed features (31) to PRISMAprepare.
The PRISMAprepare configuration contains one license server.

1.2 PRISMAprepare services and accounts

The default user that runs the PRISMAprepare services is:

- The “Local System” account.

The following services are deployed on the computer where PRISMAprepare and/or the Floating Licence Server are installed:

- **Floating Licence Server**
  This service manages the Floating Licence Server. It writes to the log files “lmgrdFile.log”, “flexlmService.log” and “ocelicenseserverconfiguration.InstallLog”.
- **Hot folders for PRISMAprepare**
  This service monitors the hot folders. It writes to the log files “PPHotFolder.log” and “PPHotFolderConsole.log”.
- **TeamViewer 10**
  This service manages the TeamViewer Remote Software.

The following service is deployed on all computers where PRISMA Core is installed:

- **PRISMAprepare ORS service**
  This service handles the connection between PRISMAprepare and Océ Remote Service.

The following table shows which services run on each component of PRISMAprepare.

PRISMAprepare	Floating Licence Server
• Floating Licence Server • Hot folders for PRISMAprepare • PRISMAprepare ORS service • TeamViewer 10	• Floating Licence Server

1.3 Configurations of PRISMAprepare and its deployment

PRISMAprepare can be installed in a number of configurations on one or more computers.

Configuration	Composition
Centralized	PRISMAprepare + Floating Licence Server installed on *one* computer
Distributed	PRISMAprepare + Floating Licence Server installed on separate computers
Extended	PRISMAprepare + Order processing workstation of PRISMAdirect installed on *one* computer

2 System security

2.1 Security aspects

Security is covered by the “Software Security Data Sheet” for PRISMAprepare. Its conformance includes:

- Validation of input parameters of all public interfaces.
- Critical information like passwords are stored encrypted.
- Possibility to use secured communication channel
- Validation that delivered code is virus free
- Documentation of external API, of Channel/Port, etc.

When possible, the built-in OS security mechanisms are used. For instance:

- HTTPS is offered via a standard Web Server (IIS, Tomcat…)
- File System protection, including for shared drives, is offered in the OS

Other security aspects:

- A PDF file protected against modification cannot be edited by the PDF Library, even if the document protection allows printing and the changes are only relevant for printing (for instance: adding print marks).
  This situation might require circumventing the protection.
- An encrypted PDF file or Office file can be read only if using the password.

2.2 Programming languages and technology

- PRISMAcore and PRISMAprepare are based on .NET Framework 4.7.1. The programming language is C# 5.0.
- The interfaces to C/C++ libraries are mapped to C# using wrappers.
- The WebUIs are used for the integration of PRISMA Core and PRISMAdirect. The Web UIs are built using HTML5, CSS and Javascript. The server side of the websites is built with C# on ASP.NET. Other technologies used include JQuery and AngularJS.

2.3 Antivirus software

Antivirus software is encouraged as long as it does not lock legitimate files especially in temporary folders. The following temporary folders are used by PRISMAprepare and should be excluded from antivirus scanning:

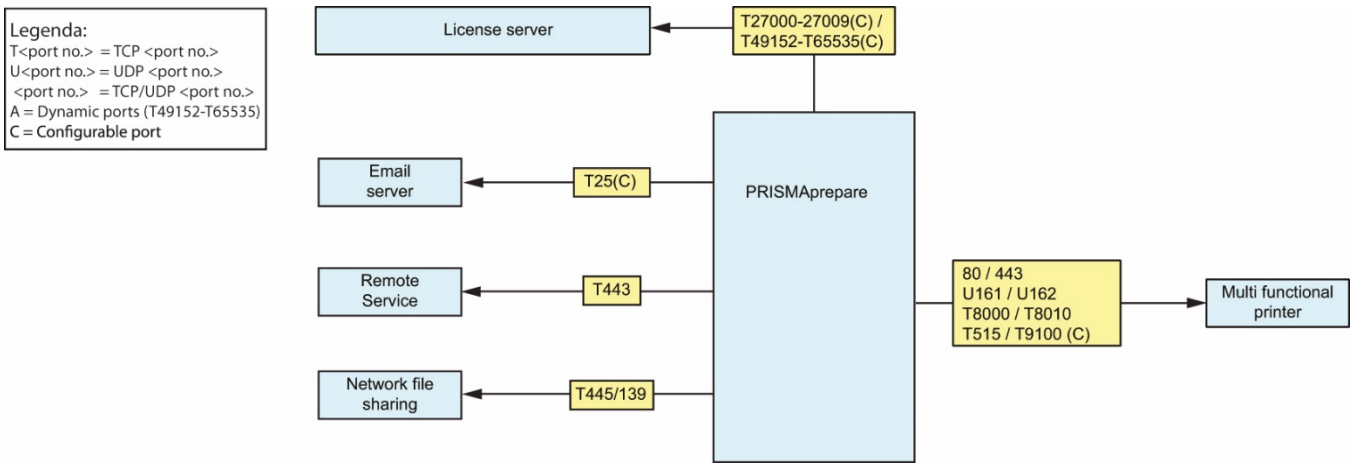
- C:\Users\<username>\AddData\Local\Temp
  This is the default temporary folder path. The path can be changed in option “Data directory” in the “PRISMAprepare Administration”.
- C:\ProgramData\Oce\PRISMAprepare\Temp\

PRISMAprepare is checked against recent versions of the following antivirus packages:

- McAfee 7.2.1.16
- TrendMicro 12.0.1226
- Sophos 1.3.2
- Kaspersky 19.0.0.188(b)
- Norton 22.15.0.88

3 Network security

3.1 Diagram of the protocols and ports



The following tables list the protocols and port numbers used by PRISMAprepare.
Legend for the tables:
(C) = configurable port

3.2 PRISMAprepare

Component	Application protocol	Protocol & port no.	Direction	Main purpose
License server	Proprietary	TCP 27000 –27009 (C) TCP 49152 – 65535 (C)	Outbound	License for PRISMAprepare
Email server	SMTP	TCP 25 (C)	Outbound	
Océ Remote Services	HTTPS	TCP 443	Outbound	
Network file sharing	SMB / CIFS	TCP 445 TCP / UDP 139	Outbound	TCP 445: SMB file sharing. The implementation of the SMB protocol is OS dependent. TCP / UDP 139: NetBIOS Session Service
Multi-functional printer	HTTP HTTPS SNMP SNMP JMF JMF LPR/RAW	TCP / UDP 80 TCP / UDP 443 UDP 161 UDP 162 TCP 8000 TCP 8010 TCP 515 / T9100(C)	Outbound	HTTP(S): Data to printers SNMP 161 + SNMP 162: status JMF 8000 + JMF 8010: JMF communication LPR 515: Printer port RAW 9100 (C): Printer port
Internal ports	Proprietary	TCP / UDP 4526		TCP 10253: Hot folders

		TCP 10253 TCP 10254		TCP 10254: Preflight. When executing preflight on multiple PRISMAprepare sessions, a different port is used for each session.

3.3 License server

Component	Application protocol	Protocol & port no.	Direction	Main purpose
License server	Proprietary	TCP 27000 –27009 (C) TCP 49152 – 65535 (C)	Inbound	

4 Access control

The default user that runs PRISMAprepare is:

- The currently logged on Windows user.

A number of actions in the “PRISMAprepare Administration” module require Windows administration rights. For example, only an administrator can enable and configure Océ Remote Service.

PRISMAprepare encrypts any passwords used for hot folders and Océ Remote Service. The encrypted passwords are stored in the configuration files of the hot folders and Océ Remote Service.

5 Data and data security

5.1 Data at rest

Generally, PRISMAprepare stores all received data indefinitely. PDF files and optional JDF tickets are stored on disk without encryption. Operators can delete the files.

The email address of the operator is stored in the following configuration file:
C:\ProgramData\Oce\PRISMAprepare\MailServerConfiguration.xml
This configuration file is created when the operator enters the SMTP information in the application.

Sent emails are not stored, they are (re)generated when sending them.
License information from the license server is cached and periodically renewed.

5.2 Data in transit

5.2.1 File system

PRISMAprepare transmits data to and from the file system:

- Open and save PDF files.
  The configuration of PRISMAprepares determines if a proof PDF file is stored on the file system or emailed to the customer.
- Open native files.
  The application automatically converts native files to PDF when the files are opened for page programming, see Automatic conversion.
  Data sources for Variable Data Printing documents are never converted. The supported data source types are: *.accdb, *.mdb, *.xlsx, *.xls and *.csv.
- Import / export the media catalogue file.
- Storage of the configuration settings (xxx), including the name and port number of the licence server and the configuration of the log level.
- Backup / restore of the configuration of PRISMAprepare.
- Storage of the automation templates for automated page programming.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Network file sharing	SMB / CIFS	TCP 445 TCP / UDP 139	Outbound	TCP 445: SMB file sharing. The implementation of the SMB protocol is OS dependent. TCP / UDP 139: NetBIOS Session Service

5.2.2 Clipboard

PRISMAprepare copies data to and from the clipboard:

- Page content, including any VDP frames, but excluding any page programming.
- Images and graphical objects.

The operator can copy / paste the data in the same PDF file. The data can also be used between multiple instances of PRISMAprepare that are running within the same Windows session.

5.2.3 Automatic conversion

PRISMAprepare can open Microsoft Office documents and documents supported by Microsoft Office. PRISMAprepare converts these documents automatically to PDF by calling the related Microsoft Office application.

5.2.4 Internal ports

1. You can change the default TCP port for preflighting if it clashes with another application. Change port “PrepareApplicationPort” in configuration file: C:\ProgramData\Oce\PRISMAcore\Configuration\PRISMAcore.Plugin.PRISMAprepare_legacy.AppSettings.config
2. You can change the default TCP port for the hot folders if it clashes with another application. Change port “HotFolderPort” in configuration file: C:\ProgramData\Oce\PRISMAcore\Configuration\PRISMAcore.Plugin.PRISMAprepare_legacy.AppSettings.configin folder

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Internal ports	Proprietary	TCP / UDP 4526 TCP 10253 TCP 10254		TCP 10253: Hot folders TCP 10254: Preflight. When executing preflight on multiple PRISMAprepare sessions, a different port is used for each session.

5.2.5 Hot folder

PRISMAprepare can process files directly from the file system using a hot folder:

- Import native files and/or PDF files.
- Export the original file, modified file and the log file to the output folder.

A PDF file, page-programmed or not, can be dropped into a hot folder from which is it automatically opened in PRISMAprepare in unattended mode. When the file is processed, the original file, the modified file and the log file are saved in the corresponding output folder.

Any folder supported by the Windows File System can be configured as a hot folder for PRISMAprepare. The input and output folders of a hot folder can also be created on network shares. The account that runs the 'Hot folders for PRISMAprepare' service must have access rights to the input and output folder, e.g. on a network share.

The 'Hot folders for PRISMAprepare' service monitors the input folder and automatically retrieves new files.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Network file sharing	SMB / CIFS	TCP 445 TCP / UDP 139	Outbound	TCP 445: SMB file sharing. The implementation of the SMB protocol is OS dependent. TCP / UDP 139: NetBIOS Session Service

5.2.6 Ultimate Bindery

PRISMAprepare can send JDF tickets to Ultimate Bindery using a hot folder. Because of security restrictions, the hot folder must be located in folder "*C:\Users\Public*\" on the PRISMAprepare computer. Ultimate Bindery monitors the hot folder and automatically retrieves any new JDF tickets.

Ultimate Bindery checks the JDF tickets against the capabilities of the finisher. You can verify the checked result in Ultimate Bindery using a web browser.

5.2.7 DPconvert

The DPconvert module can convert Xerox RDO archive files into PDF files.

A Xerox archive in RDO format can be converted into a page-programmed document by the module DPconvert. Internally, this module calls the DIX2ICA converter.
The DIX2ICA interface allows page programming specified in a DIX ticket applied onto a clean PDF document. The result is a page programmed PDF document usable in PRISMAprepare.

5.2.8 External applications

PRISMAprepare allows the operator to edit a PDF file (15) in an external application, e.g. Adobe Acrobat. The changed file is sent to PRISMAprepare again.

5.2.9 Scanned jobs via TWAIN interface

Scanned jobs can be received through the TWAIN interface.

5.2.10 Web Bootstrap

PRISMAprepare can be called on a .NET interface by the PRISMAdirect bootstrap.

- The bootstrap allows the operator of PRISMAdirect to page programme a PDF file, or to print a PDF file via PRISMAprepare.
- The bootstrap can return a page programmed PDF file to PRISMAdirect.
- A service of the PRISMAdirect bootstrap synchronizes the automation templates from PRISMAprepare to PRISMAdirect.

The web bootstrap is not part of PRISMAprepare. It is a component of PRISMAdirect that can be obtained and installed from the PRISMAdirect downloads page.
After installation, the web bootstrap handles all communication between PRISMAdirect and PRISMAprepare. See the Security White Paper of PRISMAdirect for information concerning the web bootstrap.

5.2.11 Email server

PRISMAprepare uses an email server to send proof PDF files to customers.
The configuration of PRISMAprepares determines if a proof PDF file is stored on the file system or emailed to the customer.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Email server	SMTP	TCP 25 (C)	Inbound	Data

5.2.12 PRISMAproduction

Optionally, PRISMAprepare can send jobs to PRISMAproduction using the printer driver of PRISMAproduction (xxx). The communication is one-way only. No status information is sent back from PRISMAproduction to PRISMAprepare.
Printing to PRISMAproduction is provided via PDF over JDF/JMF.

5.2.13 Printers

PRISMAprepare can send page programmed PDF files to the printers and receive status information.
PRISMAprepare can receive the printer configuration of a number of printers.

PRISMAprepare can import the media catalogue from PRISMAsync controllers and EFI controllers.

PRISMAprepare handles print related tasks using the PRISMA Core component. This component:

- Manages printers and their configuration
- Handles print jobs

The PRISMA Core is responsible for printer communication.

A print protocol must be selected for standard TCP/IP printers with a printer driver. For each printer, the print protocol can be either LPR or RAW. LPR always uses TCP 515. The default port for RAW is TCP 9100, but this port is configurable. Add a rule to the firewall depending on the selected print protocol and port.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Multi-functional printer	HTTP HTTPS SNMP SNMP JMF JMF LPR/RAW	TCP / UDP 80 TCP / UDP 443 UDP 161 UDP 162 TCP 8000 TCP 8010 TCP 515 / T9100(C)	Outbound	HTTP(S): Data to printers SNMP 161 + SNMP 162: status JMF 8000 + JMF 8010: JMF communication LPR 515: Printer port RAW 9100: Printer port

5.2.14 Océ Remote Service + Remote assistance

PRISMAprepare sends a heartbeat to Océ Remote Service (ORS) to check the connection. Upon request by the administrator, ORS pushes license and software updates to PRISMAprepare.

Remote assistance installs TeamViewer for remote customer support. TeamViewer can only be used in combination with ORS. Using TeamViewer, the support team can remotely connect to the customer computer for support and analysis. The customer must allow the remote connection in the “PRISMAprepare System Administration” console.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Océ Remote Services	HTTPS	TCP 443	Inbound	

5.2.15 Media catalogue

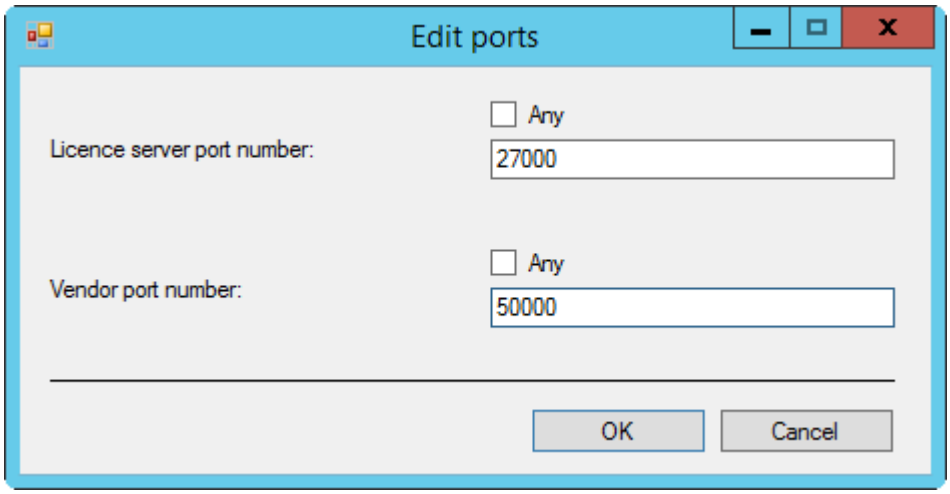
The media catalogue of PRISMAprepare can be exported to a file or to a printer.
PRISMAprepare can import the media catalogue from PRISMAsync controllers and EFI controllers.

5.2.16 License server

PRISMAprepare retrieves the license information from the remote license server via a proprietary protocol. The license information is cached on the server. Periodically, PRISMAprepare polls for any changes in the license information. The following license information is checked:

- Name
- Version
- Maximum instances

- Used instances
- Expiration date



1. The licence server port
   The licensed application uses this port number to initiate communications with the FLS. The lmgrd.exe process listens on the licence server port.
   Range: [27000 - 27009] or [ANY].
   If the port number is [ANY], the FLS uses the first available port in the range [27000 - 27009] to listen for the licensed application. The licensed application tries to connect to the FLS starting with port 27000. If the FLS does not respond, the licensed application tries the next port. When all ports in the range [27000 - 27009] are blocked or in use by other applications, the licensed application cannot connect to FLS.
2. The vendor port
   When the licensed application connects to the licence server port, it receives the vendor port number from the FLS. Then, the licensed application opens the vendor port. The ocelmgrd.exe process listens on the vendor port.
   Range: [49152 - 65535] or [ANY].
   If the port number is [ANY], the first available port in the range [49152 - 65535] is used by the FLS and the licensed application.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
License server	Proprietary	TCP 27000 –27009 (C) TCP 49152 – 65535 (C)	Inbound	